Configuring the Catalyst 3900

You might not have to configure the Catalyst 3900 for it to work in your network; it is shipped with default configuration parameters and can function with these defaults. However, if you want or need to alter the configuration of the Catalyst 3900, you can use a console session. This chapter provides information on the following:

- Configuration Overview
- Configuring Basic Switch and Stack Parameters
- Viewing Module Information
- Configuring VLANs and VTP
- Configuring IP Information
- Configuring SNMP Parameters
- Configuring Spanning-Tree Parameters
- Configuring Port Parameters
- Configuring the Cisco Discovery Protocol Parameters
- Monitoring Port Traffic
- Using TokenChannels
- Limiting Scope and Access
- Configuring Address Aging
- Setting a Password

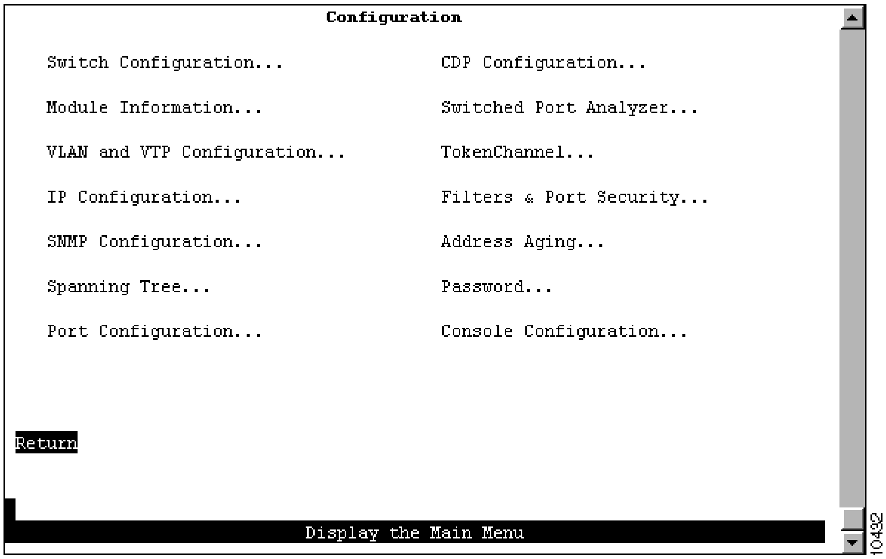
Configuration Overview

To alter the configuration of your Catalyst 3900, follow these steps:

Step 1 If one has not already been established, establish a console session. For information about establishing a console session, refer to the "Planning for Configuration and Management" section.

Step 2 At the Main Menu, select **Configuration**. The Configuration Menu panel (Figure 6-1) is displayed.

Figure 6-1 Configuration Menu Panel



```
                              Configuration

   Switch Configuration...              CDP Configuration...

   Module Information...                Switched Port Analyzer...

   VLAN and VTP Configuration...        TokenChannel...

   IP Configuration...                  Filters & Port Security...

   SNMP Configuration...                Address Aging...

   Spanning Tree...                     Password...

   Port Configuration...                Console Configuration...



Return


                          Display the Main Menu
```

Step 3 Select the menu option you want.

Step 4 Change or enter values.

Step 5 When you have changed or entered all of the required configuration parameters, save the changes and return to the Cisco Catalyst 3900 Main Menu. Configuration is complete.

Guidelines for Using the Console Panels

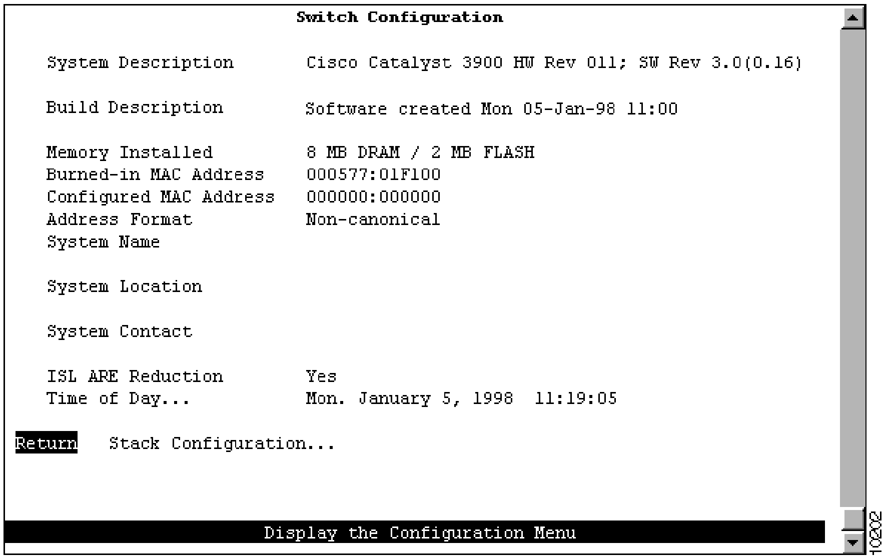
As you move through the console panels, follow these guidelines:

- To select a menu or action item, move the cursor to the item and press **Enter**.
- To make changes to a parameter, move the cursor to the parameter name and press **Enter**. You will then be prompted to enter the new data or select from a list of valid choices.
- To make changes to a list entry, select **Change** and specify the entry identifier (index number). You will then be prompted to enter the new data or select from a list of valid choices. Some list entries consist of multiple parameters. To retain the current value of any parameter, enter a null value at the prompt.
- To save any changes made to the configuration panels in NVRAM, you must select **Return**. In most cases, changes will not take effect until you have exited the panel by selecting Return.
- To return to the main menu without saving your changes, press **Ctrl-P**. Changes made to the current panel will not be saved.
- To return to the previous panel without saving your changes, press the backspace key.
- To refresh the console panel at any time, press **Ctrl-L**.
- If the Catalyst 3900 is part of a stack, you will be prompted to select a box (Catalyst 3900) when you access certain configuration panels, such as the Switch/Stack Information panel.
- In some cases, more information is available than can be displayed on the panel. To scroll to the next panel of information, select **More**.

Configuring Basic Switch and Stack Parameters

To view or change basic switch and stack information, such as the system name, system location, or system contact, select **Switch Configuration** on the Configuration Menu. The Switch Configuration panel (Figure 6-2) is displayed.

Figure 6-2 Switch Configuration Panel



```
                            Switch Configuration

   System Description       Cisco Catalyst 3900 HW Rev 011; SW Rev 3.0(0.16)

   Build Description        Software created Mon 05-Jan-98 11:00

   Memory Installed         8 MB DRAM / 2 MB FLASH
   Burned-in MAC Address    000577:01F100
   Configured MAC Address   000000:000000
   Address Format           Non-canonical
   System Name

   System Location

   System Contact

   ISL ARE Reduction        Yes
   Time of Day...           Mon. January 5, 1998  11:19:05

Return   Stack Configuration...


                      Display the Configuration Menu
```

The following information is displayed on this panel:

- System Description—Full name and version identification of the system's hardware.
- Build Description—Version identification of the firmware.
- Memory Installed—Amount (in megabytes) of dynamic RAM (DRAM) and Flash memory installed. Information in this field cannot be changed.
- Burned-in MAC Address—Factory-assigned MAC address of the Catalyst 3900. Information in this field cannot be changed. This address is used as the basis for the MAC addresses of the ports and VLANs of the switch. For more information about how MAC addresses are assigned, refer to the "Codes and IDs" appendix.
- Configured MAC Address—MAC address that is configured for the Catalyst 3900. If a locally administered address is assigned to the Catalyst 3900, this field displays that address. Otherwise, the field displays all 0s. To assign a locally administered address, select this field and enter the new address. The new address will take effect the next time the Catalyst 3900 is reset.
- Address Format—Format used for MAC addresses (non-canonical or canonical). Non-canonical is typically used in Token Ring networks and is also known as *most significant bit first*. The two parts of a non-canonical address are separated by a colon. Canonical format is typically used in Ethernet networks and is also known as *least significant bit first*. The two parts of a canonical address are separated by a dash. If you change the address format, the new format will be used for displaying addresses by all switches in the stack and will take effect immediately.
- System Name—Locally assigned name of this Catalyst 3900. This name will appear in SNMP traps.
- System Location—Location information for this Catalyst 3900. This location will appear in SNMP traps.

- System Contact—Name of system contact for this Catalyst 3900.
- ISL ARE Reduction—Whether the ARE reduction feature for the ISL module is enabled. Possible values are Yes and No. The default is Yes. This field is displayed only if there is an ISL module installed in the Catalyst 3900 or in a switch in the stack to which the Catalyst 3900 belongs.
- Time of Day—Time according to the internal clock of the Catalyst 3900.

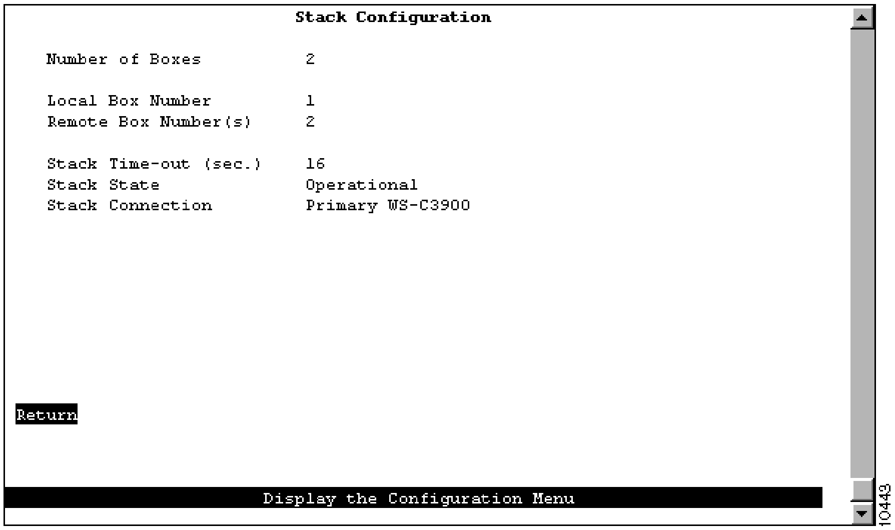
Note If this Catalyst 3900 is part of a stack, updates to the Address Format, System Name, System Location, and System Contact are propagated throughout the stack.

To	Select	Then
Change the current settings...	The appropriate parameter...	Specify the new value.
View additional information about the switch...	**Stack Configuration**	Refer to the “Configuring Stack Parameters” section.
Save your changes...	**Return**	

Configuring Stack Parameters

To configure stack parameters, select **Stack Configuration** on the Switch Configuration panel. The Stack Configuration panel (Figure 6-3) is displayed.

Figure 6-3 Stack Configuration Panel



```
                              Stack Configuration

   Number of Boxes           2

   Local Box Number          1
   Remote Box Number(s)      2

   Stack Time-out (sec.)     16
   Stack State               Operational
   Stack Connection          Primary WS-C3900
```

The following information is displayed on this panel:

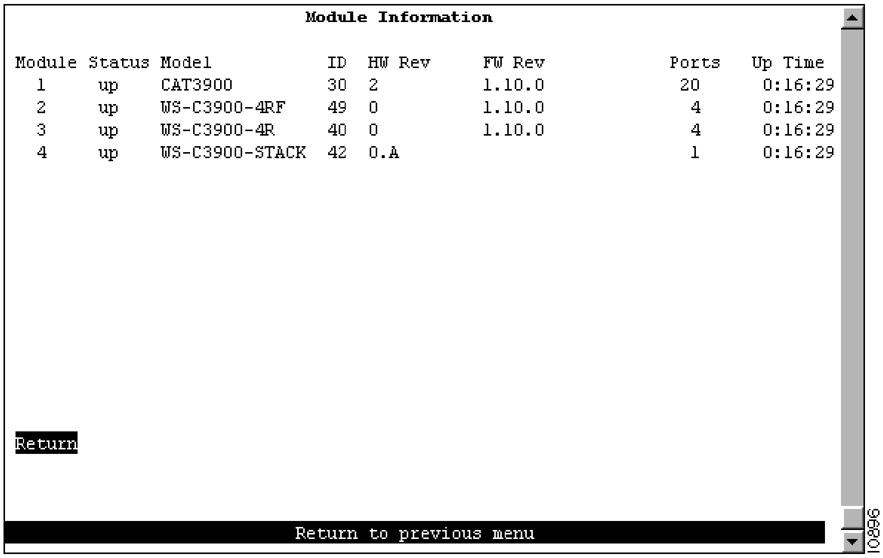
- Number of Boxes—Number of switches currently participating in the stack. Information in this field cannot be changed.
- Local Box Number—Number assigned to the switch to which the console is connected. The local box is also the source of the information displayed on this panel. Information in this field cannot be changed.

- Remote Box Number(s)—Number of switches (in addition to this one) in the stack. Information in this field cannot be changed.
- Stack Time-out (sec.)—If a switch goes off line, the length of time (in seconds) during which the stack tries to re-establish communication with the switch. The default is 16 seconds.
- Stack State—Indicates whether the ProStack is operational. Information in this field cannot be changed. Possible states are:
  - Idle—The initial state.
  - Discovery—The Catalyst 3900 is checking to see if a stack exists and, if so, what the values of the stack parameters are.
  - Split Stack—A stack has been detected, but the parameters are different than those configured for this Catalyst 3900. To resolve a split stack, you must reset the Catalyst 3900 by pressing the System Request button.
  - DP Update—Parameters for the stack are being updated.
  - BI Update—The Catalyst 3900 is sending out information about its configuration.
  - VLAN BI Update—A port on the Catalyst 3900 has changed TrBRF assignments and the Catalyst 3900 is sending out updated configuration information.
  - Operational—The stack has been formed successfully.
  - Not Operational—The stack has not been formed. This may be because there is no stack port installed in the expansion slot or there is no connection between the stack port and any other Catalyst 3900 or Catalyst Matrix.
- Stack Connection—Indicates whether the ProStack is connected. Information in this field cannot be changed. Possible values are Not Connected, Not Present, or Primary WS-3900.

Viewing Module Information

To view general information about the Catalyst 3900 and any expansion modules installed, select **Module Information** on the Configuration Menu. The Module Information panel (Figure 6-4) is displayed.

Figure 6-4 Module Information Panel



```
                              Module Information

Module Status Model           ID   HW Rev     FW Rev           Ports   Up Time
  1     up    CAT3900         30   2          1.10.0            20      0:16:29
  2     up    WS-C3900-4RF    49   0          1.10.0             4      0:16:29
  3     up    WS-C3900-4R     40   0          1.10.0             4      0:16:29
  4     up    WS-C3900-STACK  42   0.A                           1      0:16:29









Return


                           Return to previous menu
```

The following information is displayed on this panel:

- Module—Module number. The module numbers displayed on the Module Information panel have the following meaning:
  - 1—Base switch
  - 2—Front, left expansion slot
  - 3—Front, right expansion slot
  - 4—Rear stack port slot
- Status—Indicates whether the module is up, down, or the slot is empty. Up indicates that the module is properly installed. It does not imply that any ports on the module are connected and operational.
- Model—Type of module. CAT3900 is listed for the base switch. For other modules, this field displays the product number.
- ID—Identifier of the board in decimal. For a list of possible board IDs, refer to the “Board IDs” section in the “Codes and IDs” appendix.
- HW Rev—Hardware revision level of the module. For the stack module, this field displays the hardware revision level of the stack module followed by the revision level of the Proprietary Fat Pipe. A stack module Revision B will be displayed as 0.B.
- FW Rev—Firmware revision level of the module.
- Ports—Number of ports on the module.
- Up Time—Amount of time (in hours, minutes, and seconds) that the module has been up since the last reset.

You cannot change the information that appears on this panel.

Configuring VLANs and VTP

You can partition a single Catalyst 3900 into multiple VLANs. A VLAN can be configured with its own IP address and managed with SNMP. A VLAN can contain ports from multiple switches in the same stack. Any VLAN can participate independently in the Spanning-Tree Protocol. Once VLANs have been established, packets are forwarded between ports belonging to the same VLAN only.

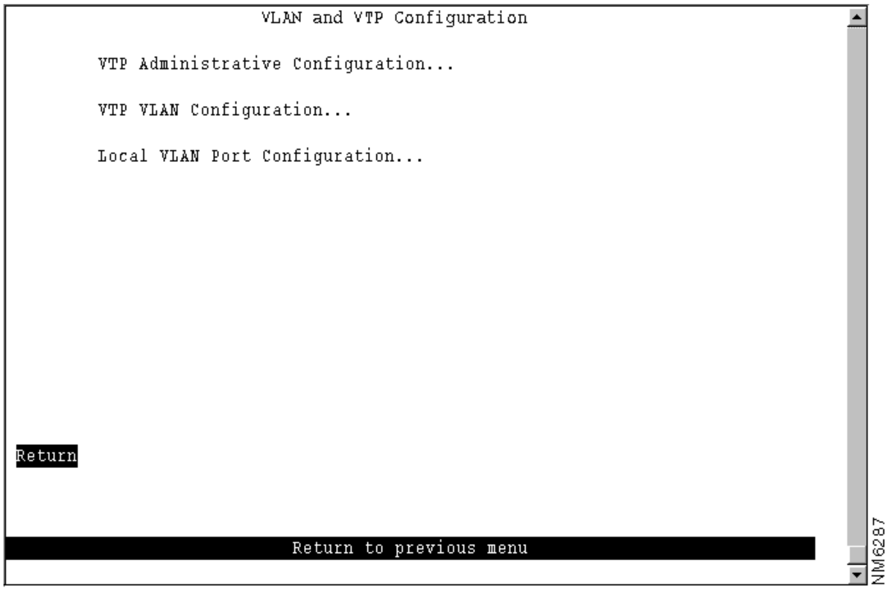
You can use VTP to set up and manage VLANs across an entire administrative domain. When new VLANs are added to a Catalyst switch in an administrative domain, VTP can be used to automatically distribute the information to the trunk ports of all the devices in the administrative domain. This allows VLAN naming consistency and connectivity between all devices in the administrative domain.

An *administrative* or *management domain* is a logical grouping of VLANs used by the VLAN Trunking Protocol (VTP) for the purpose of administration and management. VTP parameters are propagated throughout the VLANs within a single management domain. While you can have duplicate VLAN names in a network, each VLAN name within a management domain must be unique. A management domain is not device specific. Different devices may belong to the same management domain if the VLANs defined for the devices belong to the same management domain. Likewise, a device may belong to multiple management domains if the VLANs defined for the device belong to different management domains.

For more information about Token Ring VLANs, refer to the “Token Ring VLANs” section of the “Understanding Token Ring Switching” appendix.

To configure VLANs and the VTP for the Catalyst 3900, select **VLAN and VTP Configuration** on the Configuration Menu. The VLAN and VTP Configuration panel (Figure 6-5) is displayed.

Figure 6-5 VLAN and VTP Configuration Panel



```
                    VLAN and VTP Configuration

       VTP Administrative Configuration...

       VTP VLAN Configuration...

       Local VLAN Port Configuration...
```

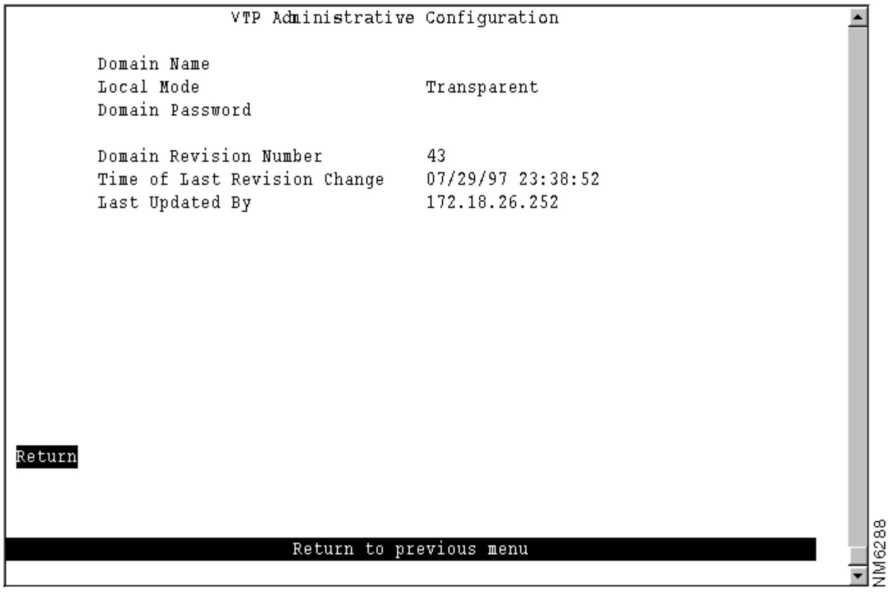
The following options are displayed on this panel:

- VTP Administrative Configuration—Select this option to display the current VTP parameters. Refer to the "Viewing VTP Parameters" section for more information.
- VTP VLAN Configuration—Select this option to define VLANs. Refer to the "Configuring VLANs" section for more information.
- Local VLAN Port Configuration—Select this option to display a list of the VLAN port assignments. Refer to the "Displaying VLAN Port Assignments" section for more information.

Viewing VTP Parameters

To view parameters for the VTP, select **VTP Administrative Configuration** on the VLAN and VTP Configuration panel. The VTP Administrative Configuration panel (Figure 6-6) is displayed.

Figure 6-6 VTP Administrative Configuration Panel



```
                  VTP Administrative Configuration

        Domain Name
        Local Mode                      Transparent
        Domain Password

        Domain Revision Number          43
        Time of Last Revision Change    07/29/97 23:38:52
        Last Updated By                 172.18.26.252
```

The following information is displayed on this panel:

- Domain Name—Name of the administrative domain the device is participating in (accepting updates from and propagating configuration changes to).
- Local Mode—VTP mode of the switch. Possible values are Server, Client, and Transparent. The default is Transparent.
  - — Server mode permits configuration changes from the local device. All devices in Server mode must be capable of storing configurations for all the VLANs in the administrative domain. The switch will not allow the user to configure VLANs in excess of 63. If this number is exceeded, the switch will automatically enter Client mode.
  - — Client mode accepts configuration changes only from other devices.
  - — Transparent mode passes along any VTP packets received. Transparent mode also accepts and stores changes to the local VLAN configuration database, but does not propagate the changes to other devices.

