

GS-3012/GS-3012F Series

Gigabit Ethernet Switch

User's Guide

Version 3.70

11/2006

Edition 1



About This User's Guide

Intended Audience

This manual is intended for people who want to configure the switch using the web configurator or via commands. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

Related Documentation

- Quick Start Guide
The Quick Start Guide is designed to help you get up and running right away. It contains information on hardware installation of your switch.
- Web Configurator Online Help
Embedded web help for descriptions of individual screens and supplementary information.



It is recommended you use the web configurator to configure the switch.

- Supporting Disk
Refer to the included CD for support documents.
- ZyXEL Web Site
Please refer to www.zyxel.com for additional support documentation and product certifications.

User Guide Feedback

Help us help you. Send all User Guide-related comments, questions or suggestions for improvement to the following address, or use e-mail instead. Thank you!

The Technical Writing Team,
ZyXEL Communications Corp.,
6 Innovation Road II,
Science-Based Industrial Park,
Hsinchu, 300, Taiwan.

E-mail: techwriters@zyxel.com.tw

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.



Warnings tell you about things that could harm you or your device.












Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The GS-3012 or the GS-3012F may be referred to as the “switch”, the “device” or the “system” in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the “enter” or “return” key on your keyboard.
- “Enter” means for you to type one or more characters and then press the [ENTER] key. “Select” or “choose” means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the “metric” value or the “scientific” value. For example, “k” for kilo may denote “1000” or “1024”, “M” for mega may denote “1000000” or “1048576” and so on.
- “e.g.,” is a shorthand for “for instance”, and “i.e.,” means “that is” or “in other words”.

Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The switch icon is not an exact representation of your device.

The switch 	Computer 	Notebook computer 
Server 	DSLAM 	Firewall 
Telephone 	Switch 	Router 

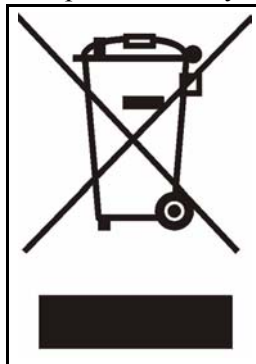
Safety Warnings



For your safety, be sure to read and follow all warning notices and instructions.

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the power outlet.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- The length of exposed (bare) power wire should not exceed 7mm.

This product is recyclable. Dispose of it properly.



Contents Overview

Introduction and Hardware Overview	31
Getting to Know Your Switch	33
Hardware Installation and Connection	39
Hardware Overview	43
Basic Settings	51
Introducing the Web Configurator	53
Initial Setup Example	61
System Status and Port Details	65
Basic Setting	71
Advanced Settings	83
VLAN	85
Static MAC Forward Setup	97
Filtering	101
Spanning Tree Protocol	103
Bandwidth Control	113
Broadcast Storm Control	115
Mirroring	117
Link Aggregation	119
Port Authentication	123
Port Security	129
Classifier	133
Policy Rule	139
Queuing Method	145
Multicast	149
DHCP Relay	161
Static Routing and Management	163
Routing Protocol	165
Maintenance	167
Access Control	175
Diagnostic	187
Syslog	189
Cluster Management	193
MAC Table	199
ARP Table	201

Configure Clone	203
Commands and Troubleshooting	205
Introducing the Commands	207
Command Examples	239
IEEE 802.1Q Tagged VLAN Commands	257
Troubleshooting	265
Appendices and Index	267

Table of Contents

About This User's Guide	3
Document Conventions.....	4
Safety Warnings.....	6
Contents Overview	9
Table of Contents.....	11
List of Figures	21
List of Tables.....	27
Part I: Introduction and Hardware Overview	31
Chapter 1	
Getting to Know Your Switch.....	33
1.1 Introduction	33
1.1.1 Backbone Application	33
1.1.2 Bridging Example	34
1.1.3 High Performance Switched Workgroup Example	35
1.1.4 IEEE 802.1Q VLAN Application Examples	35
1.2 Ways to Manage the Switch	36
1.3 Good Habits for Managing the switch	37
Chapter 2	
Hardware Installation and Connection	39
2.1 Installation Scenarios	39
2.2 Desktop Installation Procedure	39
2.3 Mounting the Switch on a Rack	40
2.3.1 Rack-mounted Installation Requirements	40
2.3.2 Attaching the Mounting Brackets to the Switch	40
2.3.3 Mounting the Switch on a Rack	41
Chapter 3	
Hardware Overview.....	43
3.1 Front Panel	43
3.1.1 Console Port	44

3.1.2 Gigabit Ports	44
3.1.3 Mini-GBIC Slots	45
3.1.4 Management Port	47
3.2 Rear Panel	47
3.2.1 Power Connector	47
3.3 LEDs	48
3.4 Configuring the Switch	49
Part II: Basic Settings	51
Chapter 4	
Introducing the Web Configurator	53
4.1 Introduction	53
4.2 System Login	53
4.3 Status Screen	54
4.3.1 Change Your Password	57
4.4 Switch Lockout	57
4.5 Resetting the Switch	58
4.5.1 Reload the Configuration File	58
4.5.2 Logging Out of the Web Configurator	59
4.5.3 Help	59
Chapter 5	
Initial Setup Example	61
5.1 Overview	61
5.1.1 Creating a VLAN	61
5.1.2 Setting Port VID	62
5.2 Configuring Switch Management IP Address	63
Chapter 6	
System Status and Port Details	65
6.1 About System Statistics and Information	65
6.2 Port Status Summary	65
6.2.1 Port Details	66
Chapter 7	
Basic Setting	71
7.1 Introducing the Basic Setting Screens	71
7.2 System Information	71
7.3 General Setup	73
7.4 Introduction to VLANs	75

7.5 Switch Setup Screen	75
7.6 IP Setup	77
7.6.1 Management IP Addresses	77
7.7 Port Setup	80
Part III: Advanced Settings	83
Chapter 8	
VLAN	85
8.1 Introduction to IEEE 802.1Q Tagged VLAN	85
8.1.1 Forwarding Tagged and Untagged Frames	85
8.1.2 Automatic VLAN Registration	86
8.1.3 Port VLAN Trunking	86
8.2 Select the VLAN Type	87
8.3 802.1Q VLAN	87
8.3.1 802.1Q VLAN Detail	88
8.3.2 802.1Q VLAN Port Settings	89
8.3.3 802.1Q Static VLAN	90
8.3.4 Viewing and Editing VLAN Settings	92
8.4 Introduction to Port-based VLANs	93
8.4.1 Configuring a Port-based VLAN	94
Chapter 9	
Static MAC Forward Setup	97
9.1 Introduction to Static MAC Forward Setup	97
9.2 Configuring Static MAC Forwarding	97
9.3 Viewing and Editing Static MAC Forwarding Rules	98
Chapter 10	
Filtering	101
10.1 Introduction to Filtering	101
10.2 Configuring a Filtering Rule	101
10.3 Viewing and Editing Filter Rules	102
Chapter 11	
Spanning Tree Protocol	103
11.1 STP/RSTP Overview	103
11.1.1 STP Terminology	103
11.1.2 How STP Works	104
11.1.3 STP Port States	105
11.1.4 Multiple RSTP	105

11.2 Spanning Tree Protocol Main Screen	106
11.3 Configure Rapid Spanning Tree Protocol	106
11.4 Rapid Spanning Tree Protocol Status	108
11.5 Configure Multiple Rapid Spanning Tree Protocol	109
11.6 Multiple Rapid Spanning Tree Protocol Status	111
Chapter 12	
Bandwidth Control.....	113
12.1 Introduction to Bandwidth Control	113
12.1.1 CIR and PIR	113
12.1.2 Bandwidth Control Setup	113
Chapter 13	
Broadcast Storm Control	115
13.1 Introducing Broadcast Storm Control	115
13.2 Configuring Broadcast Storm Control	115
Chapter 14	
Mirroring	117
14.1 Introduction to Port Mirroring	117
14.2 Port Mirroring Configuration	117
Chapter 15	
Link Aggregation	119
15.1 Introduction to Link Aggregation	119
15.1.1 Dynamic Link Aggregation	119
15.1.2 Link Aggregation ID	120
15.2 Link Aggregation Protocol Status	120
15.3 Link Aggregation Setup	121
Chapter 16	
Port Authentication.....	123
16.1 Introduction to Authentication	123
16.1.1 RADIUS	123
16.2 Configuring Port Authentication	125
16.2.1 Configuring RADIUS Server Settings	125
16.2.2 Configuring IEEE802.1x	126
Chapter 17	
Port Security.....	129
17.1 About Port Security	129
17.2 Port Security Setup	129

Chapter 18	
Classifier	133
18.1 About the Classifier and QoS	133
18.2 Configuring the Classifier	133
18.3 Viewing and Editing Classifier Configuration	136
18.4 Classifier Example	137
Chapter 19	
Policy Rule	139
19.1 About Policy Rules	139
19.1.1 DiffServ	139
19.1.2 DSCP and Per-Hop Behavior	139
19.2 Configuring Policy Rules	140
19.3 Viewing and Editing Policy Configuration	142
19.4 Policy Example	143
Chapter 20	
Queuing Method	145
20.1 Introduction to Queuing	145
20.1.1 Strict Priority Queuing (SPQ)	145
20.1.2 Weighted Round Robin Scheduling (WRR)	146
20.2 Configuring Queuing	146
Chapter 21	
Multicast	149
21.1 Multicast Overview	149
21.1.1 IP Multicast Addresses	149
21.1.2 IGMP Filtering	149
21.1.3 IGMP Snooping	149
21.2 Multicast Status	150
21.3 Multicast Setup	150
21.4 IGMP Filtering Profile	153
21.5 MVR Overview	154
21.5.1 Types of MVR Ports	154
21.5.2 MVR Modes	154
21.5.3 How MVR Works	155
21.6 General MVR Configuration	155
21.7 MVR Group Configuration	157
21.7.1 MVR Configuration Example	159
Chapter 22	
DHCP Relay	161
22.1 DHCP Relay Overview	161

22.1.1 DHCP “Relay Agent Information Option”	161
22.1.2 DHCP Relay Agent Circuit ID Sub-option Format	161
22.2 DHCP Relay Configuration	161
Part IV: Static Routing and Management	163
Chapter 23	
Routing Protocol	165
23.1 Static Route Overview	165
Chapter 24	
Maintenance	167
24.1 Maintenance	167
24.2 Firmware Upgrade	168
24.3 Restore a Configuration File	169
24.4 Backing Up a Configuration File	169
24.5 Load Factory Defaults	170
24.6 Save Configuration	170
24.7 Reboot System	171
24.8 Command Line FTP	171
24.8.1 Filename Conventions	171
24.8.2 FTP Command Line Procedure	172
24.8.3 GUI-based FTP Clients	173
24.8.4 FTP Restrictions	173
Chapter 25	
Access Control.....	175
25.1 About Access Control	175
25.2 Access Control Overview	175
25.3 About SNMP	176
25.3.1 Supported MIBs	177
25.3.2 SNMP Traps	177
25.3.3 Configuring SNMP	177
25.3.4 Setting Up Login Accounts	178
25.4 SSH Overview	180
25.5 How SSH works	180
25.6 SSH Implementation	181
25.6.1 Requirements for Using SSH	181
25.7 Introduction to HTTPS	181
25.7.1 HTTPS Example	182
25.7.2 Internet Explorer Warning Messages	182

25.7.3 Netscape Navigator Warning Messages	182
25.7.4 Login Screen	183
25.8 Service Access Control	184
25.9 Remote Management	185
Chapter 26	
Diagnostic.....	187
26.1 Diagnostic	187
Chapter 27	
Syslog	189
27.1 Syslog	189
27.2 Syslog Setup	189
27.3 Syslog Server Setup	190
Chapter 28	
Cluster Management.....	193
28.1 Introduction to Cluster Management	193
28.2 Cluster Management Status	194
28.2.1 Cluster Member Switch Management	194
28.3 Configuring Cluster Management	196
Chapter 29	
MAC Table.....	199
29.1 Introduction to MAC Table	199
29.2 Viewing MAC Table	200
Chapter 30	
ARP Table	201
30.1 Introduction to ARP Table	201
30.1.1 How ARP Works	201
30.2 Viewing ARP Table	201
Chapter 31	
Configure Clone	203
31.1 Configure Clone	203
Part V: Commands and Troubleshooting	205
Chapter 32	
Introducing the Commands	207

32.1 Overview	207
32.1.1 Switch Configuration File	207
32.2 Accessing the CLI	207
32.2.1 Access Priority	208
32.2.2 The Console Port	208
32.2.3 Telnet	208
32.3 The Login Screen	209
32.4 Command Syntax Conventions	209
32.5 Getting Help	210
32.5.1 List of Available Commands	210
32.5.2 Detailed Command Information	210
32.6 Privilege Levels	211
32.7 Command Modes	211
32.8 Using Command History	213
32.9 Saving Your Configuration	213
32.9.1 Logging Out	213
32.10 Command Summary	214
32.10.1 User Mode	214
32.10.2 Enable Mode	215
32.10.3 Configure Mode	220
32.10.4 config-vlan Commands	232
32.10.5 interface port-channel Commands	233
32.10.6 mvr Commands	236
Chapter 33	
Command Examples.....	239
33.1 Overview	239
33.2 show Commands	239
33.2.1 show system-information	239
33.2.2 show hardware-monitor	240
33.2.3 show ip	240
33.2.4 show logging	241
33.2.5 show interface	241
33.2.6 show mac address-table	242
33.3 ping	243
33.4 traceroute	243
33.5 Enabling RSTP	244
33.6 Configuration File Maintenance	244
33.6.1 Backing up Configuration	244
33.6.2 Restoring Configuration	245
33.6.3 Using a Different Configuration File	246
33.6.4 Resetting to the Factory Default	246
33.7 Example no Commands	247

33.7.1 no mirror-port	247
33.7.2 no trunk	247
33.7.3 no port-access-authenticator	248
33.7.4 no ssh	248
33.8 interface Commands	249
33.8.1 interface port-channel	249
33.8.2 bpdu-control	249
33.8.3 broadcast-limit	250
33.8.4 bandwidth-limit	250
33.8.5 mirror	251
33.8.6 gvrp	251
33.8.7 ingress-check	252
33.8.8 vlan-trunking	252
33.8.9 weight	253
33.8.10 egress set	253
33.8.11 qos priority	253
33.8.12 name	254
33.8.13 speed-duplex	254
Chapter 34	
IEEE 802.1Q Tagged VLAN Commands	257
34.1 IEEE 802.1Q Tagged VLAN Overview	257
34.2 VLAN Databases	257
34.2.1 Static Entries (SVLAN Table)	257
34.2.2 Dynamic Entries (DVLAN Table)	257
34.3 Configuring Tagged VLAN	258
34.4 Global VLAN1Q Tagged VLAN Configuration Commands	258
34.4.1 GARP Status	259
34.4.2 GARP Timer	259
34.4.3 Show GVRP	260
34.4.4 Enable GVRP	260
34.4.5 Disable GVRP	260
34.5 Port VLAN Commands	260
34.5.1 Set Port VID	260
34.5.2 Set Acceptable Frame Type	261
34.5.3 Enable or Disable Port GVRP	261
34.5.4 Modify Static VLAN	261
34.5.5 Delete VLAN ID	263
34.6 Enable VLAN	263
34.7 Disable VLAN	263
34.8 Show VLAN Setting	263
Chapter 35	
Troubleshooting.....	265

Part VI: Appendices and Index	267
Appendix A Product Specifications.....	269
Appendix B Browser Setup	273
Appendix C IP Addresses and Subnetting	279
Appendix D Legal Information	287
Appendix E Customer Support.....	291
Index.....	295

List of Figures

Figure 1 Backbone Application	34
Figure 2 Bridging Application	34
Figure 3 High Performance Switched Application	35
Figure 4 Tag-based VLAN Application	36
Figure 5 Shared Server Using VLAN Example	36
Figure 6 Attaching Rubber Feet	40
Figure 7 Attaching the Mounting Brackets	41
Figure 8 Mounting the Switch on a Rack	41
Figure 9 Front Panel: GS-3012	43
Figure 10 Front Panel: GS-3012F	43
Figure 11 Transceiver Installation Example	46
Figure 12 Connecting the Fiber Optic Cables	46
Figure 13 Removing the Fiber Optic Cables	46
Figure 14 Opening the Transceiver's Latch Example	46
Figure 15 Transceiver Removal Example	47
Figure 16 Rear Panel: GS-3012 AC Power Model	47
Figure 17 Rear Panel: GS-3012 DC Power Model	47
Figure 18 Rear Panel: GS-3012F AC Power Model	47
Figure 19 Rear Panel: GS-3012F DC Power Model	47
Figure 20 Web Configurator: login	53
Figure 21 Web Configurator Home Screen (Status)	54
Figure 22 Web Configurator: Change Password at Login	57
Figure 23 Resetting the Switch: Via Console Port	59
Figure 24 Web Configurator: Logout Screen	59
Figure 25 Initial Setup Network Example: VLAN	61
Figure 26 Initial Setup Network Example: Port VID	63
Figure 27 Initial Setup Example: Management IP Address	63
Figure 28 Port Status	65
Figure 29 Status: Port Details	67
Figure 30 System Info	72
Figure 31 General Setup	73
Figure 32 Switch Setup	75
Figure 33 IP Setup	78
Figure 34 Port Setup	80
Figure 35 Port VLAN Trunking	87
Figure 36 Selecting a VLAN Type	87
Figure 37 802.1Q VLAN Status	88
Figure 38 802.1Q VLAN Detail	88

Figure 39 802.1Q VLAN Port Settings	89
Figure 40 802.1Q Static VLAN	91
Figure 41 Static VLAN: Summary Table	92
Figure 42 VID1 Example Screen	93
Figure 43 Port Based VLAN Setup (All Connected)	94
Figure 44 Port Based VLAN Setup (Port isolation)	94
Figure 45 Static MAC Forwarding	97
Figure 46 Static MAC Forwarding: Summary Table	98
Figure 47 Filtering	101
Figure 48 Filtering: Summary Table	102
Figure 49 MRSTP Network Example	105
Figure 50 Spanning Tree Protocol RSTP and MRSTP	106
Figure 51 RSTP: Configuration	107
Figure 52 Rapid Spanning Tree Protocol: Status	109
Figure 53 MRSTP: Configuration	110
Figure 54 MRSTP: Status	112
Figure 55 Bandwidth Control	114
Figure 56 Broadcast Storm Control	115
Figure 57 Mirroring	117
Figure 58 Link Aggregation: Link Aggregation Protocol Status	120
Figure 59 Link Aggregation: Configuration	121
Figure 60 RADIUS Server	123
Figure 61 Port Authentication	125
Figure 62 Port Authentication: RADIUS	125
Figure 63 Port Authentication: 802.1x	126
Figure 64 Port Security	130
Figure 65 Classifier	134
Figure 66 Classifier: Summary Table	136
Figure 67 Classifier: Example	138
Figure 68 Policy	140
Figure 69 Policy: Summary Table	142
Figure 70 Policy Example	144
Figure 71 Queuing Method	147
Figure 72 Multicast Status	150
Figure 73 Multicast Setting	151
Figure 74 Multicast: IGMP Filtering Profile	153
Figure 75 MVR Network Example	154
Figure 76 MVR Multicast Television Example	155
Figure 77 MVR	156
Figure 78 MVR Group Configuration	158
Figure 79 MVR Configuration Example	159
Figure 80 MVR Configuration Example	159
Figure 81 MVR Configuration Example	160

Figure 82 MVR Configuration Example	160
Figure 83 DHCP Relay	162
Figure 84 Static Routing	165
Figure 85 Static Routing: Summary Table	166
Figure 86 Maintenance	167
Figure 87 Firmware Upgrade	168
Figure 88 Restore Configuration	169
Figure 89 Backup Configuration	169
Figure 90 Confirm Load Factory Defaults	170
Figure 91 Close Browser after Load Factory Defaults	170
Figure 92 Reboot System: Confirmation	171
Figure 93 Access Control	175
Figure 94 Console Port Priority	176
Figure 95 SNMP Management Model	176
Figure 96 Access Control: SNMP	178
Figure 97 Access Control: Logins	179
Figure 98 SSH Communication Example	180
Figure 99 How SSH Works	180
Figure 100 HTTPS Implementation	181
Figure 101 Security Alert Dialog Box (Internet Explorer)	182
Figure 102 Security Certificate 1 (Netscape)	183
Figure 103 Security Certificate 2 (Netscape)	183
Figure 104 Example: Lock Denoting a Secure Connection	184
Figure 105 Access Control: Service Access Control	184
Figure 106 Access Control: Remote Management	185
Figure 107 Diagnostic	187
Figure 108 Syslog Setup	190
Figure 109 Syslog Server Setup	191
Figure 110 Clustering Application Example	193
Figure 111 Cluster Management Status	194
Figure 112 Cluster Member Web Configuration Screen	195
Figure 113 Example: Uploading Firmware to a Cluster Member Switch	195
Figure 114 Configuring Cluster Management	196
Figure 115 MAC Table Flowchart	199
Figure 116 MAC Table	200
Figure 117 ARP Table	202
Figure 118 Configure Clone	203
Figure 119 Initial Console Port Screen	208
Figure 120 CLI: Login Screen	209
Figure 121 CLI Help: List of Commands: Example 1	210
Figure 122 CLI Help: List of Commands: Example 2	210
Figure 123 CLI Help: Detailed Command Information: Example 1	211
Figure 124 CLI: Help: Detailed Command Information: Example 2	211

Figure 125 CLI: History Command Example	213
Figure 126 CLI: write memory	213
Figure 127 show system-information Command Example	239
Figure 128 how hardware-monitor Command Example	240
Figure 129 show ip Command Example	240
Figure 130 show logging Command Example	241
Figure 131 show interface Command Example	242
Figure 132 show mac address-table Command Example	243
Figure 133 ping Command Example	243
Figure 134 traceroute Command Example	244
Figure 135 Enable RSTP Command Example	244
Figure 136 CLI: Backup Configuration Example	245
Figure 137 CLI: Restore Configuration Example	245
Figure 138 boot config Command Example	246
Figure 139 CLI: reload config Command Example	246
Figure 140 CLI: Reset to the Factory Default Example	246
Figure 141 no mirror-port Command Example	247
Figure 142 no trunk Command Example	247
Figure 143 no port-access-authenticator Command Example	248
Figure 144 no ssh Command Example	249
Figure 145 interface port-channel Command Example	249
Figure 146 interface bpdu-control Command Example	250
Figure 147 broadcast-limit Command Example	250
Figure 148 bandwidth-limit Command Example	251
Figure 149 mirror Command Example	251
Figure 150 gvrp Command Example	252
Figure 151 ingress-check Command Example	252
Figure 152 vlan-trunking Command Example	252
Figure 153 weight Command Example	253
Figure 154 egress set Command Example	253
Figure 155 qos priority Command Example	254
Figure 156 name Command Example	254
Figure 157 speed-duplex Command Example	255
Figure 158 Tagged VLAN Configuration and Activation Example	258
Figure 159 CPU VLAN Configuration and Activation Example	258
Figure 160 garp status Command Example	259
Figure 161 show gvrp Command Example	260
Figure 162 port default vid Command Example	261
Figure 163 frame type Command Example	261
Figure 164 no gvrp Command Example	261
Figure 165 Modifying Static VLAN Example	262
Figure 166 no vlan Command Example	263
Figure 167 show vlan Command Example	264

Figure 168 Pop-up Blocker	273
Figure 169 Internet Options	274
Figure 170 Internet Options	275
Figure 171 Pop-up Blocker Settings	275
Figure 172 Internet Options	276
Figure 173 Security Settings - Java Scripting	277
Figure 174 Security Settings - Java	277
Figure 175 Java (Sun)	278
Figure 176 Network Number and Host ID	280
Figure 177 Subnetting Example: Before Subnetting	282
Figure 178 Subnetting Example: After Subnetting	283

List of Tables

Table 1 Front Panel Connections	44
Table 2 LED Descriptions	48
Table 3 Navigation Panel Sub-links Overview	54
Table 4 Web Configurator Screen Sub-links Details	55
Table 5 Navigation Panel Sub-link Descriptions	55
Table 6 Port Status	66
Table 7 Status: Port Details	67
Table 8 System Info	72
Table 9 General Setup	74
Table 10 Switch Setup	76
Table 11 IP Setup	78
Table 12 Port Setup	80
Table 13 IEEE 802.1Q VLAN terminology	86
Table 14 802.1Q VLAN Status	88
Table 15 802.1Q VLAN Detail	89
Table 16 802.1Q VLAN Port Settings	90
Table 17 802.1Q Static VLAN	91
Table 18 Static VLAN: Summary Table	92
Table 19 Port Based VLAN Setup	95
Table 20 Static MAC Forwarding	98
Table 21 Static MAC Forwarding: Summary Table	98
Table 22 Filtering	101
Table 23 Filtering: Summary Table	102
Table 24 STP Path Costs	104
Table 25 STP Port States	105
Table 26 Spanning Tree Protocol: Status	106
Table 27 RSTP: Configuration	107
Table 28 Rapid Spanning Tree Protocol: Status	109
Table 29 MRSTP: Configuration	110
Table 30 Spanning Tree Protocol: Status	112
Table 31 Bandwidth Control	114
Table 32 Broadcast Storm Control	116
Table 33 Mirroring	118
Table 34 Link Aggregation ID: Local Switch	120
Table 35 Link Aggregation ID: Peer Switch	120
Table 36 Link Aggregation: Link Aggregation Protocol Status	120
Table 37 Link Aggregation: Configuration	121
Table 38 Supported VSA	124

Table 39 Supported Tunnel Protocol Attribute	124
Table 40 Port Authentication: RADIUS	125
Table 41 Port Authentication: 802.1x	126
Table 42 Port Security	130
Table 43 Classifier	134
Table 44 Classifier: Summary Table	136
Table 45 Common Ethernet Types and Protocol Number	136
Table 46 Common IP Ports	137
Table 47 Policy	141
Table 48 Policy: Summary Table	143
Table 49 Physical Queue Priority	145
Table 50 Queuing Method	147
Table 51 Multicast Status	150
Table 52 Multicast Setting	151
Table 53 Multicast: IGMP Filtering Profile	153
Table 54 MVR	156
Table 55 MVR Group Configuration	158
Table 56 DHCP Relay	162
Table 57 Static Routing	165
Table 58 Static Routing: Summary Table	166
Table 59 Maintenance	167
Table 60 Filename Conventions	172
Table 61 General Commands for GUI-based FTP Clients	173
Table 62 Access Control Overview	175
Table 63 SNMP Commands	176
Table 64 SNMP Traps	177
Table 65 Access Control: SNMP	178
Table 66 Access Control: Logins	179
Table 67 Access Control: Service Access Control	185
Table 68 Access Control: Remote Management	185
Table 69 Diagnostic	187
Table 70 Syslog Severity Levels	189
Table 71 Syslog Setup	190
Table 72 Syslog Server Setup	191
Table 73 ZyXEL Clustering Management Specifications	193
Table 74 Cluster Management Status	194
Table 75 FTP Upload to Cluster member Example	195
Table 76 Configuring Cluster Management	197
Table 77 MAC Table	200
Table 78 ARP Table	202
Table 79 Configure Clone	204
Table 80 Command Interpreter Mode Summary	212
Table 81 Command Summary: User Mode	214

Table 82 Command Summary: Enable Mode	215
Table 83 Command Summary: Configure Mode	220
Table 84 Command Summary: config-vlan Commands	232
Table 85 Command Summary: Interface	233
Table 86 Command Summary: mvr Commands	236
Table 87 Troubleshooting the Start-Up of Your Switch	265
Table 88 Troubleshooting Accessing the Switch	265
Table 89 Troubleshooting the Password	266
Table 90 General Product Specifications	269
Table 91 Performance and Management Specifications	270
Table 92 Physical and Environmental Specifications	271
Table 93 Firmware Features	271
Table 94 Subnet Mask Example	280
Table 95 Subnet Masks	281
Table 96 Maximum Host Numbers	281
Table 97 Alternative Subnet Mask Notation	281
Table 98 Subnet 1	283
Table 99 Subnet 2	284
Table 100 Subnet 3	284
Table 101 Subnet 4	284
Table 102 Eight Subnets	284
Table 103 24-bit Network Number Subnet Planning	285
Table 104 16-bit Network Number Subnet Planning	285

PART I

Introduction and Hardware Overview

Getting to Know Your Switch (33)

Hardware Installation and Connection (39)

Hardware Overview (43)

Getting to Know Your Switch

This chapter describes the key features, benefits and applications of the switch.

1.1 Introduction

The GS-3012 and GS-3012F are layer 2 stand-alone Gigabit Ethernet switches.

The GS-3012 has 12 100/1000Mbps ports and four mini-GBIC slots for optical uplinking. There are two GS-3012 models. The GS-3012 DC model requires DC power supply input of -48 VDC to -60 VDC, 1.5A Max. The GS-3012 AC model requires 100~240VAC/1.5A power.

The GS-3012F has 12 mini-GBIC slots and four 100/1000Mbps ports for uplinking. There are two GS-3012F models. The GS-3012F DC model requires DC power supply input of -48 VDC to -60 VDC, 1.25A Max. The GS-3012F AC model requires 100~240VAC/1.5A power.

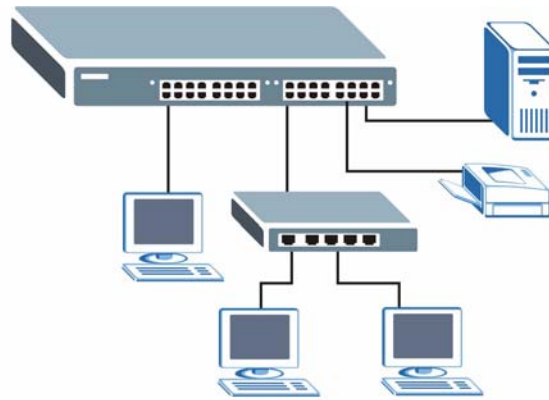
This section shows a few examples of using the switch in various network environments.

1.1.1 Backbone Application

In this application, the switch is an ideal solution for small networks where rapid growth can be expected in the near future. The switch can be used standalone for a group of heavy traffic users. You can connect computers directly to the switch's ports or connect other switches to the switch.

In this example, all computers connected directly or indirectly to the switch can share super high-speed applications on the Gigabit server. To expand the network, simply add more networking devices such as switches, routers, firewalls, print servers etc.

