

Console Configuration

This chapter explains how to set up and modify the configuration of the Catalyst 3000 using a directly-attached console.

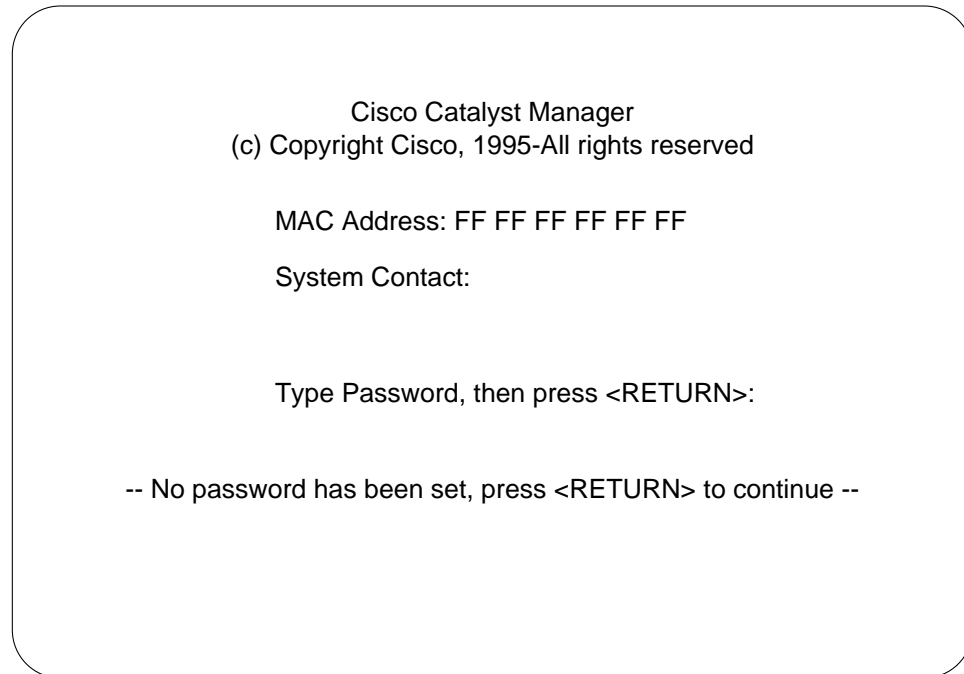
In this chapter covers the following topics:

- General Guidelines
- Main Menu Screen
- Selecting Configuration From Main Menu
- SwitchProbe Menu from the Configuration Menu
- Spanning-Tree Protocol (STP)
- EtherChannel
- Address Filtering
- Address Aging
- Broadcast Suppression from the Configuration Menu
- Console or Telnet Sessions
- Download Menu From the Main Menu
- Reset Heading from Main Menu

General Guidelines

To work within the console menus, follow these guidelines:

- To select a menu item, use the arrow keys to move the “highlight” over the selection, then press RETURN. If you need to specify additional information for that item—for example, selecting “Yes” or “No” or supplying a value—a prompt appears on the screen.
- In most cases, new values are saved when you select Return to Previous Menu.
- The term “More” means there is more information that can be displayed on one screen. Selecting More and pressing RETURN displays the next screen of information.
- The term “Port” refers to the number of a specific port on a Catalyst 3000.
- The term “Index” refers to the numerical order of a list.
- To return to the Main Menu from any screen within the menus, press **Ctrl-P**. Note that any changes made to the screen you were in are not saved. To return to the Greeting screen, press **Ctrl-B**.
- If using Catalyst VLAN, be sure to set up IP, SNMP, and Spanning Tree values.
- The console automatically returns to the Greeting screen after five minutes of inactivity. Five minutes is the default value. The time can be changed at the Console Configuration menu as explained later in this chapter. The Console Configuration menu is within the Configuration menu, under the Main Menu.
- For protection against inadvertent or unauthorized access to configuration screens, you may establish a password that users must enter at the Greeting screen. If no password is configured, just press RETURN and the Main Menu Screen is presented. To establish a password, see Password Menu from the Configuration Menu, later in this chapter. The Password menu can be accessed through the Configuration menu, which is under the Main Menu. For more information on the Greeting screen see Chapter 6, “Console Configuration.”



H4630

Navigating Within the Menus

Use the “ARROW” keys (also referred to as cursor keys) to move the highlight over a selection. If the selection is a menu, pressing the RETURN key displays a new screen of information; if the selection is a command, such as “Reset”, pressing the RETURN key initiates that function.

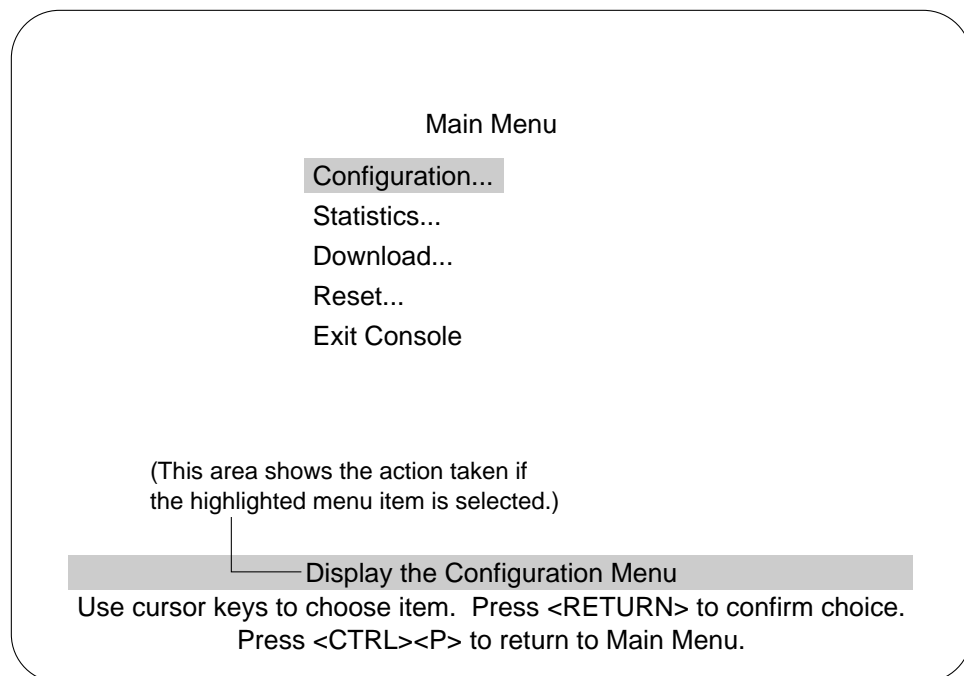
A heading with three “dots” after it means that when that heading is selected more information about that heading is displayed.

Unless specified differently, all the screens or menus are accessed in the same way.

Main Menu Screen

The following lists the headings for the Main menu screen and a description of those headings.

Main Menu Screen



Configuration Menu

Displays the Configuration menu, which enables you to view and set the Catalyst 3000 configuration parameters. The Configuration section and its sub-menus are described later in this chapter.

Statistics Menu

Displays Statistics menu for the Catalyst 3000. Explanations of screens in the Statistics Menu are in Chapter 8, “Monitoring the Network With Out-of-Band Management.”

Download Menu

Explained in this chapter immediately after the sections describing the Configuration menu.

Reset...

Explained in this chapter after the sections describing the Download menu.

Exit Console

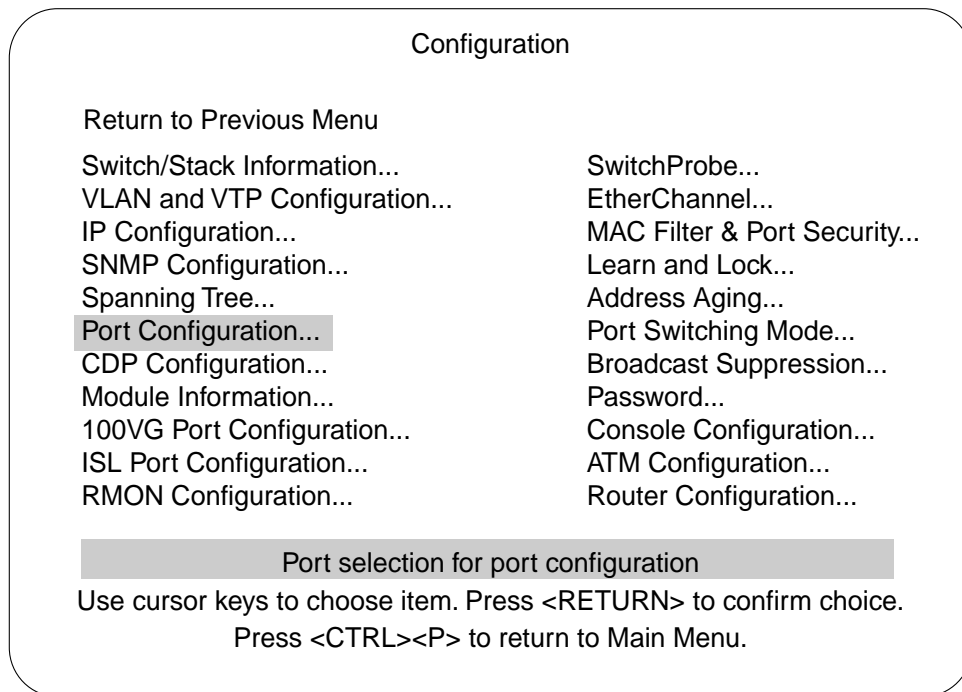
Highlighting this selection and pressing the RETURN key return the console to the Greeting screen (on a Telnet session, this causes the session to close).

Selecting Configuration From Main Menu

The Configuration menu enables you to view and set the Catalyst 3000 configuration parameters. The following section describes the Configuration menu and its sub-menus.

Configuration Screen

The following screen is displayed when the Configuration heading is selected from the Main menu.



H4636

Note Menus VLAN and EtherChannel are options available only with Catalyst 3000 enhanced software. To obtain an upgrade, contact your sales representative.

The following is a list of the headings in the Configuration menu. Details descriptions and views of the menu screens for these headings are after this list.

Switch/Stack Information

Displays System Information screen.

Catalyst VLAN Configuration

Displays options for configuring VLAN. (Enhanced version only.)

IP Configuration

Displays screen for changing IP addresses and subnet masks and for sending a PING.

SNMP Configuration

Displays selections for setting attributes related to SNMP.

Spanning Tree

Displays selections for configuring Spanning-Tree Protocol.

Port Configuration

Displays screen for changing port configuration.

Module Information

Displays information on optional Expansion Modules.

Selecting Configuration From Main Menu

SwitchProbe

Displays the screen for selecting a port to monitor.

EtherChannel

Displays options for creating an EtherChannel. (Enhanced version only.)

Mac Filter and Port Security

Menu for configuring address filtering.

Address Aging

Displays a screen for setting a different aging time for the addresses in memory for the system and ports.

Port Switching Mode

Displays the options available for setting the error handling modes for each port.

Broadcast Suppression

Displays a screen used to set up the control Broadcast packet traffic.

Password

Displays screen for setting up and changing the password for access to the console.

Console Configuration

Displays choices for setting-up console or Telnet sessions with the Catalyst 3000.

Switch/Stack Information

Use the Switch/Stack Information screen to view system information and to view or change the system name, location, contact, and time of day. To add or change the system name, location, contact or time of day, use the arrow keys to move the highlight to the selection and press the RETURN key. A prompt appears near the bottom of the screen for entering text for that selection. Pressing RETURN again enters that text.

