

Part No. 311208-A Rev 00
September 2000

4401 Great America Parkway
Santa Clara, CA 95054

Configuring Business Policy Switches with Optivity Quick2Config 2.2

NORTEL
NETWORKS™

Copyright © 2000 Nortel Networks

All rights reserved. September 2000.

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 NA Inc.

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license. The software license agreement is included in this document.

Trademarks

NORTEL NETWORKS is a trademark of Nortel Networks.

Optivity is a registered trademark and BayStack, Business Policy Switch, and Quick2Config are trademarks of Nortel Networks.

Microsoft and Windows NT are registered trademarks of Microsoft Corporation.

All other trademarks and registered trademarks are the property of their respective owners.

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 NA Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks NA 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 NA Inc. Optivity® network management software license agreement

NOTICE: Please carefully read this license agreement before copying or using the accompanying Optivity network management software or installing the hardware unit with pre-enabled Optivity network management software (each of which is referred to as “Software” in this Agreement). BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH NORTEL NETWORKS WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

1. License grant. Nortel Networks NA Inc. (“Nortel Networks”) grants the end user of the Software (“Licensee”) a personal, nonexclusive license: a) to use the Software either on a single computer or, if applicable, on a single authorized device identified by host ID; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the associated user manual solely in support of authorized use of the Software by Licensee. This license applies to the Software only and does not extend to Nortel Networks Agent software or other Nortel Networks software products. Nortel Networks Agent software or other Nortel Networks software products are licensed for use under the terms of the applicable Nortel Networks NA Inc. Software License Agreement that accompanies such software and upon payment by the end user of the applicable license fees for such software.

2. Restrictions on use; reservation of rights. The Software and user manuals are protected under copyright laws. Nortel Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Nortel Networks or its licensors. The copyright notice must be reproduced and included with any copy of any portion of the Software or user manuals. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from the Software or user manuals or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or user manuals, in whole or in part. The Software and user manuals embody Nortel Networks’ and its licensors’ confidential and proprietary intellectual property. Licensee shall not disclose to any third party the Software, or any information about the operation, design, performance, or implementation of the Software and user manuals that is confidential to Nortel Networks and its licensors; however, Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee’s facility, provided they have agreed to use the Software only in accordance with the terms of this license.

3. Limited warranty. Nortel Networks warrants each item of Software, as delivered by Nortel Networks and properly installed and operated on Nortel Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Nortel Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Nortel Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date the Software is first shipped to Licensee. Nortel Networks will replace defective media at no charge if it is returned to Nortel Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee’s intended results and for the installation, use, and results obtained from the Software. Nortel Networks does not warrant a) that the functions contained in the software will meet the Licensee’s requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Nortel Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Nortel Networks or in accordance with its instructions; (ii) used in conjunction with another vendor’s product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS

ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

4. Limitation of liability. IN NO EVENT WILL NORTEL NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF NORTEL NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO NORTEL NETWORKS FOR THE SOFTWARE LICENSE.

5. Government licensees. This provision applies to all Software and documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights, and use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR 52.227-19 and the limitations set out in this license for civilian agencies, and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, for agencies of the Department of Defense or their successors, whichever is applicable.

6. Use of software in the European Community. This provision applies to all Software acquired for use within the European Community. If Licensee uses the Software within a country in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. Licensee agrees to notify Nortel Networks of any such intended examination of the Software and may procure support and assistance from Nortel Networks.

7. Term and termination. This license is effective until terminated; however, all of the restrictions with respect to Nortel Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Nortel Networks copyright; those restrictions relating to use and disclosure of Nortel Networks' confidential information shall continue in effect. Licensee may terminate this license at any time. The license will automatically terminate if Licensee fails to comply with any of the terms and conditions of the license. Upon termination for any reason, Licensee will immediately destroy or return to Nortel Networks the Software, user manuals, and all copies. Nortel Networks is not liable to Licensee for damages in any form solely by reason of the termination of this license.

8. Export and re-export. Licensee agrees not to export, directly or indirectly, the Software or related technical data or information without first obtaining any required export licenses or other governmental approvals. Without limiting the foregoing, Licensee, on behalf of itself and its subsidiaries and affiliates, agrees that it will not, without first obtaining all export licenses and approvals required by the U.S. Government: (i) export, re-export, transfer, or divert any such Software or technical data, or any direct product thereof, to any country to which such exports or re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries; or (ii) provide the Software or related technical data or information to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.

9. General. If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the state of California.

Should you have any questions concerning this Agreement, contact Nortel Networks, 4401 Great America Parkway, P.O. Box 58185, Santa Clara, California 95054-8185.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT

THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN NORTEL NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST NORTEL NETWORKS UNLESS NORTEL NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Contents

Preface	15
Before you begin	15
Text conventions	15
Acronyms	16
Related publications	17
Hard-copy technical manuals	19
How to get help	19
 Chapter 1	
Configuring switches	21
Prerequisites	22
Importing configurations	22
Creating switch configurations	23
Adding or changing system information	24
Configuring basic properties	25
Configuring Ethernet ports	26
Configuring ATM MDA ports (BayStack 450 only)	27
Configuring LEC failover	29
Configuring IP	30
Configuring SNMP	31
Exporting configurations	32
 Chapter 2	
Configuring VLANs	35
About VLAN services	35
VLAN types	36
802.1Q frame tagging	37
VLAN learning modes	37

Creating VLANs	38
Configuring a port-based VLAN	39
Configuring a protocol-based VLAN	40
Configuring a MAC SA-based VLAN	41
Configuring VLAN ports	43
 Chapter 3	
Configuring IGMP snooping	45
About IP multicast and IGMP	45
IGMP host membership reports	46
IGMP snooping	46
Proxy reports	47
IGMP snooping configuration rules	47
Enabling IGMP snooping	47
Creating static router ports	49
 Chapter 4	
Configuring multilink trunks	51
About multilink trunking	51
MLT configuration guidelines	52
Creating an MLT group	53
 Chapter 5	
Configuring spanning tree	55
About the Spanning Tree Protocol	55
Configuring STP ports	55
Changing the STP learning state	56
Disabling STP port participation	57
Viewing and configuring STP group properties	58
 Chapter 6	
Configuring QoS filters	61
About QoS policy filters	61
DiffServ architecture	62
DiffServ codepoints	63

Configuration summary	63
Dynamic DiffServ management	64
Static DiffServ management	64
Configuring dynamic QoS management	65
Configuring COPS connections	67
Configuring COPS retry settings	68
Configuring policies locally	69
Configuring classifications and filter groups	69
Configuring IP filter classifications	70
Configuring Layer 2 classifications	71
Configuring IP and Layer 2 filter groups	74
Configuring filter actions	75
Configuring policies	76
Configuring QoS interfaces	78
Predefined role combinations	78
Creating new role combinations	79
Assigning ports to QoS roles	81
User priority and DSCP mapping	82
Configuring priority mapping	82
Viewing DSCP mapping	83
Viewing transmit queue information	84
Viewing the Interface Queue table	85
Viewing user priority assignments	86
Viewing DSCP assignments	87
Resetting QoS values in Quick2Config	88
 Appendix A	
Downloading image files	91
 Index	93

Figures

Figure 1	Stack and Switch Palette templates	23
Figure 2	Basic tab system properties	25
Figure 3	Basic port properties	26
Figure 4	ATM MDA ports	28
Figure 5	ATM port properties	28
Figure 6	IP properties	30
Figure 7	SNMP properties	31
Figure 8	Port-based VLAN	39
Figure 9	Protocol-based VLAN properties	40
Figure 10	MAC-based VLAN properties	42
Figure 11	Port VLAN tab	44
Figure 12	IGMP properties	48
Figure 13	Port IGMP tab	49
Figure 14	MLT properties	53
Figure 15	STP port properties	56
Figure 16	Spanning Tree Protocol Group tab	58
Figure 17	QoS policy agent Basic properties	65
Figure 18	COPS Configuration table	67
Figure 19	COPS Retry Setting tab	68
Figure 20	QoS IP Filter table	70
Figure 21	QoS 802 Filter table	72
Figure 22	QoS IP Filter Group table	74
Figure 23	QoS Action table	75
Figure 24	QoS Policy table	77
Figure 25	QoS Role Combination properties	79
Figure 26	Ports assigned to a role combination	81
Figure 27	QoS Priority Mapping table	83
Figure 28	QoS DSCP Mapping table	84
Figure 29	QoS Interface Queue table	85

12 Figures

Figure 30	QoS Priority Queue Assignment table	87
Figure 31	QoS DSCP Assignment table	88
Figure 32	QoS Advanced tab	89
Figure 33	Image Download Wizard	92

Tables

Table 1	VLAN types	36
Table 2	STP port read-only properties	57
Table 3	Spanning Tree Protocol Group properties	58
Table 4	QoS policy agent properties	66
Table 5	COPS Configuration table properties	67
Table 6	COPS Retry Setting properties	69
Table 7	QoS IP Filter table properties	70
Table 8	QoS 802 Filter properties	72
Table 9	QoS IP and 802 Filter Group table properties	74
Table 10	QoS Action table properties	75
Table 11	QoS Policy table properties	77
Table 12	QoS role combination properties	79
Table 13	Priority mapping for Nortel Networks IP service classes	82
Table 14	QoS Interface Queue table properties	85

Preface

Optivity Quick2Config™ is a graphical network configuration application you can use to configure the Business Policy Switch™ 2000 and switches in the BayStack™ 450 product group (BayStack 450, 410, and 350 switches).

Before you begin

This guide is intended for network managers using a Microsoft® Windows NT® or UNIX-based management station. Prior knowledge of Optivity Quick2Config 2.2 is not required. This guide assumes that you have the following background:

- Working knowledge of the operating system and network management platform (for example, Windows NT or Sun Domain Manager) on the system with which you are using a Quick2Config client or server
- Understanding of the transmission and management protocols used on your network, and of your Business Policy Switch 2000 or BayStack devices.
- Experience with windowing systems or graphical user interfaces (GUIs)

Text conventions

This guide uses the following text conventions:

italic text

Indicates new terms and book titles.

separator (>)

Shows menu paths.

Example: Protocols > IP identifies the IP option on the Protocols menu.

Acronyms

This guide uses the following acronyms:

BPDU	Bridge Protocol Data Unit
COPS	Common Open Policy Services
CoS	class of service
DS	Differentiated Services (DiffServ)
DSCP	DiffServ codepoint
ELAN	emulated LAN
GUI	graphical user interface
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Gateway Management Protocol
IP	Internet Protocol
LAN	local area network
IVL	independent VLAN learning
LANE	LAN emulation
LDAP	Lightweight Directory Access Protocol
LEC	LAN emulation client
LES	LAN emulation server
MAC	media access control
MDA	media-dependent adapter
MLT	multilink trunk
MIB	management information base
NVRAM	non-volatile random access memory
PID	protocol identifier
PVID	port VLAN identifier
SVL	shared VLAN learning
ToS	type of service

QoS	Quality of Service
SNMP	Simple Network Management Protocol
STG	Spanning Tree Group
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
VLAN	virtual local area network

Related publications

For more information about Optivity Quick2Config 2.2, Business Policy Switch 2000 and BayStack devices, and Optivity Policy Server software, see the following publications.

Optivity Quick2Config

- *Release Notes for Optivity Quick2Config for Business Policy Switch 2000* (part number 310621-A Rev 00)

Lists new features in the release, bugs fixed, and last-minute information that is not included in the Optivity Quick2Config guides.

- *Installing and Administering Optivity Quick2Config 2.2* (part number 207809-B Rev 00)

Intended for Quick2Config administrators, this guide describes how to install the Quick2Config server and client software and how to administer the server.

- *Using the Optivity Quick2Config 2.2 Client Software* (part number 207810-B Rev 00)

This guide describes how to use the Quick2Config client software to configure and maintain networks with Business Policy Switch 2000 and BayStack devices.

Optivity Policy Server

- *Optivity Policy Services for the Business Policy Switch* (part number 303969-D Rev 00)

This guide describes how to set up and use Optivity Policy Services (OPS) and provides overview information on policy-related protocols.

Business Policy Switch 2000

- *Using the Business Policy Switch 2000* (part number 208700-A)
This guide describes how to use the Business Policy Switch 2000.
- *Using Web-Based Management for the Business Policy Switch 2000* (part number 209570-A)

This guide provides configuration settings and information using the Business Policy Switch Web-based management software.

BayStack 450 product group

- *Using the BayStack 450 10/100/1000 Series Switch* (part number 309978-A Rev 00)
This guide provides instructions for using the BayStack 450 products.
- *Reference for the BayStack 350/410/450 Management Software Operations* (part number 304935-B)

This guide describes the Nortel Networks™ Device Manager software that you use to configure and manage the BayStack 350/410/450 switches.

Hard-copy technical manuals

You can print selected technical manuals and release notes free, directly from the Internet. Go to the support.baynetworks.com/library/tpubs/ 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 www.adobe.com to download a free copy of Acrobat Reader.

You can purchase selected documentation sets, CDs, and technical publications through the Internet at the www1.fatbrain.com/documentation/nortel/ URL.