Figure 1 Backbone Application



1.1.2 Bridging Example

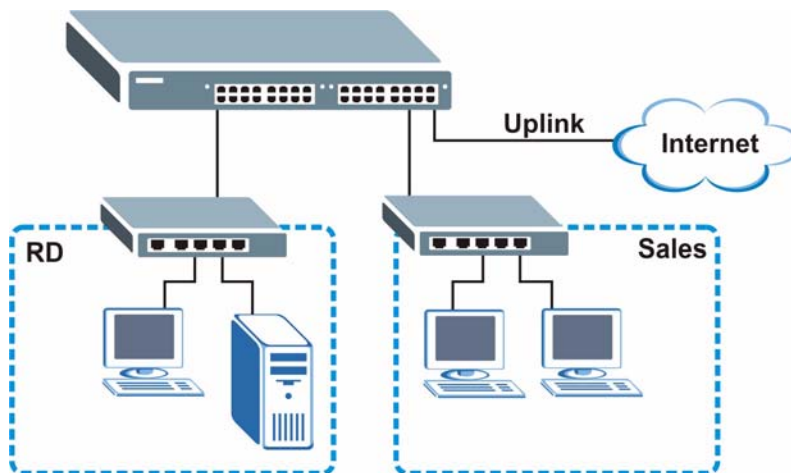
In this example application the switch is the ideal solution for different company departments to connect to the corporate backbone. It can alleviate bandwidth contention and eliminate server and network bottlenecks. All users that need high bandwidth can connect to high-speed department servers via the switch. You can provide a super-fast uplink connection by installing the transceiver(s) in the mini-GBIC slots.

Moreover, the switch eases supervision and maintenance by allowing network managers to centralize multiple servers at a single location.



Full-duplex mode operation only applies to point-to-point access (for example, when attaching the switch to a workstation, server, or another switch). When connecting to hubs, use a standard cascaded connection set at half-duplex operation.

Figure 2 Bridging Application



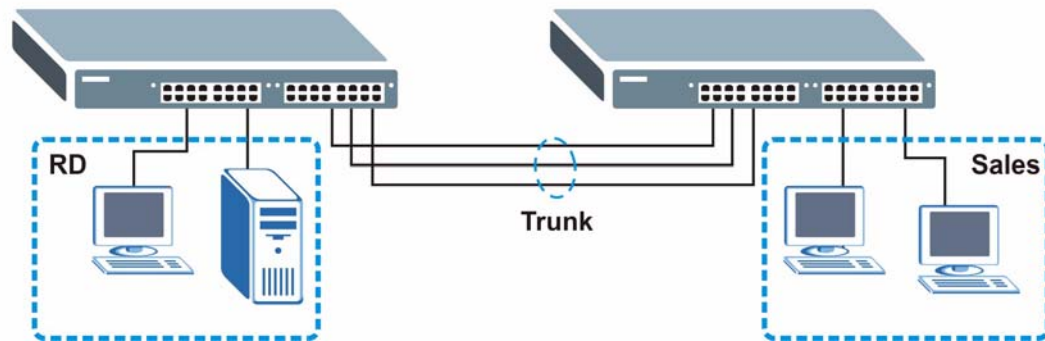
1.1.3 High Performance Switched Workgroup Example

The switch is ideal for connecting two power workgroups that need high bandwidth. In the following example, use trunking to connect these two power workgroups.

Switching to higher-speed LANs such as FDDI or ATM is not feasible for most people due to the expense of replacing all existing Ethernet cables and adapter cards, restructuring your network and complex maintenance.

The switch can provide the same bandwidth as FDDI and ATM at much lower cost while still being able to use existing adapters and switches. Moreover, the current LAN structure can be retained as all ports can freely communicate with each other.

Figure 3 High Performance Switched Application

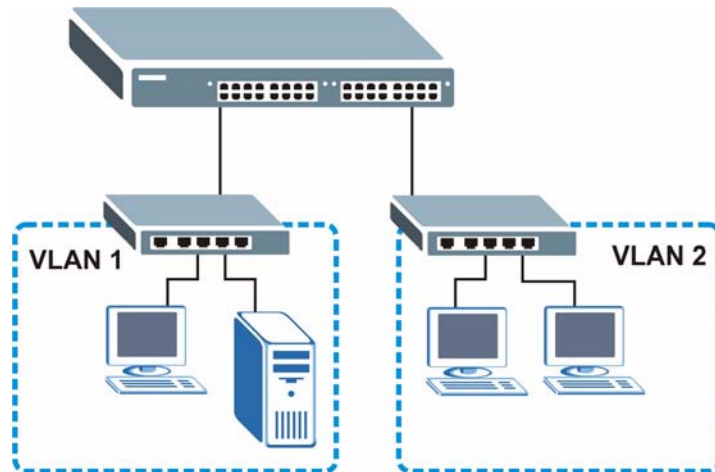


1.1.4 IEEE 802.1Q VLAN Application Examples

This section shows a workgroup and a shared server example using 802.1Q tagged VLANs. For more information on VLANs, see the Switch Setup section and the VLAN Setup chapter in this User's Guide. A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Stations on a logical network belong to one group. A station can belong to more than one group. With VLAN, a station cannot directly talk to or hear from stations that are not in the same group(s) unless such traffic first goes through a router.

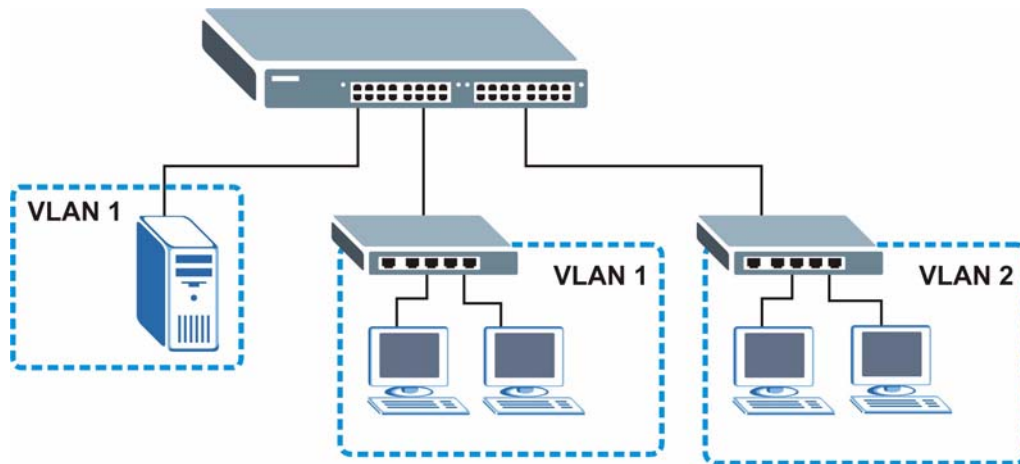
1.1.4.1 Tag-based VLAN Workgroup Example

Ports in the same VLAN group share the same broadcast domain thus increase network performance through reduced broadcast traffic. VLAN groups can be modified at any time by adding, moving or changing ports without any re-cabling.

Figure 4 Tag-based VLAN Application

1.1.4.2 VLAN Shared Server Example

Shared resources such as a server can be used by all ports in the same VLAN as the server, as shown in the following example. In this example, only ports that need access to the server need belong to VLAN 1 while they can belong to other VLAN groups too.

Figure 5 Shared Server Using VLAN Example

1.2 Ways to Manage the Switch

Use any of the following methods to manage the switch.

- Web Configurator. This is recommended for everyday management of the switch using a (supported) web browser. See [Chapter 4 on page 53](#).
- Command Line Interface. Line commands offer an alternative to the web configurator and in some cases are necessary to configure advanced features. See [Chapter 32 on page 207](#).
- FTP. Use FTP for firmware upgrades and configuration backup/restore. See [Section 24.8 on page 171](#).

- SNMP. The switch can be monitored by an SNMP manager. See [Section 25.3 on page 176](#).
- Cluster Management. Cluster Management allows you to manage multiple switches through one switch, called the cluster manager. See [Chapter 28 on page 193](#).

1.3 Good Habits for Managing the switch

Do the following things regularly to make the switch more secure and to manage the switch more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the switch to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the switch. You could simply restore your last configuration.

Hardware Installation and Connection

This chapter shows you how to install and connect the switch.

2.1 Installation Scenarios

The switch can be placed on a desktop or rack-mounted on a standard EIA rack. Use the rubber feet in a desktop installation and the brackets in a rack-mounted installation.

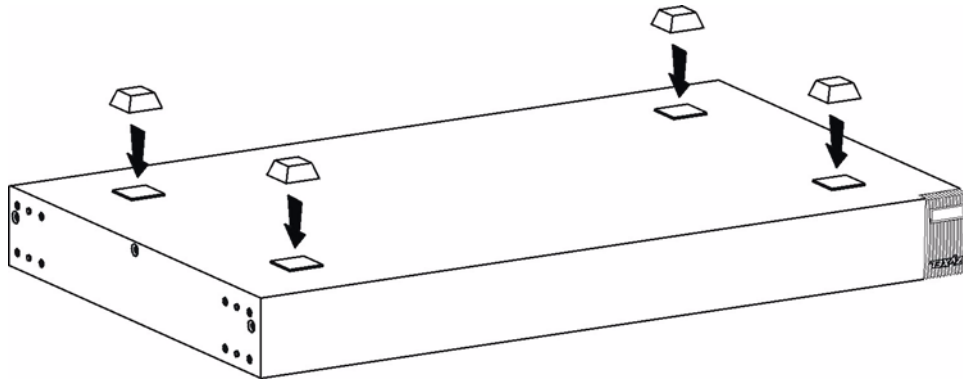


For proper ventilation, allow at least 4 inches (10 cm) of clearance at the front and 3.4 inches (8 cm) at the back of the switch. This is especially important for enclosed rack installations.

2.2 Desktop Installation Procedure

- 1 Make sure the switch is clean and dry.
- 2 Set the switch on a smooth, level surface strong enough to support the weight of the switch and the connected cables. Make sure there is a power outlet nearby.
- 3 Make sure there is enough clearance around the switch to allow air circulation and the attachment of cables and the power cord.
- 4 Remove the adhesive backing from the rubber feet.
- 5 Attach the rubber feet to each corner on the bottom of the switch. These rubber feet help protect the switch from shock or vibration and ensure space between devices when stacking.

Figure 6 Attaching Rubber Feet



Do NOT block the ventilation holes. Leave space between devices when stacking.

2.3 Mounting the Switch on a Rack

The switch can be mounted on an EIA standard size, 19-inch rack or in a wiring closet with other equipment. Follow the steps below to mount your switch on a standard EIA rack using a rack-mounting kit.

2.3.1 Rack-mounted Installation Requirements

- Two mounting brackets.
- Eight M3 flat head screws and a #2 Philips screwdriver.
- Four M5 flat head screws and a #2 Philips screwdriver.



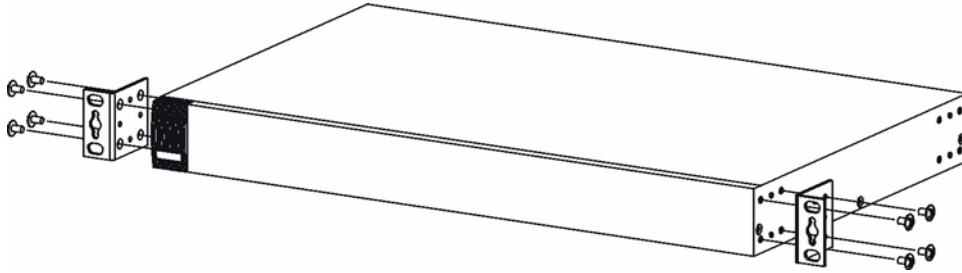
Failure to use the proper screws may damage the unit.

2.3.1.1 Precautions

- Make sure the rack will safely support the combined weight of all the equipment it contains.
- Make sure the position of the switch does not make the rack unstable or top-heavy. Take all necessary precautions to anchor the rack securely before installing the unit.

2.3.2 Attaching the Mounting Brackets to the Switch

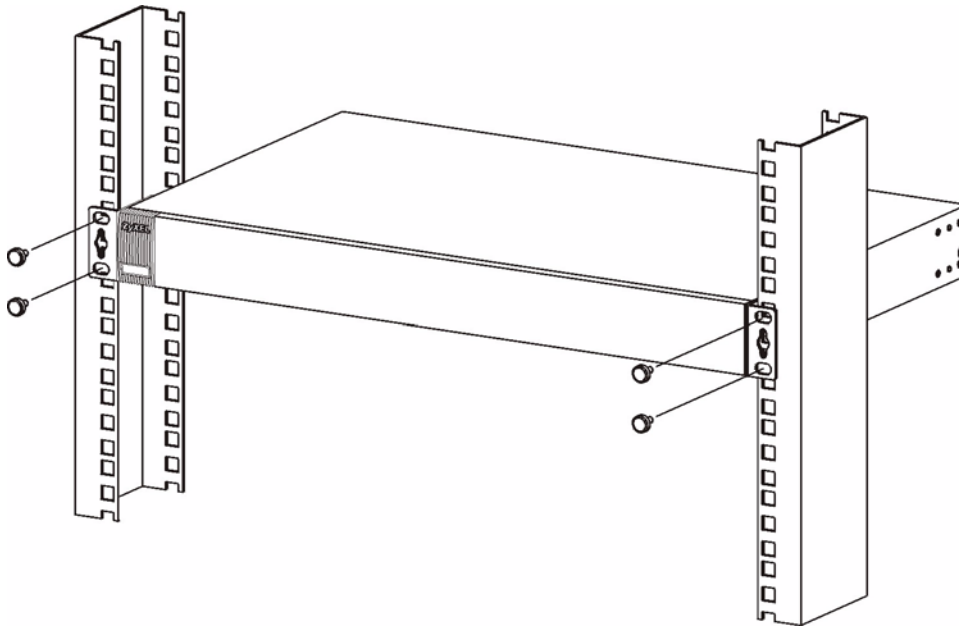
- 1 Position a mounting bracket on one side of the switch, lining up the four screw holes on the bracket with the screw holes on the side of the switch.

Figure 7 Attaching the Mounting Brackets

- 2 Using a #2 Philips screwdriver, install the M3 flat head screws through the mounting bracket holes into the switch.
- 3 Repeat steps 1 and 2 to install the second mounting bracket on the other side of the switch.
- 4 You may now mount the switch on a rack. Proceed to the next section.

2.3.3 Mounting the Switch on a Rack

- 1 Position a mounting bracket (that is already attached to the switch) on one side of the rack, lining up the two screw holes on the bracket with the screw holes on the side of the rack.

Figure 8 Mounting the Switch on a Rack

- 2 Using a #2 Philips screwdriver, install the M5 flat head screws through the mounting bracket holes into the rack.
- 3 Repeat steps 1 and 2 to attach the second mounting bracket on the other side of the rack.

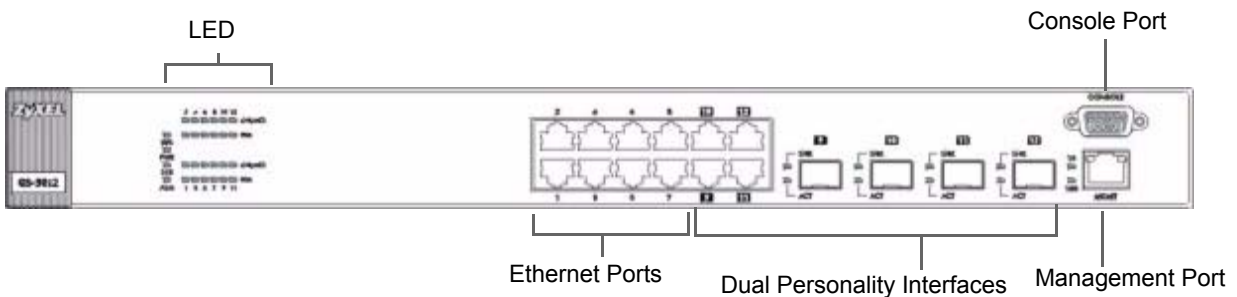
Hardware Overview

This chapter describes the front panel and rear panel of the switch and shows you how to make the hardware connections.

3.1 Front Panel

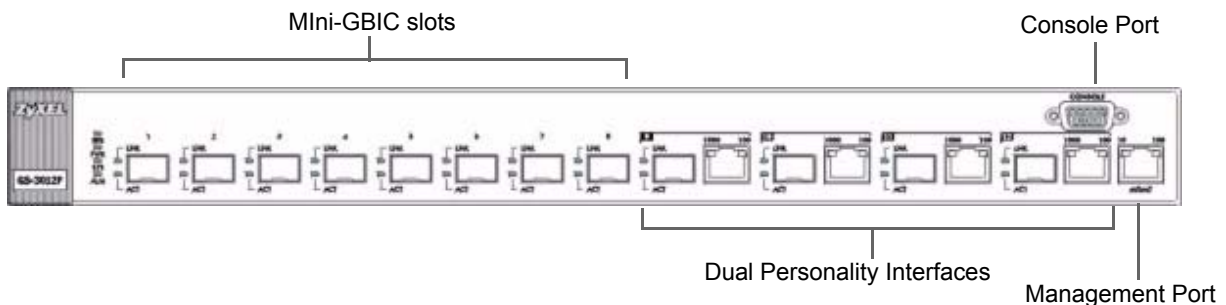
The following figure shows the front panel of the GS-3012. The front panel contains the switch LEDs, 8 RJ-45 gigabit ports, four dual personality interfaces each consisting of a mini-GBIC slot and an RJ-45 gigabit port as well as a console and management port for local management.

Figure 9 Front Panel: GS-3012



The following figure shows the front panel of the GS-3012F. The front panel contains the switch LEDs, 8 mini-GBIC slots, four dual personality interfaces each consisting of a mini-GBIC slot and an RJ-45 gigabit port as well as a console and management port for local management.

Figure 10 Front Panel: GS-3012F



The following table describes the port labels on the front panel.

Table 1 Front Panel Connections

LABEL	DESCRIPTION
8 100/1000 Mbps RJ-45 Ethernet Ports (GS-3012)	Connect these 1Gbps Electrical Ethernet ports to high-bandwidth backbone network Ethernet switches or use them to daisy-chain other switches.
8 Mini-GBIC Slots (GS-3012F)	Use mini-GBIC transceivers in these slots for fiber-optic connections to backbone Ethernet switches.
Four Dual Personality Interfaces	Each interface has one 1000 Base-T copper RJ-45 port and one Small Form-Factor Pluggable (SFP) fiber port, with one port active at a time.
	<ul style="list-style-type: none"> • 4 100/1000 Mbps RJ-45 Gigabit Ports: Connect these Gigabit Ethernet ports to high-bandwidth backbone network Ethernet switches. • 4 Mini-GBIC Slots: Use mini-GBIC transceivers in these slots for fiber-optic connections to backbone Ethernet switches.
Console Port	The console port is for local configuration of the switch.
Management Port	Connect to a computer using an RJ-45 Ethernet cable for local configuration of the switch.

3.1.1 Console Port

For local management, you can use a computer with terminal emulation software configured to the following parameters:

- VT100
- Terminal emulation
- 9600 bps
- No parity, 8 data bits, 1 stop bit
- No flow control

Connect the male 9-pin end of the console cable to the console port of the GS-3012F switch. Connect the female end to a serial port (COM1, COM2 or other COM port) of your computer.

3.1.2 Gigabit Ports

The GS-3012 has 100/1000Mbps auto-negotiating, auto-crossover Gigabit ports. The speed of the Gigabit ports can be 100Mbps or 1000Mbps and the duplex mode can be half duplex (for 100 Mbps) or full duplex. The GS-3012's mini-GBIC slots are paired with Gigabit ports.

The GS-3012F has 100/1000Mbps auto-negotiating, auto-crossover Gigabit ports. The speed of the Gigabit ports can be 100Mbps or 1000Mbps and the duplex mode can be half duplex (for 100 Mbps) or full duplex. The GS-3012F's Gigabit ports are paired with mini-GBIC slots.

The switch uses up to one connection for each mini-GBIC and Gigabit pair. The mini-GBIC ports have priority over the Gigabit ports. This means that if a mini-GBIC port and the corresponding Gigabit port are connected at the same time, the Gigabit port will be disabled.

When auto-negotiation is turned on, a Gigabit port negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer Ethernet port does not support auto-negotiation or turns off this feature, the switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the switch's auto-negotiation is turned off, a Gigabit port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer Ethernet port are the same in order to connect.

3.1.2.1 Default Ethernet Negotiation Settings

The factory default negotiation settings for the Gigabit ports on the GS-3012 are:

- Speed: Auto
- Duplex: Auto
- Flow control: Off
- Link Aggregation: Disabled

The factory default negotiation settings for the Gigabit ports on the GS-3012F are:

- Speed: Auto
- Duplex: Auto
- Flow control: Off
- Link Aggregation: Disabled

3.1.2.2 Auto-crossover

All ports are auto-crossover, that is auto-MDIX ports (Media Dependent Interface Crossover), so you may use either a straight-through Ethernet cable or crossover Ethernet cable for all Gigabit port connections. Auto-crossover ports automatically sense whether they need to function as crossover or straight ports, so crossover cables can connect both computers and switches/hubs.

3.1.3 Mini-GBIC Slots

These are slots for mini-GBIC (Gigabit Interface Converter) transceivers. A transceiver is a single unit that houses a transmitter and a receiver. The GS does not come with transceivers. You must use transceivers that comply with the Small Form-factor Pluggable (SFP) Transceiver MultiSource Agreement (MSA). See the SFF committee's INF-8074i specification Rev 1.0 for details.

You can change transceivers while the switch is operating. You can use different transceivers to connect to Ethernet switches with different types of fiber-optic connectors.



To avoid possible eye injury, do not look into an operating fiber-optic module's connectors.

- Type: SFP connection interface
- Connection speed: 1 Gigabit per second (Gbps)

3.1.3.1 Transceiver Installation

Use the following steps to install a mini-GBIC transceiver (SFP module).

- 1 Insert the transceiver into the slot with the exposed section of PCB board facing down.
- 2 Press the transceiver firmly until it clicks into place.
- 3 The switch automatically detects the installed transceiver. Check the LEDs to verify that it is functioning properly.
- 4 Close the transceiver's latch (latch styles vary).
- 5 Connect the fiber optic cables to the transceiver.

Figure 11 Transceiver Installation Example

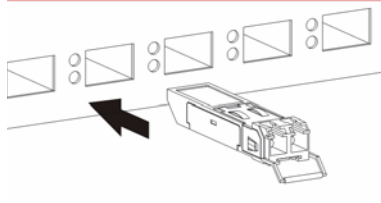
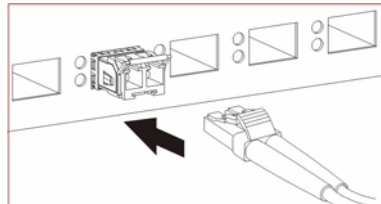


Figure 12 Connecting the Fiber Optic Cables



3.1.3.2 Transceiver Removal

Use the following steps to remove a mini-GBIC transceiver (SFP module).

- 1 Remove the fiber optic cables from the transceiver.
- 2 Open the transceiver's latch (latch styles vary).
- 3 Pull the transceiver out of the slot.

Figure 13 Removing the Fiber Optic Cables

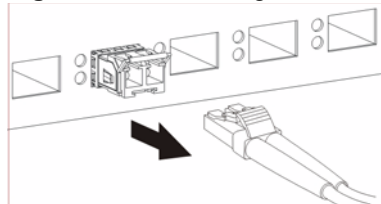


Figure 14 Opening the Transceiver's Latch Example

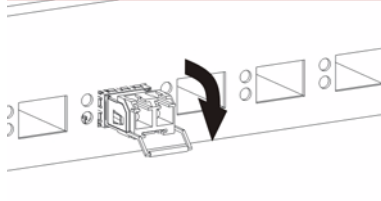
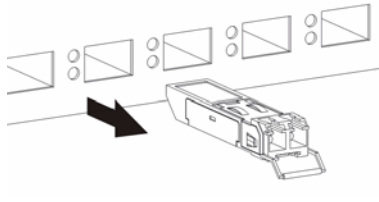


Figure 15 Transceiver Removal Example

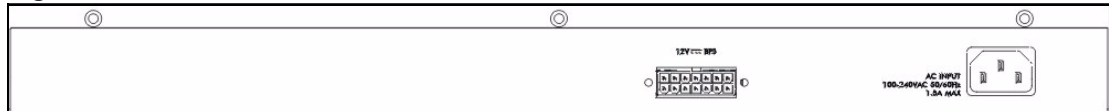
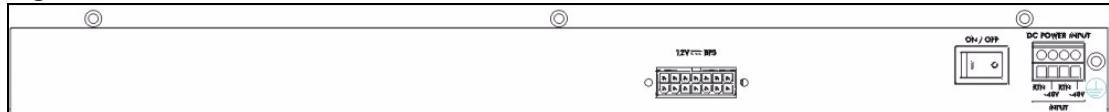
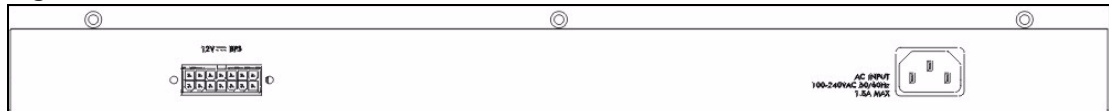
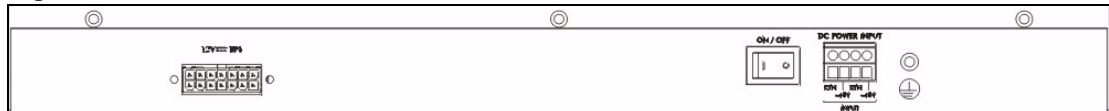
3.1.4 Management Port

The **MGMT** (management) port is used for local management. Connect directly to this port using an Ethernet cable. You can configure the switch via Telnet or the web configurator.

The default IP address of the management port is 192.168.0.1 with a subnet mask of 255.255.255.0.

3.2 Rear Panel

The following figures show the rear panels of the GS-3012 AC and DC power models followed by the GS-3012F AC and DC power models. The rear panel contains the power receptacle and a connector for external backup power supply.

Figure 16 Rear Panel: GS-3012 AC Power Model**Figure 17** Rear Panel: GS-3012 DC Power Model**Figure 18** Rear Panel: GS-3012F AC Power Model**Figure 19** Rear Panel: GS-3012F DC Power Model

3.2.1 Power Connector



Make sure you are using the correct power source as shown on the panel.

To connect the power to the AC power model, insert the female end of power cord to the power receptacle on the rear panel. Connect the other end of the supplied power cord to a 100~240VAC/1.5A power outlet. Make sure that no objects obstruct the airflow of the fans (located on the side of the unit).

The DC power models require DC power supply input of -48 VDC to -60 VDC. The GS-3012 DC power model requires 1.5A Max. The GS-3012F DC power model requires 1.25A Max. To connect the power to the unit, insert the one end of the supplied power cord to the power receptacle on the rear panel and the other end to a power outlet.

3.3 LEDs

After you connect the power to the switch, view the LEDs to ensure proper functioning of the switch and as an aid in troubleshooting.

Table 2 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
BPS	Green	Blinking	The system is receiving power from the backup power supply.
		On	The backup power supply is connected and active.
		Off	The backup power supply is not ready or not active.
	Amber	Blinking	The system cannot get power from the backup power supply.
PWR	Green	On	The system is turned on.
		Off	The system is off.
SYS	Green	Blinking	The system is rebooting and performing self-diagnostic tests.
		On	The system is on and functioning properly.
		Off	The power is off or the system is not ready/malfunctioning.
ALM	Red	On	There is a hardware failure.
		Off	The system is functioning normally.
Mini-GBIC Slots			
LNK	Green	On	The link to this port is up.
		Off	The link to this port is not connected.
ACT	Green	Blinking	This port is receiving or transmitting data.
Gigabit Ports			
LNK/ACT (GS-3012)	Green	Blinking	The system is transmitting/receiving to/from an Ethernet network.
		On	The link to a 1000 Mbps Ethernet network is up.
	Amber	Blinking	The system is transmitting/receiving to/from an Ethernet network.
		On	The link to a 100 Mbps Ethernet network is up.
	Off	The link to an Ethernet network is down.	
FDX (GS-3012)	Amber	On	The Gigabit port is negotiating in full-duplex mode.
		Off	The Gigabit port is negotiating in half-duplex mode.

Table 2 LED Descriptions (continued)

LED	COLOR	STATUS	DESCRIPTION
1000 (GS-3012F)	Green	Blinking	The system is transmitting/receiving to/from an Ethernet network.
		On	The link to a 1000 Mbps Ethernet network is up.
		Off	The link to a 1000 Mbps Ethernet network is down.
100 (GS-3012F)	Amber	Blinking	The system is transmitting/receiving to/from an Ethernet network.
		On	The link to a 100 Mbps Ethernet network is up.
		Off	The link to a 100 Mbps Ethernet network is down.
MGMT			
10	Green	Blinking	The system is transmitting/receiving to/from an Ethernet device.
		On	The port is connected at 10Mbps.
		Off	The port is not connected at 10Mbps or to an Ethernet device.
100	Amber	Blinking	The system is transmitting/receiving to/from an Ethernet device.
		On	The port is connected at 100Mbps.
		Off	The port is not connected at 100Mbps or to an Ethernet device.

3.4 Configuring the Switch

You may use the embedded web configurator or command line interface to configure the switch. If you're using the web configurator, you need Internet Explorer 5.5 and later or Netscape Navigator 6 and later.

You can access the command line interface using a terminal emulation program on a computer connected to the switch console port (see [Section 3.1.1 on page 44](#)) or access the switch using Telnet.

The next part of this guide discusses configuring the switch using the web configurator.

PART II

Basic Settings

Introducing the Web Configurator (53)

Initial Setup Example (61)

System Status and Port Details (65)

Basic Setting (71)

Introducing the Web Configurator

This section introduces the configuration and functions of the web configurator.

4.1 Introduction

The embedded web configurator allows you to manage the switch from anywhere through a standard browser such as Microsoft Internet Explorer or Netscape Navigator.



Use Internet Explorer 5.5 and later or Netscape Navigator 6 and later versions.

4.2 System Login

- 1 Start your Internet Explorer or Netscape Navigator web browser.
- 2 Type “http://” and the IP address of the switch (for example, the default for the management port is 192.168.0.1 and for the switch port is 192.168.1.1) in the **Location** or **Address** field. Press **Enter**.
- 3 The login screen appears. The default username is **admin** and the associated default password is **1234**. The date and time display as shown if you have not configured a time server nor manually entered a time and date in the **General Setup** screen.

Figure 20 Web Configurator: login

Enter Network Password

Please type your user name and password.

