

Part No. 217328-A  
February 2005

4655 Great America Parkway  
Santa Clara, CA 95054

# **Web Management for Nortel Ethernet Routing Switch 3510-24T, Software Release 4.0.3**



**NORTEL**

## Copyright © 2005 Nortel Networks

All rights reserved. February 2005.

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

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

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

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

Java is a trademark of Sun Microsystems, Inc.

Cisco is a trademark of Cisco Systems, Inc.

The asterisk after a name denotes a trademarked item.

### Restricted rights legend

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

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

### Statement of conditions

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

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

### International regulatory statements of conformity

This is to certify that the Nortel Ethernet Routing Switch 3510-24T was evaluated to the international regulatory standards for electromagnetic compliance (EMC) and safety and were found to have met the requirements for the following international standards:

- EMC - Electromagnetic Emissions – CISPR 22, Class A
- EMC - Electromagnetic Immunity – CISPR 24
- Electrical Safety – IEC 60950, with CB member national deviations

Further, the equipment has been certified as compliant with the national standards as detailed below.

---

## National electromagnetic compliance (EMC) statements of compliance

### FCC statement (USA only)

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the Federal Communications Commission (FCC) rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy. If it is not installed and used in accordance with the instruction manual, it may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to take whatever measures may be necessary to correct the interference at their own expense.

### ICES statement (Canada only)

#### Canadian Department of Communications Radio Interference Regulations

This digital apparatus (Nortel Ethernet Routing Switch 3510-24T) does not exceed the Class A limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

#### Règlement sur le brouillage radioélectrique du ministère des Communications

Cet appareil numérique (Nortel Ethernet Routing Switch 3510-24T) respecte les limites de bruits radioélectriques visant les appareils numériques de classe A prescrites dans le Règlement sur le brouillage radioélectrique du ministère des Communications du Canada.

### CE marking statement (Europe only)

#### EN 55 022 statements

This is to certify that the Nortel Ethernet Routing Switch 3510-24T is shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC. Conformity is declared by the application of EN 55 022 Class A (CISPR 22).



**Caution:** This device is a Class A product. In a domestic environment, this device can cause radio interference, in which case the user may be required to take appropriate measures.

---

#### EN 55 024 statement

This is to certify that the Nortel Ethernet Routing Switch 3510-24T switches is shielded against the susceptibility to radio interference in accordance with the application of Council Directive 89/336/EEC. Conformity is declared by the application of EN 55 024 (CISPR 24).

#### EC Declaration of Conformity

This product conforms to the provisions of the R&TTE Directive 1999/5/EC.

**VCCI statement (Japan/Nippon only)**

This is a Class A product based on the standard of the Voluntary Control Council for Interference (VCCI) for information technology equipment. If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

**BSMI statement for Nortel Ethernet Routing Switch 3510-24T (Taiwan only)**

This is a Class A product based on the standard of the Bureau of Standards, Metrology and Inspection (BSMI) CNS 13438, Class A.

**警告使用者：**

這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

**MIC notice for Nortel Ethernet Routing Switch 3510-24T (Republic of Korea only)**

This device has been approved for use in Business applications only per the Class A requirements of the Republic of Korea Ministry of Information and Communications (MIC). This device may not be sold for use in a non-business application.

Observe the Regulatory Marking label on the bottom surface of the chassis for specific certification information pertaining to this model. Each model in the Nortel Ethernet Routing Switch which is approved for shipment to/usage in Korea is labeled as such, with all appropriate text and the appropriate MIC reference number.

**National safety statements of compliance****CE marking statement (Europe only)****EN 60 950 statement**

This is to certify that the Nortel Ethernet Routing Switch 3510-24T is in compliance with the requirements of EN 60 950 in accordance with the Low Voltage Directive. Additional national differences for all European Union countries have been evaluated for compliance.

---

## **NOM statement Nortel Ethernet Routing Switch 3510-24T (Mexico only)**

The following information is provided on the devices described in this document in compliance with the safety requirements of the Norma Oficial Mexicana (NOM):

Exporter: Nortel Networks, Inc.  
4655 Great America Parkway  
Santa Clara CA 95054 USA

Importer: Nortel Networks de México, S.A. de C.V.  
Avenida Insurgentes Sur #1605  
Piso 30, Oficina  
Col. San Jose Insurgentes  
Deleg-Benito Juarez  
México D.F. 03900

Tel: 52 5 480 2100

Fax: 52 5 480 2199

Input: Nortel Ethernet Routing Switch 3510-24T  
100 - 240 VAC 50/60 Hz 1.3A max

### **Información NOM (unicamente para México)**

La información siguiente se proporciona en el dispositivo o en los dispositivos descritos en este documento, en cumplimiento con los requisitos de la Norma Oficial Mexicana (NOM):

Exportador: Nortel Networks, Inc.  
4655 Great America Parkway  
Santa Clara, CA 95054 USA

Importador: Nortel Networks de México, S.A. de C.V.  
Avenida Insurgentes Sur #1605  
Piso 30, Oficina  
Col. San Jose Insurgentes  
Deleg-Benito Juarez  
México D.F. 03900

Tel: 52 5 480 2100

Fax: 52 5 480 2199

Embarcar a: Nortel Ethernet Routing Switch 3510-24T  
100 - 240 VAC 50/60 Hz 1.3A max

## Nortel Networks Inc. software license agreement

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

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

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

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

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

### 4.General

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

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

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

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

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

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

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

## Revision History

Date Revised	Version	Reason for revision
February 2005	1.0	Nortel Ethernet Routing Switch 3510-24T.

---

# Contents

---

<b>Preface</b> .....	<b>23</b>
Before you Begin .....	23
Text conventions .....	24
Related Publications .....	24
How to Get Help .....	25
<b>Chapter 1</b>	
<b>Using the Web-based Management Interface</b> .....	<b>27</b>
Requirements .....	27
Logging in to the Web-based Management Interface .....	28
Web Page Layout .....	29
Menu .....	29
Management Page .....	32
<b>Chapter 2</b>	
<b>Administering the switch</b> .....	<b>35</b>
Viewing General Information .....	35
Viewing System Information .....	35
Configuring System Security .....	37
Setting Console, Telnet, and Web Passwords .....	37
Configuring RADIUS Security .....	39
Logging on to the Web Management Interface .....	40
Resetting the Ethernet Routing Switch .....	42
Resetting the Ethernet Routing Switch to system defaults .....	44
Logging out of the Management Interface .....	45

---

<b>Chapter 3</b>	
<b>Viewing Summary Information</b> .....	<b>47</b>
Viewing Summary Switch Information .....	47
<b>Chapter 4</b>	
<b>Configuring the Switch</b> .....	<b>51</b>
Configuring BootP, IP, and Gateway Settings .....	52
Modifying System Settings .....	55
Managing Remote Access by IP Address .....	56
Simple Network Management Protocol .....	58
Configuring SNMPv1 .....	58
Configuring SNMPv3 .....	60
SNMPv3 Table Entries Stored in NVRAM .....	60
Viewing SNMPv3 System Information .....	61
Configuring User Access to SNMPv3 .....	63
Creating an SNMPv3 system user configuration .....	64
Deleting an SNMPv3 System User Configuration .....	66
Configuring an SNMPv3 System User Group Membership .....	66
Mapping an SNMPv3 System User to a Group .....	66
Deleting an SNMPv3 group membership configuration .....	68
Configuring SNMPv3 Group Access Rights .....	69
Creating an SNMPv3 Group Access Rights Configuration .....	69
Deleting an SNMPv3 Group Access Rights Configuration .....	71
Configuring an SNMPv3 Management Information View .....	72
Creating an SNMPv3 Management Information View Configuration .....	72
Deleting an SNMPv3 Management Information View Configuration .....	74
Configuring an SNMPv3 System Notification Entry .....	75
Creating an SNMPv3 System Notification Configuration .....	75
Deleting an SNMPv3 System Notification Configuration .....	77
Configuring an SNMPv3 Management Target Address .....	78
Creating an SNMPv3 Target Address Configuration .....	78
Deleting an SNMPv3 Target Address Configuration .....	80
Configuring an SNMPv3 Management Target Parameter .....	80
Creating an SNMPv3 Target Parameter Configuration .....	80
Deleting an SNMPv3 Target Parameter Configuration .....	82

---

Configuring SNMP Traps .....	83
Creating an SNMP Trap Receiver Configuration .....	83
Deleting an SNMP Trap Receiver Configuration .....	84
Configuring EAPOL-based Security .....	85
Configuring MAC Address-based Security .....	88
Configuring MAC Address-based Security .....	89
Enabling Security on Ports .....	91
Deleting Ports .....	93
Port Lists .....	93
Adding MAC Addresses .....	96
Clearing Ports .....	98
Filtering MAC Destination Addresses .....	99
Deleting MAC DAs .....	101
Viewing Learned MAC Addresses by VLAN .....	101
Locating a Specific MAC Address .....	103
Configuring Port's Autonegotiation, Speed, Duplex, Status, and Alias .....	104
Configuring High Speed Flow Control .....	107
Downloading Switch Images .....	109
Storing and Retrieving Switch Configuration File from TFTP Server .....	111
Configuring Port Communication Speed .....	113
<b>Chapter 5</b>	
<b>Configuring Remote Network Monitoring .....</b>	<b>117</b>
Configuring RMON Fault Threshold Parameters .....	117
Creating an RMON Fault Threshold .....	117
Deleting an RMON Threshold Configuration .....	120
Viewing the RMON Fault Event Log .....	121
Viewing the System Log .....	122
Viewing RMON Ethernet Statistics .....	124
Viewing RMON History .....	127
<b>Chapter 6</b>	
<b>Viewing System Statistics .....</b>	<b>131</b>
Viewing Port Statistics .....	131
Zeroing Ports .....	134

---

Viewing all Port Errors .....	134
Viewing Interface Statistics .....	136
Viewing Ethernet Error Statistics .....	138
Viewing Transparent Bridging Statistics .....	140
<b>Chapter 7</b>	
<b>Configuring Application Settings .....</b>	<b>143</b>
Configuring Port Mirroring .....	143
Configuring Rate Limiting .....	147
Configuring IGMP .....	150
Viewing Multicast Group Membership Configurations .....	153
Creating and Managing Virtual LANs .....	154
Port-based VLANs .....	155
Protocol-based VLANs .....	155
Configuring VLANs .....	155
Creating a Port-based VLAN .....	157
Modifying a Port-based VLAN .....	159
Creating a Protocol-based VLAN .....	160
Modifying a Protocol-based VLAN .....	164
Selecting a Management VLAN .....	166
Deleting a VLAN Configuration .....	166
Configuring Broadcast Domains .....	167
Viewing VLAN Port Information .....	168
Managing Spanning Tree Groups .....	170
Creating Spanning Tree Groups .....	171
Modifying Spanning Tree Groups .....	174
Deleting a Spanning Tree Group .....	176
Associating STG with VLAN Membership .....	177
Configuring Ports for Spanning Tree .....	179
Changing Spanning Tree Bridge Switch Settings .....	181
Configuring MultiLink Trunk Members .....	184
Monitoring MLT Traffic .....	187

---

<b>Chapter 8</b>	
<b>Implementing QoS</b>	<b>189</b>
Configuring an Interface Group	190
Creating an Interface Group Configuration	190
Displaying Interface ID Table	193
Adding or Removing Interface Group Members	195
Deleting Ports or an Entire Interface Group Configuration	196
Configuring 802.1p Priority Queue Assignment	197
Configuring 802.1p Priority Mapping	199
Configuring DSCP Mapping	200
Configuring IP Classifier Elements	203
Creating an IP Classifier Element	204
Deleting an IP Classifier Element Configuration	209
Configuring Layer 2 Classifier Elements	209
Creating a Layer 2 Classifier Element Configuration	210
Deleting a Layer 2 Classifier Element Configuration	215
Classifier Configurations	216
Creating Classifiers	217
Viewing Classifier Details	218
Deleting a Classifier	219
Classifier Block Configurations	220
Creating Classifier Blocks	221
Modifying a Classifier Block	222
Deleting a Classifier Block	223
Configuring QoS Actions	224
Creating an Action Configuration	224
Modifying an Action Configuration	227
Deleting an Action Configuration	228
Using the Interface Action Extension	229
Creating an Interface Action Extension Configuration	229
Deleting an Interface Action Extension Configuration	231
Configuring QoS Meters	232
Creating a Meter	232
Viewing Meters	234
Deleting a Meter	235

---

Configuring QoS Policies .....	235
Installing Defined Filters .....	236
Viewing Hardware Policy Statistics .....	238
Deleting a Hardware Policy Configuration .....	240
Configuring QoS Policy Agent Characteristics .....	241
Using QoS Diagnostics .....	243
<b>Chapter 9</b>	
<b>Support Menu .....</b>	<b>251</b>
Using the Online Help Option .....	251
Downloading Technical Publications .....	252
Manuals Option .....	254
Upgrade Option .....	255
<b>Index .....</b>	<b>257</b>

---

# Figures

---

Figure 1	Web-based management interface home page	28
Figure 2	Web page layout	29
Figure 3	Console page	32
Figure 4	System Information home page	36
Figure 5	Console Password setting page	38
Figure 6	RADIUS page	39
Figure 7	Web-based management interface log on page	41
Figure 8	System Information home page	42
Figure 9	Reset page	43
Figure 10	Reset to Default page	44
Figure 11	Switch Information page	48
Figure 12	IP page for a Ethernet Routing Switch	52
Figure 13	System page	55
Figure 14	Remote Access page	57
Figure 15	SNMPv1 page	59
Figure 16	System Information page	62
Figure 17	User Specification page	64
Figure 18	Group Membership page	67
Figure 19	Group Access Rights page	70
Figure 20	Management Information View page	73
Figure 21	Notification page	76
Figure 22	Target Address page	78
Figure 23	Target Parameter page	81
Figure 24	SNMP Trap Receiver page	83
Figure 25	EAPOL Security Configuration page	86
Figure 26	Security Configuration page	89
Figure 27	Port Configuration page	92
Figure 28	Port Lists page	94
Figure 29	Port List View, Port List page	95

---

Figure 30	Port List View, Learn by Ports page	96
Figure 31	Security Table page	97
Figure 32	Port List View, Clear by Ports page	99
Figure 33	DA MAC Filtering page	100
Figure 34	MAC Address Table page	102
Figure 35	Find MAC Address Table page	103
Figure 36	Port Management page	105
Figure 37	High Speed Flow Control page	107
Figure 38	Software Download page	110
Figure 39	Configuration File Download/Upload page	112
Figure 40	Console/Communication Port page	114
Figure 41	RMON Threshold page	118
Figure 42	RMON Event Log page	122
Figure 43	System Log page	123
Figure 44	RMON Ethernet page (1 of 2)	125
Figure 45	RMON Ethernet page (2 of 2)	126
Figure 46	RMON History page	128
Figure 47	Port page	132
Figure 48	Port Error Summary page	135
Figure 49	Interface page	137
Figure 50	Ethernet Errors page	139
Figure 51	Transparent Bridging page	141
Figure 52	Port Mirroring page	144
Figure 53	Rate Limiting page	148
Figure 54	IGMP Configuration page	150
Figure 55	IGMP: VLAN Configuration page	151
Figure 56	IGMP Multicast Group Membership page	153
Figure 57	VLAN Configuration page	156
Figure 58	VLAN Configuration: Port Based setting page	158
Figure 59	VLAN Configuration: Port Based modification page	159
Figure 60	VLAN Configuration: Protocol Based setting page	161
Figure 61	VLAN Configuration: Protocol Based modification page	165
Figure 62	Port Configuration page	167
Figure 63	Port Information page	169
Figure 64	Spanning Tree Group Configuration page	172

---

Figure 65	Group Configuration modification page	175
Figure 66	Spanning Tree VLAN Membership page	177
Figure 67	Spanning Tree Add VLAN page	178
Figure 68	Spanning Tree Remove VLAN page	178
Figure 69	Spanning Tree Port Configuration page	179
Figure 70	Spanning Tree Bridge Information page	182
Figure 71	Group page	185
Figure 72	Utilization page	187
Figure 73	QoS Interface Configuration page	191
Figure 74	Interface ID page	194
Figure 75	Interface Group Assignment page	195
Figure 76	802.1p Priority Queue Assignment page	198
Figure 77	802.1p Priority Mapping page	199
Figure 78	DSCP Mapping page	201
Figure 79	DSCP Mapping Modification page	202
Figure 80	IP Classifier Element page (1 of 2)	205
Figure 81	IP Classifier Element page (2 of 2)	205
Figure 82	Layer2 Classifier Element page	210
Figure 83	Classifier page	216
Figure 84	Classifier Creation page	217
Figure 85	Classifier View page	219
Figure 86	Classifier Block page	220
Figure 87	Classifier Block Creation/Modification page	221
Figure 88	Classifier Creation/Block Modification page	223
Figure 89	Action page	225
Figure 90	Action Modification page	228
Figure 91	Interface Action Extension page	230
Figure 92	Meter page	233
Figure 93	Policy page	236
Figure 94	Policy Statistics page	239
Figure 95	Agent page (1 of 2)	241
Figure 96	Agent page (2 of 2)	242
Figure 97	Diagnostics page (1 of 3)	244
Figure 98	Diagnostics page (2 of 3)	245
Figure 99	Diagnostics page (3 of 3)	246

Figure 100	Diagnostics value and mask display for selected range . . . . .	248
Figure 101	Diagnostics rule and mask display for selected classifier . . . . .	249
Figure 102	Online help window . . . . .	252
Figure 103	Nortel Technical Documentation Web site . . . . .	253
Figure 104	Nortel technical Documentation Web site . . . . .	254
Figure 105	Nortel Customer Support Web site . . . . .	255

---

## Tables

---

Table 1	Main headings and options .....	30
Table 2	Menu icons .....	31
Table 3	Page buttons and icons .....	33
Table 4	System Information page items .....	37
Table 5	Console page items .....	38
Table 6	RADIUS page items .....	39
Table 7	User levels and access levels .....	42
Table 8	Switch Information page fields .....	48
Table 9	IP page items .....	53
Table 10	System page items .....	55
Table 11	Remote Access page fields .....	57
Table 12	SNMPv1 page items .....	60
Table 13	System Information section fields .....	62
Table 14	SNMPv3 Counters section fields .....	63
Table 15	User Specification Table section items .....	65
Table 16	User Specification Creation section items .....	65
Table 17	Group Membership page items .....	67
Table 18	Group Access Rights page items .....	71
Table 19	Management Information View page items .....	73
Table 20	Notification page items .....	76
Table 21	Target Address page items .....	79
Table 22	Target Parameter page items .....	81
Table 23	SNMP Trap Receiver page items .....	84
Table 24	EAPOL Security Configuration page fields .....	86
Table 25	Security Configuration page items .....	90
Table 26	Port Configuration page items .....	92
Table 27	Ports Lists page items .....	94
Table 28	Security Table page items .....	97
Table 29	DA MAC Filtering page items .....	100

---

Table 30	MAC Address Table page items	102
Table 31	Find MAC Address Table page items	104
Table 32	Port Management page items	106
Table 33	High Speed Flow Control page items	108
Table 34	Software Download page items	110
Table 35	Configuration File page items	112
Table 36	Requirements for retrieving configuration parameters on TFTP server	113
Table 37	Parameters not saved to the configuration file	113
Table 38	Console/Communication Port Setting page items	114
Table 39	RMON Threshold page items	118
Table 40	RMON Event Log page fields	122
Table 41	System Log page fields	123
Table 42	RMON Ethernet page items	126
Table 43	RMON History page items	128
Table 44	Port page items	132
Table 45	Port Error Summary Table fields	135
Table 46	Interface page items	137
Table 47	Ethernet Errors page items	139
Table 48	Transparent Bridging page items	141
Table 49	Port Mirroring page items	145
Table 50	Port-based monitoring modes	146
Table 51	Address-based monitoring modes	147
Table 52	Rate Limiting page items	148
Table 53	IGMP Configuration page items	150
Table 54	IGMP: VLAN Configuration page items	152
Table 55	IGMP Multicast Group Membership page items	154
Table 56	VLAN Configuration page items	157
Table 57	VLAN Configuration: Port Based setting page items	158
Table 58	VLAN Configuration: Port Based modification page items	159
Table 59	VLAN Configuration: Protocol Based setting page items	161
Table 60	Standard protocol-based VLANs and PID types	162
Table 61	Predefined Protocol Identifier (PID)	164
Table 62	VLAN Configuration: Protocol Based modification page items	165
Table 63	Port Configuration page items	168
Table 64	Port Information page items	169

---

Table 65	Spanning Tree Group Configuration page items	173
Table 66	Spanning Tree Group Configuration modification page items	175
Table 67	Spanning Tree Port Configuration page items	180
Table 68	Spanning Tree Bridge Information page items	182
Table 69	Group page items	186
Table 70	Utilization page items	188
Table 71	QoS Interface Queue Table section items	191
Table 72	Interface Group Table section items	192
Table 73	Interface Group Creation section page items	193
Table 74	Interface ID page items	194
Table 75	Interface Group Assignment page items	196
Table 76	802.1p Priority Assignment Table section page items	198
Table 77	802.1p Priority Mapping page items	200
Table 78	DSCP Mapping page items	201
Table 79	DSCP Mapping Modification page items	202
Table 80	IP Classifier Element Table and Classifier Element Creation	206
Table 81	Layer2 Classifier Element Table and Layer2 Classifier Element Creation	211
Table 82	Classifier Page items	216
Table 83	Classifier Block Page items	221
Table 84	Action page items	225
Table 85	Interface Action Extension page items	230
Table 86	Meter Creation fields	233
Table 87	Meter Table fields	234
Table 88	Policy page items	237
Table 89	Policy Statistics page items	239
Table 90	Filter Statistics table items	240
Table 91	Agent page items	242
Table 92	Diagnostics page items	246



---

## Preface

---

Welcome to the Web Management for the Nortel\* Ethernet Routing Switch 3510-24T, Software Release 4.0.3. This document provides instructions on configuring and managing the Nortel Ethernet Routing Switch 3510-24T through the Web browser.

The Web-based management interface is one of the many tools specifically designed to assist the network manager in creating complex standalone or network configurations.

In addition to the Web-based management system discussed in this book, you can manage the Ethernet Routing Switch by using Simple Network Management Protocol (SNMP), the Nortel Command Line Interface (NCLI), Device Manager (DM), or the Console Interface (CI) menus.

Refer to the documents listed in the [“Related Publications” on page 24](#) for information on using and managing the Ethernet Routing Switch.

This guide describes how to use the Web-based management user interface to configure and maintain the Ethernet Routing Switch and the devices connected within its framework.

## Before you Begin

This guide is intended for network managers who are responsible for configuring the Ethernet Routing Switch. Consequently, this guide assumes prior knowledge and understanding of the terminology, theories, practices, and specific knowledge about networking devices, protocols, and interfaces that comprise your network.

You should have working knowledge of the Windows\* operating system, Graphical User Interfaces (GUIs), and Web browsers.

## Text conventions

This guide uses the following text conventions:

italic text	Indicates new terms and book titles.
separator (>)	Shows menu paths. Example: Configuration > Port Management identifies the Port Management option on the Configuration menu.

## Related Publications

For more information on using the Web-based management user interface and the Ethernet Routing Switch, refer to the following publications:

- *Release Notes for Nortel Ethernet Routing Switch 3510-24T, Software Release 4.0.3* (part number 217331-A)  
Documents important changes about the software and hardware that are not covered in other related publications.
- *Installing the Nortel Ethernet Routing Switch 3510-24T, Software Release 4.0.3* (part number 217326-A)  
Describes how to install the Ethernet Routing Switch.
- *Application Guide for Nortel Ethernet Routing Switch 3510-24T, Software Release 4.0.3* (part number 217327-A)  
Describes how to use the Ethernet Routing Switch.
- *NCLI Configuration Guide for Nortel Ethernet Routing Switch 3510-24T, Software Release 4.0.3* (part number 217330-A)  
Describes how to use Nortel Command Line Interface (NCLI) commands to configure and manage the Ethernet Routing Switch.
- *Switch Management for Nortel Ethernet Routing Switch 3510-24T, Software Release 4.0.3* (part number 217329-A)  
Describes how to use the Java-based device-level software management application.

You can print selected technical manuals and release notes free, directly from the Internet. Go to [www.nortel.com/support](http://www.nortel.com/support). 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](http://www.adobe.com) to download a free copy of the Adobe Acrobat Reader.

## How to Get Help

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

If you have purchased a Nortel service program, contact Nortel Technical Support. To obtain contact information online, go to [www.nortel.com/support](http://www.nortel.com/support), and then click on Technical Support.

From the Technical Support page, you can open a Customer Service Request online or find the telephone number for the nearest Technical Solutions Center. If you are not connected to the Internet, you can call 1-800-4NORTEL (1-800-466-7835) to learn the telephone number for the nearest Technical Solutions Center.

An Express Routing Code (ERC) is available for many Nortel 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 [www.nortel.com/support](http://www.nortel.com/support) and click Express Routing Codes located on the right side bottom of the page.



---

# Chapter 1

## Using the Web-based Management Interface

---

This chapter describes the requirements for using the Web-based management interface and how to use it as a tool to configure the Ethernet Routing Switch. This chapter discusses the following topics:

- “Requirements, next
- “Logging in to the Web-based Management Interface” on page 28
- “Web Page Layout” on page 29

## Requirements

To use the Web-based management interface, you will need the following items:

- A computer connected to any of the network ports.
- One of the following Web browsers installed on the computer (check the memory requirements):
  - Microsoft Internet Explorer\*, version 4.0 or later (Windows 95/98/NT/XP/2000)
  - Netscape Navigator\*, version 4.51 or later (Windows 95/98/NT/XP/2000 and Unix)
- The IP address of the Ethernet Routing Switch
- A web browser optimized for 800 by 600 pixel screen size



**Note:** The Web-based management interface Web pages may load at different speeds depending on the Web browser you use.

---

## Logging in to the Web-based Management Interface

Before you log in to the Web-based management interface, use the console interface to verify the VLAN port assignments and to ensure that your switch CPU and your computer are assigned to the same VLAN. If the devices are not connected to the same VLAN, you cannot access the Web-based management system.

To log in to the Web-based management interface, follow these steps:

- 1 Start your Web browser.
- 2 In the Web address field, enter the IP address for your host switch. For example, `http://10.30.31.105`, and press [Enter].

The home page opens (Figure 1).

**Figure 1** Web-based management interface home page

### Administration > System Information

## Ethernet Switch 3510-24T

<b>sysDescription</b>	Ethernet Switch 3510-24T HW:01 FW:4.0.0.4 SW:v4.0.3.00
<b>sysUpTime</b>	6 Days 22 Hours 17 Minutes 22 Seconds
<b>sysContact</b>	
<b>sysName</b>	
<b>sysLocation</b>	



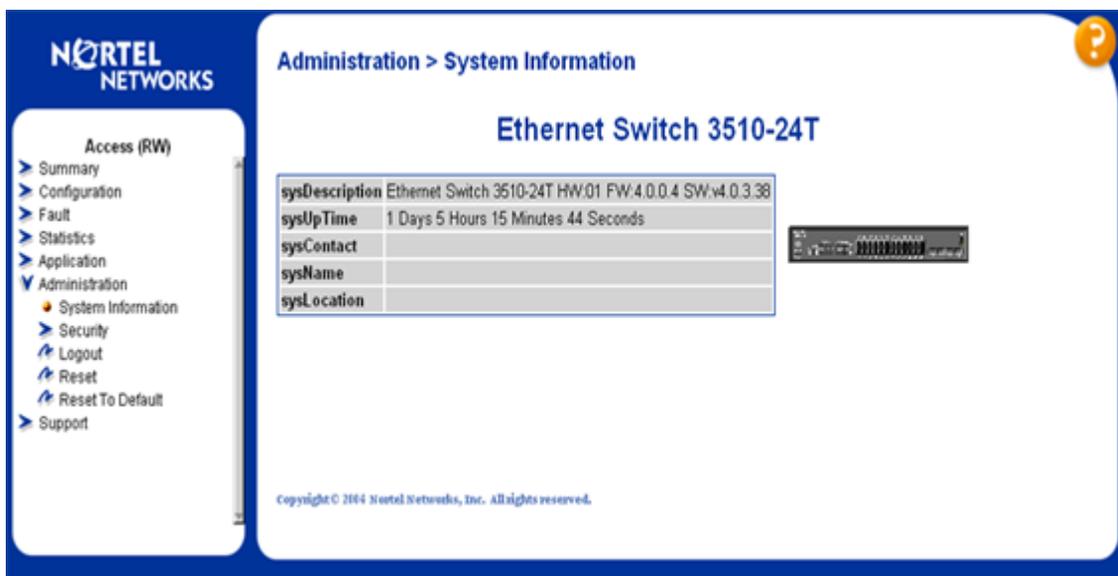
Network security does not yet exist the first time you access the Web-based management user interface. As the system administrator, you must create access parameters and passwords to protect the integrity of your network configuration(s).

For more information on setting access parameters and system passwords, refer to [Configuring the Switch](#).

## Web Page Layout

The Home page ([Figure 2](#)) and all successive pages have a common layout. Each page is divided into two sections – the menu, and the management page. All Web pages are optimized for a 800 x 600 pixel screen size.

**Figure 2** Web page layout



## Menu

The menu, as shown in [Figure 2](#), contains a list of seven main titles and their corresponding options.

To navigate the Web-based management interface menu, click a menu title and then click one of its options. When you click an option, the corresponding page opens.

**Table 1** Main headings in the Web-based management user interface and their associated options.

**Table 1** Main headings and options

Main menu titles	Options
Summary	Switch Information
Configuration	IP System Remote Access SNMPv1 SNMPv3* SNMP Trap MAC Address Table Find MAC Address Port Management High Speed Flow Control Software Download Configuration File Console/Comm Port
Fault	RMON threshold RMON Event Log System Log
Statistics	Port Port Error Summary Interface Ethernet Errors Transparent Bridging RMON Ethernet RMON History
Application	Port Mirroring Rate Limiting EAPOL Security MAC Address Security* IGMP* VLAN* Spanning Tree* Multilink Trunk* QoS*
Administration	System Information Security* Logout Reset Reset to Default

**Table 1** Main headings and options

Main menu titles	Options
Support	Help Release Notes Manuals Upgrade
*Has additional menu options.	

Tools are provided in the menu to assist you in navigating the Web-based management interface.



**Caution:** Web browser capabilities such as page bookmarking, refresh, and page forward and page back, function as they would in any other Web site. However, these capabilities do not enhance the functionality of the Web-based management interface. Nortel recommends you to use only the navigation tools provided in the management interface.

Table 2 describes the icons that appear on the menu.

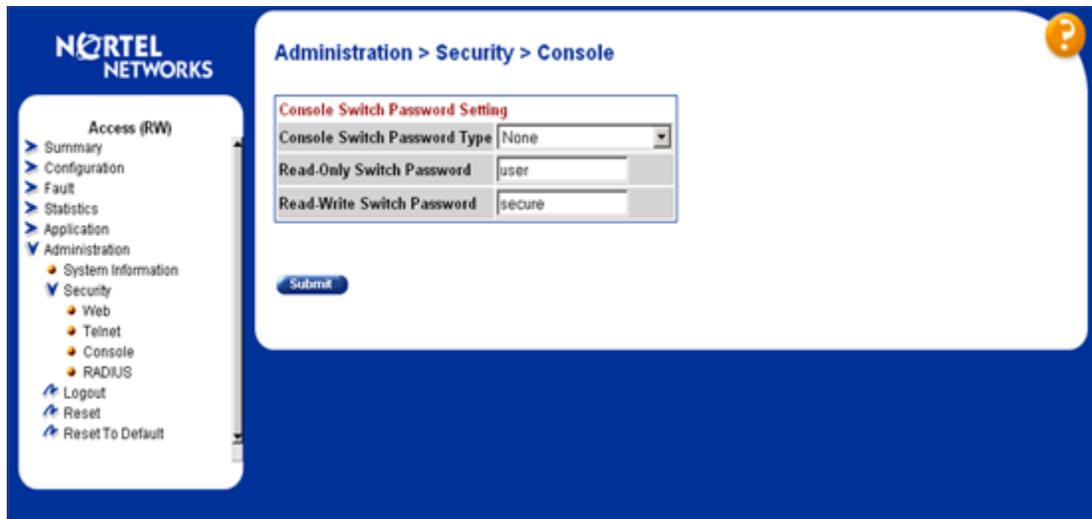
**Table 2** Menu icons

Button or icon	Description
	This icon identifies a menu title. Click this icon to display its options.
	This icon identifies a menu title option. Click this icon to display the corresponding page.
	This icon identifies a menu title option with a hyperlink to related pages.
	This icon is linked to an action, for example logout, reset, or reset to system defaults.
	Clicking on the Nortel Networks logo opens the corporate home page in a new Web browser.

## Management Page

When you click a menu option, the corresponding management page opens. [Figure 3](#) shows the page which is displayed for the Administration > Security > Console option.

**Figure 3** Console page



A page is composed of one or more of the following elements:

- Tables and input forms

The gray cells in a page are display only, and white cells are input fields.

- Check boxes

You can enable or disable a selection by clicking a check box. When a check mark is displayed in the box, that selection is enabled. You can disable a clearing the check box.

- Icons and buttons

Icons and buttons perform an action concerning the displayed page or the switch. Some pages include a button that opens another page or updates the values shown on the current page. Other pages include icons that initiate an action, such as reformatting the current displayed data as a bar or pie chart.

Table 3 describes the icons that may appear on a page to assist you in navigation.

**Table 3** Page buttons and icons

Icon	Name	Description
	Modify	Accesses a modification page for the selected row.
	View	Accesses a view only statistics page for the selected row.
	Delete	Deletes a row.
	Help	Accesses the Help menu in a new Web browser.
	Item-Specific Help	Accesses the item-specific Help menu in a new Web browser.
		Note: Text within a table that is highlighted blue and underlined is a hyperlink to a related management page.



---

## Chapter 2

# Administering the switch

---

The administrative options available are:

- [“Viewing General Information”](#), next
- [“Configuring System Security”](#) on page 37
- [“Logging on to the Web Management Interface”](#) on page 40
- [“Resetting the Ethernet Routing Switch”](#) on page 42
- [“Resetting the Ethernet Routing Switch to system defaults”](#) on page 44
- [“Logging out of the Management Interface”](#) on page 45

For more information on the features discussed in this chapter, refer to the *Application Guide for Nortel Ethernet Routing Switch 3510-24T, Software Release 4.0.3*. This book also has instructions on using the Console Interface (CI) menus to configure and manage the switch. Refer to the *NCLI Configuration Guide for Nortel Ethernet Routing Switch 3510-24T, Software Release 4.0.3* for instructions on managing the Ethernet Routing Switch by CLI. *Switch Management for Nortel Ethernet Routing Switch 3510-24T, Software Release 4.0.3* contains instructions on managing the switch by using the Device Manager.

## Viewing General Information

You can view an image of the Ethernet Routing Switch in the following way:

### Viewing System Information

You can view an image of the Ethernet Routing Switch configuration, information about the host device and, if provided, the contact person or manager for the switch. The System Information page is also the Web-based management interface home page.

To view system information:

- 1 From the main menu, choose Administration > System Information.

The System Information page opens (Figure 4).



**Note:** You create or modify existing system information parameters on the System page.

---

**Figure 4** System Information home page

### Administration > System Information

## Ethernet Switch 3510-24T

<b>sysDescription</b>	Ethernet Switch 3510-24T HW:01 FW:4.0.0.4 SW:v4.0.3.00
<b>sysUpTime</b>	1 Weeks 30 Minutes 38 Seconds
<b>sysContact</b>	
<b>sysName</b>	
<b>sysLocation</b>	



[Table 4](#) describes the items on the System Information page.

**Table 4** System Information page items

Item	Description
sysDescription	The default description of the Ethernet Routing Switch, including the hardware, firmware, and software.
sysUpTime	The elapsed time since the last network management portion of the system was last re-initialized.
sysContact	The name and email contact information of the administratively assigned person to contact regarding switch operation.
sysName	The name created by the network administrator to identify the switch, for example Finance Group.
sysLocation	The location name created by the network administrator to identify the switch location, for example, first floor.

## Configuring System Security

This section describes the steps you use to build and manage security using the Web-based management interface.

For more information on setting security systems, refer to setting EAPOL, MAC security, and IP manager list in [Configuring the Switch](#).

### Setting Console, Telnet, and Web Passwords

To set console, Telnet, and Web passwords:

- 1 From the main menu, choose Administration > Security and Console, Telnet, or Web.

The selected password page opens ([Figure 5](#)).



**Note:** The title of the page corresponds to the menu selection you choose. In [Figure 5](#), the network administrator selected Administration > Security > Console.



**Note:** The Console has its own switch password type; whereas Telnet and Web access methods share the same switch password type. The Console, Telnet, and Web all share the same passwords when they are set to the same password type.

**Figure 5** Console Password setting page

### Administration > Security > Console

**Console Switch Password Setting**

<b>Console Switch Password Type</b>	None <input type="button" value="v"/>
<b>Read-Only Switch Password</b>	user <input type="button" value="x"/>
<b>Read-Write Switch Password</b>	secure <input type="button" value="x"/>

Table 5 describes the items on the Console page.

**Table 5** Console page items

Section	Item	Setting	Description
Console Switch Password Setting	Console Switch Password Setting Type	(1) None (2) Local Password (3) RADIUS Authentication	Displays the switch password types.  Note: The default is None.
	Read-Only Switch Password	1 to 15 string (printable characters)	Type the read-only password setting for the read-only access user. Re-enter the read-only switch password for verification.
	Read-Write Switch Password	1 to 15 string (printable characters)	Type the read-write password setting for the read-write access user. Re-enter the read-write switch password for verification.

**2** Type the information, or make a selection from the list.

- 3 Click Submit.

## Configuring RADIUS Security

To configure RADIUS security parameters:

- 1 From the main menu, choose Administration > Security > RADIUS.  
The RADIUS page opens.
- 2 Type the information.
- 3 Click Submit.

