Doc. No. 78-4545-01 Rev. A0

2.2(1) Version Software Configuration Note Catalyst 3000 Series

This note provides specific information regarding the configuration of Catalyst 3000 series equipment and software.

This configuration note introduces and describes the following features:

- Dynamic Inter-Switch Link Protocol (DISL)
- Cisco Group Management Protocol (CGMP)

Note New ATM firmware for the Catalyst 3000 series ATM expansion modules has been released for the 2.2(1) software release. The new firmware is version 14. It is fully compatible with existing main images. The new version firmware must be installed in the ATM module in order for CGMP to work when CGMP messages from the router arrive over ATM.

For the latest information on limitations or anomalies for the 2.2(1) software release refer to the "2.2(1) Version Software Release Note Catalyst 3000 Series".

For detailed information about configuring a Catalyst 3000 series switch, refer to the Installation and Configuration Guide for that model of the Catalyst switch.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

Dynamic Inter-Switch Link Protocol

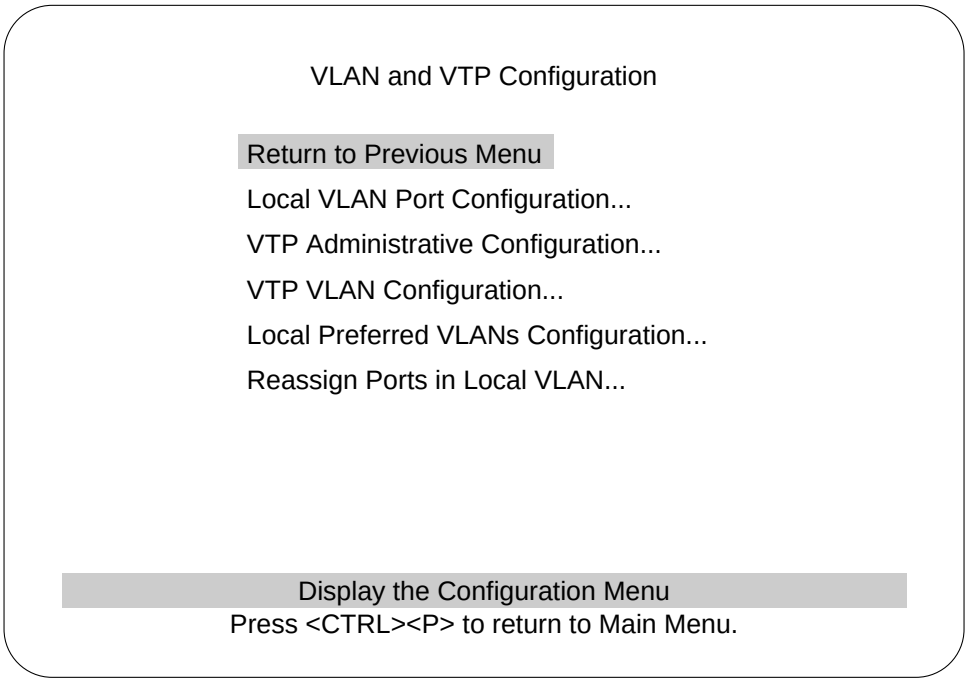
Dynamic Inter-Switch Link Protocol (DISL) synchronizes the configuration of two interconnected Fast Ethernet interfaces into an ISL trunk. DISL minimizes VLAN trunk configuration procedures because only one end of a link needs to be configured as a trunk.

Configuring DISL

Use the following steps to configure trunking on ISL ports. For a complete description of VLANs, ISL, VTP, or port configuration, see the Installation and Configuration Guide of your model of Catalyst 3000 series switch.

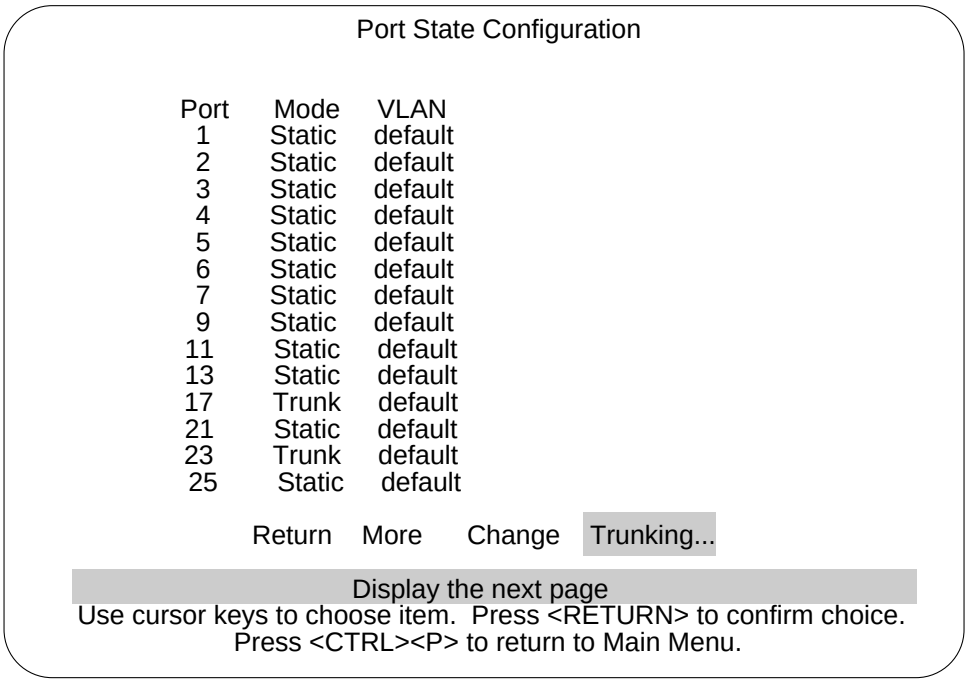
Step 1 Using the console, access the VLAN and VTP Configuration menu (see Figure 1).