Site: 192.168.1.1

Realm: GS-3012F at Thu Jan 29 10:24:03 2004

User Name

Password

Save this password in your password list

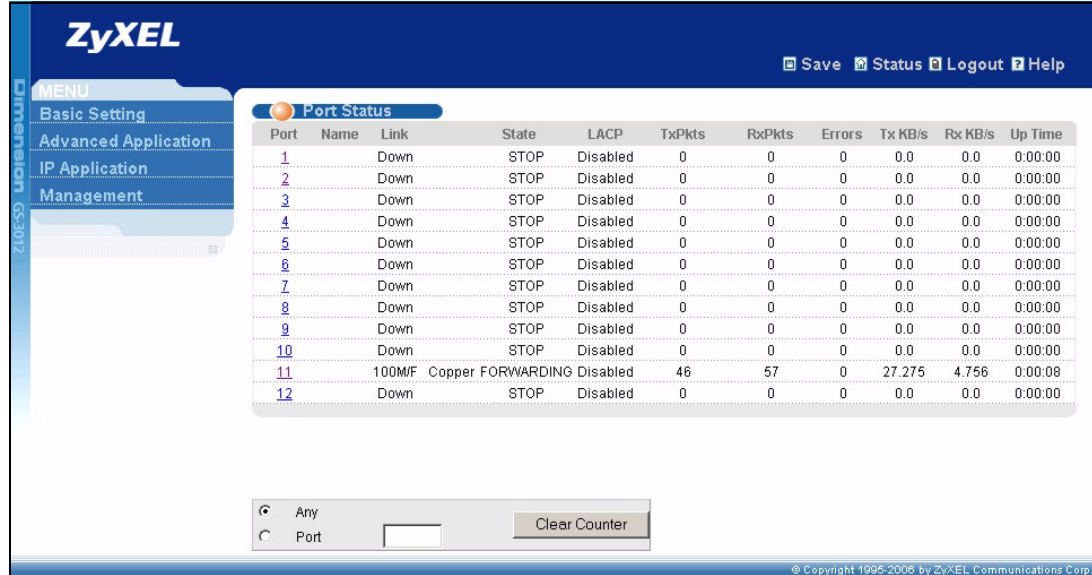
OK Cancel

- 4 Click **OK** to view the first web configurator screen.

4.3 Status Screen

The **Status** screen is the first web configurator screen you see after you log in. The following figure shows the navigating components of a web configurator screen.

Figure 21 Web Configurator Home Screen (Status)



In the navigation panel, click a main link to reveal a list of submenu links.

Table 3 Navigation Panel Sub-links Overview

BASIC SETTING	ADVANCED APPLICATION	IP APPLICATION	MANAGEMENT
<ul style="list-style-type: none"> System Info General Setup Switch Setup IP Setup Port Setup 	<ul style="list-style-type: none"> VLAN Static MAC Forwarding Filtering Spanning Tree Protocol Bandwidth Control Broadcast Storm Control Mirroring Link Aggregation Port Authentication Port Security Classifier Policy Rule Queueing Method Multicast DHCP Relay 	<ul style="list-style-type: none"> Static Routing 	<ul style="list-style-type: none"> Maintenance Access Control Diagnostic Syslog Cluster Management MAC Table ARP Table Configure Clone

The following table lists the various web configurator screens within the sub-links.

Table 4 Web Configurator Screen Sub-links Details

BASIC SETTING	ADVANCED APPLICATION	IP APPLICATION	MANAGEMENT
System Info General Setup Switch Setup IP Setup Port Setup	VLAN Status VLAN Port Setting Static VLAN Port Based VLAN Setup Static MAC Forwarding Filtering Spanning Tree Protocol Spanning Tree Protocol Status Spanning Tree Configuration Multiple Rapid Spanning Tree Protocol Status Multiple Rapid Spanning Tree Configuration Bandwidth Control Broadcast Storm Control Mirroring Link Aggregation Status Link Aggregation Configuration Port Authentication RADIUS 802.1x Port Security Classifier Policy Rule Queuing Method Multicast Multicast Status Multicast Setting IGMP Filtering Profile MVR DHCP Relay	Static Routing	Maintenance Firmware Upgrade Restore Configuration Backup Configuration Load Factory Default Save Configuration Reboot System Access Control SNMP Logins Service Access Control Remote Management Diagnostic Syslog Syslog Setup Syslog Server Setup Cluster Management Status Cluster Management Configuration MAC Table ARP Table Configure Clone

The following table summarizes these sub-links in the navigation panel.

Table 5 Navigation Panel Sub-link Descriptions

LABEL	DESCRIPTION
Basic Setting	
System Info	This link takes you to a screen that displays general system and hardware monitoring information.
General Setup	This link takes you to a screen where you can configure general identification information about the switch.
Switch Setup	This link takes you to a screen where you can set up global switch parameters such as VLAN type, MAC address learning, GARP and priority queues.
IP Setup	This link takes you to a screen where you can configure the IP address, subnet mask (necessary for switch management) and DNS (domain name server).

Table 5 Navigation Panel Sub-link Descriptions (continued)

LABEL	DESCRIPTION
Port Setup	This link takes you to screens where you can configure settings for individual switch ports.
Advanced Application	
VLAN	This link takes you to screens where you can configure port-based or 802.1Q VLAN (depending on what you configured in the Switch Setup menu).
Static MAC Forwarding	This link takes you to screens where you can configure static MAC addresses for a port. These static MAC addresses do not age out.
Filtering	This link takes you to a screen to set up filtering rules.
Spanning Tree Protocol	This link takes you to screens where you can configure spanning tree settings to prevent network loops.
Bandwidth Control	This link takes you to screens where you can cap the maximum bandwidth allowed from specified source(s) to specified destination(s).
Broadcast Storm Control	This link takes you to a screen to set up broadcast filters.
Mirroring	This link takes you to screens where you can copy traffic from one port or ports to another port in order that you can examine the traffic from the first port without interference
Link Aggregation	This link takes you to a screen where you can logically trunk physical links to form one logical, higher-bandwidth link.
Port Authentication	This link takes you to a screen where you can configure RADIUS (Remote Authentication Dial-In User Service), a protocol for user authentication that allows you to use an external server to validate an unlimited number of users.
Port Security	This link takes you to a screen where you can activate MAC address learning and set the maximum number of MAC addresses to learn on a port.
Classifier	This link takes you to a screen where you can configure classifiers.
Policy Rule	This link takes you to a screen where you can configure policy rules.
Queuing Method	This link takes you to a screen where you can configure SPQ or WRR with associated queue weights for each port.
Multicast	This link takes you to a screen where you can configure various multicast features and create multicast VLANs.
DHCP Relay	This link takes you to a screen where you can configure DHCP relay information.
IP Application	
Static Routing	This link takes you to screens where you can configure static routes. A static route defines how the switch should forward traffic by configuring the TCP/IP parameters manually.
Management	
Maintenance	This link takes you to screens where you can perform firmware and configuration file maintenance as well as reboot the system.
Access Control	This link takes you to screens where you can change the system login password and configure SNMP and remote management.
Diagnostic	This link takes you to screens where you can view system logs and test port(s).
Syslog	This link takes you to screens where you can configure the device's system logging settings.
Cluster Management	This link takes you to a screen where you can configure clustering management and view its status.

Table 5 Navigation Panel Sub-link Descriptions (continued)

LABEL	DESCRIPTION
MAC Table	This link takes you to a screen where you can view the MAC addresses (and types) of devices attached to what ports and VLAN IDs.
ARP Table	This link takes you to a screen where you can view the MAC addresses – IP address resolution table.
Configure Clone	This link takes you to a screen where you can copy attributes of one port to other ports.

4.3.1 Change Your Password

After you log in for the first time, it is recommended you change the default Administrator password in the **Logins** screen. Click **Advanced Application**, **Access Control** and then **Logins** to display the next screen.

Figure 22 Web Configurator: Change Password at Login

Logins [Access Control](#)

Administrator

Old Password

New Password

Retype to confirm

Please record your new password whenever you change it. The system will lock you out if you have forgotten your password.

Edit Logins

Login	User Name	Password	Retype to confirm
1	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>

Apply Cancel

4.4 Switch Lockout

You could block yourself (and all others) from using in-band-management (managing through the data ports) by doing one of the following:

- 1 Deleting the management VLAN (default is VLAN 1).
- 2 Deleting all port-based VLANs with the CPU port as a member. The “CPU port” is the management port of the switch.
- 3 Filtering all traffic to the CPU port.
- 4 Disabling all ports.

- 5 Assigning minimum bandwidth to the CPU port. If you limit bandwidth to the CPU port, you may find that the switch performs sluggishly or not at all.



Be careful not to lock yourself and others out of the switch. If you do lock yourself out, try using out-of-band management (via the management port) to configure the switch.

4.5 Resetting the Switch

If you lock yourself (and others) from the switch or forget the switch password, you will need to reload the factory-default configuration file.

4.5.1 Reload the Configuration File

Uploading the factory-default configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all previous configurations and the speed of the console port will be reset to the default of 9600bps with 8 data bit, no parity, one stop bit and flow control set to none. The password will also be reset to “1234” and the IP address to 192.168.1.1.

To upload the configuration file, do the following:

- 1 Connect to the console port using a computer with terminal emulation software. See the chapter on hardware connections for details.
- 2 Disconnect and reconnect the switch’s power to begin a session. When you reconnect the switch’s power, you will see the initial screen.
- 3 When you see the message “Press any key to enter Debug Mode within 3 seconds” press any key to enter debug mode.
- 4 Type `atlc` after the “Enter Debug Mode” message.
- 5 Wait for the “Starting XMODEM upload” message before activating XMODEM upload on your terminal.
- 6 After a successful configuration file upload, type `atgo` to finish starting the switch.

Figure 23 Resetting the Switch: Via Console Port

```

Bootbase Version: V3.00 | 01/14/2005 22:06:52
RAM:Size = 32 Mbytes
DRAM POST: Testing: 32768K OK
DRAM Test SUCCESS !
FLASH: Intel 32M

ZyNOS Version: V3.70(LR.0)b0 | 10/20/2006 14:53:11
Press any key to enter debug mode within 3 seconds.
.....
Enter Debug Mode
sysname> atlc
Starting XMODEM upload (CRC mode)....
CCCCCCCCCCCCCCCC
Total 393216 bytes received.
Erasing..
.....
OK
sysname> atgo

```

The switch is now reinitialized with a default configuration file including the default password of “1234”.

4.5.2 Logging Out of the Web Configurator

Click **Logout** in a screen to exit the web configurator. You have to log in with your password again after you log out. This is recommended after you finish a management session both for security reasons and so as you don’t lock out other switch administrators.

Figure 24 Web Configurator: Logout Screen

4.5.3 Help

The web configurator’s online help has descriptions of individual screens and some supplementary information.

Click the **Help** link from a web configurator screen to view an online help description of that screen.

Initial Setup Example

This chapter shows how to set up the switch for an example network.

5.1 Overview

The following lists the configuration steps for the initial setup:

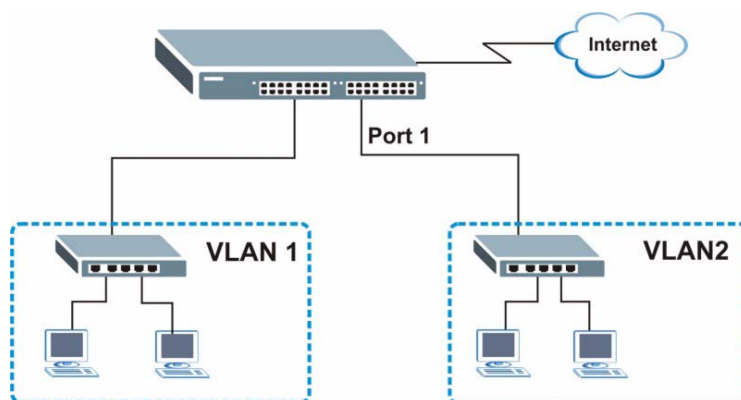
- Create a VLAN
- Set port VLAN ID
- Configure the switch IP management address

5.1.1 Creating a VLAN

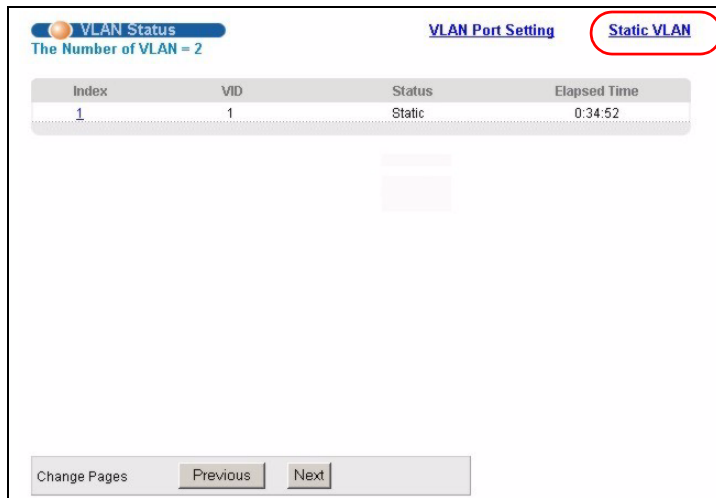
VLANs confine broadcast frames to the VLAN group in which the port(s) belongs. You can do this with port-based VLAN or tagged static VLAN with fixed port members.

In this example, you want to configure port 1 as a member of VLAN 2.

Figure 25 Initial Setup Network Example: VLAN



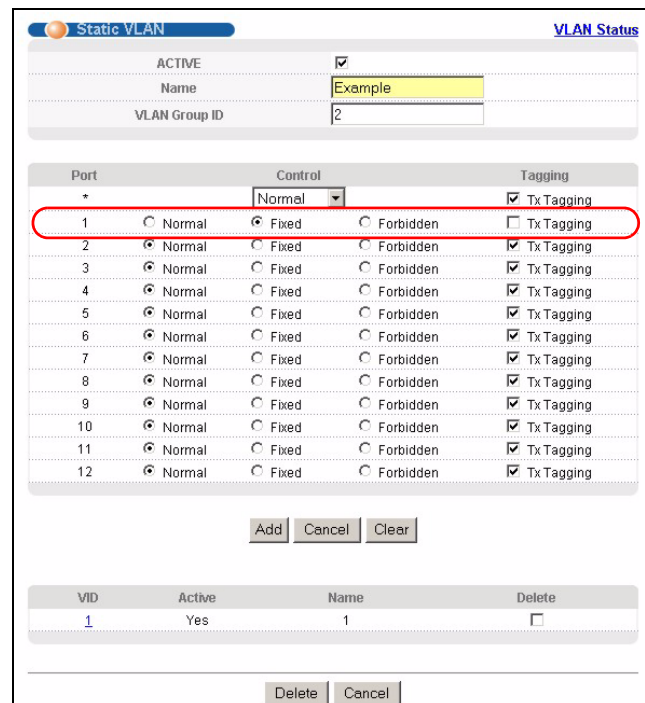
- 1 Click **Advanced Application** and **VLAN** in the navigation panel and click the **Static VLAN** link.



- 2 In the **Static VLAN** screen, select **ACTIVE**, enter a descriptive name in the **Name** field and enter 2 in the **VLAN Group ID** field for the **VLAN2** network.

Note: The **VLAN Group ID** field in this screen and the **VID** field in the **IP Setup** screen refer to the same VLAN ID.

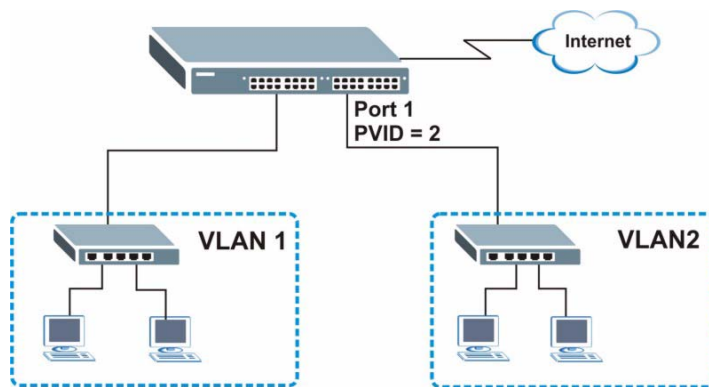
- 3 Since the **VLAN2** network is connected to port 1 on the switch, select **Fixed** to configure port 1 to be a permanent member of the VLAN only.
- 4 To ensure that VLAN-unaware devices (such as computers and hubs) can receive frames properly, clear the **TX Tagging** check box to set the switch to remove VLAN tags before sending.
- 5 Click **Add** to save the settings to the run-time memory. Settings in the run-time memory are lost when the switch's power is turned off.



5.1.2 Setting Port VID

Use PVID to add a tag to incoming untagged frames received on that port so that the frames are forwarded to the VLAN group that the tag defines.

In the example network, configure 2 as the port VID on port 1 so that any untagged frames received on that port get sent to VLAN 2.

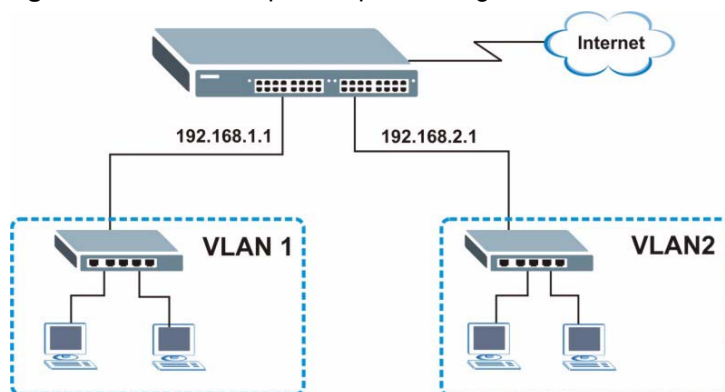
Figure 26 Initial Setup Network Example: Port VID

- 1 Click **Advanced Applications** and **VLAN** in the navigation panel. Then click the **VLAN Port Setting** link.
- 2 Enter 2 in the **PVID** field for port 1 and click **Apply** to save your changes back to the run-time memory. Settings in the run-time memory are lost when the switch's power is turned off.

Port	Ingress Check	PVID	GVRP	Acceptable Frame Type	VLAN Trunking
1	<input type="checkbox"/>	2	<input type="checkbox"/>	All	<input type="checkbox"/>
2	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
3	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
4	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
5	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
6	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
7	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
8	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
9	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
10	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
11	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
12	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>

5.2 Configuring Switch Management IP Address

The default management IP address of the switch is 192.168.1.1. You can configure another IP address in a different subnet for management purposes. The following figure shows an example.

Figure 27 Initial Setup Example: Management IP Address

- 1 Connect your computer to any Ethernet port on the switch. Make sure your computer is in the same subnet as the switch.
- 2 Open your web browser and enter 192.168.1.1 (the default IP address) in the address bar to access the web configurator. See [Section 4.2 on page 53](#) for more information.
- 3 Click **Basic Setting** and **IP Setup** in the navigation panel.
- 4 Configure the related fields in the **IP Setup** screen.
- 5 For the **VLAN2** network, enter 192.168.2.1 as the IP address and 255.255.255.0 as the subnet mask.
- 6 In the **VID** field, enter the ID of the VLAN group to which you want this management IP address to belong. This is the same as the VLAN ID you configure in the **Static VLAN** screen.
- 7 Click **Add** to save your changes back to the run-time memory. Settings in the run-time memory are lost when the switch's power is turned off.

The screenshot displays the 'IP Setup' configuration page. At the top, there is a 'Domain Name Server' field set to '0.0.0.0' and a 'Default Management' section with radio buttons for 'In-band' (selected) and 'Out-of-band'. Below this, the 'In-band Management IP Address' section has radio buttons for 'DHCP Client' and 'Static IP Address' (selected). Under 'Static IP Address', there are fields for 'IP Address' (192.168.1.1), 'IP Subnet Mask' (255.255.255.0), and 'Default Gateway' (0.0.0.0). A 'VID' field is set to '1'. The 'Out-of-band Management IP Address' section has similar fields for 'IP Address' (192.168.0.1), 'IP Subnet Mask' (255.255.255.0), and 'Default Gateway' (0.0.0.0). 'Apply' and 'Cancel' buttons are located below these sections.

The 'In-band IP Addresses' section is highlighted with a red rounded rectangle. It contains a table with the following data:

IP Address	IP Subnet Mask	VID	Default Gateway
192.168.2.1	255.255.255.0	2	0.0.0.0

Below the table are 'Add' and 'Cancel' buttons. At the bottom of the page, there is a table with columns: 'Index', 'IP Address', 'IP Subnet Mask', 'VID', 'Default Gateway', and 'Delete'. Below this table are 'Delete' and 'Cancel' buttons.

System Status and Port Details

This chapter describes the system status (web configurator home page) and port details screens.

6.1 About System Statistics and Information

The status screen of the web configurator displays a port statistical summary with links to each port showing statistical details.

6.2 Port Status Summary

To view the port statistics, click **Status** in all web configurator screens to display the **Port Status** screen as shown next.

Figure 28 Port Status

Port	Name	Link	State	LACP	TxPkts	RxPkts	Errors	Tx KB/s	Rx KB/s	Up Time
1		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
2		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
3		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
4		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
5		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
6		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
7		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
8		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
9		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
10		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
11	100M/F Copper	FORWARDING	Disabled	Disabled	244	415	0	3.777	2.864	0:01:41
12		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00

Any
 Port

The following table describes the labels in this screen.

Table 6 Port Status

LABEL	DESCRIPTION
Port	This identifies the Gigabit port. Click a port number to display the Port Details screen (refer to Figure 29 on page 67).
Name	This field displays the port name you configured in the Port Setup screen.
Link	This field displays the speed (either 10M for 10Mbps, 100M for 100Mbps or 1000M for 1000Mbps) and the duplex (F for full duplex or H for half duplex). It also shows the cable type (Copper or Fiber) for the combo ports.
State	If STP (Spanning Tree Protocol) is enabled, this field displays the STP state of the port (see Section 11.1.3 on page 105 for more information). If STP is disabled, this field displays FORWARDING if the link is up, otherwise, it displays STOP .
LACP	This field displays whether the Link Aggregation Control Protocol (LACP) has been enabled on the port.
TxPkts	This field shows the number of transmitted frames on this port.
RxPkts	This field shows the number of received frames on this port.
Errors	This field shows the number of received errors on this port.
Tx KB/s	This field shows the number of kilobytes per second transmitted on this port.
Rx KB/s	This field shows the number of kilobytes per second received on this port.
Up Time	This field shows the total amount of time in hours, minutes and seconds the port has been up.
Clear Counter	Select Any and then click Clear Counter to erase the recorded statistical information for all ports. Otherwise, select Port and enter a port number and then click Clear Counter to erase the recorded statistical information for that port.

6.2.1 Port Details

Click a number in the **Port** column in the **Status** screen to display individual port statistics. Use this screen to check status and detailed performance data about an individual port on the switch.

Figure 29 Status: Port Details

Port Details		Port Status
Port Info	Port NO.	11
	Name	
	Link	100MF Copper
	Status	FORWARDING
	LACP	Disabled
	TxPkts	71
	RxPkts	95
	Errors	0
	Tx KBs/s	0.0
	Rx KBs/s	0.0
	Up Time	0:11:33
TX Packet	TX Packets	71
	Multicast	0
	Broadcast	0
	Pause	0
	Tagged	0
RX Packet	RX Packets	95
	Multicast	0
	Broadcast	35
	Pause	0
	Control	0
TX Collision	Single	0
	Multiple	0
	Excessive	0
	Late	0
Error Packet	RX CRC	0
	Length	0
	Runt	0
Distribution	64	70
	65 to 127	31
	128 to 255	6
	256 to 511	13
	512 to 1023	5
	1024 to 1518	41
	Giant	0

The following table describes the labels in this screen.

Table 7 Status: Port Details

LABEL	DESCRIPTION
Port Info	
Port NO.	This field identifies the Gigabit port described in this screen.
Name	This field displays the port name you configured in the Port Setup screen.
Link	This field shows whether the port connection is down, and the speed/duplex mode. It also shows the cable type (Copper or Fiber) for the combo ports.
Status	If STP (Spanning Tree Protocol) is enabled, this field displays the STP state of the port (see Section 11.1.3 on page 105 for more information). If STP is disabled, this field displays FORWARDING if the link is up, otherwise, it displays STOP .
LACP	This field shows if LACP is enabled on this port or not.

Table 7 Status: Port Details (continued)

LABEL	DESCRIPTION
TxPkts	This field shows the number of transmitted frames on this port
RxPkts	This field shows the number of received frames on this port
Errors	This field shows the number of received errors on this port.
Tx KB/s	This field shows the number kilobytes per second transmitted on this port.
Rx KB/s	This field shows the number of kilobytes per second received on this port.
Up Time	This field shows the total amount of time the connection has been up.
Tx Packet The following fields display detailed information about frames transmitted.	
TX Packets	This field shows the number of good frames (unicast, multicast and broadcast) transmitted.
Multicast	This field shows the number of good multicast frames transmitted.
Broadcast	This field shows the number of good broadcast frames transmitted.
Pause	This field shows the number of 802.3x Pause frames transmitted.
Tagged	This field shows the number of frames with VLAN tags transmitted.
Rx Packet The following fields display detailed information about frames received.	
RX Packets	This field shows the number of good frames (unicast, multicast and broadcast) received.
Multicast	This field shows the number of good multicast frames received.
Broadcast	This field shows the number of good broadcast frames received.
Pause	This field shows the number of 802.3x Pause frames received.
Control	This field shows the number of control received (including those with CRC error) but it does not include the 802.3x Pause frames.
TX Collision The following fields display information on collisions while transmitting.	
Single	This is a count of successfully transmitted frames for which transmission is inhibited by exactly one collision.
Multiple	This is a count of successfully transmitted frames for which transmission was inhibited by more than one collision.
Excessive	This is a count of frames for which transmission failed due to excessive collisions. Excessive collision is defined as the number of maximum collisions before the retransmission count is reset.
Late	This is the number of times a late collision is detected, that is, after 512 bits of the frame have already been transmitted.
Error Packet The following fields display detailed information about frames received that were in error.	
RX CRC	This field shows the number of frames received with CRC (Cyclic Redundant Check) error(s).
Length	This field shows the number of frames received with a length that was out of range.
Runt	This field shows the number of frames received that were too short (shorter than 64 octets), including the ones with CRC errors.
Distribution This field shows the distribution of good packets (unicast, multicast and broadcast) received.	
64	This field shows the number of packets (including bad packets) received that were 64 octets in length.

Table 7 Status: Port Details (continued)

LABEL	DESCRIPTION
65-127	This field shows the number of packets (including bad packets) received that were between 65 and 127 octets in length.
128-255	This field shows the number of packets (including bad packets) received that were between 128 and 255 octets in length.
256-511	This field shows the number of packets (including bad packets) received that were between 256 and 511 octets in length.
512-1023	This field shows the number of packets (including bad packets) received that were between 512 and 1023 octets in length.
1024-1518	This field shows the number of packets (including bad packets) received that were between 1024 and 1518 octets in length.
Giant	This field shows the number of packets dropped because they were bigger than the maximum frame size.

Basic Setting

This chapter describes how to configure the **System Info**, **General Setup**, **Switch Setup**, **IP Setup** and **Port Setup** screens.

7.1 Introducing the Basic Setting Screens

The **System Info** screen displays general switch information (such as firmware version number) and hardware polling information (such as fan speeds). The **General Setup** screen allows you to configure general switch identification information. The **General Setup** screen also allows you to set the system time manually or get the current time and date from an external server when you turn on your switch. The real time is then displayed in the switch logs. The **Switch Setup** screen allows you to set up and configure global switch features. The **IP Setup** screen allows you to configure a switch IP address, subnet mask and DNS (domain name server) for management purposes.

7.2 System Information

In the navigation panel, click **Basic Setting** and then **System Info** to display the screen as shown. You can check the firmware version number and monitor the switch temperature, fan speeds and voltage in this screen.

Figure 30 System Info

System Info					
System Name	GS-3012				
ZyNOS F/W Version	V3.70(ABM.0)b3 10/03/2006				
Ethernet Address	00:a0:c5:da:d3:17				
Hardware Monitor					
Temperature Unit	<input type="button" value="C"/>				
Temperature (C)	Current	MAX	MIN	Threshold	Status
MAC	33.0	33.0	26.0	65.0	Normal
CPU	32.5	32.5	26.0	65.0	Normal
PHY	30.5	30.5	26.0	65.0	Normal
FAN Speed (RPM)	Current	MAX	MIN	Threshold	Status
FAN1	5763	5810	5625	4500	Normal
FAN2	5859	5859	5536	4500	Normal
FAN3	5716	5763	5580	4500	Normal
Voltage (V)	Current	MAX	MIN	Threshold	Status
2.5	2.560	2.560	2.560	+/-8%	Normal
1.25	1.232	1.232	1.232	+/-11%	Normal
3.3	3.312	3.312	3.296	+/-7%	Normal
12	11.977	12.038	11.977	+/-11%	Normal
5	4.999	4.999	4.999	+/-7%	Normal
1.3	1.296	1.296	1.296	+/-10%	Normal
1.25	1.232	1.232	1.232	+/-8%	Normal
BPS_12VIN	--	--	--	--	Absent

The following table describes the labels in this screen.

Table 8 System Info

LABEL	DESCRIPTION
System Name	This field displays the switch's model name.
ZyNOS F/W Version	This field displays the version number of the switch's current firmware including the date created.
Ethernet Address	This field refers to the Ethernet MAC (Media Access Control) address of the switch.
Hardware Monitor	
Temperature Unit	The switch has temperature sensors that are capable of detecting and reporting if the temperature rises above the threshold. You may choose the temperature unit (Centigrade or Fahrenheit) in this field.
Temperature	MAC , CPU and PHY refer to the location of the temperature sensors on the switch printed circuit board.
Current	This field displays the current temperature measured at this sensor.
MAX	This field displays the maximum temperature measured at this sensor.
MIN	This field displays the minimum temperature measured at this sensor.
Threshold	This field displays the upper temperature limit at this sensor.
Status	This field displays Normal for temperatures below the threshold and Error for those above.
Fan speed (RPM)	A properly functioning fan is an essential component (along with a sufficiently ventilated, cool operating environment) in order for the device to stay within the temperature threshold. Each fan has a sensor that is capable of detecting and reporting if the fan speed falls below the threshold shown.
Current	This field displays this fan's current speed in Revolutions Per Minute (RPM)

Table 8 System Info (continued)

LABEL	DESCRIPTION
MAX	This field displays this fan's maximum speed measured in Revolutions Per Minute (RPM).
MIN	This field displays this fan's minimum speed measured in Revolutions Per Minute (RPM).
Threshold	This field displays the minimum speed at which a normal fan should work.
Status	Normal indicates that this fan is functioning above the minimum speed. Error indicates that this fan is functioning below the minimum speed.
Voltage (V)	The power supply for each voltage has a sensor that is capable of detecting and reporting if the voltage falls out of the tolerance range.
Current	This is the current voltage reading.
MAX	This field displays the maximum voltage measured at this point.
MIN	This field displays the minimum voltage measured at this point.
Threshold	This field displays the minimum voltage at which the switch should work.
Status	Normal indicates that the voltage is within an acceptable operating range at this point; otherwise Error is displayed.

7.3 General Setup

Click **Basic Setting** and **General Setup** in the navigation panel to display the screen as shown. Use this screen to configure general settings such as the system name and time.

Figure 31 General Setup

General Setup

System Name: GS-3012F

Location:

Contact Person's Name:

Login Precedence: Local Only

Use Time Server when Bootup: None

Time Server IP Address: 0.0.0.0

Current Time: 00 : 06 : 31

New Time (hh:mm:ss): 00 : 06 : 31

Current Date: 1970 - 01 - 01

New Date (yyyy-mm-dd): 1970 - 01 - 01

Time Zone: UTC

It will take 60 seconds if time server is unreachable.