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
EMEA	(33) (4) 92-966-968
North America	(800) 2LANWAN or (800) 252-6926
Asia Pacific	(61) (2) 9927-8800
China	(800) 810-5000

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 www12.nortelnetworks.com/ URL and click ERC at the bottom of the page.

Chapter 1

Configuring switches

You can use Optivity Quick2Config 2.2 to view and modify configuration data for Nortel Networks Business Policy Switch 2000 and BayStack 450, 410, and 350 Series switches.

Read this chapter for information about how to start working with configuration data, and instructions for setting or changing the properties of default switch configuration objects.

- [“Prerequisites” on page 22](#)
- [“Importing configurations” on page 22](#)
- [“Creating switch configurations” on page 23](#)
- [“Adding or changing system information” on page 24](#)
- [“Exporting configurations” on page 32](#)

Prerequisites

Before you can use Optivity Quick2Config 2.2 to configure a Business Policy Switch 2000 or BayStack switch, the switch must be:

- Accessible to the Optivity configuration server through an established Simple Network Management Protocol (SNMP) connection.

For the initial setup of a switch, you configure an IP address, subnet mask, and gateway address for the switch or stack. For a standalone switch, you enter the in-band IP address. For a stack configuration, you enter the stack IP address. For detailed information about setting up the initial network connection, see the documentation that came with your switch.



Note: The default management virtual LAN (VLAN) is *VLAN 1*.

- Visible in the Quick2Config Configuration Data folder.

You can import existing configurations to the Quick2Config database, or you can create configurations off-line. For information about importing existing configuration data, see [“Importing configurations,”](#) next. For information about adding configuration data manually, see [“Creating switch configurations” on page 23](#).

Importing configurations

You can import existing configuration data from the Business Policy Switch 2000 and BayStack 450 devices in your network to the Quick2Config database.

Business Policy Switch 2000 devices use SNMP to transfer configuration data; they do not support Trivial File Transfer Protocol (TFTP).



Note: Although the Import > From TFTP option on the Quick2Config File menu is not disabled, this option does not work for Business Policy Switch 2000 and BayStack switches.

For import procedures, see *Using the Optivity Quick2Config 2.2 Client Software*.

Before you attempt to import data from a switch, make sure that the switch SNMP agent is available, and that you can supply the device IP address and community string.

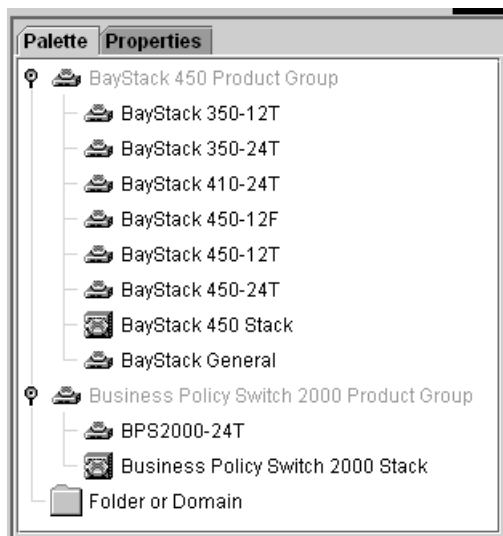
Quick2Config initially determines system information from the switch. After you import a configuration to the Quick2Config database, you do not have to modify any system data unless you want to change something in the existing configuration.

Creating switch configurations

You can use the Configuration Data Palette to create new standalone switch and stack configurations.

The Palette lists templates by product group ([Figure 1](#)).

Figure 1 Stack and Switch Palette templates



Note: To learn how to use Quick2Config to add switch configuration data, see *Using the Optivity Quick2Config 2.2 Client Software*.

When you create standalone and stack templates, Quick2Config creates default IP, MLT, SNMP, STP, and QoS (Business Policy Switch 2000 only) configuration objects in the navigation pane tree. Standalone switches also automatically include configuration objects for switch ports and a default port-based VLAN.



Note: You cannot delete these default configuration objects, or create them from the Palette.

To match the actual configuration of the device you are creating, you can use the Palette to add the following configuration objects to a standalone or stack system:

- 1 to 8 stack units (each includes switch ports and a default, port-based VLAN)
- Media-dependent adapter (MDA) hardware
- VLANs
- Internet Gateway Management Protocol (IGMP)

Adding or changing system information

This section describes how to use Quick2Config to initially configure a switch that you created from the Configuration Data Palette, or to modify the imported system information for a managed switch.



Note: In most cases, you do not have to modify the system information in an imported configuration.

You can configure several system properties:

- To set or change the system name, contact, or location information, see [“Configuring basic properties,”](#) next.
- To enable or disable Ethernet switch and MDA ports, or to configure Ethernet line speed, see [“Configuring Ethernet ports” on page 26.](#)
- To enable or disable ATM switch and MDA ports on a BayStack switch, or to configure the port ATM properties, see [“Configuring ATM MDA ports \(BayStack 450 only\)” on page 27.](#)

- To set or change the switch IP address or subnet mask, see [“Configuring IP” on page 30](#).
- To supply the required SNMP community strings or to enable SNMP traps, see [“Configuring SNMP” on page 31](#).

Configuring basic properties

When you import a switch, some general system information is added to the database. You can view or configure the system name, contact, and location strings for a switch.

To modify the basic system properties for a switch:

- 1 In the navigation pane, select the switch.
- 2 In the context-sensitive pane, click the Properties tab.
- 3 Click the Basic tab ([Figure 2](#)).

Figure 2 Basic tab system properties

Property	Value
System Contact	M. Jordan
System Location	Chicago
System Name	Loop1
System Up Time	0 hours, 10 minutes, 2 seconds.
Hardware Version	ab
Firmware Version	V0.34
Software Version	v1.0.0.79

- 4 In the System Contact, System Location, and System Name fields, enter ASCII strings to identify the switch.

Each string can be up to 56 characters.

Quick2Config queries the system management information base (MIB) to report the hardware, firmware, and software versions running on the switch, and the length of time since the last reset. You cannot edit these fields.

Configuring Ethernet ports

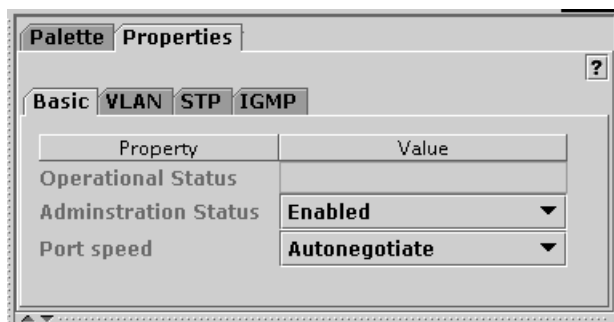
You can use Quick2Config to enable or disable switch and MDA ports, and to set the port speed for an Ethernet port.

To set basic Ethernet port properties:

- 1 In the navigation pane, open the switch or Ethernet MDA and select a port. To assign the same properties to a group of ports on the same switch, select multiple ports in the navigation pane.

The port Basic tab opens in the context-sensitive pane ([Figure 3](#)).

Figure 3 Basic port properties



The Operational Status field indicates the current link state of the port, as follows:

- Up indicates that the port is connected and operational.
- Down indicates that the port is not connected or is not operational.

The field is blank when you are working offline to create a new configuration.

- 2 From the Administration Status list, choose Enabled or Disabled to force the link up or down.
- 3 From the Port speed list, choose the Ethernet line speed and duplex mode combinations for the selected port; or, choose Autonegotiate to configure the port to match the best service provided by the connected station, up to 100 Mb/s Full Duplex.

Valid options depend on the MDA hardware. Fiber optic links do not use autonegotiation.

Full duplex operation is intended for directly connected links, such as between two switches or between a switch and an end station. Half duplex operation, where transmission occurs in one direction at a time, is usually the best choice for shared links that require access control and collision detection.

Note the following:

- You can set gigabit MDA ports to Autonegotiate or 1000 Mb/s Full Duplex only.
- Business Policy Switch 2000 fiber optic ports support only 100 Mb/s Full Duplex.
- BayStack 450 fiber optic ports support 100 Mb/s Half Duplex or 100 Mb/s Full Duplex.

You can also set the following additional properties at the port level:

- VLAN port properties — see [“Configuring VLAN ports” on page 42](#)
- Spanning tree protocol (STP) port properties — see [“Configuring spanning tree” on page 55](#)
- Internet Group Management Protocol (IGMP) static router port property — see [“Creating static router ports” on page 49](#)

Configuring ATM MDA ports (BayStack 450 only)

On BayStack 450 switches running agent version 3.1 or later, you can use Quick2Config to configure the ATM ports on 2M3 and 2S3 MDA modules to participate in an emulated LAN (ELAN).

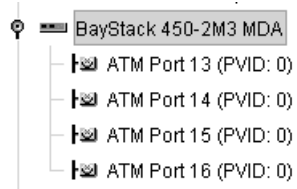
Using ATM Forum LAN emulation (LANE), the BayStack 450 switch can communicate transparently with ATM servers and other LAN clients. As LAN emulation clients (LECs), the MDA ports perform data forwarding, address resolution, and ATM control functions. A LAN Emulation server (LES) in the network provides MAC-to-ATM address translation for the LECs.

This section describes how to use the Basic properties tab to enable or disable ATM ports, set the port speed, enable or disable the LEC software, and to configure LEC failover.

To view or set basic ATM port properties:

- 1 In the navigation pane, open the MDA and select a port ([Figure 4](#)).

Figure 4 ATM MDA ports



To assign the same properties to a group of ports, select multiple ports in the navigation pane.

The port Basic tab opens in the context-sensitive pane ([Figure 5](#)).

Figure 5 ATM port properties

A screenshot of the 'ATM port properties' configuration window. The window has three tabs: 'Basic', 'VLAN', and 'STP'. The 'Basic' tab is selected. Below the tabs is a table with two columns: 'Property' and 'Value'.

Property	Value
Operational Status	Down
Administration Status	Enabled ▼
Port speed	Autonegotiate ▼
ELAN Name	
LEC State	Not Active
LEC Status	Disabled ▼
Desired Physical Port	A1 ▼
Actual Physical Port	A1 ▼
LEC Fail Over	Disabled ▼

The Operational Status property indicates the current link state of the port, as follows:

- Up indicates that the port is connected and operational.
- Down indicates that the port is not connected or is not operational.

The LEC State field indicates whether the LAN emulation client is currently active.

- 2 From the Administration Status list, choose Enabled.
- 3 From the Port speed list, choose a line speed and duplex mode for the selected port, or choose Autonegotiate to match the best service available.
- 4 In the ELAN Name field, type the name of the ELAN.
- 5 To configure LEC Failover, see [“Configuring LEC failover,”](#) next.

You can also set VLAN and STP properties for each ATM port. For information, see:

- [“Configuring VLAN ports” on page 42](#)
- [“Configuring spanning tree” on page 55](#)

Configuring LEC failover

LEC Failover allows ELAN traffic to move from a failing port to another available port. A unique ATM address identifies each LEC, which the LANE protocol associates with one or more port MAC addresses, or *LEC instances*.

To configure LEC failover:

- 1 From the LEC Status list, choose Disabled.
You must disable the LEC before you can modify the failover properties.
- 2 From the Actual Physical Port list, choose A1 or A2 to identify the port that is currently carrying traffic.
- 3 From the Desired Physical Port list, choose the alternate port to use in a failover.
For example, if the Actual Physical Port is A1, choose A2.
- 4 From the LEC Fail Over list, choose Enabled.

Configuring IP

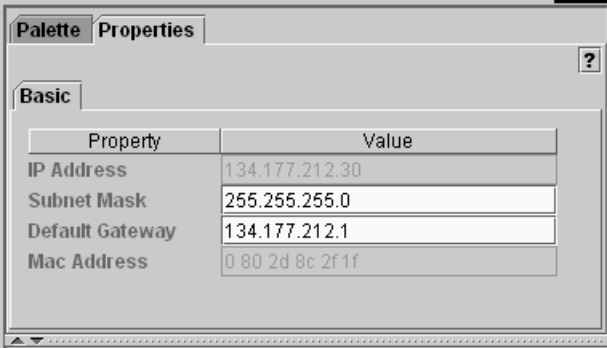
You can use Quick2Config to configure the subnet mask and default gateway for a switch, and to view the switch MAC and IP addresses. The static or standalone IP and MAC addresses are imported from the device and are read-only.

To set IP properties:

- 1 In the navigation pane, open the switch object and select IP.

The IP Basic tab opens in the context-sensitive pane ([Figure 6](#)).

Figure 6 IP properties



The screenshot shows a software interface with a 'Properties' tab selected. Under the 'Basic' sub-tab, there is a table with the following data:

Property	Value
IP Address	134.177.212.30
Subnet Mask	255.255.255.0
Default Gateway	134.177.212.1
Mac Address	0 80 2d 8c 2f 1f

- 2 Type the subnet mask for the IP address.

Network routers use the subnet mask to determine the network or subnet address portion of a host's IP address. The bits in the IP address that contain the network address (including the subnet) are set to 1 in the address mask, and the bits that contain the host identifier are set to 0.

