CHAPTER 5

Out-of-Band Management

This chapter describes how to configure and manage your network with the management console. Table 5-1 shows the default settings for many parameters and the menus you use to set them.

Table 5-1 Default Settings and Their Management Menus

Feature	Default Setting	Management Console Menu
Switching mode	FastForward	System Configuration
Spanning-Tree Protocol	Enabled	Spanning-Tree Configuration
Addressing security	Disabled	Port Addressing
VLAN configuration	VLAN1	VLAN Configuration
Port monitoring	Disabled	Monitoring Configuration
Flooding unknown unicast packets	Enabled	Port Addressing
Flooding unregistered multicast packets	Enabled	Port Addressing
Broadcast storm control	Disabled	System Configuration
Full duplex for Catalyst 2820 1-port 100BaseT modules or 1900 100BaseTX and 100BaseFX ports	Disabled	Port Configuration
Assign IP address to Catalyst 2820 or 1900	0.0.0.0	IP Configuration
Define trap manager	0.0.0.0	Network Management (SNMP) Configuration
Action on address violation	Suspend	System Configuration
Cisco Group Management Protocol (CGMP)	Enabled	Network Management
CDP	Enabled	Network Management
RMON	Enabled	–

Connecting the Catalyst 2820 or 1900 to a Terminal

When connected to a terminal or modem, the Catalyst 2820 and 1900 must be configured to the same baud rate and character format as the terminal or modem. Although the Match Baud Rate option (autobaud) matches the baud rate when the switch is answering an incoming call, the Catalyst 2820 and 1900 do not change from their configured rates when dialing out. Also, the Catalyst 2820 and 1900 only match a rate lower than their configured rate. When they complete a call and disconnect, they always return to the last configured baud rate.

Following are the default RS-232 characteristics for the Catalyst 2820 and 1900:

- 9600 baud
- Eight data bits
- One stop bit
- Parity: none

These characteristics can be changed using the RS-232 Port Configuration Menu. If you are using SNMP, they can be changed with the objects listed in the “RS-232 MIB (RFC 1317)” section in the “In-Band Management” chapter.

Using the Management Console

When you change switch configuration parameters with the management console, the changes take effect immediately. However, changed parameters might not be written to permanent storage for up to 30 seconds. If you turn off the switch before the new parameters are written to permanent storage, the change does not take effect.

The management console is a menu-driven system using the following other conventions:

- To select a menu, enter the letter in square brackets that precedes or follows the selection. The selected menu is displayed immediately.
- Press **Return** after entering any parameters. When pressed at the beginning of a parameter entry, **Return** cancels the attempt, and the menu redisplays.
- Enter an **X** to return to the previous menu. Enter an **X** at the Main Menu to exit the management console and return to the command prompt.

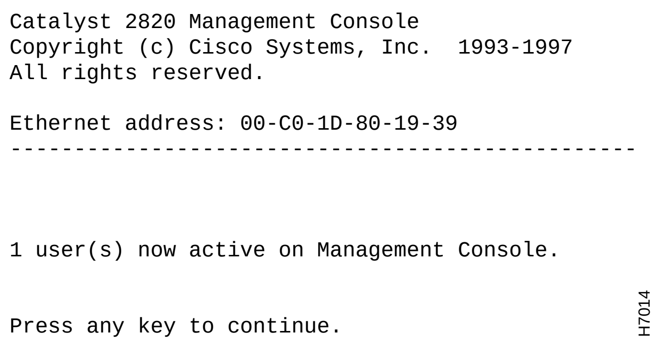
- Certain menus, such as the RS-232 Interface Configuration Menu, allow activation of the given parameters as a group.
- Menus display the current values used by the switch, except when parameters are activated as a group.
- The information you enter is not case sensitive, except when entered as a descriptive string that preserves case.
- The **Backspace** key works as expected; it erases the character previously entered. When pressed at the beginning of a parameter entry, **Backspace** causes the entry to be cleared.

You can use the management console locally or with a modem. The autobaud function can automatically match your modem settings. See the “Connecting the Catalyst 2820 or 1900 to a Terminal” section in this chapter for a description of this feature.

Logging on to the Management Console

Although you can assign a password to limit access to the management console, it is not required. Figure 5-1 shows the management console logon screen. Press **Return** to display the Main Menu.

Figure 5-1 Management Console Logon Screen



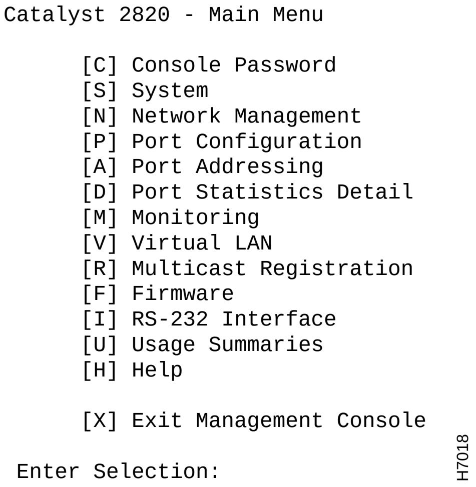
```
Catalyst 2820 Management Console
Copyright (c) Cisco Systems, Inc.  1993-1997
All rights reserved.

Ethernet address: 00-C0-1D-80-19-39
-------------------------------------------------



1 user(s) now active on Management Console.


Press any key to continue.
```

1 user(s) now active on Management Console. There can be up to seven simultaneous Telnet sessions. Changes made by one Telnet user are reflected in all other Telnet sessions. The current number of users is displayed here.

Main Menu

Select an option from the Main Menu, shown in Figure 5-2, by entering the letter in brackets next to it. You do not need to press **Return**.

Figure 5-2 Management Console Main Menu



```
Catalyst 2820 - Main Menu

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

      [X] Exit Management Console

 Enter Selection:
```

Press the **H** key to display the online help and to change the expertise level for online prompts. Press the **X** key to return to the Logon Security Menu. The other options of this menu are presented sequentially in the following sections.

Configuration Menus

The first eleven options on the Main Menu are for configuring the Catalyst 2820 or 1900.

Console Password

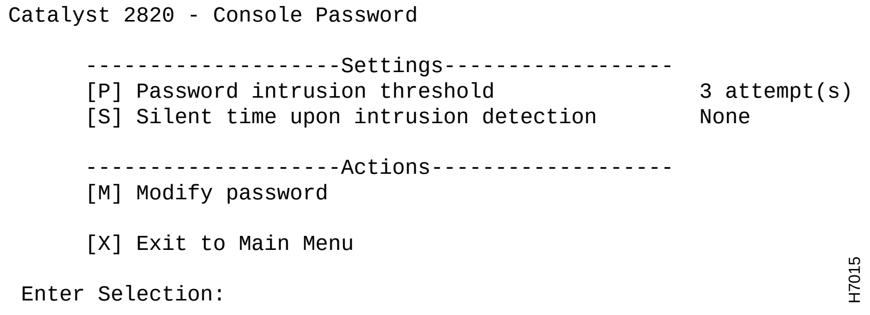
Display this menu, shown in Figure 5-3, by entering **C** on the Main Menu. Use it to change your password, set the number of password intrusions allowed, and define how long the management console remains silent after an intrusion.

If you forget your password and you are using firmware with a boot version of 1.09 or higher, you can display the factory-installed password with the Diagnostic Console described in the "Troubleshooting" chapter.

Note The boot firmware version of your switch is displayed on the Systems Engineering menu shown in Figure 7-2.

If you are using firmware with a boot version lower than 1.09, call Cisco Systems with the Ethernet address displayed on the Management Console Logon screen. You will be issued the factory-installed password for your switch. Use this password to enter the system, and then change the password using the Console Password Menu option **M**.

Figure 5-3 Console Password



```
Catalyst 2820 - Console Password

      --------------------Settings------------------
      [P] Password intrusion threshold              3 attempt(s)
      [S] Silent time upon intrusion detection      None

      --------------------Actions-------------------
      [M] Modify password

      [X] Exit to Main Menu

 Enter Selection:
```

[P] Password intrusion threshold. Enter the number of failed password attempts allowed. After this number is reached, the management console becomes quiet for a user-defined amount of time before allowing the next logon. To change the threshold value, enter the new setting next to the prompt and press **Return**.

[S] Silent time upon intrusion detection. Enter the number of minutes this management console is to wait before allowing logon after a password intrusion. You can specify from 0 to 65,500 minutes. Enter **0** for no silent time. Press **Return**.

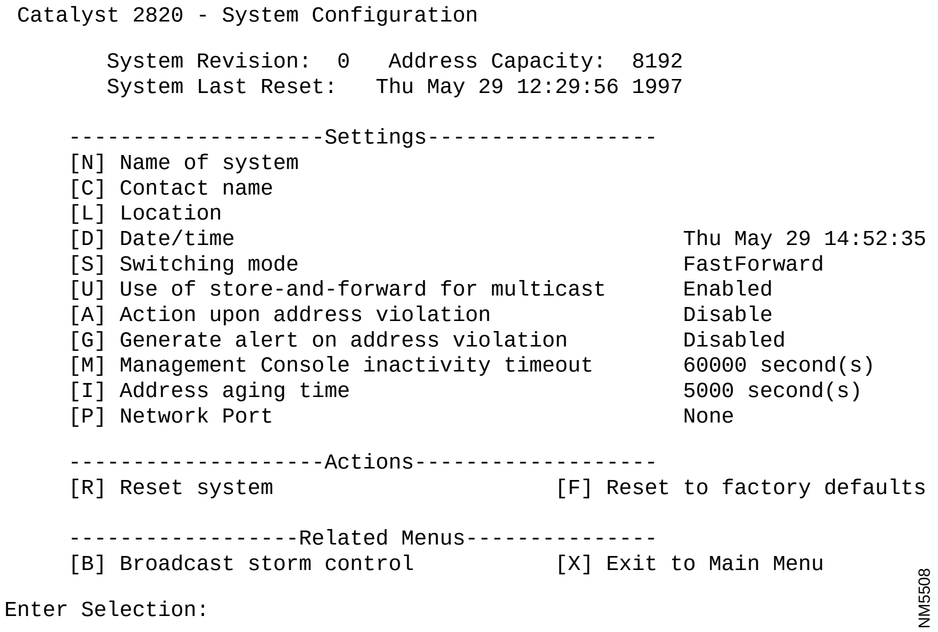
[M] Modify password. Enter a new password of four to eight characters. You can use any character found on the keyboard, but case is not considered. (If you have a current password, you have to enter it before it can be changed.) Enter the new password. Verify the password by entering it a second time and then pressing **Return**.

System Configuration

Use the System Configuration Menu, shown in Figure 5-4, to define the Catalyst 2820 and 1900 system-wide parameters and to reset the system. See the “Concepts” chapter for more details on switching modes and address violations.

Display this menu by entering **S** on the Main Menu.

Figure 5-4 System Configuration Menu



```
 Catalyst 2820 - System Configuration

        System Revision:  0   Address Capacity:  8192
        System Last Reset:   Thu May 29 12:29:56 1997

     --------------------Settings------------------
     [N] Name of system
     [C] Contact name
     [L] Location
     [D] Date/time                                Thu May 29 14:52:35 1997
     [S] Switching mode                           FastForward
     [U] Use of store-and-forward for multicast   Enabled
     [A] Action upon address violation            Disable
     [G] Generate alert on address violation      Disabled
     [M] Management Console inactivity timeout    60000 second(s)
     [I] Address aging time                       5000 second(s)
     [P] Network Port                             None

     --------------------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. Enter a name for the system of up to 255 characters and press **Return**.

[C] Contact name. Use this option to enter the name of the person or organization responsible for managing the system. Enter up to 255 characters and press **Return**.

[L] Location. The system location is an informal indication of where the Catalyst 2820 or 1900 is located. You can enter up to 255 characters. Enter the location and press **Return**.

[D] Date/time. First change the date by entering new values at the prompt and pressing **Return.** You are then prompted to enter a new time. Enter the time in the given format and press **Return**.

```
Current date/time ===> Fri Sep 24 07:21:05 1995
New date (mm-dd-yy) ===> Sat Sep 25 09:35:23 1995
New time (hh:mm:ss) ===>
```

[S] Switching mode. Set the Catalyst 2820 or 1900 switching mode to one of the three available options. Read the “Switching Modes” section in the “Concepts” chapter for a complete description of their characteristics. Enter the appropriate number and press **Return**.

[U] Use of store-and-forward for multicast. The store-and-forward switching mode is always used for broadcast frames. Enable this option to force store-and-forward mode for multicast frames. With this option set to disabled, multicast frames adhere to the switch’s configured switching mode. Enter **E** or **D** and press **Return**.

[A] Action upon address violation. Use this option to 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 will exceed its defined maximum number of addresses. Enter one of the following values at the prompt and press **Return**.

[S]uspend	The port stops forwarding until a packet with a valid source address is received.
[D]isable	The port is disabled until its status is returned to enabled by an administrator.
[I]gnore	The port status remains unchanged.

[G] Generate alert on address violation. Whether or not the Catalyst 2820 or 1900 changes the port status when an address violation occurs, it can also send an SNMP alert to a management station. Traps are sent to the IP addresses defined for the trap manager with the SNMP Management Menu. Select this option to enable or disable this feature. Enter **E** or **D** at the prompt and press **Return**.

[M] Management console inactivity time-out. Use this option to define the length of time the management console can remain idle before it times out. After a time-out, you'll need to re-enter the password to use the application. The time-out period is set in seconds; a time-out of zero means the management console will never time-out. Enter **0** or a number between 30 and 65,500 and press **Return**.

[I] Address aging time. Use this option to define the time, in seconds, after which an unused dynamic address is automatically removed. During a topology change, ports are aged more quickly by using the forward-delay parameter. When the topology stabilizes, this value again takes effect.

Possible values range from 10 to 1,000,000 seconds (about 11 1/2 days). The default is 300 seconds, or 5 minutes. This value applies to all dynamic addresses in the switch address table. Enter a value at the prompt and press **Return**.