Switch/Stack Information

Return to Previous Menu	Stack State	Operational
Number of Boxes 3	Stack Connection	Primary WS-C3020
Local Box Number 1		1 WS-C3020 Module
Remote Box Number(s) 14		
Stack Time-Out (sec) 16		
System Description	Cisco Catalyst System	
System ID	1.3.6.1.4.1.197.2.5	
System Name		
System Location		
System Contact		
Time of Day...	Mon. November 20, 1995 10:42:53	
<div style="background-color: #cccccc; padding: 2px; display: inline-block;">Switch Information...</div>		
Display and change switch configuration Press <CTRL><P> to return to Main Menu.		

H5587

Number of Boxes

The number of boxes within this Stack.

Selecting Configuration From Main Menu

Local Box Number

The box number of the (local) Catalyst 3000 the console is connected to. The local box is also the source of the information displayed in these screens.

Remote Box Number(s)

The amount of boxes that are in the Stack besides the one displaying this information.

Stack Timeout (sec.)

If a box goes off-line, the amount of time the Stack tries to re-establish communications with the box.

Default: 16 seconds

Stack State

Displays whether the Stack is operational or not.

Stack Connection

The type of unit connected to the Stack.

The following headings refer to the information in the local Catalyst 3000 as part of a network system.

System Description

Name and model of this unit.

System ID

Unique identification code for this Catalyst 3000, assigned at the factory.

System Name

Any name you choose to assign to the switch (on a TCP/IP network, it could be the IP hostname.)

System Location

Location of the switch.

System Contact

Person to contact if questions should arise.

Time of Day

An internal clock is used to calculate total time of operation and time of day. To adjust the time, select this item, press RETURN, then enter the month, day, hour, or minute.

Note If you cannot set the Time of Day, the lithium battery may need replacing. If this is the case, contact your local reseller.

The heading “Switch Information...” from the “Switch/Stack” menu is described in the following section.

Selecting Configuration From Main Menu

The following section describes the Switch Information menu.

Box 1 Switch Information

Return to Previous Menu	
MAC Address	192.345.678.543
Interface Description	Catalyst 3000 HW 1.3.6.1.4.1.197.2.3 Rev. B
DRAM Installed	8 MB
Enhanced Features	Enabled

Display the Switch/Stack Menu

Use cursor keys to choose item. Press <RETURN> to confirm choice.
Press <CTRL><P> to return to Main Menu.

H5275

MAC Address

The MAC address of this unit.

Interface Description

The type of hardware and software and their version levels.

DRAM Installed

Number of megabytes of dynamic random-access memory in the Catalyst 3000. If a 4MB SIMM is installed, (standard configuration) the user sees “DRAM Installed 4MB.” In the standard configuration, (4MB) 6,000 addresses are allowed in each switch. With the 8MB SIMM installed, 10,000 addresses are allowed. The maximum number of addresses allowed is displayed under Main menu: “Statistics,” then under “Switch Statistics” as Maximum Number of Stations.

Flash Memory Installed

Number of flash memory installed on the Catalyst 3000. If a single flash is installed the number on the screen is 512KB. If two flashes are installed the number on the screen is 1024KB.

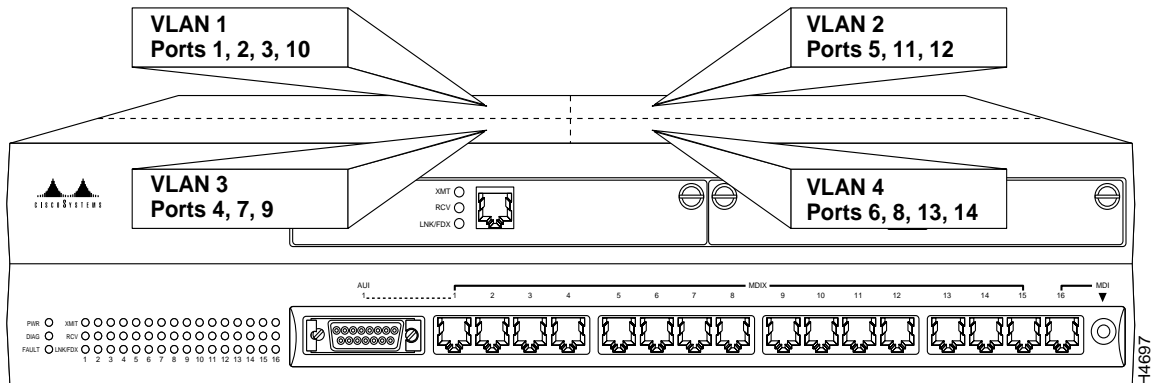
Enhanced Features

“Enabled” indicates that the optional Catalyst 3000 Enhanced feature set is enabled. To enable the feature set, call your local reseller to obtain a 10-digit “key.” Highlight the field, enter the key (code), and press RETURN. If you purchased the Catalyst 3000 with the Enhanced feature set and you need to re-enter the code, the code is on the bottom of the unit.

Virtual LAN (VLAN)

This section describes VLAN, the next selection on the Configuration menu. The optional VLAN feature is available on the Enhanced version of the Catalyst 3000 (contact your Cisco sales representative for information). Using the VLAN feature, you can partition a single Catalyst 3000 into a VLAN each containing its own set of ports. Packets are forwarded only between ports belonging to the same VLAN. The benefit of VLAN is to restrict access from one segment to another, either for security purposes or to reduce intersegment traffic. Figure 7-1 illustrates a Catalyst with four VLANs.

Figure 7-1 Catalyst with Four VLANs



To set up VLANs using the VLAN Configuration menu, specify the ports belonging to the VLANs, then set up the IP configurations, trap configuration (trap receivers are associated with a set of VLANs and a receiver IP address) and spanning tree configurations specific to the appropriate VLANs. If you have already supplied configuration information using the main configuration menus, that information applies to VLAN “default.”

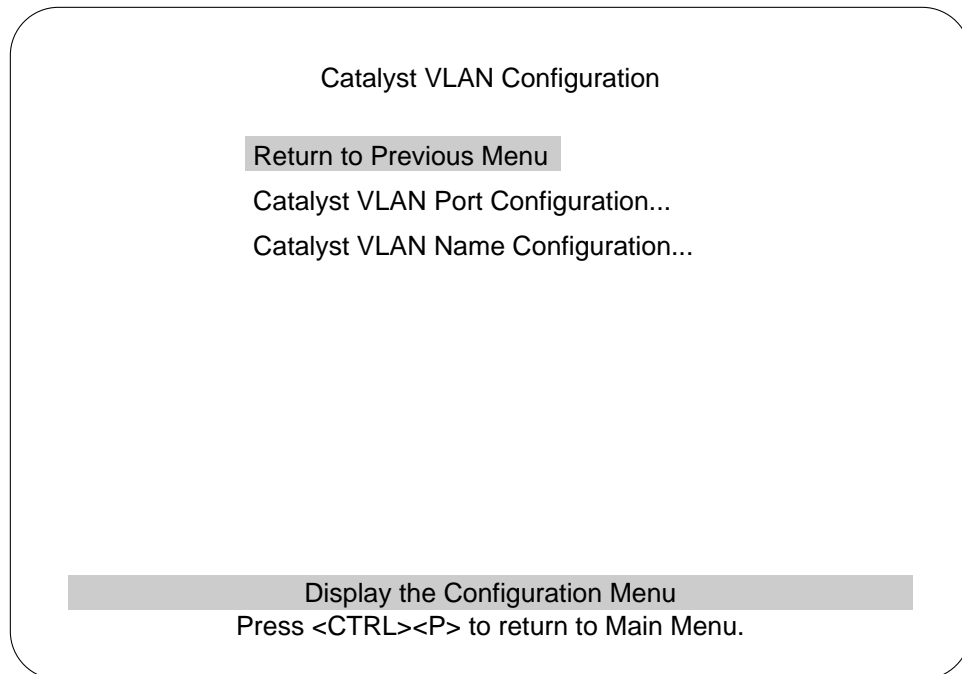
The VLAN affects other Catalyst 3000 features in the following ways:

- *Spanning tree.* If you are using spanning tree in a certain VLAN, you must supply spanning tree information for that VLAN. The spanning tree software treats ports on other VLANs as non-existent. VLANs do not affect port priorities and port costs. You set these parameters using the Spanning Tree Configuration menu that you select from the main Configuration menu.
- *SNMP trap tables.* Each VLAN appears to the NMS as a physically different Catalyst unit. Certain MIB II objects and Cisco proprietary objects are VLAN-sensitive, while others are not. For a list of VLAN-sensitive objects, see Chapter 9, “Monitoring the Network with SNMP.”
- *IP.* You must give each VLAN an IP address, subnet mask, and gateway address definition.
- *Address filters.* VLANs have no effect on address filters. For example, suppose you create two VLANs: one containing ports 1–8 and the other ports 9–15. Adding an address filter to ports 7, 8, 9, and 10, the filter continues to work properly even though it applies to ports in other VLANs.
- *EtherChannel.* All ports in a single EtherChannel must belong to the same VLAN. Therefore, the console software prevents you from defining an EtherChannel that includes ports in different VLANs. It also prevents you from assigning the ports in an existing EtherChannel to different VLANs.

Virtual LAN (VLAN)

Catalyst VLAN Configuration Menu

The two headings within this menu are accessible only when the Enhanced Feature Option is installed.



More information on Port and Name Configuration follows these brief explanations.

Catalyst VLAN Port Configuration

Displays the VLAN Configuration menu, which you use to assign ports to VLANs.

Catalyst VLAN Name Configuration

Displays the assigned name of the VLAN. The names can be changed by using the prompts displayed on that screen.

Virtual LAN (VLAN)

Catalyst VLAN Port Configuration Screen

Use the Catalyst VLAN Port Configuration screen to assign ports to a particular VLAN.

Catalyst VLAN Port Configuration		
<u>Index</u>	<u>Name</u>	
1	Default	
2	Default	
3	Default	
4	Default	
5	Default	
6	Default	
7	Default	
8	Default	
9	Default	
10	Default	
11	Default	
12	Default	
13	Default	
14	Default	
Return	More	Change

Use cursor keys to choose item
Press <RETURN> to confirm choice

H4789

Index

The index number that you want to assign to a VLAN.

Name

The name of the VLAN where you are assigning the ports.

When you select “Change” and press the RETURN key, you are prompted to enter the port number, and select the name of the VLAN.

For each VLAN you set up, you must set up the IP parameters and spanning tree parameters.

Virtual LAN (VLAN)

VLAN Name Configuration Screen

Use the VLAN Name Configuration screen to describe each VLAN. The VLAN name can be a maximum of 20 characters in length.

Catalyst VLAN Name Configuration

Index	Name
1	VLAN01
2	VLAN02
3	VLAN03
4	VLAN04
5	VLAN05
6	VLAN06
7	VLAN07
8	VLAN08
9	VLAN09
10	VLAN10
11	VLAN11
12	VLAN12
13	VLAN13
14	VLAN14

Return More Change

Use cursor keys to choose item
Press <RETURN> to confirm choice

H4639

Index

Number of the VLAN index.

Name

Name or description of this VLAN.

IP Configuration from the Configuration Menu

Select this menu from the Configuration menu. Use this menu to view or change the IP configuration information.