- 3 Type the IP address of the default gateway host.

Configuring SNMP

You can use Quick2Config to supply the required SNMP community strings for a switch, and to enable SNMP traps.

Traps are SNMP management information packets generated by devices on the network. You can configure 1 to 4 management stations as trap receivers, to receive all SNMP trap messages from the selected switch.

To set the SNMP properties for a switch:

- 1 In the navigation pane, open the switch and select the SNMP object.

The SNMP Basic tab opens in the context-sensitive pane ([Figure 7](#)).

Figure 7 SNMP properties

Property	Value
Read Only Community String	public
Read-Write Community String	public

Trap Receivers	IP Address	Community String
+		

Property	Value
Authentication Trap	Enabled ▼

- 2 For in-band SNMP operations, type the ASCII string of the read/write and read-only community strings that are currently set for the switch.



Note: You must specify the correct community strings in order to communicate with the switch. You cannot use Quick2Config to change a community string.

- 3 To configure SNMP trap receivers for the switch, enter the IP address and community string for one to four trap receivers in the Trap Receivers table.
 - a To add a new trap receiver to the table, click the green plus sign (+).
 - b Type the IP address and community string of each trap receiver you want to specify.
- 4 If you want the switch to send a trap when there is an SNMP authentication failure, enable the Authentication Trap property.

Exporting configurations

Business Policy Switch 2000 devices use SNMP to transfer configuration data; they do not support TFTP. For export procedures, see *Using the Quick2Config 2.2 Client Software*.



Note: Although the Export > From TFTP option on the Quick2Config File menu is not disabled, this option does not work for Business Policy Switch 2000 and BayStack switches.

When you export a configuration, Quick2Config sends SNMP set requests to the switch, updating the switch properties that you modified. Before exporting configuration data, Quick2Config verifies that the following information in the exported configuration data matches the information on the target switch:

- Device IP address
- Community string
- Model number and type of switch
- Units in a stack
- MDA hardware

Quick2Config also validates the following VLAN configuration data:

- Port VLAN identifier (PVID) values — Each PVID must match a VLAN ID configured on the same device.
- VLAN names — The VLAN name property must not be empty, duplicated, or more than 16 characters.

If one of the verifications fails, the export process stops immediately and displays an error message.

Chapter 2

Configuring VLANs

You use virtual local area networks (VLANs) to create scalable broadcast domains in your network.

Read the sections of this chapter to learn how to use Optivity Quick2Config 2.2 to configure Business Policy Switch 2000 and BayStack devices in one or more VLAN:

- [“About VLAN services,”](#) next
- [“Creating VLANs”](#) on page 38

About VLAN services

When you add a Business Policy Switch 2000 or BayStack device to the Configuration Data folder, Quick2Config automatically creates a default port-based VLAN (VLAN ID 1) that is configured with all ports on the device.

On each switch, you can modify the default VLAN, and create as many as 63 additional VLANs.

This section includes the following topics about VLAN services on Business Policy Switch 2000 devices:

- [“VLAN types”](#) on page 36
- [“802.1Q frame tagging”](#) on page 37
- [“VLAN learning modes”](#) on page 37

VLAN types

The criteria used to determine membership in a VLAN determines the VLAN type. [Table 1](#) describes the types of VLAN you can build with Quick2Config. All VLANs are defined by IEEE 802.1d. Business Policy Switch 2000 devices support all three types. The BayStack 450 product family supports port-based and protocol-based VLANs.

Table 1 VLAN types

Type	Membership based on	IEEE 802.1d standard	Advantages/disadvantages
Port	Destination MAC address (switch port address)	Layer 1 ¹	Forwards packets within a single network, but requires routers to forward the packets between port VLANs and to other networks. Can be added easily to an existing network topology. The main disadvantage is that if the ports used by VLAN members change, reconfiguration is required.
MAC ²	Source MAC address (network adapter address)	Layer 2	Use to enforce a MAC-level security scheme that differentiates groups of users. Configured devices may be freely relocated without having to reconfigure them. The main disadvantage is that this type is difficult to set up in large existing networks.
Protocol	Protocol header	Layer 2	You can configure a single port in multiple protocol-based VLANs; one for each protocol type. A good choice in heterogeneous networks where the devices to be added to VLANs are already segmented by protocol. The main disadvantage is that this type restricts VLAN membership.

¹ If they are in the same bridge group on a single device, ports in the same VLAN can communicate using IEEE 802.1Q level 2 switching.

² The switch supports up to 48 MAC-based VLANs.

In a typical network, a switched port that belongs to one or more protocol-based VLANs also belongs to a port-based VLAN. The protocol-based VLAN defines the broadcast domain for packets that can be classified by protocol type. The port-based VLAN defines the broadcast domain for all other types of packets.

802.1Q frame tagging

Business Policy Switch 2000 devices operate in accordance with the IEEE 802.1Q tagging rules. The 802.1Q specification defines a method to coordinate VLANs across multiple switches. A tagged port inserts an additional 4-octet header (*tag*) in each frame, after the source MAC address and before the frame type.

The switches that route VLAN frames are VLAN-aware, whereas devices that receive the frames (user workstations and printers, for example) may be VLAN-unaware. This distinction is the basis for the two types of VLAN connections:

- *Trunk links* (or *tagged links*) connect VLAN devices that are VLAN-aware (the switches that perform routing, for example). A frame transmitted across a trunk link is *explicitly* tagged with a 802.1Q VLAN header tag. The routing device gets the destination of a tagged VLAN frame by consulting a filtering database. You can configure VLAN trunk links to filter tagged frames, untagged frames, or both.
- *Access links* (or *untagged links*) connect a VLAN-aware device to a VLAN-unaware device. Frames transmitted across an access link do not include VLAN headers. By default, all ports are configured as access links, untagged members of the default VLAN (*VLAN #1*).

VLAN learning modes

The 802.1Q specification defines two ways that VLAN devices store MAC addresses in their bridging tables:

- Independent VLAN learning (IVL) — allows the same MAC address to appear in different broadcast domains. An IVL-capable device maintains independent bridge tables for each VLAN, allowing devices to reuse a MAC address in different VLANs.
- Shared VLAN learning (SVL) — constrains a MAC address to only one VLAN. SVL-based devices build a giant bridge table, but allow a MAC address to appear only once in the table, regardless of how many VLANs exist.

Business Policy Switch 2000 and BayStack switches can support either method. When you configure the VLAN, you indicate which learning mode to use.

Creating VLANs

Before you can build a VLAN using Optivity Quick2Config 2.2, you must install and initially configure the network devices. For information about importing switch configurations, see [“Importing configurations” on page 22](#).

The following summarizes the steps to create and configure a VLAN:



Note: For detailed procedures, see the sections that follow.

- 1 Use the Quick2Config Palette to add a VLAN to the switch.
- 2 Assign the VLAN ID and name.
- 3 Configure additional VLAN properties. How you configure the VLAN depends on the VLAN type:
 - Port-based VLAN (next)
 - Protocol-based VLAN ([page 39](#))
 - MAC-based VLAN ([page 41](#))
- 4 Assign VLAN ports.
- 5 Optionally, configure IGMP snooping. For information, see [Chapter 3, “Configuring IGMP snooping.”](#)
- 6 Export configuration data to the switches on the network.

Configuring a port-based VLAN

For each switch that participates in the VLAN:

- 1 Create the VLAN from the Palette.
 - a In the navigation pane, open each participating switch and select the VLAN.
 - b In the context-sensitive pane, click the Properties tab.
 - c Add a port-based VLAN to the participating switches.
- 2 In the navigation pane, select the VLAN.

- 3 In the context-sensitive pane, click the Properties tab (Figure 8).

Figure 8 Port-based VLAN

Property	ID	Name
VLAN	1	Default

Property	Value
VLAN State	Active
IVL/SVL	IVL

- 4 In the Basic tab, assign the VLAN ID and name.
 - a Keep the default VLAN ID 1, or specify a VLAN ID of 2 to 64. The ID must be identical in each participating switch. By coordinating VLAN IDs, you can extend a VLAN to multiple switches.
 - b Type a descriptive VLAN name, 1 to 16 characters, to identify the VLAN. The name must be unique, and identical in each participating switch.
- 5 In the IVL/SVL list, choose independent VLAN learning (IVL) or shared VLAN learning (SVL) bridging tables for this VLAN.
For information, see “[VLAN learning modes](#)” on page 37.
- 6 Configure the participating ports.
See “[Configuring VLAN ports](#)” on page 42.

Configuring a protocol-based VLAN

For each switch that participates in the VLAN:

- 1 Create the VLAN from the Palette.
 - a In the navigation pane, select the switches that will participate in the VLAN.
 - b In the context-sensitive pane, open the VLANs folder in the Palette tab.
 - c Add a protocol-based VLAN to the participating switches.

- 2 In the navigation pane, select the VLAN.
- 3 In the context-sensitive pane, click the Properties tab ([Figure 9](#)).

Figure 9 Protocol-based VLAN properties

The screenshot shows a configuration window with two tabs: 'Palette' and 'Properties'. The 'Properties' tab is active. Inside, there are two sub-tabs: 'Basic' and 'IGMP'. The 'Basic' sub-tab is selected. The window contains several tables for configuration:

Property	ID	Name
VLAN	5	proto5

Property	Value
VLAN State	Inactive
IVL/SVL	IVL

Property	ID	User defined PID
Protocol	IP Ether2	

- 4 Assign the VLAN ID and name.
 - a Keep the default VLAN ID 1, or specify a VLAN ID of 2 to 64. The ID must be identical in each participating switch.
 - b Type a descriptive VLAN name, 1 to 16 characters, to identify the VLAN. The name must be unique, and identical in each participating switch.
- 5 In the IVL/SVL list, choose whether the switch should use independent VLAN learning (IVL) or shared VLAN learning (SVL) bridging tables for this VLAN.

For information, see [“VLAN learning modes” on page 37](#).
- 6 In the Protocol table, choose a predefined protocol, or choose User-Defined to specify a protocol not listed.

If you choose User-Defined, type an IETF RFC 1356 protocol identifier (PID) in the User defined PID field.
- 7 Configure the ports to participate in the VLAN. See [“Configuring VLAN ports” on page 42](#).

Configuring a MAC SA-based VLAN

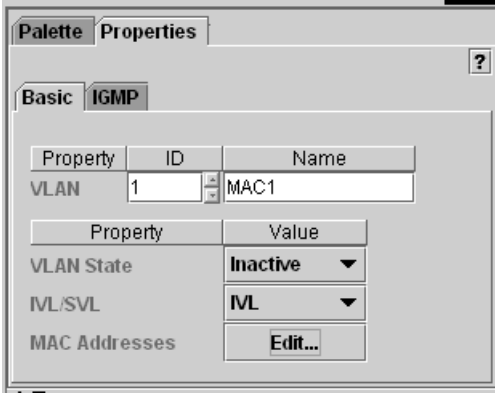
You can configure up to 48 MAC SA-based VLANs on a switch.

In a VLAN based on the MAC source address (SA), a frame is associated with a VLAN only if the source MAC address is on an explicit list of MAC addresses that comprise the VLAN. Because it is necessary to explicitly associate MAC addresses with a MAC SA-based VLAN, the administrative overhead can be high.

To configure a MAC SA-based VLAN, complete these steps for each switch that participates in the VLAN:

- 1 Create the VLAN from the Palette.
 - a In the navigation pane, select the switches that will participate in the VLAN.
 - b In the context-sensitive pane, open the VLANs folder in the Palette tab.
 - c Add the desired type of VLAN to the participating switches.
- 2 In the navigation pane, select the VLAN.
- 3 In the context-sensitive pane, click the Properties tab (Figure 10).

Figure 10 MAC-based VLAN properties



Property	ID	Name
VLAN	1	MAC1

Property	Value
VLAN State	Inactive
IVL/SVL	IVL
MAC Addresses	Edit...

- 4 In the IVL/SVL list, choose whether the switch should use independent VLAN learning (IVL) or shared VLAN learning (SVL) bridging tables for this VLAN.

For information, see [“VLAN learning modes” on page 37](#).

- 5 In the MAC Addresses field, click Edit.

The MAC Addresses window opens.

- 6 Specify MAC addresses, one line at a time.

Use the following format:

```
aa:bb:cc:dd:00:11
```



Note: You can cut and paste MAC addresses from a text, word processing, or spreadsheet file.

- 7 Configure the ports to participate in the VLAN. See [“Configuring VLAN ports,”](#) next.

Configuring VLAN ports

To assign switch ports to participate in a VLAN:

- 1 In the navigation pane, select the switch ports.

As you select VLAN ports, note the following:

- A switch port can be an ingress member of only one port-based VLAN.
- No port can be a member of more than one protocol-based VLAN with the same protocol.
- A tagged port can have two protocol-based VLANs of the same protocol type.

- 2 Create shortcuts from the ports to the VLAN.

- a Right-click the selected ports, then choose Copy.
- b In the navigation pane, select the VLAN.
- c Right-click, then choose Paste as Shortcut.

