Part No. 209419-D
September 2002

4655 Great America Parkway
Santa Clara, CA 95054

Release Notes for the BayStack 420 10/100/1000 Switch
Software Version 1.1.0

209419-D

NORTEL NETWORKS™

Copyright © 2002 Nortel Networks

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks Inc.

Trademarks

Nortel Networks, the Nortel Networks logo, the Globemark, Unified Networks, BayStack 420, and Optivity are trademarks of Nortel Networks.

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

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

Java is a trademark of Sun Microsystems, Inc.

Macintosh is a trademark of Apple Computer, Inc.

Netscape Navigator is a trademark of Netscape Communications Corporation.

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.

Contents

Introduction

These release notes contain important information about Nortel Networks BayStack 420 10/100/1000 Switch software and operational issues that is not available in the following related documents:

- *Using the BayStack 420 10/100/1000 Switch* (part number 209418-A)

  Describes how to use the BayStack 420 10/100/1000 Switch for network configuration.

- *Using Web-Based Management for the BayStack 420 10/100/1000 Switch* (part number 211252-A)

  Describes how to use the Web-based management tool to configure switch features.

- *Installing the BayStack 420 10/100/1000 Switch* (part number 209420-A)

  Describes how to install the BayStack 420 Switch.

- *Getting Started with BayStack 420 Software* (part number 211250-A)

  Describes how to install the Java-based device level software management application.

- *Reference for the BayStack 420 Management Software* (part number 211251-A)

  Describes how to use the Java-based device level software management application.

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.

These release notes contain the following sections:

- IGMP
- IEEE 802.1P
- ASCII configuration file
- Command Line Interface
- Known issues
- Known limitations

IGMP Snooping

BayStack 420 10/100/1000 Switches can sense Internet Group Management Protocol (IGMP) host membership reports from attached stations and use this information to set up a dedicated path between the requesting station and a local IP Multicast router. After the pathway is established, the BayStack 420 10/100/1000 Switch blocks the IP Multicast stream from exiting any other port that does not connect to another host member, thus conserving bandwidth. The following section describes how BayStack 420 10/100/1000 Switches provide the same benefit as IP Multicast routers, but in the local area.

IGMP is used by IP Multicast routers to learn about the existence of host group members on their directly attached subnets (see RFC 2236). The IP Multicast routers get this information by broadcasting IGMP queries and listening for IP hosts reporting their host group memberships. This process is used to set up a client/server relationship between an IP Multicast source that provides the data streams and the clients that want to receive the data.

Figure 1 shows how IGMP is used to set up the path between the client and server. As shown in this example, the IGMP host provides an IP Multicast stream to designated routers that forward the IP Multicast stream on their local network only if there is a recipient.

The client/server path is set up as follows:

1. The designated router sends out a host membership query to the subnet and receives host membership reports from end stations on the subnet.

2 The designated routers then set up a path between the IP Multicast stream source and the end stations.

3 Periodically, the router continues to query end stations on whether or not to continue participation.

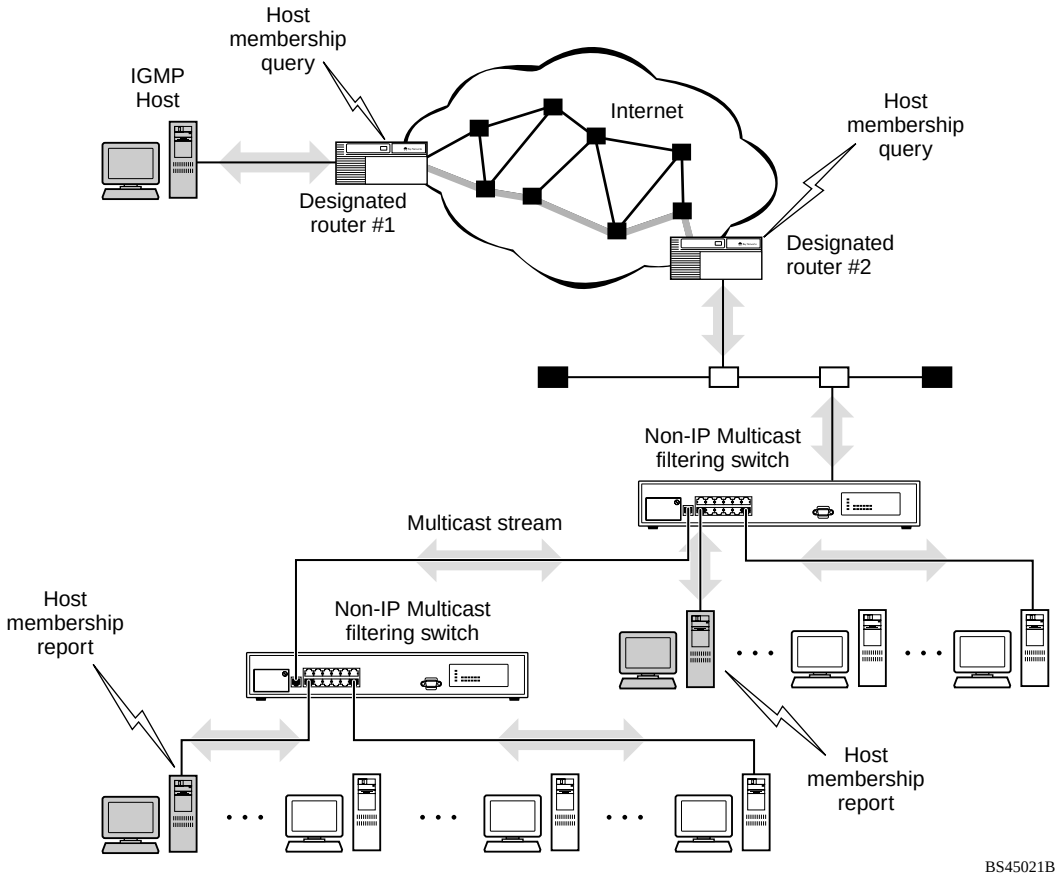
4 As long as any client continues to participate, all clients, including nonparticipating end stations on that subnet, receive the IP Multicast stream.

Note: Although the nonparticipating end stations can filter the IP Multicast traffic, the IP Multicast traffic still exists on the subnet and consumes bandwidth.

IP Multicast can be optimized in a LAN by using IP Multicast filtering switches, such as the BayStack 420 10/100/1000 Switch.

As shown in Figure 1, a non-IP Multicast filtering switch causes IP Multicast traffic to be sent to all segments on the local subnet.