IP Configuration - default

Return to Previous Menu	
IP Address	192.121.254.22
Default Gateway	0.0.0.0
Subnet Mask	0.0.0.0
IP State	BootP When Needed
IP Packet Type	ETHERNET
Send PING	

Enter the IP state (Down/Up with optional BootP/Up with mandatory BootP)
Use cursor keys to choose item. Press <RETURN> to confirm choice.
Press <ESC> to cancel, <CTRL><P> to discard changes and pop to Main Menu.

H4688

IP Address

Displays the current IP address. To change it, highlight the selection and press RETURN.

Default: 0.0.0.0

Virtual LAN (VLAN)

Default Gateway

Displays current gateway address. The default is the IP address of the gateway or router through which information must pass to get to the NMS application.

Default: 0.0.0.0

Subnet Mask

Displays the current subnet mask.

Default: 0.0.0.0

IP State

Select choices of IP Disabled, BootP When Needed or BootP Always by highlighting IP State and pressing RETURN, then highlighting one of the choices and pressing RETURN.

Default: BootP when Needed

IP Packet Type

Display type of Ethernet packet being presented.

Send PING

Prompts for entering an IP address, then sends a PING to that address.

IP Disabled

When a VLAN is IP-disabled, it does not process any IP or ARP packets it receives. This means that no SNMP, Ping, Telnet, or ARP Packets will be responded to when received.

Note Sending a Ping from an IP-disabled VLAN or a VLAN whose IP address is 0.0.0.0 may cause system problems.

BootP When Needed

In this state, IP is enabled for the VLAN and will function immediately if a non-zero IP address has been stored in NVRAM when the Catalyst 3000 initializes. In each VLAN that an IP address of 0.0.0.0 and a state of BootP When Needed are stored in NVRAM on boot (or NVRAM is not initialized on boot), the Catalyst will broadcast BootP requests in an attempt to determine its own IP address. Until it receives a reply, this is the only IP function the Catalyst will support (in the VLAN).

BootP When Needed is the factory-set default. A Catalyst for which NVRAM is not initialized (for instance, a new Catalyst out of the box or on a bootup after NVRAM is cleared) or one whose NVRAM is corrupted and unreadable, will therefore always attempt to use BootP the first time.

BootP Always

In this state, IP is enabled for the VLAN but will not function fully on boot until a BootP reply has been received. If a non-zero IP address is stored in NVRAM for a given VLAN in this state when booted, it is cleared to 0.0.0.0 since it would never be used.

BootP Requests and Parameters

When using BootP to determine its IP address, the Catalyst repeats BootP requests at regular intervals, beginning at 1 second each and eventually decreasing to every 5 minutes over time until it receives a valid reply. If the IP display for the VLAN is accessed from the console (or via Telnet from another VLAN) during that time, the Catalyst may cease using BootP if the parameters are set (on display exit) in such a way that BootP would no longer be necessary - for instance, if the IP state is switched from BootP Always to IP-disabled or if a non-zero IP address is specified in any IP state.

Once the Catalyst has ceased sending BootP requests on a VLAN, it does not restart sending requests on that VLAN for any reason besides an entire Catalyst reset. It also does not recognize BootP responses on that VLAN from that point onward.

Besides the IP address, several other parameters in a BootP response are also recognized and recorded in NVRAM, when received in the same response:

- Default Gateway (see note below)
- Subnet Mask

Virtual LAN (VLAN)

- TFTP Bootfile Name
- TFTP Server Address (only recognized if the Bootfile name is present)

One other parameter, the TFTP VLAN, is inferred whenever a TFTP Bootfile name is present in the BootP response. That is, if the Catalyst receives a BootP response that specifies a TFTP Bootfile name, the Catalyst automatically records the VLAN on which the response was received as the TFTP VLAN number. Therefore, the bootfile name should not be specified on a VLAN from which the TFTP server cannot be accessed, either directly or through the VLAN's default gateway (if one exists). More information on TFTP is available under the section "TFTP" within this chapter.

Note The default gateway accepted is the first one in the list of routers whose net/subnet address is the same as that of the IP address specified. If no routers are specified or if none qualify, the gateway address for the VLAN will be zeroed out and recorded as such in NVRAM when the IP screen is exited.

SNMP Configuration from the Configuration Menu

The next selection of the Configuration Menu is the SNMP Configuration menu.

Screen displays and explanations of this menu and its sub-menus are presented in Chapter 9, "Monitoring the Network with SNMP."

The next section describes spanning tree and the Spanning Tree menus from the Configuration menu.

Spanning-Tree Protocol (STP)

The Spanning-Tree Protocol is a bridge-to-bridge link management protocol that provides path redundancy while preventing undesirable loops. To provide path redundancy, the Spanning-Tree Protocol defines a tree that spans all switches and bridges in the extended network; if one of the network segments in the tree becomes inaccessible, the spanning tree reconfigures itself to re-establish the links. To prevent loops, the spanning tree selects just one Catalyst 3000 port as the designated path to the root, assigning it the Forwarding, or active state. It assigns all other ports the Blocking, or standby, state. A port in the Blocking state does not forward any transmitted frames in any direction.

To set up the Catalyst 3000 to use the Spanning-Tree Protocol, you must assign a *path cost* and *path priority* to each network segment.

Note In the VLAN STP configuration menu, for the selection of port priority/port path cost, select only the ports which are part of the current VLAN. Do not configure ports in other VLANs.

The path cost indicates the relative speed of the segment: The higher the speed of the segment, the lower the path cost. Switches and bridges in the network attempt to determine the path to the route with the lowest path cost. IEEE 802.1D recommends that you assign path costs using the following formula:

Path cost = 1000/LAN speed in Mbps

If two ports to the root have the same path cost, the spanning tree device selects the one with the highest priority (lowest value), an arbitrary value that you assign. To block traffic on a particular segment, assign it low path priority (high value).

The following section describes using Spanning Tree.

Spanning-Tree Protocol (STP)

Spanning Tree Menu

Select the Spanning Tree menu from the Configuration menu. Use the Spanning Tree menu to specify whether the Catalyst 3000 is participating in the spanning tree and, if so, to configure spanning tree bridge and port parameters.

Spanning Tree - default

Return to Previous Menu	
Participate in Spanning Tree	No
Switch Priority	32768
Switch Hello Time (in Seconds)	2
Switch Maximum Message Age (in Seconds)	20
Switch Forward Delay (in Seconds)	15
Port Priority...	
Port Path Cost...	
Current Spanning Tree Information	

Display the Configuration Menu

Use cursor keys to choose item. Press <RETURN> to confirm choice.
Press <CTRL><P> to return to Main Menu.

H44687

Participate in Spanning Tree

Select Yes or No by moving highlight to heading, pressing RETURN, move highlight to Yes or No and press RETURN. If you select No, the remaining values on the menu will be saved, but will have no effect. Selecting Yes will enable spanning tree upon exiting this screen.

Default: No

Note Telnet user-sessions are terminated when any changes are made to spanning tree parameters.

Switch Priority

Enter a priority value for this Catalyst 3000. The Catalyst 3000 with the lowest priority value in a spanning tree becomes the root. (To change individual port priorities, select *Port Priority Menu*.)

Range: 0–65535

Default: 32768

Switch Hello Time (in Seconds)

Enter a time between configuration messages when this switch is root. The minimum value may not be less than 1. The maximum may not be more than the lower of 10 or *Switch Maximum Message Age/2 - 1*. The upper range limit that appears reflects the value currently selected for *Switch Maximum Message Age*.

Default: 2

Spanning-Tree Protocol (STP)

Switch Maximum Message Age (in Seconds)

Enter the maximum message age displayed when this switch is root. The minimum value may not be less than the higher of 6 or $(2 \times (\text{Switch Hello Time} + 1))$. The maximum may not be more than the lower of 40 or $(2 \times (\text{Switch Forward Delay} - 1))$. The range limits that appear reflect the values currently selected for *Switch Hello Time* and *Switch Forward Delay*.

Default: 20

Switch Forward Delay (in Seconds)

Enter the time the switch waits between transitions from listening to learning, and from learning to forwarding. The minimum may not be less than the larger of 4 or $(2 \times (\text{Switch Maximum Message Age}/2 + 1))$. The maximum may not be higher than 30. The lower range limit that appears reflects the value currently selected for *Switch Maximum Age*.

Default: 15

Port Priority Menu

Displays a list of the port priorities of user selectable values (see beginning of this section for a description of the calculation).

Port Path Cost Menu

Displays a list of port path costs of user selectable values (see beginning of this section for a description of the calculation).

Current Spanning Tree Information

This selection displays more information if spanning tree is set up (“Yes” is selected under “Participate in Spanning Tree” prompt).

When the spanning tree is turned off—that is, you have selected “No” for the “Participate in Spanning Tree” prompt—this menu cannot be selected.

Port Priority Screen from Spanning Tree Menu

View the Port Priority Menu to set up Spanning Tree priorities for each port.

Port Priority

<u>Port</u>	<u>Priority</u>
1	128
2	128
3	128
4	128
5	128
6	128
7	128
8	128
9	128
10	128
11	128
12	128
13	128
14	128

Return More Change

Return to Previous Menu

Use cursor keys to choose item. Press <RETURN> to confirm choice.
Press <CTRL><P> to return to Main Menu.

H4686

Spanning-Tree Protocol (STP)

Port

The number of the port.

Priority

Select the port whose priority value you want to change, highlight “Change” and then press the RETURN key, enter the port number, then enter the new value. The port with the lowest number has the highest priority. New values take effect when you return to the previous menu.

Range: 0–255.

Default: 128

More

To view more ports in the table.

Change

To change or add values to specific ports.

Port Path Cost Menu

Use the Port Path Cost Menu to view and change the spanning tree path cost associated with each port. The Spanning Tree uses port path costs to determine which port to select as a forwarding port.

Port Path Cost	
<u>Port</u>	<u>Cost</u>
1	100
2	100
3	100
4	100
5	100
6	100
7	100
8	100
9	100
10	100
11	100
12	100
13	100
14	100

Return More Change

Return to Previous Menu

Use cursor keys to choose item. Press <RETURN> to confirm choice.
Press <CTRL><P> to return to Main Menu.

H4685

Spanning-Tree Protocol (STP)

Port

Select the port whose cost you want to change, press RETURN.

Cost

After selecting the port, enter a new value. When the spanning tree reconfigures itself, it selects forwarding ports based on the port cost. Therefore, assign lower numbers to ports attached to faster media (such as Full-Duplex Ethernet, Fast Ethernet or EtherChannel), and higher numbers to ports attached to lower-bandwidth media, such as Half-Duplex Ethernet. New values take effect when exiting this screen by choosing *Return to Previous Menu*.

Range: 0–65535.

Default: 100

Change

To change or add values to specific ports.

Current Spanning Tree Information Screen

Use the Current Spanning Tree Information screen to view a summary of all spanning tree information for each port; the information is updated every second. You cannot change any information on this screen. When the spanning tree is turned off—that is, you have selected “No” for the “Participate in Spanning Tree” prompt—this menu cannot be selected.

When the Catalyst 3000 is configured with EtherChannels, spanning tree packets use the primary port of the EtherChannel.