Note To enable ring number learning for TrCRFs, the Local Mode must be set to Transparent (which is the default) and the Ring Number on the VTP VLAN Parameter Configuration for the TrCRF must be set to auto (which is the default). If you have set the Local Mode to Client or Server, you cannot set the Ring Number to auto. Also, if you have previously set the Local Mode to Transparent and the Ring Number to auto, you cannot change the Local Mode while ring number learning is in progress.

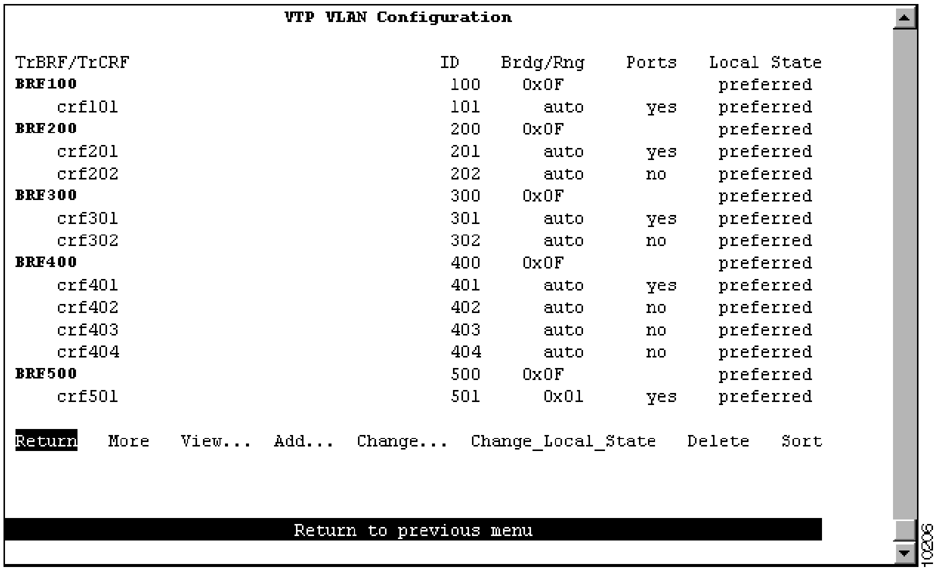
- Domain Password—Password of up to 64 characters common to all devices in the administrative domain. A configuration will not pass between two devices with different passwords even if they are configured with the same administrative domain name.
- Domain Revision Number—Revision number of the current configuration database implemented on this device.
- Time of Last Revision Change—Time the revision of the current configuration database implement on this device was created.
- Last Updated By—IP address of the server where the revision of the current configuration database implemented on this device was created.

Configuring VLANs

You can define VLANs for the entire network from a single switch. The VLAN configuration is propagated to all switches in the same administrative domain using the VTP advertisement protocol. To define VLANs, select **VTP VLAN Configuration** on the VLAN and VTP Configuration panel. The VTP VLAN Configuration panel (Figure 6-7) is displayed. The panel lists the VLANs with respect to their parent-child relationships. Each TrBRF is followed by an indented list of the TrCRFs for which it is a parent. You can also sort the entries on the panel by VLAN ID. This is particularly useful when you are searching for a particular VLAN or when you want to add a VLAN and need to see the IDs that have already been assigned.

Note This panel displays all VLANs in the administrative domain regardless of whether they are a VLAN type that is supported by the Catalyst 3900.

Figure 6-7 VTP VLAN Configuration Panel



```
                         VTP VLAN Configuration

TrBRF/TrCRF                         ID    Brdg/Rng    Ports   Local State
BRF100                              100    0x0F               preferred
   crf101                           101      auto      yes    preferred
BRF200                              200    0x0F               preferred
   crf201                           201      auto      yes    preferred
   crf202                           202      auto      no     preferred
BRF300                              300    0x0F               preferred
   crf301                           301      auto      yes    preferred
   crf302                           302      auto      no     preferred
BRF400                              400    0x0F               preferred
   crf401                           401      auto      yes    preferred
   crf402                           402      auto      no     preferred
   crf403                           403      auto      no     preferred
   crf404                           404      auto      no     preferred
BRF500                              500    0x0F               preferred
   crf501                           501      0x01      yes    preferred

Return   More   View...  Add...  Change...  Change_Local_State   Delete   Sort



                         Return to previous menu
```

The following information is displayed on this panel:

- TrBRF/TrCRF—ASCII name associated with the VLAN, which is synonymous with the VLAN's emulated LAN name on LANE trunks.
- ID—Numeric VTP ID, which is synonymous with the VLAN's ISL ID associated with the VLAN packets on ISL trunks.
- Brdg/Rng—Bridge number for TrBRFs or ring number for TrCRFs. The bridge and ring numbers are displayed in hexadecimal.
- Ports—For TrCRFs, whether or not ports have been associated.
- Local State—Indicates whether a VLAN (TrCRF or TrBRF) is used on the local switch. Possible values are not-local, preferred, and automatic.
  - — Not-local indicates that the VLAN is not designated for use on the local switch.
  - — Preferred indicates that the VLAN is designated for use on the local switch. A preferred VLAN is guaranteed access on the switch. Any TrCRF to which ports on the local switch are assigned is designated as preferred. In addition, you can designate other TrCRFs and TrBRFs as preferred using the Change_Local_State option. Up to 63 TrCRFs and 63 TrBRFs can be designated as preferred.
  - — Automatic indicates that the VLAN can be used on the local switch if access is available. An automatic VLAN is not guaranteed access on the switch. Automatic VLANs are given access as space is available (if less than 63 VLANs have been designated as preferred).

  When setting the local state for a VLAN, keep the following in mind:

  - — New TrBRFs are assigned a local state of not-local.
  - — If you add a TrCRF to a TrBRF with a local state of not-local, the TrCRF is assigned a local state of not-local.
  - — If you add a TrCRF to a TrBRF with a local state of preferred, the TrCRF is assigned a local state of automatic.
  - — If you add a TrCRF to the preferred list and the parent TrBRF is not already designated as preferred, the local state of the parent TrBRF will also be changed to preferred.

- — If you add a TrBRF to the preferred list and its children have a local state of not-local, the local state of the children will be changed to automatic.
- — You cannot change the state of any TrBRF that contains a TrCRF in the preferred state.
- — You cannot change the state of any TrCRF to which ports are assigned.
- — If you remove a TrBRF from the preferred list, the local state will be changed to not-local.
- — If you remove a TrCRF from the preferred list, the local state will be changed to automatic (if there are less than 63 TrCRFs that have been granted access through the switch) or not-local.

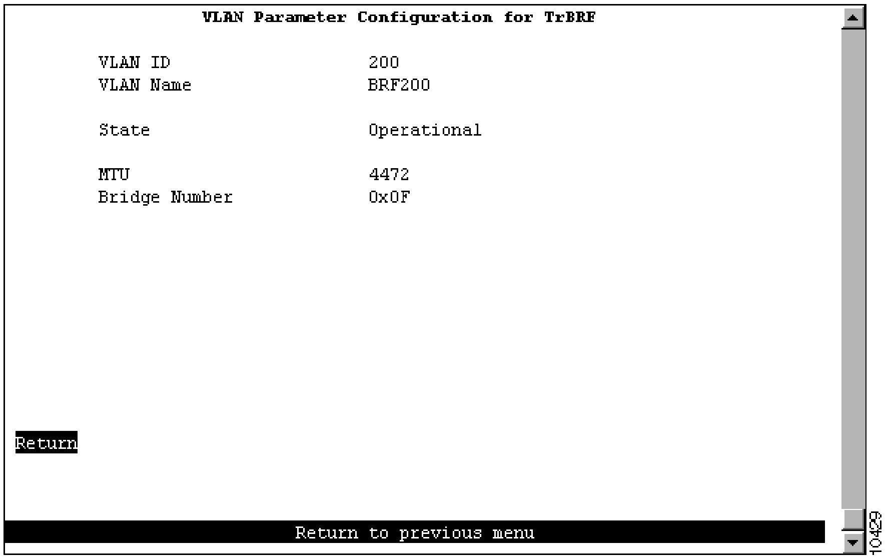
To	Select	Then
View the current configuration of a VLAN, including a list of associated ports for a TrCRF...	**View**	Specify the VLAN ID.
Add a new TrBRF VLAN configuration...	**Add**	Specify the VLAN ID. Select **TrBRF**. Refer to the “Adding or Changing TrBRF VLAN Parameters” section.
Add a new TrCRF VLAN configuration...	**Add**	Specify the VLAN ID. Select **TrCRF**. Refer to the “Adding or Changing TrCRF VLAN Parameters” section.
Change an existing TrBRF VLAN configuration...	**Change**	Specify the VLAN ID and refer to the “Adding or Changing TrBRF VLAN Parameters” section.
Change an existing TrCRF VLAN configuration...	**Change**	Specify the VLAN ID and refer to the “Adding or Changing TrCRF VLAN Parameters” section.
Add or remove a TrBRF or TrCRF from the list of preferred VLANS...	**Change_Local_State**	Specify the VLAN ID and confirm your request to add or remove the VLAN from the preferred list. Then, press any key to refresh the panel.
Delete a VLAN...	**Delete**	Specify the VLAN ID.
Display a list of VLANs sorted by VLAN ID...	**Sort**	Select **Sort_by_VLAN_ID**.
Save your changes...	**Return**	

Note The VLAN with the VLAN name of “default” is an Ethernet VLAN and is the VLAN that will be used to transmit information for Cisco proprietary protocols, such as VTP and CDP.

Adding or Changing TrBRF VLAN Parameters

To add a new TrBRF, select **Add** on the VTP VLAN Configuration panel, enter the VLAN ID (2 through 1001) and select TrBRF. To change the definition of an existing TrBRF, select **Change** on the VTP VLAN Configuration panel and specify the VLAN ID. In either case, the VLAN Parameter Configuration for TrBRF panel (Figure 6-8) is displayed.

Figure 6-8 VLAN Parameter Configuration for TrBRF Panel



```
                    VLAN Parameter Configuration for TrBRF

         VLAN ID                   200
         VLAN Name                 BRF200

         State                     Operational

         MTU                       4472
         Bridge Number             0x0F
```

The following information is displayed on this panel:

- VLAN ID—Numeric VTP ID, which is synonymous with the VLAN's ISL ID associated with the VLANs packets on ISL trunks. For a TrBRF, possible values are 2 through 1001, and 1005 (the default).
- VLAN Name—ASCII name associated with the TrBRF. Up to 32 characters are allowed.
- State—Current state of the TrBRF. The possible values for the State of a TrBRF are Operational and Suspended. By default, all VLANs are Operational. You can change the states for TrBRFs and TrCRFs only. Consider the following when changing the state of a TrBRF:
  - If you change the state of a TrBRF to Suspended, the state of any associated TrCRFs will also be changed to Suspended.
  - If you change the state of a TrBRF to Operational, the state of any associated TrCRFs will also be changed to Operational. This will cause all the ports associated with the TrBRF to begin forwarding traffic.
- MTU—Maximum transmission unit of the TrBRF. Possible values are 1500 through 18190. The default is 4472. You cannot configure an MTU greater than 4472 unless you have the Stack Port module Revision B or later installed.

Note If you reduce the MTU for a TrBRF to a value that is less than the MTU currently configured for the individual ports in the TrBRF, the MTU for the ports will automatically be reduced to a value (1500, 4472, 8144, or 17800) that is less than that specified for the TrBRF.

- Bridge Number—Source-routing bridge number (in hexadecimal format) for this TrBRF. Possible values are 00 through 0F. The default is 0F.

Adding or Changing TrCRF VLAN Parameters

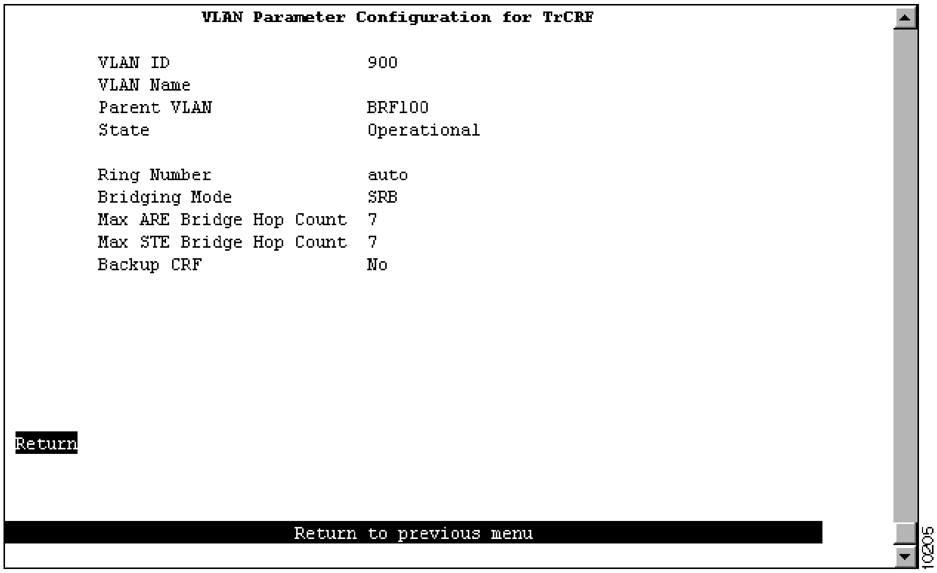
To add a new TrCRF, select **Add** on the VTP VLAN Configuration panel, enter the VLAN ID (2 through 1001) and select TrCRF. To change the definition of an existing TrCRF, select **Change** on the VTP VLAN Configuration panel and specify the VLAN ID. In either case, the VLAN Parameter Configuration for TrCRF panel (Figure 6-9) is displayed.

Note If you select **View** on the VTP VLAN Configuration panel and specify the VLAN ID of a TrCRF, this panel also displays a list of the ports assigned to the specified TrCRF.

As described in the "Token Ring VLANs and ISL" section of the "Understanding Token Ring Switching" appendix, you can configure a TrCRF as a backup path in the event that the ISL link fails. When configuring a backup TrCRF, keep the following in mind:

- Only one port in a TrCRF can be designated as a member of a backup TrCRF.
- Only one TrCRF in a TrBRF can be designated as a backup TrCRF. However, there can be other TrCRFs in a TrBRF.

Figure 6-9 VLAN Parameter Configuration for TrCRF Panel



```
                  VLAN Parameter Configuration for TrCRF

        VLAN ID                   900
        VLAN Name
        Parent VLAN               BRF100
        State                     Operational

        Ring Number               auto
        Bridging Mode             SRB
        Max ARE Bridge Hop Count  7
        Max STE Bridge Hop Count  7
        Backup CRF                No
```

The following information is displayed on this panel:

- VLAN ID—Numeric VTP ID, which is synonymous with the VLAN's ISL ID associated with the VLANs packets on ISL trunks. For a TrCRF, possible values are 2 through 1001, and 1003 (the default).
- VLAN Name—ASCII name associated with the TrCRF, which is synonymous with the emulated LAN name on LANE trunks. Up to 32 characters are allowed.
- State—Current state of the TrCRF. The possible values for the state of a TrCRF are Operational and Suspended. By default, all VLANs are Operational. You can change the states for TrBRFs and TrCRFs only. Consider the following when changing the state of a TrCRF:
  - — If you change the state of a TrCRF to Suspended or if the state is changed as a result of a change in the state of the parent TrBRF, any traffic (including BPDUs) that is received by ports assigned to the TrCRF will be discarded.

- — If you change the state of a TrCRF to Operational, the state of the parent TrBRF will automatically be changed to Operational as well. The state of any other TrCRFs associated with the parent TrBRFs will remain unchanged.
- — The fact that a VLAN is operational does not mean that you can assign spanning-tree parameters to it. You can assign certain parameters, such as IP and spanning-tree parameters, to only those TrCRFs for which ports have been assigned. And you can assign ports to only those TrCRFs that have been configured for the local switch.

- Parent VLAN—TrBRF to which this TrCRF belongs.
- Ring Number—Logical ring number (in hexadecimal format) assigned to this TrCRF. Possible values are auto and 01 through FFF. The default is auto, meaning that the ring number will be learned. If the ring number has been learned, the ring number will be displayed in the format A-xxx.

Note To enable ring number learning, the Local Mode (on the VTP Administrative Configuration panel) must be set to Transparent (which is the default) and the ring number must be set to auto (which is the default). If you have set the local mode to Client or Server, you cannot set the ring number to auto. Also, if you have previously set the local mode to Transparent and the ring number to auto, you cannot change the Local Mode while ring number learning is in progress.

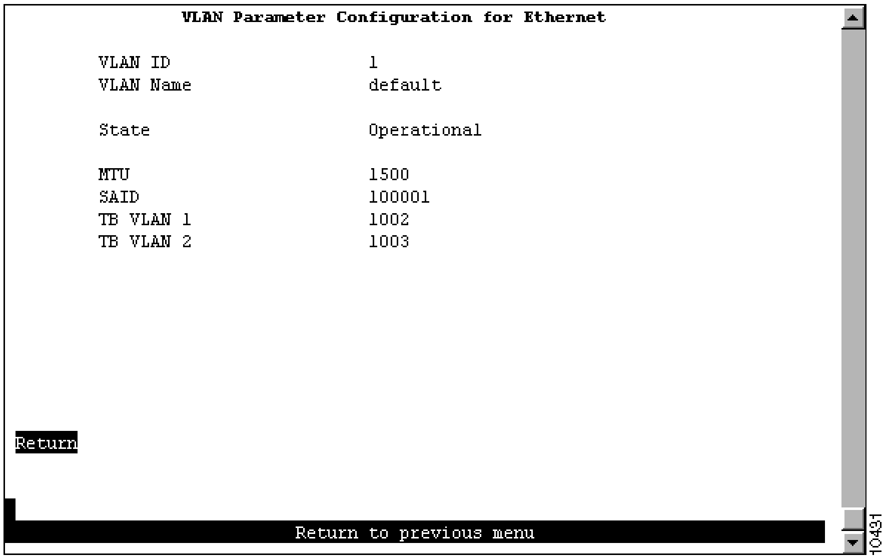
Caution If the ports of the TrCRF VLAN are connected to a ring that contains only workstations, the port will be unable to learn the ring number. In this case, you must configure the ring number.

- Bridging Mode—Bridging mode for this TrCRF. Possible values are SRB and SRT. The default is SRB.
- Max ARE Bridge Hop Count—Maximum number of hops for all-routes explorer (ARE) frames. Possible values are 1 through 13. The default is 7.
- Max STE Bridge Hop Count—Maximum number of hops for spanning-tree explorer (STE) frames. Possible values are 1 through 13. The default is 7.
- Backup CRF—Whether the TrCRF is to be used as a backup TrCRF. Possible values are No and Yes. The default is No.

Changing Ethernet VLAN Parameters

To change the definition of an existing Ethernet VLAN, select **Change** on the VTP VLAN Configuration panel and specify the VLAN ID. The VLAN Parameter Configuration for Ethernet panel (Figure 6-10) is displayed. You can change the values of the security association identifier and the translationally bridged VLANs only.

Figure 6-10 VLAN Parameter Configuration for Ethernet Panel



```
                 VLAN Parameter Configuration for Ethernet

         VLAN ID                  1
         VLAN Name                default

         State                    Operational

         MTU                      1500
         SAID                     100001
         TB VLAN 1                1002
         TB VLAN 2                1003





Return


                              Return to previous menu
```

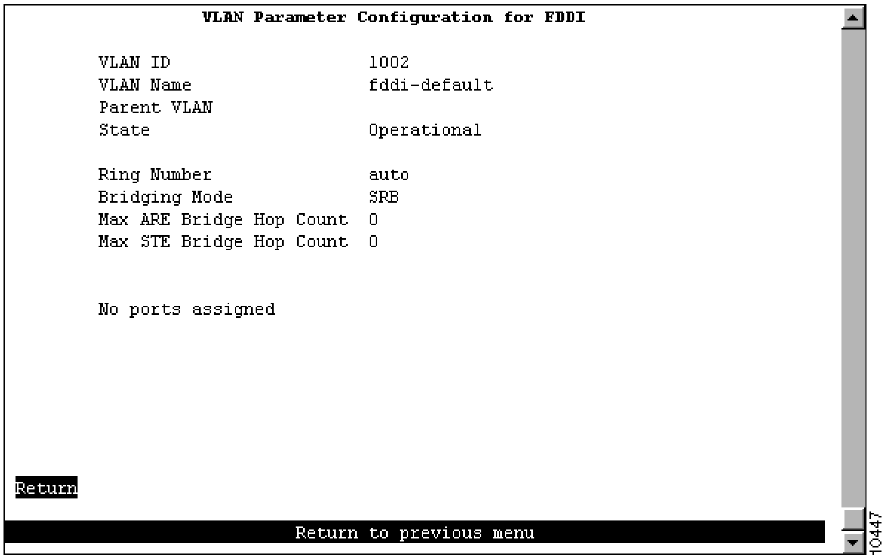
The following information is displayed on this panel:

- VLAN ID—Numeric VTP ID, which is synonymous with the VLAN’s ISL ID associated with the VLANs packets on ISL trunks.
- VLAN Name—ASCII name associated with the VLAN, which is synonymous with the VLAN’s emulated LAN name on LANE trunks.
- State—Current state of the VLAN. Possible values are Operational and Suspended. VLANs in operational state are functional. VLANs in suspended state do not pass packets.
- MTU—Maximum transmission unit of the VLAN.
- SAID—Security association identifier. Possible values are 1 through 2147483647. The default is 100100.
- TB VLAN 1—ID of a VLAN that is translationally bridged to this VLAN. Possible values are 0 through 1005.
- TB VLAN2—ID of a VLAN that is translationally bridged to this VLAN. Possible values are 0 through 1005.

Viewing FDDI and FDDI-Net VLAN Parameters

To view the definition of an existing FDDI or FDDI-Net VLAN, select **View** on the VTP VLAN Configuration panel and specify the VLAN ID. The VLAN Parameter Configuration for FDDI (or the VLAN Parameter Configuration for FDDI-net) panel (Figure 6-11) is displayed. You can view the definition of an FDDI or FDDI-Net VLAN, but cannot change it.