To configure VLAN ports:

- 1 In the navigation pane, select the VLAN ports.

You can set properties on individual ports, or configure groups together.

- 2 In the context-sensitive pane, click the Properties tab.
- 3 Click the VLAN tab (Figure 11).

Figure 11 Port VLAN tab

Property	Value
Port Number	1
Port Type	Access
PVID	1
Port Priority	0

Filter ☐ Tagged frames ☐ Untagged frames

By default, all ports are configured as access ports with Priority 0.

- 4 From the Port Type list, choose Trunk.

For information about access and trunk connections, see [“802.1Q frame tagging” on page 37](#).

The port icon changes, so you can differentiate trunk and access ports in the navigation pane.

- 5 In the PVID field, match the VLAN ID number.
- 6 In the Port Priority field, type or choose an 802.1p user priority value for this port. By default, all ports have priority 0.



Note: To see how the 802.1p user priorities map to standard Nortel Networks IP class of service values, refer to [Table 13 on page 82](#).

- 7 Configure how the port filters 802.1Q tagged frames.

In the Filter field, check Tagged frames to dropped frames with the 802.1Q tag, or check Untagged to drop frames that do not have the tag. To disregard frame tagging, clear both check boxes. To discard all frames on this port, check both.

Chapter 3

Configuring IGMP snooping

You can use Internet Group Management Protocol (IGMP) snooping to conserve bandwidth and control IP multicast streams.

Read the sections of this chapter to learn how to use Optivity Quick2Config 2.2 to configure IGMP snooping:

- [“About IP multicast and IGMP,”](#) next
- [“IGMP snooping configuration rules”](#) on page 47
- [“Enabling IGMP snooping”](#) on page 47
- [“Creating static router ports”](#) on page 49

About IP multicast and IGMP

IP hosts use IGMP and IP multicast addressing to report their group memberships to immediate neighboring multicast routers. Routers send IGMP queries to all hosts, and IGMP hosts respond by sending IGMP reports to the multicast address of the group they want to participate in.

The switch uses the information learned from IGMP activity to map IP multicast groups to switch ports. Packets destined to a particular multicast group are delivered only to those member ports.



Note: The Business Policy Switch 2000 and BayStack 450 product group are neither IGMP routers nor IGMP hosts. The IGMP snooping feature optimizes IP multicast in a bridged Ethernet environment.

IGMP host membership reports

IP multicast routers use IGMP to learn about the existence of host group members on their directly attached subnets. 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.

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 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 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: Even if nonparticipating end stations filter the IP multicast stream, IP multicast traffic still consumes bandwidth on the subnet.

IGMP snooping

The IGMP snooping feature provides the same benefit as IP multicast routers, but in the local area.

With IGMP snooping enabled, a switch senses IGMP host membership reports from attached stations and uses this information to set up a dedicated path between the requesting station and a local IP multicast router. After the path is established, the switch blocks the IP multicast stream from exiting any other port that does not connect to another host member, thus conserving bandwidth.

Proxy reports

IGMP snooping allows the switch to send multicast data to the members of a multicast group in a given VLAN only. When a switch acts as IGMP proxy, it forwards only one report to the router instead of one report for every member of the multicast group.

IGMP snooping configuration rules

Consider the following to determine how IGMP snooping affects a network topology:

- Static router ports must be port members of at least one VLAN.
- If you configure an SVL VLAN port as a static router port, is configured as a static router port for all VLANs on that port. If you remove a static router port from an SVL VLAN, the port is removed as a member of all of its configured VLANs. The IGMP configuration of IVL VLANs is not propagated to all VLANs on the port.
- You cannot configure a port that is configured for port mirroring as a static router port, and you cannot configure a static router port for port mirroring.
- If you configure a multilink trunk (MLT) member as a static router port, all of the MLT members are configured as static router ports. If you remove a static router port that is an MLT member, all members are automatically removed as static router port members.
- The IGMP snooping feature is not dependent on the Spanning Tree Protocol.
- The IGMP snooping feature is not dependent on rate limiting.

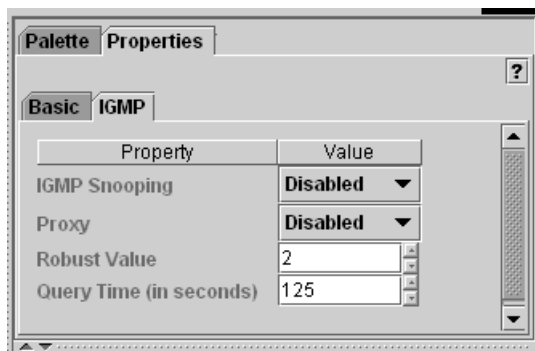
Enabling IGMP snooping

To enable IGMP snooping and configure IGMP properties on a VLAN:

- 1 In the navigation pane, select the VLAN.
- 2 In the context-sensitive pane, click Properties.

- 3 Click the IGMP tab (Figure 12).

Figure 12 IGMP properties



- 4 From the IGMP Snooping list, choose Enabled.
Enabling IGMP Snooping on an SVL VLAN enables the feature on all VLANs configured for the switch.
- 5 If you want this switch to consolidate the IGMP host membership reports it receives on downstream ports before forwarding, choose Enabled from the Proxy list.
Enabling Proxy on an SVL VLAN enables consolidated proxy reports on all VLANs in the switch.
- 6 If packet losses on a subnet are unacceptably high, increase the Robust Value to offset the expected packet loss.
From the Robust Value list, choose a value between 1 and 64.
- 7 To change the frequency of IGMP queries allowed in this subnet from the IP multicast router, change the default Query Time value of 125 seconds.
From the Query Time list, choose a value between 1 and 512 seconds.
- 8 Configure one or more static router ports from the VLAN to an IP multicast router. See [“Creating static router ports,”](#) next.

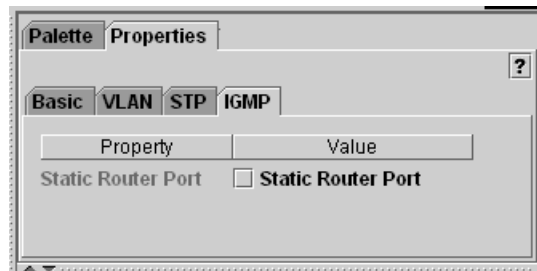
Creating static router ports

With IGMP snooping enabled, determine which VLAN ports have a path to an IP multicast router, then configure those links as static router ports.

To configure a switch port as an IGMP static router port:

- 1 In the navigation pane, select one or more VLAN ports with a path to a multicast router. It is not necessary for the path to be direct.
- 2 In the context-sensitive pane, click the Properties tab.
- 3 Click the IGMP tab (Figure 13).

Figure 13 Port IGMP tab



- 4 Check Static Router Port.

If the port is a member of an MLT group, all MLT members become IGMP static router ports.

Chapter 4

Configuring multilink trunks

You can use multilink trunks (MLTs) to combine Ethernet ports in a single, logical connection.

Read the sections of this chapter to learn how to use Optivity Quick2Config 2.2 to configure MLTs:

- [“About multilink trunking,”](#) next
- [“MLT configuration guidelines”](#) on page 52
- [“Creating an MLT group”](#) on page 53

About multilink trunking

In an MLT group, 2 to 4 ports form a single link to another switch or server. In full-duplex mode, the aggregate throughput between the two devices can increase up to 800 Mb/s. MLT software detects misconfigured or broken trunk links and redirects traffic on the link to other members within the trunk group.

You can configure trunk members within a single unit, within any of the units in a stack configuration, or distribute trunk members between stacks (*distributed trunking*).

To learn more about the ports you can configure in an MLT group, see [“MLT configuration guidelines”](#) on page 52.

MLT configuration guidelines

You can configure up to 6 MLT groups on each switch or stack. The Spanning Tree Protocol considers an MLT to be a single port.

To plan for each MLT:

- Determine which switch ports to combine as trunk members.

Choose a minimum of 2 and a maximum of 4 Ethernet ports for each trunk. Make sure that the ports you choose are:

- Enabled
- Not probe ports
- Not members of another MLT
- Members of the same VLAN, if they are VLAN participants

On the trunk member ports, the following properties must have same values:

- Port speed
- VLAN port type
- STP participation
- IGMP static router



Note: If you configure an MLT member to filter tagged or untagged frames, all of the MLT group members are automatically configured for 802.1q frame tagging.

- Consider how existing VLANs will be affected by the addition of each trunk. See [“Configuring VLANs” on page 35](#).
- Consider how the existing spanning tree will react to the trunk configurations. See [“Configuring spanning tree” on page 55](#).
- To avoid errors, make sure that all network cabling is complete and stable before you export a new trunk configuration.

Creating an MLT group

To configure 2 to 4 switch ports in an MLT group:

- 1 In the navigation pane, open a switch and select the ports.

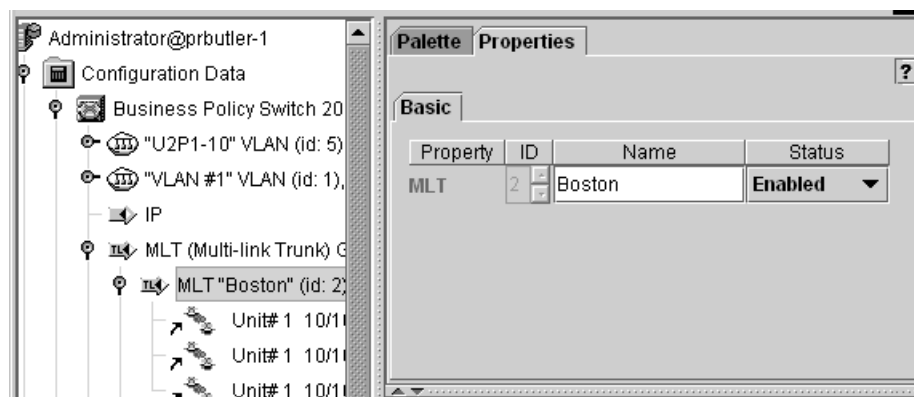
For information about the ports you can configure in an MLT group, see [“MLT configuration guidelines” on page 52](#).

- 2 Open the MLT Group folder.
- 3 Create shortcuts from the ports to the MLT.

There are 6 MLT templates in the MLT Group folder. Use any unconfigured MLT.

- a Right-click the selected ports, then choose Copy.
 - b In the navigation pane, select the MLT.
 - c Right-click, then choose Paste as Shortcut.
- 4 In the navigation pane, select the MLT.
- 5 In the context-sensitive pane, click the Properties tab ([Figure 14](#)).

Figure 14 MLT properties



- 6 In the Name field, type a descriptive name to identify the trunk.
- 7 From the Status list, choose Enabled.

Chapter 5

Configuring spanning tree

By default, all switch ports are enabled for participation in the Spanning Tree Protocol (STP).

Read the sections of this chapter to learn how to use Quick2Config to disable STP on individual ports or MLT trunks, view STP group and port values, and customize STP group properties:

- [“About the Spanning Tree Protocol,”](#) next
- [“Configuring STP ports”](#) on page 55
- [“Viewing and configuring STP group properties”](#) on page 58

About the Spanning Tree Protocol

The Spanning Tree Protocol, defined in the IEEE 802.1D standard, determines the best path between segments of a bridged network. When multiple paths exist, the spanning tree algorithm configures the network to use only the most efficient path. If the selected path fails, STP automatically reconfigures the network to make another path active and sustain network operation.

Configuring STP ports

By default, all switch ports participate in the spanning tree algorithm. For each switch port or MLT group, you can:

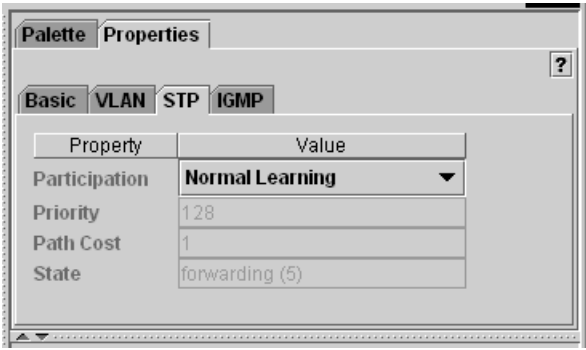
- Change the STP learning state
- Disable STP participation

Changing the STP learning state

To change the learning state:

- 1 In the navigation pane, select one or more switches or MDA ports.
Select only ports that do not currently belong to an existing STP group.
- 2 In the context-sensitive pane, click the Properties tab.
- 3 Click the STP tab ([Figure 15](#)).

Figure 15 STP port properties



Property	Value
Participation	Normal Learning ▼
Priority	128
Path Cost	1
State	forwarding (5)

- 4 From the Participation list, choose a learning state for this port or change the state to Forwarding only.

By default, all ports are configured for Normal Learning. Fast Learning reduces the state transition timer to 2 seconds.

In the remaining fields, Quick2Config reports the read-only values of STP port properties (Table 2).