Figure 1 VLAN and VTP Configuration Menu



Step 2 At the VLAN and VTP Configuration menu, select the Local VLAN Port Configuration menu. The menu titled Port State Configuration is displayed (see Figure 2). This menu shows the VLANs that are carried on each port, and whether each port is a Trunk or is Static.

Figure 2 Port Configuration Menu



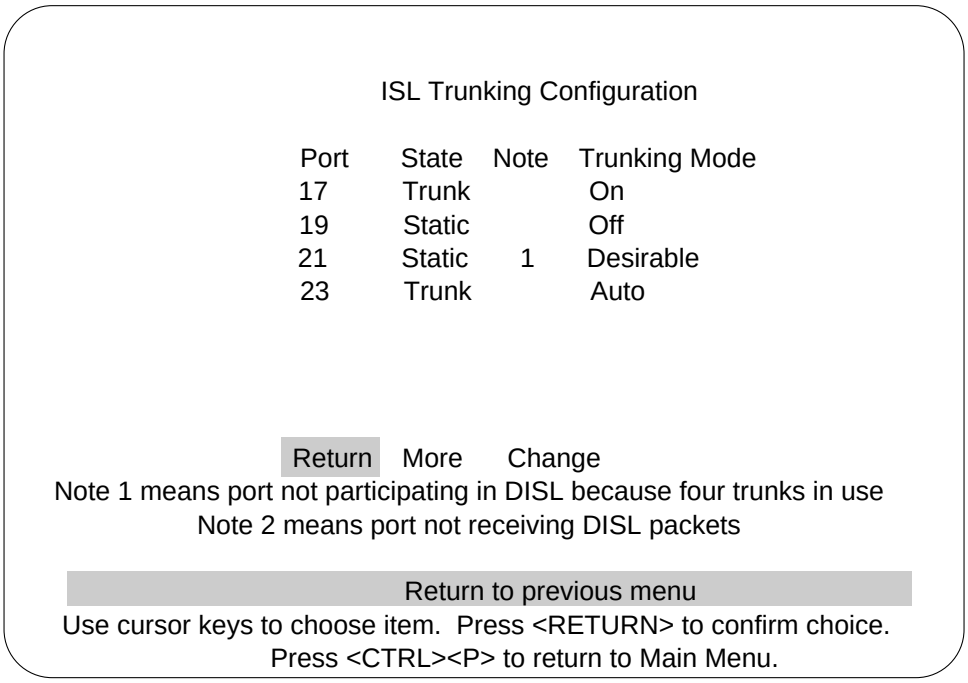
Step 3 From the Port State Configuration menu, choose the Trunking mode option to display the ISL Trunking Configuration screen. An example of this screen is shown in Figure 3. Use this screen to configure the DISL trunking mode for each ISL port.

The ISL Trunking Configuration screen displays:

- A list of each ISL port available on the switch
- The current trunking state of the port
- Special notes regarding the trunking state
- The port's DISL trunking mode.

The State and Note columns refresh automatically every few seconds to display the current state of each ISL port.

Figure 3 ISL Trunking Configuration Screen Example



Note With the 2.2(1) release, the ISL Configuration screen is replaced by the ISL Trunking Configuration screen.

Step 4 To change the trunking mode of any port, select the Change option.

Step 5 When the prompt, “Enter port number to change” is displayed, enter the number of the ISL port that you want to change. If you enter a port number that isn’t an ISL port, a warning message is displayed and you can enter another port number.

Step 6 Once you enter an ISL port number, four options representing the four DISL trunking modes are presented:

- Auto
  - A port set to Auto becomes a trunk only if the port it's connected to (its neighbor) is a trunk. If the neighbor is not a trunk, the port will function as normal in the Static mode.
- Desirable
  - If you want an ISL port to be a DISL trunk when a neighbor port supports DISL trunking.
- On or Off
  - The On and Off trunking modes are intended to be used when an ISL port is connected to another ISL port that does not support the DISL protocol. The On or Off trunking modes are not recommended to be used when the DISL protocol is in use. The following section describes precautions when using the On and Off trunking modes.

Step 7 Select one of these choices to change the chosen port to the selected trunking mode. This menu activates changes as soon as they are selected.