```
Enter aging time (10 to 1000000 seconds):
Current setting ===> 300 second(s)
New setting ===>
```

[P] Network Port. Use this option to define a port to be the destination port for all packets with unknown unicast addresses. A Network Port must be the only port connected to a network. Other ports should be connected to end stations. Also, set the address aging time when using a Network Port to a value higher than the arp-cache aging time set for routers on the segment.

If you select a secure port to act as the Network Port, you are prompted to disable the security feature before continuing. Enter a port according to the conventions in the prompt and press **Return**.

[R] Reset system. Use this command to reset the switch. All configured system parameters and static addresses will be retained; all dynamic addresses will be removed. Enter **Y** or **N** and press **Return**.

[F] Reset with factory defaults. Use this option to reset the switch and return it to its factory settings. All static and dynamic addresses are removed, as is the IP address and all other configuration parameters. Enter **Y** or **N** and press **Return**.

[B] Broadcast storm control. Select this option to display the Broadcast Storm Control Menu. You can use this menu to inhibit the forwarding of broadcast packets when large numbers or *storms* of them are received by a port.

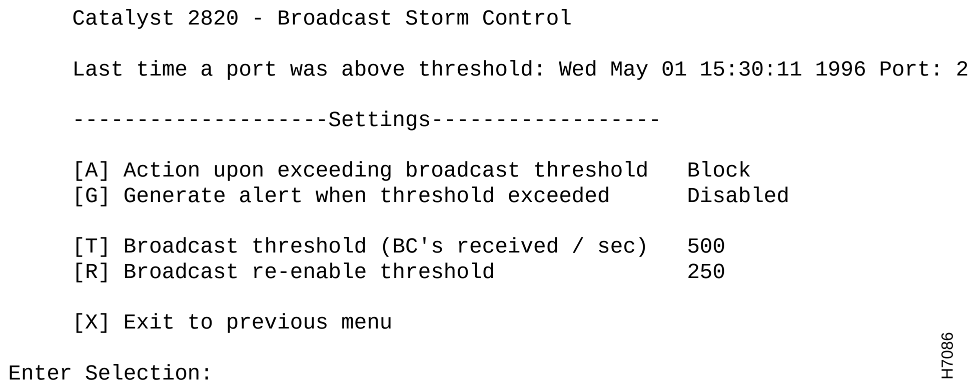
Broadcast Storm Control

A large number of broadcast packets received through a port can become a *broadcast storm* that degrades system performance and causes network time-outs. The Broadcast Storm Control Menu, shown in Figure 5-5, lets you generate SNMP alerts and inhibit the forwarding of broadcast packets when an excessive number of them arrive from a given port.

You can set a threshold of broadcast-packets-per-second as a trigger for enabling broadcast storm control. You can set a second threshold for automatically disabling broadcast storm control when the number of broadcast packets decreases.

Although it operates on a per-port basis, broadcast storm control is configured for the system as a whole. 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 2820 - Broadcast Storm Control

     Last time a port was above threshold: Wed May 01 15:30:11 1996 Port: 2

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

     [A] Action upon exceeding broadcast threshold   Block
     [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. Use this option to define the action to take when the number of broadcast packets reaches the broadcast threshold. The switch can block the broadcast storm, or it can ignore it. If you choose the block option, the switch drops all broadcast packets received from a port when the rate of broadcast packets exceeds the broadcast threshold. The switch begins forwarding again when the rate of broadcast packets received drops below the re-enabled threshold. Enter **B** (block) or **I** (ignore) at the prompt and press **Return**.

[G] Generate alert when threshold exceeded. Use this option to generate SNMP alerts when the broadcast threshold is exceeded. The alert generated is the trap broadcastStorm. A maximum of 1 trap is generated every 30 seconds. Enter **E** or **D** at the prompt and press **Return**.

[T] Broadcast threshold (BCs received / sec). Select this option to set the broadcast threshold. This measurement is the number of packets per second arriving on a port. When this threshold is exceeded, the system blocks the forwarding of packets on the port and generates an SNMP alert, if configured to do so. The default is 500 packets per second. Enter a number between 10 and 14,400 and press **Return**.

[R] Broadcast re-enabled threshold. Use this option to define when broadcast storm control is automatically disabled. Once a port has been blocked, the number of broadcast packets received from the port must drop below this re-enable threshold before packet forwarding is re-enabled. The default is 250 packets per second. Enter a number between 10 and 14,400 and press **Return**.

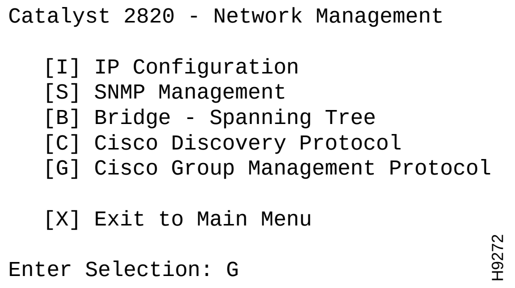
Network Management

This menu, shown in Figure 5-6, leads to menus for the following:

- IP Configuration
- SNMP Management
- Bridge and Spanning-Tree Protocol configuration
- Cisco Discovery Protocol
- Cisco Group Management Protocol

Display this menu by entering **N** on the Main Menu.

Figure 5-6 Network Management Menu



```
Catalyst 2820 - Network Management

   [I] IP Configuration
   [S] SNMP Management
   [B] Bridge - Spanning Tree
   [C] Cisco Discovery Protocol
   [G] Cisco Group Management Protocol

   [X] Exit to Main Menu

Enter Selection: G
```

[I] IP Configuration. Select this option to assign IP addresses, subnet masks, and a default gateway.

[S] SNMP Management. Select this option to display the SNMP Management Menu you use to define SNMP parameters.

[B] Bridge–Spanning-Tree. Select this option to display the Bridge–Spanning-Tree Menu.

[C] Cisco Discovery Protocol. Select this option to display the CDP Menu.

[G] Cisco Group Management Protocol. Select this option to enable the protocol.

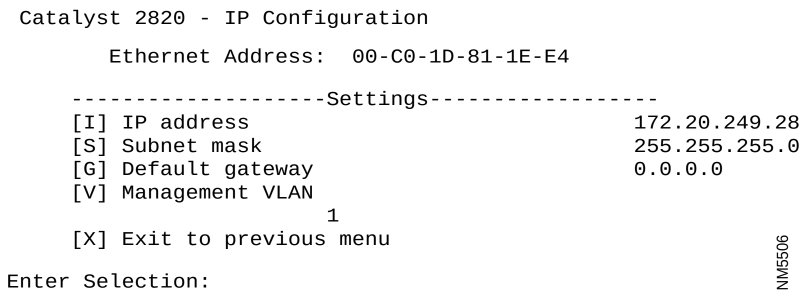
IP Configuration

Before the Catalyst 2820 and 1900 can be managed in-band, they must be configured with an IP address. Use the IP Configuration Menu, shown in Figure 5-7, to assign an IP address, or use BOOTP to assign one.

Note The first time you assign an IP address to the switch, the address takes effect immediately. When you change the IP address, however, the switch has to be reset for the IP address to take effect. To reset the switch, use the System Menu described in the section "System Configuration" of this chapter.

Display this menu by entering **N** on the Main Menu and **I** on the Network Management Menu.

Figure 5-7 IP Configuration Menu



```
 Catalyst 2820 - IP Configuration

        Ethernet Address:  00-C0-1D-81-1E-E4

     --------------------Settings------------------
     [I] IP address                                172.20.249.28
     [S] Subnet mask                               255.255.255.0
     [G] Default gateway                           0.0.0.0
     [V] Management VLAN
                         1
     [X] Exit to previous menu

Enter Selection:
```

[I] IP address. Select this option to assign the Catalyst 2820 or 1900 an IP address for in-band management. The first time you assign an IP address, it takes effect immediately. If you change the IP address, you must reset the Catalyst 2820 or 1900 before the new IP address takes effect.

[S] Subnet mask. If IP subnetting is used, use this option to enter a subnet mask for the system or management VLAN. The new value takes effect immediately. If subnetting is not used, the subnet mask is the same as the network mask. If VLAN1 does not contain all ports as member ports, you are prompted for the VLAN number and then the subnet mask. Enter the IP address and press **Return**.

```
Enter IP subnet mask in dotted quad format (nnn.nnn.nnn.nnn):
Current setting ===> 0.  0.  0.  0
New setting ===>
```

[V] Management VLAN. Use this option to assign the switch IP address to a management VLAN.

[G] Default gateway. Use this option to assign a default gateway address for SNMP management. Enter the new gateway address and press **Return**.

```
Type the address in dotted quad format(nnn.nnn.nnn.nnn):
Current setting ===> 0.  0.  0.  0
New setting ===>
```

Network Management (SNMP) Configuration

SNMP management, based on the Catalyst 2820 and 1900 Management Information Base (MIB), allows you to define management stations authorized to set configuration parameters and receive certain traps. If you have set up VLANs, each VLAN acts as a discrete bridge and contains its own bridge MIB information.

Up to four management stations can be defined to set MIB objects, and up to three stations can receive traps. If no management station is explicitly defined, any SNMP station can perform sets if the correct WRITE community string accompanies the request. Once a WRITE-manager IP address is defined, however, only explicitly defined management stations can issue set operations on the switch.

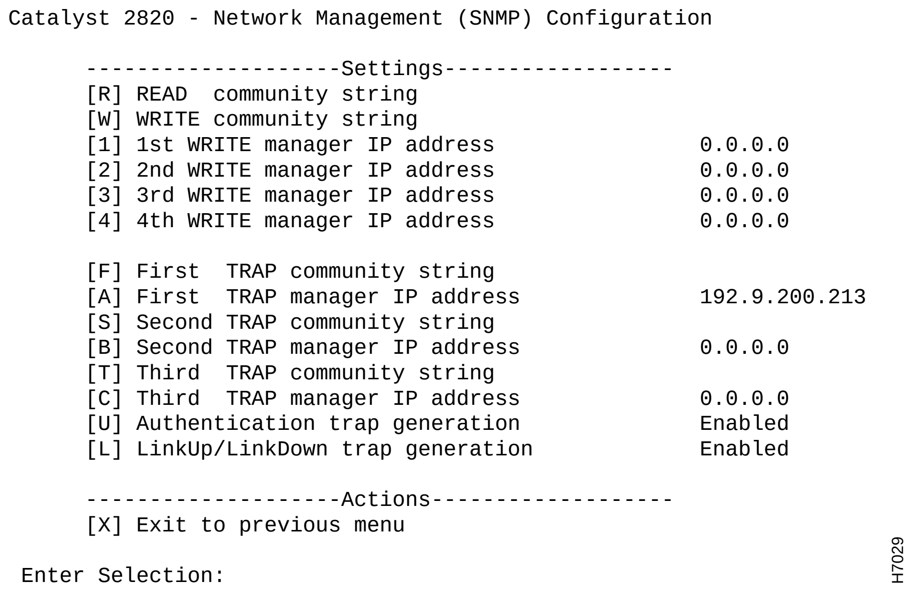
You can use this menu (shown in Figure 5-8) to enable two traps and assign the management stations to receive them. Once a management station has been assigned, it receives all traps issued by the switch, as documented in the "Trap Clients and Traps" section in the "In-Band Management" chapter. All objects in the Catalyst 2820 and 1900 MIB are documented in the *Catalyst 2820 Series and Catalyst 1900 Series MIB Reference Manual*.

Use the SNMP Management Menu to define the following:

- Which management stations can set switch MIB objects
- The READ and WRITE community strings
- Which SNMP traps are enabled and which stations receive them
- The community strings that accompany traps sent by the switch

Display this menu by entering **N** on the Main Menu and **S** on the Network Management Menu.

Figure 5-8 Network Management (SNMP) Configuration Menu



```
Catalyst 2820 - Network Management (SNMP) Configuration

      --------------------Settings------------------
      [R] READ  community string
      [W] WRITE community string
      [1] 1st WRITE manager IP address               0.0.0.0
      [2] 2nd WRITE manager IP address               0.0.0.0
      [3] 3rd WRITE manager IP address               0.0.0.0
      [4] 4th WRITE manager IP address               0.0.0.0

      [F] First  TRAP community string
      [A] First  TRAP manager IP address             192.9.200.213
      [S] Second TRAP community string
      [B] Second TRAP manager IP address             0.0.0.0
      [T] Third  TRAP community string
      [C] Third  TRAP manager IP address             0.0.0.0
      [U] Authentication trap generation             Enabled
      [L] LinkUp/LinkDown trap generation            Enabled

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

 Enter Selection:
```

[R] READ community string. Select this option to change the SNMP agent’s Get community string. The switch automatically attaches a number to the string you enter to create a unique string for each of the four possible VLANs. For example, if you enter the string FINANCE, it becomes the READ community string for VLAN1, and FINANCE2, FINANCE3, and FINANCE4 become the READ community strings for VLAN2, VLAN3, and VLAN4, respectively. Enter a string of up to 32 characters and press **Return**.

[W] WRITE community string. Select this option to define a WRITE community string for the switch. It will automatically attach a number to the string you enter to create a unique string for each of the four possible VLANs. The example for entering a READ community string applies equally here. Enter a string of up to 32 characters and press **Return**.

[1] 1st WRITE manager IP address

[2] 2nd WRITE manager IP address

[3] 3rd WRITE manager IP address

[4] 4th WRITE manager IP address

Select one of these options to define the IP address of a station authorized to issue WRITE requests to the switch. To remove an entry, enter **0. 0. 0. 0**. Enter the IP address at the following prompt and press **Return**.