Figure 6-11 VLAN Parameter Configuration for FDDI Panel



```
                VLAN Parameter Configuration for FDDI

        VLAN ID                   1002
        VLAN Name                 fddi-default
        Parent VLAN
        State                     Operational

        Ring Number               auto
        Bridging Mode             SRB
        Max ARE Bridge Hop Count  0
        Max STE Bridge Hop Count  0


        No ports assigned







Return

                         Return to previous menu
```

The following information is displayed on this panel:

- VLAN ID—Numeric VTP ID, which is synonymous with the VLAN’s ISL ID associated with the VLANs packets on ISL trunks. Possible values are 2 through 1001, 1002 (the default for FDDI), and 1004 (the default for FDDI-net).
- VLAN Name—ASCII name associated with the VLAN. Up to 32 characters are allowed.
- State—Current state of the VLAN. Possible values are Operational and Suspended. VLANs in operational state are functional. VLANs in suspended state do not pass packets. The default is Operational.

FDDI VLANs

If the VLAN type is FDDI, the following additional information is displayed for FDDI VLANs:

- Parent VLAN—FDDI-Net to which this VLAN belongs.
- Ring Number—Logical ring number (in hexadecimal format) assigned to this VLAN. Possible values are auto and 01 through FFF. The default is auto, meaning that the ring number will be learned. If the ring number has been learned, the ring number will be displayed in the format A-xxx.
- Bridging Mode—Bridging mode for this VLAN. Possible values are SRB and SRT. The default is SRB.
- Max ARE Bridge Hop Count—Maximum number of hops for ARE frames. Possible values are 1 through 13. The default is 7.
- Max STE Bridge Hop Count—Maximum number of hops for STE frames. Possible values are 1 through 13. The default is 7.

FDDI-Net VLANs

If the VLAN type is FDDI-Net, the following additional information is displayed for FDDI-Net VLANs:

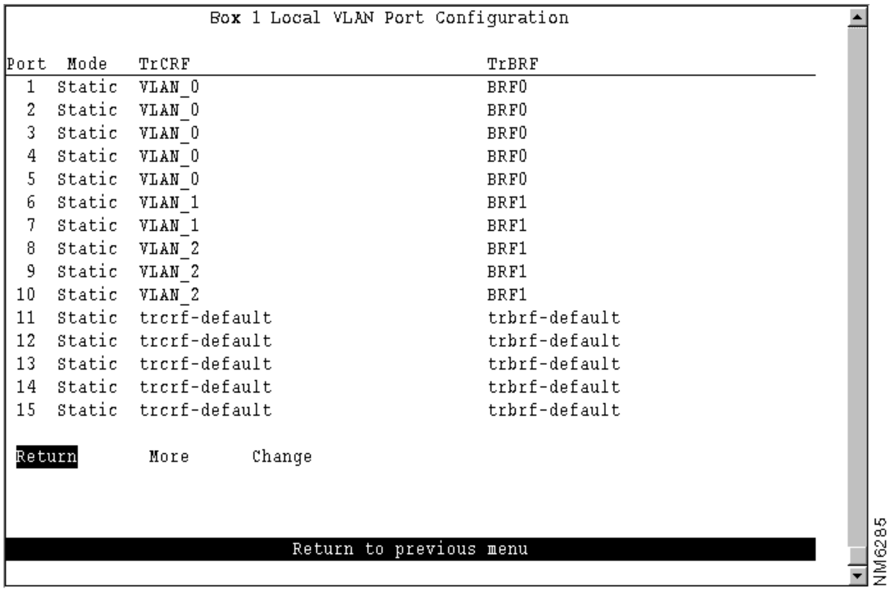
- MTU—Maximum transmission unit of the VLAN. Possible values are 1500 through 18190.
- Bridge Number—Source-route bridging number (in hexadecimal format) for this bridge. Possible values are 00 through 0F.

Displaying VLAN Port Assignments

To display a list of the TrCRFs and TrBRFs to which ports are assigned, select **Local VLAN Port Configuration** on the VLAN and VTP Configuration panel. The Local VLAN Port Configuration panel (Figure 6-12) is displayed.

By default, all local TrCRFs and TrBRFs that are defined on a switch when the switch is started (or restarted) are enabled for the ISL port. However, you can disable a TrCRF or TrBRF for the ISL port.

Figure 6-12 Local VLAN Port Configuration Panel



```
                    Box 1 Local VLAN Port Configuration

Port  Mode   TrCRF                              TrBRF
  1  Static  VLAN_0                             BRF0
  2  Static  VLAN_0                             BRF0
  3  Static  VLAN_0                             BRF0
  4  Static  VLAN_0                             BRF0
  5  Static  VLAN_0                             BRF0
  6  Static  VLAN_1                             BRF1
  7  Static  VLAN_1                             BRF1
  8  Static  VLAN_2                             BRF1
  9  Static  VLAN_2                             BRF1
 10  Static  VLAN_2                             BRF1
 11  Static  trcrf-default                      trbrf-default
 12  Static  trcrf-default                      trbrf-default
 13  Static  trcrf-default                      trbrf-default
 14  Static  trcrf-default                      trbrf-default
 15  Static  trcrf-default                      trbrf-default

                          Return to previous menu
```

This panel displays the following information about the VLAN port assignments:

- Port—Port number.
- Mode—VLAN mode of the port. Possible values are Static and Trunk.
- TrCRF—TrCRF to which the port is currently assigned. By default, all ports are assigned to trcrf-default. For ISL ports, this field lists the TrCRFs that are enabled for the port. If a TrBRF is enabled for an ISL port but none of the related TrCRFs are enabled for the port, this field displays "none".
- TrBRF—Parent VLAN of the TrCRF to which the port is currently assigned. The default is trbrf-default. For ISL ports, this field lists the TrBRFs that are enabled for the port.

To	Select	Then
Change the TrCRF to which the port is assigned...	**Change**	Select the VLAN from the displayed list of TrCRFs.

To	Select	Then
Change the TrCRFs or TrBRFs enabled for an ISL port ...	**Change**	Specify the ISL port to change, select the TrBRF from the list of TrBRFs and enable or disable the TrCRF as desired.
Save your changes...	**Return**	

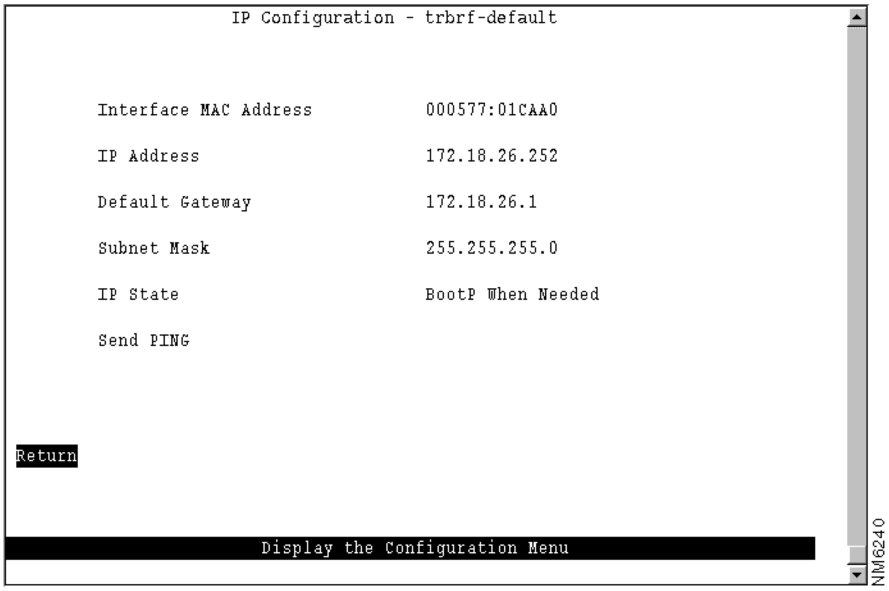
When changing VLAN assignments for an ISL module, keep the following in mind:

- TrBRFs enabled for an ISL port are noted in the TrBRF list with an asterisk.
- To enable a TrBRF for an ISL port, while in the TrBRF list move your cursor to the desired TrBRF and press the space bar.
- To change the enabled state of TrCRF for an ISL port, select the TrBRF (by pressing S) from the TrBRF list and use the space bar to toggle between whether the TrCRF is enabled for the ISL port.
- You cannot select a TrBRF that is not yet enabled for the ISL port. You must first enable the TrBRF for the ISL port.
- If you disable a TrBRF for the ISL port, all TrCRFs for which the TrBRF is a parent are automatically disabled for the ISL port.

Configuring IP Information

To view or change IP information associated with a TrBRF, such as the IP address, subnet mask, or IP state, or to send PINGs, select **IP Configuration** on the Configuration Menu. The IP information that you can configure is associated with a TrBRF. Therefore, if the ports of the Catalyst 3900 are assigned to more than one TrBRF, when you select IP configuration you will be presented with a list of possible TrBRFs from which to choose. The IP Configuration panel (Figure 6-13) is displayed.

Figure 6-13 IP Configuration Panel



```
                      IP Configuration - trbrf-default


         Interface MAC Address           000577:01CAA0

         IP Address                      172.18.26.252

         Default Gateway                 172.18.26.1

         Subnet Mask                     255.255.255.0

         IP State                        BootP When Needed

         Send PING



Return


                        Display the Configuration Menu
```

The following information is displayed on this panel:

- Interface MAC Address—MAC address of the switch.
- IP Address—Current IP address for the TrBRF. The default is 0.0.0.0.
- Default Gateway—Default gateway address. The default is 0.0.0.0.
- Subnet Mask—Current subnet mask. The default is 0.0.0.0.
- IP State—Current IP state. The default for the default TrBRF (trbrf-default) is “BootP When Needed”. The default for all other TrBRFs is “IP Disabled”.
  - IP Disabled—Domain will not process any IP or Address Resolution Protocol (ARP) frames it receives. It will not respond to SNMP, PING, Telnet, or ARP frames that are received.
  - BootP When Needed—If the IP address is zero (0.0.0.0), BootP requests will be broadcast by the Catalyst 3900 in an effort to learn its IP address. All other IP functions are disabled until it receives a reply. If a nonzero IP address has been configured (and stored in NVRAM), IP is enabled for the domain and will function immediately.
  - BootP Always—IP is enabled for the domain, but will not function until a BOOTP reply is received. If a nonzero IP address for the domain is stored in NVRAM, it will be cleared to zero when the Catalyst 3900 is booted.

When you select either of the BootP options for the IP state, the Catalyst 3900 repeats BootP requests at regular intervals, beginning at 1 second intervals and eventually decreasing to 5 minute intervals until it has received a valid response.

The following BootP response parameters are recognized and recorded in NVRAM:

- IP Address
- Default Gateway
- Subnet Mask
- TFTP Bootfile Name
- TFTP Server Address

The BootP requests will also cease if a valid IP address is configured via the console panels or if the IP state is set to IP Disabled. Once the Catalyst 3900 stops sending BootP requests on a domain, it does not resume sending requests or recognize BootP responses on that domain unless the Catalyst 3900 is reset.

For more information about BootP, refer to the appendix “Understanding BootP”.

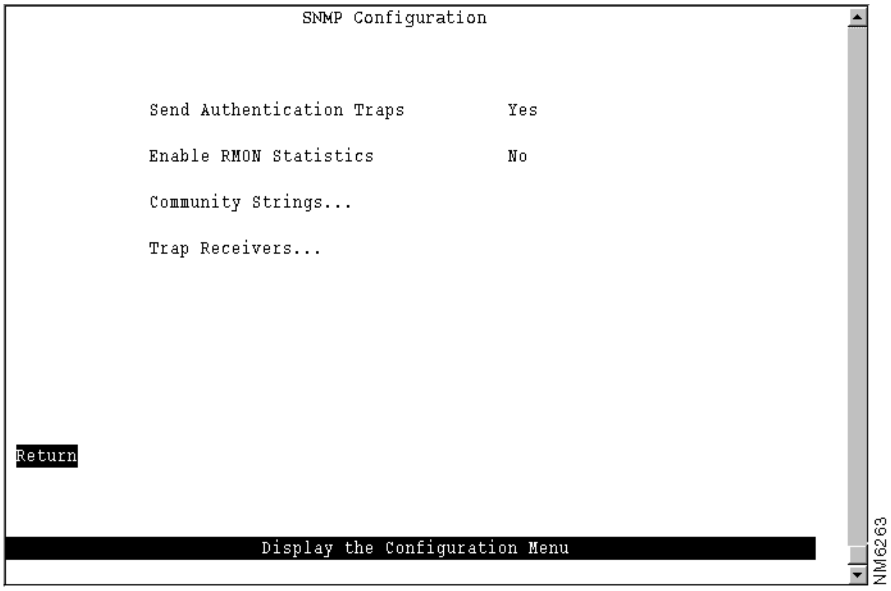
To	Select	Then
Change the current settings...	The appropriate parameter...	Specify the value.
Verify the network availability of a particular resource...	**Send PING**	Specify the IP address of the resource.
Save your changes...	**Return**	

Note IP addresses are always entered in dotted-decimal notation (a set of 4 decimal numbers from 0 through 255 separated by periods). The default is 0.0.0.0. If the default is used, no SNMP management will be available until the switch learns its address.

Configuring SNMP Parameters

To allow the Catalyst 3900 to be managed by an SNMP manager, you must first configure the SNMP parameters. To view or set SNMP parameters, such as the community names, where traps are to be sent, and whether authentication failure traps should be sent, select **SNMP Configuration** on the Configuration Menu. The SNMP Configuration panel (Figure 6-14) is displayed.

Figure 6-14 SNMP Configuration Panel



```
                         SNMP Configuration


            Send Authentication Traps          Yes

            Enable RMON Statistics             No

            Community Strings...

            Trap Receivers...







Return


                     Display the Configuration Menu
```

The following information is displayed on this panel:

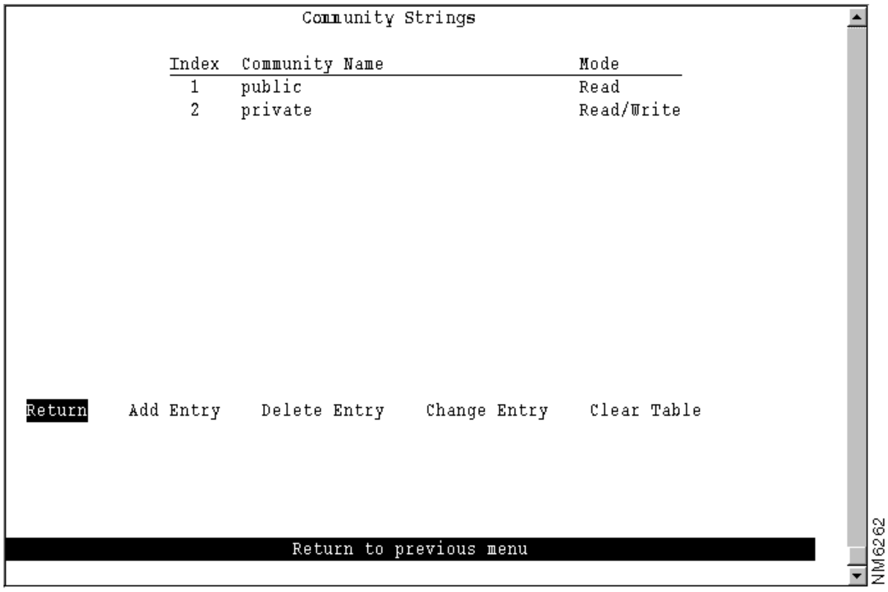
- Send Authentication Traps—Indicates whether an authentication trap should be issued to Trap Receivers whenever authentication of an SNMP request fails. Traps indicating cold and warm boots are always sent. Possible values are Yes and No. The default is Yes.
- Enable RMON statistics—Enables the gathering of a subset of the RMON statistics from the RMON MIB (if you have requested the RMON option). Possible values are Yes and No. Changes to this field are effective after the switch is reset. The default is No. The following statistics are collected:
  - — Token Ring Statistics
  - — History
  - — Events
  - — Alarms

To	Select	Then
Change the current settings…	The appropriate parameter…	Specify the value.
View or change SNMP community names and privileges…	**Community Strings**	Refer to the “Specifying Community Names” section.
View or change which SNMP managers are to receive traps for which domains…	**Trap Receivers**	Refer to the “Specifying Trap Receivers” section.
Save your changes…	**Return**	

Specifying Community Names

A *community name* is a password that a set of SNMP managers use to manage a specified device. Each community name is associated with a specific privilege level of management. To view or change the community names for the domains of the Catalyst 3900, select **Community Strings** on the SNMP Configuration panel. The Community Strings panel (Figure 6-15) is displayed.

Figure 6-15 Community Strings Panel



```
                    Community Strings

          Index  Community Name               Mode
            1    public                       Read
            2    private                      Read/Write
```

The following information is displayed on this panel:

- Index—Identifier of the community name entry.
- Community Name—Name, or password, used to identify the SNMP managers.
- Mode—The privilege level assigned to this name. Read specifies that SNMP managers can only view SNMP information. Read/Write specifies that SNMP managers can both view and change SNMP information.

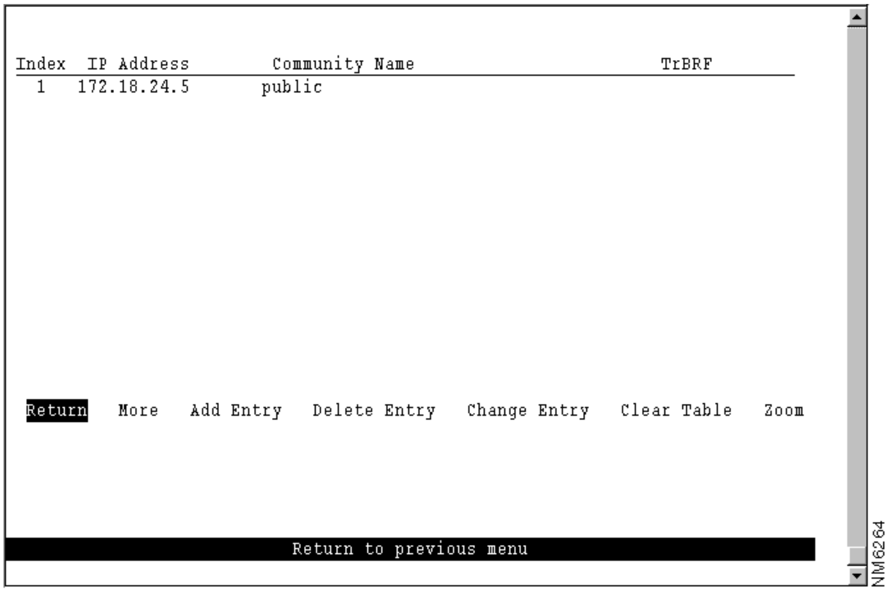
Entries are displayed in the order in which they are entered. Only five community names can be entered.

To	Select	Then
Add a community name…	**Add Entry**	Specify the community name and privilege.
Delete a community name…	**Delete Entry**	Specify the name to be deleted.
Change a community name or privilege…	**Change Entry**	Specify the index number of the entry to be changed and enter the new information.
Delete all community names…	**Clear Table**	
Save your changes…	**Return**	

Specifying Trap Receivers

To view or change the list of SNMP managers to which traps are sent, select **Trap Receivers** on the SNMP Configuration panel. The SNMP Trap Receivers information that you can configure is associated with a TrBRF. Therefore, if the ports of the Catalyst 3900 are assigned to more than one TrBRF and you select **Trap Receivers** on the SNMP Configuration panel, you will be presented with a list of possible TrBRFs from which to choose. The Trap Receivers panel (Figure 6-16) is displayed.

Figure 6-16 Trap Receivers Panel



```
Index  IP Address        Community Name                       TrBRF
  1   172.18.24.5       public
```

The following information is displayed on this panel:

- Index—Identifier of the trap receivers entry.
- IP Address—IP address of the SNMP manager.
- Community Name—Name used to identify the SNMP managers.
- TrBRF—VLANs for which traps are sent to the specified SNMP manager.

The trap receivers list can contain a maximum of six entries.

To	Select	Then
Add an entry to the list…	**Add Entry**	Specify the IP address, community name, and domain.
Delete an entry…	**Delete Entry**	Specify the index number of the entry to be deleted.
Change an entry in the list…	**Change Entry**	Specify the index number of the entry to be changed and enter the new information.
Delete all entries…	**Clear Table**	
Display the complete list of TrBRFs assigned to an IP address…	**Zoom**	Specify the index number.
Save your changes…	**Return**	

Configuring Spanning-Tree Parameters

Enabling the Catalyst 3900 to participate in a spanning tree allows you to configure redundant (backup) paths in the switch topology and have the switch automatically disable redundant paths to prevent loops. If an active path is broken and a backup path is available, the switch will locate the redundant path and enable it. Without a spanning tree, a path failure means the loss of connectivity for the affected part of the network.

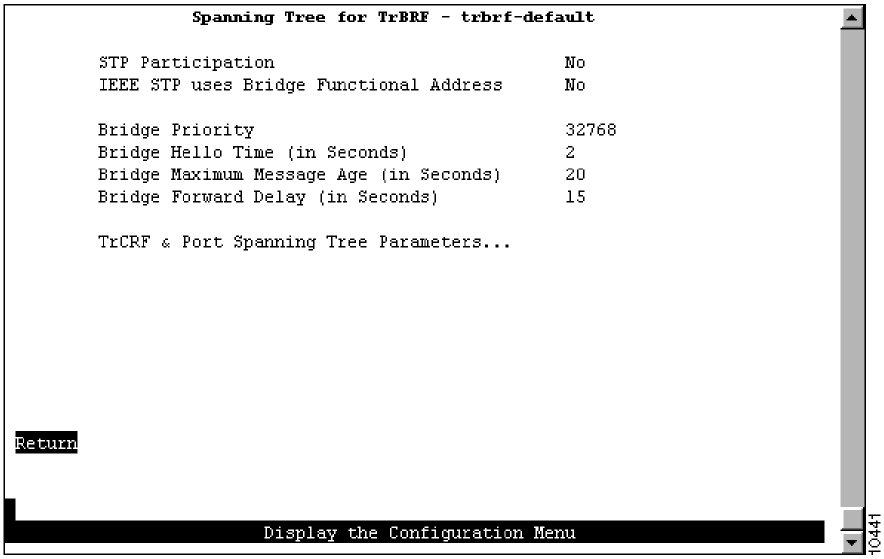
For more information about spanning tree, refer to the “Spanning-Tree Protocol” section of the “Understanding Token Ring Switching” appendix.