Precautions for On Trunking Mode

The On (or Off) trunking modes may cause configuration problems. The On or Off modes are intended to be used when an ISL port is connected to a neighbor port that you know does *not* support the DISL protocol. Since configurations can change, it is preferable to set the trunking mode to Auto or Desirable. If the neighbor port does not support DISL, the port functions as normal in Static mode.

Using the On trunking mode when DISL protocol is in use may lead to ISL-mode mismatches where one end of the link is trunking while the other end is not. If a trunk is desired, the Desirable trunking mode should be used.

Using the Off trunking mode is also not recommended when using DISL protocol. The risk of creating an ISL-mode mismatch is lower with the Off mode, but if a trunk is not desired, Auto mode should be used.

The Notes Column in the ISL Trunking Configuration Screen

A 1 or a 2 is displayed in the Note column of the ISL Trunking Configuration screen to indicate why an ISL port is not a trunk when the configuration implies that it should be.

Note 1 is displayed if this port is not sending or processing DISL packets because it cannot be configured as a trunk port since it would exceed the limit of four trunk ports on that switch.

Note ATM ports are always trunks, so each ATM port is considered part of the four trunk limit.

Note 2 means that the neighboring ISL port does not appear to be processing or sending DISL packets.

Note There may not be an immediate indication of the neighboring ISL port not processing or sending DISL packets, so note 2 may take several minutes to appear.

Trunking Mode Notes

If the selected trunking mode causes a port to change between the Trunk and Static states, the console may operate slowly for a few seconds. The State and Note columns of the screen update automatically after the port changes between states.

The Port State Configuration screen also shows whether ports are trunks or not. This screen does *not* update automatically. To update the screen, exit and reenter this screen, or choose the More option.

Four-Trunk Limit

There is a limit of four trunks that can be configured on a Catalyst 3000 series switch. This is not a factor on the Catalyst 3000 or 3100 because they have an installation limit of four high-speed ports. However, the Catalyst 3200 can have up to 14 high-speed ports installed (which can be configured with ISL). This means (potentially) more than four ports on that switch can be configured in trunking modes that allow a port to become a trunk (on, auto, and desirable). Once a Catalyst 3200 has four trunk ports configured, DISL packets are not sent or received on any static ISL ports. This prevents the Catalyst 3200's static ports, and any neighboring ISL ports, from switching into trunk ports (unless the On Trunking Mode is used as described in the section "Precautions for On Trunking Mode").

Dynamic Trunking Modes with Version 2.2(1)

With versions 2.0 and 2.1 software releases, ISL ports have only two (non-dynamic) trunking modes: ISL Trunk and Non-ISL. With the 2.2(1) upgrade, ISL ports that were configured as ISL Trunk are automatically changed to the Desirable trunking mode and ISL ports that were configured as Non-ISL are automatically changed to the Auto trunking mode.

Cisco Group Management Protocol

CGMP manages multicast traffic in Catalyst 3000 series switches by allowing directed switching of IP multicast traffic within a network.

CGMP offers the following benefits:

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

How CGMP Works

CGMP works in conjunction with Internet Group Management Protocol (IGMP) messages to dynamically configure Catalyst 3000 series switch ports so that IP multicast traffic is forwarded only to those ports associated with IP multicast hosts.

Note For information on IP multicast, including IGMP, refer to RFC 1112.

CGMP software components run on both the router and the Catalyst 3000 (and 5000) series switches. A CGMP-capable IP multicast router sees all IGMP packets and, therefore, can inform the Catalyst 3000 series switch when specific hosts join or leave IP multicast groups. When the CGMP-capable router receives an IGMP membership request packet, it creates a CGMP packet that contains the request type (either join or leave), the multicast group address, and the actual MAC address of the host. The router then sends the CGMP packet to a well-known address to which all Catalyst 3000 series switches listen. When a switch receives the CGMP packet, the processor interprets the packet and modifies the forwarding table. This process is performed automatically.

If a spanning-tree VLAN topology changes, the CGMP-learned multicast groups on the VLAN are purged. In this case, the CGMP-capable router will generate new multicast group information.

If a CGMP-learned port link is disabled for any reason, CGMP removes that port from any multicast group memberships.

Joining a Multicast Group

When a particular host wants to join an IP multicast group, it sends an IGMP join message specifying its MAC address and which IP multicast group it wants to join. The CGMP-capable router then builds a CGMP join message and multicasts the join message to the well-known address to which the Catalyst 3000 series switches listen. Upon receipt of the join message, each Catalyst 3000 series switch searches a table to determine if it contains the MAC address of the host asking to join the multicast group. If a switch finds the host's MAC address in the table associating the MAC address with a port, the switch creates a multicast forwarding entry in the forwarding table. The host associated with that port will now receive multicast traffic for that multicast group. In this way, the table automatically learns the MAC addresses and port numbers of the IP multicast hosts.

Leaving a Multicast Group

The CGMP-capable router sends periodic multicast-group queries. If a host wants to remain in a multicast group, it responds to the query from the router. In this case, the router does nothing. If a host does not want to remain in the multicast group, it does not respond to the router query. If after a number of queries, the router receives no reports from any host in a multicast group, the router sends a CGMP command to the Catalyst 3000 series switch, telling it to remove the multicast group from its forwarding tables.