Current Spanning Tree Information

Exit Hello Time: 2. Max Message Age: 20. Forward Delay: 15
 Root: 32768.008024013F57. Root Port: This Bridge is Root

Port ID	Port Cost	Port STS	Desig Cost	Designated Switch/Bridge ID	Desig Port ID	#Topo Chgs	Time Since Last Change
128.1	100	FWD	0	32768.00802401375F	128.1	1	0:01:58
128.2	100	FWD	0	32768.00802401375F	128.2	1	0:01:58
128.3	100	FWD	0	32768.00802401375F	128.3	1	0:01:58
128.4	100	FWD	0	32768.00802401375F	128.4	1	0:01:58
128.5	100	FWD	0	32768.00802401375F	128.5	1	0:01:58
128.6	100	FWD	0	32768.00802401375F	128.6	1	0:01:58
128.7	100	FWD	0	32768.00802401375F	128.7	1	0:01:58
128.8	100	FWD	0	32768.00802401375F	128.8	1	0:01:58
128.9	100	FWD	0	32768.00802401375F	128.9	1	0:01:58
128.10	100	FWD	0	32768.00802401375F	128.10	1	0:01:58
128.11	100	FWD	0	32768.00802401375F	128.11	1	0:01:58
128.12	100	FWD	0	32768.00802401375F	128.12	1	0:01:58
128.13	100	FWD	0	32768.00802401375F	128.13	1	0:01:58
128.14	100	FWD	0	32768.00802401375F	128.14	1	0:01:58
128.15	100	FWD	0	32768.00802401375F	128.15	1	0:01:58

Return to Previous Menu

Use cursor keys to choose item. Press <RETURN> to confirm choice.
 Press <CTRL><P> to return to Main Menu.

H4684

Hello Time

The Hello Time, in seconds, advertised by the root and used by all bridges and switches in the active topology of the spanning tree network.

Spanning-Tree Protocol (STP)

Max Message Age

The Maximum Message Age, in seconds, advertised by the root and used by all bridges and switches in the spanning tree network.

Forward Delay

The Forward Delay Time, in seconds, advertised by the root and used by all bridges and switches in the spanning tree network.

Root

The priority and MAC address of the switch in the spanning tree that this switch has accepted as the root device.

Root Port

The number of the port on this switch that is closest to the root. This switch communicates with the root through this port. If this switch is the root, “This Bridge is Root” is displayed.

Port ID

The port ID, used to determine the role of the port in the spanning tree. The port ID is expressed in the form *<port priority>.<port number>*. All ports in an EtherChannel have the same ID number.

Port (Path) Cost

The *Port Path Cost* for each port on the switch. The Port Path Cost helps determine the role of the port in the spanning tree network.

Port STS

Current state of this port within the spanning tree: DSB (disabled), BLK (blocked), LSN (listening), LRN (learning), or FWD (forwarding). The rules that define the state of the port are as follows:

- A port on a network segment with no other bridge or switch is always forwarding.
- Two ports of the switch are connected to the same network segment and there is no other bridge or switch, the port with the smaller ID is forwarding and the other is blocked.
- When the switch is booted, all ports are blocked initially, then some of them change to a different state: listening, learning, and forwarding, in order. To see the change in states you must repeatedly exit from this menu, then select it again. All ports that are going to change states from blocking to forwarding will have done so after:

$\text{MaxMessAge} + (2 * \text{Switch Forward Delay})$

Designated Cost

The cost for a packet to travel from this port to the root in the current spanning tree configuration. The slower the media, the higher the cost.

Designated Switch/Bridge ID

Priority and MAC address of the device through which this port has determined it must communicate with the root of the spanning tree.

Designated Port ID

Port on the designated device through which this switch will communicate with the root of the spanning tree. This information is useful if the Catalyst 3000 is the designated switch on one or more network segments.

Topo Changes

Number of topology changes, which is the number of times the port has entered the Forwarding state plus the number of times the port has made the transition from Forwarding to Blocking. The counter is reset when the switch is reset or the spanning tree is turned on: whichever is most recent.

Spanning-Tree Protocol (STP)

Time Since Last Change

The time since the last time the port entered the Forwarding state or made the transition from Forwarding to Blocking.

Port Configuration Screen from Configuration Menu

You can enable or disable a port using the Port Configuration Menu. The menu also reports other port settings.

Note To change the Duplex mode, you must change the Duplex DIP switch settings (located on the back panel of the Catalyst 3000); you cannot change the duplex mode from the Port Configuration menu.

Port Configuration							
Port	Type	Link	MDI/MDIX	Speed	Mode	Duplex	Enabled/Disabled
1	AUI	up	MDIX	10	A-CT	Half	Enabled
2	10BaseT	down	MDIX	10	A-CT	Half	Enabled
3	10BaseT	down	MDIX	10	A-CT	Half	Enabled
4	10BaseT	down	MDIX	10	A-CT	Half	Enabled
5	10BaseT	down	MDIX	10	A-CT	Half	Enabled
6	10BaseT	down	MDIX	10	A-CT	Half	Enabled
7	10BaseT	down	MDIX	10	A-CT	Half	Enabled
8	10BaseT	down	MDIX	10	A-CT	Half	Enabled
9	10BaseT	down	MDIX	10	A-CT	Half	Enabled
10	10BaseT	down	MDIX	10	A-CT	Half	Enabled
11	10BaseT	down	MDIX	10	A-CT	Half	Enabled
12	10BaseT	down	MDIX	10	A-CT	Half	Enabled
13	10BaseT	down	MDIX	10	A-CT	Half	Enabled
14	10BaseT	down	MDIX	10	A-CT	Half	Enabled

Return More Change

Return to previous menu

Use cursor keys to choose item. Press <RETURN> to confirm choice.
Press <CTRL><P> to return to Main Menu.

H4683

Port

The port number.

Type

Type of interface associated with this port

Spanning-Tree Protocol (STP)

Link

Whether a valid link status signal is associated with the port. “Up” means a device is connected to the port, “down” means that no device is connected, and “unknown” refers to 10Base-T port 1. Port 1 is not recommended for this use. See Chapter 5, “Installation” for an explanation on the use of port 1.

MDI/MDIX

The MDI setting for 10Base-T ports.

Speed

The Ethernet speed for that port.

Mode

Shows error handling mode, such as Cut-Through or Store and Forward.

Duplex

For 10Base-T ports; shows the current setting of the Duplex DIP switch for this port, which is located on the back panel. New duplex settings take effect when the DIP switch is moved.

Enabled/Disabled

Operational status of ports. Toggle between enabled and disabled by selecting the port and pressing RETURN. The new status takes effect immediately.

Default: Enabled

Spanning-Tree Protocol (STP)

Module Information Screen from the Configuration Menu

This menu provides information on any expansion modules that were installed. The Catalyst 3000 is listed as the first module.

Box 2 Module Information							
Module	Status	Model	Board Id	Revision	Ports	Mode	Up Time
1	up	WS-X3002	6	1	4		321:49:27
2	up	WS-X3010	26	0	2		321:49:27
3	up	WS-X3002	6	1	4		321:49:27
4	up	WS-X3013	7	15	3		321:49:27
5	empty						
6	up	WS-X3007/8	14	0	2		321:49:27
7	up	WS-X3002	6	1	4		321:49:27
8	up	WS-X3004	2	0	1		321:49:27

Return

Display the next page of port configuration table
Use cursor keys to choose item. Press <RETURN> to confirm choice.
Press <CTRL><P> to return to Main Menu.

H4662

Status

Lists if the module slot is populated and if so, if it is enabled (up/down).

Type

Lists the type of module.

Revision

Lists the revision level of the module.

Ports

Lists how many ports are on the module.

Up Time

Lists how long the module has been active.

SwitchProbe Menu from the Configuration Menu

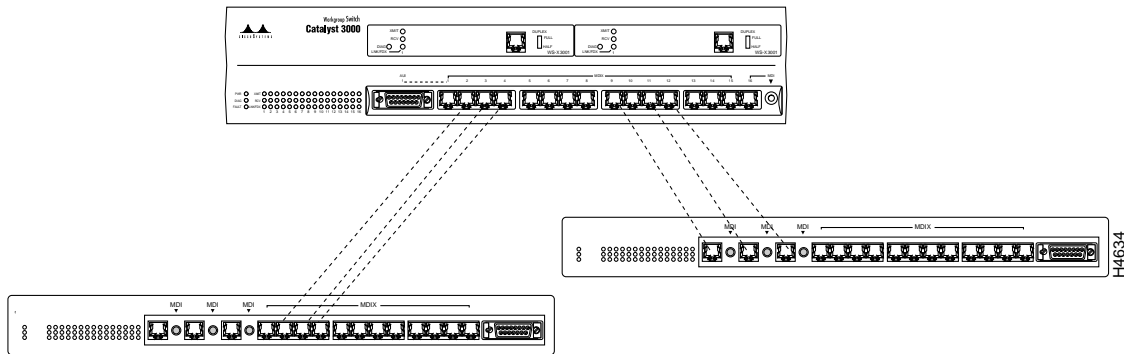
The screen displays and explanations of this menu and its sub-menus are presented in Chapter 10, “Monitoring Port Activity with SwitchProbe.”

The following section is a description of EtherChannel and how it is used with the Catalyst 3000.

EtherChannel

To improve interswitch bandwidth, you can create an EtherChannel by connecting two Cisco Catalyst 3000 devices that have two to seven links. An EtherChannel provides bandwidth of from 20-80 Mbps in Half-Duplex mode, or from 40-160 Mbps in Full-Duplex mode. You can create an EtherChannel only between two Catalyst 3000 devices or between a Catalyst 3000 and a CiscoPro unit, and not between a Catalyst 3000 and a workstation.

Figure 7-2 Setting up EtherChannels



The EtherChannel feature affects other Catalyst 3000 features in the following ways:

- *Half-duplex and Full-duplex.* A single EtherChannel can include a combination of half-duplex and full-duplex connections—for example, an EtherChannel containing three ports can have two full-duplex and one half-duplex connection. However, each pair of interconnected ports must both be either half duplex or full duplex.
- *Statistics reporting.* Statistics for the EtherChannel are displayed for individual ports, not for the EtherChannel as a whole. Station addresses are distributed among the ports in the EtherChannel. See Chapter 8, “Monitoring the Network With Out-of-Band Management.”
- *Address Filtering.* Address filters are automatically added to every port in an EtherChannel.

EtherChannel software learns addresses differently than regular ports, as follows:

- *New source address.* When a packet arrives at an EtherChannel port with an unknown source address, the system module creates an entry in the master table and the port table for the EtherChannel. The system module assigns the primary port in the EtherChannel as the port of entry.

For additional source addresses, the system module assigns ports of entries alternately to other ports in the EtherChannel. When all ports in the EtherChannel have at least one address assigned, the system module starts assigning from the primary port again.