```
Enter First Write Manager IP address in dotted quad format
(nnn.nnn.nnn.nnn):
Current setting ===> 0.  0.  0.  0
New setting ===>
```

[F] First TRAP community string

[A] First manager IP address

[S] Second TRAP community string

[B] Second manager IP address

[T] Third TRAP community string

[C] Third TRAP manager IP address

A trap manager, or trap client, is a management workstation configured to receive and process traps. If a trap manager has not been defined, the switch does not send any traps. Use these options to define up to three trap clients and their accompanying community strings. See the “Trap Clients and Traps” section in the ”In-Band Management” chapter for more information.

Enter **F** and a trap manager community string of up to 32 characters and press **Return**.

Enter **A** to define the IP address for the first trap manager. Enter the IP address of the station and press **Return** at the prompt:

```
Enter First Trap Manager IP address in dotted quad format nnn.nnn.nnn.nnn:
Current setting ===> 0.  0.  0.  0
New setting ===>
```

Continue with further definitions as needed.

[U] Authentication trap generation. Select this option to enable or disable 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 can be generated if no trap manager addresses have been defined. Enter **E** or **D** at the prompt and press **Return**.

[L] LinkUp/LinkDown trap generation. The Catalyst 2820 and 1900 generate the linkDown trap whenever a port changes to a suspended or disabled state due to the following:

- Spanning-Tree Protocol
- 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 enabled state due to the following:

- Presence of linkbeat
- Spanning-Tree Protocol
- Management intervention

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

Select this option to enable or disable the linkUp/linkDown trap. Enter an **E** or **D** at the prompt and press **Return**.

Once you have defined a management workstation to receive traps, the Catalyst 2820 and 1900 will generate the traps in the following list by default. These traps are described in more detail in the “Trap Clients and Traps” section in the ”In-Band Management” chapter.

- coldStart
- warmStart
- logonIntruder

- switchDiagnostic
- newRoot
- TopologyChange
- addressViolation
- broadcastStormControl
- rpsFailed

Spanning-Tree Configuration

Use this menu to display and configure the Spanning-Tree Protocol parameters defined for the switch. The menu consists of an Information section that represents parameters controlled by Spanning-Tree Protocol operation as influenced by other bridges on the network and a Settings section that defines Spanning-Tree Protocol parameters that are global to this bridge. There is also an Actions section that allows you to scroll through the VLANs, which are each considered a separate bridge by Spanning-Tree Protocol. For more information, read the “Spanning-Tree Protocol” section in the “Concepts” chapter.

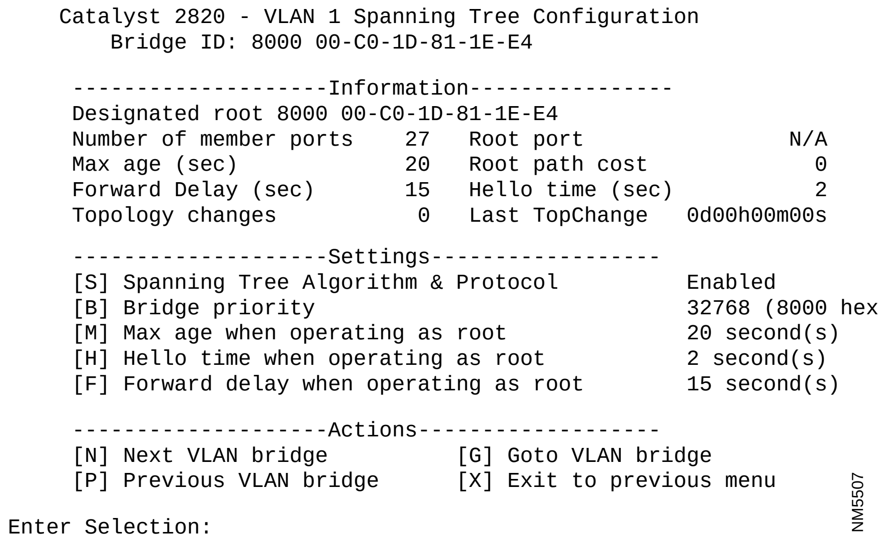
Display this menu by entering **N** on the Main Menu and **B** on the Network Management Menu. The following prompt appears if all ports do not belong to VLAN1:

```
An 802.1d Bridge is associated with a VLAN. Identify VLAN [1-4], to which
Bridge configuration applies.

Select [1-4]:
```

Enter a VLAN to display the menu shown in Figure 5-9. If no VLANs have been configured, all ports belong to VLAN1.

Note The Port Fast option bypasses several of the Spanning-Tree Protocol states and can bring a port from a disabled state directly to a forwarding state. See the “Port Configuration” section in this chapter for configuration instructions.

Figure 5-9 Spanning-Tree Configuration Menu



```
    Catalyst 2820 - VLAN 1 Spanning Tree Configuration
        Bridge ID: 8000 00-C0-1D-81-1E-E4

     --------------------Information----------------
     Designated root 8000 00-C0-1D-81-1E-E4
     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 VLAN bridge         [G] Goto VLAN bridge
     [P] Previous VLAN bridge     [X] Exit to previous menu

Enter Selection:
```

To use this menu, you need to understand the following terms:

Bridge ID — A unique identifier assigned to this bridge. This hexadecimal number consists of a bridge priority and a unique MAC address. You can change the bridge priority from this menu.

Designated root — The bridge ID of the bridge assumed to be the root by Spanning-Tree Protocol.

Root path cost — The 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.

Root port

The port on this bridge with the lowest cost path to the root bridge. It 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

The maximum time in seconds a bridge waits without receiving Spanning-Tree Protocol configuration messages before attempting a reconfiguration. This parameter takes effect when a bridge is operating as the root bridge. Bridges not acting as the root use the root bridge's Max age parameter.

Hello time

The current time interval in seconds between the transmission of Spanning-Tree Protocol configuration messages. All bridges send configuration messages during reconfiguration to elect the designated root bridge. Bridges not acting as a root bridge use the root bridge hello-time value. After the topology is stabilized, only designated bridges send configuration messages.

Forward delay

The time interval in seconds spent waiting to change a port 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.

Number of TopChanges The number of bridge topology changes experienced by this bridge. A topology change occurs as ports on this bridge change from a nonforwarding state to forwarding. A topology change also occurs when a new root is selected.

Time since last TopChange The time measured in days (d), hours (h), minutes (m), and seconds (s) since the last topology change.

[S] Spanning-Tree Algorithm and Protocol. Select this option to enable or disable the Spanning-Tree Protocol, an industry standard to ensure a loop-free configuration in the bridge topology. When Spanning-Tree Protocol is enabled, redundant ports are kept in a standby (suspended) status and are automatically enabled when needed.

This parameter applies to all VLANs.

Enter **E** or **D** at this prompt and press **Return**.

[B] Bridge priority. Select this option to force a bridge to be selected as the root bridge or as a designated bridge. The bridge priority is a value 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. Enter a value at the prompt and press **Return**.

```
Enter bridge priority value (0 to 65535)
Current setting ===> 32768 (8000 hex)
New setting ===>
```

[M] Max age when operating as root. Use this option to define the time in seconds to be used as the Max age interval when this switch becomes the root bridge. After this period expires, other bridges will notice that the root has not sent a configuration message and a new root will be selected. The default value is 20 seconds. Enter the new number at the prompt and press **Return**.

```
Enter Max Age value (6 to 40 seconds):
Current setting ===> 20 second(s)
New setting ===>
```

[H] Hello time when operating as root. Select this option to define the hello-time interval when this switch becomes the root bridge. Valid values range from 1 to 10 seconds; the default is 2 seconds. Enter the new value at the prompt and press **Return**.

```
Enter Hello time value (1 to 10 seconds):
Current setting ===> 2 second(s)
New setting ===>
```

[F] Forward delay when operating as root. Select this option to define the time in seconds to be used as the forward delay interval when this switch becomes the root bridge. Possible values are 4 to 30 seconds; the default value is 15 seconds.

Note Spanning-Tree Protocol also uses this value to accelerate address aging when the spanning tree is reconfigured. See the "Spanning-Tree Protocol" section in the "Concepts" chapter for more information.

Enter a number at the prompt and press **Return**.

```
Enter forward delay value (4 to 30 seconds):
Current setting ===> 15 second(s)
New setting ===>
```

[N] Next VLAN bridge. Use this option to scroll through the VLANs on the switch.

[P] Previous VLAN bridge. Use this option to scroll through the VLANs on the switch.

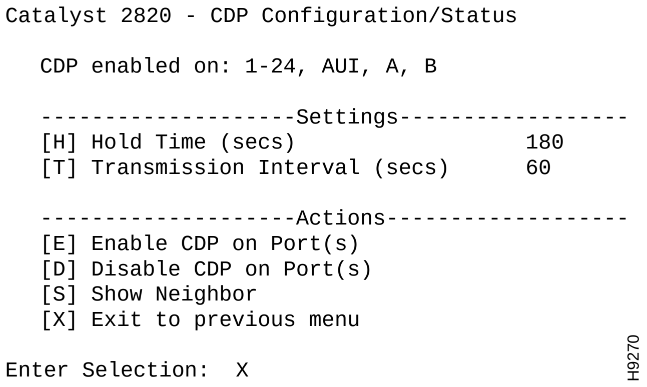
[G] Goto VLAN bridge. Use this option to enter the number of the VLAN whose parameters you want to display. Enter a number at the prompt and press **Return**.

CDP Configuration Status

Use this menu, shown in Figure 5-10, to enable CDP on some or all of the switch ports. You can also use this menu to set the timing for transmission and use of CDP messages.

To display this menu, enter **C** on the Network Management menu.

Figure 5-10 CDP Configuration/Status



```
Catalyst 2820 - 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:  X
```

[H] Hold Time. Select this option to 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 and press **Return**.

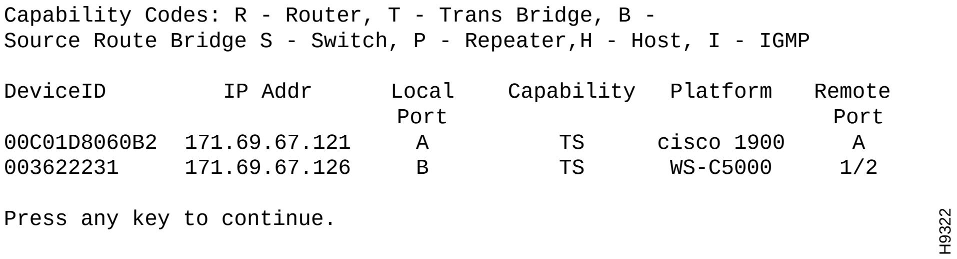
[T] Transmission Interval. Select this option to set the number of seconds between transmission of CDP messages. Enter a number between 5 and 900 and press **Return**.

[E] Enable CDP on Port(s). Select this option to enable CDP on one or more ports. You can separate the port numbers with a hyphen to create a range or use commas or spaces between port numbers. Enter the high-speed ports or expansion slots as A or 26 (left) or B or 27 (right). The word ALL creates a list of ports with all the switch ports. Enter port numbers according to these conventions and press **Return**.

[D] Disable CDP on Port(s).Select this option to disable CDP on one or more ports. Enter the port numbers according to the conventions described in the previous paragraph and press **Return**.

[S] Show Neighbor. Select this option to display the information available about neighboring devices. 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    Capability   Platform   Remote
                                Port                              Port
00C01D8060B2  171.69.67.121     A           TS      cisco 1900     A
003622231     171.69.67.126     B           TS       WS-C5000     1/2

Press any key to continue.
```

Cisco Group Management Protocol

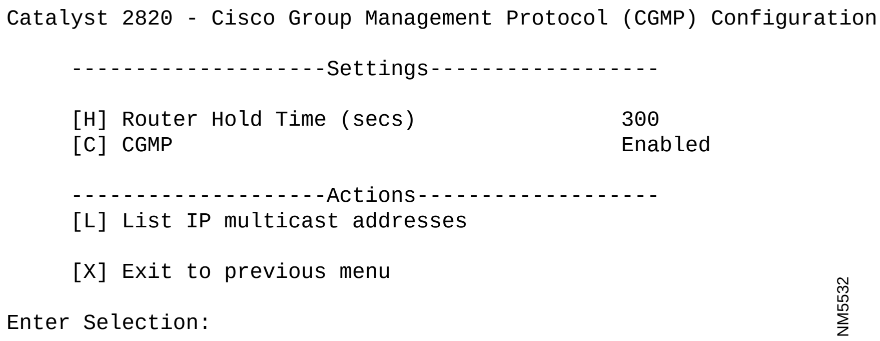
A router supporting IP multicasting can use CGMP to distribute membership of each IP multicast group to switches. As a result, CGMP-capable switches can automatically restrict the forwarding of IP multicast packets to only those ports belonging to a specific group. Multicast addresses learned through CGMP are not saved in non-volatile storage: the switch acquires the IP multicast information every time it starts up.

The IP multicast router also notifies switches to delete an IP multicast group when there are no nodes requesting the traffic of the group.

Caution All ports on the switch must belong to the same VLAN for CGMP to work properly.

Display this menu, shown in Figure 5-12, by entering **G** on the Network Management menu**.**

Figure 5-12 CGMP Configuration Menu



```
Catalyst 2820 - Cisco Group Management Protocol (CGMP) Configuration

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

     [H] Router Hold Time (secs)               300
     [C] CGMP                                  Enabled

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

     [X] Exit to previous menu

Enter Selection:
```

[H] Router Hold Time (secs). CGMP-capable routers send periodic keep alive messages. When the last CGMP-capable router goes down, the switch discards the multicast-group information from the router. Select this option to enter the number of seconds the switch is to wait for keep alive messages before deleting CGMP-learned multicast groups. Enter a number between 5 and 900 and press **Return**.

[C] CGMP. Select this option to enable or disable CGMP. Enter an **E** (enable) or a **D** (disable) at the prompt and press **Return**.

[L] List IP multicast addresses. Select this option to list the IP multicast addresses currently being managed by CGMP**.**

Monitoring Configuration

The Catalyst 2820 and 1900 enable you to route a copy of incoming and outgoing port traffic to a monitor port for analysis and troubleshooting. When a port is selected as the monitor port, it sends out only traffic seen on the ports defined in the port capture list.