Table 2 STP port read-only properties

Property	Description
Priority	Indicates the STP priority for this port. Port priority determines the root bridge. A lower number establishes a higher priority. When one or more ports have the same path cost, the spanning tree algorithm selects the path with the highest priority (lowest numerical value).
Path Cost	STP uses the path cost of each port to determine the most efficient path to the root bridge. The higher the LAN speed, the lower the path cost. Path Cost = 1000/LAN speed (in Mb/s). The default value is 1 for gigabit ports, 10 for 100 Mb/s ports, and 100 for 10 Mb/s ports.
State	Indicates the current port state within the spanning tree network: Disabled, Blocking, Listening, Learning, Forwarding. STP ports transition to various states, as determined by the Participation property. When you disable Participation, the port transitions only to the Forwarding state. When the Participation is enabled, the port transitions through the Blocking, Listening, and Learning states before entering the Forwarding state. The default value is dependent on topology.

Disabling STP port participation

When you disable STP participation, the port does not participate in the spanning tree algorithm and transitions to the Forwarding state.

To disable a port or MLT group from spanning tree participation:

- 1 In the navigation pane, select one or more switch or MDA ports.
Select only ports that do not currently belong to an existing STP group.
- 2 In the context-sensitive pane, click the Properties tab.
- 3 Click the STP tab (Figure 15).
- 4 From the Participation list, choose Disabled.

Viewing and configuring STP group properties

To configure a spanning tree group (STG):

- 1 In the navigation pane, open the Spanning Tree Protocol Group folder.
- 2 Select the STG ID.

The STP Basic tab opens (Figure 16).

Figure 16 Spanning Tree Protocol Group tab

Property	Value
ID	
Designated Root	
Root Port	
Root Path Cost	
Hello Time	
Maximum Age Time	
Forward Delay	
Bridge Priority	8000
Bridge Hello Time	2
Bridge Maximum Age Time	20
Bridge Forward Delay	15

Table 3 describes the STP group properties. You can customize the value of Bridge Priority, Bridge Hello Time, Bridge Maximum Age Time, and Bridge Forward Delay.

Table 3 Spanning Tree Protocol Group properties

Parameter	Description	Action
ID	Identification number for this STG.	Read-only value
Designated Root	The bridge ID of the root bridge, as determined by the spanning tree algorithm.	Read-only value
Root Port	The switch port number that offers the lowest path cost to the root bridge.	Read-only value

Table 3 Spanning Tree Protocol Group properties (continued)

Parameter	Description	Action
Root Path Cost	The path cost from this switch port to the root bridge.	Read-only value
Hello Time	The Actual Hello Interval, the amount of time between transmissions of configuration Bridge Protocol Data Units (BPDUs) that the root bridge is currently using. All bridges participating in the spanning tree network use the root bridge's Hello Interval parameter value. See also Bridge Hello Time.	Read-only value
Maximum Age Time	The Maximum Age Time parameter value that the root bridge is currently using. This value specifies the maximum age that a Hello message can attain before it is discarded. The root bridge's Maximum Age Time parameter value becomes the actual Maximum Age Time parameter value for all bridges participating in the spanning tree network. See also Bridge Maximum Age Time.	Read-only value
Forward Delay	The Forward Delay parameter value that the root bridge is currently using. This value specifies the amount of time that the bridge ports remain in the Listening and Learning states before entering the Forwarding state. The root bridge's Forward Delay parameter value becomes the actual Forward Delay parameter value for all bridges participating in the spanning tree network. See also Bridge Forward Delay.	Read-only value
Bridge Priority	The management-assigned priority value of the bridge ID in hexadecimal notation, which is the most significant byte of the bridge ID. The STA uses this parameter to determine the root bridge (or designated bridge). For example, the bridge with the lowest bridge ID becomes the root bridge, with Bridge Priority values compared first, followed by the hardware addresses.	Type a value from 0 to 65535. The default value is 8000.
Bridge Hello Time	The Hello Interval (the amount of time between transmissions of BPDUs) specified by management for this bridge. This property takes effect only when this bridge becomes the root bridge. Although you can set the Hello Interval for a bridge using bridge management software, once the spanning tree computation process is complete, all bridges participating in the spanning tree network use the root bridge's Hello Interval parameter value. If any bridge becomes the root bridge, its Hello Interval parameter value becomes the Actual Hello Interval parameter value for all bridges participating in the spanning tree network. See also Hello Time.	Choose a value from 1 to 10 seconds, or keep the default value of 2 seconds.
Bridge Maximum Age Time	The maximum age that a Hello message can attain before it is discarded. This parameter, specified by management for this bridge, takes effect only when the bridge becomes the root bridge. If this bridge becomes the root bridge, its Maximum Age Time parameter value becomes the Actual Maximum Age Time parameter value for all bridges participating in the spanning tree network. See also Maximum Age Time.	Choose a value from 6 to 40 seconds, or keep the default value of 20 seconds.

Table 3 Spanning Tree Protocol Group properties (continued)

Parameter	Description	Action
Bridge Forward Delay	<p>The Forward Delay parameter value specified by management for this bridge. This parameter takes effect only when this bridge becomes the root bridge.</p> <p>The Forward Delay parameter value specifies the amount of time that the bridge ports remain in the Listening and Learning states before entering the Forwarding state.</p> <p>All bridges participating in the spanning tree network use the root bridge's Forward Delay parameter value. See also Forward Delay.</p>	Choose a value from 4 to 30 seconds, or keep the default value of 15 seconds.

Chapter 6

Configuring QoS filters

You configure quality of service (QoS) policy filters on a Business Policy Switch to prioritize critical applications or sensitive traffic and to help tailor network performance.

Read the sections of this chapter to learn how to use Optivity Quick2Config 2.2 to enable, view, configure, or modify QoS policy filters:

- [“About QoS policy filters,”](#) next
- [“Configuration summary”](#) on page 63
- [“Configuring dynamic QoS management”](#) on page 65
- [“Configuring policies locally”](#) on page 69
- [“Configuring QoS interfaces”](#) on page 78
- [“User priority and DSCP mapping”](#) on page 82
- [“Viewing transmit queue information”](#) on page 84
- [“Resetting QoS values in Quick2Config”](#) on page 88

About QoS policy filters

A QoS *policy* is a set of rules that a network interface uses to identify and process particular network traffic patterns. When traffic has the same attributes as those specified in a configured QoS policy filter, the policy instructs the interface to perform a specified action.

The Business Policy Switch 2000 employs Differentiated Services (DiffServ) to participate in policy-based network traffic control. DiffServ is a QoS architecture developed by the Internet Engineering Task Force (IETF); it provides different types of services to different IP traffic flows.

Most Business Policy Switches obtain QoS policy information from a server in the network that runs QoS policy management software such as Optivity Policy Services (OPS). The Optivity policy server transfers DiffServ information to policy client devices using the Common Open Policy Services (COPS) protocol.

To manage QoS policies on the switch rather than from a policy server, you must work with many components. Each filter incorporates interface, classification, and action definitions. User priority values, DiffServ codepoint (DSCP) mapping, and priority and DSCP queue assignments also affect QoS policies.

For more information, see [“DiffServ architecture,”](#) next, or [“Configuration summary”](#) on page 63.

DiffServ architecture

The DiffServ QoS architecture operates as follows:

- 1 A QoS policy server sends policy information to network policy clients in the form of DiffServ filters.

For example, a host running Optivity Policy Services software operates as policy server for Business Policy Switches in a policy-enabled network.

- 2 When packets arrive at a policy client interface, the switch classifies the packets according to DiffServ classifications from the policy server.

Packet classifications select packets according to a particular content in the packet header such as the source address, destination address, source port number, destination port number, or incoming interface.

- 3 The interface directs classified packets to traffic conditioners for further processing such as marking or dropping.

Marking is the process of setting the Differentiated Services (DS) field of the packet to a particular value. *Dropping* is the process of discarding some or all of the packets to comply with a traffic profile.

- 4 The interface applies forwarding actions, or per-hop behaviors, to the conditioned packets. These actions include queuing and shaping functions.

DiffServ codepoints

DiffServ architecture relies on a special encoding of the first 6 bits of the DS byte in the IP header—the Ipv4 Type of Service (ToS) byte or the Ipv6 Traffic Class byte. These first 6 bits of the ToS or Traffic Class byte are called the DiffServ codepoint (DSCP).

The DSCP signifies the quality of service that a flow of packets should receive when handled by a policy-enabled network.



Note: For packet prioritization in layer 2 switches that do not recognize DSCP but are able to process 802.1Q packets, an IEEE 802.1p class of service (CoS) user priority is added as packet are transmitted.

Configuration summary

The Business Policy Switch has predefined QoS role combinations for its external, MDA, and cascade ports. Optionally, you can create custom role combinations for the switch interfaces. See [“Creating new role combinations” on page 79](#).

On each switch, you implement DiffServ QoS policy management in static or dynamic mode.

- With *dynamic* DiffServ management, a policy server in the network sends all QoS policy information to the switch using the COPS protocol. You do not manually configure QoS policies, but you must enable dynamic management and configure COPS information for policy server connections.
- With *static* DiffServ management, the internal policy agent on the switch manages all QoS information. You must manually configure the QoS policies.

By default, the Business Policy Switch is set to static DiffServ management.

Dynamic DiffServ management

In a policy-enabled network that uses a centralized policy server, each client device operates in dynamic mode. There can be a single policy server for each DiffServ domain, but a hierarchy of policy clients within the domain.

To operate with a COPS policy server in dynamic mode, you need to:

- Choose dynamic DiffServ management in the QoS Properties tab. See [“Configuring dynamic QoS management” on page 65](#).
- Configure COPS information for policy server connections. See [“Configuring COPS connections” on page 67](#).

Static DiffServ management

By default, a Business Policy Switch manages its QoS policies locally, without a centralized COPS server. With static management, each switch is a DiffServ domain.

In static mode, you must create the packet classification and filter action components of QoS filters before you can configure QoS policies. See [“Configuring policies locally” on page 69](#).

You can also change the DSCP-to-802.1p mapping for packets that are marked at egress. See [“User priority and DSCP mapping” on page 82](#).

Configuring dynamic QoS management

With dynamic DiffServ management enabled, a COPS policy server manages QoS policies on the switch.

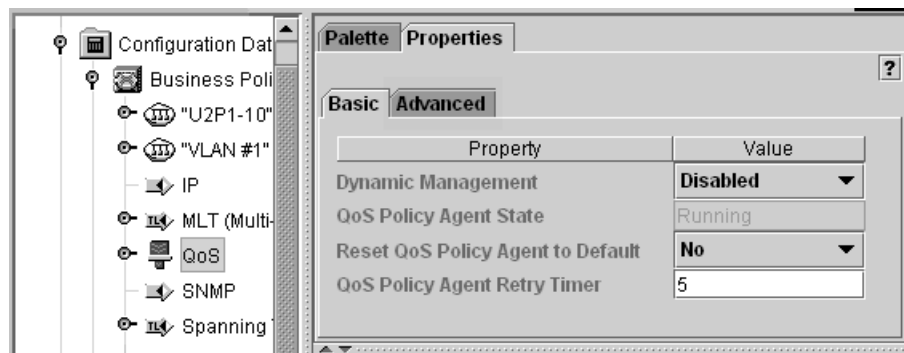


Note: With dynamic DiffServ management disabled (the default), the switch manages all QoS operation and you must configure policies locally. See [“Configuring policies locally” on page 69](#).

To enable a Business Policy Switch 2000 as a QoS policy client:

- 1 In the navigation pane, expand the switch device tree.
- 2 Select QoS.
- 3 Click the Properties tab to view the QoS policy agent Basic properties ([Figure 17](#)).

Figure 17 QoS policy agent Basic properties



4 Use the information in [Table 4](#) to configure property values.

Table 4 QoS policy agent properties

Property	Description	Action
Dynamic Management	Determines whether QoS filters are configured locally (static management) or dynamically, by a policy server.	To disable internal QoS management to operate with a policy server, choose Enabled. To manage policies locally, disable dynamic management. With dynamic management, you must configure COPS. See "Configuring COPS connections" on page 67 .
QoS Policy Agent State	The current status of the QoS software on the switch: Running, Initializing, or Disabled.	None; this a read-only property.
Reset QoS Policy Agent State to Default	Resets the switch to the default QoS policy agent settings. Quick2Config deletes all non-default values in the Classification, Action, and Policy tables. Note: To reset the QoS configuration changes you have made during a Quick2Config session, see "Resetting QoS values in Quick2Config" on page 88 .	To reset the switch to default settings, choose Yes. Note: If Dynamic Management is enabled, resetting the default values restores static management.
QoS Policy Agent Retry Timer	The time between the receipt of a connection termination or rejection from the switch QoS software and the start of a new policy server connection request. By default, the timer is set to the maximum value, 86400 s.	Type the number of seconds to wait between connection retries. To disable connection retries, type -1.

Configuring COPS connections

With dynamic management enabled, the DiffServ policy server uses the Common Open Policy Service (COPS) protocol to transfer DiffServ information to the switch, and the switch uses COPS to report its client policy information to the server. COPS uses the Transmission Control Protocol (TCP) to exchange messages.

