Part No. 314725-B Rev 00
May 2003

4655 Great America Parkway
Santa Clara, CA 95054

Configuring Layer 2 Operations: VLANs, Spanning Tree, and MultiLink Trunking

Passport 8000 Series Software Release 3.5

314725-B REV 00

NORTEL NETWORKS™

Copyright © 2003 Nortel Networks

Trademarks

Nortel Networks, the Nortel Networks logo, the Globemark, Unified Networks, and PASSPORT are trademarks of Nortel Networks.

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation.

The asterisk after a name denotes a trademarked item.

Restricted rights legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Nortel Networks Inc. software license agreement

This Software License Agreement ("License Agreement") is between you, the end-user ("Customer") and Nortel Networks Corporation and its subsidiaries and affiliates ("Nortel Networks"). PLEASE READ THE FOLLOWING CAREFULLY. YOU MUST ACCEPT THESE LICENSE TERMS IN ORDER TO DOWNLOAD AND/OR USE THE SOFTWARE. USE OF THE SOFTWARE CONSTITUTES YOUR ACCEPTANCE OF THIS LICENSE AGREEMENT. If you do not accept these terms and conditions, return the Software, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

"Software" is owned or licensed by Nortel Networks, its parent or one of its subsidiaries or affiliates, and is copyrighted and licensed, not sold. Software consists of machine-readable instructions, its components, data, audio-visual content (such as images, text, recordings or pictures) and related licensed materials including all whole or partial copies. Nortel Networks grants you a license to use the Software only in the country where you acquired the Software. You obtain no rights other than those granted to you under this License Agreement. You are responsible for the selection of the Software and for the installation of, use of, and results obtained from the Software.

1. Licensed Use of Software. Nortel Networks grants Customer a nonexclusive license to use a copy of the Software on only one machine at any one time or to the extent of the activation or authorized usage level, whichever is applicable. To the extent Software is furnished for use with designated hardware or Customer furnished equipment ("CFE"), Customer is granted a nonexclusive license to use Software only on such hardware or CFE, as applicable. Software contains trade secrets and Customer agrees to treat Software as confidential information using the same care and discretion Customer uses with its own similar information that it does not wish to disclose, publish or disseminate. Customer will ensure that anyone who uses the Software does so only in compliance with the terms of this Agreement. Customer shall not a) use, copy, modify, transfer or distribute the Software except as expressly authorized; b) reverse assemble, reverse compile, reverse engineer or otherwise translate the Software; c) create derivative works or modifications unless expressly authorized; or d) sublicense, rent or lease the Software. Licensors of intellectual property to Nortel Networks are beneficiaries of this provision. Upon termination or breach of the license by Customer or in the event designated hardware or CFE is no longer in use, Customer will promptly return the Software to Nortel Networks or certify its destruction. Nortel Networks may audit by remote polling or other reasonable means to determine Customer's Software activation or usage levels. If suppliers of third party software included in Software require Nortel Networks to include additional or different terms, Customer agrees to abide by such terms provided by Nortel Networks with respect to such third party software.

2. Warranty. Except as may be otherwise expressly agreed to in writing between Nortel Networks and Customer, Software is provided "AS IS" without any warranties (conditions) of any kind. NORTEL NETWORKS DISCLAIMS ALL WARRANTIES (CONDITIONS) FOR THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF NON-INFRINGEMENT. Nortel Networks is not obligated to provide support of any kind for the Software. Some jurisdictions do not allow exclusion of implied warranties, and, in such event, the above exclusions may not apply.

3. Limitation of Remedies. IN NO EVENT SHALL NORTEL NETWORKS OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: a) DAMAGES BASED ON ANY THIRD PARTY CLAIM; b) LOSS OF, OR DAMAGE TO, CUSTOMER'S RECORDS, FILES OR DATA; OR c) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN ADVISED OF THEIR POSSIBILITY. The forgoing limitations of remedies also apply to any developer and/or supplier of the Software. Such developer and/or supplier is an intended beneficiary of this Section. Some jurisdictions do not allow these limitations or exclusions and, in such event, they may not apply.

4. General

a. If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States

Government, the respective rights to the software and software documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-DoD entities) and 48 C.F.R. 227.7202 (for DoD entities).

b. Customer may terminate the license at any time. Nortel Networks may terminate the license if Customer fails to comply with the terms and conditions of this license. In either event, upon termination, Customer must either return the Software to Nortel Networks or certify its destruction.

c. Customer is responsible for payment of any taxes, including personal property taxes, resulting from Customer’s use of the Software. Customer agrees to comply with all applicable laws including all applicable export and import laws and regulations.

d. Neither party may bring an action, regardless of form, more than two years after the cause of the action arose.

e. The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel Networks.

f. This License Agreement is governed by the laws of the country in which Customer acquires the Software. If the Software is acquired in the United States, then this License Agreement is governed by the laws of the state of New York.

Contents

Chapter 6

Chapter 7

Tables

Figures

Preface

This guide describes the 8000 Series switch Layer 2 operations, and provides information about using both Device Manager and the command line interface (CLI) to configure them.

Before you begin

This guide is intended for network administrators with the following background:

- Basic knowledge of networks, Ethernet bridging, and IP routing
- Familiarity with networking concepts and terminology
- Experience with windowing systems or graphical user interfaces (GUIs)
- Basic knowledge of network topologies

Before using this guide, you must complete the following procedures. For a new switch:

- Install the switch (see the installation guide that came with your switch).
- Connect the switch to the network (see the publication, *Getting Started with the Management Software* for more information).

Make sure that you are running the latest version of Nortel Networks* 8000 Series and Device Manager software. For information about upgrading the 8000 Series and Device Manager, see the upgrading guide for your version of the 8000 Series.

Text conventions

This guide uses the following text conventions:

angle brackets (< >)

Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command.

Example: If the command syntax is `ping` <*`ip_address`*>, you enter `ping 192.32.10.12`

italic text

Indicates new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore.

Example: If the command syntax is `show at` <*`valid_route`*>, *`valid_route`* is one variable and you substitute one value for it.

`plain Courier text`

Indicates command syntax and system output, for example, prompts and system messages.

Example: `Set Trap Monitor Filters`

Hard-copy technical manuals

You can print selected technical manuals and release notes free, directly from the Internet. Go to the www.nortelnetworks.com/documentation URL. Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Use Adobe* Acrobat Reader* to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to Adobe Systems at the www.adobe.com URL to download a free copy of the Adobe Acrobat Reader.

Note: The list of related publications for this manual can be found in the release notes that came with your software.

How to get help

If you purchased a service contract for your Nortel Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Nortel Networks service program, contact one of the following Nortel Networks Technical Solutions Centers:

Technical Solutions Center	**Telephone**
Europe, Middle East, and Africa	(33) (4) 92-966-968
North America	(800) 4NORTEL or (800) 466-7835
Asia Pacific	(61) (2) 9927-8800
China	(800) 810-5000

Additional information about the Nortel Networks Technical Solutions Centers is available from the www.nortelnetworks.com/help/contact/global URL.

An Express Routing Code (ERC) is available for many Nortel Networks products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to the http://www.nortelnetworks.com/help/contact/erc/index.html URL.

Chapter 1
Layer 2 operational concepts

This section describes layer 2 features and includes the following topics:

About VLANs

A virtual LAN (VLAN) lets you divide your LAN into smaller groups without interfering with the physical network. VLAN practical applications include:

- You can create VLANs, or workgroups, for common interest groups.
- You can create VLANs, or workgroups, for specific types of network traffic.
- You can add, move, or delete members from these workgroups without making any physical changes to the network.

By dividing the network into separate VLANs, you can create separate broadcast domains. This arrangement conserves bandwidth, especially in networks supporting broadcast and multicast applications that flood the network with traffic. A VLAN workgroup may include members from a number of dispersed physical segments on the network, improving traffic flow between them.

The 8000 Series switch performs the layer 2 switching functions necessary to transmit information within VLANs as well as the layer 3 routing functions necessary for VLANs to communicate with one another. A VLAN can be defined for a single switch or it can span multiple switches. A port can be a member of multiple VLANs.

This section includes the following topics:

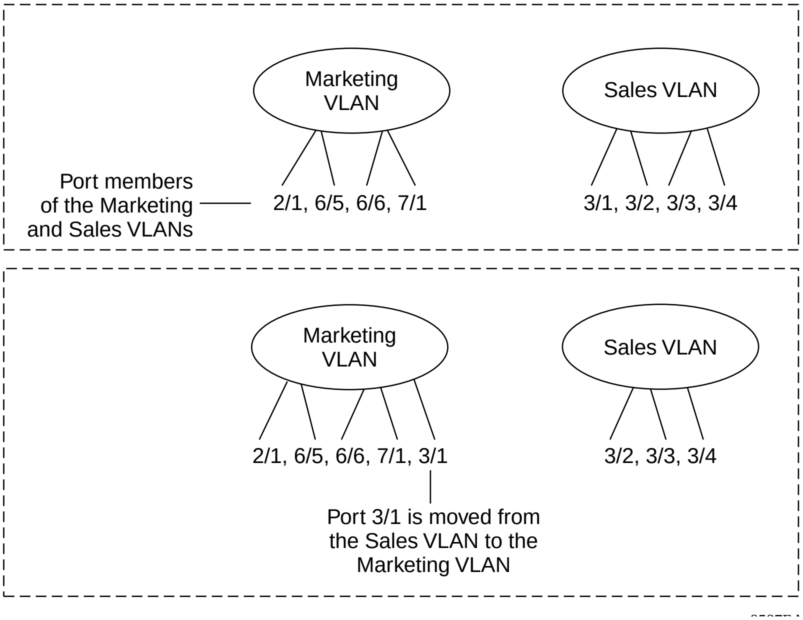
About port-based VLANs

A port-based VLAN is a VLAN in which the ports are explicitly configured to be in the VLAN. When creating a port-based VLAN on a switch, you assign a VLAN identification number (VLAN ID) and specify which ports belong to the VLAN. The VLAN ID is used to coordinate VLANs across multiple switches.

Note: Port-based VLANs created on a Passport 8100 have the MAC address 00:00:00:00:00:00.

The example in Figure 1 shows two port-based VLANs: one for the marketing department and one for the sales department. Ports are assigned to each port-based VLAN. A change in the sales area can move the sales representative at port 3/1 (the first port in the I/O module in chassis slot 3) to the marketing department without moving cables. With a port-based VLAN, you only need to indicate in Device Manager or the CLI that port 3/1 in the sales VLAN now is a member of the marketing VLAN.

Figure 1 Port-based VLAN



About policy-based VLANs

A policy-based VLAN is a VLAN in which ports are dynamically added to the VLAN based on the traffic coming into the port.

In a policy-based VLAN on a Passport 8000 Series routing or edge switch, ports are designated as always a member or never a member of the VLAN. In addition, you can designate a port as a potential member of the VLAN on the 8000 Series switch. When a port is designated as a potential member of the VLAN, and the incoming traffic matches the policy, the port is dynamically added to the VLAN. Potential member ports that joined the VLAN are removed (“timed out”) from the VLAN when that VLAN’s timeout (“aging time”) period expires.

A port’s membership in a VLAN is determined by the traffic coming into the port; therefore, Nortel Networks recommends that at least some ports be designated as always a member of the VLAN. One situation in which a port should be designated always a member of a VLAN is if a server or router connects to the port. If a server is connected to a port that is only a potential member and the server sends out very little traffic, a client will fail to reach the server if the server port has timed out of the VLAN.

Note: A port can belong to one port-based VLAN and many policy-based VLANs.

Table 1 lists supported policy-based VLANs by module type:

Table 1 Policy-based VLAN types

VLAN type	8600	8100
Protocol-based	supported	supported
User-defined protocol-based	supported	unsupported
MAC address-based	supported	unsupported
IP subnet-based	supported	unsupported
Stacked VLANs	supported	unsupported

About protocol-based VLANs

Protocol-based VLANs are an effective way to segment your network into broadcast domains according to the network protocols in use. Traffic generated by any network protocol—IPX, Appletalk, PPPoE—can be automatically confined to its own VLAN.

All ports within a protocol-based VLAN must be in the same port-based VLAN. However, the same port within a port-based VLAN can belong to multiple protocol-based VLANs. Port tagging is not required for a port to be a member of multiple protocol-based VLANs.

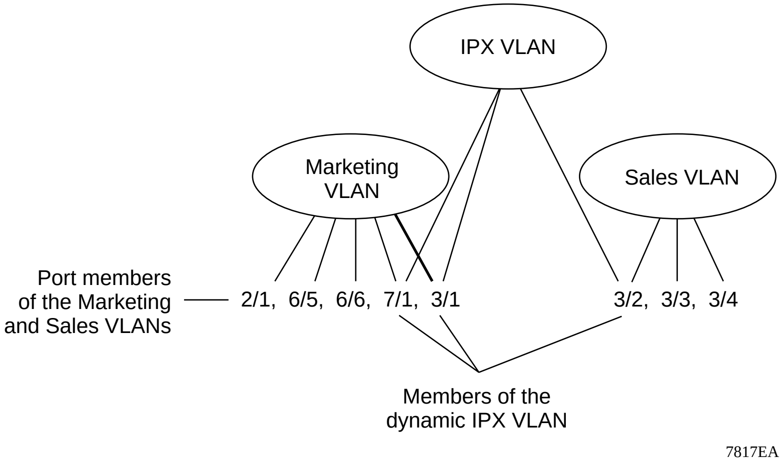
The 8000 Series switch supports the following protocol-based VLANs:

- IP version 4 (ip)
- Novell IPX on Ethernet 802.3 frames (ipx802dot3)
- Novell IPX on IEEE 802.2 frames (ipx802dot2)
- Novell IPX on Ethernet SNAP frames (ipxSnap)
- Novell IPX on Ethernet Type 2 frames (ipxEthernet2)
- AppleTalk on Ethernet Type 2 and Ethernet SNAP frames (AppleTalk)
- DEC LAT Protocol (decLat)
- Other DEC protocols (decOther)
- IBM SNA on IEEE 802.2 frames (sna802dot2)
- IBM SNA on Ethernet Type 2 frames (snaEthernet2)
- NetBIOS Protocol (netBIOS)
- Xerox XNS (xns)
- Banyan VINES (vines)
- IP version 6 (ipv6)
- Reverse Address Resolution Protocol (RARP)
- Point-to-point protocol over Ethernet (PPPoE)
- User-defined protocols

Example: IPX protocol-based VLAN

You can create a VLAN for the IPX protocol and place ports carrying substantial IPX traffic into this new VLAN. In Figure 2, the network manager has placed ports 7/1, 3/1, and 3/2 in an IPX VLAN. These ports still belong to their respective marketing and sales VLANs, but they are also new members of the IPX VLAN. This arrangement localizes traffic and ensures that only three ports are flooded with IPX broadcast packets.

Figure 2 Dynamic protocol-based VLAN


IPX VLAN
Marketing VLAN
Sales VLAN
Port members of the Marketing and Sales VLANs
2/1, 6/5, 6/6, 7/1, 3/1
3/2, 3/3, 3/4
Members of the dynamic IPX VLAN
7817EA

Example: PPPoE protocol-based VLAN

Note: This information applies to 8600 modules only.

Point-to-point protocol over Ethernet (PPPoE) lets you connect multiple computers on an Ethernet to a remote site through a device such as a modem so that multiple users can share a common line connection to the Internet.

PPPoE combines the Point-to-Point protocol, commonly used in dial-up connections, with the Ethernet protocol, which supports multiple users in a local area network by encapsulating the PPPoE protocol within an Ethernet frame.

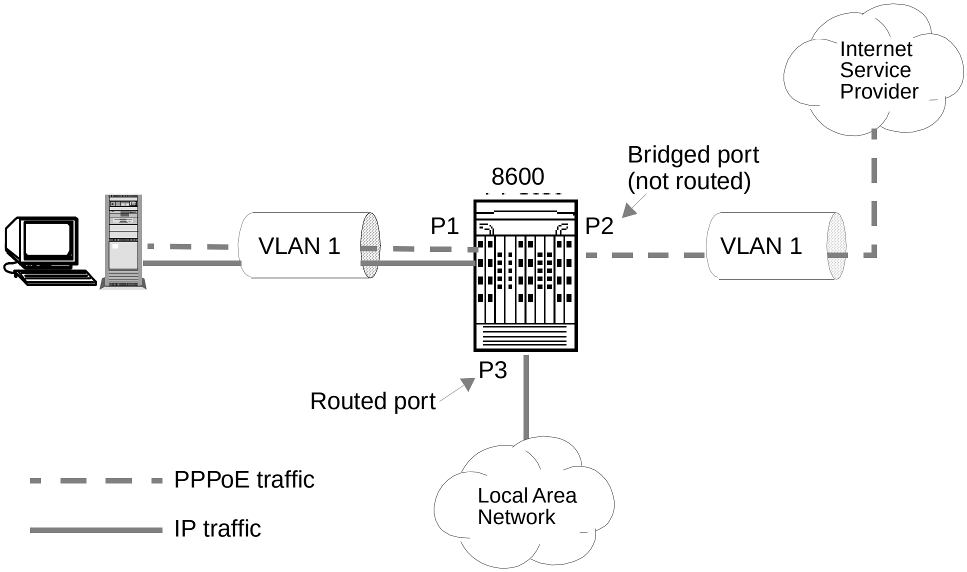
PPPoE occurs in two stages—a discovery stage and a PPP session stage. TheEther_Type field in the Ethernet frame identifies the stage:

- The discovery stage uses 0x8863 Ether_Type
- The session stage uses 0x8864 Ether_Type

In Figure 3, VLAN 1 is a protocol-based VLAN that transports PPPoE traffic to the Internet Service Provider (ISP) network. The traffic to the ISP is bridged.

IP traffic can also be routed to the local area network (LAN) using, for example, port-based VLANs, IP protocol-based VLANs, or IP subnet-based VLANs.

Figure 3 PPPoE and IP configuration



About user-defined protocol-based VLANs

You can create user-defined protocol-based VLANs in support of networks with non-standard protocols. For user-defined protocol-based VLANs, you can specify the Protocol Identifier (PID) for the VLAN. Frames that match the specified PID for the following are assigned to that user-defined VLAN:

- The ethertype for Ethernet type 2 frames
- The PID in Ethernet SNAP frames
- The DSAP or SSAP value in Ethernet 802.2 frames

Table 2 lists reserved, predefined policy-based PIDs which cannot be used as user-defined PIDs.

Table 2 PIDs which cannot be used for user-defined protocol-based VLANs

PID (hex)	Description
04xx, xx04	sna802dot2
F0xx, xxF0	netBIOS
0000-05DC	Overlaps with 802.3 frame length
0600, 0807	xns
0BAD	VINES
4242	IEEE 802.1D BPDUs
6000-6003, 6005-6009	decOther
6004	decLat
0800, 0806	ip
8035	RARP
809B, 80F3	AppleTalk
8100	Reserved by IEEE 802.1Q for tagged frames
8137, 8138	ipxEthernet2 and ipxSnap
80D5	snaEthernet2
86DD	ipv6
8808	IEEE 802.3x pause frames
9000	Used by diagnostic loopback frames
8863, 8864	PPPoE

About MAC address-based VLANs

As with all policy-based VLANs, using source MAC address VLANs allows 8600 modules to associate frames with a VLAN based on the frame content. With source MAC-based VLANs, a frame is associated with a VLAN if the source MAC address is one of the MAC addresses explicitly associated with the VLAN. To create a source MAC-based VLAN, you add the MAC address to a list of MAC addresses that constitutes the VLAN. However, because it is necessary to explicitly associate MAC addresses with a source MAC-based VLAN, the administrative overhead can be quite high.

Use source MAC-based VLANs when you want to enforce a MAC level security scheme to differentiate groups of users. For example, in a university environment, the students will be part of a student VLAN with certain services and access privileges, and the faculty will be part of a source MAC-based VLAN with faculty services and access privileges. Therefore, a student and a faculty member could plug into the same port but have access to a different range of services. In order to provide the correct services throughout the campus, the source MAC-based VLAN would need to be defined on 8000 Series switches throughout the campus, which entails administrative overhead.

Note: When a source MAC VLAN is created, not all of the port members of the STG are automatically made potential members of the VLAN by default.

About IP subnet-based VLANs

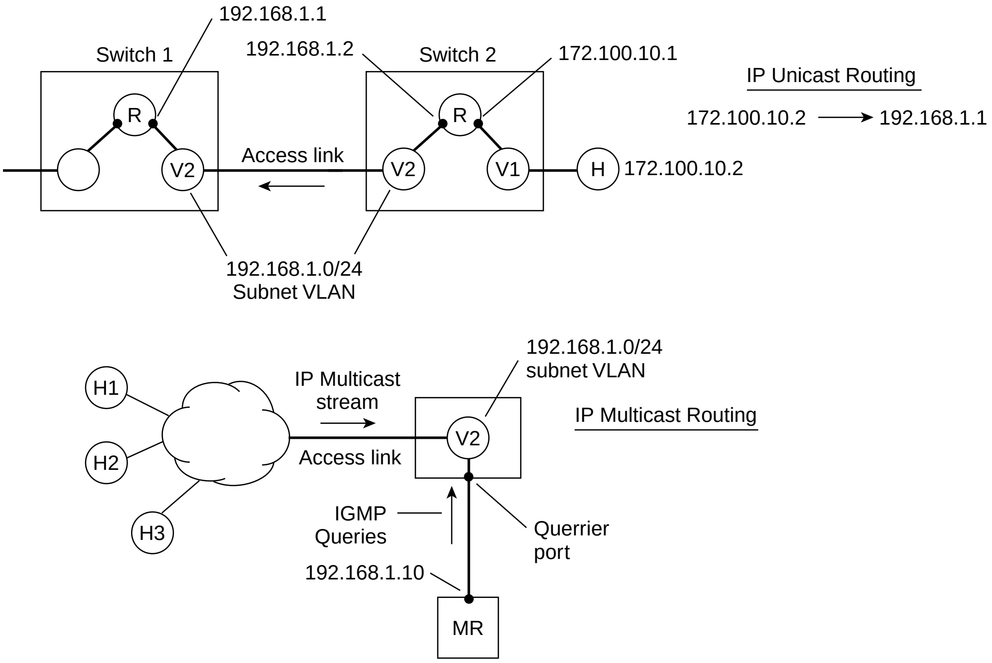
8600 modules support policy-based VLANs based on IP subnets. Access ports can be assigned to multiple subnet-based VLANs. A frame's membership in a subnet-based VLAN is based on the IP source address associated with a mask. Subnet-based VLANs are optionally routable. Using source IP subnet-based VLANs, multiple workstations on a single port can belong to different subnets, similar to multinetting.

Note: IP subnet-based VLANs cannot be used on segments that act as a transit network.

Figure 4 shows two examples of the incorrect use of IP subnet-based VLANs that result in traffic loss. In the IP unicast routing example, the host on 172.100.10.2 sends traffic to switch 2 (172.100.10.1) destined for the router in switch 1 (192.168.1.1). Switch 2 attempts to route the IP traffic, but that traffic will not arrive at the router in switch 1. Switch 1 will not assign this frame to IP subnet-based VLAN 2 because the traffic's IP source address does not match the IP subnet assigned to VLAN 2. If the access link in VLAN 2 connecting switch 1 and 2 was a tagged link instead, the traffic would be associated with the VLAN tag, not the IP address, and would be forwarded correctly to switch 1.

In the IP multicast routing example, the multicast stream is on an access link that is part of IP subnet-based VLAN 2. Because the source IP address in the multicast data packets received from the access port is not necessarily within the subnet of VLAN 2, the multicast stream will not reach the multicast router (MR).

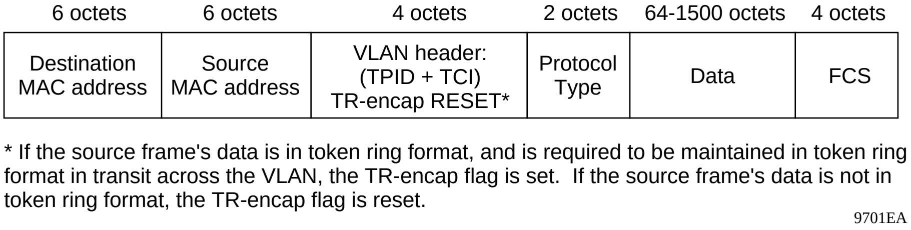
Figure 4 Incorrect use of an IP subnet-based VLAN



About VLAN tagging and port types

8000 Series switches support the IEEE 802.1Q specification for “tagging” frames and coordinating VLANs across multiple switches. Figure 5 shows how an additional 4-octet (“tag”) header is inserted in a frame after the source address and before the frame type. The tag contains the VLAN ID associated with the frame.

Figure 5 VLAN tag insertion



6 octets	6 octets	4 octets	2 octets	64-1500 octets	4 octets
Destination MAC address	Source MAC address	VLAN header: (TPID + TCI) TR-encap RESET*	Protocol Type	Data	FCS

* If the source frame's data is in token ring format, and is required to be maintained in token ring format in transit across the VLAN, the TR-encap flag is set. If the source frame's data is not in token ring format, the TR-encap flag is reset.

9701EA

About 802.1Q tagged ports

Tagging a frame adds four octets to a frame, making it bigger than the traditional maximum frame size. These frames are sometimes referred to as “baby giant” frames. If a device does not support IEEE 802.1Q tagging, it may have problems interpreting tagged frames and receiving baby giant frames.

In the 8000 Series switch, whether or not tagged frames are sent or received depends on what you configure at the port level. Tagging is set as true or false for the port and is applied to all VLANs on that port.

Note: When you enable tagging on an untagged port, the port’s previous configuration of VLANs, STGs, and MLTs is lost. In addition, the port resets and runs Spanning Tree Protocol, thus breaking connectivity while the protocol goes through the normal blocking and learning states before the forwarding state.

An 8000 Series switch port with tagging enabled sends frames explicitly tagged with a VLAN ID. Tagged ports are typically used to multiplex traffic belonging to multiple VLANs to other IEEE-802.1Q-compliant devices.

If tagging is disabled on an 8000 Series switch port, it does not send tagged frames. A nontagged port connects 8000 Series switches to devices that do not support IEEE 802.1Q tagging. If a tagged frame is forwarded out a port with tagging set to false, the Passport 8000 Series switch removes the tag from the frame before sending it out the port.

Treatment of tagged and untagged frames

An 8000 Series switch associates a frame with a VLAN based on the data content of the frame and the configuration of the destination port. Whether the frame is tagged or untagged dictates how that frame is treated.

If a tagged frame is received on a tagged port, with a VLAN ID specified in the tag, the 8000 Series switch directs it to that VLAN, if it is present. For tagged frames received on an untagged port, you can configure that port to either discard the frame or accept it. If you choose not to discard tagged frames, the 8000 Series switch sends the frame to the VLAN identified in the frame’s tag.

For untagged frames, VLAN membership is implied from the content of the frame itself. For untagged frames received on a tagged port, you can configure the port to either discard or accept the frame. If you configure a tagged port to accept untagged frames, the port must be assigned to a port-based VLAN in spanning tree group 1 (STG1).

How the frame is forwarded is based on the VLAN on which the frame is received and on the forwarding options available for that VLAN. Passport 8000 Series switches try to associate untagged frames with a VLAN in the following order:

- Does the frame belong to a source MAC-based VLAN? (8600 modules only)
- Does the frame belong to a source IP subnet-based VLAN? (8600 modules only)
- Does the frame belong to a protocol-based VLAN?
- What is the port-based VLAN of the receiving port?

If the frame meets none of the criteria listed above, it is discarded.

About VLAN router interfaces

Virtual router interfaces correspond to routing on a virtual port that is associated with a VLAN. This type of routing is the routing of IP traffic to and from a VLAN. Because a given port can belong to multiple VLANs (some of which are configured for routing on the switch and some of which are not), there is no longer a one-to-one correspondence between the physical port and the router interface. For VLAN routing, the router interface for the VLAN is called a virtual router interface because the IP address is assigned to an interface on the routing entity in the switch. This initial interface has a one-to-one correspondence with a VLAN on any given switch.

IP routing and VLANs

8600 modules support IP routing on the following types of VLANs only:

- Port-based VLANs
- Source IP subnet-based VLANs
- IP protocol-based VLANs
- Source MAC-based VLANs

IP routing is not supported on VLANs based on other protocols, including IP version 6 and user-defined protocol-based VLANs.

IPX routing and VLANs

8600 modules support IPX routing on IPX-protocol VLANs and on port-based VLANs.

The IPX network number is associated with a VLAN, and the VLAN can consist of one or more ports with one of the four supported frame formats: Ethernet II, 802.3-SNAP, 802.2-RAW, and 802.3-LLC.

You can configure up to four IPX protocol-based VLANs on one port as long as each of these VLANs uses a different IPX encapsulation. With port-based VLANs, you can associate the same VID with any or all of the four IPX encapsulation formats.

You can configure IPX protocol-based VLANs and port-based VLANs on the same port, but traffic will route to the protocol-based VLAN and not to the port-based VLAN, given that protocol-based VLANs have precedence over port-based VLANs.

VLAN implementation on the 8000 Series switch

This section describes how to implement VLANs on 8000 Series switches and describes Passport 8000 Series default VLANs, unassigned VLANs, and brouter ports. It also summarizes the defaults and rules regarding VLAN creation on 8000 Series switches.

This section includes the following topics:

- "About the default VLAN," next
- "About the unassigned VLAN" on page 37
- "About brouter ports" on page 37 (8600 modules only)
- "VLAN rules" on page 38

About the default VLAN

8000 Series switches are factory configured with all ports in a port-based VLAN called the default VLAN. With all ports in the default VLAN, the switch behaves like a layer 2 switch. The VLAN ID of this default VLAN is always 1, and it is always a port-based VLAN. The default VLAN cannot be deleted.

About the unassigned VLAN

Internally, a 8000 Series switch supports a placeholder for ports that is called an unassigned port-based VLAN. This unassigned concept is used for ports that are removed from all port-based VLANs. Ports can belong to policy-based VLANs as well as to the unassigned VLAN. If a frame does not meet any policy criteria and there is no underlying port-based VLAN, the port belongs to the unassigned VLAN and the frame is dropped. Only ports in the unassigned VLAN have no spanning tree group association, so these ports do not participate in Spanning Tree Protocol negotiation; that is, no BPDUs are sent out of ports in the unassigned VLAN.

Because it is an internal construct, the unassigned VLAN cannot be deleted. If a user-defined spanning tree group is deleted, the ports are moved to the unassigned VLAN and can later be assigned to another spanning tree group. Moving the ports to the unassigned VLAN avoids creating unwanted loops and duplicate connections. If routing is disabled in these ports, the port is completely isolated and no layer 2 or layer 3 functionality is provided.

The concept of the unassigned VLAN is useful for security concerns or when using a port for monitoring a mirrored port.

About brouter ports

A brouter port is actually a one-port VLAN. The difference between a brouter port and a standard IP protocol-based VLAN configured to do routing is that the routing interface of the brouter port is not subject to the spanning tree state of the port.

VLAN rules

Table 3 lists 8000 Series switch VLAN rules.

Table 3 VLAN rules

The following rules apply to all 8000 Series switch VLANs:
• In addition to the default VLAN, the 8100 Series switch can support up to 2000 VLANs; and the 8600 Series switch can support up to 1980 VLANs. VLAN IDs range from 1 to 4094.
• If you enable tagging on a port that is in a VLAN, the spanning tree group configuration for that port is lost. To preserve VLAN assignment of ports, enable tagging on the ports before you assign the ports to VLANs.
• A tagged port can belong to multiple VLANs and multiple spanning tree groups. When a tagged port belongs to multiple spanning tree groups, the BPDUs are tagged for all spanning tree groups except for spanning tree group 1. Under the default configuration, the default spanning tree group is number 1.
• An untagged port can belong to one and only one port-based VLAN. A port in a port-based VLAN can belong to other policy-based VLANs.
• An untagged port can belong to one and only one policy-based VLAN for a given protocol. For example, a port can belong to only one policy-based VLAN where the policy is IPX802dot2 protocol.
In addition to the rules that apply to all 8000 Series switch VLANs, the following rules apply to 8600 modules only:
• For every VLAN with MultiLink Trunking that you create, you reduce by eight the number of available VLANs.
• A VLAN cannot span multiple spanning tree groups; that is, the ports in the VLAN must all be within one spanning tree group. Spanning tree group IDs can range in value from 1 to 25.
• A frame’s VLAN membership is determined by the following order of precedence: VLAN ID, then source MAC-based VLAN, then IP subnet-based VLAN, then protocol-based VLAN, then port-based VLAN.
• The IP subnet-based VLAN should not be assigned to a transit network, a network routing to a bridged subnet.
In addition to the rules that apply to all 8000 Series switch VLANs, this rule applies to 8100 modules only:
• A frame’s membership in a VLAN is determined in the following order of precedence: 1) VLAN ID 2) protocol-based VLAN 3) port-based VLAN

VLAN features supported on the 8100 and 8600 modules

Support for VLANs and related features is different on different module types of the 8000 Series switch. Table 4 summarizes the features supported on 8600 modules and 8100 modules.

Note: Table 4 is subject to change. Please refer to the release notes that came with your switch to obtain the latest scalability information.

Table 4 VLAN, STG, and MLT support in the 8000 Series switch

Feature	**8100 module**	**8600 module**
Number of VLANs	2000 VLANs	1980 VLANs
Port-based VLANs	Supported	Supported
Policy-based VLANs • Protocol-based • Source MAC-based • Source IP subnet-based	 Supported Not supported Not supported	 Supported Supported Supported
IEEE 802.1Q tagging	Supported	Supported
IP routing and VLANs	Not supported	Supported
IPX routing and VLANs	Not supported	Supported
Special VLANs • Default VLAN • Unassigned VLAN • Brouter ports	 Supported Supported Not supported	 Supported Supported Supported
Stacked VLAN	Not supported	Supported
Number of spanning tree groups	1	64 (with only 25 actually supported)
Passport 8000 Series Spanning Tree FastStart	Supported	Supported
MLT	6	32
Number of links per MLT	4	8

About MultiLink trunking and VLAN scalability

In release 3.2 and earlier, the maximum number of VLANs depended on whether the VLANs resided on an MLT trunk. With Enhanced operation mode, you can now increase the maximum number of VLANs when using MLT (1980) and SMLT (989). Enhanced mode requires 8600 E or M modules.

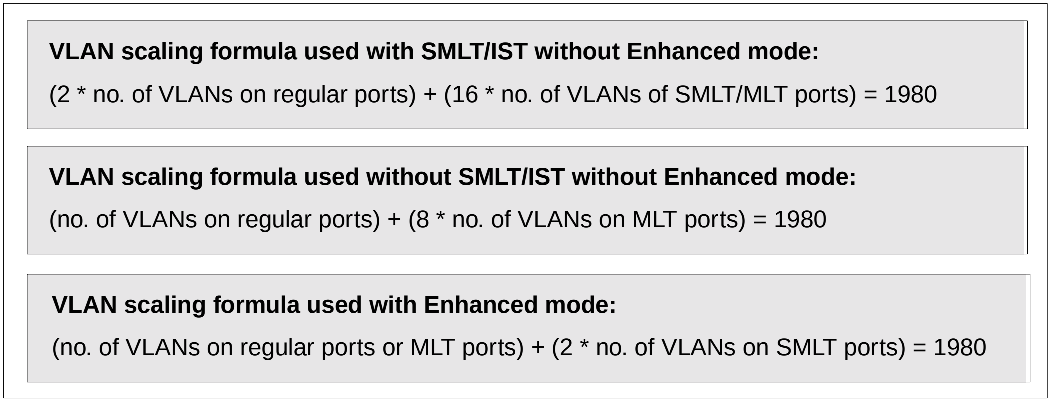
Caution: When Enhanced operation mode is enabled, only 8600 E- and M-modules are initialized (other modules are placed offline). To avoid losing modules and network connectivity, replace non-E-modules or move the network connections to an E-module before enabling Enhanced mode.

For instructions on configuring Enhanced operation mode, see:

- "Configuring Enhanced Operation mode" on page 121 (Device Manager)
- "Configuring Enhanced Operation mode" on page 204 (CLI)

Figure 6 shows the formulas used for VLAN scaling:

Figure 6 Formulas used for VLAN scaling



VLAN scaling formula used with SMLT/IST without Enhanced mode:

(2 * no. of VLANs on regular ports) + (16 * no. of VLANs of SMLT/MLT ports) = 1980

VLAN scaling formula used without SMLT/IST without Enhanced mode:

(no. of VLANs on regular ports) + (8 * no. of VLANs on MLT ports) = 1980

VLAN scaling formula used with Enhanced mode:

(no. of VLANs on regular ports or MLT ports) + (2 * no. of VLANs on SMLT ports) = 1980

Table 5 shows the maximum number of VLANs available with and without Enhanced operation mode.

Table 5 Maximum numbers of port/protocol-based VLANs

VLAN type	Maximum VLAN support with Enhanced mode enabled	Maximum VLAN support with Enhanced mode disabled
MLT	1980	240
IST/SMLT	989	120

Table 6 compares the behavior of 8600 modules with and without Enhanced operational mode:

Table 6 Comparison—Module behavior with and without Enhanced mode

Module type	Enhanced operation mode setting	Behavior
E-module or M-module	Enable (true)	The module is initialized and comes online. It can be configured with up to 1980 VLANs with MLT.
E-module or M-module	Disable (false)	The module is initialized and comes online. It can be configured with up to 240 VLANs with MLT.
Legacy module	Enable (true)	The module is not initialized and remains offline. The following error message is displayed and a trap is sent: `[12/18/01 15:17:25] Card taken off-line: Slot=1 Type= -- [12/18/01 15:17:25] ERROR Code=0x3006b Task=rcStart chCardIn: can't initialize a non ETICKET card in enhanced operation mode`
Legacy module	Disable (false)	The module is initialized and remains online. It can be configured with up to 240 VLANs with MLT.

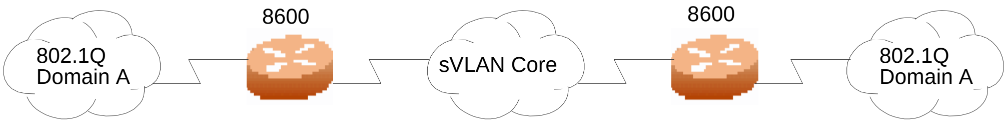
About stacked VLANs

Note: This information applies to Passport 8600 modules only.

A stacked VLAN (sVLAN) transparently tunnels packets through an sVLAN domain by adding an additional 4-byte header to each packet. The packet may already have an IEEE 802.1Q tag, but it is not required.

Figure 7 shows a basic sVLAN model using Passport 8600 switches.

Figure 7 sVLAN



Routing cannot be enabled on an sVLAN port. sVLAN user-to-network interface (UNI) ports are VLAN unaware and classify any traffic into the sVLAN which is configured on the port. sVLAN network-to-network interface (NNI) ports connect sVLAN switches together and support multiple sVLANs per port.

Note: You can enable sVLANs on all ports. If the port belongs to an MLT, however, you should perform all of the sVLAN configuration at the MLT level.

sVLAN specifications

sVLANs provide the following features:

- VLAN transparency for IEEE 802.1Q tagged or untagged traffic through service provider core networks
- A solution to VLAN scalability issues by allowing you to summarize customer VLANs into core sVLANs
- Use layered architecture to improve scalability

sVLAN rules

The following are sVLAN configuration rules.

- IP filters are not supported on sVLAN.
- To apply QoS to sVLAN, use the per VLAN QoS option.
- Since regular VLANs are not supported on an sVLAN NNI port, sVLAN switches cannot be managed in-band. An out-of-band or parallel network is recommended for managing the devices.
- When creating an sVLAN spanning tree group, the tagged BPDU address of the spanning tree group should be different from the standardized BDPU MAC address.
- The sVLAN is created with the UNI and NNI ports.
- An sVLAN cannot span multiple spanning tree groups; that is, the ports in the sVLAN must all be within one spanning tree group. Spanning tree group IDs can range in value from 1 to 64.
- sVLANs cannot have routing enabled.
- sVLAN UNI and NNI ports are applicable on a per Octapid basis. All ports on a Octapid can either be normal ports or sVLAN NNI/UNI ports. For more information, see Appendix A, “Tap and OctaPID assignment” on page 261.

sVLAN Levels

You can stack sVLANs in a hierarchy to achieve greater VLAN scalability. An sVLAN level defines the hierarchy for the operating switch. When configuring the switch, you must specify only one level at a time.

You must configure UNI ports on both ends of the tunnel at the same level. Since sVLAN switching is MAC-addressed based, the normal issues of VLAN switching apply.

- If you build sVLAN networks with multiple levels, the network MAC addresses you specify must all be unique.
- Independent VLAN learning is only applicable within the outer level of sVLAN and does not take inner tags into account.

Note: Spanning Tree Protocol (STP) is not supported in multi-level sVLAN networks. It is supported for single level sVLAN networks only.

Figure 8 shows a one layer sVLAN.

Figure 8 One layer sVLAN

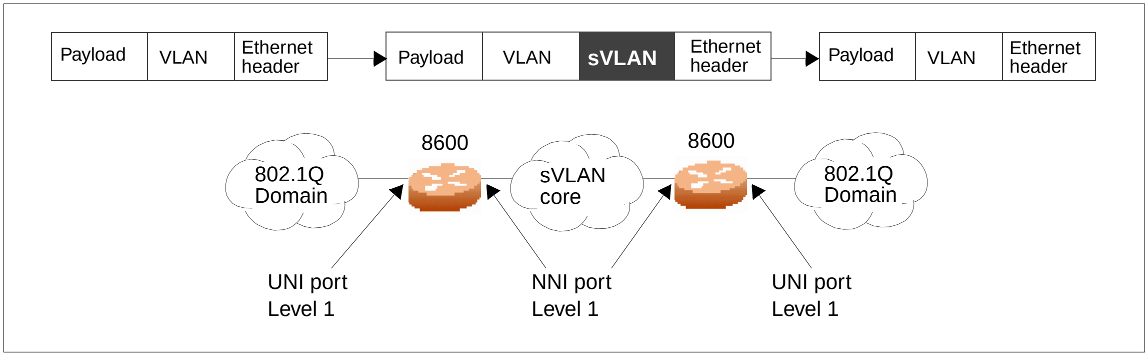
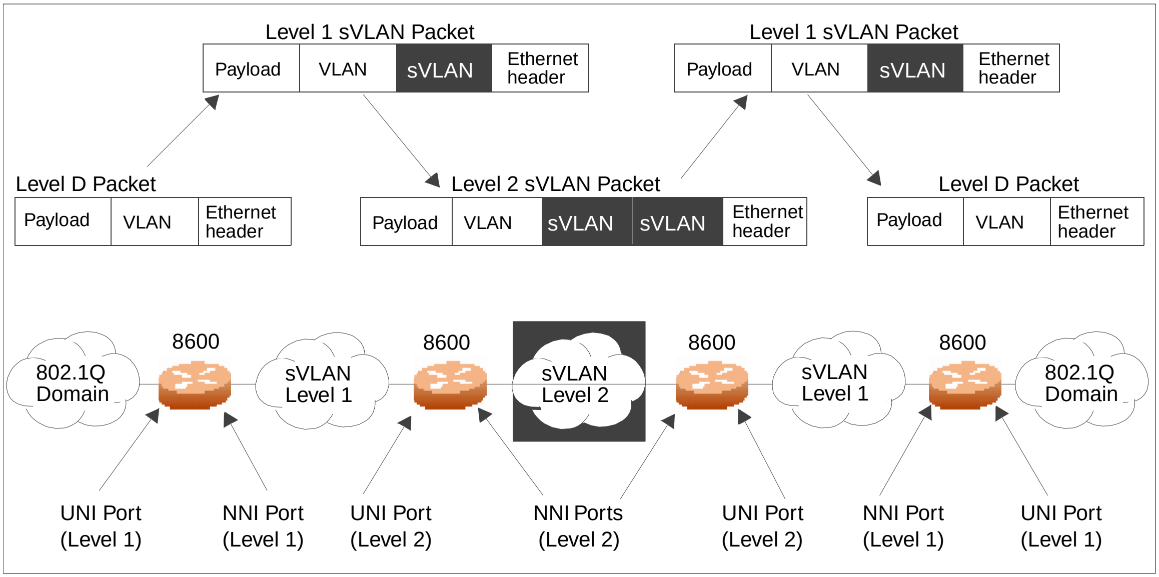


Figure 9 shows a two layer sVLAN.

Figure 9 Two layer sVLAN



sVLAN UNI and NNI ports

The ports in the switch can be configured as sVLAN user-to-network interface (UNI), sVLAN network-to-network interface (NNI), or normal.

Note: You must change the switch level to 1 or above before you configure sVLAN UNI or NNI ports.

You must configure the ports to which you want to provide VLAN transparency as UNI ports. UNI ports can only belong to one sVLAN. When you configure a UNI port in the CLI, the tagged-frames-discard parameter is automatically enabled.

NNI ports interconnect the switches in the core network, drop untagged frames on ingress, and insert the sVLAN tag at the egress. NNI ports can belong to multiple sVLANs. An NNI port sends sVLAN tagged frames. When you configure an NNI port in the CLI, the untagged-frames-discard parameter is automatically enabled.

- If a Spanning Tree Group (STG) contains both UNI and NNI ports, you should change the standardized MAC addresses used for BPDUs to a non-standardized BPDU MAC address to avoid interference with regular customer BPDUs.
- The UNI and NNI ports are kept in sVLAN type STG.
- All of the ports in the MLT should have the same port type (normal/UNI/NNI).
- Large frame support is automatically enabled on UNI/NNI ports.

When you change the sVLAN port type from normal to UNI/NNI, all the affected ports are removed from the configured STGs and VLANs. Similarly, when you change the sVLAN port type from UNI/NNI to normal, all the affected ports are removed from the configured STGs and VLANs and added to the default STG and default VLAN.

Note: The affected ports are all the ports in the Octapid. See Appendix A, “Tap and OctaPID assignment” on page 261.

Note: An NNI port belonging to default VLAN and default STG is not saved across reboots. To avoid this, do not configure an NNI port under default VLAN/STG.

About Spanning Tree protocol (STP)

You can control path redundancy for VLANs by implementing the Spanning Tree Protocol (STP). A network may include multiple instances of STP. The collection of ports in one spanning tree instance is called a spanning tree group.

- 8600 modules support STP and up to 25 spanning tree groups.
- 8100 modules support STP and only one spanning tree group.

As defined in the IEEE 802.1D standard, the Spanning Tree Protocol detects and eliminates logical loops in a bridged or switched network. When multiple paths exist, the spanning tree algorithm configures the network so that a bridge or switch uses only the most efficient path. If that path fails, the protocol automatically reconfigures the network to make another path become active, thus sustaining network operations.

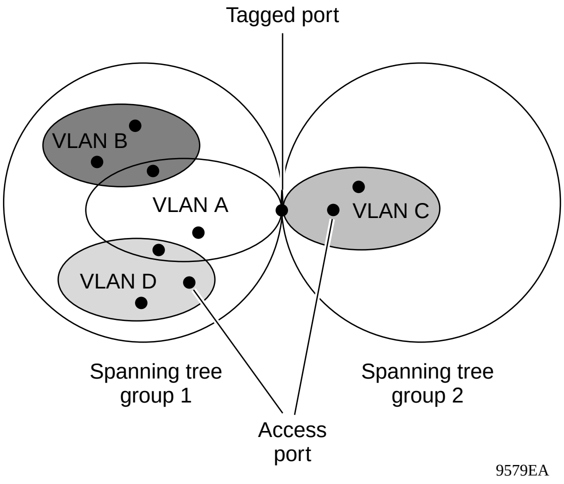
About spanning tree groups

8000 Series switches support STP as defined in IEEE 802.1D. In addition, an 8000 Series switch can support a spanning tree group (STG), which is a collection of ports that belong to the same instance of an STP.

For 8600 modules, multiple STGs are possible within the same switch; that is, the routing switch can participate in the negotiation for multiple spanning trees.

Figure 10 shows multiple spanning tree groups.

Figure 10 Multiple spanning tree groups



Spanning Tree protocol controls

The ports associated with a VLAN and VLANs themselves must be contained within a single spanning tree group. Not allowing a VLAN to span multiple STGs avoids problems with spanning tree blocking ports and causing a loss of connectivity within the VLAN.

Each untagged port can belong to one and only one STG, while tagged ports can belong to more than one STG. When a tagged port belongs to more than one STG, the spanning tree bridge protocol data units (BPDUs) are tagged to distinguish the BPDUs of one STG from those of another STG. BPDUs from STG 1 are not tagged. The tagged BPDUs are transmitted using a multicast MAC address as tagged frames with a VLAN ID, and you specify the multicast MAC address and the VLAN ID. Because tagged BPDUs are not part of the IEEE 802.1D standard, not all devices can interpret tagged BPDUs.

You can enable or disable the Spanning Tree Protocol at the port or at the spanning tree group level. If you disable the protocol at the group level, received BPDUs are handled like a MAC-level multicast and flooded out the other ports of the STG. Note that an STG can contain one or more VLANs. Remember that MAC broadcasts are flooded out on all ports of a VLAN; a BPDU is a MAC-level message, but the BPDU is flooded out all ports on the STG, which may encompass many VLANs.

When STP is globally enabled on the STG, BPDU handling depends on the STP setting of the port:

- When STP is enabled on the port, received BPDUs are processed in accordance with STP.
- When STP is disabled on the port, the port stays in a forwarding state, received BPDUs are dropped and not processed, and no BPDU is generated.

An alternative to disabling the Spanning Tree Protocol is to enable Passport 8000 Series Spanning Tree FastStart.

About Spanning Tree FastStart

Spanning Tree FastStart is an enhanced port mode supported by 8000 Series switches. If you enable Spanning Tree FastStart on a port with no other bridges, the port is brought up more quickly following switch initialization or a spanning tree change. The port goes through the normal blocking and learning states before the forwarding state, but the hold times for these states is the bridge hello timer (2 seconds by default) instead of the bridge forward delay timer (15 seconds by default). If the port sees a BPDU, it will revert to regular behavior.

FastStart is intended for access ports where only one device is connected to the switch (as in workstations with no other spanning tree devices). It may not be desirable to wait the usual 30 to 35 seconds for spanning tree initialization and bridge learning.

Note: Use Passport 8000 Series Spanning Tree FastStart with caution. This procedure is contrary to that specified in the IEEE 802.1D standard for Spanning Tree Protocol (STP), in which a port enters the blocking state following the initialization of the bridging device or from the disabled state when the port is enabled through configuration.

Understanding STGs and VLANs

For the purposes of Spanning Tree Protocol negotiation, the ports on a 8000 Series switch can be divided into groups of ports where each group of ports performs its own spanning tree negotiation with neighboring devices. In a 8000 Series switch, these groups of ports are called spanning tree groups (STGs).

- The Passport 8100 Switch supports one STG.
- The Passport 8600 Switch supports 25 STGs.

The ports in a VLAN are always a subset of the ports in a STG. A VLAN can include all the ports in a given STG, and there can be multiple VLANs in a STG, but a VLAN will never have more ports than exist in the STG. Because VLANs are always subsets of STGs, the recommended practice is to plan STGs and then create VLANs.

In the default configuration, the 8000 Series switch contains a single STG encompassing all the ports in the switch. For most applications, this configuration is sufficient. The default STG has ID 1 (STG1).

If a VLAN spans multiple switches, it must be within the same STG across all switches; that is, the ID of the STG in which it is defined must be the same across all devices.

About Spanning Tree protocol topology change detection

Change detection enables the detection of topology changes and sends a topology change notification (TCN) to the Root on a per port basis. Change detection is enabled by default. When change detection is enabled and a topology change occurs, a trap is sent containing the following information so that you can identify the device:

- the MAC address of the STG sending the TCN
- the port number
- the STG ID

You can disable change detection on ports where a single end station is connected, and where powering that end station on and off would trigger the TCN. Change detection is referenced in IEEE STD 802.1D.

Topology change detection configuration rules

When working with the change detection setting:

- You can configure change detection only on access ports. This also applies to MLT ports.
- If you disable change detection and then change the port from access to tagging-enabled, the switch automatically sets change-detection to `enabled` for the port. This also applies to MLT ports.
- In an MLT with access ports, modifications to change detection for a member port are automatically applied to the remaining member ports.

To configure change detection using Device Manager, see “Configuring topology change detection” on page 152.

To configure change detection using the CLI, see “Configuring topology change detection” on page 225.

About MultiLink Trunking

MultiLink Trunking (MLT) is a point-to-point connection that aggregates multiple ports so that they logically act like a single port with the aggregated bandwidth. Grouping multiple ports into a logical link provides higher aggregate throughput on a switch-to-switch or switch-to-server application. MultiLink Trunking provides media and module redundancy.

MLT traffic distribution algorithm

An MLT can be used to aggregate bandwidth between two switches. The 8600 Series switch uses one of two algorithms to determine which active port in the MLT should be used for each packet. The MLT algorithms are intended to provide load sharing while ensuring that packets do not arrive out of sequence.

The MLT traffic distribution algorithms are:

- For any bridged packet except IP, the following MLT traffic distribution algorithm is used:

MOD (DestMAC[5:0] XOR SrcMAC[5:0], # of active links)

- For any bridged and routed IP or routed IPX, the following MLT traffic distribution algorithm is used:

  MOD (DestIP(X)[5:0] XOR SrcIP(X)[5:0], # of active links)

MultiLink Trunking rules

All 8000 Series switch MLTs operate under the following basic set of rules:

- MLT is supported on 10BASE-T, 100BASE-TX, 100BASE-FX, and Gigabit Ethernet ports.
- All ports in an MLT must be of the same media type (copper or fiber) and have the same speed and duplex settings.
- All ports in an MLT must be in the same spanning tree group.
- MLT is compatible with the Spanning Tree Protocol.
- IEEE 802.1Q tagging is supported on an MLT.

8600 module MLTs have the following general features and requirements:

- Up to 32 MLT groups are supported with as many as eight same-type ports belonging to a single MLT.
- The ports in an MLT can span modules, providing module redundancy.
- All ports in an MLT must be in the same spanning tree group, unless they are tagged; then they can belong to multiple STGs.
- Bridged packet traffic (except for IP distribution) is distributed across the MLT using a source and destination MAC address-based algorithm.
- Bridged and routed IP traffic, or routed Internet packet exchange (IPX) traffic, is distributed across the MLT using a source and destination IP address-based algorithm.

8100 module MLTs have the following features and requirements:

- Up to six MLT groups are supported with as many as four same-type ports belonging to a single MLT.
- All ports in an MLT must be in the one spanning tree group.

- To optimize performance, the switch will distribute traffic to an MLT on the same module. If there is no MLT on the module, a round robin algorithm determines which MLT should receive the traffic. This algorithm is based on the source MAC address and the port on which that MAC address was learned.