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

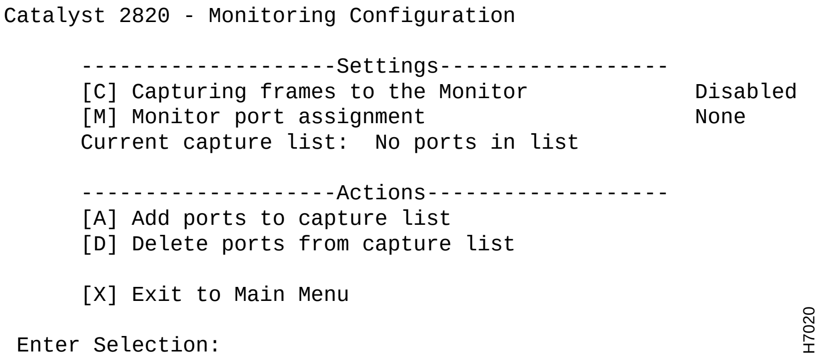
Use this menu, shown in Figure 5-13, to do the following:

- 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.

Display this menu by pressing **M** on the Main Menu.

Figure 5-13 Monitoring Configuration Menu



```
Catalyst 2820 - 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. Select this option to enable or disable frame capturing. Enter a **D** or **E** at the prompt and press **Return**.

[M] Monitor port assignment. Use this option to define the port where captured frames are to be sent. Enter a port number at the prompt and press **Return**.

[A] Add ports to capture list. Use this option to add ports to the capture list. Enter the numbers according to the example in the prompt and press **Return**.

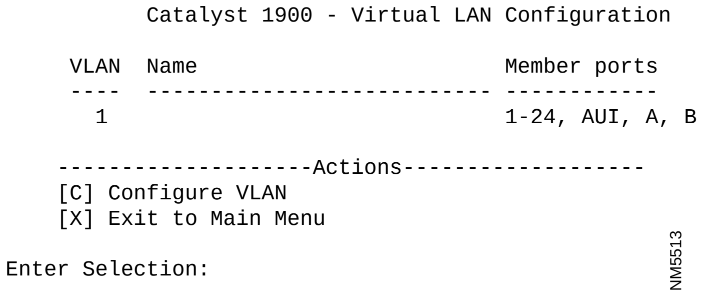
[D] Delete ports from capture list. Use this option to delete port numbers from the capture list. Enter the numbers in the list you want to delete and press **Return**.

Virtual LAN Configuration

Use this menu, shown in Figure 5-14, to list the VLANs defined for this switch and to display the VLAN Configuration Menu. See the “VLANs” section in the “Concepts” chapter for more information and several sample configurations.

Display this menu by entering **V** on the Main Menu.

Figure 5-14 Virtual LAN Menu



```
           Catalyst 1900 - Virtual LAN Configuration

     VLAN  Name                        Member ports
     ----  --------------------------- ------------
       1                               1-24, AUI, A, B

    --------------------Actions-------------------
    [C] Configure VLAN
    [X] Exit to Main Menu

Enter Selection:
```

[C] Configure VLAN. This option displays the VLAN Configuration Menu shown in Figure 5-15.

VLAN Configuration

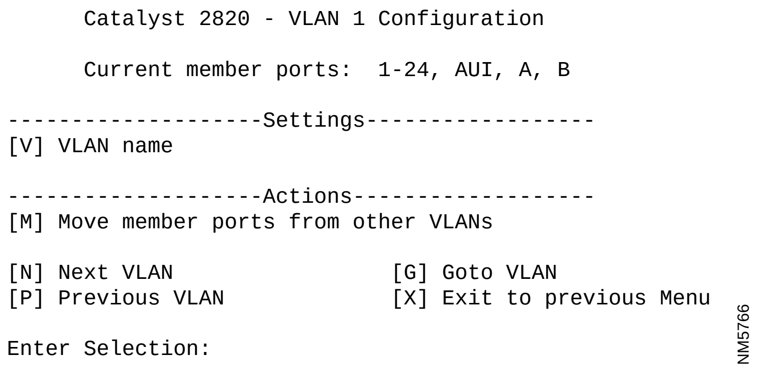
Use this menu, shown in Figure 5-15, to define up to four separate VLANs. Every port can belong to only one VLAN. The Catalyst 2820 and 1900 are shipped with all ports belonging to VLAN1; all other VLANs are empty. For more details about Catalyst 2820 and 1900 VLANs, see the “VLANs” section in the “Concepts” chapter.

Display this menu by pressing **V** on the Main Menu and **C**, Configure VLAN, on the Virtual LAN Configuration Menu. Before the menu is displayed, you are prompted for which VLAN to display:

```
Identify VLAN: [1 - 4]
Select [1 - 4]:
```

Enter the number of the VLAN you want to display and press **Return**.

Figure 5-15 VLAN Configuration Menu



```
      Catalyst 2820 - VLAN 1 Configuration

      Current member ports:  1-24, AUI, A, B

--------------------Settings------------------
[V] VLAN name

--------------------Actions-------------------
[M] Move member ports from other VLANs

[N] Next VLAN                [G] Goto VLAN
[P] Previous VLAN            [X] Exit to previous Menu

Enter Selection:
```

Note Certain conventions are used when moving ports from one VLAN to another. Use number 26 or **A** for port A, and 27 or **B** for port B. 1 to AUI are entered as **1** to **AUI**. Separate port numbers by a comma or a space. You can also enter ranges of ports, such as **5-10**.

[V] VLAN name. Select this option to enter a VLAN name of up to 60 characters. Enter the name and press **Return**.

[M] Move member ports from other VLANs. Select this option to add ports to this VLAN and remove them from their previously configured VLAN. The Catalyst 2820 and 1900 are shipped with all ports belonging to VLAN1. Enter the numbers according to the conventions described and press **Return**.

```
Example: 1, 2, 3, 8-12, A

Enter port numbers:
```

[N] Next VLAN. Select this option to scroll through the available VLANs.

[P] Previous VLAN. Select this option to scroll through the available VLANs.

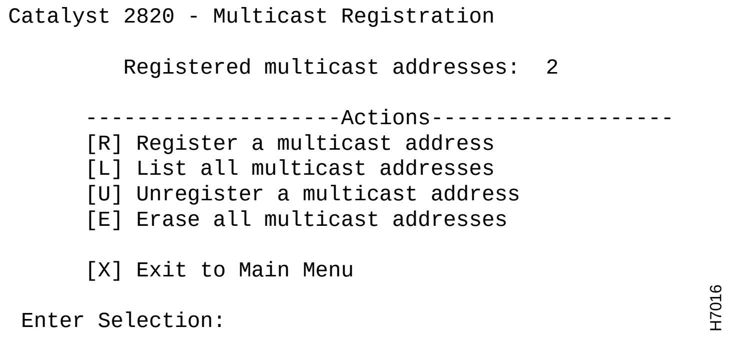
[G] Goto VLAN. Select this option to enter a VLAN to display. Enter a number at the prompt and press **Return**.

Multicast Registration

By default, all multicast frames are forwarded to all ports in a VLAN. You can, however, register multicast addresses so that they are sent to only the ports you define. Because these packets are then *not* forwarded to other ports, this reduces the amount of flooding performed by the switch. For more information on this feature, see the “Multicast Registration and Filtering” section in the “Concepts” chapter.

Display this menu by pressing **R** on the Main Menu. The first line of the menu, shown in Figure 5-16, displays the number of registered multicast addresses.

Figure 5-16 Multicast Registration Menu



```
Catalyst 2820 - Multicast Registration

         Registered multicast addresses:  2

      --------------------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. Select this option to register a multicast address. You are prompted for both the address and the ports to which frames destined for this address are to be forwarded.

If you are using CGMP to learn IP multicast groups from routers, do not manually register IP multicast addresses.

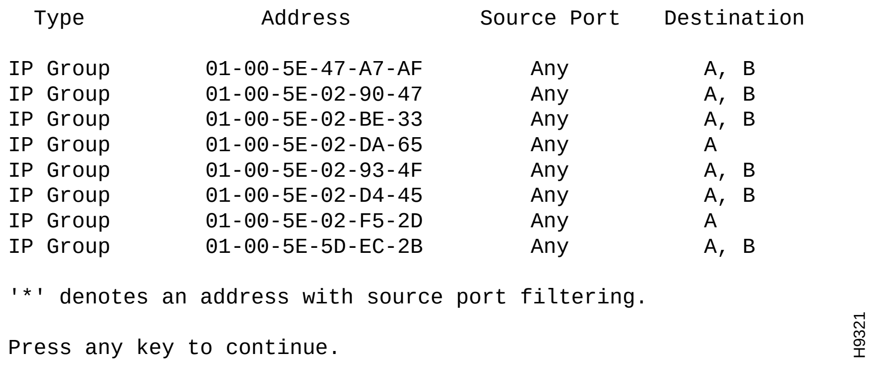
If you enter an invalid multicast address, the prompt refreshes itself so you can try again. Invalid addresses include non-multicast addresses, the broadcast address, and reserved multicast addresses, such as those used for Spanning-Tree Protocol.

When you enter a valid address, the following prompt is displayed:

```
Enter the destination port numbers (separated by commas or spaces)
e.g. 2,3,6,7,12

Default ports ===> All ports

    New ports ===>
```

Enter the port numbers and press **Return**. Typing errors cause the prompt to be refreshed.

[L] List all registered multicast addresses. Use this option to 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. Note that the list also shows whether the address is part of an IP multicast group as defined by CGMP, as in this example:



```
  Type              Address          Source Port   Destination

IP Group       01-00-5E-47-A7-AF        Any           A, B
IP Group       01-00-5E-02-90-47        Any           A, B
IP Group       01-00-5E-02-BE-33        Any           A, B
IP Group       01-00-5E-02-DA-65        Any           A
IP Group       01-00-5E-02-93-4F        Any           A, B
IP Group       01-00-5E-02-D4-45        Any           A, B
IP Group       01-00-5E-02-F5-2D        Any           A
IP Group       01-00-5E-5D-EC-2B        Any           A, B

'*' denotes an address with source port filtering.

Press any key to continue.
```

See the “Flooding Controls” section in the “Concepts” chapter for more information.

[U] Unregister a multicast address. Select this option to delete registered multicast addresses. You cannot delete those multicast addresses that are not considered registered.

If you delete an IP group address, CGMP deletes the members of the group. Packets destined for the IP group address are flooded. The switch reestablishes the IP group only when it receives a message from a CGMP-capable router. Enter the address at the prompt and press **Return**.

[E] Erase all registered multicast addresses. Select this option to remove all registered multicast addresses. Press **Y** at the prompt.

Port Configuration

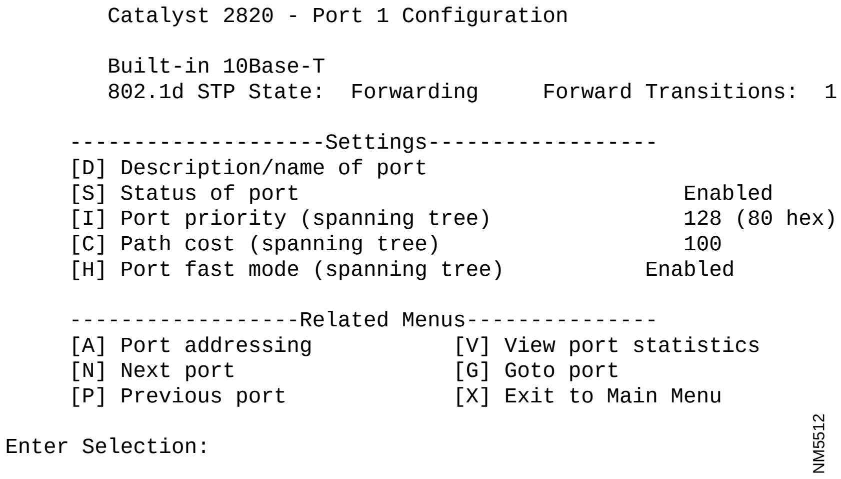
Use this menu, shown in Figure 5-17, to display the status of a port or module, enter a port description, change the port status, and define various Spanning-Tree Protocol parameters.

Display this menu by pressing **P** on the Main Menu. The following prompt is displayed:

```
Identify port: 1 to 24, AUI,[A1],[B1]
Select [1 - 24, AUI, A1, B1]:
```

The menu displayed varies, depending on whether it is a 10BaseT port or an expansion slot with a 100BaseTX, 100BaseFX, or FDDI module installed.

Figure 5-17 Port Configuration Menu



```
        Catalyst 2820 - Port 1 Configuration

        Built-in 10Base-T
        802.1d STP State:  Forwarding     Forward Transitions:  1

     --------------------Settings------------------
     [D] Description/name of port
     [S] Status of port                              Enabled
     [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:
```

The following terms are used to describe the STP status of the port:

802.1d STP State
The current Spanning-Tree Protocol state, as follows:

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.

Forward Transitions
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. Select this option to assign a name to the port. This could be **Engineering Segment** or any 60-character string. Enter the port name at the prompt and press **Return**.

[S] Status of port. Select this option to enable a disabled port or disable a port in an operational state. If the port is an expansion slot with a multiport repeater, you can use this option to enable or disable one repeater port while leaving the others unaffected. To enable or disable all ports of a module, use the module status parameter. The operational states a port can have are listed under the next menu option, Module status. Enter **E** or **D** at the prompt and press **Return**.

[M] Module status. (Catalyst 2820 only) Select this option to enable a module that has been disabled or to disable a module that is currently in an enabled operational state. If the module is a multiport repeater, this parameter affects all the repeater ports. Attempts to enable a module that is disabled due to a hardware failure will not succeed, and the module will automatically return to a disabled state. Enter **E** or **D** at the prompt and press **Return**.

The status indication shown on this menu is one of the following:

Enabled	Normal operation. Port can transmit and receive.
Disabled-mgmt	Disabled by explicit management action.
Suspended-linkbeat	Suspended due to the absence of a linkbeat. This is usually due to the attached station being disconnected or powered-down.
Suspended-jabber	Suspended because attached station is jabbering.
Suspended-violation	Suspended due to address violation.
Suspended-ring-down	Port is not connected to a ring or the ring is in the process of configuring (FDDI only).
Suspended-Spanning-Tree Protocol	Spanning-Tree Protocol not forwarding.
Suspended-not-present	No module in the expansion slot.
Suspended-not-recognized	Unrecognized module inserted in the expansion slot.
Disabled-self-test	Disabled because port failed self-test.
Disabled-violation	Disabled due to address violation.
Reset	Port is currently in the reset state.