To configure the COPS connections for this switch when operating in dynamic management mode:

- 1 In the navigation pane, expand the switch and select COPS.
- 2 In the context-sensitive pane, click Properties to open the COPS Configuration table ([Figure 18](#)).

Figure 18 COPS Configuration table

	Address Type	Address	Client Type	Auth Type	TCP Port	Priority
0	IPv4	1.1.1.1	2	None	1111	1
1	IPv4	20.20.20.20	2	None	7770	7
2	IPv4	132.245.252.22	2	None	6060	8

- 3 Use the information in [Table 5](#) to configure property values.

Table 5 COPS Configuration table properties

Property	Description	Action
Address Type	Indicates whether the value of the Address property is a DNS, IPv4, or IPv6 address.	None; this is a read-only value.
Address	The network address of a COPS policy server.	Type an IPv4, IPv6, or DNS address.

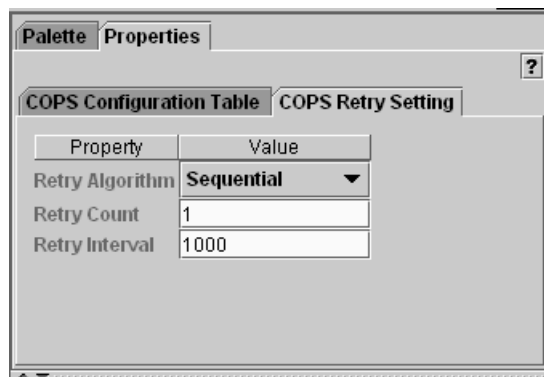
Table 5 COPS Configuration table properties (continued)

Property	Description	Action
Client Type	The protocol client type for this COPS server. A value of 0 (zero) indicates that this entry contains information about the underlying connection.	None; this is a read-only value. Note: A single COPS server can support multiple clients.
Auth Type	The authentication mechanism that this switch uses to negotiate security at the start of a connection to the COPS server.	None; this is a read-only value.
TCP Port	The TCP port number on the COPS server that the switch uses to connect.	Type the port number.
Priority	The level of priority assigned to this policy server. Higher number servers have higher priority and are contacted first.	Type the priority number.

Configuring COPS retry settings

To set the retry settings for COPS connections:

- 1 In the navigation pane, expand the switch and select COPS.
- 2 In the Properties tab, click COPS Retry Setting ([Figure 19](#)).

Figure 19 COPS Retry Setting tab

- 3 Use the information in [Table 6](#) to configure property values.

Table 6 COPS Retry Setting properties

Property	Description	Action
Retry Algorithm	The type of algorithm to use to determine when to retry a connection attempt.	Choose Sequential, Round Robin, or Other.
Retry Count	The number of retries to attempt.	Type the number of retry attempts.
Retry Interval	The length of time between retries.	Type the number of seconds between retries.

Configuring policies locally

When a Business Policy Switch operates in static mode, without a central policy server in the network, you create and apply the components of QoS polices locally. See the following sections:

- [“Configuring classifications and filter groups,”](#) next
- [“Configuring filter actions” on page 75](#)
- [“Configuring policies” on page 76](#)

Configuring classifications and filter groups

Policies are comprised of traffic conditions and actions that result in access to network services or denial of services. In order for a packet to be processed by a configured filter, the packet must match all the fields that you specify in a classification.

You can configure both IP (Layer 3) classifications and LLC 802.2 (Layer 2) classifications, and can group both types of classification into filter groups to create more complex policies.

Configuring IP filter classifications

To configure IP filter classes:

- 1 In the navigation pane, expand the switch device and the QoS folder.
- 2 Select IP Classification.
- 3 Click the Properties tab to view the IP Filter table (Figure 20).

Figure 20 QoS IP Filter table

	Index	Dest Addr	Dest Addr Mask	Src Addr	Src Addr Mask	DSCP	Protocol	Destination L4 Port	Source L4 Port
0	1	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	-1	Match All	65535	0
1	2	12.12.12.1	255.255.255.0	13.13.13.1	255.0.0.0	10	TCP	0	65535

- 4 Use the information in Table 7 to configure property values.

Table 7 QoS IP Filter table properties

Property	Description	Action
Index	Uniquely identifies this class.	Type a number to uniquely identify this class.
Dest Addr	The address used to match against the destination address in the packet's IP header.	Type the destination IP address in dotted-decimal notation.
Dest Addr Mask	The destination address subnet mask.	Type the destination address subnet mask. A zero bit in the mask means that the corresponding bit in the address always matches.
Src Addr	The address to match against the packet's source IP address.	Type the source IP address in dotted-decimal notation.
Src Addr Mask	The source subnet mask.	Type the source address subnet mask.

Table 7 QoS IP Filter table properties (continued)

Property	Description	Action
DSCP	Sets the IP filter to match packets with a specific DSCP value in the IP header. On untrusted interfaces, the packet's DSCP value must be re-marked.	Type the hex value of the DSCP in the packet, from 0x00 (0 decimal value) to 0x3F (63 decimal value). To ignore the DSCP value in the packet, choose the default (-1).
Protocol	Selects one or all of the following IP protocols to match against the packet protocol: <ul style="list-style-type: none"> • TCP • UDP • ICMP • IGMP • RSVP 	Choose the IP protocol to match against the packet's IP protocol. To match all IP protocols, choose Match All.
Destination L4 Port	The value of the packet's Layer 4 destination port number.	Choose the port number, 0 to 65535.
Source L4 Port	The value of the packet's Layer 4 source port number.	Choose the port number, 0 to 65535.
Permit	Determines whether to process the next filter (True) or go to next filter group (False).	This field is always True.

Next, create filter groups from the configured IP classifications. See [“Configuring IP and Layer 2 filter groups” on page 74](#).

Configuring Layer 2 classifications

To configure 802.2 filter classifications:

- 1 In the navigation pane, expand the switch device and the QoS folder.
- 2 Select Layer 2 Classification.
- 3 In the Palette tab, create a Layer 2 Filter template.
- 4 Select the new filter object and click the Properties tab ([Figure 21](#)).

Figure 21 QoS 802 Filter table

	Index	VLAN ID	VLAN Tag Required	Ether Type	DSCP	Protocol	Dest L4 Port Min	Dest L4 Port Max	Source L4 Port
0	1	-1	Tagged Only	800	-1	TCP	0	65535	0

- 5 Use the information in [Table 8](#) to configure values for the Layer 2 filter properties.

Table 8 QoS 802 Filter properties

Property	Description	Action
Index	Uniquely identifies this policy rule instance.	Type a number to uniquely identify this policy rule.
VLAN ID	Uniquely identifies the VLAN.	Type the VLAN ID.
VLAN Tag Required	Set the filter profile to match on the presence or absence of a VLAN tag.	Choose one of the following to determine how to match VLAN tagging: <ul style="list-style-type: none"> Tagged Only Priority Type Plus Untagged Only Ignore Tagged
Ether Type	Sets the filter profile to match a value in the EtherType field of an Ethernet header.	Type an EtherType value.
DSCP	Sets the IP filter to match packets with a specific DSCP value in the IP header. On untrusted interfaces, the packet's DSCP value must be re-marked.	Type the hex value of the DSCP in the packet, from 0x00 (0 decimal value) to 0x3F (63 decimal value). To ignore the DSCP value in the packet, choose the default (-1).

Table 8 QoS 802 Filter properties (continued)

Property	Description	Action
Protocol	Selects one or all of the following IP protocols to match against the packet protocol: <ul style="list-style-type: none"> • TCP • UDP • ICMP • IGMP • RSVP 	Choose the IP protocol to match against the packet's IP protocol. To match all IP protocols, choose Match All.
Dest L4 Port Min	The minimum value of the packet's Layer 4 destination port number.	Choose the port number, 0 to 65535. In release 1.0x of BPS agent software, the value must match the Dest L4 Port Max.
Dest L4 Port Max	The maximum value of the packet's Layer 4 destination port number.	Choose the port number, 0 to 65535. In release 1.0x of BPS agent software, the value must match the Dest L4 Port Max.
Source L4 Port Min	The minimum value of the packet's Layer 4 source port number.	Choose the port number, 0 to 65535. In release 1.0x of BPS agent software, the value must match the Source L4 Port Max.
Source L4 Port Max	The maximum value of the packet's Layer 4 source port number.	Choose the port number, 0 to 65535. In release 1.0x of BPS agent software, the value must match the Source L4 Port Min.
User Priority One User Priority Two User Priority Three User Priority Four User Priority Five User Priority Six User Priority Seven User Priority Ignore	Set the filter profile to match or ignore the value in the User Priority field of an Ethernet header.	Choose a user priority value, or choose User Priority Ignore to disregard the user priority value when matching packets.

Next, create filter groups from the configured Layer 2 classifications.

Configuring IP and Layer 2 filter groups

You can configure filter groups of IP (Layer 3) and 802.2 (Layer 2) classifications.

To configure filter groups:

- 1 In the navigation pane, select IP Classification or Layer2 Classification.
- 2 In the Properties tab, click the IP Filter Group or 802 Filter Group table tab.

Figure 22 shows an example IP Filter Group table. The 802 Filter Group table has the same properties.

Figure 22 QoS IP Filter Group table

	Index	Filter Group ID	Filter Index	Filter Order
0	1	1	1	1
1	2	2	2	2

- 3 Use the information in Table 9 to configure property values.

Table 9 QoS IP and 802 Filter Group table properties

Property	Description	Action
Index	Uniquely identifies this policy rule instance.	Type a number to uniquely identify this policy rule.
Filter Group ID	Uniquely identifies this filter group.	Type a number to identify this filter group.
Filter Index	The number of the filter, found in the Index column of the Filter table. See “Configuring IP filter classifications” on page 70 or “Configuring Layer 2 classifications” on page 71 .	Type the number of the classification filter.
Filter Order	The order of precedence for this filter. Lower precedence numbers are matched first.	Type the order number. The highest precedence number is 0.

Configuring filter actions

An *action* specifies the type of behavior you want the policy to apply to a filter group. Actions can control packet size and flow rate, deny packet flow, drop packets, or apply a predefined class of service to a flow of packets.

A policy can have only one action applied to it, but you can apply an action to multiple policies.

To configure filter actions:

- 1 In the navigation pane, expand the switch device and the QoS folder.
- 2 Select Action Table.
- 3 Click the Properties tab to view the Action table ([Figure 23](#)).

Figure 23 QoS Action table

	Index	Drop	Update DSCP	Set Drop Precedence	Update Priority
0	1	False	10	Use Default	Use Default

- 4 Use the information in [Table 10](#) to configure property values.

Table 10 QoS Action table properties

Property	Description	Action
Index	Uniquely identifies this table entry. This number identifies the instance of the QoS Action class.	Type a number to uniquely identify the action. You use this value to specify an action in the Policy table. See “Configuring policies” on page 76 .
Drop	Determines whether the matching frame should be dropped (True) or not dropped (False).	Choose True or False.

Table 10 QoS Action table properties (continued)

Property	Description	Action
Update DSCP	Updates the DS field of an associated IP datagram with a specified value. For example, 0x2f changes the DSCP value to the decimal value 47 in the match packet.	Type a hex value, or -1 to use the existing DSCP.
Set Drop Precedence	Specifies an IP drop precedence.	Choose a packet drop precedence value. <ul style="list-style-type: none"> • A value from 1-4 specifies a high drop precedence • A value from 5-8 specifies a low precedence. • Choose Use Default to leave the existing precedence.
Update Priority	Updates the user priority field with a specified value. Priority 1 specifies a low priority.	Choose from Priority 0 (lowest priority) to Priority 7 (highest priority), or choose Use Default to leave the existing priority.

Configuring policies

When the switch does not receive policy information from a DiffServ policy server in the network, use the Policy table to apply QoS policy filters. To define a policy, you match configured classification filters with interface role combinations, and assign a precedence order.

To configure the policies for a Business Policy Switch 2000:

- 1 In the navigation pane, expand the switch device and the QoS folder.
- 2 Select Policy Table.
- 3 Click the Properties tab to view the Policy table ([Figure 24](#)).

Figure 24 QoS Policy table

Index	Filter Group ID	Filter Group Type	Role Combination	Interface Direction	Order	Action Index
0		IP Filter Group		Ingress		

4 Use the information in [Table 11](#) to configure property values.

Table 11 QoS Policy table properties

Property	Description	Action
Index	Uniquely identifies the action for this policy.	Type a configured Index number from the Action table. See “Configuring filter actions” on page 75 .
Filter Group ID	Identifies the configured filter group for this policy.	Type the filter number from the IP or 802 Filter Group table. See “Configuring IP and Layer 2 filter groups” on page 74 .
Filter Group Type	Determines whether the filter group is an IP or 802 filter group.	Choose IP Filter Group or Layer 2 Filter Group.
Role Combination	Specifies the role combination to which this policy applies.	Type the role combination. See “Creating new role combinations” on page 79 .
Interface Direction	Indicates whether the policy is applied at ingress or egress.	None; this is a read-only property.
Order	Determines the order in which policies are applied. As packets are processed, the policy with the lowest order number performs the matching process first. If the traffic criteria does not match this policy, the next policy in order examines the traffic. Establish an ordering scheme that allows for modifications. For example, use multiples of 10 so you can insert policies in the appropriate filter order later.	After planning a system for ordering policies, type the number for this policy.
Action Index	Specifies the configured action to use for this policy.	Type the Index number of an action in the Action table. See “Configuring filter actions” on page 75 .