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

Enhanced Leave Processing

Leave-Processing allows IGMP hosts attached to the Catalyst switch to leave without causing any abnormal functionality of other hosts in the same or different groups.

Enhanced Leave Processing Requirements

Note For Enhanced Leave Processing (ELP) to be fully effective, observe the following important requirements.

In order for the a host to take full advantage of the Enhanced Leave Processing feature, it's IGMP implement must:

- Support IGMPv2 (Version 2) software.
- The IGMPv2 leave group request should be sent to the all-routers IP multicast group address (224.0.0.2) and it should always be sent when the host leaves a group. If the leave group request is sent to the group being left, the switch will not see the request and be unable to process a leave for that host.

How ELP Works

When a host decides to leave a group, it sends an IGMPv2 leave message on the network segment. The Catalyst switch intercepts and processes the leave request and sends (on the port from which it received the leave request) a query to the all-systems IP multicast group (224.0.0.1), with the Ethernet destination address being the group specific MAC address.

The Catalyst switch starts a timer in response to the host leaving the group on that port and waits for other members in the group, if any, to respond. The members who receive this query respond with an IGMP report which is forwarded to the CGMP router. The CGMP Router processes these IGMP reports and generates CGMP Join messages for each of the IGMP reports. If one of these CGMP Joins is for a host on a port and a group being left, the Catalyst cancels the associated timer before it expires. If the timer does expires, the port will be deleted as a port member of the group.

When there are no more non-router ports in the group, the Catalyst switch sends an IGMP leave for the group, to the multicast routers.

Note It is normal if a Network General Sniffer reports "Mis-directed frames" on the IGMP query messages that the switch sends in response to the IGMP leaves.

ELP Unassigned IP Address

The Catalyst switch uses the IP address assigned to that VLAN on the switch as the source IP address for both the IGMP Query and IGMP Leave group messages that the switch generates as part of the Enhanced Leave Processing. If no IP address is assigned to the VLAN, the unspecified IP address of 0.0.0.0 is used. If this causes problems there are two solutions:

- Assign an IP address to the VLANs being used
- Disable IGMP Enhanced Leave Processing

CGMP Limitations

1. CGMP will not be effective in limiting multicast traffic received on a Catalyst 3000 series ATM interface.

   It is not possible to limit the destinations to which received multicast traffic will be forwarded when multicast traffic is received on a the Catalyst 3000 series ATM interface. Multicast traffic is forwarded (flooded) to all other ports in the switch or Stack that are in that same broadcast domain.

2. Since the Catalyst 3000 ATM interfaces do not forward any multicast traffic to the CPU including those packets that contain unknown source or destination addresses, it is possible that a host which is connected to the switch via an ATM interface and which is only sending multicast traffic, will never have it's MAC address learned. Since CGMP depends on finding the host's MAC address to determine which ports to add as members of a multicast group, CGMP will be unable to add the ATM port as a member. To avoid this, the switch will, by default, configure ATM ports as multicast router ports. This will ensure multicast traffic is sent out the ATM interface. Be aware that this will cause all multicast traffic to be forwarded out the ATM port and reduce the effectiveness of CGMP to limit multicast traffic.

   If it is felt that this situation will not occur on any of the VLANs that the ATM port carries, the ATM port may be deleted as a multicast router port.

Note Deleting the ATM port as a multicast port will delete it as a multicast port on *all* VLANs.

3. IGMP packets that use IEEE 802.3 packet encapsulation are not supported in this release.
4. The IP multicast groups that map to the MAC addresses 01:00:5E:00:00:00 to 01:00:5E:00:00:FF will not be processed by CGMP. These address are processed as regular multicasts would be processed (forwarded to all ports in the broadcast domain).

CGMP Configuration Notes

1. CGMP filtering requires a network connection from the Catalyst 3000 series switch to a router capable of running CGMP (does not have to be a direct connection).
2. By default:

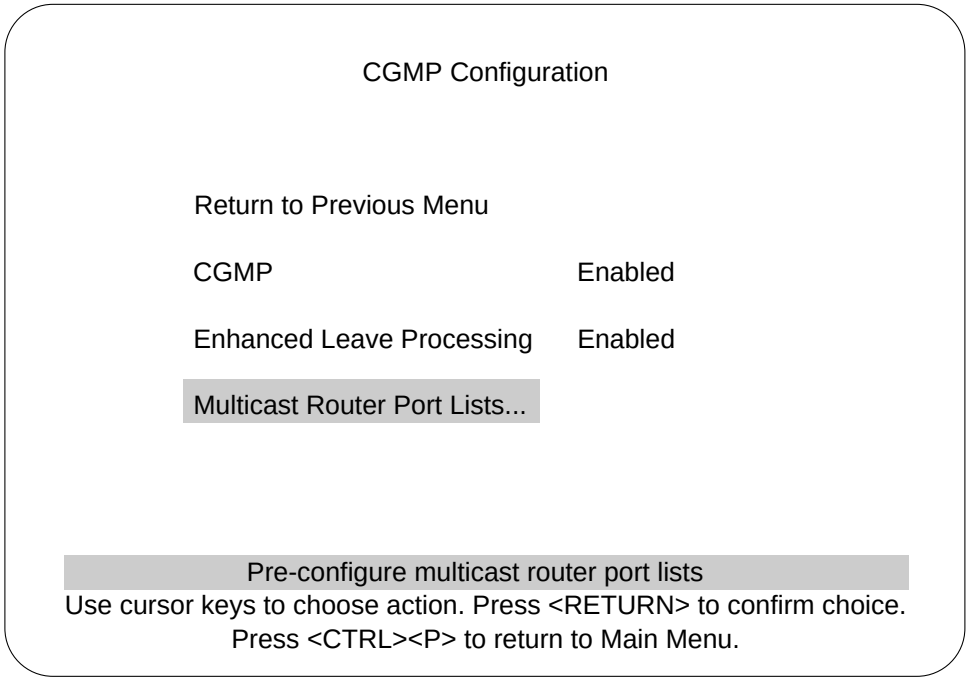
- CGMP is enabled
- IGMP/Enhanced Leave Processing is disabled

3. When CGMP is enabled, it automatically identifies the ports to which the CGMP-capable router is attached.
4. The Multicast Router Port screen allows you to statically configure multicast router ports.

Configuring CGMP Using the Console Menus

Step 1 Access the Configuration Menu and select the CGMP Configuration menu. The CGMP Configuration menu is shown in Figure 4.

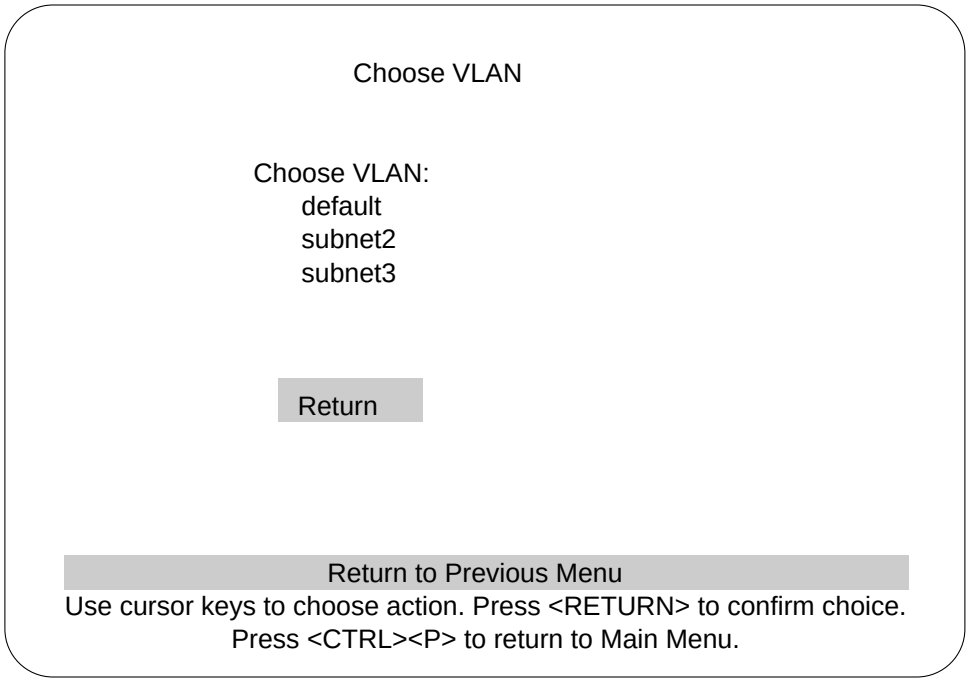
Figure 4 CGMP Configuration Menu



Step 2 Use the CGMP Configuration menu to enable or disable CGMP or Enhanced Leave Processing and to select ports to configure.

Step 3 Select “Multicast Router Ports...” to configure specific CGMP ports (use the Choose VLAN screen, as shown in Figure 5, to select the VLAN for configuring).The Multicast Router Ports (Figure 6) screen is displayed.