To view or change the spanning-tree parameters associated with a VLAN, such as the switch priority and the port path cost, select **Spanning Tree** on the Configuration Menu and then select the desired TrBRF. The Spanning Tree for TrBRF panel (Figure 6-17) is displayed.

When you configure spanning-tree parameters for a TrBRF, you:

- Use the STP Participation field on the Spanning Tree for TrBRF panel to specify whether the TrBRF is to participate in a spanning tree and, if so, which Spanning-Tree Protocol is to be used.
- Use the STP Mode field on the Spanning Tree for TrCRF panel to specify the forwarding state of each logical port in the TrBRF. The forwarding state can be forwarding, blocked, or auto. For a mode of auto, the forwarding state is determined by the Spanning-Tree Protocol.

Figure 6-17 Spanning Tree for TrBRF Panel



```
                 Spanning Tree for TrBRF - trbrf-default

        STP Participation                            No
        IEEE STP uses Bridge Functional Address      No

        Bridge Priority                              32768
        Bridge Hello Time (in Seconds)               2
        Bridge Maximum Message Age (in Seconds)      20
        Bridge Forward Delay (in Seconds)            15

        TrCRF & Port Spanning Tree Parameters...




Return


                        Display the Configuration Menu
```

The following information is displayed on this panel:

- STP Participation—Indicates whether this TrBRF participates in the Spanning-Tree Protocol and, if so, the protocol to be used. Possible values are no, IEEE, IBM, and base on bridging mode. The default is no.
  - — If STP participation is set to no, then all TrCRFs with this TrBRF as a parent will be set to forwarding mode.
  - — If STP participation is set to IEEE or IBM, then the selected protocol will be used to determine the forwarding/blocked mode of the TrCRFs that are configured with an STP mode of auto.

— If STP participation is set to base on bridging mode, then the Spanning-Tree Protocol used is based on the bridging mode of the TrCRF. If the bridging mode is SRB, the IBM Spanning-Tree Protocol is used. If the bridging mode is SRT, the IEEE 802.1d Spanning-Tree Protocol is used.

Note You can create your own spanning tree by setting the STP Participation to no and manually controlling the forwarding state of each logical and physical port using the STP Mode fields. However, if you then decide to use one of the standard Spanning-Tree Protocols and change the STP Participation to a value other than no, you must set the STP Mode for each port to auto. The Catalyst 3900 will not automatically change the forwarding mode of related ports when you change the STP Participation from no to one of the Spanning-Tree Protocols.

- IEEE STP uses Bridge Functional Address—Indicates whether to use the bridge functional address instead of the IEEE Spanning Tree Protocol address when the TrBRF is configured to use the IEEE Spanning Tree Protocol.
- Bridge Priority—Priority value for this Catalyst 3900 (0 through 65535). The lower the priority value, the higher the priority. The bridge or switch with the lowest priority value in a spanning tree becomes the root. The default is 32768.
- Bridge Hello Time (in Seconds)—Time the Catalyst 3900 waits before sending the next configuration message when this Catalyst 3900 is the root switch. The minimum value is 1. The maximum value is the lower of 10 or (Switch Maximum Message Age ÷ 2) – 1. The default is 2.

  The valid range for this parameter is displayed when you select Switch Hello Time.
- Bridge Maximum Message Age (in Seconds)—Maximum message age used when this Catalyst 3900 is the root switch. This parameter sets the time at which the configuration message used by the spanning-tree algorithm should be discarded. The minimum value is the higher of 6 or 2 x (Switch Hello Time + 1). The default is 20.

  The maximum cannot be more than the lower of 40 or 2 x (Switch Forward Delay – 1).

  The range limits that appear when you select this parameter are calculated using the values currently selected for Switch Hello Time and Switch Forward Delay.
- Bridge Forward Delay (in Seconds)—Time the Catalyst 3900 waits between transitions from listening to learning and from learning to forwarding. The minimum is the larger of 4 or (Switch Maximum Message Age ÷ 2) + 1. The default is 15. The maximum is 30.

  The lower range limit that appears when you select this parameter reflects the value currently selected for Switch Maximum Age.

To	Select	Then
Change the current settings…	The appropriate parameter…	Specify the value.
View or change the spanning-tree parameters for one of the TrCRFs associated with this TrBRF…	**TrCRF & Port Spanning Tree Parameters**	Refer to the “Changing Spanning-Tree Parameters for a TrCRF” section.
Save your changes…	**Return**	

Changing Spanning-Tree Parameters for a TrCRF

To view or change the spanning-tree parameters for a TrCRF associated with the selected TrBRF, select **TrCRF & Port Spanning Tree Parameters** on the Spanning Tree panel and then select the desired TrCRF. The Spanning Tree for TrCRF panel (Figure 6-18) is displayed.

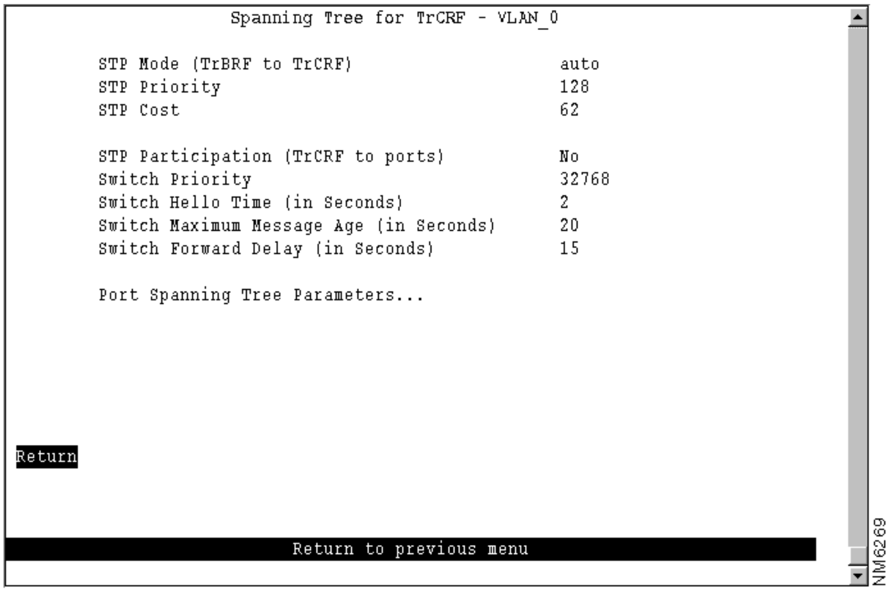
When you configure the spanning-tree parameters for a TrCRF, you:

- Use the STP Participation field on the Spanning Tree for TrCRF panel to specify whether the TrCRF is to participate in a spanning tree and, if so, which Spanning-Tree Protocol is to be used.
- Use the STP Mode field on the Port Spanning Tree Parameters panel to specify the forwarding state of each physical port in the TrCRF. The forwarding state can be forwarding, blocked, or auto. For a mode of auto, the forwarding state is determined by the Spanning-Tree Protocol.

The Spanning-Tree Protocol that is run on the ISL link depends on the type of TrCRF:

- With an undistributed TrCRF, the Spanning-Tree Protocol specified for the TrBRF is used.
- With a default TrCRF, the Spanning-Tree Protocol specified for the TrCRF is used.

Figure 6-18 Spanning Tree for TrCRF Panel



```
                   Spanning Tree for TrCRF - VLAN_0

        STP Mode (TrBRF to TrCRF)                    auto
        STP Priority                                 128
        STP Cost                                     62

        STP Participation (TrCRF to ports)           No
        Switch Priority                              32768
        Switch Hello Time (in Seconds)               2
        Switch Maximum Message Age (in Seconds)      20
        Switch Forward Delay (in Seconds)            15

        Port Spanning Tree Parameters...

Return

                      Return to previous menu
```

The following information is displayed on this panel:

- STP Mode (TrBRF to TrCRF)—Determines the mode of the link from this TrCRF to its TrBRF. Possible values are auto, forwarding, and blocked. If the parent TrBRF is participating in spanning tree, then auto is the default. If the TrBRF is not participating in spanning tree, then forwarding is the default.
- STP Priority—Priority associated with the TrCRF. The VLAN with the lowest priority value has the highest priority and will forward the spanning-tree frames. The possible range is 0 through 255 (decimal). The default is 128. If all VLANs have the same priority value, the lowest VLAN ID forwards the spanning-tree frames. This is the port priority of the internal logical port that connects the TrCRF to its parent TrBRF. This value is used by the TrBRF only if the TrBRF and the TrCRF are both running the IEEE protocol.

- STP Cost—Cost associated with the TrCRF. The Spanning-Tree Protocol uses path costs to determine which VLAN to select as a forwarding VLAN. Therefore, lower numbers should be assigned to VLANs that use faster media (such as FDX or TokenChannel), and higher numbers should be assigned to VLANs that use slower media. The possible range is 1 to 65535. The default is 62. A rule of thumb for the path cost is 1000 ÷ LAN speed in megabits per second.
- STP Participation (TrCRF to ports)—Whether this TrCRF participates in the Spanning-Tree Protocol and, if so, the protocol to be used. Possible values are no, IEEE, and Cisco. The default is no. The Cisco Spanning-Tree Protocol is based on IEEE 802.1d, however, the bridge protocol data unit (BPDU) messages are sent to a different functional address.
    - If STP Participation is set to no, then all ports belonging to this TrCRF will be set to forwarding mode.
    - If STP Participation is set to IEEE or Cisco, then the selected protocol will be used to determine the forwarding/blocking mode of the ports that are configured with an Spanning-Tree Protocol mode of auto.

Note You can create your own spanning tree by setting the STP Participation to no and manually controlling the forwarding state of each logical and physical port using the STP Mode fields. However, if you then decide to use one of the standard Spanning-Tree Protocols and change the STP Participation to a value other than no, you must set the STP Mode for each port to auto. The Catalyst 3900 will not automatically change the forwarding mode of related ports when you change the STP Participation from no to one of the Spanning-Tree Protocols.

- Switch Priority—Priority associated with this Catalyst 3900 (0 through 65535). The lower the priority value, the higher the priority. The bridge or switch with the lowest priority value in a spanning tree becomes the root. The default is 32768. This value is used in the priority field of the Bridge ID used by the TrCRF in the Spanning Tree protocol at TrCRF level.

  To change individual port properties, select **Port Spanning Tree Parameters**.
- Switch Hello Time (in Seconds)—Time the Catalyst 3900 waits before sending the next configuration message when this Catalyst 3900 is the root switch. The minimum value is 1. The maximum value is the lower of 10 or (Switch Maximum Message Age ÷ 2) – 1. The default is 2.

  The valid range for this parameter is displayed when you select Switch Hello Time.
- Switch Maximum Message Age (in Seconds)—Maximum message age used when this Catalyst 3900 is the root switch. This parameter sets the time at which the configuration message used by the spanning-tree algorithm should be discarded. The minimum value is the higher of 6 or 2 x (Switch Hello Time + 1). The default is 20.

  The maximum cannot be more than the lower of 40 or 2 x (Switch Forward Delay – 1).

  The range limits that appear when you select this parameter are calculated using the values currently selected for Switch Hello Time and Switch Forward Delay.
- Switch Forward Delay (in Seconds)—Time the Catalyst 3900 waits between transitions from listening to learning and from learning to forwarding. The minimum is the larger of 4 or (Switch Maximum Message Age ÷ 2) + 1. The default is 15. The maximum is 30.

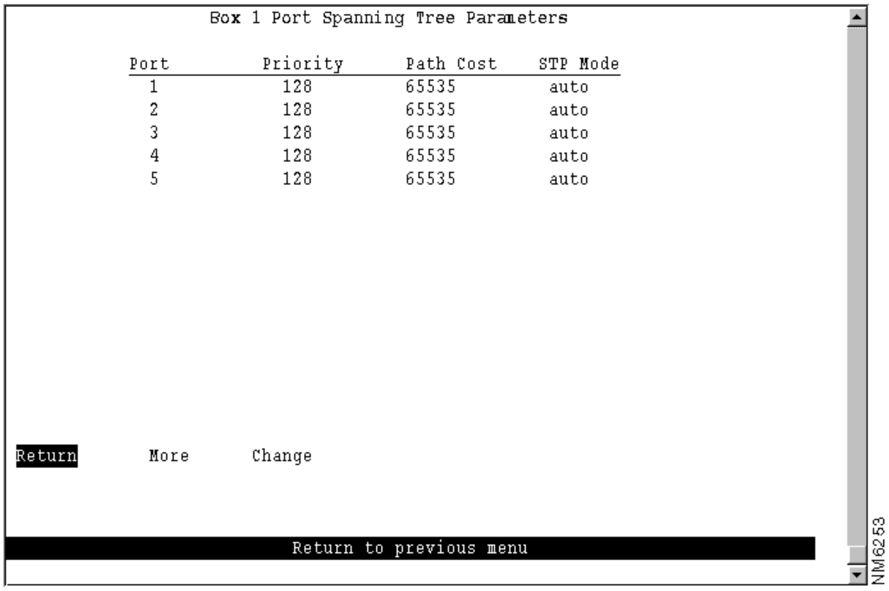
The lower range limit that appears when you select this parameter reflects the value currently selected for Switch Maximum Age.

To	Select	Then
Change the current settings…	The appropriate parameter…	Specify the value.
View or change the spanning-tree parameters for the ports that belong to this TrCRF...	**Port Spanning Tree Parameters**	Refer to the “Changing Spanning-Tree Parameters for a Port” section.
Save your changes…	**Return**	

Changing Spanning-Tree Parameters for a Port

To view or change the priority, path cost, and spanning-tree mode of a port, select **Port Spanning Tree Parameters** on the Spanning Tree panel. The Port Spanning Tree Parameters panel (Figure 6-19) is displayed.

Figure 6-19 Port Spanning Tree Parameters Panel



```
                Box 1 Port Spanning Tree Parameters

          Port          Priority      Path Cost    STP Mode
           1              128          65535         auto
           2              128          65535         auto
           3              128          65535         auto
           4              128          65535         auto
           5              128          65535         auto
```

```
                        Return to previous menu
```

The following information is displayed on this panel:

- Port—Identifier of the port.
- Priority—Priority associated with the port. The port with the lowest priority value has the highest priority and will forward the spanning-tree frames. The possible range is 0 through 255 (decimal). The default is 128. If all ports have the same priority value, the lowest port number forwards the spanning-tree frames.
- Path Cost—Cost associated with the port. The Spanning-Tree Protocol uses port path costs to determine which port to select as a forwarding port. Therefore, lower numbers should be assigned to ports attached to faster media (such as FDX or TokenChannel), and higher numbers should be assigned to ports attached to slower media. The possible range is 1 to 65535. The default is 62. A rule of thumb for path cost is 1000 ÷ LAN speed in megabits per second.

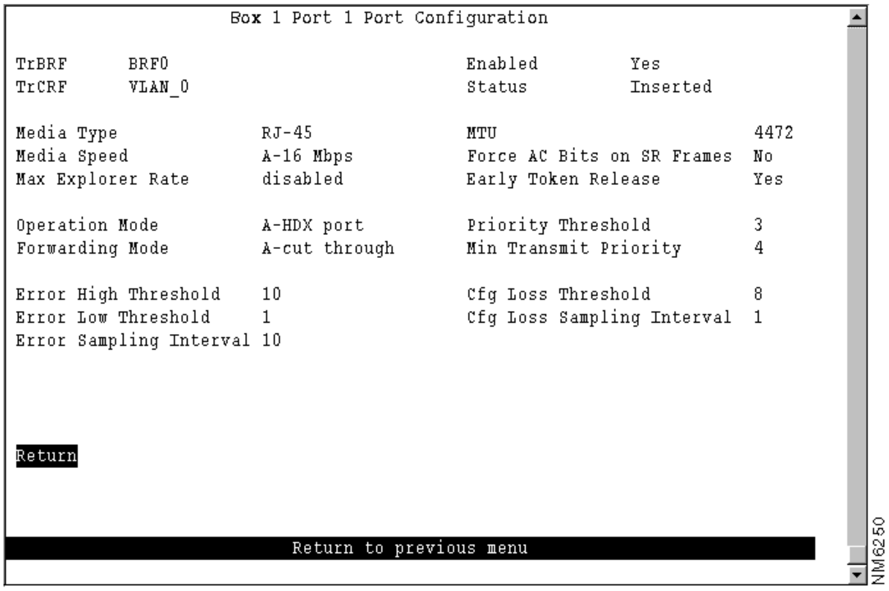
- STP Mode—Port’s spanning-tree mode. Possible values are forwarding, blocked, and auto. If the TrCRF to which the port belongs is participating in the spanning tree (Cisco or IEEE), then auto is the default and the selected protocol will be used to determine whether the port is forwarding or blocked. If the TrCRF to which the port belongs is not participating in the spanning tree, then forwarding is the default.

To	Select	Then
Change a parameter associated with a port…	**Change**	Specify the port number, select the appropriate parameter, and then specify the new value.
Save your changes…	**Return**	

Configuring Port Parameters

To view or change the configuration parameters of a port such as the mode, type, and speed, select **Port Configuration** on the Configuration Menu and specify the port number. The Port Configuration panel (Figure 6-20) is displayed. If you specify the port number of an ATM module, the ATM Configuration panel is displayed. See the “Configuring the ATM Port” section for more information. If you specify the port number of an ISL module, the ISL Port Configuration panel is displayed. See the “Configuring the ISL Port” section for more information.

Figure 6-20 Port Configuration Panel



```
                      Box 1 Port 1 Port Configuration

TrBRF      BRF0                                 Enabled         Yes
TrCRF      VLAN_0                               Status          Inserted

Media Type              RJ-45                   MTU                         4472
Media Speed             A-16 Mbps               Force AC Bits on SR Frames  No
Max Explorer Rate       disabled                Early Token Release         Yes

Operation Mode          A-HDX port              Priority Threshold          3
Forwarding Mode         A-cut through           Min Transmit Priority       4

Error High Threshold    10                      Cfg Loss Threshold          8
Error Low Threshold     1                       Cfg Loss Sampling Interval  1
Error Sampling Interval 10



Return


                            Return to previous menu
```

The following information is displayed on this panel:

- TrBRF—TrBRF that is the parent of the TrCRF to which the port is assigned.
- TrCRF—TrCRF to which this port is assigned.
- Enabled—Indicates whether the port is currently enabled. Possible values are Yes (to enable) and No (to disable). The default is Yes. If a port has been disabled by the Catalyst 3900 software, this field displays **No (auto-disabled)**. To manually enable the port, select this field and then select **Yes.**

- Status—Current status of the port. Possible values are Inserted, Not Inserted, Wire Fault, Lobe Test Fail, HDX Frame Error, Heart Beat Fail, FDX New Station, FDX Prot Error, Speed Error, Remove Received.
- Media Type—Media type as determined by the module to which the port belongs. Possible values are RJ-45 and ST Fiber.
- Media Speed—Token Ring media speed. Possible values are 4 Mbps, 16 Mbps, and auto. The default is auto.

Note A port configured with a media speed of auto will not insert into an empty ring as the port will be unable to determine the media speed.

- Max Explorer Rate—Maximum explorer frame-forwarding rate (in frames per second). Possible values are 0 through 5000 and disabled. The default is disabled. If you set this parameter to 0, no explorers are forwarded. To change the value from a numeric value to disabled, select the field and enter a null value when prompted.
- MTU—Possible values are 1500, 4472, 8144, and 17800. The default is 4472. You cannot configure an MTU greater than 4472 unless you have the Stack Port module Revision B or later installed. Also, you cannot configure a port MTU that is greater than the MTU configured for the TrBRF to which the port belongs.
- Force AC Bits on SR Frames—Indicates whether the address recognized (A) bit and the frame copied (C) bit should be set unconditionally on repeated source-routed LLC frames. These include source-routed frames with RIF length greater than 2 and all spanning-tree explorer and all-routes explorer frames. The default is no. If this parameter is set to no, the setting of these bits is based on whether the frame was actually forwarded.
- Early Token Release—Indicates whether the port is enabled for Early Token Release. Possible values are Yes and No. The default is Yes. Early Token Release is valid for 16 Mbps media only. If the Early Token Release is set to Yes and the media speed is 4 Mbps, the switch will force Early Token Release to No.
- Operation Mode—Port operation mode. Possible values are auto, HDX port, HDX station, FDX port, FDX station, and RI/RO. The default is auto. Only HDX and FDX modes can be automatically detected. The operation mode of RI/RO can be set for ports 19 and 20 only.
- Forwarding Mode—Forwarding mode that will be used to transmit frames. Possible values are auto, cut through, and store & forward. The default is auto. If the forwarding mode is set to auto, the actual mode will depend on the number of errors that occur during the sampling interval. If the error rate is below the error low threshold, then cut-through mode is used. If the error rate is above the error high threshold, then store & forward is used. Store & forward mode is always used for ports with a media speed of 4 Mbps.
- Priority Threshold—Highest Token Ring frame priority in the Frame Control field of the frame that the switch should place in the low-priority transmit queue. Possible values are 0 through 7. The default is 3.
- Min Transmit Priority—Minimum reservation priority used when requesting a token on a busy ring. Possible values are 0 through 6. The default is 4.
- Error High Threshold—Value (in percentage) used to force a port to store & forward mode. When the percentage of errors detected in the error sampling interval is more than the error high threshold, then the port is forced to store-and-forward mode. Possible values are 0 through 100. The default is 10. This field is valid only when the forwarding mode is set to auto.