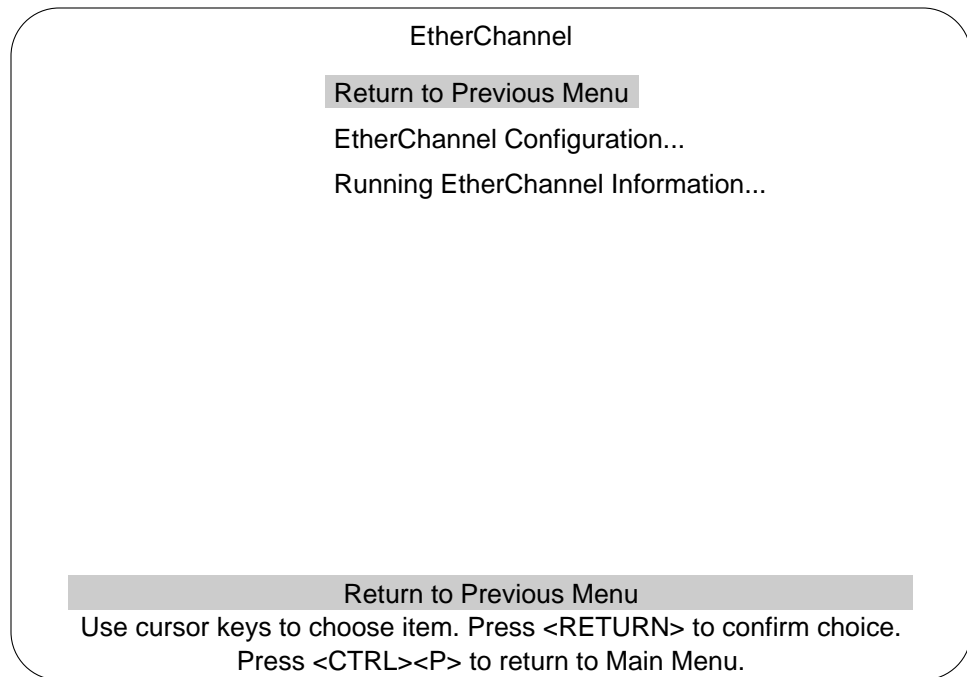
Note When using EtherChannel, set the Address Aging Time (System Information Menu) to 60 minutes or more. More frequent aging is undesirable because the time it takes to remove inactive addresses may affect Catalyst 3000 performance.

- *New destination address.* An unknown destination address packet is sent out the primary ports of the EtherChannel, but entries are not made in port tables until a reply packet comes back. Entries in port tables depend upon the destination.
- *Broadcast and multicast packets.* Broadcast and multicast packets go to the primary port of each EtherChannel.
- *Link Failure.* If one link in an EtherChannel fails, a trap is sent and the entire EtherChannel is disabled.

EtherChannel

EtherChannel Screen from the Configuration Menu

Use the EtherChannel menu to add, delete, and change EtherChannels.



EtherChannel Configuration Menu

Use the EtherChannel Configuration menu to add, delete, and change EtherChannels. A description of creating an EtherChannel follows.

EtherChannel Configuration

<u>EtherChannel</u>	<u>Ports</u>
1	not defined
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 Entry

Press <RETURN> to display table
Press <CTRL><P> to return to Main Menu.

H4638

EtherChannel

List of different EtherChannel set ups.

Ports

The ports within that specific EtherChannel.

EtherChannel

Add Entry

Prompts you to enter port numbers in the EtherChannel. Enter at least 2 ports, but no more than 7 ports, from lowest number to highest, separated by spaces. Don't use 10Base-T port 1 for EtherChannel.

Delete Entry

Asks whether you want to remove the entry, then deletes the selected EtherChannel.

Change Entry

Prompts you to re-enter the port numbers in the selected EtherChannel, from lowest to highest, separated by spaces.

Clear Entry

Deletes all EtherChannels.

Setting up an EtherChannel

Follow these steps to set up an EtherChannel:

- Step 1** Disconnect the ports you want to add to the EtherChannel, or disable them using the Port Configuration menu.
- Step 2** For one Catalyst, select the EtherChannel menu (shown later in this section), then choose Add Entry from the menu bar at the bottom on the screen.
- Step 3** Enter the ports (port 1 is not recommended for EtherChannel use) for the EtherChannel column, separated by spaces.
- Step 4** Choose Exit.
- Step 5** Repeat steps 1–4 for the other Catalyst devices.
- Step 6** Set the *Address Aging Time* to the same value for the Catalyst devices.
- Step 7** If you disconnected the ports in the EtherChannel, reconnect them. If you disabled them using the Port Configuration menu, use the menu to re-enable them.

Running EtherChannel Information Menu

Use the Running EtherChannel Configuration menu to display the status of the EtherChannel.

Running EtherChannel Information

<u>EtherChannel</u>	<u>State</u>	<u>Ports</u>
1	up	5 6 7

Return

Return to Previous Menu

Use cursor keys to choose item. Press <RETURN> to confirm choice.
Press <CTRL><P> to return to Main Menu.

H6277

EtherChannel

EtherChannel

The number of the EtherChannel referring to the information displayed on the present screen.

State

Whether the specified EtherChannel is active or not.

Ports

What ports are in that EtherChannel.

Address Filtering

The Address Filtering feature enables you to restrict certain users from communicating with other users. To do this, you can specify source and destination MAC-layer Ethernet addresses to be filtered at the source port. Ethernet addresses can be unicast, multicast, or broadcast.

The advantage of address filtering is increased access control and network segmentation. For example, suppose one port is connected to a server containing confidential information from the engineering workgroup. You can prevent access to the server by setting up filters for the addresses of connections from workgroups other than engineering. This is an example of two “types” of filters, “allowing a source address” (engineering) or “blocking a source address(es)” (other workgroups). Examples of different types of filters are allowing, forcing, or blocking packets from a source address, or allowing, forcing, or blocking packets to a destination address. A detailed explanation of filter types is in the section [Configure Filters Screen](#) from the MAC Filter and Port Security Menu

Observe the following guidelines when setting up address filters:

- Use the Port Configuration menu to create port filters.
- Filters are port specific and applied to a Catalyst 3000 incoming port only.
- Up to 100 “filters” can be created for each Catalyst 3000 (the filters must be applied to specific ports at a specified Catalyst 3000). A “filter” is a combination of a MAC address *and* the “type” of filter it is. For example, if the MAC address 0000A3 C00021 is configured as source type at a port and also configured as a destination type, that would count as two different filters (towards the maximum of 100 filters).

Address Filtering

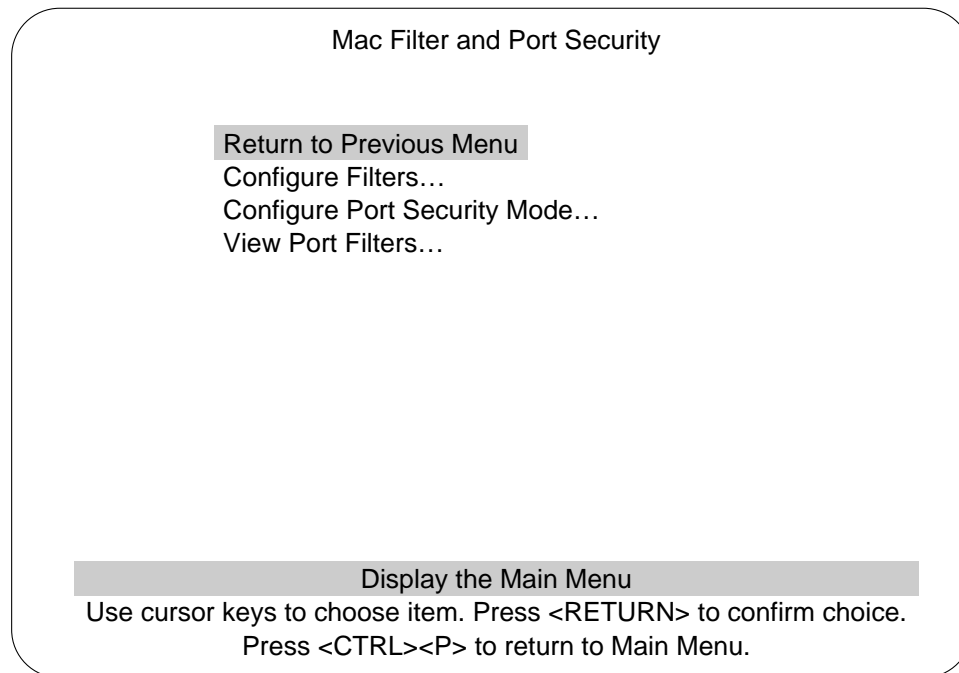
- You can apply these filters to any combination of ports as long as there is a maximum of 100 *filters* (not 100 ports, because more than one port can be part of a filter). For example:
 - Filter “A” (MAC address 0000A3 C00021, source type) can be applied to ports 1, 5, 7, 14 (or to all 16 ports)
 - Filter “B” (MAC address 0000A3 C00021, destination type) can be applied to the same ports, or different ports, or once again, to all the ports
 - Filter “C” (MAC address 0340B7 A02026, source type) can be applied to any combination of ports; until a maximum of 100 *filters* are created.
- If you set up a filter for broadcast packets, hosts on the other side of the Catalyst 3000 may not see ARP broadcast packets. To prevent this, let the Catalyst 3000 learn the host addresses before implementing the filter. Most hosts time out their local address entries and attempt to relearn with a broadcast ARP.

Note To restrict access from one segment to an entire segment—not just an address—see “Virtual LAN (VLAN).”

The following menus, in this Address Filtering section, are used to set up address filtering. More explanations of address filtering are presented as functions within these menus are described.

MAC Filter and Port Security Screen from the Configuration Menu

The MAC Filter and Port Security Screen:



H4792

Address Filtering

Configure Filters

Used to establish specific filtering of addresses.

Configure Port Security Mode

Establishes address security at specific ports.

View Port Filters

Displays filtering set up for specific ports.

Configure Filters Screen from the MAC Filter and Port Security Menu

Configure Filters

<u>Index</u>	<u>Mac Address</u>	<u>Type</u>	<u>Applied Ports</u>	<u>Exit Ports</u>
--------------	--------------------	-------------	----------------------	-------------------

Return Zoom More Add Entry Delete Entry Clear Table

Return to Previous Menu

Use cursor keys to choose item. Press <RETURN> to confirm choice.
Press <CTRL><P> to return to Main Menu.

H4793

Configuring Filters

When the Add Entry is selected, a list is displayed of the available filter functions with a selectable highlight. After the user makes a choice, the program then prompts for the necessary parameters.

There are four filter functions from which to choose. They are:

- Block a packet with a source address
That is, any packet from that specific address is blocked from entering the specified port(s)
- Block a packet with a destination address
Any packet with the specified destination address is blocked at the specified port(s)
- Allow a packet with the source address to be sent to certain ports
If a packet is received from a specific address it is allowed to go to specific port(s)
- Force a packet with the destination address to certain ports
When a packet with a specific address must go to specified port(s)

The following is a description of the above filter functions:

Block A Packet With a Source Address

The purpose of this filter is to restrict a certain address, on filtered port(s), from sending any packets. If you select this filter, the following parameter fields appear for you to enter data:

```
Please enter the MAC address (xx xx xx xx xx xx)
Please enter the port(s) to apply this filter:
```

Block A Packet With a Destination Address

The purpose of this filter is to restrict a certain address, on filtered port(s), from receiving any packets. If you select this filter, the following parameter fields appear for you to enter data:

Please enter the MAC address (xx xx xx xx xx xx)
Please enter the port(s) to apply this filter:

Allow a Packet with the Source Address To be Sent To Certain Ports

The purpose of this filter is to restrict a certain address, on filtered port(s), so it can send packets only to specific ports. If you select this filter, the following parameter fields appear for you to enter data:

Please enter the MAC address (xx xx xx xx xx xx)
Please enter the port(s) where a matching packet is allowed to go:
Please enter the port(s) to apply this filter:

Force A Packet with the Destination Address To Certain Ports

The purpose of this filter is to constrain a certain address, on filtered port(s), so any packets sent to it are forced to specific ports. If you select this filter, the following parameter fields appear for you to enter data:

Please enter the MAC address (xx xx xx xx xx xx)
Please enter the port(s) where a matching packet must go:
Please enter the port(s) to apply this filter:

Note The table displayed in the filter screen is updated as a filter is added.