Figure 1 IP Multicast propagation with IGMP routing

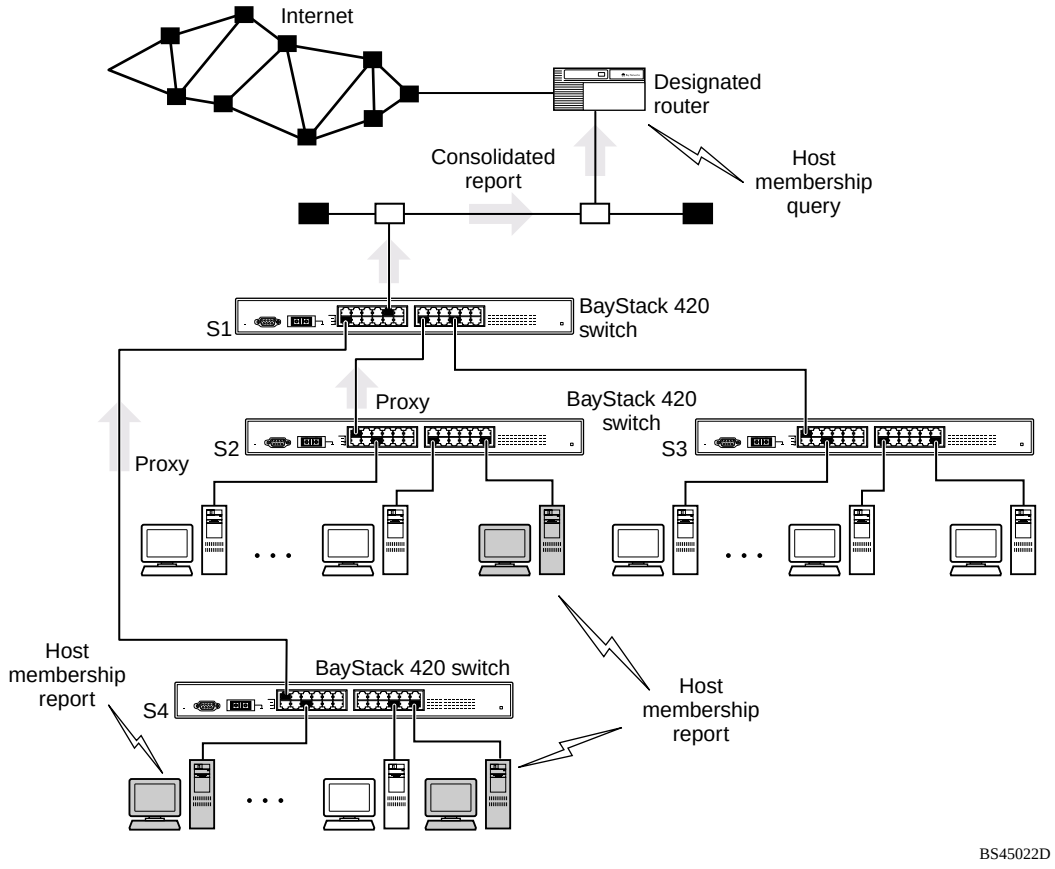


The BayStack 420 10/100/1000 Switch can automatically set up IP Multicast filters so the IP Multicast traffic is only directed to the participating end nodes (see Figure 2).

In Figure 2, switches S1 to S4 represent a LAN connected to an IP Multicast router. The router periodically sends Host Membership Queries to the LAN and listens for a response from end stations. All of the clients connected to switches S1 to S4 are aware of the queries from the router.

One client, connected to S2, responds with a host membership report. Switch S2 intercepts the report from that port, and generates a *proxy* report to its upstream neighbor, S1. Also, two clients connected to S4 respond with host membership reports, causing S4 to intercept the reports and to generate a *consolidated proxy report* to its upstream neighbor, S1.

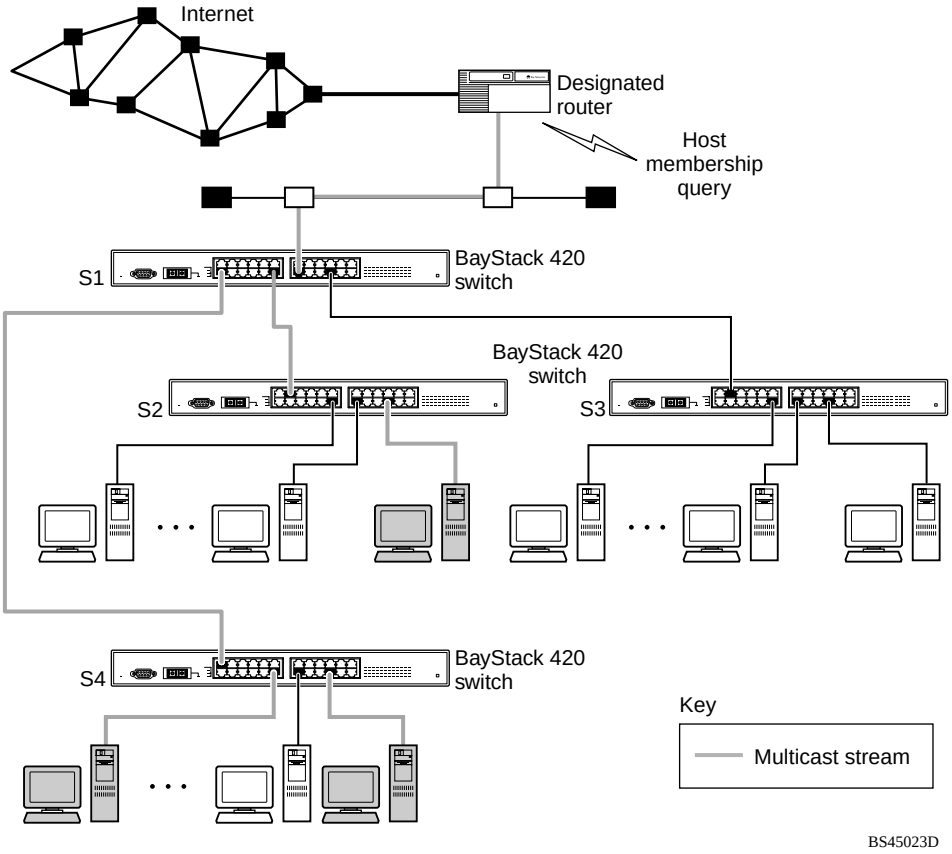
Figure 2 BayStack 420 10/100/1000 Switch filtering IP multicast streams (1 of 2)



Switch S1 treats the consolidated proxy reports from S2 and S4 as if they were reports from any client connected to its ports, and generates a consolidated proxy report to the designated router. In this way, the router receives a single consolidated report from that entire subnet.

After the switches learn which ports are requesting access to the IP Multicast stream, all other ports not responding to the queries are blocked from receiving the IP Multicast (Figure 3).

Figure 3 BayStack 420 10/100/1000 Switch filtering IP multicast streams (2 of 2)



The consolidated proxy report generated by the switch remains transparent to layer 3 of the International Organization for Standardization, Open Systems Interconnection (ISO/OSI) model. (The switch IP address and MAC address are not part of proxy report generation.) The last reporting IGMP group member in each VLAN represents all of the hosts in that VLAN and IGMP group.

IGMP snooping configuration rules

The IGMP snooping feature operates according to specific configuration rules. When configuring your switch for IGMP snooping, consider the following rules that determine how the configuration reacts in any network topology:

- A port that is configured for port mirroring cannot be configured as a static router port.
- If a MultiLink Trunk member is configured as a static router port, all of the MultiLink trunk members are configured as static router ports. Also, if a static router port is removed, and it is a MultiLink Trunk member, all MultiLink trunk members are removed as static router port members, automatically.
- Static router ports must be port members of at least one VLAN.
- If a static router port is removed, the membership for that port is removed from all VLANs of that port.
- The IGMP snooping feature is not STP-dependent.
- The IGMP snooping feature is not Rate Limiting-dependent.
- The snooping field must be enabled for the proxy field to have any valid meaning.
- Static router ports are configured per VLAN and per IGMP Version.

Note: Because IGMP snooping is set up per VLAN, all IGMP changes are implemented according to the VLAN configuration for the specified ports.

IGMP Configuration screen

To open the IGMP Configuration screen:

1. Select IGMP Configuration (or press g) from the Switch Configuration Menu screen to access the IGMP Configuration Menu screen.
2. In the IGMP Configuration Menu screen, Select IGMP Configuration.

   The IGMP Configuration screen (Figure 4) opens.
3. In the IGMP Configuration screen select the parameters and enter the values that you want to use in the screen fields. See Table 1.

Figure 4 IGMP Configuration screen

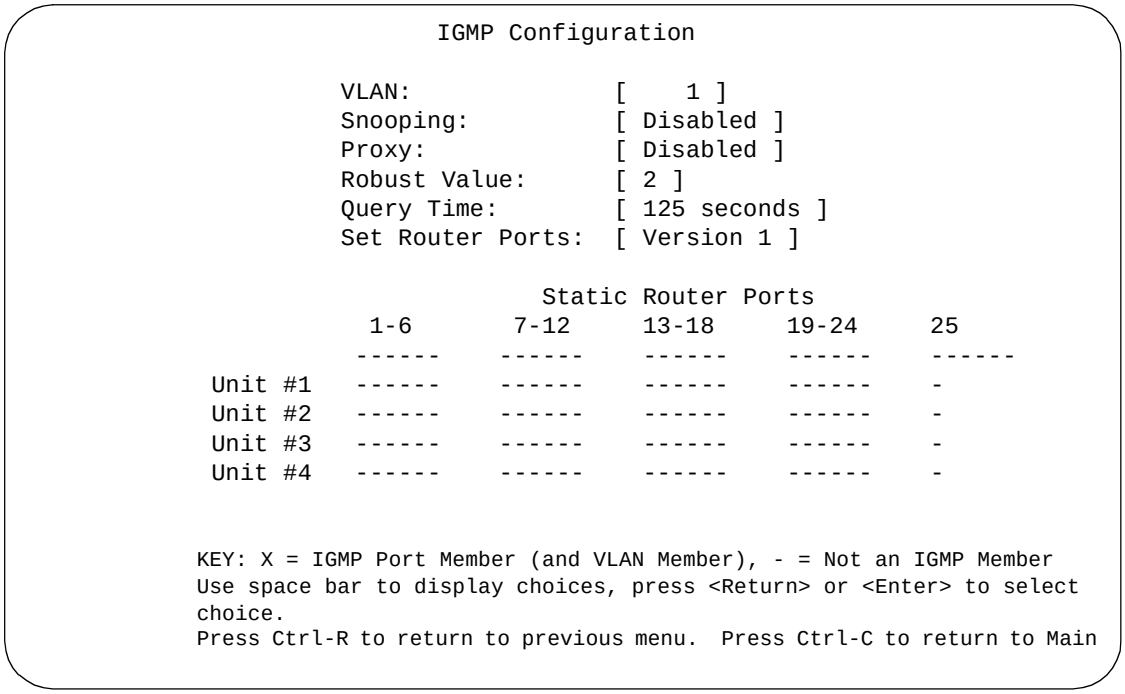


Table 1 describes the IGMP Configuration screen fields.