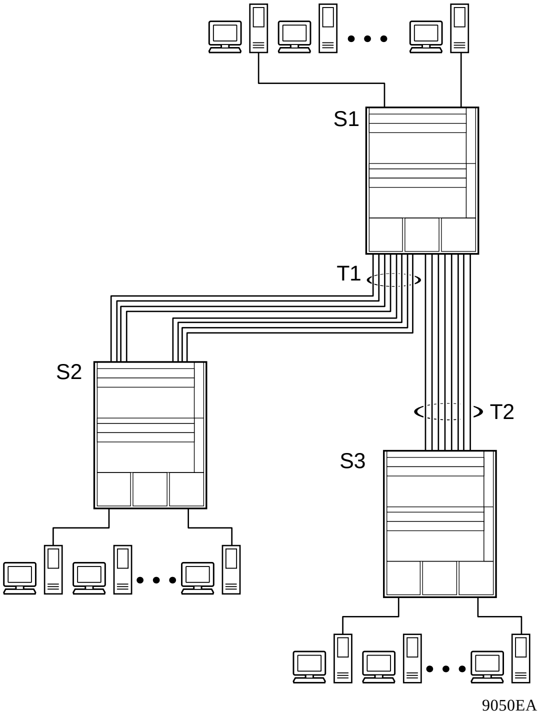
MultiLink Trunking examples

MultiLink Trunks allow you to group switch ports together to form a link to another switch or server, thus increasing aggregate throughput of the interconnection between the devices. When the Spanning Tree Protocol is enabled, MultiLink Trunking software detects misconfigured or broken trunk links and removes the port from the MLT group.

Switch-to-switch MLT configuration

Figure 11 shows two trunks (T1 and T2) connecting switch S1 to switches S2 and S3.

Figure 11 Switch-to-switch MLT configuration

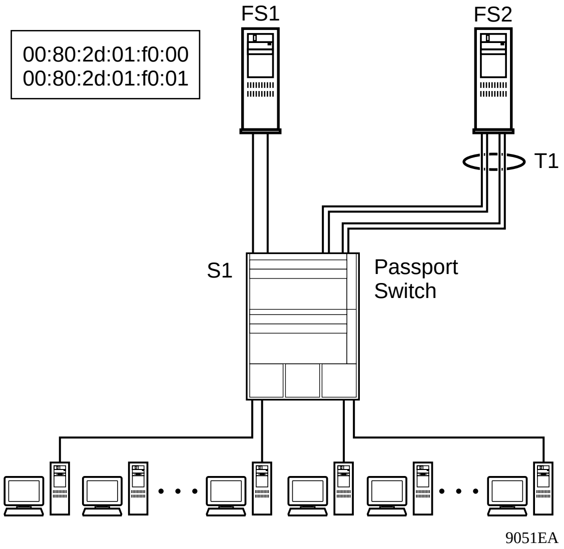


Each of the trunks shown in Figure 11 can be configured with multiple switch ports to increase bandwidth and redundancy. When traffic between switch-to-switch connections approaches single port bandwidth limitations, creating a MultiLink Trunk can supply the additional bandwidth required to improve performance.

Switch-to-server MLT configuration

Figure 12 shows a typical switch-to-server trunk configuration. In this example, file server FS1 utilizes dual MAC addresses, using one MAC address for each network interface card (NIC). No MLT is configured to FS1. FS2 is a single MAC server (with a 4-port NIC) and is set up as trunk configuration T1.

Figure 12 Switch-to-server MLT configuration

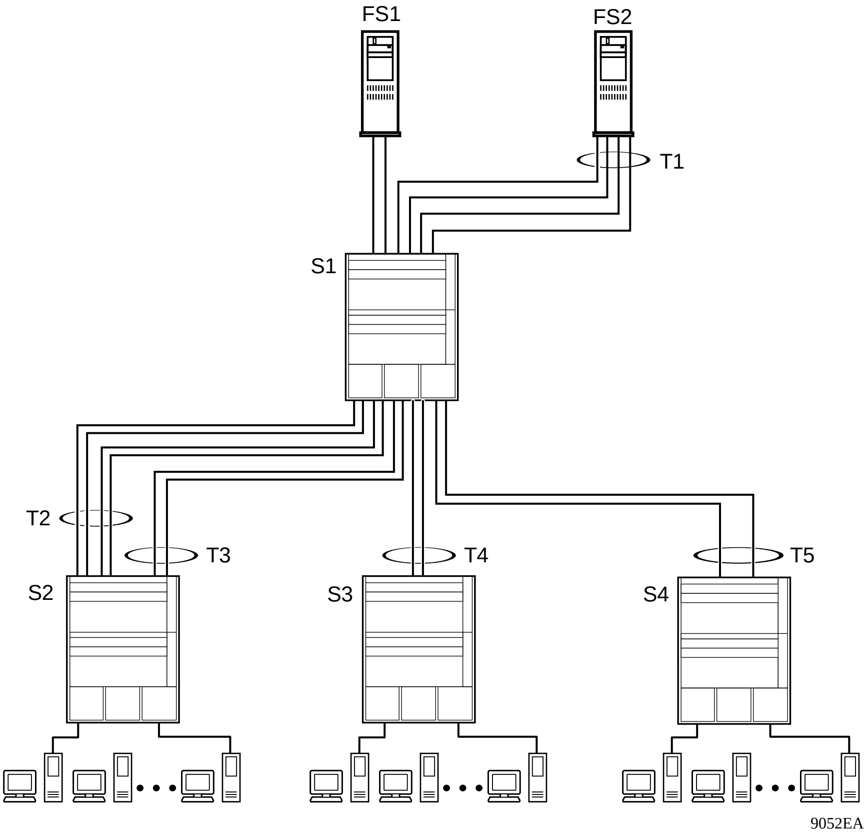


Client/server MLT configuration

Figure 13 shows an example of how MultiLink Trunks can be used in a client/server configuration. In this example, both servers are connected directly to switch S1. FS2 is connected through a trunk configuration (T1). The switch-to-switch connections are through trunks (T2, T3, T4, and T5). Clients accessing data from the servers (FS1 and FS2) are provided with maximized bandwidth through trunks T1, T2, T3, T4, and T5. On the 8000 Series switch, trunk members (the ports making up each trunk) do not have to be consecutive switch ports; they can be selected across different modules for module redundancy.

With spanning tree *enabled* and trunks T2 and T3 in the same spanning tree group, one of the trunks (T2 or T3) acts as a redundant (backup) trunk to switch S2, and STP will block one of the trunks. With spanning tree *disabled*, neither trunk T2 nor trunk T3 is blocked; they must be configured into separate VLANs to avoid a loop in the network.

Figure 13 Client/Server MLT configuration



With spanning tree enabled, ports that belong to the same MultiLink Trunk operate as follows. All ports in the MLT must belong to the same spanning tree group if spanning tree is enabled. Identical bridge protocol data units (BPDUs) are sent out of each port. The MLT port ID is the ID of the lowest numbered port. If identical BPDUs are received on all ports, the MLT mode is forwarding. If no BPDU is received on a port or if BPDU tagging and port tagging do not match, the individual port is taken offline. Path cost is inversely proportional to the active MLT bandwidth.

Multicast flow distribution over MLT

MultiLink Trunking (MLT) provides a mechanism for distributing multicast streams over an MLT. It does so based on source-subnet and group addresses and in the process provides you with the ability to choose the address and the bytes in the address for the distribution algorithm. As a result, you can now distribute the load on different ports of the MLT and aim (whenever possible) to achieve an even distribution of the streams. In applications like TV distribution, multicast traffic distribution is particularly important since the bandwidth requirements can be substantial when a large number of TV streams are employed.

Note: The multicast distribution over MLT feature is supported only on 8000 Series E-modules. As a result, all the cards that have ports in an MLT must be 8000 Series E-cards in order to enable multicast flow distribution over MLT.

Multicast distribution algorithm

To determine the port for a particular Source, Group (S,G) pair, the number of active ports of the MLT is used to MOD the number generated by the XOR of each byte of the masked group address with the masked source address. By default, the group mask and source mask is 255.255.255.255. A byte with a value of 255 in the mask means that the corresponding byte in the group or source address is taken into account when the algorithm is applied.

For example, consider:

> Group address G[0].G[1].G[2].G[3], Group Mask GM[0].GM[1].GM[2].GM[3], Source Subnet address S[0].S[1].S[2].S[3], Source Mask SM[0].SM[1].SM[2].SM[3]

Then, the Port =:

> (((((G[0] AND GM[0]) xor (S[0] AND SM[0])) xor ((G[1] AND GM[0]) xor (S[1] AND SM[1]))) xor ((G[2] AND GM[2]) xor (S[2] AND SM[2]))) xor ((G[3] AND GM[3]) xor (S[3] AND SM[3]))) MOD (active ports of the MLT)

The algorithm used for traffic distribution causes the distribution to be sequential if the streams are similar to those in the example that follows. Assume that the MLT ports are 1/1-1/4, that mask configuration is 0.0.0.0 for the source mask and 0.0.0.255 for the group mask, and that source A.B.C.D sends to groups:

X.Y.Z.1

X.Y.Z.2

X.Y.Z.3

.....

X.Y.Z.10

The algorithm chooses link 1/1 for group X.Y.Z.1, then X.Y.Z.2 goes on 1/2, X.Y.Z.3 goes on 1/3. X.Y.Z.4 goes on 1/4, X.Y.Z.5 goes on 1/1 and so on.

In the following configuration example, only the first byte of the grp-mask, and the first two bytes of the src-subnet mask are considered when distributing the streams.

```
config sys mcast-mlt-distribution grp-mask 255.0.0.0

config sys mcast-mlt-distribution src-mask 255.255.0.0

config sys mcast-mlt-distribution enable

config sys mcast-mlt-distribution redistribution enable
```

Note: When configuring flow distribution over MLT, it is recommended that you choose source and group masks that result in the most even traffic distribution over the MLT links. For example, if you find in the network group addressing that group addresses change incrementally, while there are few sources always sending to different groups, you should use a source mask of 0.0.0.0 and a group mask of 255.255.255.255. In most cases, this will provide a sequential distribution of traffic on the links of the MLT.

For a detailed description of commands used to configure Multicast flow distribution over MLT, see the publication, *Configuring IP Routing Multicast Protocols*.

Multicast traffic redistribution

The overall goal of traffic redistribution is to achieve a distribution of the streams on the MLT links in the event of an MLT configuration change. For example, ports might be added or deleted. By default, redistribution is disabled. When a link is added or removed from the MLT, the active streams continue flowing on their original links if redistribution is disabled.

If redistribution is enabled, however, the active streams are redistributed according to the distribution algorithm on the links of the MLT. Note that this may cause minor traffic interruptions. To minimize the effect of redistribution of multicast traffic on the MLTs, the implementation does not move the streams to the appropriate links all at once. Instead, it redistributes a few streams at every time tick of the system.

To that end, when an MLT port becomes inactive and redistribution is disabled, only the affected streams are redistributed on the remaining active ports. If redistribution is enabled, all the streams are redistributed on the MLT ports based on the assignment provided by the distribution algorithm. For more information, see the previous section, “Multicast distribution algorithm” on page 56.

When a new port becomes active in an MLT and redistribution is disabled, existing streams will remain on their original links. If you need to redistribute the streams dynamically to split the load on all the links of the MLT, you should enable redistribution. This will result in a few streams being redistributed every system time tick.

For a detailed description of the commands used to configure Multicast flow distribution over MLT, see the publication, *Configuring IP Routing Multicast Protocols*.

About Split Multilink Trunking (SMLT)

In order to provide device redundancy, most enterprise networks are designed with redundant connections between aggregation (core) switches and user access switches. For networks with just one aggregation switch, MLT provides redundancy and load sharing.

SMLT improves the reliability of a layer 2 (L2) network operating between a building's user access switches and the network center aggregation switch by providing:

- loadsharing among all links
- fast failover in case of link failures

An Inter Switch Trunk (IST) operates between the aggregation switches and allows them to exchange information. This permits the rapid detection of any faults and the modification of forwarding paths.

Note: Although SMLT is primarily designed for layer 2 networks, it also provides benefits for layer 3 networks.

In an SMLT network, 8000 Series switches are typically used as follows:

- 8100 or other layer 2 switch is used as edge (user access) switch.
- 8600 switch is used as aggregation (core) switch.

Note: An edge (layer 2) switch must support MLT to allow communication with an SMLT aggregation switch.

The 8100 Switch uses an MLT algorithm for load-sharing among MLT link aggregation switches. In the event of failure, traffic is rapidly diverted from one MLT link to another.

Advantages of SMLT

SMLT provides the following advantages:

- Eliminates single point of failure
- Recovers, in case of failure, as quickly as possible
- Provides a transparent and interoperable solution
- Removes Spanning Tree Protocol (STP) convergence issues

These advantages are described in more detail in the sections that follow.

Single point of failure elimination

SMLT helps eliminate all single points of failure and create multiple paths from all user access switches to the core of the network. In case of failure, SMLT recovers as quickly as possible so that no unused capacity is created. Finally, SMLT provides a transparent and interoperable solution that requires no modification on the part of the majority of existing user access devices.

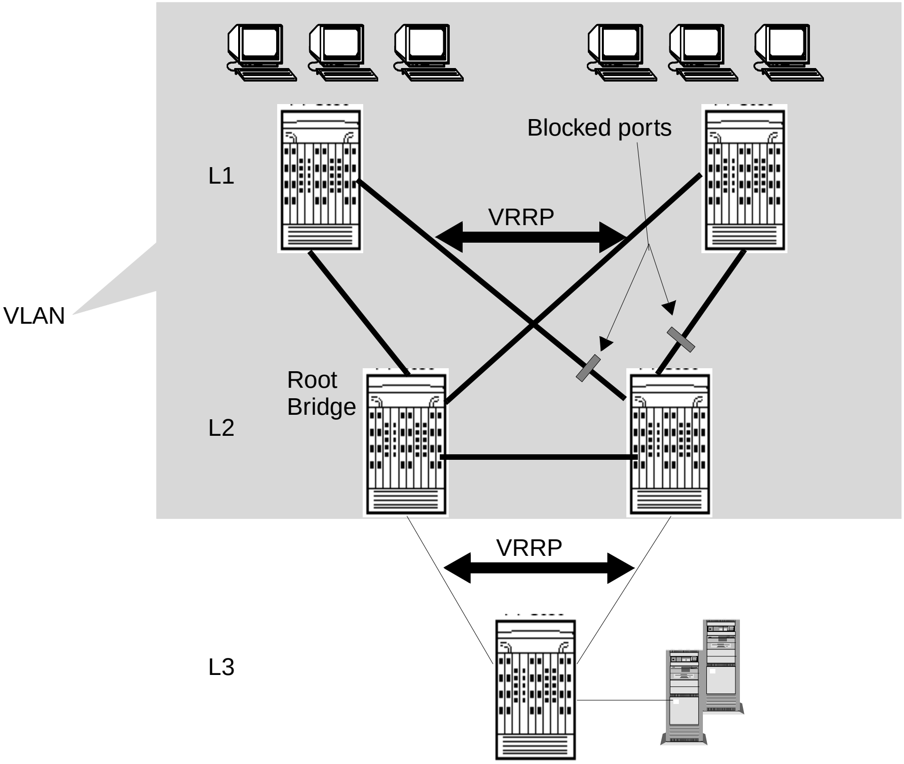
STP convergence issues

Networks that are designed to have user access switches dual-homed to two aggregation switches and have VLANs spanning two or more user access switches experience the following design constraints:

- Spanning Tree must be used to detect loops
- No load sharing exists over redundant links
- Slow network convergence exists in case of failure

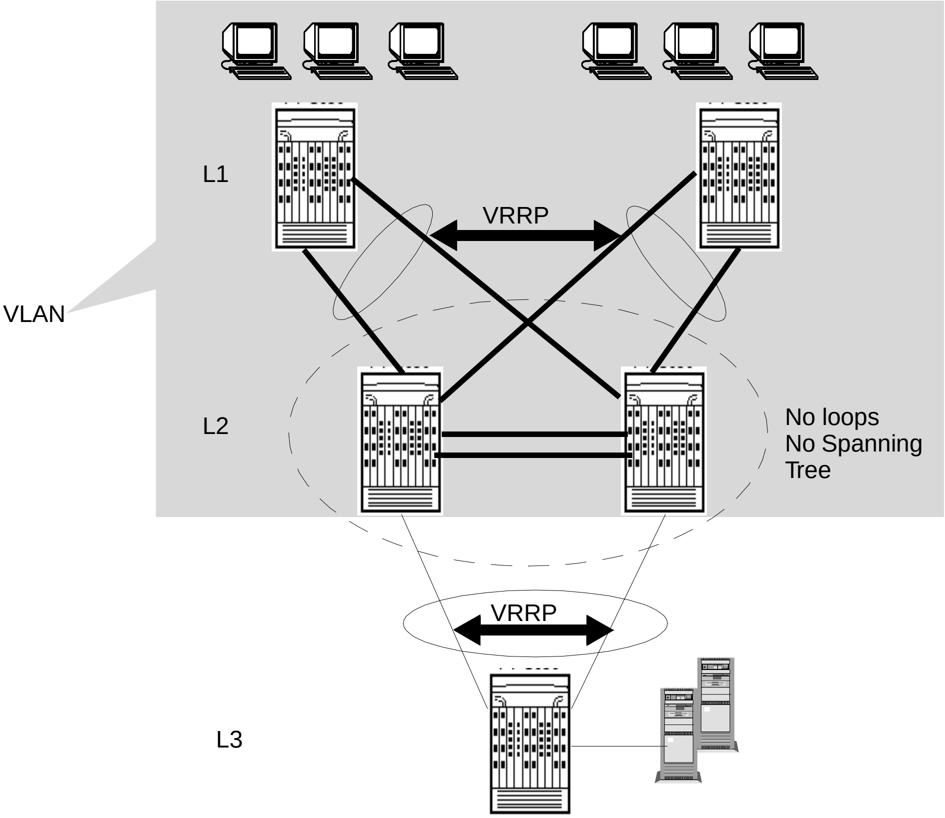
(Figure 14) shows a typical aggregator switch configuration that is dependent upon STP for loop detection.

Figure 14 Resilient networks with Spanning Tree Protocol



With the introduction of SMLT, all dual-homed layer 2 frame-switched network devices are no longer dependent upon the Spanning Tree Protocol (Figure 15) for loop detection. Similarly, layer 3 networks can now benefit from SMLT as well.

Figure 15 Resilient networks with SMLT

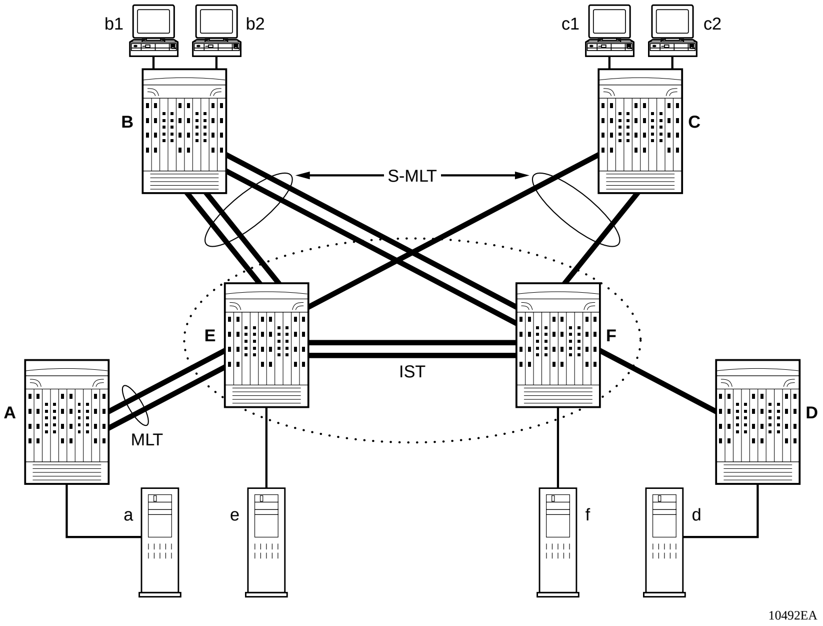


SMLT solves the Spanning Tree problem by combining two aggregation switches into one “logical” MLT entity, thus making it transparent to any type of edge switch. In the process, it provides quick convergence, while load sharing across all available trunks.

How does SMLT work?

Figure 16 illustrates an SMLT configuration with a pair of 8600 Series aggregation switches (E and F). Also included are four separate user access switches (A, B, C, and D).

Figure 16 8000 Series switches as SMLT aggregation switches



About Inter-switch trunk (IST)

User access switches B and C are connected to the aggregation switches via multilink trunks split between the two aggregation switches. As shown in Figure 16, the implementation of SMLT only requires two SMLT capable aggregation switches. Those switches must be connected via an IST.

Aggregation switches use the IST to:

- Confirm that they are alive and exchange MAC address forwarding tables.
- Send traffic between single switches attached to the aggregation switches.
- Serve as a backup if one SMLT link fails.

Since the IST is required for the SMLT to operate properly, it represents a single point of failure. As a result, it is recommended that you use multiple links on the IST to ensure reliability and high availability. Nortel Networks recommends using Gigabit Ethernet links for IST connectivity in order to provide enough bandwidth for potential cross traffic.

➡ **Note:** ATM and POS are not supported for use as IST links.

About CP-Limit and SMLT IST

Control packet rate limit (CP-Limit) controls the amount of multicast and/or broadcast traffic that can be sent to the CPU from a physical port. It protects the CPU from being flooded by traffic from a single, unstable port. The CP-Limit default settings are:

- default state = enabled
- default multicast packets-per-second (pps) value = 15,000
- default broadcast pps value = 10,000

If the actual rate of packets-per-second sent from a port exceeds the defined rate, then the port is administratively shut down to protect the CPU from continued bombardment.

Disabling IST ports in this way could impair network traffic flow, as this is a critical port for SMLT configurations.

Nortel Networks recommends that an IST MLT contain at least 2 physical ports, although this is not a requirement. Nortel Networks also recommends that CP-Limit be disabled on all physical ports that are members of an IST MLT.

Disabling CP-Limit on IST MLT ports forces another, less-critical port to be disabled if the defined CP-Limits are exceeded. In doing so, you preserve network stability should a protection condition (CP-Limit) arise. Please note that, although it is likely that one of the SMLT MLT ports (risers) would be disabled in such a condition, traffic would continue to flow uninterrupted through the remaining SMLT ports.

Note: CP-Limit can only be configured from the CLI.

The command syntax to disable CP-limit is:

```
config ethernet <slot/port> cp-limit <enable|disable>
```

Switch connections

Figure 16 also includes end stations connected to each of the switches. In this example, a, b1, b2, c1, c2, and d are clients and printers, while e and f might be servers or routers.

User access switches B and C may use any method for determining which link of their multilink trunk connections to use for forwarding a packet, as long as the same link is used for a given Source/Destination (SA/DA) pair. This is true, regardless of whether or not the DA is known by B or C. SMLT aggregation switches always send traffic directly to a user access switch and only use the IST for traffic that they cannot forward in another more direct way.

The examples that follow explain the process in more detail.

Example 1- Traffic flow from a to b1 or b2

Assuming a and b1/b2 are communicating via layer 2, traffic flows from A to switch E and is then forwarded over its direct link to B. Traffic coming from b1 or b2 to a is sent by B on one of its MLT ports.

B could then send traffic from b1 to a on the link to switch E, and traffic from b2 to a on the link to F. In the case of traffic from b1, switch E forwards the traffic directly to switch A, while traffic from b2, which arrived at F, is forwarded across the IST to E and then on to A.

Example 2- Traffic flow from b1/b2 to c1/c2

Traffic from b1/b2 to c1/c2 will be always be sent by switch B down its MLT to the core. No matter which switch (E or F) it arrives at, it will then be sent directly to C through the local link.

Example 3- Traffic flow from a to d

Traffic from a to d and vice versa is forwarded across the IST because it is the shortest path. This is treated purely as a standard link with no account taken of SMLT and the fact that it is also an IST.

Example 4- Traffic flow from f to c1/c2

Traffic from f to c1/c2 will be sent out directly from F. Return traffic from c1/c2 allows you to have one active VRRP Master per IP subnet. It will then be passed across the IST if switch C sends it down the link to E.

SMLT and VRRP

The current implementation of VRRP lets you have one active primary router per IP subnet, with all other network VRRP interfaces in backup mode.

With SMLT, this becomes less efficient. Users that access switches aggregated into two Split-MLT switches, send their shared traffic load (based on source and destination MAC or IP addresses) on all uplinks towards the SMLT aggregation switches.

VRRP, however, has only one active routing interface enabled. All other interfaces are in backup (standby) mode. In this case all traffic is forwarded over the IST link towards the primary VRRP switch. Potentially, all traffic which arrives at the VRRP backup interface is forwarded over, so there will be not enough bandwidth on the IST to carry all the aggregated riser traffic.

A small enhancement in VRRP overcomes this issue, however, by ensuring that the IST trunk is not used in such a case for primary data forwarding.

VRRP backup master

If enabled, the VRRP backup master feature also acts as an IP router for packets destined for the logical VRRP IP address. Thus, all traffic is directly routed to the subnetworks it is destined for and not L2- switched to the VRRP master. This eliminates a potential limitation in the available IST bandwidth.

Note: The VRRP backup master feature for SMLT is to be used only on interfaces that have been defined for SMLT to avoid potential frame duplication problems. It cannot be used in conjunction with HUBs to avoid frame duplication. Also, it is not to be used on brouter or VLAN interfaces.

About single port SMLT

Single port SMLT lets you configure a split multilink trunk using a single port. The single port SMLT behaves just like an MLT-based SMLT and can coexist with SMLTs in the same system. Single port SMLT lets you scale the number of split multilink trunks on a switch to a maximum number of available ports.

Split MLT links may exist in the following combinations on the SMLT aggregation switch pair:

- MLT-based SMLT + MLT-based SMLT
- MLT-based SMLT + single link SMLT
- single link SMLT + single link SMLT

Rules for configuring single port SMLT:

- The dual-homed device connecting to the aggregation switches must be capable of supporting MLT.
- Single port SMLT is supported on Ethernet, POS, and ATM ports.

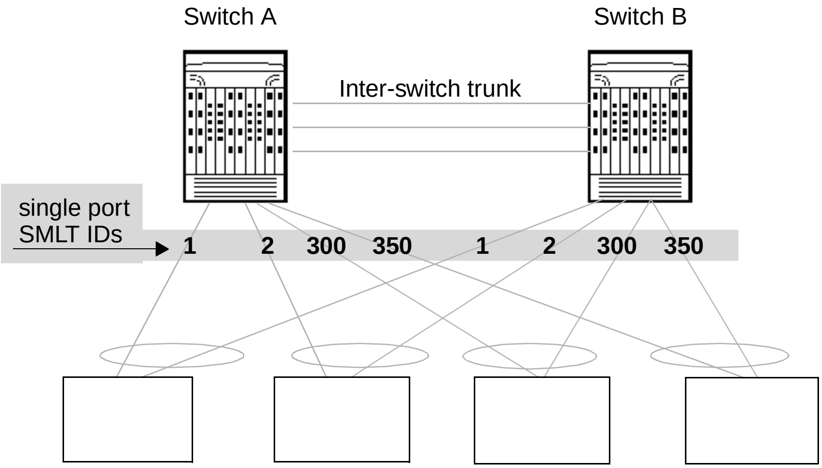
Note: Single port SMLT is not supported on 10 Gig Ethernet ports with release 3.5.

- Each single port SMLT is assigned an SMLT ID from 1 to 512.

- Single port SMLT ports can be designated as Access or Trunk (that is, IEEE 802.1Q tagged or not), and changing the type does not affect their behavior.
- You cannot change a single port SMLT into an MLT-based SMLT by adding more ports. You must delete the single port SMLT, and then reconfigure the port as SMLT/MLT.
- You cannot change an MLT-based SMLT into a single port SMLT by deleting all ports but one. You must first remove the SMLT/MLT and then reconfigure the port as single port SMLT.
- A port cannot be configured as MLT-based SMLT and as single port SMLT at the same time.

Figure 17 shows a configuration in which both aggregation switches have single port SMLTs with the same IDs. This configuration allows as many single port SMLTs as there are available ports on the switch.

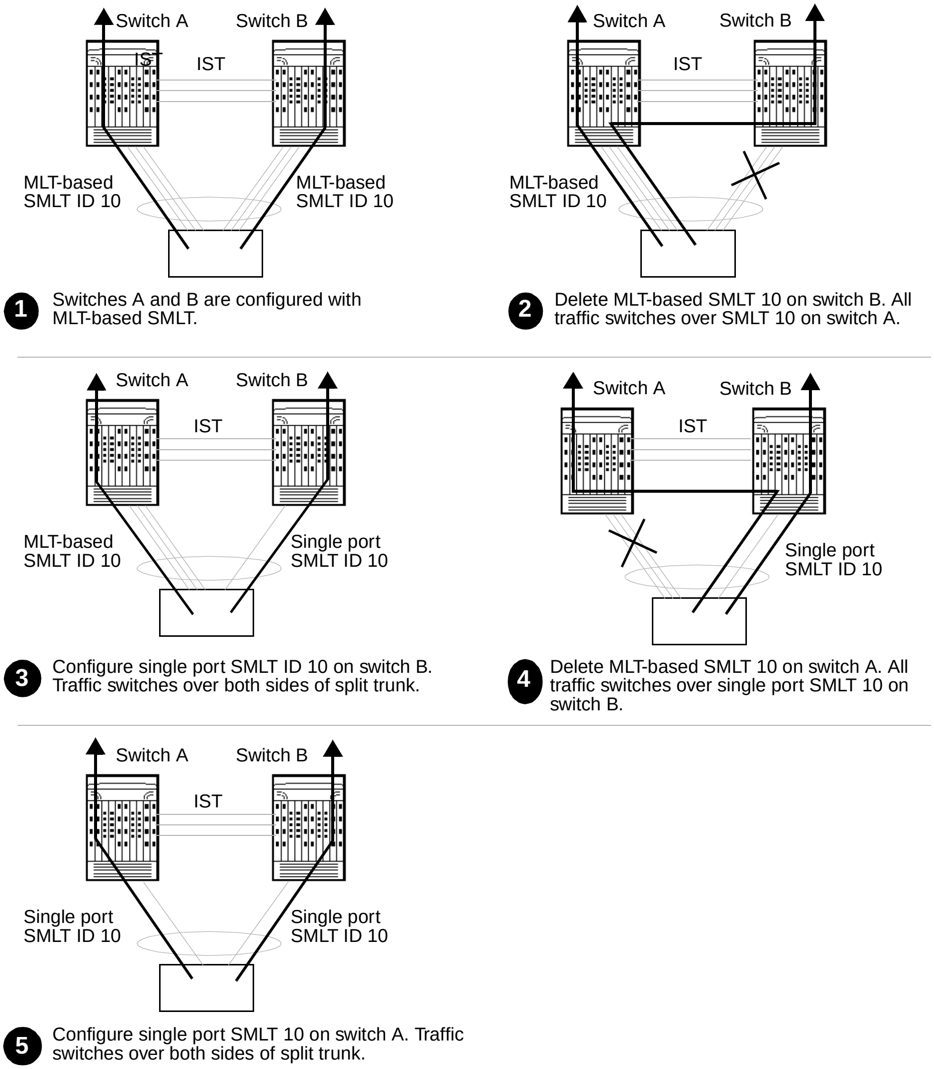
Figure 17 Single port SMLT example



Using MLT-based SMLT with single port SMLT

You can configure a split trunk with a single port SMLT on one side and an MLT-based SMLT on the other. Both must have the same SMLT ID. In addition to general use, Figure 18 shows how this configuration can be used for upgrading an MLT-based SMLT to a single port SMLT without taking down the split trunk.

Figure 18 Changing a split trunk from MLT-based SMLT to single port SMLT



1 Switches A and B are configured with MLT-based SMLT.

2 Delete MLT-based SMLT 10 on switch B. All traffic switches over SMLT 10 on switch A.

3 Configure single port SMLT ID 10 on switch B. Traffic switches over both sides of split trunk.

4 Delete MLT-based SMLT 10 on switch A. All traffic switches over single port SMLT 10 on switch B.

5 Configure single port SMLT 10 on switch A. Traffic switches over both sides of split trunk.

To configure single port SMLT using Device Manager, see “Configuring single port SMLT” on page 177.

To configure single port SMLT using the CLI, see “Creating a single port SMLT” on page 245.

Chapter 2
Configuring VLANs using Device Manager

This section describes using Device Manager to configure VLANs on an 8600 module or an 8100 module and includes the following topics:

- "Displaying defined VLANs" on page 71
- "Creating a VLAN" on page 74
- "Managing a VLAN" on page 100
- "Managing VLAN bridging" on page 109
- "Configuring directed broadcast on a VLAN" on page 119
- "Configuring Enhanced Operation mode" on page 121

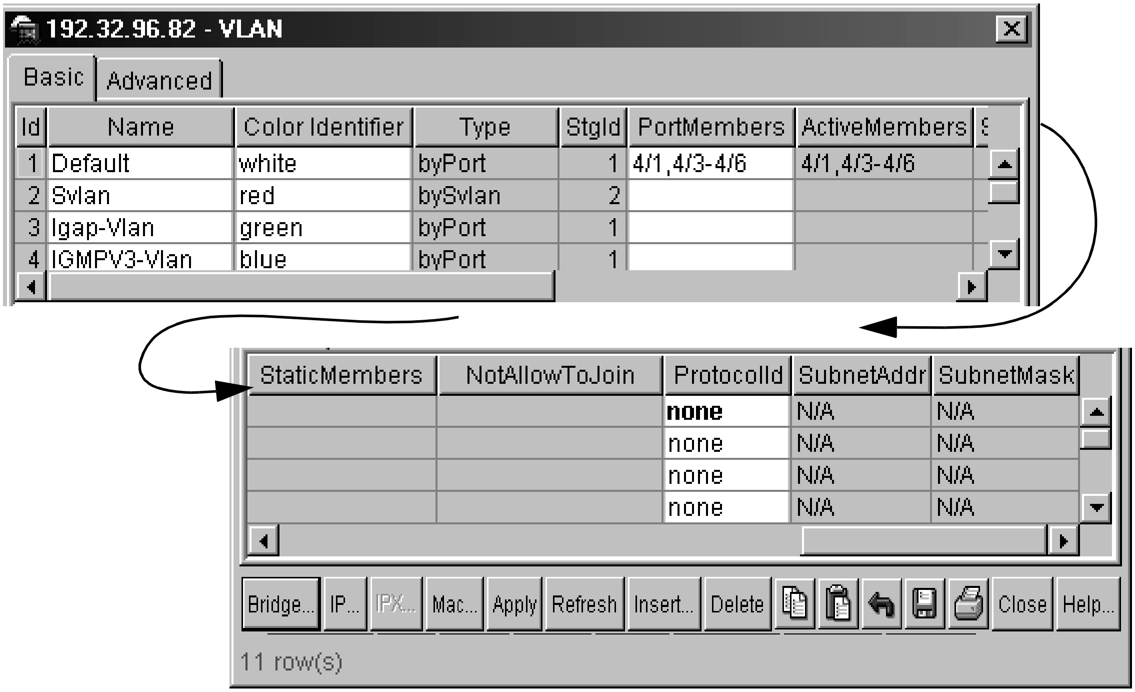
For conceptual information about VLANs, see "About VLANs" on page 6.

Displaying defined VLANs

To display all defined VLANs, their configurations, and their current status, choose VLAN > VLANs.

The VLAN dialog box opens to the Basic tab (Figure 19), displaying all defined VLANs.

Figure 19 VLAN dialog box—Basic tab



Id	Name	Color Identifier	Type	StgId	PortMembers	ActiveMembers
1	Default	white	byPort	1	4/1,4/3-4/6	4/1,4/3-4/6
2	Svlan	red	bySvlan	2		
3	Igap-Vlan	green	byPort	1		
4	IGMPV3-Vlan	blue	byPort	1		

StaticMembers	NotAllowToJoin	ProtocolId	SubnetAddr	SubnetMask
		none	N/A	N/A
		none	N/A	N/A
		none	N/A	N/A
		none	N/A	N/A

11 row(s)

Table 7 describes fields on the VLAN Basic tab.

Table 7 VLAN Basic tab fields

Field	**Description**
Id	VLAN ID (1 - 4092) for the VLAN.
Name	Name of the VLAN.
Color Identifier	A proprietary color scheme to associate a color with the VLAN. Color does not affect how frames are forwarded.
Type	Type of VLAN: • byPort • byIpSubnet • byProtocolId (8600 modules and 8100 modules) • bySrcMac (8600 modules only) • bySvlan (8600 modules only)
StgId	The ID of the spanning tree group to which the VLAN belongs.
PortMembers	The slot/port of each possible VLAN member.

Table 7 VLAN Basic tab fields (continued)

Field	**Description**
ActiveMembers	The slot/port of each activeVLAN member, including all static members and potential members meeting the policy.
StaticMembers	Slot/port of each static (always) member of a protocol-based VLAN.
NotAllowToJoin	The slot/ports that are never allowed to become a member of the protocol-based VLAN.
ProtocolId	Specify the network protocol for protocol-based VLANs. This value is taken from the Assigned Numbers RFC. • ip (IP version 4) • ipx802dot3 (Novell IPX on Ethernet 802.3 frames) • ipx802dot2 (Novell IPX on IEEE 802.2 frames) • ipxSnap (Novell IPX on Ethernet SNAP frames) • ipxEthernet2 (Novell IPX on Ethernet Type 2 frames) • appleTalk (AppleTalk on Ethernet Type 2 and Ethernet SNAP frames) • decLat (DEC LAT protocol) • decOther (Other DEC protocols) • sna802dot2 (IBM SNA on IEEE 802.2 frames) • snaEthernet2 (IBM SNA on Ethernet Type 2 frames) • netBIOS (NetBIOS protocol) • xns (Xerox XNS) • vines (Banyan VINES) • ipv6 (IP version 6) • usrDefined (user-defined protocol) • RARP (Reverse Address Resolution protocol) • PPPoE (Point-to-point protocol over Ethernet) **Note**: if the VLAN type is port-based, *None* is displayed in the Basic tab ProtocolId field.
UserDefinedPid	Specify the 16-bit user-defined network protocol identifier when the ProtocolId (above) is set to usrDefined for a protocol-based VLAN type. **Note**: When in Enhanced Mode, you cannot create more than 748 UserDefined protocol-based VLANS.
SubnetAddr	The source IP subnet address (IP subnet-based VLANs only).
SubnetMask	The source IP subnet mask (IP subnet-based VLANs only).

Table 7 VLAN Basic tab fields (continued)

Field	**Description**
AgingTime	Indicates the timeout period in seconds (10 - 1000000) for aging out the VLAN's dynamic port members. This field is only relevant for policy-based VLANs. The default is 600 seconds.
QosLevel	Indicate the quality of service level of the incoming frames with this destination Mac Address. • level0 (lowest priority) • level1 (default) • level2 • level3 • level4 • level5 • level6 • level7 (highest priority)

Creating a VLAN

You can create VLANs using the following procedures:

- "Creating a port-based VLAN" on page 74
- "Creating a source IP subnet-based VLAN" on page 81
- "Creating a protocol-based VLAN" on page 84
- "Configuring user-defined protocols in protocol-based VLANs" on page 87
- "Creating a source MAC address-based VLAN" on page 90

When creating a VLAN, keep in mind the rules described in "VLAN rules" on page 38.

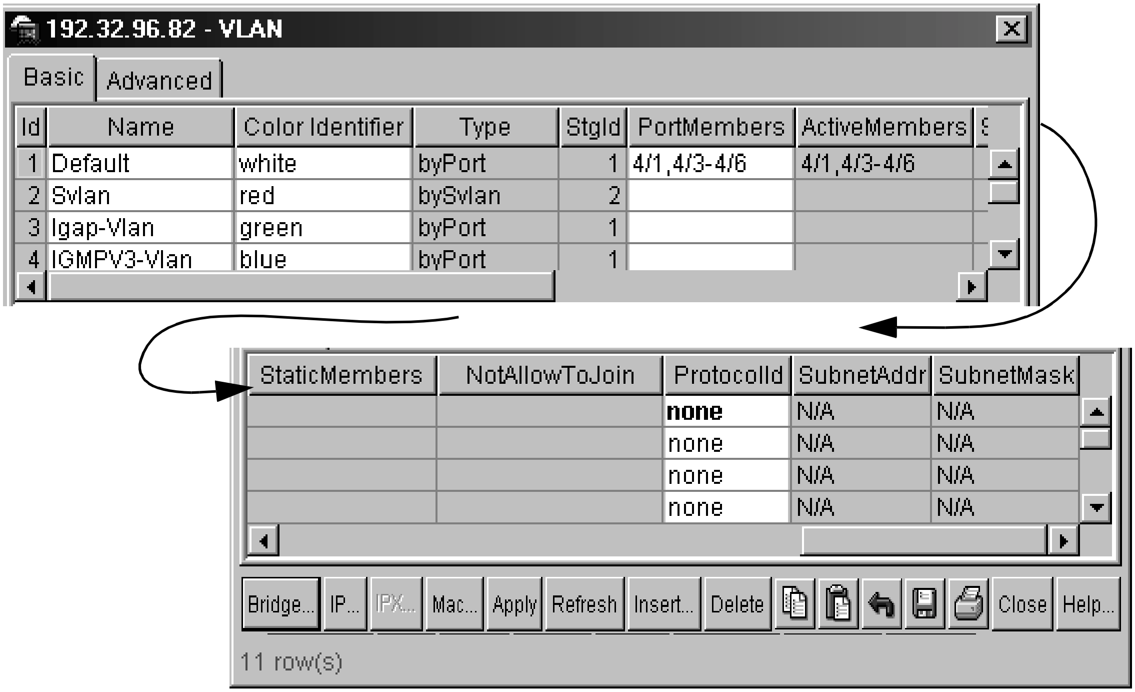
Creating a port-based VLAN

To create a port-based VLAN:

1 From the Device Manager menu bar, choose VLAN > VLANs.

The VLAN dialog box opens to the Basic tab (Figure 20).

Figure 20 VLAN dialog box—Basic tab



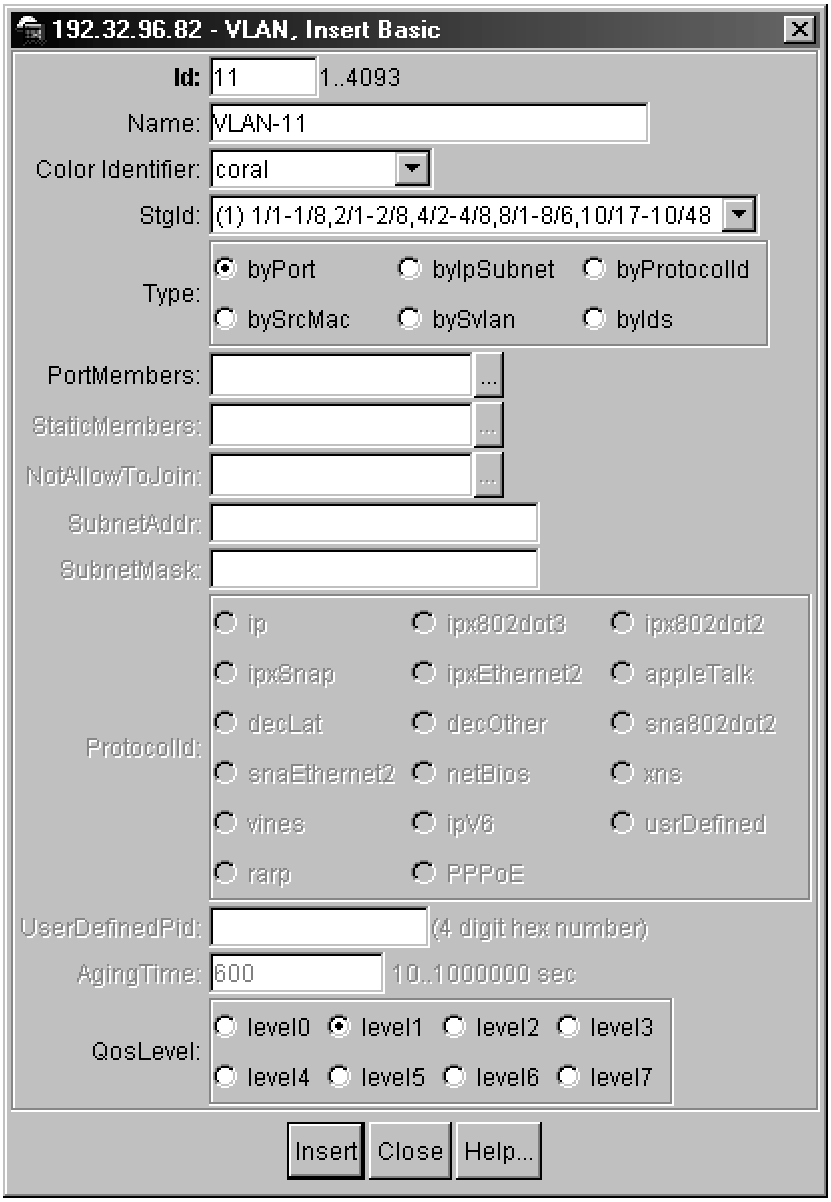
Id	Name	Color Identifier	Type	StgId	PortMembers	ActiveMembers
1	Default	white	byPort	1	4/1,4/3-4/6	4/1,4/3-4/6
2	Svlan	red	bySvlan	2		
3	Igap-Vlan	green	byPort	1		
4	IGMPV3-Vlan	blue	byPort	1		

StaticMembers	NotAllowToJoin	ProtocolId	SubnetAddr	SubnetMask
		none	N/A	N/A
		none	N/A	N/A
		none	N/A	N/A
		none	N/A	N/A

2 Click Insert.

The VLAN, Insert Basic dialog box opens (Figure 21).

Figure 21 VLAN, Insert Basic dialog box—for port-based VLANs



192.32.96.82 - VLAN, Insert Basic

Id: 11 1..4093

Name: VLAN-11

Color Identifier: coral

StgId: (1) 1/1-1/8,2/1-2/8,4/2-4/8,8/1-8/6,10/17-10/48

Type: ● byPort ○ byIpSubnet ○ byProtocolId ○ bySrcMac ○ bySvlan ○ byIds

PortMembers:

StaticMembers:

NotAllowToJoin:

SubnetAddr:

SubnetMask:

ProtocolId: ○ ip ○ ipx802dot3 ○ ipx802dot2 ○ ipxSnap ○ ipxEthernet2 ○ appleTalk ○ decLat ○ decOther ○ sna802dot2 ○ snaEthernet2 ○ netBios ○ xns ○ vines ○ ipV6 ○ usrDefined ○ rarp ○ PPPoE

UserDefinedPid: (4 digit hex number)

AgingTime: 600 10..1000000 sec

QosLevel: ○ level0 ● level1 ○ level2 ○ level3 ○ level4 ○ level5 ○ level6 ○ level7

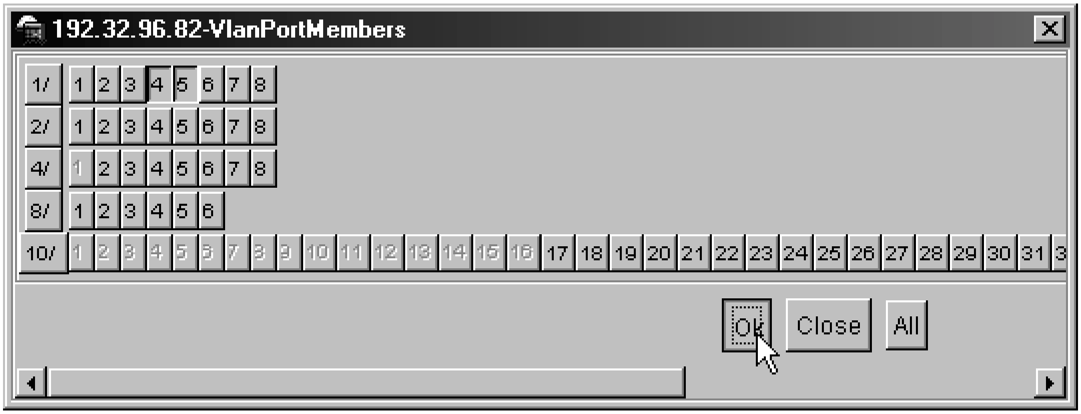
3 In the ID field, enter an unused VLAN ID (1 - 4094), or use the ID provided.

4 (Optional) In the Name field, type the VLAN name, or use the name provided.

5. (Optional) In the Color Identifier field, click the down arrow and choose a color from the dropdown list, or use the color provided.
6. In the StgId field, type or select the spanning tree group ID of the VLAN.
7. In the Type field, select byPort.
8. In the PortMembers field, click the ellipsis (...).

   The VlanPortMembers dialog box opens (Figure 22).

Figure 22 VlanPortMembers dialog box



9. Click the ports that are always members. Selected ports display depressed, while the non selected ports display not depressed. Port numbers that display in gray indicate ports that cannot be selected to belong to the VLAN. (For example, you cannot select ports that do not have the same spanning tree group ID as that of the new VLAN.)
10. Click OK.

    The Port Membership dialog box closes and the port members appear in the Insert Basic dialog box.
11. On the VLAN, Insert Basic dialog box, click Insert.

    The Insert dialog box closes and the VLAN appears in the Basic tab.
12. Do one of the following:

    - If you are configuring an 8600 module, click Close.

      The VLAN is configured and the VLAN dialog box closes.

- If you are configuring a VLAN for an 8100 module, use one of the following procedures to configure routing:

  "Configuring an IP address for a VLAN" on page 78

  "Configuring a network address and encapsulation for a VLAN" on page 79

Configuring an IP address for a VLAN

To configure an IP address for a VLAN:

1 From the Device Manager menu bar, choose VLAN > VLANs.

The VLAN dialog box opens to the Basic tab (Figure 20 on page 75).

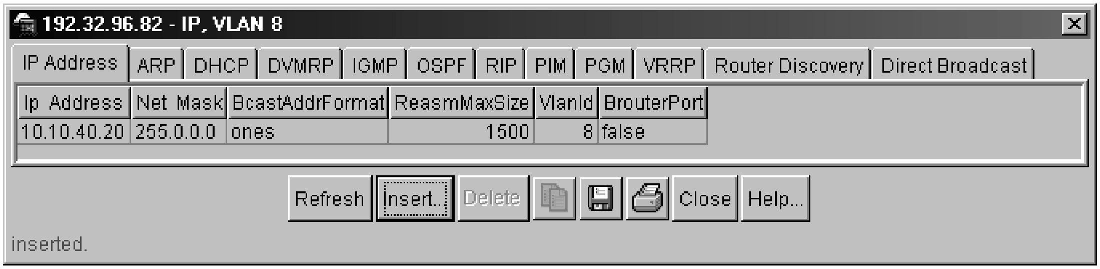
2 In the Basic tab, select the VLAN for which you are configuring an IP address.

The VLAN is highlighted.

3 Click IP.

The IP, VLAN dialog box (Figure 23) opens for the VLAN.

Figure 23 IP, VLAN dialog box



192.32.96.82 - IP, VLAN 8

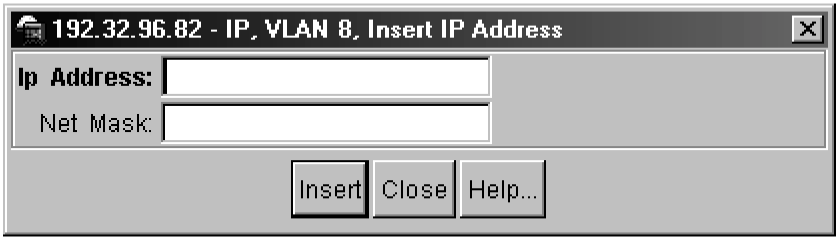
Ip Address	Net Mask	BcastAddrFormat	ReasmMaxSize	VlanId	BrouterPort
10.10.40.20	255.0.0.0	ones	1500	8	false

inserted.

4 Click Insert.

The Insert IP Address dialog box opens.

Figure 24 Insert IP Address dialog box


192.32.96.82 - IP, VLAN 8, Insert IP Address

Ip Address:

Net Mask:

5 Enter an IP address and NetMask for routing.

6 Click Insert > Close.

The Insert IP dialog box closes and the IP address and Net Mask appear in the IP, VLAN dialog box.

7 In the IP, VLAN dialog box and the VLAN dialog box, click Close.

The IP subnet-based VLAN is configured.

Configuring a network address and encapsulation for a VLAN

To configure an IPX network address and select an encapsulation method:

1 From the Device Manager menu bar, choose VLAN > VLANs.

The VLAN dialog box opens to the Basic tab (Figure 20 on page 75).

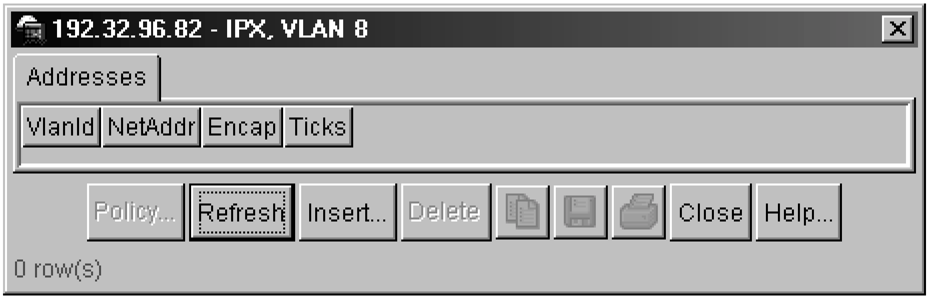
2 In the Basic tab, select the VLAN for which you are configuring a network address and encapsulation.

The VLAN is highlighted.

3 Click IPX.

The IPX, VLAN dialog box (Figure 25) opens for the VLAN.

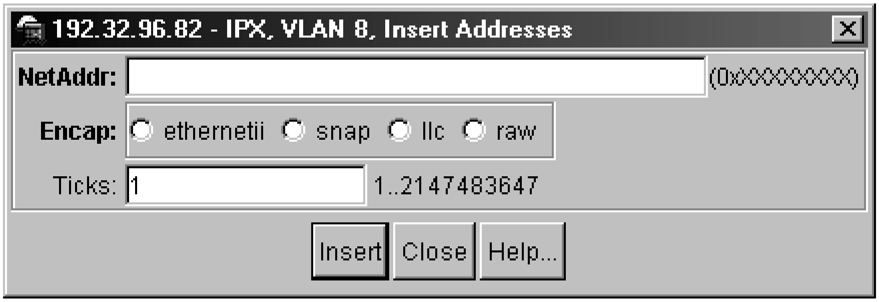
Figure 25 IPX, VLAN dialog box



4 Click Insert.

The IPX, VLAN, Insert Addresses dialog box opens.

Figure 26 IPX, VLAN, Insert Addresses dialog box



NetAddr: (0xXXXXXXXX)

Encap: ○ ethernetii ○ snap ○ llc ○ raw

Ticks: 1 1..2147483647

5 In the NetAddr field, enter a network address for routing.

6 In the Encap field, click an encapsulation method (Ethernet II, SNAP, LLC, or RAW).

7 Click Insert.

The Insert dialog box closes and the network address and encapsulation method appear in the IPX, VLAN dialog box.