- Error Low Threshold—Value (in percentage) used to return a port to cut-through mode. When the percentage of errors detected in the error sampling interval is less than the error low threshold, then the port is allowed to return to cut-through mode. Possible values are 0 through 100. The default is 1. This field is valid only when the forwarding mode is set to auto.
- Error Sampling Interval—Sampling period (in minutes) used when counting errors to determine a port's forwarding mode. Possible values are 1 through 60. The default is 10. This field is valid only when the forwarding mode is set to auto.
- Cfg Loss Threshold—Value used to control the number of configuration losses that can occur within the configuration loss sampling interval. Configuration loss occurs when a port completes a connection, allows data traffic to flow, and subsequently closes. When the threshold is exceeded, the port is disabled and must be enabled via this panel or an SNMP manager. Possible values are 1 through 100. The default is 8.
- Cfg Loss Sampling Interval—Sampling period (in minutes) used when measuring the number of configuration losses occurring. Possible values are 1 through 60. The default is 1.

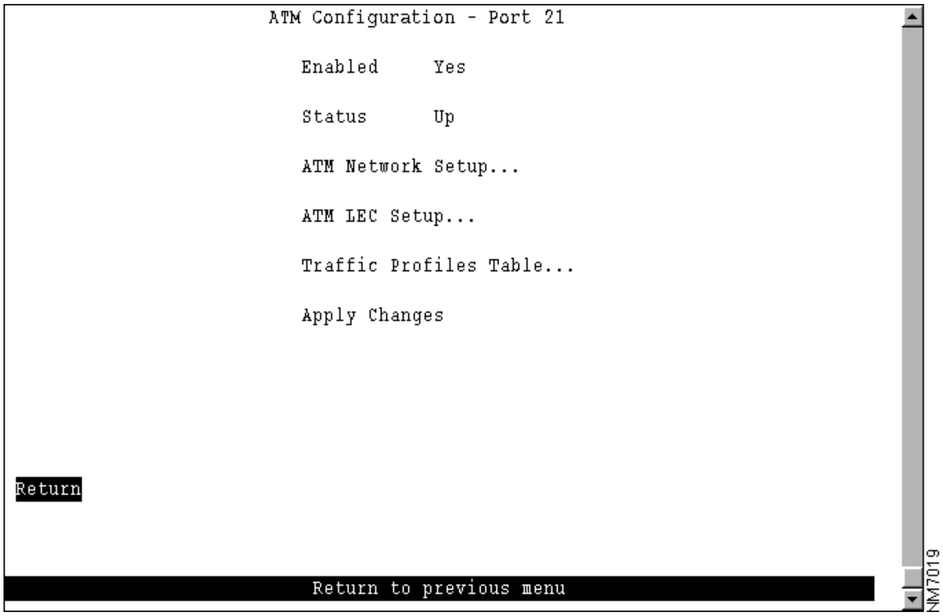
Note If you change any configuration parameters of a connected port, the port will close and reopen and you will lose all address information and statistics for that port.

To	Select	Then
Change the current settings...	The appropriate parameter...	Specify the new value.
Save your changes…	**Return**	

Configuring the ATM Port

To configure your ATM expansion module, select **Port Configuration** from the Configuration Menu panel. You are prompted to specify the port you want to configure. When you specify a port on an ATM module, the ATM Configuration panel (Figure 6-21) is displayed. The possible port numbers for the ATM module are 21 (if the module is installed in slot 1) and 25 (if the module is installed in slot 2).

Figure 6-21 ATM Configuration Panel



```
                     ATM Configuration - Port 21

                        Enabled     Yes

                        Status      Up

                        ATM Network Setup...

                        ATM LEC Setup...

                        Traffic Profiles Table...

                        Apply Changes



Return

                        Return to previous menu
```

The following information is displayed on this panel:

- Enabled—Indicates whether the ATM port is enabled. Possible values are Yes and No. The default is Yes.
- Status—Current status of the port. Possible values are Down, Going Up, Up, Going Down, and Failing. You cannot change this field.

The following options are displayed on this panel:

- ATM Network Setup—Select this option to define ATM network parameters for the specified port. Refer to the "Configuring ATM Network Parameters" section for more information.
- ATM LEC Setup—Select this option to define parameters for the LEC. Refer to the "Configuring LEC Parameters" section for more information.
- Traffic Profiles Table—Select this option to configure the traffic profiles table. Refer to the "Configuring Traffic Profiles Tables" section for more information.

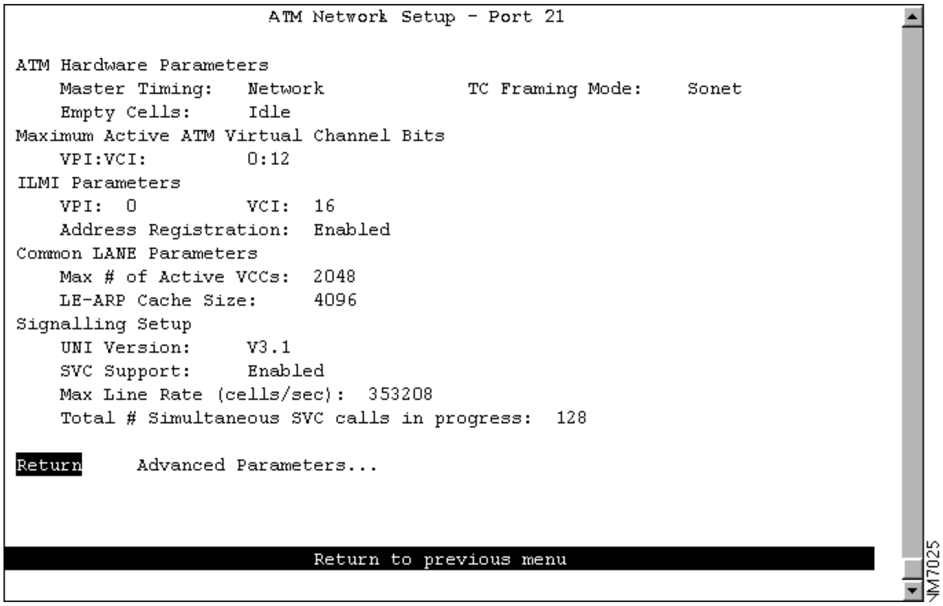
When you change a parameter on a panel and select Return, the change is saved in NVRAM. The change will not be implemented, however, until you restart the Catalyst 3900 or select **Apply Changes**.

Caution Selecting **Apply Changes** will cause all emulated LANs to close and could, therefore, disrupt the network.

Configuring ATM Network Parameters

To configure ATM physical-layer network parameters, select **ATM Network Setup** from the ATM Configuration panel. The ATM Network Setup panel (Figure 6-22) is displayed.

Figure 6-22 ATM Network Setup Panel



```
                        ATM Network Setup - Port 21

ATM Hardware Parameters
    Master Timing:   Network             TC Framing Mode:    Sonet
    Empty Cells:     Idle
Maximum Active ATM Virtual Channel Bits
    VPI:VCI:         0:12
ILMI Parameters
    VPI:  0          VCI:  16
    Address Registration:  Enabled
Common LANE Parameters
    Max # of Active VCCs:  2048
    LE-ARP Cache Size:     4096
Signalling Setup
    UNI Version:     V3.1
    SVC Support:     Enabled
    Max Line Rate (cells/sec):  353208
    Total # Simultaneous SVC calls in progress:  128

Return     Advanced Parameters...



                            Return to previous menu
```

The following information is displayed on this panel:

- ATM Hardware Parameters
  - — Master Timing—Source of the transmit timing. Possible values are Local and Network. The default is Network.
  - — TC Framing Mode—Transmission convergence framing mode. Possible values are Sonet and SDH. The default is Sonet.
  - — Empty Cells—Idle cell generation mode. Possible values are Idle and Unassigned. The default is Idle.
- Maximum Active ATM Virtual Channel Bits
  - — VPI:VCI—Maximum active Virtual Path Identifier (VPI) and Virtual Connection Identifier (VCI) bit combination. Possible values are 0:12, 1:11, 2:10. The default is 0:12.
- ILMI Parameters
  - — VPI—VPI for the ILMI. Possible values are 0 through 3. The default is 0.
  - — VCI—VCI for the ILMI. Possible values are 0 through 4095. The default is 4095.
  - — Address Registration—Indicates whether to enable ILMI address registration support. Possible values are Enabled and Disabled. The default is Enabled.
- Common LANE Parameters
  - — Max # of Active VCCs—Maximum number of concurrently open Virtual Channel Connections VCCs. Possible values are 10 through 2048. The default is 2048.
  - — LE-ARP Cache Size—Size (in bytes) of the LAN Emulation-Address Resolution Protocol (LE-ARP) cache. Possible values are 256 through 4096. The default is 4096.

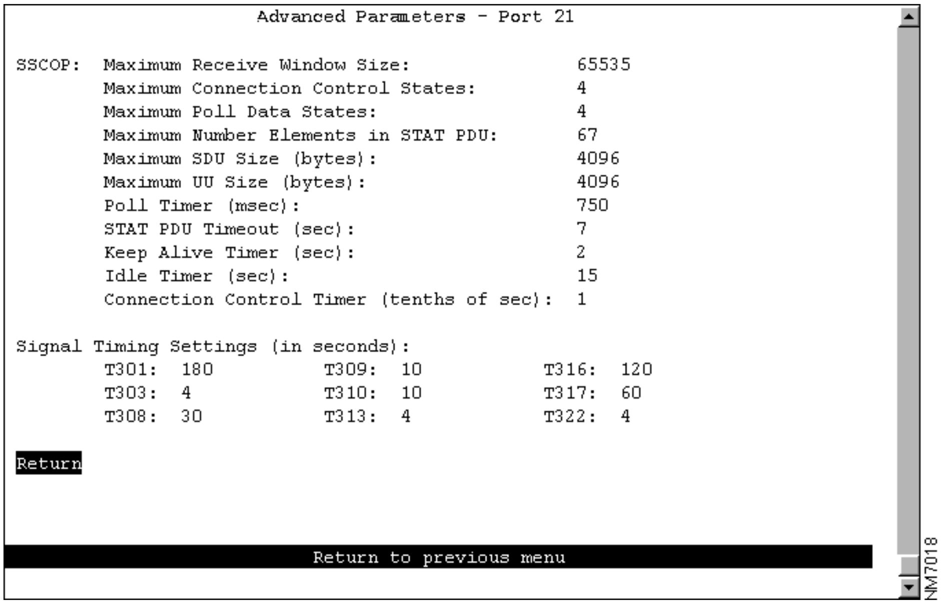
- Signalling Setup
  - — UNI Version—User-Network Interface (UNI) version. Possible values are V3.0, V3.1, and V4.0. The default is V3.1.
  - — SVC Support—Indicates whether Switched Virtual Connection (SVC) support is enabled. Possible values are Enabled and Disabled. The default is Enabled.
  - — Max Line Rate (cells/sec)—Maximum line rate in cells per second. Possible values are 1 through 353208.
  - — Total # Simultaneous SVC calls in progress—Maximum number of SVC calls that can be processed simultaneously. Possible values are 1 through 128. The default is 128.

To	Select	Then
Change the current settings...	The appropriate parameter...	Specify the value.
Configure advanced ATM parameters...	**Advanced Parameters**	Refer to the "Configuring Advanced ATM Parameters" section.
Save your changes...	**Return**	

Configuring Advanced ATM Parameters

To configure advanced ATM parameters, select **Advanced Parameters** on the ATM Network Setup panel. The Advanced Parameters panel (Figure 6-23) is displayed. We recommend only experienced users configure the parameters listed on this panel. Changing these parameters may impact your network, therefore, use caution when altering the values for these parameters.

Figure 6-23 Advanced Parameters Panel



```
                       Advanced Parameters - Port 21

SSCOP:  Maximum Receive Window Size:              65535
        Maximum Connection Control States:        4
        Maximum Poll Data States:                 4
        Maximum Number Elements in STAT PDU:      67
        Maximum SDU Size (bytes):                 4096
        Maximum UU Size (bytes):                  4096
        Poll Timer (msec):                        750
        STAT PDU Timeout (sec):                   7
        Keep Alive Timer (sec):                   2
        Idle Timer (sec):                         15
        Connection Control Timer (tenths of sec): 1

Signal Timing Settings (in seconds):
        T301:  180          T309:  10           T316:  120
        T303:  4            T310:  10           T317:  60
        T308:  30           T313:  4            T322:  4

Return



                         Return to previous menu
```

The following information is displayed on this panel:

- SSCOP
    - Maximum Receive Window Size—Maximum size of the SSCOP receive window. Possible values are 1 through 16777215. The default is 65535.
    - Maximum Connection Control States—Maximum number of transmissions of a BGN (establishment), END (release), ER (error recovery), or RS (resynchronization) protocol data unit. Possible values are 1 through 255. The default is 4.
    - Maximum Poll Data States—Maximum number of transmissions between polls. Possible values are 1 through 255. The default is 4.
    - Maximum Number Elements in STAT PDU—Maximum number of list elements placed in a STAT protocol data unit. Possible values are (odd numbers) from 3 through 1023. The default is 67.
    - Maximum SDU Size (bytes)—Maximum size (in bytes) of the SSCOP SAAL service data unit. Possible values are 512 through 16384. The default is 4096.
    - Maximum UU Size (bytes)—Maximum size (in bytes) of the SSCOP user-to-user data unit. Possible values are 512 through 16384. The default is 4096.
    - Poll Timer (msec)—Peer poll time (in milliseconds). Possible values are 1 through 10000. The default is 750.
    - STAT PDU Timeout (sec)—Maximum interval (in seconds) for receiving a STAT protocol data unit. Possible values are 1 through 255. The default is 7.
    - Keep Alive Timer (sec)—Interval (in seconds) at which keep alive messages are sent. Possible values are 1 through 255. The default is 2.
    - Idle Timer (sec)—Period (in seconds) during which no POLL protocol data units are sent. Possible values are 1 through 255. The default is 15.
    - Connection Control Timer (tenths of sec)—Maximum time (in tenths of seconds) to wait for a response during the outgoing link establish, release, resynchronize, and recovery phases. Possible values are 1 through 255. The default is 1.
- Signal Timing Settings (in seconds)
    - T301—Maximum time (in seconds) to wait for a connect after receiving an alert. Possible values are 1 through 65535. The default is 180.
    - T303—Maximum time (in seconds) to wait for a network response to a setup request. Possible values are 1 through 255. The default is 4.
    - T308—Maximum time (in seconds) to wait for a network response to a release request. Possible values are 1 through 255. The default is 30.
    - T309—Maximum time (in seconds) to wait during a SSCOP connection loss. Possible values are 1 through 255. The default is 10.
    - T310—Maximum time (in seconds) to wait for a final response after receiving a call proceeding. Possible values are 1 through 255. The default is 10.
    - T313—Maximum time (in seconds) to wait for a network response to a connect request. Possible values are 1 through 255. The default is 4.
    - T316—Maximum time (in seconds) to wait for a network response to a restart request. Possible values are 1 through 255. The default is 120.

- — T317—Maximum time (in seconds) to act on a restart request. Possible values are 1 through 255. The default is 60.
- — T322—Maximum time (in seconds) to wait for a network response to a status enquiry request. Possible values are 1 through 255. The default is 4.

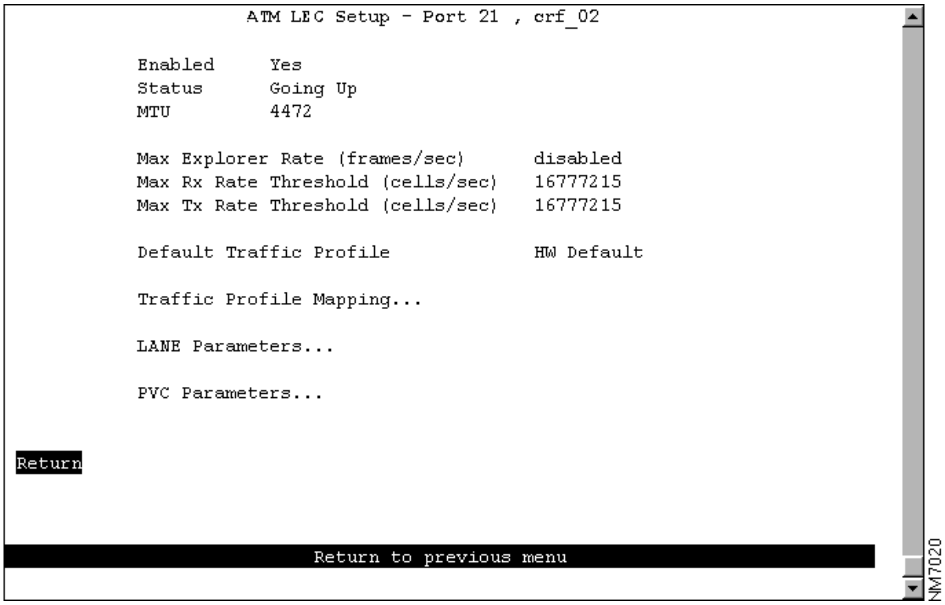
To	Select	Then
Change the current settings...	The appropriate parameter...	Specify the value.
Save your changes...	**Return**	

Configuring LEC Parameters

Before you can configure parameters for an LEC, you must first assign the module to a TrCRF and TrBRF. Only one TrCRF per TrBRF can contain an ATM port, therefore, you cannot bridge traffic between emulated LANs. For more information about defining TrCRFs and TrBRFs, refer to the “Configuring VLANs and VTP” section of the *Catalyst 3900 Token Ring Switch User Guide*.

To configure LEC parameters, select **ATM LEC Setup** from the Configuration panel. Select the TrCRF to which the module is assigned. The ATM LEC Setup panel (Figure 6-24) is displayed.

Figure 6-24 ATM LEC Setup Panel



```
                    ATM LEC Setup - Port 21 , crf_02

          Enabled     Yes
          Status      Going Up
          MTU         4472

          Max Explorer Rate (frames/sec)      disabled
          Max Rx Rate Threshold (cells/sec)   16777215
          Max Tx Rate Threshold (cells/sec)   16777215

          Default Traffic Profile             HW Default

          Traffic Profile Mapping...

          LANE Parameters...

          PVC Parameters...


Return


                         Return to previous menu
```

The following information is displayed on this panel:

- Enabled—Administrative status for this LEC. Possible values are Yes and No. The default is Yes.
- Status—Current status of the LEC. Possible values are Disabled, Going Up, Up, Going Admin Down, Admin Down, Failing, Waiting for Module Up, and Forwarding. You cannot change this field.
- MTU—Maximum transmission unit. Possible values are 1500, 4472, 8144, and 17800. The default is 4472.

- Max Explorer Rate (frames/sec)—Maximum explorer frame-forwarding rate (in frames per second). Possible values are 0 through 5000 and disabled. The default is disabled. If you set this parameter to 0, no explorers are forwarded. To change the value from a numeric value to disabled, select the field and enter a null value (by pressing Enter without specifying any value).
- Max Rx Rate Threshold (cells/sec)—Maximum difference between the requested receive rate and the line rate (in cells per second) beyond which the call is rejected. Possible values are 0 through 16777215. The default is 16777215.
- Max Tx Rate Threshold (cells/sec)—Maximum difference between the requested transmit rate and the closest matching profile (in cells per second) beyond which the call is rejected. Possible values are 0 through 16777215. The default is 16777215.
- Default Traffic Profile—Traffic profile to be used as the default. Possible values are 0 through 63. If you specify a null entry, the hardware default (255) is used.

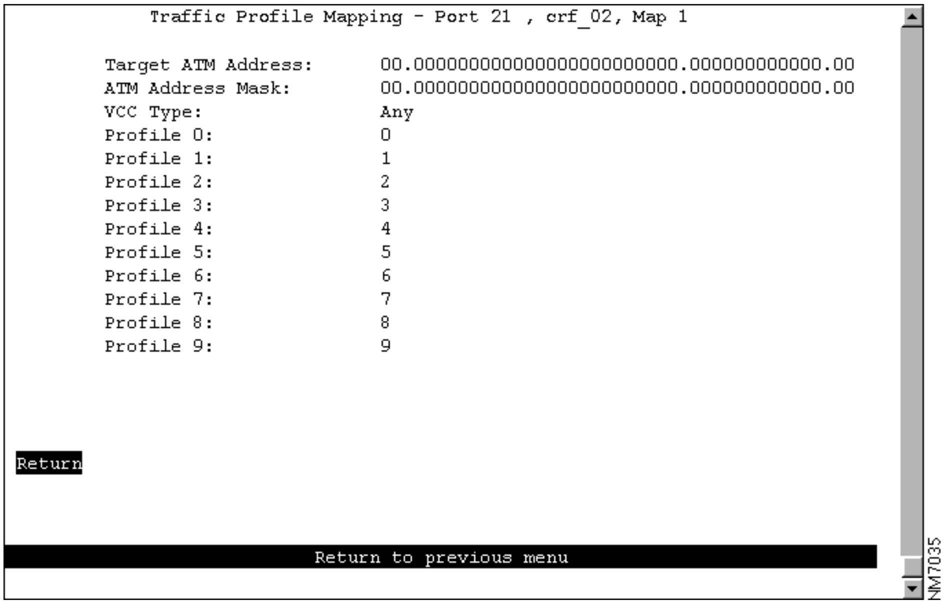
The following options are displayed on this panel:

- Traffic Profile Mapping—Select this option to map traffic profiles for this emulated LAN. Refer to the “Configuring Traffic Profile Mapping” section for more information.
- LANE Parameters—Select this option to configure LAN emulation parameters for this emulated LAN. Refer to the “Configuring LANE Parameters” section for more information.
- PVC Parameters—Select this option to configure PVCs for this emulated LAN. Refer to the “Configuring PVC Parameters” section for more information.

Configuring Traffic Profile Mapping

To define the list of traffic profiles to be used for mapping outgoing traffic, select **Traffic Profile Mapping** on the ATM LEC Setup panel and specify the map number (0 through 9). The Traffic Profile Mapping panel (Figure 6-25) is displayed.