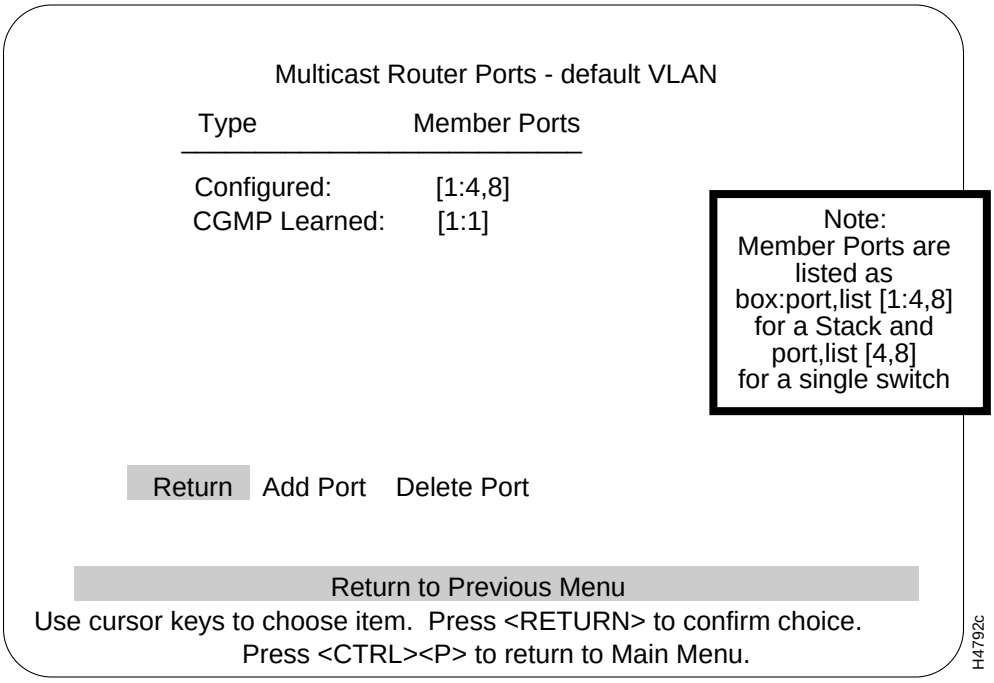
Figure 5 Choose VLAN Screen



Step 4 Use the Multicast Router Ports screen (Figure 6) to add or delete a port.

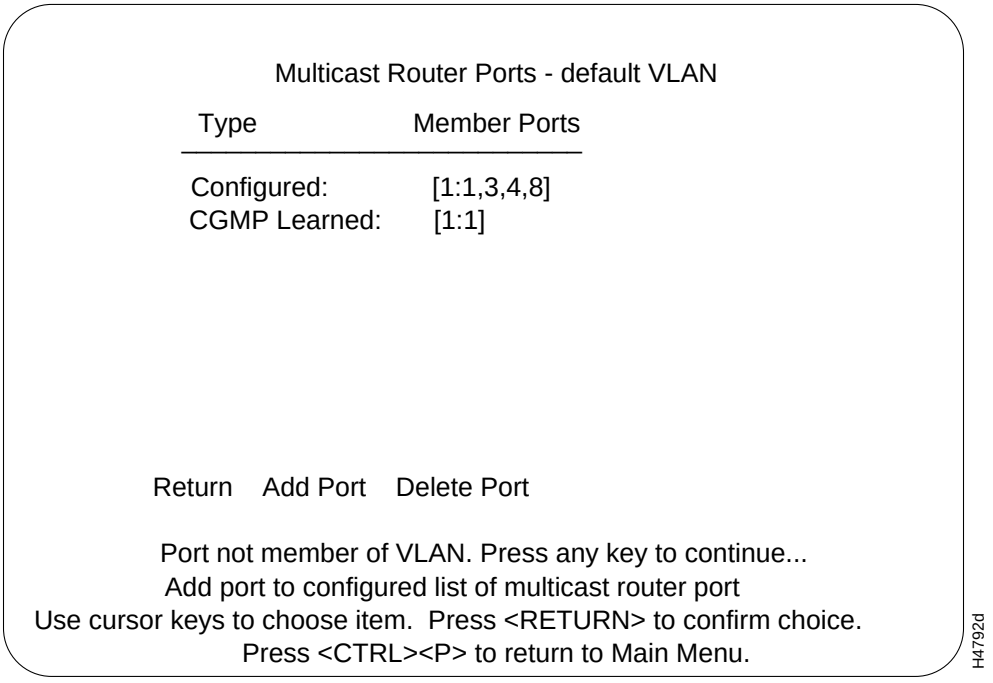
Note A message is displayed on the Multicast Router Ports screen if you select a port that is a trunk. The message is a warning that the trunk will be added as a router port on all VLANs to which it is configured. You are asked to confirm the addition or deletion.

Figure 6 Multicast Router Ports Screen



Note If you try to add a port that is not in the VLAN, the error note (as shown in Figure 7) is displayed on the Multicast Router Ports screen.

Figure 7 Multicast Router Ports Error Screen



CGMP Statistics

To view the status of CGMP, use the following CGMP statistic screens.The CGMP Statistic screen (Figure 8) is accessed from the main Statistics menu. From the CGMP Statistic menu, select the CGMP Protocol Statistics screen (Figure 9) to display the current status of CGMP information (after the Choose VLAN menu).