**Figure 6** RADIUS page

### Administration > Security > RADIUS

RADIUS Authentication Setting	
Primary RADIUS Server	<input type="text" value="0.0.0.0"/>
Secondary RADIUS Server	<input type="text" value="0.0.0.0"/>
UDP RADIUS Port	<input type="text" value="1645"/>
RADIUS Shared Secret	<input type="text"/>

Table 6 describes the items on the RADIUS page.

**Table 6** RADIUS page items

Item	Setting	Description
Primary RADIUS Server	XXX.XXX.XXX.XXX	Type a Primary RADIUS server IP address in the appropriate format.
Secondary RADIUS Server	XXX.XXX.XXX.XXX	Type a Secondary RADIUS server IP address in the appropriate format.

**Table 6** RADIUS page items

Item	Setting	Description
UDP RADIUS Port	Integer	Type the UDP RADIUS port number.
RADIUS Shared Secret	1to 16	Type a unique character string to create a secret password. Re-enter the secret password for verification.



**Note:** If you enter an incorrect password while using RADIUS authentication to restrict management access to the device, the following error message appears:

no response from RADIUS servers

---



**Note:** Authentication using a secondary RADIUS server does not work when the primary RADIUS server is the CiscoSecure ACS v3.0 For Windows. The following error message appears:

Access Denied  
from RADIUS.

---

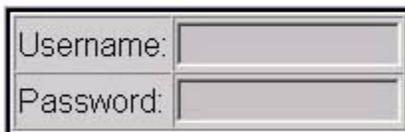
## Logging on to the Web Management Interface

After you enable the switch password authentication (the password type is either “Local Password” or “RADIUS Authentication”) and you set the switch passwords, any user attempting to use the application will be presented with the login page ([Figure 7](#)).

**Figure 7** Web-based management interface log on page

*This graphical network device management tool is compatible with the latest versions of Internet Explorer (version 4.0 minimum) and Netscape Navigator (version 4.5 minimum).*

*Optimized for 800 x 600 pixel display.*

A screenshot of a web-based management interface log on page. It features two text input fields: the top one is labeled 'Username:' and the bottom one is labeled 'Password:'. Both fields are empty and have a light gray background with a thin border. The labels are positioned to the left of each field.

**Log On**

To log on to the Web-based management interface:

- 1** In the Username text box, type **RO** for read-only access or **RW** in uppercase for read-write access.
- 2** In the Password text box, type your password.
- 3** Click Log On.

The System Information home page opens ([Figure 8](#)).

**Figure 8** System Information home page**Administration > System Information****Ethernet Switch 3510-24T**

<b>sysDescription</b>	Ethernet Switch 3510-24T HW:01 FW:4.0.0.4 SW:v4.0.3.00
<b>sysUpTime</b>	1 Weeks 30 Minutes 38 Seconds
<b>sysContact</b>	
<b>sysName</b>	
<b>sysLocation</b>	



With Web access enabled, the switch can support up to four concurrent Web sessions, where each session is defined by a unique IP address from where the session is originating. Two predefined user levels are available, and each user level has a corresponding username and password.

[Table 7](#) shows an example of the two predefined user levels available and their access level within the Web-based management user interface.

**Table 7** User levels and access levels

User level	User name for each level in upper case	Password for each user level	Access Level
Read-only	RO	XXXXXXXX	Read only
Read-write	RW	XXXXXXXX	Full read/write access

## Resetting the Ethernet Routing Switch

You can reset a switch without erasing any configured switch parameters. While resetting, the switch initiates a self-test that comprises various diagnostic routines and subtests. (Resetting means rebooting in this context.)

---

To reset the Ethernet Routing Switch without making changes (since your last Submit request):

- 1 From the main menu, choose Administration > Reset.

The Reset page opens (Figure 9).



**Note:** When you are working on the switch, the system returns the message:

Are you sure you want to reset the switch?

When you press OK, the switch resets.

---

**Figure 9** Reset page



- 2 Click Submit.



**Note:** If you have not configured system password security, a reset returns you to the home page, as shown in [Figure 1 on page 28](#). If you have configured system password security, a reset returns you to a log on page, as shown in [Figure 7 on page 41](#).

---

## Resetting the Ethernet Routing Switch to system defaults

You can reset the Ethernet Routing Switch, thereby replacing all configured switch parameters with the factory default values.



**Caution:** If you choose reset to default settings, all configured settings are replaced with factory default settings when you click Submit (IP is reset to 0.0.0.0.). For more information on factory default settings, refer to *Application Guide for Nortel Ethernet Routing Switch 3510-24T, Software Release 4.0.3*.

---

During the reset process, the switch initiates a self-test that comprises various diagnostic routines and subtests.

To reset the Ethernet Routing Switch to system defaults:

- 1 From the main menu, choose Administration > Reset to Default.

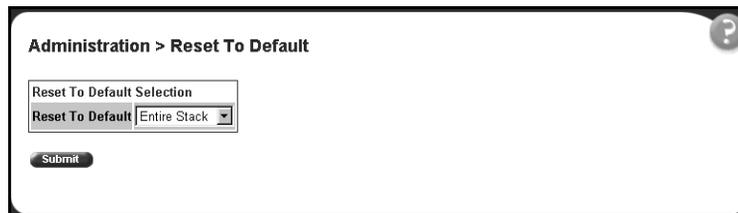


**Note:** When you are working on the switch, the system returns the message:

Are you sure your want to reset the switch?  
When you press OK, the switch resets.

---

**Figure 10** Reset to Default page



- 2 Click Submit.

## Logging out of the Management Interface

To log out of the Web-based management interface:

- 1 From the main menu, choose Administration > Logout.

A message opens prompting you to confirm your request

- 2 Do one of the following:

- Click OK to logout of the Web-based management interface.
- Click Cancel to return to the Web-based management interface home page.



**Note:** After ten minutes of idle time you will automatically be logged out. This means that if Web authentication is enabled, you will have to login again to the Switch Web access.

---



---

## Chapter 3

# Viewing Summary Information

---

The summary information options of the Ethernet Routing Switch 3510-24T are:

- [“Viewing Summary Switch Information”](#), next

## Viewing Summary Switch Information

You can view the summary information of the switch, for example, the physical description and serial number of the switch.

To view summary switch information:

- From the main menu, choose Summary > Switch Information.

The Switch Information page opens ([Figure 11](#)).

**Figure 11** Switch Information page**Summary > Switch Information**

<b>Switch Information</b>	
<b>Module Description</b>	Ethernet Switch 3510-24T 24 10/100/1000BaseTX plus 4 Overlapped GBIC slots
<b>GBIC Port 21</b>	None
<b>GBIC Port 22</b>	None
<b>GBIC Port 23</b>	None
<b>GBIC Port 24</b>	None
<b>Firmware Version</b>	4.0.0.4
<b>Software Version</b>	v4.0.3.00
<b>Manufacturing Date Code</b>	10062004
<b>Hardware Version</b>	3510-24T HW:01
<b>Serial #</b>	SDL01000L
<b>Operational State</b>	Normal
<b>Mac Address</b>	00-0F-3D-E5-28-00
<b>IP Address</b>	192.168.151.176
<b>Power Status</b>	Primary Power. RPSU not present.

[Table 8](#) describes the fields on the Switch Information page.

**Table 8** Switch Information page fields

<b>Item</b>	<b>Description</b>
Module Description	The factory set description of the policy switch.
GBIC Port 21	Description of the type of GBIC. The default value is None. It can be SX, LX, CWDM.
GBIC Port 22	Description of the type of GBIC. The default value is None. It can be SX, LX, CWDM.
GBIC Port 23	Description of the type of GBIC. The default value is None. It can be SX, LX, CWDM.
GBIC Port 24	Description of the type of GBIC. The default value is None. It can be SX, LX, CWDM.
Firmware Version	The version of the running firmware.
Software Version	The version of the running software.
Manufacturing Date Code	The date of manufacture of the board in ASCII format.
Hardware Version	The hardware version of the switch.
Serial Number	The serial number of the policy switch.
Operational State	The current operational state of the device. The operational states are: Other, Not Available, Removed, Disabled, Normal, Reset in Progress, Testing, Warning, Non Fatal Errors, Fatal Error, and Not Configured.
Mac Address	The MAC address of the device.

**Table 8** Switch Information page fields

Item	Description
IP Address	The IP address of the device.
Power Status	The current power status of the device. Primary Power. RPSU not present.



---

## Chapter 4

# Configuring the Switch

---

The switch configuration options available to you are:

- [“Configuring BootP, IP, and Gateway Settings”](#), next
- [“Modifying System Settings”](#) on page 55
- [“Simple Network Management Protocol”](#) on page 58
- [“Configuring SNMPv1”](#) on page 58
- [“Configuring SNMPv3”](#) on page 60
- [“Configuring SNMP Traps”](#) on page 83
- [“Configuring EAPOL-based Security”](#) on page 85
- [“Managing Remote Access by IP Address”](#) on page 56
- [“Configuring MAC Address-based Security”](#) on page 88
- [“Viewing Learned MAC Addresses by VLAN”](#) on page 101
- [“Locating a Specific MAC Address”](#) on page 103
- [“Configuring Port’s Autonegotiation, Speed, Duplex, Status, and Alias”](#) on page 104
- [“Configuring High Speed Flow Control”](#) on page 107
- [“Downloading Switch Images”](#) on page 109
- [“Storing and Retrieving Switch Configuration File from TFTP Server”](#) on page 111
- [“Configuring Port Communication Speed”](#) on page 113

## Configuring BootP, IP, and Gateway Settings

You can configure your BootP mode settings, create and modify your in-band switch IP addresses and in-band subnet mask parameters, and configure the IP address of your default gateway.



**Note:** Settings take effect immediately when you click Submit.

To configure BootP, IP, and gateway settings:

- 1 From the main menu, choose Configuration > IP  
The IP page opens (Figure 12).

**Figure 12** IP page for a Ethernet Routing Switch

### Configuration > IP

IP Setting			
	Configurable	In Use	Last BootP
BootP Request Mode	BootP When Needed ▾		
In-Band Switch IP Address	192.168.151.176	192.168.151.176	0.0.0.0
In-Band Subnet Mask	0.0.0.0	255.255.255.0	0.0.0.0
Default Gateway	192.168.151.1	192.168.151.1	0.0.0.0

Submit

Table 9 describes the items on the IP page.

**Table 9** IP page items

Section	Item	Range	Description
Boot Mode Setting	BootP Request Mode	BootP When Needed	<p>Choose this mode to inform the switch to send a BootP request when the switch IP address stored in nonvolatile memory is the factory default value. If the stored IP address differs from the factory default value, the switch uses the stored network parameters. If the switch cannot find a BootP server, it tries five more times to find one and then defaults to the factory settings.</p> <p>Note: This is the default.</p>
		BootP Always	<p>Choose this mode to inform the switch, each time the switch boots, to ignore any stored network parameters and send a BootP request. If the BootP request fails, the switch boots with the factory default IP configuration. This setting disables remote management if no BootP server is set up for the switch, but it allows the switch to boot normally.</p>
		BootP Disabled	<p>Choose this mode to inform the switch, each time the switch boots, to use the IP configuration parameters stored in non-volatile memory. If a BootP configuration is in progress when you issue this command, the BootP configuration stops.</p>
		BootP or Last Address	<p>Choose this mode to inform the switch, at each startup, to obtain its IP configuration using BootP. If the BootP request fails, the switch uses the network parameters stored in its non-volatile memory.</p> <p>Note: Valid parameters obtained in using BootP always replace current information stored in the non-volatile memory.</p> <p>Note: Whenever the switch is broadcasting BootP requests, the BootP process times out if a reply is not received within (approximately) 7 minutes. When the process times out, the BootP request mode automatically changes to BootP Disabled mode. To restart the BootP process, change the BootP request mode to any of the three following modes: BootP When Needed, BootP Always, or to BootP or Last Address.</p>

**Table 9** IP page items (continued)

Section	Item	Range	Description
IP Setting	In-Band Switch IP Address	XXX.XXX.XXX.XXX	Type a new switch IP address in the appropriate format.  Note: When the IP address is entered in the In-Band IP Address field, and the In-Band Subnet Mask field value is not present, the software provides an <i>in-use</i> default value for the In-Band Subnet Mask field that is based on the class of the IP address entered in the In-Band IP Address field.
	In-Band Subnet Mast	XXX.XXX.XXX.XXX	Type a new subnet mask in the appropriate format.
	In-Use		The column header for the read-only fields in this screen. The data displayed in this column represents data that is currently in use.
	Last BootP		The column header for the read-only fields in this screen. The read-only data displayed in this column represents data obtained from the last BootP reply received.
Gateway Setting	Default Gateway	XXX.XXX.XXX.XXX	Type an IP address for the default gateway in the appropriate format.



**Note:** If an IP address is assigned to the device and the BootP process times out, the BootP mode remains the default mode of BootP when needed.

However, if the device does not have an assigned IP address and the BootP process times out, the BootP mode automatically changes to BootP disabled. This change to BootP disabled is not stored, and the BootP reverts to the default value of BootP when needed after rebooting the device.

- 2 Type information in the text boxes, or select from a list.
- 3 Click Submit.

## Modifying System Settings

You can create or modify the system name, system location, and network manager contact information.



**Note:** The configurable parameters on the System page are displayed in a read only-format on the Web-based management user interface System Information home page (see [Figure 1 on page 28](#)).

To configure system settings:

- 1 From the main menu, choose Configuration > System.

The System page opens ([Figure 13](#)).

**Figure 13** System page

### Configuration > System

System Characteristics Setting	
System Description	Ethernet Switch 3510-24T HW:01 FW:4.0.0.4 SW:v4.0.3.00
System Object ID	1.3.6.1.4.1.45.3.66
System Up Time	7:1:19:3
System Contact	<input type="text"/>
System Name	<input type="text"/>
System Location	<input type="text"/>

[Table 10](#) describes the items on the System page.

**Table 10** System page items

Item	Range	Description
System Description		The factory set description of the hardware and software versions.
System Object ID		The character string that the vendor created to uniquely identify this device.

**Table 10** System page items

Item	Range	Description
System Up Time		The elapsed time since the last network management portion of the system was last re-initialized.  Note: This field is updated only when the screen is redisplayed.
System Contact	0 to 255	Type a character string to create the contact information for the network manager or the selected person to contact regarding switch operation, for example, mcarlson@company.com  Note: To operate correctly with the Web interface, the system contact should be an e-mail address.
System Name	0 to 255	Type a character string to create a name to identify the switch, for example Finance Group.
System Location	0 to 255	Type a character string to create a name for the switch location, for example, First Floor.

- 2 Type information in the text boxes.
- 3 Click Submit.

## Managing Remote Access by IP Address

You can configure the remote access you want to allow. You can specify up to 10 IP addresses to allow Web access, SNMP access, or Telnet access to the Ethernet Routing Switch.

To configure remote access using the Web-based management system:

- 1 From the main menu of the Ethernet Routing Switch Web-based Manager, choose Configuration > Remote Access.

The Remote Access page opens ([Figure 14](#)).

Figure 14 Remote Access page

**Configuration > Remote Access**

Remote Access Settings		
	Access	Use List
Telnet	Allowed	Yes
SNMP	Allowed	Yes
Web Page	Allowed	Yes

**Submit**

Allowed Source IP and Subnet Mask		
#	Allowed Source IP	Allowed Source Mask
1	0.0.0.0	0.0.0.0
2	255.255.255.255	255.255.255.255
3	255.255.255.255	255.255.255.255
4	255.255.255.255	255.255.255.255
5	255.255.255.255	255.255.255.255
6	255.255.255.255	255.255.255.255
7	255.255.255.255	255.255.255.255
8	255.255.255.255	255.255.255.255
9	255.255.255.255	255.255.255.255
10	255.255.255.255	255.255.255.255

**Submit**

Table 11 describes the fields on the Remote Access page.

Table 11 Remote Access page fields

Section	Item	Range	Description
Remote Access Settings	Telnet/Access	(1) Allowed (2) Disallowed	Allows Telnet access.
	Telnet/Use List	(1) Yes (2) No	Restricts Telnet access to the specified 10 source IP addresses.

**Table 11** Remote Access page fields (continued)

Section	Item	Range	Description
	SNMP/Access	(1) Allowed (2) Disallowed	Allows SNMP access.
	SNMP/Use List	(1) Yes (2) No	Restricts SNMP access to the specified 10 source IP addresses.
	Web Page/Access		Displays allowed Web access.
	Web/Use List	(1) Yes (2) No	Restricts Web access to the specified 10 source IP addresses.
Allowed Source IP and Subnet Mask	Allowed Source IP	XXX.XXX.XXX.XXX	Enter the source IP address you want to allow switch access.
	Allowed Source Mask	XXX.XXX.XXX.XXX	Enter the source IP mask you want to allow switch access.

- 2 Complete fields as described in the table.
- 3 Click Submit.

## Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is the standard for network management that uses a common software agent to manage local and wide area network equipment from different vendors; part of the Transmission Control Protocol/Internet Protocol (TCP/IP) suite and defined in RFC1157. SNMPv1 is version one, or the original standard protocol. SNMPv3 is a combination of proposal updates to SNMP, most of which deal with security.

## Configuring SNMPv1

You can configure SNMPv1 read-write and read-only community strings, enable or disable trap mode settings, and/or enable or disable the Autotopology feature. The Autotopology feature, when enabled, performs a process that recognizes any device on the managed network and defines and maps its relation to other network devices in real time.

To configure the community string, trap mode, and Autotopology settings and features:

- 1 From the main menu, choose Configuration > SNMPv1.

The SNMPv1 page opens (Figure 15).

Figure 15 SNMPv1 page

### Configuration > SNMPv1

Community String Setting	
Read-Only Community String	<input type="text" value="public"/>
Read-Write Community String	<input type="text" value="private"/>

Trap Mode Setting	
Authentication Trap	<input type="text" value="Enabled"/> ▾

AutoTopology Setting	
AutoTopology	<input type="text" value="Enabled"/> ▾

Table 12 describes the items on the SNMPv1 page.

**Table 12** SNMPv1 page items

Section	Item	Range	Description
Community String Setting	Read-Only Community String	1 to 32	Type a character string to identify the community string for the SNMPv1 read-only community, for example, public or private.  The default value is public.
	Read-Write Community String	1 to 32	Type a character string to identify the community string for the SNMPv1 read-write community, for example, public or private.  The default value is private.
Trap Mode Setting	Authentication Trap	(1) Enabled (2) Disabled	Choose to enable or disable the authentication trap.
AutoTopology Setting	AutoTopology	(1) Enabled (2) Disabled	Choose to enable or disable the autotopology feature.

- 2 Type information in the text boxes, or select from a list.
- 3 Click Submit in any section to save your changes.

## Configuring SNMPv3

This section describes the steps to build and manage SNMPv3 in the Web-based management user interface.

### SNMPv3 Table Entries Stored in NVRAM

The number of nonvolatile entries (entries stored in NVRAM) allowed in the SNMPv3 tables is shown in the following list. The system does not allow you to create more entries marked nonvolatile once you reach these limits:

- snmpCommunityTable: 20
- vacmViewTreeFamilyTable: 60
- vacmSecurityToGroupTable: 40

- vacmAccessTable: 40
- usmUserTable: 20
- snmpNotifyTable: 20
- snmpTargetAddrTable: 20
- snmpTargetParamsTable: 20

## Viewing SNMPv3 System Information

You can view information about the SNMPv3 engine that exists and the private protocols that are supported in your network configuration. You can also view information about packets received by the system having particular errors, such as unavailable contexts, unknown contexts, decrypting errors, or unknown user names.

To view SNMPv3 system information:

- 1 From the main menu, choose Configuration > SNMPv3 > System Information.

The System Information page opens ([Figure 16](#)).

**Figure 16** System Information page**Configuration > SNMPv3 > System Information**

<b>System Information</b>	
<b>SNMP Engine ID</b>	80-00-02-32-80-02-00-13-53-44-4c-49-30-31-30-30
<b>SNMP Engine Boots</b>	9
<b>SNMP Engine Time</b>	0:1:41:41
<b>SNMP Engine Maximum Message Size</b>	2048
<b>SNMP Engine Dialects</b>	SNMPv1, SNMPv2c, SNMPv3
<b>Authentication Protocols Supported</b>	HMAC MD5
<b>Private Protocols Supported</b>	None

<b>SNMPv3 Counters</b>	
<b>Unavailable Contexts</b>	0
<b>Unknown Contexts</b>	0
<b>Unsupported Security Levels</b>	0
<b>Not In Time Windows</b>	0
<b>Unknown User Names</b>	0
<b>Unknown Engine IDs</b>	7
<b>Wrong Digests</b>	0
<b>Decryption Errors</b>	0

[Table 13](#) describes the fields on the System Information section of the SNMPv3 System Information page.

**Table 13** System Information section fields

<b>Item</b>	<b>Description</b>
SNMP Engine ID	The SNMP engine's identification number.
SNMP Engine Boots	The number of times that the SNMP engine has re-initialized itself since its initial configuration.
SNMP Engine Time	The number of seconds since the SNMP engine last incremented the snmpEngineBoots object.
SNMP Engine Maximum Message Size	The maximum length, in octets, of an SNMP message which this SNMP engine can send or receive and process determined as the minimum of the maximum message size values supported among all transports available to and supported by the engine.

**Table 13** System Information section fields

Item	Description
SNMP Engine Dialects	The SNMP dialect the engine recognizes. The dialects are:SNMP1v1, SNMPv2C, and SNMPv3.
Authentication Protocols Supported	The registration point for standards-track authentication protocols used in SNMP Management Frameworks. The registration points is: None, HMAC MD5.
Private Protocols Supported	The registration point for standards-track privacy protocols used in SNMP Management Frameworks. The registration points is: None.

[Table 14](#) describes the fields on the SNMPv3 Counters section of the SNMPv3 System Information page.

**Table 14** SNMPv3 Counters section fields

Item	Description
Unavailable Contexts	The total number of packets dropped by the SNMP engine because the context contained in the message was unavailable.
Unknown Contexts	The total number of packets dropped by the SNMP engine because the context contained in the message was unknown.
Unsupported Security Levels	The total number of packets dropped by the SNMP engine because they requested a security level that was unknown to the SNMP engine or otherwise unavailable.
Not in Time Windows	The total number of packets dropped by the SNMP engine because they appeared outside of the authoritative SNMP engine's window.
Unknown User Names	The total number of packets dropped by the SNMP engine because they referenced an unknown user.
Unknown Engine IDs	The total number of packets dropped by the SNMP engine because they referenced an snmpEngineID that was not known to the SNMP engine.
Wrong Digests	The total number of packets dropped by the SNMP engine because they did not contain the expected digest value.
Decryption Errors	The total number of packets dropped by the SNMP engine because they could not be decrypted.

## Configuring User Access to SNMPv3

You can view a table of all current SNMPv3 user security information such as authentication/privacy protocols in use, and create or delete SNMPv3 system user configurations.

## Creating an SNMPv3 system user configuration

To create an SNMPv3 system user configuration:

- 1 From the main menu choose Configuration > SNMPv3 > User Specification.  
The User Specification page opens (Figure 17).

**Figure 17** User Specification page

### Configuration > SNMPv3 > User Specification

User Specification Table				
Action	User Name	Authentication Protocol	Privacy Protocol	Entry Storage
<input checked="" type="checkbox"/>	initial	HMAC MD5	None	Non Volatile
<input checked="" type="checkbox"/>	templateMD5	HMAC MD5	None	Non Volatile

User Specification Creation	
User Name	<input type="text"/>
Authentication Protocol	None ▾
Authentication Passphrase	<input type="text"/>
Privacy Protocol	None ▾
Privacy Passphrase	<input type="text"/>
Entry Storage	Volatile ▾

Table 15 describes the items on the User Specification Table section of the User Specification page.

**Table 15** User Specification Table section items

Item and MIB association	Description
	Deletes the row.
User Name (usmUserSecurityName)	The name of an existing SNMPv3 user.
Authentication Protocol (usmUserAuthProtocol)	Indicates whether the message sent on behalf of this user to/from the SNMP engine identified UserEngineID can be authenticated by the MD5 authentication protocol.
Private Protocol (usmUserPrivProtocol)	Displays whether or not messages sent on behalf of this user to or from the SNMP engine identified by usmUserEngineID can be protected from disclosure, and if so, the type of privacy protocol which is used.
Entry Storage	The current storage type for this row. If "Volatile" is displayed, information is dropped (lost) when you turn the power off. If non-volatile is displayed, information is saved in NVRAM when you turn the power off

Table 16 describes the items on the User Specification Creation section of the User Specification page.

**Table 16** User Specification Creation section items

Item and MIB association	Range	Description
User Name	1to 32	Type a string of characters to create an identity for the user.
Authentication Protocol (usmUserAuthProtocol)	None MD5	Choose whether or not the message sent on behalf of this user to/from the SNMP engine identified UserEngineID can be authenticated with the MD5 protocol.
Authentication Passphrase (usmUserAuthPassword)	1to 32	Type a string of character to create a password to use in conjunction with the authorization protocol.
Privacy Protocol	None	The privacy protocol you want to use.
Privacy Passphrase	Must be at least 8 characters long	Enter a string of at least 8 characters to create the passphrase. This passphrase is used to generate an encryption key for the user.
Entry Storage (usmUserStorageType)	(1) Volatile (2) Non-Volatile	Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off.

**2** In the User Specification Creation section, type information in the text boxes, or select from a list.

**3** Click Submit.

The new configuration is displayed in the User Specification Table (Figure 17).

## Deleting an SNMPv3 System User Configuration

To delete an existing SNMPv3 user configuration:

**1** From the main menu, choose Configuration > SNMPv3 > User Specification. The User Specification page opens (Figure 17).

**2** In the User Specification Table, click the Delete icon for the entry you want to delete.

A message opens prompting you to confirm your request.

**3** Do one of the following:

- Click Yes to delete the SNMPv3 user configuration.
- Click Cancel to return to the User Specification page without making changes.

## Configuring an SNMPv3 System User Group Membership

You can view a table of existing SNMPv3 group membership configurations and map or delete an SNMPv3 user to group configuration.

### Mapping an SNMPv3 System User to a Group

To map an SNMPv3 system user to a group:

**1** From the main menu, choose Configuration > SNMPv3 > Group Membership.

The Group Membership page opens (Figure 18).

Figure 18 Group Membership page

## Configuration &gt; SNMPv3 &gt; Group Membership

Group Membership Table				
Action	Security Name	Security Model	Group Name	Entry Storage
<input type="checkbox"/>	s5AgTrpRcvrComm0	SNMPv1	communitySnmpNotify	Read Only
<input type="checkbox"/>	s5AgTrpRcvrComm1	SNMPv1	communitySnmpNotify	Read Only
<input type="checkbox"/>	s5AgTrpRcvrComm2	SNMPv1	communitySnmpNotify	Read Only
<input type="checkbox"/>	s5AgTrpRcvrComm3	SNMPv1	communitySnmpNotify	Read Only
<input type="checkbox"/>	read_only_community	SNMPv1	communitySnmpRead	Read Only
<input type="checkbox"/>	read_write_community	SNMPv1	communitySnmpWrite	Read Only
<input type="checkbox"/>	s5AgTrpRcvrComm0	SNMPv2c	communitySnmpNotify	Read Only
<input type="checkbox"/>	s5AgTrpRcvrComm1	SNMPv2c	communitySnmpNotify	Read Only
<input type="checkbox"/>	s5AgTrpRcvrComm2	SNMPv2c	communitySnmpNotify	Read Only
<input type="checkbox"/>	s5AgTrpRcvrComm3	SNMPv2c	communitySnmpNotify	Read Only
<input type="checkbox"/>	read_only_community	SNMPv2c	communitySnmpRead	Read Only
<input type="checkbox"/>	read_write_community	SNMPv2c	communitySnmpWrite	Read Only
<input checked="" type="checkbox"/>	initial	USM	initial	Non Volatile
<input type="checkbox"/>	nncli	NNCLI	nncli	Read Only

Group Membership Creation	
Security Name (i.e. User Name)	<input type="text"/>
Security Model	SNMPv1 <input type="button" value="v"/>
Group Name	<input type="text"/>
Entry Storage	Volatile <input type="button" value="v"/>
<input type="button" value="Submit"/>	

Table 17 describes the items on the Group Membership page.

Table 17 Group Membership page items

Item and MIB association	Range	Description
<input checked="" type="checkbox"/>		Deletes the row.
Security Name (vacmSecurityToGroupStatus)	1 to 32	Type a string of character to create a security name for the principal which is mapped by this entry to a group name.

**Table 17** Group Membership page items

Item and MIB association	Range	Description
Security Model (vacmSecurityToGroupStatus)	(1) SNMPv1 (2) SNMPv2c (3) USM	Choose the security model within which the security name to group name mapping is valid.
Group Name (vacmGroupName)	1 to 32	Type a string of character to specify the group name.
Entry Storage (vacmSecurityToGroupStorageType)	(1) Volatile (2) Non-Volatile	Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off.

- 2 In the Group Membership Creation section, type information in the text boxes, or select from a list.
- 3 Click Submit.

The new entry appears in the Group Membership Table.

## Deleting an SNMPv3 group membership configuration

To delete an SNMPv3 group membership configuration:

- 1 From the main menu, choose Configuration > SNMPv3 > Group Membership.  
The Group Membership page opens ([Figure 18](#)).
- 2 In the Group Membership Table, click the Delete icon for the entry you want to delete.  
A message opens prompting you to confirm your request.
- 3 Do one of the following:
  - Click Yes to delete the group membership configuration.

- Click Cancel to return to the Group Membership page without making changes.



**Note:** This Group Membership Table section of the Group Membership page contains hyperlinks to the SNMPv3 User Specification and Group Access Rights pages. For more information on these pages, see [“Configuring User Access to SNMPv3” on page 63](#) and [“Configuring SNMPv3 Group Access Rights” on page 69](#).

---

## Configuring SNMPv3 Group Access Rights

You can view a table of existing SNMPv3 group access rights configurations, and you can create or delete a group’s SNMPv3 system-level access rights.

### Creating an SNMPv3 Group Access Rights Configuration

To create a group’s SNMPv3 system-level access right configuration:

- 1 From the main menu, choose Configuration > SNMPv3 > Group Access Rights.

The Group Access Rights page opens ([Figure 19](#)).

Figure 19 Group Access Rights page

## Configuration &gt; SNMPv3 &gt; Group Access Rights

Group Access Table							
Action	Group Name	Security Model	Security Level	Read View	Write View	Notify View	Entry Storage
<input type="checkbox"/>	nncli	NNCLI	noAuthNoPriv	<a href="#">nncli</a>	<a href="#">nncli</a>	-- null --	Read Only
<input checked="" type="checkbox"/>	initial	USM	noAuthNoPriv	<a href="#">restricted</a>	-- null --	<a href="#">restricted</a>	Non Volatile
<input checked="" type="checkbox"/>	initial	USM	authNoPriv	<a href="#">internet</a>	<a href="#">internet</a>	<a href="#">internet</a>	Non Volatile
<input type="checkbox"/>	communitySnmpRead	SNMPv1	noAuthNoPriv	<a href="#">snmpv1Objs</a>	-- null --	-- null --	Read Only
<input type="checkbox"/>	communitySnmpRead	SNMPv2c	noAuthNoPriv	<a href="#">snmpv1Objs</a>	-- null --	-- null --	Read Only
<input type="checkbox"/>	communitySnmpWrite	SNMPv1	noAuthNoPriv	<a href="#">snmpv1Objs</a>	<a href="#">snmpv1Objs</a>	-- null --	Read Only
<input type="checkbox"/>	communitySnmpWrite	SNMPv2c	noAuthNoPriv	<a href="#">snmpv1Objs</a>	<a href="#">snmpv1Objs</a>	-- null --	Read Only
<input type="checkbox"/>	communitySnmpNotify	SNMPv1	noAuthNoPriv	-- null --	-- null --	<a href="#">snmpv1Objs</a>	Read Only
<input type="checkbox"/>	communitySnmpNotify	SNMPv2c	noAuthNoPriv	-- null --	-- null --	<a href="#">snmpv1Objs</a>	Read Only

Group Access Creation	
Group Name	<input type="text"/>
Security Model	<input type="text" value="SNMPv1"/>
Security Level	<input type="text" value="noAuthNoPriv"/>
Read View	<input type="text"/>
Write View	<input type="text"/>
Notify View	<input type="text"/>
Entry Storage	<input type="text" value="Volatile"/>

Table 18 describes the items on the Group Access Rights page.

**Table 18** Group Access Rights page items

Item and MIB association	Range	Description
		Deletes the row.
Group Name (vacmAccessToGroupStatus)	1 to 32	Type a character string to specify the group name to which access is granted.
Security Model (vacmAccessSecurityModel)	(1) SNMPv1 (2) SNMPv2c (3) USM	Choose the security model to which access is granted.
Security Level (vacmAccessSecurityLevel)	(1) noAuthNoPriv (2) authNoPriv	Choose the minimum level of security required in order to gain the access rights allowed to the group.
Read View (vacmAccessReadViewName)	1 to 32	Type a character string to identify the MIB view of the SNMP context to which this entry authorizes read access.
Write View (vacmAccessWriteViewName)	1 to 32	Type a character string to identify the MIB view of the SNMP context to which this entry authorizes write access.
Notify View (vacmAccessNotifyViewName)	1 to 32	Type a character string to identify the MIB view to which this entry authorizes access to notifications.
Entry Storage (vacmSecurityToGroupStorageType)	(1) Volatile (2) Non-Volatile	Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off.

- 2 In the Group Access Creation section, type information in the text boxes, or select from a list.
- 3 Click Submit.

The new entry appears in the Group Access Table.

### Deleting an SNMPv3 Group Access Rights Configuration

To delete a n SNMPv3 group access configuration:

- 1 From the main menu, choose Configuration > SNMPv3 > Group Access Rights.

The Group Access Rights page opens (Figure 19).

- 2 In the Group Access Table, click the Delete icon for the entry you want to delete.

A message opens prompting you to confirm your request.

- 3 Do one of the following:
  - Click Yes to delete the group access configuration.
  - Click Cancel to return to the Group Access Rights page without making changes.



**Note:** This Group Access Table section of the Group Access Rights page contains hyperlinks to the Management Information View page. For more information, see “[Configuring an SNMPv3 Management Information View](#)” on page 72.

---

## Configuring an SNMPv3 Management Information View

You can view a table of existing SNMPv3 management information view configurations, and you can create or delete SNMPv3 management information view configurations.



**Note:** A view may consist of multiple entries in the table, each with the same view name, but a different view subtree.

---

### Creating an SNMPv3 Management Information View Configuration

To create an SNMPv3 management information view configuration:

- 1 From the main menu, choose Configuration > SNMPv3 > Management Info View.

The Management Information page opens (Figure 20).

Figure 20 Management Information View page

Configuration > SNMPv3 > Management Information View

Management Information Table					
Action	View Name	View Subtree	View Mask	View Type	Entry Storage
<input checked="" type="checkbox"/>	nncli	1.3	all ones	Included	Read Only
<input checked="" type="checkbox"/>	nncli	1.0.8802	all ones	Included	Read Only
<input checked="" type="checkbox"/>	nncli	1.2.840.10006.300.43	all ones	Included	Read Only
<input checked="" type="checkbox"/>	internet	1.0.8802	all ones	Included	Non Volatile
<input checked="" type="checkbox"/>	internet	1.3.6.1	all ones	Included	Non Volatile
<input checked="" type="checkbox"/>	restricted	1.0.8802	all ones	Included	Non Volatile
<input checked="" type="checkbox"/>	restricted	1.3.6.1	all ones	Included	Non Volatile
<input checked="" type="checkbox"/>	snmpv1Objs	1.3	all ones	Included	Read Only
<input checked="" type="checkbox"/>	snmpv1Objs	1.0.8802	all ones	Included	Read Only
<input checked="" type="checkbox"/>	snmpv1Objs	1.3.6.1.6	all ones	Excluded	Read Only
<input checked="" type="checkbox"/>	snmpv1Objs	1.2.840.10006.300.43	all ones	Included	Read Only
<input checked="" type="checkbox"/>	snmpv1Objs	1.3.6.1.6.3.10	all ones	Included	Read Only

Management Information Creation	
View Name	<input type="text"/>
View Subtree	<input type="text"/> (e.g., 1.3.6.1)
View Mask	<input type="text"/> (e.g., FF:CO:full [zero length])
View Type	Include ▾
Entry Storage	Volatile ▾

Table 19 describes the items on the Management Information View page.

Table 19 Management Information View page items

Item and MIB association	Range	Description
		Deletes the row.
View Name (vacmViewTreeFamilyViewName)	1 to 32	Type a character string to create a name for a family of view subtrees.

**Table 19** Management Information View page items

Item and MIB association	Range	Description
View Subtree (vacmViewTreeFamilySubtree)	X.X.X.X.X...	Type an object identifier (OID) to specify the MIB subtree which, when combined with the corresponding instance of vacmViewTreeFamilyMask, defines a family of view subtrees.  Note: If no OID is entered and the field is blank, a default mask value consisting of "1s" is recognized.
View Mask (vacmViewTreeFamilyMask)	Octet String (0..16)	Type the bit mask which, in combination with the corresponding instance of vacmViewFamilySubtree, defines a family of view subtrees.
View Type (vacmViewTreeFamilyType)	(1) Include (2) Exclude	Choose to include or exclude a family of view subtrees.
Entry Storage (vacmSecurityToGroupStorageType)	(1) Volatile (2) Non-Volatile	Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off.

- 2 In the Management Information Creation section, type information in the text boxes, or select from a list.
- 3 Click Submit.

The new entry appears in the Management Information Table (Figure 20).

## Deleting an SNMPv3 Management Information View Configuration

To delete an existing SNMPv3 management information view configuration:

- 1 From the main menu, choose Configuration > SNMPv3 > Management Info View.

The Management Information page opens (Figure 20).

- 2 In the Management Information Table, click the Delete icon for the entry you want to delete.

A message opens prompting you to confirm your request.

- 3** Do one of the following:
  - Click Yes to delete the management information view configuration.
  - Click Cancel to return to the table without making changes.