8 In both the IP, VLAN dialog box and the VLAN dialog box, click Close.

The network address and encapsulation method are configured for the VLAN.

Creating a source IP subnet-based VLAN

To create a source IP subnet-based VLAN:

1. From the Device Manager menu bar, choose VLAN > VLANs.

   The VLAN dialog box opens to the Basic tab (Figure 20 on page 75).

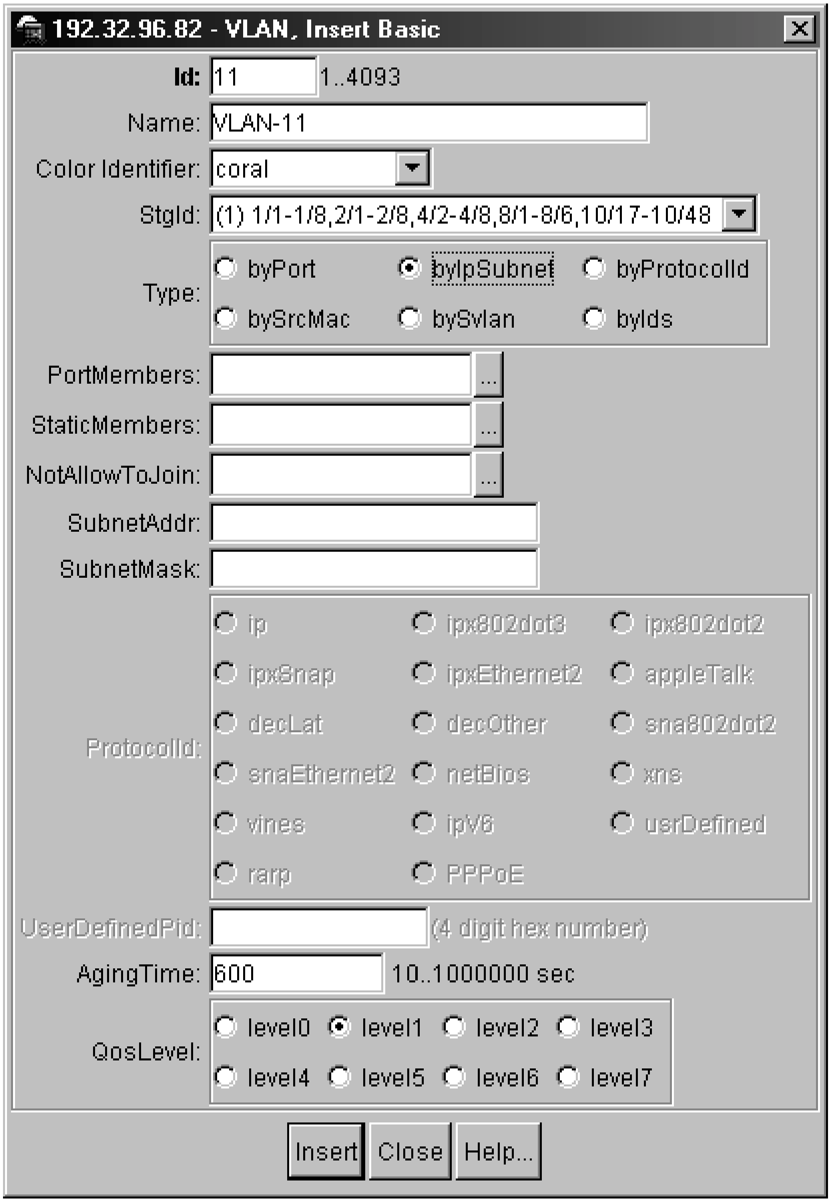
2. In the VLAN dialog box, click Insert.

   The VLAN, Insert Basic dialog box opens.

3. In the Type field, click byIpSubnet.

   The fields needed to set up IP subnet-based VLANs are activated (Figure 27).

Figure 27 VLAN, Insert Basic dialog box—for IP subnet-based VLANs



192.32.96.82 - VLAN, Insert Basic

Id: 11 1..4093

Name: VLAN-11

Color Identifier: coral

StgId: (1) 1/1-1/8,2/1-2/8,4/2-4/8,8/1-8/6,10/17-10/48

Type: ○ byPort ● byIpSubnet ○ byProtocolId ○ bySrcMac ○ bySvlan ○ byIds

PortMembers:

StaticMembers:

NotAllowToJoin:

SubnetAddr:

SubnetMask:

ProtocolId: ○ ip ○ ipx802dot3 ○ ipx802dot2 ○ ipxSnap ○ ipxEthernet2 ○ appleTalk ○ decLat ○ decOther ○ sna802dot2 ○ snaEthernet2 ○ netBios ○ xns ○ vines ○ ipV6 ○ usrDefined ○ rarp ○ PPPoE

UserDefinedPid: (4 digit hex number)

AgingTime: 600 10..1000000 sec

QosLevel: ○ level0 ● level1 ○ level2 ○ level3 ○ level4 ○ level5 ○ level6 ○ level7

4 In the ID field, type the VLAN ID.

5 (Optional) In the Name field, type the VLAN name.

If no name is entered, a default is created.

6 (Optional) In the Color Identifier field, select the color or use the color provided.

This color is used by VLAN Manager to visually distinguish the VLANs in a network.

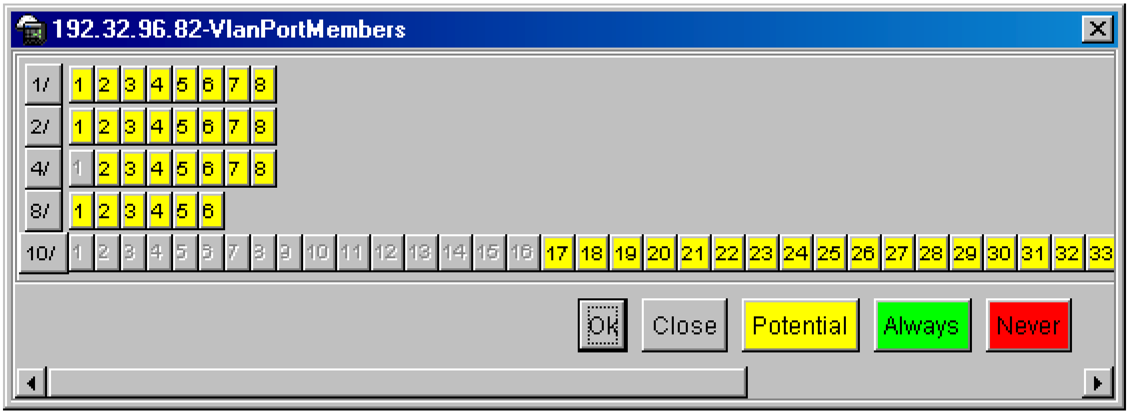
7 In the StgId field, select the spanning tree group ID of the VLAN.

8 Specify port membership by clicking the ellipsis (...) for one of the following:

- PortMembers (use this for VLAN by IpSubnet, Protocolid, or SrcMac)
- StaticMembers
- NotAllowedToJoin

The VlanPortMembers dialog box opens (Figure 28).

Figure 28 VlanPortMembers dialog box



9 Click each port to achieve the desired color:

- Yellow—Potential members, treated as always members.
- Green—Always members, static
- Red—Never members, not allowed to join

Note: In a source IP subnet-based VLAN, a potential member becomes an active member of the VLAN when a frame is received from the specified source IP address.

10 Click OK.

The Port Membership dialog box closes, and the port members appears in the VLAN, Insert Basic dialog box.

11 In the source IP subnet address field, enter an IP address for the VLAN.

12 In the IP subnet mask field, enter an IP subnet mask for the VLAN.

13 In the AgingTime field, enter the timeout period in seconds for aging out the dynamic VLAN member ports, or use the 600 second default.

14 (Optional) In the QosLevel field, click a quality of service level (0 - 7).

15 Click Insert.

The VLAN, Insert Basic dialog box closes, and the source IP subnet-based VLAN appears in the Basic tab.

Creating a protocol-based VLAN

To create a protocol-based VLAN:

1 From the Device Manager menu bar, choose VLAN > VLANs.

The VLAN dialog box opens to the Basic tab (Figure 20 on page 75).

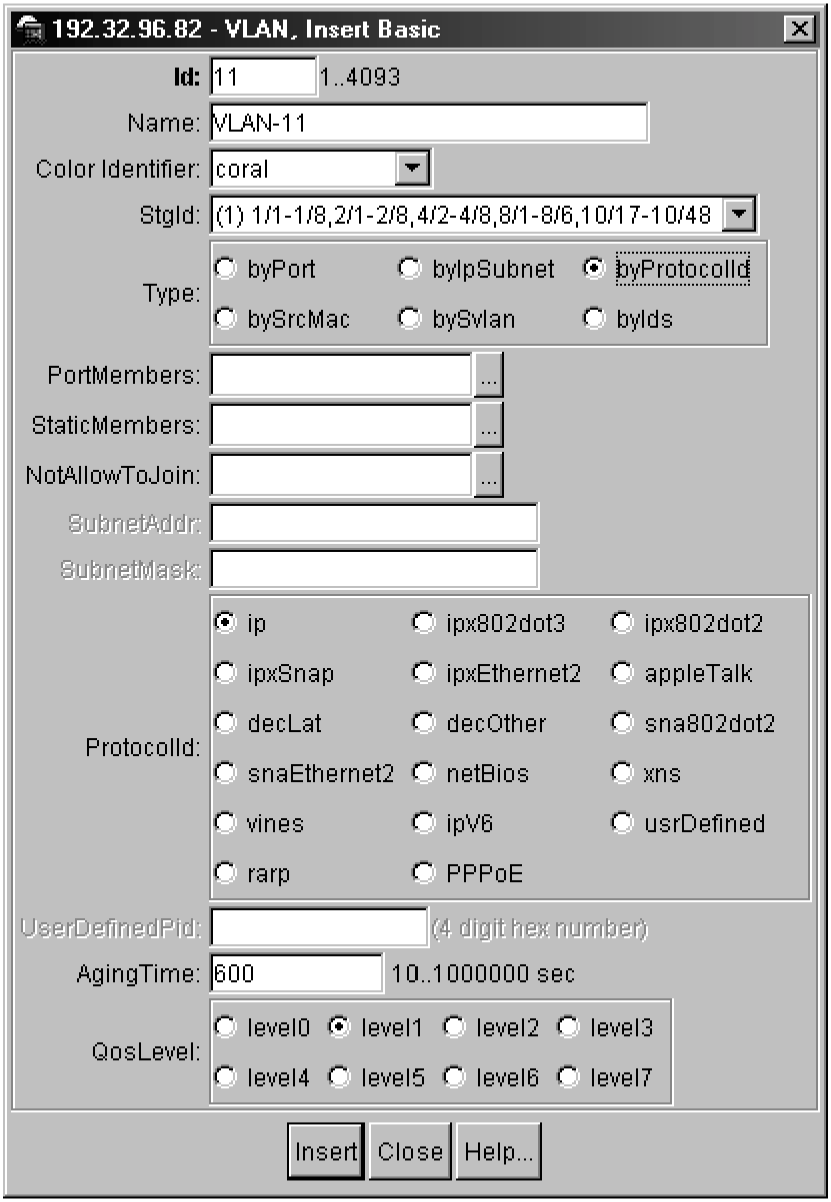
2 In the Basic tab, click Insert.

The VLAN, Insert Basic dialog box opens.

3 In the Type field, click byProtocolId.

The dialog box activates additional fields needed to set up protocol-based VLANs (Figure 29).

Figure 29 VLAN, Insert Basic dialog box—for protocol-based VLANs



192.32.96.82 - VLAN, Insert Basic

Id: 11 1..4093

Name: VLAN-11

Color Identifier: coral

StgId: (1) 1/1-1/8,2/1-2/8,4/2-4/8,8/1-8/6,10/17-10/48

Type: ○ byPort ○ byIpSubnet ● byProtocolId ○ bySrcMac ○ bySvlan ○ byIds

PortMembers:

StaticMembers:

NotAllowToJoin:

SubnetAddr:

SubnetMask:

ProtocolId: ● ip ○ ipx802dot3 ○ ipx802dot2 ○ ipxSnap ○ ipxEthernet2 ○ appleTalk ○ decLat ○ decOther ○ sna802dot2 ○ snaEthernet2 ○ netBios ○ xns ○ vines ○ ipV6 ○ usrDefined ○ rarp ○ PPPoE

UserDefinedPid: (4 digit hex number)

AgingTime: 600 10..1000000 sec

QosLevel: ○ level0 ● level1 ○ level2 ○ level3 ○ level4 ○ level5 ○ level6 ○ level7

4 In the ID field, type the unique VLAN ID, or use the ID provided.

5 (Optional) In the Name field, type the VLAN name, or use the name provided.

6 (Optional) In the Color Identifier field, select the color, or use the color provided.

This color is used by VLAN Manager to visually distinguish the VLANs in a network.

7 In the StgID field, select the spanning tree group ID of the VLAN.

8 To specify the VLAN port membership, click the ellipsis (...) for one of the following fields.

- Port Members
- StaticMembers
- NotAllowedToJoin

The VlanPortMembers dialog box opens (Figure 28 on page 83).

9 In the VlanPortMembers dialog box, click each port button to achieve the desired membership color.

- Yellow: Potential members—dynamic. Potential members are treated as always members.
- Green: Always members—static
- Red: Never members—not allowed to join

When you have two VLANs with potential members and you want to move ports from one VLAN to the other, you must first change their port membership to Never. Then you can assign the ports to the other VLAN. This requirement applies to both the 8600 modules and 8100 modules.

Note: When a protocol-based VLAN is created, all ports in the underlying STG will automatically be added as potential members if they are not already members of an existing protocol-based VLAN of the same type.
Note: In a protocol-based VLAN for an 8600 module, a potential member becomes an active member of the VLAN when a frame of the specified protocol is received.

10 Click OK.

The VlanPortMembers dialog box closes and the port members are added to the Insert Basic dialog box.

11 In the ProtocolID field, select a protocol ID.

To configure a non-standard protocol, see “Configuring user-defined protocols in protocol-based VLANs,” next.

12 Do one of the following:

- For 8100 modules, go to Step 13.
- For 8600 modules, in the AgingTime field, specify the timeout period, in seconds, for aging out the dynamic member ports of the VLAN, or use the default of 600 seconds.

13 In the QosLevel field, click a level (0-7).

14 Click Insert.

The VLAN, Insert Basic dialog box closes, and the protocol-based VLAN is added to the Basic tab of the VLAN dialog box.

15 Do one of the following:

- If you are configuring an 8600 module, click Close.

  The VLAN is configured and the VLAN dialog box closes.

- If you are configuring an 8100 module, use one of the following procedures to configure routing:

  “Configuring an IP address for a VLAN” on page 78

  “Configuring a network address and encapsulation for a VLAN” on page 79

Configuring user-defined protocols in protocol-based VLANs

You can create user-defined protocol-based VLANs in support of networks with non-standard protocols.

To create a user-defined protocol for a protocol-based VLAN:

1 From the Device Manager menu bar, choose VLAN > VLANs.

The VLAN dialog box opens to the Basic tab (Figure 20 on page 75).

2 In the VLAN dialog box, click Insert.

The VLAN, Insert Basic dialog box (Figure 30 on page 89) opens.

3 In the Type field, click byProtocolId.

4 To specify the VLAN port membership, click the ellipsis (...) for one of the following fields.

- Port Members
- StaticMembers
- NotAllowedToJoin

The VlanPortMembers dialog box opens (Figure 28 on page 83).

5 In the VlanPortMembers dialog box, click each port button to achieve the desired membership color.

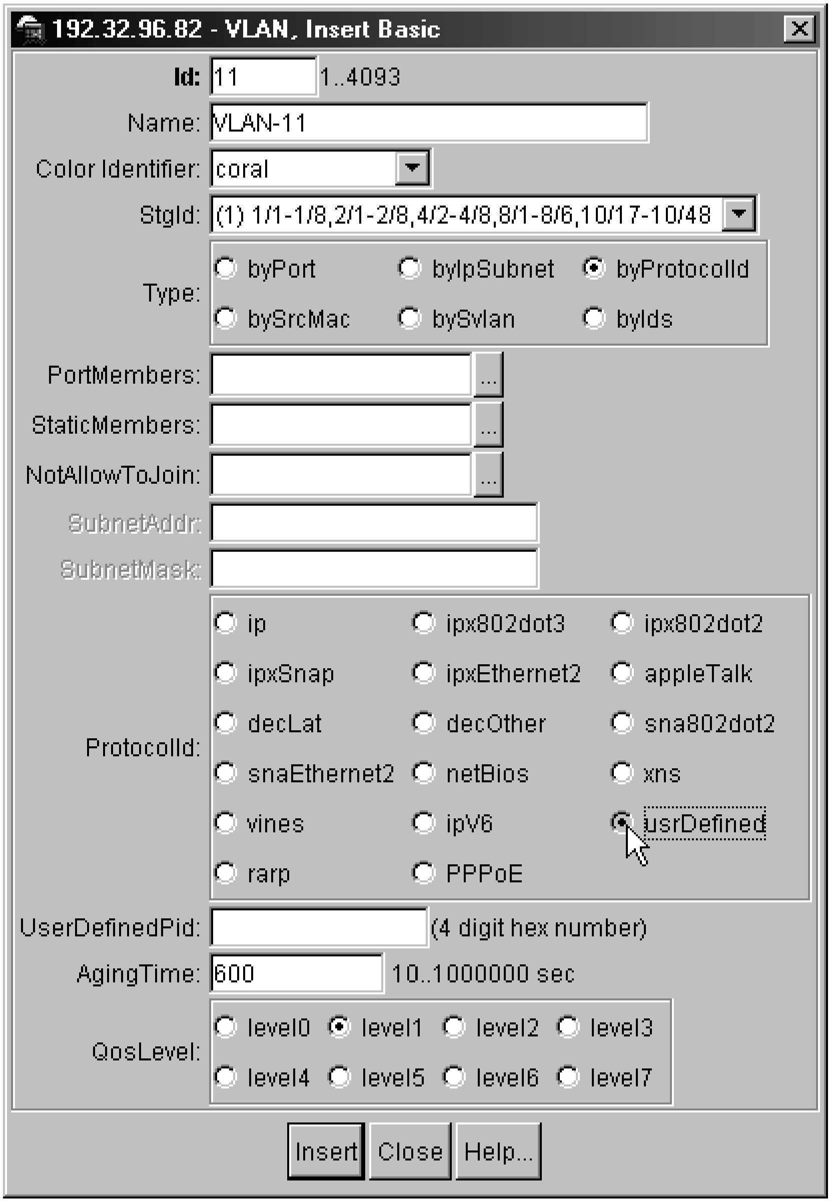
- Yellow: Potential members—dynamic. Potential members are treated as always members.
- Green: Always members—static
- Red: Never members—not allowed to join

Note: In a user-defined protocol-based VLAN on an 8600 module, a potential member becomes an active member when a frame from the specified protocol is received. On an 8100 module, all potential members are active members.

6 In the Protocolid field, click usrDefined.

The UserDefinedPID field becomes editable (Figure 30 on page 89).

Figure 30 VLAN, Insert a user-defined, protocol-based VLAN



192.32.96.82 - VLAN, Insert Basic

Id: 11 1..4093

Name: VLAN-11

Color Identifier: coral

StgId: (1) 1/1-1/8,2/1-2/8,4/2-4/8,8/1-8/6,10/17-10/48

Type: ○ byPort ○ byIpSubnet ● byProtocolId ○ bySrcMac ○ bySvlan ○ byIds

PortMembers:

StaticMembers:

NotAllowToJoin:

SubnetAddr:

SubnetMask:

ProtocolId: ○ ip ○ ipx802dot3 ○ ipx802dot2 ○ ipxSnap ○ ipxEthernet2 ○ appleTalk ○ decLat ○ decOther ○ sna802dot2 ○ snaEthernet2 ○ netBios ○ xns ○ vines ○ ipV6 ● usrDefined ○ rarp ○ PPPoE

UserDefinedPid: (4 digit hex number)

AgingTime: 600 10..1000000 sec

QosLevel: ○ level0 ● level1 ○ level2 ○ level3 ○ level4 ○ level5 ○ level6 ○ level7

7 In the UserDefinedPID field, enter the PID for the protocol in the format: 0x (protocol type in hexadecimal).

In the 8600 modules, the 16-bit PID assigned to a protocol-based VLAN specifies either an Ethertype, a DSAP/SSAP, or a SNAP PID, depending on whether the frame encapsulation is Ethernet 2, 802.2, or LLC-SNAP, respectively.

In the 8100 modules, the 16-bit PID assigned to a protocol-based VLAN only specifies an Ethertype for Ethernet 2 frame encapsulation.

The following PIDs are not valid:

- PID0x0000 through 0x05dc: overlap with the 802.3 frame length
- PIDs of predefined protocols (for example, IP, IPX, AppleTalk)
- PID 0x8100: reserved by 802.1Q to identify tagged frames
- PID0x9000: used by the diagnostic loopback frames
- PID0x8808: used by 802.3x pause frames
- PID0x4242: overlaps with the BPDU DSAP/SSAP

8 Do one of the following:

- For 8100 modules, go to Step 9.
- For 8600 modules, in the AgingTime field, specify the timeout period, in seconds, for aging out the dynamic member ports of the VLAN, or use the default of 600 seconds.

9 In the QosLevel field, click a level (0-7).

10 Click Insert.

The VLAN, Insert Basic dialog box closes, and the protocol-based VLAN is added to the Basic tab of the VLAN dialog box.

11 Click Apply > Close.

The non-standard protocol-based VLAN is configured.

Creating a source MAC address-based VLAN

Before creating a source MAC-based VLAN, you must first enable source MAC address-based VLANs in the system (f you have not done so previously).

This section includes the following topics:

- "Enabling source MAC address-based VLANs on the system" on page 91
- "Configuring a source MAC address-based VLAN" on page 93
- "Creating a source MAC address-based VLAN using batch files" on page 97

Enabling source MAC address-based VLANs on the system

To enable source MAC address-based VLANs on the system:

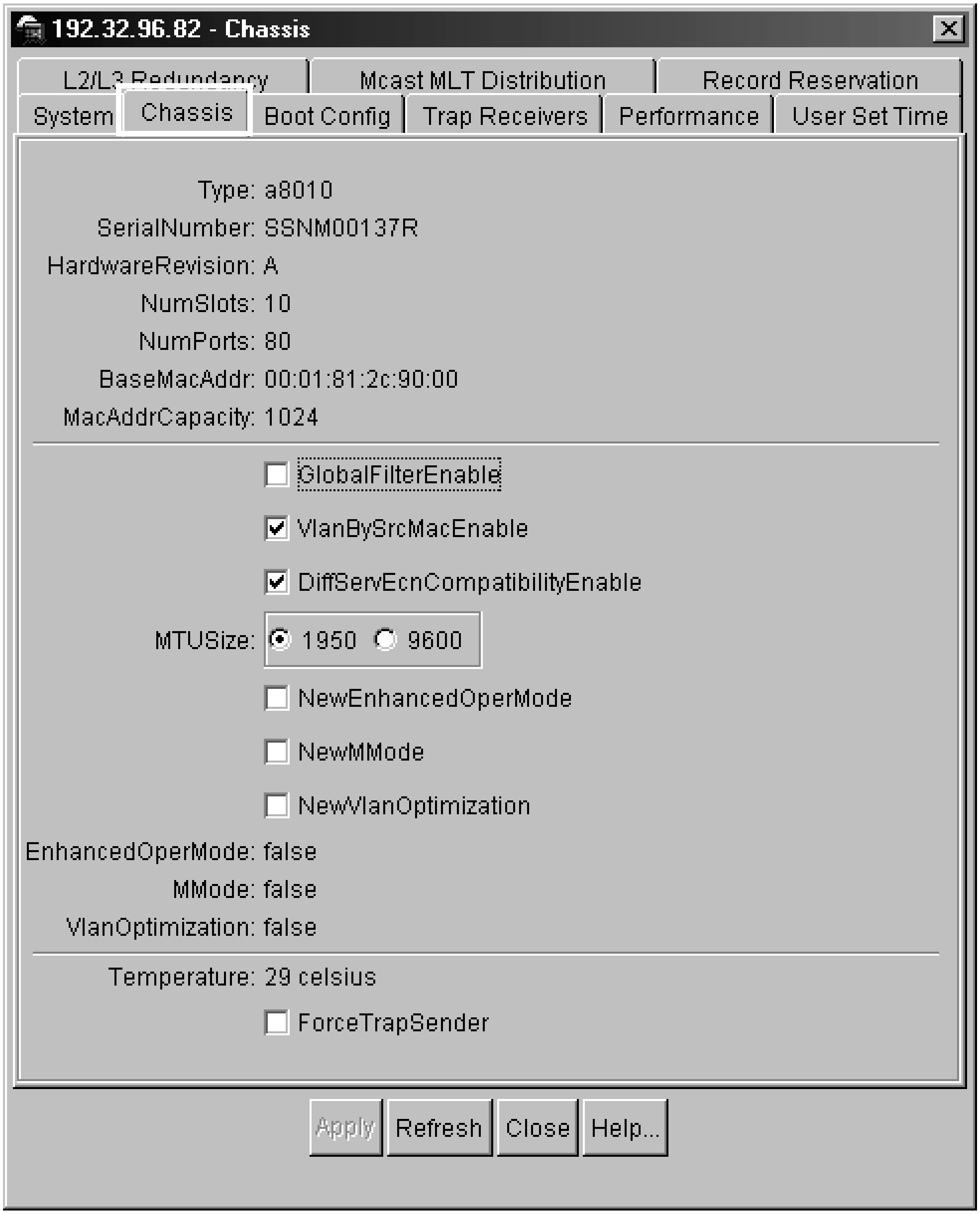
1 From the Device Manager menu bar, choose Edit > Chassis.

   The Chassis dialog box opens to the System tab.

2 Click the Chassis tab.

   The Chassis tab opens (Figure 31).

Figure 31 Chassis tab—enabling VLAN by source MAC address



Type: a8010

SerialNumber: SSNM00137R

HardwareRevision: A

NumSlots: 10

NumPorts: 80

BaseMacAddr: 00:01:81:2c:90:00

MacAddrCapacity: 1024

□ GlobalFilterEnable

☑ VlanBySrcMacEnable

☑ DiffServEcnCompatibilityEnable

MTUSize: ● 1950 ○ 9600

□ NewEnhancedOperMode

□ NewMMode

□ NewVlanOptimization

EnhancedOperMode: false

MMode: false

VlanOptimization: false

Temperature: 29 celsius

□ ForceTrapSender

3 Click GlobalFilterEnable to disable global filters in the system.

4 Click Apply.

5 Click VlanBySrcMacEnable to enable source MAC-based VLANs in the system.

6 Click Apply > Close.

The Chassis dialog box closes and source MAC address-based VLANs are enabled on the system.

Configuring a source MAC address-based VLAN

Before configuring a source MAC address-based VLAN, you must first enable source MAC address-based VLANs on the system. If you have not already done so, use the following procedure:

"Enabling source MAC address-based VLANs on the system" on page 91.

To configure a source MAC-address-based VLAN:

1 From the Device Manager menu bar, choose VLAN > VLANs.

The VLAN dialog box opens to the Basic tab (Figure 20 on page 75).

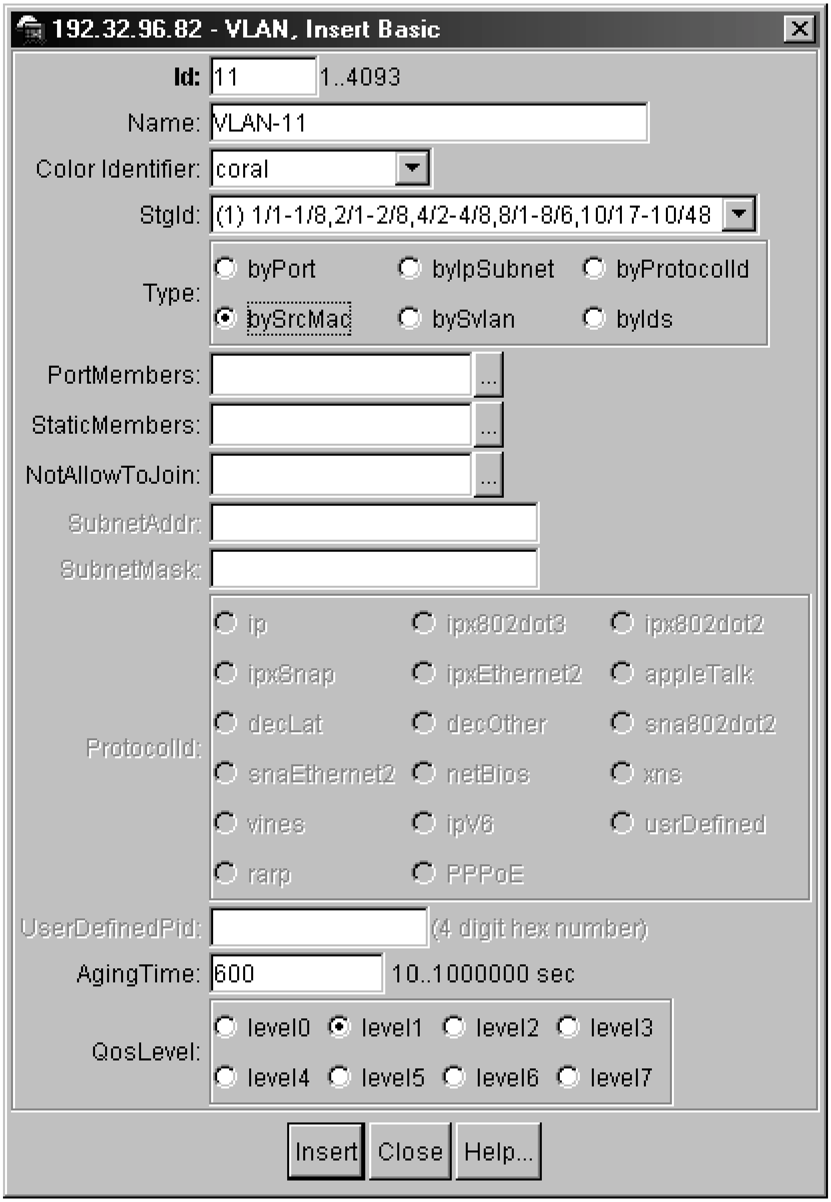
2 Click Insert.

The VLAN, Insert Basic dialog box opens (Figure 21 on page 76).

3 In the Type field, click bySrcMac.

The fields needed to set up source MAC-based VLANs become editable (Figure 32).

Figure 32 VLAN, Insert Basic dialog box—for source MAC-based VLANs



192.32.96.82 - VLAN, Insert Basic

Id: 11 1..4093

Name: VLAN-11

Color Identifier: coral

StgId: (1) 1/1-1/8,2/1-2/8,4/2-4/8,8/1-8/6,10/17-10/48

Type: ○ byPort ○ byIpSubnet ○ byProtocolId ● bySrcMac ○ bySvlan ○ byIds

PortMembers:

StaticMembers:

NotAllowToJoin:

SubnetAddr:

SubnetMask:

ProtocolId: ○ ip ○ ipx802dot3 ○ ipx802dot2 ○ ipxSnap ○ ipxEthernet2 ○ appleTalk ○ decLat ○ decOther ○ sna802dot2 ○ snaEthernet2 ○ netBios ○ xns ○ vines ○ ipV6 ○ usrDefined ○ rarp ○ PPPoE

UserDefinedPid: (4 digit hex number)

AgingTime: 600 10..1000000 sec

QosLevel: ○ level0 ● level1 ○ level2 ○ level3 ○ level4 ○ level5 ○ level6 ○ level7

4 In the ID field, type the unique VLAN ID.

5 (Optional) In the Name field, type the VLAN name, or use the one provided.

6 (Optional) In the Color Identifier field, select a color, or use the one provided.

   This color is used by VLAN Manager to visually distinguish the VLANs in a network.

7 In the StgId field, click the down arrow, and select a spanning tree group ID for the VLAN.

8 To specify the VLAN port membership, click the ellipsis (...) for one of the following fields.

   - Port Members
   - StaticMembers
   - NotAllowedToJoin

   The VlanPortMembers dialog box opens (Figure 28 on page 83).

9 Click each port until the desired color is achieved.

   - Yellow—Potential members, dynamic (Potential members are treated as always members.)
   - Green—Always members, static
   - Red—Never members, not allowed to join

10 Click OK.

   The VlanPortMembers dialog box closes, and the selected port members appear in the VLAN, Insert Basic dialog box.

11 In the Aging Time field, specify the timeout period in seconds for aging out the dynamic member ports of the VLAN, or use the default of 600 seconds.

12 (Optional) In the QosLevel field, click a quality of service level, or use the default, level 1.

13 In the VLAN, Insert Basic dialog box, click Insert.

   The VLAN, Insert Basic dialog box closes, and the VLAN appears in the Basic tab.

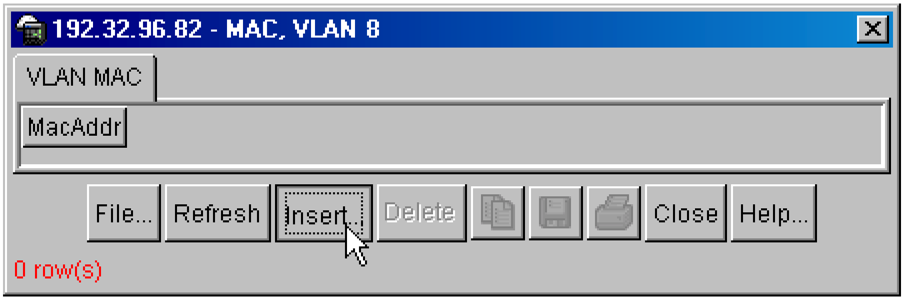
14 In the VLAN Basic tab, select the newly created VLAN.

   The VLAN is highlighted.

15 Click Mac.

   The MAC, VLAN dialog box (Figure 33) opens.

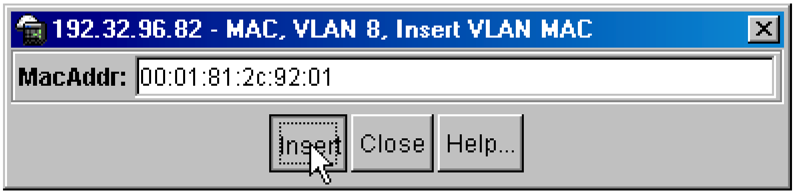
Figure 33 MAC, VLAN dialog box



16 Click Insert.

The Insert VLAN MAC dialog box opens (Figure 34).

Figure 34 Insert VLAN MAC dialog box



MacAddr: 00:01:81:2c:92:01

17 In the MacAddr field, type a source MAC address for the Vlan.

18 Click Insert.

The Insert VLAN MAC dialog box closes and the MAC address appears in the MAC, VLAN dialog box.

19 Click Close > Close.

The MAC, VLAN and VLAN dialog boxes close, and the Source MAC address-based VLAN is configured.

Note: In a source MAC-based VLAN, a potential member becomes an active member of the VLAN when a frame with the specified source MAC address is received.

Creating a source MAC address-based VLAN using batch files

Before configuring a source MAC address-based VLAN, you must first enable source MAC address-based VLANs on the system. If you have not already done so, use the following procedure:

"Enabling source MAC address-based VLANs on the system" on page 91.

To create a source MAC address-based VLAN using batch files:

1 From the Device Manager menu bar, choose VLAN > VLANs.

The VLAN dialog box opens to the Basic tab (Figure 20 on page 75).

2 Click Insert.

The VLAN, Insert Basic dialog box opens (Figure 21 on page 76).

3 In the Type field, click bySrcMac.

The fields needed to set up source MAC-based VLANs become editable (Figure 29 on page 85).

4 In the ID field, type the unique VLAN ID.

5 (Optional) In the Name field, type the VLAN name, or use the one provided.

6 (Optional) In the Color Identifier field, select a color, or use the one provided.

This color is used by VLAN Manager to visually distinguish the VLANs in a network.

7 In the StgId field, click the down arrow, and select a spanning tree group ID for the VLAN.

8 To specify the VLAN port membership, click the ellipsis (...) for one of the following fields.

- Port Members
- StaticMembers
- NotAllowedToJoin

The VlanPortMembers dialog box opens (Figure 28 on page 83).

9 Click each port until the desired color is achieved.

- Yellow—Potential members, dynamic (Potential members are treated as always members.)
- Green—Always members, static
- Red—Never members, not allowed to join

Note: In a source MAC address-based VLAN, a potential member becomes an active member of the VLAN when a frame with the specified source MAC address is received.

10 Click OK.

The VlanPortMembers dialog box closes, and the selected port members appear in the VLAN, Insert Basic dialog box.

11 In the Aging Time field, specify the timeout period, in seconds, for aging out the dynamic VLAN member ports, or use the default of 600 seconds.

12 (Optional) In the QosLevel field, click a quality of service level, or use the default, level 1.

13 Click Insert.

The VLAN, Insert Basic dialog box closes, and the VLAN appears in the Basic tab.

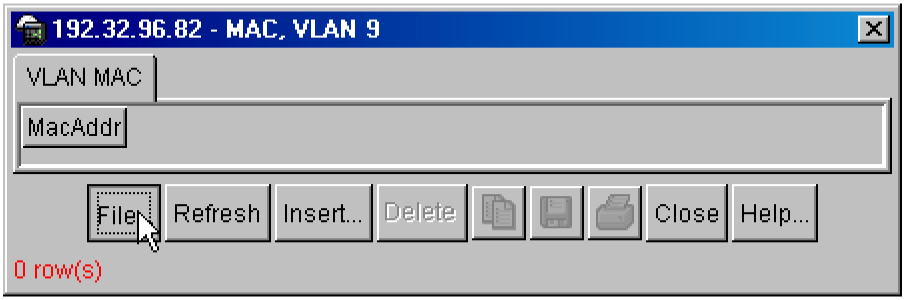
14 In the VLAN Basic tab, select the newly created VLAN.

The VLAN is highlighted.

15 Click Mac.

The MAC, VLAN dialog box (Figure 35 on page 99) opens.

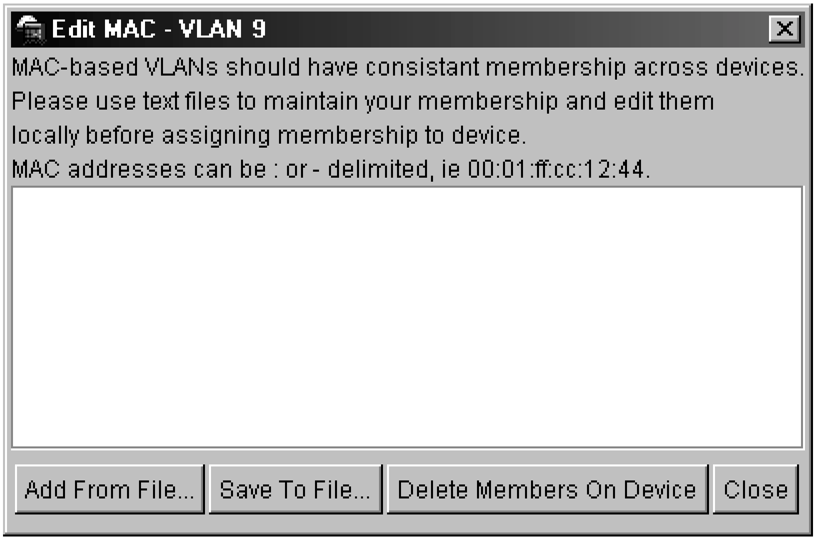
Figure 35 MAC, VLAN dialog box



16 Click File.

The Edit MAC VLAN dialog box opens (Figure 36).

Figure 36 Edit MAC VLAN dialog box



MAC-based VLANs should have consistant membership across devices.
Please use text files to maintain your membership and edit them
locally before assigning membership to device.
MAC addresses can be : or - delimited, ie 00:01:ff:cc:12:44.

17 Do one of the following:

- To add a MAC address from a file, click Add From File and use the selection dialog box to browse for the file location.
- To save a MAC address to a file, select it, click Save to File, and use the selection dialog box to browse for a save location.
- To delete a MAC address, select it, and click Delete Members on Device.

18 Click Close.

The Edit MAC dialog box closes.

19 Click Close in the MAC VLAN, and VLAN dialog boxes.

The source MAC address-based VLAN is configured.

Managing a VLAN

This section includes the following topics:

- "Changing VLAN port membership" on page 100
- "Configuring advanced VLAN features" on page 101
- "Configuring MAC address auto-learning on a VLAN" on page 105
- "Modifying auto-learned MAC addresses" on page 108

Note: After a VLAN is created, you cannot change its type. You must first delete the VLAN, and then create a new VLAN of a different type.

Changing VLAN port membership

To change a VLAN's port membership:

1 On the Device Manager menu bar, choose VLAN > VLANs.

The VLAN dialog box opens to the Basic tab (Figure 19 on page 72).

2 Double-click the PortMember field for the VLAN whose ports you want to change.

The VLAN's Port Member dialog box opens.

3 Click the port members to add or remove.

4 Click OK.

The Port Member dialog box closes and the changes appear in the Basic tab.

5 In the VLAN dialog box, click Apply > Close.

The VLAN's port membership is changed and the VLAN dialog box closes.

Configuring advanced VLAN features

The Advanced tab contains advanced fields including the Action field, which may be useful in troubleshooting.

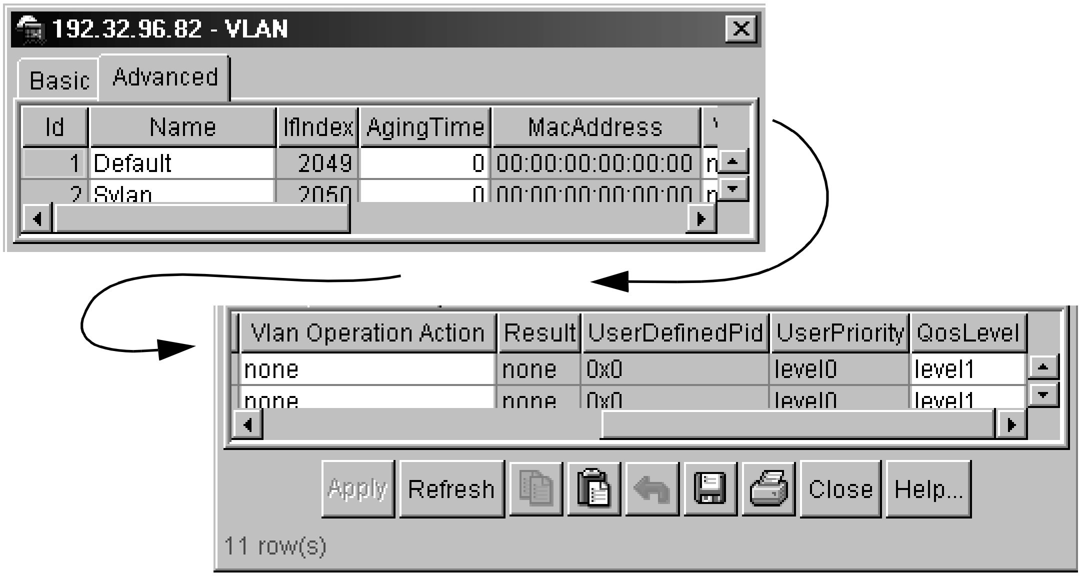
1. From the Device Manager menu bar, choose VLAN > VLANs.

   The VLAN dialog box opens to the Basic tab (Figure 19 on page 72).

2. Click the Advanced tab.

   The Advanced tab opens (Figure 37).

Figure 37 VLAN dialog box—Advanced tab



Id	Name	IfIndex	AgingTime	MacAddress
1	Default	2049	0	00:00:00:00:00:00
2	Svlan	2050	0	00:00:00:00:00:00

Vlan Operation Action	Result	UserDefinedPid	UserPriority	QosLevel
none	none	0x0	level0	level1
none	none	0x0	level0	level1

11 row(s)

Table 8 describes the VLAN Advanced tab fields.

Table 8 Advanced tab fields

Field	**Description**
Id	The VLAN ID.
Name	The name of the VLAN.
IfIndex	The logical interface index assigned to the VLAN; select a value from 2049 to 4095.

Table 8 Advanced tab fields (continued)

Field	**Description**
AgingTime	The timeout period in seconds for aging out the dynamic member ports of policy-based VLANs.
MacAddress	The MAC address assigned to the virtual router interface for this VLAN. *This field is relevant only when the VLAN is configured for routing*. This MAC address is used as the Source MAC in routed frames, ARP replies, or RIP and OSPF frames.
Vlan Operation Action	One of the following VLAN-related actions: • flushMacFdb—flush MAC forwarding table for VLAN • flushArp—flush ARP table for VLAN • flushIp—flush IP route table for VLAN • flushDynMemb—flush dynamic VLAN port members • all—flush all tables for VLAN • flushSnoopMem—flush dynamically learned multicast group membership • triggerRipUpdate—set automatic triggered updates for RIP • flushSnoopMRtr—flush learned multicast router ports
Result	Result code for action.
UserDefinedPid	User-defined protocol ID if the user has selected and defined a protocol type.
UserPriority	User-assigned priority level.
QosLevel	User-assigned Quality of Service level.

Configuring a VLAN to accept tagged or untagged frames

To configure a VLAN to accept tagged or untagged frames from a port:

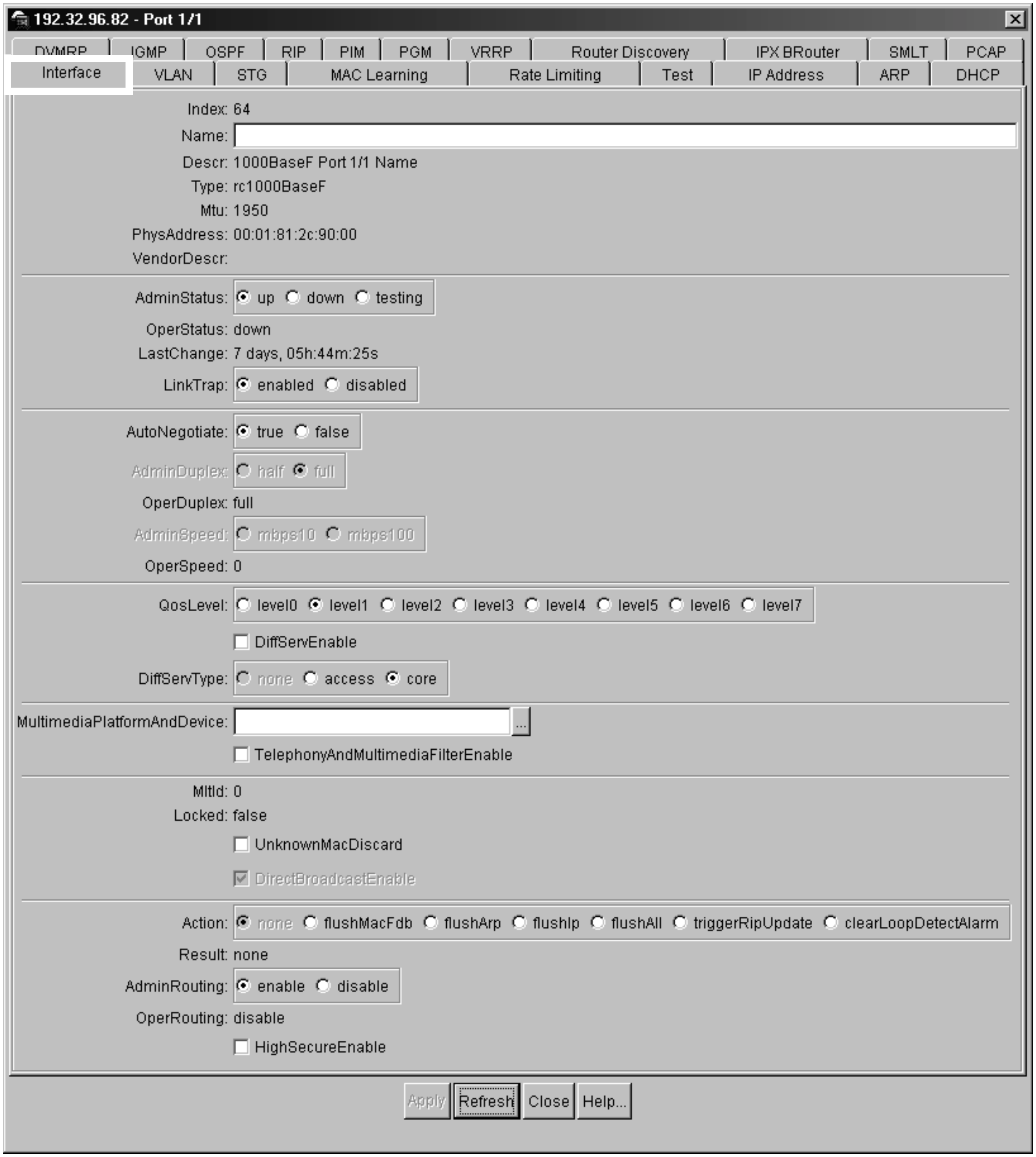
1. In the Device Manager Main window, select the port.

   The port is highlighted.

2. From the Device Manager menu bar, choose Edit > Port.

   The Port dialog box opens to the Interface tab (Figure 38). The tab label may vary, depending on the module that you selected.

Figure 38 Port dialog box—Interface tab



Index: 64

Name:

Descr: 1000BaseF Port 1/1 Name

Type: rc1000BaseF

Mtu: 1950

PhysAddress: 00:01:81:2c:90:00

VendorDescr:

AdminStatus: ● up ○ down ○ testing

OperStatus: down

LastChange: 7 days, 05h:44m:25s

LinkTrap: ● enabled ○ disabled

AutoNegotiate: ● true ○ false

AdminDuplex: ○ half ● full

OperDuplex: full

AdminSpeed: ○ mbps10 ○ mbps100

OperSpeed: 0

QosLevel: ○ level0 ● level1 ○ level2 ○ level3 ○ level4 ○ level5 ○ level6 ○ level7

□ DiffServEnable

DiffServType: ○ none ○ access ● core

MultimediaPlatformAndDevice: ...

□ TelephonyAndMultimediaFilterEnable

MltId: 0

Locked: false

□ UnknownMacDiscard

☑ DirectBroadcastEnable

Action: ● none ○ flushMacFdb ○ flushArp ○ flushIp ○ flushAll ○ triggerRipUpdate ○ clearLoopDetectAlarm

Result: none

AdminRouting: ● enable ○ disable

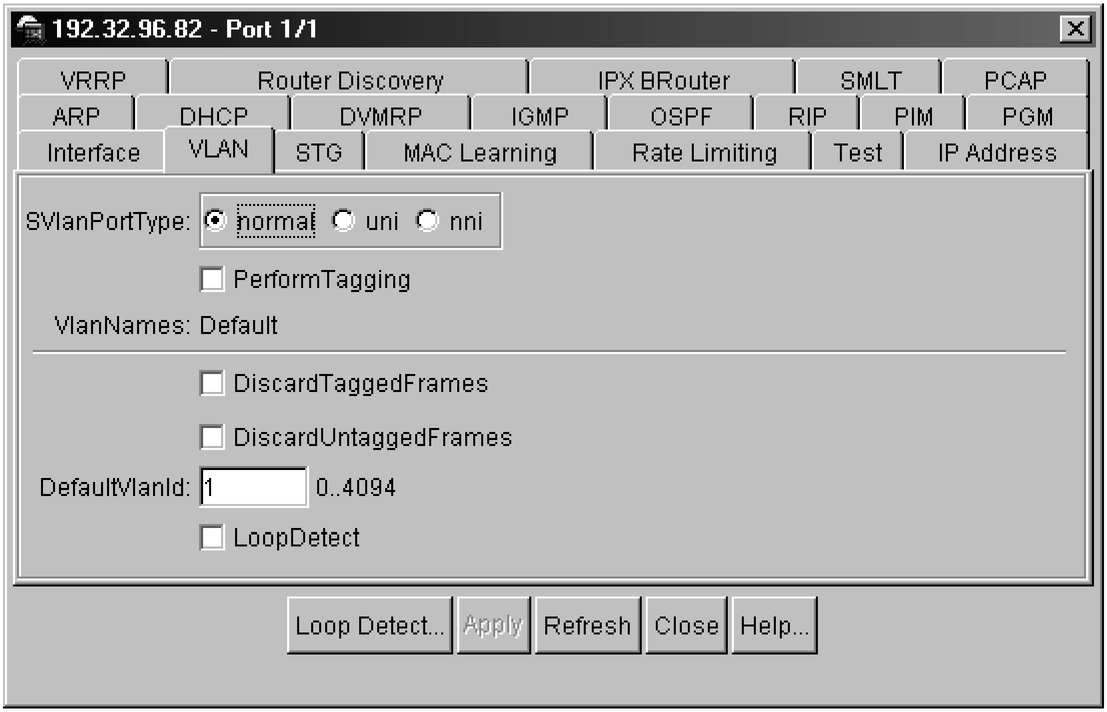
OperRouting: disable

□ HighSecureEnable

3 Click the VLAN tab.

The VLAN tab opens (Figure 39).

Figure 39 Port dialog box—VLAN tab



192.32.96.82 - Port 1/1

SVlanPortType: ● normal ○ uni ○ nni

□ PerformTagging

VlanNames: Default

□ DiscardTaggedFrames

□ DiscardUntaggedFrames

DefaultVlanId: 1 0..4094

□ LoopDetect

4 To configure tagging on the port, click the PerformTagging field. This setting is applied to all VLANs associated with the port.

If the box is checked, tagging is enabled. All frames sent from this port are tagged. You can either discard the tagged frames (go to Step 5) or forward them to a VLAN (go to Step 6).

- If the box is unchecked, tagging is disabled. The port does not send tagged frames. The switch removes the tag before sending the frame out the port. You can either discard the untagged frames (go to Step 5) or forward them to a VLAN (go to Step 6).

Note: When you enable tagging on an untagged port, the port's previous configuration of VLANs, STGs, and MLTs is lost. In addition, the port resets and runs Spanning Tree Protocol, thus breaking connectivity while the protocol goes through the normal blocking and learning states before the forwarding state.

5 Do one of the following:

- To discard tagged frames on a port for which tagging is disabled, click DiscardTaggedFrames.
- To discard untagged frames on a port for which tagging is enabled, click DiscardUntaggedFrames.

Note: To optimize performance, on untagged ports in configurations where you do not expect to see tagged frames, you should set DiscardTaggedFrames to true. However, on untagged ports for interconnecting switches, it is probably better to set DiscardTaggedFrames to false.

6 To designate a default VLAN to associate with discarded frames, enter a VLAN ID in the Default VLAN ID field (or use the default VLAN 1).

7 Click Apply > Close.

Tagging is configured for the port.