[F] Full duplex. Select this option to enable or disable full-duplex transmission on 100-Mbps ports. Full duplex is simultaneous 100-Mbps transmission in both directions, yielding an aggregate bandwidth of 200 Mbps. As both ends must be configured for full duplex, the port cannot be connected to a repeater. A likely scenario would be to connect a

100BaseTX port or 100BaseFX 1-port module to a server with a 100BaseTX adapter configured for full duplex. You could also connect it to another Catalyst 2820 or 1900 or other 100BaseT switch or router configured for full-duplex operation. Enter an **E** or a **D** at the prompt and press **Return**.

Note On the Catalyst 2820, full-duplex operation cannot be enabled for a multiport 100BaseTX or for 100BaseFX modules.

[I] Port priority. Select this option to define which port is to remain enabled by Spanning-Tree Protocol if two ports form a loop. Enter a number from 0 to 255 and press **Return**.

[C] Path cost. Select this option to define the Spanning-Tree Protocol path cost of the port. It is inversely proportional to the LAN speed of the network interface at the port. A high path cost means the port has low bandwidth and should not be used if possible.The default is 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 at the prompt and press **Return**.

[H] Port fast mode. Select this option to accelerate the time it takes for Spanning-Tree Protocol to bring a port into the forwarding state. Enter an **E** or **D** at the prompt and press **Return**.

[A] Port addressing. Select this option to display the Port Addressing Menu.

[V] View port statistics. Select this option to display the Detailed Port Statistics Menu.

FDDI Port Configuration

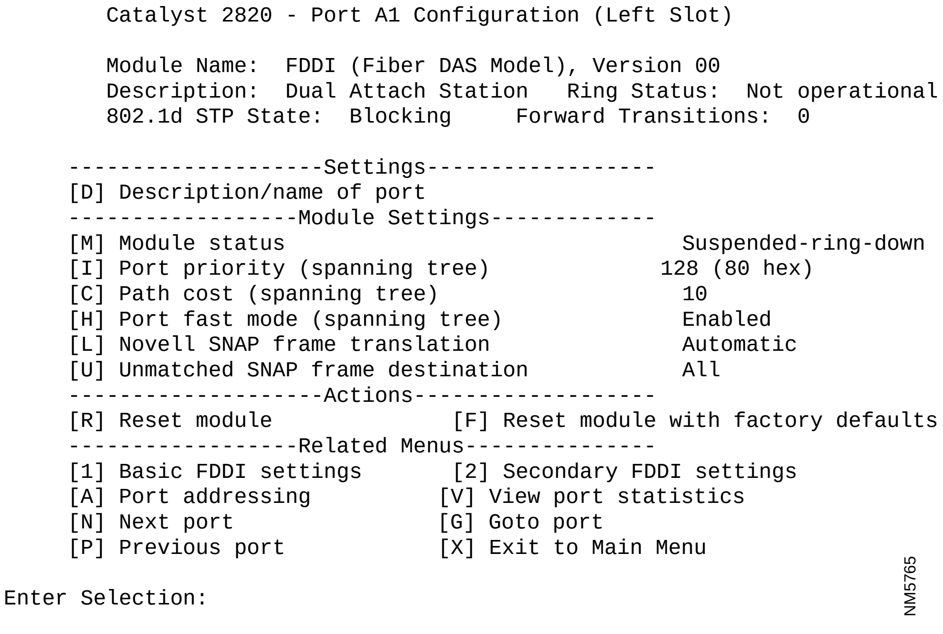
The following options are available for FDDI modules and are in addition to the other port configuration menu options discussed in the “Port Configuration” section in this chapter.

Display this menu, shown in Figure 5-18, by pressing **P** on the Main Menu and the letter (A or B) of an expansion slot containing a Catalyst 2820 FDDI module.

Ring Status. This field indicates whether the module is successfully attached to the ring or not. The two possible values are *operational* and *non-operational*.

[L] Novell SNAP frame translation. Use this option to define how you want to translate Novell SNAP FDDI frames. For more information about the translation options, refer to the *Catalyst 2820 Modules User Guide*. Enter the number associated with your choice at the prompt and press **Return**.

Figure 5-18 Port Configuration for FDDI Menu



```
        Catalyst 2820 - Port A1 Configuration (Left Slot)

        Module Name:  FDDI (Fiber DAS Model), Version 00
        Description:  Dual Attach Station   Ring Status:  Not operational
        802.1d STP State:  Blocking     Forward Transitions:  0

     --------------------Settings------------------
     [D] Description/name of port
     ------------------Module Settings-------------
     [M] Module status                               Suspended-ring-down
     [I] Port priority (spanning tree)             128 (80 hex)
     [C] Path cost (spanning tree)                   10
     [H] Port fast mode (spanning tree)              Enabled
     [L] Novell SNAP frame translation               Automatic
     [U] Unmatched SNAP frame destination            All
     --------------------Actions-------------------
     [R] Reset module              [F] Reset module with factory defaults
     ------------------Related Menus---------------
     [1] Basic FDDI settings       [2] Secondary FDDI settings
     [A] Port addressing          [V] View port statistics
     [N] Next port                [G] Goto port
     [P] Previous port            [X] Exit to Main Menu

Enter Selection:
```

[U] Unmatched SNAP frame destination. This option appears only when the you have selected Automatic as the SNAP translation format. You use it to select which FDDI-to-Ethernet translation to use for packets whose destinations cannot be determined from the Novell SNAP translation table. Enter the number associated with your choice at the prompt and press **Return**.

[R] Reset FDDI module. Use this option to reset the FDDI module. Enter **Y** or **N** at the prompt and press **Return**.

[F] Reset FDDI with factory defaults. Select this option to restore the factory default settings on the FDDI module. The module will be reset, and the new settings take effect immediately. Enter **Y** or **N** at the prompt and press **Return**.

[1] Basic FDDI settings. Display the Basic FDDI Settings Menu described in the "Basic FDDI Settings" section in this chapter.

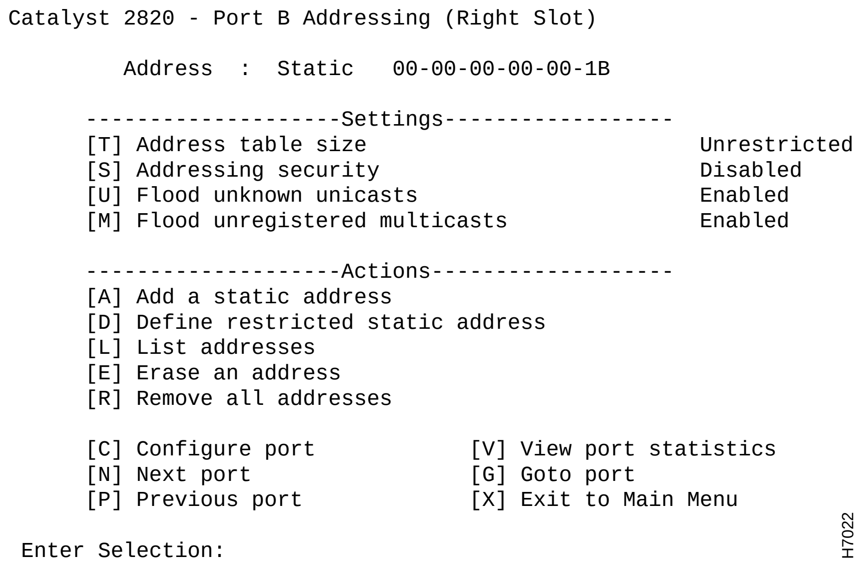
[2] Secondary FDDI settings. Display the Secondary FDDI Menu described in the "Secondary FDDI Settings" section in this chapter.

Port Addressing

Use this menu to configure address security of a port and define static unicast and multicast addresses. You can use this menu to 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. For more information on these features, see the "Flooding Controls" section in the "Concepts" chapter.

Display this menu, shown in Figure 5-19, by pressing **A** on the Main Menu and then entering the port number at the prompt.

Figure 5-19 Port Addressing Menu



```
Catalyst 2820 - Port B Addressing (Right Slot)

         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.

[T] Address Table Size. Select this option to define the size of the address table for a secured port. Enter a number between 1 and 132 at the prompt and press **Return**.

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

[S] Addressing security. Select this option to secure a port. 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 in the “Concepts” chapter for more information. Enter an **E** or **D** at the prompt and press **Return**.

[U] Flood unknown unicasts. When a frame with an unrecognized unicast destination address is received on any port, the default action is to forward the packet to all enabled ports. Select this option to inhibit the forwarding of unknown unicasts to this port. Enter **E** or **D** at the prompt and press **Return**.

[M] Flood unregistered multicasts. When a frame with an unregistered multicast destination address is received on any port, the default action is to forward the packet to all enabled ports. Select this option to inhibit the forwarding of unregistered multicast addresses to this port. Enter **E** or **D** at the prompt and press **Return**.

[A] Add a static address. If there is room in the port’s address table, you can use this option to add a static unicast address to it. Enter a unicast address and press **Return**. If the address table is already full, an error message is generated. You can change the size of the address table with this menu’s option **[T] Address Table Size**.

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

You are then prompted for the port numbers allowed to send to this address. Enter the port numbers at the prompt and press **Return**. The switch checks the list of ports for typing errors and, if there are any, redisplays the prompt.

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

[E] Erase an address. Use this option to erase a dynamic or static address assigned to the current port. Enter the address at the prompt and press **Return**.

[R] Remove all addresses. Select this option to remove all dynamic and static addresses currently associated with the port. Enter **Y** or **N** at the confirmation prompt and press **Return**.

[C] Configure port. Select this option to display the Port Menu.

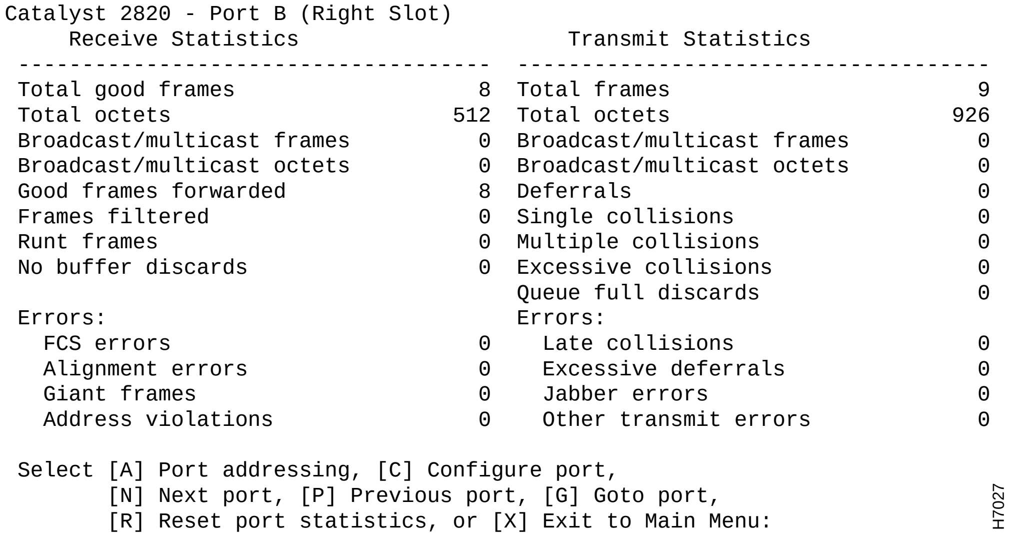
[V] View port statistics. Select this option to display the Detailed Port Statistics Menu.

Port Statistics Report

This display-only menu shows frame transmit and receive statistics captured by the switch. The statistics and errors can be displayed for all ports on a per-port basis and can vary if a Catalyst 2820 module is installed. Figure 5-20 is a statistics report for an installed 100BaseT module. Figure 5-21 is a statistics report for an installed FDDI module. Statistics are automatically updated every 5 seconds if you are using VT100 emulation.

Display the menu by pressing **D** on the Main Menu or **V** on the Port Configuration Menu or Port Addressing Menu.

Figure 5-20 Detailed Port Statistics Report

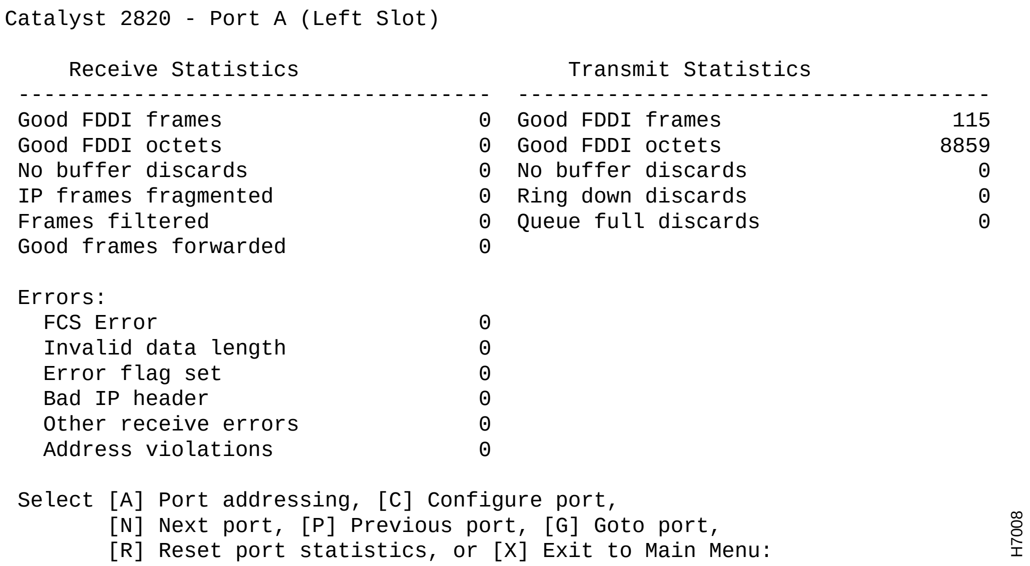