## Configuring an SNMPv3 System Notification Entry

You can view a table of existing SNMPv3 system notification configurations, and you can configure specific SNMPv3 system notification types with particular message recipients and delete SNMPv3 notification configurations.

### Creating an SNMPv3 System Notification Configuration

To create an SNMPv3 system notification configuration:

- 1** From the main menu, choose Configuration > SNMPv3 > Notification.  
The Notification page opens ([Figure 21](#)).

Figure 21 Notification page

**Configuration > SNMPv3 > Notification**

Notification Table				
Action	Notify Name	Notify Tag	Notify Type	Entry Storage
	inform	<a href="#">inform</a>	Inform	Read Only
	s5AgTrpRcwr	<a href="#">s5AgTrpRcwr</a>	Trap	Read Only
	trap	<a href="#">trap</a>	Trap	Read Only

Notification Creation	
Notify Name	<input type="text"/>
Notify Tag	<input type="text"/>
Notify Type	Trap <input type="button" value="v"/>
Entry Storage	Volatile <input type="button" value="v"/>

**Submit**

Table 20 describes the items on the Notification page.

Table 20 Notification page items

Item and MIB association	Range	Description
		Deletes the row.
Notify Name (snmpNotifyRowStatus)	1 to 32	Type a character string to identify the entry.
Notify Tag (snmpNotifyTag)	1 to 32	Type a value which to use to select entries in the snmpTargetAddrTable. Any entry in the snmpTargetAddrTable which contains a tag value which is equal to the value of an instance of this object is selected. If this object carries a zero length, no entries are selected.

**Table 20** Notification page items

Item and MIB association	Range	Description
Notify Type (snmpNotifyType)	(1) Trap (2) Inform	Choose the type of notification to generate.
Entry Storage (snmpNotifyStorageType)	(1) Volatile (2) Non-Volatile	Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off.

- 2 In the Notification Creation section, type information in the text boxes, or select from a list.
- 3 Click Submit.

The new entry appears in the Notification Table ([Figure 21](#)).



**Note:** This Notification Table section of the Notification page contains hyperlinks to the Target Parameter page. For more information, see [“Configuring an SNMPv3 Management Target Parameter”](#) on page 80.

## Deleting an SNMPv3 System Notification Configuration

To delete an SNMPv3 notification configuration:

- 1 From the main menu, choose Configuration > SNMPv3 > Notification.  
The Notification page opens ([Figure 21](#)).
- 2 In the Notification Table, click the Delete icon for the entry you want to delete.  
A message opens prompting you to confirm your request.
- 3 Do one of the following:
  - Click Yes to delete the notification configuration.
  - Click Cancel to return to the table without making changes.

## Configuring an SNMPv3 Management Target Address

You can view a table of existing SNMPv3 management target configurations, create SNMPv3 management target address configurations that associate notifications with particular recipients and delete SNMPv3 target address configurations.

### Creating an SNMPv3 Target Address Configuration

To create an SNMPv3 target address configuration:

- 1 From the main menu, choose Configuration > SNMPv3 > Target Address. The Target Address page opens (Figure 22).

**Figure 22** Target Address page

#### Configuration > SNMPv3 > Target Address

Target Address Table								
Action	Target Name	Target Domain	Target Address	Timeout	Retry Count	Tag List	Target Parameters	Entry Storage

Target Address Creation	
Target Name	<input type="text"/>
Target Address	<input type="text"/> (e.g., 1.2.3.4:160)
Target Timeout	<input type="text" value="1500"/> seconds (0 .. 2147483647)
Target Retry Count	<input type="text" value="3"/> (0 .. 255)
Target Tag List	<input type="text"/>
Target Param Entry	<input type="text"/>
Entry Storage	<input type="text" value="Volatile"/> <input type="button" value="v"/>

Table 21 describes the items on the Target Address page.

**Table 21** Target Address page items

Item and MIB association	Range	Description
		Deletes the row.
Target Name (snmpTargetAddrName)	1 to 32	Type a character string to create a target name.
Target Domain (snmpTargetAddrTDomain)	1 to 32	The transport type of the address contained in the snmpTargetAddrTAddress object.
Target Address (snmpTargetAddrTAddress)	XXX.XXX.XXX.XXX:XXX	Type a transport address in the format of an IP address, colon, and UDP port number.  For example: 10.30.31.99:162 (see <a href="#">Figure 22 on page 78</a> ).
Target Timeout (snmpTargetAddrTimeout)	Integer	Type the number, in seconds, to designate as the maximum time to wait for a response to an inform notification before re-sending the "Inform" notification.
Target Retry Count (snmpTargetAddrRetryCount)	0 to 255	Type the default number of retries to be attempted when a response is not received for a generated message. An application may provide its own retry count, in which case the value of this object is ignored.
Target Tag List (snmpTargetAddrTagList)	1 to 20	Type the space-separated list of tag values to be used to select target addresses for a particular operation.
Target Parameter Entry (snmpTargetAddr)	1 to 32	Type a numeric string to identify an entry in the snmpTargetParamsTable. The identified entry contains SNMP parameters to be used when generated messages to be sent to this transport address
Entry Storage	(1) Volatile (2) Non-Volatile	Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off.

- 2 In the Target Address Creation section, type information in the text boxes, or select from a list.
- 3 Click Submit.

The new entry appears in the Target Address Table ([Figure 22](#)).



**Note:** This Target Address Table section of the Target Address page contains hyperlinks to the Target Parameter page. For more information, see [“Configuring an SNMPv3 Management Target Parameter”](#) on [page 80](#).

---

## Deleting an SNMPv3 Target Address Configuration

To delete an SNMPv3 target address configuration:

- 1 From the main menu, choose Configuration > SNMPv3 > Target Address.  
The Target Address page opens ([Figure 22](#)).
- 2 In the Target Address Table, click the Delete icon for the entry you want to delete.  
A message opens prompting you to confirm your request.
- 3 Do one of the following:
  - Click Yes to delete the target address configuration.
  - Click Cancel to return to the table without making changes.

## Configuring an SNMPv3 Management Target Parameter

SNMPv3 management target parameters are used during notification generation to specify the communication parameters used for exchanges with notification recipients.

You can view a table of existing SNMPv3 target parameter configurations, create SNMPv3 target parameters that associate notifications with particular recipients, and delete existing SNMPv3 target parameter configurations.

### Creating an SNMPv3 Target Parameter Configuration

To create an SNMPv3 target parameter configuration:

- 1 From the main menu, choose Configuration > SNMPv3 > Target Parameter.

The Target Parameter page opens (Figure 23).

**Figure 23** Target Parameter page

### Configuration > SNMPv3 > Target Parameter

Target Parameter Table																		
Action	Parameter Tag	Msg Processing Model	Security Model	Security Name	Security Level	Entry Storage												
<table border="1"> <thead> <tr> <th colspan="2">Target Parameter Creation</th> </tr> </thead> <tbody> <tr> <td>Parameter Tag</td> <td><input type="text"/></td> </tr> <tr> <td>Msg Processing Model</td> <td>SNMPv1 <input type="button" value="v"/></td> </tr> <tr> <td>Security Name</td> <td><input type="text"/></td> </tr> <tr> <td>Security Level</td> <td>noAuthNoPriv <input type="button" value="v"/></td> </tr> <tr> <td>Entry Storage</td> <td>Volatile <input type="button" value="v"/></td> </tr> </tbody> </table>							Target Parameter Creation		Parameter Tag	<input type="text"/>	Msg Processing Model	SNMPv1 <input type="button" value="v"/>	Security Name	<input type="text"/>	Security Level	noAuthNoPriv <input type="button" value="v"/>	Entry Storage	Volatile <input type="button" value="v"/>
Target Parameter Creation																		
Parameter Tag	<input type="text"/>																	
Msg Processing Model	SNMPv1 <input type="button" value="v"/>																	
Security Name	<input type="text"/>																	
Security Level	noAuthNoPriv <input type="button" value="v"/>																	
Entry Storage	Volatile <input type="button" value="v"/>																	
<input type="button" value="Submit"/>																		

Table 22 describes the items on the Target Parameter page.

**Table 22** Target Parameter page items

Item	Range	Description
		Deletes the row.
Parameter Tag (snmpTargetParamsRowStatus)	1 to 32	Type a unique character string to identify the parameter tag.
Msg Processing Model (snmpTargetParamsMPModel)	SNMPv1 SNMPv2c SNMPv3 /USM	Choose the message processing model to be used when generating SNMP messages using this entry.
Security Name (snmpTargetParamsSecuirtyName)	1 to 32	Type the principal on whose behalf SNMP messages are generated using this entry

**Table 22** Target Parameter page items

Item	Range	Description
Security Level (snmpTargetParamsSecuirtyLevel)	(1) noAuthNoPriv (2) authNoPriv	Choose the level of security to be used when generating SNMP messages using this entry.
Entry Storage (snmpTargetParamsStorageType)	(1) Volatile (2) Non-Volatile	Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off.

**2** In the Target Parameter Creation section, type information in the text boxes, or select from a list.

**3** Click Submit.

The new entry appears in the Target Parameter Table ([Figure 23](#)).

## Deleting an SNMPv3 Target Parameter Configuration

To delete an SNMPv3 target parameter configuration:

**1** From the main menu, choose Configuration > SNMPv3 > Target Address.

The Target Address page opens ([Figure 22](#)).

**2** In the Target Parameter Table, click the Delete icon for the entry you want to delete.

A message opens prompting you to confirm your request.

**3** Do one of the following:

- Click Yes to delete the target parameter configuration.
- Click Cancel to return to the table without making changes.

## Configuring SNMP Traps

You can configure the IP address and community string for a new SNMP trap receiver, view a table of existing SNMP trap receiver configurations, or delete an existing SNMP trap receiver configuration(s).



**Note:** The SNMP Trap Receiver Table is an alternative to using the SNMPv3 Target Table and SNMPv3 Parameter Table. However, only SNMPv1 traps are configurable using this table.

### Creating an SNMP Trap Receiver Configuration

To create an SNMP trap receiver configuration:

- 1 From the main menu, choose Configuration > SNMP Trap.  
The SNMP Trap Receiver page opens (Figure 24).

**Figure 24** SNMP Trap Receiver page

### Configuration > SNMP Trap Receiver

Trap Receiver Table			
Action	Index	IP Address	Community

Trap Receiver Creation	
Trap Receiver Index	1 ▾
IP Address	<input type="text"/> (xxx.xxx.xxx.xxx)
Community	<input type="text"/>

[Table 23](#) describes the items on the Trap Receiver Table and Trap Receiver Creation sections of the SNMP Trap Receiver page.

**Table 23** SNMP Trap Receiver page items

Items	Range	Description
		Deletes the row.
Trap Receiver Index	1 to 4	Choose the number of the trap receiver to create or modify.
IP Address	XXX.XXX.XXX.XXX	Type the network address for the SNMP manager that is to receive the specified trap.
Community	0 to 32	Type the community string for the specified trap receiver.

**2** In the Trap Receiver Creation section, type information in the text boxes, or select from a list.

**3** Click Submit.

The new entry appears in the Trap Receiver Table ([Figure 24](#)).

## Deleting an SNMP Trap Receiver Configuration

To delete SNMP trap receiver configurations:

**1** From the main menu, choose Configuration > SNMP Trap.

The SNMP Trap Receiver page opens ([Figure 24](#)).

**2** In the Trap Receiver Table, click the Delete icon for the entry you want to delete.

A message opens prompting you to confirm your request.

**3** Do one of the following:

- Click Yes to delete the SNMP trap receiver configuration.
- Click Cancel to return to the table without making changes.

## Configuring EAPOL-based Security

You can configure security based on the Extensible Authentication Protocol over LAN (EAPOL) protocol. Refer to the *Application Guide for Nortel Ethernet Routing Switch 3510-24T, Software Release 4.0.3* for more information on EAPOL-based security.

To configure EAPOL:

- 1 From the main menu, choose Application > EAPOL Security.

The EAPOL Security Configuration page opens ([Figure 25](#)). Use the scroll bar on the right to move down the page and the scroll bar on the bottom to move across the page.

Figure 25 EAPOL Security Configuration page

**Application > EAPOL Security Configuration**

**EAPOL Administrative State Setting**  
 EAPOL Administrative State

**EAPOL Security Setting**

Port	Initialize	Administrative Status	Operational Status	Administrative Traffic Control	Operational Traffic Control	Re-authenticate Now	Re-authentication
1	<input type="text" value="No"/>	<input type="text" value="Force Authorized"/>	Authorized	<input type="text" value="In &amp; Out"/>	In & Out	<input type="text" value="No"/>	<input type="text" value="Disabled"/>
2	<input type="text" value="No"/>	<input type="text" value="Force Authorized"/>	Authorized	<input type="text" value="In &amp; Out"/>	In & Out	<input type="text" value="No"/>	<input type="text" value="Disabled"/>
3	<input type="text" value="No"/>	<input type="text" value="Force Authorized"/>	Authorized	<input type="text" value="In &amp; Out"/>	In & Out	<input type="text" value="No"/>	<input type="text" value="Disabled"/>
4	<input type="text" value="No"/>	<input type="text" value="Force Authorized"/>	Authorized	<input type="text" value="In &amp; Out"/>	In & Out	<input type="text" value="No"/>	<input type="text" value="Disabled"/>
5	<input type="text" value="No"/>	<input type="text" value="Force Authorized"/>	Authorized	<input type="text" value="In &amp; Out"/>	In & Out	<input type="text" value="No"/>	<input type="text" value="Disabled"/>
6	<input type="text" value="No"/>	<input type="text" value="Force Authorized"/>	Authorized	<input type="text" value="In &amp; Out"/>	In & Out	<input type="text" value="No"/>	<input type="text" value="Disabled"/>
7	<input type="text" value="No"/>	<input type="text" value="Force Authorized"/>	Authorized	<input type="text" value="In &amp; Out"/>	In & Out	<input type="text" value="No"/>	<input type="text" value="Disabled"/>
8	<input type="text" value="No"/>	<input type="text" value="Force Authorized"/>	Authorized	<input type="text" value="In &amp; Out"/>	In & Out	<input type="text" value="No"/>	<input type="text" value="Disabled"/>
9	<input type="text" value="No"/>	<input type="text" value="Force Authorized"/>	Authorized	<input type="text" value="In &amp; Out"/>	In & Out	<input type="text" value="No"/>	<input type="text" value="Disabled"/>
10	<input type="text" value="No"/>	<input type="text" value="Force Authorized"/>	Authorized	<input type="text" value="In &amp; Out"/>	In & Out	<input type="text" value="No"/>	<input type="text" value="Disabled"/>
11	<input type="text" value="No"/>	<input type="text" value="Force Authorized"/>	Authorized	<input type="text" value="In &amp; Out"/>	In & Out	<input type="text" value="No"/>	<input type="text" value="Disabled"/>
12	<input type="text" value="No"/>	<input type="text" value="Force Authorized"/>	Authorized	<input type="text" value="In &amp; Out"/>	In & Out	<input type="text" value="No"/>	<input type="text" value="Disabled"/>
Switch	<input type="text" value="No"/> <input type="checkbox"/>	<input type="text" value="Force Authorized"/> <input type="checkbox"/>		<input type="text" value="In &amp; Out"/> <input type="checkbox"/>		<input type="text" value="No"/> <input type="checkbox"/>	<input type="text" value="Enabled"/> <input type="checkbox"/>

Table 24 describes the fields on the EAPOL Security Configuration page.

Table 24 EAPOL Security Configuration page fields

Section	Item	Range	Description
EAPOL Administration State Setting		Enabled Disabled	Allows you to enable or disable the EAPOL security configuration.
EAPOL Security Setting	Port	1 to 24	Displays the port number.

**Table 24** EAPOL Security Configuration page fields (continued)

Section	Item	Range	Description
	Initialize	(1) Yes (2) No	Activates EAPOL state on this port.
	Administrative Status	(1) Force Unauthorized (2) Auto (3) Force Authorized	Allows you to set the EAPOL authorization status: Force Unauthorized—Always unauthorized Auto—Status depends on EAP authentication results Force Authorized—Always authorized
	Operational Status	(1) Authorized (2) Unauthorized	Displays the current authorization status.
	Administrative Traffic Control	(1) In & Out (2) In Only	Allows you to set EAPOL authentication either for incoming and outgoing traffic or for incoming traffic only.
	Operational Traffic Control	(1) In & Out (2) In Only	Displays the current administrative traffic control setting.
	Re-authenticate Now	(1) No (2) Yes	Allows you to activate EAPOL authentication immediately, without waiting for the re-authentication period to expire.
	Re-authentication	(1) Disabled (2) Enabled	Allows you to repeat EAPOL authentication according to the time value specified in Re-authentication Period field.
	Re-authentication Period	1to 604800	With Re-authentication enabled, allows you to specify the time period between successive EAPOL authentications.
	Quiet Period	0 to 65535	Allows you to specify the time interval between an authentication failure and the start of a new authentication attempt.
	Transmit Period	1to 65535	Allows you to specify how long the switch waits for the supplicant to respond to EAP Request/Identity packets.
	Supplicant Timeout	1to 65535	Allows you to specify how long the switch waits for the supplicant to respond to all EAP packets, except EAP Request/Identity packets.
	Server Timeout	1to 65535	Allows you to specify how long the switch waits for the RADIUS server to respond to all EAP packets.
	Maximum Requests	1to 10	Allows you to specify the number of times the switch attempts to resend EAP packets to a supplicant.

- 2 Complete fields as described in the table.
- 3 Click Submit.

## Configuring MAC Address-based Security

The MAC address-based security system allows you to specify a range of system responses to unauthorized network access to your switch with the Web-based management system.

The system response can range from sending a trap to disabling the port. The network access control is based on the MAC source addresses (SAs) of the authorized stations. You can specify a list of up to 448 MAC SAs that are authorized to access the switch. You can also specify the ports that each MAC SA is allowed to access. The options for allowed MAC SA port access include: NONE, ALL, and single or multiple ports that are specified in a list, for example, 1-4, 6, 9, and so forth. You must also include the MAC SA of any router connected to any secure ports.

When the switch software detects an SA security violation, the response can be to send a trap, turn on destination address (DA) filtering for all SAs, disable the specific port, or any combination of these three options.

You can configure the Ethernet Routing Switch to drop all packets having a specified MAC destination address (DA). You can create a list of up to 10 MAC DAs you want to filter. The packet with the specified MAC DA will be dropped regardless of the ingress port, source address (SA) intrusion, or VLAN membership.



**Note:** Ensure that you do not enter the MAC address of the switch you are working on.

---



**Note:** You must ensure that the ports are enabled after configuring the MAC address-based security.

---

## Configuring MAC Address-based Security

To configure MAC address-based security using the Web-based management system:

- 1 From the main menu, choose Application > MAC Address Security > Security Configuration.

The Security Configuration page opens (Figure 26).

**Figure 26** Security Configuration page

### Application > MAC Address Security > Security Configuration

MAC Address Security Setting	
MAC Address Security	Disabled ▾
MAC Address Security SNMP-Locked	Disabled ▾
Partition Port on Intrusion Detected	Disabled ▾
Partition Time	<input type="text"/> (1... 65535)
DA Filtering on Intrusion Detected	Disabled ▾
Generate SNMP Trap on Intrusion	Disabled ▾

**Submit**

MAC Security Table			
	Action	Port List	Current Learning Mode
Clear by Ports			
Learn by Ports			Disabled ▾

**Submit**

Table 25 describes the items on the Security Configuration page.

**Table 25** Security Configuration page items

Section	Item	Range	Description
MAC Address Security Setting	MAC Address Security	(1) Enabled (2) Disabled	Enables the MAC address security features.
	MAC Address Security SNMP-Locked	(1) Enabled (2) Disabled	Enables locking SNMP, so that you cannot use SNMP to modify the MAC address security features.
	Partition Port on Intrusion Detected	(1) Forever (2) Enabled (3) Disabled	Configures how the switch reacts to an intrusion event: Forever—The port is disabled and remains disabled (partitioned) until reset. The port does not reset after the Partition Time elapses. Enabled—The port is disabled, then automatically reset to enabled after the time specified in the Partition Time field elapses. Disabled—The port remains enabled, even if an intrusion event is detected.
	Partition Time	1 to 65535	Sets the time to partition a port on intrusion.  Note: Use this field only if the Partition Port on Intrusion Detected field is set to Enabled.
	DA Filtering on Intrusion Detected	(1) Enabled (2) Disabled	Enables you to isolate the intruding node (discard) the packets.
	Generate SNMP Trap on Intrusion	(1) Enabled (2) Disabled	Enables generation of an SNMP when an intrusion is detected.
MAC Security Table/Clear by Ports	Action		Allows you to clear specific ports from participation in the MAC address security features.
	Port List		Will be blank.
	Current Learning Mode		Will be blank.
MAC Security Table/Learn by Ports	Action		Allows you to identify ports that will learn incoming MAC addresses. All source MAC addresses of any packets received on a specified port(s) are added to the MAC Security Table (maximum of 448 MAC addresses allowed).

**Table 25** Security Configuration page items (continued)

Section	Item	Range	Description
	Port List		Displays all the ports that will learn incoming MAC address to detect intrusions (unallowed MAC addresses).
	Current Learning Mode	(1) Enabled (2) Disabled	Enables learning.

- 2 On the Security Configuration page, type information in the text boxes, or select from a list.
- 3 Click Submit.

## Enabling Security on Ports

To enable or disable MAC address-based security on the port:

- 1 From the main menu, choose Application > MAC Address Security > Port Configuration.

The Port Configuration page opens ([Figure 27](#)).

**Figure 27** Port Configuration page**Application > MAC Address Security > Port Configuration**

MAC Address Security > Port Configuration		
Port	Trunk	Security
1		Disabled ▾
2		Disabled ▾
3		Disabled ▾
4		Disabled ▾
5		Disabled ▾
6		Disabled ▾
7		Disabled ▾
8		Disabled ▾
9		Disabled ▾
10		Disabled ▾
11		Disabled ▾
12		Disabled ▾
13		Disabled ▾
14		Disabled ▾
15		Disabled ▾
16		Disabled ▾
17		Disabled ▾
18		Disabled ▾
19		Disabled ▾
20		Disabled ▾

[Table 26](#) describes the items on the Port Configuration page.

**Table 26** Port Configuration page items

Item	Range	Description
Port	1 to 24	Lists each port on the unit.

**Table 26** Port Configuration page items

Item	Range	Description
Trunk	Blank, 1 to 6	Displays the MultiLink Trunk that the port belongs to.
Security	(1) Enabled (2) Disabled	Enables MAC address-based security on that port.  Note: You must configure the port for MAC address-based security before enabling the security.

## Deleting Ports

You can delete ports from the security system in a variety of ways:

- In the Ports List View, Port List page ([Figure 29](#)), click on the checkmark of a selected port to delete that port from the specified port list.
- In the Ports List View, Learn by Ports page ([Figure 30](#)), click on the checkmark of a selected port to remove that port from those that learn MAC addresses.
- In the Port Configuration page ([Figure 27](#)), click Disabled to remove that port from the MAC address-based security system; it will disable all MAC address-based security on that port.

## Port Lists

In this section, you create a list of ports, and you can add ports to or delete ports from each list.

To activate an entry or add or delete ports to a list:

- 1 From the main menu, choose Application > MAC Address Security > Port Lists.

The Port Lists page opens ([Figure 28](#)).

**Figure 28** Port Lists page**Application > MAC Address Security > Port Lists**

Application > MAC Address Security > Port Lists		
Entry	Action	Port List
S1		1-4,6-24
S2		2
S3		
S4		
S5		
S6		
S7		
S8		
S9		
S10		
S11		
S12		
S13		
S14		
S15		
S16		
S17		
S18		
S19		
S20		

[Table 27](#) describes the items on the Ports Lists page.

**Table 27** Ports Lists page items

Item	Description
Entry	These are the lists of ports.
Action	 Allows you to add or delete ports to the lists. The range is 1 to 24.
Port List	Displays which ports are associated with each list.

- 2 To add or delete ports to a list, click the icon in the Action column in the list row you want.

The Port List View, Port List page opens (Figure 29).

**Figure 29** Port List View, Port List page

### Application > MAC Address Security: Port List View

Application > MAC Address Security > Port List (Entry S1)																								
Port All	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Submit Back

- a Click the ports you want to add to the selected list or click All.
  - b To delete a port from a list, uncheck the box by clicking it.
  - c Click Submit.
- 3 From the main menu, choose Application > MAC Address Security > Security Configuration.  
The Security Configuration page opens (Figure 26).
  - 4 In the MAC Security Table section of the Security Configuration page, click the icon in the Action column of the Learn By Ports row.  
The Port List View, Learn by Ports page opens (Figure 30).

**Figure 30** Port List View, Learn by Ports page**Application > MAC Address Security: Port List View**

**Application > MAC Address Security > Security Configuration: Learn by Ports**

Port	All	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
	<input type="checkbox"/>																								

- a Click the ports through which you want the switch to learn MAC addresses or click All.
  - b If you want that port to no longer learn MAC addresses, click the checked box to uncheck it.
  - c Click Submit.
- 5 In the MAC Security Table section of the Security Configuration page, choose Enabled in the Current Learning Mode column of the Learn By Ports row.
  - 6 Click Submit.



**Note:** You cannot include any of the port values you have chosen for the secure ports field.

## Adding MAC Addresses

To add MAC address to the MAC address-based security system:

- 1 In the main menu, choose Applications > MAC Address Security > Security Table.

It may take awhile for the required addresses to be learned. Then, the Security Table page opens (Figure 31).

**Figure 31** Security Table page**Application > MAC Address Security > Security Table**

MAC Address Security Table		
Action	MAC Address	Allowed Source

MAC Address Security Table Entry Creation		
MAC Address	<input type="text"/>	
Allowed Source	Port: <input type="text"/>	Entry: <input type="text"/>



**Note:** Using this page, you can instruct the switch to allow the specified MAC address access *only* through the specified port or port list.

Table 28 describes the items on the Security Table page.

**Table 28** Security Table page items

Section	Item	Range	Description
MAC Address Security Table	Action		Allows you to delete a MAC address.
	MAC Address		Displays the MAC address.
	Allowed Source	(1) Port (2) Entry	Displays the entry through which the MAC address is allowed.
MAC Address Security Table Entry Creation	MAC Address		Enter the MAC address you want to allow to access the switch.
	Allowed Source		Select the port through which the MAC address is allowed.
	Entry		Select the port list through which the MAC address is allowed.

- 2 Complete fields as described in the table.



**Note:** If you choose an Entry as the Allowed Source, you must have configured that specific entry on the Port View List, Port List page.

---

- 3 On the Security Table page, type information in the text boxes, or select from a list.
- 4 Click Submit.



**Note:** Be certain to include the MAC address for the default LAN router as an allowed source MAC address.

---

## Clearing Ports

You can clear all information from the specified port(s) for the list of ports that learn MAC addresses. If Learn by Ports is enabled, the specified ports will begin again to learn the MAC addresses.

To clear information from selected ports:

- 1 From the main menu, choose Application > MAC Address Security > Security Configuration.

The Security Configuration page opens ([Figure 26](#)).

- 2 In the MAC Security Table section of the Security Configuration page, click the icon in the Action column of the Clear By Ports row.

The Port List View, Clear by Ports page opens ([Figure 32](#)).

**Figure 32** Port List View, Clear by Ports page**Application > MAC Address Security: Port List View**

**Application > MAC Address Security > Security Configuration: Clear by Ports**

Port	All	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
	<input type="checkbox"/>																								

- 3 Select the ports you want to clear or click All.
- 4 Click Submit.



**Note:** When you specify a port (or ports) to be cleared using this field, the specific port (or ports) will be cleared for each of the entries listed in the MAC Address Security Table. If you totally clear the allowed Source Port(s) field (leaving a blank field) for an entry, the associated MAC address for that entry is also cleared.

## Filtering MAC Destination Addresses

To drop all packets from a specified MAC destination address (DA):

- 1 From the main menu, choose Application > MAC Address Security > DA MAC Filtering.

The DA MAC Filtering page opens ([Figure 33](#)).

**Figure 33** DA MAC Filtering page**Application > MAC Address Security > DA MAC Filtering**

Destination MAC Address Filtering Table		
Action	Index	MAC Address

DA MAC Filtering Entry Creation	
DA MAC Address	<input type="text" value="(XX-XX-XX-XX-XX-XX)"/>

Table 29 describes the items on the DA MAC Filtering page.

**Table 29** DA MAC Filtering page items

Section	Item	Range	Description
Destination MAC Address Filtering Table	Action		Allows you to delete a MAC DA you are filtering.
	Index		Displays index number of the MAC DA you want filtered.
	MAC Address	1 -10	Displays list of MAC DAs you want filtered.
DA MAC Filtering Entry Creation	DA MAC Address	XX-XX-XX-XX-XX-XX	Enter the MAC DA you want to filter.



**Note:** Ensure that you do not enter the MAC address of the management station.

- In the DA MAC Filtering Entry Creation area, enter the MAC DA you want to filter.

You can list up to 10 MAC DAs to filter.

- 3 Click Submit.

The system returns you to the DA MAC Filtering page ([Table 33](#)) with the new DA listed in the table.

## Deleting MAC DAs

To delete a MAC DA:

- 1 From the main menu, choose Application > MAC Address Security > DA MAC Filtering.

The DA MAC Filtering page opens ([Figure 33](#)).

- 2 In the Destination MAC Address Filtering Table, click the Delete icon for the entry you want to delete.

A message opens prompting you to confirm your request.

- 3 Do one of the following:

- Click Yes to delete the target parameter configuration.
- Click Cancel to return to the table without making changes.

## Viewing Learned MAC Addresses by VLAN

You can view MAC addresses and their associated port or trunk that the switch configuration has learned, based on the VLAN you select.

To view learned MAC addresses and their associated port or trunk:

- 1 From the main menu, choose Configuration > MAC Address Table.

The MAC Address Table page opens ([Figure 34](#)).

**Figure 34** MAC Address Table page**Configuration > MAC Address Table**

**MAC Address Setting**

Aging Time  seconds

Select VLAN

**Submit**

**MAC Address Table**  
(Number of addresses: 18)

MAC Address	Source
-------------	--------

[Table 30](#) describes the items on the MAC Address Table page.

**Table 30** MAC Address Table page items

Section	Item	Range	Description
MAC Address Setting	Aging Time	10 to 1000000	Type the timeout period, in seconds, for aging out dynamically learned forwarding information. If the entry is inactive for a period of time that exceeds the specified aging time, the address is removed.  Note: Nortel recommends using the default value of 300 seconds.
	Select VLAN	1 to 256	Choose the VLAN on which to view learned MAC addresses.
MAC Address Table	MAC Address		The unicast MAC address for which the bridge has forwarding and/or filtering information.
	Source		The source of the discovered MAC address.

- 2** In the MAC Address Setting section, choose the aging time and VLAN you want to view learned MAC addresses on.
- 3** Click Submit.

Your request is displayed in the MAC Address Table ([Figure 34](#)).

## Locating a Specific MAC Address

You can search for a specific MAC address among all the MAC addresses learned from all the VLANs. This is a useful tool for finding whether or not a switch has learned a particular address.

To locate a specific MAC addresses:

- 1 From the main menu, choose Configuration > Find MAC Address.

The Find MAC Address page opens (Figure 35).

**Figure 35** Find MAC Address Table page

### Configuration > Find MAC Address Table

Find MAC Address Setting	
Find MAC Address	00-00-00-00-00-00 Not Found

Submit

MAC Address Table	
MAC Address	Source
00-00-81-9B-12-77	Port: 21
00-00-81-9B-12-78	Port: 21
00-00-E2-13-38-38	Port: 21
00-00-E2-13-AB-63	Port: 21
00-00-E2-1F-9D-0D	Port: 21
00-09-97-89-82-C1	Port: 21
00-09-97-F7-9E-00	Port: 21
00-0C-F8-61-00-00	
00-0E-62-CD-13-F4	Port: 21
00-0F-CD-BF-1E-81	Port: 21
00-80-2D-6E-47-38	Port: 21
00-80-2D-6E-47-82	Port: 21

[Table 31](#) describes the items on the Find MAC Address Table page.

**Table 31** Find MAC Address Table page items

Section	Item	Description
Find MAC Address Settings	Find MAC Address	Determine if the bridge has forwarding and (or) filtering information for the specified MAC address
Mac Address Table	MAC Address	The unicast MAC address for which the bridge has forwarding and (or) filtering information.
	Source	The source of the discovered MAC address.

- 2 In the MAC Address Setting section, type the MAC address you want to search for.
- 3 Click Submit to enter the request.

If the address is located, it is shown in the first row in the MAC Address Table section. If the address is not located, the system response “Not Found” is shown to the right of the Find MAC Address input field.

## Configuring Port’s Autonegotiation, Speed, Duplex, Status, and Alias

You can configure a specific switch port or all switch ports to autonegotiate for the highest available speed of the connected station or you can set the speed for selected switch ports.

You can name each port, or assign an alias to it, using 27 alphanumeric characters.

To configure a switch port’s alias, status, autonegotiation and speed/duplex:

- 1 From the main menu, choose Configuration > Port Management.  
The Port Management page opens ([Figure 36](#)).

Figure 36 Port Management page

**Configuration > Port Management**

Port Management Setting							
Port	Alias	Trunk	Status	Link	Link Trap	Autonegotiation	Speed / Duplex
1	<input type="text"/>	<input type="checkbox"/>	Enabled ▾	Down	On ▾	Enabled ▾	<input type="text"/>
2	<input type="text"/>	<input type="checkbox"/>	Enabled ▾	Down	On ▾	Enabled ▾	<input type="text"/>
3	<input type="text"/>	<input type="checkbox"/>	Enabled ▾	Down	On ▾	Enabled ▾	<input type="text"/>
4	<input type="text"/>	<input type="checkbox"/>	Enabled ▾	Down	On ▾	Enabled ▾	<input type="text"/>
5	<input type="text"/>	<input type="checkbox"/>	Enabled ▾	Down	On ▾	Enabled ▾	<input type="text"/>
6	<input type="text"/>	<input type="checkbox"/>	Enabled ▾	Down	On ▾	Enabled ▾	<input type="text"/>
7	<input type="text"/>	<input type="checkbox"/>	Enabled ▾	Up	On ▾	Enabled ▾	100Mbps / Full ▾
8	<input type="text"/>	<input type="checkbox"/>	Enabled ▾	Down	On ▾	Enabled ▾	<input type="text"/>
9	<input type="text"/>	<input type="checkbox"/>	Enabled ▾	Down	On ▾	Enabled ▾	<input type="text"/>
10	<input type="text"/>	<input type="checkbox"/>	Enabled ▾	Down	On ▾	Enabled ▾	<input type="text"/>
11	<input type="text"/>	<input type="checkbox"/>	Enabled ▾	Down	On ▾	Enabled ▾	<input type="text"/>
12	<input type="text"/>	<input type="checkbox"/>	Enabled ▾	Down	On ▾	Enabled ▾	<input type="text"/>
Switch		<input type="checkbox"/>	Enable ▾ <input type="checkbox"/>		On ▾ <input type="checkbox"/>	Enable ▾ <input type="checkbox"/>	<input type="text"/> <input type="checkbox"/>

Submit

[Ports 13 - 24](#)

[Table 32](#) describes the items on the Port Management page.

**Table 32** Port Management page items

Item	Range	Description
Port		The switch port number of the corresponding row. To select the switch row, click the check box to the right. The values that you set in each switch row affect all switch ports. For information on setting high speed flow control for SFP GBICs, see <a href="#">“Configuring High Speed Flow Control” on page 107</a> .
Alias	27 alphanumeric characters	Displays the name, or alias, you assigned the port. To assign a name or to change the name, enter up to 26 alphanumeric characters.
Trunk		The trunk group that the switch port belongs to as specified in the Trunk Member fields on the MultiLink Trunk page. For more information, see <a href="#">“Configuring MultiLink Trunk Members” on page 184</a> .
Status	(1) Enabled (2) Disabled	Choose to enable or disable the port. You can also use this field to control access to any switch port.  The default setting is Enabled.
Link		The current link state of the corresponding port as follows: Up: The port is connected and operational Down: The port is not connected or is not operational.
Link/Trap	(1) On (2) Off	Choose to control whether link up/down traps are sent to the configured trap sink from the switch.  The default setting is On.
Autonegotiation	(1) Enabled (2) Disabled	Choose to enable or disable the autonegotiation feature.  Choosing to enable autonegotiation sets the corresponding port speed to match the best service provided by the connected station, up to 100Mb/s in full-duplex mode.  <b>Note</b> Autonegotiation also enables autopolarity and auto mdi/mdix.  The default setting is Enabled.
Speed / Duplex	(1) 10Mbps / Half (2) 10Mbps / Full (3) 100Mbps / Half (4) 100Mbps / Full (5) 1000Mbps / Full	Choose the Ethernet speed you want the port to support.  The default setting is 100Mbps/Half when autonegotiation is disabled and 1000 Mb/s full-duplex for gigabit ports only.

- 2** In the port row of your choice, select from the lists.
- 3** Click Submit.

## Configuring High Speed Flow Control

Use this screen to set autonegotiation for all gigabit ports.

To configure high speed flow control:

- 1 From the main menu, choose Configuration > High Speed Flow Control.  
The High Speed Flow Control page opens (Figure 37).

**Figure 37** High Speed Flow Control page

### Configuration > High Speed Flow Control

High Speed Flow Control Setting			
Port	Autonegotiation	Speed / Duplex	Flow Control
1	Enabled	Unknown	N/A
2	Enabled	Unknown	N/A
3	Enabled	Unknown	N/A
4	Enabled	Unknown	N/A
5	Enabled	Unknown	N/A
6	Enabled	Unknown	N/A
7	Enabled	100Mbps / Full	N/A
8	Enabled	Unknown	N/A
9	Enabled	Unknown	N/A
10	Enabled	Unknown	N/A
11	Enabled	Unknown	N/A
12	Enabled	Unknown	N/A
Switch			Disabled <input type="checkbox"/>

Submit

Table 33 describes the items on the High Speed Flow Control page.