Table 1 IGMP Configuration screen fields

Field	Description
VLAN	Allows you to set up or view IGMP VLAN configurations on specified VLANs. You can use the space bar to toggle to any *existing* IGMP VLAN configurations (the maximum number of VLANs that can be displayed is 256). Default 1 Range 1 to 4094
Snooping	Allows you to enable or disable IGMP Snooping. This field affects all VLANs (for example, if you disable snooping on the VLAN specified in the screen's VLAN field, ALL VLANs are disabled for snooping). Default Value Enabled Range Enabled, Disabled

Table 1 IGMP Configuration screen fields (continued)

Field	Description
Proxy	Allows the switch to consolidate IGMP Host Membership Reports received on its downstream ports and to generate a consolidated proxy report for forwarding to its upstream neighbor. This field affects all VLANs (for example, if you disable proxy on the VLAN specified in the screen's VLAN field, ALL VLANs are disabled for proxy). The Proxy field cannot be disabled unless the Snooping field is enabled. Default Value Enabled Range Enabled, Disabled
Robust Value	Allows a user to set the switch to offset expected packet loss on a subnet. If packet losses on a subnet are unacceptably high, the Robust Value field can be increased to a higher value. This field affects only the VLAN specified in the screen's VLAN field (for example, if you change the robust value on the VLAN specified in the screen's VLAN field, other VLANs are not affected). Default Value 2 Range 1 to 256
Query Time	Allows a user to control the number of IGMP messages allowed on the subnet by varying the *Query Interval* (the Query Interval is the interval between general queries sent by the multicast router). This field affects only the VLAN specified in the screen's VLAN field (for example, if you change the Query Time value field on the VLAN specified in the screen's VLAN field, other VLANs are not affected). Default Value 125 seconds Range 1 to 512 seconds
Set Router Ports	Selects the IGMP version according to the IGMPv1 (Version 1) or IGMPv2 (Version 2) standard (see RFC 2236). Use this field in conjunction with the Static Router Ports field (see next field description) to select the IGMP version to set. You can also use this field to view which static router ports are set to Version 1 or to Version 2. Use the space bar to toggle between the two versions and view the static router ports settings. This field affects all VLANs (for example, if you change the value of the Set Router Ports field on the VLAN specified in the screen's VLAN field, ALL VLANs are affected). Default Value Version 1 Range Version 1, Version 2

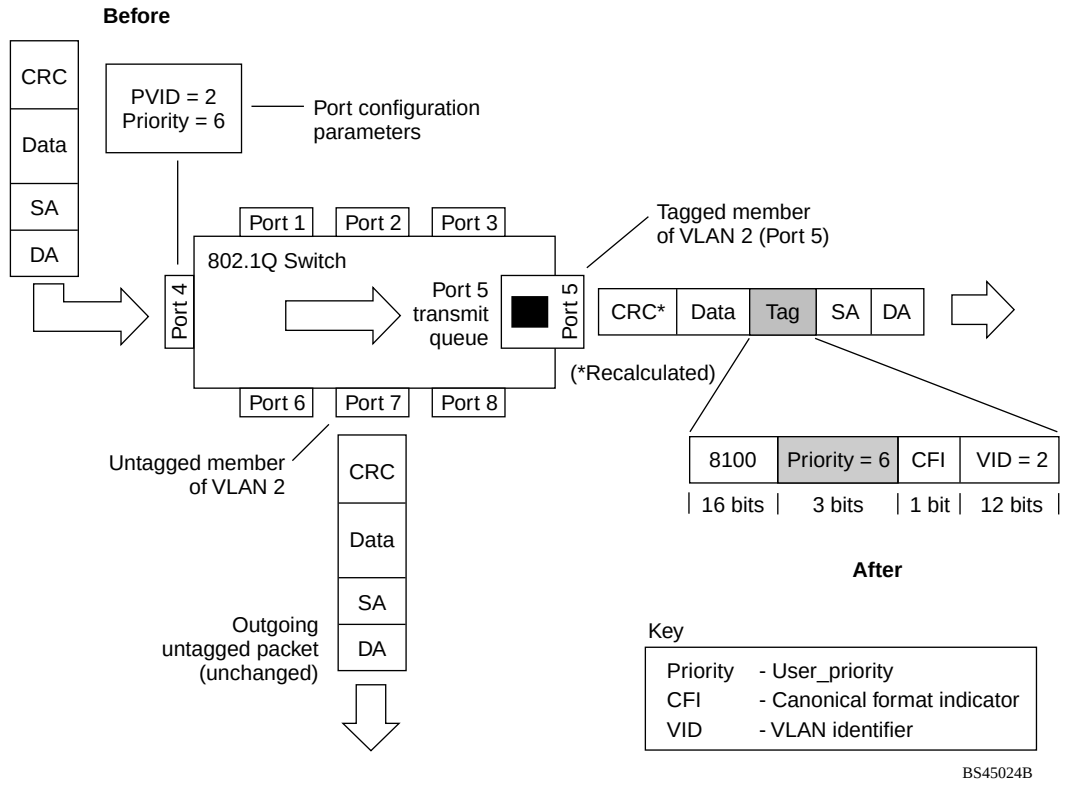
Table 1 IGMP Configuration screen fields (continued)

Field	Description
Static Router Ports	Allows a user to assign switch ports to any port that has a path to a multicast router. The configured ports do not filter any IP Multicast traffic. The Static Router Ports fields are displayed in six-port groups (for example, 1-6, 7-12, 13-18). The number of ports displayed depends on the switch model. This field affects all VLANs (for example, if you assign a port as a static router port in this screen, the port becomes a static router port for the VLAN specified in the screen's VLAN field, and also for any other VLAN where this port is a member). Default Value - Range -, X

IEEE 802.1p prioritizing

You can use the VLAN Configuration screens to prioritize the order in which the switch forwards packets, on a per-port basis. For example, if messages from a specific segment are crucial to your operation, you can set the switch port connected to that segment to a higher priority level (by default, all switch ports are set to low priority). Untagged packets received by the switch on that port are tagged according to the priority level you assign to the port (see Figure 5).

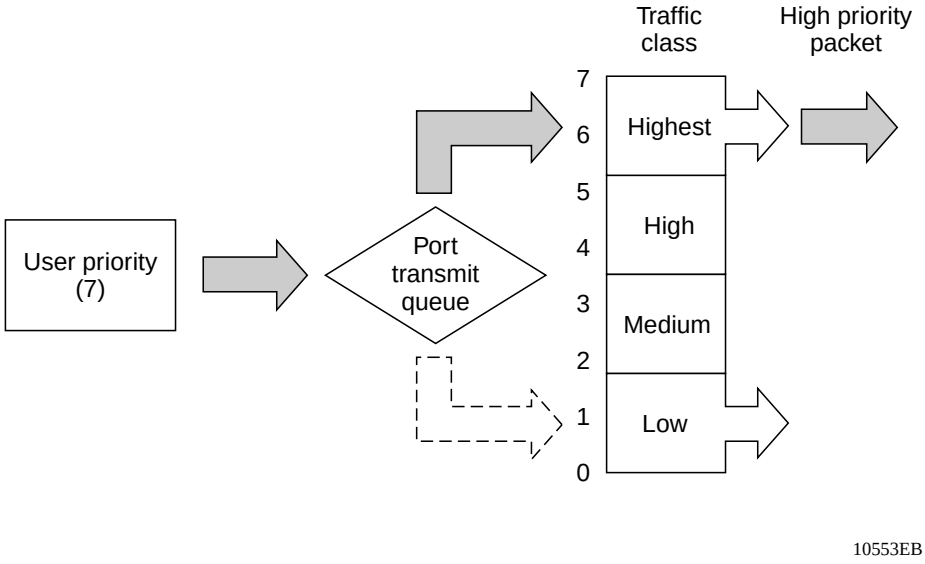
Figure 5 Prioritizing packets



The newly tagged frame is read within the switch and sent to the port's transmit queue for disposition.