```
Catalyst 2820 - Port B (Right Slot)
     Receive Statistics                     Transmit Statistics
 -------------------------------------  -------------------------------------
 Total good frames                   8  Total frames                        9
 Total octets                      512  Total octets                      926
 Broadcast/multicast frames          0  Broadcast/multicast frames          0
 Broadcast/multicast octets          0  Broadcast/multicast octets          0
 Good frames forwarded               8  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:
```

Performance or connectivity problems could be evident in the port statistics, particularly those under the heading Errors. For example, FCS and alignment errors could be the result of cabling problems such as the following:

- Exceeding the cabling-distance specifications
- Split pairs
- Defective patch-panel ports
- Wrong cable type
- Misconfigured full-duplex connection

Figure 5-21 Detailed FDDI Port Statistics



```
Catalyst 2820 - Port A (Left Slot)

     Receive Statistics                       Transmit Statistics
 -------------------------------------  -------------------------------------
 Good FDDI frames                    0  Good FDDI frames                  115
 Good FDDI octets                    0  Good FDDI octets                 8859
 No buffer discards                  0  No buffer discards                  0
 IP frames fragmented                0  Ring down discards                  0
 Frames filtered                     0  Queue full discards                 0
 Good frames forwarded               0

 Errors:
   FCS Error                         0
   Invalid data length               0
   Error flag set                    0
   Bad IP header                     0
   Other receive errors              0
   Address violations                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:
```

For more information on responding to the errors found here, see the “Troubleshooting” chapter. The following definitions of the types of errors found on this menu are taken from RFC 1398:

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.

Invalid data length (FDDI) — FDDI packets that have not been completely received.

Error flag set (FDDI) — The E indicator of the FDDI frame status has been set.

Bad IP header (FDDI)	Bad data in the IP header.
Giant frames	A count of frames received on a particular interface that exceeds 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] Port configuration. Display the Port Menu.

[R] Reset port statistics. Select this option to clear this port's statistics. Enter **Y** at the prompt and press **Return**.

To update the screen press the **Spacebar.**

Firmware Configuration

Use this menu to display the firmware version currently used by the switch and to perform firmware upgrades. You can also upgrade the firmware for Catalyst 2820 FDDI modules and download diagnostic software for use by customer support. The version number of the currently executing firmware and the size of the system's Flash memory is displayed under System Information. If there is a firmware upgrade in progress, its status is displayed in the Upgrade status field.

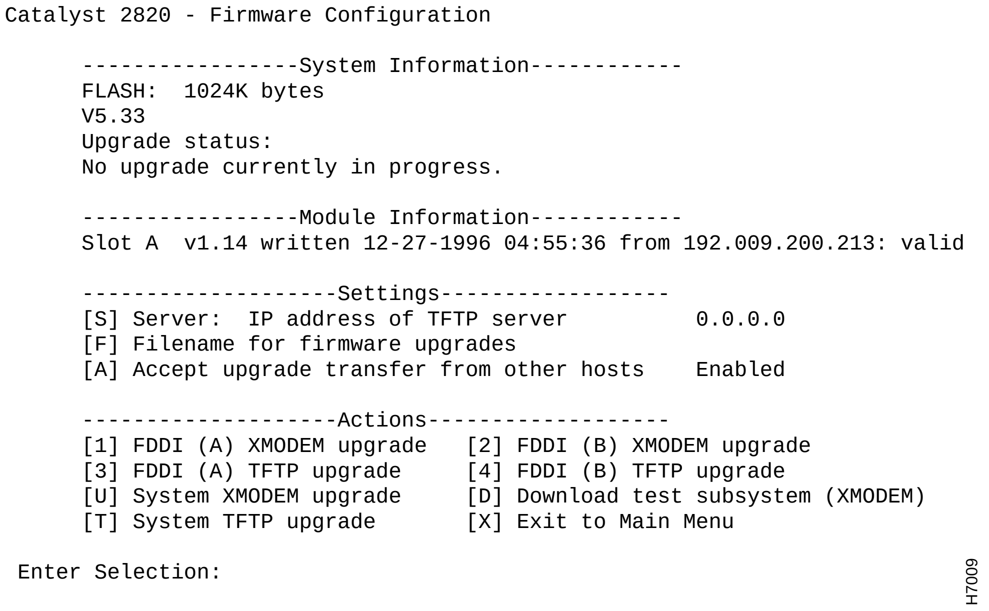
Note It is important to note that firmware for the FDDI modules is different from the switch firmware. If you upgrade the firmware for your Catalyst 2820, it has no effect on an installed FDDI module. In the same way, upgrading the FDDI module firmware leaves the switch firmware unchanged.

You upgrade Catalyst 2820 and 1900 firmware by first downloading an upgrade file into a temporary area. After it is validated by the existing firmware, the new image is transferred into Flash memory, the switch resets, and the new firmware begins executing immediately. If the upgrade file is invalid, the temporary image is discarded, the existing firmware continues to execute, and the firmware upgrade ends.

Caution During the transfer of the upgrade file, the switch might not respond to commands for as long as 1 minute. This is normal and correct. If you interrupt the transfer by turning the switch off and on, the firmware could be corrupted. If this happens, follow the procedure described in the "Diagnostic Console Recovery Procedures" section in the "Troubleshooting" chapter to restart the firmware.

Display this menu, shown in Figure 5-22, by pressing **F** on the Main Menu.

Figure 5-22 Firmware Configuration Menu



```
Catalyst 2820 - Firmware Configuration

      -----------------System Information------------
      FLASH:  1024K bytes
      V5.33
      Upgrade status:
      No upgrade currently in progress.

      -----------------Module Information------------
      Slot A  v1.14 written 12-27-1996 04:55:36 from 192.009.200.213: valid

      --------------------Settings------------------
      [S] Server:  IP address of TFTP server          0.0.0.0
      [F] Filename for firmware upgrades
      [A] Accept upgrade transfer from other hosts    Enabled

      --------------------Actions-------------------
      [1] FDDI (A) XMODEM upgrade   [2] FDDI (B) XMODEM upgrade
      [3] FDDI (A) TFTP upgrade     [4] FDDI (B) TFTP upgrade
      [U] System XMODEM upgrade     [D] Download test subsystem (XMODEM)
      [T] System TFTP upgrade       [X] Exit to Main Menu

 Enter Selection:
```

How you upgrade the firmware depends on your installation. There are three possibilities:

- From a TFTP server

  Before the upgrade can be performed, you need to enter the name of the TFTP server and the name of the file containing the upgrade. The actual upgrade can be initiated through the management console or with any SNMP-compatible management station. As a result, the switch retrieves the upgrade file from the server via TFTP.

- From a TFTP client

  A TFTP client can put the firmware upgrade into the switch.

- With the XMODEM protocol

  Use a terminal attached to the RS-232 port at the back of the switch to transfer the firmware via the XMODEM protocol.

Upgrading Catalyst 2820 and 1900 Firmware with a TFTP Server

Step 1 Select option **S** and enter the IP address of the server where the upgrade file is located.

Step 2 Select option **F** and enter the name of the firmware-upgrade file.

Step 3 Make sure the switch can reach the TFTP server. Select option **T** to initiate the TFTP transfer; the switch contacts the server to get the upgrade file.

Step 4 Verify the upgrade is in progress by checking the System Information section of the Firmware Upgrade Menu. During the transfer, the switch does not respond to commands for about 1 minute.

Step 5 When the transfer is complete, the switch resets and begins using the new firmware.

Note You can also initiate a TFTP transfer by setting the MIB object upgradeTFTPInitiate. This object is described in the *Catalyst 2820 Series and Catalyst 1900 Series MIB Reference Manual.*

Upgrading Catalyst 2820 and 1900 Firmware with a TFTP Client

Step 1 On 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 At the command line enter **put** and the filename.

Step 4 Verify the upgrade is in progress by checking the System Information section of the Firmware Upgrade Menu. During the transfer, the switch does not respond to commands for about one minute.

Step 5 When the transfer is complete, the switch resets and begins using the new firmware.

Upgrading Catalyst 2820 and 1900 Firmware with XMODEM

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

Step 1 Select option **U**.

Step 2 When the first XMODEM request appears, use the appropriate command to start the transfer. After the transfer, the switch does not respond to commands for about one minute.

Step 3 The switch resets after a successful transfer, the newly downloaded firmware begins to reset, and the Logon Security Menu is displayed.

Upgrading FDDI Firmware with a TFTP Server

This procedure is for upgrading the FDDI module firmware, *not* the switch firmware.

The options you use in this procedure depend on the expansion slot containing the Catalyst 2820 FDDI module.

Step 1 Select option **S** and enter the IP address of the server where the FDDI upgrade file is located.

Step 2 Select option **F** and enter the name of the firmware-upgrade file.

Step 3 Select option **3** (for the A slot) or **4** (for the B slot) to initiate the TFTP transfer; the switch contacts the server to get the upgrade file.

Upgrading FDDI Firmware with a TFTP Client

The following procedure is for upgrading the FDDI module firmware, *not* the switch firmware.

Step 1 On 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 At the command line, enter **put** and the filename. If there are two FDDI modules installed, the following rules apply:

- If the firmware in one of the FDDI modules is invalid, it is automatically upgraded.
- If the upgrade firmware has a higher version number than the firmware in slot A, then upgrade slot A.
- If slot A firmware has the same or a higher version number, then upgrade slot B.

Step 4 Verify the upgrade is in progress by checking the System Information section of the Firmware Upgrade Menu. If the upgrade is in progress, the field reads: `in-progress.`

Step 5 When the transfer is complete, the FDDI module resets and begins using the new firmware.

Upgrading FDDI Firmware with XMODEM

The following procedure is for upgrading the FDDI module firmware, *not* the switch firmware. It is dependent on the modem software you're using.

Step 1 Select option **1** for expansion slot A or **2** for expansion slot B.

Step 2 When the first XMODEM request appears, use the appropriate command to start the transfer.

Step 3 FDDI resets after a successful transfer.

[S] Server: IP address or 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**. The file should be on a TFTP server.

[A] Accept upgrade transfer from other hosts. You have the option of accepting upgrades from TFTP clients on the network. Use this option to enable or disable this function and press **Return**.

[1] FDDI (A) XMODEM upgrade. Start an XMODEM upgrade of the FDDI firmware in expansion slot A. The complete procedure is described in the section “Upgrading FDDI Firmware with XMODEM.”

[2] FDDI (B) XMODEM upgrade. Start an XMODEM upgrade of the FDDI firmware in expansion slot B. The complete procedure is described in the section “Upgrading FDDI Firmware with XMODEM.”

[3] FDDI (A) TFTP upgrade. Initiate a TFTP transfer of FDDI firmware to slot A. The complete procedure is described in the section “Upgrading FDDI Firmware with a TFTP Server.”

[4] FDDI (B) TFTP upgrade. Initiate a TFTP transfer of FDDI firmware to slot B. The complete procedure is described in the section “Upgrading FDDI Firmware with a TFTP Server.”

[U] System XMODEM upgrade. Select this option to upgrade the firmware using a modem. Enter **N** to return to the Firmware Upgrade Menu or **Y** to begin the transfer. 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 transfer. Upon completion of the transfer, the switch resets and the newly downloaded firmware begins to execute. The Logon Security Menu is displayed.

[T] System TFTP upgrade. Use this option to upgrade the firmware from a TFTP server. The address of the server and the name of the file must already be set.

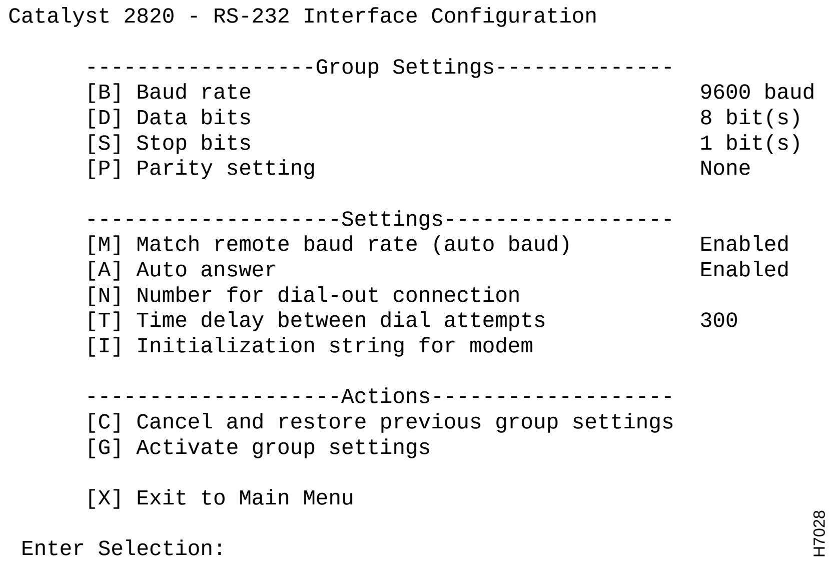
[D] Download test subsystem (XMODEM). This option is reserved for use by the customer support group and is used to download diagnostic software.

RS-232 Interface Configuration

Use this menu, shown in Figure 5-23, to define the physical characteristics of the RS-232 port—baud rate, stop bits, and the like—and call-features such as the time delay between outgoing calls. Note that 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 return to the previous settings.

Display this menu by pressing **I** on the Main Menu.

Figure 5-23 RS-232 Port Configuration Menu