Configuring MAC address auto-learning on a VLAN

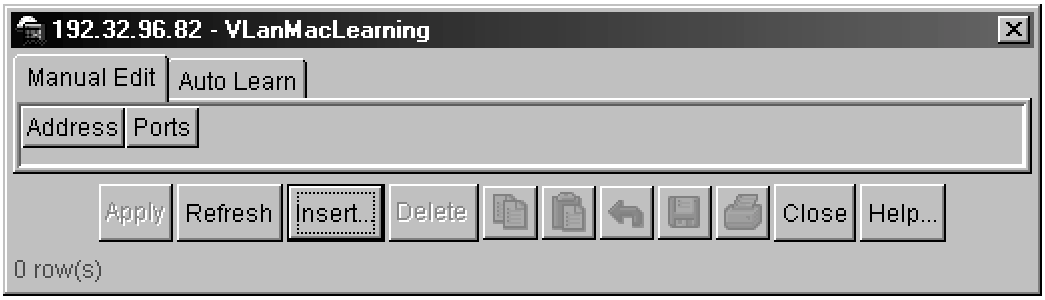
You can use MAC address auto-learning to define VLAN ports that you want to automatically learn MAC addresses.

To configure MAC address learning for a VLAN:

1 From the Device Manager menu bar, choose VLAN > MAC Learning.

The VlanMacLearning dialog box opens to the Manual Edit tab (Figure 40).

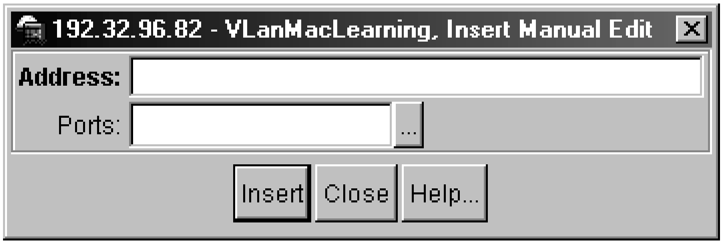
Figure 40 VlanMacLearning, Edit tab



2 Click Insert.

The VLAN MAC Learning, Insert Manual Edit dialog box opens (Figure 41).

Figure 41 VLAN MAC Learning, Insert Manual Edit dialog box

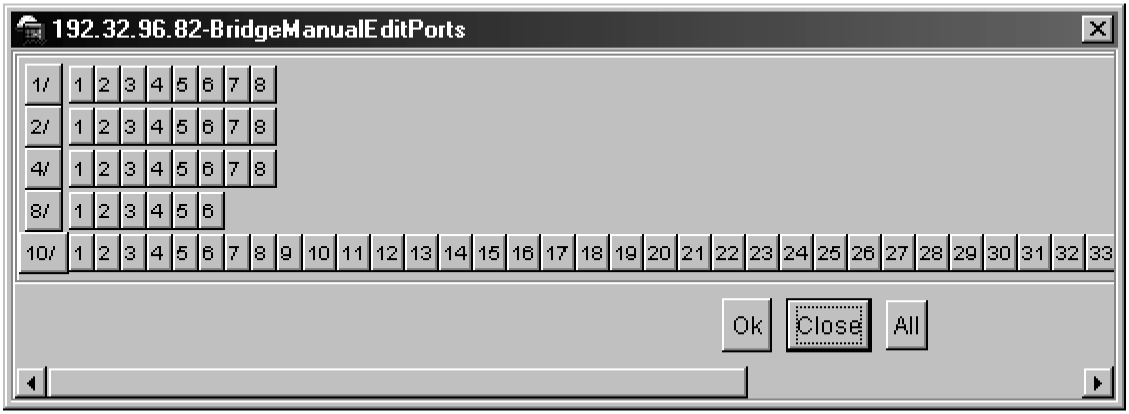


3 In the Address field, enter the source MAC address.

4 In the Ports field, click the ellipsis (...).

The BridgeManualEditPorts dialog box opens, showing the available ports (Figure 42).

Figure 42 Bridge Manual Edit Ports dialog box



5 Click the ports you want to perform the VLAN MAC learning, and click Close.

The BridgeManualEditPorts dialog box closes and the port numbers are added to the Insert Manual Edit dialog box.

6 In the Insert Manual Edit dialog box, click Insert.

The Insert Manual Edit dialog box closes and the MAC address and ports are added to the VLAN MAC Learning Manual Edit dialog box.

7 In the VLAN MAC Learning Manual Edit dialog box, click Apply > Close.

VLAN MAC learning is configured and the dialog box closes.

Table 9 describes the Insert Manual Edit tab fields.

Table 9 VLAN MAC Learning, Insert Manual Edit tab fields

Field	**Description**
Address	The source MAC address of an entry.
Ports	The allowed ports on which the MAC address of this entry are learned.

Modifying auto-learned MAC addresses

Use the Auto Learn tab to change a MAC address which has been automatically learned to one which can be manually edited.

To modify a MAC address that was automatically learned:

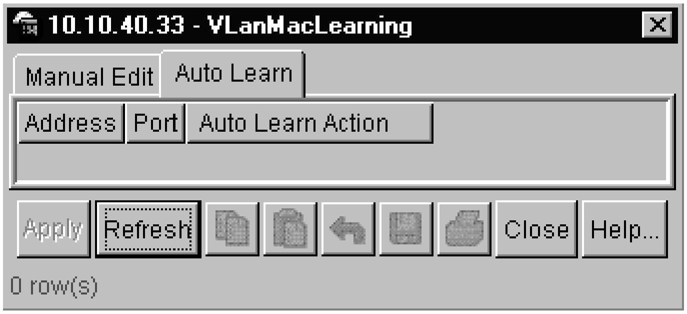
1. On the Device Manager menu bar, choose VLAN > MAC Learning.

   The VlanMacLearning dialog box opens to the Manual Edit tab (Figure 37 on page 101).

2. Click the Auto Learn tab.

   The Auto Learn tab opens (Figure 43), displaying any MAC addresses which were automatically learned.

Figure 43 VlanMacLearning dialog box—Auto Learn tab



3. Double-click in the Auto Learn Action field for the address you want to change, and select convertToManualEdit from the dropdown list.

4. Click Apply.

   The Auto Learn Action is changed.

Table 10 describes the VLAN Auto Learn tab fields.

Table 10 VLAN Auto Learn tab fields

Field	Description
Address	The source MAC address of the auto-learned entries.
Ports	The port where the MAC address was learned.
Auto Learn Action	This field is for converting an auto-learned MAC address entry to a manual edit MAC address entry. The variable provides a mechanism for you to move a MAC address entry from the auto-learned table to the Manual Edit table. Settings: • None • convertToManualEdit

Managing VLAN bridging

Bridging occurs in layer 2 of the OSI model, where only the MAC address in the packet header is considered when forwarding. With the 8000 Series switch, all bridging is done within the context of a VLAN where each VLAN has its own bridging configuration and forwarding table.

This section includes the following topics:

- "Configuring and monitoring bridging" on page 110
- "Viewing the forwarding database" on page 111
- "Clearing learned MAC addresses from the forwarding database" on page 113
- "Configuring static forwarding" on page 114
- "About MAC-layer bridge packet filtering" on page 117
- "Configuring a MAC-layer bridge filter" on page 117

Configuring and monitoring bridging

To configure and monitor bridging:

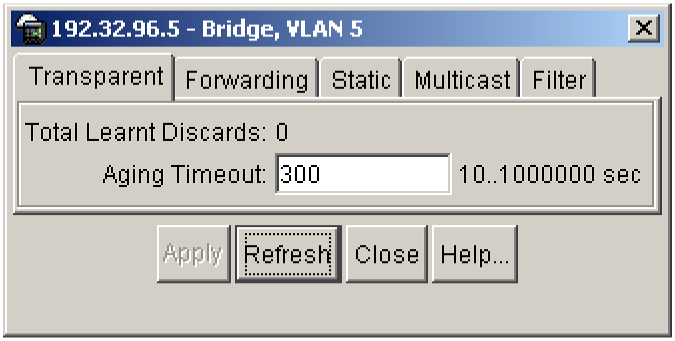
1 From the Device Manager menu bar, choose VLAN > VLANs.

  The VLAN dialog box opens to the Basic tab (Figure 20 on page 75).

2 In the VLAN dialog box, select a VLAN and click Bridge.

  The Bridge, VLAN dialog box opens to the Transparent tab (Figure 44), where you can view learned entry discards.

Figure 44 Bridge, VLAN dialog box—Transparent tab



192.32.96.5 - Bridge, VLAN 5

Total Learnt Discards: 0

Aging Timeout: 300 10..1000000 sec

3 In the Aging Timeout field, enter an interval, in seconds (10 - 1000000) for aging out dynamically learned forwarding information, or keep the default (300 seconds).

4 Click Apply > Close.

  The changes are applied and the Bridge, VLAN dialog box closes.

Table 11 describes the Transparent tab fields on the Bridge, VLAN dialog box.

Table 11 Bridge VLAN—Transparent tab fields

Field	Description
LearnedEntryDiscards	The total number of Forwarding Database entries that have been or would have been learned but have been discarded due to a lack of space in the Forwarding Database. If this counter is increasing, it indicates that the Forwarding Database is regularly becoming full (a condition that affects subnetwork performance). If this counter has a significant value but is not presently increasing, it indicates that the problem has been occurring but is not persistent.
AgingTime	The timeout period in seconds for aging out dynamically learned forwarding information.The IEEE 802.1D-1990 standard recommends a default of 300 seconds. You can assign an actual aging time up to two times the AgingTime value.

Viewing the forwarding database

The Forwarding tab shows the forwarding database for the VLAN and contains unicast information about bridge forwarding and/or filtering.This information is used by transparent bridging to determine how to forward a received frame.

To access the Forwarding tab:

1. From the Device Manager menu bar, choose VLAN > VLANs.

   The VLAN dialog box opens to the Basic tab (Figure 20 on page 75).

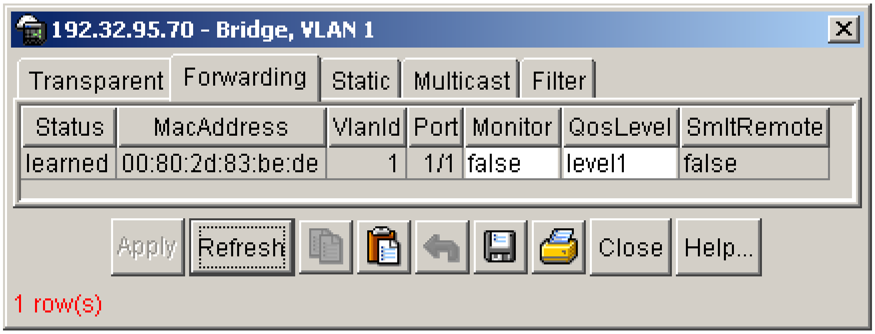
2. In the VLAN dialog box, select a VLAN and click Bridge.

   The Bridge, VLAN dialog box opens to the Transparent tab (Figure 44 on page 110).

3. Click the forwarding Forwarding tab.

   The Forwarding tab opens (Figure 45).

Figure 45 Bridge, VLAN dialog box—Forwarding tab



192.32.95.70 - Bridge, VLAN 1

Status	MacAddress	VlanId	Port	Monitor	QosLevel	SmltRemote
learned	00:80:2d:83:be:de	1	1/1	false	level1	false

1 row(s)

Table 12 describes the Bridge VLAN Forwarding tab fields.

Table 12 Bridge VLAN Forwarding tab fields

Field	Description
Status	Values include: • self—one of the bridge's addresses • learned—a learned entry that is being used • mgmt—a static entry
MacAddress	A unicast MAC address for which the bridge has forwarding and/or filtering information.
Port	Either a value of zero (0) or the port number of the port on which a frame having the specified MAC address has been seen. A value of 0 indicates a self-assigned MAC address.
Monitor	Select true or false to copy packets with a MAC address in the source or destination field. Used with port mirroring.
QosLevel	Quality of Service level.
SmltRemote	Specifies whether you want to use split multilink trunking.

Clearing learned MAC addresses from the forwarding database

For troubleshooting, you may need to manually flush the bridge forwarding database of learned MAC addresses. This operation can be done for all MAC addresses using one of the following procedures:

- “Clearing learned MAC addresses by VLAN” on page 113
- “Clearing learned MAC addresses for all VLANs by port” on page 114

Clearing learned MAC addresses by VLAN

To clear the forwarding database of learned MAC addresses for a VLAN:

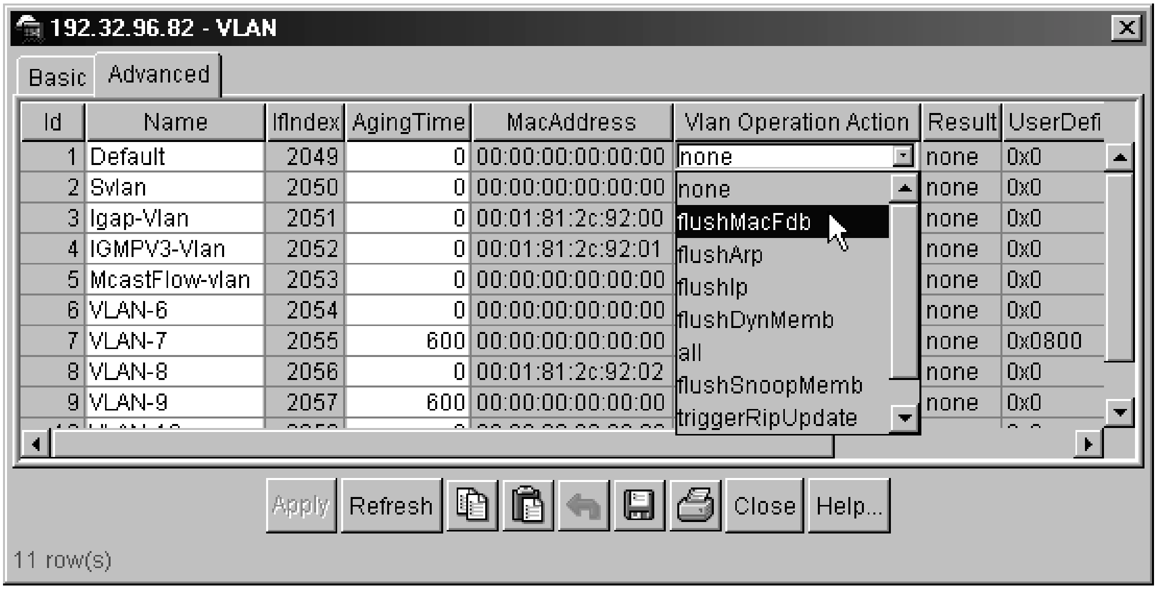
1 From the Device Manager menu bar, choose VLAN > VLANs.

The VLAN dialog box opens to the Basic tab (Figure 20 on page 75).

2 In the VLAN dialog box, click the Advanced tab.

The Advanced tab opens (Figure 46).

Figure 46 VLAN dialog box—Advanced tab—flushing the forwarding database



Id	Name	IfIndex	AgingTime	MacAddress	Vlan Operation Action	Result	UserDefi
1	Default	2049	0	00:00:00:00:00:00	none	none	0x0
2	Svlan	2050	0	00:00:00:00:00:00		none	0x0
3	Igap-Vlan	2051	0	00:01:81:2c:92:00		none	0x0
4	IGMPV3-Vlan	2052	0	00:01:81:2c:92:01		none	0x0
5	McastFlow-vlan	2053	0	00:00:00:00:00:00		none	0x0
6	VLAN-6	2054	0	00:00:00:00:00:00		none	0x0
7	VLAN-7	2055	600	00:00:00:00:00:00		none	0x0800
8	VLAN-8	2056	0	00:01:81:2c:92:02		none	0x0
9	VLAN-9	2057	600	00:00:00:00:00:00		none	0x0

11 row(s)

3 Double-click the VLAN Operation Action field, and choose FlushMacFdb from the dropdown list.

4 Click Apply.

The VLAN is set for flushing the bridge forwarding database

Clearing learned MAC addresses for all VLANs by port

To clear learned MAC addresses from the forwarding database for all VLANs by port:

1 From the Device Manager Main window, select a port.

The port is highlighted.

2 From the menu bar, choose Edit > Port.

The Port dialog box opens to the Interface tab (Figure 38 on page 103).

3 In the Action field, click FlushMacFdb.

4 Click Apply >Close.

All learned MAC addresses are cleared from the forwarding database for VLANs associated with this port.

Configuring static forwarding

The Static tab (Figure 48) contains static forwarding information configured into the bridge by local or network management specifying the set of ports to which frames received and containing specific destination addresses are allowed to be forwarded. Entries are valid for unicast and for group/broadcast addresses.

To configure forwarding information:

1 From the Device Manager menu bar, choose VLAN > VLANs.

The VLAN dialog box opens to the Basic tab (Figure 20 on page 75).

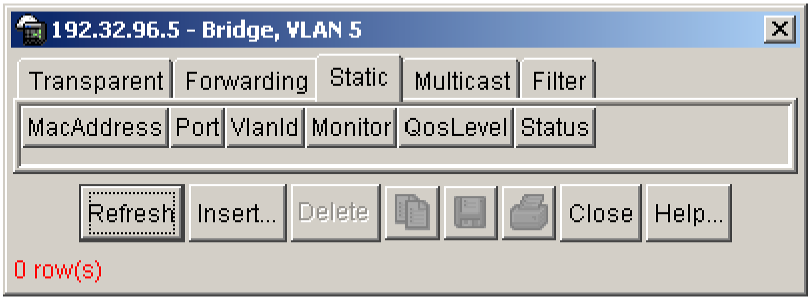
2 In the VLAN dialog box, select a VLAN and click Bridge.

The Bridge, VLAN dialog box opens (Figure 44 on page 110).

3 In the Bridge, VLAN dialog box, click the Static tab.

The Static tab is displayed (Figure 47).

Figure 47 Bridge, VLAN—Static tab

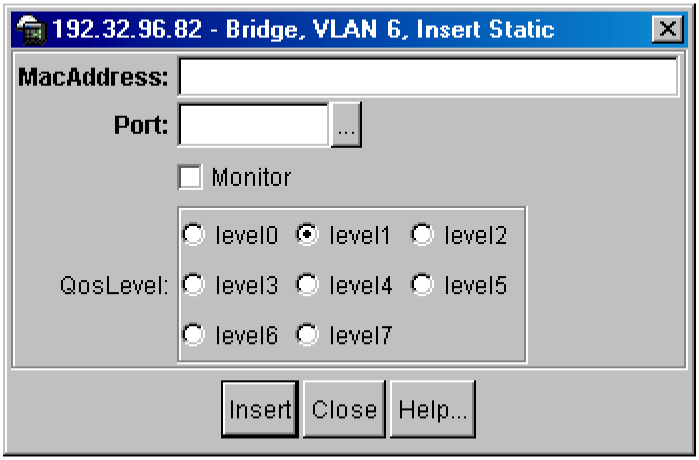


0 row(s)

4 In the Static tab, click Insert.

The Bridge, VLAN Insert Static dialog box opens (Figure 48).

Figure 48 Bridge, VLAN Insert Static dialog box



MacAddress:

Port: ...

□ Monitor

QosLevel: ○ level0 ● level1 ○ level2 ○ level3 ○ level4 ○ level5 ○ level6 ○ level7

5 In the MacAddress field, enter a forwarding destination MAC address.

6 In the Port field, click the ellipsis (...).

The Bridge Static Port dialog box opens.

7 Select the port on which the frame is received.

8 Click OK.

The Bridge Static Port dialog box closes and the selected port appears in the Insert Static dialog box.

9 To copy packets with a MAC address in the source or destination field, click Monitor.

10 In the QoS field, click a quality of service level (0 - 8), or keep the default, level 1.

11 Click Insert.

The Insert Static dialog box closes and the static information appears in the Bridge, VLAN Static tab.

12 Click Close.

The static forwarding information is configured, and the Bridge VLAN dialog box closes.

Table 13 describes the bridge, VLAN static fields.

Table 13 Bridge VLAN static fields

Field	**Description**
MacAddress	The destination MAC address in a frame to which this entry's forwarding information applies. This object can take the value of a unicast address.
Port	The port number of the port on which the frame is received.
Monitor	Setting to copy packets with a MAC address in the source or destination field. Used with port mirroring. In Static tab, display = true or false.
Status	In the Static tab, displays the status of this entry. Select one of the following values: • permanent—in use and will remain so after the next bridge reset. This is the default value. • deleteOnReset—in use and will remain so until the next bridge reset. • deleteOnTimeout—currently in use and will remain so until it is aged. • other—in use but the conditions under which it will remain so are different from other values.
QosLevel	Quality of Service level.

About MAC-layer bridge packet filtering

To perform MAC-layer bridging, the switch must know the destination MAC-layer address of each device on each attached network so it can forward packets to the appropriate destination. MAC-layer addresses are then stored in the bridging table, and you can filter packet traffic based on the destination MAC-layer address information.

The MAC filtering supported in the 8000 Series switch is the Bridge MIB filtering (RFC 1493). The number of MAC filters is limited to 100. You create a filter entry in much the same way as you create a static MAC entry, by entering a MAC address and the port on which it resides. In the MAC filter record, you also specify which ports for which to discard source or destination packets for the MAC address on a port.

Configuring a MAC-layer bridge filter

To configure a MAC layer bridge filter:

1. From the Device Manager menu bar, choose VLAN > VLANs.

   The VLAN dialog box opens to the Basic tab (Figure 20 on page 75).

2. In the VLAN dialog box, select a VLAN and click Bridge.

   The Bridge, VLAN dialog box opens (Figure 44 on page 110).

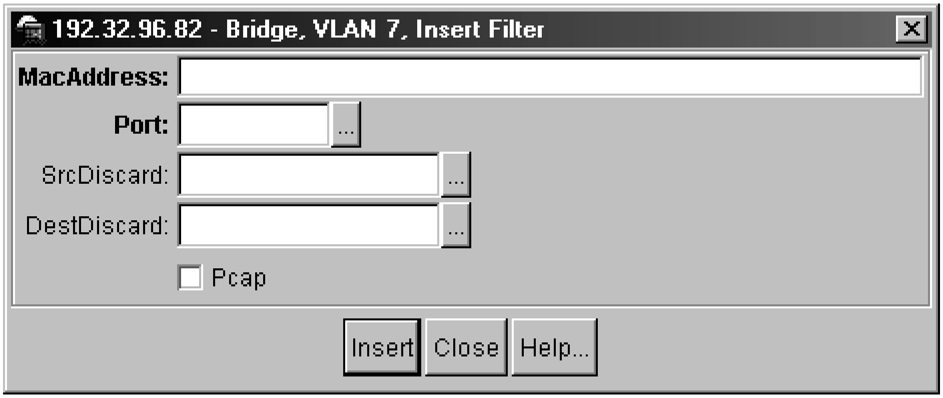
3. In the Bridge, VLAN dialog box, click the Filter tab.

   The Filter tab opens.

4. From the Filter tab, click Insert.

   The Bridge, VLAN Insert Filter dialog box opens (Figure 49).

Figure 49 Bridge, VLAN Insert Filter dialog box



5 In the MacAddress field, enter the MAC address used to match the destination address of incoming packets.

6 In the Port field, click the ellipsis (...)

The BridgeFilterPort dialog box opens.

7 Click the port where this MAC address is found, and click OK.

The BridgeFilterPort dialog box closes and the port is added to the Port field on the Bridge, VLAN, Insert Filter dialog box.

8 In the Source Discard field, click the ellipsis (...).

The Bridge Filter Source Discard dialog box opens.

9 Click the ports from which you do not want packet traffic received by this MAC address, and click OK.

The dialog box closes and the ports are added to the Source Discard field in the Bridge, VLAN, Insert Filter dialog box.

10 In the Destination Discard field, click the ellipsis (...).

The Bridge Filter Destination Discard dialog box opens.

11 Click the ports to which you do not want packet traffic sent from this MAC address, and click OK.

The dialog box closes and the ports are added to the Destination Discard field in the Bridge, VLAN, Insert Filter dialog box.

12 Click Insert.

The Insert Filter dialog box closes and the filter appears in the Filter tab.

13 In the Bridge VLAN dialog box and the VLAN dialog box, click Close.

The MAC layer bridge filter is configured.

Table 14 describes the Bridge VLAN Filter fields.

Table 14 Bridge, VLAN, Filter fields

Field	Description
MacAddress	The MAC address of this entry. This address is used to match the destination address of incoming packets.
Port	Port on which this MAC address is found.
SrcDiscard	Specify a set of ports. Traffic arriving on any of the specified ports is not forwarded to this MAC address.
DestDiscard	Specify a set of ports. Traffic arriving on any of the specified ports from this MAC address is discarded.
Pcap	Enable or disable the packet capture tool (PCAP) for the MAC address (fdb filter). For more information about PCAP, see the publication *Using the Packet Capture Tool*, part number 315023.

Configuring directed broadcast on a VLAN

You can enable or disable directed broadcast traffic forwarding for an IP-interface on the Direct Broadcast tab.

To configure IP-directed broadcast for a VLAN:

1 From the Device Manager menu bar, choose VLAN > VLANs.

The VLAN dialog box opens to the Basic tab (Figure 20 on page 75).

2 Select a VLAN.

The VLAN is highlighted.

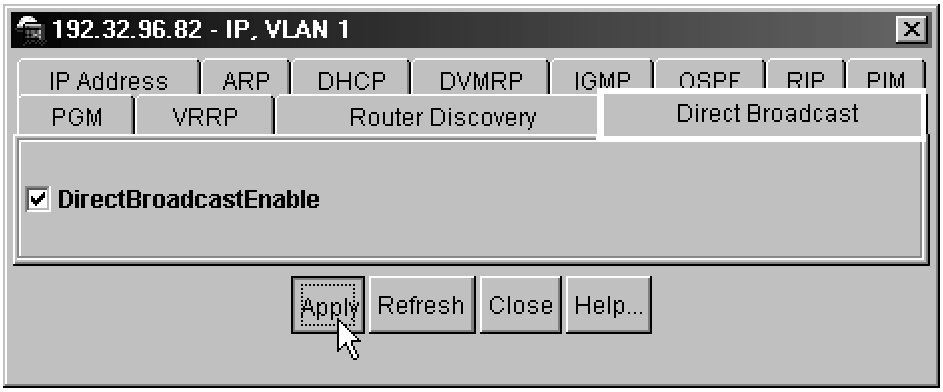
3 Click IP.

The IP, VLAN dialog box opens to the IP Address tab.

4 Click the Direct Broadcast tab.

The Direct Broadcast tab opens (Figure 50).

Figure 50 IP, VLAN dialog box—Direct Broadcast tab



☑ DirectBroadcastEnable

5 Click DirectBroadcastEnable.

- If checked, IP-directed broadcasts are enabled.
- If unchecked, IP-directed broadcasts are suppressed.

Note: Multiple VLANs/IRPs in the same subnet but in different switches must be configured simultaneously.

6 Click Apply > Close.

Directed broadcast is configured for the VLAN.

Table 15 describes the Direct Broadcast tab.

Table 15 IP, VLAN Direct Broadcast tab

Field	**Description**
DirectBroadcastEnable	If enabled, an Isolated Routing Port (IRP) can forward directed broadcast traffic. A directed broadcast is a frame sent to the subnet broadcast address on a remote IP subnet. By disabling or suppressing directed broadcast on an interface, all frames sent to the subnet broadcast address for a local router interface are dropped. Disabling this function protects a host from possible denial of service (DOS) attacks. **Note**: This feature is enabled by default. With the feature enabled, the CPU does not receive a copy of the directed broadcast. As a result, the switch does not respond to a subnet broadcast ping sent from a remote subnet.

Configuring Enhanced Operation mode

For more information about Enhanced Operation, see "About MultiLink trunking and VLAN scalability" on page 40.

To enable Enhanced Operation mode:

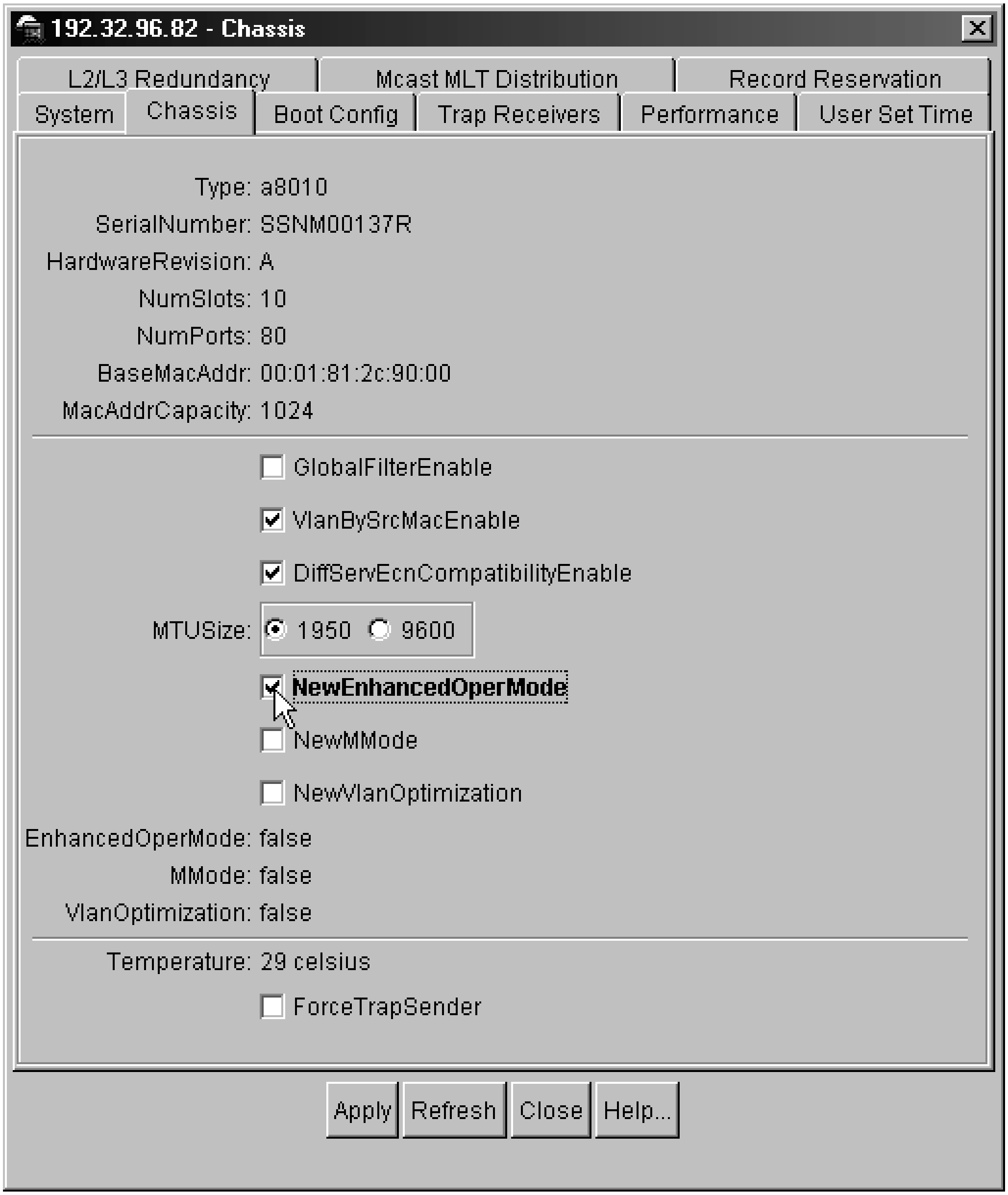
1 From the Device Manager menu bar, choose Edit > Chassis.

The Chassis dialog box opens to the System tab.

2 Click the Chassis tab.

The Chassis tab opens (Figure 51).

Figure 51 Chassis dialog box — Chassis tab



Type: a8010
SerialNumber: SSNM00137R
HardwareRevision: A
NumSlots: 10
NumPorts: 80
BaseMacAddr: 00:01:81:2c:90:00
MacAddrCapacity: 1024

□ GlobalFilterEnable
☑ VlanBySrcMacEnable
☑ DiffServEcnCompatibilityEnable

MTUSize: ● 1950 ○ 9600

☑ NewEnhancedOperMode
□ NewMMode
□ NewVlanOptimization

EnhancedOperMode: false
MMode: false
VlanOptimization: false

Temperature: 29 celsius

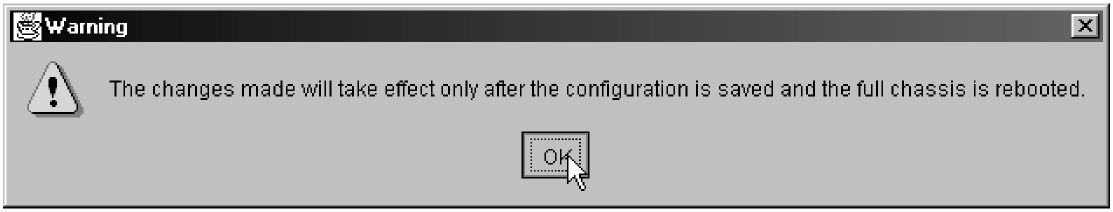
□ ForceTrapSender

3 Click the NewEnhancedOperMode field.

4 Click Apply.

The system notifies you that the setting will take effect after save and reboot.

Figure 52 Chassis configuration change notification



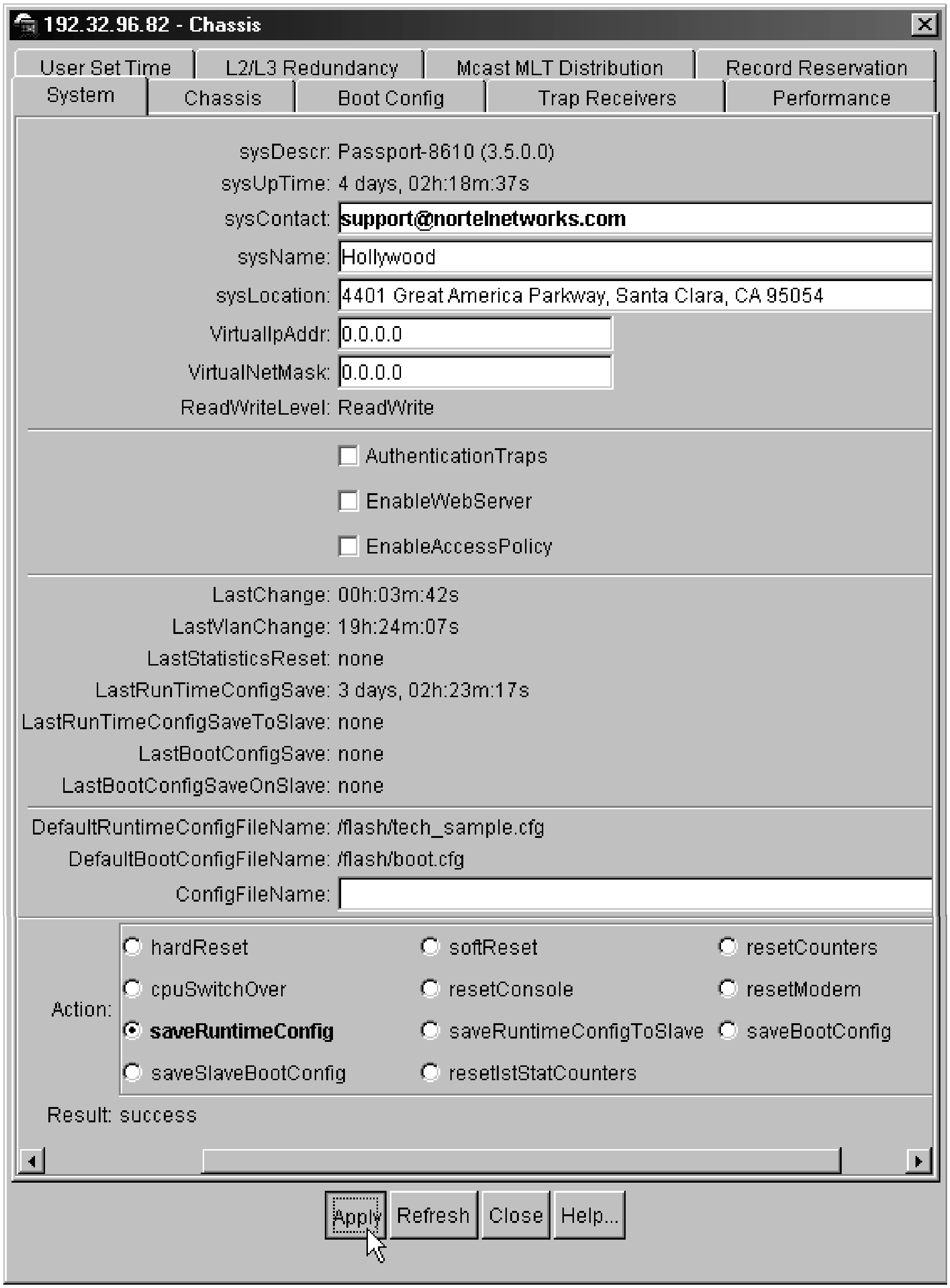
The changes made will take effect only after the configuration is saved and the full chassis is rebooted.

5 Click OK.

6 Click the System tab.

The System tab opens (Figure 53).

Figure 53 Chassis—System tab



sysDescr: Passport-8610 (3.5.0.0)
sysUpTime: 4 days, 02h:18m:37s
sysContact: **support@nortelnetworks.com**
sysName: Hollywood
sysLocation: 4401 Great America Parkway, Santa Clara, CA 95054
VirtualIpAddr: 0.0.0.0
VirtualNetMask: 0.0.0.0
ReadWriteLevel: ReadWrite

□ AuthenticationTraps
□ EnableWebServer
□ EnableAccessPolicy

LastChange: 00h:03m:42s
LastVlanChange: 19h:24m:07s
LastStatisticsReset: none
LastRunTimeConfigSave: 3 days, 02h:23m:17s
LastRunTimeConfigSaveToSlave: none
LastBootConfigSave: none
LastBootConfigSaveOnSlave: none

DefaultRuntimeConfigFileName: /flash/tech_sample.cfg
DefaultBootConfigFileName: /flash/boot.cfg
ConfigFileName:

Action:
○ hardReset ○ softReset ○ resetCounters
○ cpuSwitchOver ○ resetConsole ○ resetModem
● **saveRuntimeConfig** ○ saveRuntimeConfigToSlave ○ saveBootConfig
○ saveSlaveBootConfig ○ resetIstStatCounters

Result: success

7 In the Action field, click saveRuntimeConfig.

8 Click Apply > Close.

Enhanced mode is configured.

Caution: When enhanced operation mode is enabled, only 8600 E-modules are initialized (non E-modules are placed offline). To avoid losing modules and network connectivity, either replace any non-E-modules or move the network connections to a E-module.

Chapter 3 Configuring sVLAN using Device Manager

This section describes using Device Manager to configure sVLAN on an 8600 module or an 8100 module and includes the following topics:

Stacked VLAN configuration overview

The stacked VLAN (sVLAN) protocol transparently transports packets through an sVLAN domain by adding an additional 4-byte header to each packet. For more information, see "About stacked VLANs" on page 42.

Follow these steps to configure an sVLAN using Device Manager:

Note: You must follow these steps in sequence to configure an sVLAN.

1. Change the Ether type and set the switch level to a 1 or above.

   For more information, see page 128, "Setting the sVLAN Ethertype and switch level."

2. Configure UNI and NNI ports.

   For more information, see page 130, "Setting the sVLAN port type"

3. Create a STG of type sVLAN.

   For more information, see page 134, "Creating an sVLAN STG."

4 Create a VLAN of type sVLAN within the STG created in Step 3 and add ports to it.

For more information, see page 136, "Creating an sVLAN."

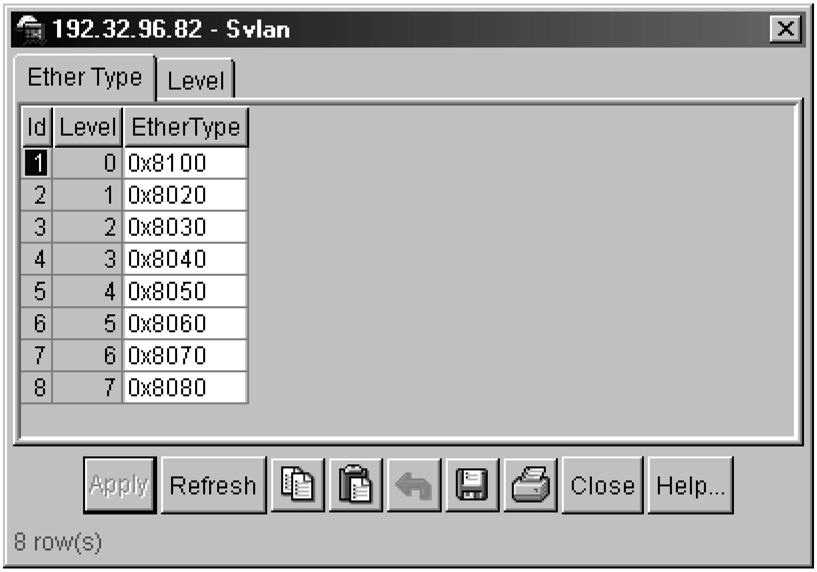
Setting the sVLAN Ethertype and switch level

To configure the sVLAN Ethertype and switch level for the switch:

5 From the Device Manager menu bar choose VLAN > sVLAN.

The sVLAN dialog box opens to the Ether Type tab (Figure 54), displaying the ether types used for sVLAN tagging.

Figure 54 sVLAN dialog box- Ether Type tab



Id	Level	EtherType
1	0	0x8100
2	1	0x8020
3	2	0x8030
4	3	0x8040
5	4	0x8050
6	5	0x8060
7	6	0x8070
8	7	0x8080

6 Do one of the following:

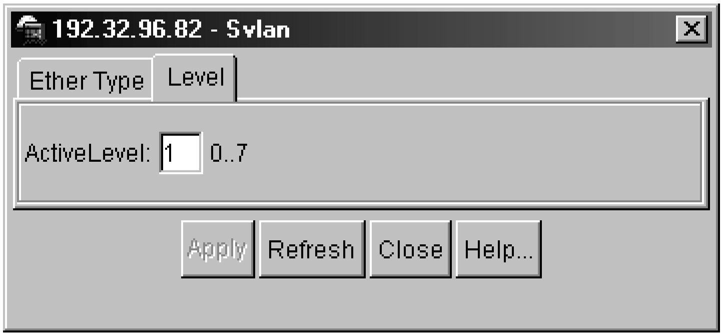
- Use the default Ether Type-Switch Level mapping and continue to Step 7.
- To modify an Ethertype, double-click an EtherType field, enter a new value, and click Apply.

  The Ethertype is changed.

7 Click the Level tab.

The Level tab opens (Figure 55).

Figure 55 sVLAN dialog box- Level tab



ActiveLevel: 1 0..7

8 In the Active Level field, enter an active switch level (1 - 7).

Note: The switch level default of 0 must be changed to a value of 1 through 7 before configuring UNI or NNI ports.

9 Click Apply.

The Ethertype and active switch level associated are configured.

Table 16 describes the sVLAN Ether Type tab.

Table 16 sVLAN—Ether Type tab

Field	**Description**
Id	Index ID for this row in the table of switch levels.

Table 16 sVLAN—Ether Type tab (continued)

Field	Description
Level	The switch level associated with this entry.
EtherType	Specifies the Ether type used for sVLAN tagging. The following are the default Ether types and switch levels: • Level 0 — 0x8100 (Ethertype defined by IEEE for 802.1Q tagged frames) • Level 1 — 0x8020 • Level 2 — 0x8030 • Level 3 — 0x8040 • Level 4 — 0x8050 • Level 5 — 0x8060 • Level 6 — 0x8070 • Level 7 — 0x8080

Table 17 describes the sVLAN Level tab.

Table 17 sVLAN—Level tab

Field	Description
Active Level	Specify the active level (0 - 7) for the switch. The default is Level 0. **Note**: You must configure the switch level to 1 or above before configuring UNI or NNI ports.

Setting the sVLAN port type

Note: You must change the switch level to 1 or above before you configure UNI or NNI ports. See "Setting the sVLAN Ethertype and switch level" on page 128."

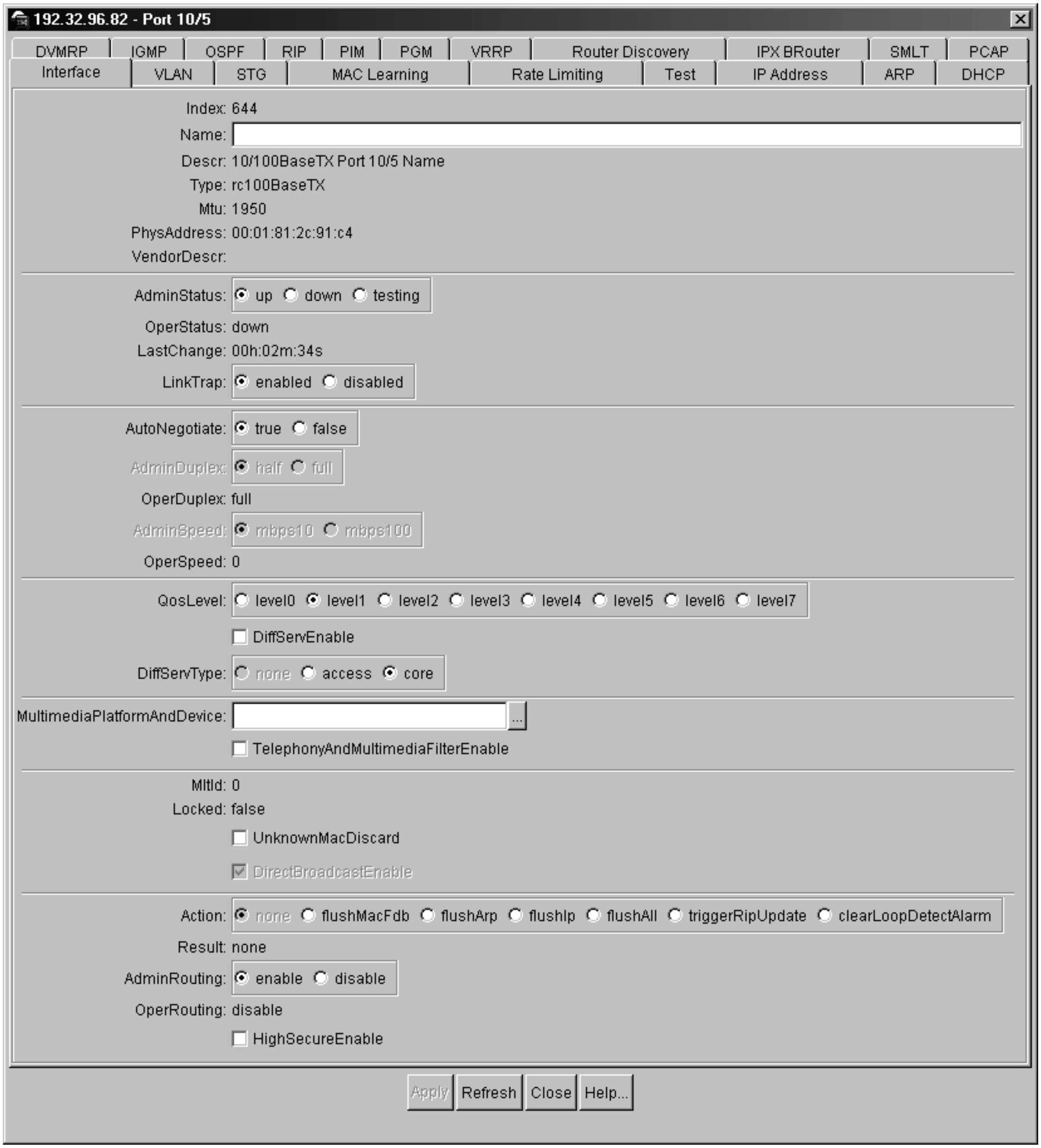
To set the sVLAN port type:

1 From the device view, select the port.

2 From the Device Manager menu bar, choose Edit > Port.

The Port dialog box opens to the Interface tab (Figure 56).

Figure 56 Port dialog box -- Interface tab



Index: 644

Name:

Descr: 10/100BaseTX Port 10/5 Name

Type: rc100BaseTX

Mtu: 1950

PhysAddress: 00:01:81:2c:91:c4

VendorDescr:

AdminStatus: ● up ○ down ○ testing

OperStatus: down

LastChange: 00h:02m:34s

LinkTrap: ● enabled ○ disabled

AutoNegotiate: ● true ○ false

AdminDuplex: ● half ○ full

OperDuplex: full

AdminSpeed: ● mbps10 ○ mbps100

OperSpeed: 0

QosLevel: ○ level0 ● level1 ○ level2 ○ level3 ○ level4 ○ level5 ○ level6 ○ level7

□ DiffServEnable

DiffServType: ○ none ○ access ● core

MultimediaPlatformAndDevice: ...

□ TelephonyAndMultimediaFilterEnable

MltId: 0

Locked: false

□ UnknownMacDiscard

☑ DirectBroadcastEnable

Action: ● none ○ flushMacFdb ○ flushArp ○ flushIp ○ flushAll ○ triggerRipUpdate ○ clearLoopDetectAlarm

Result: none

AdminRouting: ● enable ○ disable

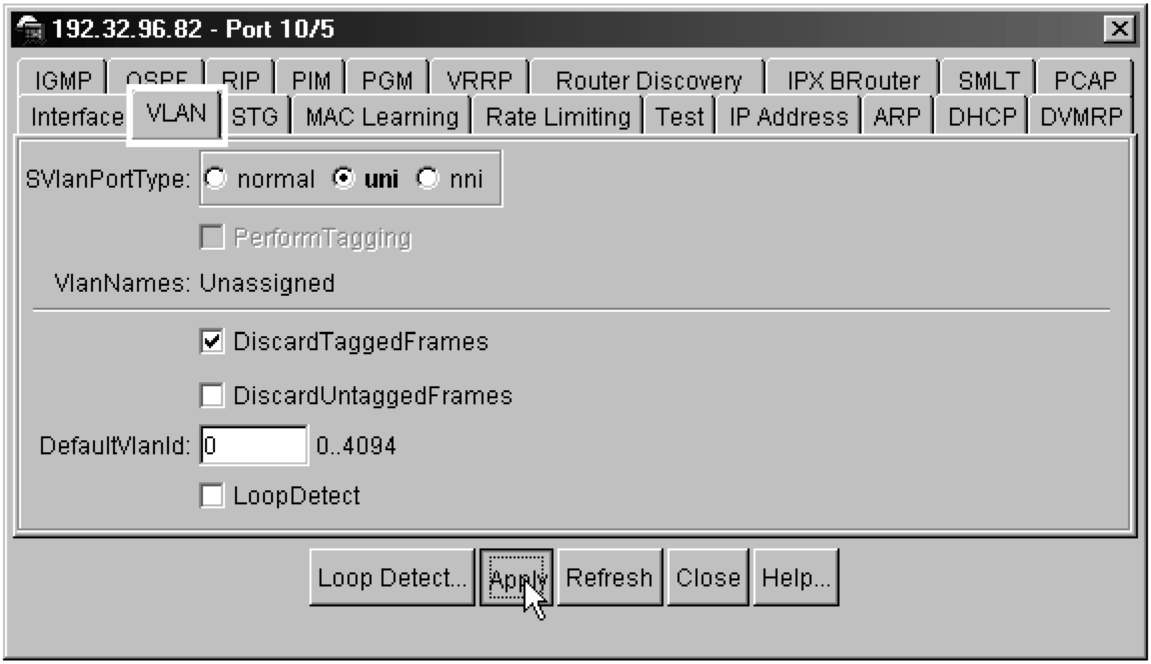
OperRouting: disable

□ HighSecureEnable

3 Click the VLAN tab.

The VLAN tab opens (Figure 57).

Figure 57 Port dialog box-- VLAN tab



192.32.96.82 - Port 10/5

SVlanPortType: ○ normal ● uni ○ nni

□ PerformTagging

VlanNames: Unassigned

☑ DiscardTaggedFrames

□ DiscardUntaggedFrames

DefaultVlanId: 0 0..4094

□ LoopDetect

4 In the sVLANPortType field, click one of the following:

- uni—User-to-Network interface.

  You must configure ports for which you want to provide VLAN transparency as UNI ports. UNI ports can only belong to one sVLAN. When you designate a port as a UNI port, the DiscardTaggedFrames parameter is automatically enabled. This prevents traffic from leaking to other VLANs.

- nni—Network-to-Network interface.

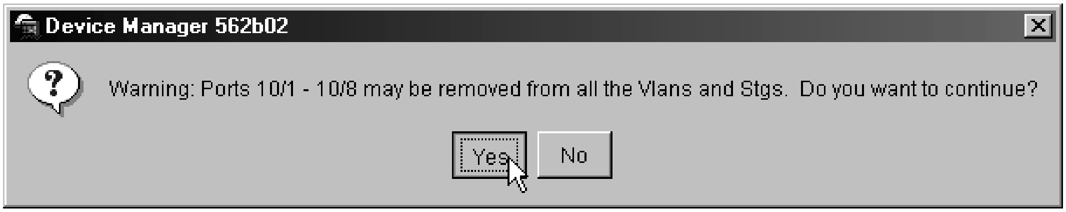
  NNI ports interconnect the switches in the core network, drop untagged frames on ingress, and insert the sVLAN tag at the egress. When you configure an NNI port, the DiscardUnTaggedFrames parameter is automatically enabled.

Note: All ports within the same OctaPID have the same designation, that is all eight ports are either Normal, or all eight ports are UNI/NNI. When you change a port from normal to UNI/NNI, the other seven ports are changed automatically, and vice versa. See "Tap and OctaPID assignment" on page 261" for more details.

5 Click Apply.

The system warns you that by changing the port type, all ports in the OctaPID may be removed from all VLANs and STGs (Figure 58). This message displays the port range for the OctaPID. If you have changed a port from Normal to UNI/NNI, the other seven ports in the OctaPID are changed automatically.

Figure 58 sVLAN configuration warning



Device Manager 562b02

Warning: Ports 10/1 - 10/8 may be removed from all the Vlans and Stgs. Do you want to continue?

6 To continue applying the configuration, click Yes.

The sVLAN port type is configured.

7 Click Close.

The Port dialog box closes.

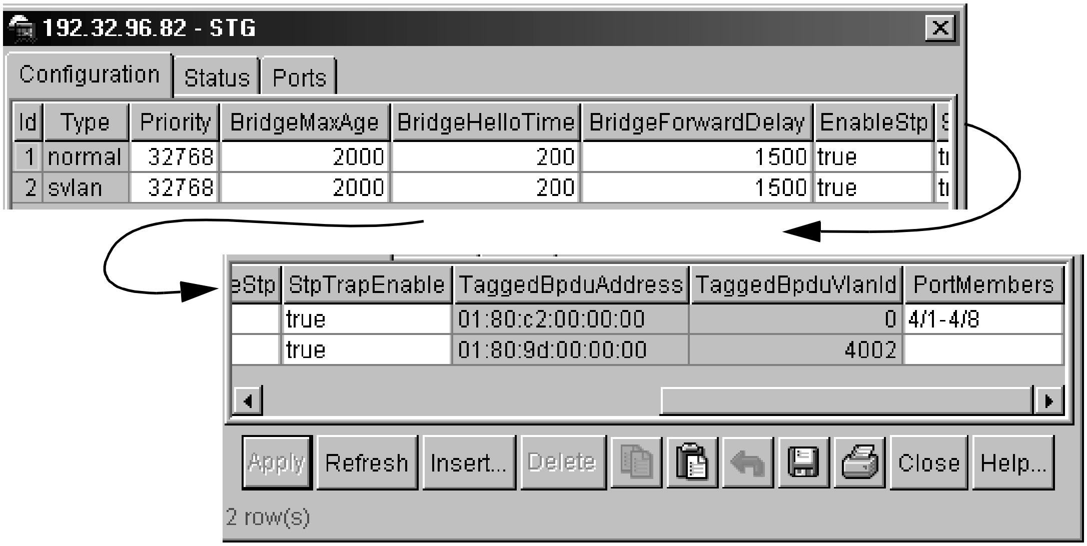
Creating an sVLAN STG

To create an sVLAN STG:

1 From the Device Manager menu bar, choose VLAN > STG.

The STG dialog box opens to the Configuration tab (Figure 59).