Apply Cancel

The following table describes the labels in this screen.

Table 9 General Setup

LABEL	DESCRIPTION
System Name	Choose a descriptive name for identification purposes. This name consists of up to 64 printable characters; spaces are allowed.
Location	Enter the geographic location (up to 32 characters) of your switch.
Contact Person's Name	Enter the name (up to 32 characters) of the person in charge of this switch.
Login Precedence	<p>Configure the local user accounts in the Access Control Logins screen. The RADIUS is an external server. Use this drop-down list box to select which database the switch should use (first) to authenticate a user.</p> <p>Before you specify the priority, make sure you have set up the corresponding database correctly first.</p> <p>Select Local Only to have the switch just check the local user accounts configured in the Access Control Logins screen.</p> <p>Select Local then RADIUS to have the switch check the local user accounts configured in the Access Control Logins screen. If the user name is not found, the switch then checks the user database on the specified RADIUS server. You need to configure the Port Authentication Radius screen first.</p> <p>Select RADIUS Only to have the switch just check the user database on the specified RADIUS server for a login username and password.</p>
Use Time Server When Bootup	<p>Enter the time service protocol that a timeserver sends when you turn on the switch. Not all timeservers support all protocols, so you may have to use trial and error to find a protocol that works. The main differences between them are the time format.</p> <p>When you select the Daytime (RFC 867) format, the switch displays the day, month, year and time with no time zone adjustment. When you use this format, it is recommended that you use a Daytime timeserver within your geographical time zone.</p> <p>Time (RFC-868) format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0.</p> <p>NTP (RFC-1305) is similar to Time (RFC-868)</p> <p>None is the default value. Enter the time manually. Each time you turn on the switch, the time and date will be reset to 1970-1-1 0:0.</p>
Time Server IP Address	Enter the IP address of your timeserver. The switch searches for the timeserver for up to 60 seconds. If you select a timeserver that is unreachable, then this screen will appear locked for 60 seconds. Please wait.
Current Time	This field displays the time you open this menu (or refresh the menu).
New Time (hh:min:ss)	Enter the new time in hour, minute and second format. The new time then appears in the Current Time field after you click Apply .
Current Date	This field displays the date you open this menu.
New Date (yyyy-mm-dd)	Enter the new date in year, month and day format. The new date then appears in the Current Date field after you click Apply .
Time Zone	Select the time difference between UTC (Universal Time Coordinated, formerly known as GMT, Greenwich Mean Time) and your time zone from the drop-down list box.
Apply	Click Apply to save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to start configuring the screen again.

7.4 Introduction to VLANs

A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.

In MTU (Multi-Tenant Unit) applications, VLAN is vital in providing isolation and security among the subscribers. When properly configured, VLAN prevents one subscriber from accessing the network resources of another on the same LAN, thus a user will not see the printers and hard disks of another user in the same building.

VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

Note that VLAN is unidirectional; it only governs outgoing traffic.

See the chapter on VLAN for information on port-based and 802.1Q tagged VLANs.

7.5 Switch Setup Screen

Click **Basic Setting** and then **Switch Setup** in the navigation panel display the screen as shown. The VLAN setup screens change depending on whether you choose **802.1Q** or **Port Based** in the **VLAN Type** field in this screen. Refer to the chapter on VLANs.

Figure 32 Switch Setup

Switch Setup	
VLAN Type	<input checked="" type="radio"/> 802.1Q <input type="radio"/> Port Based
Bridge Control Protocol Transparency	Active <input type="checkbox"/>
MAC Address Learning	Aging Time: <input type="text" value="300"/> seconds Join Timer: <input type="text" value="200"/> milliseconds
GARP Timer	Leave Timer: <input type="text" value="600"/> milliseconds Leave All Timer: <input type="text" value="10000"/> milliseconds
Priority Queue Assignment	level7: <input type="text" value="7"/> level6: <input type="text" value="6"/> level5: <input type="text" value="5"/> level4: <input type="text" value="4"/> level3: <input type="text" value="3"/> level2: <input type="text" value="1"/> level1: <input type="text" value="0"/> level0: <input type="text" value="2"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

The following table describes the labels in this screen.

Table 10 Switch Setup

LABEL	DESCRIPTION
VLAN Type	Choose 802.1Q or Port Based . The VLAN Setup screen changes depending on whether you choose 802.1Q VLAN Type or Port Based VLAN Type in this screen. See Section 7.4 on page 75 and the chapter on VLAN for more information on VLANs.
Bridge Control Protocol Transparency	Select Active to allow the switch to handle bridging control protocols (STP for example). You also need to define how to treat a BPDU in the Port Setup screen.
MAC Address Learning	MAC address learning reduces outgoing traffic broadcasts. For MAC address learning to occur on a port, the port must be active.
Aging Time	Enter a time from 10 to 3000 seconds. This is how long all dynamically learned MAC addresses remain in the MAC address table before they age out (and must be relearned).
GARP Timer Switches join VLANs by making a declaration. A declaration is made by issuing a Join message using GARP. Declarations are withdrawn by issuing a Leave message. A Leave All message terminates all registrations. GARP timers set declaration timeout values. See the chapter on VLAN setup for more background information.	
Join Timer	Join Timer sets the duration of the Join Period timer for GVRP in milliseconds. Each port has a Join Period timer. The allowed Join Time range is between 100 and 65535 milliseconds; the default is 200 milliseconds. See the chapter on VLAN setup for more background information.
Leave Timer	Leave Timer sets the duration of the Leave Period timer for GVRP in milliseconds. Each port has a single Leave Period timer. Leave Time must be two times larger than Join Timer. The default is 600 milliseconds.
Leave All Timer	Leave All Timer sets the duration of the Leave All Period timer for GVRP in milliseconds. Each port has a single Leave All Period timer. Leave All Timer must be larger than Leave Timer. The default is 10000 milliseconds.
Priority Queue Assignment IEEE 802.1p defines up to eight separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Frames without an explicit priority tag are given the default priority of the ingress port. Use these fields to configure the priority level-to-physical queue mapping. The switch has eight physical queues that you can map to the eight priority levels. On the switch, traffic assigned to higher index queues gets through faster while traffic in lower index queues is dropped if the network is congested. See also Queuing Method and 802.1p Priority in Port Setup for related information.	
Priority Level (The following descriptions are based on the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p).	
Level 7	Typically used for network control traffic such as router configuration messages.
Level 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).
Level 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.
Level 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.
Level 3	Typically used for “excellent effort” or better than best effort and would include important business traffic that can tolerate some delay.
Level 2	This is for “spare bandwidth”.
Level 1	This is typically used for non-critical “background” traffic such as bulk transfers that are allowed but that should not affect other applications and users.

Table 10 Switch Setup (continued)

LABEL	DESCRIPTION
Level 0	Typically used for best-effort traffic.
Apply	Click Apply to save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

7.6 IP Setup

Use the **IP Setup** screen to configure the switch IP address, default gateway device, the default domain name server and the management VLAN ID. The default gateway specifies the IP address of the default gateway (next hop) for outgoing traffic.

7.6.1 Management IP Addresses

The switch needs an IP address for it to be managed over the network. The factory default IP address is 192.168.1.1. The subnet mask specifies the network number portion of an IP address. The factory default subnet mask is 255.255.255.0.

You can configure up to 64 IP addresses which are used to access and manage the switch from the ports belonging to the pre-defined VLAN(s).



You must configure a VLAN first.

Figure 33 IP Setup

The following table describes the labels in this screen.

Table 11 IP Setup

LABEL	DESCRIPTION
Domain Name Server	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. Enter a domain name server IP address in order to be able to use a domain name instead of an IP address.
Default Management	Specify which traffic flow (In-Band or Out-of-band) the switch is to send packets originating from itself (such as SNMP traps) or packets with unknown source. Select Out-of-band to have the switch send the packets to the out-of-band management port. This means that device(s) connected to the other port(s) do not receive these packets. Select In-Band to have the switch send the packets to all ports except the out-of-band management port to which connected device(s) do not receive these packets.
In-Band Management IP Address	

Table 11 IP Setup (continued)

LABEL	DESCRIPTION
DHCP Client	Select this option if you have a DHCP server that can assign the switch an IP address, subnet mask, a default gateway IP address and a domain name server IP address automatically.
Static IP Address	Select this option if you don't have a DHCP server or if you wish to assign static IP address information to the switch. You need to fill in the following fields when you select this option.
IP Address	Enter the IP address of your switch in dotted decimal notation for example 192.168.1.1.
IP Subnet Mask	Enter the IP subnet mask of your switch in dotted decimal notation for example 255.255.255.0.
Default Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.254.
VID	Enter the VLAN identification number associated with the switch IP address. This is the VLAN ID of the CPU and is used for management only. The default is "1". All ports, by default, are fixed members of this "management VLAN" in order to manage the device from any port. If a port is not a member of this VLAN, then users on that port cannot access the device. To access the switch make sure the port that you are connected to is a member of Management VLAN.
Out-of-band Management IP Address	
IP Address	Enter the IP address of your switch in dotted decimal notation for example 192.168.0.1. If you change this IP address, make sure the computer connected to this management port is in the same subnet before accessing the GS.
Subnet Mask	Enter the IP subnet mask of your switch in dotted decimal notation for example 255.255.255.0.
Default Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.254.
Apply	Click Apply to save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring the fields again.
In-band IP Addresses You can create up to 64 IP addresses, which are used to access and manage the switch from the ports belonging to the pre-defined VLAN(s). You must configure a VLAN first.	
IP Address	Enter the IP address for managing the switch by the members of the VLAN specified in the VID field below.
IP Subnet Mask	Enter the IP subnet mask in dotted decimal notation.
VID	Type the VLAN group identification number.
Default Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation.
Add	Click Add to insert the entry to the summary table below and save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to your previous configuration.
Index	This field displays the index number of the rule. Click an index number to edit the rule.
IP Address	This field displays the IP address.

Table 11 IP Setup (continued)

LABEL	DESCRIPTION
IP Subnet Mask	This field displays the subnet mask.
VID	This field displays the ID number of the VLAN group.
Default Gateway	This field displays the IP address of the default gateway.
Delete	Check the rule(s) that you want to remove in the Delete column, then click the Delete button.
Cancel	Click Cancel to clear the selected checkboxes in the Delete column.

7.7 Port Setup

Click **Basic Setting** and then **Port Setup** in the navigation panel to enter the port configuration screen. Use this screen to configure switch port settings.

Figure 34 Port Setup

Port	Active	Name	Type	Speed / Duplex	Flow Control	802.1p Priority	BPDU Control
*	<input type="checkbox"/>		-	Auto	<input type="checkbox"/>	0	Peer
1	<input checked="" type="checkbox"/>		10/100/1000M	Auto	<input type="checkbox"/>	0	Peer
2	<input checked="" type="checkbox"/>		10/100/1000M	Auto	<input type="checkbox"/>	0	Peer
3	<input checked="" type="checkbox"/>		10/100/1000M	Auto	<input type="checkbox"/>	0	Peer
4	<input checked="" type="checkbox"/>		10/100/1000M	Auto	<input type="checkbox"/>	0	Peer
5	<input checked="" type="checkbox"/>		10/100/1000M	Auto	<input type="checkbox"/>	0	Peer
6	<input checked="" type="checkbox"/>		10/100/1000M	Auto	<input type="checkbox"/>	0	Peer
7	<input checked="" type="checkbox"/>		10/100/1000M	Auto	<input type="checkbox"/>	0	Peer
8	<input checked="" type="checkbox"/>		10/100/1000M	Auto	<input type="checkbox"/>	0	Peer
9	<input checked="" type="checkbox"/>		10/100/1000M	Auto	<input type="checkbox"/>	0	Peer
10	<input checked="" type="checkbox"/>		10/100/1000M	Auto	<input type="checkbox"/>	0	Peer
11	<input checked="" type="checkbox"/>		10/100/1000M	Auto	<input type="checkbox"/>	0	Peer
12	<input checked="" type="checkbox"/>		10/100/1000M	Auto	<input type="checkbox"/>	0	Peer

Apply Cancel

The following table describes the fields in this screen.

Table 12 Port Setup

LABEL	DESCRIPTION
Port	This is the port index number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to enable a port. The factory default for all ports is enabled. A port must be enabled for data transmission to occur.

Table 12 Port Setup (continued)

LABEL	DESCRIPTION
Name	<p>Enter a descriptive name that identifies this port. You can enter up to 64 alphanumeric characters.</p> <p>Note: Due to space limitation, the port name may be truncated in some web configurator screens.</p>
Type	<p>This field displays 10/100/1000M (Gigabit) or 1000M (GBIC).</p>
Speed/ Duplex	<p>Select the speed and the duplex mode of the connection on this port. Choices are Auto, 10M/Half Duplex, 10M/Full Duplex, 100M/Half Duplex, 100M/Full Duplex and 1000M/Full Duplex (for Gigabit ports only).</p> <p>Selecting Auto (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a port on the switch negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer port does not support auto-negotiation or turns off this feature, the switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the switch's auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect.</p>
Flow Control	<p>A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses. Flow Control is used to regulate transmission of signals to match the bandwidth of the receiving port.</p> <p>The switch uses IEEE802.3x flow control in full duplex mode and backpressure flow control in half duplex mode.</p> <p>IEEE802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill.</p> <p>Back Pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later. Select this option to enable flow control.</p>
802.1P Priority	<p>This priority value is added to incoming frames without a (802.1p) priority queue tag. See Priority Queue Assignment in Switch Setup and Queuing Method for related information.</p>
BPDU Control	<p>Configure the way to treat BPDUs received on this port.</p> <p>Note: You must activate bridging control protocol transparency in the Switch Setup screen first.</p> <p>Select Peer to process any BPDU (Bridge Protocol Data Units) received on this port. Select Tunnel to forward BPDUs received on this port. Select Discard to drop any BPDU received on this port. Select Network to process a BPDU with no VLAN tag and forward a tagged BPDU.</p>
Apply	<p>Click Apply to save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.</p>
Cancel	<p>Click Cancel to begin configuring this screen afresh.</p>

PART III

Advanced Settings

VLAN (85)
Static MAC Forward Setup (97)
Filtering (101)
Spanning Tree Protocol (103)
Bandwidth Control (113)
Broadcast Storm Control (115)
Mirroring (117)
Link Aggregation (119)
Port Authentication (123)
Port Security (129)
Classifier (133)
Policy Rule (139)
Queuing Method (145)
Multicast (149)
DHCP Relay (161)

The type of screen you see here depends on the **VLAN Type** you selected in the **Switch Setup** screen. This chapter shows you how to configure 802.1Q tagged and port-based VLANs. See the General, Switch and IP Setup chapter for more information.

8.1 Introduction to IEEE 802.1Q Tagged VLAN

Tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges - they are not confined to the switch on which they were created. The VLANs can be created statically by hand or dynamically through GVRP. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is four bytes longer than an untagged frame and contains two bytes of TPID (Tag Protocol Identifier, residing within the type/length field of the Ethernet frame) and two bytes of TCI (Tag Control Information, starts after the source address field of the Ethernet frame).

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4,096 VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

TPID 2 Bytes	User Priority 3 Bits	CFI 1 Bit	VLAN ID 12 bits
-----------------	-------------------------	--------------	--------------------

8.1.1 Forwarding Tagged and Untagged Frames

Each port on the switch is capable of passing tagged or untagged frames. To forward a frame from an 802.1Q VLAN-aware switch to an 802.1Q VLAN-unaware switch, the switch first decides where to forward the frame and then strips off the VLAN tag. To forward a frame from an 802.1Q VLAN-unaware switch to an 802.1Q VLAN-aware switch, the switch first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID. The default PVID is VLAN 1 for all ports, but this can be changed.

8.1.2 Automatic VLAN Registration

GARP and GVRP are the protocols used to automatically register VLAN membership across switches.

8.1.2.1 GARP

GARP (Generic Attribute Registration Protocol) allows network switches to register and de-register attribute values with other GARP participants within a bridged LAN. GARP is a protocol that provides a generic mechanism for protocols that serve a more specific application, for example, GVRP.

8.1.2.2 GARP Timers

Switches join VLANs by making a declaration. A declaration is made by issuing a Join message using GARP. Declarations are withdrawn by issuing a Leave message. A Leave All message terminates all registrations. GARP timers set declaration timeout values.

8.1.2.3 GVRP

GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way for switches to register necessary VLAN members on ports across the network. Enable this function to permit VLANs groups beyond the local switch.

Please refer to the following table for common IEEE 802.1Q VLAN terminology.

Table 13 IEEE 802.1Q VLAN terminology

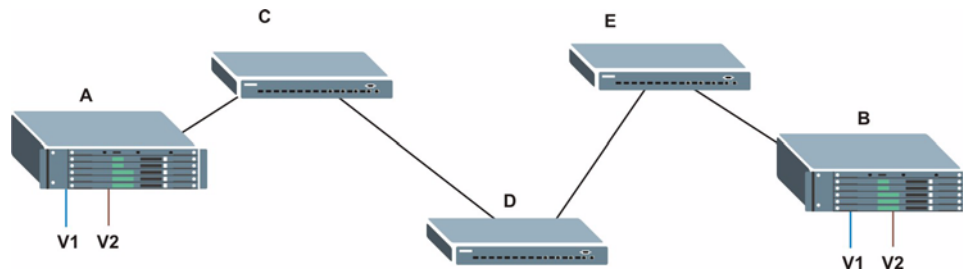
VLAN PARAMETER	TERM	DESCRIPTION
VLAN Type	Permanent VLAN	This is a static VLAN created manually.
	Dynamic VLAN	This is a VLAN configured by a GVRP registration/deregistration process.
VLAN Administrative Control	Registration Fixed	Fixed registration ports are permanent VLAN members.
	Registration Forbidden	Ports with registration forbidden are forbidden to join the specified VLAN.
	Normal Registration	Ports dynamically join a VLAN using GVRP.
VLAN Tag Control	Tagged	Ports belonging to the specified VLAN tag all outgoing frames transmitted.
	Untagged	Ports belonging to the specified don't tag all outgoing frames transmitted.
VLAN Port	Port VID	This is the VLAN ID assigned to untagged frames that this port received.
	Acceptable frame type	You may choose to accept both tagged and untagged incoming frames or just tagged incoming frames on a port.
	Ingress filtering	If set, the switch discards incoming frames for VLANs that do not have this port as a member

8.1.3 Port VLAN Trunking

Enable **VLAN Trunking** on a port to allow frames belonging to unknown VLAN groups to pass through that port. This is useful if you want to set up VLAN groups on end devices without having to configure the same VLAN groups on intermediary devices.

Refer to the following figure. Suppose you want to create VLAN groups 1 and 2 (V1 and V2) on devices A and B. Without **VLAN Trunking**, you must configure VLAN groups 1 and 2 on all intermediary switches C, D and E; otherwise they will drop frames with unknown VLAN group tags. However, with **VLAN Trunking** enabled on a port(s) in each intermediary switch you only need to create VLAN groups in the end devices (A and B). C, D and E automatically allow frames with VLAN group tags 1 and 2 (VLAN groups that are unknown to those switches) to pass through their VLAN trunking port(s).

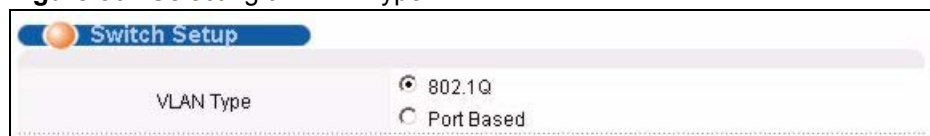
Figure 35 Port VLAN Trunking



8.2 Select the VLAN Type

Select a VLAN type in the **Switch Setup** screen.

Figure 36 Selecting a VLAN Type



8.3 802.1Q VLAN

Follow the steps below to set the **802.1Q VLAN Type** on the switch.

- 1 Select **802.1Q** as the **VLAN Type** in the **Switch Setup** screen (under **Basic Setting**) and click **Apply**.
- 2 Click **VLAN** under **Advanced Application** to display the **VLAN Status** screen as shown next. These fields describe the status of the IEEE 802.1Q VLAN.

Figure 37 802.1Q VLAN Status

Index	VID	Elapsed Time	Status
1	1	0:45:17	Static
2	123	0:00:04	Static

The following table describes the labels in this screen.

Table 14 802.1Q VLAN Status

LABEL	DESCRIPTION
The Number of VLAN	This is the number of VLANs configured on the switch.
Index	This is the VLAN index number.
VID	This is the VLAN identification number.
Elapsed Time	This field shows how long it has been since a normal VLAN was registered or a static VLAN was set up.
Status	This field shows how this VLAN was added to the switch; dynamic - using GVRP, static - added as a permanent entry or other - added using Multicast VLAN Registration (MVR).
Change Pages	Click Previous or Next to show the previous/next screen if all status information cannot be seen in one screen.

8.3.1 802.1Q VLAN Detail

Click on an index number in the **VLAN Status** screen to display VLAN details. Use this screen to view detailed port settings and status of the VLAN group. See [Section 8.1 on page 85](#) for more information on static VLAN.

Figure 38 802.1Q VLAN Detail

VID	Port Number						Elapsed Time	Status
	2	4	6	8	10	12		
1	U	U	U	U	U	U	0:47:06	Static
	U	U	U	U	U	U		

The following table describes the labels in this screen.

Table 15 802.1Q VLAN Detail

LABEL	DESCRIPTION
VLAN Status	Click this to go to the VLAN Status screen.
VID	This is the VLAN identification number.
Port Number	This column displays the ports that are participating in a VLAN. A tagged port is marked as T , an untagged port is marked as U and ports not participating in a VLAN in marked as “-”.
Elapsed Time	This field shows how long it has been since a normal VLAN was registered or a static VLAN was set up.
Status	This field shows how this VLAN was added to the switch; dynamic - using GVRP, static - added as a permanent entry or other - added using Multicast VLAN Registration (MVR).

8.3.2 802.1Q VLAN Port Settings

Use this screen to configure the 802.1Q VLAN settings on a port. See [Section 8.1 on page 85](#) for more information on static VLAN. Click the **VLAN Port Setting** link in the **VLAN Status** screen.

Figure 39 802.1Q VLAN Port Settings

Port	Ingress Check	PVID	GVRP	Acceptable Frame Type	VLAN Trunking
*	<input type="checkbox"/>		<input type="checkbox"/>	All	<input type="checkbox"/>
1	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
2	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
3	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
4	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
5	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
6	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
7	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
8	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
9	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
10	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
11	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
12	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>

The following table describes the labels in this screen.

Table 16 802.1Q VLAN Port Settings

LABEL	DESCRIPTION
GVRP	GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way for switches to dynamically register necessary VLAN members on ports across the network. Select this check box to permit VLAN groups beyond the local switch.
Port Isolation	Port Isolation allows each port (1 to 8) to communicate with the CPU port and the shared GBIC ports (9 to 12). The isolated ports (1 to 8) cannot communicate with each other. However, the shared GBIC ports (9 to 12) and the CPU port can communicate with all ports. This option is the most limiting but also the most secure.
Port	This field displays the port numbers.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Ingress Check	If this check box is selected for a port, the device discards incoming frames for VLANs that do not include this port in its member set.
PVID	Each port on the switch is capable of passing tagged or untagged frames. To forward a frame from an 802.1Q VLAN-unaware switch to an 802.1Q VLAN-aware switch, the switch first decides where to forward the frame, and then inserts a VLAN tag reflecting the default ingress port's VLAN ID, the PVID. The default PVID is VLAN 1 for all ports, but this can be changed to any number between 0 and 4094.
GVRP	Select this check box to permit VLANs groups beyond the local switch on this port. GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way for switches to register necessary VLAN members on ports across the network.
Acceptable Frame Type	Specify the type of frames allowed on a port. Choices are All and Tag Only . Select All to accept all frames with untagged or tagged frames on this port. This is the default setting. Select Tag Only to accept only tagged frames on this port. All untagged frames are dropped.
VLAN Trunking	Enable VLAN Trunking on ports connected to other switches or routers (but not ports directly connected to end users) to allow frames belonging to unknown VLAN groups to pass through the switch.
Apply	Click Apply to save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to start configuring the screen again.

8.3.3 802.1Q Static VLAN

Use this screen to configure and view 802.1Q VLAN parameters for the switch. You can dynamically have a port join a VLAN group using GVRP, permanently assign a port to be a member of a VLAN group or prohibit a port from joining a VLAN group in this screen. Click **Static VLAN** in the **VLAN Status** screen to display the screen as shown next.

Figure 40 802.1Q Static VLAN

Static VLAN VLAN Status

ACTIVE

Name

VLAN Group ID

Port	Control			Tagging
*	Normal			<input checked="" type="checkbox"/> Tx Tagging
1	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
2	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
3	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
4	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
5	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
6	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
7	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
8	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
9	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
10	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
11	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
12	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging

Add Cancel Clear

VID	Active	Name	Delete
1	Yes		<input type="checkbox"/>
123	Yes	test	<input type="checkbox"/>

Delete Cancel

The following table describes the labels in this screen.

Table 17 802.1Q Static VLAN

LABEL	DESCRIPTION
Active	Select this check box to enable the VLAN.
Name	Enter a descriptive name for this VLAN group for identification purposes.
VLAN Group ID	Enter the VLAN ID for this static VLAN entry; the valid range is between 1 and 4094.
Port	The port number identifies the port you are configuring.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Control	Select Normal for the port to dynamically join this VLAN group using GVRP. This is the default selection. Select Fixed for the port to be a permanent member of this VLAN group. Select Forbidden if you want to prohibit the port from joining this VLAN group.
Tagging	Select TX Tagging if you want the port to tag all outgoing frames transmitted with this VLAN Group ID.

Table 17 802.1Q Static VLAN (continued)

LABEL	DESCRIPTION
Add	Click Add to insert the entry in the summary table below and save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to your previous configuration.
Clear	Click Clear to clear the fields to the factory defaults.

8.3.4 Viewing and Editing VLAN Settings

To view a summary of the VLAN configuration, scroll down to the summary table at the bottom of the **Static VLAN** screen.

To change the settings of a rule, click a number in the **VID** field.

Figure 41 Static VLAN: Summary Table

VID	Active	Name	Delete
1	Yes	1	<input type="checkbox"/>

Delete Cancel

The following table describes the labels in this screen.

Table 18 Static VLAN: Summary Table

LABEL	DESCRIPTION
VID	This field displays the ID number of the VLAN group. Click the number to edit the VLAN settings.
Active	This field indicates whether the VLAN settings are enabled (Yes) or disabled (No).
Name	This field displays the descriptive name for this VLAN group.
Delete	Check the rule(s) that you want to remove in the Delete column, then click the Delete button.
Cancel	Click Cancel to clear the Delete check boxes.

8.3.4.1 VID1 Example Screen

Figure 42 VID1 Example Screen

Port	Control	Tagging
*	Fixed	<input type="checkbox"/> Tx Tagging
1	<input checked="" type="radio"/> Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
2	<input type="radio"/> Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
3	<input type="radio"/> Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
4	<input type="radio"/> Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
5	<input type="radio"/> Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
6	<input type="radio"/> Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
7	<input type="radio"/> Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
8	<input type="radio"/> Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
9	<input type="radio"/> Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
10	<input type="radio"/> Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
11	<input type="radio"/> Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
12	<input type="radio"/> Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging

8.4 Introduction to Port-based VLANs

Port-based VLANs are VLANs where the packet forwarding decision is based on the destination MAC address and its associated port.

Port-based VLANs require allowed outgoing ports to be defined for each port. Therefore, if you wish to allow two subscriber ports to talk to each other, for example, between conference rooms in a hotel, you must define the egress (an egress port is an outgoing port, that is, a port through which a data packet leaves) for both ports.

Port-based VLANs are specific only to the switch on which they were created.



When you activate port-based VLAN, the switch uses a default VLAN ID of 1. You cannot change it.



In screens (such as **IP Setup** and **Filtering**) that require a VID, you must enter 1 as the VID.

The port-based VLAN setup screen is shown next. The **CPU** management port forms a VLAN with all Ethernet ports.

8.4.1 Configuring a Port-based VLAN

Select **Port Based** as the **VLAN Type** in the **Switch Setup** screen under **Basic Setting** and then click **VLAN** under **Advanced Application** to display the next screen.

Figure 43 Port Based VLAN Setup (All Connected)

Setting Wizard: All connected [Apply]

		Incoming													
		1	2	3	4	5	6	7	8	9	10	11	12		
Outgoing	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1
	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2
	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3
	4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	4
	5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	5
	6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	6
	7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	7
	8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	8
	9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	9
	10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	10
	11	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	11
	12	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	12
CPU	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	CPU	
		1	2	3	4	5	6	7	8	9	10	11	12		

[Apply] [Cancel]

Figure 44 Port Based VLAN Setup (Port isolation)

Setting Wizard: Port isolation [Apply]

		Incoming												
		1	2	3	4	5	6	7	8	9	10	11	12	
Outgoing	1	<input checked="" 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"/>	1
	2	<input type="checkbox"/>	<input checked="" 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"/>	2
	3	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" 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"/>	3
	4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" 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"/>	4
	5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	5
	6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	6
	7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	7
	8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	8
	9	<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 checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	9
	10	<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 checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	10
	11	<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 checked="" type="checkbox"/>	<input type="checkbox"/>	11
	12	<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 checked="" type="checkbox"/>	12
CPU	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	CPU
		1	2	3	4	5	6	7	8	9	10	11	12	

[Apply] [Cancel]

The following table describes the labels in this screen.

Table 19 Port Based VLAN Setup

LABEL	DESCRIPTION
Setting Wizard	<p>Choose from All connected or Port isolation.</p> <p>All connected means all ports can communicate with each other, that is, there are no virtual LANs. All incoming and outgoing ports are selected (see Figure 43 on page 94). This option is the most flexible but also the least secure.</p> <p>Port isolation means that each port can only communicate with the CPU management port and cannot communicate with each other. All incoming ports are selected while only the CPU outgoing port is selected (see Figure 44 on page 94). This option is the most limiting but also the most secure.</p> <p>After you make your selection, click Apply (top right of screen) to display the screens as mentioned above. You can still customize these settings by adding/deleting incoming or outgoing ports, but you must also click Apply at the bottom of the screen.</p>
Incoming	<p>These are the ingress ports; an ingress port is an incoming port, that is, a port through which a data packet enters. If you wish to allow two subscriber ports to talk to each other, you must define the ingress port for both ports. The numbers in the top row denote the incoming port for the corresponding port listed on the left (its outgoing port). CPU refers to the switch management port. By default it forms a VLAN with all Gigabit ports. If it does not form a VLAN with a particular port then the switch cannot be managed from that port.</p>
Outgoing	<p>These are the egress ports; an egress port is an outgoing port, that is, a port through which a data packet leaves. If you wish to allow two subscriber ports to talk to each other, you must define the egress port for both ports. CPU refers to the switch management port. By default it forms a VLAN with all Gigabit ports. If it does not form a VLAN with a particular port then the switch cannot be managed from that port.</p>
Apply	<p>Click Apply to save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.</p>
Cancel	<p>Click Cancel to start configuring the screen again.</p>

Static MAC Forward Setup

Use these screens to configure forwarding rules based on MAC addresses of devices on your network.