For a stack configuration you cannot enter more than one port on any remote box. You can enter more than one port on the local box.

Address Filtering

The information in each column of the Configure Filters menu is described as follows:

MAC Address

The address the filter is applied to.

Type

It is determined by the filter function selected. The type of functions are:

- Src (Source) applies to the source address in a packet.

The two types of source addresses are:

- Block a packet with a source address
- Allow a packet with the source address to be sent to certain ports

- Dst (Destination) applies to the destination address in a packet.

The two types of source addresses are:

- Block a packet with a destination address
- Force a packet with the destination address to certain ports.

Applied Ports

The port(s) where this filter entry is applied for that specified MAC address.

Exit Ports

The specified port(s) where a packet is allowed to go, or forced to go (for that specific MAC address).

The type of filter functions that would *not* have an exit port are:

- Block a packet with a source address, or
- Block a packet with a destination address:

Value is 0 when either of the above two entries are selected, since any matching packet is blocked and has no exit port

The type of filter functions that would have an exit port are:

- Allow a packet with the source address to be sent to certain ports

At this entry, it is the only port(s) where a matching packet is allowed to go

- Force a packet with the destination address to certain ports

At this entry, it is exactly the port(s) where a matching packet is forced to go

Address Filtering

Configure Port Security Mode

This mode establishes secure address levels for specific ports.

Note This function “disables the address learning” capability of the Catalyst 3000 and totally blocks (secures) specific addresses at selected ports.

Selecting this heading at the MAC Filter and Port Security screen, presents a screen with the Configure Port Security table on it, as shown below.

There are four address security choices:

- Normal
- Send the specified source address (this blocks all other addresses)
- Send the specified destination address (this blocks all other addresses)
- Send the specified source and destination addresses (this blocks all other addresses)

Configure Port Security Mode

<u>Port</u>	<u>Security Mode</u>
1	Normal
2	Secure Source Address
3	Secure Destination Address
4	Secure Both Source and Destination Address
5	Normal
6	Normal
7	Normal
8	Normal
9	Normal
10	Normal
11	Normal
12	Normal
13	Normal
14	Normal

Return More Change

Return to Previous Menu

Use cursor keys to choose item. Press <RETURN> to confirm choice.
Press <CTRL><P> to return to Main Menu.

H4679

Address Filtering

View Port Filters Screen

The following screens are examples of ports using the MAC address filters and port security.

Port 1 - View Port Filters

<u>Index</u>	<u>MAC Address</u>	<u>Description</u>
1	0000A3 C00021	This address is blocked
2	000824 07FE31	This address is allowed to talk to port(s) 11 12 13

More

Port 1 Security Mode: Normal

Use cursor keys to choose item. Press <RETURN> to confirm choice.
Press <CTRL><P> to return to Main Menu.

H4678

Index

Numerical order of entries.

MAC Address

Filter Address

Description

List of descriptions of security modes as assigned at Configure Port Security Mode menu:

- This address is blocked
- This address is allowed to talk to ports (as specified)
- This address cannot be reached from this port
- Traffic to this address will be forced to ports (as specified)

Return

Return to main menu.

More

Displays additional entries in the filter table if the table contains multiple pages.

Port (number) Security Mode

The type of security mode applied to this port.

Address Aging

You can set the per-port aging value using the Address Aging menu. The following describes the types of address aging.

There are two types of aging:

- Port aging
 - Any address in a port's address table that has not been active for a port's configured aging time will be removed from the port's table
 - Set at the Port Address Table Aging menu
- System aging
 - Addresses that are local to a port but did not fit in its address table will be removed from the master and all port address tables after the system aging time
 - Set at the Master Address Table Aging menu

There are two levels to set for the port and master aging tables:

Time Interval Aging is a time limit, in minutes, which will drop “older” addresses after the selected time.

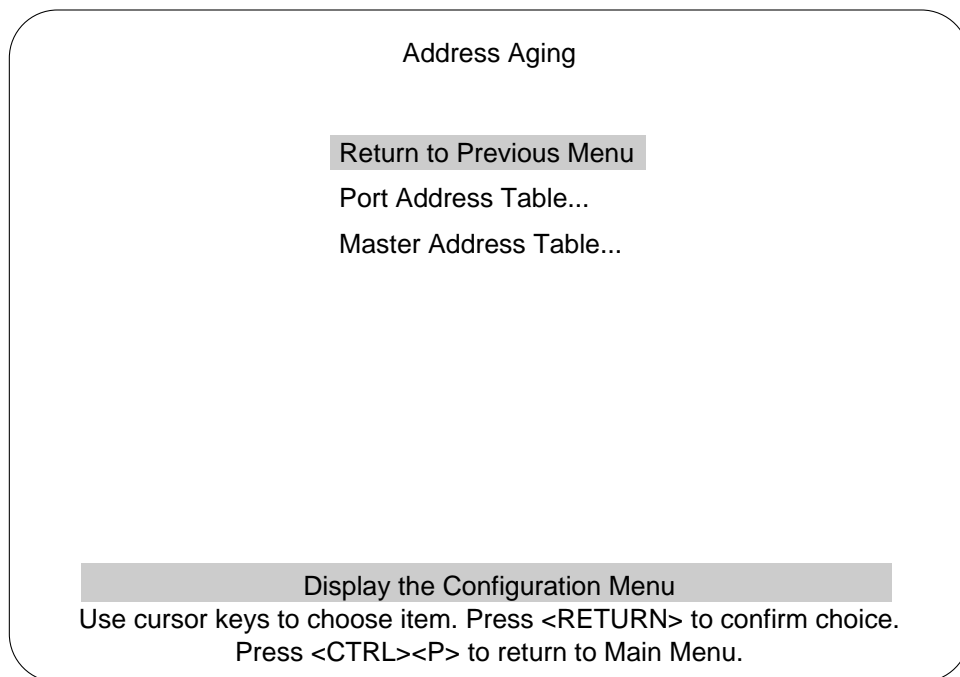
Automatic On-Demand Aging stores addresses until reaching maximum capacity of the table, then deletes addresses, (in the following specific order) down to a selected percentage level and continues to cycle in the same manner.

- Random remote addresses
- Sequential remote addresses
 - Sequentially aged from the top of the Address Aging table to the bottom of the table
- Random local addresses
- Sequential local addresses

More information on address aging and the address aging screens is presented in the following sections.

Address Aging Menu from the Configuration Menu

Address aging is accessed through the Address Aging heading from the Configuration Menu.



Port Address Table...

Highlighting this selection and pressing RETURN will display the Port Address Table Aging menu. Use this menu is to set each port on the Catalyst 3000 to the aging time, in minutes, and to the demand aging level percentage you want.

Address Aging

Master Address Table...

This screen shows the Master Aging Time and Demand Aging Level. An example of that selection is shown after the Port Address Table Aging screen.

The following displays a view of the Port and Master Address Table Aging screens and describes the information within them.

Port Address Table Aging Menu

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

Return More Change

Return to Previous Menu

Use cursor keys to choose item. Press <RETURN> to confirm choice.
Press <CTRL><P> to return to Main Menu.

H4675

Port

The port to which you want to assign an aging time.

Aging Time

A valid port aging time associated with the port. Addresses will be discarded after reaching the set time limit. The default setting for this parameter is 15 minutes. The maximum time for this value is 9999 minutes.

Demand Aging Level

Sets a 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.

Address Aging

Master Address Table Aging

The Master Address Table Aging is the aging value of a set time, in minutes, and a set percentage level after which unused addresses are removed from its table. Addresses that are local to a port but did not fit in its address table (“orphans”) will be removed from the master and all port address tables after the master aging time, regardless of whether the address has been seen within that time period. This is to ensure that no unused address will remain in memory for an indefinite time.

Master Address Table Aging screen:

Box 1 Master Address Table Aging

Return	
Aging Time	15 minutes
Demand Aging Level	90 %

Return to Previous Menu

Use cursor keys to select action. Press <RETURN> to confirm choice.
Press <CTRL><P> to return to Main Menu.

H4676

The Master Address Table Aging screen contains two main headings:

Box (number)

The box (Catalyst 3000) that this Master Address Table Aging screen is in reference to.

Aging Time

This value is set by selecting the heading, pressing RETURN and entering a number, in minutes, from 0 to 9999. Addresses will be discarded after reaching the set time limit. Using the setting value of 0 turns aging off.

Demand Aging Level

This parameter works in the same way as Port Demand Aging Level, only using the system address table.

Port Switching Mode from the Configuration Menu

This screen shows the status of the switching error-handling modes available on the Catalyst 3000.

Box 1 Port Switching Mode

Port	Switching Mode	Error Water Mark	Runt-free Mode
1	Auto	50%	on
2	Cut-Through	35%	off
3	Store&Forward	90%	on
4	Auto	50%	off
5	Auto	50%	off
6	Auto	50%	off
7	Auto	50%	off
8	Auto	50%	off
9	Auto	50%	off
10	Auto	50%	off
11	Auto	50%	off
12	Auto	50%	off
13	Auto	50%	off
14	Auto	50%	off

Return More Change

Return to Previous Menu

Use cursor keys to choose item. Press <RETURN> to confirm choice.
Press <CTRL><P> to return to Main Menu.

H4677

Switching Mode

Displays three modes of error-handling switching:

- *Automatic* - Automatically converts error-handling from Cut-Through to Store and Forward. The user sets a percentage threshold, which is called an “error water mark”, at the Port Switching Mode screen. When set to automatic switching, the error handling is normally in cut-through mode, but if the error rate exceeds the error water mark, error-handling is automatically converted to store and forward. If the error rate once again falls below the error water mark, the error-handling automatically reverts back to cut-through. This process continues under automatic control as long as this mode is selected.
- *Cut-Through* - (Forced) error-handling only in the cut-through mode. Cut-Through mode reduces latency times by not reading the whole incoming packet. Only the beginning of the packet is read and immediately routed to its destination.
- *Store and Forward* - (Forced) error-handling only in the store and forward mode. The complete incoming packet is read, stored and then forwarded to its destination.

To change the mode, highlight “Change” and press RETURN. You are prompted to select mode, then the high water percentage (if Auto mode selected) and finally the setting for Runt-free mode.

Error Water Mark

If Auto mode is selected for that port, set at what percentage level of errors the Catalyst 3000 will switch from cut-through to store-and-forward mode. Percentage level is set by the user.

Runt-free Mode

The last item this screen displays is the setting and displaying of the Runt-free mode. This mode is set to either on or off; on means that an incomplete packet (less than 64 bytes) will be discarded, and a runt packet error is logged and displayed under the Statistics menus; off means runt packets will be forwarded.

Broadcast Suppression from the Configuration Menu

As the name implies, this feature is to suppress broadcast packets. This function is set on a per port basis at the Broadcast Suppression screen. If set to on (enable), that port is set to a percentage threshold level (Broadcast Water Mark) at which broadcast packets are suppressed (percentage is based on total traffic). If the broadcast level on a specific port exceeds the set threshold, all broadcasts originating from that port are blocked until the broadcast level drops below that mark.

Box 1 Broadcast Suppression

<u>Port</u>	<u>Broadcast Suppression</u>	<u>Broadcast Water Mark</u>
1	on	50%
2	off	

Return More Change

Return to Previous Menu

Use cursor keys to choose item. Press <RETURN> to confirm choice.
Press <CTRL><P> to return to Main Menu.