```
Catalyst 2820 - 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:
```

[B] Baud rate. Enter the baud rate of the RS-232 serial port and press **Return**.

[D] Data bits. Enter the data bits value for the serial port and press **Return**. Valid values are 7 and 8.

[S] Stop bits. Enter the stop bits value for the serial port and press **Return**.

[P] Parity settings. Change the parity settings for the serial port and press **Return**.

[M] Match remote baud rate. Select this feature to enable the RS-232 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.

[A] Auto answer. Select this feature to enable the auto-answer feature. Enter **E** or **D** at the prompt and press **Return**.

[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.

Up to 48 characters can be entered. Use the **Backspace** followed by **Return** to delete the number. Using the format required by your modem, enter the number at the prompt and press **Return**.

[T] Time delay between attempts. Enter the amount of time in seconds between dial-out attempts and press **Return**. Zero disables retry.

[I] Initialization string for modem. Change the initialization string to match your modem requirements. Up to 48 characters can be entered. Enter the new string at the prompt and press **Return**.

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

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

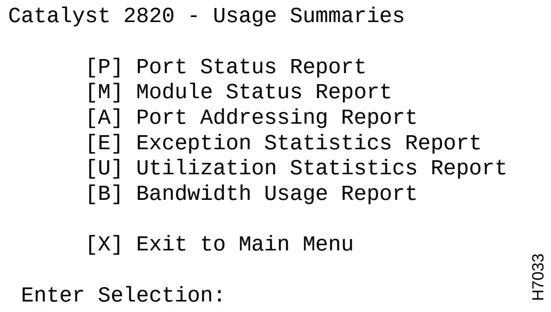
[G] Activate group settings. This option activates the setting you have entered for baud rate, data bits, stops bits, and parity settings. After selecting this option, configure the attached terminal to match the new settings. Enter **Y** or **N** at the prompt and press **Return**.

Usage Summaries

This section describes statistics generated by the Catalyst 2820 and 1900 Management Console. If you are using VT100 terminal emulation, the screens displaying the statistics are refreshed every 5 seconds. If you are connected to the Management Console via a modem running at less than 2400 baud, the screens displaying the statistics are refreshed every 8 seconds.

Use this menu, shown in Figure 5-24, to display network statistics in the form of summary displays showing all ports. Press **U** on the Main Menu to display this menu. These statistics are read only; press **Return** or the **Spacebar** to refresh them at any time.

Figure 5-24 Usage Summary Menu



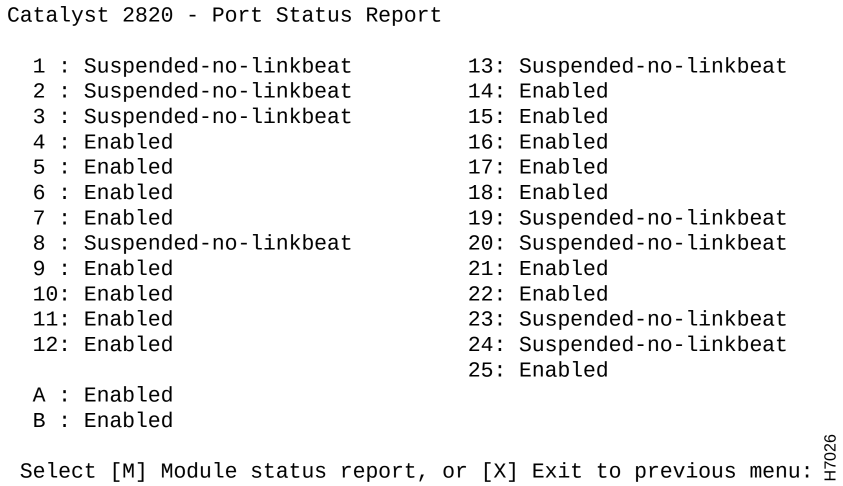
```
Catalyst 2820 - Usage Summaries

      [P] Port Status Report
      [M] Module 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:
```

Port Status Report

This report, shown in Figure 5-25, summarizes the status of all ports as defined on the Ports Menu. Definitions of these terms can be found in the “Port Configuration” section in this chapter.

Display this report by pressing **U** on the Main Menu and **P** on the Usage Summary Menu.

Figure 5-25 Port Status Report



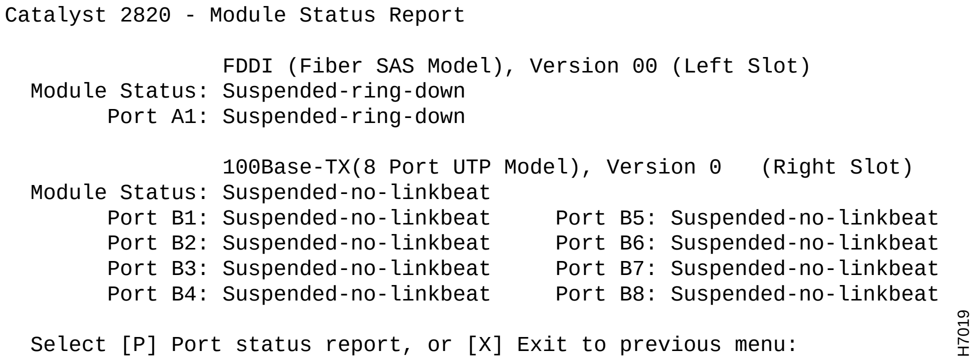
```
Catalyst 2820 - Port Status Report

  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
                                    25: Enabled
  A : Enabled
  B : Enabled

 Select [M] Module status report, or [X] Exit to previous menu:
```

Module Status Report

This report displays the status of the installed modules. Definitions of these terms can be found in the “Port Configuration” section in this chapter.

Display this report, shown in Figure 5-26, by pressing **U** on the Main Menu and **P** on the Usage Summary Menu.

Figure 5-26 Module Status Report



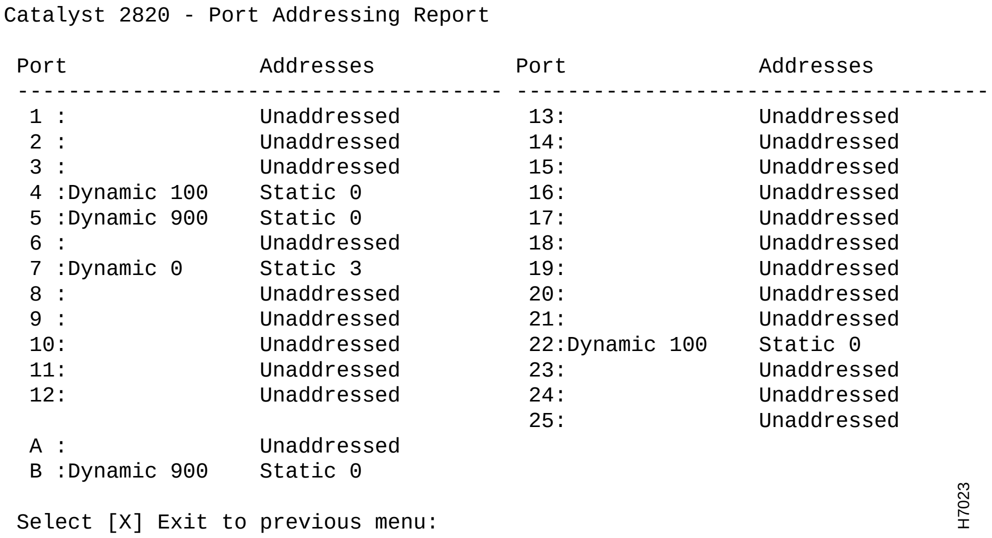
```
Catalyst 2820 - Module Status Report

                 FDDI (Fiber SAS Model), Version 00 (Left Slot)
  Module Status: Suspended-ring-down
        Port A1: Suspended-ring-down

                 100Base-TX(8 Port UTP Model), Version 0   (Right Slot)
  Module Status: Suspended-no-linkbeat
        Port B1: Suspended-no-linkbeat     Port B5: Suspended-no-linkbeat
        Port B2: Suspended-no-linkbeat     Port B6: Suspended-no-linkbeat
        Port B3: Suspended-no-linkbeat     Port B7: Suspended-no-linkbeat
        Port B4: Suspended-no-linkbeat     Port B8: Suspended-no-linkbeat

  Select [P] Port status report, or [X] Exit to previous menu:
```

Port Addressing Report

This report displays the port’s address mode, dynamic or static, and how many addresses have been assigned to the port.

Display this report, shown in Figure 5-27, by pressing **U** on the Main Menu and **A** on the Usage Summary Menu.

Figure 5-27 Port Addressing Report



```
Catalyst 2820 - Port Addressing Report

 Port               Addresses           Port              Addresses
 -------------------------------------- -------------------------------------
  1 :               Unaddressed          13:               Unaddressed
  2 :               Unaddressed          14:               Unaddressed
  3 :               Unaddressed          15:               Unaddressed
  4 :Dynamic 100    Static 0             16:               Unaddressed
  5 :Dynamic 900    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:Dynamic 100    Static 0
  11:               Unaddressed          23:               Unaddressed
  12:               Unaddressed          24:               Unaddressed
                                         25:               Unaddressed
  A :               Unaddressed
  B :Dynamic 900    Static 0

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

The two columns on this menu have the following values:

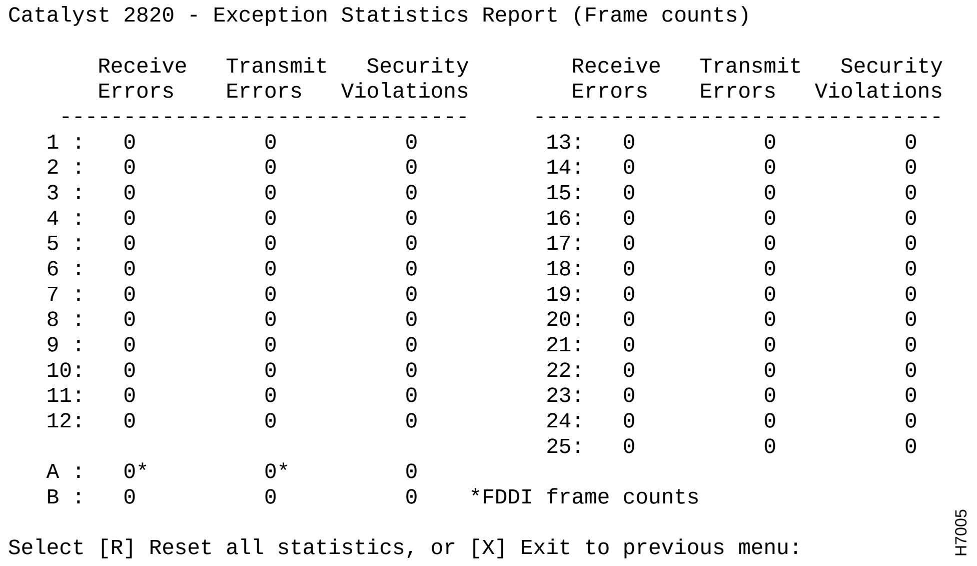
Port — Whether the port is enabled for dynamic learning or secured.

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.

Exception Statistics Report

This report displays the number of receive errors, transmit errors, and security violations for each port. Display this report, shown in Figure 5-28, by pressing **U** on the Main Menu and **E** on the Usage Summary Menu.

Figure 5-28 Exception Statistics Report



```
Catalyst 2820 - 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
                                          25:   0          0          0
   A :   0*         0*         0
   B :   0          0          0    *FDDI frame counts

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, FCS, and alignment errors

Transmit errors — The combined number of excessive deferrals, late collisions, jabber errors and other transmit errors

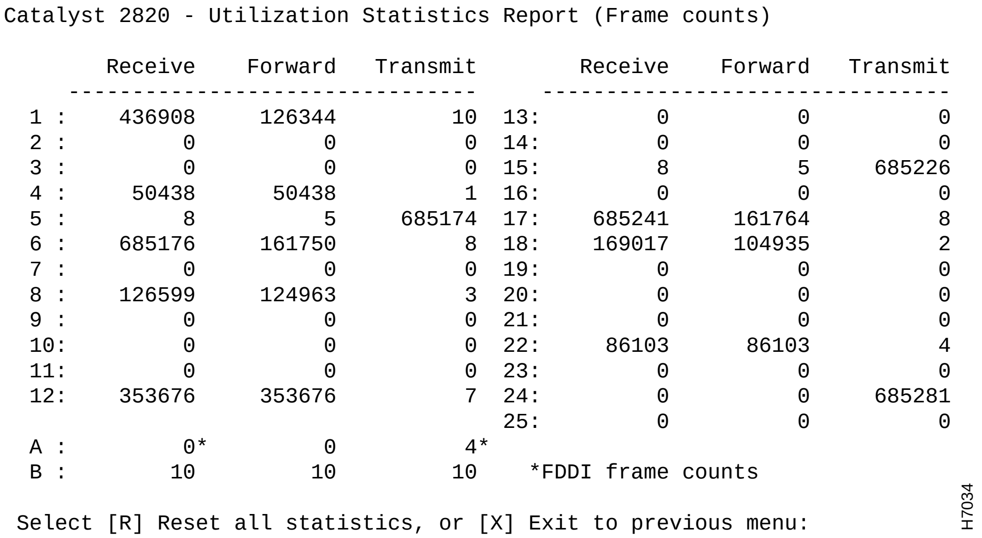
Security violations — The combined number of secure address violations caused by address mismatches or duplications

[R] Reset all statistics. Select this option to reset all statistics to zero. Respond to the confirmation prompt and press **Return**.

Utilization Statistics Report

This report displays the frame-count statistics generated by the Catalyst 2820 and 1900. Display this report, shown in Figure 5-29, by pressing **U** on the Main Menu and **U** on the Usage Summary Menu.

Figure 5-29 Utilization Statistics Report



```
Catalyst 2820 - 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 :         8          5     685174  17:    685241     161764          8
  6 :    685176     161750          8  18:    169017     104935          2
  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
                                       25:         0          0          0
  A :         0*         0          4*
  B :        10         10         10    *FDDI frame counts

 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

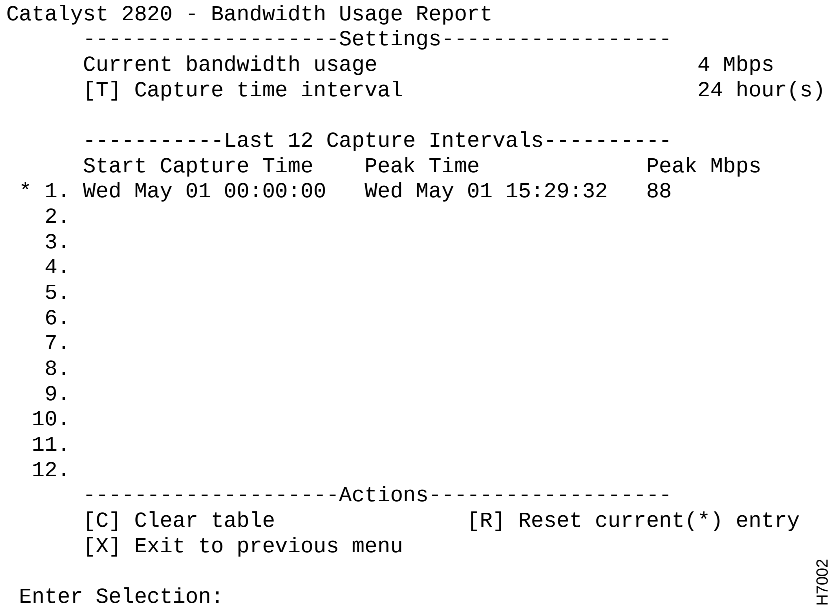
Transmit The combined number of transmitted unicast frames, multicast frames, and broadcast frames

[R] Reset all statistics. Select this option to reset all statistics to zero. Respond to the confirmation prompt and press **Return**.