9.1 Introduction to Static MAC Forward Setup

A static MAC address is an address that has been manually entered in the MAC address table. Static MAC addresses do not age out. When you set up static MAC address rules, you are setting static MAC addresses for a port. This may reduce the need for broadcasting.

Static MAC address forwarding together with port security allow only computers in the MAC address table on a port to access the switch. See [Chapter 17 on page 129](#) for more information on port security.

9.2 Configuring Static MAC Forwarding

Click **Static MAC Forwarding** to display the configuration screen as shown.

Figure 45 Static MAC Forwarding

The screenshot shows the 'Static MAC Forwarding' configuration interface. It includes the following elements:

- Title Bar:** 'Static MAC Forwarding' with an orange circle icon.
- Form Fields:**
 - Active:** A checkbox.
 - Name:** A text input field.
 - MAC Address:** Six input boxes separated by colons (e.g., [] : [] : [] : [] : [] : []).
 - VID:** A text input field.
 - Port:** A text input field.
- Buttons:** 'Add', 'Cancel', and 'Clear' buttons are located below the form fields.
- Table:** A table with the following columns: Index, Active, Name, MAC Address, VID, Port, and Delete.
- Bottom Buttons:** 'Delete' and 'Cancel' buttons are located below the table.

The following table describes the labels in this screen.

Table 20 Static MAC Forwarding

LABEL	DESCRIPTION
Active	Select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by clearing this check box.
Name	Enter a descriptive name for identification purposes for this static MAC address forwarding rule.
MAC Address	Enter the MAC address in valid MAC address format, that is, six hexadecimal character pairs. Note: Static MAC addresses do not age out.
VID	Enter the VLAN identification number.
Port	Type the number of a port where the MAC address entered in the previous field will be automatically forwarded.
Add	Click Add to insert the entry in the summary table below and save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to your previous configuration.
Clear	Click Clear to clear the fields to the factory defaults.

9.3 Viewing and Editing Static MAC Forwarding Rules

To view a summary of the rule configuration, scroll down to the summary table at the bottom of the **Static MAC Forwarding** screen.

To change the settings of a rule, click a number in the **Index** field.

Figure 46 Static MAC Forwarding: Summary Table

Index	Active	Name	MAC Address	VID	Port	Delete
1	Yes	test	0a:b2:a0:81:f3:73	1	1	<input type="checkbox"/>

The following table describes the labels in this screen.

Table 21 Static MAC Forwarding: Summary Table

LABEL	DESCRIPTION
Index	Click an index number to modify a static MAC address rule for a port.
Active	This field displays whether this static MAC address forwarding rule is active (Yes) or not (No). You may temporarily deactivate a rule without deleting it.
Name	This field displays the descriptive name for identification purposes for this static MAC address-forwarding rule.
MAC Address	This field displays the MAC address that will be forwarded.
VID	This field displays the VLAN identification number to which the MAC address belongs.
Port	This field displays the port where the MAC address shown in the next field will be forwarded.

Table 21 Static MAC Forwarding: Summary Table (continued)

LABEL	DESCRIPTION
Delete	Check the rule(s) that you want to remove in the Delete column, then click the Delete button.
Cancel	Click Cancel to clear the selected checkboxes in the Delete column.

Filtering

This chapter discusses static IP and MAC address port filtering.

10.1 Introduction to Filtering

Filtering means sifting traffic going through the switch based on the source and/or destination MAC addresses and VLAN group (ID).

10.2 Configuring a Filtering Rule

Click **Advanced Application** and **Filtering** to display the screen as shown next.

Figure 47 Filtering

The following table describes the related labels in this screen.

Table 22 Filtering

LABEL	DESCRIPTION
Active	Make sure to select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by deselecting this check box.
Name	Type a descriptive name for this filter rule. This is for identification purpose only.

Table 22 Filtering (continued)

LABEL	DESCRIPTION
Action	Select Discard source to drop frame from the source MAC address (specified in the MAC field). The switch can still send frames to the MAC address. Select Discard destination to drop frames to the destination MAC address (specified in the MAC address). The switch can still receive frames originating from the MAC address. Select Discard source and Discard destination to block traffic to/from the MAC address specified in the MAC field.
MAC	Type a MAC address in valid MAC address format, that is, six hexadecimal character pairs to apply the filter rule to the specified MAC address and VLAN group
VID	Type the VLAN group identification number.
Add	Click Add to insert the entry in the summary table below and save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to your previous configuration.
Clear	Click Clear to clear the fields to the factory defaults.

10.3 Viewing and Editing Filter Rules

To view a summary of the rule configuration, scroll down to the summary table at the bottom of the **Filtering** screen.

To change the settings of a rule, click a number in the **Index** field.

Figure 48 Filtering: Summary Table

Index	Active	Name	MAC Address	VID	Action	Delete
1	Yes	example	00:a0:c5:00:07:21	1	Discard source	<input type="checkbox"/>

Delete Cancel

The following table describes the labels in the summary table.

Table 23 Filtering: Summary Table

LABEL	DESCRIPTION
Index	This field displays the index number of the rule. Click an index number to edit the rule.
Active	This field displays Yes when the rule is activated and No when is it deactivated.
Name	This field displays the descriptive name for this rule. This is for identification purpose only.
MAC Address	This field displays the source/destination MAC address.
VID	This field displays the VLAN identification number to which the MAC address belongs.
Action	This field displays the filtering action (Discard both , Discard source or Discard dest.).
Delete	Check the rule(s) that you want to remove in the Delete column and then click the Delete button.
Cancel	Click Cancel to clear the selected checkboxes in the Delete column.

Spanning Tree Protocol

The switch supports Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) as defined in the following standards.

- IEEE 802.1D Spanning Tree Protocol
- IEEE 802.1w Rapid Spanning Tree Protocol

The switch also allows you to set up multiple STP configurations (or trees). Ports can then be assigned to the trees.

11.1 STP/RSTP Overview

(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a switch to interact with other (R)STP -compliant switches in your network to ensure that only one path exists between any two stations on the network.

The switch uses IEEE 802.1w RSTP (Rapid Spanning Tree Protocol) that allows faster convergence of the spanning tree than STP (while also being backwards compatible with STP-only aware bridges). In RSTP, topology change information is directly propagated throughout the network from the device that generates the topology change. In STP, a longer delay is required as the device that causes a topology change first notifies the root bridge that then notifies the network. Both RSTP and STP flush unwanted learned addresses from the filtering database. In RSTP, the port states are Discarding, Learning, and Forwarding.

Note: In this user's guide, "STP" refers to both STP and RSTP.

11.1.1 STP Terminology

The root bridge is the base of the spanning tree.

Path cost is the cost of transmitting a frame onto a LAN through that port. It is assigned according to the speed of the link to which a port is attached. The slower the media, the higher the cost.

Table 24 STP Path Costs

	LINK SPEED	RECOMMENDED VALUE	RECOMMENDED RANGE	ALLOWED RANGE
Path Cost	4Mbps	250	100 to 1000	1 to 65535
Path Cost	10Mbps	100	50 to 600	1 to 65535
Path Cost	16Mbps	62	40 to 400	1 to 65535
Path Cost	100Mbps	19	10 to 60	1 to 65535
Path Cost	1Gbps	4	3 to 10	1 to 65535
Path Cost	10Gbps	2	1 to 5	1 to 65535

On each bridge, the root port is the port through which this bridge communicates with the root. It is the port on this switch with the lowest path cost to the root (the root path cost). If there is no root port, then this switch has been accepted as the root bridge of the spanning tree network.

For each LAN segment, a designated bridge is selected. This bridge has the lowest cost to the root among the bridges connected to the LAN.

11.1.2 How STP Works

After a bridge determines the lowest cost-spanning tree with STP, it enables the root port and the ports that are the designated ports for connected LANs, and disables all other ports that participate in STP. Network packets are therefore only forwarded between enabled ports, eliminating any possible network loops.

STP-aware switches exchange Bridge Protocol Data Units (BPDUs) periodically. When the bridged LAN topology changes, a new spanning tree is constructed.

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDUs after a predefined interval (Max Age), the bridge assumes that the link to the root bridge is down. This bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

11.1.3 STP Port States

STP assigns five port states to eliminate packet looping. A bridge port is not allowed to go directly from blocking state to forwarding state so as to eliminate transient loops.

Table 25 STP Port States

PORT STATE	DESCRIPTION
Disabled	STP is disabled (default).
Blocking	Only configuration and management BPDUs are received and processed.
Listening	All BPDUs are received and processed.
Learning	All BPDUs are received and processed. Information frames are submitted to the learning process but not forwarded.
Forwarding	All BPDUs are received and processed. All information frames are received and forwarded.

11.1.4 Multiple RSTP

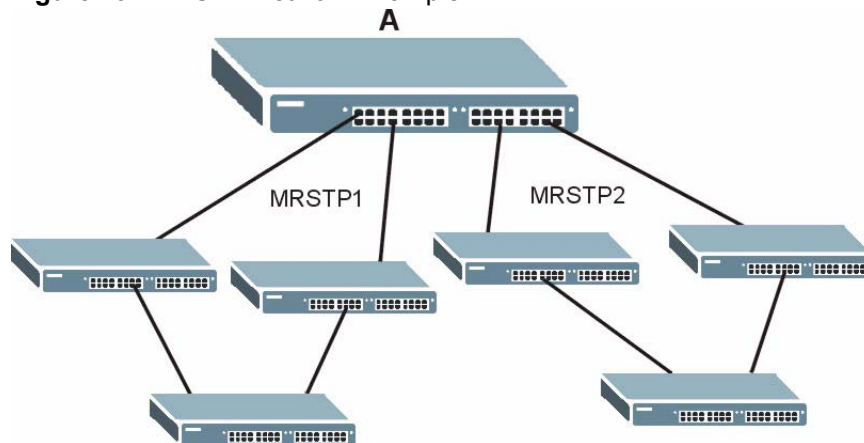
MRSTP (Multiple RSTP) is ZyXEL's proprietary feature that is compatible with RSTP and STP. With MRSTP, you can have more than one spanning tree on your switch and assign port(s) to each tree. Each spanning tree operates independently with its own bridge information.

In the following example, there are two RSTP instances (**MRSTP 1** and **MRSTP2**) on switch **A**.

To set up MRSTP, activate MRSTP on the switch and specify which port(s) belong to which spanning tree.

Note: Each port can belong to one STP tree only.

Figure 49 MRSTP Network Example



11.2 Spanning Tree Protocol Main Screen

The switch allows you to configure a single RSTP configuration or you can configure multiple configurations. See [Section 11.1 on page 103](#) for more information on RSTP. Click **Advanced Application, Spanning Tree Protocol** in the navigation panel to choose whether you want to configure multiple or a single Spanning Tree Protocol configuration.

Note: This screen is only available if neither RSTP or MRSTP is active. Once you select RSTP or MRSTP this screen displays the status of your configuration.

Figure 50 Spanning Tree Protocol RSTP and MRSTP



The following table describes the labels in this screen.

Table 26 Spanning Tree Protocol: Status

LABEL	DESCRIPTION
RSTP	This link takes you to the Rapid Spanning Tree Protocol configuration screen. See Section 11.3 on page 106 .
MRSTP	This link takes you to the Multiple Rapid Spanning Tree Protocol configuration screen. See Section 11.5 on page 109 .

11.3 Configure Rapid Spanning Tree Protocol

Use this screen to configure RSTP settings, see [Section 11.1 on page 103](#) for more information on RSTP. Click **RSTP** in the **Advanced Application, Spanning Tree Protocol** screen.

Figure 51 RSTP: Configuration

Port	Active	Priority	Path Cost
*	<input type="checkbox"/>		
1	<input type="checkbox"/>	128	4
2	<input type="checkbox"/>	128	4
3	<input type="checkbox"/>	128	4
4	<input type="checkbox"/>	128	4
5	<input type="checkbox"/>	128	4
6	<input type="checkbox"/>	128	4
7	<input type="checkbox"/>	128	4
8	<input type="checkbox"/>	128	4
9	<input type="checkbox"/>	128	4
10	<input type="checkbox"/>	128	4
11	<input type="checkbox"/>	128	4
12	<input type="checkbox"/>	128	4

The following table describes the labels in this screen.

Table 27 RSTP: Configuration

LABEL	DESCRIPTION
Status	Click Status to display the RSTP Status screen (see Figure 52 on page 109).
Active	Select this check box to activate RSTP. Clear this checkbox to disable RSTP.
Bridge Priority	<p>Bridge priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch. Select a value from the drop-down list box.</p> <p>The lower the numeric value you assign, the higher the priority for this bridge.</p> <p>Bridge Priority determines the root bridge, which in turn determines Hello Time, Max Age and Forwarding Delay.</p>
Hello Time	This is the time interval in seconds between BPDUs (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.

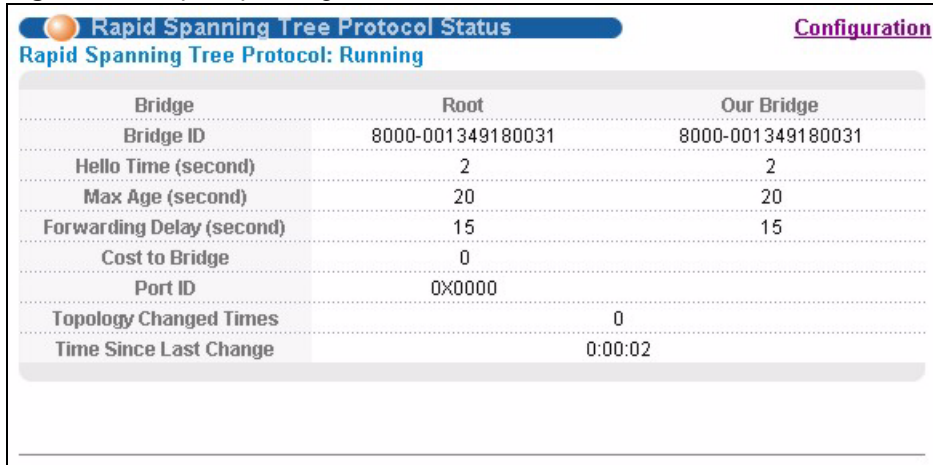
Table 27 RSTP: Configuration (continued)

LABEL	DESCRIPTION
Max Age	This is the maximum time (in seconds) a switch can wait without receiving a BPDU before attempting to reconfigure. All switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the switch ports attached to the network. The allowed range is 6 to 40 seconds.
Forwarding Delay	This is the maximum time (in seconds) a switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds. As a general rule: Note: $2 * (\text{Forward Delay} - 1) \geq \text{Max Age} \geq 2 * (\text{Hello Time} + 1)$
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to activate RSTP on this port.
Priority	Configure the priority for each port here. Priority decides which port should be disabled when more than one port forms a loop in a switch. Ports with a higher priority numeric value are disabled first. The allowed range is between 0 and 255 and the default value is 128.
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is assigned according to the speed of the bridge. The slower the media, the higher the cost - see Table 24 on page 104 for more information.
Apply	Click Apply to save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields.

11.4 Rapid Spanning Tree Protocol Status

Click **Advanced Application, Spanning Tree Protocol** in the navigation panel to display the status screen as shown next. See [Section 11.1 on page 103](#) for more information on RSTP.

Note: This screen is only available after you activate RSTP on the switch.

Figure 52 Rapid Spanning Tree Protocol: Status


Bridge	Root	Our Bridge
Bridge ID	8000-001349180031	8000-001349180031
Hello Time (second)	2	2
Max Age (second)	20	20
Forwarding Delay (second)	15	15
Cost to Bridge	0	
Port ID	0x0000	
Topology Changed Times		0
Time Since Last Change		0:00:02

The following table describes the labels in this screen.

Table 28 Rapid Spanning Tree Protocol: Status

LABEL	DESCRIPTION
Configuration	Click Configuration to configure RSTP settings. Refer to Section 11.3 on page 106 .
Bridge	Root refers to the base of the spanning tree (the root bridge). Our Bridge is this switch. This switch may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same for Root and Our Bridge if the switch is the root switch.
Hello Time (second)	This is the time interval (in seconds) at which the root switch transmits a configuration message. The root bridge determines Hello Time , Max Age and Forwarding Delay .
Max Age (second)	This is the maximum time (in seconds) a switch can wait without receiving a configuration message before attempting to reconfigure.
Forwarding Delay (second)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding).
Cost to Bridge	This is the path cost from the root port on this switch to the root switch.
Port ID	This is the priority and number of the port on the switch through which this switch must communicate with the root of the Spanning Tree.
Topology Changed Times	This is the number of times the spanning tree has been reconfigured.
Time Since Last Change	This is the time since the spanning tree was last reconfigured.

11.5 Configure Multiple Rapid Spanning Tree Protocol

To configure MRSTP, select **MRSTP** in the **Advanced Application, Spanning Tree Protocol** screen. See [Section 11.1 on page 103](#) for more information on MRSTP.

Figure 53 MRSTP: Configuration

Tree	Active	Bridge Priority	Hello Time	MAX Age	Forwarding Delay
1	<input type="checkbox"/>	32768	2 seconds	20 seconds	15
2	<input type="checkbox"/>	32768	2 seconds	20 seconds	15

Port	Active	Priority	Path Cost	Tree
*	<input type="checkbox"/>			1
1	<input type="checkbox"/>	128	4	1
2	<input type="checkbox"/>	128	4	1
3	<input type="checkbox"/>	128	4	1
4	<input type="checkbox"/>	128	4	1
5	<input type="checkbox"/>	128	4	1
6	<input type="checkbox"/>	128	4	1
7	<input type="checkbox"/>	128	4	1
8	<input type="checkbox"/>	128	4	1
9	<input type="checkbox"/>	128	4	1
10	<input type="checkbox"/>	128	4	1
11	<input type="checkbox"/>	128	4	1
12	<input type="checkbox"/>	128	4	1

Apply Cancel

The following table describes the labels in this screen.

Table 29 MRSTP: Configuration

LABEL	DESCRIPTION
Status	Click Status to display the MRSTP Status screen (see Figure 54 on page 112).
Tree	This is a read only index number of the STP trees.
Active	Select this check box to activate an STP tree. Clear this checkbox to disable an STP tree.
Bridge Priority	<p>Bridge priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch. Select a value from the drop-down list box.</p> <p>The lower the numeric value you assign, the higher the priority for this bridge.</p> <p>Bridge Priority determines the root bridge, which in turn determines Hello Time, Max Age and Forwarding Delay.</p>
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.
Max Age	This is the maximum time (in seconds) a switch can wait without receiving a BPDU before attempting to reconfigure. All switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the switch ports attached to the network. The allowed range is 6 to 40 seconds.

Table 29 MRSTP: Configuration (continued)

LABEL	DESCRIPTION
Forwarding Delay	<p>This is the maximum time (in seconds) a switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds.</p> <p>As a general rule:</p> <p>Note: $2 * (\text{Forward Delay} - 1) \geq \text{Max Age} \geq 2 * (\text{Hello Time} + 1)$</p>
Port	This field displays the port number.
*	<p>Settings in this row apply to all ports.</p> <p>Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis.</p> <p>Note: Changes in this row are copied to all the ports as soon as you make them.</p>
Active	Select this check box to activate STP on this port.
Priority	<p>Configure the priority for each port here.</p> <p>Priority decides which port should be disabled when more than one port forms a loop in a switch. Ports with a higher priority numeric value are disabled first. The allowed range is between 0 and 255 and the default value is 128.</p>
Path Cost	<p>Path cost is the cost of transmitting a frame on to a LAN through that port. It is assigned according to the speed of the bridge. The slower the media, the higher the cost - see Table 24 on page 104 for more information.</p>
Tree	Select which STP tree configuration this port should participate in.
Apply	<p>Click Apply to save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.</p>
Cancel	Click Cancel to reset the fields.

11.6 Multiple Rapid Spanning Tree Protocol Status

Click **Advanced Application, Spanning Tree Protocol** in the navigation panel to display the status screen as shown next. See [Section 11.1 on page 103](#) for more information on MRSTP.

Note: This screen is only available after you activate MRSTP on the switch.

Figure 54 MRSTP: Status

Bridge	Root	Our Bridge
Bridge ID	8000-001349180031	8000-001349180031
Hello Time (second)	2	2
Max Age (second)	20	20
Forwarding Delay (second)	15	15
Cost to Bridge	0	
Port ID	0X0000	
Topology Changed Times		0
Time Since Last Change		0:00:03

The following table describes the labels in this screen.

Table 30 Spanning Tree Protocol: Status

LABEL	DESCRIPTION
Configuration	Click Configuration to configure MRSTP settings. Refer to Section 11.5 on page 109 .
Tree	Select which STP tree configuration you want to view.
Bridge	Root refers to the base of the spanning tree (the root bridge). Our Bridge is this switch. This switch may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same for Root and Our Bridge if the switch is the root switch.
Hello Time (second)	This is the time interval (in seconds) at which the root switch transmits a configuration message. The root bridge determines Hello Time , Max Age and Forwarding Delay .
Max Age (second)	This is the maximum time (in seconds) a switch can wait without receiving a configuration message before attempting to reconfigure.
Forwarding Delay (second)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding).
Cost to Bridge	This is the path cost from the root port on this switch to the root switch.
Port ID	This is the priority and number of the port on the switch through which this switch must communicate with the root of the Spanning Tree.
Topology Changed Times	This is the number of times the spanning tree has been reconfigured.
Time Since Last Change	This is the time since the spanning tree was last reconfigured.

Bandwidth Control

This chapter shows you how you can set the maximum bandwidth allowed for traffic flows on a port using the Bandwidth Control setup screens.

12.1 Introduction to Bandwidth Control

Bandwidth control means defining a maximum allowable bandwidth for incoming and/or outgoing traffic flows on a port.

12.1.1 CIR and PIR

The Committed Information Rate (CIR) is the guaranteed bandwidth for the incoming traffic flow on a port. The Peak Information Rate (PIR) is the maximum bandwidth allowed for the incoming traffic flow on a port when there is no network congestion.

The CIR and PIR should be set for all ports that use the same uplink bandwidth. If the CIR is reached, packets are sent at the rate up to the PIR. When network congestion occurs, packets through the ingress port exceeding the CIR will be marked for drop.



The CIR should be less than the PIR.
The sum of CIRs cannot be greater than or equal to the uplink bandwidth.

12.1.2 Bandwidth Control Setup

Click **Advanced Application** and then **Bandwidth Control** in the navigation panel to bring up the screen as shown next.

Figure 55 Bandwidth Control

Port	Active	Commit Rate	Ingress Rate Active	Peak Rate	Active	Egress Rate
*	<input type="checkbox"/>	<input type="text"/> Kbps	<input type="checkbox"/>	<input type="text"/> Kbps	<input type="checkbox"/>	<input type="text"/> Kbps
1	<input type="checkbox"/>	<input type="text"/> Kbps	<input type="checkbox"/>	<input type="text"/> Kbps	<input type="checkbox"/>	<input type="text"/> Kbps
2	<input type="checkbox"/>	<input type="text"/> Kbps	<input type="checkbox"/>	<input type="text"/> Kbps	<input type="checkbox"/>	<input type="text"/> Kbps
3	<input type="checkbox"/>	<input type="text"/> Kbps	<input type="checkbox"/>	<input type="text"/> Kbps	<input type="checkbox"/>	<input type="text"/> Kbps
4	<input type="checkbox"/>	<input type="text"/> Kbps	<input type="checkbox"/>	<input type="text"/> Kbps	<input type="checkbox"/>	<input type="text"/> Kbps
5	<input type="checkbox"/>	<input type="text"/> Kbps	<input type="checkbox"/>	<input type="text"/> Kbps	<input type="checkbox"/>	<input type="text"/> Kbps
6	<input type="checkbox"/>	<input type="text"/> Kbps	<input type="checkbox"/>	<input type="text"/> Kbps	<input type="checkbox"/>	<input type="text"/> Kbps
7	<input type="checkbox"/>	<input type="text"/> Kbps	<input type="checkbox"/>	<input type="text"/> Kbps	<input type="checkbox"/>	<input type="text"/> Kbps
8	<input type="checkbox"/>	<input type="text"/> Kbps	<input type="checkbox"/>	<input type="text"/> Kbps	<input type="checkbox"/>	<input type="text"/> Kbps
9	<input type="checkbox"/>	<input type="text"/> Kbps	<input type="checkbox"/>	<input type="text"/> Kbps	<input type="checkbox"/>	<input type="text"/> Kbps
10	<input type="checkbox"/>	<input type="text"/> Kbps	<input type="checkbox"/>	<input type="text"/> Kbps	<input type="checkbox"/>	<input type="text"/> Kbps
11	<input type="checkbox"/>	<input type="text"/> Kbps	<input type="checkbox"/>	<input type="text"/> Kbps	<input type="checkbox"/>	<input type="text"/> Kbps
12	<input type="checkbox"/>	<input type="text"/> Kbps	<input type="checkbox"/>	<input type="text"/> Kbps	<input type="checkbox"/>	<input type="text"/> Kbps

Apply Cancel

The following table describes the labels in this screen.

Table 31 Bandwidth Control

LABEL	DESCRIPTION
Active	Select this check box to activate bandwidth control.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Ingress Rate	
Active	Select this check box to activate commit rate limits on this port.
Commit Rate	Specify the guaranteed bandwidth allowed in kilobits per second (Kbps) for the incoming traffic flow on a port. The commit rate should be less than the peak rate. The sum of commit rates cannot be greater than or equal to the uplink bandwidth.
Active	Select this check box to activate peak rate limits on this port.
Peak Rate	Specify the maximum bandwidth allowed in kilobits per second (Kbps) for the incoming traffic flow on a port.
Active	Select this check box to activate egress rate limits on this port.
Egress Rate	Specify the maximum bandwidth allowed in kilobits per second (Kbps) for the out-going traffic flow on a port. Enter a number between 1 and 1000000.
Apply	Click Apply to save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to your previous configuration.

Broadcast Storm Control

13.1 Introducing Broadcast Storm Control

Broadcast storm control limits the number of broadcast, multicast and destination lookup failure (DLF) packets the switch receives per second on the ports. When the maximum number of allowable broadcast, multicast and/or DLF packets is reached per second, the subsequent packets are discarded. Enable this feature to reduce broadcast, multicast and/or DLF packets in your network. You can specify limits for each packet type on each port.

13.2 Configuring Broadcast Storm Control

Click **Advanced Application, Broadcast Storm Control** in the navigation panel to display the screen as shown next.

Figure 56 Broadcast Storm Control

Port	Broadcast (pkt/s)	Multicast (pkt/s)	DLF (pkt/s)
*	<input type="checkbox"/> []	<input type="checkbox"/> []	<input type="checkbox"/> []
1	<input type="checkbox"/> 0	<input type="checkbox"/> 0	<input type="checkbox"/> 0
2	<input type="checkbox"/> 0	<input type="checkbox"/> 0	<input type="checkbox"/> 0
3	<input type="checkbox"/> 0	<input type="checkbox"/> 0	<input type="checkbox"/> 0
4	<input type="checkbox"/> 0	<input type="checkbox"/> 0	<input type="checkbox"/> 0
5	<input type="checkbox"/> 0	<input type="checkbox"/> 0	<input type="checkbox"/> 0
6	<input type="checkbox"/> 0	<input type="checkbox"/> 0	<input type="checkbox"/> 0
7	<input type="checkbox"/> 0	<input type="checkbox"/> 0	<input type="checkbox"/> 0
8	<input type="checkbox"/> 0	<input type="checkbox"/> 0	<input type="checkbox"/> 0
9	<input type="checkbox"/> 0	<input type="checkbox"/> 0	<input type="checkbox"/> 0
10	<input type="checkbox"/> 0	<input type="checkbox"/> 0	<input type="checkbox"/> 0
11	<input type="checkbox"/> 0	<input type="checkbox"/> 0	<input type="checkbox"/> 0
12	<input type="checkbox"/> 0	<input type="checkbox"/> 0	<input type="checkbox"/> 0

Apply Cancel

The following table describes the labels in this screen.

Table 32 Broadcast Storm Control

LABEL	DESCRIPTION
Active	Select this check box to enable traffic storm control on the switch.
Port	This field displays a port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Broadcast (pkt/s)	Select this option and specify the maximum number of broadcast packets the port can receive per second.
Multicast (pkt/s)	Select this option and specify the maximum number of multicast packets the port can receive per second.
DLF (pkt/s)	Select this option and specify the maximum number of destination lookup failure (DLF) packets the port can receive per second.
Apply	Click Apply to save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

Mirroring

This chapter discusses the Mirror setup screens.

14.1 Introduction to Port Mirroring

Port mirroring allows you to copy a traffic flow to a monitor port (the port you copy the traffic to) in order that you can examine the traffic from the monitor port without interference.

14.2 Port Mirroring Configuration

Click **Advanced Application, Mirroring** in the navigation panel to display the **Mirroring** screen.

Use this screen to select a monitor port and specify the traffic flow to be copied to the monitor port.

Figure 57 Mirroring

Port	Mirrored	Direction
*	<input type="checkbox"/>	Ingress
1	<input type="checkbox"/>	Ingress
2	<input type="checkbox"/>	Ingress
3	<input type="checkbox"/>	Ingress
4	<input type="checkbox"/>	Ingress
5	<input type="checkbox"/>	Ingress
6	<input type="checkbox"/>	Ingress
7	<input type="checkbox"/>	Ingress
8	<input type="checkbox"/>	Ingress
9	<input type="checkbox"/>	Ingress
10	<input type="checkbox"/>	Ingress
11	<input type="checkbox"/>	Ingress
12	<input type="checkbox"/>	Ingress

The following table describes the related labels in this screen.

Table 33 Mirroring

LABEL	DESCRIPTION
Active	Clear this check box to deactivate port mirroring on the switch.
Monitor Port	The monitor port is the port you copy the traffic to in order to examine it in more detail without interfering with the traffic flow on the original port(s). Select this port from this drop-down list box.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Mirrored	Select this option to mirror the traffic on a port.
Direction	Specify the direction of the traffic to mirror. Choices are Egress (outgoing), Ingress (incoming) and Both .
Apply	Click Apply to save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields.

Link Aggregation

This chapter shows you how to logically aggregate physical links to form one logical, higher-bandwidth link.

15.1 Introduction to Link Aggregation

Link aggregation (trunking) is the grouping of physical ports into one logical higher-capacity link. You may want to trunk ports if for example, it is cheaper to use multiple lower-speed links than to under-utilize a high-speed, but more costly, single-port link. Link aggregation also allows port redundancy, that is, if a port fails, the traffic automatically goes through another trunk group member port.

However, the more ports you aggregate then the fewer available ports you have. A trunk group is one logical link containing multiple ports.

The beginning port of each trunk group must be physically connected to form a trunk group.

15.1.1 Dynamic Link Aggregation

The switch adheres to the 802.3ad standard for static and dynamic (LACP) port trunking.