Figure 6-25 Traffic Profile Mapping Panel



```
            Traffic Profile Mapping - Port 21  , crf_02, Map 1

        Target ATM Address:       00.0000000000000000000000000.000000000000.00
        ATM Address Mask:         00.0000000000000000000000000.000000000000.00
        VCC Type:                 Any
        Profile 0:                0
        Profile 1:                1
        Profile 2:                2
        Profile 3:                3
        Profile 4:                4
        Profile 5:                5
        Profile 6:                6
        Profile 7:                7
        Profile 8:                8
        Profile 9:                9



Return


                          Return to previous menu
```

The following information is displayed on this panel:

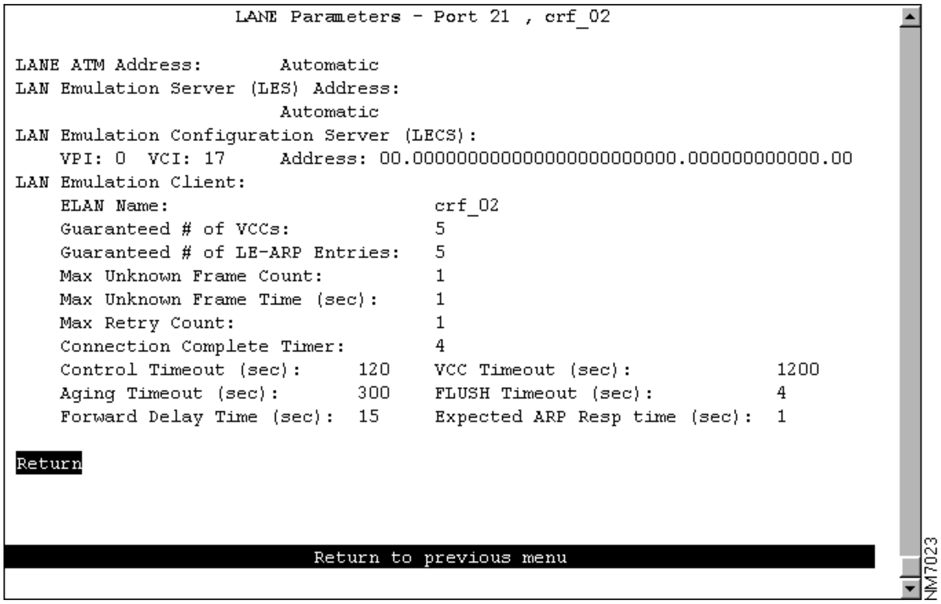
- Target ATM Address—Destination ATM address to which to apply this traffic profile map.
- ATM Address Mask—Bit mask to be applied to the address before comparing it with the Target ATM Address.
- VCC Type—VCC type to which to apply this traffic profile map. Possible values are Any, Data, Direct, Distribute, Send, and Forward. The default is Any.
- Profile 0 through 9—Indentifier of the entry in the traffic profile table. Possible values are 0 through 63. The default for each profile is 0 through 9 respectively.

To	Select	Then
Change the current settings...	The appropriate parameter...	Specify the value.
Save your changes...	**Return**	

Configuring LANE Parameters

To configure LANE parameters for this LEC, select **LANE Parameters** on the ATM LEC Setup panel. The LANE Parameters panel (Figure 6-26) is displayed.

Figure 6-26 LANE Parameters Panel



```
                    LANE Parameters - Port 21 , crf_02

LANE ATM Address:       Automatic
LAN Emulation Server (LES) Address:
                        Automatic
LAN Emulation Configuration Server (LECS):
    VPI: 0  VCI: 17     Address: 00.000000000000000000000000.000000000000.00
LAN Emulation Client:
    ELAN Name:                        crf_02
    Guaranteed # of VCCs:             5
    Guaranteed # of LE-ARP Entries:   5
    Max Unknown Frame Count:          1
    Max Unknown Frame Time (sec):     1
    Max Retry Count:                  1
    Connection Complete Timer:        4
    Control Timeout (sec):     120    VCC Timeout (sec):             1200
    Aging Timeout (sec):       300    FLUSH Timeout (sec):           4
    Forward Delay Time (sec):  15     Expected ARP Resp time (sec):  1

Return



                          Return to previous menu
```

The following information is displayed on this panel:

- LANE ATM Address—Indicates whether the ATM address for this emulated LAN is assigned manually or automatically. Possible values are Manual and Automatic. The default is Automatic. If the address is assigned manually, this field also displays the address.
- LAN Emulation Server (LES) Address—Indicates whether the ATM address of the LES is obtained automatically or manually. If you select Manual, you must specify the ATM address of the LES. If the LES address is specified, then the LECS information is not needed.

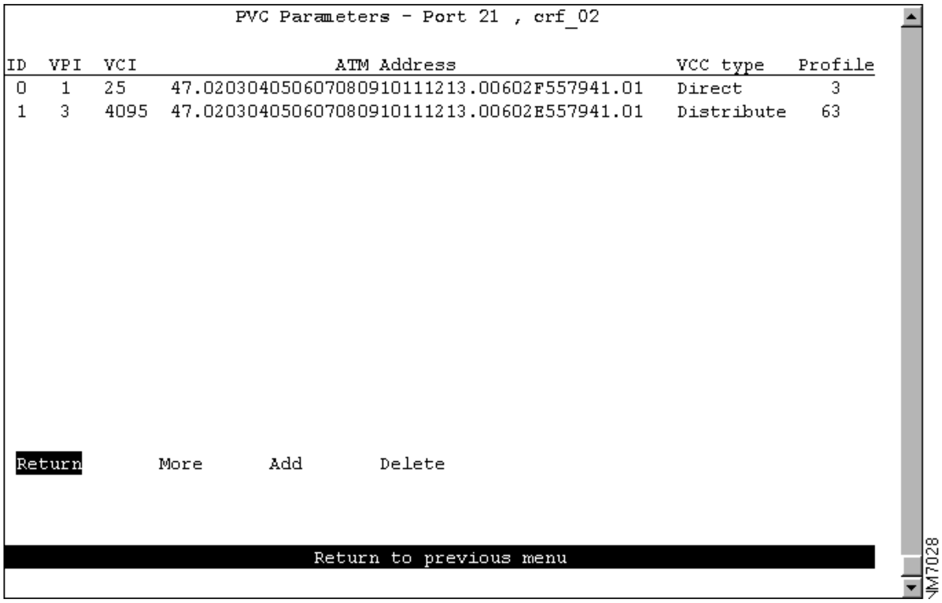
- LAN Emulation Configuration Server (LECS)
    - VPI—VPI of the LECS to which this emulated LAN connects. Possible values are 0 through 3. The default is 0.
    - VCI—VCI of the LECS to which this emulated LAN connects. Possible values are 0 through 4095. The default is 17.
    - Address—ATM address of the LECS.
- LAN Emulation Client
    - ELAN Name—Name of the preferred emulated LAN to join.
    - Guaranteed # of VCCs—Guaranteed number of VCCs. Possible values are 5 through 2048. The default is 5.
    - Guaranteed # of LE-ARP Entries—Guaranteed number of LE-ARP entries. Possible values are 2 through 4096. The default is 2.
    - Max Unknown Frame Count—Maximum number of frames that can be sent to a unicast MAC address within the Max Unknown Frame Time. Possible values are 1 through 10. The default is 1.
    - Max Unknown Frame Time (sec)—Time (in seconds) during which the Max Unknown Frame Count is measured. Possible values are 1 through 60. The default is 1.
    - Max Retry Count—Maximum number of LE-ARP retries for a given destination. Possible values are 0 through 2. The default is 1.
    - Connection Complete Timer—Length of time (in seconds) in which the LEC expects data or a READY_IND message from a calling party. Possible values are 1 through 10. The default is 4.
    - Control Timeout (sec)—Amount of time (in seconds) before most request/response frames are timed out. Possible values are 10 through 300. The default is 120.
    - VCC Timeout (sec)—Length of time (in seconds) after which the LEC will release a VCC if the VCC has not been used to transmit or receive any frames. Possible values are 10 through 1200. The default is 1200.
    - Aging Timeout (sec)—Maximum time (in seconds) between LE-ARP verifications for a DD-VCC. Possible values are 10 through 300. The default is 300.
    - FLUSH Timeout (sec)—FLUSH protocol time period. Possible values are 1 through 4. The default is 4.
    - Forward Delay Time (sec)—Maximum time (in seconds) that a remote destination table entry may keep a DD-VCC without LE-ARP verification. Possible values are 0 through 30. The default is 15.
    - Expected ARP Response time (sec)—Maximum time (in seconds) the LEC will wait for a flush response after sending a flush request. If this value is exceeded, the LEC will take recovery action. Possible values are 1 through 30. The default is 1.

To	Select	Then
Change the current settings...	The appropriate parameter...	Specify the value.
Save your changes...	**Return**	

Configuring PVC Parameters

To configure the PVCs to be assigned to this LEC, select **PVC Parameters** on the ATM LEC Setup panel. The PVC Parameters panel (Figure 6-27) is displayed.

Figure 6-27 PVC Parameters Panel



```
                         PVC Parameters - Port 21 , crf_02

ID  VPI  VCI                   ATM Address                          VCC type   Profile
 0    1  25     47.02030405060708091011213.00602F557941.01   Direct         3
 1    3  4095   47.02030405060708091011213.00602E557941.01   Distribute    63
```

```
                              Return to previous menu
```

The following information is displayed on this panel:

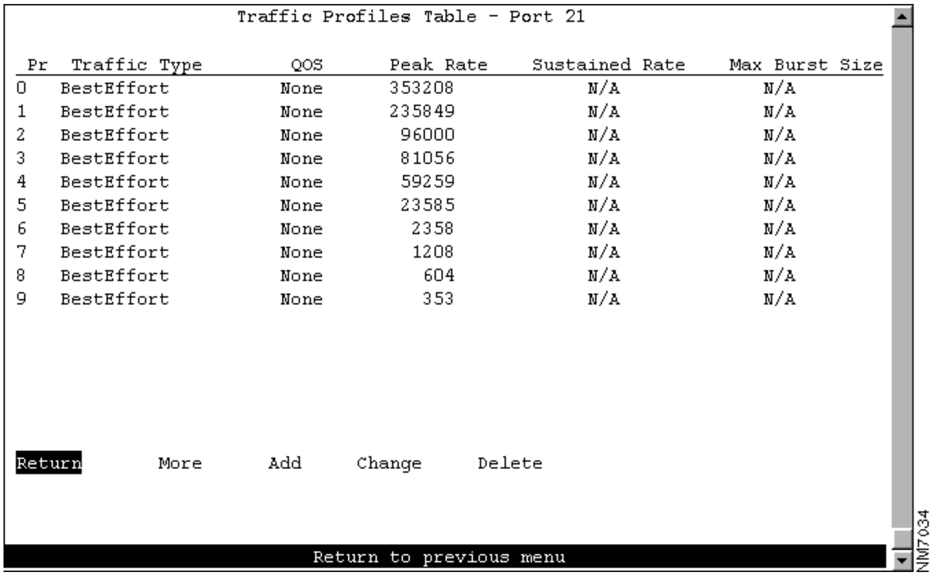
- ID—Identifier of the PVC entry.
- VPI—VPI of this PVC. Possible values are 0 through 3.
- VCI—VCI of this PVC. Possible values are 0 through 4095.
- ATM Address—ATM address of this PVC.
- VCC Type—Type of VCC connection to this PVC. Possible values are Data, Direct, Distribute, Send, and Forward.
- Profile—Traffic profile (from the traffic profile table) to be used. Possible values are 0 through 63.

To	Select	Then
Add a PVC...	**Add**	Specify the VPI, VCI, ATM address, VCC type, and profile.
Delete a PVC...	**Delete**	
Save your changes...	**Return**	

Configuring Traffic Profiles Tables

To configure the traffic profile table, select **Traffic Profiles Table** on the ATM Configuration panel. The Traffic Profiles Table panel (Figure 6-28) is displayed.

Figure 6-28 Traffic Profile Table Panel



```
                      Traffic Profiles Table - Port 21

 Pr  Traffic Type        QOS      Peak Rate    Sustained Rate    Max Burst Size
0   BestEffort          None     353208            N/A              N/A
1   BestEffort          None     235849            N/A              N/A
2   BestEffort          None      96000            N/A              N/A
3   BestEffort          None      81056            N/A              N/A
4   BestEffort          None      59259            N/A              N/A
5   BestEffort          None      23585            N/A              N/A
6   BestEffort          None       2358            N/A              N/A
7   BestEffort          None       1208            N/A              N/A
8   BestEffort          None        604            N/A              N/A
9   BestEffort          None        353            N/A              N/A




Return        More      Add      Change      Delete



                          Return to previous menu
```

The following information is displayed on this panel:

- Pr—Identifier of the profile in the table. Possible values are 0 through 63.
- Traffic Type—Possible values are NoClpNoScr (no cell loss priority/no sustained cell rate), NoClpScr (no cell loss priority/sustained cell rate), ClpNo-TaggingScr (cell loss priority/no tagging sustained cell rate) ClpTaggingScr (cell loss priority/ tagging sustained cell rate), and BestEffort. The default is BestEffort.

  Normally, traffic profiles used with LAN Emulation, Classical IP, or Multiprotocol Encapsulation over ATM are of type BestEffort (or UBR). For this type of traffic profile, the network does not guarantee any specific bandwidth.

  For a BestEffort traffic profile, the Peak Rate is the only valid parameter. The Peak Rate parameter can be used to limit the maximum transmission rate that the adapter will use to avoid congestion if the device at the other end of the connection is a slower device.
- QOS—Quality of Service. Possible values are Class 1, Class 2, Class 3, Class 4, and None. The default is None.
- Peak Rate—Maximum rate (in kilobits per second) at which a virtual circuit can transmit. Possible values are 353 through 353208.
- Sustained Rate—Average rate (in kilobits per second) at which a virtual circuit can transmit. Possible values are 353 through 353208 and N/A. This parameter is not applicable if the Traffic Type is BestEffort.
- Max Burst Size—Maximum number of ATM cells the virtual circuit can transmit to the network at the peak rate of the PVC. Possible values are 0 through 356 and N/A. This parameter is not applicable if the Traffic Type is BestEffort.

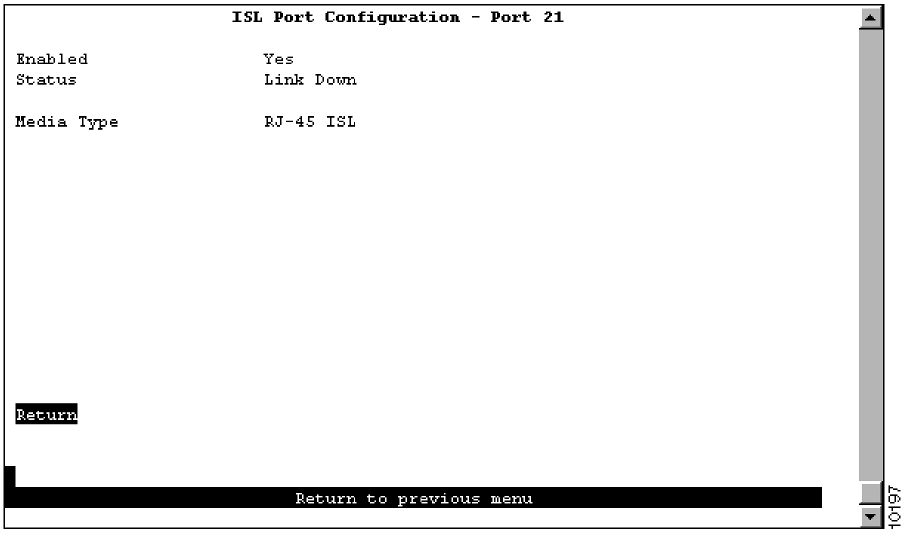
To	Select	Then
Add an entry	**Add**	Specify the profile identifier, traffic type, QOS, peak rate, sustained rate, and maximum burst size.

To	Select	Then
Change the current settings...	**Change**	Specify the profile identifier, traffic type, QOS, peak rate, sustained rate, and maximum burst size.
Remove an entry	**Delete**	Specify the profile identifier.
Save your changes...	**Return**	

Configuring the ISL Port

To configure port parameters your ISL expansion module, select **Port Configuration** from the Configuration Menu panel. You are prompted to specify the port you want to configure. When you specify a port on an ISL module, the ISL Port Configuration panel (Figure 6-29) is displayed. The possible port values for the 2-port ISL expansion module are 21 and 23 (if the module is inserted in slot 1) and 25 and 27 (if the module is inserted in slot 2).

Figure 6-29 ISL Port Configuration Panel



```
                    ISL Port Configuration - Port 21

Enabled                 Yes
Status                  Link Down

Media Type              RJ-45 ISL











Return


                         Return to previous menu
```

The following information is displayed on this panel:

- Enabled—Indicates whether the ISL port is enabled. Possible values are Yes and No. The default is Yes.
- Status—Current status of the port. Possible values are Link Up, if the module is up and operational, or Link Down, if the module is not up and operational. You cannot change this field.
- Media Type—Connection media of the port. Possible values are RJ-45 ISL and SC Fiber ISL.

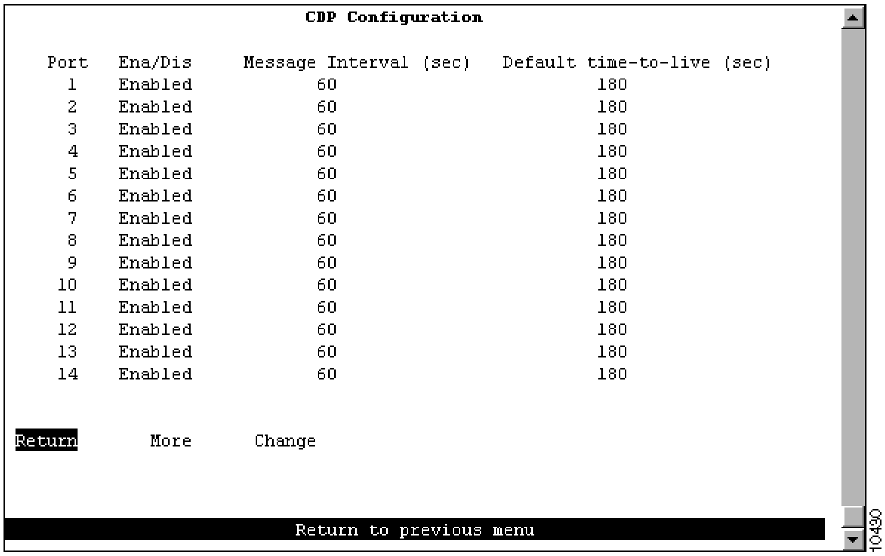
Configuring the Cisco Discovery Protocol Parameters

The CDP is used with Cisco IOS software to establish communication between different models of Cisco equipment (such as between a Cisco Catalyst 3900 switch and a Cisco 7000 router).

Each device configured for CDP sends periodic messages to a multicast address. Each device advertises at least one address at which it can receive SNMP messages. The advertisements also contain time-to-live, or holdtime, information, which indicates the length of time a receiving device should hold CDP information before discarding it.

To configure CDP parameters, select **CDP Configuration** on the Configuration Menu. The CDP Configuration panel (Figure 6-30) is displayed.

Figure 6-30 CDP Configuration Panel



```
                              CDP Configuration

   Port   Ena/Dis     Message Interval (sec)   Default time-to-live (sec)
    1     Enabled             60                         180
    2     Enabled             60                         180
    3     Enabled             60                         180
    4     Enabled             60                         180
    5     Enabled             60                         180
    6     Enabled             60                         180
    7     Enabled             60                         180
    8     Enabled             60                         180
    9     Enabled             60                         180
   10     Enabled             60                         180
   11     Enabled             60                         180
   12     Enabled             60                         180
   13     Enabled             60                         180
   14     Enabled             60                         180
```

The following information is displayed on this panel:

- Port—Identifier of the port.
- Ena/Dis—Indicates whether CDP is enabled for the port. The default is Enabled.
- Message Interval (sec)—Time (in seconds) between CDP messages. The default is 60.
- Default time-to-live (sec)—Time (in seconds) that a receiving device should hold a CDP packet from your switch before discarding it. The CDP hold time must be set to a greater number of seconds than the time between CDP transmissions (the transmission frequency time). The default is 180.

To	Select	Then
Change a parameter associated with a port…	**Change**	Specify the port number, select the appropriate parameter, and then specify the new value.
Save your changes…	**Return**	

Monitoring Port Traffic

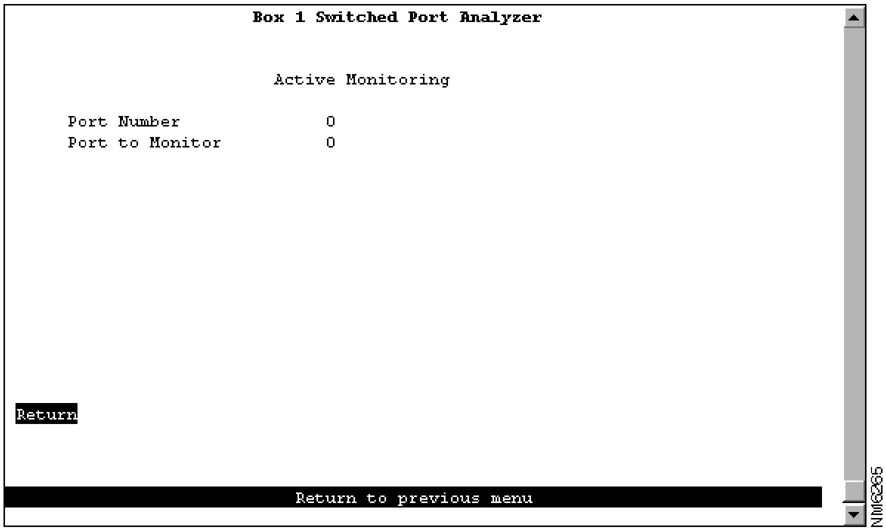
The Catalyst 3900 allows you to configure a Switched Port Analyzer (SPAN) port for monitoring port traffic. A SPAN port performs the function of port mirroring. Traffic on the monitored port is copied to the monitoring port, thereby allowing you to monitor traffic on any of the Token Ring ports.