The newly tagged frame is read within the switch and sent to the port's transmit queue for disposition. The port transmit queue example shown in Figure 5 applies to all ports in the BayStack 420 switch.

Figure 6 Port Transmit Queue



The switch provides four transmission queues, *Highest*, *High*, *Medium*, and *Low* for any given port. Frames are assigned to one of these queues on the basis of the user_priority value, using a *traffic class table*. This table is managed by using the Traffic Class Configuration screen. The table indicates the traffic class assigned to the frame for each user_priority value. If the frame leaves the switch formatted as a tagged packet, the traffic class assigned to the frame is carried forward to the next 802.1p-capable switch. This allows the packet to carry the assigned traffic class priority through the network until it reaches its destination.

The Traffic Class Policy Configuration screen prioritizes the order in which a switch forwards packets, on a per-port basis. BayStack 420 provides four transmission queues. Frames are assigned to one of these queues on the basis of the user-priority using a traffic class table. The table indicates the traffic class that is assigned to the frame for each possible user-priority value.

To use the Traffic Class Policy Configuration screen , follow these steps:

1 Select Policy Configuration from the Traffic Class Configuration menu.

The Traffic Class Policy Configuration screen (Figure 7) opens.

Figure 7 Traffic Class Policy Configuration Screen

```
Traffic Class Policy Configuration




Policy type:                [ Weighted RR ]

Bound Delay:                [ 32 us ]

Low     Q weight:           [ 32  ]
Med     Q weight:           [ 64  ]
High    Q weight:           [ 96  ]
Highest Q weight:           [ 128 ]


Are you sure you want to change policy to the new settings? [ No ]


Use space bar to display choices, press <Return> or <Enter> to
select choice.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to
Main Menu.
```

Table 2 Traffic Class Policy Configuration screen fields

Field	Description
Policy Type	Specifies the type of policy. There are 3 types: weighted round robin, bounded round robin, and strict.
Weighted RR	Each queue is assigned a weight. This value indicates how many packets may be transmitted out of the queue before the next highest queue is serviced. Control may transfer to the next highest queue even though the higher priority queues have not emptied To determine the percentage of bandwidth allocated to each queue, add the total weight and then divide each queue weight by that value. This formula works only when all queues are fully utilized.
Bounded RR	Bounded RR works the same as weighted RR except that it uses the bounded delay parameter to specify the maximum amount that a packet may wait in the priority queue before the round robin algorithm starts again at the highest priority queue..
Strict	The strict dequeuing algorithm empties the higher priority queues first Once the higher priority queue is empty, then the next priority queue is serviced. If a packet comes out of a higher priority queue transmission out of the lower priority queue is suspended until transmission from the higher priority queues finish transmitting.
Bounded Delay	Specifies the maximum amount of time that a packet may wait in the highest priority queue before the round robin algorithm starts again at the highest priority queue.
Q Weight	.This value indicates how many packets may be transmitted out of the queue before the next highest queue is serviced.

2 Use the space bar to toggle to the options available for Policy type, Bounded Delay, and Q Weight.

The following steps show how to use the Traffic Class Priority Configuration screen to configure the port priority level.

To configure the priority level, follow these steps:

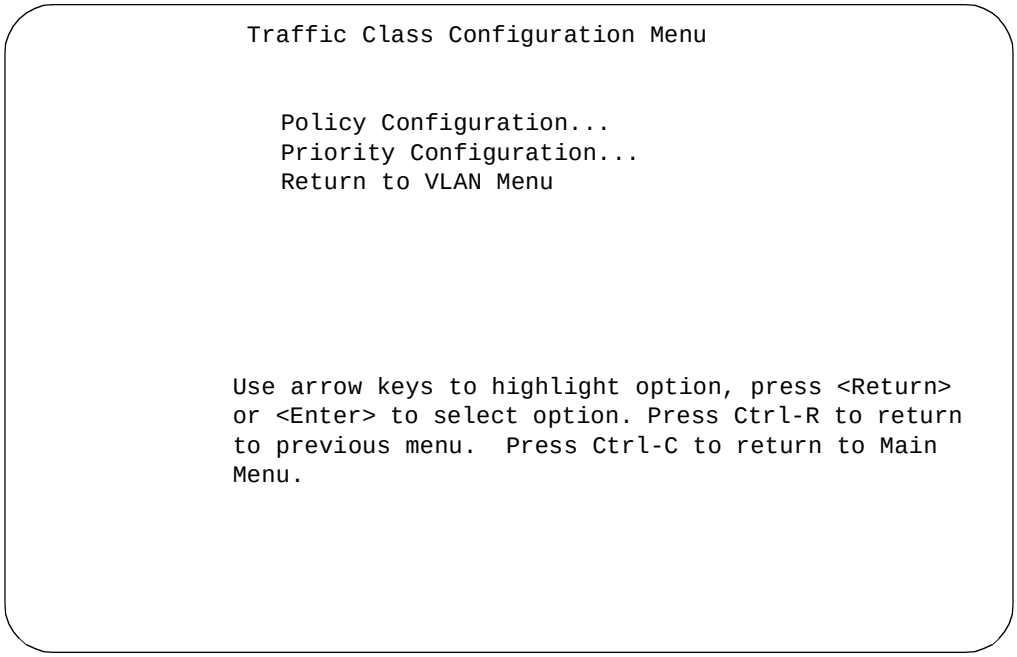
1. Determine the priority level you want to assign to the switch port.

   User priority levels are assigned default settings in all BayStack 420 switches. The range is from 0 to 7. The traffic class table can be modified. You can view or make changes to the settings shown in the Traffic Class Priority configuration screen, and then set the port priority in the VLAN Port Configuration screen.

2. In the VLAN Configuration Menu, select Traffic Class Configuration.

   The Traffic Class Configuration Menu screen (Figure 8) opens.

Figure 8 Traffic Class Configuration Menu Screen



3. Select Priority Configuration.

   The Traffic Class Priority Configuration screen (Figure 9) opens.

4. Select a priority level from the range shown in the Traffic Class Priority Configuration screen.

5. To assign the priority level to ports, use the VLAN Port Configuration screen:

a Press [Ctrl}-R twice to return to the VLAN Configuration Menu.

b From the VLAN Configuration Menu, select VLAN Port Configuration.