The switch supports the link aggregation IEEE802.3ad standard. This standard describes the Link Aggregate Control Protocol (LACP), which is a protocol that dynamically creates and manages trunk groups.

When you enable LACP link aggregation on a port, the port can automatically negotiate with the ports at the remote end of a link to establish trunk groups.

Please note that:

- You must connect all ports point-to-point to the same Ethernet switch and configure the ports for LACP trunking.
- LACP only works on full-duplex links.
- All ports in the same trunk group must have the same media type, speed, duplex mode and flow control settings.

Configure trunk groups or LACP before you connect the Ethernet switch to avoid causing network topology loops.

15.1.2 Link Aggregation ID

LACP aggregation ID consists of the following information:

Table 34 Link Aggregation ID: Local Switch

SYSTEM PRIORITY	MAC ADDRESS	KEY	PORT PRIORITY	PORT NUMBER
0000	00-00-00-00-00	0000	00	0000

Table 35 Link Aggregation ID: Peer Switch

SYSTEM PRIORITY	MAC ADDRESS	KEY	PORT PRIORITY	PORT NUMBER
0000	00-00-00-00-00	0000	00	0000

15.2 Link Aggregation Protocol Status

Click **Advanced Application**, **Link Aggregation** in the navigation panel to display the **Link Aggregation Protocol Status** screen.

Figure 58 Link Aggregation: Link Aggregation Protocol Status

Index	Aggregator ID	Enabled Ports	Synchronized Ports
1	[(0000,00-00-00-00-00-00,0000,00,0000)] [(0000,00-00-00-00-00-00,0000,00,0000)]	-	-
2	[(0000,00-00-00-00-00-00,0000,00,0000)] [(0000,00-00-00-00-00-00,0000,00,0000)]	-	-
3	[(0000,00-00-00-00-00-00,0000,00,0000)] [(0000,00-00-00-00-00-00,0000,00,0000)]	-	-
4	[(0000,00-00-00-00-00-00,0000,00,0000)] [(0000,00-00-00-00-00-00,0000,00,0000)]	-	-
5	[(0000,00-00-00-00-00-00,0000,00,0000)] [(0000,00-00-00-00-00-00,0000,00,0000)]	-	-
6	[(0000,00-00-00-00-00-00,0000,00,0000)] [(0000,00-00-00-00-00-00,0000,00,0000)]	-	-

The following table describes the labels in this screen.

Table 36 Link Aggregation: Link Aggregation Protocol Status

LABEL	DESCRIPTION
Index	This field displays the trunk ID to identify a trunk group, that is, one logical link containing multiple ports.
Aggregator ID	This field displays the link aggregation ID. Link aggregation ID consists of the following: system priority, MAC address, key, port priority and port number. Refer to Section 15.1.2 on page 120 for more information on this field.
Enabled Port	These are the ports you have configured in the Link Aggregation screen to be in the trunk group.
Synchronized Ports	These are the ports that are currently transmitting data as one logical link in this trunk group.

15.3 Link Aggregation Setup

Click **Configuration** in the **Link Aggregation Protocol Status** screen to display the screen shown next.

You can configure up to six link aggregation groups and each group can aggregate up to eight ports.

Figure 59 Link Aggregation: Configuration

Link Aggregation Status

Link Aggregation Control Protocol

Active

System Priority

Group ID	Active	Dynamic(LACP)
T1	<input type="checkbox"/>	<input type="checkbox"/>
T2	<input type="checkbox"/>	<input type="checkbox"/>
T3	<input type="checkbox"/>	<input type="checkbox"/>
T4	<input type="checkbox"/>	<input type="checkbox"/>
T5	<input type="checkbox"/>	<input type="checkbox"/>
T6	<input type="checkbox"/>	<input type="checkbox"/>

Port	Group	LACP Timeout
*	-	30 seconds
1	None	30 seconds
2	None	30 seconds
3	None	30 seconds
4	None	30 seconds
5	None	30 seconds
6	None	30 seconds
7	None	30 seconds
8	None	30 seconds
9	None	30 seconds
10	None	30 seconds
11	None	30 seconds
12	None	30 seconds

Apply Cancel

The following table describes the labels in this screen.

Table 37 Link Aggregation: Configuration

LABEL	DESCRIPTION
Link Aggregation Control Protocol	
Active	Select this checkbox to enable Link Aggregation Control Protocol (LACP).

Table 37 Link Aggregation: Configuration (continued)

LABEL	DESCRIPTION
System Priority	LACP system priority is a number between 1 and 65,535. The switch with the lowest system priority (and lowest port number if system priority is the same) becomes the LACP “server”. The LACP “server” controls the operation of LACP setup. Enter a number to set the priority of an active port using Link Aggregate Control Protocol (LACP). The smaller the number, the higher the priority level.
Group ID	The field identifies the link aggregation group, that is, one logical link containing multiple ports
Active	Select this option to activate a trunk group.
Dynamic (LACP)	Select this check box to enable LACP for a trunk.
Port	This field displays the port number.
*	<p>Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis.</p> <p>Note: Changes in this row are copied to all the ports as soon as you make them.</p>
Group	Select the trunk group to which a port belongs.
LACP Timeout	<p>Timeout is the time interval between the individual port exchanges of LACP packets in order to check that the peer port in the trunk group is still up. If a port does not respond after three tries, then it is deemed to be “down” and is removed from the trunk. Set a short timeout (one second) for busy trunked links to ensure that disabled ports are removed from the trunk group as soon as possible.</p> <p>Select either 1 second or 30 seconds.</p>
Apply	Click Apply to save your changes to the switch’s run-time memory. The switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

Port Authentication

This chapter describes the 802.1x authentication method and RADIUS server connection setup.

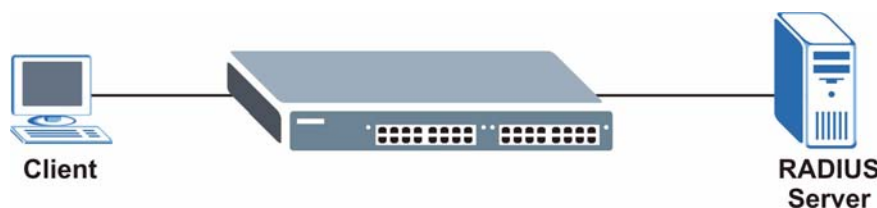
16.1 Introduction to Authentication

IEEE 802.1x is an extended authentication protocol¹ that allows support of RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile management on a network RADIUS server.

16.1.1 RADIUS

RADIUS (Remote Authentication Dial-In User Service) authentication is a popular protocol used to authenticate users by means of an external server instead of (or in addition to) an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS authentication allows you to validate an unlimited number of users from a central location.

Figure 60 RADIUS Server



16.1.1.1 Vendor Specific Attribute

A Vendor Specific Attribute (VSA) is an attribute-value pair that is sent between a RADIUS server and the switch. Configure VSAs on the RADIUS server to set the switch to perform the following actions on an authenticated user:

- Limit bandwidth on incoming or outgoing traffic
- Assign account privilege levels

1. At the time of writing, Windows XP of the Microsoft operating systems supports 802.1x. See the Microsoft web site for information on other Windows operating system support. For other operating systems, see its documentation. If your operating system does not support 802.1x, then you may need to install 802.1x client software.



Refer to the documentation that comes with your RADIUS server on how to configure a VSA.

The following table describes the VSAs supported on the switch.

Table 38 Supported VSA

FUNCTION	ATTRIBUTE
Ingress Bandwidth Assignment	Vendor-Id = 890 (ZyXEL) Vendor-Type = 1 Vendor-data = ingress rate (decimal)
Egress Bandwidth Assignment	Vendor-Id = 890 (ZyXEL) Vendor-Type = 2 Vendor-data = egress rate (decimal)
Privilege Assignment	Vendor-ID = 890 (ZyXEL) Vendor-Type = 3 Vendor-Data = " shell:priv-lvl=N " or Vendor-ID = 9 (CISCO) Vendor-Type = 1 (CISCO-AVPAIR) Vendor-Data = " shell:priv-lvl=N " where N is a privilege level (from 0 to 14). Note: If you set the privilege level of a login account differently on the RADIUS server(s) and the switch, the user is assigned a privilege level from the database (RADIUS or local) the switch uses first for user authentication.

16.1.1.2 Tunnel Protocol Attribute

You can configure tunnel protocol attributes on the RADIUS server to assign a port on the switch to a VLAN (fixed, untagged). This will also set the port's VID. Refer to RFC 3580 for more information.

Table 39 Supported Tunnel Protocol Attribute

FUNCTION	ATTRIBUTE
VLAN Assignment	Tunnel-Type = VLAN (13) Tunnel-Medium-Type = 802 (6) Tunnel-Private-Group-ID = VLAN ID Note: You must also create a VLAN with the specified VID on the switch.

16.2 Configuring Port Authentication

To enable port authentication, first activate IEEE802.1x security (both on the switch and the port(s)) then configure the RADIUS server settings.

Click **Port Authentication** under **Advanced Application** in the navigation panel to display the screen as shown.

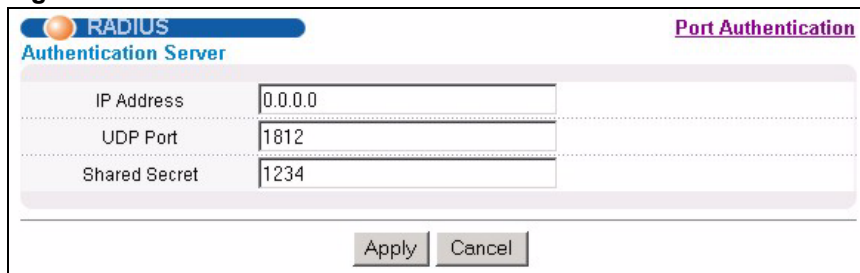
Figure 61 Port Authentication



16.2.1 Configuring RADIUS Server Settings

Use this screen to configure your RADIUS server settings. See [Section 16.1.1 on page 123](#) for more information on RADIUS servers. From the **Port Authentication** screen, click **RADIUS** to display the configuration screen as shown.

Figure 62 Port Authentication: RADIUS



The following table describes the labels in this screen.

Table 40 Port Authentication: RADIUS

LABEL	DESCRIPTION
Authentication Server	
IP Address	Enter the IP address of the external RADIUS server in dotted decimal notation.
UDP Port	The default port of the RADIUS server for authentication is 1812 . You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external RADIUS server and the switch. This key is not sent over the network. This key must be the same on the external RADIUS server and the switch.
Apply	Click Apply to save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

16.2.2 Configuring IEEE802.1x

Use this screen to activate IEEE 802.1x security. From the **Port Authentication** screen, click **802.1x** to display the configuration screen as shown.

Figure 63 Port Authentication: 802.1x

Port	Active	Reauthentication	Reauthentication Timer
*	<input type="checkbox"/>	On	seconds
1	<input type="checkbox"/>	On	3600 seconds
2	<input type="checkbox"/>	On	3600 seconds
3	<input type="checkbox"/>	On	3600 seconds
4	<input type="checkbox"/>	On	3600 seconds
5	<input type="checkbox"/>	On	3600 seconds
6	<input type="checkbox"/>	On	3600 seconds
7	<input type="checkbox"/>	On	3600 seconds
8	<input type="checkbox"/>	On	3600 seconds
9	<input type="checkbox"/>	On	3600 seconds
10	<input type="checkbox"/>	On	3600 seconds
11	<input type="checkbox"/>	On	3600 seconds
12	<input type="checkbox"/>	On	3600 seconds

The following table describes the labels in this screen.

Table 41 Port Authentication: 802.1x

LABEL	DESCRIPTION
Active	Select this check box to permit 802.1x authentication on the switch. Note: You must first allow 802.1x authentication on the switch before configuring it on each port.
Port	This field displays a port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this checkbox to permit 802.1x authentication on this port. You must first allow 802.1x authentication on the switch before configuring it on each port.
Reauthentication	Specify if a subscriber has to periodically re-enter his or her username and password to stay connected to the port.

Table 41 Port Authentication: 802.1x (continued)

LABEL	DESCRIPTION
Reauthentication Timer	Specify how often a client has to re-enter his or her username and password to stay connected to the port.
Apply	Click Apply to save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

Port Security

This chapter shows you how to set up port security.

17.1 About Port Security

Port security allows only packets with dynamically learned MAC addresses and/or configured static MAC addresses to pass through a port on the switch. The switch can learn up to 16K MAC addresses in total with no limit on individual ports other than the sum cannot exceed 16K.

For maximum port security, enable this feature, disable MAC address learning and configure static MAC address(es) for a port. It is not recommended you disable port security together with MAC address learning as this will result in many broadcasts.

17.2 Port Security Setup

Click **Advanced Application, Port Security** in the navigation panel to display the screen as shown.

Figure 64 Port Security

Port	Active	Address Learning	Limited Number of Learned MAC Address
*	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text"/>
1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
5	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
7	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
8	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
9	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
10	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
11	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
12	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>

The following table describes the labels in this screen.

Table 42 Port Security

LABEL	DESCRIPTION
Active	Select this check box to enable the port security feature on the switch.
Port	This field displays a port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to enable the port security feature on this port. The switch forwards packets whose MAC address(es) is in the MAC address table on this port. Packets with no matching MAC address(es) are dropped. Clear this check box to disable the port security feature. The switch forwards all packets on this port.
Address Learning	MAC address learning reduces outgoing broadcast traffic. For MAC address learning to occur on a port, the port itself must be active with address learning enabled.
Limited Number of Learned MAC Address	Use this field to limit the number of (dynamic) MAC addresses that may be learned on a port. For example, if you set this field to "5" on port 2, then only the devices with these five learned MAC addresses may access port 2 at any one time. A sixth device would have to wait until one of the five learned MAC addresses aged out. MAC-address aging out time can be set in the Switch Setup screen. The valid range is from 0 to 16K (16384 bytes). 0 means this feature is disabled, so the switch will learn MAC addresses up to the global limit of 16K.

Table 42 Port Security (continued)

LABEL	DESCRIPTION
Apply	Click Apply to save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

Classifier

This chapter introduces and shows you how to configure the packet classifier on the switch.

18.1 About the Classifier and QoS

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical application such as video-on-demand.

A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming port number. For example, you can configure a classifier to select traffic from the same protocol port (such as Telnet) to form a flow.

Configure QoS on the switch to group and prioritize application traffic and fine-tune network performance. Setting up QoS involves two separate steps:

- 1 Configure classifiers to sort traffic into different flows.
- 2 Configure policy rules to define actions to be performed for a classified traffic flow (refer to [Chapter 19 on page 139](#) to configure policy rules).

18.2 Configuring the Classifier

Use the **Classifier** screen to define the classifiers. After you define the classifier, you can specify actions (or policy) to act upon the traffic that matches the rules. To configure policy rules, refer to [Chapter 19 on page 139](#).

Click **Advanced Application** and **Classifier** in the navigation panel to display the configuration screen as shown.

Figure 65 Classifier

The following table describes the labels in this screen.

Table 43 Classifier

LABEL	DESCRIPTION
Active	Select this option to enable this rule.
Name	Enter a descriptive name for this rule for identifying purposes.
Packet Format	Specify the format of the packet. Choices are All , 802.3 tagged , 802.3 untagged , Ethernet II tagged and Ethernet II untagged . A value of 802.3 indicates that the packets are formatted according to the IEEE 802.3 standards. A value of Ethernet II indicates that the packets are formatted according to RFC 894, Ethernet II encapsulation.
Layer 2	Specify the fields below to configure a layer 2 classifier.
VLAN	Select Any to classify traffic from any VLAN or select the second option and specify the source VLAN ID in the field provided.
Priority	Select Any to classify traffic from any priority level or select the second option and specify a priority level in the field provided.

Table 43 Classifier (continued)

LABEL	DESCRIPTION
Ethernet Type	Select an Ethernet type or select Others and enter the Ethernet type number in hexadecimal value. Refer to Table 45 on page 136 for information.
Source	
MAC Address	Select Any to apply the rule to all MAC addresses. To specify a source, select the second choice and type a MAC address in valid MAC address format (six hexadecimal character pairs).
Port	Type the port number to which the rule should be applied. You may specify one port only or all ports (Any).
Destination	
MAC Address	Select Any to apply the rule to all MAC addresses. To specify a destination, select the second choice and type a MAC address in valid MAC address format (six hexadecimal character pairs).
Layer 3 Specify the fields below to configure a layer 3 classifier.	
DSCP	Select Any to classify traffic from any DSCP or select the second option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.
IP Protocol	Select an IP protocol type or select Others and enter the protocol number in decimal value. Refer to Table 46 on page 137 for more information. You may select Establish Only for TCP protocol type. This means that the switch will pick out the packets that are sent to establish TCP connections.
Source	
IP Address/ Address Prefix	Enter a source IP address in dotted decimal notation. Specify the address prefix by entering the number of ones in the subnet mask.
Socket Number	Note: You MUST select either UDP or TCP in the IP Protocol field before you configure the socket numbers. Select Any to apply the rule to all TCP/UDP protocol port numbers or select the second option and enter a TCP/UDP protocol port number.
Destination	
IP Address/ Address Prefix	Enter a destination IP address in dotted decimal notation. Specify the address prefix by entering the number of ones in the subnet mask.
Socket Number	Note: You MUST select either UDP or TCP in the IP Protocol field before you configure the socket numbers. Select Any to apply the rule to all TCP/UDP protocol port numbers or select the second option and enter a TCP/UDP protocol port number.
Add	Click Add to insert the entry in the summary table below and save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields back to your previous configuration.
Clear	Click Clear to set the above fields back to the factory defaults.

18.3 Viewing and Editing Classifier Configuration

To view a summary of the classifier configuration, scroll down to the summary table at the bottom of the **Classifier** screen. To change the settings of a rule, click a number in the **Index** field.



When two rules conflict with each other, a higher layer rule has priority over lower layer rule.

Figure 66 Classifier: Summary Table

Index	Active	Name	Rule	Delete
1	Yes	Example	EtherType = IP; SrcMac = 00:50:ba:ad:4f:81; SrcPort = port 2;	<input type="checkbox"/>

Delete Cancel

The following table describes the labels in this screen.

Table 44 Classifier: Summary Table

LABE L	DESCRIPTION
Index	This field displays the index number of the rule. Click an index number to edit the rule.
Active	This field displays Yes when the rule is activated and No when it is deactivated.
Name	This field displays the descriptive name for this rule. This is for identification purpose only.
Rule	This field displays a summary of the classifier rule's settings.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the Delete check boxes.

The following table shows some other common Ethernet types and the corresponding protocol number.

Table 45 Common Ethernet Types and Protocol Number

ETHERNET TYPE	PROTOCOL NUMBER
IP ETHII	0800
X.75 Internet	0801
NBS Internet	0802
ECMA Internet	0803
Chaosnet	0804
X.25 Level 3	0805
XNS Compat	0807
Banyan Systems	0BAD
BBN Simnet	5208
IBM SNA	80D5
AppleTalk AARP	80F3

Some of the most common IP ports are:

Table 46 Common IP Ports

PORT NUMBER	PORT NAME
21	FTP
23	Telnet
25	SMTP
53	DNS
80	HTTP
110	POP3

18.4 Classifier Example

The following figure shows an example where you configure a classifier that identifies all traffic from MAC address 00:50:ba:ad:4f:81 on port 2.

After you have configured a classifier, you can configure a policy (in the **Policy** screen) to define action(s) on the classified traffic flow.

Figure 67 Classifier: Example

Classifier

Active

Name

Packet Format

Layer 2

VLAN Any

Priority Any

Ethernet Type All
 Others (Hex)

Source

MAC Address Any
 MAC : : : : :

Port Any

Destination

MAC Address Any
 MAC : : : : :

Layer 3

DSCP Any

IP Protocol All Establish Only
 Others (Dec)

Source

IP Address / Address Prefix /

Socket Number Any

Destination

IP Address / Address Prefix /

Socket Number Any

Policy Rule

This chapter shows you how to configure policy rules.

19.1 About Policy Rules

A classifier distinguishes traffic into flows based on the configured criteria (refer to [Chapter 18 on page 133](#) for more information). A policy rule ensures that a traffic flow gets the requested treatment in the network.

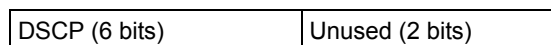
19.1.1 DiffServ

DiffServ (Differentiated Services) is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

19.1.2 DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.



The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different kinds of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

19.2 Configuring Policy Rules



You must first configure a classifier in the **Classifier** screen. Refer to [Chapter 18 on page 133](#) for more information.

Click **Advanced Applications** and then **Policy Rule** in the navigation panel to display the screen as shown.

Figure 68 Policy

Policy							
Active	<input type="checkbox"/>						
Name	<input type="text"/>						
Classifier(s)	<input type="text"/>						
Parameters	<table border="0"> <tr> <td>VLAN ID</td> <td><input type="text"/></td> <td>General</td> <td><input type="text"/></td> <td>Metering</td> <td><input type="text"/></td> Kbps</tr></table>	VLAN ID	<input type="text"/>	General	<input type="text"/>	Metering	<input type="text"/>
	VLAN ID	<input type="text"/>	General	<input type="text"/>	Metering	<input type="text"/>	
	Egress Port	<input type="text" value="1"/>	Bandwidth	<input type="text"/>	Out-of-Profile	<input type="text"/>	
	Outgoing packet format for Egress port	<input checked="" type="radio"/> Tag <input type="radio"/> Untag		DSCP	<input type="text"/>		
	Priority	<input type="text" value="0"/>					
	DSCP	<input type="text"/>					
	TOS	<input type="text" value="0"/>					

| Action | Forwarding |
| No change |
| Discard the packet |
| Do not drop the matching frame previously marked for dropping |
| Priority |
| No change |
| Set the packet's 802.1 priority |
| Send the packet to priority queue |
| Replace the 802.1 priority field with the IP TOS value |
| Diffserv |
| No change |
| Set the packet's TOS field |
| Replace the IP TOS field with the 802.1 priority value |
| Set the Diffserv Codepoint field in the frame |
| Outgoing |
| Send the packet to the mirror port |
| Send the packet to the egress port |
| Send the matching frames(broadcast or DLF, multicast, marked for dropping or to be sent to the CPU) to the egress port |
| Set the packet's VLAN ID |
| Metering |
| Enable |
| Out-of-profile action |
| Drop the packet |
| Change the DSCP value |
| Set Out-Drop Precedence |
| Do not drop the matching frame previously marked for dropping |
| | |

The following table describes the labels in this screen.

Table 47 Policy

LABEL	DESCRIPTION
Active	Select this option to enable the policy.
Name	Enter a descriptive name for identification purposes.
Classifier(s)	This field displays the active classifier(s) you configure in the Classifier screen (refer to Chapter 18 on page 133). Select the classifier(s) to which this policy rule applies. To select more than one classifier, press [SHIFT] and select the choices at the same time.
Parameters Set the fields below for this policy. You only have to set the field(s) that is related to the action(s) you configure in the Action field.	
General	
VLAN ID	Specify a VLAN ID number.
Egress Port	Type the number of an outgoing port.
Outgoing packet format for Egress Port	Select Tag to add the specified VID to packets on the specified outgoing port. Otherwise, select Untag .
Priority	Specify a priority level.
DSCP	Specify a DSCP (DiffServ Code Point) number between 0 and 63.
TOS	Specify the type of service (TOS) priority level.
Metering	You can configure the desired bandwidth available to a traffic flow. Traffic that exceeds the maximum bandwidth allocated (in cases where the network is congested) is called out-of-profile traffic.
Bandwidth	Specify the bandwidth in kilobits per second (Kbps). Enter a number between 1 and 1000000.
Out of Profile DSCP	Specify a new DSCP number (between 0 and 63) if you want to replace or remark the DSCP number for out-of-profile traffic.
Action Specify the action(s) the switch takes on the associated classified traffic flow.	
Forwarding	Select No change to forward the packets. Select Discard packet to drop the packets. Select Do not drop the matching frame previously marked for dropping to retain the frames that were marked to be dropped before.
Priority	Select No change to keep the priority setting of the frames. Select Set the packet's 802.1 priority to replace the 802.1 priority field with the value you set in the Priority field. Select Send the packet to priority queue to put the packets in the designated queue. Select Replace the 802.1 priority field with IP TOS value to replace the 802.1 priority field with the value you set in the TOS field.

Table 47 Policy (continued)

LABEL	DESCRIPTION
DiffServ	Select No change to keep the TOS and/or DSCP fields in the packets. Select Set the packet's TOS field to set the TOS field with the value you configure in the TOS field. Select Replace the IP TOS with the 802.1 priority value to replace the TOS field with the value you configure in the Priority field. Select Set the Diffserv Codepoint field in the frame to set the DSCP field with the value you configure in the DSCP field.
Outgoing	Select Send the packet to the mirror port to send the packet to the mirror port. Select Send the packet to the egress port to send the packet to the egress port. Select Send the matching frames (broadcast or DLF, multicast, marked for dropping or to be sent to the CPU) to the egress port to send the broadcast, multicast, DLF, marked-to-drop or CPU frames to the egress port. Select Set the packet's VLANID to set the VLAN ID of the packet with the value you configure in the VLANID field.
Metering	Select Enable to activate bandwidth limitation on the traffic flow(s) then set the actions to be taken on out-of-profile packets.
Out-of-profile action	Select the action(s) to be performed for out-of-profile traffic. Select Drop the packet to discard the out-of-profile traffic. Select Change the DSCP Value to replace the DSCP field with the value specified in the Out of profile DSCP field. Set Out-Drop Precedence is related to the metering bandwidth setting. The switch marks traffic that is higher than the metering bandwidth setting as drop precedence. Select Set Out-Drop Precedence to drop packets that are marked drop-precedence first when there is traffic congestion. Select Do not drop the matching frame previously marked for dropping to queue the frames that are marked to be dropped.
Add	Click Add to insert the entry to the summary table below and save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields back to your previous configuration.
Clear	Click Clear to set the above fields back to the factory defaults.

19.3 Viewing and Editing Policy Configuration

To view a summary of the classifier configuration, scroll down to the summary table at the bottom of the **Policy** screen. To change the settings of a rule, click a number in the **Index** field.

Figure 69 Policy: Summary Table

Index	Active	Name	Classifier(s)	Delete
1	Yes	Test	Example;	<input type="checkbox"/>

The following table describes the labels in this screen.

Table 48 Policy: Summary Table

LABEL	DESCRIPTION
Index	This field displays the policy index number. Click an index number to edit the policy.
Active	This field displays Yes when policy is activated and No when it is deactivated.
Name	This field displays the descriptive name for this policy. This is for identification purposes only.
Classifier(s)	This field displays the name(s) of the classifier to which this policy applies.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the Delete check boxes.

19.4 Policy Example

The figure below shows an example **Policy** screen where you configure a policy to limit bandwidth and discard out-of-band traffic on a traffic flow classified using the **Example** classifier (refer to [Section 18.4 on page 137](#)).

Figure 70 Policy Example

Policy

Active	<input checked="" type="checkbox"/>	
Name	Test	
Classifier(s)	<div style="border: 1px solid gray; padding: 2px;"> Example </div>	

	General	Metering
Parameters	VLAN ID: <input type="text" value="1"/>	Bandwidth: <input type="text" value="10000"/> Kbps
	Egress Port: <input type="text" value="1"/>	Out-of-Profile: <input type="text"/>
	Outgoing packet format for Egress port: <input checked="" type="radio"/> Tag <input type="radio"/> Untag	DSCP: <input type="text"/>
	Priority: <input type="text" value="0"/>	
	DSCP: <input type="text"/>	
	TOS: <input type="text" value="0"/>	

	Action
Forwarding	<input checked="" type="radio"/> No change <input type="radio"/> Discard the packet <input type="radio"/> Do not drop the matching frame previously marked for dropping
Priority	<input checked="" type="radio"/> No change <input type="radio"/> Set the packet's 802.1 priority <input type="radio"/> Send the packet to priority queue <input type="radio"/> Replace the 802.1 priority field with the IP TOS value
Diffserv	<input checked="" type="radio"/> No change <input type="radio"/> Set the packet's TOS field <input type="radio"/> Replace the IP TOS field with the 802.1 priority value <input type="radio"/> Set the Diffserv Codepoint field in the frame
Outgoing	<input type="checkbox"/> Send the packet to the mirror port <input type="checkbox"/> Send the packet to the egress port <input type="checkbox"/> Send the matching frames(broadcast or DLF, multicast, marked for dropping or to be sent to the CPU) to the egress port <input type="checkbox"/> Set the packet's VLAN ID
Metering	<input checked="" type="checkbox"/> Enable <div style="margin-left: 20px;"> <input checked="" type="checkbox"/> Drop the packet <input type="checkbox"/> Change the DSCP value <input type="checkbox"/> Set Out-Drop Precedence <input type="checkbox"/> Do not drop the matching frame previously marked for dropping </div>

Queuing Method

This chapter introduces SPQ and WFQ.

20.1 Introduction to Queuing

Queuing is used to help solve performance degradation when there is network congestion. Use the **Queuing Method** screen to configure queuing algorithms for outgoing traffic. See also **Priority Queue Assignment in Switch Setup** and **802.1p Priority in Port Setup** for related information.

Queuing algorithms allow switches to maintain separate queues for packets from each individual source or flow and prevent a source from monopolizing the bandwidth.

The switch has eight physical queues, Q0 to Q7. Q7 has the highest priority and Q0 has the lowest.

Table 49 Physical Queue Priority

QUEUE	PRIORITY
Q7	8 (highest)
Q6	7
Q5	6
Q4	5
Q3	4
Q2	3
Q1	2
Q0	1 (lowest)

20.1.1 Strict Priority Queuing (SPQ)

Strict Priority Queuing (SPQ) services queues based on priority only. As traffic comes into the switch, traffic on the highest priority queue, Q7 is transmitted first. When that queue empties, traffic on the next highest-priority queue, Q6 is transmitted until Q6 empties, and then traffic is transmitted on Q5 and so on. If higher priority queues never empty, then traffic on lower priority queues never gets sent. SPQ does not automatically adapt to changing network requirements.

20.1.2 Weighted Round Robin Scheduling (WRR)

Round Robin Scheduling services queues on a rotating basis and is activated only when a port has more traffic than it can handle. A queue is given an amount of bandwidth irrespective of the incoming traffic on that port. This queue then moves to the back of the list. The next queue is given an equal amount of bandwidth, and then moves to the end of the list; and so on, depending on the number of queues being used. This works in a looping fashion until a queue is empty.

Weighted Round Robin Scheduling (WRR) uses the same algorithm as round robin scheduling, but services queues based on their priority and queue weight (the number you configure in the **Weight** field – see [Figure 71 on page 147](#)) rather than a fixed amount of bandwidth. WRR is activated only when a port has more traffic than it can handle. Queues with larger weights get more service than queues with smaller weights. This queuing mechanism is highly efficient in that it divides any available bandwidth across the different traffic queues and returns to queues that have not yet emptied.