An active port monitor allows you to use a customer-supplied trace tool, such as a Network General Sniffer, to monitor only the LLC traffic that is switched by the monitored port. The MAC frames are not monitored.

Note Before you can use a SPAN port to monitor traffic, the SPAN port must be in its own TrCRF and TrBRF. You cannot designate a port as a SPAN port if it is not isolated in it's own TrCRF and TrBRF. See "Configuring VLANs and VTP" for more information about how to define a TrBRF and a TrCRF and how to assign a port to a TrCRF.

To configure a SPAN port, select **Switched Port Analyzer** on the Configuration Menu. The Switched Port Analyzer panel (Figure 6-31) is displayed.

Figure 6-31 Switched Port Analyzer Panel



```
                    Box 1 Switched Port Analyzer


                        Active Monitoring

     Port Number               0
     Port to Monitor           0
```

The following information is displayed on this panel:

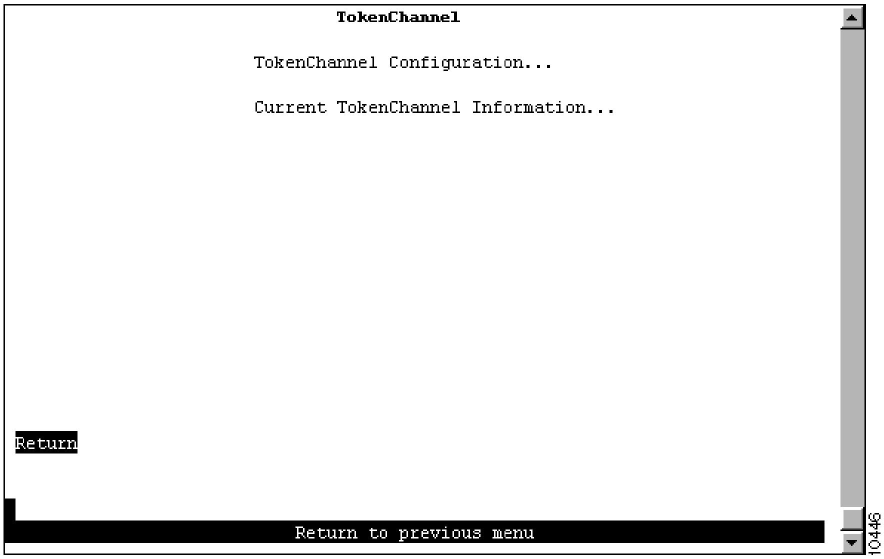
- Port Number—Port to which the network analyzer or RMON probe will be attached. Possible values are 0 through 28. You cannot specify a port that is a member of a TokenChannel as a monitoring port. Likewise, you cannot add a port that has been specified as a monitoring port to a TokenChannel. You also cannot specify an ATM or ISL port.
- Port To Monitor—Port that will be monitored. Possible values are 0 through 28. If you specify an ATM port, you will be prompted to select one or more TrCRFs that you want to monitor. If you specify an ISL port, you will be prompted to select the TrCRF that you want to monitor.

To	Select	Then
Change the current settings…	The appropriate parameter…	Specify the value.
Disable the SPAN port…	**Port to Monitor**	Specify 0.
Save your changes…	**Return**	

Using TokenChannels

To view or change the TokenChannel definitions, select **TokenChannel** on the Configuration Menu. The TokenChannel panel (Figure 6-32) is displayed.

Figure 6-32 TokenChannel Panel



```
                              TokenChannel

                         TokenChannel Configuration...

                         Current TokenChannel Information...

Return

                          Return to previous menu
```

The following options are displayed on this panel:

- TokenChannel Configuration—Select this option to configure a TokenChannel. Refer to the “Configuring TokenChannels” section for more information.
- Current TokenChannel Information—Select this option to view the configuration of current TokenChannels. Refer to the “Viewing Current TokenChannel Configuration” section for more information.

Configuring TokenChannels

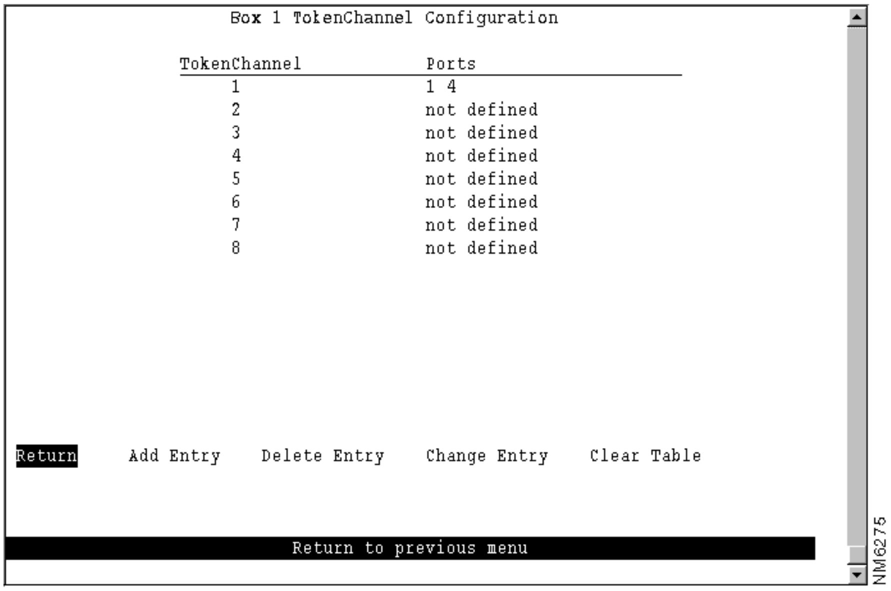
To configure one or more TokenChannels, select **TokenChannel Configuration** on the TokenChannel panel. The TokenChannel Configuration panel (Figure 6-33) is displayed.

A single TokenChannel can consist of a combination of HDX and FDX connections. For example, a TokenChannel consisting of three connections can have one HDX and two FDX connections. However, both ports in each interconnected pair must be either HDX or FDX. In addition, all ports in a single TokenChannel must belong to the same TrCRF on the Catalyst 3900.

Neither ATM nor ISL ports cannot be used in a TokenChannel.

Caution While you can use TokenChannels to interconnect Catalyst 3900s and Catalyst 3920s, you cannot use TokenChannels to interconnect other different models of switches. For example, you cannot use a TokenChannel to interconnect a Catalyst 2600 and a Catalyst 3900. Likewise, you cannot use a TokenChannel to interconnect a Catalyst 3900 and a non-Cisco switch.

Figure 6-33 TokenChannel Configuration Panel



```
              Box 1 TokenChannel Configuration

           TokenChannel           Ports
           ________________________________________
               1                  1 4
               2                  not defined
               3                  not defined
               4                  not defined
               5                  not defined
               6                  not defined
               7                  not defined
               8                  not defined





Return     Add Entry    Delete Entry    Change Entry    Clear Table



                   Return to previous menu
```

The following information is displayed on this panel:

- TokenChannel—Identifier of the TokenChannel (1 through 8).
- Ports—List of ports assigned to this TokenChannel.

You must define the TokenChannels for both connected Catalyst 3900s before physically connecting the linked ports. Therefore, make sure that you have either disabled the ports or disconnected the cables before you configure the TokenChannel. Otherwise, you will create loops.

Note When you physically connect the linked ports, make sure that the ports with the lowest port numbers are connected. For example, if a TokenChannel links ports 3, 6, and 7 of one Catalyst 3900 and ports 2, 4, and 5 of another Catalyst 3900, the ports must be connected to each other in the following manner: port 3 to port 2, port 6 to port 4, and port 7 to port 5.

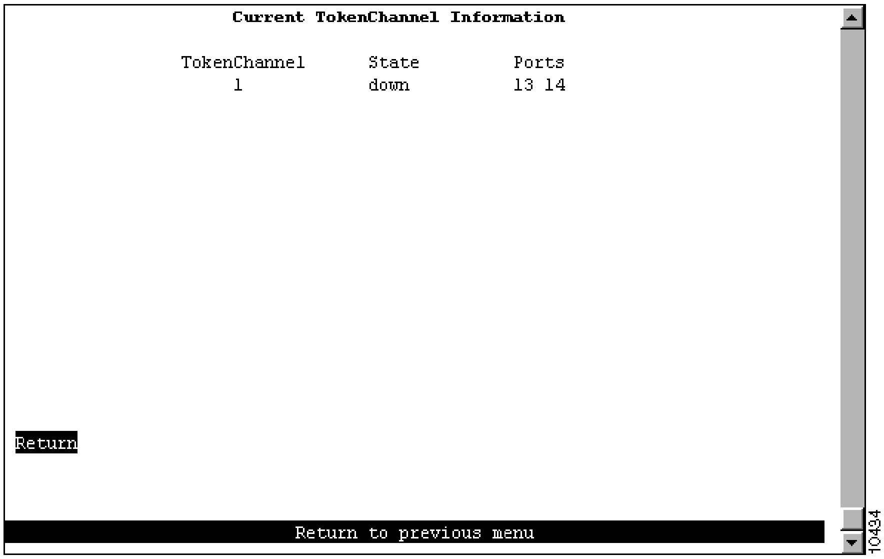
To	Select	Then
Define a new TokenChannel…	**Add Entry**	Specify the ports that compose the new TokenChannel. The port numbers must be entered from lowest to highest and be separated by spaces. You cannot specify more than 8 ports.
Delete the definition for a TokenChannel…	**Delete Entry**	Specify the identifier of the TokenChannel to be deleted.
Change the definition of a TokenChannel…	**Change Entry**	Specify the identifier of the TokenChannel to be changed and enter the new information. The ports associated with a TokenChannel must be disabled or disconnected before you change the TokenChannel definition.

To	Select	Then
Delete all TokenChannel definitions…	**Clear Table**	Confirm the deletion of all TokenChannel definitions.
Save your changes…	**Return**	

Viewing Current TokenChannel Configuration

To view the configuration of currently defined TokenChannels, select **Current TokenChannel Information** on the TokenChannel panel. The Current TokenChannel Information panel (Figure 6-34) is displayed.

Figure 6-34 Current TokenChannel Information Panel



```
                    Current TokenChannel Information

              TokenChannel      State         Ports
                   1            down          13 14
```

The following information is displayed on this panel:

- TokenChannel—Identifier of the TokenChannel.
- State—Indicates whether the TokenChannel is up or down.
- Ports—List of ports assigned to this TokenChannel.

Caution If one of the links in a TokenChannel goes down, the whole TokenChannel will become inoperative.

Limiting Scope and Access

For network security, you can isolate parts of your network by limiting the scope and access of your users. For example, you might want to limit access to a specific file server to a select group of users.

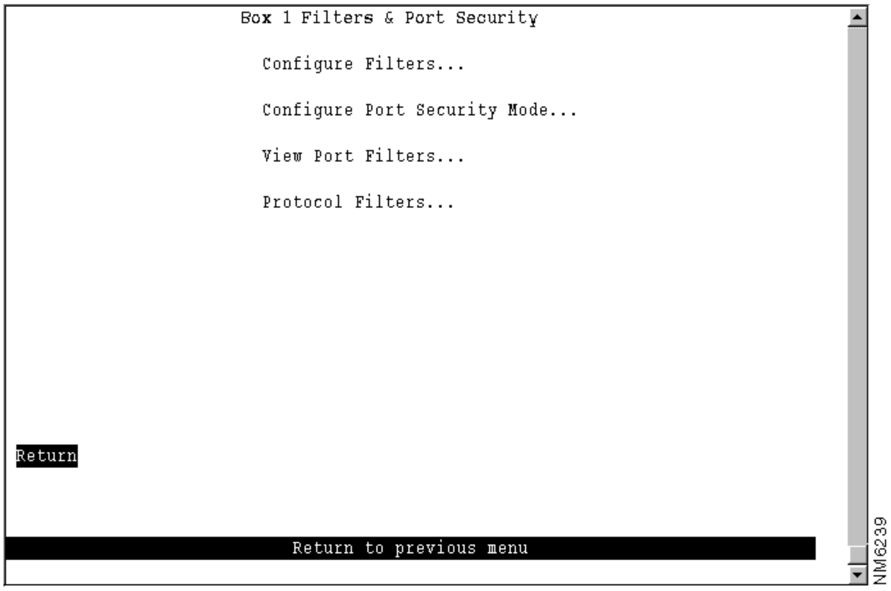
To limit access, you can do the following:

- Attach the printer to a single port on the Catalyst 3900.
- Create a filter that blocks all data to a port except that which is explicitly allowed (using Port Security).
- Define a filter that explicitly allows data from the select group of users (based on MAC address) to be sent to that port (using MAC Filters).

To limit the scope and access of users on segments attached to the Catalyst 3900, select **Filters & Port Security** from the Configuration Menu. The Filters & Port Security panel (Figure 6-35) is displayed.

Note The ISL module does not support Media Access Control (MAC) or protocol filtering.

Figure 6-35 Filters & Port Security Panel



Box 1 Filters & Port Security

Configure Filters...

Configure Port Security Mode...

View Port Filters...

Protocol Filters...

Return

Return to previous menu

The following options are displayed on this panel:

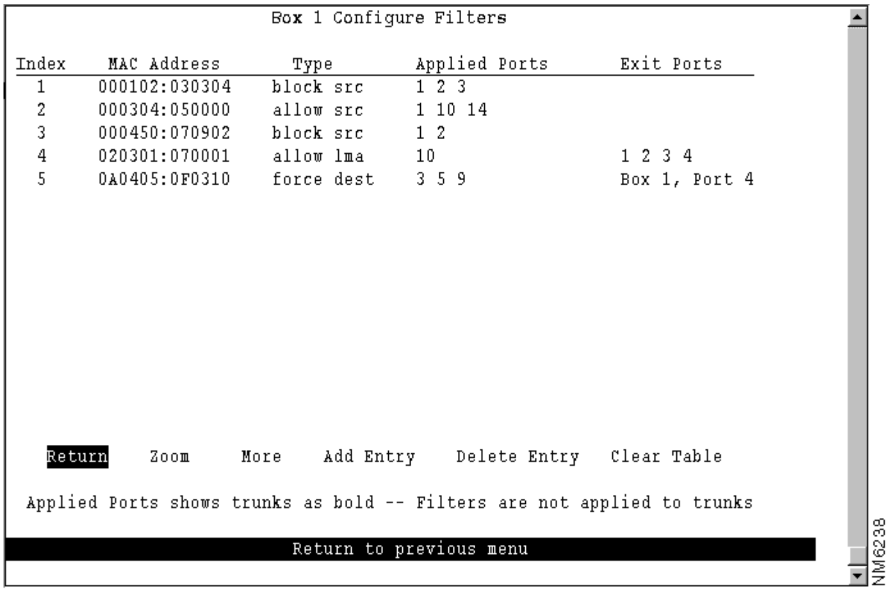
- Configure Filters—Select this option to configure MAC address filters. For more information, refer to the “Filtering Data Based on MAC Address” section.
- Configure Port Security Mode—Select this option to block communication at selected ports. For more information, refer to the “Securing Ports” section.
- View Port Filters—Select this option to view the currently defined filters. For more information, refer to the “Viewing Filters for a Specific Port” section.
- Protocol Filters—Select this option to configure protocol filters. For more information, refer to the “Filtering Data Based on Protocol” section.

Filtering Data Based on MAC Address

To restrict certain users from communicating with other users or resources (such as printers or servers), select **Configure Filters** on the Filters & Port Security panel. The Configure Filters panel (Figure 6-36) is displayed.

Note When configuring MAC address filters for a port, you cannot configure multiple filters for a port that include the same MAC address. For example, you cannot specify the same MAC address in both a block destination address filter and a block source address filter for the same port. Also, you cannot specify the same MAC address in both an allow destination address filter and an allow source address filter for the same port.

Figure 6-36 Configure Filters Panel



```
                         Box 1 Configure Filters

Index    MAC Address       Type        Applied Ports       Exit Ports
  1     000102:030304    block src     1 2 3
  2     000304:050000    allow src     1 10 14
  3     000450:070902    block src     1 2
  4     020301:070001    allow lma     10                  1 2 3 4
  5     0A0405:0F0310    force dest    3 5 9               Box 1, Port 4


    Return    Zoom     More    Add Entry    Delete Entry   Clear Table

  Applied Ports shows trunks as bold -- Filters are not applied to trunks

                         Return to previous menu
```

The following information is displayed on this panel:

- Index—Identifier of the filter.
- MAC Address—MAC address contained in packets to be filtered.
- Type—Possible types are:
    - block src—Block any packet with source address.
    - block dest—Block any packet with destination address.
    - allow src—Allow any packet with source address.
    - allow dest—Allow any packet with destination address.
    - allow lma—Allow any packet with limited multicast address to port(s).
    - force dest—Force any packet with the designated destination address to port.
- Applied Ports—Input port where the filtering takes place. You specify applied ports for all filters.
- Exit Ports—Port, if any, that is to receive the filtered packets. This applies only to filters defined as “Allow any packet with the designated Source address to port(s)” or “Force any packet with the designated Destination Address to port(s).”

You can define up to 250 source or destination MAC addresses to be filtered at the port of entry into the Catalyst 3900. MAC addresses can be unicast, multicast (group), or broadcast. All 250 addresses can be associated with one port or divided among the available ports.

To	Select	Then
Display the complete list of Entry Ports and Exit Ports for a filter…	**Zoom**	Specify the index number.
Add a filter…	**Add Entry**	Specify the filter type, the MAC address, and the ports. The port numbers should be listed from lowest to highest and be separated by spaces. If you do not specify a port number, the filter will be applied to all ports.
Delete a filter…	**Delete Entry**	Specify the index number of the filter to be deleted.
Delete all filters…	**Clear Table**	Confirm the deletion of all filters.
Save your changes…	**Return**	

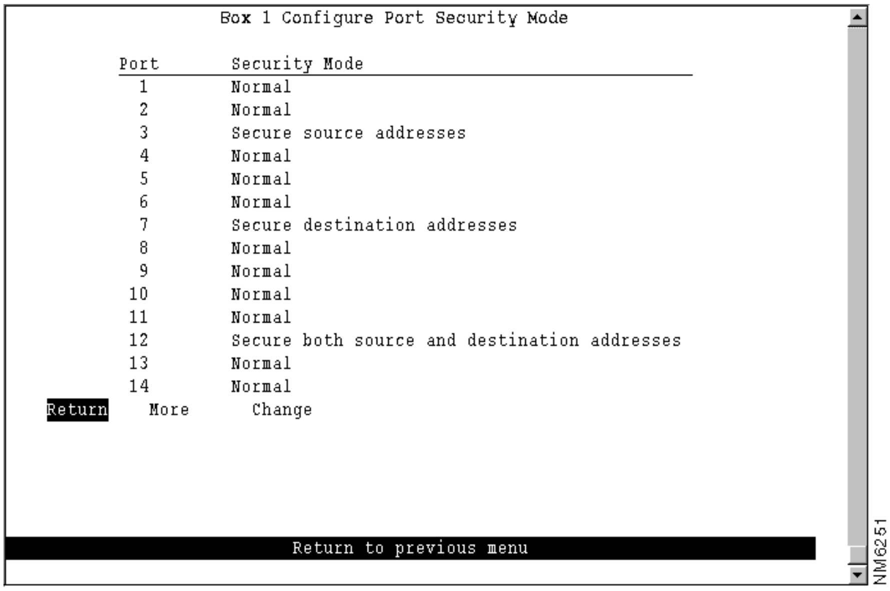
Note If you set up a filter for broadcast packets, hosts on the other side of the Catalyst 3900 will not see the ARP broadcast packets. To prevent this, allow time for the Catalyst 3900 to learn the host addresses before implementing the filter.

Note If you are defining a filter for a TokenChannel, the filter must be defined for all ports in the TokenChannel.

Securing Ports

The Catalyst 3900 also allows you to totally block (secure) communication at selected ports, unless explicitly allowed by a MAC filter. Addresses that have been allowed or forced by a configured filter are not blocked. To define the security attributes of each port, select **Configure Port Security Mode** on the Filters & Port Security panel. The Configure Port Security Mode panel (Figure 6-37) is displayed.

Figure 6-37 Configure Port Security Mode Panel



```
                   Box 1 Configure Port Security Mode

          Port       Security Mode
            1        Normal
            2        Normal
            3        Secure source addresses
            4        Normal
            5        Normal
            6        Normal
            7        Secure destination addresses
            8        Normal
            9        Normal
           10        Normal
           11        Normal
           12        Secure both source and destination addresses
           13        Normal
           14        Normal
    Return    More      Change




                         Return to previous menu
```

The following information is displayed on this panel:

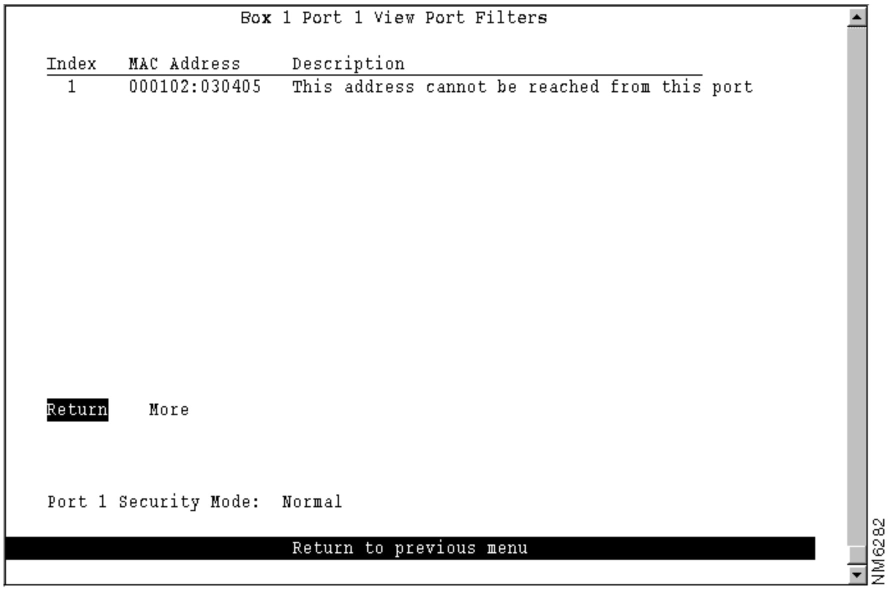
- Port—Identifier of the port.
- Security Mode—Level of security defined for that port. Possible values include:
    - Normal—No security mode is defined for a port. This mode is the default.
    - Secure source addresses—Block all source addresses, except those allowed by a configured filter.
    - Secure destination addresses—Block all destination addresses, except those forced by a configured filter.
    - Secure both source and destination addresses—Block all source and destination addresses, except those allowed or forced by a configured filter.