Figure 9 Traffic Class Priority Configuration screen

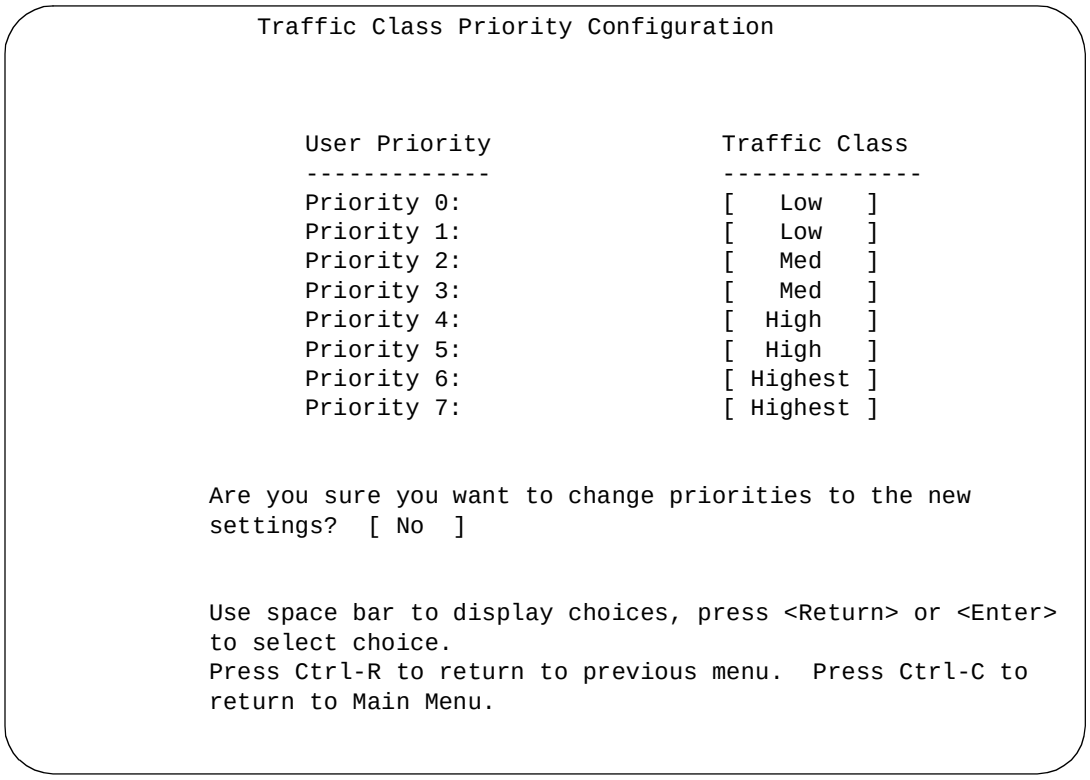


Table 3 Traffic Class Priority screen fields

Field	Description
User Priority	Specifies the 802.1p priority for different classes of users.
Traffic Class	Specifies the associated traffic class from low to highest.

ASCII configuration file

The BayStack 420 Switch can download a user-editable ASCII configuration file from a TFTP server. You can load the ASCII configuration file automatically at boot time or on demand using the management systems (console menus or CLI). Once downloaded, the configuration file automatically configures the switch or stack according to the Command Line Interface (CLI) commands in the file. This feature allows the flexibility of generating command configuration files that can be use on several switches or stacks with minor modifications. (The maximum size for an ASCII configuration file is 100 KBs; larger configuration files must be split into multiple files.)

Use a text editor to edit the ASCII configuration; the command format is the same as that of the CLI.

You can initiate the ASCII configuration file download using CLI commands only while connected to the base unit, and the ASCII configuration script will execute to completion. When you initiate downloading the ASCII configuration file from the console interface, the console does not display output. For this reason, it is important that you review the commands in the file to ensure accuracy and completeness.

Sample ASCII configuration file

This section shows a sample ASCII configuration file. This file is an example only and shows a basic configuration for a standalone BayStack 420 Switch that includes Multi-Link Trunking, VLANs, port speed and duplex, and SNMP configurations.

```
! ----------------------------------------------------------
! example script to configure different features from CLI
! ----------------------------------------------------------
!
enable
configure terminal
!
!
! ----------------------------------------------------------
! add several MLTs and enable
! ----------------------------------------------------------
mlt 3 name lag3 enable member 13-14
mlt 4 name lag4 enable member 15-16
mlt 5 name lag5 enable member 17-18
!
!
! ----------------------------------------------------------
! add vlans and ports
! ----------------------------------------------------------
!
! create vlan portbased
vlan create 100 name vlan100 type port
!
! add Mlts created above to this VLAN
vlan members add 100 17
!
! create vlan ip protocol based
vlan create 150 name vlan150 type protocol-ipEther2
!
! add ports to this VLAN
! in this case all ports
vlan members add 150 ALL
vlan ports ALL priority 3
!
```

```
! ----------------------------------------------------
! Examples of changing interface parameters
! ----------------------------------------------------
! change speed of port 3
interface Fastethernet 3
speed 10
duplex half
exit
!
! change speed of port 4
interface Fastethernet 4
speed auto
duplex auto
!
!
! ----------------------------------------------------
! SNMP configuration
! ----------------------------------------------------
snmp host 192.168.100.125 private
snmp community private
!
!
exit
end
! ----------------------------------------------------
! Finished
! ----------------------------------------------------
```

Note: To add comments to the ASCII configuration file, add an exclamation point (!) to the beginning of the line.

Command Line Interface

Refer to the *Reference for the BayStack 420 10/100/1000 Command Line Interface, Software Version 1.1.0* for more detailed information on using the Comand Line Interface (CLI) commands.

General issues

The following are general issues for the BayStack 420 10/100/1000 Switch, Software Version 1.1.0:

Download over a MLT Trunk

Downloading new software over an MLT link may fail if one of the trunk members is disconnected during the download process. If this should occur simply re-initiate the download process.

Autonegotiation

When connecting the BayStack 420 to other devices, please ensure that either autonegotiation is enabled on both ends of the link, or that the duplex and speed settings match.

MAC Address table

In addition to MAC Addresses learned on ports receiving unicast packets, the switch also display multicast addresses in its MAC Address table. As expected, these addresses are listed with no port association.

MAC Security on links between switches

If Mac Security is enabled on a port that is connected to another switch, the MAC address of the attached switch should be entered in MAC Address Security Table to ensure that BPDUs do not trigger a security event such as partitioning a port

Important stacking information

The BayStack 420-24T hardware can be stacked to form a unidirectional ring with a data rate of 1 gigabit per second. A stacking cable connects the Up connector of one unit in a stack to the Down connector of the next unit in the stack. A stack cable is also used to join the top and bottom units in a stack to complete the ring. For larger stacks, this requires a 100 cm cable.

After you have completed the cabling of a stack, and have pressed the Unit Select switch for the base unit in the stack, you can turn on the power for the switch. If the stack ring is broken by the removal of a cable or the loss of power to any unit in the stack, then all of the units in the stack become standalone units.

If you make any changes to the size of a stack by adding or removing units, you will need to turn the power to the stack back on after you have connected all the cables and completed the new stack ring. Once the power is turned on, it takes about three minutes to build the new stack. However, Nortel recommends that you make changes to a stack at times of low network use in order to minimize the effect on other network users.

You can find more information about the BayStack 420-24T hardware in the *Using the BayStack 420 10/100/1000 Switch* manual. This document can be found on the CD in the documentation kit that comes with the switch.

Known issues

The following issues are known to exist in version 1.1.0 of the BayStack 420 software:

802.1p

When modifying the Port Priority configuration parameter, you may receive an "Unexpected Error" message. This error message provides no useful information to the user and should be ignored. (CR Q00385128)

IGMP

If you are running IGMP and move both your server and host to different ports at the same time without allowing the ports to time out, or disabling the ports, then there is the possibility that IGMP packets will flood the network. Please make sure that you disable IGMP before moving the host and the server simultaneously. (CR Q00386792)

Autotopology

The BayStack 420 does not forward Autotopology multicast packets when the Autotopology feature is disabled. (CR Q00411390)

Spanning Tree

When making changes to the STP configuration using the Console interface, make those changes on a per switch basis. Do not apply STP configuration changes to the entire stack. (CR Q00504926)

Secondary Radius Server

The BayStack 420 software does not currently support a Secondary Radius Server. (CR Q00225383)

Monitor Port

If you are using port mirroring and reset the switch or stack, then the monitor port's spanning tree mode will be set to normal learning. (CR Q00316540)

Multilink trunking issues

Multilink trunking for the BayStack 420 10/100/100 switch has the following issue:

- If you add a new trunk link when a link already exists between the BayStack 420 switch and a Passport 8600 switch, the traffic flowing between the two switches may be interrupted for up to 10 minutes. This occurs when the Passport 8600 switch does not flush the MAC table because of a a topology change, and because the Spanning Tree Protocol (STP) is blocking the ports associated with the existing link.
- If you change the Spanning Tree Mode of an MLT link, all other MLT links will inherit that mode if the unit reboots, therefore it is highly recommended that you have all MLT links configured identically when it comes to the Spanning Tree Mode. (CR Q00495416)

Web-based management issues

The BayStack 420 10/100/1000 Switch has the following Web-based management issues:

- In Web-based management, Switch view shows Cas in/out instead of Cas Up/Down.
- When you use Web-based management to access the Switch view, you may receive security warnings. This is normal.
- Netscape* Communicator 4.6 does not show the switch view screen in Web-based management. You should use Netscape Communicator 4.77 to access the switch view.
- In Web-based management, you cannot change a non-base unit's console port speed. You can only change the speed of the base-unit console port using the Web interface.
- In Web-based management, you cannot disable a port that is a trunk member. You should use the console or Telnet interface to disable the port.
- Resizing the Netscape browser window reloads the main Web-based management page.
- The ability to select FastLearn on the Spanning Tree Cfg Web Interface screen does not function properly. The Console interface should be used to perform this function. (CR Q00248805)

Port statistics issues

The BayStack 420 10/100/1000 Switch has the following port statistics issue:

- Port Statistics do not display the number of packets received and transmitted as separate counts. The statistics display the number of packets received and transmitted as one aggregate number.