H5279

Broadcast Suppression

Displays whether broadcast suppression is enabled or disabled for that specific port.

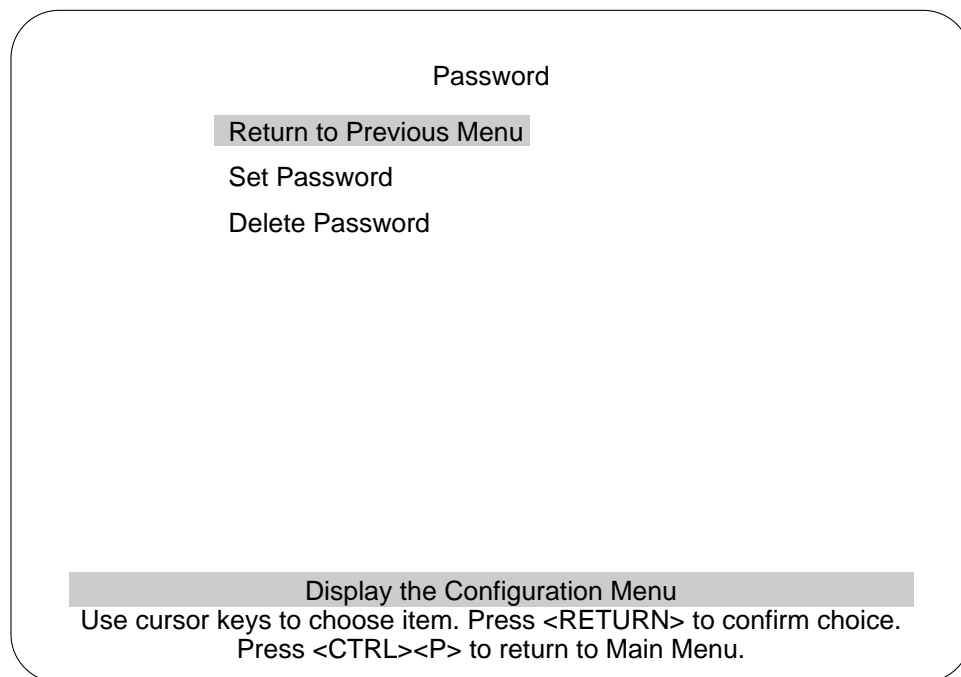
Broadcast Water Mark

A user defined percentage level based on broadcast traffic compared to the total traffic on that port. If broadcast traffic exceeds this level, packets are suppressed until they fall below that level.

Broadcast Suppression from the Configuration Menu

Password Menu from the Configuration Menu

Use the Password menu to add, change, or delete a password. If you establish a password, users must enter it to access the Console menus. If there is no password, just press RETURN at the password prompt.



Set Password

Establishes or changes the password.

Delete Password

Deletes the password.

The system prompts you to enter the present password before it allows you to change or delete the password. If you are establishing a new password, press RETURN at the Set Password prompt.

The password is saved across warm boots and power cycles.

Note The Catalyst 3000 must have a different password than the Catalyst Stack. If you have forgotten the password, you can delete it by depressing the **Sys Req** button on the back panel of the Catalyst 3000 for 1 second, releasing it, then selecting Clear Non-Volatile RAM from the menu that appears. You must then re-enter **all** system configuration information, including reentering the key for the optional Enhanced feature set.

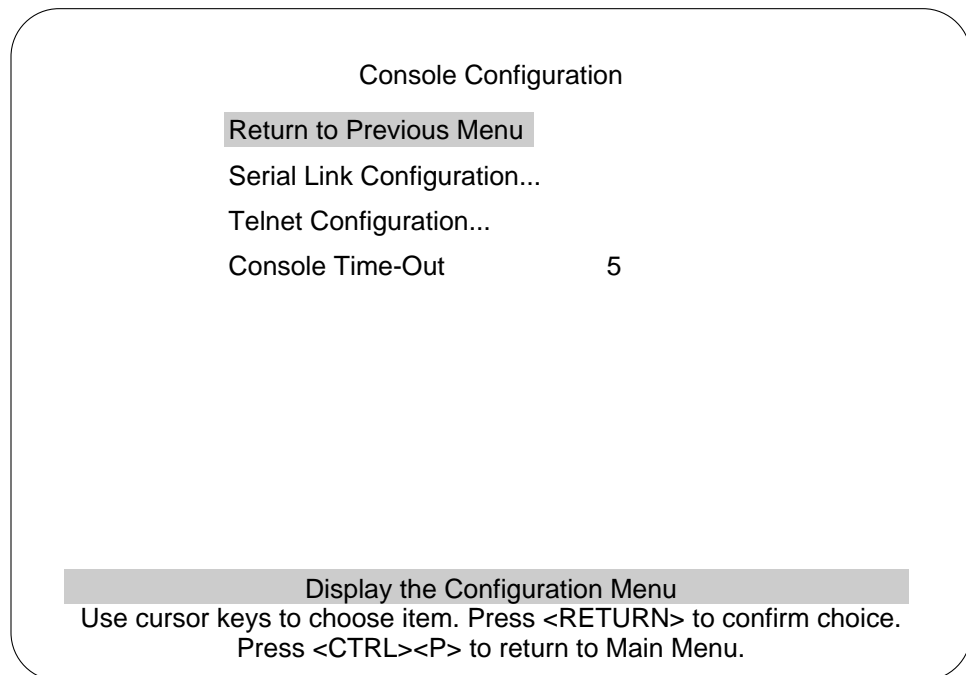
Console or Telnet Sessions

The following procedure describes how to establish a console or Telnet session.

Console Configuration

This menu has the selections for configuring console and Telnet sessions.

There are three selections in the Console Configuration menu:



H4674

Serial Link Configuration

An example of that screen and an explanation of its contents follows.

Telnet Configuration

An example of that screen and an explanation of its contents follows.

Console Timeout (in minutes)

A value that can be set to determine when the console session will timeout and return to the Greeting menu. If the value is set to zero, the console will never time out.

Serial Link Configuration Menu

Use the Serial Link Configuration Menu to configure the Catalyst 3000 to communicate with the console via modem. The default baud is 9600.

Serial Link Configuration

Return to Previous Menu

Hardware Flow Control	Disabled
Software Flow Control	Disabled
Autobaud Upon Break	Enabled
Console Baud Rate	38400

Return to Previous Menu

Use cursor keys to choose item. Press <RETURN> to confirm choice.
Press <CTRL><P> to return to Main Menu.

H4672

To set up a modem, as part of the Serial Link Configuration, follow these steps:

- Step 1** Set *Wait for a Connection* to 45 sec.
- Step 2** Set *Pause Between Calls* to 6 sec.
- Step 3** Set *Autobaud Detect* to On.

Step 4 Set the *Drop DTR* (Data Terminal Ready) to Yes.

Step 5 Set the *Send CR Between Calls* to Yes.

Step 6 Set *Send init if CD High* to Yes

Hardware Flow Control

Enables or disables RTS/CTS handshaking.

Default: Disabled



Caution Hardware handshaking must be turned on at both the terminal and the Catalyst 3000 and you must have a 7-wire or a 9-wire cable to the terminal. If hardware handshaking is off and you are using a 3-wire cable, a catastrophic failure of the Catalyst 3000 could occur.

Software Flow Control

Enables the XON and XOFF characters, which are 11 and 13 hex, respectively.

Default: Disabled

Autobaud Upon Break

Enables the Autobaud feature. When a BREAK key is sent or received the baud rate is reset when you press the RETURN key rapidly for five seconds. It is recommended that this feature is not disabled.

Default: Enabled

Console Baud Rate

Default: 9600

Starting the Console Session

Start the console by pressing RETURN after re-booting the system. If a Telnet session is active, press RETURN at the console to terminate the Telnet session and press RETURN again to start the console session.

Stopping the Console Session

Pressing **Ctrl-P** returns the console session to the Main Menu and pressing **Ctrl-B** returns to the Greeting Menu.

Unix Users

A Telnet session can be terminated abnormally in a UNIX environment, especially by being killed by another process. If the user environment seems to have locked after termination of the Telnet session, try typing `<CTRL><J>stty sane<CTRL><J>`. Because the Telnet Server is doing the echoing for the user, the user's terminal capabilities have been modified for the duration of the Telnet Session due to the Telnet option negotiation. If the user's Telnet process or task is abruptly terminated, the user's terminal may be left in a no-echo, raw mode.

Telnet Configuration

The following menu and functions describe Telnet configurations.

Telnet Configuration

Return to Previous Menu

Number of Telnet Sessions Allowed 5

Disallow new Telnet Session no

Terminate all Active Telnet Sessions

Telnet Sessions...

Display the Configuration Menu

Use cursor keys to choose item. Press <RETURN> to confirm choice.
Press <CTRL><P> to return to Main Menu.

H4671

Console or Telnet Sessions

Return to Previous Menu

Returns to Console Configuration menu.

Number of Telnet Sessions Allowed

Limits the number of Telnet sessions. Numbers allowed are from 1 to 5. Highlight this selection and press RETURN and enter the number.

Disallow New Telnet Session

Choice of Yes or No to allow or disallow a new Telnet session. Press RETURN at this selection and use arrow keys to highlight Yes or No and press RETURN.

Terminate All Active Telnet Sessions

If this selection is highlighted and RETURN is pressed any Telnet sessions will be terminated.

Telnet Sessions...

Shows status of "Remote" and "Local" Telnet sessions.

Screen of Telnet Session:

Telnet Sessions

Index	Box	--- Remote ---		--- Local ---		Status
		IP	Port	IP	Port	
1	1	192.216.254.19	16	192.216.254.41	8	Open

Return Close Session

Return to Previous Menu

Use cursor keys to choose item. Press <RETURN> to confirm choice.
Press <CTRL><P> to return to Main Menu.

H4670

Console or Telnet Sessions

Index

Numerical order of entries.

Box

The number ID of the Catalyst 3000 in a stack.

Remote

Lists the IP address and the port number of the Remote Telnet session.

Local

Lists the IP address and the port number of the Local Telnet session.

Starting the Telnet Session

The observe the following when starting a Telnet session to the Catalyst 3000.

- In the IP Information menu, the IP State must be set to “BootP When Needed” or “BootP Always” for the IP stack and Telnet to work.
- The Telnet must be pre-configured to have a VT100/VT220 compatible setup.
- Only one type of session is supported at any time, either the console or Telnet session. Starting a Telnet session before ending the console session causes the screen to display a “Console is currently in use” message.
- There may be conflicts between Telnet sessions. If one Telnet session is disrupted by the user at the console, the Telnet session’s configuration may not have been completed. In some menus, changes take effect immediately, as in adding filters, and in other menus, such as STP, the changes are not saved until the menu is exited.

Stopping the Telnet Session

The Telnet session can be terminated by pressing **Ctrl-B** or any other means available through the user’s Telnet application.

Involuntary Termination of the Telnet Session

The following can terminate a Telnet session:

- A Telnet session can be terminated involuntarily by the console or by itself. When the console is idle and Telnet is active, a user at the console can terminate the Telnet session without warning. When the Telnet session ends, the Telnet session screen displays the message: “Your session has been terminated due to system maintenance work.”
- If any changes are made in the spanning tree configuration.
- The Telnet session also ends if a user makes changes in any of the following IP parameters:
 - IP address
 - Default gateway
 - Subnet mask
 - IP state
- The Telnet session also times out if there has been no activity for 5 minutes.