**Table 33** High Speed Flow Control page items

Item	Range	Description
Port	1 to 24	Displays the port number.
Autonegotiation	(1) Enabled (2) Disabled	Displays whether autonegotiation is enabled or disabled.  <b>NOTE:</b> You enable or disable autonegotiation on the Port Management page.  When enabled, the port advertises support for flow control autonegotiation.
Speed/Duplex	(1) 10Mbps / Half (2) 10Mbps / Full (3) 100Mbps / Half (4) 100Mbps / Full (5) 1000Mbps / Full (6) Unknown	Displays the speed and duplex values for each port.
Flow Control	(1) Disabled (2) Symmetric (3) Asymmetric	Displays flow control settings for each port.
Switch	(1) Disabled (2) Symmetric (3) Asymmetric	Choose the flow control preference to control traffic and avoid congestion.

**2** Select from the lists.

**3** Click Submit.

## Downloading Switch Images

You can download the Ethernet Routing Switch software image that is located in non-volatile flash memory. To download the Ethernet Routing Switch software image, a properly configured Trivial File Transfer Protocol (TFTP) server must be present in your network, and the policy switch must have an IP address. To learn how to configure the switch IP address, refer to [“Configuring BootP, IP, and Gateway Settings” on page 52](#).



**Caution:** Do not interrupt power to the device during the software download process. A power interruption can corrupt the firmware image.

---

To download a switch image:

- 1 From the main menu, choose Configuration > Software Download.  
The Software Download page opens ([Figure 38](#)).

**Figure 38** Software Download page**Configuration > Software Download**

Software Download Setting	
Current Running Version	v4.0.3.00
Local Store Version	v4.0.3.00
Software Image Filename	docu/dragline_403.img
Diagnostics Image Filename	<input type="text"/>
TFTP Server IP Address	198.202.188.174 <small>(xxx.xxx.xxx.xxx)</small>
Start TFTP Load of New Image	No <input type="button" value="v"/>

Table 34 describes the items on the Software Download page.

**Table 34** Software Download page items

Item	Range	Description
Current Running Version		The version of the current running software.
Local Store Version		The local version of the software in the flash memory.
Software Image Filename	1 to 30	Type the software image load filename.
Diagnostics Image Filename	1 to 30	Type the diagnostics filename.
TFTP Server IP Address	XXX.XXX.XXX.XXX	Type the IP address of your TFTP load host.
Start TFTP Load of New Image	(1) No (2) Software Image (3) Diagnostics Image (4) Software Image If Newer	Choose the software image to load.

- 2 Type information in the text boxes, or select from a list.
- 3 Click Submit.

The software download process automatically completes without user intervention. The process erases the contents of flash memory and replaces it with a new software image. Take care not to interrupt the download process until after it runs to completion (the process can take up to 10 minutes, depending on network conditions).

When the download process is complete, the switch automatically resets and the new software image initiates a self-test.

During the download process, the Ethernet Routing Switch is not operational.

## Storing and Retrieving Switch Configuration File from TFTP Server

You can store the switch configuration parameters on a Trivial File Transfer Protocol (TFTP) server. You can retrieve the configuration parameters of the switch and use the retrieved parameters to automatically configure a replacement switch..

To store a switch configuration, you must set up the file on your TFTP server and set the filename read/write permission to enabled.

To download the Ethernet Routing Switch configuration file, a properly configured TFTP server must be present in your network, and the policy switch must have an IP address. To learn how to configure the switch IP address, refer to [“Configuring BootP, IP, and Gateway Settings” on page 52](#).

To store or retrieve a switch configuration file:

- 1 From the main menu, choose Configuration > Configuration File.

The Configuration File Download/Upload page opens ([Figure 39](#)).

**Figure 39** Configuration File Download/Upload page**Configuration > Configuration File Download/Upload**

<b>Configuration File Setting</b>	
Configuration Image Filename	<input type="text"/>
TFTP Server IP Address	198.202.188.174 <small>(xxx.xxx.xxx.xxx)</small>
Copy Configuration Image to Server	No ▾
Retrieve Configuration Image from Server	No ▾

**Submit**

Table 35 describes the items on the Configuration File page.

**Table 35** Configuration File page items

Item	Range	Description
Configuration Image Filename	1 to 32	Type the configuration file name.
TFTP Server IP Address	XXX.XXX.XXX.XXX	Type the IP address of the TFTP load host.
Copy Configuration Image to Server	(1) Yes (2) No	Choose whether or not to copy the configuration image to the server.
Retrieve Configuration Image from Server	(1) Yes (2) No	Choose whether or not to retrieve the configuration image from a server. If you choose Yes, the download process begins immediately and, when completed, causes the switch to reset with the new configuration parameters.

- 2 Type information in the text boxes, or select from a list.
- 3 Click Submit.

[Table 36](#) describes the requirements for storing or retrieving configuration parameters on a TFTP server./

**Table 36** Requirements for retrieving configuration parameters on TFTP server

Requirements
<ul style="list-style-type: none"> <li>The Configuration File feature can only be used to copy <i>switch configuration parameters to other switches</i>.</li> </ul>
<ul style="list-style-type: none"> <li>A configuration file obtained from the switch can only be used to configure other switches that have the same firmware revision and model type as the donor switch.</li> </ul>
<ul style="list-style-type: none"> <li>The configuration file also duplicates any settings that exist for any SFP GBIC that is installed in the donor switch.</li> </ul>
<ul style="list-style-type: none"> <li>If you use the configuration file to configure another switch that has the same SFP GBIC model installed, the configuration file settings will also apply to and override the existing SFP GBIC settings.</li> </ul>

[Table 37](#) describes the parameters that are not saved to the configuration file.

**Table 37** Parameters not saved to the configuration file

These parameters are not saved	Used in this screen	See page:
In-Band Switch IP Address	IP Configuration	
In-Band Subnet Mask	IP Configuration	
Default Gateway	IP Configuration	
Configuration Image Filename	Configuration File Download/Upload	<a href="#">111</a>
TFTP Server IP Address	Configuration File Download/Upload	
Console Read-Only Switch Password	Console/Comm Port Configuration	<a href="#">113</a>
Console Read-Write Switch Password	Console/Comm Port Configuration	



**Note:** The console Read-Only and Read-Write switch passwords are for the Telnet, Web and CLI interface.

## Configuring Port Communication Speed

You can view the current console/communication port settings and configure the console port baud rate to match the baud rate of the console terminal.

To view current console/communication port settings and configure console port speed:

- 1 From the main menu, choose Configuration > Console/Comm Port.

The Console/Communication Port page opens (Figure 40).

**Figure 40** Console/Communication Port page

Table 38 describes the items on the Console/Communication Port page.

**Table 38** Console/Communication Port Setting page items

Item	Range	Description
Comm Port Data Bits		Displays the current console communication port data bit setting.
Comm Port Parity		Displays the current console communication port parity setting.
Comm Port Stop Bits		Displays the current console communication port stop bit setting.
Console Port Speed	2400 4800 9600 19200 38400	Choose the console port speed baud rate.  Note: The default setting is 9600.
		<b>Caution:</b> If you choose a baud rate that does not match your console terminal baud rate, you will lose communication with the configuration interface when you click Submit.

- 2** Select from the list.
- 3** Click Submit.



---

## Chapter 5

# Configuring Remote Network Monitoring

---

The Configuring Remote Network Monitoring (RMON) Management Information Base (MIB) is an interface between the RMON agent on a Ethernet Routing Switch and RMON management applications such as the Web-based management user interface. It defines objects that are suitable for the management of any type of network. Some groups are specifically targeted for Ethernet networks.

The RMON agent continuously collects statistics and proactively monitors the switch.

The RMON options available are:

- [“Configuring RMON Fault Threshold Parameters”](#), next
- [“Viewing the RMON Fault Event Log”](#) on page 121
- [“Viewing the System Log”](#) on page 122
- [“Viewing RMON Ethernet Statistics”](#) on page 124
- [“Viewing RMON History”](#) on page 127

## Configuring RMON Fault Threshold Parameters

Alarms are useful when you need to know when the value of some variable goes out of range. RMON alarms can be defined on any MIB variable that resolves to an integer value. String variables (such as system description) cannot be used as alarm variables.

### Creating an RMON Fault Threshold

You can create the RMON threshold parameters for fault notification (alarms).

To create an RMON threshold:

- 1 From the main menu, choose Fault > RMON Threshold.

The RMON Threshold page opens (Figure 41).

**Figure 41** RMON Threshold page

### Fault > RMON Threshold

RMON Threshold Table										
Action	Index	Target	Parameter	Current Level	Rising Level	Rising Action	Falling Level	Falling Action	Interval	Sample
<div style="border: 1px solid black; padding: 5px;"> <p><b>RMON Threshold Creation</b></p> <p>Alarm Index <input type="text"/></p> <p>Port <input type="text"/></p> <p>Parameter <input type="text" value="Good-Bytes"/></p> <p>Rising Level <input type="text"/></p> <p>Falling Level <input type="text"/></p> <p>Rising Action <input type="text" value="None"/></p> <p>Interval <input type="text"/> seconds</p> <p>Alarm Sample <input type="text" value="Absolute"/></p> <p style="text-align: center;"><input type="button" value="Submit"/></p> </div>										

Table 39 describes the items on the RMON Threshold page.

**Table 39** RMON Threshold page items

Item	Range	Description
		Deletes the row.
Alarm Index		Type the unique number to identify the alarm entry.
Port	1 to 24	Choose the port on which to set an alarm.

**Table 39** RMON Threshold page items (continued)

Item	Range	Description
Parameter	(1) Good-Bytes (2) Good-Packets (3) Multicast (4) Broadcast (5) CRC-Errors (6) Runts (7) Fragments (8) Frame-Too-Long (9) Collisions	Choose the sampled statistic.
Rising Level	Integer	Type the event entry to be used when a rising threshold is crossed.  Note: When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event will be generated. After a rising event is generated, another such event is not generated until the sampled value falls below this threshold and reaches the Falling Threshold.
Falling Level	Integer	Type the event entry to be used when a falling threshold is crossed.  Note: When the current sampled value is lower than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single event will be generated. After a falling event is generated, another such event is not generated until the sampled value rises over this threshold and reaches the Rising Threshold.
Rising Action	(1) None (2) Log (3) SNMP-Trap (4) Log-and-Trap	Choose the type of notification for the event. Selecting Log generates an entry in the RMON Event Log table for each event. Selecting SNMP Trap sends an SNMP trap to one or more management stations.
Interval		Type the time period (in seconds) to sample data and compare the data to the rising and falling thresholds.

**Table 39** RMON Threshold page items (continued)

Item	Range	Description
Alarm Sample	(1) Absolute (2) Delta	<p>Choose the sampling method:</p> <p><b>Absolute:</b> <i>Absolute</i> alarms are defined on the current value of the alarm variable. An example of an alarm defined with absolute value is card operating status. Because this value is not cumulative, but instead represents states, such as card up (value 1) and card down (value 2), you set it for absolute value. Therefore, an alarm could be created with a rising value of 2 and a falling value of 1 to alert a user to whether the card is up or down.</p> <p><b>Delta:</b> Most alarm variables related to Ethernet traffic are set to <i>delta</i> value. Delta alarms are defined based on the difference in the value of the alarm variable between the start of the polling period and the end of the polling period. Delta alarms are sampled twice per polling period. For each sample, the last two values are added together and compared to the threshold values. This process increases precision and allows for the detection of threshold crossings that span the sampling boundary. Therefore, if you keep track of the current values of a given delta-valued alarm and add them together, the result is twice the actual value. (This result is not an error in the software.)</p>

- 2 In the RMON Threshold Creation section, type information in the text boxes, or select from a list.
- 3 Click Submit.

The new configuration is displayed in the RMON Threshold Table (Figure 41).



**Note:** RMON threshold configurations are not modifiable. They must be deleted and the information recreated.

## Deleting an RMON Threshold Configuration

To delete an existing RMON threshold configuration:

- 1 From the main menu, choose Fault > RMON Threshold.  
The RMON Threshold page opens (Figure 41).
- 2 In the RMON Threshold Table, click the Delete icon for the entry you want to delete.

A message opens prompting you to confirm your request.

- 3** Do one of the following:
  - Click Yes to delete the RMON threshold configuration.
  - Click Cancel to return to the RMON Threshold page without making changes.

## Viewing the RMON Fault Event Log

RMON events and alarms work together to notify you when values in your network go out of a specified range. When values pass the specified ranges, the alarm is triggered and “fires.” The event specifies how the activity is recorded.

An event specifies whether a trap, a log, or a trap and a log are generated to view alarm activity. When RMON is globally enabled, two default events are generated:

- Rising Event
- Falling Event

Default events specify that when an alarm goes out of range, the firing of the alarm is tracked in both a trap and a log. For example, when an alarm fires at the rising threshold, the rising event specifies that this information be sent to both a trap and a log. The RMON Event Log page works in conjunction with the RMON Threshold page to enable you to view a history of RMON fault events.

To view a history of RMON fault events:

- From the main menu, choose Fault > RMON Event Log.

The RMON Event Log page opens ([Figure 42](#)).

**Figure 42** RMON Event Log page**Fault > RMON Event Log**

RMON Event Log			
Time Stamp	Description	Triggered By	ID

[Table 40](#) describes the fields on the RMON Event Log page.

**Table 40** RMON Event Log page fields

Item	Description
Time Stamp	The time the event occurred since the system was last rebooted.
Description	An implementation dependent description of the event that activated this log entry.
Triggered By	A comment describing the source of the event.
ID	The event that generated this log entry.

## Viewing the System Log

You can view a display of messages contained in non-volatile random access memory (NVRAM) or dynamic random access memory (DRAM) and NVRAM.

To open the System Log page:

- 1 From the main menu, choose **Fault > System Log**.

The System Log page opens ([Figure 43](#)).

**Figure 43** System Log page**Fault > System Log**

System Log (View By)	
Display Messages From	Non Volatile
Clear Messages From	None

Submit

System Log			
Index	Time Stamp	Message Type	Message

Table 41 describes the fields on the System Log page.

**Table 41** System Log page fields

Section	Item	Range	Description
System Log (View By)	Display Messages From	(1) Non Volatile (2) Volatile + Non Volatile	Choose to display messages from Non Volatile memory (NVRAM) or Volatile (DRAM) and Non Volatile memory.  The default settings is Non Volatile.
	Clear Messages From	(1) Volatile (2) Volatile + Non Volatile (3) None	Choose to clear messages from Volatile memory or Volatile and Non Volatile memory.  The default settings is None (do not clear messages)
System Log	Index		The number of the event.
	Time Stamp		The time, in hundreths of a second, between system initialization and the time the log messages entered the system.

**Table 41** System Log page fields

Section	Item	Range	Description
	Message Type		The type of message. The options are (1) Critical, (2) Serious, and (3) Informational.
	Message		A character string that identifies the origin of the message and the reason why the message was generated.

- 2** In the System Log (View By) section do one or more of the following:
  - Choose where to display messages from.
  - Choose to clear messages from Volatile or Non Volatile memory.
- 3** Click Submit.

The results of your request are displayed in the System Log section ([Figure 43](#)).

## Viewing RMON Ethernet Statistics

You can gather and graph RMON Ethernet statistics in a variety of formats.

To gather and graph RMON Ethernet statistics:

- 1** From the main menu, choose Statistics > RMON Ethernet.

The RMON Ethernet page opens ([Figure 44](#)).

Figure 44 RMON Ethernet page (1 of 2)

## Statistics &gt; RMON Ethernet

RMON Ethernet Statistics Table									
Port	Drop Events	Octets	Packets	Broadcast	Multicast	CRC Align Errors	Undersize	Fragments	Collisions
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	127	83128567	1239758	838462	390666	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0

**Figure 45** RMON Ethernet page (2 of 2)

Packets 64 - 127 bytes	Packets 128 - 255 bytes	Packets 256 - 511 bytes	Packets 512 - 1023 bytes	Packets 1024 - 1518 bytes	Packets 1522 - 9216 bytes
0	0	0	0	0	0
0	0	0	0	0	0
0	0	0	0	0	0
0	0	0	0	0	0
0	0	0	0	0	0
0	0	0	0	0	0

Table 42 describes the items on the RMON Ethernet page.

**Table 42** RMON Ethernet page items

Item	Description
Port	The port number that corresponds to the selected switch.
Drop Events	The number of events in which packets were dropped by the interface due to a lack of resources.
Octets	The number of octets of data (including those in bad packets) received on the network (excluding framing bits, but including Frame Check Sequence (FCS) octets).
Packets	The number of good packets received that were directed to the broadcast address. This <i>does not</i> include multicast packets.
Broadcast	The number of good packets received that were directed to the broadcast address. This <i>does not</i> include multicast packets.
Multicast	The number of good packets received that were directed to the multicast address. This <i>does not</i> include packets sent to the broadcast address.
CRC Align Errors	The number of packets received that had a length (excluding and 1518 octets, inclusive, but had a bad Frame FCS with an integral number of octets (FCS errors).
Undersize	The number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well-formed.
Fragments	The number of packets received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either FCS or frame error.
Collisions	The “best estimate” number of collisions on this Ethernet segment.

**Table 42** RMON Ethernet page items (continued)

Item	Description
Jabbers	The number of packets received that were longer than 1518 octets in length (excluding framing bits, but including FCS octets), and had either FCS or frame error.
Packets < = 64 bytes 65-127 bytes 128-255 bytes 256-511 bytes 512-1023 bytes 1024-1518 bytes 1522-9216 bytes	The number of octets received (including bad packets) in length (excluding framing bits, but including FCS octets).

- 2 Click Submit.

The RMON Ethernet Statistics Table is updated with information about the selected device (Figure 44).

## Viewing RMON History

You can view a periodic statistical sampling of data from various types of networks.

To view periodic statistical data:

- 1 From the main menu, choose Statistics > RMON History.

The RMON History page opens (Figure 46).

Figure 46 RMON History page

## Statistics &gt; RMON History

**RMON History Statistics (View By)**  
 Port

Submit

**RMON History Statistics Table**

Start	Drop Events	Octets	Packets	Broadcast	Multicast	CRC Align Errors	Undersize	Oversize
1 Weeks 3 Hours 13 Minutes 11 Seconds	0	0	0	0	0	0	0	0
1 Weeks 3 Hours 13 Minutes 41 Seconds	0	0	0	0	0	0	0	0
1 Weeks 3 Hours 14 Minutes 11 Seconds	0	0	0	0	0	0	0	0
1 Weeks 3 Hours 14 Minutes 41 Seconds	0	0	0	0	0	0	0	0
1 Weeks 3 Hours 15 Minutes 11 Seconds	0	0	0	0	0	0	0	0
1 Weeks 3 Hours 15 Minutes 41 Seconds	0	0	0	0	0	0	0	0
1 Weeks 3 Hours 16 Minutes 11 Seconds	0	0	0	0	0	0	0	0
1 Weeks 3 Hours 16 Minutes 41 Seconds	0	0	0	0	0	0	0	0
1 Weeks 3 Hours 17 Minutes 11 Seconds	0	0	0	0	0	0	0	0
1 Weeks 3 Hours 17 Minutes 41 Seconds	0	0	0	0	0	0	0	0
1 Weeks 3 Hours 18 Minutes 11 Seconds	0	0	0	0	0	0	0	0
1 Weeks 3 Hours 18 Minutes 41 Seconds	0	0	0	0	0	0	0	0
1 Weeks 3 Hours 19 Minutes 11 Seconds	0	0	0	0	0	0	0	0
1 Weeks 3 Hours 19 Minutes 41 Seconds	0	0	0	0	0	0	0	0
1 Weeks 3 Hours 20 Minutes 11 Seconds	0	0	0	0	0	0	0	0

Table 43 describes the items on the RMON History page.

Table 43 RMON History page items

Section	Item	Description
RMON History Statistics (View By)	Port	Choose the port number to be monitored.
RMON History Statistics Table	Start	The value of the sysUptime at the start of the interval over which this sample was measured.
	Drop Events	The number of events in which packets were dropped by the interface due to a lack of resources.

**Table 43** RMON History page items

Section	Item	Description
	Octets	The number of octets of data (including those in bad packets) received on the network (excluding framing bits, but including Frame Check Sequence (FCS) octets).
	Packets	The number of good packets received that were directed to the broadcast address. This <i>does not</i> include multicast packets.
	Broadcast	The number of good packets received that were directed to the broadcast address. This <i>does not</i> include multicast packets.
	Multicast	The number of good packets received that were directed to the multicast address. This <i>does not</i> include packets sent to the broadcast address.
	CRC Align Errors	The number of packets received that had a length (excluding and 1518 octets, inclusive, but had a bad Frame FCS with an integral number of octets (FCS errors).
	Undersize	The number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well-formed.
	Oversize	The number of packets received that were longer than 1518 octets long (excluding framing bits, but including FCS octets) and were otherwise well-formed.

- 2 In the RMON History Statistics section, choose the unit and port number to be monitored.
- 3 Click Submit.

The RMON History Statistics Table is updated with information about the selected device and port (Figure 46).



---

## Chapter 6

# Viewing System Statistics

---

The options available to monitor system statistical data are:

- “Viewing Port Statistics”, next
- “Viewing all Port Errors” on page 134
- “Viewing Interface Statistics” on page 136
- “Viewing Ethernet Error Statistics” on page 138
- “Viewing Transparent Bridging Statistics” on page 140

## Viewing Port Statistics

You can view detailed statistics about a selected switch port. Both received and transmitted statistics are displayed so that you can compare throughput or other port parameters.

To view statistical data about a selected switch port:

- 1 From the main menu, choose Statistics > Port.

The Port page opens (Figure 47).

Figure 47 Port page

**Statistics > Port**

**Port Statistics (View By)**

Port

Port Statistics Table			
Received		Transmitted	
Packets	<input type="text" value="0"/>	Packets	<input type="text" value="0"/>
Multicasts	<input type="text" value="0"/>	Multicasts	<input type="text" value="0"/>
Broadcasts	<input type="text" value="0"/>	Broadcasts	<input type="text" value="0"/>
Total Octets	<input type="text" value="0"/>	Total Octets	<input type="text" value="0"/>
Pause Frames	<input type="text" value="0"/>	Pause Frames	<input type="text" value="0"/>
FCS/Frame Errors	<input type="text" value="0"/>	Collisions	<input type="text" value="0"/>
Undersized Packets	<input type="text" value="0"/>	Single Collisions	<input type="text" value="0"/>
Oversized Packets	<input type="text" value="0"/>	Multiple Collisions	<input type="text" value="0"/>
Filtered Packets	<input type="text" value="0"/>	Excessive Collisions	<input type="text" value="0"/>
		Late Collisions	<input type="text" value="0"/>
		Deferred Packets	<input type="text" value="0"/>
Packets Received and Transmitted			
64 bytes	<input type="text" value="0"/>	65-127 bytes	<input type="text" value="0"/>
128-255 bytes	<input type="text" value="0"/>	256-511 bytes	<input type="text" value="0"/>
512-1023 bytes	<input type="text" value="0"/>	1024-1518 bytes	<input type="text" value="0"/>
1522-9216 bytes	<input type="text" value="0"/>		<input type="text" value="0"/>

Table 44 describes the items on the Port page.

Table 44 Port page items

Section	Item	Description
Port Statistics (View By)	Port	Choose the switch's port number to monitor.

**Table 44** Port page items (continued)

Section	Item	Description
Port Statistics Table	Packets	The number of packets received/transmitted on this port, including bad packets, broadcast packets, and multicast packets.
	Multicast	The number of good multicast packets received/transmitted on this port, excluding broadcast packets.
	Broadcasts	The number of good broadcast packets received/transmitted on this port.
	Total Octets	The number of octets of data received/transmitted on this port, including data in bad packets and FCS octets, and framing bits.
	Pause Frames	The number of pause frames received/transmitted on this port.
	FCS/Frame Errors	The number of valid-size packets received on this port with proper framing but discarded because of FCS or frame errors.
	Undersized Packets	The number of packets received on this port with fewer than 64 bytes and with proper CRC and framing (also known as short frames or runts).
	Oversized Packets	The number of packets that were received on this port with proper CRC and framing that meet the following requirements:  1518 bytes if no VLAN tag exists 1522 bytes if a VLAN tag exists
	Filtered Packets	The number of packets that were received on this port and discarded because of the specific configuration. This counter does not count the FCS/Frames error packets; they are counted in that counter. This counter counts packets discarded because STP is not set to forwarding, the frame setting in VLAN directs discarding, or a mismatch in ingress/egress port speeds.
	Collisions	The number of collisions detected on this port.
	Single Collisions	The number of packets that were transmitted successfully on this port after a single collision.
	Multiple Collisions	The number of packets that were transmitted successfully on this port after more than one collision.
	Excessive Collisions	The number of packets lost on this port due to excessive collisions.

**Table 44** Port page items (continued)

Section	Item	Description
	Late Collisions	The number of packets collisions that occurred after a total length of time that exceeded 512 bit-times of packet transmission.
	Deferred Packets	The number of packets that were received on this port that were delayed on the first transmission attempt, but never incurred a collision.
Packets Received and Transmitted	Packets 64 bytes 65-127 bytes 128-255 bytes 256-511 bytes 512-1023 bytes 1024-1518 bytes 1522-9216 bytes	The number of packets received/transmitted on the port.

**2** Click Submit.

The Port Statistics Table is updated with information about the selected device and port (Figure 47).

**3** To update the statistical information, click Update.

## Zeroing Ports

To clear the statistical information for the currently displayed port:

➤ Click Zero Port.

To clear the statistical information for all ports in a switch:

➤ Click Zero All Ports.

## Viewing all Port Errors

You can view all ports that have errors. If a particular port has no errors, it will not be displayed.

To view a summary of the port errors for the Ethernet Routing Switch:

- 1 From the main menu, choose Statistics > Port Error Summary.

The Port Error Summary page opens (Figure 48).

**Figure 48** Port Error Summary page

### Statistics > Port Error Summary

Port Error Summary Table									
Port	Status	Link	Speed/Duplex	FCS/Frame Errors	Collisions	Single Collisions	Multiple Collisions	Excessive Collisions	Late Collisions
<input type="button" value="Update"/>									

Table 45 describes the read-only information displayed in the Port Error Summary Table.

**Table 45** Port Error Summary Table fields

Item	Description
Port	Displays the port number.
Status	Displays the status of the port (Enabled/Disabled).
Link	Displays the link status of the port (Up/Down).
Speed/Duplex	Displays the speed at which the port is operating, as well as whether it is in half- or full-duplex mode.
FCS/Frame Errors	Displays the number of frame check sequence (FCS) and frame errors received on this port.
Collisions	Displays the number of collision errors received on this port.
Single Collisions	Displays the number of single collision errors received on this port.
Multiple Collisions	Displays the number of multiple collision errors received on this port.

**Table 45** Port Error Summary Table fields (continued)

Item	Description
Excessive Collisions	Displays the number of excessive collision errors received on this port.
Late Collisions	Displays the number of late collision errors received on this port.

- 2 To view the latest port statistics, click the Update button at the bottom of the page.

## Viewing Interface Statistics

You can view selected switch interface statistics.

To view the interface statistical information of an interface:

- 1 From the main menu, choose Statistics > Interface.

The Interface page opens ([Figure 49](#)).

Figure 49 Interface page

## Statistics &gt; Interface

**Interface Statistics Table**

Port	In Octets	Out Octets	In Unicast	Out Unicast	In Non-Unicast	Out Non-Unicast	In Discards	Out Discards	In Errors	Out Errors	In Unknown Protos
1	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0
7	144638	53047	77	94	2038	79	18	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0	0	0	0

Update

Table 46 describes the items on the Interface page.

Table 46 Interface page items

Item	Description
Port	The port number corresponding to the selected switch.
In Octets	The number of octets received on the interface, including framing characters.

**Table 46** Interface page items (continued)

Item	Description
Out Octets	The number of octets transmitted out of the interface, including framing characters.
In Unicast	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Out Unicast	The number of packets that higher-layer protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
In Non-Unicast	The number of non-unicast packets, for example, subnetwork-broadcast or subnetwork-multicast packets, delivered to a higher protocol.
Out Non-Unicast	The number of packets that higher-level protocols requested be transmitted to a non-unicast address. For example, a subnetwork-broadcast or a subnetwork multicast address, including those that were discarded or not sent.
In Discards	The number of inbound packets which were selected to be discarded even though no errors were detected to prevent their being delivered to a higher-layer protocol. Packet discarding is not arbitrary. One reason for discarding packets is to free buffer space.
Out Discards	The number of outbound packets which were selected to be discarded even though no errors were detected to prevent their being transmitted. Packet discarding is not arbitrary. One reason for discarding packets is to free buffer space.
In Errors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Out Errors	The number of outbound packets that could not be transmitted because of errors.
In Unknown Protos	The number of packets received through the interface that were discarded because of an unknown or unsupported protocol.

**2** To update the statistical information, click Update.

## Viewing Ethernet Error Statistics

You can view Ethernet error statistics for each monitored interface linked to the Ethernet Routing Switch.

To view Ethernet error statistics:

**1** From the main menu, choose Statistics > Ethernet Errors.

The Ethernet Errors page opens (Figure 50).

Figure 50 Ethernet Errors page

## Statistics &gt; Ethernet Errors

Ethernet Errors Statistics Table										
Port	FCS/Frame Errors	Internal MAC Transmit Errors	Internal MAC Receive Errors	Carrier Sense Errors	SOE Test Errors	Deferred Transmissions	Single Collisions Frames	Multiple Collisions Frames	Late Collisions	Excessive Collisions
1	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0	0	0

Update

Table 47 describes the items on the Ethernet Errors page.

Table 47 Ethernet Errors page items

Item	Description
Port	The port number corresponding to the selected switch.
FCS/Frame Errors	The number of frames received on a particular interface that are an integral number of octets in length, but do not pass the FCS check or have frame errors.
Internal MAC Transmit Errors	The number of frames for which transmission on a particular interface fails because of an internal MAC sublayer transmit error. A frame only is counted by an instance of this object if it is not counted by the corresponding instance of either the dot3StatsLateCollisions object, the dot3StatsExcessiveCollisions object, or the dot3StatsCarrierSenseErrors object.

**Table 47** Ethernet Errors page items (continued)

Item	Description
Internal MAC Receive Errors	The number of frames for which reception on a particular interface fails because of an internal MAC sublayer transmit error. A frame only is counted by an instance of this object if it is not counted by the corresponding instance of either the dot3StatsLateCollisions object, the dot3StatsExcessiveCollisions object, or the dot3StatsCarrierSenseErrors object.
Carrier Sense Errors	The number of times that the carrier sense conditions were lost or never asserted when attempting to transmit a frame on a particular interface.
SQE Test Errors	The number of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface. The SQE TEST ERROR is defined in section 7.2.2.2.4 of ANSI/IEEE 802.3-1985, and its generation is described in section 7.2.4.6 of the same document.
Deferred Transmissions	The number of frames for which the first transmission attempt on a particular interface is delayed because the medium is busy.
Single Collision Frames	The number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.
Multiple Collision Frames	The number of successfully transmitted frames on a particular interface for which transmission is inhibited by a single collision.
Late Collisions	The number of times a collision is detected on a particular interface later than 512 bit-times into the transmission of a packet.
Excessive Collisions	The number of frames for which transmission on a particular interface fails due to excessive collisions.

- 2 To refresh the statistical information, click Update.

## Viewing Transparent Bridging Statistics

You can view the transparent bridging statistics measured for each monitored interface on the device.

To view transparent bridging statistics:

- 1 From the main menu, choose Statistics > Transparent Bridging.

The Transparent Bridging page opens ([Figure 51](#)).

Figure 51 Transparent Bridging page

**Statistics > Transparent Bridging**

Transparent Bridging Statistics Table			
Port	In Frames	Out Frames	In Discards
1	0	0	0
2	0	1	0
3	0	1	0
4	0	1	0
5	0	1	0
6	0	1	0
7	0	1	0
8	0	1	0
9	0	1	0
10	0	1	0
11	0	1	0
12	0	1	0
13	0	1	0
14	0	1	0
15	0	1	0
16	0	1	0
17	0	1	0
18	0	1	0
19	0	1	0
20	0	1	0
21	1562829	82853	428
22	0	1	0
23	0	1	0
24	0	0	0

[Update](#)

Table 48 describes the items on the Transparent Bridging page.

Table 48 Transparent Bridging page items

Item	Description
Port	The port number that corresponds to the selected switch.
In Frames (dot1dTpPortInFrames)	The number of frames that have been received by this port from its segment. A frame received on the interface corresponding to this port is counted only if it is for a protocol being processed by the local bridging function, including bridge management errors.

**Table 48** Transparent Bridging page items

<b>Item</b>	<b>Description</b>
Out Frames (dot1dTpPortOutFrames)	The number of frames that have been transmitted by this port from its segment. A frame received on the interface corresponding to this port is counted only if it is for a protocol being processed by the local bridging function, including bridge management errors.
In Discards (dot1dTpPortInDiscards)	The number of valid frames received which were discarded by the forwarding process.

**2** To refresh the statistical information, click Update.

---

## Chapter 7

# Configuring Application Settings

---

The options available to configure application settings are:

- “Configuring Port Mirroring”, next
- “Configuring Rate Limiting” on page 147
- “Configuring IGMP” on page 150
- “Viewing Multicast Group Membership Configurations” on page 153
- “Creating and Managing Virtual LANs” on page 154
- “Configuring VLANs” on page 155
- “Configuring Broadcast Domains” on page 167
- “Viewing VLAN Port Information” on page 168
- “Managing Spanning Tree Groups” on page 170
- “Configuring Ports for Spanning Tree” on page 179
- “Changing Spanning Tree Bridge Switch Settings” on page 181
- “Configuring MultiLink Trunk Members” on page 184
- “Monitoring MLT Traffic” on page 187

## Configuring Port Mirroring

The Ethernet Routing Switch supports port mirroring to analyze traffic. You can view existing port mirroring activity and you can configure a specific switch port to mirror up to two specified ports or two MAC addresses. When you configure port mirroring, you have the option to specify either port-based monitoring or address-based monitoring.

Refer to the *Application Guide for Nortel Ethernet Routing Switch 3510-24T, Software Release 4.0.3* for configuration guidelines for port-mirroring.

To configure port mirroring:

- 1 From the main menu, choose Application > Port Mirroring.  
The Port Mirroring page opens (Figure 52).

**Figure 52** Port Mirroring page

## Application > Port Mirroring

Port Mirroring Setting	
Monitoring Mode	Disabled <input type="button" value="v"/>
Monitor Port	<input type="button" value="v"/>
Port X	<input type="button" value="v"/>
Port Y	<input type="button" value="v"/>
Address A	<input type="text"/> (XX-XX-XX-XX-XX-XX)
Address B	<input type="text"/> (XX-XX-XX-XX-XX-XX)

Port Mirroring Active	
Monitoring Mode	Disabled



**Note:** The Port Mirroring Active section of this only displays those port mirroring configurations you set. If you set no port mirroring configurations, the area will not show rows.

---



**Note:** If the port which is monitored is in full duplex, only unicast packets which are addressed to the device that is connected to the port are monitored. If the port which is monitored is half duplex, all the packets which are addressed to the device that is connected to the port are monitored.

Table 49 describes the items on the Port Mirroring page.

**Table 49** Port Mirroring page items

Item	Range	Description
Monitoring Mode	(1) Disabled (2) --> Port X (3) Port X --> (4) <-- --> Port X (5) -->Port X or Port Y --> (6) -->Port X and Port Y --> (7) <-- --> Port X and <-- --> Port Y (8) Address A --> any Address (9) any Address --> Address A (10) <-- --> Address A (11) Address A --> Address B (12) Address A <-- --> Address B	Choose any one of the six port-based monitoring modes or any one of the five address-based monitoring modes.  For more information on selecting one of the six port-based modes that activates the port X and port Y screen fields, where you can choose up to two ports to monitor, see <a href="#">Table 50 on page 146</a> .  For more information on selecting one of the five address-based modes that activates the Address A and Address B screen fields, where you can specify MAC addresses to monitor, see <a href="#">Table 51 on page 147</a> .  The default setting is Disabled.
Monitor Port		Choose the switch port to designate as the monitor port.
Port X		Choose the first switch port to be monitored by the designated monitor port. This port is monitored according to the value "X" in the Monitoring Mode field.
Port Y		Choose the second switch port to be monitored by the designated monitor port. This port is monitored according to the value "Y" in the Monitoring Mode field.
Address A	XX-XX-XX-XX-XX-XX	Type the MAC address to monitor by the designated monitor port. This address is monitored according to the value "Address A" in the Monitoring Mode field.
Address B	XX-XX-XX-XX-XX-XX	Type the MAC address to monitor by the designated monitor port. This address is monitored according to the value "Address B" in the Monitoring Mode field.

- 2 Type information in the text boxes, or select from a list.
- 3 Click Submit.

Selecting one of the port-based monitoring modes activates the port X and/or the port Y screen fields, where you can choose up to two ports to monitor.

Table 50 describes the port-based monitoring modes.

**Table 50** Port-based monitoring modes

Item	Description
Disabled	Choose this option to disable port-based monitoring.  The default setting is Disabled.
--> Port X	Choose this option to monitor all traffic received by port X.
Port X -->	Choose this option to monitor all traffic transmitted by port X.
<-- --> Port X	Choose this option to monitor all traffic received and transmitted by port X.
--> Port X or Port Y -->	Choose this option to monitor all traffic received by port X or transmitted by port Y. Note: Do not use this mode for multicast and broadcast traffic.
--> Port X and Port Y -->	Choose this option to monitor all traffic received by port X (destined to port Y) and then transmitted by port Y (one way conversation steering). Note: Do not use this mode for multicast and broadcast traffic
<-- --> Port X and Port Y <-- -->	Choose this option to monitor all traffic received by port X and then transmitted by port Y or transmitted by port X and received by port Y (two way conversation steering). Note: Do not use this mode for multicast and broadcast traffic

Selecting any one of the address-based monitoring modes activates the Address A and Address B screen fields, where you can specify MAC addresses to monitor.

Table 51 describes the address-based monitoring modes.