Figure 59 STG dialog box

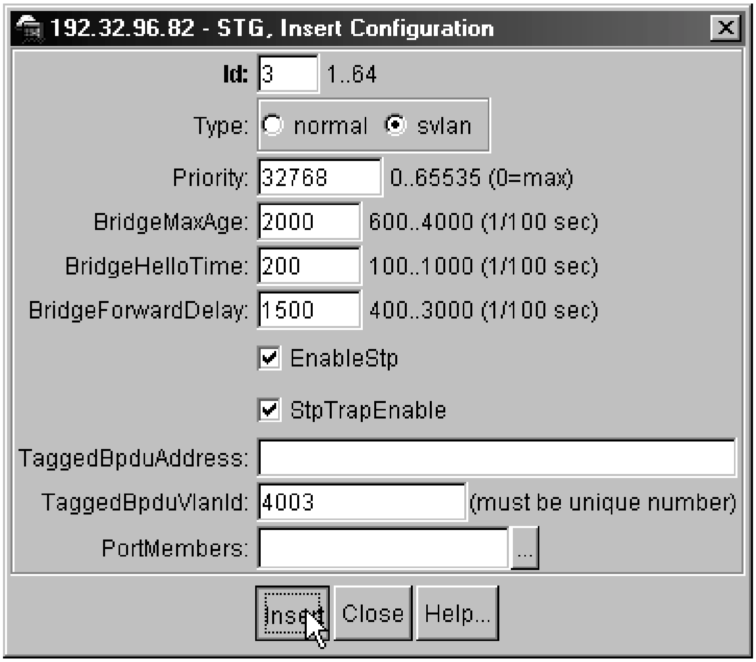


Id	Type	Priority	BridgeMaxAge	BridgeHelloTime	BridgeForwardDelay	EnableStp	StpTrapEnable	TaggedBpduAddress	TaggedBpduVlanId	PortMembers
1	normal	32768	2000	200	1500	true	true	01:80:c2:00:00:00	0	4/1-4/8
2	svlan	32768	2000	200	1500	true	true	01:80:9d:00:00:00	4002	

2 Click Insert.

The STG, Insert Configuration dialog box opens (Figure 60).

Figure 60 STG, Insert Configuration dialog box



192.32.96.82 - STG, Insert Configuration

Id: 3 1..64

Type: ○ normal ● svlan

Priority: 32768 0..65535 (0=max)

BridgeMaxAge: 2000 600..4000 (1/100 sec)

BridgeHelloTime: 200 100..1000 (1/100 sec)

BridgeForwardDelay: 1500 400..3000 (1/100 sec)

☑ EnableStp

☑ StpTrapEnable

TaggedBpduAddress:

TaggedBpduVlanId: 4003 (must be unique number)

PortMembers:

3 In the ID field, enter an STG ID, or use the displayed ID.

4 In the Type field, click svlan.

5 In the TaggedBpduAddress field, enter a MAC address to be assigned to the destination MAC address field in tagged BPDUs.

> **Note:** The MAC address you enter must be different from the standardized BPDU MAC address.

6 In the PortMembers field, click the ellipsis (...).

The STG Port Members dialog box opens, displaying available ports.

7 Click the ports to include in the sVLAN STG, and click OK.

The STG Port Members dialog box closes, and the ports appear in the STG, Insert Configuration dialog box.

8 Click Insert.

The STG appears in the Configuration tab.

9 From the Configuration tab, click Close.

The STG is configured and the STG dialog box closes.

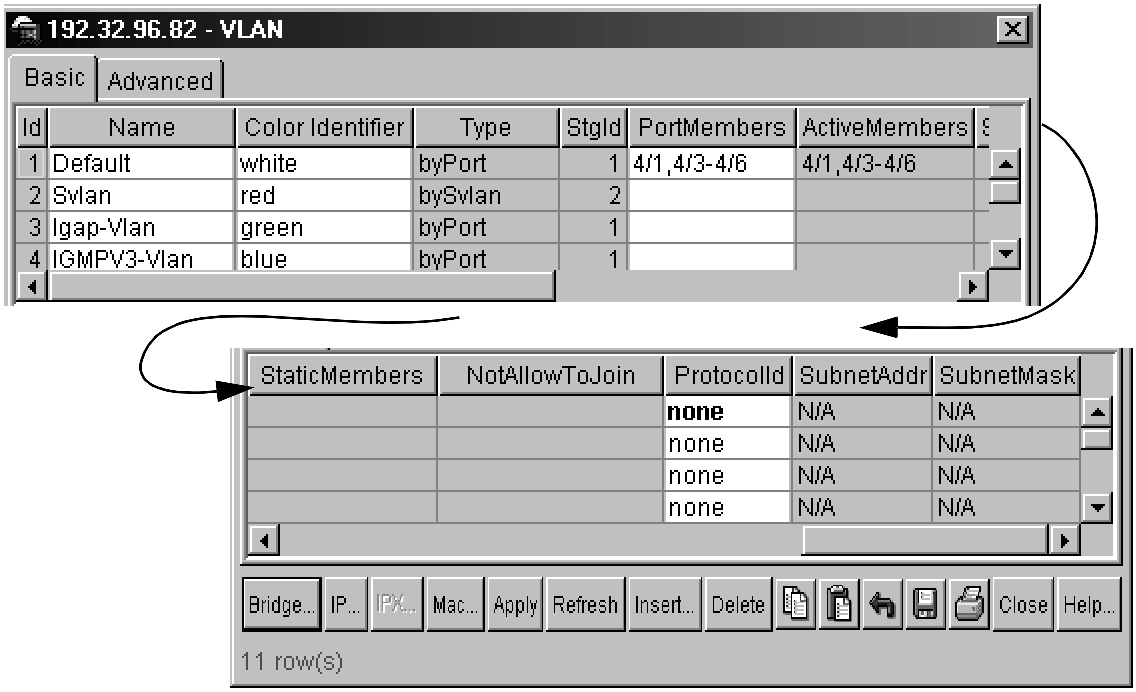
Creating an sVLAN

To create an sVLAN:

1 From the Device Manager menu bar, choose VLAN > VLANs.

The VLAN dialog box opens to the Basic tab (Figure 61).

Figure 61 VLAN dialog box-- Basic tab

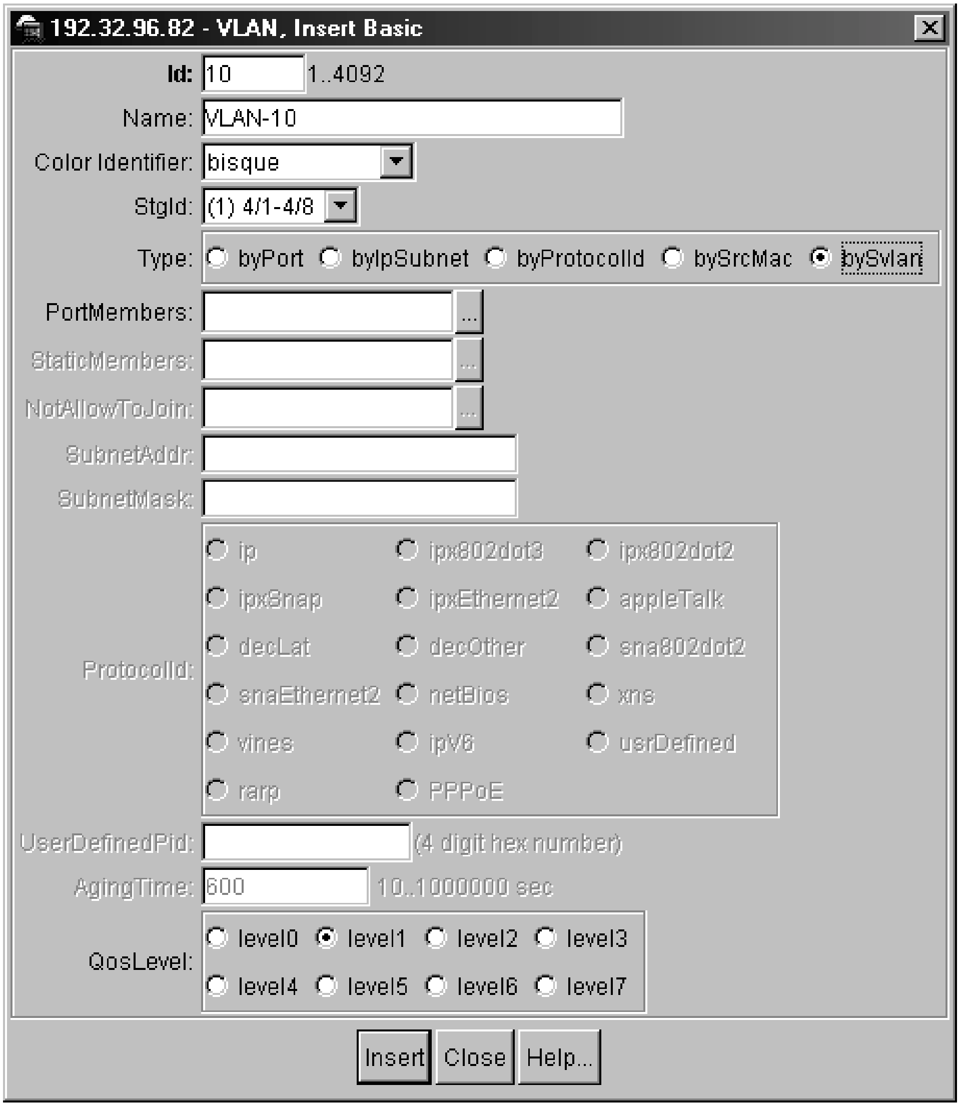


Id	Name	Color Identifier	Type	StgId	PortMembers	ActiveMembers	StaticMembers	NotAllowToJoin	ProtocolId	SubnetAddr	SubnetMask
1	Default	white	byPort	1	4/1,4/3-4/6	4/1,4/3-4/6			none	N/A	N/A
2	Svlan	red	bySvlan	2					none	N/A	N/A
3	Igap-Vlan	green	byPort	1					none	N/A	N/A
4	IGMPV3-Vlan	blue	byPort	1					none	N/A	N/A

2 Click Insert.

The VLAN, Insert Basic dialog box opens (Figure 62).

Figure 62 Insert Basic dialog box—for stacked VLANs



192.32.96.82 - VLAN, Insert Basic

Id: 10 1..4092

Name: VLAN-10

Color Identifier: bisque

StgId: (1) 4/1-4/8

Type: ○ byPort ○ byIpSubnet ○ byProtocolId ○ bySrcMac ● bySvlan

PortMembers:

StaticMembers:

NotAllowToJoin:

SubnetAddr:

SubnetMask:

ProtocolId: ○ ip ○ ipx802dot3 ○ ipx802dot2 ○ ipxSnap ○ ipxEthernet2 ○ appleTalk ○ decLat ○ decOther ○ sna802dot2 ○ snaEthernet2 ○ netBios ○ xns ○ vines ○ ipV6 ○ usrDefined ○ rarp ○ PPPoE

UserDefinedPid: (4 digit hex number)

AgingTime: 600 10..1000000 sec

QosLevel: ○ level0 ● level1 ○ level2 ○ level3 ○ level4 ○ level5 ○ level6 ○ level7

3 In the ID field, enter an unused VLAN ID (1 - 4094) or use the ID provided. The default VLAN is VLAN ID 1.

4 (Optional) In the Name field, type the VLAN name, or use the name provided.

5 (Optional) In the Color Identifier field, click the down arrow and choose a color from the dropdown list, or use the color provided.

Device Manager suggests a color, but you can change it.This color is used by VLAN Manager to display the different VLANs in a network.

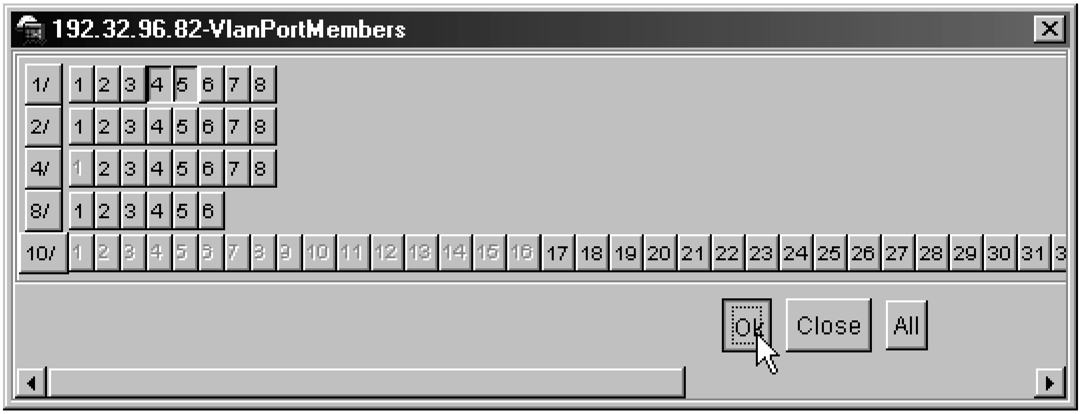
6 In the StgId field, type or select the spanning tree group ID for the VLAN.

7 In the Type field, click bySvlan.

8 In the PortMembers field, click the ellipsis (...).

The VlanPortMembers dialog box opens (Figure 63).

Figure 63 VlanPortMembers dialog box



9 Click the ports to include in the new VLAN.

10 Click OK.

The Port Membership dialog box closes and the port members appear in the Insert Basic dialog box.

11 (Optional) In the QoS field, click a quality of service level.

12 On the VLAN, Insert Basic dialog box, click Insert.

The Insert dialog box closes and the VLAN appears in the Basic tab.

13 In the VLAN, Basic tab, click Close.

The VLAN is configured and the VLAN dialog box closes.

Chapter 4
Configuring STGs using Device Manager

This section discusses using Device Manager to create, manage, and monitor spanning tree groups (STGs), and includes the following topics:

- "Creating an STG," next
- "Editing an STG" on page 144
- "Adding ports to an STG" on page 145
- "Viewing STG status" on page 146
- "Viewing STG ports" on page 148
- "Enabling STP on a port" on page 151
- "Deleting an STG" on page 152
- "Configuring topology change detection" on page 152

Creating an STG

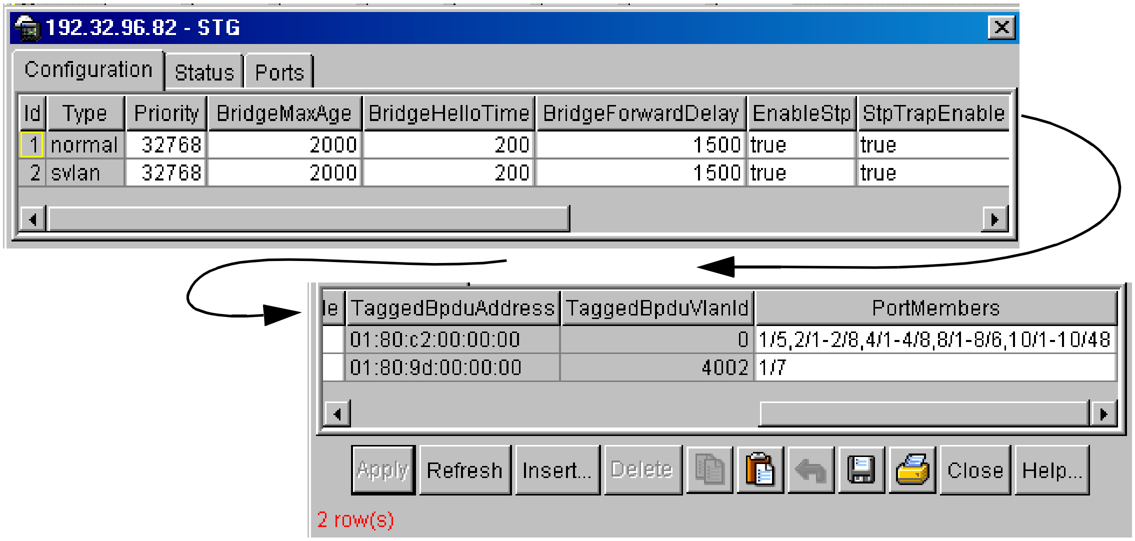
Note: This information applies to Passport 8600 modules only.
Note: Spanning Tree protocol is currently not supported on SMLT or IST ports.

To create an STG:

1 From the Device Manager menu bar, choose VLAN > STG.

The STG dialog box opens to the Configuration tab (Figure 64).

Figure 64 STG dialog box



Id	Type	Priority	BridgeMaxAge	BridgeHelloTime	BridgeForwardDelay	EnableStp	StpTrapEnable
1	normal	32768	2000	200	1500	true	true
2	svlan	32768	2000	200	1500	true	true

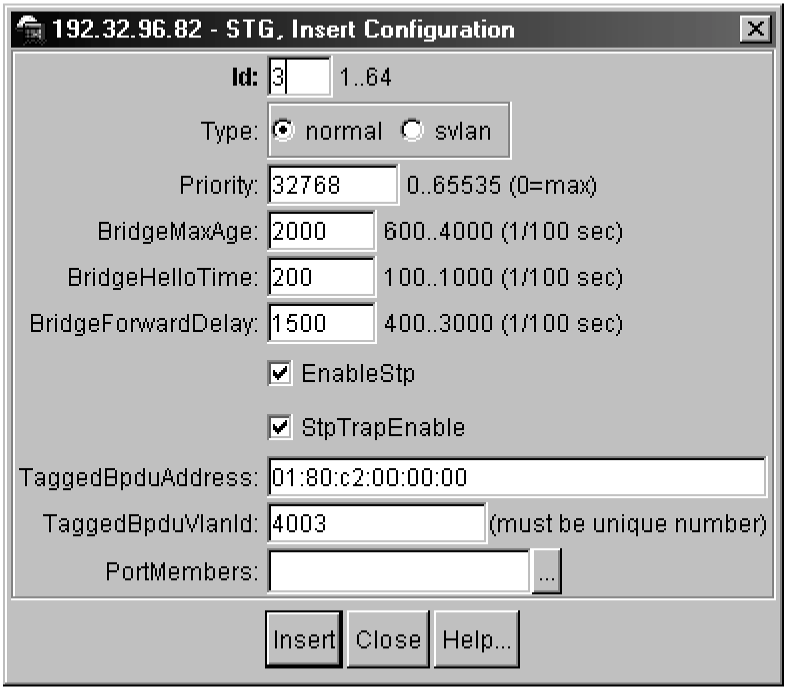
le	TaggedBpduAddress	TaggedBpduVlanId	PortMembers
	01:80:c2:00:00:00	0	1/5,2/1-2/8,4/1-4/8,8/1-8/6,10/1-10/48
	01:80:9d:00:00:00	4002	1/7

2 row(s)

2 From the Configuration tab, click Insert.

The STG, Insert Configuration dialog box opens (Figure 65). For field descriptions, see Table 18 on page 143.

Figure 65 STG, Insert Configuration dialog box



192.32.96.82 - STG, Insert Configuration

Id: 3 1..64

Type: ● normal ○ svlan

Priority: 32768 0..65535 (0=max)

BridgeMaxAge: 2000 600..4000 (1/100 sec)

BridgeHelloTime: 200 100..1000 (1/100 sec)

BridgeForwardDelay: 1500 400..3000 (1/100 sec)

☑ EnableStp

☑ StpTrapEnable

TaggedBpduAddress: 01:80:c2:00:00:00

TaggedBpduVlanId: 4003 (must be unique number)

PortMembers:

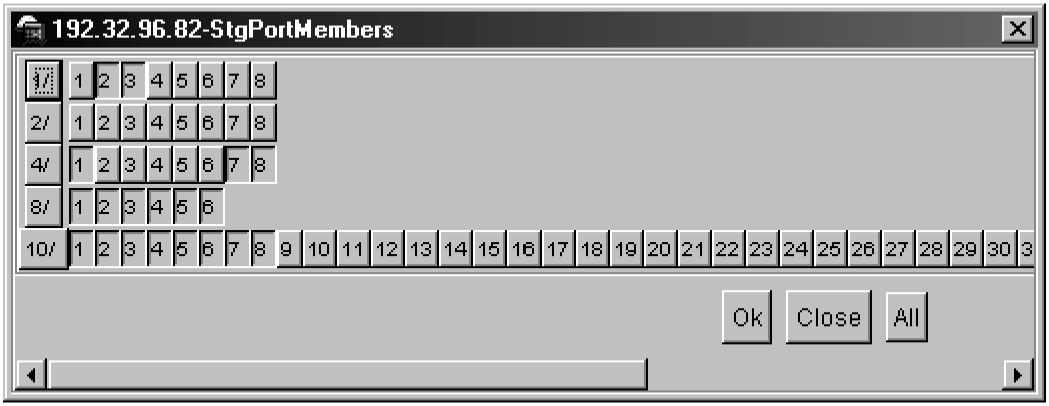
3 Use the fields in the STG, Insert Configuration dialog box to configure the STG.

Note: In the STG table, the STG ID and TaggedBpduVlanId must be unique. If you change the STG ID without updating TaggedBpduVlandId, the insertion may fail because of a duplicate TaggedBpduVlanId.

4 To add ports to the STG, click the ellipses (...) in the PortMembers field.

The Port Members dialog box (Figure 66)opens.

Figure 66 STG Port Members dialog box



5 Click the ports you want to add to the STG, and click OK.

The Port Members dialog box closes, and the ports are added to the Port Members field in the Insert Configuration dialog box.

Note: Spanning Tree protocol is not supported on SMLT or IST ports.

6 Click Insert.

The Insert Configuration dialog box closes, and the STG appears in the Configuration tab.

7 Click Apply.

The STG is configured.

Table 18 describes the STG Configuration fields.

Table 18 STG configuration fields

Field	**Description**
Id	The ID number for the STG. Note: The STG ID and TaggedBpduVlanId must be unique in the STG table. If you change the STG ID without updating TaggedBpduVlanId, the insertion may fail because of a duplicate TaggedBpduVlanId.
Type	Specifies the type of STG. • normal = normal STG • svlan = stacked VLAN STG
Priority	Sets the STP bridge priority, in decimal. The range is 0 (highest priority) to 65535 (lowest priority). The default is 32768.
BridgeMaxAge	The value in hundredths of a second that all bridges use for MaxAge when this bridge is acting as the root. **Note:** The 802.1D-1990 standard specifies that the BridgeMaxAge range is related to the value of dot1dStpBridgeHelloTime. The default is 2000 (20 seconds).
BridgeHelloTime	The value in hundredths of a second that all bridges use for HelloTime when this bridge is acting as the root. The granularity of this timer is specified by the IEEE 802.1D-1990 standard to be in increments of 1/100 of a second. The default is 200 (2 seconds).
BridgeForwardDelay	The value in hundredths of a second that all bridges use for Forward Delay when this bridge is acting as the root. The default is 1500 (15 seconds).
EnableSTP	Enables or disables the spanning tree algorithm for the STG.
StpTrapEnable	Enables SNMP traps to be sent to trace receiver every time an STP topology occurs.
TaggedBpduAddress	Represents a MAC address; specifically for tagged BPDUs.

Table 18 STG configuration fields (continued)

Field	**Description**
TaggedBpduVlanId	Represents the VLAN tag associated with the STG. This ID is used to tag BPDUs through a non-IEEE tagging bridge to another 8000 Series switch. Note: By default, the TaggedBpduVlanId is an address calculated based on the STG ID by Device Manager. Accepting the default value calculated by Device Manager makes it much simpler to coordinate STGs across multiple switches. If you enter a custom value for this field, you must manually coordinate it across all switches. Note: The STG ID and TaggedBpduVlanId must be unique in the STG table. If you change the STG ID without updating TaggedBpduVlanId, the insertion may fail because of a duplicate TaggedBpduVlanId.
Port Members	The ports you want to become members of the new STG. Ports are not selectable if: • configured as single port SMLT, MLT-base SMLT, or IST • configured as members of any other STG

Note: Nontagged ports can only belong to one STG.

Editing an STG

Note: This information applies to 8600 modules only.

To edit an STG:

1 From the Device Manager menu bar, choose VLAN > STG.

The STG dialog box opens to the Configuration tab (Figure 64).

2 Double-click the field for the STG you want to edit.

The field becomes editable.

3 Enter a new value in the field or select a new setting from the dropdown menu.

4 Click Apply.

The changes are applied to the STG.

Adding ports to an STG

To add ports to a spanning tree group:

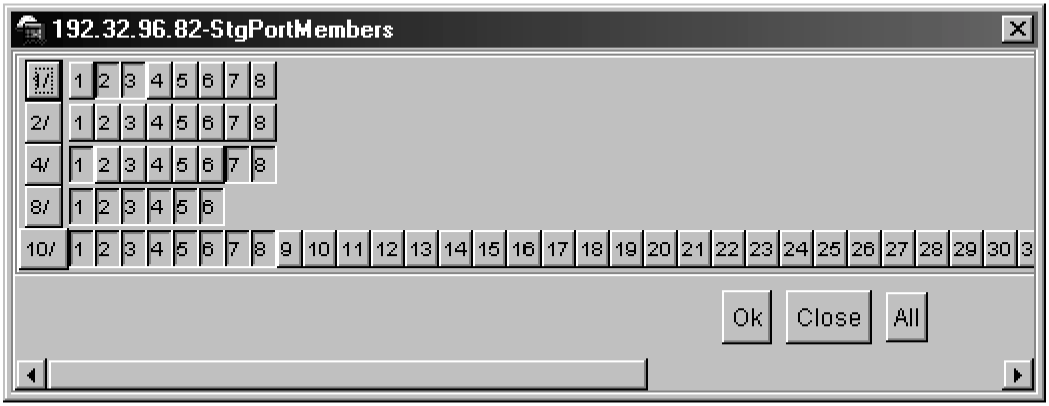
1 From the Device Manager menu bar, choose VLAN > STG.

The STG dialog box opens to the Configuration tab (Figure 64 on page 140).

2 Double-click the Port Members field for the STG.

The Port Members dialog box (Figure 67)opens, indicating the port members assigned to this STG.

Figure 67 STG Port Members dialog box



3 Click the ports you want to add to the STG, and click OK.

The Port Members dialog box closes, and the ports are added to the Port Members field in the Configuration tab.

Note: Spanning Tree protocol is not supported on SMLT or IST ports.

4 Click Apply.

The ports are added to the STG.

Viewing STG status

The STG Status tab allows you to view the status of the spanning tree for each STG that is associated with the network.

To view STG status:

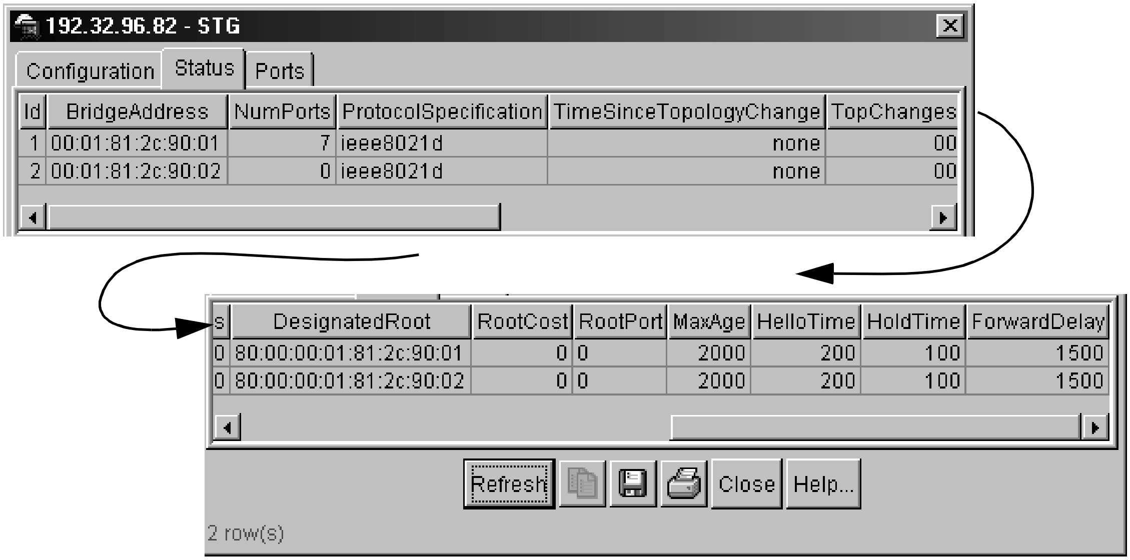
1 From the Device Manager menu bar, choose VLAN > STG.

The STG dialog box opens to the Configuration tab (Figure 64).

2 Click the Status tab.

The Status tab opens (Figure 68), displaying STG status.

Figure 68 STG dialog box—Status tab



Id	BridgeAddress	NumPorts	ProtocolSpecification	TimeSinceTopologyChange	TopChanges
1	00:01:81:2c:90:01	7	ieee8021d	none	00
2	00:01:81:2c:90:02	0	ieee8021d	none	00

s	DesignatedRoot	RootCost	RootPort	MaxAge	HelloTime	HoldTime	ForwardDelay
0	80:00:00:01:81:2c:90:01	0	0	2000	200	100	1500
0	80:00:00:01:81:2c:90:02	0	0	2000	200	100	1500

2 row(s)

Table 19 describes the STG status fields.

Table 19 STG status fields

Field	Description
BridgeAddress	The MAC address used by this bridge when it must be referred to in a unique fashion.
NumPorts	The number of ports controlled by this bridging entity.
ProtocolSpecification	An indication of what version of the Spanning Tree Protocol is being run. The IEEE 802.1d implementations will return ieee8021d.
TimeSinceTopologyChange	The time in hundredths of a second since the last time a topology change was detected by the bridge entity or STG.
TopChanges	A topology change trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state. The trap is not sent if a new root trap is sent for the same transition. Implementation of this trap is optional.
DesignatedRoot	The bridge identifier of the root of the spanning tree as determined by the Spanning Tree Protocol as executed by this node. This value is used as the Root Identifier parameter in all Configuration Bridge PDUs originated by this node.
RootCost	The cost of the path to the root as seen from this bridge.
RootPort	The port number of the port that offers the lowest cost path from this bridge to the root bridge.
MaxAge	The maximum age of Spanning Tree Protocol information learned from the network on any port before it is discarded, in units of hundredths of a second. This is the actual value that this bridge is currently using.
HelloTime	The amount of time in hundredths of a second between transmission of config BPDUs by this node on any port when it is the root of the spanning tree. The default value is 200 (2 seconds).

Table 19 STG status fields (continued)

Field	Description
HoldTime	The time interval in hundredths of a second during which no more than two Configuration bridge PDUs shall be transmitted by this node. The default value is 100 (1 second).
ForwardDelay	The time interval in hundredths of a second that controls how fast a port changes its spanning state when moving toward the Forwarding state. The value determines how long the port stays in each of the Listening and Learning states, which precede the Forwarding state. This value is also used when a topology change has been detected and is under way, to age all dynamic entries in the Forwarding Database. [Note that this value is the one this bridge is currently using, in contrast to rcStgBridgeForwardDelay, which is the value that this bridge and all others would start using if/when this bridge were to become the root.] The default value is 1500 (15 seconds).

Viewing STG ports

The Ports tab allows you to view the status of ports for each STG that is associated with the network.

To view STG ports:

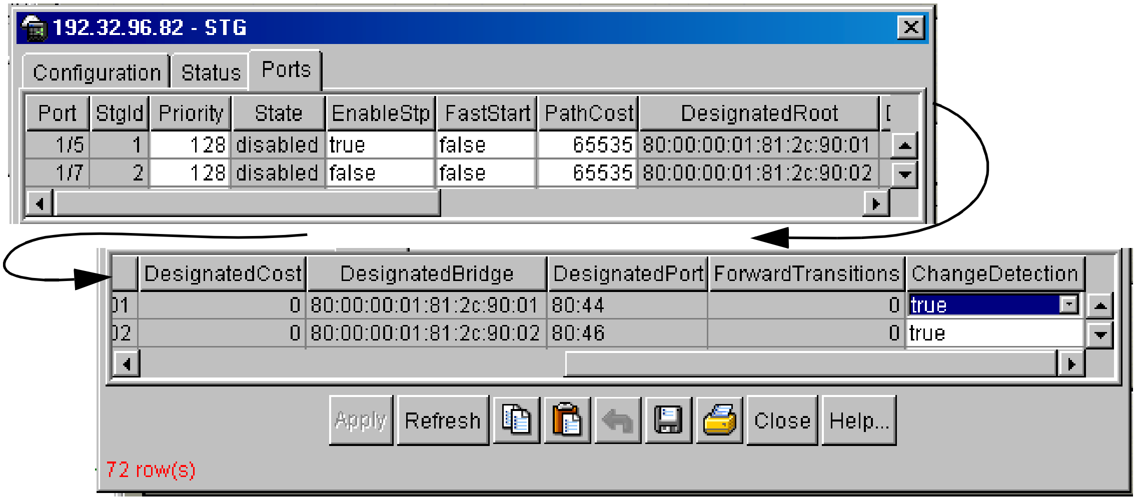
1 From the Device Manager menu bar, choose VLAN > STG.

The STG dialog box opens to the Configuration tab (Figure 64 on page 140).

2 Click the Ports tab.

The Ports tab opens (Figure 69). For field definitions, see "STG Ports tab fields" on page 149.

Figure 69 STG dialog box—Ports tab



Port	StgId	Priority	State	EnableStp	FastStart	PathCost	DesignatedRoot	[
1/5	1	128	disabled	true	false	65535	80:00:00:01:81:2c:90:01	
1/7	2	128	disabled	false	false	65535	80:00:00:01:81:2c:90:02	

	DesignatedCost	DesignatedBridge	DesignatedPort	ForwardTransitions	ChangeDetection
01	0	80:00:00:01:81:2c:90:01	80:44	0	true
02	0	80:00:00:01:81:2c:90:02	80:46	0	true

72 row(s)

Table 20 describes the Ports tab fields.

Table 20 STG Ports tab fields

Field	**Description**
Port	The port number of the port for which this entry contains Spanning Tree Protocol management information.
StgId	The STG identifier assigned to this port.
Priority	The value of the priority field which is contained in the first octet of the (2 octet long) Port ID. The other octet of the Port ID is given by the value of rcStgPort. Note: Although port priority values can range from 0-255, on the 8600 Series switch, only the following values are used: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240.

Table 20 STG Ports tab fields (continued)

Field	**Description**
State	The port’s current state as defined by the application of the Spanning Tree Protocol. • disabled(1), • blocking(2), • listening(3), • learning(4), • forwarding(5), • broken(6) This state controls what action a port takes on reception of the frame. If the bridge has detected a port that is malfunctioning, it will place that port into the Broken (6) state. For ports that are disabled, this object will have a value of disable.
EnableStp	The STP state of the port. • Enabled—BPDUs are processed in accordance with STP. • Disabled—The port stays in a forwarding state, received BPDUs are dropped and not processed, and no BPDU is generated.
FastStart	When this flag is set, the port is moved straight to the Forwarding (5) state upon being enabled. • true (enables FastStart for the port) • false (default, disables FastStart for the port) Note: This setting is contrary to that specified in the IEEE 802.1D standard for Spanning Tree Protocol (STP), in which a port enters the blocking state following the initialization of the bridging device or from the disabled state when the port is enabled through configuration.
PathCost	The contribution of this port to the path cost of paths toward the spanning tree root that includes this port. The 802.1D-1990 protocol recommends that the default value of this parameter be in inverse proportion to the speed of the attached LAN.
DesignatedRoot	The unique Bridge Identifier of the Bridge recorded as the Root in the Configuration BPDUs transmitted by the Designated Bridge for the segment to which the port is attached.
DesignatedCost	The path cost of the Designated Port of the segment connected to this port. This value is compared to the Root Path Cost field in received bridge PDUs.
DesignatedBridge	The Bridge Identifier of the bridge that this port considers to be the Designated Bridge for this port’s segment.
DesignatedPort	The Port Identifier of the port on the Designated Bridge for this port’s segment.

Table 20 STG Ports tab fields (continued)

Field	**Description**
ForwardTransitions	The number of times this port has transitioned from the Learning state to the Forwarding state.
ChangeDetection	The change detection setting (true or false) for this port. Can only be configured on Access ports. If you enable change detection on an MLT with access ports, the setting is automatically applied to all ports in the MLT. See "About Spanning Tree protocol topology change detection" on page 49.

Enabling STP on a port

To enable STP for a port:

1 From the Device Manager menu bar, choose VLAN > STG.

The STG dialog box opens to the Configuration tab (Figure 64 on page 140).

2 Click the Ports tab.

The Ports tab opens (Figure 69).

3 Click in the EnableStp field for the port you want to enable.

The dropdown menu opens.

4 From the dropdown menu, choose true.

The EnableStp setting changes.

5 Click Apply.

STP is enabled for the port.

Deleting an STG

Note: The following procedure applies to 8600 modules only.

To delete an STG:

1 From the Device Manager menu bar, choose VLAN > STG.

The STG dialog box opens to the Configuration tab (Figure 64 on page 140).

2 Click the STG that you want to delete.

3 Click Delete.

Note: All VLANs must be deleted from an STG before you can remove it.

Configuring topology change detection

To configure topology change detection on a port:

1 From the Device Manager menu bar, choose VLAN > STG.

The STG dialog box opens to the Configuration tab (Figure 64 on page 140).

2 Click the Ports tab.

The Ports tab opens (Figure 69).

3 Double-click the ChangeDetection field.

The dropdown menu of change detection settings opens.

4 From the dropdown menu, choose one of the following:

- To enable change detection on the port, choose True.
- To disable change detection on the port, choose False.

5 Click Apply.

Change detection is configured for the port.

For more information about change detection, see "About Spanning Tree protocol topology change detection" on page 49.

Chapter 5
Configuring MLTs and SMLTs using Device Manager

This section describes how to configure MultiLink Trunking (MLT) and Split MultiLink Trunking (SMLT) in your network, and includes the following topics:

- "Configuring an MLT" on page 155
- "Configuring an SMLT" on page 168

For conceptual information about MultiLink trunking, see:"

- "About MultiLink Trunking" on page 50
- "About Split Multilink Trunking (SMLT)" on page 59

Configuring an MLT

This section describes how to configure and manage a MultiLink Trunk, and includes the following topics:

- "Adding an MLT" on page 156
- "Adding ports to an MLT" on page 161
- "Viewing MLT interface statistics" on page 162
- "Viewing MLT Ethernet error statistics" on page 164

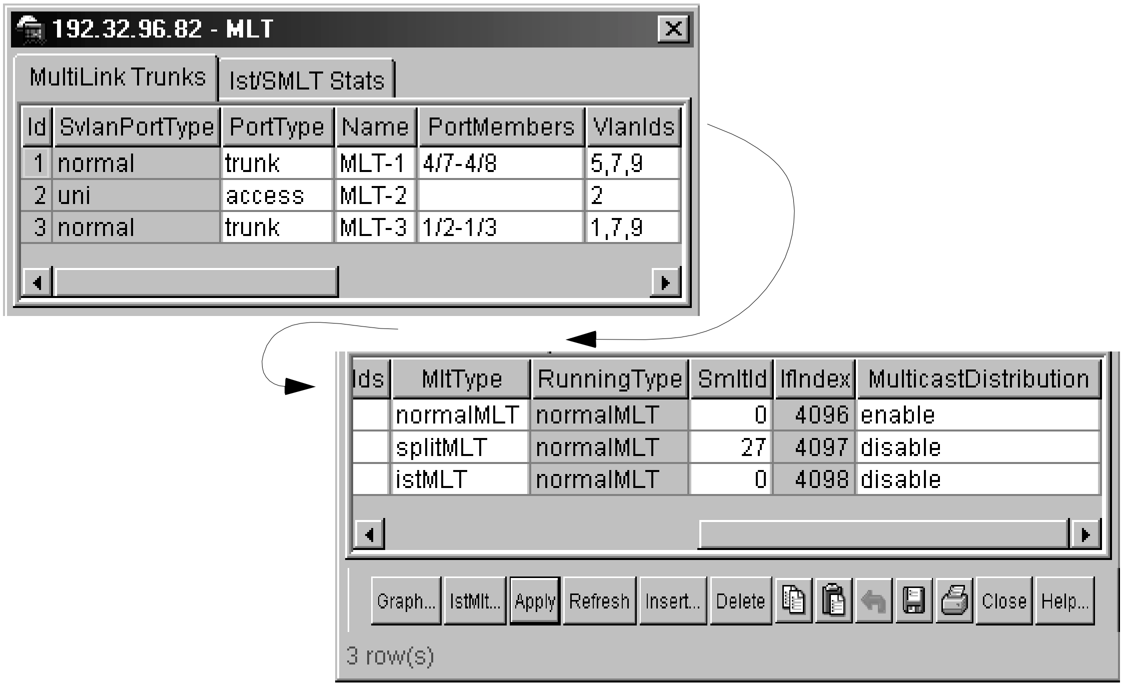
Adding an MLT

To add a MultiLink Trunk:

1 From the Device Manager menu bar, choose VLAN > MLT.

The MLT dialog box (Figure 70) opens, displaying active MLTs.

Figure 70 MLT dialog box



Id	SvlanPortType	PortType	Name	PortMembers	VlanIds
1	normal	trunk	MLT-1	4/7-4/8	5,7,9
2	uni	access	MLT-2		2
3	normal	trunk	MLT-3	1/2-1/3	1,7,9

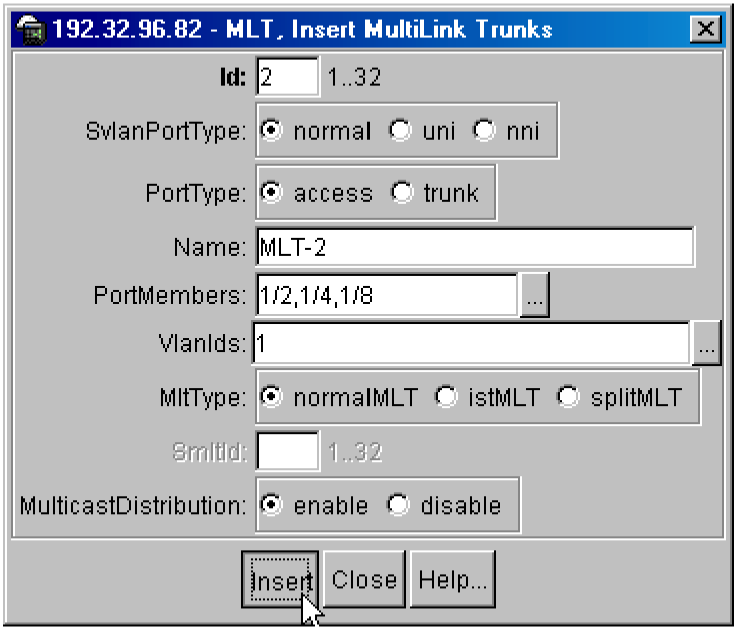
Ids	MltType	RunningType	SmltId	IfIndex	MulticastDistribution
	normalMLT	normalMLT	0	4096	enable
	splitMLT	normalMLT	27	4097	disable
	istMLT	normalMLT	0	4098	disable

3 row(s)

2 In the MLT dialog box, click Insert.

The MLT, Insert MultiLink Trunks dialog box (Figure 71) opens. See Table 21 on page 160 for field descriptions.

Figure 71 MLT, Insert MultiLink Trunks dialog box



192.32.96.82 - MLT, Insert MultiLink Trunks

Id: 2 1..32

SvlanPortType: ● normal ○ uni ○ nni

PortType: ● access ○ trunk

Name: MLT-2

PortMembers: 1/2,1/4,1/8 ...

VlanIds: 1 ...

MltType: ● normalMLT ○ istMLT ○ splitMLT

SmltId: 1..32

MulticastDistribution: ● enable ○ disable

3 In the ID field, type the ID number for the MultiLink Trunk.

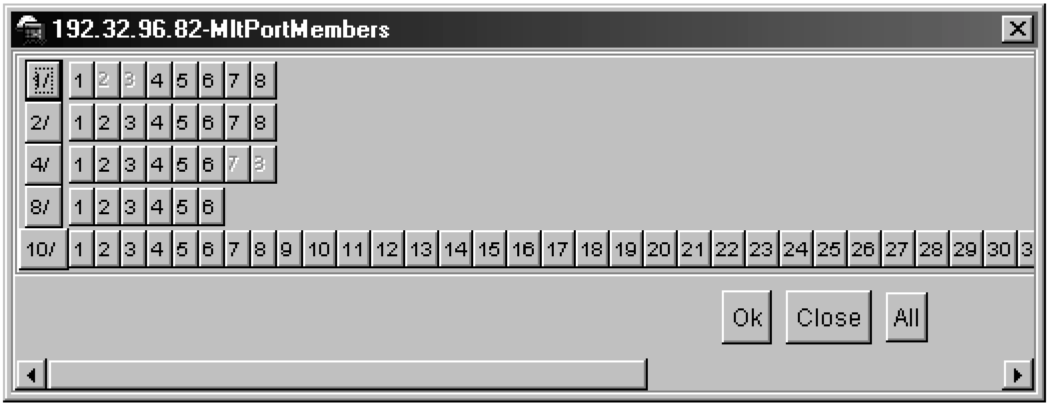
4 In the PortType field, click Access or Trunk.

5 In the Name field, type a name for the MultiLink Trunk port.

6 In the PortMembers field, click the ellipsis (...).

The MltPortMembers dialog box (Figure 72) opens.

Figure 72 MLT Port Members dialog box



7 In the MltPortMembers dialog box, click the ports to include in the MultiLink Trunk port.

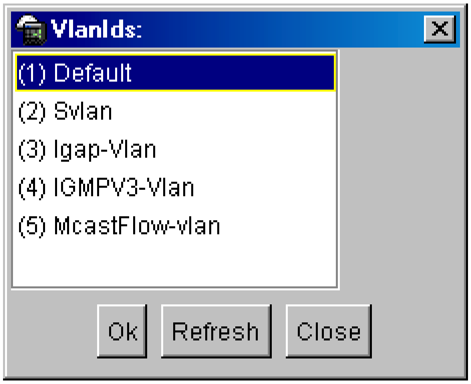
8 Click OK.

The MltPortMembers dialog box closes, and the ports are added to the PortMembers field on the Insert MultiLink Trunks dialog box.

9 In the VlanIds field, click the ellipsis (...).

The VlanIds dialog box (Figure 73) opens.

Figure 73 MLT VLAN IDs dialog box



10 Choose a VLAN for the MultiLink Trunk port and click OK.

The VlanIds dialog box closes and the VLAN is added to the VlanIds field on the Insert MultiLink Trunks dialog box.

11 In the MltType field, click normalMLT or istMLT.

For information about configuring SMLT, see "Adding an MLT-based SMLT" on page 168.

12 In the Multicast Distribution field, click Enable or Disable.

Note: Multicast distribution over MLT is supported only on 8000 Series E-modules. For detailed information about configuring multicast distribution over MLT, see the publication, *Configuring IP Routing Multicast Protocols*.

13 Click Insert.

The MLT is added to the MultiLink Trunks tab in the MLT dialog box.

14 In the MLT dialog box, click Apply.

The MLT is added.

Table 21 defines the MultiLink Trunks tab fields.

Table 21 MLT MultiLink Trunks fields

Field	Description
Id	A value that uniquely identifies the MultiLink Trunk. • For 8600 modules, up to 32 MLTs (IDs 1-32) are supported. • For 8100 modules, up to 6 MLTs (IDs 1-6) are supported.
SvlanPortType	Set MLT port type: • normal (default) • uni (User-to-Network Interface) You must configure ports to which you want to provide VLAN transparency as UNI ports. UNI ports can only belong to one SVLAN. When you designate a port as a UNI port, the DiscardTaggedFrames parameter is automatically configured (Edit>Port>VLAN). This prevents traffic from leaking to other VLANs. • nni (Network-to-Network Interface) NNI ports interconnect the switches in the core network, drop untagged frames on ingress, and insert the SVLAN tag at the egress. When you configure an NNI port, the DiscardUnTaggedFrames parameter is automatically configured (Edit>Port> VLAN). Before configuring a port as uni or nni, you must change the switch level to 1 or above (Edit>VLAN> SVLAN>Level).
PortType	Access or trunk port.
Name	The name given to the MLT.
PortMembers	The ports assigned to the MLT. MLT is supported on 10BASE-T, 100BASE-TX, 100BASE-FX, and Gigabit Ethernet ports. All ports in an MLT must be of the same media type (copper or fiber), and have the same settings for speed and duplex. All untagged ports must belong to the same spanning tree group. For 8600 modules, up to 8 same-type ports can belong to a single MLT. For 8100 modules, up to 4 same-type ports can belong to a single MLT.
VlanIds	The VLAN(s) to which the ports belong.

Table 21 MLT MultiLink Trunks fields (continued)

Field	Description
MltType	Editable field for specifying the type of MLT: • normalMLT • istMLT • splitMLT
RunningType	Read only field displaying the MLT operational type: • normalMLT • istMLT • splitMLT Note: This field is read only on the MultiLink Trunks tab, and does not appear on the Insert MLT dialog box.
SmltId	The split MLT ID (1-32) assigned to both ends of the split trunk. Note: The corresponding SMLTs between aggregation switches must have the same SMLT ID.
IfIndex	Read only field, displaying the Interface Index number (4096 to 4127) identifying the MLT to the software.
Multicast Distribution	The multicast distribution state on MLT ports: • Enabled • Disabled (default) Multicast distribution must also be configured on the chassis (Edit > Chassis> Mcast MLT Distribution). For more information, see the publication, *Configuring IP Routing Multicast Protocols*. **Note**: Multicast distribution over MLT is supported only on 8000 Series E-modules.

Adding ports to an MLT

To add ports to an existing MultiLink Trunk:

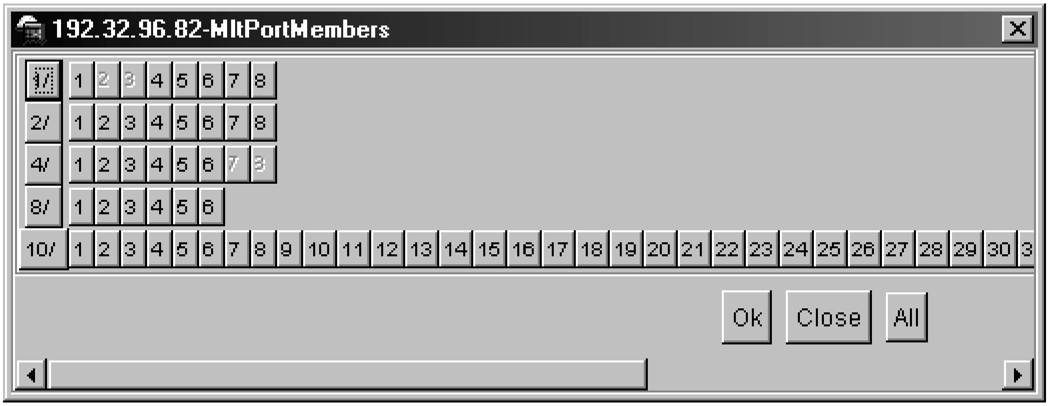
1 From the Device Manager menu bar, choose VLAN > MLT.

The MLT dialog box (Figure 71 on page 157) opens, displaying active MLTs. For field definitions, see Table 21 on page 160.

2 Double-click in the PortMembers field for the MLT to which you are adding ports.

The PortMembers dialog box (Figure 74) opens, showing the ports currently assigned for the selected MLT. Available ports are editable.

Figure 74 MltPortMembers dialog box



3 In the PortMembers dialog box, click the port numbers to be added, or click All to add all ports to the MLT.

- For 8600 modules, up to 8 same-type ports can belong to a single MLT.
- For 8100 modules, up to 4 same-type ports can belong to a single MLT.

4 Click OK.

The PortMembers dialog box closes. The port numbers are added to the selected MLT on the MultiLink Trunks tab in the MLT dialog box.

5 From the MLT dialog box, click Apply.

The ports are added to the MLT.

Viewing MLT interface statistics

To view MultiLink Trunk interface statistics:

1 From the Device Manager menu bar, choose VLAN > MLT.

The MLT dialog box (Figure 71 on page 157) opens, displaying active MLTs.

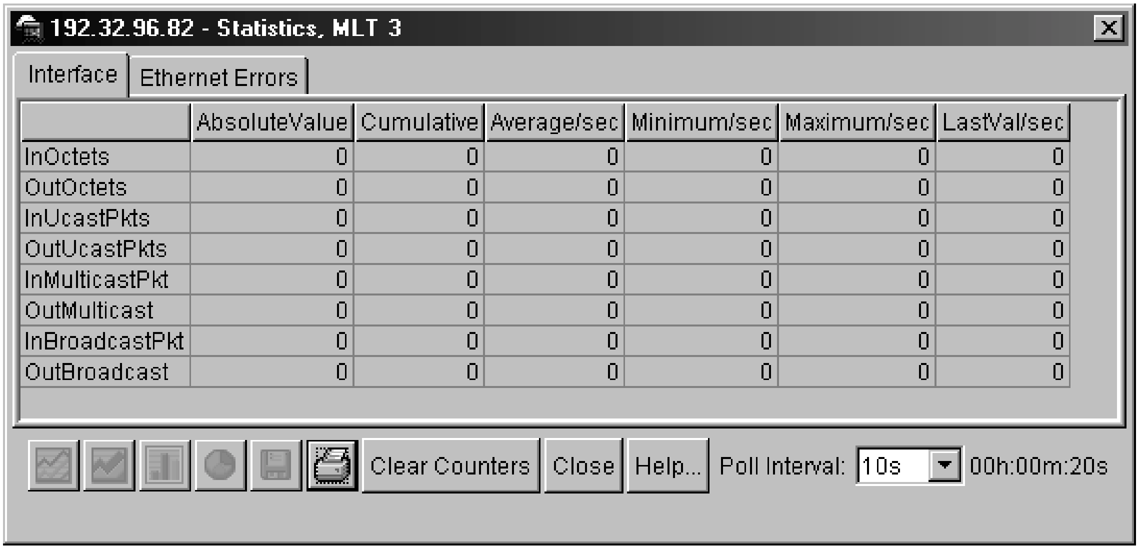
2 From the MLT dialog box, select an MLT.