Note If you are in a Telnet session and change the IP parameters either in the IP Information Session menu or Catalyst VLAN IP Configuration menu, and save the changes using the Exit option from the menu, you will lose the connection to your Telnet session, even if the IP parameters you change are in another VLAN.

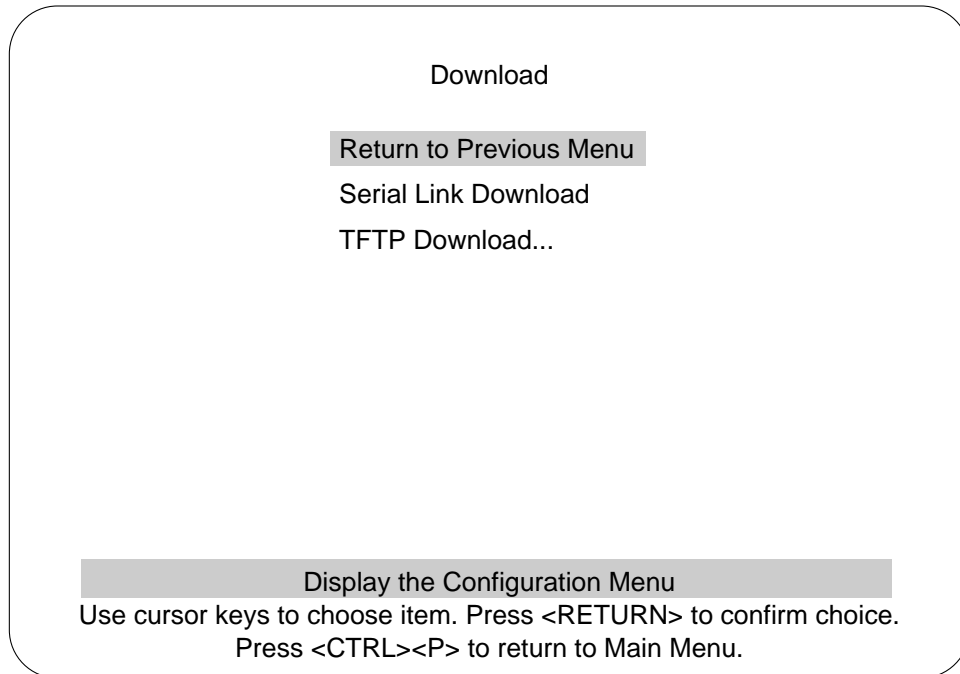
Download Menu From the Main Menu

The Download menu is accessed from the Main Menu.

Downloading is used to load the Flash Memory within the Catalyst 3000. The Download menu displays two download choices. The two choices are TFTP (Trivial File Transfer Protocol) download and the Serial Link download (console).

Note Downloading (such as updating firmware levels) to an individual Catalyst 3000 while it is part of a Stack may cause conflicts within the Stack. Except for very specific situations, downloading should be done to a Catalyst 3000 as a stand-alone unit. If the unit is part of a Stack, disconnect the Stack Port cable before downloading.

Note Operating a Stack with Catalyst 3000 units that are at different levels (versions) of firmware (software code) is not recommended (for example, version 1.1.1 verses 1.1.2). When Catalyst 3000 units attempt to join a Stack and the Catalyst 3000 units have different software (firmware) versions, the console screen displays a warning that different versions are attempting to form a Stack.



Serial Link download is for downloading via the console. Selecting the Serial Link download displays a prompt requesting to “confirm new code download via serial port (Y or N)”. Selecting Yes starts the Serial Link downloading. Follow the prompts as they are displayed.

The next section describes TFTP, and the TFTP downloading.

TFTP Downloading Procedure

TFTP is not invoked automatically on the Catalyst 3000 as it is on certain other network devices such as a diskless workstation. This is because there should normally be a functional software image in Flash memory and, therefore, TFTP is not a standard part of the Catalyst 3000 bootup procedure (under normal circumstances). TFTP is intended for use during software upgrades and, once a new image is installed, there should be no need for TFTP until the next software upgrade is installed.

In view of this, the TFTP function in the Catalyst 3000 is designed as an explicitly requested operation with operator-settable parameters. Note that changes to these parameters may be altered and are used when starting a download in the display, however they are not recorded until the display is exited normally.

The TFTP Download menu is accessed through the Main Menu. From the Main Menu select the Download Menu and then select the TFTP Download Menu.

TFTP Download Menu

TFTP Download

Return to Previous Menu

TFTP Server Address 192.216.254.39

Download VLAN default

Download Filename /ftpboot/cat3_111.gz

Execute Network Download

Execute Stack Network Download

Display the Configuration Menu

Use cursor keys to choose item. Press <RETURN> to confirm choice.
Press <CTRL><P> to return to Main Menu.

H4690

TFTP Server Address

The address of the host serving as the TFTP server.

Download VLAN

The VLAN name through which the download is attempted.

Download Menu From the Main Menu

Download Filename

The file the Catalyst 3000 attempts to download, as it is to be received and interpreted by the TFTP server. (The security mode in use on the TFTP server may affect this.)

Note By using Download VLANs default server if it has one, the file may be downloaded from another network anywhere on the Internet from which the VLAN can get packets routed - even another directly connected VLAN. In the latter case, the Catalyst 3000 actually loads, or attempts to load, through the gateway and not ignore its Download VLAN parameter. If the Catalyst 3000 seems unable to reach a TFTP server to which it should have a direct or indirect route, an incorrectly set Download VLAN may be the reason.

Execute Network Download

The function "Execute Network Download" initiates the download. The screen displays which block it last received from the server (Block 0 if no reply has been received) until the last packet arrives. The Catalyst 3000 does not attempt to load any of the image into FLASH memory until it receives the final packet. Therefore, if interrupted or cancelled for any reason before the last packet, the previous system image remains intact in FLASH memory.

Once the last packet has arrived, the Catalyst 3000 immediately begins clearing FLASH memory and then loading it with the new image.

The Catalyst 3000 continues to use its previously loaded software until its next reset by whatever means, then the newly stored image becomes functional.

Note Do not use this function for downloading to a stack configurations

Note Be careful - if the process is interrupted during this time, the stored image may be corrupted and the Catalyst 3000 is not able to boot normally! If this happens, it is necessary to download the Catalyst 3000 via its console port since the system boot image does not contain software capable of operating the Catalyst 3000 network hardware or understanding IP and TFTP protocols. During this fairly short vulnerable period of time, the diagnostic LED on the Catalyst 3000 blinks to indicate the clearing (slow blink) and reloading (faster blink) of FLASH memory. The screen also displays messages indicating these events.

Execute Stack Network Download

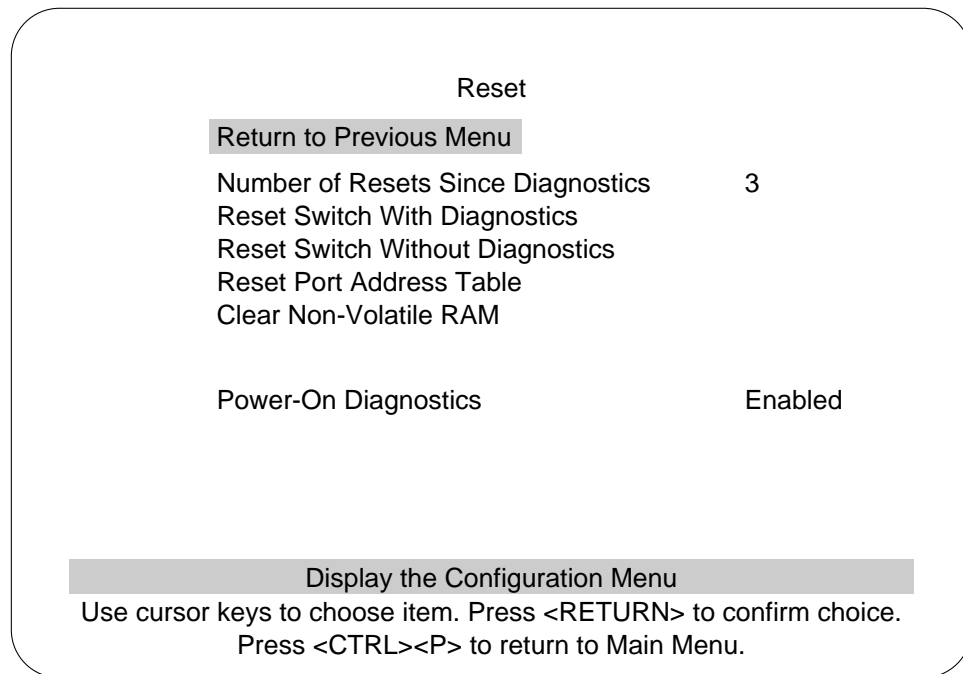
Use this function for a Stack configuration. This function initiates downloading for the Stack. The procedure is similar to the above single stand-alone Catalyst 3000 download; however, the Stack download procedure downloads to the entire Stack of switches in one operation. (Downloading is done one switch at a time, until all of the switches are completed.)

When the Stack download procedure is used, only the same code or the same level of code can be downloaded for all of the switches in the Stack.

Reset Heading from Main Menu

The Reset menu is accessed from the Main Menu.

The Reset screen, as shown below, displays the reset options available with the Catalyst 3000.



Number of Resets Since Diagnostics

Number of times the switch has been reset since the switch was powered on or ran power-on diagnostics. This is an informational heading, the data cannot be changed.

This number is not reset to 0 when Non-volatile RAM is cleared.

The following four headings within the Reset menu are command functions that can be selected and initiated by moving the highlight over the heading and pressing RETURN.

Reset Switch With Diagnostics

A reset function is initiated with this selection. It resets the switch hardware; runs diagnostic tests; clears all counters, including address tables; and restarts the Catalyst 3000. When the Catalyst 3000 reboots, administrative parameters from nonvolatile memory are used to initialize the operational parameters. This takes approximately 4 to 5 minutes.

Reset Switch Without Diagnostics

This command resets the switch hardware; clears all counters, including address tables; and starts the Catalyst 3000. When the Catalyst 3000 reboots, administrative parameters from nonvolatile memory are used to initialize the operational parameters. This takes approximately 40 seconds.

Reset Port Address Table

Selecting this command clears all address table entries for a specified port (user is queried for which port to reset), sets port traffic counters to zero, and sets Time Since Last Reset for this port to zero.

Reset Heading from Main Menu

Clear Nonvolatile RAM

Deletes all user-configured parameters; baud rate, IP address information, EtherChannel, VLAN, Spanning Tree and then resets the switch.

Note Clearing NVRAM (Nonvolatile RAM) erases all configuration parameters, including the Enhanced feature key. Follow these guidelines if you must clear NVRAM:

- If you are using the EtherChannel feature, be sure to disconnect the affected ports—or disable them on the Port Configuration menu and reset the switch—*before* clearing NVRAM.
- If you are using the Spanning Tree option, be aware that port costs and priorities are lost, which may result in loops. Use the menus to re-establish port costs and priorities, then reset the switch to make the new parameters take effect.
- To re-enable the Enhanced feature set, see the “Switch/Stack Information” section later in this chapter. For units shipped with the Enhanced feature set, the key is on the bottom of the unit.

Power-On Diagnostics

This is a selectable option that determines whether diagnostics are, or are not, initiated during power-on. To change the selection, highlight the heading and press RETURN, then select Enabled or Disabled, and press RETURN.

Default: Enabled