**Table 51** Address-based monitoring modes

Item	Description
Disabled	Choose this option to disable port-based monitoring.  The default setting is Disabled.
Address A --> any Address	Choose this option to monitor all traffic transmitted from Address A to any address.
any Address --> Address A	Choose this option to monitor all traffic received by Address A from any address.
<-- --> Address A	Choose this option to monitor all traffic received by or transmitted by Address A.
Address A --> Address B	Choose this option to monitor all traffic transmitted by Address A that goes to Address B (one way conversation steering).
Address A <-- --> Address B	Choose this option to monitor all traffic received by Address A and then transmitted by Address B or transmitted by Address A and received by Address B (two way conversation steering).

## Configuring Rate Limiting

You can view the current forwarding rate of broadcast and/or multicast packets, and configure the Ethernet Routing Switch to limit the forwarding rate of broadcast and multicast packets on each interface. When you configure rate limiting, you are setting the percentage of port bandwidth allowed for a packet type. When the threshold is exceeded, additional packets are discarded.



**Note:** If a port is configured for rate limiting, and it is a MultiLink trunk member, all trunk member ports implement rate limiting. If the port becomes disabled, all trunk members become disabled.

To configure rate limiting:

- 1 From the main menu, choose Application > Rate Limiting.  
The Rate Limiting page opens (Figure 53).

Figure 53 Rate Limiting page

## Application &gt; Rate Limiting

Rate Limiting Table					
Port	Packet Type	Limit	Last 5 Minutes	Last Hour	Last 24 Hours
1	Both	None	0.0%	0.0%	0.0%
2	Both	None	0.0%	0.0%	0.0%
3	Both	None	0.0%	0.0%	0.0%
4	Both	None	0.0%	0.0%	0.0%
5	Both	None	0.0%	0.0%	0.0%
6	Both	None	0.0%	0.0%	0.0%
7	Both	None	0.0%	0.0%	0.0%
8	Both	None	0.0%	0.0%	0.0%
9	Both	None	0.0%	0.0%	0.0%
10	Both	None	0.0%	0.0%	0.0%
11	Both	None	0.0%	0.0%	0.0%
12	Both	None	0.0%	0.0%	0.0%
Switch	Both	<input type="checkbox"/>	None	<input type="checkbox"/>	

Submit

[Ports 13 - 24](#)

Table 52 describes the items on the Rate Limiting page.

Table 52 Rate Limiting page items

Item	Range	Description
Port	1 to 24	The selected port number.
Packet Type	(1) Multicast (2) Broadcast (3) Both	Choose the packet type to view on the table.  The default setting is Both.

**Table 52** Rate Limiting page items (continued)

Item	Range	Description
Limit	None, 1-10%	<p>Choose the percentage, if any, of bandwidth allowed for forwarding the packet type specified in the Packet Type field. When the threshold is exceeded, any additional packets are discarded.</p> <p>Note: Rate limiting is disabled if this field is set to none. This allows you to select and view the percentage of specific packet types present in the network, without inadvertently limiting the forwarding rate.</p> <p>The default setting is None.</p>
Last 5 Minutes	0..100%	The percentage of packets received by the port in the last five minutes. This field provides a running average of network activity and is updated every 15 seconds.
Last Hour	0..100%	The percentage of packets received by the port in the last hour. This field provides a running average of network activity and is updated every five minutes.
Last 24 Hours	0..100%	<p>The percentage of packets received by the port in the last 24 hours. This field provides a running average of network activity and is updated every hour.</p> <p>Note: The Last 5 Minutes, Last Hour, and Last 24 Hours fields indicate the receiving port's view of network activity regardless of the rate limiting setting.</p>

- 2 Type information in the text boxes, or select from a list.
- 3 Click Submit.



**Note:** To avoid broadcast storms (when the volume of a particular packet type is extreme, placing severe strain on the network), set the forwarding rate of the packet type to not exceed a lower percentage of the total available bandwidth.

## Configuring IGMP

You can configure a VLAN's switch ports to optimize IP multicast packets in a bridged Ethernet environment, and you can view a table of existing IGMP configurations. For more information about IGMP configuration, see the *Application Guide for Nortel Ethernet Routing Switch 3510-24T, Software Release 4.0.3*.



**Note:** The Ethernet Routing Switch supports 256 IGMP groups.

To configure IGMP:

- 1 From the main menu, choose Application > IGMP > IGMP Configuration. The IGMP Configuration page opens ([Figure 54](#)).

**Figure 54** IGMP Configuration page

### Application > IGMP > IGMP Configuration

IGMP Table					
Action	VLAN	Snooping	Proxy	Robust Value	Query Time (seconds)
	1	Disabled	Disabled	2	125

[Table 53](#) describes the items on the IGMP Configuration page.

**Table 53** IGMP Configuration page items

Item	Description
	Displays a modification page for the selected VLAN.
VLAN	The number assigned to the VLAN when the VLAN was created. For more information on creating VLANs, see <a href="#">“Creating and Managing Virtual LANs” on page 154</a> .
Snooping	The operational status for the IGMP snooping feature.

**Table 53** IGMP Configuration page items

Item	Description
Proxy	If enabled, this feature allows the switch to consolidate IGMP Host Membership Reports received on its downstream ports and to generate a consolidated proxy report for forwarding to its upstream neighbor.  Note: This field affects <i>all</i> VLANs.
Robust Value	The predetermined value set by the administrator to offset expected packet loss on a subnet. If packet losses on a subnet are unacceptably high, the Robust Value field can be increased to a higher value.  Note: This field affects <i>only</i> the VLAN specified in the page's VLAN field.
Query Time	The query interval (the interval between general queries sent by the multicast router).

2 In the VLAN row of your choice, click the Modify icon.

The IGMP: VLAN Configuration page opens (Figure 55).

**Figure 55** IGMP: VLAN Configuration page

### Application > IGMP: VLAN Configuration

**IGMP VLAN Setting**

VLAN: 1

Snooping: Disabled ▾

Proxy: Disabled ▾

Robust Value:  (0 .. 255)

Query Time:  seconds (1 .. 65535)

**Static Router Ports (Version 1)**

Port	All	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
	<input type="checkbox"/>																								

**Static Router Ports (Version 2)**

Port	All	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
	<input type="checkbox"/>																								

Table 54 describes the items on the IGMP: VLAN Configuration page.

**Table 54** IGMP: VLAN Configuration page items

Item	Range	Description
VLAN	1 to 4094	The number assigned to the VLAN when the VLAN was created. For more information on creating VLANs, see <a href="#">“Creating and Managing Virtual LANs” on page 154</a> .
Snooping	(1) Enabled (2) Disabled	Choose to enable or disable the IGMP snooping feature.  Note: This field affects only the VLAN specified in the VLAN field listed in the page.  The default setting is Disabled.
Proxy	(1) Enabled (2) Disabled	Choose to enable or disable the proxy feature. This feature allows the switch to consolidate IGMP Host Membership Reports received on its downstream ports and to generate a consolidated proxy report for forwarding to its upstream neighbor.  Note: This field affects only the VLAN specified in the VLAN field listed in the page.  The default setting is Disabled.
Robust Value	0..255	Type the robust value in the appropriate format. This feature allows you to set the switch to offset expected packet loss on a subnet. If packet losses on a subnet are unacceptably high, the Robust Value field can be increased to a higher value.  Note: This field affects <i>only</i> the VLAN specified in the page’s VLAN field.  The default settings is 2.
Query Time	1 to 65535	Type the query time (in seconds) in the appropriate format. This feature allows you to control the number of IGMP messages allowed on the subnet by varying the Query Interval (the interval between general queries sent by the multicast router).  Note: This field affects <i>only</i> the VLAN specified in the page’s VLAN field.  The default settings is 125 seconds.
Static Router Ports (Version 1 and Version 2)		Click the check boxes of the router ports to associate with the VLAN (alternatively, click the check box to deselect a selected router port).  Note: This field affects <i>all</i> VLANs.

**3** Type information in the text boxes, or select from a list.

- 4 In the Static Router Ports section(s), click the check boxes of the router ports to associate with the VLAN.
- 5 Do one of the following:
  - Click Submit.
  - Click Back to return to the IGMP page without making changes.The new configuration is displayed in the IGMP Table (Figure 54).

## Viewing Multicast Group Membership Configurations

You can view a table configured IP multicast group addresses for a selected VLAN.



**Note:** The Ethernet Routing Switch supports 256 IGMP groups.

To view multicast group membership configurations for a selected VLAN:

- 1 From the main menu, choose Application > IGMP > IGMP Multicast Group. The IGMP Multicast Group Membership page opens (Figure 56).

**Figure 56** IGMP Multicast Group Membership page



[Table 55](#) describes the items on the IGMP Multicast Group Membership page.

**Table 55** IGMP Multicast Group Membership page items

Section	Item	Description
Multicast Group Membership Selection (View By)	VLAN	Choose the VLAN on which to view configured IP addresses.
Multicast Group Membership Table	Multicast Group Address	The IP multicast group addresses that are currently active on the associated port.
	Port	The port numbers associated with the IP multicast group addresses displayed in the IP Multicast Group Address field.

**2** In the Multicast Group Membership Selection section, choose the number of VLAN on which to view configured IP addresses.

**3** Click Submit.

The results are displayed in the Multicast Group Membership Table ([Figure 56](#)).

## Creating and Managing Virtual LANs

A Virtual LAN (VLANs) is a collection of switch ports that make up a single broadcast domain. You can configure a VLAN for a single switch, or for multiple switches. When you create a VLAN, you can control traffic flow and ease the administration of moves, adds, and changes on the network, by eliminating the need to change physical cabling.

You can configure two types of VLAN in the Web-based management interface:

- Port-based
- Protocol-based

You have 256 port- and protocol-based VLANs.

## Port-based VLANs

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

The automatic PVID feature automatically sets the PVID when you configure a port-based VLAN. The PVID value will be the same value as VLAN. The user can also manually change the PVID value. The default setting for AutoPVID is enable.

## Protocol-based VLANs

You can configure as many as 255 protocol-based VLANs, with up to 7 different protocols.

A protocol-based VLAN is a VLAN in which the switch ports are configured as members of a broadcast domain, based on the protocol information within a packet. A protocol-based VLAN can localize broadcast traffic and assure that only the protocol-based VLAN ports are flooded with the specified protocol-type packets.

For protocol-based VLANs, the VLAN classification of the frame is dependent on the protocol of the incoming untagged frame. The frame is forwarded only if that VLAN is registered at the egress port.

## Configuring VLANs

You can create VLANs by assigning switch ports and protocols as VLAN members, and you can designate an existing VLAN to act as the management VLAN.



**Note:** For guidelines on configuring VLANs—as well as interoperability guidelines between VLANs, MultiLink Trunking, and multiple Spanning Tree Protocol Groups—refer to the *Application Guide for Nortel Ethernet Routing Switch 3510-24T, Software Release 4.0.3*.

---

To open the VLAN Configuration page:

- From the main menu, choose Application > VLAN > VLAN Configuration.

The VLAN Configuration page opens (Figure 57).

**Figure 57** VLAN Configuration page

### Application > VLAN > VLAN Configuration

VLAN Table							
Action	VLAN	VLAN Name	VLAN Type	Protocol	User Defined Protocol	Learning Constraint	State
 	1	VLAN #1	Port	None	0x0	VL	Active

**VLAN Creation**  
VLAN Type

**VLAN Setting**  
Management VLAN

**AutoPVID Setting**  
AutoPVID

Table 56 describes the items on the VLAN Configuration page.

**Table 56** VLAN Configuration page items

Section	Item	Description
VLAN Table		Displays a modification page.
		Deletes the row.
	VLAN	The number assigned to the VLAN when the VLAN was created.
	VLAN Name	The name assigned to the VLAN when the VLAN was created.
	VLAN Type	The base-type assigned when the VLAN was created. The base types are: Port-based and Protocol-based.
	Protocol	The protocol assigned when the VLAN was created. The protocol types are: IP, IPX 802.2, 1PX 802.3, IPX Snap, IPX Ethernet II, DEC Lat, SNA Ethernet II, Net Bios, XNS, Vines, Ipv6, User Defined, and RARP. For more information, see <a href="#">Table 60 on page 162</a> .
	User Defined Protocol	The user-defined protocol assigned when the VLAN was created.
	Learning Constraint	All VLANs on the Ethernet Routing Switch have IVL as the learning constraint. With IVL, the VLAN uses an independent filtering database from all other VLANs.
	State	The current operational state of the VLAN.
VLAN Creation	VLAN Type	Choose the type of VLAN to create and click Create VLAN. Your options are: port-based ( <a href="#">page 157</a> ) and protocol-based ( <a href="#">page 160</a> ).
VLAN Setting	Management VLAN	Choose the VLAN to designate as the management VLAN.
AutoPVID Setting	AutoPVID	Choose Enabled to activate the Automatic PVID feature and click Submit.  Note: Use this <i>only</i> with port-based VLANs.

## Creating a Port-based VLAN

To create a port-based VLAN:

- 1 From the main menu choose Application > VLAN > VLAN Configuration.

The VLAN Configuration page opens ([Figure 57](#)).

- 2 In the VLAN Creation section, choose Port.
- 3 Click Create VLAN.

The VLAN Configuration: Port Based setting page opens (Figure 58).

**Figure 58** VLAN Configuration: Port Based setting page

### Application > VLAN > VLAN Configuration: Port Based

VLAN - Port Based Setting																									
VLAN	101																								
VLAN Name	VLAN#101																								
Learning Constraint	ML																								
	Port Membership																								
Port	All	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																				

Submit Back

Table 57 describes the items on the VLAN Configuration: Port Based setting page.

**Table 57** VLAN Configuration: Port Based setting page items

Section	Item	Description
VLAN	1to 4094	The number assigned to the VLAN when the VLAN was created.
VLAN Name	1to 16	Type a character string to create a unique name to identify the VLAN, for example, VLAN1.

- 4 Type information in the text boxes, or select from a list.
- 5 Do one of the following:
  - Click Submit.
  - Click Back to return to the VLAN Configuration page without making changes.

The new port-based VLAN configuration appears in the VLAN Table on the VLAN Configuration page (Figure 57).

## Modifying a Port-based VLAN

To modify an existing port-based VLAN:

- 1 From the main menu, choose Application > VLAN > VLAN Configuration. The VLAN Configuration page opens (Figure 57).
- 2 In the VLAN Table section, in the port-based VLAN row of your choice, click the Modify icon. The VLAN Configuration: Port Based modification page opens (Figure 59).

**Figure 59** VLAN Configuration: Port Based modification page

Application > VLAN > VLAN Configuration: Port Based

VLAN - Port Based Setting	
VLAN	1
VLAN Name	VLAN #1
Learning Constraint	VL
	Port Membership
Port	All 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
	<input type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>
<input type="button" value="Submit"/> <input type="button" value="Back"/>	

Table 58 describes the items on the VLAN Configuration: Port Based modification page.

**Table 58** VLAN Configuration: Port Based modification page items

Item	Description
VLAN	The number assigned to the VLAN when the VLAN was created.
VLAN Name	(Re)name the VLAN.

**Table 58** VLAN Configuration: Port Based modification page items

Item	Description
Learning Constraint	All Ethernet Routing Switches use IVL, which means that the VLAN uses an independent filtering database from all other VLANs.
Port Membership	<p>Click the check boxes for the switch ports to associate them with the VLAN or, if the port is already a member, click the check box to deselect the it as a member of the VLAN.</p> <p>A port can be configured in one or more VLANs.</p> <p>This field is dependent on the Tagging field value in the VLAN Port Configuration screen. For example:</p> <p>When the Tagging field is set to <i>Untagged Access</i>, you can set the Port Membership field as an untagged port member or as a non-VLAN port member.</p> <p>When the Tagging field is set to <i>Tagged Trunk</i>, you can set the Port Membership field as a tagged port member or as a non-VLAN port member.</p>

- 3 Type information in the text boxes, or click the check box of a port to associate it with the VLAN or, if the port is already a member, click the check box to deselect it as a member of the VLAN.
- 4 Do one of the following:
  - Click Submit.
  - Click Back to return to the VLAN Configuration page without making changes.

The modified VLAN configuration is displayed in the VLAN Table (Figure 57).

## Creating a Protocol-based VLAN

To create a protocol-based VLAN:

- 1 From the main menu, choose Application > VLAN > VLAN Configuration. The VLAN Configuration page opens (Figure 57).
- 2 In the VLAN Creation section, choose Protocol.
- 3 Click Create VLAN.

The VLAN Configuration: Protocol Based setting page opens (Figure 60).

**Figure 60** VLAN Configuration: Protocol Based setting page

**Application > VLAN > VLAN Configuration: Protocol Based**

**VLAN - Protocol Based Setting**

VLAN

VLAN Name

Protocol

User Defined Protocol  (e.g. 0:8137)

Table 59 describes the items on the VLAN Configuration: Protocol Based setting page.

**Table 59** VLAN Configuration: Protocol Based setting page items

Item	Range	Description
VLAN	1 to 4094	Type a unique number to identify the VLAN.
VLAN Name	1 to 16	Type a unique name to identify the VLAN.

**Table 59** VLAN Configuration: Protocol Based setting page items

Item	Range	Description
Protocol	IP, IPX 802.2, 1PX 802.3, IPX Snap, IPX Ethernet II, DEC Lat, SNA Ethernet II, Net Bios, XNS, Vines, Ipv6, User Defined, and RARP.	Choose the supported protocol for the VLAN. For more information, see <a href="#">Table 60 on page 162</a> .
User Defined Protocol		<p>If you selected “User Defined” from the Protocol pulldown list, specify the protocol identifier for the VLAN.</p> <p>Note: Any frames that match the specified PID, in any of the following ways are assigned to that user defined VLAN:</p> <ul style="list-style-type: none"> <li>The ethertype for Ethernet type 2 frames</li> <li>The PID in Ethernet SNAP frames</li> <li>The DSAP or SSAP value in Ethernet 802.2 frames.</li> </ul> <p>For a list of reserved PIDs that are unavailable for user-defined PIDs, see <a href="#">Table 61 on page 164</a>.</p>

**4** Type information in the text boxes, or select from a list.

**5** Do one of the following:

- Click Submit.
- Click Back to return to the VLAN Configuration page without making changes.

The new protocol-based VLAN configuration appears in the VLAN Table on the VLAN Configuration page ([Figure 57](#)).

[Table 60](#) defines the standard protocol-based VLANs and PID types that are supported by the Ethernet Routing Switch.

**Table 60** Standard protocol-based VLANs and PID types

PID Name	Encapsulation	PID Value (hex)	VLAN Type
IP Ether2	Ethernet type 2	0800, 0806	Standard IP on Ethernet Type 2 frames
IPX 802.3	Ethernet 802.3	FFFF	Novell IPX on Ethernet 802.3 frames
IPX 802.2	Ethernet 802.2	E0 E0	Novell IPX on Ethernet 802.2 frames
IPX Snap	Ethernet Snap	8137, 8138	Novell IPX on Ethernet SNAP frames

**Table 60** Standard protocol-based VLANs and PID types (continued)

PID Name	Encapsulation	PID Value (hex)	VLAN Type
IPX Ethernet II	Ethernet type 2	8137, 8138	Novell IPX on Ethernet Type 2 frames
DEC Lat	Ethernet type 2	6004	DEC LAT protocol
Sna Ethernet II	Ethernet type 2	80D5	IBM SNA on Ethernet Type 2 frames
NetBios	Ethernet type 2	F0**, **F0	NetBIOS protocol
XNS	Ethernet type 2	0600, 0807	Xerox XNS
Vines	Ethernet type 2	0BAD	Banyan VINES
IPv6	Ethernet type 2	86DD	IP version 6
RARP	Ethernet type 2	8035	Reverse Address Resolution Protocol (RARP): RARP is a protocol used by some old diskless devices to obtain IP addresses by providing the MAC layer address. When you create a VLAN based on RARP, you can limit the RARP broadcasts to the ports that lead to the RARP server.
User-Defined	Ethernet type 2, Ethernet 802.2, or Ethernet Snap	User-defined 16 bit value	If you select "User Defined" from the Protocol pulldown list, specify the protocol identifier for the VLAN.  Note: Any frames that match the specified PID, in any of the following ways are assigned to that user defined VLAN: The ethertype for Ethernet type 2 frames The PID in Ethernet SNAP frames The DSAP or SSAP value in Ethernet 802.2 frames.  For a list of reserved PIDs that are unavailable for user-defined PIDs, see <a href="#">Table 60 on page 162</a>

[Table 61](#) describes the PIDS that are reserved and not available for user-defined PIDs.

**Table 61** Predefined Protocol Identifier (PID)

PID Name	Encapsulation	PID Value (hex)	VLAN Type
IPX 802.3	Ethernet 802.3	FF FF	Novell IPX on Ethernet 802.3 frames
IPX 802.2	Ethernet 802.2	E0 E0	Novell IPX on Ethernet 802.2 frames
IPX Snap	Ethernet Snap	8137, 8138	Novell IPX on Ethernet SNAP frames
IP Ether2	Ethernet type 2	0800, 0806	Standard IP on Ethernet Type 2 frames
IPX Ethernet II	Ethernet type 2	8137, 8138	Novell IPX on Ethernet Type 2 frames
ApITk Ether2 Snap	Ethernet type 2 or Ethernet Snap	809B, 80F3	AppleTalk on Ethernet Type 2 and Ethernet Snap frames
Declat Ether2	Ethernet type 2	6004	DEC LAT protocol
Sna Ether2	Ethernet type 2	80D5	IBM SNA on Ethernet Type 2 frames
NetBios 802.2	Ethernet type 2	F0**, **F0	NetBIOS protocol
Xns Ether2	Ethernet type 2	0600, 0807	Xerox XNS
Vines Ether2	Ethernet type 2	0BAD	Banyan VINES
Ipv6 Ether2	Ethernet type 2	86DD	IP version 6
User-Defined	Ethernet type 2, Ethernet 802.2, or Ethernet Snap	User-defined 16 bit value	User-defined protocol-based VLAN.  For a list of rereserved PIDs that are unavailable for user-defined PIDs, see <a href="#">Table 61 on page 164</a> .

## Modifying a Protocol-based VLAN

To modify an existing protocol-based VLAN:

- 1 From the main menu, choose Application > VLAN > VLAN Configuration.  
The VLAN Configuration page opens ([Figure 57](#)).
- 2 In the VLAN Table section, in the protocol-based VLAN row of your choice, click the Modify icon.

The VLAN Configuration: Protocol Based modification page opens ([Figure 61](#)).

**Figure 61** VLAN Configuration: Protocol Based modification page

Application > VLAN > VLAN Configuration: Protocol Based

**VLAN - Protocol Based Setting**

VLAN	31
VLAN Name	Test
Protocol	P
User Defined Protocol	0x0
Learning Constraint	IVL
Port Membership	
Port	All 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
	<input type="checkbox"/>

Submit Back

Table 62 describes the items on the VLAN Configuration: Protocol Based modification page.

**Table 62** VLAN Configuration: Protocol Based modification page items

Item	Description
VLAN	The number assigned to the VLAN when the VLAN was created.
VLAN Name	(Re)name the VLAN.
Learning Constraint	All Ethernet Routing Switches use IVL, which means that the VLAN uses an independent filtering database from all other VLANs.
Port Membership	Click the check boxes beneath a port to associate the port with the VLAN or, if the port is already selected click the check box to deselect the port as a member of the VLAN.

- 3 Type information in the text boxes, or click the check box of a port to associate it with the VLAN or, if the port is already a member, click the check box to deselect it as a member of the VLAN.
- 4 Do one of the following:
  - Click Submit.
  - Click Back to return to the VLAN Configuration page without making changes.

The modified VLAN configuration is displayed in the VLAN Table (Figure 57).

## Selecting a Management VLAN

You can select any VLAN to perform as the management VLAN. VLAN 1 is the default management VLAN for the switch. To set this field, the VLAN State field value must be active.

To select a VLAN as the management VLAN:

- 1 From the main menu, choose Application > VLAN > VLAN Configuration. The VLAN Configuration page opens (Figure 57).
- 2 In the VLAN Setting section, choose the VLAN to assign as your management VLAN.
- 3 Click Submit.

## Deleting a VLAN Configuration

To delete a VLAN configuration:

- 1 From the main menu, choose Application > VLAN > VLAN Configuration. The VLAN Configuration page opens (Figure 57).
- 2 In the VLAN Table, click the Delete icon for the entry you want to delete. A message opens prompting you to confirm your request.
- 3 Do one of the following:
  - Click Yes to delete the VLAN configuration.
  - Click Cancel to return to the VLAN Configuration page without making changes.



**Note:** You cannot delete VLAN 1.

---

## Configuring Broadcast Domains

You can configure specified VLAN switch ports with the appropriate PVID/VLAN association that enables the creation of broadcast domains. If you have enabled automatic PVID, you can change the PVID number on this screen. You can configure specified switch ports to filter (discard) all received tagged frames, untagged frames, or unregistered frames. You can also prioritize the order in which the switch forwards untagged packets, on a per-port basis.

To configure broadcast domains:

- 1 From the main menu, choose Application > VLAN > Port Configuration.  
The Port Configuration page opens (Figure 62).

**Figure 62** Port Configuration page

**Application > VLAN > Port Configuration**

**VLAN Port Setting**

Port	Port Name	Filter Untagged Frames	Filter Unregistered Frames	PVID	Port Priority	Tagging
1	Port 1	No	No	1	0	Tag All
2	Port 2	No	No	1	0	Tag All
3	Port 3	No	No	1	0	Tag All
4	Port 4	No	No	1	0	Tag All
5	Port 5	No	No	1	0	Tag All
6	Port 6	No	No	1	0	Tag All
7	Port 7	No	No	1	0	Tag All
8	Port 8	No	No	1	0	Tag All
9	Port 9	No	No	1	0	Untag All
10	Port 10	No	No	1	0	Untag All
11	Port 11	No	No	1	0	Untag All
12	Port 12	No	No	1	0	Untag PVID Only

[Ports 13 - 24](#)

Table 63 describes the items on the Port Configuration page.

**Table 63** Port Configuration page items

Item	Range	Description
Port	1to 24	The port number.
Port Name	1to 16	Type character string to create a unique port name, for example, Unit 1, Port 1.
Filter Untagged Frames	(1) Yes (2) No	Choose how to process filter untagged frames.  When a flag is set, the frames are discarded by the forwarding process.  The default setting is No (no frames discarded).
Filter Unregistered Frames	(1) Yes (2) No	Displays yes/no if a flag is set. If yes, unregistered frames are discarded by the forwarding process, which is to say that frames with a VID that this port does not belong to are discarded. When the flag is reset, unregistered frames are processed normally.  The default settings is No.
PVID	1to 4094	Type the number of the VLAN ID to assign to untagged frames received on this trunk port. For example, a port with a PVID of 3 assigns all untagged frames received on this port to VLAN 3.  The default setting is 1.  Note: If AutoPVID is enabled and you want another PVID, enter the desired PVID here.
Port Priority	0-7	Choose the level of priority for each port.
Tagging	(1) Untag All (2) Tag All (3) Untag PVID Only (4) Tag PVID Only	Choose the egress tagging for each port.

- 2 Type information in the text boxes, or select from a list.
- 3 Click Submit.

## Viewing VLAN Port Information

You can view VLAN information about a selected switch port.

To view VLAN port information:

- 1 From the main menu, choose Application > VLAN > Port Information.  
The Port Information page opens (Figure 63).

**Figure 63** Port Information page

### Application > VLAN > Port Information

VLAN Port Information (View By)	
Port	1 ▾
PVID	1
Port Name	Port 1

Submit

VLAN Port Information Table		
VLAN	VLAN Name	VLAN Type
1	VLAN #1	Port
2	VLAN #2	Port
10	VLAN #10	Port
90	VLAN #90	Port

Table 64 describes the items on the Port Information page.

**Table 64** Port Information page items

Section	Item	Range	Description
VLAN Port Information	Port	1 to 24	Choose the number of the switch's port to view.
	PVID		The PVID assigned when the VLAN port was created.
	Port Name		The port name assigned when the VLAN port was created.
VLAN Port Information Table	VLAN		The number assigned to the VLAN when it was created.

**Table 64** Port Information page items

Section	Item	Range	Description
	VLAN Name		The name assigned to the VLAN when it was created.
	VLAN Type		The VLAN type assigned to the VLAN when it was created.

2 In the VLAN Port Information (View By) section, enter the port number of the VLAN you want to view.

3 Click Submit.

The results of your request are displayed in the VLAN Port Information Table (Figure 63).

## Managing Spanning Tree Groups

You can configure system parameters for Spanning Tree Protocol, the industry standard for avoiding loops in switched networks. You can configure individual switch ports or all switch ports for participation in the spanning tree algorithm (STA).



**Note:** STP resolves duplicate paths in networks and is not necessary for ports that have workstations directly attached to the switch. When STP is enabled on these ports (the default), workstations are unable to attach to servers for a few seconds while STP stabilizes.

---

The Ethernet Routing Switch supports multiple instances (8) of spanning tree groups (STGs) running simultaneously in a switch. Each STG sends its own Bridge Protocol Data Units (BPDUs), and each STG must be independently configured.

You can choose which VLAN in the STG will send the tagged BPDU.

In the default configuration of the Ethernet Routing Switch, a single STG with the ID of 1 includes all ports on the switch. It is called the Default STG and sends only untagged BPDUs in order to operate with all devices that support only one instance of STP. Although ports can be added to or deleted from the Default STG, the Default STG itself cannot be deleted from the system. All other STGs, except the Default STG, must be created by the user.



**Note:** To become active, each STG must be enabled by the user after creation. For guidelines on configuring STGs—as well as interoperability guidelines between VLANs, MultiLink Trunking, and multiple Spanning Tree Protocol Groups—refer to the *Application Guide for Nortel Ethernet Routing Switch 3510-24T, Software Release 4.0.3*.

---

You can set the spanning tree priority and path cost for each individual port, and you can set the STG Multicast MAC address.

## Creating Spanning Tree Groups

To configure spanning tree groups:

- 1 From the main menu, choose Application > Spanning Tree > Group Configuration.

The Group Configuration page opens ([Figure 64](#)).

Figure 64 Spanning Tree Group Configuration page

## Application &gt; Spanning Tree &gt; Group Configuration

STP Group Table									
Action	Group	Bridge Priority (hex)	Hello Time	Max. Age Time (sec.)	Forward Delay Time (sec.)	Tagged BPDU on Tagged Port	VID used for Tagged BPDU	STP Multicast Address	STP Group State
 	1	8000	2	20	15	No	4001	01-80-c2-00-00-00	Enabled

STP Group Creation	
STP Group Index	Group 2 ▾
Bridge Priority	8000 ▾ (hex)
Hello Time	2 <input type="text"/> seconds (1 .. 10)
Max. Age Time	20 <input type="text"/> seconds (6 .. 40)
Forward Delay Time	15 <input type="text"/> seconds (4 .. 30)
Tagged BPDU on Tagged Port	Yes ▾
VID used for Tagged BPDU	4002 <input type="text"/> (1 .. 4094)
STP Multicast Address	01-80-c2-00-00-00 <input type="text"/> (xx.xx.xx.xx.xx.xx)

Submit

Table 65 describes the items on the Spanning Tree Group Configuration page.

**Table 65** Spanning Tree Group Configuration page items

Section	Item	Description
STP Group Table	 	Modifies or deletes the group.
	Group	The number assigned to the spanning tree group when the group was created.
	Bridge Priority	For the STP Group, indicates the management-assigned priority value of the bridge ID in hexadecimal notation, which is the most significant byte of the bridge ID. The spanning tree algorithm 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.
	Hello Time	For the STP Group, indicates the Hello Interval (the amount of time between transmissions of BPDUs) specified by management for this bridge. This parameter takes effect only when this bridge becomes the root bridge.  Note that, 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.
	Max. Age time (sec.)	For the STP Group, specifies the maximum age (in seconds) 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.  Note that, 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.
	Forward Delay Time (sec.)	For the STP Group indicates the Forward Delay parameter value specified by management for this bridge. This parameter takes effect only when this bridge becomes the root bridge.  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.  Note that all bridges participating in the spanning tree network use the root bridge's Forward Delay parameter value.

**Table 65** Spanning Tree Group Configuration page items (continued)

Section	Item	Description
	Tagged BPDU on Tagged Port	Displays whether you are sending either tagged or untagged BPDUs from a tagged port.
	VID used for Tagged BPDU	Displays the VLAN ID you are sending the tagged BPDUs for the specified STG to.
	STP Multicast Address	Enter the STP Multicast MAC address.
	STPG Group State	The current operational state of the spanning tree group: Enabled or Disabled.
STP Group Creation	STP Group Index	Choose the group number you want to create.
	Bridge Priority	Select the priority you want.
	Hello Time	Enter the hello time you want for this STG in seconds; range is 1 to 10.
	Max. Age time (sec.)	Enter the maximum age time you want for this STG in seconds; range is 6 to 40.
	Forward Delay Time (sec.)	Enter the forward delay time you want for this STG in seconds; range is 4 to 30.
	Tagged BPDU on Tagged Port	Set the frames as tagged (Yes) or untagged (No) on tagged ports.
	VID used for Tagged BPDU	Enter the VLAN ID you want to send the tagged BPDUs for the specified STG. Note: The default VIDs are 4001 through 4008 for STG 1 through 8, respectively.
	STP Multicast Address	Enter the STP Multicast MAC address.

- 2 Complete the fields as shown.
- 3 Click Submit.

## Modifying Spanning Tree Groups

To modify an STG:

- 1 From the main menu, choose Application > Spanning Tree > Group Configuration.

The Group Configuration page opens (Figure 64).

- In the STP Group Table section, in the row of your choice, click the Modify icon.

The Group Configuration modification page opens (Figure 65).

**Figure 65** Group Configuration modification page

**Application > Spanning Tree > Group Configuration**

Spanning Tree - Group Configuration	
STP Group	2
Bridge Priority	0000 (hex)
Bridge Hello Time	2 seconds (1..10)
Bridge Maximum Age Time	20 seconds (6..40)
Bridge Forward Delay	15 seconds (4..30)
Tagged BPDU on Tagged Port	Yes
VID used for Tagged BPDU	4002 (1..4094)
STP Multicast Address	01-80-c2-00-00-00 (xx.xx.xx.xx.xx.xx)
STP Group State	Disabled

Submit Back

Table 66 describes the items on the Group Configuration modification page.

**Table 66** Spanning Tree Group Configuration modification page items

Section	Item	Range	Description
STP Group Creation	STP Group Index		Choose the group number you want to create.
	Bridge Priority		Select the priority you want.
	Bridge Hello Time	1 to 10	Enter the hello time you want for this STG in seconds.
	Bridge Max. Age time (sec.)	6 to 40	Enter the maximum age time you want for this STG in seconds.
	Bridge Forward Delay Time (sec.)	4 to 30	Enter the forward delay time you want for this STG in seconds.
	Tagged BPDU on Tagged Port		Set the frames as tagged (Yes) or untagged (No) on tagged ports.

**Table 66** Spanning Tree Group Configuration modification page items

Section	Item	Range	Description
	VID used for Tagged BPDU		Enter the VLAN ID you want to send the tagged BPDUs for the specified STG. Note: The default VIDs are 4001 through 4008 for STG 1 through 8, respectively.
	STP Multicast Address		Enter the STP Multicast MAC address.
	STP group state		Indicates the STP group status.

- 3** Type information in the text boxes, or select from the pull-down menu.
- 4** Do one of the following:
  - Click Submit.
  - Click Back to return to the Group Configuration page without making changes.

The modified Group configuration is displayed in the STG Group Table (Figure 64).

## Deleting a Spanning Tree Group

To delete an STG configuration:

- 1** From the main menu, choose Application > Spanning Tree > Group Configuration.  
The Group Configuration page opens (Figure 64).
- 2** In the STG Group Table, click the Delete icon for the entry you want to delete.  
A message opens prompting you to confirm your request.
- 3** Do one of the following:
  - Click Yes to delete the STG configuration.

- Click Cancel to return to the Group Configuration page without making changes.



**Note:** You cannot delete STG 1.

## Associating STG with VLAN Membership

To add a VLAN to an STG:

- 1 From the main menu, choose Application > Spanning Tree > VLAN Membership.

The Spanning Tree VLAN Membership page opens (Figure 66).

**Figure 66** Spanning Tree VLAN Membership page

Application > Spanning Tree > VLAN Membership

STP Group VLAN Membership			
STP Group	Add VLAN	Remove VLAN	Current VLAN Membership
1			1, 10, 20, 30, 40, 50, 60, 70, 80, 90, 2, 3, 4, 5, 6, 7, 8, 100, 101, 9, 11
2			

[Back](#)

The table displays the spanning tree group and the current VLAN membership.

You can add or remove one or more VLANs to or from an STG.



**Note:** You can move a VLAN from one STG to another by simply adding the VLAN to the specified STG.

- 2 To add a VLAN:
  - a Click the modification icon in the Add VLAN column.

The Spanning Tree VLAN Membership Add VLAN page opens (Figure 67).

**Figure 67** Spanning Tree Add VLAN page

**Application > Spanning Tree: VLAN Membership**

**Application > Spanning Tree: Add VLAN**

Current VLAN Membership 1, 10, 20, 30, 40, 50, 60, 70, 80, 90, 2, 3, 4, 5, 6, 7, 8, 100, 101, 9, 11

Add VLAN Membership

**Note: Please use SPACE to separate VLAN numbers.**

- b** Enter the number of the VLAN(s) you want to add to the STG.
  - c** Click Submit.
- 3** To remove a VLAN:

- a** Click the modification icon in the Remove VLAN column.

The Spanning Tree VLAN Membership Remove VLAN page opens (Figure 68).

**Figure 68** Spanning Tree Remove VLAN page

**Application > Spanning Tree: VLAN Membership**

**Application > Spanning Tree: Remove VLAN**

Current VLAN Membership 1, 10, 20, 30, 40, 50, 60, 70, 80, 90, 2, 3, 4, 5, 6, 7, 8, 100, 101, 9, 11

Remove VLAN Membership

**Note: Please use SPACE to separate VLAN numbers.**

- b** Enter the number of the VLAN(s) you want to remove to the STG.