To	Select	Then
Change the security mode for a port…	**Change**	Specify the port and the desired security mode.
Save your changes…	**Return**	

Viewing Filters for a Specific Port

To display the defined filters for a specific port, select **View Port Filters** on the Filters & Port Security panel and specify the port number. The View Port Filters panel (Figure 6-38) is displayed.

Figure 6-38 View Port Filters Panel



```
                 Box 1 Port 1 View Port Filters

Index   MAC Address     Description
  1     000102:030405   This address cannot be reached from this port




Return    More



Port 1 Security Mode:  Normal
                         Return to previous menu
```

The following information is displayed on this panel:

- Index—Identifier of the filter entry.
- MAC Address—MAC address contained in the packets to be filtered.
- Description—Filter action to take on the packet with the specified MAC address.

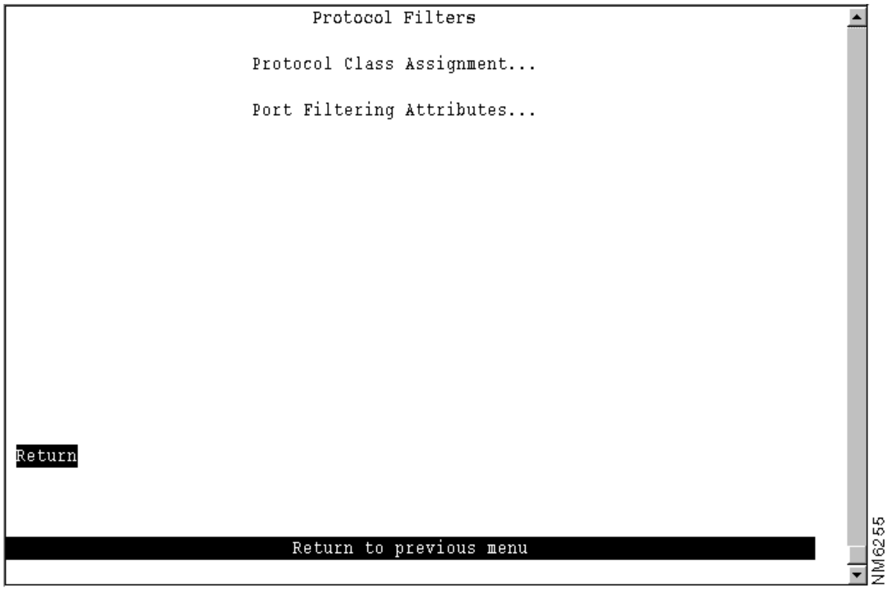
You cannot change any information on this panel.

Filtering Data Based on Protocol

To filter data based on protocol, you can define protocol classes and then assign filtering attributes to these classes on a per-port basis. In protocol filtering, each incoming frame is assigned to one of the protocol classes based on the DSAP or Ethertype of the frame. If the DSAP is 0xAA (which indicates SNAP), the assignment is based on the Ethertype of the SNAP header. The mapping from DSAP or Ethertype to protocol class is common for all switch ports in a stack.

To filter data based on protocol, select **Protocol Filters** on the Filters & Port Security panel. The Protocol Filters panel (Figure 6-39) is displayed.

Figure 6-39 Protocol Filters Panel



```
                        Protocol Filters

                   Protocol Class Assignment...

                   Port Filtering Attributes...









Return



                    Return to previous menu
```

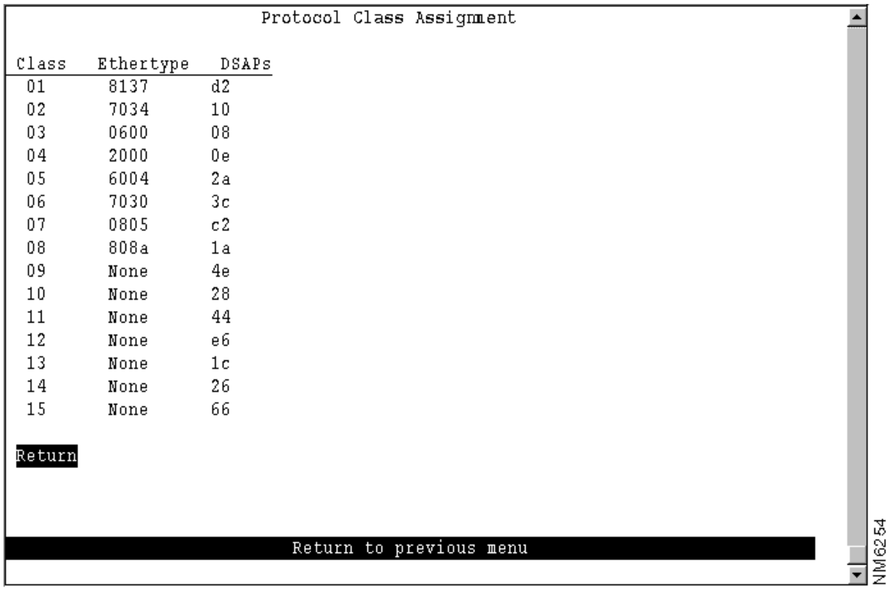
The following options are displayed on this panel:

- Protocol Class Assignment—Select this option to define protocol classes. For more information, refer to the “Assigning Classes for Protocol Filtering” section.
- Port Filtering Attributes—Select this option to define the behavior attributes for a protocol filter. For more information, refer to the “Defining Protocol Filter Behavior for a Port” section.

Assigning Classes for Protocol Filtering

To use protocol filtering, you must first define the protocol classes. You can define up to 15 protocol classes for use in protocol filtering. To define the protocol classes, select **Protocol Class Assignment** on the Protocol Filters panel. The Protocol Class Assignment panel (Figure 6-40) is displayed.

Figure 6-40 Protocol Class Assignment Panel



```
                         Protocol Class Assignment

Class   Ethertype   DSAPs
 01       8137      d2
 02       7034      10
 03       0600      08
 04       2000      0e
 05       6004      2a
 06       7030      3c
 07       0805      c2
 08       808a      1a
 09       None      4e
 10       None      28
 11       None      44
 12       None      e6
 13       None      1c
 14       None      26
 15       None      66

Return

                            Return to previous menu
```

The following information is displayed on this panel:

- Class—Identifier of the protocol class. By default, the names are 01 through 15.
- Ethertype—List of the Ethernet protocol types that you want to filter. You can specify a single Ethertype (in its 4-digit hexadecimal format). You cannot specify an Ethertype for protocol classes 9 through 15. For a list of possible Ethertypes, refer to the "Ethertypes" section of the "Codes and IDs" appendix.
- DSAPs—List of the DSAPs that you want to filter. You can specify up to 16 DSAPs (in hexadecimal format) separated by spaces. For a list of possible service access points (SAPs), refer to the "Service Access Points" section of the "Codes and IDs" appendix.

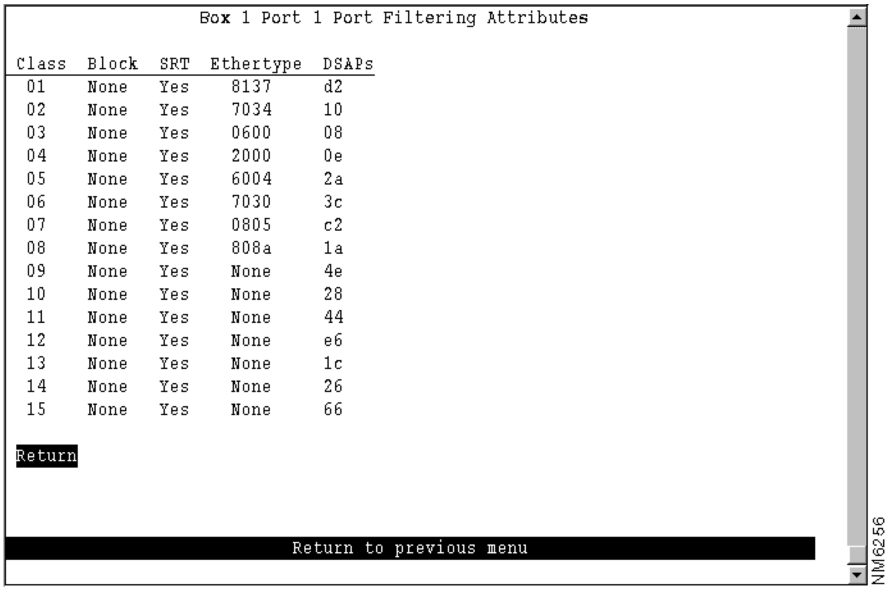
Note All DSAPs that are not specifically assigned to a protocol class are assigned to class 0.

To	Select	Then
Change the current settings…	The appropriate port...	Specify the value.
Save your changes…	**Return**	

Defining Protocol Filter Behavior for a Port

After you have defined your protocol classes, you can define how a port handles frames for each protocol class. To define how each class is handled, select **Port Filtering Attributes** on the Protocol Filters panel and specify the port number. The Port Filtering Attributes panel (Figure 6-41) is displayed.

Figure 6-41 Filtering Attributes for a Port Panel



```
                    Box 1 Port 1 Port Filtering Attributes

 Class  Block  SRT  Ethertype  DSAPs
   01   None   Yes    8137      d2
   02   None   Yes    7034      10
   03   None   Yes    0600      08
   04   None   Yes    2000      0e
   05   None   Yes    6004      2a
   06   None   Yes    7030      3c
   07   None   Yes    0805      c2
   08   None   Yes    808a      1a
   09   None   Yes    None      4e
   10   None   Yes    None      28
   11   None   Yes    None      44
   12   None   Yes    None      e6
   13   None   Yes    None      1c
   14   None   Yes    None      26
   15   None   Yes    None      66

 Return



                          Return to previous menu
```

The following information is displayed on this panel:

- Class—Identifier of the class.
- Block—How the port handles frames that fall into this protocol class. Possible values are:
  - All—Block all frames in this protocol class.
  - SR—Block all source-routed frames in this protocol class.
  - NSR—Block all non-source-routed frames in this protocol class.
  - None—Allow all frames in this protocol class.

  The default is None.
- SRT—Indicates whether the port allows transparent bridging of frames in this protocol class.
- Ethertype—Ethertypes defined for this class.
- DSAPs—DSAPs defined for this class.

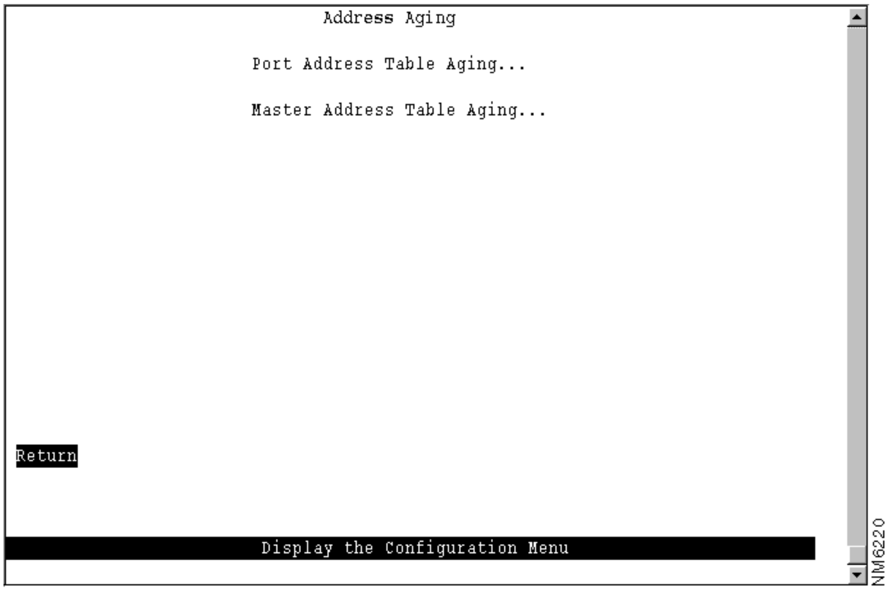
Note For protocol class 0, Block is set to None and SRT is set to Yes.

To	Select	Then
Change the current settings…	The appropriate parameter...	Specify the value.
Save your changes…	**Return**	

Configuring Address Aging

To ensure that the address tables (per port and master) are kept to a minimum size, you can configure an *aging limit*. The aging limit is used to determine when inactive MAC addresses are removed from the address table. To define address table aging limits, select **Address Aging** from the Configuration Menu. The Address Aging panel (Figure 6-42) is displayed.

Figure 6-42 Address Aging Panel



```
Address Aging

Port Address Table Aging...

Master Address Table Aging...
```

The following options are displayed on this panel:

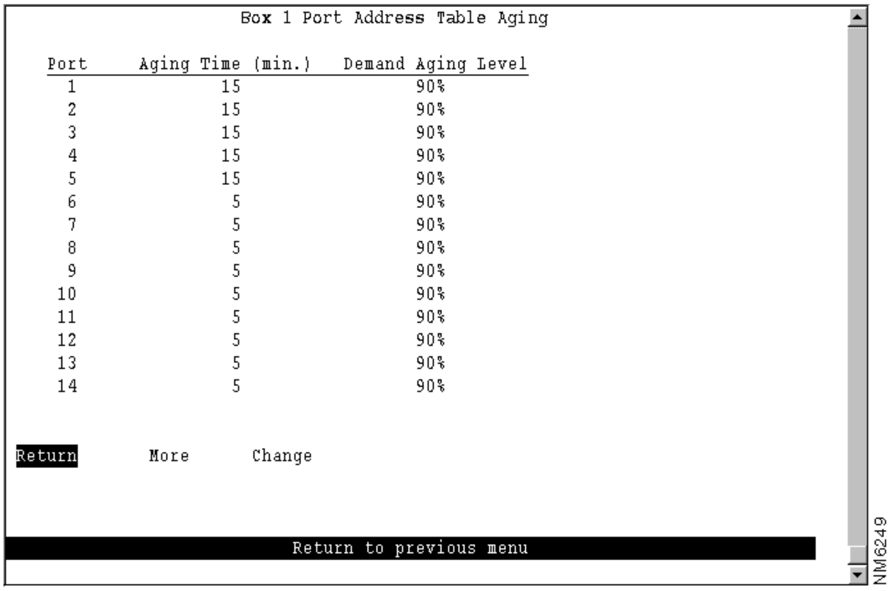
- Port Address Table Aging—Select this option to define the address aging limits for each port address table. For more information, refer to the “Defining Address Aging Limits by Port” section.
- Master Address Table Aging—Select this option to define the address aging limits for the master address table. For more information, refer to the “Defining Address Aging Limits for the Master Address Table” section.

Note To completely disable address aging, you must disable address aging for the ports and the master address table.

Defining Address Aging Limits by Port

To define the address aging limits of each port, select **Port Address Table Aging** on the Address Aging panel. The Port Address Table Aging panel (Figure 6-43) is displayed.

Figure 6-43 Port Address Table Aging Panel



```
                    Box 1 Port Address Table Aging

   Port     Aging Time (min.)   Demand Aging Level
     1              15                 90%
     2              15                 90%
     3              15                 90%
     4              15                 90%
     5              15                 90%
     6               5                 90%
     7               5                 90%
     8               5                 90%
     9               5                 90%
    10               5                 90%
    11               5                 90%
    12               5                 90%
    13               5                 90%
    14               5                 90%


Return       More      Change



                      Return to previous menu
```

The following information is displayed on this panel:

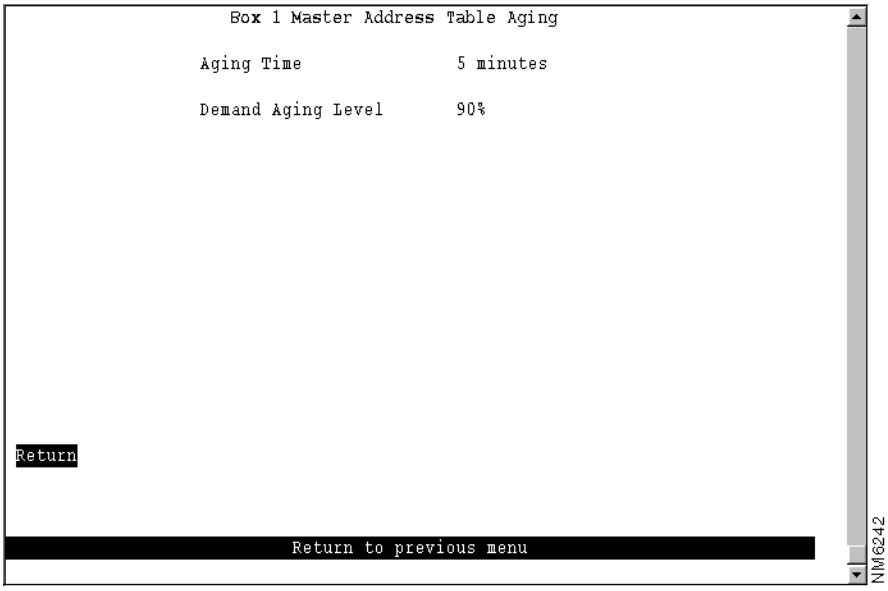
- Port—Identifier of the port.
- Aging Time (min.)—Time (in minutes) an inactive MAC address will remain in the port's address table. Possible values are 0 through 9999 minutes. The default is 5 minutes. Zero indicates that address aging is disabled.
- Demand Aging Level—Percentage threshold of address table capacity to ensure that the port's address table is populated only by the most frequently used addresses. Addresses are stored until reaching the maximum capacity of the table, then discarded in a specific order until the set percentage of table capacity is reached and then cycles in the same manner. Possible values are 50, 60, 70, 80, 90 percent, and Disable. The default is 90 percent.

To	Select	Then
Change the aging time limit and the address table aging level…	**Change**	Specify the port, the new aging time, and the new aging level.
Disable address removal for a port based on address age…	**Change**	Specify an Aging Time of 0.
Disable address removal for a port based on address table capacity…	**Change**	Specify a Demand Aging Level of Disable.
Save your changes…	**Return**	

Defining Address Aging Limits for the Master Address Table

To define the address aging limits of the master address table, select **Master Address Table Aging** on the Address Aging panel. The Master Address Table Aging panel (Figure 6-44) is displayed.

Figure 6-44 Master Address Table Aging Panel



```
                  Box 1 Master Address Table Aging

                Aging Time              5 minutes

                Demand Aging Level      90%
```

```
Return to previous menu
```

The following information is displayed on this panel:

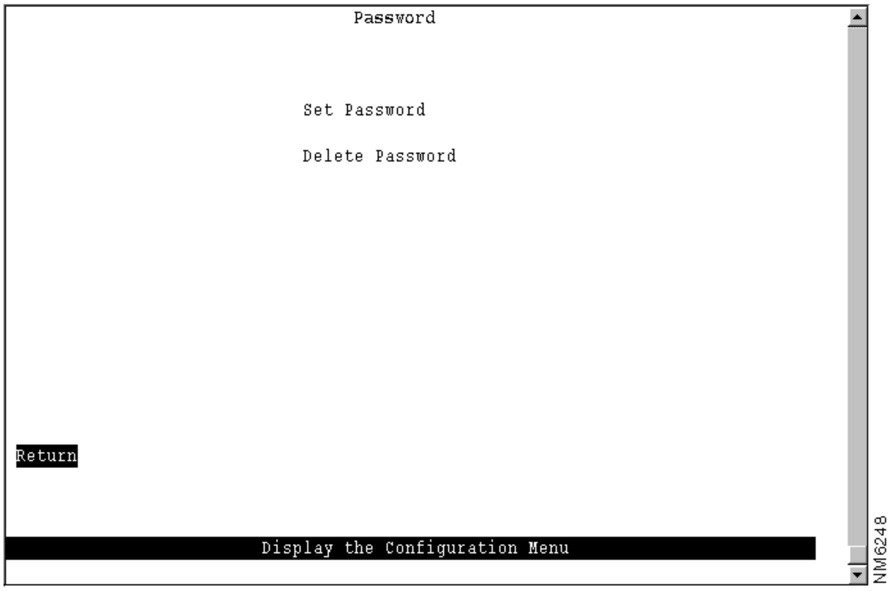
- Table Aging Time—Time (in minutes) an inactive MAC address will remain in the master address table. Possible values are 0 through 9999 minutes. The default is 5 minutes. A value of 0 will disable the removal of addresses based on age.
- Demand Aging Level—Percentage threshold of address table capacity to ensure that the master address table is populated only by the most frequently used addresses. Addresses are stored until reaching the maximum capacity of the table, then discarded in a specific order until the set percentage of table capacity is reached and then cycles in the same manner. Possible values are 50, 60, 70, 80, 90 percent, and Disable. The default is 90 percent.

To	Select	Then
Change the aging time limit or the address table aging level…	The appropriate parameter	Specify the new value.
Disable address removal based on address age…	**Aging Time**	Specify 0.
Disable address removal based on address table aging level…	**Demand Aging Level**	Specify Disable.
Save your changes…	**Return**	

Setting a Password

The Catalyst 3900 allows you to set a password to protect its configuration. If you establish a password, users must enter it to obtain access to the Main Menu. To set a password, select **Password** on the Configuration Menu. The Password panel (Figure 6-45) is displayed.

Figure 6-45 Password Panel



Display the Configuration Menu

To	Select	Then
Add a password…	**Set Password**	Press **Enter** at the Old Password prompt and specify a new password.
Change the password…	**Set Password**	Specify the current password and the new password.
Delete the password…	**Delete Password**	Specify the current password.
Save your changes…	**Return**	

Note If you have forgotten your password, press the System Request button to access the System Request menu, and then select **Clear the system password**. This will clear only the system password. All other configuration parameters saved in NVRAM will be retained.