Configuring QoS interfaces

In a policy-enabled network, you can group device interfaces according to a logical function, rather than by the actual packet content of the network traffic they control. For example, a policy might apply only to Accounting department traffic, or to a certain building in an enterprise campus.

Role combination definitions map the physical interfaces on a switch to a logical function. To apply QoS policies, you assign switch ports to the appropriate roles (see [“Assigning ports to QoS roles” on page 81](#)). You can use one of the three default role combinations (see [“Predefined role combinations,”](#) next), or define new ones (see [“Creating new role combinations” on page 79](#)).



Note: You must apply interface role combinations whether the switch QoS software operates in dynamic mode with a COPS server, or in static mode using locally configured policies.

Predefined role combinations

Quick2Config includes the following predefined role combinations for the Business Policy Switch 2000:

- BPS Cascade Int Ifcs — Assigned by default to all cascade ports. Associates the ports with Queue Set 2 (Priority Queueing).
- BPS Hybrid Ext Ifcs — Assigned by default to all external switch ports. Associates the ports with Queue Set 1 (a hybrid of Weighted Fair Queueing and Priority Queueing).
- BPS Priority Ext Ifcs — Assigned by default to all Gigabit MDA ports. Associates the ports with Queue Set 2 (Priority Queueing).

The predefined role combinations consider all ports to be untrusted interfaces, except cascade ports connected to other Business Policy Switch units in the stack.

To view the interface queue configuration, see [“Viewing the Interface Queue table” on page 85](#).

Creating new role combinations

To add an interface role combination to the QoS Interface Configuration:

- 1 In the navigation pane, expand the QoS item.
- 2 Select Interface Configuration.
- 3 In the Palette tab, create a new Role Combination.
- 4 Click the Properties tab (Figure 25).

Figure 25 QoS Role Combination properties

Property	Value
Index	3
Role Combination	BPS Cascade Int l fcs
Queue Set	2
Capabilities	inputtpClassification input802Classification
Interface Class	Untrusted
Entry Storage	Read Only

- 5 Use the information in Table 12 to configure property values.

Table 12 QoS role combination properties

Property	Description	Action
Index	Uniquely identifies this role combination.	Type a number (0-63) to identify this interface type.
Role Combination	Classifies a set of physical interfaces in a group and maps a logical function to the interface group. You can then associate this role combination with the policy rules and actions of a particular queue set.	Type an identifying string (up to 255 characters) to describe the port's logical function. For example, you could classify the ports that handle traffic to and from the Accounting department with an Accounting role.

Table 12 QoS role combination properties (continued)

Property	Description	Action
Queue Set	<p>The queue set associated with this role combination:</p> <ul style="list-style-type: none"> Queue Set 1 has four queues. The first is serviced by a Priority Queuing discipline. The other three queues are serviced in a weighted round robin (Fair Queueing) fashion. Queue Set 2 has two queues that are serviced by a Priority Queuing discipline. 	Type the queue set ID, 1 or 2.
Capabilities	<p>The interface capabilities the policy server uses to select which policies and configurations to distribute to the switch. The Business Policy Switch 2000 capabilities are:</p> <ul style="list-style-type: none"> inputIpClassification outputIpClassification input802Classification output802Classification singleQueuingDiscipline hybridQueuingDiscipline Other 	None; this property is read-only.
Interface Class	<p>Determines whether the policy server considers this to be a trusted or untrusted interface.</p> <p>On untrusted interfaces, the DSCP value on incoming packets is re-marked and assigned to a queue according to the DSCP Mapping and Priority Mapping tables. See “User priority and DSCP mapping” on page 82.</p> <p>On trusted interfaces, the switch does not change a packet’s DSCP. The DSCP is used to assign 802.1p user priority, based on the Priority Queue Assignment table (“Viewing user priority assignments” on page 86).</p>	<p>Choose Trusted or Untrusted.</p> <p>Usually, trusted ports are trunk links, connected to the core of the DiffServ network. Untrusted ports are typically access links that are connected to end stations.</p>
Entry Storage	Determines whether the switch saves this row in non-volatile random access memory (NVRM), or loses the information at shutdown.	When this property is Read Only, all properties in the table are read-only.

Assigning ports to QoS roles

You identify interface groups by assigning a role to the ports that will filter traffic.



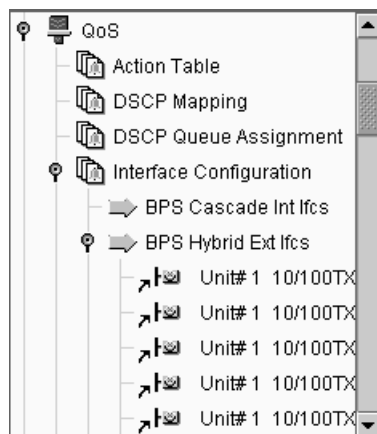
Note: All external switch ports are initially assigned to the predefined BPS Hybrid Ext Ifcs role combination.

To assign a QoS policy role for one or more switch port:

- 1 In the navigation pane, expand the QoS Interface Configuration item.
- 2 Select one or more switch ports.
- 3 Create shortcuts from the ports to a configured Role Combination.
 - a Right-click the selected ports, then choose Copy from the pop-up menu.
 - b In the navigation pane, select the Role Combination.
 - c Right-click, then choose Paste as Shortcut.

Figure 26 shows several ports assigned to the default role combination for external ports.

Figure 26 Ports assigned to a role combination



User priority and DSCP mapping

On untrusted interfaces in the packet forwarding path, the DSCP in the IP header is mapped to the IEEE 802.1p User Priority field in the IEEE 802.1Q frame, and both of these fields are mapped to an IP Layer 2 drop precedence value that determines the forwarding treatment at each network node along the path.

[Table 13](#) maps standard Nortel Networks IP class of service values to the 802.1p user priorities.

Table 13 Priority mapping for Nortel Networks IP service classes

IP service class	802.1p user priority
Network	7
Critical	7
Premium	6
Platinum	5
Gold	4
Silver	3
Bronze	2
Standard	0

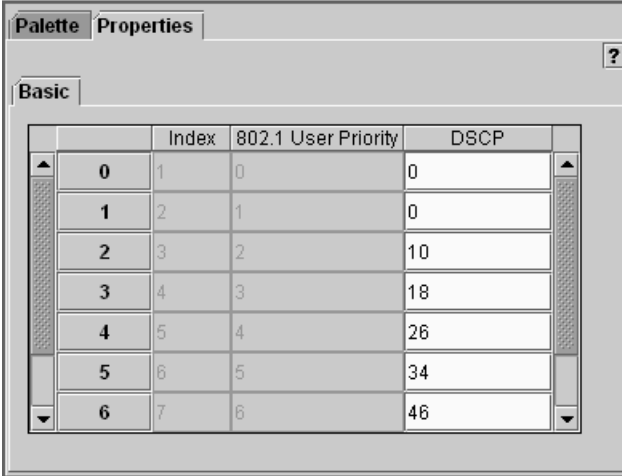
Configuring priority mapping

To assign the 802.1p user priority to map to a DSCP value at ingress:

- 1 In the navigation pane, expand the switch and the QoS folder.
- 2 Select Priority Mapping.

- 3 Click the Properties tab to view the Priority Mapping table (Figure 27).

Figure 27 QoS Priority Mapping table



	Index	802.1 User Priority	DSCP
0	1	0	0
1	2	1	0
2	3	2	10
3	4	3	18
4	5	4	26
5	6	5	34
6	7	6	46

- 4 In the DSCP column, type the DSCP value that you want to associate with the specified 802.1p user priority value.

Viewing DSCP mapping

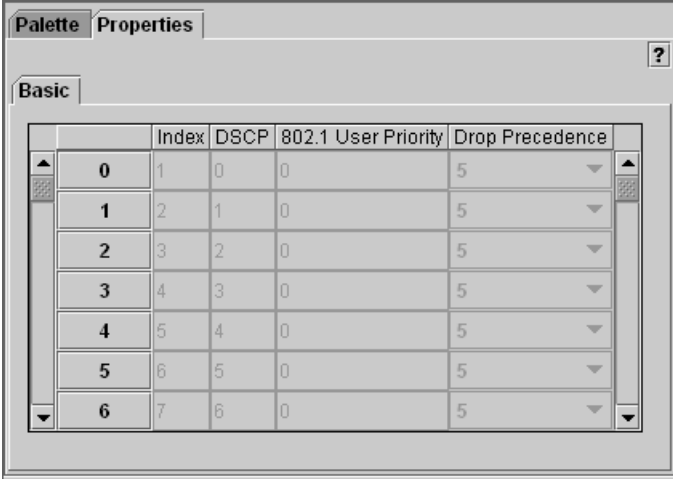
To view how DSCP values are mapped to 802.1p user priority and drop precedence values for your Business Policy Switch 2000:

- 1 In the navigation pane, expand the switch device and the QoS folder.
- 2 Select DSCP Mapping.

- Click the Properties tab to view the DSCP Mapping table ([Figure 28](#)).

DSCP codepoints 0 through 63 are mapped to specific user priority and drop precedence values.

Figure 28 QoS DSCP Mapping table



	Index	DSCP	802.1 User Priority	Drop Precedence
0	1	0	0	5
1	2	1	0	5
2	3	2	0	5
3	4	3	0	5
4	5	4	0	5
5	6	5	0	5
6	7	6	0	5

Viewing transmit queue information

The Interface Queue Table displays the QoS information configured for each interface transmit queue on the switch. To view the queueing information for each transmit queue, see [“Viewing the Interface Queue table,”](#) next.

The switch uses 802.1p user priority and DSCP values to assign egress traffic to the outbound interface queues.



Note: For packet prioritization in layer 2 switches that do not recognize DSCP but are able to process 802.1Q packets, an IEEE 802.1p class of service (CoS) user priority is added as packets are transmitted.

To view the priority and DSCP values assigned to each interface queue, see:

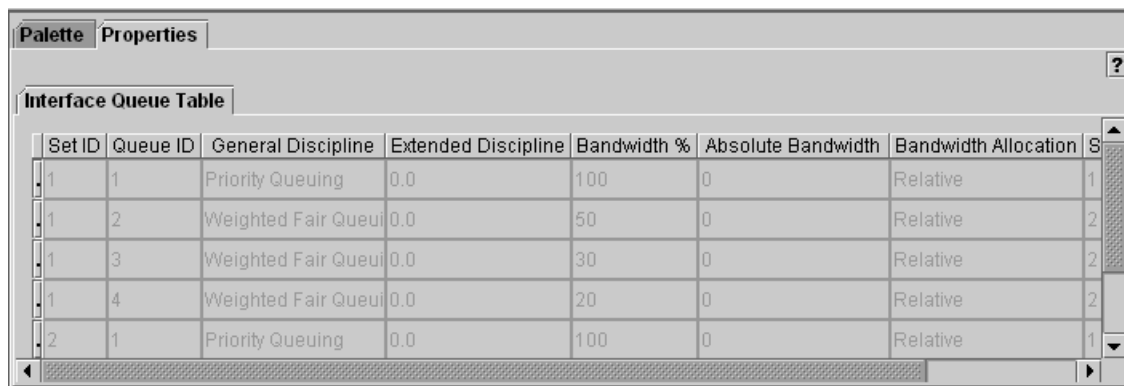
- [“Viewing user priority assignments” on page 86](#)
- [“Viewing DSCP assignments” on page 87](#)

Viewing the Interface Queue table

To view the Interface Queue table:

- 1 In the navigation pane, expand the switch device and the QoS folder.
- 2 Select Interface Configuration.
- 3 Click the Properties tab to view the Interface Queue table ([Figure 29](#)).

Figure 29 QoS Interface Queue table



Set ID	Queue ID	General Discipline	Extended Discipline	Bandwidth %	Absolute Bandwidth	Bandwidth Allocation	S
1	1	Priority Queuing	0.0	100	0	Relative	1
1	2	Weighted Fair Queueing	0.0	50	0	Relative	2
1	3	Weighted Fair Queueing	0.0	30	0	Relative	2
1	4	Weighted Fair Queueing	0.0	20	0	Relative	2
2	1	Priority Queuing	0.0	100	0	Relative	1

[Table 14](#) describes the information in the Interface Queue table. This information is read-only.

Table 14 QoS Interface Queue table properties

Property	Description
Set ID	Specifies whether this queue is one of the four queues in Queue Set 1, or one of the two queues in Queue Set 2. See Table 12 on page 79 .
Queue ID	Combined with the Queue Set ID, uniquely identifies the queue.
General Discipline	The type of queueing associated with the queue. Values are: <ul style="list-style-type: none"> First In First Out Queueing Priority Queueing Fair Queueing (round-robin) Weighted Fair Queueing Other (see Extended Discipline)
Extended Discipline	Specifies a queueing mechanism not listed as a General Discipline option.