- c Click Submit.



**Note:** You cannot delete VLAN 1 from STG 1.

## Configuring Ports for Spanning Tree

To configure switch ports for Spanning Tree participation:

- 1 From the main menu, choose Application > Spanning Tree > Port Configuration.

The Spanning Tree Port Configuration page opens (Figure 69).

**Figure 69** Spanning Tree Port Configuration page

**Application > Spanning Tree > Port Configuration**

STP Group  
Group | Group 1 ▾

Submit

Spanning Tree - Port Setting						
Port	Trunk	Tagging	Participation	Priority (hex)	Path Cost	State
1		Tag All	Normal Learning ▾	80 ▾	1	Forwarding
2		Tag All	Normal Learning ▾	80 ▾	1	Forwarding
3		Tag All	Normal Learning ▾	80 ▾	1	Forwarding
4		Tag All	Normal Learning ▾	80 ▾	1	Forwarding
5		Tag All	Normal Learning ▾	80 ▾	1	Forwarding
6		Tag All	Normal Learning ▾	80 ▾	1	Forwarding
7		Tag All	Normal Learning ▾	80 ▾	1	Forwarding
8		Tag All	Normal Learning ▾	80 ▾	1	Forwarding
9		Untag All	Disabled ▾	80 ▾	1	Disabled
10		Untag All	Disabled ▾	80 ▾	1	Disabled
11		Untag All	Disabled ▾	80 ▾	1	Disabled
12		Untag PVID Only	Disabled ▾	80 ▾	1	Disabled
Switch			Normal Learning ▾ <input type="checkbox"/>	80 ▾ <input type="checkbox"/>		

Submit

Ports 13 - 24

Table 67 describes the items on the Spanning Tree Port Configuration page.

**Table 67** Spanning Tree Port Configuration page items

Section	Item	Description
STP Group	Group	Choose the STG Group you want to view.
Spanning Tree - Port Setting	Port	The port number of the currently displayed unit.
	Trunk	Displays the trunk that corresponds to the switch ports specified as MLT members.
	Tagging	Displays the egress tagging settings for the port.
	Participation	<p>Choose any (or all) of the switch ports for Spanning Tree participation. Your options are:</p> <ul style="list-style-type: none"> <li>(1) Normal Learning</li> <li>(2) Fast Learning</li> <li>(3) Disabled</li> </ul> <p>Note: When an individual port is a trunk member, changing this setting for one of the trunk members changes the setting for all members of that trunk. Consider the effect changing this value has in your network topology before making changes.</p> <p>The default settings is Normal Learning.</p>
	Priority	The bridge spanning tree parameter that prioritizes the port's lowest path cost to the root. When one or more ports have the same path cost, the STA selects the path with the highest priority (lowest numerical value).
	Path Cost	The bridge spanning tree parameter that determines the lowest path cost to the root.
State	<p>The current state of the port as defined by application of the Spanning Tree Protocol. This state controls what action a port takes on reception of a frame.</p> <p>Note: If the bridge has detected a port that is malfunctioning, it will place that port into the broken (6) state. For ports which are disabled, this object will have a value of disabled (1).</p>	

- 2 Using the Spanning Tree - Port Settings fields, in the port row(s) of your choice, choose to enable STP (normal learning or fast learning) or disable STP.
- 3 Enter the spanning tree priority value for the specified port.  
You do not have to enter a value if you want to use the default priority of 128.

- 4 Enter the spanning tree path cost value for the specified port.  
You do not have to enter a value if you want to use the default path cost of 1.
- 5 Click Submit.

## Changing Spanning Tree Bridge Switch Settings

You can view and configure existing Spanning Tree switch settings.

To configure Spanning Tree switch settings:

- 1 From the main menu, choose Application > Spanning Tree > Bridge Information.

The Spanning Tree Bridge Information page opens ([Figure 70](#)).

**Figure 70** Spanning Tree Bridge Information page

**Application > Spanning Tree > Bridge Information**

**STP Group**  
 Group

---

**Spanning Tree - Bridge Information**

Bridge Priority	<input type="text" value="8000"/> (hex)
Designated Root	80-00-00-0c-18-61-00-01
Root Port	Port 0
Root Path Cost	0
Hello Time	2 seconds
Maximum Age Time	20 seconds
Forward Delay	15 seconds
Bridge Hello Time	<input type="text" value="2"/> seconds (1 - 10)
Bridge Maximum Age Time	<input type="text" value="20"/> seconds (6 - 40)
Bridge Forward Delay	<input type="text" value="15"/> seconds (4 - 30)
Tagged BPDU on Tagged Port	<input type="text" value="No"/>
VID used for Tagged BPDU	<input type="text" value="4001"/> (1 - 4094)
STP Multicast Address	<input type="text" value="01-80-c2-00-00-00"/> (xx-xx-xx-xx-xx-xx)

[Table 68](#) describes the items on the Spanning Tree Bridge Information page.

**Table 68** Spanning Tree Bridge Information page items

Section	Item	Range	Description
STP Group	Group		Choose the STP Group you want to work with.
Spanning Tree - Bridge Information	Bridge Priority	0..0xFFFF	Select the priority value of the bridge ID in hexadecimal notation, which is the most significant byte of the bridge ID. The Spanning Tree Algorithm 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.  The default setting is 8000.
	Designated Root	XXXXXXXX XXXXXXXX	The bridge ID of the root bridge, as determined by the Spanning Tree Algorithm.

**Table 68** Spanning Tree Bridge Information page items

Section	Item	Range	Description
	Root Port		The port number of the port which offers the lowest cost past from this bridge to the root bridge.
	Root Path Cost	Integer	The cost of the path to the root as seen from this bridge.
	Hello Time	1to 10 seconds	The actual Hello Interval, the amount of time between transmissions of configuration Bridge Protocol Data Units (BPDUs) that the root bridge is currently using.  Note: Bridges participating in the spanning tree network use the root bridge's Hello Interval parameter value. See also Bridge Hello Time.
	Maximum Age Time	6 to 40 seconds	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.  Note: 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.
	Forward Delay	4 to 30 seconds	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.  Note: 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.
	Bridge Hello Time	1to 10 seconds	The Hello Interval (the amount of time between transmissions of BPDUs) specified by management for this bridge. This parameter takes effect only when this bridge becomes the root bridge.  Note: 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.  The default setting is 2 seconds.

**Table 68** Spanning Tree Bridge Information page items

Section	Item	Range	Description
	Bridge Forward Delay	4 to 30 seconds	The amount of time that the bridge ports remains in the Listening and Learning states before entering the Forwarding state.  Note: All bridges participating in the spanning tree network use the root bridge's Forward Delay parameter value. See also Forward Delay.  The default setting is 15 seconds.
	Bridge Maximum Age Time	6 to 40 seconds	The maximum age (in seconds) 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.  Note: 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.  The default setting is 20 seconds.
	Tagged BPDU on Tagged Port	(1) Yes (2) No	Displays whether you are sending either tagged or untagged BPDUs from a tagged port.
	VID used for Tagged BPDU	1-4094	Displays the VLAN ID you are sending the tagged BPDUs for the specified STG to.
	STP Multicast Address		Enter the STP Multicast Address.

- 2 Type information in the text boxes, or select from a list.
- 3 Click Submit.

## Configuring MultiLink Trunk Members

You can configure groups of links between the Ethernet Routing Switch and another switch or a server to provide higher bandwidth with active redundant links.

You can configure two to four switch ports together as members of a trunk to a maximum of six trunks.

To configure MultiLink Trunk members:

- 1 From the main menu, choose Application > MultiLink Trunk > Group.  
The Group page opens (Figure 71).

**Figure 71** Group page

**Application > MultiLink Trunk > Group**

MultiLink Trunk Group Setting								
Trunk	Trunk Members				STP Learning	Trunk Mode	Trunk Name	Trunk Status
1	2	3			Normal ▾	Basic	Trunk #1	Disabled ▾
2					Normal ▾	Basic	Trunk #2	Disabled ▾
3					Normal ▾	Basic	Trunk #3	Disabled ▾
4	6	7			Normal ▾	Basic	Trunk #4	Disabled ▾
5					Normal ▾	Basic	Trunk #5	Disabled ▾
6					Normal ▾	Basic	Trunk #6	Disabled ▾

Table 69 describes the items on the Group page.

**Table 69** Group page items

Section	Item	Range	Description
MultiLink Trunk Group Setting	Trunk	1 to 6	<p>This column contains fields in each row that can be configured to create the corresponding trunk. Each port can only be a member of a single trunk. The appropriate trunk number for each trunk member configured within this field is shown adjacent to the corresponding switch port on the following management pages: Port Configuration (see <a href="#">Figure 7 on page 41</a>) and Spanning Tree Configuration (see <a href="#">Figure 62 on page 167</a>).</p> <p>There are no default settings.</p>
	Trunk Members		<p>Type the switch and port numbers to associate with the corresponding trunk.</p> <p>Note: You can configure two to four switch ports together as members of a trunk to a maximum of six trunks. Switch ports can only be assigned a member of a single trunk.</p> <p>There are no default settings.</p>
	STP Learning	(1) Normal (2) Fast (3) Disabled	<p>Choose the parameter that allows the specified trunk to participate in the spanning tree. This setting overrides those of the individual trunk members. Selecting Fast shortens the state transition timer by two seconds.</p> <p>The default setting is Normal.</p>
	Trunk Mode	Basic	<p>The default operating mode of the switch. When in Basic mode, source MAC addresses are dynamically assigned to specific trunk members for flooding and forwarding. This allows the switch to stabilize and distribute the data streams of source addresses across the trunk members.</p>
	Trunk Name	1 to 16	<p>Type a character string to create a unique name to identify the trunk, for example, Trunk1.</p> <p>The name, if chosen carefully, can provide meaningful information to you. For example, S1:T1 to FS2 indicates that Trunk1, in Switch1 connects to File Server 2.</p>
	Trunk Status	(1) Enabled (2) Disabled	<p>Choose to enable or disable any of the existing MultiLink Trunks.</p> <p>Note: When a trunk is not active (Trunk Status field set to Disabled), configuration changes do not take effect until you set the Trunk Status field to enabled.</p>

- 2 Type information in the text boxes, or select from a list.
- 3 Click Submit in any section to save your changes.

## Monitoring MLT Traffic

You can monitor the bandwidth usage for the MultiLink Trunk (MLT) member ports within each trunk in your configuration by selecting the traffic type to monitor.

To monitor MultiLink Trunk traffic:

- 1 From the main menu, choose Application > MultiLink Trunk > Utilization.  
The Utilization page opens (Figure 72).

**Figure 72** Utilization page

### Application > MultiLink Trunk > Utilization

MultiLink Trunk Utilization Selection (View By)	
Trunk	1 ▾
Traffic Type	Px and Tx ▾

Submit

MultiLink Trunk Utilization Table			
Port	Last 5 Minutes	Last 30 Minutes	Last Hour

[Table 70](#) describes the items on the Utilization page.

**Table 70** Utilization page items

Section	Item	Range	Description
MultiLink Trunk Utilization Selection (View By)	Trunk	1 to 16	Choose the trunk to be monitored.
	Traffic Type	(1) RX and TX (2) RX (3) TX	Choose the traffic type to be monitored for percentage of bandwidth utilization.
MultiLink Trunk Utilization Table	Port		A list of the trunk member switch ports that correspond to the trunk specified in the Trunk column.
	Last 5 Minutes		The percentage of packets (of the type specified in the Traffic Type field) used by the port in the last five minutes. This field provides a running average of network activity, and is updated every 15 seconds.
	Last 30 Minutes		The percentage of packets (of the type specified in the Traffic Type field) used by the port in the last 30 minutes. This field provides a running average of network activity, and is updated every 15 seconds.
	Last Hour		The percentage of packets (of the type specified in the Traffic Type field) used by the port in the last 60 minutes. This field provides a running average of network activity, and is updated every 15 seconds.

- 2** In the MultiLink Trunk Utilization Selection section, type the Trunk number and traffic type to be monitored.
- 3** Click Submit.

The results of your request are displayed in the MultiLink Trunk Utilization Table ([Figure 72](#)).

---

## Chapter 8

# Implementing QoS

---

The QoS application delivers a set of tools that, when optimally configured, combats escalating bandwidth costs and optimizes application performance in your network.

QoS tools allow you to prioritize your critical applications and sensitive traffic. You can tailor appropriate services to support this traffic over the wide area, thus maintaining the necessary performance levels on an end-to-end basis.

You can configure Quality of Service (QoS) features in your network by using the the QoS configuration pages available in the Web-based management user interface.

Refer to the *Application Guide for Nortel Ethernet Routing Switch 3510-24T, Software Release 4.0.3* for a sample QoS configuration using the QoS Web pages.

This chapter explains configuring QoS using the QoS pages. The chapter covers the following topics:

- [“Configuring an Interface Group”](#), next
- [“Configuring 802.1p Priority Queue Assignment”](#) on page 197
- [“Configuring 802.1p Priority Mapping”](#) on page 199
- [“Configuring DSCP Mapping”](#) on page 200
- [“Configuring IP Classifier Elements”](#) on page 203
- [“Configuring Layer 2 Classifier Elements”](#) on page 209
- [“Classifier Configurations”](#) on page 216
- [“Classifier Block Configurations”](#) on page 220
- [“Configuring QoS Actions”](#) on page 224
- [“Using the Interface Action Extension”](#) on page 229
- [“Configuring QoS Meters”](#) on page 232

- [“Configuring QoS Policies” on page 235](#)
- [“Configuring QoS Policy Agent Characteristics” on page 241](#)
- [“Using QoS Diagnostics” on page 243](#)

## Configuring an Interface Group

You view existing interface group configurations, or create or modify an interface group if you want a port (or ports) to assign the same QoS policy to all interfaces in the group.



**Note:** One default role combination covers all ports of the device.

---

## Creating an Interface Group Configuration

To create an interface group configuration:

- 1 From the main menu, choose Application > QoS > Devices > Interface Configuration.

The Interface Configuration page opens ([Figure 73](#)).

**Figure 73** QoS Interface Configuration page**Application > QoS > Devices > Interface Configuration**

Interface Queue Table							
Set ID	Queue ID	General Discipline	Bandwidth %	Absolute Bandwidth (Kbps)	Bandwidth Allocation	Service Order	Size (Bytes)
1	1	Priority Queuing	100	0	Relative	1	131072
	2	Priority Queuing	100	0	Relative	2	106496
3	1	Priority Queuing	100	0	Relative	1	65536
	2	Weighted Round Robin	75	0	Relative	2	57344
4	3	Weighted Round Robin	25	0	Relative	2	49152
	1	Priority Queuing	100	0	Relative	1	57344
	2	Weighted Round Robin	65	0	Relative	2	51200
	3	Weighted Round Robin	26	0	Relative	2	38912
5	4	Weighted Round Robin	9	0	Relative	2	24576
	1	Priority Queuing	100	0	Relative	1	46080
	2	Weighted Round Robin	58	0	Relative	2	41984
	3	Weighted Round Robin	27	0	Relative	2	36840
	4	Weighted Round Robin	11	0	Relative	2	28160
6	5	Weighted Round Robin	4	0	Relative	2	19968
	1	Priority Queuing	100	0	Relative	1	36864
	2	Weighted Round Robin	52	0	Relative	2	33792
	3	Weighted Round Robin	24	0	Relative	2	31744
	4	Weighted Round Robin	14	0	Relative	2	26624
	5	Weighted Round Robin	7	0	Relative	2	21504
6	6	Weighted Round Robin	3	0	Relative	2	18432



**Note:** For more information on QoS interface groups, or role combinations, refer to the *Application Guide for Nortel Ethernet Routing Switch 3510-24T, Software Release 4.0.3*.

**Table 71** describes the items on the Interface Queue Table section of the QoS Interface Configuration page.

**Table 71** QoS Interface Queue Table section items

Item	Description
Set ID	The number that identifies a specific queue set.
Queue ID	The number that identifies the queue in the given set.
General Discipline	The queuing discipline that is associated with the specified queue. The options are: (1) Priority Queuing and (2) Weighted Round Robin.

**Table 71** QoS Interface Queue Table section items

Item	Description
Bandwidth	The percentage of available bandwidth consumable to service the queue in one cycle.
Absolute Bandwidth	The absolute bandwidth consumable to service the queue in one cycle.
Bandwidth Allocation	Displays whether absolute or relative bandwidth is specified.
Service Order	The order in which a queue is serviced based on the defined discipline.
Size	The maximum size of the queue in bytes.

[Table 72](#) describes the items on the Interface Group Table section of the QoS Interface Group page.

**Table 72** Interface Group Table section items

Item	Description
	Opens a modification page.
	Deletes the row.
Role Combination	The tag used to identify interfaces with the characteristics specified by the attributes of this class instance (string 1 to 32). These identifiers are used within a number of classes to logically identify a physical set of interfaces to which policy rules and actions are applied.
Capabilities	A list of the interface capabilities used by the PDP or network manager to select which policies and configurations may be pushed to the Policy Enforcement Point (PEP). The options are: (1) Input Ip Classification, (2) Output Ip Classification, (3) Input 802 Classification, and (4) Output 802 Classification.
Interface Class	The type of traffic received on interfaces associated with the specified role combination. The options are Trusted, Untrusted, and Unrestricted. The default is Unrestricted.
Entry Storage	Specifies whether or not the interface group can be deleted.



**Note:** For more information on QoS interface classes—or trusted, untrusted, and unrestricted ports—refer to the *Application Guide for Nortel Ethernet Routing Switch 3510-24T, Software Release 4.0.3*.

[Table 73](#) describes the items on the Interface Group Creation section of the QoS Interface Group page.

**Table 73** Interface Group Creation section page items

Item	Range	Description
Role Combination	1 to 31	Type a character string to identify the role combination.
Interface Class	Trusted Untrusted Unrestricted	Choose an interface class: trusted untrusted unrestricted  Refer to <i>Application Guide for Nortel Ethernet Routing Switch 3510-24T, Software Release 4.0.3</i> for more information on interface classes.  The default setting is Unrestricted.

- 2 In the Interface Group Creation section, type a role combination name in the text boxes, and select the interface class from the list.
- 3 Click Submit.  
  
The new interface group configuration appears in the Interface Group Table ([Figure 73](#)).

## Displaying Interface ID Table

To display the Interface ID Table:

- 1 From the main menu, choose Application > QoS > Devices > Interface Configuration.  
  
The QoS Interface Configuration page opens ([Figure 73](#)).
- 2 Click Display Interface ID Table.  
  
The Interface ID page opens ([Figure 74](#)). The table displays all interfaces and the interface group (role combination) to which it belongs. If an interface does not belong to an interface group (role combination), it does not display in the table.

The table displays a mapping of each interface to its interface group.

**Figure 74** Interface ID page

**Application > QoS > Devices > Interface ID**

Interface ID Table		
Interface	Role Combination	Queue Set
1	allBayStackfcs	8
2	allBayStackfcs	8
3	allBayStackfcs	8
4	allBayStackfcs	8
5	allBayStackfcs	8
6	allBayStackfcs	8
7	allBayStackfcs	8
8	allBayStackfcs	8
9	allBayStackfcs	8
10	allBayStackfcs	8
11	allBayStackfcs	8
12	allBayStackfcs	8
13	allBayStackfcs	8
14	allBayStackfcs	8
15	allBayStackfcs	8
16	allBayStackfcs	8
17	allBayStackfcs	8
18	allBayStackfcs	8
19	allBayStackfcs	8
20	allBayStackfcs	8
21	allBayStackfcs	8
22	allBayStackfcs	8
23	allBayStackfcs	8
24	allBayStackfcs	8

[Back](#)

Table 74 describes the items on the Interface ID page.

**Table 74** Interface ID page items

Item	Description
Interface	Displays the unit and port number.
Role Combination	Displays the role combination associated with the interface.
Queue Sets	Displays the queue set associated with this interface.

## Adding or Removing Interface Group Members

To select or deselect ports as members of an existing interface group:

- 1 From the main menu, choose Application > QoS > Devices > Interface Configuration.

The QoS Interface Configuration page opens (Figure 73).

- 2 In the Interface Group Table section, in the row of your choice, click the Modify icon.

The Interface Group Assignment page opens (Figure 75).

**Figure 75** Interface Group Assignment page

**Application > QoS > Devices > Interface Group Assignment**

QoS - Interface Group Port Assignment	
<b>Role Combination</b>	allBayStackIcfs
<b>Capabilities</b>	Input 802 Classification Input IP Classification
<b>Interface Class</b>	Untrusted
	<b>Port Membership</b>
<b>Port</b>	All 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
	<input type="checkbox"/> <input checked="" type="checkbox"/>
<input type="button" value="Submit"/> <input type="button" value="Back"/>	

[Table 75](#) describes the items on the Interface Group Assignment page.

**Table 75** Interface Group Assignment page items

Item	Description
Role Combination	The tag used to identify interfaces with the characteristics specified by the attributes of this class instance (string 1 to 32). These identifiers are used within a number of classes to logically identify a physical set of interfaces to which policy rules and actions are applied. This is the group of interfaces (interface group) to which policy rules and actions are applied.
Capabilities	A list of the interface capabilities used by the PDP or network manager to select which policies and configurations may be pushed to the Policy Enforcement Point (PEP). The options are: (1) Input Ip Classification, (2) Output Ip Classification, (3) Input 802 Classification, and (4) Output 802 Classification.
Interface Class	The type of traffic received on interfaces associated with the specified role combination. The options are Trusted, Untrusted, and Unrestricted.
Port Membership	Select the external ports to associate with the interface group, or select ALL to associate all ports on that unit.

- 3** In the Port Membership section, click the check boxes of the ports (or ALL to select all ports on the unit) to associate with the interface group.
- 4** Do one of the following:
  - Click Submit.
  - Click Back to return to the Interface Configuration page without making changes.

## Deleting Ports or an Entire Interface Group Configuration

To delete an Interface group configuration:

- 1** From the main menu, choose Application > QoS > Devices > Interface Configuration.  
The QoS Interface Configuration page opens ([Figure 73](#)).
- 2** In the Interface Group Table section, in the interface group configuration row of your choice, click the Modify icon.  
The Interface Group Assignment page opens ([Figure 75](#)).

- 3 In the Port Membership section, click the check boxes to deselect all ports associated with the interface group.



**Note:** You can delete all ports of one unit simultaneously, by clicking All.

---

- 4 Click Submit.  
The Interface Configuration page is displayed ([Figure 73](#)).
- 5 In the Interface Group Table section, in the configuration row of your choice, click the Delete icon.  
A message opens prompting you to confirm your request.
- 6 Do one of the following:
  - Click Yes to delete the interface group configuration.
  - Click Cancel to return to the Interface Configuration page without making changes.

## Configuring 802.1p Priority Queue Assignment

You can assign 802.1p user priority values to a queue for each interface with a specific queue set. This information is used for assigning egress traffic to outbound queues.

To configure 802.1p user priority:

- 1 From the main menu, choose Application > QoS > Devices > Priority Q Assign.  
The 802.1p Priority Queue Assignment page opens ([Figure 76](#)).

**Figure 76** 802.1p Priority Queue Assignment page**Application > QoS > Devices > 802.1p Priority Queue Assignment**

802.1p Priority Assignment (View By)

Queue Set

Submit

802.1p Priority Assignment Table

802.1p Priority	Queue
0	<input type="text" value="1"/>
1	<input type="text" value="1"/>
2	<input type="text" value="1"/>
3	<input type="text" value="1"/>
4	<input type="text" value="1"/>
5	<input type="text" value="1"/>
6	<input type="text" value="1"/>
7	<input type="text" value="1"/>

Submit



**Note:** Nortel recommends using the default 802.1p assignments to ensure end-to-end QoS connectivity.

Table 76 describes the items on the 802.1p Priority Queue Assignment page.

**Table 76** 802.1p Priority Assignment Table section page items

Item	Description
802.1p Priority	The 802.1p user priority mapped to a queue.
Queue	Type a number that signifies the desired queue in the specified queue set with which this priority is associated.

- 2 In the 802.1p Priority Assignment Table section, type the information in the text boxes.
- 3 Click Submit.

## Configuring 802.1p Priority Mapping

To configure 802.1p priority to DSCP mapping:

- 1 From the main menu, choose Application > QoS > Devices > Priority Mapping.

The 802.1p Priority Mapping page opens (Figure 77).

**Figure 77** 802.1p Priority Mapping page

### Application > QoS > Devices > 802.1p Priority Mapping

802.1p Priority Mapping Table		
802.1p Priority	DSCP	Name
0	0x0	Standard Service
1	0x0	Standard Service
2	0xA	Bronze Service
3	0x12	Silver Service
4	0x1A	Gold Service
5	0x22	Platinum Service
6	0x2E	Premium Service
7	0x30	Network Service

Submit



**Note:** The 802.1 p Priority Mapping displays several default values and their corresponding service names.



**Note:** Nortel recommends using the default 802.1p priority to DSCP mappings to ensure end-to-end QoS connectivity.

[Table 77](#) describes the items on the 802.1p Priority Mapping page.

**Table 77** 802.1p Priority Mapping page items

Item	Description
802.1p Priority	The 802.1p user priority to map to a DSCP value at ingress.
DSCP	Type the DSCP value to associate with the specified 802.1p user priority value at ingress.
Name	Enter a name that describes the mapping, using 16 alphanumeric characters.

- 2 Type the information in the text boxes.
- 3 Click Submit.

## Configuring DSCP Mapping

To configure DSCP to 802.1p user priority/drop precedence mapping:

- 1 From the main menu, choose Application > QoS > Devices > DSCP Mapping.  
The DSCP Mapping page opens ([Figure 78](#)).

**Figure 78** DSCP Mapping page**Application > QoS > Devices > DSCP Mapping**

<b>DSCP Mapping Table</b>				
<b>Action</b>	<b>DSCP</b>	<b>802.1p Priority</b>	<b>Drop Precedence</b>	<b>Service Class</b>
	0x0	0	High Drop	Standard Service
	0x1	0	High Drop	Standard Service
	0x2	0	High Drop	Standard Service
	0x3	0	High Drop	Standard Service
	0x4	0	High Drop	Standard Service
	0x5	0	High Drop	Standard Service
	0x6	0	High Drop	Standard Service
	0x7	0	High Drop	Standard Service
	0x8	2	High Drop	Bronze Service
	0x9	0	High Drop	Standard Service
	0xA	2	Low Drop	Bronze Service
	0xB	0	High Drop	Standard Service
	0xC	2	High Drop	Bronze Service
	0xD	0	High Drop	Standard Service
	0xE	2	High Drop	Bronze Service



**Note:** Nortel recommends using the default DSCP mappings to ensure end-to-end QoS connectivity.

Table 78 describes the items on the DSCP Mapping page.

**Table 78** DSCP Mapping page items

<b>Item</b>	<b>Format</b>
	Opens a modification page.
DSCP	The attribute used internally to determine the appropriate Layer 2 cost of service (CoS) mappings.
802.1p Priority	The IEEE802 CoS value used when mapping the DSCP value.

**Table 78** DSCP Mapping page items (continued)

Item	Format
Drop Precedence	The drop value precedence used for traffic with the associated 802.1p user priority value with the identified queue.  Note: Generally, low packet drop precedence receives preferential treatment.
Service Class	Displays a name that describes the mapping.

- 2 In the row of your choice, click the Modification icon.  
The DSCP Mapping Modification page opens (Figure 79).

**Figure 79** DSCP Mapping Modification page

### Application > QoS > Devices > DSCP Mapping

DSCP Mapping Modification	
DSCP	0x0
802.1p Priority	0 ▾
Drop Precedence	High Drop ▾
Service Class	Standard Service



Table 79 describes the items on the DSCP Mapping Modification page.

**Table 79** DSCP Mapping Modification page items

Item	Range	Format
DSCP	0..63	Type the attribute to use internally to determine the appropriate Layer 2 cost of service (CoS) mappings.
802.1p Priority	0..7	Choose the IEEE802 CoS value to use when mapping the DSCP value.

**Table 79** DSCP Mapping Modification page items (continued)

Item	Range	Format
Drop Precedence	High Drop Low Drop	Choose the drop value precedence to use for traffic with the associated 802.1p user priority value with the identified queue: High Drop Low Drop Note: Generally, low packet drop precedence receives preferential treatment.
Service Class	16 alphanumeric characters	Enter the service class.  Note: This field corresponds to the adjacent user priority levels.
	Note: Mappings created on the DSCP mapping modification page are used at egress for marking traffic. Refer to <i>Application Guide for Nortel Ethernet Routing Switch 3510-24T, Software Release 4.0.3</i> for more information on trusted, untrusted, and unrestricted interface classes and the relationship to traffic re-marking.	

- 3 Select from a list or enter your service class name.
- 4 Click Submit.

The modified configuration appears in the DSCP Mapping Table (Figure 78).



**Note:** For more information on QoS interface classes—or trusted, untrusted, and unrestricted ports—refer to the *Application Guide for Nortel Ethernet Routing Switch 3510-24T, Software Release 4.0.3*.

## Configuring IP Classifier Elements

You can create an IP classifier element, which enables the switch to classify traffic. In turn, IP classifier elements are then referenced by classifiers and classifier blocks, which determine access to and denial of network services.

## Creating an IP Classifier Element

To create an IP classifier element:

- 1 From the main menu, choose Application > QoS > Rules > IP Classifier Element.

The IP Classifier Element page opens ([Figure 80](#) and [Figure 81](#)).

Figure 80 IP Classifier Element page (1 of 2)

## Application &gt; QoS &gt; Rules &gt; IP Classifier Element

## IP Classifier Element Table

Action	Instance	Address Type	Destination Address	Destination Mask Length	Source Address	Source Mask Length	DSCP	IPv4 Protocol / IPv6 Next Header	Destination L4 Port	Source L4 Port	IPv6 Flow Id	Storage Type
--------	----------	--------------	---------------------	-------------------------	----------------	--------------------	------	----------------------------------	---------------------	----------------	--------------	--------------

Figure 81 IP Classifier Element page (2 of 2)

**IP Classifier Element Creation**

<b>Address Type</b>	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
<b>Destination Address</b>	<input checked="" type="radio"/> Ignore <input type="radio"/> <input type="text" value="0.0.0.0"/> <input type="text" value="0"/> Address Mask Length
<b>Source Address</b>	<input checked="" type="radio"/> Ignore <input type="radio"/> <input type="text" value="0.0.0.0"/> <input type="text" value="0"/> Address Mask Length
<b>DSCP</b>	Ignore <input type="text"/>
<b>IPv4 Protocol / IPv6 Next Header</b>	<input checked="" type="radio"/> Ignore <input type="radio"/> Preconfigured Protocol <input type="text" value="TCP"/> <input type="radio"/> User Defined Protocol <input type="text" value="0"/>
<b>Destination Layer4 Port</b>	<input checked="" type="radio"/> Ignore <input type="radio"/> Preconfigured Port # <input type="text" value="TFTP"/> <input type="radio"/> User Defined Port # <input type="text" value="0"/> to <input type="text" value="1"/> (0..65535)
<b>Source Layer4 Port</b>	<input checked="" type="radio"/> Ignore <input type="radio"/> Preconfigured Port # <input type="text" value="TFTP"/> <input type="radio"/> User Defined Port # <input type="text" value="0"/> to <input type="text" value="1"/> (0..65535)
<b>IPv6 Flow Id</b>	<input checked="" type="radio"/> Ignore <input type="radio"/> <input type="text"/> (e.g. 0xF2843)



**Note:** When you choose the Ignore value, the filter matches all criteria for that parameter.

[Table 80](#) describes the items on the IP Classifier Element Table and IP Classifier Element Creation sections.

**Table 80** IP Classifier Element Table and Classifier Element Creation

Section	Item	Range	Description
IP Classifier Element Table	Action		Deletes the row.  Note: You cannot delete a classifier element if it is referenced in a classifier or classifier block.
	Instance		Displays unique identifier.
	Address Type	IPv4 IPv6	Displays the IPv4 protocol/IPv6 next header to match against the packet's destination and/or source IP addresses.
	Destination Address		Displays the IP address to match against the packet's destination IP address.
	Destination Mask Length	0 to 32 (IPv4) 0 to 128 (IPv6)	Displays the mask length for the matching of the destination IP address.
	Source Address		Displays the IP address to match against the packet's source IP address.
	Source Mask Length	0 to 32 (IPv4) 0 to 128 (IPv6)	Displays the mask length for the matching of the source IP address.
	DSCP	Ignore, Integer (0.63)	Displays the value that the DSCP in the packet must have and match this classifier element. This displays the DSCP value that this classifier element attempts to match.
	IPv4 Protocol/IPv6 Next Header	TCP UDP ICMP IGMP RSVP Ignore	Displays the IPv4 protocol/IPv6 next header to match against the packet's IP protocol field.
	Destination L4 Port	Integer (0.65535)	Displays the value that the packet's layer 4 destination port number must have and match this classifier element.
	Source L4 Port	Integer (0.65535)	Displays the value that the packet's layer 4 source port number must have and match this classifier element.
	IPv6 Flow ID	0..0xffff	Displays the flow identifier in an IPv6 header
	Storage Type	volatile nonvolatile other	Displays whether the IP classifier element is stored across reboots: volatile—lost after a reset nonvolatile—stored across reset other—system created; cannot be deleted or referenced

**Table 80** IP Classifier Element Table and Classifier Element Creation (continued)

Section	Item	Range	Description
IP Classifier Element Creation/ Address Type		IPv4 IPv6	Click the IP address type you want.
IP Classifier Element Creation/ Destination Address	Ignore		Click if you want the classifier element to ignore the packet's destination IP address.
	Address		Click if you want the classifier element to match the packet's destination network address. Enter the IP address to match against the packet's destination IP address.
	Mask Length	0 to 32 (IPv4) 0 to 128 (IPv6)	Enter the length of the mask for the matching of the destination IP address.
IP Classifier Element Creation/Source Address	Ignore		Click if you want the classifier element to ignore the packet's source IP address.
	Address		Click if you want the classifier element to match the packet's source network address. Enter the IP address to match against the packet's source IP address.
	Mask Length	0 to 32 (IP v4) 0 to 128 (IPv6)	Enter the length of the mask for the matching of the source IP address.
IP Classifier Element Creation/DSCP	DSCP	Ignore, Integer (0.63)	Choose the value that the DSCP in the packet must have and match this classifier element.
IP Classifier Element Creation/IPv4 Protocol/IPv6 Next Header	Ignore		Click if you want the classifier element to ignore the packet's IPv4 protocol or IPv6 next header.
	Preconfigured Protocol	TCP UDP ICMP IGMP RSVP	Choose the IPv4 protocol or IPv6 next header you want the classifier element to match.
	User Defined Protocol		Enter the IPv4 protocol or IPv6 next header that the packet must have and match this classifier element.

**Table 80** IP Classifier Element Table and Classifier Element Creation (continued)

Section	Item	Range	Description
IP Classifier Element Creation/ Destination Layer4 Port	Ignore		Click if you want the classifier element to ignore the packet's layer 4 destination port.
	Preconfigured Port #	TFTP FTP Control FTP Data TELNET SMTP HTTP HTTPS	Choose the value that the packet's layer 4 destination port number must have and match this classifier element.
	User Defined Port #	Integer	Enter the range that the packet's layer 4 destination port number must have and match this classifier element by entering the starting number and choosing the final number from the pull-down menu.
IP Classifier Element Creation/ Source Layer 4 Port	Ignore		Click if you want the classifier element to ignore the packet's layer 4 source port.
	Preconfigured Port #	TFTP FTP Control FTP Data TELNET SMTP HTTP HTTPS	Choose the value that the packet's layer 4 source port number must have and match this classifier element.
	User Defined Port #	Integer	Enter the range that the packet's layer 4 source port number must have and match this classifier element by entering the starting number and choosing the final number from the pull-down menu.
IP Classifier Element Creation/IPv6 Flow ID	Ignore		Specifies that the system ignore the packet's IPv6 flow identifier field.
		0.. 0xffff	Enter the hexadecimal value of the flow identifier you want to match.

- 2 In the IP Classifier Element Creation section, type information in the text boxes, or select from a list.

**3** Click Submit.

The new IP classifier element configuration appears in the IP Classifier Table (Figure 80). This table displays all IP classifier elements you created.



**Note:** An IP classifier element configuration is not modifiable. The classifier element must be deleted and then re-created.

---

## Deleting an IP Classifier Element Configuration

To delete a IP classifier element configuration:

**1** From the main menu, choose Application > QoS Rules > IP Classifier Element.

The IP Classifier Element page opens (Figure 80 and Figure 81).

**2** In the IP Classifier Element Table, in the IP classifier element configuration row of your choice, click the Delete icon.

A message opens prompting you to confirm your request.

**3** Do one of the following:

- Click Yes to delete the IP classifier element configuration.
- Click Cancel to return to the IP Classifier Element page without making changes.



**Note:** You cannot delete a classifier element if it is referenced in a classifier or classifier block.

---

## Configuring Layer 2 Classifier Elements

You can configure layer 2 classifier elements by defining IEEE 802-based parameters. Layer 2 classifiers are defined by specifying the layer 2 classifier element to be included in the given classifier/classifier blocks.

## Creating a Layer 2 Classifier Element Configuration

To create a layer2 classifier element configuration:

- 1 From the main menu, choose Application > QoS > Rules > Layer2 Classifier Element.

The Layer2 Classifier Element page opens (Figure 82).

Figure 82 Layer2 Classifier Element page

Application > QoS > Rules > Layer2 Classifier Element

L2 Classifier Element Table										
Action	Instance	Destination MAC Addr	Destination MAC Addr Mask	Source MAC Addr	Source MAC Addr Mask	VLAN	VLAN Tag	EtherType	802.1p Priority	Storage Type
<input checked="" type="checkbox"/>	64001	Ignore	Ignore	Ignore	Ignore	Ignore	Untagged	IP	Ignore	Other
<input checked="" type="checkbox"/>	64002	Ignore	Ignore	Ignore	Ignore	Ignore	Tagged	IP	Ignore	Other

**Layer2 Classifier Element Creation**

Destination MAC Address:  Ignore  
    
 MAC Addr                      MAC Addr Mask

Source MAC Address:  Ignore  
    
 MAC Addr                      MAC Addr Mask

VLAN:  Ignore  
 VLAN Range  to  (1..4094)

VLAN Tag:

EtherType:  Ignore  
 Preconfigured   
 User Defined  (e.g. 0x8137)

802.1p Priority:



**Note:** When you choose the Ignore value, the filter matches all criteria for that parameter.

Table 81 describes the items on the Layer2 Classifier Element Table and Layer2 Classifier Element Creation sections of the Layer2 Classifier Element page.