The Graph tool is activated.

3 Click Graph.

The Statistics, MLT dialog box opens to the Interface tab (Figure 75), displaying interface statistics (Table 22) for the selected MLT.

Figure 75 Statistics, MLT dialog box—Interface tab



192.32.96.82 - Statistics, MLT 3

	AbsoluteValue	Cumulative	Average/sec	Minimum/sec	Maximum/sec	LastVal/sec
InOctets	0	0	0	0	0	0
OutOctets	0	0	0	0	0	0
InUcastPkts	0	0	0	0	0	0
OutUcastPkts	0	0	0	0	0	0
InMulticastPkt	0	0	0	0	0	0
OutMulticast	0	0	0	0	0	0
InBroadcastPkt	0	0	0	0	0	0
OutBroadcast	0	0	0	0	0	0

Poll Interval: 10s 00h:00m:20s

Table 22 defines the fields on the Interface tab.

Table 22 Statistics, MLT dialog box—Interface tab fields

Field	**Description**
InOctets	The total number of octets received on the MLT interface, including framing characters.
OutOctets	The total number of octets transmitted out of the MLT interface, including framing characters.
InUcastPkts	The number of packets delivered by this MLT to higher level protocols that were not addressed to a multicast or broadcast address at this sublayer.
OutUcastPkts	The number of packets that higher-level protocols requested be transmitted that were not addressed to a multicast address at this MLT.This total number includes those packets discarded or unsent.
InMulticastPkt	The number of packets delivered to this MLT that were addressed to a multicast address at this sublayer. For a MAC layer protocol, this number includes both Group and Functional addresses.

Table 22 Statistics, MLT dialog box—Interface tab fields (continued)

Field	Description
OutMulticast	The total number of packets that higher-level protocols requested be transmitted, and that were addressed to a multicast address at this MLT, including those that were discarded or not sent. For a MAC layer protocol, this number includes both Group and Functional addresses.
InBroadcastPkt	The number of packets delivered to this MLT that were addressed to a broadcast address at this sublayer.
OutBroadcast	The total number of packets that higher-level protocols requested be transmitted, and that were addressed to a broadcast address at this MLT, including those that were discarded or not sent.

Viewing MLT Ethernet error statistics

To view MultiLink Trunk Ethernet error statistics:

1 From the Device Manager menu bar, choose VLAN > MLT.

The MLT dialog box (Figure 71 on page 157) opens, displaying active MLTs.

2 From the MLT dialog box, select an MLT.

The Graph tool is activated.

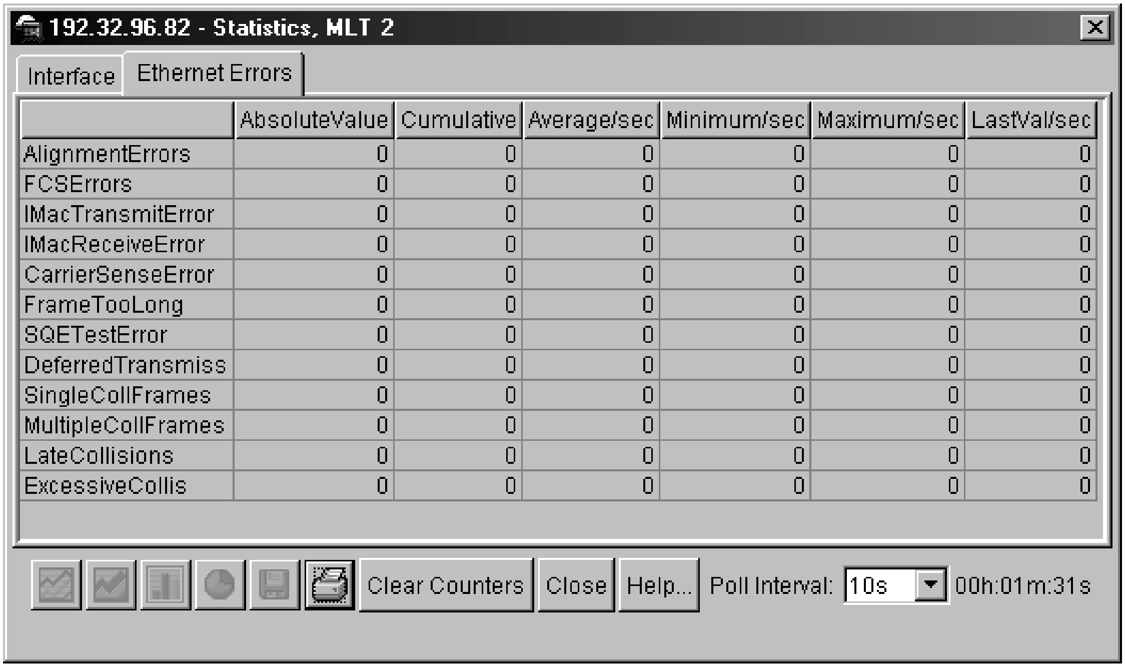
3 Click Graph.

The Statistics, MLT dialog box opens to the Interface tab.

4 Click the Ethernet Errors tab.

The Ethernet Errors tab (Figure 76) opens, displaying the statistics.

Figure 76 Statistics, MLT dialog box—Ethernet Errors tab



192.32.96.82 - Statistics, MLT 2

	AbsoluteValue	Cumulative	Average/sec	Minimum/sec	Maximum/sec	LastVal/sec
AlignmentErrors	0	0	0	0	0	0
FCSErrors	0	0	0	0	0	0
IMacTransmitError	0	0	0	0	0	0
IMacReceiveError	0	0	0	0	0	0
CarrierSenseError	0	0	0	0	0	0
FrameTooLong	0	0	0	0	0	0
SQETestError	0	0	0	0	0	0
DeferredTransmiss	0	0	0	0	0	0
SingleCollFrames	0	0	0	0	0	0
MultipleCollFrames	0	0	0	0	0	0
LateCollisions	0	0	0	0	0	0
ExcessiveCollis	0	0	0	0	0	0

Poll Interval: 10s 00h:01m:31s

Table 23 lists and defines the fields on the Ethernet Errors tab.

Table 23 Statistics, MLT dialog box—Ethernet Errors tab fields

Field	**Description**
AlignmentErrors	A count of frames received on a particular MLT that are not an integral number of octets in length and do not pass the FCS check. The count represented by an instance of this object is incremented when the alignmentError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
FCSErrors	A count of frames received on an MLT that are an integral number of octets in length but do not pass the FCS check. The count represented by an instance of this object is incremented when the frameCheckError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
IMacTransmitError	A count of frames for which transmission on a particular MLT fails due to an internal MAC sublayer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the LateCollisions object, the ExcessiveCollisions object, or the CarrierSenseErrors object.
IMacReceiveError	A count of frames for which reception on a particular MLT fails due to an internal MAC sublayer receive error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the FrameTooLongs object, the AlignmentErrors object, or the FCSErrors object. The precise meaning of the count represented by an instance of this object is implementation specific. In particular, an instance of this object may represent a count of receive errors on a particular interface that are not otherwise counted.
CarrierSenseError	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular MLT. The count represented by an instance of this object is incremented at most once per transmission attempt, even if the carrier sense condition fluctuates during a transmission attempt.

Table 23 Statistics, MLT dialog box—Ethernet Errors tab fields (continued)

Field	Description
FrameTooLong	A count of frames received on a particular MLT that exceed the maximum permitted frame size. The count represented by an instance of this object is incremented when the frameTooLong status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
SQETestError	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular MLT. The SQE TEST ERROR message is defined in section 7.2.2.2.4 of ANSI/IEEE 802.3-1985 and its generation is described in section 7.2.4.6 of the same document.
DeferredTransmiss	A count of frames for which the first transmission attempt on a particular MLT is delayed because the medium is busy. The count represented by an instance of this object does not include frames involved in collisions.
SingleCollFrames	A count of successfully transmitted frames on a particular MLT for which transmission is inhibited by exactly one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts object, the ifOutMulticastPkts object, or the ifOutBroadcastPkts object, and is not counted by the corresponding instance of the MultipleCollisionFrames object.
MultipleCollFrames	A count of successfully transmitted frames on a particular MLT for which transmission is inhibited by more than one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts object, the ifOutMulticastPkts object, or the ifOutBroadcastPkts object, and is not counted by the corresponding instance of the SingleCollisionFrames object.
LateCollisions	The number of times that a collision is detected on a particular MLT later than 512 bit-times into the transmission of a packet; 512 corresponds to 51.2 microseconds on a 10 Mb/s system. A (late) collision included in a count represented by an instance of this object is also considered as a (generic) collision for purposes of other collision-related statistics.
ExcessiveCollis	A count of frames for which transmission on a particular MLT fails due to excessive collisions.

Configuring an SMLT

This section describes how to use Device Manager (DM) to configure Split MultiLink Trunking (SMLT) and includes the following topics:

- "Adding an MLT-based SMLT" on page 168
- "Viewing SMLTs configured on your switch" on page 170
- "Adding ports to an MLT-based SMLT" on page 172
- "Configuring an IST MLT" on page 173
- "Viewing IST statistics" on page 174
- "Configuring single port SMLT" on page 177
- "Viewing configured single port SMLTs" on page 179

For more information about SMLT, see "About Split Multilink Trunking (SMLT)" on page 59.

Adding an MLT-based SMLT

If you are configuring SMLT with Device Manager, you do not need to create an MLT before creating an SMLT. You can create an SMLT by selecting the MLT type as SMLT and then specifying an SMLT ID.

To add an MLT-based SMLT:

1. From the Device Manager menu bar, choose VLAN > MLT.

   The MLT dialog box opens to the MultiLink Trunks tab (Figure 70 on page 156).

2. On the MultiLink Trunks tab, click Insert.

   The MLT, Insert MultiLink Trunks dialog box (Figure 74 on page 162) opens. For field definitions, see Table 21 on page 160.

3. In the ID field, the next available MLT ID is displayed. You can use this ID or type an available MLT ID number (1-32).
4. In the PortType field, click Access or Trunk.
5. In the Name field, type a name to identify the MLT-based SMLT port.
6. In the PortMembers field, click the ellipsis (...).

The MltPortMembers dialog box (Figure 72 on page 158) opens, displaying the available ports.

7 Click the ports to include in the MLT-based SMLT.

- For 8600 modules, up to 8 same-type ports can belong to a single MLT.
- For 8100 modules, up to 4 same-type ports can belong to a single MLT.

8 Click OK.

The MltPortMembers dialog box closes and the ports are added to the PortMembers field on the Insert MultiLink Trunks tab.

9 In the VlanIds field, click the ellipsis (...).

The VlanIds dialog box (Figure 73 on page 158) opens, displaying the available VLANs.

10 Select the VLAN IDs for the MLT-based SMLT port, and click OK.

The VlanIds dialog box closes and the VLANs are added to the VlanIds field in the MLT, Insert Trunks dialog box.

11 In the MltType field, click splitMLT.

The SmltId field becomes editable.

12 In the SmltId field, type an unused SMLT ID (1 - 32).

➡ **Note:** The corresponding SMLTs between aggregation switches must have matching SMLT IDs. The same ID number must be used on both sides.

To view the SMLT IDs currently in use on the switch, see “Viewing SMLTs configured on your switch” on page 170.

13 Click Insert.

The Insert MultiLink Trunks dialog box closes, and the new MLT-based SMLT appears in the MultiLink Trunks tab.

14 From the MultiLink Trunks tab, click Apply.

The MLT-based SMLT is added.

Viewing SMLTs configured on your switch

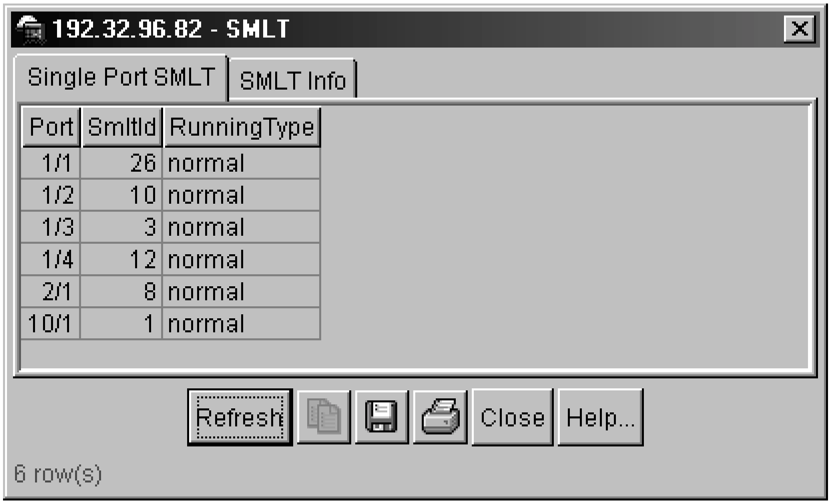
This procedure describes how to view the configured SMLTs on your switch, including both MLT-based SMLTs and single port SMLTs.

To view the SMLTs currently configured on your switch:

1 From the menu bar, choose VLAN > SMLT.

The SMLT dialog box opens to the Single Port SMLT tab (Figure 77), displaying the single port SMLTs currently configured on your switch. For field definitions, see Table 24 on page 171.

Figure 77 Single Port SMLT tab



192.32.96.82 - SMLT

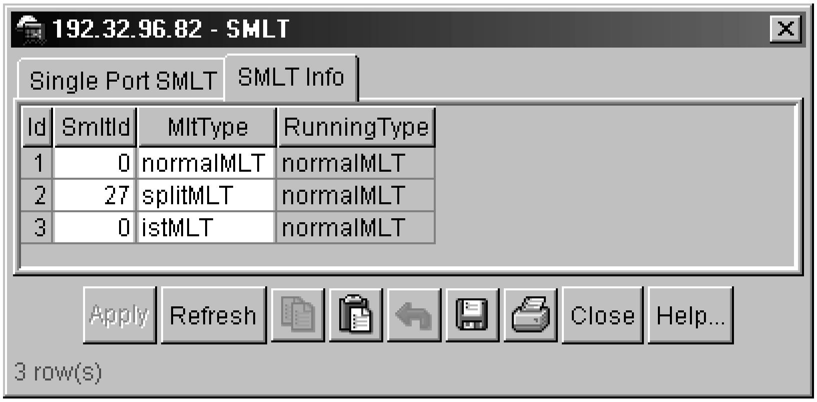
Port	SmltId	RunningType
1/1	26	normal
1/2	10	normal
1/3	3	normal
1/4	12	normal
2/1	8	normal
10/1	1	normal

6 row(s)

2 Click the SMLT Info tab.

The SMLT Info tab (Figure 78) opens, displaying all configured MLT-based SMLTs. For field definitions, see Table 25 on page 171.

Figure 78 SMLT Info tab



192.32.96.82 - SMLT

Id	SmltId	MltType	RunningType
1	0	normalMLT	normalMLT
2	27	splitMLT	normalMLT
3	0	istMLT	normalMLT

3 row(s)

Table 24 describes the fields on the Single Port SMLT tab.

Table 24 Single Port SMLT fields

Field	**Description**
Port	Read only field that displays the port’s interface index number.
SmltId	The ID number of the single port Split MLT (1 - 512).
OperType	Read only field that displays the port’s operational type: • normal • smlt (single port Split MLT)

Table 25 describes the fields on the SMLT Info tab.

Table 25 SMLT Info tab fields

Field	**Description**
Id	Read only field, displaying the MLT ID (1 - 32) for this Split MultiLink Trunk.
SmltId	The MLT-based Split MultiLink Trunk ID number (1 - 32).

Table 25 SMLT Info tab fields (continued)

Field	**Description**
MltType	Editable field for specifying the type of MLT: • normalMLT • istMLT • splitMLT
RunningType	Read only field displaying the MLT operational type: • normalMLT • istMLT • splitMLT

Adding ports to an MLT-based SMLT

To add ports to an existing MLT-based SMLT:

1 From the Device Manager menu bar, choose VLAN > MLT.

The MLT dialog box opens to the MultiLink Trunks tab (Figure 70 on page 156). For field definitions, see Table 21 on page 160.

2 Double-click the Port Members field for the MLT-based SMLT to which you are adding ports.

The MltPortMembers dialog box (Figure 74 on page 162) opens for the specified SMLT ID. Available ports are editable.

3 Select the port numbers to be added, or click All to select all ports.

- For 8600 modules, up to 8 same-type ports can belong to a single MLT.
- For 8100 modules, up to 4 same-type ports can belong to a single MLT.

4 Click OK.

The MltPortMembers dialog box closes and the ports are added to the Port Members field on the MultiLink Trunks tab.

5 From the MultiLink Trunks tab, click Apply.

The ports are added to the MLT-based SMLT.

Configuring an IST MLT

To configure an IST MLT:

1 From the Device Manager menu bar, choose VLAN > MLT.

The MLT dialog box opens to the MultiLink Trunks tab (Figure 70 on page 156).

2 In the PortMembers field for the IST MLT, click the ellipsis (...).

The MltPortMembers dialog box (Figure 72 on page 158) opens, displaying the available ports.

3 Click the port(s) to include in the IST MLT.

4 Click OK.

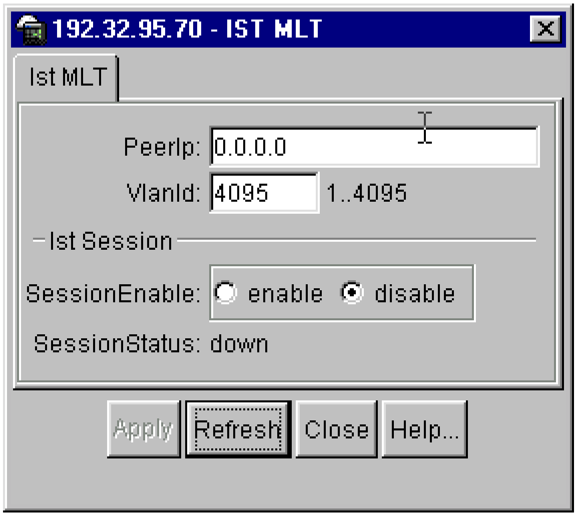
The MltPortMembers dialog box closes and the ports are added to the PortMembers field for the IST MLT in the Insert MultiLink Trunks tab.

5 Select an istMLT in the MltType field.

6 Click IstMlt.

The Ist MLT dialog box (Figure 79) opens. For field definitions, see Table 26 on page 174.

Figure 79 Ist MLT dialog box



192.32.95.70 - IST MLT

PeerIp: 0.0.0.0

VlanId: 4095 1..4095

Ist Session

SessionEnable: ○ enable ● disable

SessionStatus: down

7 In the PeerIp field, enter a peer IP address.

8 In the VlanId field, enter a VLAN ID.

9 In the Session Enable field, click either Enable or Disable.

10 Click Apply.

The IST MLT dialog box closes and the changes are applied.

11 Disable CP-Limit on the port using the CLI command:

```
config ethernet <slot/port> cp-limit disable
```

The IST MLT is configured.

For more information, see "About CP-Limit and SMLT IST" on page 64 and "Disabling CP-Limit for an IST" on page 244.

Table 26 describes the IST MLT fields.

Table 26 IST MLT fields

Field	Description
Peerip	IST MLT peer IP address.
VlanId	An IST VLAN ID number from 1 to 4095.
SessionEnable	Enable/disable IST functionality.

Viewing IST statistics

To view IST statistics on an interface:

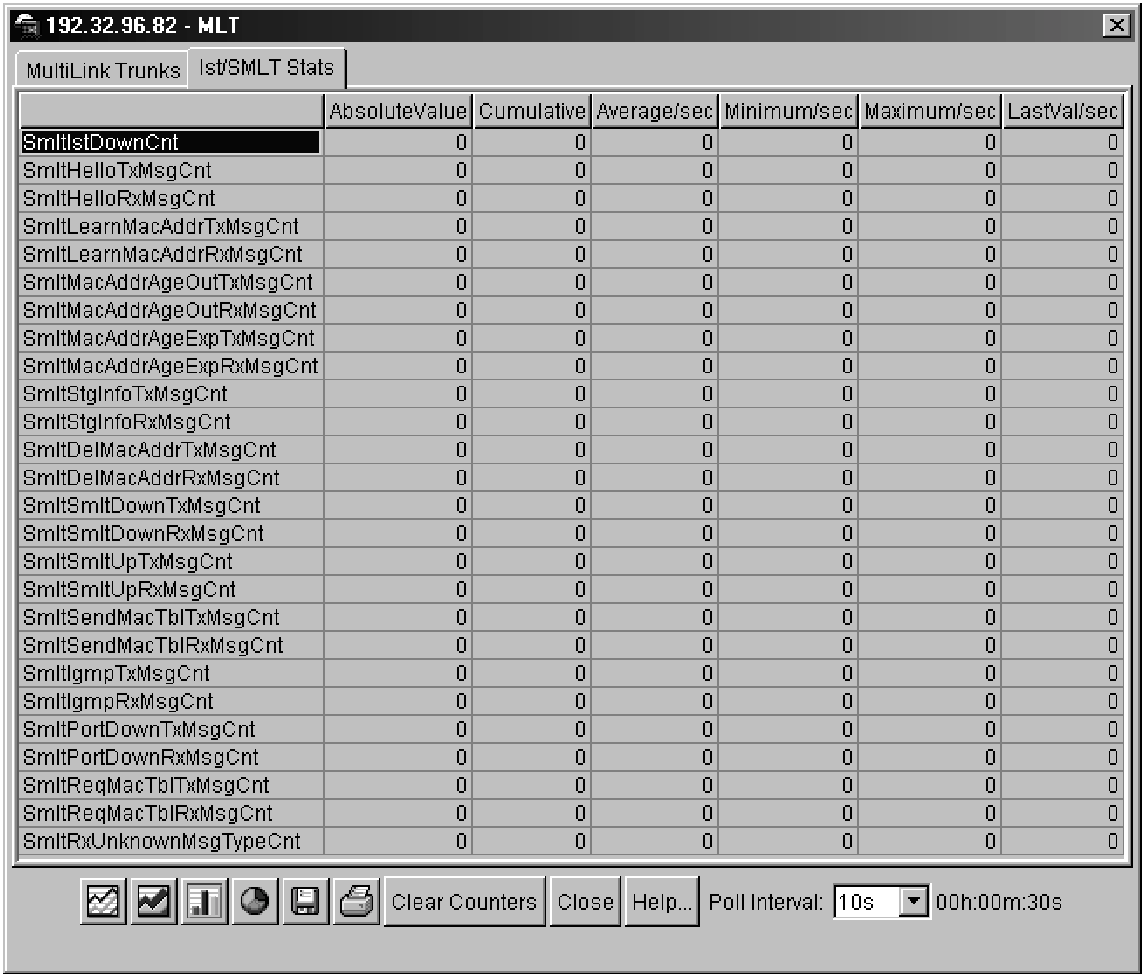
1 From the Device Manager menu bar, choose VLAN > MLT.

The MLT dialog box opens to the MultiLink Trunks tab (Figure 70 on page 156).

2 Click the Ist/SMLT Stats tab.

The IST protocol packet statistics (Figure 80) are displayed.

Figure 80 Ist/SMLT Stats tab



	AbsoluteValue	Cumulative	Average/sec	Minimum/sec	Maximum/sec	LastVal/sec
SmltIstDownCnt	0	0	0	0	0	0
SmltHelloTxMsgCnt	0	0	0	0	0	0
SmltHelloRxMsgCnt	0	0	0	0	0	0
SmltLearnMacAddrTxMsgCnt	0	0	0	0	0	0
SmltLearnMacAddrRxMsgCnt	0	0	0	0	0	0
SmltMacAddrAgeOutTxMsgCnt	0	0	0	0	0	0
SmltMacAddrAgeOutRxMsgCnt	0	0	0	0	0	0
SmltMacAddrAgeExpTxMsgCnt	0	0	0	0	0	0
SmltMacAddrAgeExpRxMsgCnt	0	0	0	0	0	0
SmltStgInfoTxMsgCnt	0	0	0	0	0	0
SmltStgInfoRxMsgCnt	0	0	0	0	0	0
SmltDelMacAddrTxMsgCnt	0	0	0	0	0	0
SmltDelMacAddrRxMsgCnt	0	0	0	0	0	0
SmltSmltDownTxMsgCnt	0	0	0	0	0	0
SmltSmltDownRxMsgCnt	0	0	0	0	0	0
SmltSmltUpTxMsgCnt	0	0	0	0	0	0
SmltSmltUpRxMsgCnt	0	0	0	0	0	0
SmltSendMacTblTxMsgCnt	0	0	0	0	0	0
SmltSendMacTblRxMsgCnt	0	0	0	0	0	0
SmltIgmpTxMsgCnt	0	0	0	0	0	0
SmltIgmpRxMsgCnt	0	0	0	0	0	0
SmltPortDownTxMsgCnt	0	0	0	0	0	0
SmltPortDownRxMsgCnt	0	0	0	0	0	0
SmltReqMacTblTxMsgCnt	0	0	0	0	0	0
SmltReqMacTblRxMsgCnt	0	0	0	0	0	0
SmltRxUnknownMsgTypeCnt	0	0	0	0	0	0

Poll Interval: 10s 00h:00m:30s

Table 27 describes the Ist/SMLT statistics.

Table 27 Ist/SMLT Stats tab fields

Field	Description
SmltIstDownCnt	The number of IST down messages.
SmltHelloTxMsgCnt	The number of hello messages transmitted.
SmltHelloRxMsgCnt	The number of hello messages received.

Table 27 Ist/SMLT Stats tab fields (continued)

Field	Description
SmltLearnMacAddrTxMsgCnt	The number of learn MAC address messages transmitted.
SmltLearnMacAddrRxMsgCnt	The number of learn MAC address messages received.
SmltMacAddrAgeOutTxMsgCnt	The number of MAC address aging out messages transmitted.
SmltMacAddrAgeOutRxMsgCnt	The number of MAC address aging out messages received.
SmltMacAddrAgeExpTxMsgCnt	The number of MAC address age expired messages transmitted.
SmltMacAddrAgeExpRxMsgCnt	The number of MAC address age expired messages received.
SmltDelMacAddrTxMsgCnt	The number of deleted MAC address messages transmitted.
SmltDelMacAddrRxMsgCnt	The number of deleted MAC address messages received.
SmltSmltDownTxMsgCnt	The number of SMLT down messages transmitted.
SmltSmltDownRxMsgCnt	The number of SMLT down messages received.
SmltSmltUpTxMsgCnt	The number of SMLT up messages transmitted.
SmltSmltUpRxMsgCnt	The number of SMLT up messages received.
SmltSendMacTblTxMsgCnt	The number of send MAC table messages transmitted.
SmltSendMacTblRxMsgCnt	The number of send MAC table messages received.
SmltIgmpTxMsgCnt	The number of IGMP messages transmitted.
SmltIgmpRxMsgCnt	The number of IGMP messages received.
SmltPortDownTxMsgCnt	The number of port down messages transmitted.
SmltPortDownRxMsgCnt	The number of port down messages received.
SmltReqMacTblTxMsgCnt	The number of request MAC table messages transmitted.
SmltReqMacTblRx MsgCnt	The number of request MAC table messages received.
SmltRxUnknownMsgTypeCnt	The number unknown SMLT messages received.

Configuring single port SMLT

Ports that are already configured as MLT or MLT-based SMLT cannot be configured as single port SMLT. You must first remove the split trunk and then reconfigure the ports as single port SMLT.

To configure single port SMLT:

1 From the Device Manager Main window, select the port.

The port is highlighted.

2 From the menu bar, choose Edit > Port.

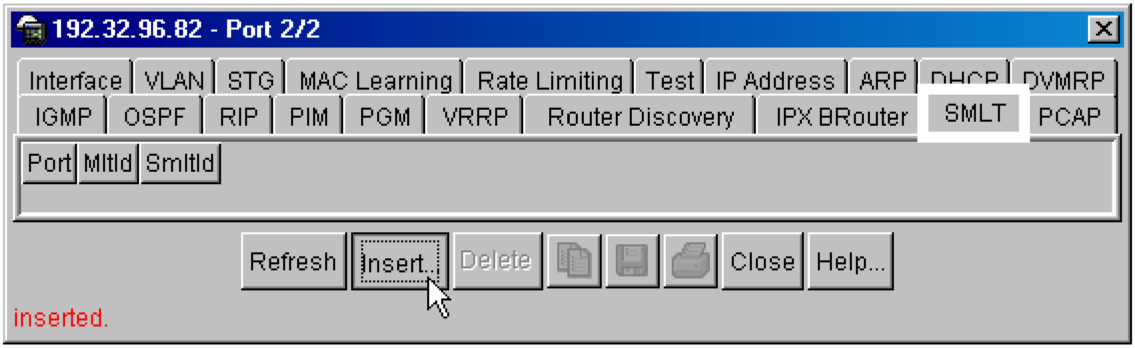
The Port dialog box opens to the Interface tab.

3 Click the SMLT tab.

The port's SMLT tab (Figure 81) opens.

➡ **Note:** This tab indicates if this port is already configured as MLT or MLT-based SMLT. If so, you cannot configure single port SMLT.

Figure 81 Port SMLT tab

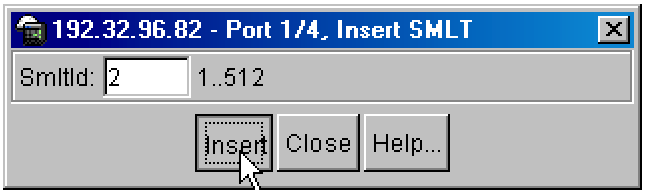


inserted.

4 Click Insert.

The Insert SMLT dialog box (Figure 82) opens.

Figure 82 Port, Insert SMLT dialog box


192.32.96.82 - Port 1/4, Insert SMLT

SmltId: 2 1..512

5 In the SmltId field, enter an unused SMLT ID number from 1 to 512.

To view the SMLT IDs that are already in use on your switch, see "Viewing SMLTs configured on your switch" on page 170.

6 Click Insert.

The Insert SMLT dialog box closes and the ID is entered into the SMLT tab.

Table 28 describes the fields on the Port SMLT tab.

Table 28 Port SMLT tab fields

Field	Description
Port	The slot/port number for the port.
MltId	Read only field, displaying one of the following: • A value of 1 - 32 indicates that the port is part of an MLT, and single port SMLT cannot be configured on this port. • A value of 0 indicates that no MLT is assigned, and the port can be configured for single port SMLT.
SmltId	The Split MLT ID, an integer from 1 to 512. • A read-only field with a value of 1-512 indicates the port's single port SMLT ID assignment. • A blank field indicates the port is not configured for single port SMLT. Find an unused SMLT ID by viewing the currently-used IDs. See "Viewing SMLTs configured on your switch" on page 170.

Deleting a single port SMLT

To delete a single port SMLT:

1 From the Device Manager Main window, select the port.

The port is highlighted.

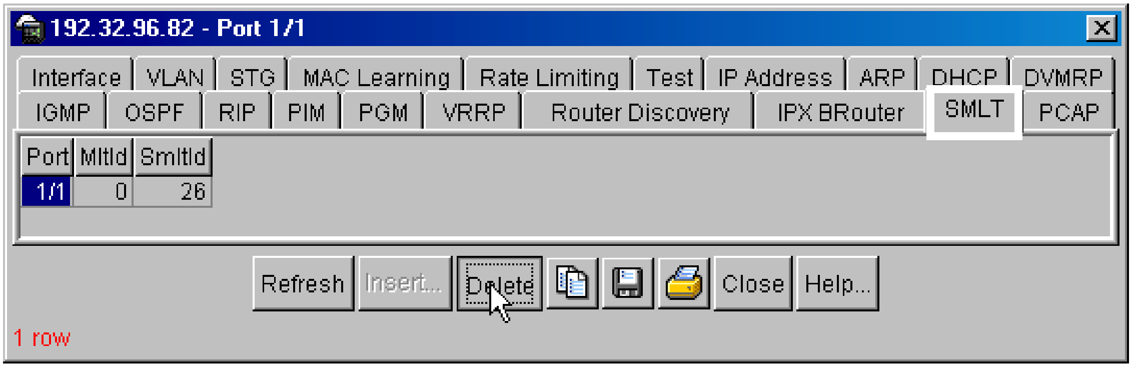
2 From the menu bar, choose Edit > Port.

The Port dialog box opens to the Interface tab.

3 Click the SMLT tab.

The port's SMLT tab (Figure 83) opens, displaying the single port SMLT ID.

Figure 83 Deleting a single port SMLT



Port	MltId	SmltId
1/1	0	26

1 row

4 Select the single port SMLT.

The single port SMLT is highlighted.

5 Click Delete >Close.

The single port SMLT is deleted.

Viewing configured single port SMLTs

This procedure describes how to view the configured single port SMLTs on your switch. To view the configured MLT-based SMLTs, see "Viewing SMLTs configured on your switch" on page 170.

To view the single port SMLTs configured on your switch:

➔ From the menu bar, choose VLAN > SMLT.

The SMLT dialog box opens to the Single Port SMLT tab (Figure 77 on page 170), displaying those currently configured.

Chapter 6
Configuring and managing VLANs using the CLI

This chapter includes overview information about VLANs and then describes a number of VLAN commands. It includes the following topics:

For more information about VLANs, see "About VLANs" on page 23.

Roadmap of VLAN commands

The following roadmap lists the VLAN commands and their parameters. Use this list as a quick reference or click on any entry for more information.

Command	Parameter
`config vlan <vid> create`	`info`
	`byipsubnet <sid> <ipaddr/mask> [name <value>] [color <value>]`
	`byport <sid> [name <value>] [color <value>]`

Command	Parameter
	byprotocol <sid> <ip|ipx802dot3|ipx802dot2|ipxSnap|ipxEthernet2|appleTalk|decLat|decOther|sna802dot2|snaEthernet2|netBios|xns|vines|ipV6|usrDefined|rarp|PPPoE> [<pid>] [name <value>] [color <value>] [encap <value>]
	bysrcmac <sid> [name <value>] [color <value>]
config vlan <vid>	info
	action <action choice>
	add-mlt <integer>
	agetime <10..1000000>
	delete
	name <vname>
	qos-level <integer>
config vlan <vid> fdb	
config vlan <vid> fdb-entry	info
	aging-time <seconds>
	flush
	monitor <mac> status <value> <true|false>
	qos-level <integer>
	sync
config vlan <vid> fdb-filter	info
	add <mac> port <value> [qos <value>]
	remove <mac>
config vlan <vid> fdb-filter notallowfrom	info
	add <mac> port <value> [qos <value>]
	remove <mac>

Command	Parameter
config vlan <vid> fdb-static	info
	add <mac> port <value> [qos <value>]
	remove <mac>
config vlan <vid> ports	info
	add <ports> [member <value>]
	remove <ports> [member <value>]
config vlan <vid> srcmac	info
	add <macaddr>
	remove <macaddr>
show vlan info all [<vid>] [by <value>]	
show vlan info fdb-entry <vid>	
show vlan info fdb-filter <vid>	
show vlan info fdb-static <vid>	
show vlan info advance [<vid>]	
show vlan info arp [<vid>]	
show vlan info basic [<vid>]	
show vlan info brouter-port [<vid>]	
show vlan info igmp [<vid>]	
show vlan info ports [<vid>]	
show vlan info srcmac [<vid>]	
config vlan <vid> ip	
show vlan info ip [<vid>]	
config sys set flag Enhanced-operational-mode	true
	false

Configuring VLANs

To create VLANs, add or remove ports in the VLAN, set priority, change a VLAN name, and perform other operation, use the VLAN configuration commands. In all VLAN commands, *vid* is the VLAN ID (from 1 to 4094).

This section includes the following procedures:

- "Creating a VLAN" on page 184," next
- "Performing general VLAN operations" on page 186
- "Configuring VLAN parameters in the forwarding database" on page 188
- "Adding or removing VLAN ports" on page 191
- "Adding or removing VLAN source MAC addresses

Creating a VLAN

To create a VLAN, use the following command:

```
config vlan <vid> create
```

You can specify the type of VLAN and assign an IP address to the VLAN using this command. The required parameter *vid* is the VLAN ID (from 1 to 4094). VLAN 1 is the default VLAN.

This command includes the following parameters:

<table>
<tr><th colspan="2"><b>config vlan <<i>vid</i>> create</b>
followed by:</th></tr>
<tr><td>info</td><td>Displays information about the type of the specified VLAN.</td></tr>
<tr><td>byipsubnet <<i>sid</i>> <<i>ipaddr/mask</i>> [name <<i>value</i>>] [color <<i>value</i>>]</td><td>Creates an IP subnet-based VLAN.
• <i>sid</i> is a spanning tree group ID from 1 to 25 characters.
• <i>ipaddr/mask</i> is the IP address and mask {a.b.c.d/x | a.b.c.d/x.x.x.x | default}.
• name <<i>value</i>> is the name of the VLAN from 0 to 20 characters.
• color <<i>value</i>> is the color of the VLAN (0 to 32). The color attribute is used by Optivity software to display the VLAN.
This command is available only for Passport 8600 switches.</td></tr>
<tr><td>byport <sid> [name <<i>value</i>>] [color <<i>value</i>>]</td><td>Creates a port-based VLAN.
• <i>sid</i> is the spanning tree group ID from 1 to 25 characters.
• name <<i>value</i>> is the name of the VLAN. from 0 to 20 characters.
• color <<i>value</i>> is the color of the VLAN {0..32}. The color attribute is used by Optivity software to display the VLAN.</td></tr>
<tr><td>byprotocol <sid> <ip|ipx802dot3|ipx802dot2|ipxSnap|ipxEthernet2|appleTalk|decLat|decOther|sna802dot2|snaEthernet2|netBios|xns|vines|ipV6|usrDefined|rarp|PPPoE> [<pid>] [name <value>] [color <value>] [encap <value>]</td><td>Creates a protocol-based VLAN.
• <i>sid</i> is spanning tree ID 1 to 25.
• <i>ip|ipx802dot3|ipx802dot2|ipxSnap|ipxEthernet2|appleTalk|decLat|decOther|sna802dot2|snaEthernet2|netBios|xns|vines|ipV6|usrDefined|rarp</i> |PPPoE specifies the protocol.
• <i>pid</i> is a user-defined protocol ID number in hexadecimal (0 to 65535).
• name <<i>value</i>> is the name of the VLAN from 0 to 20 characters.
• color <<i>value</i>> is the color of the VLAN (0 to 32). The color attribute is used by Optivity software to display the VLAN.
• encap <<i>value</i>> is the frame encapsulation method.</td></tr>
</table>

config vlan <*vid*> create followed by:	
bysrcmac <*sid*> [name <*value*>] [color <*value*>]	Creates a VLAN by source MAC address. • *sid* is spanning tree ID 1 to 25. • name <*value*> is the name of the VLAN from 0 to 20 characters. • color <*value*> is the color of the VLAN (0 to 32). The color attribute is used by Optivity software to display the VLAN. This command is available only for Passport 8600 switches.
bysvlan <*sid*> [name <*value*>] [color <*value*>]	This option is not available in the Passport 8000 software.

Figure 84 shows sample output for the **config vlan create info** command.

Figure 84 config vlan create info command output

```
8100:5# config vlan 1 create info

Sub-Context: clear config dump monitor show test trace
Current Context:

                      byport :
                                   sid - 1
                                  name - Default
                                 color - 0 (white)
```

Performing general VLAN operations

To perform general VLAN operations, such a setting a QoS level for the VLAN or adding or changing the name of a VLAN, use the following command:

config vlan <*vid*>

In all VLAN commands, *vid* is the VLAN ID (from 1 to 4094).

This command includes the following options:

config vlan <*vid*> followed by:	
`info`	Displays characteristics of the specified VLAN (Figure 85).
`action <action choice>`	Flushes a table or triggers an RIP update. - *action choice* is `{none|flushMacFdb|flushArp|flushIp|flushDynMemb|all|flushSnoopMemb|triggerRipUpdate|flushSenders|flushSnoopMRtr}`. To flush all tables, use `all`.
`add-mlt <integer>`	Adds an MLT to a VLAN. *integer* is the MLT ID (1 to 32).
`agetime <10..1000000>`	Sets the VLAN aging time in seconds (10 to 1000000).
`delete`	Deletes a VLAN.
`name <vname>`	Changes the name of a VLAN. *vname* is a string from 0 to 20 characters.
`qos-level <integer>`	Sets a Quality of Service (QoS) level for a VLAN. *integer* is the QOS level (0 to 7).

Figure 85 shows sample output for the **config vlan info** command.

Figure 85 config vlan info command output

```
8100:5# config vlan 1 info

Sub-Context: clear config dump monitor show trace
Current Context:

                      action : N/A
                     add-mlt :
                     agetime : N/A
                      delete : N/A
                    qoslevel : 1
                        name : Default
```

Configuring VLAN parameters in the forwarding database

To configure VLAN parameters in the forwarding database, enter the following command:

```
config vlan <vid> fdb
```

This section includes the following topics:

- "Configuring or modifying VLAN entries in the forwarding database," next
- "Configuring VLAN filter members" on page 189
- "Setting or modifying VLAN not allowed filter member parameters" on page 190
- "Configuring VLAN static member parameters" on page 190

Configuring or modifying VLAN entries in the forwarding database

To configure or modify VLAN entries in the forwarding database, enter the following command:

```
config vlan <vid> fdb-entry
```

This command includes the following options:

config vlan <*vid*> fdb-entry followed by:	
`info`	Displays current level parameter settings and next level directories.
`aging-time <seconds>`	Sets the forwarding database aging timer. • *seconds* indicates the time out period in seconds {10..1000000}
`flush`	Flushes forwarding database.

config vlan <*vid*> fdb-entry followed by:	
`monitor <mac> status <value> <true|false>`	Sets forwarding database monitor parameters. • *mac* indicates the MAC address • `status <value>` allows you to view the current status of the forwarding database according to one of the following choices: {other|invalid|learned|self|mgmt} • `true|false` enables or disables the monitor.
`qos-level <integer>`	Sets a QoS Level for a VLAN. • *integer* allows you to choose a QoS level from 0 through 7.
`sync`	Allows you to synchronize the switch's forwarding database with the forwarding database of the other aggregation switch.

Configuring VLAN filter members

To configure VLAN filter members, enter the following command:

```
config vlan <vid> fdb-filter
```

The **config vlan <vid> fdb-filter** command includes the following options:

config vlan <*vid*> fdb-filter followed by:	
`info`	Displays current level parameter settings and next level directories.
`add <mac> port <value> [qos <value>]`	Allows you to add a filter member to a VLAN bridge. • `<mac>` indicates the MAC address • `port <value>` indicates the port (slot/port) number. • `qos <value>` is the Quality of Service level.

config vlan <*vid*> fdb-filter followed by:	
`pcap <mac> <enable|disable>`	Allows to you enable or disable the packet capture tool (PCAP). • *<mac>* indicates the MAC address For more information about PCAP, see the publication *Using the Packet Capture Tool*, part number 315023.
`remove` *<mac>*	Allows you to remove a filter member from a VLAN bridge. • *<mac>* indicates the MAC address

Setting or modifying VLAN not allowed filter member parameters

To set or modify VLAN not allowed filter member parameters, enter the following command:

```
config vlan <vid> fdb-filter notallowfrom
```

This command includes the following options:

config vlan <*vid*> fdb-filter notallowfrom followed by:	
`info`	Displays current level parameter settings and next level directories.
`add` *<mac>* `port` *<value>*	Allows you to add a not allowed filter member to a VLAN bridge. • *<mac>* indicates the MAC address • *<value>* indicates the port (slot/port) number.
`remove` *<mac>*	Allows you to remove a not allowed filter member from a VLAN bridge. • *<mac>* indicates the MAC address

Configuring VLAN static member parameters

To configure VLAN static member parameters, enter the following command:

```
config vlan <vid> fdb-static
```

This command includes the following options:

config vlan ***<vid>*** **fdb-static** followed by:	
`info`	Displays current level parameter settings and next level directories.
`add <mac> port <value> [qos <value>]`	Allows you to add a static member to a vlan bridge. • *<mac>* indicates the MAC address • *<value>* indicates the port (slot/port) number. • `qos` *<value>* is the Quality of Service level.
`remove <mac>`	Allows you to remove a static member from a VLAN bridge. • *<mac>* indicates the MAC address

Adding or removing VLAN ports

To add or remove ports in the VLAN, enter the following command:

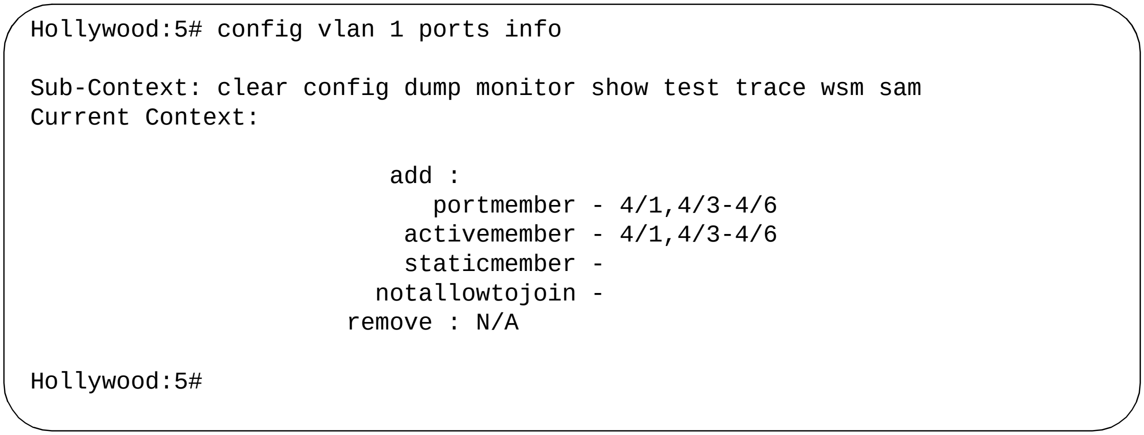
```
config vlan <vid> ports
```

This command includes the following options:

config vlan ***<vid>*** **ports** followed by:	
`info`	Displays member status of the ports in the VLAN (Figure 86 on page 192).
`add <ports> [member <value>]`	Adds one or more ports to an existing VLAN. • *ports* is the port list. • `member` *<value>* is the port member type. It can be `portmember` (always a member), `static` (sometimes a member), or `notallowed` (never a member).
`remove <ports> [member <value>]`	Removes ports from a VLAN but does not delete the VLAN. • *ports* is the port list. • `member` *<value>* is the port member type. It can be `portmember` (always a member), `static` (sometimes a member), or `notallowed` (never a member).

Figure 86 shows sample output for the **`config vlan ports info`** command.

Figure 86 config vlan ports info command output



```
Hollywood:5# config vlan 1 ports info

Sub-Context: clear config dump monitor show test trace wsm sam
Current Context:

                         add :
                            portmember - 4/1,4/3-4/6
                          activemember - 4/1,4/3-4/6
                          staticmember -
                        notallowtojoin -
                      remove : N/A

Hollywood:5#
```

Adding or removing VLAN source MAC addresses

To add or remove VLAN source MAC addresses, enter the following command:

`config vlan <vid> srcmac`

This command includes the following options:

config vlan <*vid*> srcmac followed by:	
`info`	Displays current level parameter settings and next level directories.
`add <macaddr>`	Adds a source MAC address to a VLAN. • *macaddr* is the MAC address to be added.
`remove <macaddr>`	Removes a source MAC address from a VLAN. • *macaddr* is the MAC address to be removed.

Using the VLAN show commands

To obtain configuration information about all VLANs on the switch or specified VLANs, use the **show vlan** commands.

Displaying general VLAN information

To display all general information about the VLANs on the switch or a specified VLAN, enter the following command:

```
show vlan info all [<vid>] [by <value>]
```

where:
`by <value>` groups the information by ID number or by each feature.

Displaying information for specified VLANs

To display information for the specified VLANs, use the show commands. This section provides the following show command procedures:

- "Displaying forwarding database information" on page 193," next
- "Displaying forwarding database filters" on page 194
- "Displaying database status, MAC address, and QoS levels" on page 195

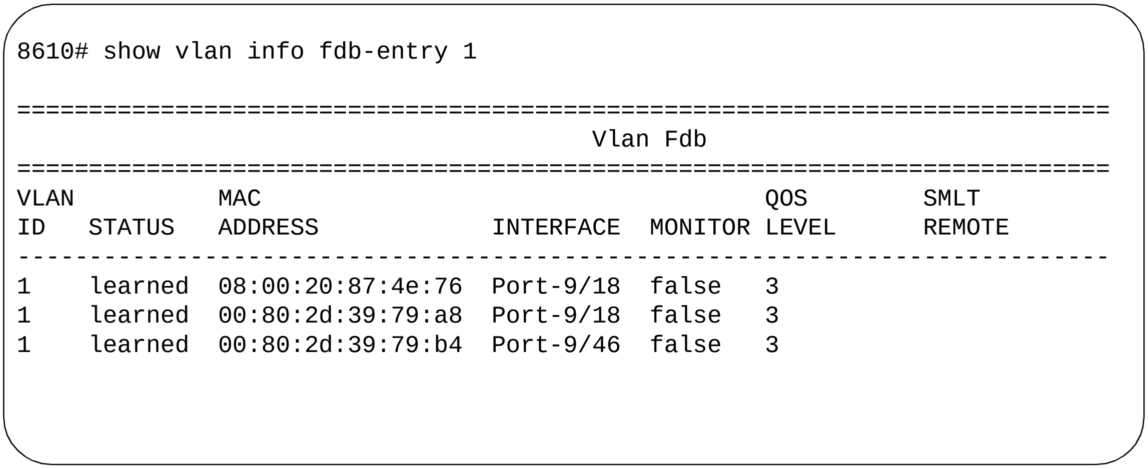
Displaying forwarding database information

To display forwarding database information for the specified VLAN, enter the following command:

```
show vlan info fdb-entry <vid>
```

Figure 87 shows sample output for the **`show vlan info fdb-entry`** command.

Figure 87 show vlan info fdb-entry command output



```
8610# show vlan info fdb-entry 1

============================================================================
                                        Vlan Fdb
============================================================================
VLAN          MAC                                          QOS        SMLT
ID   STATUS   ADDRESS            INTERFACE  MONITOR LEVEL      REMOTE
----------------------------------------------------------------------------
1    learned  08:00:20:87:4e:76  Port-9/18  false   3
1    learned  00:80:2d:39:79:a8  Port-9/18  false   3
1    learned  00:80:2d:39:79:b4  Port-9/46  false   3
```

Displaying forwarding database filters

To display the forwarding database filters for the specified VLAN, enter the following command:

```
show vlan info fdb-filter <vid>
```

The display includes the VLAN ID, the status, the VLAN MAC address, and the ports from which the VLAN is not allowed to receive frames.

This command is available only for the Passport 8600 Switch.

Figure 88 shows sample output for the **`show vlan info fdb-filter`** command.

Figure 88 show vlan info fdb-filter command output

```
8610:5# show vlan info fdb-filter 1
=============================================================================
                                        Vlan Filter
=============================================================================
VLAN           MAC                        DEST_DISCARD          SRC_DISCARD
ID   STATUS    ADDRESS       PORT PCAP    SET                   SET
-----------------------------------------------------------------------------

8610:5#
```

Displaying database status, MAC address, and QoS levels

To display the static forwarding database status, the VLAN MAC address, and the QoS level for the specified VLAN, enter the following command:

`show vlan info fdb-static <`*`vid`*`>`

Figure 89 shows sample output for the **`show vlan info fdb-static`** command.

Figure 89 show vlan info fdb-static command output

```
8610# show vlan info fdb-static 1

============================================================================
                                        Vlan Static
============================================================================
VLAN                 MAC                                QOS
ID   STATUS          ADDRESS           PORT   MONITOR LEVEL
----------------------------------------------------------------------------
1    learned        08:12:20:38:4e:76  1/1    1/2     7
```

Displaying additional parameters

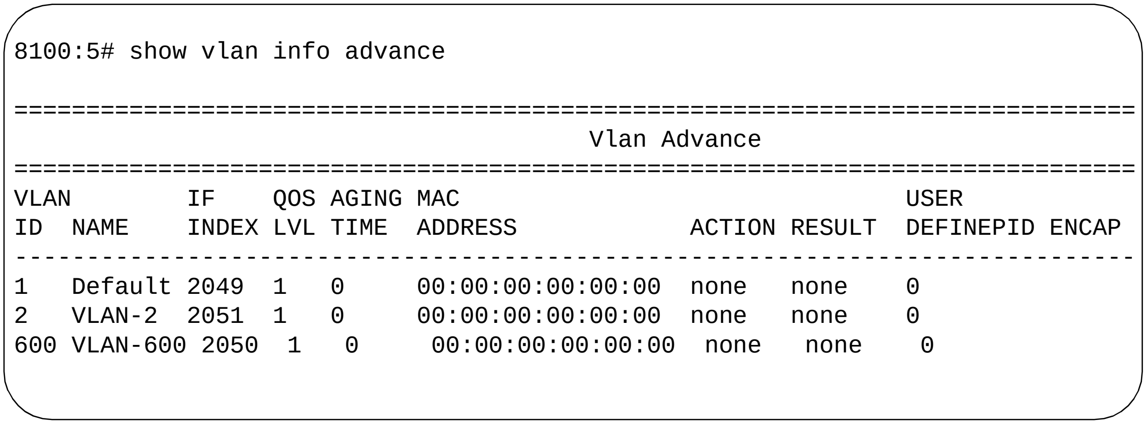
To display additional parameters for the specified VLAN or all VLANs, enter the following command:

```
show vlan info advance [<vid>]
```

All zeros in the MAC ADDRESS column indicate that there is no IP address associated with that VLAN.

Figure 90 shows sample output for the **show vlan info advance** command.

Figure 90 show vlan info advance command output



```
8100:5# show vlan info advance

==============================================================================
                                        Vlan Advance
==============================================================================
VLAN        IF    QOS AGING MAC                               USER
ID  NAME    INDEX LVL TIME  ADDRESS            ACTION RESULT  DEFINEPID ENCAP
------------------------------------------------------------------------------
1   Default 2049  1   0     00:00:00:00:00:00  none   none    0
2   VLAN-2  2051  1   0     00:00:00:00:00:00  none   none    0
600 VLAN-600 2050  1   0     00:00:00:00:00:00  none   none    0
```

Displaying ARP configuration

To display the ARP configuration for all VLANs or the specified VLAN, enter the following command:

```
show vlan info arp [<vid>]
```

Figure 91 shows sample output for the **show vlan info arp** command.

Figure 91 show vlan info arp command output

```
8010# show vlan info arp

==============================================================
                                        Vlan Arp
==============================================================
VLAN ID  DOPROXY    DORESP
--------------------------------------------------------------
1        false      true
2        false      true
3        false      true
4        false      true
```

Displaying basic configuration

To display the basic configuration for all VLANs or the specified VLAN, enter the following command:

```
show vlan info basic [<vid>]
```

Figure 92 shows sample output for the **show vlan info basic** command.