Figure 8 CGMP Statistics Menu

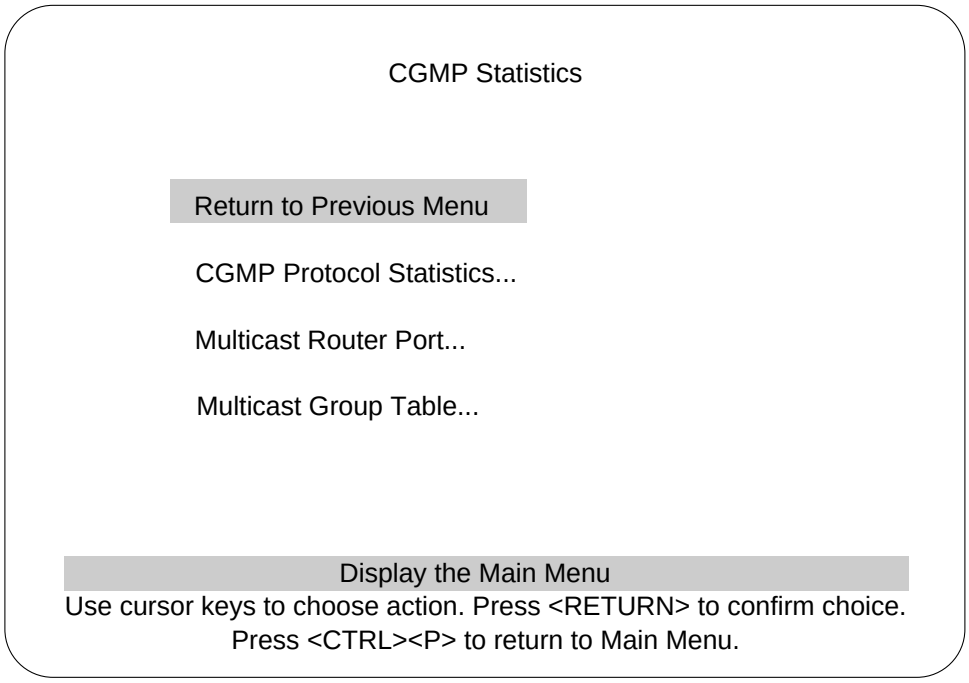
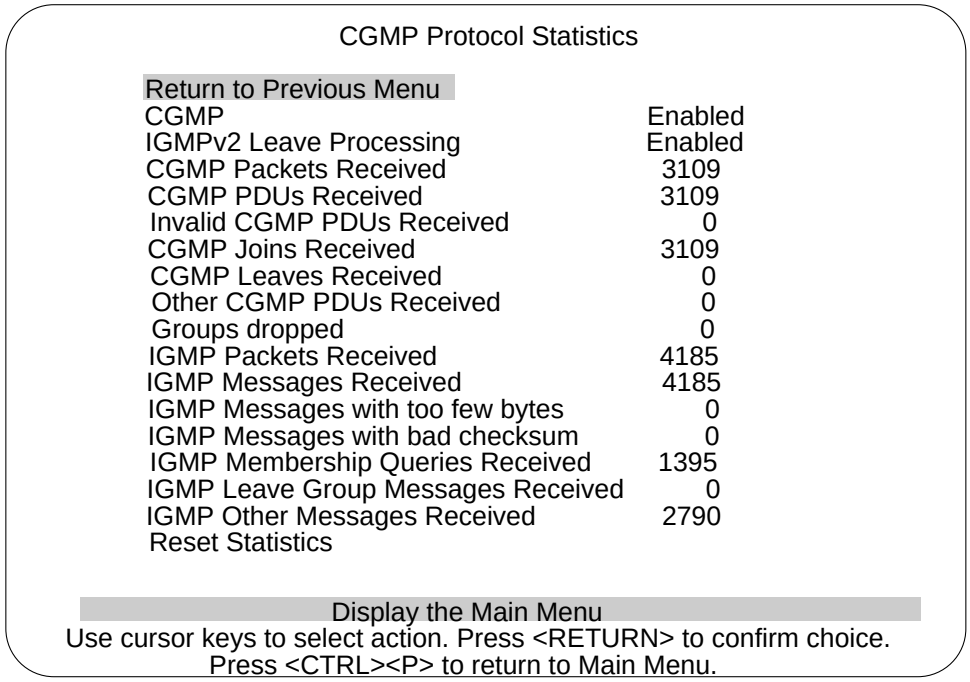
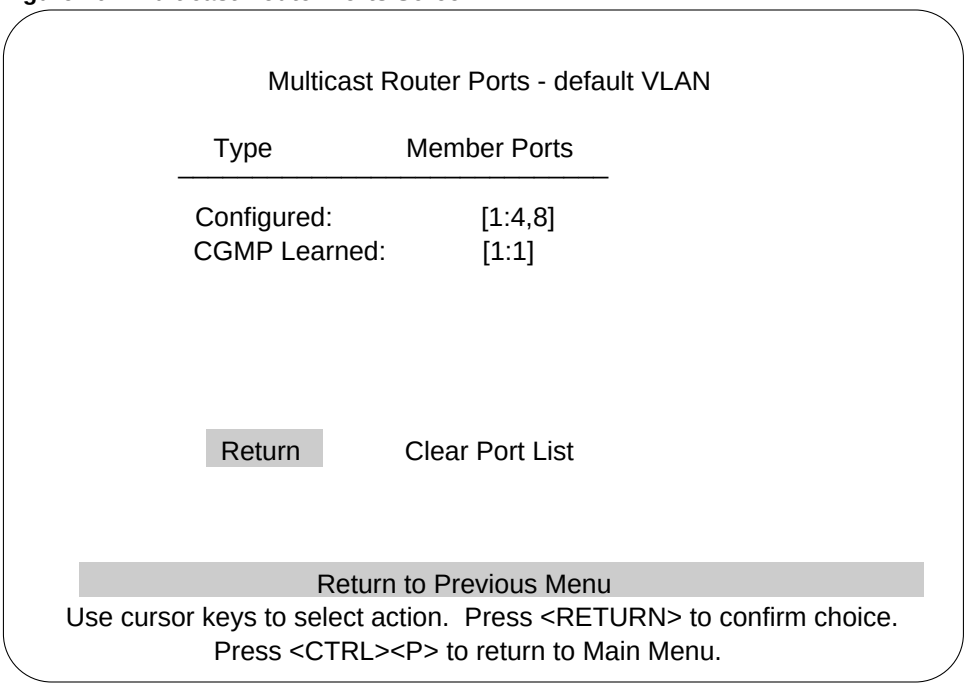