Device Manager issues

The BayStack 420 Device Manager has the following issues:

- The Device Manager requires a monitor that displays 256 or more colors to operate.
- The Device Manager does not support the Macintosh* computer.
- If you are running Microsoft* Windows* 2000 and use Device Manager to start a Telnet session, Windows 2000 opens two Telnet windows.
- Currently, there is no autoPVID feature in Device Manager because there is no MIB support.
- Version 1.3.0 of the Java* Runtime Environment (JRE) does not support dual processors under Windows 2000. However, version 1.3.0_02 of the Java Runtime Environment supports them. Go to http://java.sun.com/j2se/1.3/download-windows.html for a download of this version of the JRE software.

File names and network management software support

The following table provides agent and network management software information.

Table 4 Agent and network management support items

Item	Description
Agent File Name	bs420110_33.img
Device Manager Support	5.2 or higher
Optivity NMS Support	ONMS 9.1.0.2 and above (OIT file is required)
OIT File Name	NMS-BS420-v10-A.oit

Reference for the BayStack 420 Management Software issues

The following sections are additions to the *Reference for the BayStack 420 Management Software* (part number 211251-A).

Bridge parameters

Bridge parameters allow you to configure the global Spanning Tree and to view the MAC address table for a BayStack 420 10/100/1000 Switch. Bridge information also includes Spanning Tree Group (STG) information.

Bridge information is available in Device Manager on the following tabs:

- Base tab (next)
- Spanning tree tab (page 30)
- Transparent tab (page 33)
- Forwarding tab (page 34)
- Configuration tab (page 37)
- Status tab (page 38)
- Port tab (page 40)

Base tab

The MAC address used by the bridge must be referred to in a unique fashion; moreover, it should be the smallest MAC address (numerically) of all ports that belong to the bridge. However it is only required to be unique when integrated with dot1dStpPriority. A unique BridgeIdentifier is formed that is used in the Spanning Tree Protocol.

To view the Base tab:

➔ From the menu bar, select Edit > Bridge.

The Bridge dialog box opens with the Base tab displayed (Figure 10).

Figure 10 Base tab

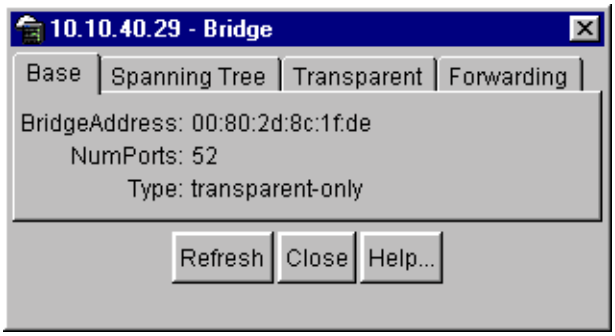


Table 5 describes the Base tab fields.

Table 5 Base tab fields

Field	Description
BridgeAddress	MAC address of the bridge when it is referred to in a unique fashion. This address should be the smallest MAC address of all ports that belong to the bridge. However, it is has to be unique. When concatenated with dot1dStpPriority, a unique bridge ID is formed that is then used in the Spanning Tree Protocol.
NumPorts	Number of ports controlled by the bridging entity.
Type	Indicates the type of bridging this bridge can perform. If the bridge is actually performing a certain type of bridging, this will be indicated by entries in the port table for the given type.

Spanning Tree tab

The Spanning Tree tab displays the version of the spanning tree protocol currently running. If future versions of the IEEE spanning tree protocol are released that are incompatible with the current version, a new value will be defined.

To view the Spanning Tree tab:

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

The Bridge dialog box opens, with the Base tab displayed (Figure 10).

2 Click the Spanning Tree tab.

The Spanning Tree tab opens (Figure 11).

Figure 11 Spanning Tree tab

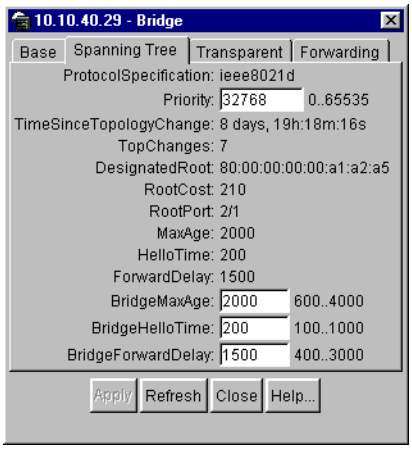


Table 6 describes the Spanning Tree tab fields.

Table 6 Spanning Tree tab fields

Field	Description
ProtocolSpecification	Version of the Spanning Tree Protocol being run. Values include: • decLb100: Indicates the DEC LANbridge 100 Spanning Tree Protocol. • ieee8021d: IEEE 802.1d implementations will return this entry. When future versions of the IEEE Spanning Tree Protocol are released that are incompatible with the current version, a new value will be defined.
Priority	Value of the writable portion of the bridge ID. That is, the first two octets of the (8-octet long) bridge ID. The last six octets of the bridge ID are given by the value of BridgeAddress.
TimeSinceTopologyChange	Time (in hundredths of a second) since the last time a topology change was detected by the bridge entity.
TopChanges	Number of topology changes detected by this bridge since the management entity was reset or initialized.
DesignatedRoot	Bridge ID of the root of the spanning tree as determined by the Spanning Tree Protocol. This is executed by the node. This value is used as the Root ID parameter in all configuration bridge PDUs originated by the node.

Table 6 Spanning Tree tab fields (continued)

Field	Description
RootCost	Cost of the path to the root as seen from this bridge.
RootPort	Port number of the port that offers the lowest cost path from this bridge to the root bridge.
MaxAge	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	Time between the transmission of Configuration bridge PDUs by the node on any port when it is the root of the spanning tree (in units of hundredths of a second). This is the actual value that the bridge is currently using.
ForwardDelay	Value (in hundredths of a second) that controls how fast a port changes its spanning state when moving towards the Forwarding state. The value determines how long the port stays in each of the Listening and Learning states, that precede the Forwarding state. The value is also used when a topology change has been detected and is underway. This ages all dynamic entries in the Forwarding database. **Note**: This value is the one that this bridge is currently using, in contrast to dot1dStpBridge ForwardDelay which is the value that this bridge and all others would start using if/when this bridge were to become the root.]
BridgeMaxAge	Value that all bridges use for the maximum age of a bridge when it is acting as the root. **Note**: 802.1D-1990 specifies that the range is related to the value of BridgeHelloTime. The granularity of this timer is specified by 802.1D-1990 to be 1 second. A badValue error may be returned if the value set is not a whole number.

Table 6 Spanning Tree tab fields (continued)

Field	Description
BridgeHelloTime	Value that the bridge uses for HelloTime when the bridge is acting as the root. The granularity of this timer is specified by 802.1D- 1990 to be one second. An agent may return a badValue error if a set is attempted to a value that is not a whole number of seconds.
TimeSinceTopologogyChange	Value that all bridges use for ForwardDelay when this bridge is acting as the root. Note: 802.1D-1990 specifies that the range for this parameter is related to the value of dot1dStpBridgeMaxAge. The granularity of this timer is specified by 802.1D-1990 to be one second. An agent may return a badValue error if a set is attempted to a value that is not a whole number of seconds.

Transparent tab

The Transparent tab contains information about a specific unicast MAC address that has forwarding information for the bridge.

To view the Transparent tab:

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

   The Bridge dialog box opens, with the Base tab displayed (Figure 10 on page 30).

2. Click the Transparent tab.

   The Transparent tab opens (Figure 12).