Figure 92 show vlan info basic command output

```
8606# show vlan info basic

==============================================================================
                                        Vlan Basic
==============================================================================
VLAN                                 STG
ID   NAME                TYPE         ID  PROTOCOLID SUBNETADDR      SUBNETMASK
------------------------------------------------------------------------------
1    Default             byPort       1   none       N/A             N/A
2    VLAN-2              byPort       2   none       N/A             N/A
3    VLAN-3              byProtocolId 3   ip         N/A             N/A
```

Displaying brouter port status

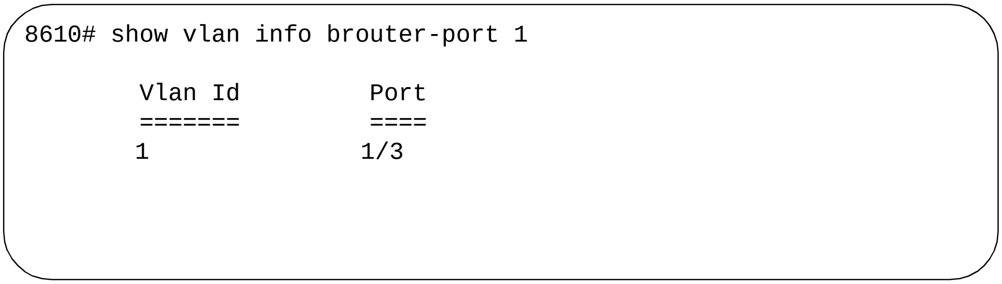
To display the brouter port status for all VLANs on the switch or for the specified VLAN, enter the following command:

```
show vlan info brouter-port [<vid>]
```

This command is available only for Passport 8600 switches.

Figure 93 shows sample output for the **`show vlan info brouter-port`** command.

Figure 93 show vlan info brouter-port command output



```
8610# show vlan info brouter-port 1

        Vlan Id         Port
        =======         ====
       1               1/3
```

Displaying IGMP switch operation information

To display information about the IGMP operation in the switch, enter the following command:

```
show vlan info igmp [<vid>]
```

Figure 94 shows sample output for the **show vlan info igmp** command.

Figure 94 show vlan info igmp command output

```
8610:6# show vlan info igmp 1

=============================================================================
                                        Vlan Ip Igmp
=============================================================================
VLAN QUERY QUERY ROBUST VERSION LAST  PROXY  SNOOP  FAST   FAST
ID   INTVL MAX                  MEMB  SNOOP  ENABLE LEAVE  LEAVE
           RESP                 QUERY ENABLE        ENABLE PORTS
-----------------------------------------------------------------------------
1    125   10    2      2       1     false  false  false
```

Displaying port member status

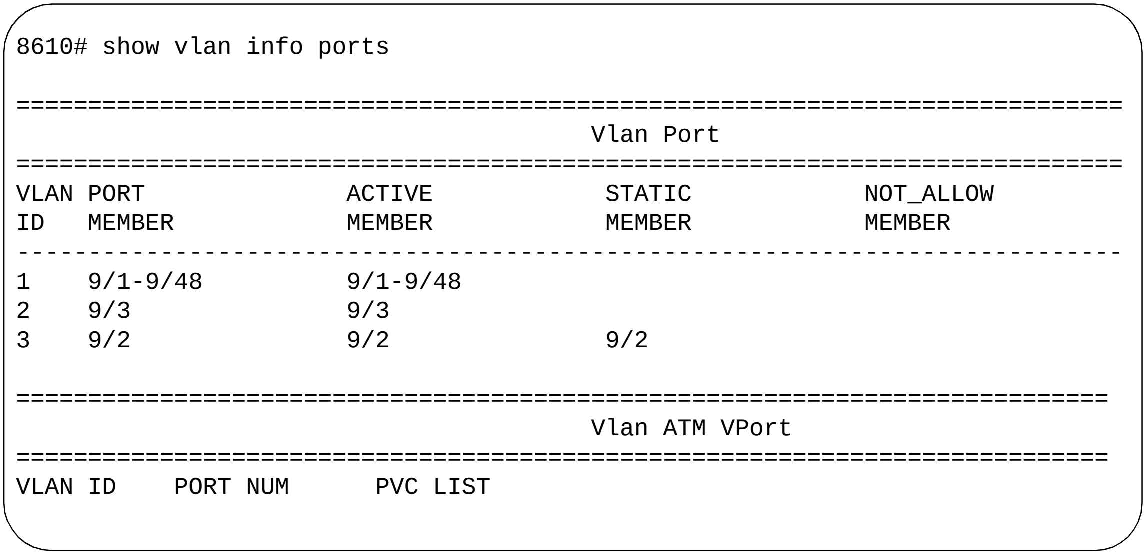
To display the port member status for all VLANs on the switch or for the specified VLAN, enter the following command:

```
show vlan info ports [<vid>]
```

A port can be an active member, a static member, or a not-allowed member.

Figure 95 shows sample output for the **`show vlan info ports`** command.

Figure 95 show vlan info ports command output



```
8610# show vlan info ports

=============================================================================
                                        Vlan Port
=============================================================================
VLAN PORT                  ACTIVE                STATIC                NOT_ALLOW
ID   MEMBER                MEMBER                MEMBER                MEMBER
-----------------------------------------------------------------------------
1    9/1-9/48              9/1-9/48
2    9/3                   9/3
3    9/2                   9/2                   9/2

============================================================================
                                        Vlan ATM VPort
============================================================================
VLAN ID     PORT NUM      PVC LIST
```

Displaying source MAC addresses

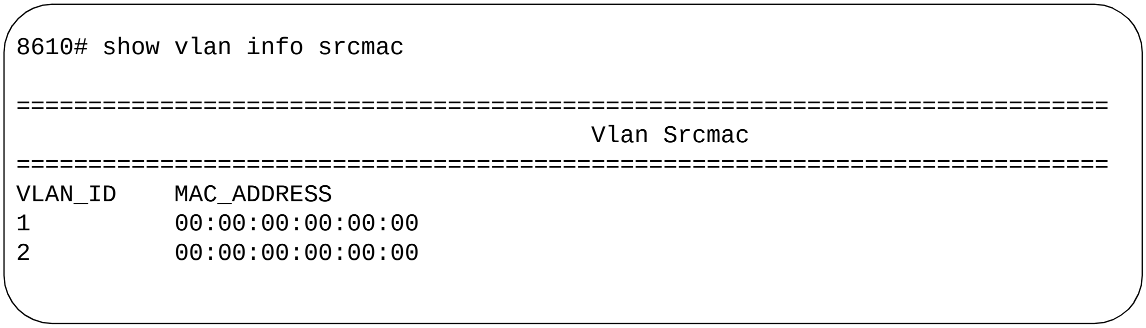
To display the source MAC address for any source MAC-based VLANs on the switch, or for the specified VLAN, if it is source MAC-based, enter the following command:

`show vlan info srcmac [<`*`vid`*`>]`

This command is available only for the Passport 8600 switch.

Figure 96 shows sample output for the **`show vlan info srcmac`** command.

Figure 96 show vlan info srcmac command output



```
8610# show vlan info srcmac

============================================================================
                                        Vlan Srcmac
============================================================================
VLAN_ID    MAC_ADDRESS
1          00:00:00:00:00:00
2          00:00:00:00:00:00
```

Using the VLAN IP commands

The VLAN IP commands described in this section are general routing commands for the VLAN. Other VLAN commands are included in the sections of this manual that describe commands used with a specific protocol or feature (for example, DHCP).

Assigning an IP address to a VLAN

To assign an IP address to a VLAN, use the following command:

```
config vlan <vid> ip
```

This command requires a VLAN ID *`vid`* from 1 to 4094.

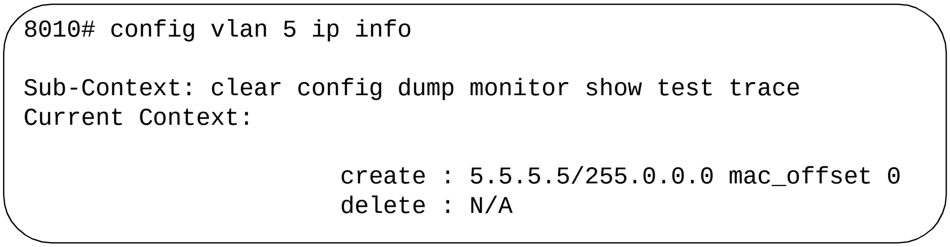
On 8100 switches, only VLAN ID 1 can be configured with an IP address.

This command includes the following options:

config vlan <*vid*> ip followed by:	
info	Displays current level parameter settings and next level directories.
create <*ipaddr/mask*> [mac_offset <*value*>]	Assigns an IP address and subnet mask to the VLAN. • *ipaddr/mask* is the IP address and mask {a.b.c.d}. • mac_offset <*value*> is a user-assigned MAC address. This MAC address is in place of the default MAC address.
delete <*ipaddr*>	Deletes the specified VLAN address.

Figure 97 shows sample output for the **config vlan ip info** command.

Figure 97 config vlan ip info command output



```
8010# config vlan 5 ip info

Sub-Context: clear config dump monitor show test trace
Current Context:

                              create : 5.5.5.5/255.0.0.0 mac_offset 0
                              delete : N/A
```

Displaying routing (IP) configuration

To display the routing (IP) configuration for all VLANs on the switch or for the specified VLAN, enter the following command:

```
show vlan info ip [<vid>]
```

Figure 98 shows sample output for the **show vlan info ip** command.

Figure 98 show vlan info ip command output

```
8610:5# show vlan info ip

=============================================================================
                                        Vlan Ip
=============================================================================
VLAN IP               NET              BCASTADDR REASM    ADVERTISE  DIRECTED
ID   ADDRESS          MASK            FORMAT    MAXSIZE  WHEN_DOWN  BROADCAST
-----------------------------------------------------------------------------
2    1.1.1.1          255.0.0.0        ones      1500     disable    enable

 rc = 00000000
 tparm = 00000000
 rc = 00000000
 tparm = 00000000
 rc = 00000000
 tparm = 00000000
```

Configuring Enhanced Operation mode

Enhanced operation mode enables the 8000 Series switch to support more VLANs. With MLT, you can create a maximum of 1980 VLANs. With SMLT, the limit is 989 VLANs. For more information on enhanced operation concepts, see "About MultiLink trunking and VLAN scalability" on page 40.

To configure enhanced operation for 1980 VLANs on the 8000 Series switch, use the following command:

```
config sys set flag Enhanced-operational-mode
```

The command includes the following parameters:

You must save the configuration and reset the chassis before the change takes effect.

The **`config sys set flag Enhanced-operational-mode`** command includes the following options:

`config sys set flag Enhanced-operational-mode` followed by:	
`true`	Enables enhanced operation mode to support 1980 VLANs for the system.
`false`	Disables enhanced operation mode for the system.

Configuration example 1

This configuration example uses the above commands to configure support for 1980 VLANs and show a summary of the results using the **`config sys set info`** command.

```
8610:5# config sys set flag Enhanced-operational-mode true
WARNING: The changes made will take effect only after reboot
8610:5# conf sys set flag info

Sub-Context: clear config dump monitor show test trace wsm
Current Context:
          em-mode: (true) -> true
          Enhanced-operational-mode: (true) -> true
8610:5#
```

Chapter 7
Configuring sVLANs using the CLI

The sVLAN protocol transparently transports packets through an sVLAN domain by adding an additional 4-byte header to each packet. This section describes how to configure sVLANs using the CLI and includes the following topics:

- "Overview of sVLAN CLI configuration" on page 207
- "Setting the ether-type and switch level" on page 208
- "Showing ether-type and switch level information" on page 211
- "Setting the sVLAN port type" on page 212
- "Creating an sVLAN STG" on page 213
- "Adding UNI or NNI ports to the STG" on page 215
- "Creating an sVLAN" on page 216
- "Configuration example" on page 217

For more information about sVLANs, see "About stacked VLANs" on page 42.

Overview of sVLAN CLI configuration

Follow these steps to create an sVLAN using the CLI:

Note: You must follow these steps in sequence to configure an sVLAN.

1 Set the sVLAN switch level to a 1 or above.

For more information, see "Setting the ether-type and switch level" on page 208."

2 Configure UNI and NNI ports.

For more information, see "Setting the sVLAN port type" on page 212."

3. Create a STG of type sVLAN and set the tagged BPDU address as different from the standardized BPDU.

   For more information, see "Creating an sVLAN STG" on page 213."

4. Add UNI or NNI ports to the STG.

   For more information, see "Adding UNI or NNI ports to the STG" on page 215."

5. Create VLAN of type sVLAN within the STG created in Step 3 and add ports to it.

   For more information, see "Creating an sVLAN" on page 216."

Setting the ether-type and switch level

To set the ether-type and switch level, use the following commands:

`config svlan ether-type level <value> <ethertype>` (sets the ether-type)

`config svlan level <value>` (sets the switch level)

For sVLAN configurations, you must set the switch level to 1 or above.

The **`config svlan`** command includes the following parameters:

`config svlan` followed by:	
`info`	Displays current configuration information for an sVLAN (Figure 99).
`ether-type [level <`*`value`*`>]<`*`ethertype`*`>`	Sets an sVLAN tag for a switch level. <*value*> is an integer value in the range of 0 to 7 <*ethertype*> 8 default values which correspond to switch levels as follows: • Level 0 — 0x8100 • Level 1 — 0x8020 • Level 2 — 0x8030 • Level 3 — 0x8040 • Level 4 — 0x8050 • Level 5 — 0x8060 • Level 6 — 0x8070 • Level 7 — 0x8080
`level <`*`value`*`>`	Allows you to specify the switch level associated with this sVLAN. • <*value*> is an integer value in the range of 0 to 7. Level 0 (normal port): 802.1Q frames are classified into port-based VLANs. Level 1-7: any frame type is transparently switched and an additional Ether type 4 bytes is added. The default level is 0.

Figure 99 shows the **`config svlan info`** command output.

Figure 99 config svlan info command output

```
Passport-8610:5/config/svlan# ether-type level 1 0x8022
Passport-8610:5/config/svlan# level 1
Passport-8610:5/config/svlan# info

Sub-Context:clear config dump monitor show test trace wsm
Current Context:

        LEVEL ETHER-TYPE
        0     0x8100
        1     0x8022
        2     0x8030
        3     0x8040
        4     0x8050
        5     0x8060
        6     0x8070
        7     0x8080

        Active-Level = 1
```

Showing ether-type and switch level information

To display sVLAN ether-type and level information, use the following commands:

`show svlan info ether-type` (displays ether-types)

`show svlan info active-level` (displays active-levels)

Figure 100 shows sample output for the **`show svlan info ether-type`** command, while Figure 101 shows output for the **`show svlan info active-level`** command.

Figure 100 show svlan info ether-type command output

```
Passport-8610:5/show/svlan/info# ether-type
==============================================================
                           Stacked Vlan Ether Type
==============================================================
LEVEL ETHER-TYPE
--------------------------------------------------------------
0     0x8100
1     0x8022
2     0x8030
3     0x8040
4     0x8050
5     0x8060
6     0x8070
7     0x8080
```

Figure 101 show svlan info level command output

```
8610:5/show/slvan/info# active-level
Active-Level = 2
```

Setting the sVLAN port type

You must set the sVLAN port type to sVLAN UNI or sVLAN NNI.

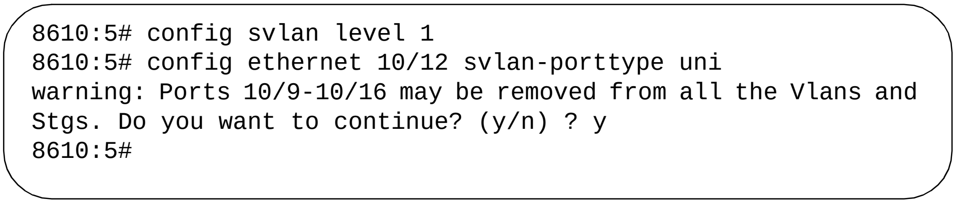
To set the sVLAN port type, use the following command:

```
config ethernet <ports> svlan-porttype <uni|nni>
```

Note: Since each OctaPID can support up to eight ports, you must designate all ports within an OctaPID as either normal or sVLAN (that is, the ports can be all Normal or a combination of UNI/NNI within the Octapid, which could be up to 8 ports). See Appendix A, ““Configuring sVLANs using the CLI” on page 207.

You will see the warning shown in Figure 102.

Figure 102 sVLAN-porttype warning



```
8610:5# config svlan level 1
8610:5# config ethernet 10/12 svlan-porttype uni
warning: Ports 10/9-10/16 may be removed from all the Vlans and
Stgs. Do you want to continue? (y/n) ? y
8610:5#
```

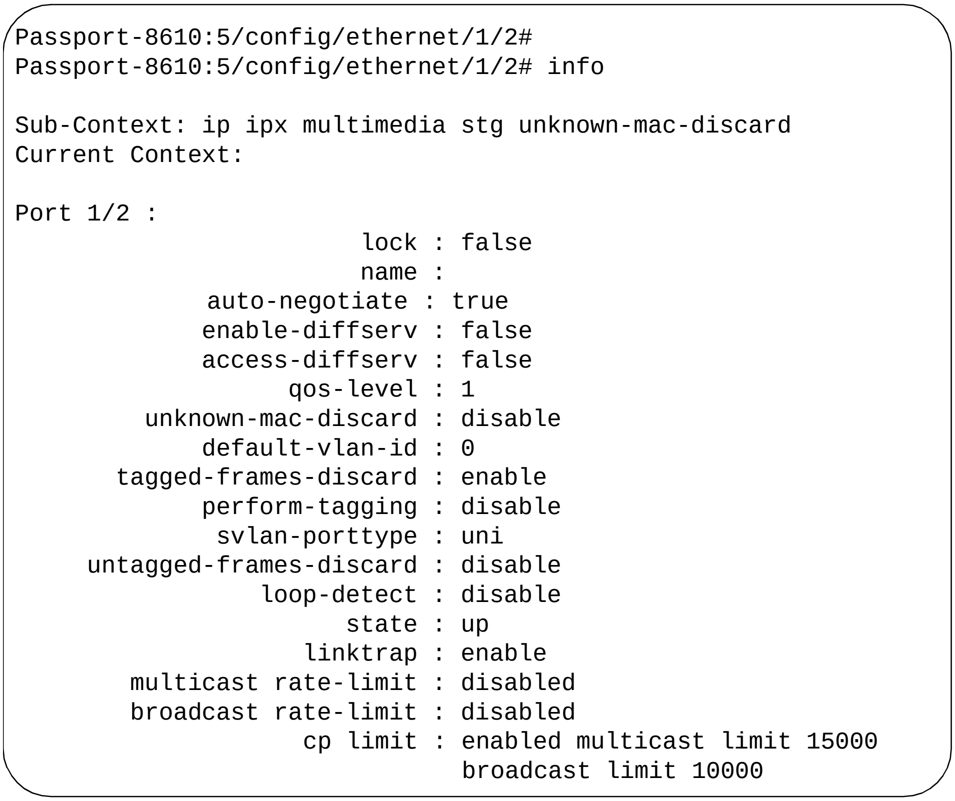
When you configure a UNI port in the CLI, the tagged-frames-discard parameter is automatically enabled. Similarly, when you configure an NNI port in the CLI, the untagged-frames-discard parameter is automatically enabled.

The **`config ethernet <ports>`** command includes the following parameters:

`config ethernet <ports>` followed by:	
`info`	Displays the current port settings (Figure 103).
`svlan-porttype <normal|uni|nni>`	Sets the port type for the sVLAN to normal, user-to-network interface (uni), or network-to-network interface (nni). The default is normal.

Figure 103 shows sample output for the **config ethernet *<ports>* info** command.

Figure 103 config ethernet <ports> info command output



```
Passport-8610:5/config/ethernet/1/2#
Passport-8610:5/config/ethernet/1/2# info

Sub-Context: ip ipx multimedia stg unknown-mac-discard
Current Context:

Port 1/2 :
                        lock : false
                        name :
             auto-negotiate : true
              enable-diffserv : false
              access-diffserv : false
                    qos-level : 1
          unknown-mac-discard : disable
              default-vlan-id : 0
        tagged-frames-discard : enable
              perform-tagging : disable
               svlan-porttype : uni
      untagged-frames-discard : disable
                  loop-detect : disable
                        state : up
                     linktrap : enable
         multicast rate-limit : disabled
         broadcast rate-limit : disabled
                     cp limit : enabled multicast limit 15000
                                broadcast limit 10000
```

Creating an sVLAN STG

To set a tagged BPDU address different from the standardized BPDU address and create an sVLAN STG, use the following commands:

```
config stg <sid> create mac <value> type <value>
```

The **config stg *<sid>*** command configures parameters for a specified spanning tree group. The required parameter ***<sid>*** (spanning tree group ID) is from 1 to 64.

The **config stg <*sid*>** command includes the following parameters:

config stg <*sid*> followed by:	
create [<*ports*>] [vlan <*value*>] [mac <*value*>] [type <stgnormal|stgsvlan>]	Creates a new spanning tree group. • <*ports*> specifies one or more ports. • vlan <*value*> is the VLAN ID. If a VLAN spans multiple switches, it must be within the same STG across all switches. • mac <*value*> is the MAC address. • type <stgnormal|stgsvlan> sets the spanning tree group to normal or sVLAN.

Figure 104 shows sample output for the **config stg info** command

Figure 104 config stg info command output

```
Passport-8610:5/config/stg/2# create mac 01:23:45:67:89:01
type stgsvlan
Passport-8610:5/config/stg/2# info

Sub-Context:
Current Context:

             add ports      :
                create      :2
                delete      : N/A
          forward-delay     : 1500
             group stp      : true
          hello-interval    : 200
                max-age     : 2000
                priority    : 32768
             remove ports   : N/A
                trp-stp     : true
                   type     : svlan
```

Adding UNI or NNI ports to the STG

To add UNI or NNI ports to the STG, use the following command:

`config stg <`*`sid`*`> add ports <`*`ports`*`>`

The **`config stg <`*`sid`*`>`** command configures parameters for a specified spanning tree group. The required parameter **<*`sid`*>** (spanning tree group ID) is from 1 to 64.

The **`config stg <`*`sid`*`>`** command includes the following options:

`config stg <`*`sid`*`>` followed by:	
`add ports <`*`ports`*`>`	Adds ports to a spanning tree group. *`ports`* specifies one or more ports.

Figure 105 shows sample output for the **`config stg <sid> info`** command.

Figure 105 config stg <sid> info command output

```
Passport-8610:5/config/stg/2# add ports 1/1-1/8
Passport-8610:5/config/stg/2# info

Sub-Context:
Current Context:

             add ports     :1/1-1/8
                 create    :2
                 delete    : N/A
          forward-delay    : 1500
             group stp     : true
          hello-interval   : 200
                 max-age   : 2000
                 priority  : 32768
             remove ports  : N/A
                 trp-stp   : true
                    type   : svlan
```

Creating an sVLAN

To create a VLAN of type sVLAN, use the following command:

`config vlan <`*`vid`*`> create bysvlan <`*`sid`*`>`

This command allows you to specify the type of VLAN. The required parameter *`vid`* is the VLAN ID (from 1 to 4094). VLAN 1 is the default VLAN.

This command includes the following parameters:

`config vlan <`*`vid`*`> create` followed by:	

`bysvlan <`*`sid`*`>`
`[name <`*`value`*`>]`
`[color <`*`value`*`>]`
	Creates an sVLAN.
	• *`sid`* is spanning tree ID 1 to 64.
	• `name <`*`value`*`>` is the name of the VLAN from 0 to 20 characters.
	• `color <`*`value`*`>` is the color of the VLAN (0 to 32). The color attribute is used by Optivity software to display the VLAN.
	This command is available only for the Passport 8600.

Figure 106 shows sample output for the **`config vlan info`** command

Figure 106 config vlan info command output

```
Passport-8610:5/config/vlan/2# create bysvlan 2 name SVLAN2
color 11
Passport-8610:5/config/vlan/2# info

Sub-Context: create-fdb-entry fdb-filter fdb-static ip ipx
ports scrmac static-mcastmac
Current Context:

                action     : N/A
                add-mlt    :
                agetime    : 0
                delete     : N/A
                qoslevel   : 1
                name       : SVLAN2
```

Configuration example

This configuration example uses all the commands required to create an sVLAN.

Note: You must enter the commands in sequence.

```
8610:5/config# svlan level 3
8610:5/config# ethernet 10/12 svlan-porttype uni
warning: Ports 10/9-10/16 may be removed from all the Vlans
and Stgs. Do you want to continue? (y/n) ? y
8610:5/config# stg 9 create mac 01:90:c2:00:00:00 type
stgsvlan
8610:5/config# vlan 1476 create bysvlan 9 name matt color 11
8610:5/config# stg 9 add ports 10/9-10/16
8610:5/config#
```

Chapter 8
Configuring STGs using the CLI

You set up spanning tree groups (STGs) by using the spanning tree group commands. You can set parameters for a group and for ports in that group. You can also enable or disable the Spanning Tree Protocol in an STG.

The Passport 8600 modules support up to 25 STGs in a switch.

The Passport 8100 modules support only one STG (STG 1) in a switch.

This chapter includes information about configuring STG and its parameters by using the appropriate commands. It includes the following topics:

Roadmap of STG commands

The following roadmap lists all the STG commands and their parameters. Use this list as a quick reference or click on any entry for more information:

Command	Parameter
`config stg <sid>`	`info`
	`add ports <ports>`
	`create [<ports>] [vlan <value>] [mac <value>]`

Command	Parameter
	delete
	forward-delay <timeval>
	group-stp <enable|disable>
	hello-interval <timeval>
	max-age <timeval>
	priority <number>
	remove ports <value>
	trap-stp <enable|disable>
config ethernet <ports> stg <sid>	info
	faststart <enable|disable>
	change-detection <enable|disable>
	pathcost <intval>
	priority <intval>
	stp <enable|disable>
show stg show-all	file <value> = filename, /pcmcia/<file> | /flash/<file> {string length 1..99}
show stg info config	
show stg info status [<sid>]	
show ports info stg main [<ports>]	
show ports info stg extended [<ports>]	
show ports stats stg [<ports>]	

Configuring STG parameters

To configure parameters for a specified spanning tree group, enter the following command:

```
config stg <sid>
```

```
where:
sid (spanning tree group ID) is a value from 1 to 25.
```

This command includes the following options:

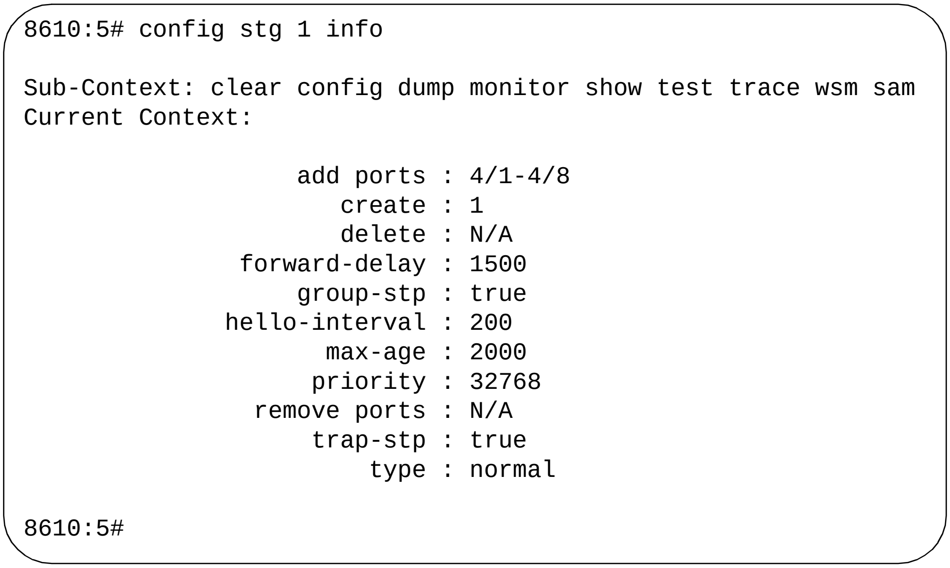
config stg ***<sid>*** followed by:	
`info`	Displays characteristics of the spanning tree group.
`add ports <ports>`	Adds port(s) to a spanning tree group. *ports* specifies one or more slot/port numbers. Ports can not be added to the STG if: • configured as single port SMLT • configured as members of another STG
`create [<ports>] [vlan <value>] [mac <value>]`	Creates a new spanning tree group. • *<ports>* specifies one or more slot/port numbers. (Note: ports cannot be added to the STG if configured as single port SMLT, or as a member of another STG.) • `vlan <value>` is the VLAN ID. If a VLAN spans multiple switches, it must be within the same STG across all switches. • `mac <value>` is the MAC address.
`delete`	Deletes the specified spanning tree group.
`forward-delay <timeval>`	Sets the bridge forward delay time in 1/100 seconds. *<timeval>* is between 400 and 3000. The default is 1500 (15 seconds).
`group-stp <enable|disable>`	Enables or disables the Spanning Tree Protocol on the specified spanning tree group.

config stg ***<sid>*** followed by:	
hello-interval *<timeval>*	Sets the bridge hello time in 1/100 seconds. *<timeval>* is between 100 and 1000. The default is 200 (2 seconds).
max-age *<timeval>*	Sets the bridge maximum age time in 1/100 seconds. *<timeval>* is between 600 and 4000. The default is 2000 (20 seconds).
priority *<number>*	Sets the bridge priority number. *<number>* is between 0 and 65535.
remove ports *<value>*	Removes ports from a spanning tree group. *<value>* is the specified port.
trap-stp <enable|disable>	Enables or disables the Spanning Tree Protocol trap for the specified spanning tree group.
type <stgnormal|stgsvlan>	Specifies the STG type. • normal = normal \STG • svlan = stacked VLAN STG

Note: Disabling the Spanning Tree Protocol can reduce CPU overhead slightly. However, unless you are using the switch in a simple network with little possibility of having loops, Nortel Networks recommends that you leave the Spanning Tree Protocol enabled.

Figure 107 shows sample output for the **`config stg info`** command.

Figure 107 config stg info command output



```
8610:5# config stg 1 info

Sub-Context: clear config dump monitor show test trace wsm sam
Current Context:

                   add ports : 4/1-4/8
                      create : 1
                      delete : N/A
               forward-delay : 1500
                   group-stp : true
              hello-interval : 200
                     max-age : 2000
                    priority : 32768
                remove ports : N/A
                    trap-stp : true
                        type : normal

8610:5#
```

Configuring STG port parameters

Ports must have tagging enabled to belong to multiple spanning tree groups.

Note: Nortel Networks recommends that you enable FastStart as an alternative to disabling Spanning Tree Protocol on an individual port.
Note: The Spanning Tree protocol is currently not supported on SMLT/ IST ports.

To configure spanning tree group port parameters, enter the following command:

`config ethernet <`*`ports`*`> stg <`*`sid`*`>`

where:
`ports` = the slot/port(s) you want to add to the STG.
`sid` = the spanning tree group ID. The valid values are 1 to 64.

This command includes the following options:

config ethernet ***<slot/port>*** **stg** ***<sid>*** followed by:	
`info`	Displays current settings for the port spanning tree group.
`faststart <enable|disable>`	Enables or disables the FastStart feature. When FastStart is enabled, the port goes through the normal listening and learning states before forwarding, but the hold time for these states is the bridge hello timer (2 seconds by default) instead of the bridge forward delay timer (15 seconds by default).
`change-detection <enable|disable>`	Enables or disables topology change detection for the specified spanning tree. The default is enable.
`pathcost <intval>`	Sets the contribution of this port to the path cost. `<intval>` is the cost (1 to 65535).
`priority <intval>`	Sets the priority of this port. `<intval>` is the priority (0 to 255).
`stp <enable|disable>`	Enables or disables the Spanning Tree Protocol. Note: Spanning Tree protocol is not supported on SMLT or IST ports.

To display the current settings for the spanning tree group, use the following command:

```
config ethernet <ports> stg <sid> info
```

Figure 108 shows sample output for this command.

Figure 108 config ethernet <slot/port> stg <sid> info command output

```
8610# config ethernet 2/1 stg 1 info

Sub-Context:
Current Context:

Port 2/1 :
             change-detection : enable
                    faststart : disable
                     pathcost : 100
                     priority : 128
                          stp : enable
```

Configuring topology change detection

Change detection is enabled by default. With change detection, when a topology change occurs, a trap is sent containing the MAC address of the STG sending the topology change notification (TCN), the port number, and the STG ID. You can use this information to identify the device. For more information about change detection, see “About Spanning Tree protocol topology change detection” on page 49.

To configure topology change detection, use the following command:

```
config ethernet <ports> stg <sid> change-detection <enable|disable>
```

where:

ports = the port on which you want to configure spanning tree topology change detection. If you enable change detection on an MLT with access ports, the setting is automatically applied to all ports in the MLT.

sid = the spanning tree (1 - 64) for which you want to enable or disable topology change detection.

enable|disable = enables or disables topology change detection for the specified spanning tree. The default is `enabled`

Querying the change-detection setting

To query the change detection setting, use the following command:

```
config ethernet <ports> stg <sid> info
```

Figure 108 on page 225 shows sample output for this command.

The **`show ports info stg main`** command (Figure 109) also displays the change detection setting.

Figure 109 show ports info stg main command output

```
8610:5# show ports info stg main

========================================================================
                                        Port Stg
========================================================================
                             ENABLE                    FORWARD    CHANGE
SID PORT_NUM PRIO STATE       STP  FASTSTART PATHCOST TRANSITION DETECTION
------------------------------------------------------------------------
1   4/1      128  disabled   false  false     100      0          true
1   4/2      128  disabled   true   false     100      0          true
1   4/3      128  disabled   true   false     100      0          true
1   4/4      128  disabled   true   false     100      0          true
1   4/5      128  disabled   true   false     100      0          true
1   4/6      128  disabled   true   false     100      0          true
1   4/7      128  disabled   true   false     65535    0          true
1   4/8      128  disabled   true   false     65535    0          true

8610:5#
```

Using the STG show commands

To display the status of spanning tree on the switch or on a port, use the **`show stg`** commands.

This section includes information on show commands that allow you to display:

- All STG information, next
- STG configuration, (page 229)
- STG status (page 230)
- Basic STG information (page 231)
- Additional STG information (page 232)
- STG statistics counters (page 233)

Displaying all STG information

To displays all Spanning Tree Group information enter the following command:

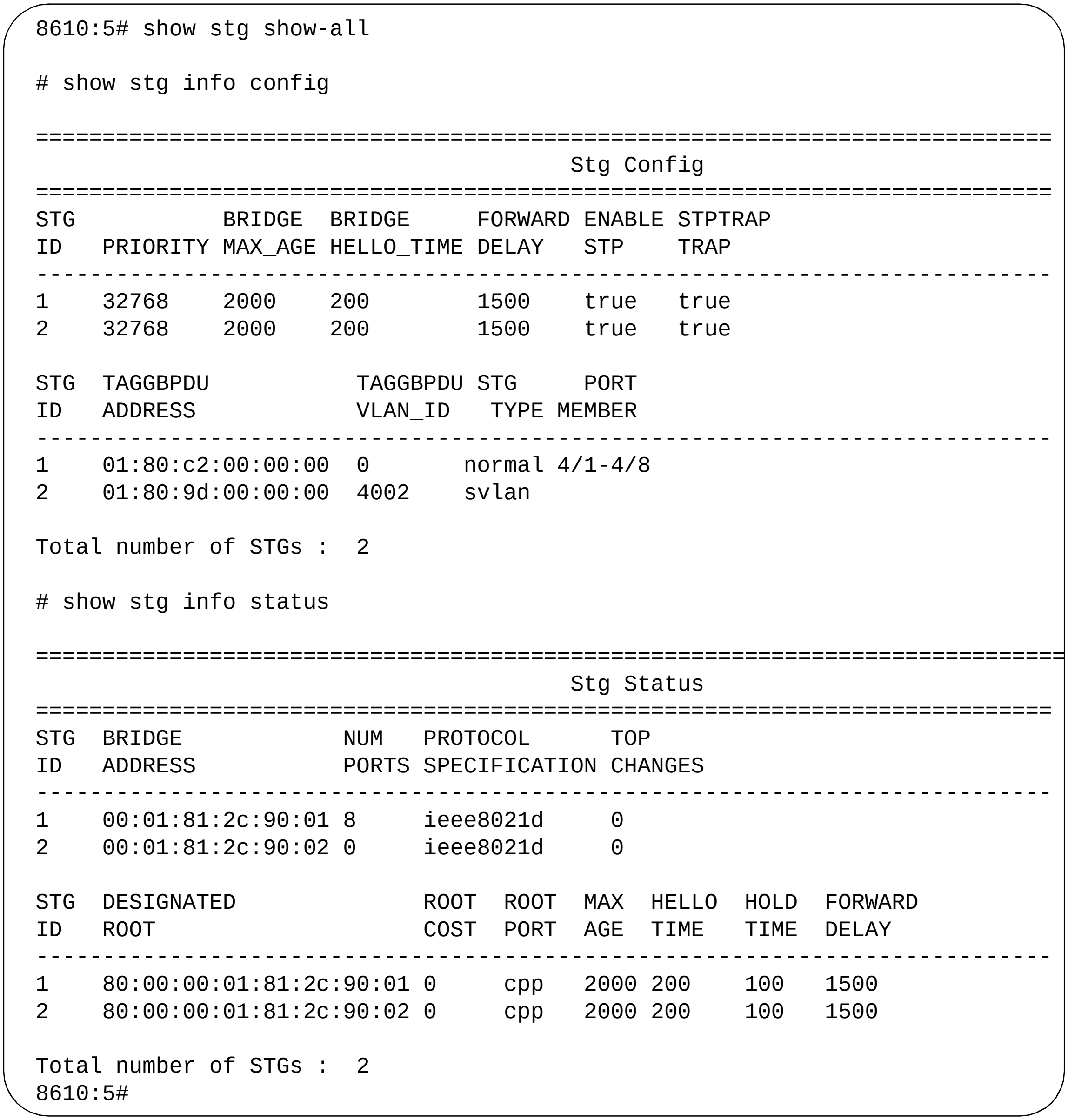
```
show stg show-all
```

The command uses the syntax:

```
show stg show-all [file <value>]
```

where <*value*> is the filename to which the output will be redirected. Figure 110 shows sample output for this command.

Figure 110 show stg show-all sample output



```
8610:5# show stg show-all

# show stg info config

============================================================================
                                        Stg Config
============================================================================
STG           BRIDGE  BRIDGE     FORWARD ENABLE STPTRAP
ID   PRIORITY MAX_AGE HELLO_TIME DELAY   STP    TRAP
----------------------------------------------------------------------------
1    32768    2000    200        1500    true   true
2    32768    2000    200        1500    true   true

STG  TAGGBPDU           TAGGBPDU STG     PORT
ID   ADDRESS            VLAN_ID   TYPE MEMBER
----------------------------------------------------------------------------
1    01:80:c2:00:00:00  0       normal 4/1-4/8
2    01:80:9d:00:00:00  4002    svlan

Total number of STGs :  2

# show stg info status

=============================================================================
                                        Stg Status
============================================================================
STG  BRIDGE            NUM   PROTOCOL      TOP
ID   ADDRESS           PORTS SPECIFICATION CHANGES
----------------------------------------------------------------------------
1    00:01:81:2c:90:01 8     ieee8021d     0
2    00:01:81:2c:90:02 0     ieee8021d     0

STG  DESIGNATED              ROOT  ROOT  MAX  HELLO  HOLD  FORWARD
ID   ROOT                    COST  PORT  AGE  TIME   TIME  DELAY
----------------------------------------------------------------------------
1    80:00:00:01:81:2c:90:01 0     cpp   2000 200    100   1500
2    80:00:00:01:81:2c:90:02 0     cpp   2000 200    100   1500

Total number of STGs :  2
8610:5#
```

Displaying STG configuration

To display the spanning tree group configuration for the switch or for the specified spanning tree group, enter the following command:

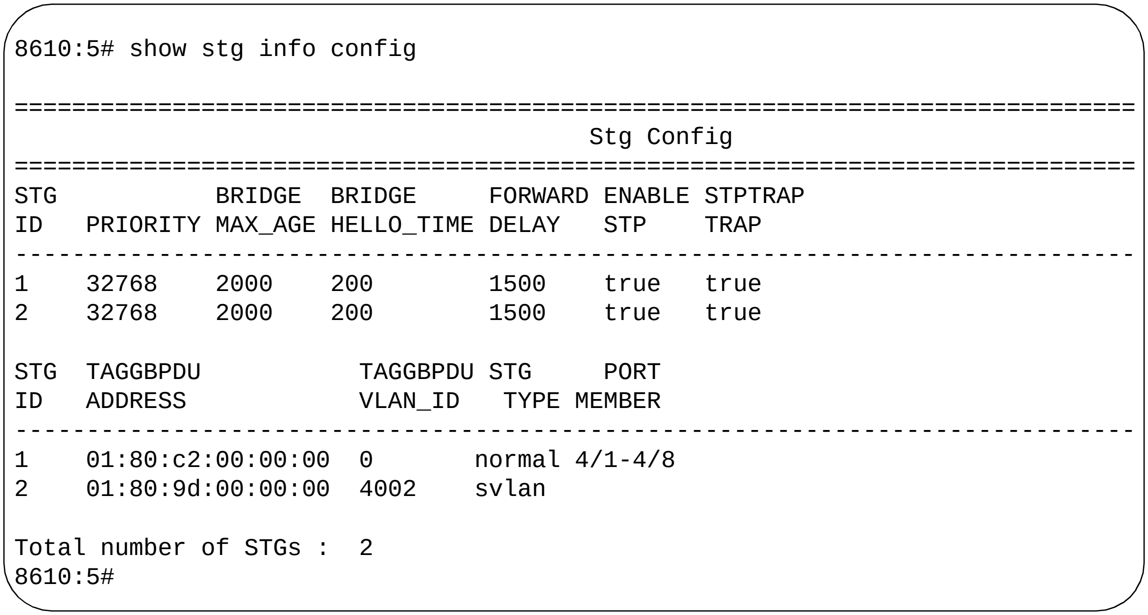
`show stg info config`

The command syntax is:

`show stg info config` [<*sid*>]

Figure 111 shows sample output for the **`show stg info config`** command.

Figure 111 show stg info config command output



```
8610:5# show stg info config

==============================================================================
                                        Stg Config
==============================================================================
STG           BRIDGE  BRIDGE     FORWARD ENABLE STPTRAP
ID   PRIORITY MAX_AGE HELLO_TIME DELAY   STP    TRAP
------------------------------------------------------------------------------
1    32768    2000    200        1500    true   true
2    32768    2000    200        1500    true   true

STG  TAGGBPDU           TAGGBPDU STG     PORT
ID   ADDRESS            VLAN_ID   TYPE MEMBER
------------------------------------------------------------------------------
1    01:80:c2:00:00:00  0       normal 4/1-4/8
2    01:80:9d:00:00:00  4002    svlan

Total number of STGs :  2
8610:5#
```

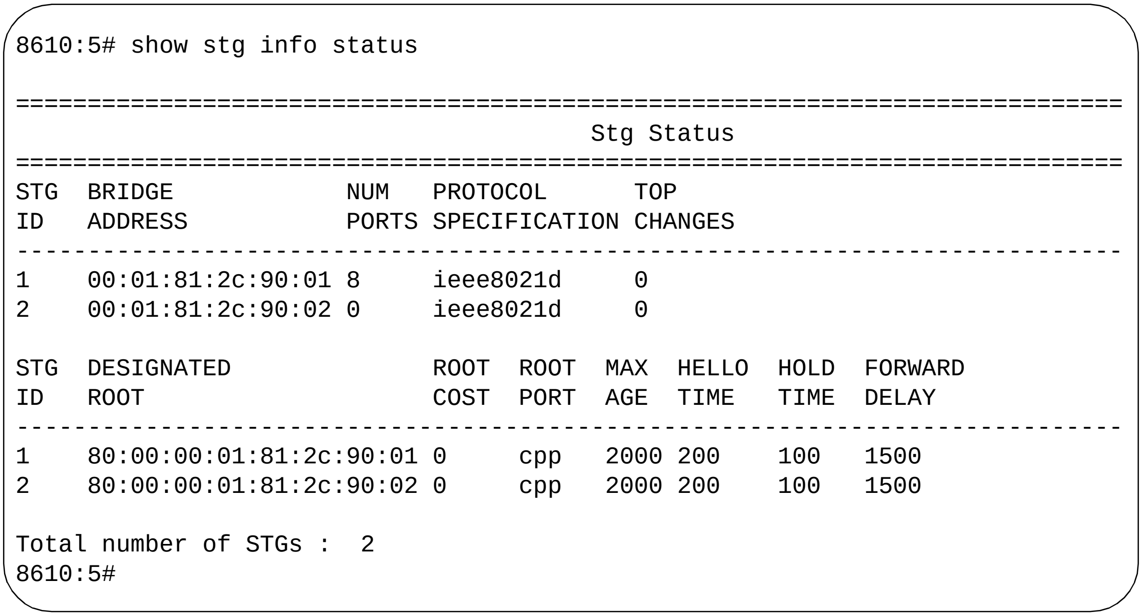
Displaying STG status

To display the spanning tree group status for the specified spanning tree group or all STGs, enter the following command:

```
show stg info status [<sid>]
```

Figure 112 shows sample output for the **show stg info status** command.

Figure 112 show stg info status command output



```
8610:5# show stg info status

=============================================================================
                                        Stg Status
=============================================================================
STG  BRIDGE            NUM   PROTOCOL      TOP
ID   ADDRESS           PORTS SPECIFICATION CHANGES
-----------------------------------------------------------------------------
1    00:01:81:2c:90:01 8     ieee8021d     0
2    00:01:81:2c:90:02 0     ieee8021d     0

STG  DESIGNATED              ROOT  ROOT  MAX  HELLO  HOLD  FORWARD
ID   ROOT                    COST  PORT  AGE  TIME   TIME  DELAY
-----------------------------------------------------------------------------
1    80:00:00:01:81:2c:90:01 0     cpp   2000 200    100   1500
2    80:00:00:01:81:2c:90:02 0     cpp   2000 200    100   1500

Total number of STGs :  2
8610:5#
```

Displaying basic STG information

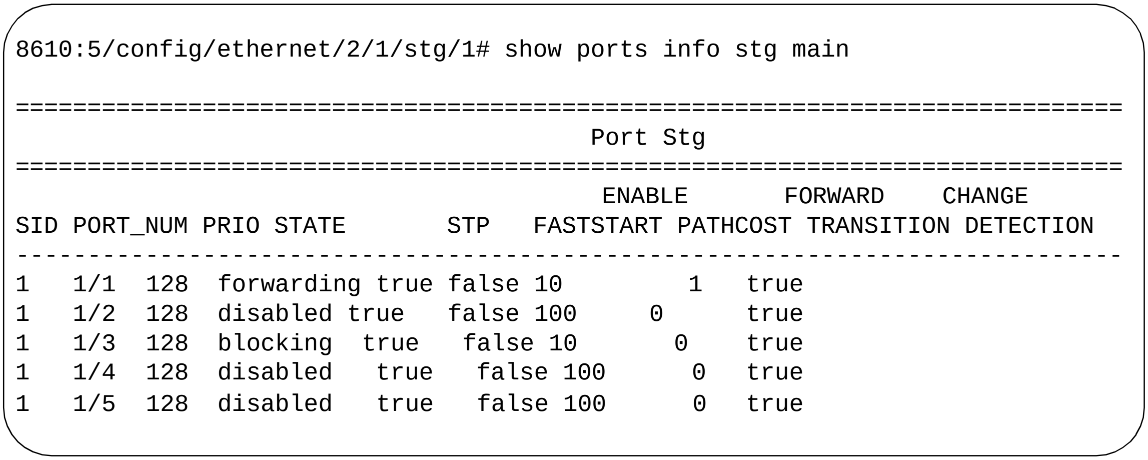
To display basic spanning tree group information about one or more specified ports or about all ports, enter the following command:

`show ports info stg main [<`*`ports`*`>]`

(See also “Displaying basic STG information” on page 231 for information on the **`show ports info stg extended`** command.)

Figure 113 shows sample output for the **`show ports info stg main`** command.

Figure 113   show ports info stg main command output



```
8610:5/config/ethernet/2/1/stg/1# show ports info stg main

=============================================================================
                                        Port Stg
=============================================================================
                                         ENABLE       FORWARD    CHANGE
SID PORT_NUM PRIO STATE       STP   FASTSTART PATHCOST TRANSITION DETECTION
-----------------------------------------------------------------------------
1   1/1  128  forwarding true false 10         1   true
1   1/2  128  disabled true   false 100     0      true
1   1/3  128  blocking  true   false 10       0    true
1   1/4  128  disabled   true   false 100      0   true
1   1/5  128  disabled   true   false 100      0   true
```

Displaying additional STG information

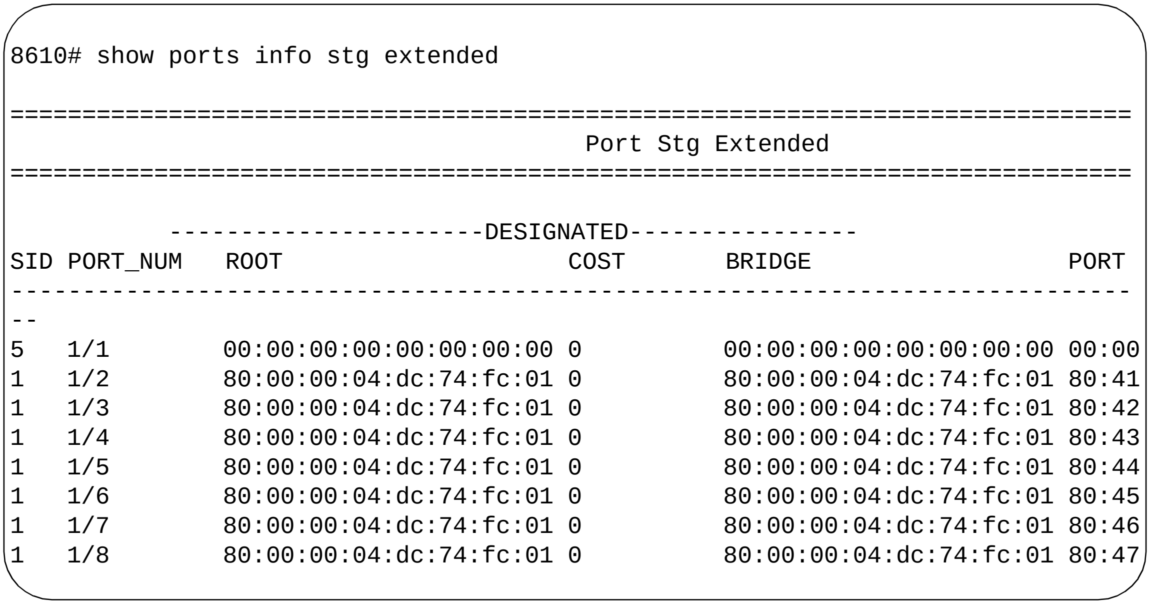
To display additional spanning tree group information about the specified port or about all ports, enter the following command:

```
show ports info stg extended [<ports>]
```

This information is less often used in switch monitoring than the information obtained with the **show ports info stg main** command (page 231).

Figure 114 shows sample output for the **show ports info stg extended** command.

Figure 114 show ports info stg extended command output



```
8610# show ports info stg extended

==============================================================================
                                        Port Stg Extended
==============================================================================

           ----------------------DESIGNATED----------------
SID PORT_NUM   ROOT                    COST       BRIDGE                  PORT
------------------------------------------------------------------------------
--
5   1/1        00:00:00:00:00:00:00:00 0          00:00:00:00:00:00:00:00 00:00
1   1/2        80:00:00:04:dc:74:fc:01 0          80:00:00:04:dc:74:fc:01 80:41
1   1/3        80:00:00:04:dc:74:fc:01 0          80:00:00:04:dc:74:fc:01 80:42
1   1/4        80:00:00:04:dc:74:fc:01 0          80:00:00:04:dc:74:fc:01 80:43
1   1/5        80:00:00:04:dc:74:fc:01 0          80:00:00:04:dc:74:fc:01 80:44
1   1/6        80:00:00:04:dc:74:fc:01 0          80:00:00:04:dc:74:fc:01 80:45
1   1/7        80:00:00:04:dc:74:fc:01 0          80:00:00:04:dc:74:fc:01 80:46
1   1/8        80:00:00:04:dc:74:fc:01 0          80:00:00:04:dc:74:fc:01 80:47
```

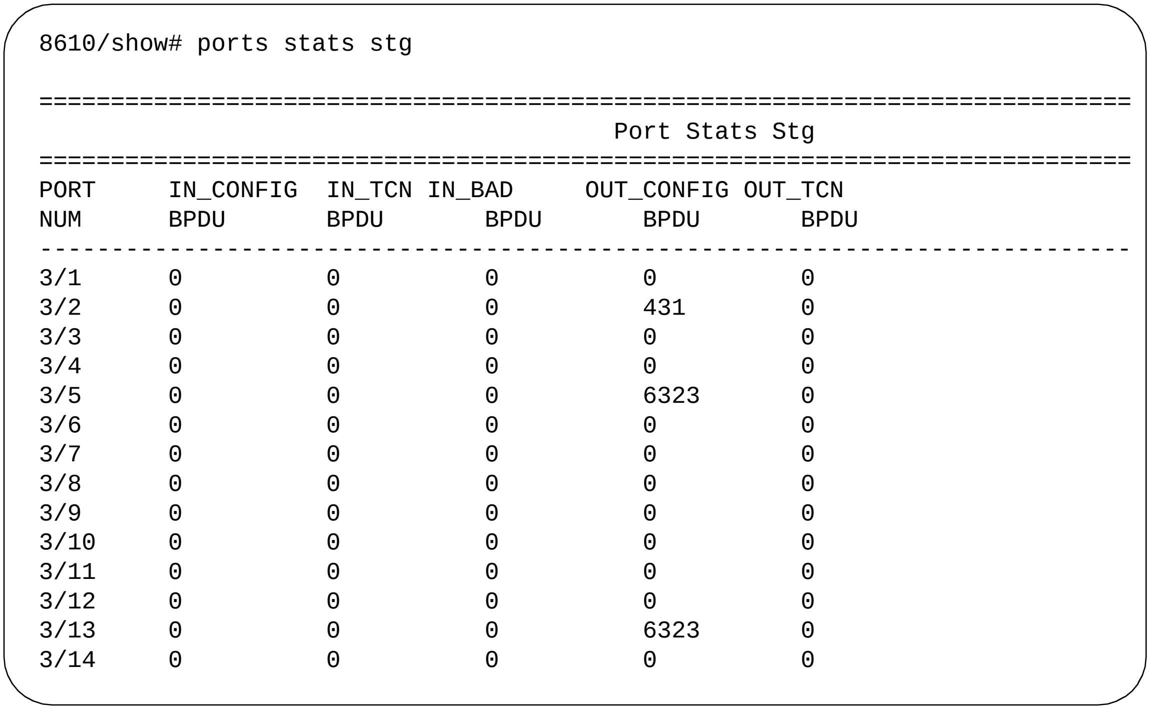
Displaying STG statistics counters

To display statistics counters for spanning tree groups on all ports or the specified port, enter the following command:

```
show ports stats stg [<ports>]
```

Figure 115 shows sample output for the **`show ports stats stg`** command.