Figure 9 CGMP Protocol Statistics Screen



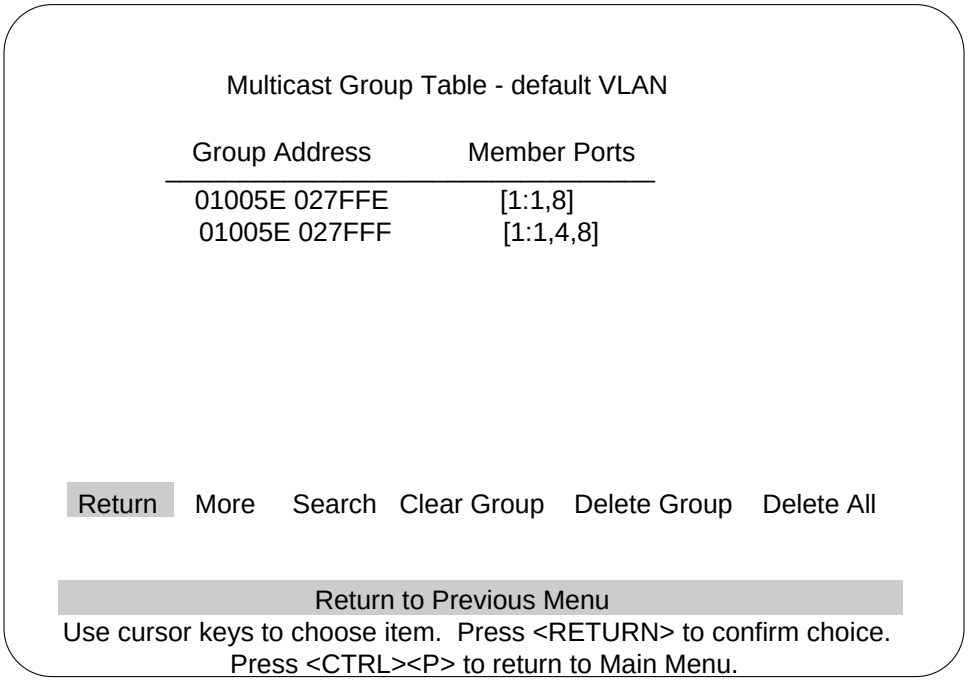
Use the following screen, Multicast Router Port Table (Figure 10), to view multicast router port lists.

Figure 10 Multicast Router Ports Screen



Use the Multicast Group Table (Figure 11) to view a multicast group table for a particular switch.

Figure 11 Multicast Group Table Screen



Obtaining Service and Support

For service and support for a product purchased from a reseller, contact the reseller. Resellers offer a wide variety of Cisco service and support programs, which are described in the section "Service and Support" in the information packet that shipped with your product.

Note If you purchased your product from a reseller, you can access Cisco Connection Online (CCO) as a guest. CCO is Cisco Systems' primary, real-time support channel. Your reseller offers programs that include direct access to CCO's services.

For service and support for a product purchased directly from Cisco, use CCO.

Cisco Connection Online

CCO is Cisco Systems' primary, real-time support channel. SMARTnet customers and partners can self-register on CCO to obtain additional information and services.

Note If you purchased your product from a reseller, you can access CCO as a guest. Your reseller offers programs that include direct access to CCO's services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CCO in the following ways:

- WWW: http://www.cisco.com
- WWW: http://www-europe.cisco.com
- WWW: http://www-china.cisco.com
- Telnet: cco.cisco.com
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact cco-help@cisco.com. For additional information, contact cco-team@cisco.com.

Note If you need technical assistance with a Cisco product that is under warranty or covered by a Cisco maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or tac@cisco.com.

Please use CCO to obtain general information about Cisco Systems, Cisco products, or upgrades. If CCO is not accessible, contact 800 553-6387, 408 526-7208, or cs-rep@cisco.com.

This document is to be used in conjunction with the Catalyst 3000 series *Configuration and Installation Guide* publication.

9704R