Figure 12 Transparent tab

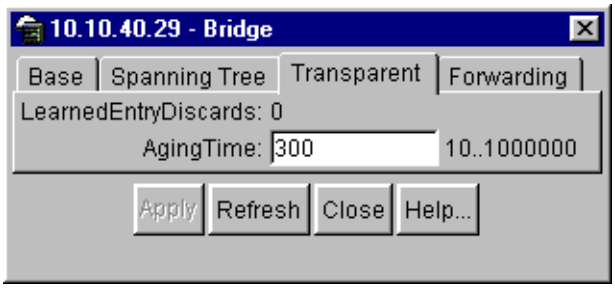


Table 7 describes the Transparent tab items.

Table 7 Transparent tab items

Item	Description
LearnedEntryDiscard	Number of Forwarding database entries learned that 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 becoming full regularly. This condition will effect the performance of the subnetwork. If the counter has a significant value and is not presently increasing, it indicates that the problem has been occurring but is not persistent.
AgingTime	Time-out period in seconds for aging out dynamically learned forwarding information. **Note**: The 802.1D-1990 specification recommends a default of 300 seconds.

Forwarding tab

The Forwarding tab displays the current state of the port, as defined by application of the Spanning Tree Protocol. This state controls what action a port takes when a frame is received. If the bridge detects a port that is malfunctioning, it places the port into the “broken” state. For ports that are disabled, the value is “disabled.”

To view the Forwarding tab:

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

The Bridge dialog box opens, with the Base tab displayed (Figure 10 on page 30).

2 Click the Forwarding tab.

The Forwarding tab opens (Figure 13).

Figure 13 Forwarding tab

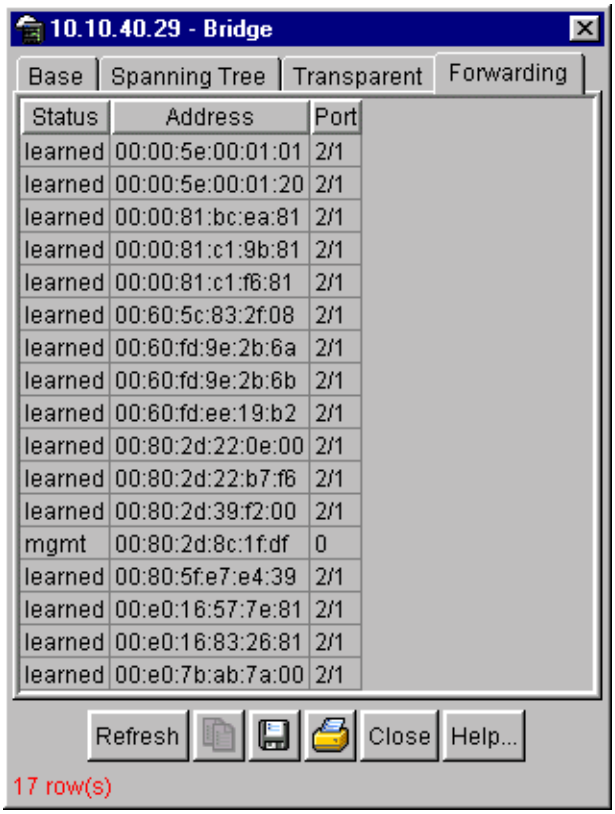


Table 8 describes the Forwarding tab fields.

Table 8 Forwarding tab fields

Field	Description
Status	The values of this fields include: • invalid: Entry is no longer valid, but has not been removed from the table. • learned: Value of the corresponding instance of dot1dTpFdbPort was learned and is being used. • self: Value of the corresponding instance of dot1dTpFdbAddress represents an address of the bridge. The corresponding instance of dot1dTpFdbPort indicates that a specific port on the bridge has this address. • mgmt(5): Value of the corresponding instance of dot1dTpFdbAddress is also the value of an existing instance of dot1dStaticAddress. • other: none of the preceding. This would include where some other MIB object (not the corresponding instance of dot1dTpFdbPort or an entry in the dot1dStaticTable) is being used to determine if a frames addressed to the value of dot1dTpFdbAddress are being forwarded.
Address	A unicast MAC address for which the bridge has forwarding or filtering information.
Port	Either the value “0” or the port number on a frame has been seen. The source address must be equal to the value of the corresponding instance of dot1dTpFdbAddress A value of “0” indicates that the port number has not been learned, so the bridge does have the forwarding/filtering information for this address (located in the dot1dStaticTable). You should assign the port value to this object whenever it is learned even for addresses for which the corresponding value of dot1dTpFdbStatus is not learned(3).

Spanning tree group (STG)

The spanning tree group (STG) information is stored in the STG dialog box. Each row in each tab specifies a different STG in the device.

Configuration tab

The Configuration tab in the STG dialog box has general information for the STG.

To view the Configuration tab:

➔ From the Device Manager menu bar, choose VLANs > STG.

The STG dialog box opens, with the Configuration tab displayed (Figure 14).

Figure 14 Configuration tab

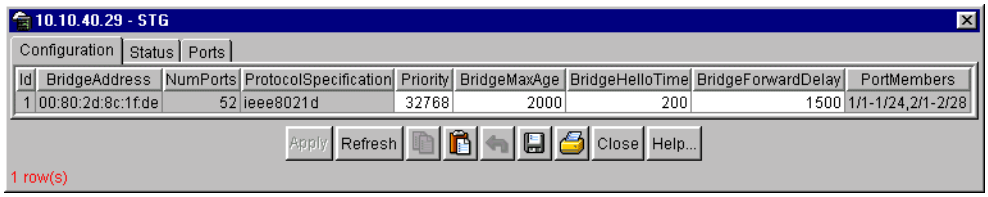


Table 9 describes the Configuration tab fields.

Table 9 Configuration tab fields

Item	Description
ID	An identifier used to identify a STG in the device.
BridgeAddress	MAC address used by a bridge when it is referred to in a unique fashion. Nortel Network recommends that the number be the smallest MAC address of all ports belonging to the bridge. However, it is only required to be unique. When concatenated with Priority, a unique bridge identifier is formed that is used in the Spanning Tree Protocol.
NumPorts	Number of ports controlled by this bridging entity.
ProtocolSpecification	Version of the spanning tree protocol being run. Values include: • decLb100: Indicates the DEC LANbridge 100 Spanning Tree Protocol. • ieee8021d: IEEE 802.1d implementations will return this entry. When future versions of the IEEE Spanning Tree Protocol are released that are incompatible with the current version, a new value will be defined.
Priority	Value of the writable portion of the bridge ID. That is, the first two octets of the (8-octet long) bridge ID. The last six octets of the bridge ID are given by the value of BridgeAddress.

Table 9 Configuration tab fields (continued)

Item	Description
BridgeMaxAge	Value that all bridges use for the maximum age of a bridge when it is acting as the root. **Note**: 802.1D-1990 specifies that the range is related to the value of BridgeHelloTime. The granularity of this timer is specified by 802.1D-1990 to be 1 second. A badValue error may be returned if the value set is not a whole number.
BridgeHelloTime	Value that all bridges use for HelloTime when a bridge is acting as the root. **Note**: The granularity of this timer is specified by 802.1D-1990 to be 1 second. A badValue error may be returned if the value set is not a whole number.
BridgeForwardDelay	Value that all bridges use for ForwardDelay when this bridge is acting as the root. **Note**: 802.1D-1990 specifies that the range is related to the value of BridgeHelloTime. The granularity of this timer is specified by 802.1D-1990 to be 1 second. A badValue error may be returned if the value set is not a whole number.
PortMembers	Bit-field used to identify the ports in the system that are members this STG. The bit-field is 32 octets long representing ports 0 to 255 (inclusive).

Status tab

The Status tab in the STG dialog box has status information for the STG.

To view the Status tab:

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

   The STG dialog box opens, with the Configuration tab displayed (Figure 14 on page 37).

2. Click the Status tab.

   The Status tab opens (Figure 15).

Figure 15 Status tab

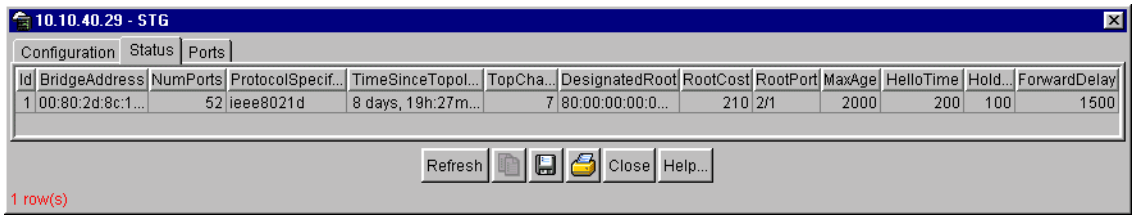


Table 10 describes the Status tab fields.