20.2 Configuring Queuing

Click **Queuing Method** under **Advanced Application** in the navigation panel.

Figure 71 Queuing Method

Port	Method	Weight							
		Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
1	<input checked="" type="radio"/> SPQ <input type="radio"/> WRR	1	2	3	4	5	6	7	8
2	<input checked="" type="radio"/> SPQ <input type="radio"/> WRR	1	2	3	4	5	6	7	8
3	<input checked="" type="radio"/> SPQ <input type="radio"/> WRR	1	2	3	4	5	6	7	8
4	<input checked="" type="radio"/> SPQ <input type="radio"/> WRR	1	2	3	4	5	6	7	8
5	<input checked="" type="radio"/> SPQ <input type="radio"/> WRR	1	2	3	4	5	6	7	8
6	<input checked="" type="radio"/> SPQ <input type="radio"/> WRR	1	2	3	4	5	6	7	8
7	<input checked="" type="radio"/> SPQ <input type="radio"/> WRR	1	2	3	4	5	6	7	8
8	<input checked="" type="radio"/> SPQ <input type="radio"/> WRR	1	2	3	4	5	6	7	8
9	<input checked="" type="radio"/> SPQ <input type="radio"/> WRR	1	2	3	4	5	6	7	8
10	<input checked="" type="radio"/> SPQ <input type="radio"/> WRR	1	2	3	4	5	6	7	8
11	<input checked="" type="radio"/> SPQ <input type="radio"/> WRR	1	2	3	4	5	6	7	8
12	<input checked="" type="radio"/> SPQ <input type="radio"/> WRR	1	2	3	4	5	6	7	8

Apply Cancel

The following table describes the labels in this screen.

Table 50 Queuing Method

LABEL	DESCRIPTION
Port	This label shows the port you are configuring.
Method	Select SPQ (Strict Priority Queuing) or WRR (Weighted Round Robin) scheduling. Strict Priority Queuing (SPQ) services queues based on priority only. When the highest priority queue empties, traffic on the next highest-priority queue begins. Q7 has the highest priority and Q0 the lowest. WRR services queues on a rotating basis based on their queue weight (the number you configure in the queue Weight field). Queues with larger weights get more service than queues with smaller weights.
Weight	When you select WRR , enter the queue weight here. Bandwidth is divided across the different traffic queues according to their weights. Queues with larger weights get more service than queues with smaller weights.
Apply	Click Apply to save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

Multicast

This chapter shows you how to configure various multicast features.

21.1 Multicast Overview

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender to 1 recipient) or Broadcast (1 sender to everybody on the network). Multicast delivers IP packets to just a group of hosts on the network.

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group - it is not used to carry user data. Refer to RFC 1112 and RFC 2236 for information on IGMP versions 1 and 2 respectively.

21.1.1 IP Multicast Addresses

In IPv4, a multicast address allows a device to send packets to a specific group of hosts (multicast group) in a different subnetwork. A multicast IP address represents a traffic receiving group, not individual receiving devices. IP addresses in the Class D range (224.0.0.0 to 239.255.255.255) are used for IP multicasting. Certain IP multicast numbers are reserved by IANA for special purposes (see the IANA web site for more information).

21.1.2 IGMP Filtering

With the IGMP filtering feature, you can control which IGMP groups a subscriber on a port can join. This allows you to control the distribution of multicast services (such as content information distribution) based on service plans and types of subscription.

You can set the switch to filter the multicast group join reports on a per-port basis by configuring an IGMP filtering profile and associating the profile to a port.

21.1.3 IGMP Snooping

IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a multicast group - it is not used to carry user data. Refer to *RFC 1112* and *RFC 2236* for information on IGMP versions 1 and 2 respectively.

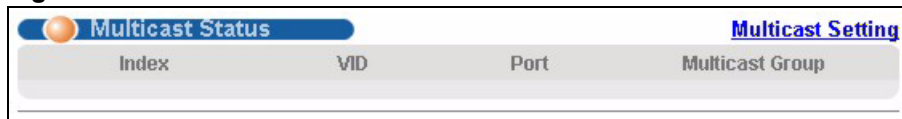
A switch can passively snoop on IGMP Query, Report and Leave (IGMP version 2) packets transferred between IP multicast routers/switches and IP multicast hosts to learn the IP multicast group membership. It checks IGMP packets passing through it, picks out the group registration information, and configures multicasting accordingly. IGMP snooping allows the switch to learn multicast groups without you having to manually configure them.

The switch forwards multicast traffic destined for multicast groups (that it has learned from IGMP snooping or that you have manually configured) to ports that are members of that group. IGMP snooping generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through your switch.

21.2 Multicast Status

Click **Advanced Applications** and **Multicast** to display the screen as shown. This screen shows the multicast group information. See [Section 21.1 on page 149](#) for more information on multicasting.

Figure 72 Multicast Status



Multicast Status		Multicast Setting	
Index	VID	Port	Multicast Group

The following table describes the labels in this screen.

Table 51 Multicast Status

LABEL	DESCRIPTION
Index	This is the index number of the entry.
VID	This field displays the multicast VLAN ID.
Port	This field displays the port number that belongs to the multicast group.
Multicast Group	This field displays IP multicast group addresses.

21.3 Multicast Setup

Click **Advanced Applications**, **Multicast** and the **Multicast Setting** link to display the screen as shown.

Figure 73 Multicast Setting

Multicast Setting [Multicast Status](#) [IGMP Filtering Profile](#) [MVR](#)

IGMP Snooping

Active

Host Timeout

Leave Timeout

802.1p Priority

IGMP Filtering

Active

Unknown Multicast Frame Flooding Drop

Reserved Multicast Group Flooding Drop

Port	Immed. Leave	Group Limited	Max Group Num.	IGMP Filtering Profile	IGMP Querier Mode
*	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	Default	Auto
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>	Default	Auto
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>	Default	Auto
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>	Default	Auto
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>	Default	Auto
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>	Default	Auto
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>	Default	Auto
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>	Default	Auto
8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>	Default	Auto
9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>	Default	Auto
10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>	Default	Auto
11	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>	Default	Auto
12	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>	Default	Auto

The following table describes the labels in this screen.

Table 52 Multicast Setting

LABEL	DESCRIPTION
IGMP Snooping	
Active	Select Active to enable IGMP snooping to forward group multicast traffic only to ports that are members of that group.
Host Timeout	Specify the time (from 1 to 16,711,450) in seconds that elapses before the switch removes an IGMP group membership entry if it does not receive report messages from the host.
Leave Timeout	Enter an IGMP leave timeout value (from 1 to 16,711,450) in seconds. This defines how many seconds the switch waits before removing an IGMP snooping membership entry when an IGMP leave message is received from a host.
802.1p Priority	Select a priority level (0-7) to which the switch changes the priority in outgoing IGMP control packets. Otherwise, select No-Change to not replace the priority.
IGMP Filtering	Select Active to enable IGMP filtering to control which IGMP groups a subscriber on a port can join.

Table 52 Multicast Setting (continued)

LABEL	DESCRIPTION
Unknown Multicast Frame	Specify the action to perform when the switch receives an unknown multicast frame. Select Drop to discard the frame(s). Select Flooding to send the frame(s) to all ports.
Reserved Multicast Group	Multicast addresses (224.0.0.0 to 224.0.0.255) are reserved for the local scope. For examples, 224.0.0.1 is for all hosts in this subnet, 224.0.0.2 is for all multicast routers in this subnet, etc. A router will not forward a packet with the destination IP address within this range. See the IANA web site for more information. Specify the action to perform when the switch receives a frame with a reserved multicast address. Select Drop to discard the frame(s). Select Flooding to send the frame(s) to all ports.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Immed. Leave	Select this option to set the switch to remove this port from the multicast tree when an IGMP version 2 leave message is received on this port. Select this option if there is only one host connected to this port.
Group Limited	Select this option to limit the number of multicast groups this port is allowed to join.
Max Group Num.	Enter the number of multicast groups this port is allowed to join. Once a port is registered in the specified number of multicast groups, any new IGMP join report frame(s) is dropped on this port.
IGMP Filtering Profile	Select the name of the IGMP filtering profile to use for this port. Otherwise, select Default to prohibit the port from joining any multicast group.
IGMP Querier Mode	The switch treats an IGMP query port as being connected to an IGMP multicast router (or server). The switch forwards IGMP join or leave packets to an IGMP query port. Select Auto to have the switch use the port as an IGMP query port if the port receives IGMP query packets. Select Fixed to have the switch always use the port as an IGMP query port. Select this when you connect an IGMP multicast server to the port. Select Edge to stop the switch from using the port as an IGMP query port. The switch will not keep any record of an IGMP router being connected to this port. The switch does not forward IGMP join or leave packets to this port.
Apply	Click Apply to save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

21.4 IGMP Filtering Profile

IGMP filter profiles allow you to control access to IGMP multicast groups. This allows you to have a service available to a specific IGMP multicast group. You can configure an IGMP filter profile for an IGMP multicast group that has access to a service (like a SIP server for example). Within a profile, configure an IGMP filter to specify the multicast IP address ranges. Then assign the IGMP filter profile to the ports (in the **Multicast Setting** screen) that are allowed to use the service.

Click **Advanced Applications** and **Multicast** in the navigation panel. Click the **Multicast Setting** link and then the **IGMP Filtering Profile** link to display the screen as shown.

Figure 74 Multicast: IGMP Filtering Profile

The following table describes the labels in this screen.

Table 53 Multicast: IGMP Filtering Profile

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name for the profile for identification purposes. To configure additional rule(s) for a profile that you have already added, enter the profile name and specify a different IP multicast address range.
Start Address	Type the starting multicast IP address for a range of multicast IP addresses that you want to belong to the IGMP filter profile.
End Address	Type the ending multicast IP address for a range of IP addresses that you want to belong to the IGMP filter profile. If you want to add a single multicast IP address, enter it in both the Start Address and End Address fields.
Add	Click Add to save the profile to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Clear	Click Clear to clear the fields to the factory defaults.
Profile Name	This field displays the descriptive name of the profile.
Start Address	This field displays the start of the multicast address range.
End Address	This field displays the end of the multicast address range.

Table 53 Multicast: IGMP Filtering Profile (continued)

LABEL	DESCRIPTION
Delete	To delete the profile(s) and all the accompanying rules, select the profile(s) that you want to remove in the Delete Profile column, then click the Delete button. To delete a rule(s) from a profile, select the rule(s) that you want to remove in the Delete Rule column, then click the Delete button.
Cancel	Click Cancel to clear the Delete Profile/Delete Rule check boxes.

21.5 MVR Overview

Multicast VLAN Registration (MVR) is designed for applications (such as Media-on-Demand (MoD)) that use multicast traffic across an Ethernet ring-based service provider network.

MVR allows one single multicast VLAN to be shared among different subscriber VLANs on the network. While isolated in different subscriber VLANs, connected devices can subscribe to and unsubscribe from the multicast stream in the multicast VLAN. This improves bandwidth utilization with reduced multicast traffic in the subscriber VLANs and simplifies multicast group management.

You must enable IGMP snooping to use MVR. However, MVR only responds to IGMP join and leave control messages from multicast groups that are configured under MVR. Join and leave reports from other multicast groups are managed by IGMP snooping.

The following figure shows a network example. The subscriber VLAN (1, 2 and 3) information is hidden from the streaming media server, S. In addition, the multicast VLAN information is only visible to the switch and S.

Figure 75 MVR Network Example

21.5.1 Types of MVR Ports

In MVR, a source port is a port on the switch that can send and receive multicast traffic in a multicast VLAN while a receiver port can only receive multicast data. Once configured, the switch maintains a forwarding table that matches the multicast stream to the associated multicast group.

21.5.2 MVR Modes

You can set your switch to operate in either dynamic or compatible mode.

In dynamic mode, the switch sends IGMP leave and join reports to the other multicast devices (such as multicast routers or servers) in the multicast VLAN. This allows the multicast devices to update the multicast forwarding table to forward or not forward multicast traffic to the receiver ports.

In compatible mode, the switch does not send any IGMP reports. In this case, you must manually configure the forwarding settings on the multicast devices in the multicast VLAN.

21.5.3 How MVR Works

The following figure shows a multicast television example where a subscriber device (such as a computer) in VLAN 1 receives multicast traffic from the streaming media server, **S**, via the switch. Multiple subscriber devices can connect through a port configured as the receiver on the switch.

When the subscriber selects a television channel, computer **A** sends an IGMP report to the switch to join the appropriate multicast group. If the IGMP report matches one of the configured MVR multicast group addresses on the switch, an entry is created in the forwarding table on the switch. This maps the subscriber VLAN to the list of forwarding destinations for the specified multicast traffic.

When the subscriber changes the channel or turns off the computer, an IGMP leave message is sent to the switch to leave the multicast group. The switch sends a query to VLAN 1 on the receiver port (in this case, a DSL port on the switch). If there is another subscriber device connected to this port in the same subscriber VLAN, the receiving port will still be on the list of forwarding destination for the multicast traffic. Otherwise, the switch removes the receiver port from the forwarding table.

Figure 76 MVR Multicast Television Example



21.6 General MVR Configuration

Use the **MVR** screen to create multicast VLANs and select the receiver port(s) and a source port for each multicast VLAN. Click **Advanced Applications** and **Multicast** in the navigation panel. Click the **Multicast Setting** link and then the **MVR** link to display the screen as shown next.



You can create up to three multicast VLANs and up to 256 multicast rules on the switch.



Your switch automatically creates a static VLAN (with the same VID) when you create a multicast VLAN in this screen.

Figure 77 MVR

Port	Source Port	Receiver Port	None	Tagging
*		None		<input type="checkbox"/>
1	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
2	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
3	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
4	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
5	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
6	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
7	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
8	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
9	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
10	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
11	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
12	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>

VLAN	Active	Name	Mode	Source Port	Receiver Port	802.1p	Delete

The following table describes the related labels in this screen.

Table 54 MVR

LABEL	DESCRIPTION
Active	Select this check box to enable MVR to allow one single multicast VLAN to be shared among different subscriber VLANs on the network.
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
Multicast VLAN ID	Enter the VLAN ID (1 to 4094) of the multicast VLAN.
802.1p Priority	Select a priority level (0-7) with which the switch replaces the priority in outgoing IGMP control packets (belonging to this multicast VLAN).

Table 54 MVR (continued)

LABEL	DESCRIPTION
Mode	Specify the MVR mode on the switch. Choices are Dynamic and Compatible . Select Dynamic to send IGMP reports to all MVR source ports in the multicast VLAN. Select Compatible to set the switch not to send IGMP reports.
Port	This field displays the port number on the switch.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Source Port	This field is applicable for Ethernet ports. Select this option to set this port as the MVR source port that sends and receives multicast traffic. All source ports must belong to a single multicast VLAN.
Receiver Port	Select this option to set this port as a receiver port that only receives multicast traffic. A receiver port cannot belong to a multicast VLAN.
None	Select this option to set the port not to participate in MVR. No MVR multicast traffic is sent or received on this port.
Tagging	Select this checkbox if you want the port to tag the VLAN ID in all outgoing frames transmitted.
Add	Click Add to save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to discard all changes.
VLAN	This field displays the multicast VLAN ID.
Active	This field displays whether the multicast group is enabled or not.
Name	This field displays the descriptive name for this setting.
Mode	This field displays the MVR mode.
Source Port	This field displays the source port number(s).
Receiver Port	This field displays the receiver port number(s).
Delete	To delete a multicast VLAN(s), select the rule(s) that you want to remove in the Delete column, then click the Delete button.
Cancel	Click Cancel to clear the Delete check boxes.

21.7 MVR Group Configuration

All source ports and receiver ports belonging to a multicast group can receive multicast data sent to this multicast group.

Configure MVR IP multicast group address(es) in the **Group Configuration** screen. Click **Group Configuration** in the **MVR** screen.



A port can belong to more than one multicast VLAN. However, IP multicast group addresses in different multicast VLANs cannot overlap.

Figure 78 MVR Group Configuration

The following table describes the labels in this screen.

Table 55 MVR Group Configuration

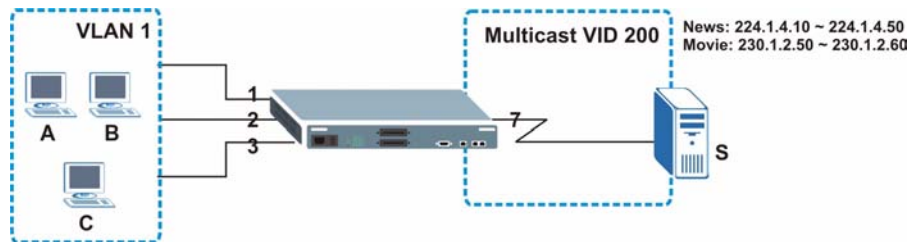
LABEL	DESCRIPTION
Multicast VLAN ID	Select a multicast VLAN ID (that you configured in the MVR screen) from the drop-down list box.
Name	Enter a descriptive name for identification purposes.
Start Address	Enter the starting IP multicast address of the multicast group in dotted decimal notation. Refer to Section 21.1.1 on page 149 for more information on IP multicast addresses.
End Address	Enter the ending IP multicast address of the multicast group in dotted decimal notation. Enter the same IP address as the Start Address field if you want to configure only one IP address for a multicast group. Refer to Section 21.1.1 on page 149 for more information on IP multicast addresses.
Add	Click Add to save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to discard all changes.
MVLAN	This field displays the multicast VLAN ID.
Name	This field displays the descriptive name for this setting.
Start Address	This field displays the starting IP address of the multicast group.
End Address	This field displays the ending IP address of the multicast group.

Table 55 MVR Group Configuration (continued)

LABEL	DESCRIPTION
Delete	Select Delete All and click Delete to remove all entries from the table. Select Delete Group and click Delete to remove the selected entry(ies) from the table.
Cancel	Select Cancel to clear the checkbox(es) in the table.

21.7.1 MVR Configuration Example

The following figure shows a network example where ports 1, 2 and 3 on the switch belong to VLAN 1. In addition, port 7 belongs to the multicast group with VID 200 to receive multicast traffic (the **News** and **Movie** channels) from the remote streaming media server, **S**. Computers **A**, **B** and **C** in VLAN are able to receive the traffic.

Figure 79 MVR Configuration Example

To configure the MVR settings on the switch, create a multicast group in the **MVR** screen and set the receiver and source ports.

Figure 80 MVR Configuration Example

The screenshot shows the MVR configuration interface. At the top, there are tabs for 'Multicast Setting' and 'Group Configuration'. The 'Group Configuration' tab is active. The settings are as follows:

- Active:
- Name: Premium
- Multicast VLAN ID: 200
- 802.1p Priority: 3
- Mode: Dynamic Compatible

Below the settings is a table with columns: Port, Source Port, Receiver Port, None, and Tagging. The table lists ports 1 through 12. Ports 1, 2, and 3 are circled in red, indicating they are configured as receiver ports. Port 7 is also circled in red, indicating it is configured as a source port.

Port	Source Port	Receiver Port	None	Tagging
*		None		<input type="checkbox"/>
1	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>
2	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>
3	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>
4	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
5	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
6	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
7	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>
8	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
9	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
10	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
11	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
12	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>

At the bottom of the table are 'Add' and 'Cancel' buttons.

To set the switch to forward the multicast group traffic to the subscribers, configure multicast group settings in the **Group Configuration** screen. The following figure shows an example where two multicast groups (**News** and **Movie**) are configured for the multicast VLAN 200.

Figure 81 MVR Configuration Example

Group Configuration MVR

Multicast VLAN ID: 200

Name	Start Address	End Address
News	224.1.4.10	224.1.4.50

Add Cancel

MVLAN	Name	Start Address	End Address	Delete All	Delete Group
200				<input type="checkbox"/>	
	Movie	230.1.2.50	230.1.2.60	<input type="checkbox"/>	<input type="checkbox"/>

Delete Cancel

Figure 82 MVR Configuration Example

Group Configuration MVR

Multicast VLAN ID: 200

Name	Start Address	End Address
	0.0.0.0	0.0.0.0

Add Cancel

MVLAN	Name	Start Address	End Address	Delete All	Delete Group
200				<input type="checkbox"/>	
	Movie	230.1.2.50	230.1.2.60	<input type="checkbox"/>	<input type="checkbox"/>
	News	224.1.4.10	224.1.4.50	<input type="checkbox"/>	<input type="checkbox"/>

Delete Cancel

DHCP Relay

This chapter describes the DHCP relay and shows you how to configure the **DHCP Relay** screen.

22.1 DHCP Relay Overview

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a DHCP server. You can configure the switch to relay client DHCP requests to a DHCP server and the server's responses back to the clients.

22.1.1 DHCP “Relay Agent Information Option”

The switch can add information to client DHCP requests that it relays to a DHCP server. This helps provide authentication about the source of the requests. You can also specify additional information for the switch to add to the client DHCP requests that it relays to the DHCP server. Please refer to RFC 3046 for more details.

22.1.2 DHCP Relay Agent Circuit ID Sub-option Format

The DHCP relay agent information feature adds an Agent Information field to the option 82 field of the DHCP headers of client DHCP request frames that the switch relays to a DHCP server. The Agent Information field that the switch adds contains an “Agent Circuit-ID sub-option” that includes the following information about where the DHCP request was received.

- Slot ID (1 byte, this is 0 with this model)
- Port ID (1 byte)
- VLAN ID (2 bytes)
- System name (up to 32 bytes, this is optional)

22.2 DHCP Relay Configuration

To configure DHCP relay information and specify the DHCP server(s), click **Advanced Application** and **DHCP Relay** to display the screen as shown next.

Figure 83 DHCP Relay

The following table describes the labels in this screen.

Table 56 DHCP Relay

LABEL	DESCRIPTION
Active	Select this check box to enable DHCP relay.
Remote DHCP Server 1 .. 3	Enter the IP address of a DHCP server in dotted decimal notation.
Relay Agent Information	Select the Option 82 check box to have the switch add information (slot number, port number and VLAN ID) to client TCP/IP configuration requests that it relays to a DHCP server.
Information	This read-only field displays the system name you configure in the General Setup screen. Select the check box to add the switch name to the DHCP client requests that the switch relays to a DHCP server.
Apply	Click Apply to save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields back to your previous configuration.

PART IV

Static Routing and Management

Routing Protocol (165)
Maintenance (167)
Access Control (175)
Diagnostic (187)
Syslog (189)
Cluster Management (193)
MAC Table (199)
ARP Table (201)
Configure Clone (203)

Routing Protocol

This chapter shows you how to configure the routing functions.

23.1 Static Route Overview

Static routes tell the switch how to forward IP traffic when you configure the TCP/IP parameters manually.

Click **Routing Protocol** in the navigation panel and then **Static Routing** to display the screen as shown.

Figure 84 Static Routing

The following table describes the related labels you use to create a static route.

Table 57 Static Routing

LABEL	DESCRIPTION
Active	This field allows you to activate/deactivate this static route.
Name	Enter a descriptive name for this route. This is for identification purpose only.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the subnet mask for this destination.

Table 57 Static Routing (continued)

LABEL	DESCRIPTION
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your switch that will forward the packet to the destination. The gateway must be a router on the same segment as your switch.
Metric	The metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Add	Click Add to insert a new static route in the summary table below and save your changes to the switch’s run-time memory. The switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to your previous configuration.
Clear	Click Clear to clear the fields to the factory defaults.

View the current static routes on the switch in the summary table at the bottom of the screen.

Figure 85 Static Routing: Summary Table

Index	Active	Name	Destination Address	Subnet Mask	Gateway Address	Metric	Delete
1	Yes	ju	172.16.1.2	255.255.0.0	192.168.1.2	2	<input type="checkbox"/>

The following table describes the labels in the summary table.

Table 58 Static Routing: Summary Table

LABEL	DESCRIPTION
Index	This field displays the index number of the route. Click a number to edit the static route entry.
Active	This field displays Yes when the static route is activated and NO when is it deactivated.
Name	This field displays the descriptive name for this route. This is for identification purpose only.
Destination Address	This field displays the IP network address of the final destination.
Subnet Mask	This field displays the subnet mask for this destination.
Gateway Address	This field displays the IP address of the gateway. The gateway is an immediate neighbor of your switch that will forward the packet to the destination.
Metric	This field displays the cost of transmission for routing purposes.
Delete	Check the rule(s) that you want to remove in the Delete column, and then click the Delete button.
Cancel	Click Cancel to clear the selected checkboxes in the Delete column.

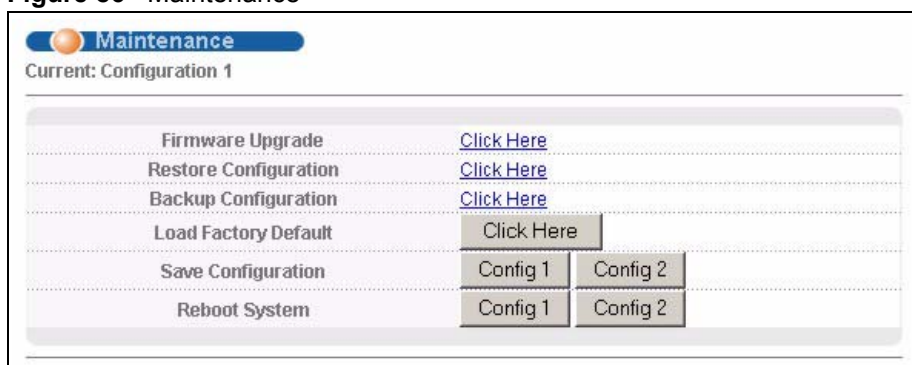
Maintenance

This chapter explains how to configure the maintenance screens. The links on the upper right of the **Maintenance** screen lead to different screens that let you maintain the firmware and configuration files.

24.1 Maintenance

Click **Management** and then **Maintenance** in the navigation panel to open the following screen. The maintenance screens allow you to upload new firmware, manage configuration, reset to factory defaults and restart your switch.

Figure 86 Maintenance



The following table describes the labels in this screen.

Table 59 Maintenance

LABEL	DESCRIPTION
Current	This field displays which configuration (Configuration 1 or Configuration 2) is currently operating on the switch.
Firmware Upgrade	Click Click Here to go to the Firmware Upgrade screen.
Restore Configuration	Click Click Here to go to the Restore Configuration screen.
Backup Configuration	Click Click Here to go to the Backup Configuration screen.
Load Factory Default	Click Click Here to reset the configuration to the factory default settings.

Table 59 Maintenance (continued)

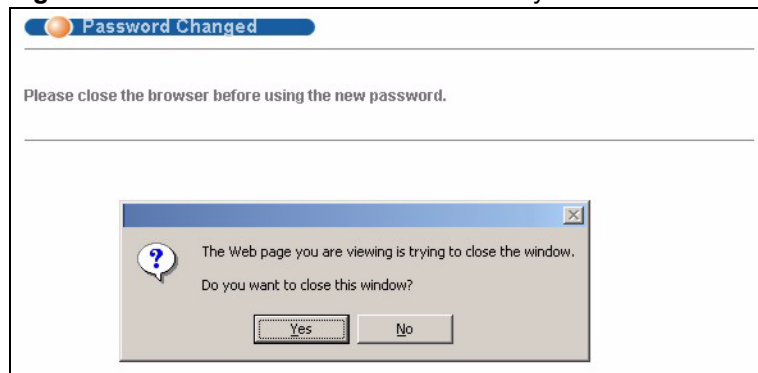
LABEL	DESCRIPTION
Save Configuration	Click Config 1 to save the current configuration settings to Configuration 1 on the switch. Click Config 2 to save the current configuration settings to Configuration 2 on the switch.
Reboot System	Click Config 1 to reboot the system and load Configuration 1 on the switch. Click Config 2 to reboot the system and load Configuration 2 on the switch. Note: Make sure to click the Save button in any screen to save your settings to the current configuration on the switch.

24.2 Load Factory Defaults

Press the **Click Here** button next to **Load Factory Defaults** to clear all switch configuration information you configured and return to the factory defaults. The following message appears.

Figure 87 Confirm Load Factory Defaults

Click **OK** to the confirmation screen and go to the next screen.

Figure 88 Close Browser after Load Factory Defaults

Click **Yes** to close this window. Open a new browser window to access the switch web configurator again. You may need to change the IP address of your computer to be in the same subnet as that of the default switch IP address (192.168.1.1).

24.3 Save Configuration

Click **Config 1** to save the current configuration settings permanently to **Configuration 1** on the switch.

Click **Config 2** to save the current configuration settings to **Configuration 2** on the switch.

Alternatively, click **Save** on the top right-hand corner in any screen to save the configuration changes to the current configuration.



Clicking the **Apply** or **Add** button does NOT save the changes permanently. All unsaved changes are erased after you reboot the switch.

24.4 Reboot System

Reboot System allows you to restart the switch without physically turning the power off. It also allows you to load configuration one (**Config 1**) or configuration two (**Config 2**) when you reboot. Follow the steps below to reboot the switch.

- 1 In the **Maintenance** screen, click the **Config 1** button next to **Reboot System** to reboot and load configuration one. The following screen displays.

Figure 89 Reboot System: Confirmation



- 2 Click **OK** and then wait for the switch to finish rebooting before you attempt to access the switch again. This takes up to two minutes. This does not affect the switch's configuration.

Click **Config 2** and follow steps 1 to 2 to reboot and load configuration two on the switch.

24.5 Firmware Upgrade

Click **Firmware Upgrade** in the **Maintenance** screen if you want to upgrade your switch firmware. See the **System Info** screen to verify your current firmware version number. Make sure you have downloaded (and unzipped) the correct model firmware and version to your computer before uploading to the device.



Be sure to upload the correct model firmware as uploading the wrong model firmware may damage your device.

From the **Maintenance** screen, display the **Firmware Upgrade** screen as shown next.

Figure 90 Firmware Upgrade

Type the path and file name of the firmware file you wish to upload to the switch in the **File Path** text box or click **Browse** to locate it. After you have specified the file, click **Upgrade**.



The system does not restart automatically after you upload the firmware. You need to use the web configurator or the `boot config` command to restart the system to complete firmware upgrade.

24.6 Restore a Configuration File

Restore a previously saved configuration from your computer to the switch using the **Restore Configuration** screen.

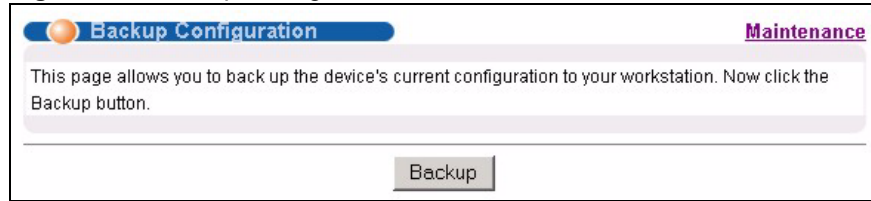
Figure 91 Restore Configuration

Type the path and file name of the configuration file you wish to restore in the **File Path** text box or click **Browse** to display a **Choose File** screen from which you can locate it. After you have specified the file, click **Restore**. "config" is the name of the configuration file on the switch, so your backup configuration file is automatically renamed when you restore using this screen.