Bandwidth Usage Report

This report displays the peak bandwidth of the network during a given period of time. The switch displays a list of the last twelve recordings of maximum bandwidth, in Mbps, according to a time interval you set. Display this report, shown in Figure 5-30, by pressing **U** on the Main Menu and **B** on the Usage Summary Menu.

Figure 5-30 Bandwidth Usage Report



```
Catalyst 2820 - Bandwidth Usage Report
      --------------------Settings------------------
      Current bandwidth usage                         4 Mbps
      [T] Capture time interval                       24 hour(s)

      -----------Last 12 Capture Intervals----------
      Start Capture Time    Peak Time            Peak Mbps
 * 1. Wed May 01 00:00:00   Wed May 01 15:29:32   88
   2.
   3.
   4.
   5.
   6.
   7.
   8.
   9.
  10.
  11.
  12.
      --------------------Actions-------------------
      [C] Clear table              [R] Reset current(*) entry
      [X] Exit to previous menu

 Enter Selection:
```

[T] Capture time interval. Use this option to define the time interval during which data is collected to calculate bandwidth usage. Table 1-6 in the chapter “Overview” shows the bandwidth associated with each LED. Enter a number between 1 and 24 and press **Return**.

[C] Clear table. Select this option to clear the bandwidth table. Enter **Y** or **N** at the confirmation prompt and press **Return**.

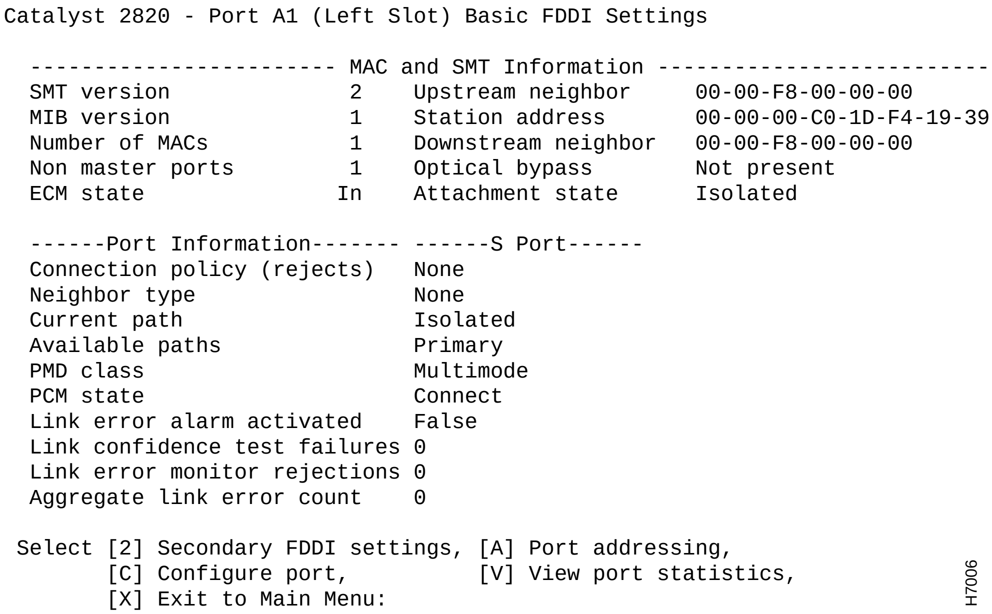
[R] Reset current entry. This option sets the current table entry to zero and allows new information to be recorded. The current table entry is marked by an asterisk (*). Enter **Y** or **N** at the confirmation prompt and press **Return**.

Basic FDDI Settings

This screen displays the most common FDDI settings, but does not allow you to set any parameters. Each parameter is described below.

Display this menu, shown in Figure 5-31, by entering **1** on the Port Configuration Menu.

Figure 5-31 Basic FDDI Settings



```
Catalyst 2820 - Port A1 (Left Slot) Basic FDDI Settings

  ------------------------ MAC and SMT Information --------------------------
  SMT version              2    Upstream neighbor     00-00-F8-00-00-00
  MIB version              1    Station address       00-00-00-C0-1D-F4-19-39
  Number of MACs           1    Downstream neighbor   00-00-F8-00-00-00
  Non master ports         1    Optical bypass        Not present
  ECM state               In    Attachment state      Isolated

  ------Port Information------- ------S Port------
  Connection policy (rejects)   None
  Neighbor type                 None
  Current path                  Isolated
  Available paths               Primary
  PMD class                     Multimode
  PCM state                     Connect
  Link error alarm activated    False
  Link confidence test failures 0
  Link error monitor rejections 0
  Aggregate link error count    0

 Select [2] Secondary FDDI settings, [A] Port addressing,
        [C] Configure port,          [V] View port statistics,
        [X] Exit to Main Menu:
```

[2] Secondary FDDI settings. Display the menu described in the “Secondary FDDI Settings” section in this chapter.

[C] Configure port. Display the menu described in the “Port Configuration” section in this chapter.

[A] Port addressing. Display the menu described in the “Port Addressing” section in this chapter.

[V] View port statistics. Display the port statistics report described in the “Port Statistics Report” section in this chapter.

MAC and SMT Information

SMT version
The version number of this particular Station Management (SMT) implementation.

MIB version
The version number of this FDDI MIB implementation.

Number of MACs
The number of MACs that this FDDI entity implements.

Non master ports
The number of *non-master* ports residing on the FDDI module. Non-master ports are any ports other than the M type.

Optical bypass
If an optical bypass device is attached to the FDDI module, this item is `Present`; otherwise it is `Not present`.

Upstream neighbor
The station address of the upstream neighbor.

Station address
The station address of the FDDI module.

Downstream neighbor
The station address of the downstream neighbor.

ECM state
The current status of the ECM (entity coordination management) state machine. The ECM handles the management and coordination of all of the ports in the node. During normal operation, this has the value `In`. The other possible values, `Out`, `Trace`, `Leave`, `Path_test`, `Insert`, `Check`, or `Deinsert`, can indicate that the ECM state machine has detected an error.

Attachment state
The current attachment configuration for the module. The normal state, `Thru`, indicates that both ports are connected to the ring. The value `Isolated` indicates that both ports A and B are disconnected from the ring, `Wrap_A` indicates that only port A is connected to the ring, and `Wrap_B` indicates that only port B is connected to the ring.

Port Information

Connection policy (rejects)

The types of connections that are not allowed for each port. For example, if port types A and S are listed under port A, then port A of the FDDI module cannot be connected to an A port or an S port on another station.

Neighbor type

The port type to which each port is currently attached. Possible values are `A`, `B`, `S`, `M`, and `NONE`.

Current path

The path into which each port is currently inserted. For Catalyst 2820 FDDI, the value will be `Primary`, `Secondary`, or `Isolated`.

Available paths

The possible paths into which each port can theoretically be inserted. For Catalyst 2820 FDDI DAS, this value will always be `Primary+Secondary`; for FDDI SAS, the value will be `Primary`.

PMD class

The class of the PMD (physical layer media dependent). The value is `multimode` or `twisted-pair`.

PCM state

The current state of the PCM (physical connection management) state machine. The PCM covers the management of the physical connection between the port and the connected port on the adjacent node. The possible values are `Off`, `Break`, `Trace`, `Connect`, `Next`, `Signal`, `Join`, `Verify`, `Active`, and `Maint`.

Link error alarm activated

If this value gets set to `True`, the link error rate for the port has exceeded the alarm threshold.

Link confidence test failures

A count of the number of consecutive times the link confidence test has failed.

Link error monitor rejections

A link-error monitoring count of the number of times that a link has been rejected.

Aggregate link error count

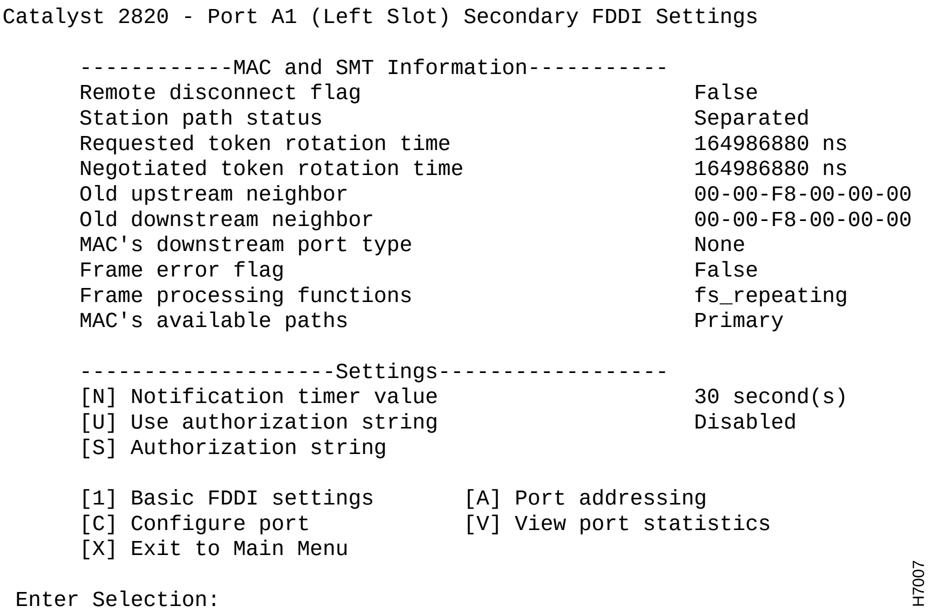
An aggregate count of link-error monitoring errors. This count is reset only at initialization.

Secondary FDDI Settings

This screen contains some of the less common FDDI settings. You can change three of the parameters; all others are display only.

Display this menu, shown in Figure 5-32, by entering **2** on the Port Configuration Menu.

Figure 5-32 Secondary FDDI Settings



```
Catalyst 2820 - Port A1 (Left Slot) Secondary FDDI Settings

      ------------MAC and SMT Information-----------
      Remote disconnect flag                          False
      Station path status                             Separated
      Requested token rotation time                   164986880 ns
      Negotiated token rotation time                  164986880 ns
      Old upstream neighbor                           00-00-F8-00-00-00
      Old downstream neighbor                         00-00-F8-00-00-00
      MAC's downstream port type                      None
      Frame error flag                                False
      Frame processing functions                      fs_repeating
      MAC's available paths                           Primary

      --------------------Settings------------------
      [N] Notification timer value                    30 second(s)
      [U] Use authorization string                    Disabled
      [S] Authorization string

      [1] Basic FDDI settings       [A] Port addressing
      [C] Configure port            [V] View port statistics
      [X] Exit to Main Menu

 Enter Selection:
```

MAC and SMT Information

Remote disconnect flag
This flag indicates whether the module was remotely disconnected from the network as a result of receiving a disconnect action in a Parameter Management Frame.

Station path status
The status of the primary and secondary paths within the module. The status is `Concatenated`, `Separated`, or `Thru`.

Requested token rotation time
The requested token rotation time in nanoseconds for the module.

Negotiated token rotation time
The negotiated token rotation time in nanoseconds. Note that this value will be the same for all stations on the ring.

Old upstream neighbor
The previous value of the MAC's upstream neighbor's MAC address.

Old downstream neighbor
The previous value of the MAC's downstream neighbor's MAC address.

MAC's downstream port type
The type of the first port that is downstream from this MAC.

Valid transmission timer
The value that the module is using for its valid transmission timer. If the module waits this amount of time without seeing a valid frame or unrestricted token, the module begins the claim process to re-create the token.

Frame error flag
This flag is set when the MAC Frame Error Condition is present. This value is cleared when the condition clears and on station reset.

Frame processing functions
This indicates the module's handling of the Error, Address, and Copied frame status indicators.

MAC's available paths
The paths that are available to the MAC.

[N] Notification timer value. Use this option to assign a new value to fddimibSMTTNotify. Enter a value according to the prompt and press **Return**.

```
This value is the timer, expressed in seconds, used in the Neighbor
Notification protocol. It has a range of 2 seconds to 30 seconds. The
default value is 30.

Current setting ==> 30
    New setting ==>
```

[U] Use authorization string. Select this option to enable or disable authorization checking for the SMT entity. When this item is selected, the following prompt is displayed:

```
When the authorization string checking is enabled, the
FDDI module will use the current authorization string to verify SMT
requests from remote stations. This value is disabled by default.

Use of authorization string checking may be [E]nabled or [D]isabled

Current setting ==> Disabled
    New setting ==>
```

[S] Authorization string. Select this option to assign a new authorization string value. The authorization string is from 0 to 32 bytes in length; the length must be a multiple of 4 bytes. When this item is selected, the following prompt is displayed:

```
The authorization string is used in the verification of SMT requests. The
length of the authorization string must be a multiple of 4 bytes.
Input the new authorization string.

Current ==> mgmtpswd
    New ==>
```

[1] Basic FDDI settings. Display the menu described in the “Basic FDDI Settings” section in this chapter.

[C] Configure port. Display the menu described in the “Port Configuration” section in this chapter.

[A] Port addressing. Display the menu described in the “Port Addressing” section in this chapter.

[V] View port statistics. Display the port statistics report described in the “Port Statistics Report” section in this chapter.