Figure 115 show ports stats stg command (partial output)



```
8610/show# ports stats stg

============================================================================
                                        Port Stats Stg
============================================================================
PORT     IN_CONFIG  IN_TCN IN_BAD     OUT_CONFIG OUT_TCN
NUM      BPDU       BPDU       BPDU       BPDU       BPDU
----------------------------------------------------------------------------
3/1      0          0          0          0          0
3/2      0          0          0          431        0
3/3      0          0          0          0          0
3/4      0          0          0          0          0
3/5      0          0          0          6323       0
3/6      0          0          0          0          0
3/7      0          0          0          0          0
3/8      0          0          0          0          0
3/9      0          0          0          0          0
3/10     0          0          0          0          0
3/11     0          0          0          0          0
3/12     0          0          0          0          0
3/13     0          0          0          6323       0
3/14     0          0          0          0          0
```

Chapter 9
Configuring MLTs and SMLTs using the CLI

This chapter describes MLT and SMLT CLI commands, and SMLT troubleshooting instructions. It includes the following topics:

For more information about MLT and SMLT, see:

- "About MultiLink Trunking" on page 50
- "About Split Multilink Trunking (SMLT)" on page 59
- "About single port SMLT" on page 67

Roadmap of MLT and SMLT commands

The following roadmap lists the MLT and SMLT commands and their parameters which are described in this chapter. Use this list as a quick reference or click on any entry for more information:

Command	Parameter
`config mlt <mid>`	`info`
	`create`

Command	Parameter
	delete
	name <string>
	perform-tagging <enable|disable>
config mlt <mid> add	info
	ports <ports>
	vlan <vid>
config mlt <mid> remove	info
	ports <ports>
	vlan <vid>
config mlt <mid> smlt	info
	create smlt-id <value>
	delete
config mlt <mid> ist	info
	create ip <value> vlan-id <value>
	delete
	disable
	enable
config mlt <mlt-id> ist create ip <peer-ip address> vlan-id <value>	
config mlt <mlt-id> ist <enable|disable>	
config mlt <mlt-id> ist delete	
config mlt <mid> mcast-distribution	enable
	disable
config <Ethernet|ATM|POS> <port> smlt <SmltId> <option>	create
	delete

Command	Parameter
config ethernet <slot/port> cp-limit	<enable|disable>
	multicast-limit <value>
	broadcast-limit <value>
show mlt show-all [file <value>]	file <value> = filename, /pcmcia/<file> | /flash/<file> {string length 1..99}
show mlt error collision [<mid>]	
show mlt error main [<mid>]	
show mlt info [<mid>]	
show mlt stats [<mid>]	
show smlt info [<mid>]	
show port info smlt	
show port info config <port>	

Configuring MLT

This section includes commands for:

- “Setting up MLTs on the switch,” next
- “Adding ports to an MLT” on page 239)
- “Removing ports from an MLT” on page 240
- “Creating an SMLT from an existing MLT” on page 241
- “Creating an IST” on page 242

Setting up MLTs on the switch

To set up MLTs on the switch, enter the following command:

```
config mlt <mid>
```

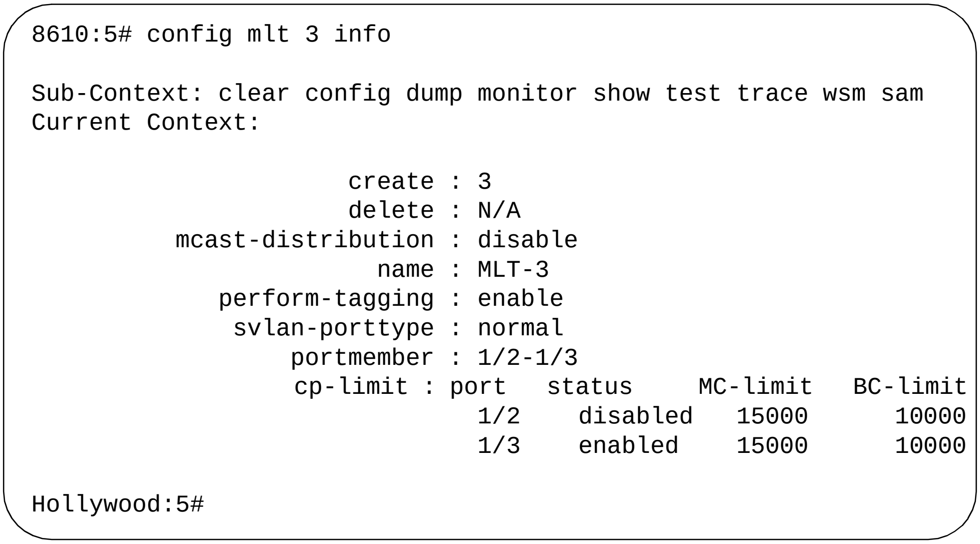
The required parameter *mid* specifies the MultiLink Trunk ID (1 to 32).

This command includes the following options:

config mlt <*mid*> followed by:	
info	Displays current settings for the specified MLT.
create	Creates an MLT.
delete	Deletes an MLT.
name <*string*>	Names an MLT. *string* is the name, from 0 to 20 characters.
mcast-distribution <enable|disable>	Enables or disables multicast distribution per MLT. Multicast distribution is disabled by default. For detailed information about commands used to configure multicast distribution over MLT, see the publication, *Configuring IP Routing Multicast Protocols*.
perform-tagging <enable|disable>	Enables or disables tagging on an MLT port.
svlan-porttype <uni|nni|normal>	This option is not available for the Passport 8000 software.

Figure 116 shows sample output for the **config mlt info** command.

Figure 116 config mlt info command output



```
8610:5# config mlt 3 info

Sub-Context: clear config dump monitor show test trace wsm sam
Current Context:

                      create : 3
                      delete : N/A
          mcast-distribution : disable
                        name : MLT-3
             perform-tagging : enable
              svlan-porttype : normal
                  portmember : 1/2-1/3
                  cp-limit : port   status     MC-limit   BC-limit
                               1/2    disabled    15000       10000
                               1/3    enabled     15000       10000

Hollywood:5#
```

Adding ports to an MLT

To add ports to an MLT and add an existing VLAN to an MLT configuration, enter the following command:

`config mlt <mid> add`

This command includes the following options:

config mlt <*mid*> add followed by:	
`info`	Displays ports and/or VLANs added to the MLT.

config mlt <*mid*> add followed by:	
ports <*ports*>	Adds ports to the MLT. • *ports* is the port number or a list of ports you want to add to the MLT. Use the following convention when adding one or more ports to the MLT: {slot/port[-slot/port][,...]}. Note: If the port you are configuring already has an SMLT ID on it, you cannot add it to the MLT.
vlan <*vid*>	Adds an existing VLAN to the MLT. • *vid* is the VLAN ID. The range is 1 to 4094 VLANs.

Removing ports from an MLT

To remove ports from an MLT and remove a VLAN from an MLT configuration, enter the following command:

```
config mlt <mid> remove
```

This command includes the following options:

config mlt <*mid*> remove followed by:	
info	Displays the ports and/or VLANs removed from the MLT.
ports <*ports*>	removes ports from the MLT. • *ports* is the port number or a list of ports you want to remove from the MLT. Use the following convention when removing one or more ports from the MLT: {slot/port[-slot/port][,...]}.
vlan <*vid*>	Removes a VLAN from the MLT. • *vid* is the VLAN ID. The range is 1 to 4094 VLANs.

Configuring multicast distribution for an MLT

Multicast distribution over MLT is supported only on 8000 Series E-modules.

To configure multicast distribution for an MLT, enter the following command:

```
config mlt <mid> mcast-distribution
```

This command includes the following options:

config mlt <*mid*> mcast-distribution followed by:	
enable	Enables multicast distribution for the MLT.
disable	Disables multicast distribution for the MLT.

For more information about multicast distribution over MLT, see the publication, *Configuring IP Routing Multicast Protocols*.

Creating an SMLT from an existing MLT

To create an SMLT from an existing MLT, enter the following command:

```
config mlt <mid> smlt
```

Note: Before you can create an SMLT, you must first create an MLT (see “Setting up MLTs on the switch” on page 238).

This command includes the following options:

config mlt <*mid*> smlt followed by:	
`info`	Displays ports and/or VLANs added to the MLT.
`create smlt-id <value>`	Creates an SMLT from an existing MLT. • *value* is an integer value with a range of 1 to 32. The value must match the peer switch's SMLT-ID. Note: If the SMLT ID already exists on a single port SMLT, you cannot assign it to an MLT-based SMLT.
`delete`	Deletes an existing SMLT.

Creating an IST

To create an IST from an existing MLT, enter the following command:

```
config mlt <mid> ist
```

This command includes the following options:

config mlt <*mid*> ist followed by:	
`info`	Displays current level parameter settings and next level directories.
`create ip <value> vlan-id <value>`	Creates an IST from an existing MLT (see "Creating an IST from an existing trunk MLT," next). • IP *value* is a peer IP address • VLAN ID *value* is an integer value with a range of 1 to 4095. Note that the peer IP address is the IP address of the IST VLAN on the other aggregation switch.
`delete`	Deletes an existing IST. **NOTE:** You must disable an IST before you can delete it.
`disable`	Disables an existing IST.
`enable`	Enables an existing IST.

Creating an IST from an existing trunk MLT

To create IST from an already created trunk MLT, enter the following command:

```
config mlt <mlt-id> ist create ip <peer-ip address> vlan-id
<value>
```

where,

mlt-id =	the multilink trunk ID number
peer-IP-address =	the IP address of the peer switch
value =	a VLAN ID number from 1 to 4095

IST is enabled when you first create it.

The peer IP address is the IP address of the IST VLAN on the peer aggregation switch. A VLAN created on the redundant aggregation switch must also be created on the second aggregation switch. The IST treats two switches as a single switch. To allow the two switches to communicate, you must assign an IP address to both VLANs.

For example:

switch A		switch B
VLAN 20		VLAN 20
10.1.1.1. /24	<--------IST-------->	10.1.1.2 /24 *

* Same subnet, same VLAN.

For more information about IST, see “About Inter-switch trunk (IST)” on page 63.

Figure 117 shows sample output for the **`config mlt ist create ip vlan-id`** command, followed by the **`info`** command.

Figure 117 config mlt ist create ip vlan-id command output

```
8610:5/config/mlt/1/ist# create ip 10.1.1.1 vlan-id 1
8610:5/config/mlt/1/ist# info

Sub-Context:
Current Context:

                Enable: false
               vlan-id: 1
                    ip: 10.1.1.1
```

Enabling/disabling an IST

To enable and disable the IST, enter the following command:

```
config mlt <mlt-id> ist <enable|disable>
```

Figure 118 shows sample output for the **config mlt ist enable** and **config mlt ist disable** commands. It includes the system warning that appears when you attempt to disable the IST.

Figure 118 config mlt ist enable/disable command output

```
8610:5/config/mlt/1/ist# enable
8610:5/config/mlt/1/smlt# disable

WARNING : Disabling IST may cause a loop in the network!
          Do you really want to DISABLE IST? (yes/no?)
```

Disabling CP-Limit for an IST

Nortel Networks recommends disabling CP-Limit on IST links. For more information, see “About CP-Limit and SMLT IST” on page 64.

To disable CP-limit for the IST, enter the following command:

```
config ethernet <slot/port> cp-limit disable
```

This command includes the following options:

`config ethernet <slot/port> cp-limit` followed by:	
`<enable|disable>`	Enables/Disables control packet rate limit (CP-Limit). The default setting is Enabled. If you want to re-enable CP-Limit on a port for which you have disabled it, you must first disable the port and then re-enable it (config ethernet slot/port state <disable | enable)).
`multicast-limit <value>`	Sets the multicast control frame packet per second rate (1000 to 100000).
`broadcast-limit <value>`	Sets the broadcast frame packet per second rate (1000 to 100000).

For information about viewing current CP-Limit status for an IST MLT, see Figure 116, "config mlt info command output" on page 239.

Deleting an IST

To delete the IST, enter the following command:

```
config mlt <mlt-id> ist delete
```

Note that you have to disable the IST before deleting it (see "Enabling/disabling an IST," preceding this section).

Creating a single port SMLT

To create a single port SMLT, enter the following command:

```
config <Ethernet|ATM|POS> <port> smlt <SmltId> <option>
```

This command includes the following options:

`config <Ethernet|ATM|POS> <slot/port> smlt <SmltId>` followed by:	
`info`	Displays the port's smlt info.
`create`	Creates a single port SMLT.
`delete`	Deletes a single port SMLT.

For more information about single port SMLT, see “About single port SMLT” on page 67.

Configuration example: single port SMLT

This configuration example uses the commands described above to create a single port SMLT on slot/port 2/2. The switch automatically disables spanning tree protocol on the port after it is configured for SMLT.

After configuring the parameters, use the **info** command to show a summary of the results.

Figure 119 Configuration example: single port SMLT

```
8610:5/config/ethernet/2/2# smlt 1
8610:5/config/ethernet/2/2/smlt/1#
8610:5/config/ethernet/2/2/smlt/1# create

INFO : The spanning tree protocol has been disabled on this port
       while configuring the port with SMLT

8610:5/config/ethernet/2/2/smlt/1# info

Sub-Context:
Current Context:

Port 2/2 :
                      create : 1
                      delete : N/A
                 Oper Status : normal

8610:5/config/ethernet/2/2/smlt/1#
```

Using the MLT and SMLT show commands

To display information and statistics about MLT operation in the switch, use the **`show mlt`** commands

This section includes information on show commands that allow you to:

- "Displaying all MLT information" on page 247
- "Displaying information about collision errors," next
- "Displaying MLT status" on page 252
- "Displaying MLT status" on page 252
- "Displaying SMLT status" on page 252
- "Displaying all ports configured for single port SMLT" on page 253
- "Displaying a port configured for single port SMLT" on page 254
- "Displaying MLT statistics" on page 255

Displaying all MLT information

The `show mlt show-all` command displays all mlt information.

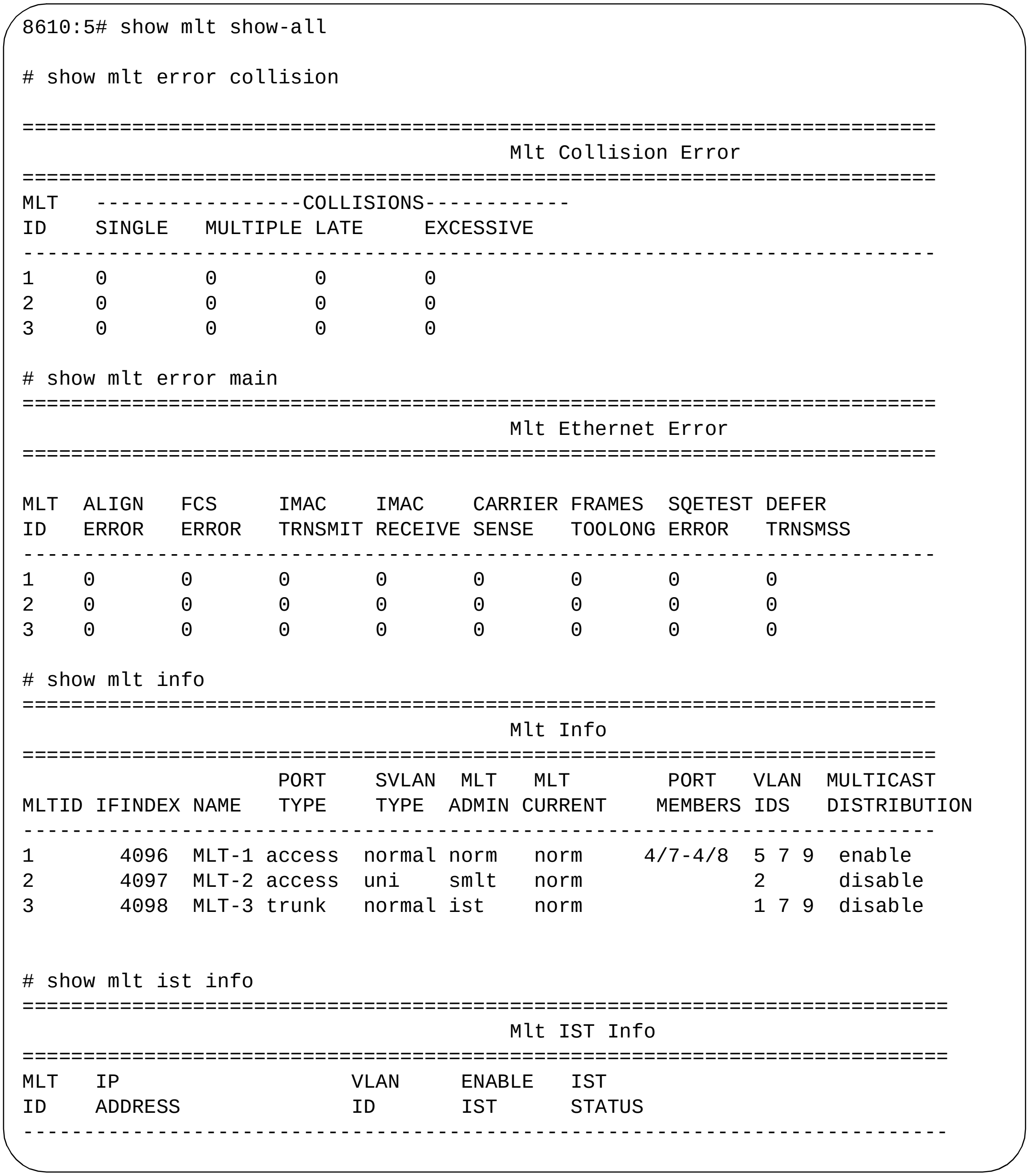
The command uses the syntax:

```
show mlt show-all [file <value>]
```

where <*value*> is the filename to which the output will be redirected.

Figure 120, Figure 121, and Figure 122 show sample output for this command.

Figure 120 show mlt show-all sample output



```
8610:5# show mlt show-all

# show mlt error collision

===========================================================================
                                        Mlt Collision Error
===========================================================================
MLT   -----------------COLLISIONS------------
ID    SINGLE   MULTIPLE LATE     EXCESSIVE
---------------------------------------------------------------------------
1     0        0        0        0
2     0        0        0        0
3     0        0        0        0

# show mlt error main
===========================================================================
                                        Mlt Ethernet Error
===========================================================================

MLT  ALIGN   FCS     IMAC    IMAC    CARRIER FRAMES  SQETEST DEFER
ID   ERROR   ERROR   TRNSMIT RECEIVE SENSE   TOOLONG ERROR   TRNSMSS
---------------------------------------------------------------------------
1    0       0       0       0       0       0       0       0
2    0       0       0       0       0       0       0       0
3    0       0       0       0       0       0       0       0

# show mlt info
===========================================================================
                                        Mlt Info
===========================================================================
                     PORT    SVLAN  MLT   MLT        PORT   VLAN  MULTICAST
MLTID IFINDEX NAME   TYPE    TYPE  ADMIN CURRENT   MEMBERS IDS   DISTRIBUTION
---------------------------------------------------------------------------
1       4096  MLT-1 access  normal norm   norm     4/7-4/8  5 7 9  enable
2       4097  MLT-2 access  uni    smlt   norm              2      disable
3       4098  MLT-3 trunk   normal ist    norm              1 7 9  disable


# show mlt ist info
============================================================================
                                        Mlt IST Info
============================================================================
MLT   IP                   VLAN     ENABLE   IST
ID    ADDRESS              ID       IST      STATUS
----------------------------------------------------------------------------
```

Figure 121 show mlt show-all sample output (continued)

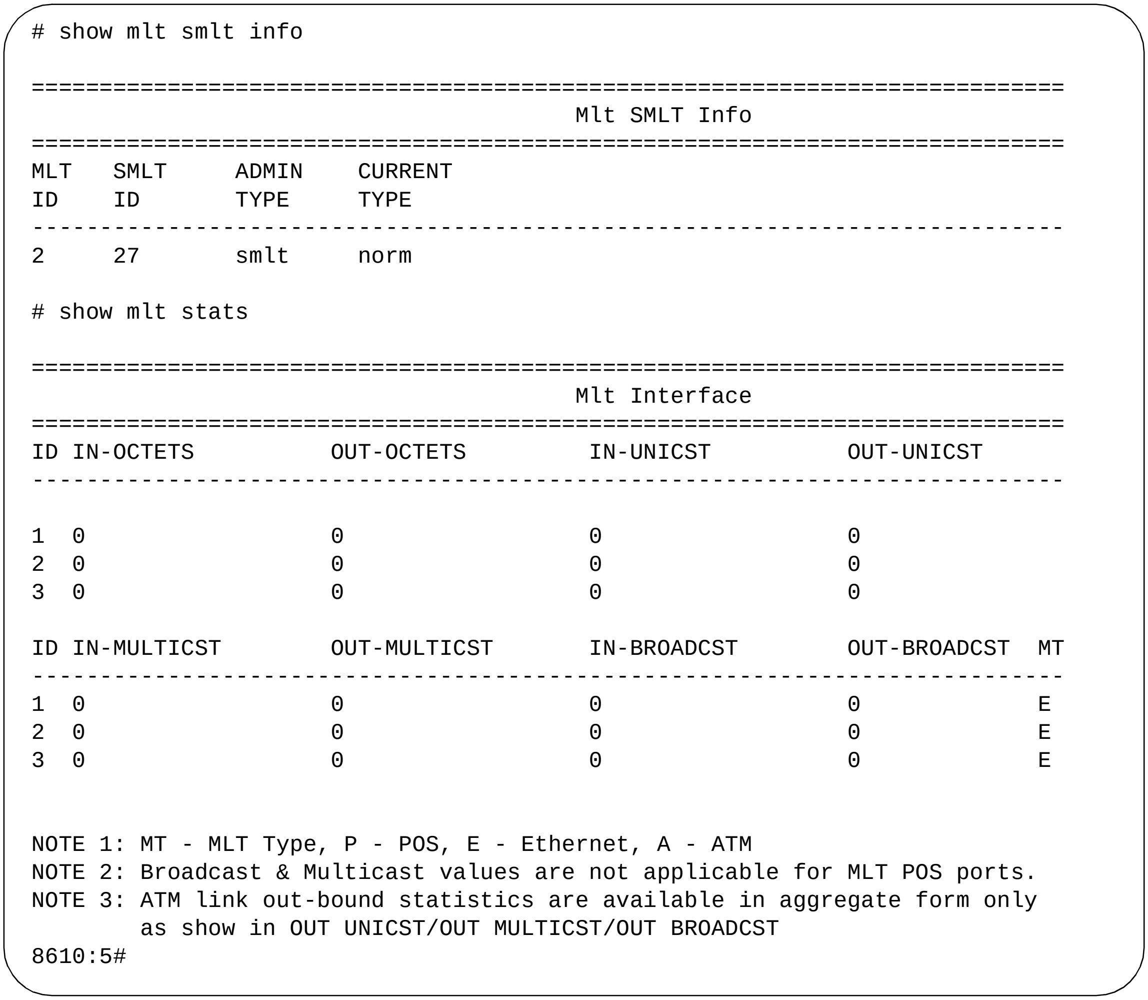
```
# show mlt ist stat


===========================================================================
                                        Mlt IST Message Statistics
===========================================================================
PROTOCOL MESSAGE            COUNT
---------------------------------------------------------------------------

Ist Down                  :  0
Hello Sent                :  0

Hello Recv                :  0
Learn MAC Address Sent    :  0
Learn MAC Address Recv    :  0
MAC Address AgeOut Sent   :  0
MAC Address AgeOut Recv   :  0
MAC Address Expired Sent :  0
MAC Address Expired Sent :  0
Delete Mac Address Sent   :  0
Delete Mac Address Recv   :  0
Smlt Down Sent            :  0
Smlt Down Recv            :  0
Smlt Up Sent              :  0
Smlt Up Recv              :  0
Send MAC Address Sent     :  0
Send MAC Address Recv     :  0
IGMP Sent                 :  0
IGMP Recv                 :  0
Port Down Sent            :  0
Port Down Recv            :  0
Request MAC Table Sent    :  0
Request MAC Table Recv    :  0
Unknown Msg Type Recv     :  0
```

Figure 122 show mlt show-all sample output (continued)



```
# show mlt smlt info

============================================================================
                                        Mlt SMLT Info
============================================================================
MLT   SMLT     ADMIN    CURRENT
ID    ID       TYPE     TYPE
----------------------------------------------------------------------------
2     27       smlt     norm

# show mlt stats

============================================================================
                                        Mlt Interface
============================================================================
ID IN-OCTETS          OUT-OCTETS         IN-UNICST          OUT-UNICST
----------------------------------------------------------------------------

1  0                  0                  0                  0
2  0                  0                  0                  0
3  0                  0                  0                  0

ID IN-MULTICST        OUT-MULTICST       IN-BROADCST        OUT-BROADCST  MT
----------------------------------------------------------------------------
1  0                  0                  0                  0             E
2  0                  0                  0                  0             E
3  0                  0                  0                  0             E


NOTE 1: MT - MLT Type, P - POS, E - Ethernet, A - ATM
NOTE 2: Broadcast & Multicast values are not applicable for MLT POS ports.
NOTE 3: ATM link out-bound statistics are available in aggregate form only
        as show in OUT UNICST/OUT MULTICST/OUT BROADCST
8610:5#
```

Displaying information about collision errors

To display information about collision errors in the specified MultiLink Trunk or all MLTs, enter the following command:

`show mlt error collision [<`*`mid`*`>]`

Figure 123 shows sample output for the **`show mlt error collision`** command.

Figure 123 show mlt error collision command output

```
8100:5# show mlt error collision

==================================================================
                         Mlt Collision Error
==================================================================
MLT   -----------------COLLISIONS------------
ID    SINGLE    MULTIPLE LATE     EXCESSIVE
------------------------------------------------------------------
1     0         0        0        0
2     0         0        0        0
```

Displaying information about Ethernet errors

To display information about the types of Ethernet errors sent and received by the specified MLT or all MLTs, enter the following command:

```
show mlt error main [<mid>]
```

Figure 124 shows sample output for the **`show mlt error main`** command. The IMAC columns refer to internal MAC address errors.

Figure 124 show mlt error main command output

```
8610# show mlt error main

=============================================================================
                         Mlt Ethernet Error
=============================================================================
MLT  ALIGN   FCS     IMAC    IMAC    CARRIER FRAMES  SQETEST DEFER
ID   ERROR   ERROR   TRNSMIT RECEIVE SENSE   TOOLONG ERROR   TRNSMSS
-----------------------------------------------------------------------------
1    0       0       0       0       0       0       0       0
```

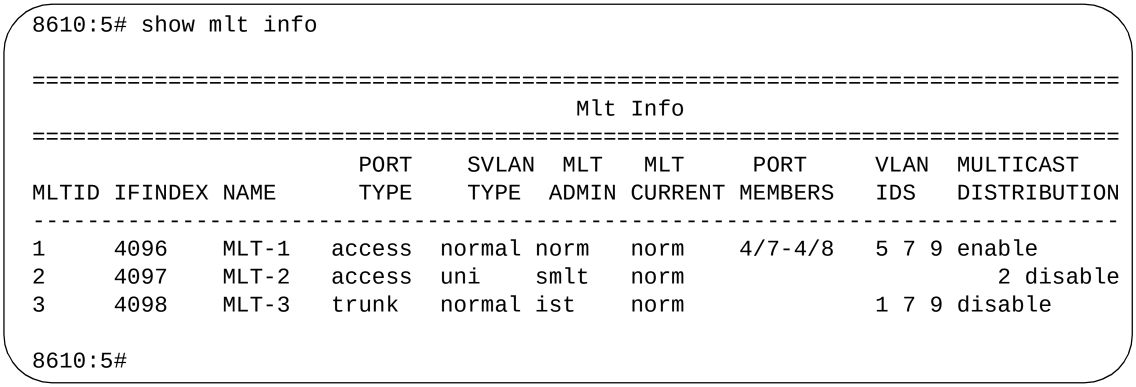
Displaying MLT status

To display the status of MultiLink Trunking for the switch or the specified MLT ID, enter the following command:

`show mlt info` [<*mid*>]

Figure 125 shows sample output for the **`show mlt info`** command.

Figure 125 show mlt info command output



```
8610:5# show mlt info

================================================================================
                                        Mlt Info
================================================================================
                        PORT    SVLAN  MLT   MLT     PORT     VLAN  MULTICAST
MLTID IFINDEX NAME      TYPE    TYPE   ADMIN CURRENT MEMBERS  IDS   DISTRIBUTION
--------------------------------------------------------------------------------
1     4096    MLT-1   access  normal norm    norm    4/7-4/8  5 7 9 enable
2     4097    MLT-2   access  uni    smlt    norm                      2 disable
3     4098    MLT-3   trunk   normal ist     norm             1 7 9 disable

8610:5#
```

Displaying SMLT status

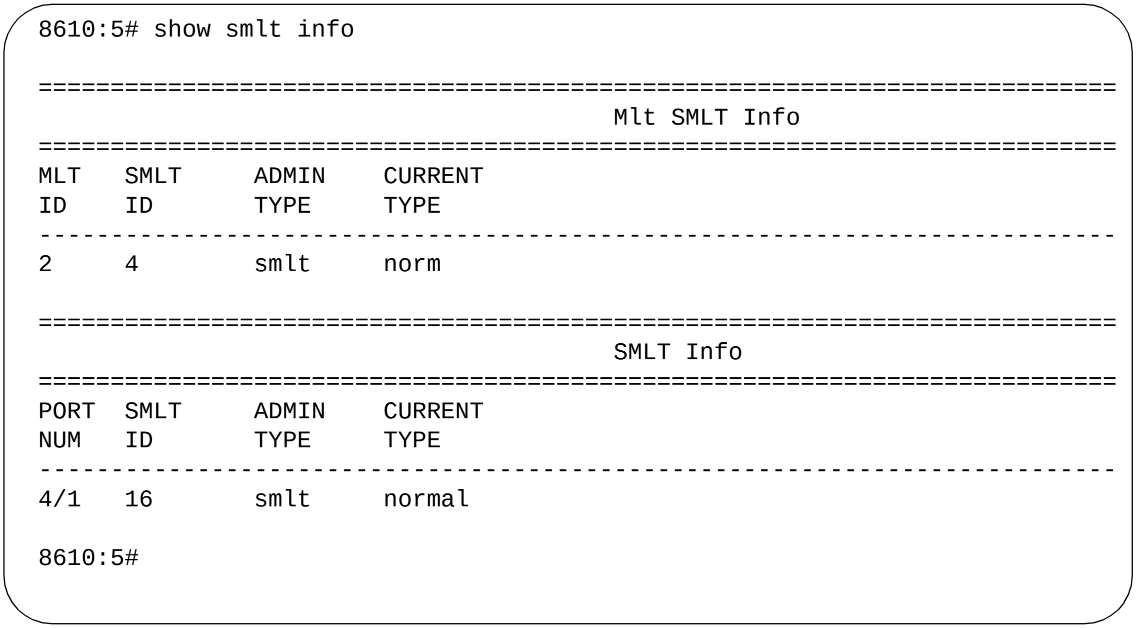
To display SMLT status for the switch or a specific SMLT ID, enter the following command:

`show smlt info [<`*`mid`*`>]`

The switch displays both MLT-based SMLT information, and single port SMLT information.

Figure 126 shows output from a sample **`show smlt info`** command.

Figure 126 show smlt info command output



```
8610:5# show smlt info

===========================================================================
                                        Mlt SMLT Info
===========================================================================
MLT   SMLT      ADMIN     CURRENT
ID    ID        TYPE      TYPE
---------------------------------------------------------------------------
2     4         smlt      norm

===========================================================================
                                        SMLT Info
===========================================================================
PORT  SMLT      ADMIN     CURRENT
NUM   ID        TYPE      TYPE
---------------------------------------------------------------------------
4/1   16        smlt      normal

8610:5#
```

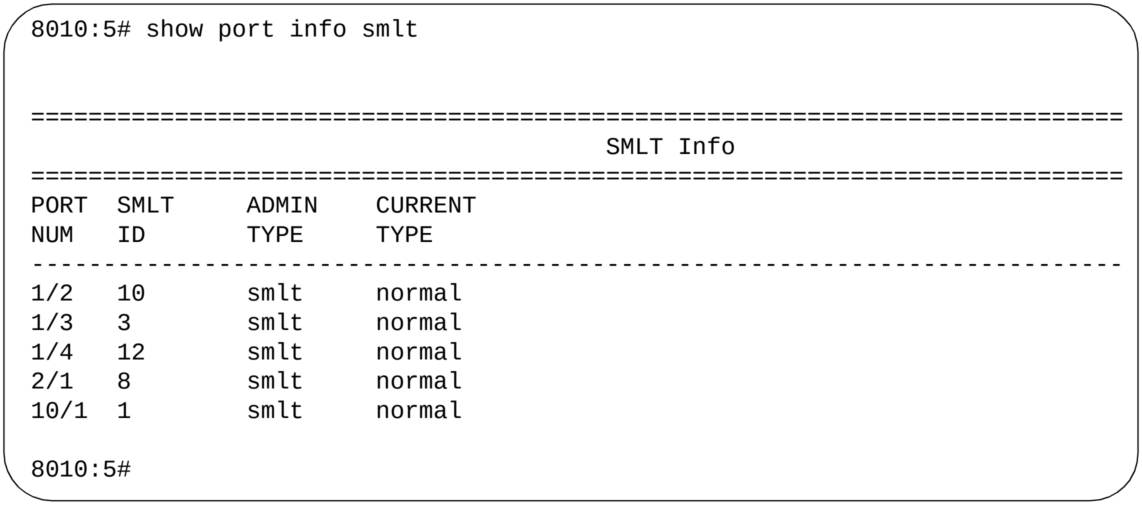
Displaying all ports configured for single port SMLT

To view all ports currently configured for single port SMLT, enter the following command:

```
show port info smlt
```

Figure 127 shows the output from a sample `show port info smlt` command.

Figure 127 show port info smlt command output



```
8010:5# show port info smlt


============================================================================
                                        SMLT Info
============================================================================
PORT  SMLT     ADMIN    CURRENT
NUM   ID       TYPE     TYPE
----------------------------------------------------------------------------
1/2   10       smlt     normal
1/3   3        smlt     normal
1/4   12       smlt     normal
2/1   8        smlt     normal
10/1  1        smlt     normal

8010:5#
```

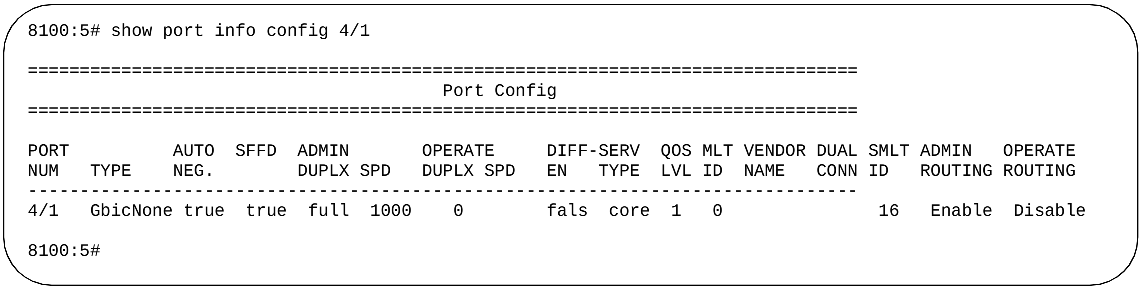
Displaying a port configured for single port SMLT

To view a port configured for single port SMLT, enter the following command:

`show port info config <`*`port`*`>`

Figure 128 shows output from a sample `show port info config <`*`port`*`>` command.

Figure 128 show port info config <*port*> command output



```
8100:5# show port info config 4/1

================================================================================
                                        Port Config
================================================================================

PORT          AUTO  SFFD  ADMIN       OPERATE     DIFF-SERV  QOS MLT VENDOR DUAL SMLT ADMIN   OPERATE
NUM   TYPE    NEG.        DUPLX SPD   DUPLX SPD   EN   TYPE  LVL ID  NAME   CONN ID   ROUTING ROUTING
--------------------------------------------------------------------------------
4/1   GbicNone true  true  full  1000    0        fals  core  1   0               16   Enable  Disable

8100:5#
```

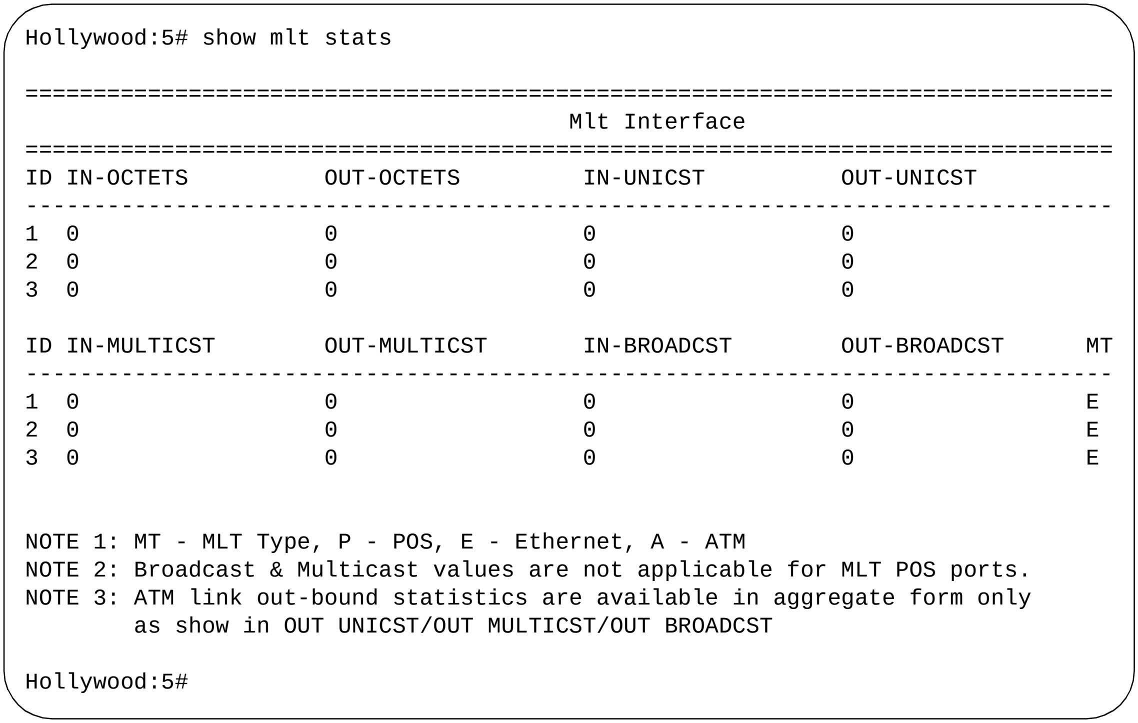
Displaying MLT statistics

To display MultiLink Trunking statistics for the switch or the specified MLT ID, enter the following command:

```
show mlt stats [<mid>]
```

Figure 129 shows sample output for the **show mlt stats** command.

Figure 129 show mlt stats command output



```
Hollywood:5# show mlt stats

================================================================================
                                        Mlt Interface
================================================================================
ID IN-OCTETS            OUT-OCTETS          IN-UNICST           OUT-UNICST
--------------------------------------------------------------------------------
1  0                    0                   0                   0
2  0                    0                   0                   0
3  0                    0                   0                   0

ID IN-MULTICST          OUT-MULTICST        IN-BROADCST         OUT-BROADCST      MT
--------------------------------------------------------------------------------
1  0                    0                   0                   0                 E
2  0                    0                   0                   0                 E
3  0                    0                   0                   0                 E


NOTE 1: MT - MLT Type, P - POS, E - Ethernet, A - ATM
NOTE 2: Broadcast & Multicast values are not applicable for MLT POS ports.
NOTE 3: ATM link out-bound statistics are available in aggregate form only
        as show in OUT UNICST/OUT MULTICST/OUT BROADCST

Hollywood:5#
```

Troubleshooting SMLT problems

This section provides procedures for troubleshooting IST problems and single-user problems.

The following topics are included:

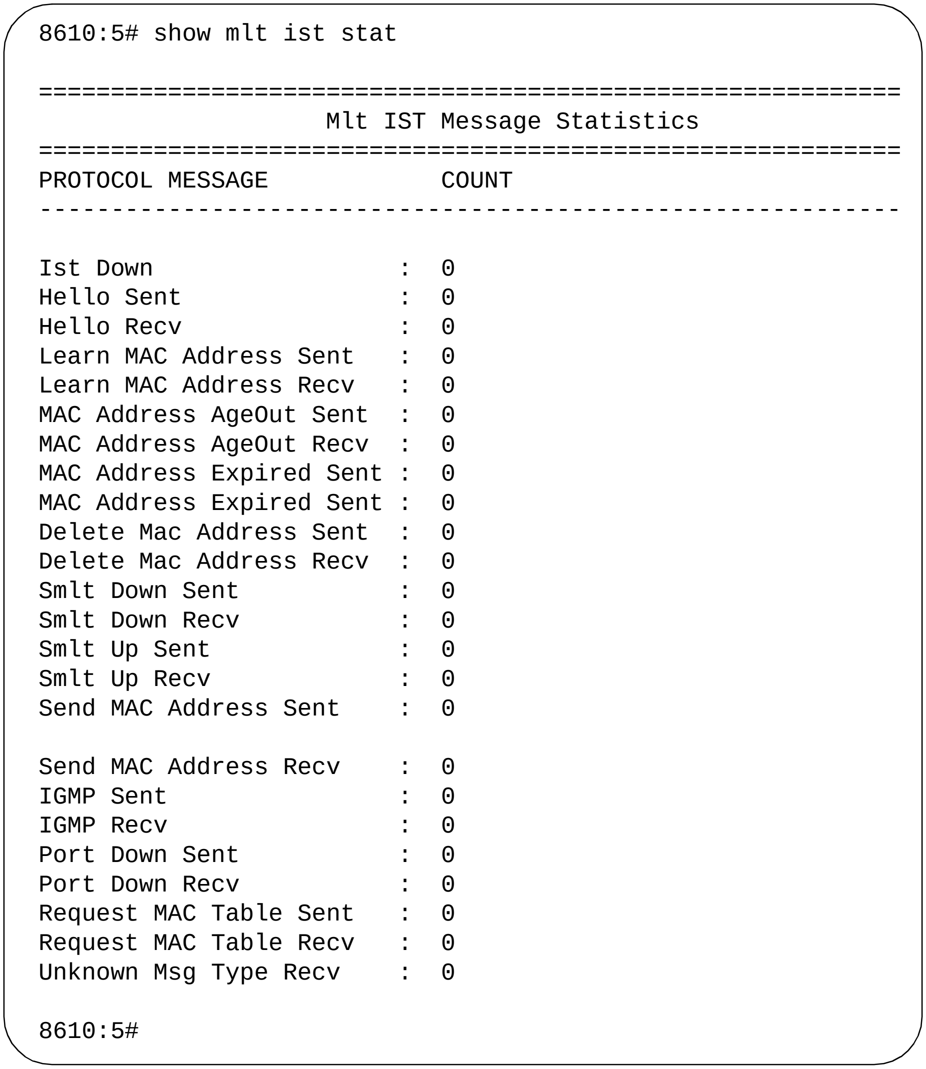
- Troubleshooting IST problems, next
- Troubleshooting problems with a single user (page 259)

Troubleshooting IST problems

To troubleshoot SMLT IST problems:

1 Enter the **`show mlt ist stat`** command to display the IST message count. (Figure 130).

Figure 130 show mlt ist stat command output



```
8610:5# show mlt ist stat

============================================================
                    Mlt IST Message Statistics
============================================================
PROTOCOL MESSAGE            COUNT
------------------------------------------------------------

Ist Down                 :  0
Hello Sent               :  0
Hello Recv               :  0
Learn MAC Address Sent   :  0
Learn MAC Address Recv   :  0
MAC Address AgeOut Sent  :  0
MAC Address AgeOut Recv  :  0
MAC Address Expired Sent :  0
MAC Address Expired Sent :  0
Delete Mac Address Sent  :  0
Delete Mac Address Recv  :  0
Smlt Down Sent           :  0
Smlt Down Recv           :  0
Smlt Up Sent             :  0
Smlt Up Recv             :  0
Send MAC Address Sent    :  0

Send MAC Address Recv    :  0
IGMP Sent                :  0
IGMP Recv                :  0
Port Down Sent           :  0
Port Down Recv           :  0
Request MAC Table Sent   :  0
Request MAC Table Recv   :  0
Unknown Msg Type Recv    :  0

8610:5#
```

2 Enter the **`show mlt info`** command to display all the MLTs in the switch, their admin-type, running type, ports, VLANs etc. (Figure 125).

3 Check to ensure that IST is up and running by using the **`show mlt ist info`** command (Figure 131).

Figure 131 show mlt ist info command output

```
8610:5# show mlt ist info

===============================================================
                    Mlt IST Info
===============================================================
MLT   IP                    VLAN     ENABLE   IST
ID    ADDRESS               ID       IST      STATUS
-------------------------------------------------------------
20     200.1.1.1           200       true   up

8610:5#
```

4 If IST is not running, check to ensure that:

a The correct VLAN ID exists on either side of the IST

b The IST configuration contains the correct local and peer IP addresses

5 If IST is running, check whether the SMLT port is operating by using the **`show mlt smlt info`** command (Figure 132).

a if the SMLT status is SMLT, the status is correct

Figure 132 show mlt smlt info command output

```
8610:5# show mlt smlt info

===============================================================
                    Mlt SMLT Info
===============================================================
MLT    SMLT   ADMIN  CURRENT
ID     ID     TYPE   TYPE
-------------------------------------------------------------
4      1      smlt   norm
8610:5#
```

b if the SMLT status is NORMAL, the link is running in a normal (single) mode and not SMLT mode. The reasons for this could be as follows:

- the remote SMLT link is not operational
- the ID is not configured on the other switch. To determine this, check to see whether the SMLT IDs match
- the IST is not up and running

Troubleshooting problems with a single user

To determine if only a single user is affected, check the VLAN FDB tables on both IST switches using the **show vlan info fdb-entry** <v*lan-id*> command. Both FDB tables should be synchronized.

The command displays whether:

- The MAC address is learned on the local SMLT port (i.e., SMLT REMOTE flag is false). See (Figure 133).

  or

- The MAC address is learned through IST from a remote SMLT port (that is, the SMLT REMOTE flag is true).

The FDB table entry for the client connected to the user access switch must specify the SMLT port as INTERFACE in both IST switches.

Figure 133 show vlan info fdb-entry command output

```
8610:5/show/vlan/info# fdb-entry 1

==============================================================
                       Vlan Fdb
==============================================================
VLAN         MAC                                QOS    SMLT
ID STATUS   ADDRESS     INTERFACE   MONITOR     LEVEL REMOTE
---------------------------------------------------------------
1 learned 00:08:c7:d0:82:cd Port-1/16 false    1      false
1 self    00:80:2d:12:36:00 -         false    1      false
2 out of 7 entries in all fdb(s) displayed.
8610:5#
```

Appendix A
Tap and OctaPID assignment

The switch fabric in the 8600 modules has nine switching taps, one for each of the eight I/O slots (1 to 4 and 7 to 10) and one for the CPU slots (5 and 6). Taps 0-7 map to the eight I/O slots and can support up to eight OctaPIDs. Each OctaPID can support up to eight ports.

In the [Product Name (long)], a physical port number is 10 bits long and has the following format:

```
9   6 5  3 2  0
+-----+----+----+
|     |    |    |
+-----+----+----+
```

bits 9–6: Tap number (0–15)

bits 5–3: OctaPID number (0–7)

bits 2-0: MAC port number (0-7)

The Tap number bits and the OctaPID number bits combined (bits 9–3) are usually referred to as the OctaPID ID.

Table 29 lists the module types that are currently available, along with the associated OctaPID ID assignments for each module.

Table 29 Available module types and OctapPID ID assignments

Module type	Port type	OctaPID ID assignment
8608GBE and 8608GBM Modules	1000BASE-SX	Table 30 next
	1000BASE-LX	
	1000BASE-ZX	
	1000BASE-XD	
8608GTE and 8608GTM Modules	1000BASE-T	Table 30 next
8608SXE Module	1000BASE-SX	Table 30 next
8616SXE Module	1000BASE-SX	Table 31 on page 263
8624FXE Module	100BASE-FX	Table 32 on page 264
8632TXE and 8632TXM Modules	10BASE-T/100BASE-TX	Table 33 on page 264
	1000BASE-SX	
	1000BASE-LX	
	1000BASE-ZX	
	1000BASE-XD	
8648TXE and 8648TXM Modules	10/100 Mb/s	Table 34 on page 264
8672ATME and 8672ATMM Modules	OC-3c MDA	Table 35 on page 265
	OC-12c MDA	
	DS3	
8681XLR Module	10GBASE-LR	Table 36 on page 265
8681XLW Module	10GBASE-LW	Table 37 on page 266
8683POSM Module	OC-3c MDA	Table 38 on page 266
	OC-12c MDA	

Table 30 describes the OctaPID ID and port assignments for the 8608GBE, 8608GBM, 8608GTE, 8608GTM, and 8608SXE modules.

Table 30 8608GBE/8608GBM/8608GTE/8608GTM, and 8608SXE modules

OctaPID ID assignment	Port assignment
OctaPID ID: 0	Port 1
OctaPID ID: 1	Port 2
OctaPID ID: 2	Port 3
OctaPID ID: 3	Port 4
OctaPID ID: 4	Port 5
OctaPID ID: 5	Port 6
OctaPID ID: 6	Port 7
OctaPID ID: 7	Port 8

Table 31 describes the OctaPID ID and port assignments for the 8616SXE Module.

Table 31 8616SXE module

OctaPID ID assignment	Port assignment
OctaPID ID: 0	Ports 1 and 2
OctaPID ID: 1	Ports 3 and 4
OctaPID ID: 2	Ports 5 and 6
OctaPID ID: 3	Ports 7 and 8
OctaPID ID: 4	Ports 9 and 10
OctaPID ID: 5	Ports 11 and 12
OctaPID ID: 6	Ports 13 and 14
OctaPID ID: 7	Ports 15 and 16

Table 32 describes the OctaPID ID and port assignments for the 8624FXE Module.

Table 32 8624FXE module

OctaPID ID assignment	Port assignment
OctaPID ID: 0	Ports 1 through 8
OctaPID ID: 1	Ports 9 through 16
OctaPID ID: 2	Ports 17 through 24

Table 33 describes the OctaPID ID and port assignments for the 8632TXE and 8632TXM Modules.

Table 33 8632TXE and 8632TZM modules

OctaPID ID assignment	Port assignment
OctaPID ID: 0	Ports 1 through 8
OctaPID ID: 1	Ports 9 through 16
OctaPID ID: 2	Ports 17 through 24
-	-
-	-
OctaPID ID: 5	Ports 25 through 32
OctaPID ID: 6	Port 33 (GBIC port)
OctaPID ID: 7	Port 34 (GBIC port)

Table 34 describes the OctaPID ID and port assignments for the 8648TXE and 8648TXM Modules.

Table 34 8648TXE and 8648TXM modules

OctaPID ID assignment	Port assignment
OctaPID ID: 0	Ports 1 through 8
OctaPID ID: 1	Ports 9 through 16
OctaPID ID: 2	Ports 17 through 24
-	-
-	-

Table 34 8648TXE and 8648TXM modules

OctaPID ID assignment	Port assignment
OctaPID ID: 5	Ports 25 through 32
OctaPID ID: 6	Port 33 through 40
OctaPID ID: 7	Port 41 through 48

Table 35 describes the OctaPID ID and port assignments for the 8672ATME and 8672ATMM Modules.

Table 35 8672ATME and 8672ATMM modules

OctaPID ID assignment	Port assignment
OctaPID ID: 0	• Ports 1 through 4 (with OC-3c MDA) • Port 1 (with OC-12c MDA) • Ports 1 through 2 (with DS-3 MDA)
OctaPID ID: 1	• Ports 5 through 8 (with OC-3c MDA) • Port 5 (with OC-12c MDA) • Ports 5 through 6 (with DS-3 MDA)
OctaPID ID: 2	Not used

Table 36 describes the OctaPID ID and port assignments for the 8681XLR Module.

Table 36 8681XLR module

OctaPID ID assignment	Port assignment
OctaPID ID: 0	Port 1
OctaPID ID: 1	
OctaPID ID: 2	
OctaPID ID: 3	
OctaPID ID: 4	
OctaPID ID: 5	
OctaPID ID: 6	
OctaPID ID: 7	

Table 37 describes the OctaPID ID and port assignments for the 8681XLW Module.

Table 37 8681XLW module

OctaPID ID assignment	Port assignment
OctaPID ID: 0	Port 1
OctaPID ID: 1	
OctaPID ID: 2	
OctaPID ID: 3	
OctaPID ID: 4	
OctaPID ID: 5	
OctaPID ID: 6	
OctaPID ID: 7	

Table 38 describes the OctaPID ID and port assignments for the 8683POSM Module.

Table 38 8683POSM module

OctaPID ID assignment	Port assignment
OctaPID ID: 0	• Ports 1 and 2 (with OC-3c MDA) • Port 1 (with OC-12c MDA)
OctaPID ID: 1	• Ports 3 and 4 (with OC-3c MDA) • Port 3 (with OC-12c MDA)
OctaPID ID: 2	• Ports 5 and 6 (with OC-3c MDA) • Port 5 (with OC-12c MDA)

Glossary

aggregation switch

A switch that aggregates multiple user access switches and provides core connections.

IST (Inter Switch Trunk)

One parallel point-to-point link that connects two aggregation switches together. This communication channel is used by the two aggregation switches for communication so that they may operate as a single logical switch for layer 2 operations. The IST also forwards data traffic like any other link does. Note that the IST should have multiple physical links in the IST MLT group.

Peer IP address

IP addresses of the neighbor IST switch VLAN that is chosen for configuring the IST. Note that the peer IP address is the IP address of the IST VLAN on the other aggregation switch. You need only configure one VLAN with an IP address for the IST protocol to work. All other VLANs on the IST do not require an IP address if you choose not to have VLAN routing enabled.

SMLT

An MLT that is split between two aggregation switches.

SMLT aggregation switches

The two switches that share the IST link.

SMLT clients

The edge switches/server that are connected to two SMLT aggregation switches through multilink trunking.

SMLT-ID

The identification number used to specify the corresponding pair of SMLT links. This number is identified between the two aggregation switches and must be paired on each aggregation switch.

SMLT set

Two SMLT aggregation switches and their directly connected SMLT clients.

SMLT square

A pair of SMLT aggregation switches connected in a full mesh as SMLT clients to another pair of SMLT aggregation switches.

SMLT triangle

A configuration where an SMLT client and the two aggregation switches form a triangle.

user access switch

A switch located at the edge of the network. End stations typically connect directly to a user access switch.

Index