**Table 81** Layer2 Classifier Element Table and Layer2 Classifier Element Creation

Section	Item	Range	Description
Layer 2 Classifier Element Table	Action		Deletes the row.
	Instance		Displays unique identifier.
	Destination MAC Addr	XX-XX-XX-XX-XX-XX	Displays the MAC address to match against the packet's destination MAC address.
	Destination MAC Addr Mask	XX-XX-XX-XX-XX-XX	Specifies the bits in the destination MAC address to be considered to match against the packet's destination MAC address.
	Source MAC Addr	XX-XX-XX-XX-XX-XX	Displays the MAC address to match against the packet's source MAC address.
	Source MAC Addr Mask	XX-XX-XX-XX-XX-XX	Specifies the bits in the source MAC address to be considered to match against the packet's source MAC address.
	VLAN	Ignore, 1-4094	Displays the VLAN range you want.
VLAN Tag	Untagged Tagged Ignore	Displays the VLAN tag type you want to check.	

**Table 81** Layer2 Classifier Element Table and Layer2 Classifier Element Creation (continued)

Section	Item	Range	Description
	EtherType	Ignore Netmap TCP Netmap XNS XTP LOOP Vines Vines IP Banyan Vines Echo Vines Banyan Echo ARP RARP IP IPv6 3Com NBP 3Com NBP Ack 3Com NBP ConnReq 3Com NBP ConnRsp 3Com NBP ConnComplt 3Com NBP CloseReq 3Com NBP CloseRsp 3Com NBP Datagram 3Com NBP Broadcast 3Com NBP NameClaim 3Com NBP DelName LAP Atalk ARP Atalk IBM Net Mon IBMRT XNS Compatibility XNS IPX Netware SNMP User-defined	Displays the Ethernet type you are filtering on.
	802.1p Priority	Ignore, 0...7.	Displays the 802.1p priority level.
	Storage Type	volatile nonvolatile other	Displays whether the L2 classifier element is stored across reboots: <ul style="list-style-type: none"> <li>• volatile—lost after a reset</li> <li>• nonvolatile—stored across reset</li> <li>• other—system created; cannot be deleted or referenced</li> </ul>

**Table 81** Layer2 Classifier Element Table and Layer2 Classifier Element Creation (continued)

Section	Item	Range	Description
Layer2 Classifier Element Creation	Destination MAC Address	Ignore	Click Ignore is you want to ignore the packet's destination MAC address.
		MAC Addr: XX-XX-XX-XX-XX-XX	Enter the MAC address to match against the packet's destination MAC address.
		MAC Addr Mask: XX-XX-XX-XX-XX-XX	Enter the bits in the destination MAC address to be considered to match against the packet's destination MAC address.
	Source MAC Address	Ignore	Click Ignore is you want to ignore the packet's source MAC address.
		MAC Addr: XX-XX-XX-XX-XX-XX	Enter the MAC address to match against the packet's source MAC address.
		MAC Addr Mask: XX-XX-XX-XX-XX-XX	Enter the bits in the source MAC address to be considered to match against the packet's source MAC address.
	VLAN	Ignore, 1-4094	Enter the starting VLAN of the range you want and select the end of the range from the pull-down menu.
	VLAN Tag	Untagged Tagged Ignore	Choose the VLAN tag type you want to check.
	EtherType	Ignore	Click if you want the classifier element to ignore the packet's Ethernet type.

**Table 81** Layer2 Classifier Element Table and Layer2 Classifier Element Creation (continued)

Section	Item	Range	Description
		Preconfigured: Netmap TCP Netmap XNS XTP LOOP Vines Vines IP Banyan Vines Echo Vines Banyan Echo ARP RARP IP IPv6 3Com NBP 3Com NBP Ack 3Com NBP ConnReq 3Com NBP ConnRsp 3Com NBP ConnComplt 3Com NBP CloseReq 3Com NBP CloseRsp 3Com NBP Datagram 3Com NBP Broadcast 3Com NBP NameClaim 3Com NBP DelName LAP Atalk ARP Atalk IBM Net Mon IBMRT XNS Compatibility XNS IPX Netware SNMP	Choose the Ethernet type you want the classifier element to match.  Note: To create a non-IP classifier element, choose any Ethernet type <i>except</i> IP or IPv6.
		User Defined	Enter the Ethernet type that the packet must have and match this classifier element.
	802.1p Priority	Ignore Priority 0 Priority 1 Priority 2 Priority 3 Priority 4 Priority 5 Priority 6 Priority 7	Choose either Ignore or the 802.1p priority level.

- 2 Type the information in the text boxes, or select from a list.
- 3 Click Submit.

The new Layer2 classifier element configuration appears in the Layer2 Classifier Element Table ([Figure 82](#)).



**Note:** You cannot delete a classifier element if it is referenced in a classifier/classifier block.

---

## Deleting a Layer 2 Classifier Element Configuration

To delete a layer 2 classifier element configuration:

- 1 From the main menu, choose Application > QoS > Rules > Layer2 Classifier Element.

The Layer2 Classifier Element page opens ([Figure 82](#)). This table displays all layer 2 classifier elements you created.

- 2 In the Layer2 Classifier Element Table, in the layer 2 classifier element configuration row of your choice, click the Delete icon.

A message opens prompting you to confirm your request.

- 3 Do one of the following:
  - Click Yes to delete the classifier element configuration.
  - Click Cancel to return to the Layer2 Classifier Element page without making changes.



**Note:** A Layer 2 classifier element configuration cannot be modified. The configuration must be deleted and then recreated.

You cannot delete a Layer 2 classifier element that is referenced by a classifier/classifier block.

---

## Classifier Configurations

You can display existing classifiers using the Web-based management system.

To display classifiers:

- 1 From the main menu, choose Application > QoS > Rules > Classifier.  
The Classifier page opens (Figure 83).

**Figure 83** Classifier page

### Application > QoS > Rules > Classifier

Classifier Table			
Action	Classifier Name	Classifier Set ID	
 	UntrustedClfrs1	64001	
 	UntrustedClfrs2	64002	

[Create Classifier](#)



**Note:** Refer to *Application Guide for Nortel Ethernet Routing Switch, Software Release 4.0.3* for more information on classifiers.

Table 82 describes the items on the Classifier page.

**Table 82** Classifier Page items

Section	Item	Range	Description
Classifier Table	Action	 	Allows you to view or delete the entry.  Note: The modify button displays a read-only page. You cannot modify a classifier. You must delete the classifier and re-create one as you want it.

**Table 82** Classifier Page items (continued)

Section	Item	Range	Description
	Classifier Name		Displays name of the classifier (either the name you assigned the classifier or the default name the system assigned).
	Classifier Set ID		Displays the set ID of the classifier that the system assigns.

## Creating Classifiers

To create a Classifier:

- 1 From the main menu, choose Application > QoS > Rules > Classifier.  
The Classifier page opens (Figure 83).
- 2 Click Create Classifier.  
The Classifier Creation page opens (Figure 84).

**Figure 84** Classifier Creation page

**Application > QoS > Rules > Classifier Creation**

Classifier Name

---

**IP Classifier Element**

Instance	Address Type	Destination Address	Destination Mask Length	Source Address	Source Mask Length	DSCP	IPv4 Protocol / IPv6 Next Header	Destination L4 Port	Source L4 Port	IPv6 Flow Id
<input checked="" type="radio"/> None										

---

**L2 Classifier Element**

Instance	Destination MAC Addr	Destination MAC Addr Mask	Source MAC Addr	Source MAC Addr Mask	VLAN	VLAN Tag	EtherType	802.1p Priority
<input checked="" type="radio"/> None								

---

**System Classifier Element**

Instance	Unknown Ucast Frames	Unknown Mcast Frames	Known Mcast Frames	Broadcast Frames	Pattern
<input checked="" type="radio"/> None					

- 3 You can enter a name for the classifier using up to 16 alphanumeric characters.

If you do not enter a name, the system assigns a name to each new classifier.



**Note:** Each classifier can have only a *single* IP classifier element *plus* a *single* L2 classifier element. You can, however, create a classifier using only one IP classifier element or only one L2 classifier element.

---

- 4 Click only one IP classifier element from those displayed on the IP Classifier Element table.
- 5 Click only one L2 classifier element from those displayed on the L2 Classifier Element table.
- 6 Click Submit.

The system returns you to the Classifier page and displays the new Classifier on the Classifier Table.



**Note:** You cannot delete a classifier that is referenced by a classifier or by a policy. You must first delete the classifier block or the policy.

---

## Viewing Classifier Details

To view classifier details:

- 1 From the main menu, choose Application > QoS > Rules > Classifier.  
The Classifier page opens ([Figure 83](#)).
- 2 Choose the classifier you want to view, and click the modify button.  
The Classifier View page opens ([Figure 85](#)).



**Note:** The modify button displays a read-only page. You cannot modify a classifier; you must delete the classifier and re-create one as you want it.

---



**Note:** Each classifier in a classifier block must match the same parameters and the same mask, range, and VLAN tag type. Additionally, all members of a classifier block must be configured consistently regarding meters and actions—that is, they must all specify meters or they must all not specify meters, and they must all specify actions or they must all not specify actions. Refer to “Using QoS Diagnostics,” for information on comparing classifiers.

**Figure 85** Classifier View page

**Application > QoS > Rules > Classifier View**

Classifier Name

IP Classifier Element											
Instance	Address Type	Destination Address	Destination Mask Length	Source Address	Source Mask Length	DSCP	IPv4 Protocol / IPv6 Next Header	Destination L4 Port	Source L4 Port	IPv6 Flow Id	Storage Type
None											

L2 Classifier Element									
Instance	Destination MAC Addr	Destination MAC Addr Mask	Source MAC Addr	Source MAC Addr Mask	VLAN	VLAN Tag	EtherType	802.1p Priority	Storage Type
64002	Ignore	Ignore	Ignore	Ignore	Ignore	Tagged IP		Ignore	Other

System Classifier Element						
Instance	Unknown Ucast Frames	Unknown Mcast Frames	Known Mcast Frames	Broadcast Frames	Pattern	Storage Type

3 Click Back.

The system returns you to the Classifier page.

## Deleting a Classifier

To delete a classifier:

1 From the main menu, choose Application > QoS > Rules > Classifier.

The Classifier page opens (Figure 83).

- 2 Click the delete icon next to the row with the classifier you want to delete.



**Note:** You cannot delete a classifier or classifier block that is referenced by a policy. You must first delete the policy.

---

## Classifier Block Configurations

You can view existing classifier blocks using the Web-based management system.

To view classifier blocks:

- 1 From the main menu, choose Application > QoS > Rules > Classifier Block.  
The Classifier Block page opens (Figure 86).

**Figure 86** Classifier Block page

**Application > QoS > Rules > Classifier Block**

Classifier Block Table		
Action	Block Name	Block Number
 	UntrustedClfrs1	64001
 	UntrustedClfrs2	64002

**Create Classifier Block**



**Note:** Refer to the *Application Guide for Nortel Ethernet Routing Switch, Software Release 4.0.3* for more information on classifier blocks.

---

Table 83 describes the items on the Classifier Block page.

**Table 83** Classifier Block Page items

Section	Item	Range	Description
Classifier Block Table	Action	 	Allows you to modify or delete the entry.
	Block Name		Displays name of the classifier block (either the name you assigned the block or the default name the system assigned).
	Block Number		Displays the number of the classifier block that the system assigns.

## Creating Classifier Blocks

To create a classifier block:

- 1 From the main menu, choose Application > QoS > Rules > Classifier Block.  
The Classifier Block page opens (Figure 86).
- 2 Click Create Classifier Block.  
The Classifier Block Creation/Modification page opens (Figure 87).

**Figure 87** Classifier Block Creation/Modification page

**Application > QoS > Rules > Classifier Block Creation / Modification**



Classifier Block Name

Classifier Block Members				
Action	Classifier Name	Classifier Set ID	Meter	Action

- 3 You can enter a name for the classifier block using up to 16 alphanumeric characters.

If you do not enter a name, the system assigns a name to each new classifier block.

- 4 Click the classifiers you want to include in the block from those listed on the Classifier Block Members table.

The table displays those meters that you created using the Meters page.

The table displays default actions and those you defined using the Actions page.



**Note:** Each classifier in a classifier block must match the same parameters and the same mask, range, and VLAN tag type. Additionally, all members of a classifier block must be configured consistently regarding meters and actions—that is, they must all specify meters or they must all not specify meters, and they must all specify actions or they must all not specify actions.

---

- 5 Click Submit.

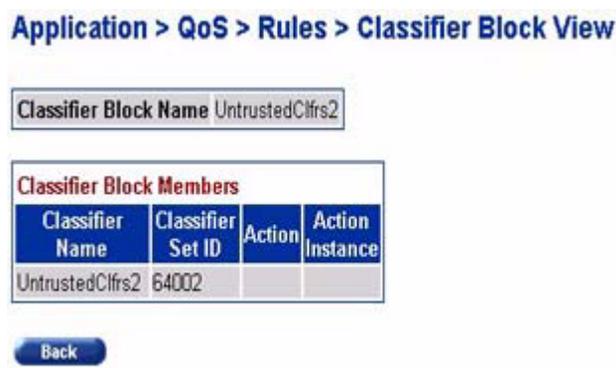
The system returns you to the Classifier Block page and displays the new classifier block on the Classifier Block Table.

## Modifying a Classifier Block

To modify a classifier block:

- 1 From the main menu, choose Application > QoS > Rules > Classifier Block. The Classifier Block page opens ([Figure 86](#)).
- 2 Click the row with the classifier block you want to modify.
- 3 Click the modify icon.

The Classifier Block Creation/Modification page opens ([Figure 88](#)) and displays the parameters of the classifier block you want to modify.

**Figure 88** Classifier Creation/Block Modification page

- 4 To add another classifier to the existing classifier block, click on that classifier.
- 5 To delete a classifier from the existing classifier block, click on that classifier.
- 6 Choose the new meters and actions you want.
- 7 Click Submit.

## Deleting a Classifier Block

To delete a classifier block:

- 1 From the main menu, choose Application > QoS > Rules > Classifier Block. The Classifier Block page opens (Figure 86).
- 2 Click the delete icon next to the classifier block you want to delete.



**Note:** You cannot delete a classifier or classifier block that is referenced by a policy. You must first delete the policy.



**Note:** Deleting the last classifier from a classifier block automatically deletes that classifier block.

## Configuring QoS Actions

When you create an action, you specify the actions to be associated with specific classifiers and classifier blocks. An action specifies the type of behavior you want a policy to apply to a flow of packets. When the filters match the incoming packets, the created actions are performed on those packets.



**Note:** There are default actions for each service class.

---

### Creating an Action Configuration

To create an action configuration:

- 1 From the main menu, choose Application > QoS > Actions.  
The Action page opens ([Figure 89](#)).

Figure 89 Action page

## Application &gt; QoS &gt; Action

Action Table									
Action	Action Name	Instance	Drop Frame	Update DSCP	Set Drop Precedence	Update 802.1p Priority	Extension	Storage Type	
 	Drop_Traffic	1	Yes	Ignore	High Drop	Ignore	<a href="#">None</a>	Read Only	
 	Standard_Service	2	Deferred Pass	0x0	High Drop	Priority 0	<a href="#">None</a>	Read Only	
 	Bronze_Service	3	Deferred Pass	0xA	Low Drop	Priority 2	<a href="#">None</a>	Read Only	
 	Silver_Service	4	Deferred Pass	0x12	Low Drop	Priority 3	<a href="#">None</a>	Read Only	
 	Gold_Service	5	Deferred Pass	0x1A	Low Drop	Priority 4	<a href="#">None</a>	Read Only	
 	Platinum_Service	6	Deferred Pass	0x22	Low Drop	Priority 5	<a href="#">None</a>	Read Only	
 	Premium_Service	7	Deferred Pass	0x2E	Low Drop	Priority 6	<a href="#">None</a>	Read Only	
 	Network_Service	8	Deferred Pass	0x30	Low Drop	Priority 7	<a href="#">None</a>	Read Only	
 	Null_Action	9	Deferred Pass	Ignore	Low Drop	Ignore	<a href="#">None</a>	Read Only	
 	UntrustedClfrs1	64001	Deferred Pass	Derive from Ingress Priority	Low Drop	Ignore	<a href="#">None</a>	Other	
 	UntrustedClfrs2	64002	Deferred Pass	0x0	High Drop	Priority 0	<a href="#">None</a>	Other	

Table 84 describes the items on the Action page.

Table 84 Action page items

Item	Range	Description
 		Modifies or deletes the row.
Action Name	1 to 16 alphanumeric characters	Type a character string to uniquely identify the action configuration.

**Table 84** Action page items (continued)

Item	Range	Description
Instance		Displays the unique identifier.
Drop Frame	Deferred Pass No Yes	<p>Choose whether the frame being evaluated should be dropped or transmitted by this attribute:</p> <p>Deferred Pass—traffic flow decision deferred to other installed policies</p> <p>No—do not drop the traffic flow</p> <p>Yes—drop the traffic flow</p> <p>The default setting is Deferred Pass.</p>
Update DSCP	Ignore or integer	<p>Choose a value. When this field is defined, it causes the value contained in the Differentiated Services (DS) field of an associated IP datagram to be updated with the value of this object.</p> <p>The default setting is Ignore.</p>
Set Drop Precedence	Low Drop High Drop	<p>Choose a packet drop precedence value.</p> <p>Note: Generally, low packet drop precedence receives preferential treatment</p> <p>The default setting is Low Drop.</p>
Update 802.1p Priority	Ignore Priority 0 Priority 1 Priority 2 Priority 3 Priority 4 Priority 5 Priority 6 Priority 7 Use TOS Precedence Use Egress DSCP	<p>Choose the action attribute that causes the value contained in the 802.1p priority field to be updated based on the value of this object. The update priority range values are 0 (lowest priority) to 7 (highest priority).</p> <p>The default setting is Ignore.</p>

**Table 84** Action page items (continued)

Item	Range	Description
Extension	None Available extensions from the Interface Action Extension Page	Choose either No Extension or one of the extensions you created on the Interface Action Extension page.  The default setting is None.
Storage Type	other read-only volatile non-volatile	This display-only field in the table shows the type of storage across reboots for each action: other—system created; cannot be deleted or referenced by the user read-only—system defaults; cannot be deleted volatile—lost after a reset nonvolatile—stored across reset

- 2 In the Action Creation section, type information in the text boxes, or select from a list
- 3 Click Submit.

The new action configuration appears in the Action Table ([Figure 89](#)).

## Modifying an Action Configuration

To modify an action configuration:

- 1 From the main menu, choose Application > QoS > Actions.  
The Action page opens ([Figure 89](#)).
- 2 In the Action Table section, in the action configuration row of your choice, click the modify icon.  
The Action Modification page appears ([Figure 90](#)).

**Figure 90** Action Modification page**Application > QoS > Action Modification**

Action Modification	
Action Name	<input type="text" value="baseAct10"/>
Drop Frame 	<input type="text" value="Deferred Pass"/>
Update DSCP	<input type="text" value="Ignore"/>
Set Drop Precedence 	<input type="text" value="Low Drop"/>
Update 802.1p Priority	<input type="text" value="Ignore"/>
Extension	<input type="text" value="No Extension"/>

3 Refer to [Table 84](#) for information on completing fields.

4 Click Submit.

The system returns you to the Action page ([Figure 89](#)) and displays the modified action.

## Deleting an Action Configuration

To delete an action configuration:

1 From the main menu, choose Application > QoS > Actions.

The Action page opens ([Figure 89](#)).

2 In the Action Table section, in the action configuration row of your choice, click the Delete icon.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the action configuration.

- Click Cancel to return to the Action page without making changes.



**Note:** You cannot delete an action that is referenced by a meter, classifier block, or policy. You must first delete the meter, classifier block, or policy.

You cannot delete a system default or system created action; the delete icon is grayed out for those actions.

---

## Using the Interface Action Extension

You create extensions to actions by using the Interface Action Extension page. These extensions allow you to filter on:

- Set an egress unicast
- Set an egress non-unicast

## Creating an Interface Action Extension Configuration

To create an interface action extension configuration:

- 1 From the main menu, choose Application > QoS >Interface Action Ext. The Interface Action Extension page opens ([Figure 91](#)).

**Figure 91** Interface Action Extension page

**Application > QoS > Interface Action Extension**

Interface Action Extension Table					
Action	Interface Action Name	Instance	Set Egress Unicast	Set Egress Non-Unicast	Storage Type
<p><b>Interface Action Extension Creation</b></p> <p>Action Name <input type="text"/></p> <p>Set Egress Unicast <input type="radio"/> Ignore <input type="radio"/> Port <input type="text"/></p> <p>Set Egress Non-Unicast <input type="radio"/> Ignore <input type="radio"/> Port <input type="text"/></p> <p><input type="button" value="Submit"/></p>					



**Note:** An interface action extension can be referenced *only* by an action.

Table 85 describes the items on the Interface Action Extension page.

**Table 85** Interface Action Extension page items

Item	Range	Description
		Deletes the row.
Interface Action Name	1 to 16 alphanumeric characters	Type a character string to uniquely identify the interface action extension configuration.
Instance		Displays the unique identifier.
Set Egress Unicast	Ignore or port	Choose either: Ignore—the system does not set an egress unicast port Choose the port you want for the egress unicasts.  The default setting is Ignore.

**Table 85** Interface Action Extension page items (continued)

Item	Range	Description
Set Egress Non-Unicast	Ignore or port	Choose either: Ignore—the system does not set an egress non-unicast port Choose the port you want for the egress non-unicasts.  The default setting is Ignore.
Storage Type	other read-only volatile non-volatile	This display-only field in the table shows the type of storage across reboots for each action: other—system created; cannot be deleted or referenced by the user read-only—system defaults; cannot be deleted volatile—lost after a reset nonvolatile—stored across reset

- 2 In the Interface Action Extension Creation section, type information in the text boxes, or select from a list
- 3 Click Submit.

The new interface action extension configuration appears in the Interface Action Extension Table ([Figure 91](#)).



You cannot modify an interface action extension entry. You must delete that entry and create another one with the configuration you want.

## Deleting an Interface Action Extension Configuration

To delete an interface action extension configuration:

- 1 From the main menu, choose Application > QoS > Interface Actions Ext.  
The Interface Action Extension page opens ([Figure 91](#)).
- 2 In the Interface Action Extension Table section, in the interface action extension configuration row of your choice, click the Delete icon.  
A message opens prompting you to confirm your request.

**3** Do one of the following:

- Click Yes to delete the interface action extension configuration.
- Click Cancel to return to the Interface Action Extension page without making changes.



**Note:** You cannot delete an interface action extension that is referenced by an action. You must first delete the action.

---

## Configuring QoS Meters

Using the QoS pages, you can create, view, or delete meters. If you do not want to meter the data in your flow, go to [“Configuring QoS Policies” on page 235](#).

### Creating a Meter

To create a meter:

- 1** From the main menu, choose Application > QoS > Meters.

The Meter page opens ([Figure 92](#)). This table displays all meters you created.

Figure 92 Meter page

Application > QoS > Meter

Meter Table							
Action	Name	Instance	Committed Rate (Kbps)	Committed Burst Size (Bytes)	In-Profile Action	Out-of-Profile Action	Storage Type

Meter Creation	
Name	<input type="text"/>
Committed Rate <sup>?</sup>	<input type="text"/> Kbps (Multiple of 1000 Kbps; 1 Kbps = 1000 bits per second)
Committed Burst Size	Maximum Burst Rate <sup>?</sup> <input type="text"/> Kbps (1 Kbps = 1000 bits per second)
	Duration <sup>?</sup> <input type="text"/>
In-Profile Action <sup>?</sup>	<input type="text" value="Drop_Traffic"/>
Out-Of-Profile Action <sup>?</sup>	<input type="text" value="Drop_Traffic"/>

Table 86 describes the fields in the Meter Creation area, which you use to set new meters.

Table 86 Meter Creation fields

Item	Range	Description
Name	1 to 16 alphanumeric characters with no spaces	Enter the name for the meter you are creating.
Committed Rate	1000 - 1023000 Kbps	Enter the Committed Rate in Kbps here. Note: You must enter the committed rate in multiples of 1000 Kbps.
Committed Burst Size	4, 8, 16, 32, 64, 128, 256, 512 Kbytes Up to 8 durations	Maximum Burst Rate—Enter the Maximum Burst Rate in Kbps. Duration—From the pull-down menu, choose 1 of up to 8 durations for the period that the Maximum Burst Rate is allowed.

**Table 86** Meter Creation fields (continued)

Item	Range	Description
In-Profile Action	Default actions plus all you created.	Choose from the pull-down menu of: Default actions All actions you created using the Action page  The default setting is Drop Traffic.
Out-Of-Profile Action	Default actions plus all you created.	Choose from the pull-down menu of: Default actions All actions you created using the Action page  The default setting is Drop Traffic.

- 2 In the Meter Creation area, create the meter.
- 3 Click Submit.



**Note:** Meter configurations are not modifiable. They must be deleted and the information re-entered.

## Viewing Meters

To view a meter:

- 1 From the main menu, choose Application > QoS > Meters.  
The Meters page opens (Figure 92).
- 2 View created meters in the Meter Table.

Table 87 describes the fields in the Meter Table area.

**Table 87** Meter Table fields

Item	Range	Description
Action		Deletes the meter.
Name		Displays the name of the meter.

**Table 87** Meter Table fields (continued)

Item	Range	Description
Instance		Displays the unique identifier.
Committed Rate	1000 - 1023000 Kbps	Displays the Committed Rate in kbps.
Committed Burst Size	4, 8, 16, 32, 64, 128, 256, 512 Kbytes Up to 8 durations	Displays the Committed Burst Size in bytes.
In-Profile Action	Configured, user-defined action	Displays the In-Profile Action for this meter.
Out-Of-Profile Action	Configured, user-defined action	Displays the Out-Of-Profile Action for this meter.
Storage Type	volatile non-volatile	This display-only field in the table shows the type of storage across reboots for each action: volatile—lost after a reset nonvolatile—stored across reset

## Deleting a Meter

To delete a meter:

- 1 From the main menu, choose Application > QoS > Meters.  
The Meter page opens (Figure 92).
- 2 In the Meter Table section, click the Delete icon to delete the meter.  
A message opens prompting you to confirm your request.
- 3 Do one of the following:
  - Click Yes to delete the meter configuration.
  - Click Cancel to return to the Meter page without making changes.

## Configuring QoS Policies

You can configure QoS policies by creating filters in the hardware that apply a set of packet filtering criteria and actions to individual interfaces.

If you want to meter your data, the In-Profile action and the Out-Profile action are referenced from the meter entry. The In-Profile action directs the switch how to handle the data flow that is within the meter you set, and the Out-Profile directs the switch how to handle all other data.

## Installing Defined Filters

To create a hardware policy filter configuration:

- 1 From the main menu, choose Application > QoS > Policy.

The Policy page opens (Figure 93).

**Figure 93** Policy page

**Application > QoS > Policy**

**Policy Table**

Action	State	Policy Name	Instance	Classifier Type	Classifier Name	Role Combination	Policy Precedence	Meter	In-Profile Action	Non-Match Action	Track Statistics	Storage Type
	Enabled	UntrustedCifrs1	64001	Classifier Block	UntrustedCifrs1	allBayStacklcs	2	-	UntrustedCifrs1a1	-	Aggregate	Other
	Enabled	UntrustedCifrs2	64002	Classifier Block	UntrustedCifrs2	allBayStacklcs	1	-	UntrustedCifrs2a2	-	Aggregate	Other

**Policy Creation**

Policy Name	<input type="text"/>
Classifier Type	Classifier
Classifier Name	None Defined
Role Combination	allBayStacklcs
Policy Precedence	11
Meter	None
In-Profile Action	None
Non-Match Action	None
Track Statistics	No

Table 88 describes the items on the Policy page.

**Table 88** Policy page items

Section	Item	Range	Description
Policy Table	Action		Opens a view only statistics table. The table displays current filter statistics in packets.
			Deletes the row.
	State	(1) Enabled (2) Disabled	Enables or disables the policy. The default setting is Enabled.
	Policy Name	1 to 16 alphanumeric characters	A list of the names of existing target configurations.
	Instance		Displays the unique identifier.
	Classifier Type	classifier classifier block	The type of classifier that is referenced by this instance of the policy. The options are: Classifier and Classifier Block.
	Classifier Name		The classifier or classifier block that is associated with this policy.
	Role Combination		The interfaces to which this policy specification applies, specified in terms of a role combination tag.
	Policy Precedence	1 to 11	The number used to determine the order of precedence for this policy specification.
	Meter		The meter associated with this entry, if there is one.
	In-Profile Action		Displays the name of the In-Profile action for this policy. Note: Metered policies have In-Profile Actions specified in the Meter entry.
	Non-Match Action		Displays the non-match action for this policy.
	Track Statistics	No Individual Classifier Aggregate Classifier	Displays whether the system is tracking statistics for this policy and the granularity of the statistics tracking.
	Storage Type	other read-only volatile non-volatile	This display-only field in the table shows the type of storage across reboots for each action: other—system created; cannot be deleted read-only—system defaults; cannot be deleted volatile—lost after a reset nonvolatile—stored across reset

**Table 88** Policy page items (continued)

Section	Item	Range	Description
Policy Creation	Policy Name	1 to 16 alphanumeric characters	Type a character string to create a unique name to identify this policy.
	Classifier Type	Classifier Classifier Block	Choose the type of filter to associate with this policy.
	Classifier Name		Choose the name of the classifier or classifier block to associate with this policy.
	Role Combination		Choose the type of interface to which this policy applies, specified in terms of a role combination, from a list of all Role Combinations created so far.
	Policy Precedence	1 to 11	Enter a number from 1 to 11 to use as a determinate of the order of precedence for this filter. Note: The highest value for precedence is evaluated first.
	Meter		Choose either: None—no meter is associated with this policy one of the meters you configured
	In-Profile Action		Choose the action you want to take for the data associated with this policy.  Note: If this policy is metered, you will not choose an In-Profile Action here; the policy is referenced from the Meter entry.
	Non-Match Action		Choose the action you want to take associated with this policy for data that is not within the configured profile.
	Track Statistics	No Individual Classifier Aggregate Classifier	Choose whether to track statistics for this policy and the granularity of the statistics you want.  The default setting is No.

- 2 Complete the fields as described.
- 3 Click Submit.

## Viewing Hardware Policy Statistics

To view statistics for a selected hardware policy configuration:

- 1 From the main menu, choose Application > QoS Policy.  
The Policy page opens (Figure 93).
- 2 In the Policy Table section under the Action column, in the policy of your choice, click the View icon.  
The Policy Statistics page opens (Figure 94).

**Figure 94** Policy Statistics page

**Application > QoS > Policy > Policy Statistics**

<b>Policy Name</b>	UntrustedClfrs1
<b>Instance</b>	64001
<b>Classifier Type</b>	Classifier Block
<b>Classifier Name</b>	UntrustedClfrs1
<b>Role Combination</b>	allBayStackIfcs
<b>Policy Precedence</b>	2
<b>Meter</b>	
<b>In-Profile Action</b>	UntrustedClfrs1
<b>Non-Match Action</b>	
<b>Track Statistics</b>	Aggregate
<b>Storage Type</b>	Other
<b>State</b>	Enabled
<b>Total In-Profile Packets</b>	58945
<b>Total Out-Profile Packets</b>	0

[Update](#) [Back](#)

Table 89 describes the items on the Policy Statistics page.

**Table 89** Policy Statistics page items

Item	Description
Policy Name	The name of the selected policy.
Instance	The number the system applies to the policy.
Classifier Type	The type of classifier that is referenced by this instance of the filter policy class. The options are: classifier or classifier block.
Classifier Name	The name of the classifier or classifier block you are associating with the policy.
Role Combination	The interfaces to which this policy applies, specified in terms of a role combination.
Policy Precedence	The precedence of this policy.
Meter	The meter associated with this policy.

**Table 89** Policy Statistics page items (continued)

Item	Description
In-Profile Action	The in-profile action associated with the policy.
Non-Match Action	The non-match action associated with this policy.
Track Statistics	The granularity of statistics tracking for this policy.
Storage Type	The type of storage across reboots for this policy.
State	The enabled or disabled state of the policy.
Total In-Profile Packets	The total number of in-profile packets for this policy.  Note: These are the total number since the policy was installed/enabled. Once you disable the policy, the counters reset to zero.
Total Out-Of-Profile Packets	The total number of out-of-profile packets for this policy.  Note: These are the total number since the policy was installed/enabled. Once you disable the policy, the counters reset to zero.

[Table 90](#) describes the items on the Filter Statistics table, which provides a breakdown of In-Profile and Out-Of-Profile packets for each classifier and each port within each policy.

**Table 90** Filter Statistics table items

Item	Description
Classifier Name	The name of the classifier you are associating with the policy.
Port	The number of the port.
In-Profile Packets	The number of in-profile packets for this filter and this port.
Out-Of-Profile Packets	The number of out-of-profile packets for this filter and this port.



**Note:** This table appears only if you configure the system to track statistics at the level of an individual classifier.

## Deleting a Hardware Policy Configuration

To delete a hardware policy configuration:

- 1 From the main menu, choose Application > QoS > Policy.

The Policy page opens (Figure 93).

- 2 In the Policy Table section, in the hardware policy configuration row of your choice, click the Delete icon.

A message opens prompting you to confirm your request.

- 3 Do one of the following:
  - Click Yes to delete the hardware policy configuration.
  - Click Cancel to return to the Policy page without making changes.

## Configuring QoS Policy Agent Characteristics

You can Configure QPA Policy Agent (QPA) operational parameters.

To open the Agent page:

- 1 From the main menu, choose Application > QoS > Agent > Configuration.

The Agent page opens (Figure 95 and Figure 96).

**Figure 95** Agent page (1 of 2)

**Application > QoS > Agent**

QoS Configuration	
QoS Policy Agent Reset To Defaults	No ▾
NVRam Commit Delay	10 seconds (0..604800)
Queue Set	8 ▾
Buffering	Regular ▾
QoS WEB Display Mode	All ▾

**Figure 96** Agent page (2 of 2)

<b>Policy Class Support Table</b>		
<b>Policy Class Name</b>	<b>Current Instances</b>	<b>Maximum Installed Instances</b>
ntrQoSPrsSupportSupportedPrs	21	0
ntrQoSPolicyDeviceIdentDescr	1	0
ntrQoSInterfaceTypeTable	1	100
ntrQoSIfQueueSetId	36	0
ntrQoSIfAssignmentRoleCombination	24	512
ntrQoSDiscpToCosDiscp	64	64
ntrQoSCosToDiscpCos	8	8
ntrQoSQsetPriAssignmentQset	64	8
ntrDsMultiFieldClfrAddrType	0	200
ntrL2MultiFieldClfrDstAddr	2	200
ntrSystemClfrUnknownUcastFrames	0	100
ntrClfrComponentSpecific	2	400
ntrClfrBlockNumber	2	200
ntrQoSIfcActionUpdateVlanId	0	64
ntrQoSBaseActionDrop	12	128
ntrQoSTBParamType	0	512
ntrQoSMeterSucceedNext	0	100
ntrQoSCountActOctets	2	300
ntrQoSFilterStatsInProfileOctets	48	0
ntrQoSPolicyClassifierType	2	200
ntrQoSIfShapingSpecific	0	512

<b>Policy Device Identification Table</b>	
<b>Description</b>	Nortel Networks QoS Policy Agent (QPAv2) v3.0.0
<b>Maximum Message Size</b>	2048 bytes

Table 91 describes the items on the Agent page.

**Table 91** Agent page items

<b>Section</b>	<b>Item</b>	<b>Range</b>	<b>Description</b>
QoS Configuration	QoS Policy Agent Reset to Defaults	No Yes	Choose whether or not to reset the policy agent to the default settings.
	NVRAM Commit Delay	0 to 604800	Type the time, in seconds, before the configuration is saved to NVRAM.
	Queue Set	4 to ;	Choose the default QoS CoS queue set.
	Buffering	Regular, Large, Maximum	Choose the QoS resource buffer allocation scheme.
	QoS WEB Display Mode	User System All	Choose to display either only user-created parameters, only system-created parameters, or all parameters for QoS.
Policy Class Support Table	Policy Class Names		The name of the policy.

**Table 91** Agent page items (continued)

Section	Item	Range	Description
	Current Instances		The current class entries.
	Maximum Installed Instances		The maximum number of allowed class entries.
Policy Device Identification Table	Description		The system description.
	Maximum Message Size		The maximum target message size supported by the device.

- 2 In the QoS Configuration section, type information in the text boxes, or select from a list.
- 3 Click Submit.

## Using QoS Diagnostics

You use the Diagnostics page:

- to view how many filters, masks, meters, and counters are used.
- to validate configuration ranges.
- to examine the raw bit form of the classifiers you are putting into a classifier block in order to compare the masks.



**Note:** You must have *already* configured the classifiers to display the rules and masks; you can display the value and mask for a range *before* you configure that range.

To open the Diagnostics page:

- 1 From the main menu, choose Application > QoS > Agent > Diagnostics.