Table 10 Status tab fields

Field	Description
ID	An identifier used to identify a STG in the device.
BridgeAddress	MAC address used by a bridge when it is referred to in a unique fashion. Nortel Networks recommends that the number be the smallest MAC address of all ports belonging to the bridge. However, it is only required to be unique. When concatenated with Priority, a unique bridge identifier is formed that is used in the Spanning Tree Protocol.
NumPorts	Number of ports controlled by this bridging entity.
ProtocolSpecification	Version of the Spanning Tree Protocol being run. Values include: • decLb100: Indicates the DEC LANbridge 100 spanning tree protocol. • ieee8021d: IEEE 802.1d implementations will return this entry. When future versions of the IEEE spanning tree protocol are released that are incompatible with the current version, a new value will be defined.
TimeSinceTopologyChange	Time (in hundredths of seconds) since the last topology change was detected by the bridge entity.
TopChange	Number of topology changes detected by the bridge since the management entity was last reset or initialized.
DesignatedRoot	Bridge identifier of the root of the spanning tree as determined by the Spanning Tree Protocol. The value is used as the root identifier parameter in all configuration bridge PDUs originated by this node.
RootCost	Cost of the path to the root as seen from the bridge.
RootPort	Port that has the lowest cost path from the bridge to the root bridge.

Table 10 Status tab fields (continued)

Field	Description
MaxAge	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	Amount of time between the transmission of configuration bridge PDUs by this node on any port when it is the root of the spanning tree (in hundredths of a seconds). This is the actual value that this bridge is currently using.
HoldTime	Value of the interval length during which no more than two configuration bridge PDUs shall be transmitted by this node (in hundredths of a second).
ForwardDelay	This time value (in hundredths of a seconds) that controls how fast a port changes its spanning state when moving towards the forwarding state. Value determines how long the port stays in each of the listening and learning states, which precede the forwarding state. This is also used when a topology change has been detected and is underway, to age all dynamic entries in the forwarding database. **Note**: This value is the one that this bridge is currently using, in contrast to BridgeForwardDelay which is the value that this bridge and all others would start using if/when this bridge were to become the root.

Ports tab

The Ports tab in the STG dialog box has port information for the STG.

To view the Ports tab:

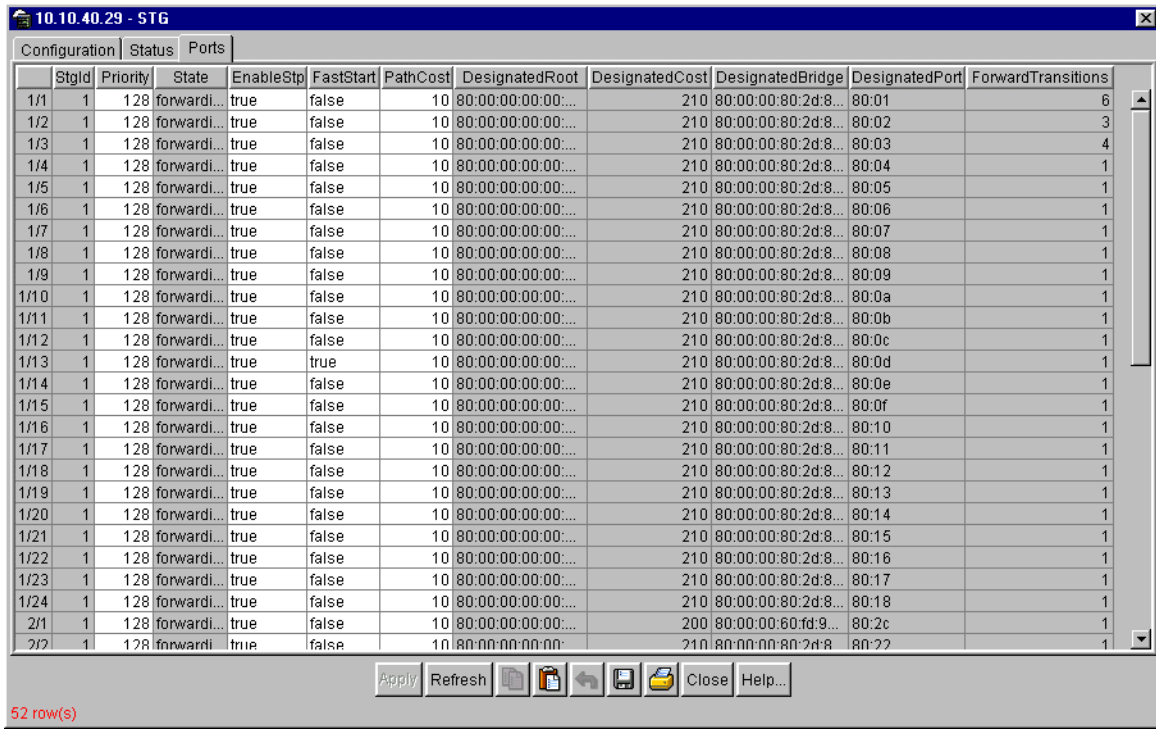
1. From the Device Manager menu bar, choose VLANs > STG.

   The STG dialog box opens, with the Configuration tab displayed (Figure 14 on page 37).

2. Click the Ports tab.

   The Ports tab opens (Figure 16).

Figure 16 Ports tab



	StgId	Priority	State	EnableStp	FastStart	PathCost	DesignatedRoot	DesignatedCost	DesignatedBridge	DesignatedPort	ForwardTransitions
1/1	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:01	6
1/2	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:02	3
1/3	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:03	4
1/4	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:04	1
1/5	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:05	1
1/6	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:06	1
1/7	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:07	1
1/8	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:08	1
1/9	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:09	1
1/10	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:0a	1
1/11	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:0b	1
1/12	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:0c	1
1/13	1	128	forwardi...	true	true	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:0d	1
1/14	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:0e	1
1/15	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:0f	1
1/16	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:10	1
1/17	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:11	1
1/18	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:12	1
1/19	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:13	1
1/20	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:14	1
1/21	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:15	1
1/22	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:16	1
1/23	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:17	1
1/24	1	128	forwardi...	true	false	10	80:00:00:00:00:...	210	80:00:00:80:2d:8...	80:18	1
2/1	1	128	forwardi...	true	false	10	80:00:00:00:00:...	200	80:00:00:60:fd:9...	80:2c	1
2/2	1	128	forwardi	true	false	10	80:00:00:00:00:00:	210	80:00:00:80:2d:8	80:22	1

Table 11 describes the Ports tab fields.

Table 11 Ports tab fields

Field	Description
StgId	STG identifier assigned to this port.
Priority	Value of the priority field contained in the first octet of the port ID. The other octet is given by the value of the “rcStgPort.”
State	The current state of the port as defined by application of the Spanning Tree Protocol. These are the instructions the port takes on a frame when it is received. If the bridge detects a port is malfunctioning, it will list it as “broken(6).” For ports that are disabled, the value is “disabled(1).”
EnableStp	Enables (True) or disables (False) the spanning tree of the port.
FastStart	When this is enabled (True), the port is move to forwarding or blocking state in 4 seconds.

Table 11 Ports tab fields (continued)

Field	Description
PathCost	Contribution of the port to the pathcost of paths towards the spanning tree root, including the current port. 802.1D-1990 specifications recommends that the default of this parameter be in inverse proportion to the speed of the attached LAN.
DesignatedRoot	The unique “Bridge Identifier.” This is recorded as Root in the configuration bridge PDUs transmitted by the Designated Bridge for the segment to that the port is attached.
DesignatedCost	Path cost of the Designated Port of the segment connected to the port. The value is compared to the Root Path Cost field in received bridge PDUs.
DesignatedBridge	Bridge identifier of the bridge that this port considers to be the Designated Bridge for this port's segment.
DesignatedPort	Port identifier of the port on the Designated Bridge for this port's segment.
ForwardTransitions	Number of times this port has transitioned from the learning state to the forwarding state.