Table 14 QoS Interface Queue table properties (continued)

Property	Description
Bandwidth %	The percent of allocated bandwidth used by this queue.
Absolute Bandwidth	The maximum interface bandwidth that is available for consumption when servicing this queue.
Bandwidth Allocation	The absolute bandwidth limit, or a bandwidth limit that is relative to other queues of the interface.
Service Order	The queue's level of priority.
Size	The size of the queue, in bytes.

Viewing user priority assignments

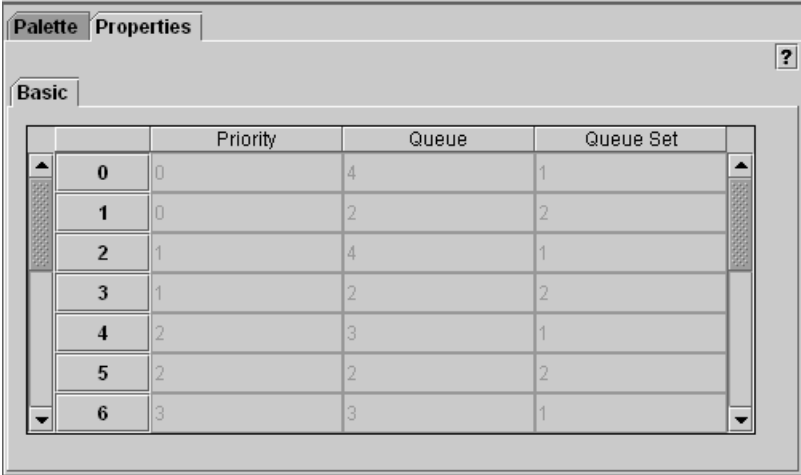
Packets that require the highest class of service are assigned to the highest priority queue; packets that use best-effort or tiered service are assigned to the other transmit queues.

To view the 802.1p user priority assignments for the switch queues:

- 1 In the navigation pane, expand the switch and QoS icons.
- 2 Click Priority Queue Assignment.

- 3 Click the Properties tab to open the Priority Queue Assignment table (Figure 30).

Figure 30 QoS Priority Queue Assignment table



	Priority	Queue	Queue Set
0	0	4	1
1	0	2	2
2	1	4	1
3	1	2	2
4	2	3	1
5	2	2	2
6	3	3	1

Each 802.1p user priority value is assigned to a queue and queue set pair.

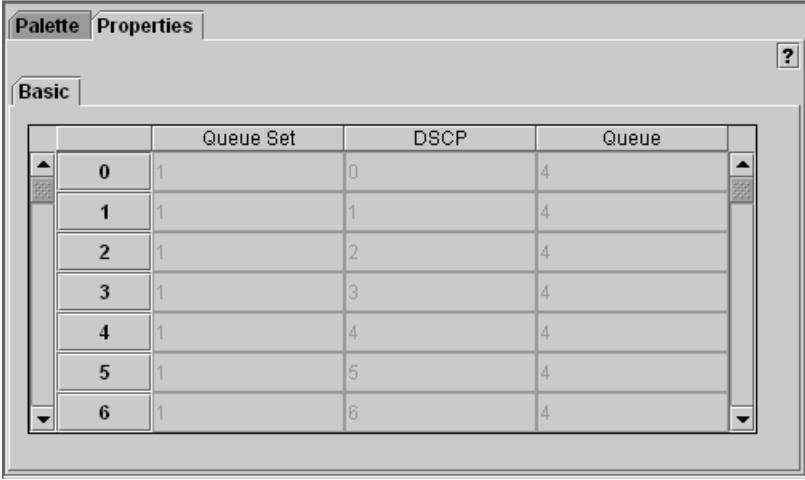
Viewing DSCP assignments

Each DSCP value is assigned to an interface queue. To view the DSCP queue assignments:

- 1 In the navigation pane, expand the QoS folder.
- 2 Click Priority Queue Assignment.

- 3 Click the Properties tab (Figure 31).

Figure 31 QoS DSCP Assignment table



	Queue Set	DSCP	Queue
0	1	0	4
1	1	1	4
2	1	2	4
3	1	3	4
4	1	4	4
5	1	5	4
6	1	6	4

DSCP values (0-63) are assigned to a queue and queue set pair.

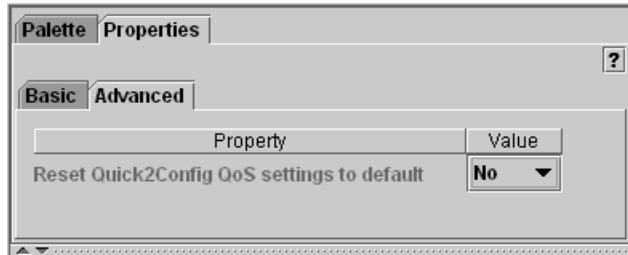
Resetting QoS values in Quick2Config

If you want to cancel the changes you made during a Quick2Config session, you can reset the Quick2Config database. To reset the QoS properties to default values within Quick2Config:

- 1 In the navigation pane, expand the switch.
- 2 Select QoS.
- 3 In the Properties tab, click Advanced.

- 4 From the Reset Quick2Config QoS settings to default list, choose Yes (Figure 32).

Figure 32 QoS Advanced tab



Appendix A

Downloading image files

You can use Quick2Config to download image files—one at a time—from a TFTP server to Business Policy Switch 2000 or BayStack 450 switches in your network. The procedure is the same for both device types.

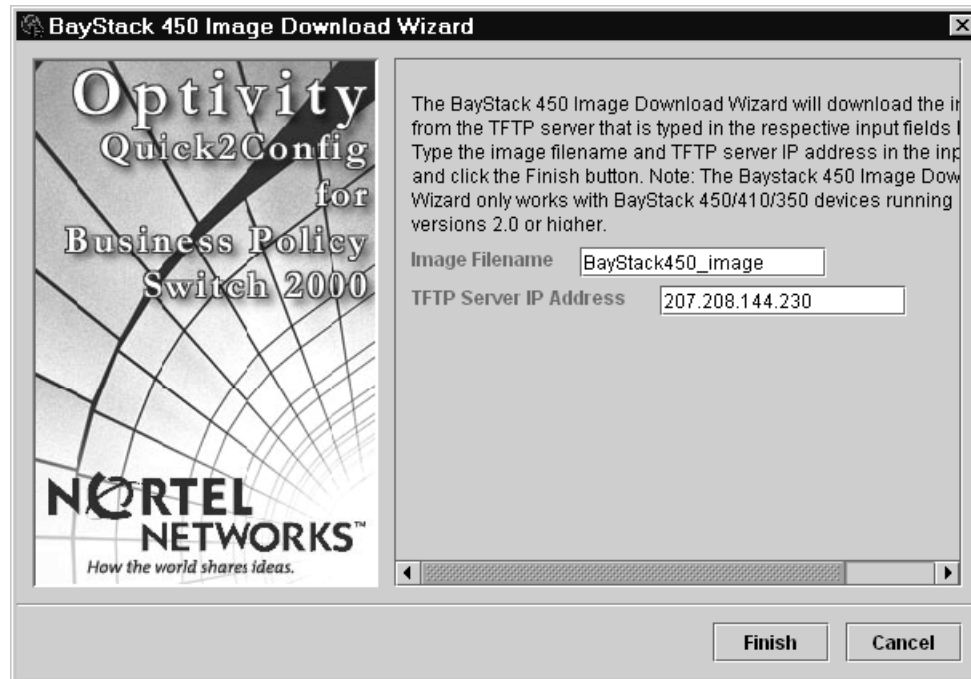


Note: Certain BayStack software releases require that you download two images: the boot code image and the agent image. For proper operation of the switch, use the Image Download Wizard to download the new boot code image first; then, download the agent image.

To download an image file to a Business Policy Switch 2000 or BayStack 450 Product Group device:

- 1 Copy the image file you want to download to a TFTP server.
- 2 In the navigation pane, select the switch to which you want to download the image file.
- 3 Right-click, and then choose Run Wizard > Business Policy Switch 2000 Image Download Wizard.

The Image Download Wizard opens ([Figure 33](#)).

Figure 33 Image Download Wizard

- 4 Type the name of the image file.
 - 5 Type the IP address of the TFTP server where you copied the file.
 - 6 Click Finish.
- Quick2Config downloads the image file from the TFTP server to the switch.

Index

Numbers

802.1p user priority
 Nortel Networks service classes 82
 Priority Mapping table 82
 queue assignment 84

802.1Q frame tagging
 configuring 44
 MLT and 52

A

access port, VLAN
 about 37
 default configuration 44
 QoS and 80

acronyms 16

address

 IP subnet 22
 switch gateway 22
 switch IP 22
 VLAN subnet 36

ATM Forum LAN emulation (LANE) 27

ATM, BayStack 450 MDA 27

autonegotiation, port line speed 26

B

BayStack 450 ATM MDAs 27

BayStack product group
 supported features 24
 supported models 15
 VLAN support 36

boot code image 91

C

classifications, QoS

 about 62
 Layer 2 71
 Layer 3 70

codepoint, DiffServ 63

Common Open Policy Services (COPS)

 about 62, 67
 configuring 67
 retry settings 68

configuration rules

 Ethernet ports 27
 IGMP snooping 47
 initial switch setup 22
 MLT 52

configurations

 adding 22
 exporting 32
 importing 22

connections, VLAN 37

conventions, text 15

Cost of Service drop precedence mappings 82

customer support 19

D

DiffServ

 architecture 62
 codepoint (DSCP) 63, 82

drop precedence mappings 82

E

emulated LAN (ELAN) 29

Ethernet ports 26

F

filters, QoS 61, 69

frame tagging

 configuring 44

 VLAN ports 44

full duplex operation 27

G

gateway address 22

H

half duplex operation 27

I

IGMP snooping

 about 46

 configuration rules 47

 enabling 48

Image Download Wizard 92

image file, downloading 91

independent VLAN learning (IVL) 39, 41, 42

Interface Type table, QoS 85

interfaces, QoS 78

IP

 configuring 30

 QoS Filter Group table 74

 QoS Filter table 70

 switch address 22

L

LAN emulation client (LEC) 27, 29

Layer 2 classifications, QoS 71

Layer 3 classifications, QoS 70

LEC, ATM MDA ports 29

M

MAC SA-based VLAN 36, 41

media dependent adapter (MDA) hardware 24

multilink trunk (MLT)

 about 51

 configuration rules 52

 creating group 53

 properties 53

P

packet

 classifications 62

 dropping 62

 marking 62

Palette templates 23

policy agent, QoS 65

policy filters

 about 61

 configuring

 actions 75

 interfaces 78

 precedence 76

 configuring classifications 69

 DSCP mapping 44

 management agent 65

ports

 ATM MDA 27, 28

 Ethernet 27

 QoS 79

 static router 46, 49

 STP 55

 trusted 80

 untrusted 80

 VLAN 36, 43

product support 19

properties

- ATM MDA ports 28
- basic switch 25
- Ethernet port 26
- IGMP 48
- IP 30
- MAC-based VLAN 42
- MLT 53
- protocol-based VLAN 40
- QoS
 - 802 Filter Group table 72, 74
 - Action table 75
 - DSCP Mapping table 84
 - Interface Queue table 85
 - Interface Type table 67, 69, 79
 - IP Filter Group table 74
 - IP Filter table 70
 - policy agent 65
- SNMP 31
- STP group 58
- system 25
- protocol-based VLAN 40
- proxy reports 46
- publications, hard copy 19

Q

- Quality of Service (QoS) 80
 - 802 Filter Group table 72, 74
 - DSCP mapping 83
 - filter actions 75
 - filters and filter groups 69
 - Interface Type table 85
 - interfaces 78
 - IP Filter Group table 74
 - IP Filter table 70
 - Layer 2 classifications 71
 - overview 61
 - policy agent 65
 - ports 79
 - role combinations 79
 - predefined 78
 - Target table 76

R

- role combination, QoS 78, 79

S

- shared VLAN learning (SVL) 39, 41, 42
- SNMP
 - authentication failure 32
 - community strings 31
 - trap receivers 31, 32
- Spanning Tree Protocol (STP)
 - designated root 58
 - disabling 57
 - group properties 58
 - learning state 56
 - ports 55
- static router ports 46, 49
- support, Nortel Networks 19
- switch information
 - editing 24
 - exporting 32
 - importing 22
- system information, changing 24

T

- tagging, IEEE 802.1q frame 44
- Target table, QoS 76
- technical publications 19
- technical support 19
- text conventions 15
- TFTP
 - and image download 92
 - option on the Quick2Config File menu 32
- traps, SNMP 31
- trunk port, VLAN
 - about 37
 - configuring 44
 - QoS and 80
- trunk, MLT 51

trusted and untrusted ports 80

U

untagged frames 44

untrusted ports 80

V

virtual local area networks (VLANs)

- configuration steps 38

- connections 37

- learning type 39, 41, 42

- MAC-based 36

- port-based 36

- ports 39, 40, 43

- protocol-based 40

- types 36

- validation at export 33