**Figure 97** Diagnostics page (1 of 3)**Application > QoS > Agent > Diagnostics**

QoS Resource Allocation Table							
Interface	QoS Masks Consumed	QoS Filters Consumed	QoS Meters Consumed	QoS Counters Consumed	Non-QoS Masks Consumed	Non-QoS Filters Consumed	Non-QoS Meters Consumed
1	2	2	0	2	6	15	0
2	2	2	0	2	6	15	0
3	2	2	0	2	6	15	0
4	2	2	0	2	6	15	0
5	2	2	0	2	6	15	0
6	2	2	0	2	6	15	0
7	2	2	0	2	6	15	0
8	2	2	0	2	6	15	0
9	2	2	0	2	6	15	0
10	2	2	0	2	6	15	0
11	2	2	0	2	6	15	0
12	2	2	0	2	6	15	0
13	2	2	0	2	6	15	0
14	2	2	0	2	6	15	0
15	2	2	0	2	6	15	0
16	2	2	0	2	6	15	0
17	2	2	0	2	6	15	0
18	2	2	0	2	6	15	0
19	2	2	0	2	6	15	0
20	2	2	0	2	6	15	0
21	2	2	0	2	6	15	0
22	2	2	0	2	6	15	0
23	2	2	0	2	6	15	0
24	2	2	0	2	6	15	0

**Figure 98** Diagnostics page (2 of 3)

<b>QoS Valid Range</b>	
Minimum Value	<input type="text" value="0"/>
Maximum Value	<input type="text" value="65535"/>
Rule Value	0x0000
Mask Value	0x0000

**Submit**

<b>QoS Encapsulating Range</b>	
Low Value	<input type="text" value="0"/>
High Value	<input type="text" value="0"/>
Minimum Value	0
Maximum Value	0

**Submit**

**Figure 99** Diagnostics page (3 of 3)

QoS Classifier Rule/Mask Comparison				
Classifier	None Defined ▾		None Defined ▾	
	Rule	Mask	Rule	Mask
Dst MAC Address				
Src MAC Address				
User Priority				
VLAN				
EtherType				
IP Version				
IP Header Length				
DSCP				
IPv4 Protocol				
IPv6 Flow ID				
IPv6 Next Header				
Src IP Address				
Dst IP Address				
Src L4 Port				
Dst L4 Port				
VLAN Tag				
Header				

[Table 92](#) describes the items on the Diagnostics page.

**Table 92** Diagnostics page items

Section	Item	Description
QoS Resource Allocation Table	Interface	Displays the port or interface number.
	QoS Masks Consumed	Displays total number of masks consumed from QoS application.
	QoS Filters Consumed	Displays total number of filters consumed from QoS application.
	QoS Meters Consumed	Displays total number of meters consumed from QoS application.
	QoS Counters Consumed	Displays total number of counters consumed from QoS application.
	Non-QoS Masks Consumed	Displays total number of masks consumed by non-QoS applications.
	Non-QoS Filters Consumed	Displays total number of filters consumed by non-QoS applications.

**Table 92** Diagnostics page items (continued)

Section	Item	Description
	Non-QoS Meters Consumed	Displays total number of meters consumed by non-QoS applications.
QoS Valid Range	Range	Enter beginning variable for any QoS range (such as VLANs, L4 Source Port, L4 Destination Port) and choose the end variable from among the system-provided values on the pull-down menu.
	Value	Displays the corresponding rule value in the IRULE entry in hardware.
	Mask	Displays the corresponding mask value in the IMASK entry in hardware.
QoS Classifier Rules/Mask Comparison	Classifier	Select the classifier(s) that you want to display the rule and mask for.
	Dst MAC Address	Displays the rule and mask for the destination MAC addresses configured.
	Src MAC Address	Displays the rule and mask for the source MAC addresses configured.
	User Priority	Displays the rule and mask for the user priority configured.
	VLAN	Displays the rule and mask for the VLANs configured.
	EtherType	Displays the rule and mask for the Ether types configured.
	IP Version	Displays the rule and mask for the IP versions configured.
	IP Header Length	Displays the rule and mask for the IP header lengths configured.
	DSCP	Displays the rule and mask for the DSCPs configured.
	IPv4 Protocol	Displays the rule and mask for the IPv4 protocols configured.
	IPv6 Flow ID	Displays the rule and mask for the IPv6 flow IDs configured.
	IPv6 Next Header	Displays the rule and mask for the IPv6 next headers configured.
	Src IP Address	Displays the rule and mask for the source IP addresses configured.
	Dst IP Address	Displays the rule and mask for the destination IP addresses configured.
	Src L4 Port	Displays the rule and mask for the source L4 ports configured.
Dst L4 Port	Displays the rule and mask for the destination L4 ports configured.	

**Table 92** Diagnostics page items (continued)

Section	Item	Description
	VLAN Tag	Displays the VLAN tag configured.
	Header	Displays the rule and mask for the first 80 bytes of the header configured.

- 2 To display a valid range:
  - a Enter the beginning number of the range you want in the box.
  - b From the pull-down menu, choose the end of the range from the system-provided choices.
  - c Click Submit.
  - d The system returns the value and mask for that range ([Figure 100](#)).

**Figure 100** Diagnostics value and mask display for selected range

QoS Valid Range	
Minimum Value	<input type="text" value="0"/>
Maximum Value	<input type="text" value="65535"/>
Rule Value	0x0000
Mask Value	0x0000

**Submit**

- 3 To display the rule and mask in order to compare them for selected classifier(s):
  - a Choose the classifier(s) you want to display from the pull-down menu.
  - b Click Submit.

The system returns the rule and mask for the classifier(s) for those parameters configured ([Figure 101](#)).

**Figure 101** Diagnostics rule and mask display for selected classifier

QoS Classifier Rule/Mask Comparison				
Classifier	None Defined	None Defined		
	Rule	Mask	Rule	Mask
Dst MAC Address				
Src MAC Address				
User Priority				
VLAN				
EtherType				
IP Version				
IP Header Length				
DSCP				
IPv4 Protocol				
IPv6 Flow ID				
IPv6 Next Header				
Src IP Address				
Dst IP Address				
Src L4 Port				
Dst L4 Port				
VLAN Tag				
Header				

Submit



**Note:** To combine classifiers into the same classifier block, the classifiers must use the same mask.



---

## Chapter 9

# Support Menu

---

The customer support options available to you are:

- Help
- Release Notes
- Manuals
- Upgrade

## Using the Online Help Option

You can read information about management page functions in the online help menu embedded in the Web-based management interface.

To open online help:

- 1 From the main menu, choose Support > Help or click the Help icon located in the upper right corner of any management page.



The Online Help menu opens in a separate Web browser ([Figure 102](#)).

**Figure 102** Online help window

- 2** Click on any content item to read information about the topic (if you clicked the Help icon on a management page, information about that page is immediately displayed).
- 3** Click Return to Top to return to the Content index.
- 4** Close the Web browser

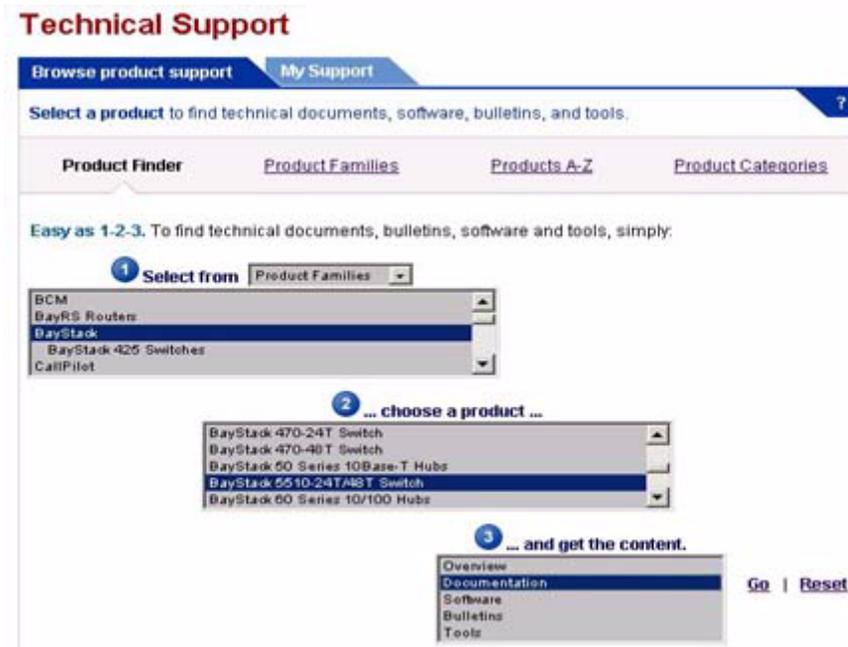
## Downloading Technical Publications

You can download current documentation about the Web-based management user interface from Nortel Technical Documentation Web site.

To download current documentation:

- 1 From the main menu, choose Support > Release Notes.  
Nortel Technical Documentation Web site opens in a separate Web browser (Figure 103).

**Figure 103** Nortel Technical Documentation Web site



- 2 Select the Product Family from the list box labeled 'Select from'.
- 3 In the 'Choose a Product' list box, select the specific product. (For example, Figure 103 displays the BayStack Family Product)
- 4 In the list box labeled "...and get the content.", select documentation.
- 5 Click Go. The page displaying the documentation for the product selected earlier is displayed.

**Figure 104** Nortel technical Documentation Web site

Sorted by: Date

Results: 1-20 of 20

Page: 1 of 1

Title	Format	Type	File	Number	Date
<a href="#">Release Notes for the BayStack 5510 10/100/1000 Switch Release 4.0.2</a>	pdf	Release Notes		--	22 Sep 2004
<a href="#">Sales Engineering Tips and Tricks, August 2004</a>	pdf	Technical Tips		volume_13	09 Aug 2004
<a href="#">Release Notes for the BayStack 5510 10/100/1000 Switch Release 4.0.1</a>	pdf	Release Notes		--	02 Aug 2004
<a href="#">BS5510 Technical Configuration Guide for CoS</a>	pdf	Configuration Guides	4.0	--	26 Jul 2004
<a href="#">BayStack 5510 Technical Configuration Guide for QoS and Filters</a>	pdf	Configuration Guides	4.0	--	17 Jun 2004
<a href="#">Addendum to Release Notes for BayStack 5510 10/100/1000 Switch Software Release 4.0</a>	pdf	Release Notes	4.0	216863A	24 May 2004
<a href="#">Release Notes for the BayStack 5510 10/100/1000 Switch Release 4.0.0.0</a>	pdf	Release Notes	Release 4.0.0.0	215082c	11 May 2004

- 6 To download the required document, do one of the following:
  - Click on the link representing the title of the document.
  - Click on the PDF hyperlink to start the download process (you need Adobe Acrobat 3.0 or later to view or print documents from this site).
- 7 Follow the prompts to download the documentation.
- 8 Close the Web browser.

## Manuals Option

This option allows you to search and download the latest technical documents. The Nortel Technical Support site is displayed when you click on this option. For more information on searching for technical documents on the Technical Support site, see [“Downloading Technical Publications” on page 252](#).

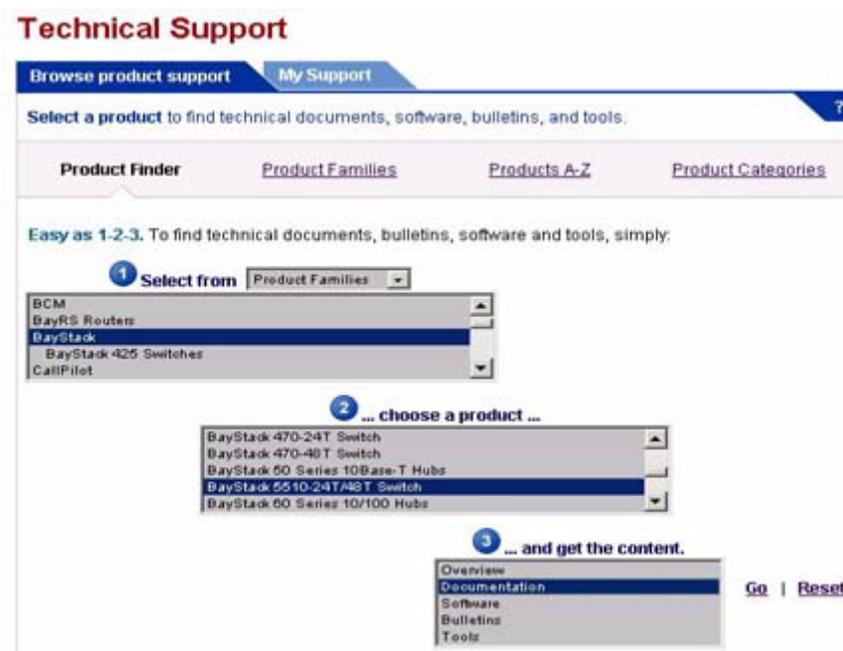
## Upgrade Option

You can upgrade your Web-based management user interface to the most recent software release.

To upgrade to the most recent software release:

- 1 From the main menu, choose Support > Upgrade.  
Nortel Customer Support opens in a separate Web browser (Figure 105).

**Figure 105** Nortel Customer Support Web site



- 2 Select the Product Family from the list box labeled ‘Select from’.
- 3 In the ‘Chose a Product’ list box, select the specific product.
- 4 In the list box labeled “...and get the content.’, select Software.
- 5 Click Go. The page displaying the software releases for the product selected earlier is displayed.
- 6 Follow the prompts to download the software.



---

# Index

---

## Numbers

802.1p Priority field 198, 200, 201, 202, 212, 214

802.1p Priority Mapping page 199

802.1p Priority Queue Assignment page 197

## A

Absolute Bandwidth field 192

access 56

console 113

number 42

RADIUS security 40

SNMP 56, 89

Telnet 56

user levels 42

Web 28

Action Creation 224

Action Name field 225

Action Table 224

Actions page 224

Active Phy field 108

Address field 207

Address Type field 206, 207

administrative options 35

logging on 40

logging out 45

resetting the switch 42

resetting to system defaults 44

security, configuring

passwords 37

remote dial-in access 39

system information, viewing 35

Administrative Status field 87

Administrative Traffic Control field 87

Agent page 241

Aging Time field 102

alarms 117, 121

Alias field 106

Allowed Source field 97

Allowed Source IP field 58

Allowed Source Mask field 58

application setting options

broadcast domains 167

IGMP 150

MultiLink Trunking 184

port mirroring 143

QoS 199

802.1p priority queue assignment 197

actions 224

DSCP mapping 200

interface groups 190

IP classifier elements 203

layer 2 classifier elements 209

meters 232

network access 204

policies (hardware filters) 235

Policy Agent (QPA) 241

role combination 190

rate limiting 147

VLANs 155

asymmetric flow control 108

Authentication Password field 65

Authentication Protocol field 65

Authentication Protocols Supported field 63

Authentication Trap field 60

authentication traps, enabling 59

autonegotiation 104  
    gigabit ports 107  
Autonegotiation field 106, 108  
autopolarity 106  
autoPVID 155, 167, 168  
AutoPVID field 157  
Autotopology 58  
AutoTopology field 60

## B

Bandwidth Allocation field 192  
Bandwidth field 192  
bandwidth utilization 188, 192  
Block Name field 221  
Block Number field 221  
BootP  
    configuring 52  
    request modes 53  
BootP Always field 53  
BootP Disabled field 53  
BootP or Last Address field 53  
BootP Request Mode field 53  
BootP When Needed field 53  
Bridge Hello Time field 183  
Bridge Information page 181  
Bridge Priority field 173, 182  
bridge settings 181  
broadcast domains, configuring 167  
Broadcast field 126, 129, 133  
broadcast traffic 147

## C

Capabilities field 196  
Carrier Sense Errors field 140  
check boxes, about 32  
Classifier Block page 220, 221, 222, 223

Classifier Block Table 221  
Classifier Name field 217, 237, 238, 239, 240  
Classifier page 216, 217, 218, 219  
Classifier Set ID field 217  
Classifier Table 216  
Classifier Type field 237, 238, 239  
Clear by Ports page 99  
Clear Message From field 123  
Collisions field 126, 133, 135  
Comm Port Data Bits field 114  
Comm Port Parity field 114  
Comm Port Stop Bits field 114  
Committed Burst Size field 233, 235  
Committed Rate field 233, 235  
Community field 84  
community strings, configuring 59  
configuration file 111, 113  
Configuration File Download/Upload page 111  
Configuration Image Filename field 112  
Console page 32, 37  
Console Password Setting page 37  
Console Port Speed field 114  
Console Switch Password Type field 38  
Console/Communication Port page 114  
conventions, text 24  
conversation steering 143  
Copy Configuration Image to Server field 112  
CRC Align Errors field 126, 129  
Current Learning Mode field 90  
Current Running Version field 110  
customer support 25

## D

DA Filtering on Intrusion Detected field 90  
DA MAC Address field 100

DA MAC Filtering page 99  
Decryption Error field 63  
Default Gateway field 54  
default mapping 198, 199, 201  
default settings 44  
Deferred Packets field 134  
Deferred Transmissions field 140  
Designated Root field 182  
Destination Address field 206, 207  
destination address filtering 88  
Destination L4 Port field 206  
Destination Layer 4 Port field 208  
Destination MAC Addr field 211  
Destination MAC Addr Mask field 211  
Destination MAC Address field 213  
Destination Mask Length field 206  
Diagnostics Image Filename field 110  
Diagnostics page 243  
Display Message From field 123  
Drop 128  
Drop Events field 126, 128  
Drop Frame field 226  
Drop Precedence field 202, 203  
DSCP  
    802.1p priority mapping 200  
    mapping 199  
DSCP field 200, 201, 202, 206, 207, 247  
DSCP Mapping Modification page 200  
DSCP Mapping page 200  
DST IP Address field 247  
Dst L4 Port field 247  
Dst MAC Address field 247

## E

EAPOL Security Configuration page 85  
EAPOL-based security 85

Entry field 94, 97  
Entry Storage field 65, 68, 71, 74, 77, 79, 82, 192  
errors 135, 136, 138, 140  
Ethernet error statistics  
    viewing 138  
Ethernet Errors page 138  
EtherType field 212, 213, 247  
Excessive Collisions field 133, 136, 140  
Extension field 227

## F

fault threshold parameters, configuring 117  
FCS/Frame Errors field 133, 135, 139  
Filter Unregistered Frames 168  
Filter Untagged Frames field 168  
Filtered Packets field 133  
Find MAC Address page 103  
Firmware Version field 48  
Flow Control field 108  
Forward Delay field 183  
Forward Delay Time field 173  
Fragments field 126

## G

gateway addresses, configuring 52  
General Discipline field 191  
Generate SNMP Trap on Intrusion field 90  
gigabit Ethernet 107  
Group Access Rights page 69  
Group Creation page 171  
Group Membership page 66  
Group Name field 68, 71  
Group page 185

**H**

hardware description 48  
Hardware Version field 48  
Header field 248  
Hello Interval 173  
Hello Time field 173, 183  
High Speed Flow Control page 107  
high speed flow control, configuring 107

**I**

icons, about 32  
IGMP 150, 153  
IGMP Multicast Group Membership page 153  
IGMP page 150  
IGMP VLAN Configuration page 151  
IGMP, configuring 150  
In Discards field 138, 142  
In Errors field 138  
In Frames field 141  
In Non-Unicast field 138  
In Octets field 137  
In Unicast field 138  
In Unknown Protos field 138  
In-Band Subnet Mask field 54  
In-Band Switch IP Address field 54  
Initialize field 87  
In-Profile Action field 234, 235, 237, 238, 240  
In-Profile Packets field 240  
Interface Action Extension page 229  
Interface Action Name field 230  
interface class  
    trusted, untrusted, and unrestricted 192, 196, 203  
Interface Class field 192, 196  
Interface Configuration page 190

Interface Group Assignment page 195  
Interface Group Creation 190  
Interface Group Table 190  
Interface ID page 193  
Interface ID Table 193  
Interface page 136  
Interface Queue Table 190  
interface statistics  
    viewing 136, 137  
Internal MAC Receive Errors field 140  
Internal MAC Transmit Errors field 139  
Interval field 119  
In-Use field 54  
IP address 52  
    per unit 52  
IP Address field 49, 84  
IP Classifier Element Creation 204  
IP Classifier Element page 204  
IP Classifier Element Table 204  
IP gateway address 52  
IP Header Length field 247  
IP manager list 56  
IP page 52  
IP Version field 247  
IPv4 207  
IPv4 Protocol field 247  
IPv4 Protocol/IPv6 Next Header field 206, 207  
IPv6 207  
IPv6 Flow ID field 247  
IPv6 Flow Id field 206, 208  
IPv6 Next Header field 247

**J**

Jabbers field 127

**L**

Last 24 Hours field 149  
Last 5 Minutes field 149  
Last BootP field 54  
Last Hour field 149  
Late Collisions field 134, 136, 140  
Layer2 Classifier Element Creation 210  
Layer2 Classifier Element page 210  
Layer2 Classifier Element Table 210  
Learn by Ports page 95  
Learning Constraint field 157, 159, 165  
LEDs 42  
Limit field 149  
Link field 106, 135  
Link/Trap field 106  
Local Store Version field 110  
logging on 40  
logging out 45

**M**

MAC address 48  
MAC Address field 97, 100, 102  
Mac Address field 48  
MAC address security 89  
    allowed source 96  
    clearing 99  
    deleting ports 93  
    learn by ports 95  
    learning 90  
    MAC DA 88, 99  
    ports 91  
    security list 93  
    security table 96  
MAC Address Security field 90  
MAC Address Security SNMP-Locked field 90  
MAC Address Table page 101  
MAC address-based port mirroring 143, 147  
MAC addresses  
    locating a specific address 102, 103  
    viewing learned addresses 101  
MAC DA filtering 88, 99  
main menu  
    headings and options 30  
    icons 31, 33  
Management Information View page 72  
Management VLAN field 157  
Manufacturing Date Code field 48  
Mask Length field 207  
Max. Age Time field 173  
Maximum Age Time field 183  
Maximum Installed Instances field 243  
Maximum Message Size field 243  
Maximum Requests field 87  
MDAs 107  
Message field 124  
Message Type field 124  
Meter Creation 232  
Meter field 237, 238, 239  
Meter page 232  
Meter Table 232  
Meters page 234  
Microsoft Internet Explorer, software version requirements 27  
Module Description field 48  
Monitor Port field 145  
Monitoring 145  
Monitoring Mode field 145  
monitoring modes 147  
Msg Processing Model field 81  
multicast 150, 153  
Multicast field 126, 129, 133  
Multicast Group Address field 154  
multicast traffic 147

MultiLink Trunking 180  
  about 184  
  configuring 184  
  monitoring traffic 187  
Multiple Collision Frames field 140  
Multiple Collisions field 133, 135  
multiple spanning tree groups 170

## N

Name field 200  
naming ports 106  
Netscape Navigator, software version  
  requirements 27  
network access, configuring IP classifier  
  elements 203  
network administrator  
  contact information 55, 56  
network monitoring 117  
network security, protecting system integrity 28  
Non-Match Action field 237, 238, 240  
Non-QoS Filters Consumed field 246  
Non-QoS Masks Consumed field 246  
Non-QoS Meters Consumed field 247  
Not in Time Window field 63  
Notification page 75  
Notify Name field 76  
Notify Tag field 76  
Notify Type field 77  
Notify View field 71  
NVRAM Commit Delay field 242

## O

Octets field 126, 129  
online help, accessing 251  
Operational State field 48  
Operational Status field 87

Operational Traffic Control field 87  
Out Discards field 138  
Out Errors field 138  
Out Frames field 142  
Out Non-Unicast field 138  
Out Octets field 138  
Out Unicast field 138  
Out-Of-Profile Action field 234, 235  
Out-Of-Profile Packets field 240  
Oversize field 129  
Oversized Packets field 133

## P

Packet Type field 148  
Packets field 126, 129, 133  
Packets length field 127, 134  
Parameter field 119  
Parameter Tag field 81  
Participation field 180  
Partition Port on Intrusion Detected field 90  
Partition Time field 90  
passwords, setting  
  console 37  
  remote dial-in access 39  
  Telnet 37  
  Web 37  
Path Cost field 180  
Pause Frames field 133  
PIDs 162  
Policy Class Name field 242  
Policy Name field 237, 239  
Policy Order field 237, 238  
Policy page 236  
Policy Precedence field 239  
Policy Statistics page 239  
port autonegotiation speed

- configuring 104
  - gigabit ports 107
  - Port Based modification page 159
  - Port Based page 157
  - port communication speed, configuring 113
  - Port Configuration page 91, 167, 179
  - Port Error Summary page 135
  - Port field 141
  - Port Information page 169
  - Port List field 90, 94
  - Port List page 95
  - Port Lists page 93
  - Port Management page 104
  - Port Membership field 196
  - port mirroring 143
    - display 144
  - Port Mirroring page 144
  - Port Name field 168, 169
  - port naming 104, 106
  - Port page 131
  - Port Priority field 168
  - port statistics
    - viewing 131, 132, 135
    - zeroing ports 134
  - port-based port mirroring 143, 146
  - port-based VLANs 154
  - ports
    - enabling 106
    - naming 106
    - trusted, untrusted, and unrestricted 192, 203
  - power status 47
  - Power Status field 49
  - Preconfigured Port # field 208
  - Preconfigured Protocol field 207
  - Primary RADIUS Server field 39
  - Priority field 180
  - Privacy Passphrase field 65
  - Privacy Protocol field 65
  - Private Protocol field 65
  - Private Protocols Supported field 63
  - product support 25
  - Protocol field 157, 162
  - protocol-based VLANs 154
  - Proxy field 151, 152
  - publications
    - hard copy 25
    - related 24
  - PVID 167
  - PVID field 168, 169
- ## Q
- QoS 198, 199, 200, 201
    - 241
    - 802.1p priority mapping, configuring 199
    - 802.1p priority, configuring 197
    - about 189
    - actions 224
    - bandwidth allocation 191
    - burst size 232
    - capabilities 192
    - classifier blocks 219, 222, 243
      - creating 220, 221
      - deleting 223
      - modifying 222
    - classifiers 218, 219, 222, 243
      - creating 216, 217, 218
      - deleting 219
    - committed rate 232
    - data specification 232
    - defined filters, installing 232, 235
    - diagnostics 243
    - discipline 191
    - drop precedence 200, 201, 203, 224
    - DSCP mapping, configuring 200
    - duration 232
    - entry storage 192
    - Ethertype 210
    - filter actions

- about 224
  - deleting 227, 228
  - hardware filters
    - deleting 240
    - installing 236
    - viewing statistics 238
  - ignore value 205, 210
  - in-profile action 236
  - interface action extensions 229
    - deleting 231
  - interface class (trusted, untrusted, unrestricted) 192, 203
  - interface classes 193, 203
  - interface groups 190
    - configuring 190
    - deleting 196
    - modifying 193
  - IP classifier elements
    - about 203
    - configuring 203
    - deleting 209
  - layer 2 classifier elements
    - about 209
    - creating 210
    - deleting 215
  - masks 243
  - matching 203, 209
  - metered data 236
  - meters 232, 236, 237
    - deleting 235
  - multiple VLANs 209
  - no meter data 236
  - non-IP filter 214
  - out-of-profile action 236
  - packet reordering 236, 241
  - policies 190
    - configuring 232, 235
    - disable 237
    - enable 237
    - statistics 238
  - policy server control 241
  - ports 190
    - adding or removing 195
    - type (trusted, untrusted, unrestricted) 192, 203
  - queue sets 197
  - role combinations
    - adding 195
    - deleting 196
    - modifying 193
    - removing 195
  - service order 191
  - statistics 236, 239, 241
  - tagging 213
  - troubleshooting 243
  - trusted ports 192, 203
  - trusted, untrusted, unrestricted ports 193, 203
  - unrestricted ports 192, 203
  - untrusted ports 192, 203
  - valid ranges 243
  - VLAN tagging 210
- QoS Classifier Rule/Mask Comparison table 247
- QoS Counters Consumed field 246
- QoS Filters Consumed field 246
- QoS Masks Consumed field 246
- QoS Meters Consumed field 246
- QoS policies
  - enabling 237
- QoS Policy Agent Reset to Defaults field 242
- QoS policy agent, configuring 241
- QoS Resource Allocation Table field 246
- QoS Valid Range field 247
- QoS WEB Display Mode field 242
- Query Time field 151, 152
- Queue field 198
- Queue Sets field 194
- Quiet Period field 87

## R

- RADIUS page 39
- RADIUS Shared Secret field 40
- RADIUS-based network security 39, 85

- 
- rate limiting
    - about 147
    - configuring 147
  - Rate Limiting page 147
  - Read View field 71
  - Read-Only Community String field 60
  - Read-Only Switch Password field 38
  - Read-Write Community String field 60
  - Read-Write Switch Password field 38
  - Re-authenticate Now field 87
  - Re-authentication field 87
  - Re-authentication Period field 87
  - redundancy 184
  - Remote Access page 56
  - remote dial-in access, configuring 39
  - Reset page 43
  - Reset to Defaults page 44
  - resetting the switch 42
  - resetting the switch, to system defaults 44
  - Retrieve Configuration Image from Server field 112
  - Rising Action 119
  - Rising Level field 119
  - RMON
    - Ethernet statistics
      - viewing 124
    - history statistics
      - viewing 127
  - RMON Ethernet page 124
  - RMON Event Log page 121
  - RMON History page 127
  - RMON options
    - fault event log, viewing 121
    - fault threshold parameters
      - configuring 117
      - deleting 120
    - history statistics
      - viewing 127
  - RMON Threshold Creation field 120
  - RMON Threshold page 118
  - RMON, about 117
  - Robust Value field 151, 152
  - Role Combination field 192, 194, 196, 237, 238, 239
  - role combinations 190
  - Root Path Cost field 183
  - Root Port field 183
- ## S
- Sample/Alarm Sample field 120
  - Secondary RADIUS Server field 39
  - security 85
    - MAC address-based 89
    - passwords 37
    - RADIUS-based 39
    - remote dial-in access 39
    - SNMPv3 58, 61
  - Security Configuration page 89
  - Security field 93
  - Security Level field 71, 82
  - Security Model field 68, 71
  - Security Name field 67, 81
  - Security page 89
  - Security Table page 96
  - Select VLANs field 102
  - Serial Number field 48
  - Server Timeout field 87
  - Service Class field 202, 203
  - Service Order field 192
  - Set Drop Precedence field 226
  - Set Egress Non-Unicast field 231
  - Set Egress Unicast field 230
  - Single Collision Frame field 140
  - Single Collisions field 133, 135
-

## SNMP

- about 58
- MAC address security 90
- NVRAM entries 60
- trap receivers
  - configuring 83
  - deleting 84
- SNMP Engine Boot field 62
- SNMP Engine Dialect field 63
- SNMP Engine ID field 62
- SNMP Engine Maximum Message Size field 62
- SNMP Engine Time field 62
- SNMP Trap Receiver page 83
- SNMP traps 83
- SNMP/Access field 58
- SNMP/Use List field 58
- SNMPv1
  - about 58
  - configuring 58
- SNMPv1 page 58
- SNMPv3 61
  - about 58
  - configuring 60
  - group access rights 69
    - deleting 71
  - group membership 66
    - deleting 68
  - management information views 72
    - deleting 74
  - system information, viewing 60, 61
  - system notification entries 75
    - deleting 77
  - target addresses 78
    - deleting 80
  - target parameters 80
    - deleting 82
  - user access 63
    - deleting 66
- Snooping field 150, 152
- software
  - downloading 109
  - upgrading 109
  - software download
    - process 109
  - Software Download page 109
  - Software Image Filename field 110
  - software upgrade 255
  - Software Version field 48
  - software version requirements
    - Microsoft Internet Explorer 27
    - Netscape Navigator 27
  - software versions 37, 109
  - Source Address field 206, 207
  - Source field 102
  - Source L4 Port field 206
  - Source Layer 4 Port field 208
  - Source MAC Addr field 211
  - Source MAC Addr Mask field 211
  - Source MAC Address field 213
  - Source Mask Length field 206
  - spanning tree 170
    - bridge information 181
    - learning mode 186
    - learning modes 180
    - port path cost 180
    - port priority 180
  - Spanning Tree Add VLAN page 177
  - spanning tree configuration 179
  - spanning tree groups 170
    - adding VLANs 177
    - bridge information 181
    - configuring 171
    - default 171
    - ports 179
    - removing VLANs 177
    - tagged BPDU 170
    - tagging 171, 174, 184
    - VLANs 177
  - spanning tree ports

- configuring 179
  - enabling 179
  - FastLearning 179
  - Speed/Duplex field 106, 108, 135
  - SQE Test Errors field 140
  - Src IP Address field 247
  - Src L4 Port field 247
  - Src MAC Address field 247
  - Start field 128
  - Start TFTP Load of New Image field 110
  - State field 157, 180, 237
  - Static Router Ports field 152
  - statistics 117, 127, 131, 134, 135, 138, 140
  - Status field 135
  - STGs 170
  - Storage Type field 206, 212, 227, 231, 235, 237, 240
  - STP Learning field 186
  - summary options
    - viewing
      - switch information 47
  - Supplicant Timeout field 87
  - Support menu
    - manuals 254
    - online help 251
    - technical publications 252
    - user interface, upgrading 255
  - support, Nortel Networks 25
  - switch configuration files
    - requirements for retrieving 113
    - requirements for storing 113
    - TFTP server 111
  - switch images, downloading 109
  - switch information
    - viewing 47
  - Switch Information page 47
  - symmetric flow control 108
  - sysContact field 37
  - sysDescription field 37
  - sysLocation field 37
  - sysName field 37
  - System choice 242
  - System Contact field 56
  - system default settings, resetting to 44
  - System Description field 55
  - System Information page 35, 41, 61
  - system information, viewing 35
  - System Location field 56
  - system location, naming 55
  - System Log page 122
  - system log, viewing 122
  - System Name field 56
  - system name, configuring 55
  - System Object ID field 55
  - System page 55
  - system settings
    - modifying 55
    - system contact 56
    - system location 56
    - system name 56
  - system statistics options, viewing
    - Ethernet error statistics 138
    - interface statistics 136
    - port statistics 131
    - QoS 238
    - transparent bridging statistics 140
  - System Up Time field 56
  - sysUpTime field 37
- ## T
- tables and input forms, about 32
  - Tagged BPDU on Tagged Port field 174, 184
  - tagged frames 167
  - Tagged Trunk 168
  - tagged trunk 160

- tagging 160, 167, 180
  - Tagging field 168, 180
  - Target Address field 79
  - Target Address page 78
  - Target Domain field 79
  - Target Name field 79
  - Target Parameter Entry field 79
  - Target Parameter page 80
  - Target Retry Count field 79
  - Target Tag List field 79
  - Target Timeout field 79
  - technical publications 25, 252
  - technical support 25
  - Telnet Password Setting page 37
  - Telnet/Access field 57
  - Telnet/Use List field 57
  - text conventions 24
  - TFTP
    - configuration file 111
    - server 111
    - software download 111
  - TFTP Server IP Address field 110, 112
  - Time Stamp field 122, 123
  - Total In-Profile Packets field 240
  - Total Octets field 133
  - Total Out-Of-Profile Packets field 240
  - Track Statistics field 237, 238, 240
  - Traffic Type field 188
  - traffic, classifying 203
  - Transmit Period field 87
  - Transparent Bridging page 140
  - transparent bridging statistics
    - viewing 140, 141
  - Trap Receiver Index field 84
  - traps 83
  - Triggered By field 122
  - troubleshooting
    - access 56
    - address filtering 88
    - autonegotiation 106
    - classifiers 218, 219, 222
    - configuration file 113
    - defaults 44
    - filter components 216
    - gigabit ports 107
    - IGMP 150, 153
    - MAC address security 98, 100
    - MLT 186
    - privacy passphrase 65
    - QoS 191, 192, 198, 199, 201, 203, 219, 222, 236, 243
    - SNMPv3 60
    - software upgrading 109
    - spanning tree groups 171, 179
    - statistics 240
    - STGs 177
    - VLANs 155, 157, 166, 179
  - Trunk field 180
  - Trunk Mode field 186
  - Trunk Name field 186
  - Trunk Port Members field 186
  - Trunk Status field 186
  - trusted ports 192, 196, 203
- ## U
- UDP RADIUS Port field 40
  - Unavailable Context field 63
  - Undersize field 126, 129
  - Undersized Packets field 133
  - Unit/Port Membership field 160, 165
  - Unknown Context field 63
  - Unknown Engine IDs field 63
  - Unknown User Name field 63
  - unregistered frames 167
  - unrestricted ports 192, 196, 203

- Unsupported Security Level field 63
  - Untagged Access 168
  - untagged access 160
  - untagged frames 167
  - untrusted ports 192, 196, 203
  - Update 802.1p Priority field 226
  - Update DSCP field 226
  - User Defined Port # field 208
  - User Defined Protocol # field 207
  - User Defined Protocol field 157, 162
  - user interface, upgrading 255
  - User Name field 65
  - User Priority field 247
  - User Specification page 63
  - Utilization page 187
- ## V
- VID used for Tagged BPDU field 174, 184
  - View Mask field 74
  - View Name field 73
  - View Subtree field 74
  - View Type field 74
  - VLAN Configuration
    - Protocol Based modification page 164, 174
    - Protocol Based setting page 160
  - VLAN Configuration page 156
  - VLAN field 211, 213, 247
  - VLAN Membership
    - Add VLAN page 178
    - Remove VLAN page 178
  - VLAN Membership page 177
  - VLAN Name field 157, 161, 165, 170
  - VLAN Tag field 211, 213, 248
  - VLAN Type field 157, 170
  - VLANs
    - about 154
    - autoPVID 155, 157
    - broadcast domains, configuring 167
    - configuring 155
    - deleting 166, 176
    - finding MAC addresses 103
    - learned MAC addresses 101
    - MLT and STGs 155
    - number of 154
    - port information
      - viewing 168
    - port-based
      - about 155
      - configuring 157
    - protocol-based
      - about 155
      - configuring 160
      - number of 155
      - reserved PID types 164
      - supported PID types 162
      - selecting a management VLAN 166
      - tagging 213
- ## W
- Web browser, requirements 27
  - Web Page/Access field 58
  - Web Password Setting page 37
  - Web/Use List field 58
  - Web-based management interface
    - home page, graphic 28
    - logging in 28
    - main menu, icons 31, 33
    - management page 32
    - navigating the menu 29
    - requirements to use 27
    - Web page layout 29
    - Web page layout, graphic 29
  - Write View field 71
  - Wrong Digest field 63