24.7 Backing Up a Configuration File

Backing up your switch configurations allows you to create various “snap shots” of your device from which you may restore at a later date.

Back up your current switch configuration to a computer using the **Configuration Backup** screen.

Figure 92 Backup Configuration

Follow the steps below to back up the current switch configuration to your computer in this screen.

- 1 Click **Backup**.
- 2 Click **Save** to display the **Save As** screen.
- 3 Choose a location to save the file on your computer from the **Save in** drop-down list box and type a descriptive name for it in the **File name** list box. Click **Save** to save the configuration file to your computer.

24.8 Command Line FTP

This section shows some examples of uploading to or downloading files from the switch using FTP commands. First, understand the filename conventions.

24.8.1 Filename Conventions

The configuration file (often called the romfile or rom-0) contains the factory default settings in the screens such as password, switch setup, IP setup, etc. Once you have customized the switch's settings, they can be saved back to your computer under a filename of your choosing.



A configuration file that you save from your switch to your computer does not include the password, the error log or the trace log.



Restoring a backup configuration file from your computer to your switch, does not change the password, the error log or the trace log.

ZyNOS (ZyXEL Network Operating System sometimes referred to as the “ras” file) is the system firmware and has a “bin” filename extension.

Table 60 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	config		This is the configuration filename on the switch. Uploading the config file replaces the specified configuration file system, including your switch configurations and system-related data.
Firmware	ras	*.bin	This is the generic name for the ZyNOS firmware on the switch.

24.8.1.1 Example FTP Commands

```
ftp> put firmware.bin ras
```

This is a sample FTP session showing the transfer of the computer file "firmware.bin" to the switch .

```
ftp> get config config.cfg
```

This is a sample FTP session saving the current configuration to a file called “config.cfg” on your computer.

If your (T)FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the switch only recognizes “config” and “ras”. Be sure you keep unaltered copies of both files for later use.



Be sure to upload the correct model firmware as uploading the wrong model firmware may damage your device.

24.8.2 FTP Command Line Procedure

- 1 Launch the FTP client on your computer.
- 2 Enter “open”, followed by a space and the IP address of your switch.
- 3 Press [ENTER] when prompted for a username.
- 4 Enter your password as requested (the default is “1234”).
- 5 Enter “bin” to set transfer mode to binary.
- 6 Use “put” to transfer files from the computer to the switch, for example, “put firmware.bin ras” transfers the firmware on your computer (firmware.bin) to the switch and renames it “ras”. Similarly, “put config.cfg config” transfers the configuration file on your computer (config.cfg) to the switch and renames it “config”. Likewise “get config config.cfg” transfers the configuration file on the switch to your computer and renames it “config.cfg.” See earlier in this chapter for more information on filename conventions.
- 7 Enter “quit” to exit the ftp prompt.

24.8.3 GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

Table 61 General Commands for GUI-based FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous. This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option. Normal. The server requires a unique User ID and Password to login.
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode. Configuration and firmware files should be transferred in binary mode.
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

24.8.4 FTP Restrictions

FTP will not work when:

- FTP service is disabled in the **Access Control** screen.
- The IP address(es) in the **Secured Client Set** in the **Remote Management** screen does not match the client IP address. If it does not match, the switch will disconnect the Telnet session immediately

Access Control

This chapter describes how to control access to the switch.

25.1 About Access Control

Click **Advanced Application, Access Control** from the navigation panel to display the screen as shown. From this screen you can configure SNMP, up to four web configurator administrators, enable/disable remote service access and configure trusted computers for remote access.

Figure 93 Access Control



25.2 Access Control Overview

The following table describes how many concurrent management sessions are permitted when the multiple login feature is either enabled or disabled.

Table 62 Access Control Overview

Multiple Login	Console port	SSH	Telnet	FTP	Web	SNMP
Enabled	One console port session	SSH and Telnet share 4 sessions.		One session	Up to five accounts	No limit
Disabled	The console port, SSH and Telnet share one session. The console port has the highest priority and Telnet has the lowest priority.			One session	Up to five accounts	No limit

With the multiple login feature disabled, a console port access control session and Telnet access control session cannot coexist. The console port has higher priority. If you telnet to the switch and someone is already logged in from the console port, then you will see the following message.

Figure 94 Console Port Priority

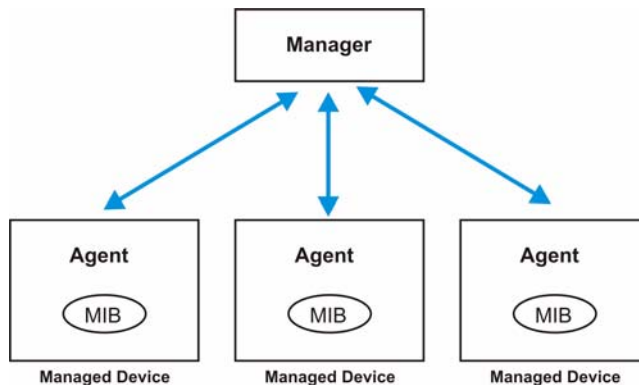
```

"Local administrator is configuring this device now!!!
Connection to host lost."

```

25.3 About SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network switches. SNMP is a member of TCP/IP protocol suite. A manager station can manage and monitor the switch through the network via SNMP version one (SNMPv1) and/or SNMP version 2c. The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

Figure 95 SNMP Management Model

An SNMP managed network consists of two main components: agents and a manager.

An agent is a management software module that resides in a managed switch (the GS). An agent translates the local management information from the managed switch into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a switch. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

Table 63 SNMP Commands

COMMAND	DESCRIPTION
Get	Allows the manager to retrieve an object variable from the agent.
GetNext	Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.

Table 63 SNMP Commands (continued)

COMMAND	DESCRIPTION
Set	Allows the manager to set values for object variables within an agent.
Trap	Used by the agent to inform the manager of some events.

25.3.1 Supported MIBs

MIBs let administrators collect statistics and monitor status and performance.

The switch supports the following MIBs:

- SNMP MIB II (RFC 1213)
- RFC 1157 SNMP v1
- RFC 1493 Bridge MIBs
- RFC 1643 Ethernet MIBs
- RFC 1155 SMI
- RFC 2674 SNMPv2, SNMPv2c
- RFC 1757 RMON
- SNMPv2, SNMPv2c or later version, compliant with RFC 2011 SNMPv2 MIB for IP, RFC 2012 SNMPv2 MIB for TCP, RFC 2013 SNMPv2 MIB for UDP

25.3.2 SNMP Traps

The switch sends traps to an SNMP manager when an event occurs. SNMP traps supported are outlined in the following table.

Table 64 SNMP Traps

OBJECT LABEL	OBJECT ID	DESCRIPTION
SNMPv2 Traps		
Cold Start	1.3.6.1.6.3.1.1.5.1	This trap is sent when the switch is turned on.
WarmStart	1.3.6.1.6.3.1.1.5.2	This trap is sent when the switch restarts.
linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.
linkUp	1.3.6.1.6.3.1.1.5.4	This trap is sent when the Ethernet link is up.
authenticationFailure	1.3.6.1.6.3.1.1.5.5	This trap is sent when an SNMP request comes from non-authenticated hosts.
RFC 1493 Traps		
newRoot	1.3.6.1.2.1.17.0.1	This trap is sent when the STP root switch changes.
topology change	1.3.6.1.2.1.17.0.2	This trap is sent when the STP topology changes.

25.3.3 Configuring SNMP

From the **Access Control** screen, display the **SNMP** screen. You can click **Access Control** to go back to the **Access Control** screen.

Figure 96 Access Control: SNMP

The screenshot shows a web-based configuration interface for SNMP. At the top left is a blue tab labeled 'SNMP' with an orange circle icon. At the top right is the text 'Access Control'. Below this is a form with four rows of input fields. The first row is 'Get Community' with the value 'public'. The second row is 'Set Community' with the value 'public'. The third row is 'Trap Community' with the value 'public'. The fourth row is 'Trap Destination' with four input fields, each containing '0.0.0.0'. At the bottom of the form are two buttons: 'Apply' and 'Cancel'.

The following table describes the labels in this screen.

Table 65 Access Control: SNMP

LABEL	DESCRIPTION
Get Community	Enter the get community, which is the password for the incoming Get- and GetNext-requests from the management station.
Set Community	Enter the set community, which is the password for incoming Set- requests from the management station.
Trap Community	Enter the trap community, which is the password sent with each trap to the SNMP manager.
Trap Destination	Enter the IP addresses of up to four stations to send your SNMP traps to.
Apply	Click Apply to save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

25.3.4 Setting Up Login Accounts

Up to five people (one administrator and four non-administrators) may access the switch via web configurator at any one time.

- 1 An administrator is someone who can both view and configure switch changes. The username for the administrator is always **admin**. The default administrator password is **1234**.



It is highly recommended that you change the default administrator password ("1234").

- 2 A non-administrator (username is something other than **admin**) is someone who can view but not configure switch changes.

Click **Access Control** from the navigation panel and then click **Logins** from this screen.

Figure 97 Access Control: Logins

The following table describes the labels in this screen.

Table 66 Access Control: Logins

LABEL	DESCRIPTION
Administrator	This is the default administrator account with the "admin" user name. You cannot change the default administrator user name. Only the administrator has read/write access.
Old Password	Type the existing system password ("1234" is the default password when shipped).
New Password	Enter your new system password.
Retype to confirm	Retype your new system password for confirmation
Edit Logins	You may configure passwords for up to four users. These users have read-only access. You can give users higher privileges via the CLI. For more information on assigning privileges see Chapter 32 on page 207 .
User Name	Set a user name (up to 32 ASCII characters long).
Password	Enter your new system password for the user name above.
Retype to confirm	Retype your new system password for confirmation
Apply	Click Apply to save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

25.4 SSH Overview

Unlike Telnet or FTP, which transmit data in clear text, SSH (Secure Shell) is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network.

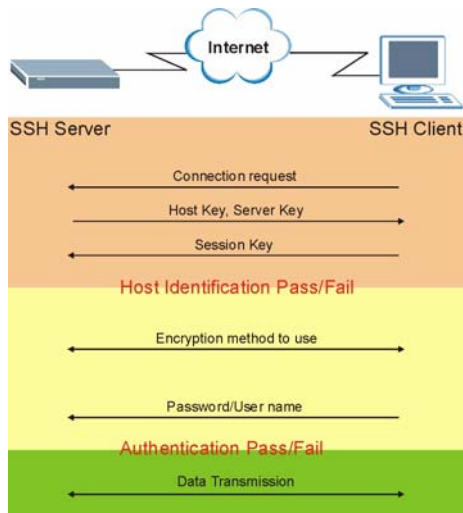
Figure 98 SSH Communication Example



25.5 How SSH works

The following table summarizes how a secure connection is established between two remote hosts.

Figure 99 How SSH Works



1 Host Identification

The SSH client sends a connection request to the SSH server. The server identifies itself with a host key. The client encrypts a randomly generated session key with the host key and server key and sends the result back to the server.

The client automatically saves any new server public keys. In subsequent connections, the server public key is checked against the saved version on the client computer.

2 Encryption Method

Once the identification is verified, both the client and server must agree on the type of encryption method to use.

3 Authentication and Data Transmission

After the identification is verified and data encryption activated, a secure tunnel is established between the client and the server. The client then sends its authentication information (user name and password) to the server to log in to the server.

25.6 SSH Implementation

Your switch supports SSH versions 1 and 2 using RSA and DSA authentication and five encryption methods (AES, 3DES, RC4, Blowfish and CAST). The SSH server is implemented on the switch for remote management and file transfer on port 22 (by default). Up to four SSH connections are allowed at a time.

25.6.1 Requirements for Using SSH

You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the switch over SSH.

25.7 Introduction to HTTPS

HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol that encrypts and decrypts web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the transferred data), authentication (one party can identify the other party) and data integrity (you know if data has been changed).

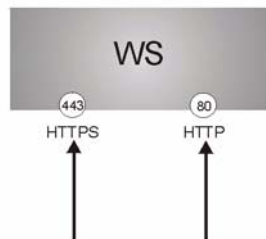
It relies upon certificates, public keys, and private keys.

HTTPS on the switch is used so that you may securely access the switch using the web configurator. The SSL protocol specifies that the SSL server (the switch) must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the switch), whereas the SSL client only should authenticate itself when the SSL server requires it to do so.

Please refer to the following figure.

- 1 HTTPS connection requests from an SSL-aware web browser go to port 443 (by default) on the switch's WS (web server).
- 2 HTTP connection requests from a web browser go to port 80 (by default) on the switch's WS (web server).

Figure 100 HTTPS Implementation



If you disable **HTTP** in the **Service Access Control** screen, then the switch blocks all HTTP connection attempts.

25.7.1 HTTPS Example

If you haven't changed the default HTTPS port on the switch, then in your browser enter "https://switch IP Address/" as the web site address where "switch IP Address" is the IP address or domain name of the switch you wish to access.

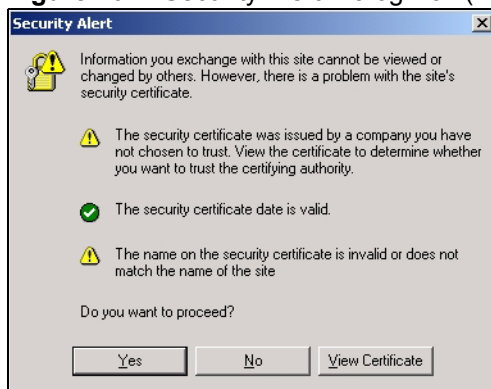
The HTTPS proxy server listens on port 443 by default. If you change the HTTPS proxy server port to a different number on the switch, for example 8443, then you must notify people who need to access the switch web configurator to use "https://switch IP Address:8443" as the URL.

25.7.2 Internet Explorer Warning Messages

When you attempt to access the switch HTTPS server, a Windows dialog box pops up asking if you trust the server certificate. Click **View Certificate** if you want to verify that the certificate is from the switch.

You see the following **Security Alert** screen in Internet Explorer. Select **Yes** to proceed to the web configurator login screen; if you select **No**, then web configurator access is blocked.

Figure 101 Security Alert Dialog Box (Internet Explorer)

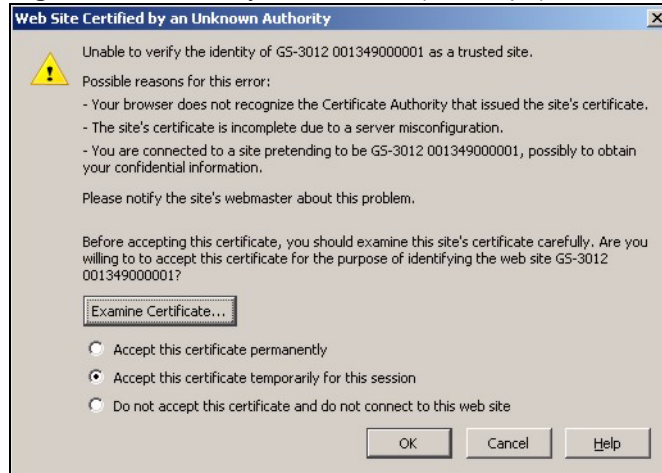


25.7.3 Netscape Navigator Warning Messages

When you attempt to access the switch HTTPS server, a **Website Certified by an Unknown Authority** screen pops up asking if you trust the server certificate. Click **Examine Certificate** if you want to verify that the certificate is from the switch.

If **Accept this certificate temporarily for this session** is selected, then click **OK** to continue in Netscape.

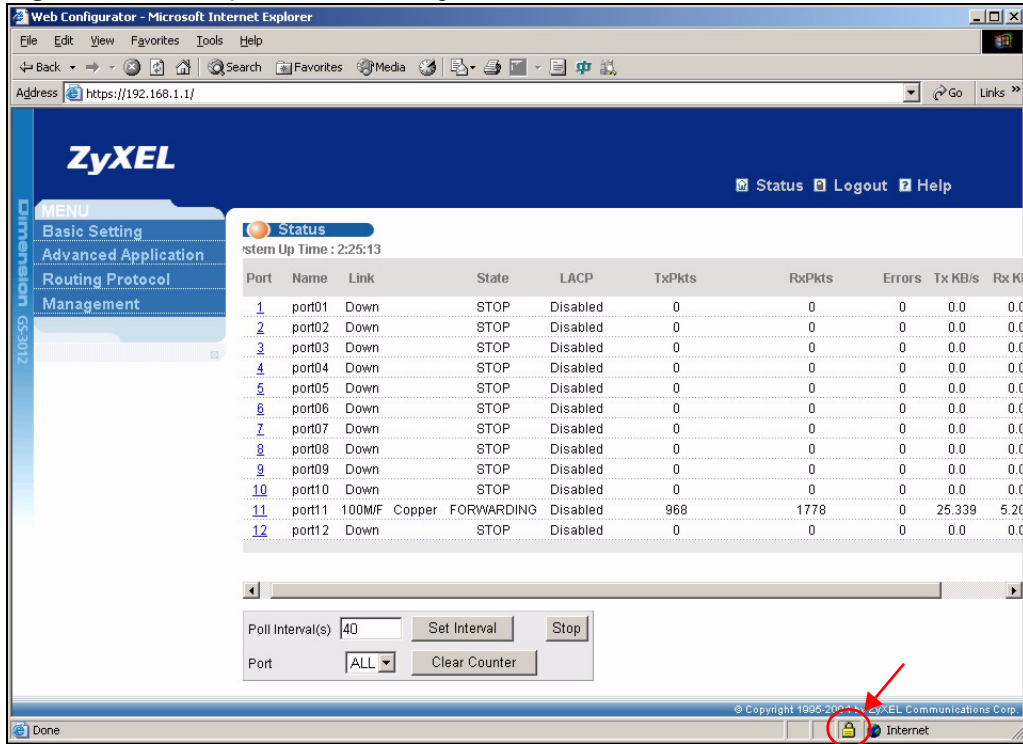
Select **Accept this certificate permanently** to import the switch's certificate into the SSL client.

Figure 102 Security Certificate 1 (Netscape)**Figure 103** Security Certificate 2 (Netscape)

25.7.4 Login Screen

After you accept the certificate and login in, the switch main screen appears. The lock displayed in the bottom of the browser status bar denotes a secure connection.

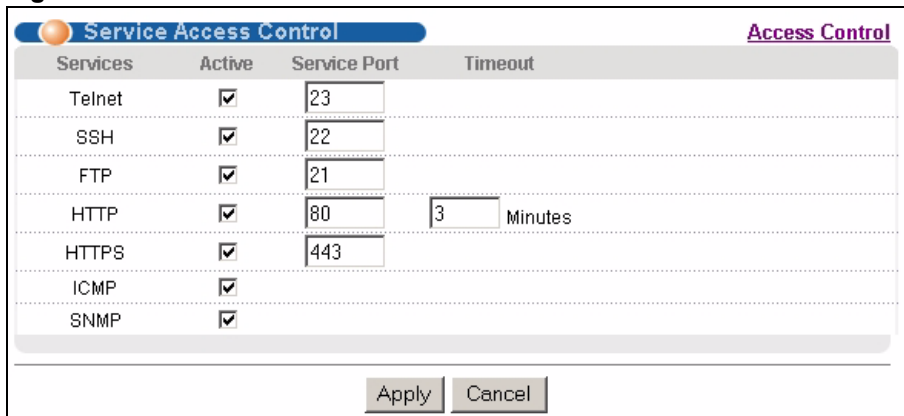
Figure 104 Example: Lock Denoting a Secure Connection



25.8 Service Access Control

Service access control allows you to decide what services you may use to access the switch. You may also change the default service port and configure “trusted computer(s)” for each service in the **Remote Management** screen (discussed later). Click **Access Control** to go back to the **Access Control** screen.

Figure 105 Access Control: Service Access Control



The following table describes the fields in this screen.

Table 67 Access Control: Service Access Control

LABEL	DESCRIPTION
Services	Services you may use to access the switch are listed here.
Active	Select this option for the corresponding services that you want to allow to access the switch.
Service Port	For Telnet, SSH, FTP, HTTP or HTTPS services, you may change the default service port by typing the new port number in the Service Port field. If you change the default port number then you will have to let people (who wish to use the service) know the new port number for that service.
Timeout	Type how many minutes a management session (via the web configurator) can be left idle before the session times out. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value greater than "0" must be entered.
Apply	Click Apply to save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

25.9 Remote Management

From the **Access Control** screen, display the **Remote Management** screen as shown next.

You can specify a group of one or more "trusted computers" from which an administrator may use a service to manage the switch. Click **Access Control** to return to the **Access Control** screen.

Figure 106 Access Control: Remote Management

Entry	Active	Start Address	End Address	Telnet	FTP	HTTP	ICMP	SNMP	SSH	HTTPS
1	<input checked="" type="checkbox"/>	0.0.0.0	0.0.0.0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	0.0.0.0	0.0.0.0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

The following table describes the labels in this screen.

Table 68 Access Control: Remote Management

LABEL	DESCRIPTION
Entry	This is the client set index number. A "client set" is a group of one or more "trusted computers" from which an administrator may use a service to manage the switch.
Active	Select this check box to activate this secured client set. Clear the check box if you wish to temporarily disable the set without deleting it.

Table 68 Access Control: Remote Management (continued)

LABEL	DESCRIPTION
Start Address End Address	Configure the IP address range of trusted computers from which you can manage this switch. The switch checks if the client IP address of a computer requesting a service or protocol matches the range set here. The switch immediately disconnects the session if it does not match.
Telnet/FTP/HTTP/ ICMP /SNMP/SSH/ HTTPS	Select services that may be used for managing the switch from the specified trusted computers.
Apply	Click Apply to save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

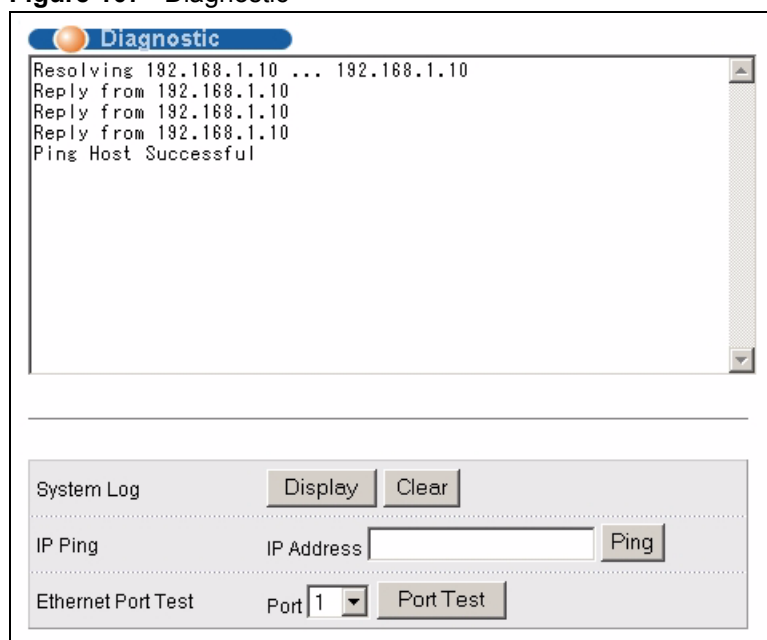
Diagnostic

This chapter explains the Diagnostic screens.

26.1 Diagnostic

Click **Management** and then **Diagnostic** in the navigation panel to display this screen. Use this screen to check system logs, ping IP addresses or perform loopback tests on a port.

Figure 107 Diagnostic



The following table describes the labels in this screen.

Table 69 Diagnostic

LABEL	DESCRIPTION
System Log	Click Display to display a log of events in the multi-line text box. Click Clear to empty the text box and reset the syslog entry.
IP Ping	Type the IP address of a device that you want to ping in order to test a connection. Click Ping to have the switch ping the IP address (in the field to the left).
Ethernet Port Test	From the Port drop-down list box, select a port number and click Port Test to perform internal loopback test.

Syslog

This chapter explains the syslog screens.

27.1 Syslog

The syslog protocol allows devices to send event notification messages across an IP network to syslog servers that collect the event messages. A syslog-enabled device can generate a syslog message and send it to a syslog server.

Syslog is defined in RFC 3164. The RFC defines the packet format, content and system log related information of syslog messages. Each syslog message has a facility and severity level. The syslog facility identifies a file in the syslog server. Refer to the documentation of your syslog program for details. The following table describes the syslog severity levels.

Table 70 Syslog Severity Levels

NUMERIC L CODE	SEVERITY
0	Emergency: The system is unusable.
1	Alert: Action must be taken immediately.
2	Critical: The system condition is critical.
3	Error: There is an error condition on the system.
4	Warning: There is a warning condition on the system.
5	Notice: There is a normal but significant condition on the system.
6	Informational: The syslog contains an informational message.
7	Debug: The message is intended for debug-level purposes.

27.2 Syslog Setup

Click **Management** and then **Syslog** in the navigation panel to display this screen. The syslog feature sends logs to an external syslog server. Use this screen to configure the device's system logging settings.

Figure 108 Syslog Setup

Logging type	Active	Facility
System	<input type="checkbox"/>	local use 0
Interface	<input type="checkbox"/>	local use 0
Switch	<input type="checkbox"/>	local use 0
Authentication	<input type="checkbox"/>	local use 0
IP	<input type="checkbox"/>	local use 0

The following table describes the labels in this screen.

Table 71 Syslog Setup

LABEL	DESCRIPTION
Syslog	Select this check box to turn on syslog (system logging) and then configure the syslog settings.
Logging type	This column displays the names of the categories of logs that the device can generate.
Active	Select this option to set the device to generate logs for the corresponding category.
Facility	The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Apply	Click Apply to save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

27.3 Syslog Server Setup

Click **Management** and then **Syslog** in the navigation panel to display the **Syslog Setup** screen. Click the **Syslog Server Setup** link to open the following screen. Use this screen to configure a list of external syslog servers.

Figure 109 Syslog Server Setup

Index	Active	IP Address	Log Level	Delete
1	Yes	1.2.3.4	0	<input type="checkbox"/>
2	Yes	1.2.3.5	0-1	<input type="checkbox"/>
3	No	1.2.3.6	0-2	<input type="checkbox"/>

The following table describes the labels in this screen.

Table 72 Syslog Server Setup

LABEL	DESCRIPTION
Active	Select this check box to have the device send logs to this syslog server. Clear the check box if you want to create a syslog server entry but not have the device send logs to it (you can edit the entry later).
Server Address	Enter the IP address of the syslog server.
Log Level	Select the severity level(s) of the logs that you want the device to send to this syslog server. The lower the number, the more critical the logs are.
Add	Click Add to insert the entry in the summary table below and save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Clear	Click Clear to return the fields to the factory defaults.
Index	This is the index number of a syslog server entry. Click this number to edit the entry.
Active	This field displays Yes if the device is to send logs to the syslog server. No displays if the device is not to send logs to the syslog server.
IP Address	This field displays the IP address of the syslog server.
Log Level	This field displays the severity level of the logs that the device is to send to this syslog server.
Delete	Select an entry's Delete check box and click Delete to remove the entry.
Cancel	Click Cancel to begin configuring this screen afresh.

Cluster Management

This chapter introduces cluster management.

28.1 Introduction to Cluster Management

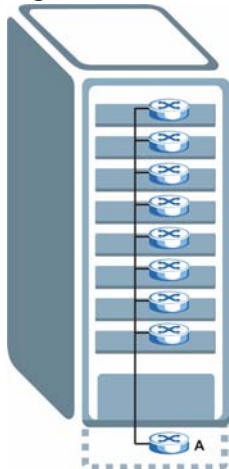
Cluster Management² allows you to manage switches through one switch, called the cluster manager. The switches must be directly connected and be in the same VLAN group so as to be able to communicate with one another.

Table 73 ZyXEL Clustering Management Specifications

Maximum number of cluster members	24
Cluster Member Models	Must be compatible with ZyXEL cluster management implementation.
Cluster Manager	The switch through which you manage the cluster member switches.
Cluster Members	The switches being managed by the cluster manager switch.

In the following example, switch **A** in the basement is the cluster manager and the other switches on the upper floors of the building are cluster members.

Figure 110 Clustering Application Example



2. Cluster management may also be referred to as "iStacking" in other ZyXEL documentation.

28.2 Cluster Management Status

Click **Management** in the navigation panel and then **Cluster Management** to display the following screen.

Figure 111 Cluster Management Status

Index	MacAddr	Name	Model	Status
1	00:a0:c5:3f:91:5d	ES-4024	ES-4024	Online
2	00:a0:c5:6d:e4:77			Error

The following table describes the labels in this screen.

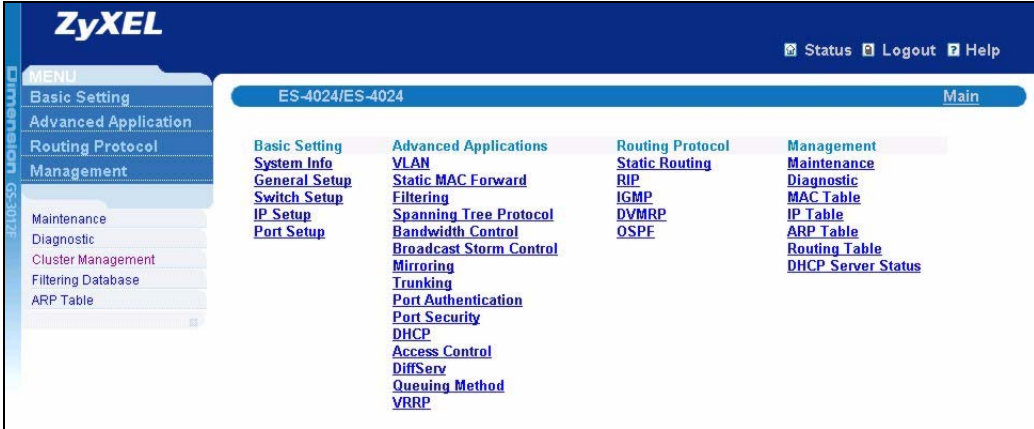
Table 74 Cluster Management Status

LABEL	DESCRIPTION
	A cluster can only have one manager.
Status	This field displays the role of this switch within the cluster. Manager Member (you see this if you access this screen in the cluster member switch directly and not via the cluster manager) None (neither a manager nor a member of a cluster)
Manager	This field displays the cluster manager switch's hardware MAC Address.
The Number of Member	This field displays the number of switches that make up this cluster. The following fields describe the cluster member switches.
Index	You can manage cluster member switches via the cluster manager switch. Each number in the Index column is a hyperlink leading to the cluster member switch's web configurator (see Figure 112 on page 195).
MacAddr	This is the cluster member switch's hardware MAC Address.
Name	This is the cluster member switch's System Name .
Model	This field displays the model name.
Status	This field displays: Online (the cluster member switch is accessible) Error (for example the cluster member switch password was changed or the switch was set as the manager and so left the member list, etc.) Offline (the switch is disconnected - Offline shows approximately 1.5 minutes after the link between cluster member and manager goes down).

28.2.1 Cluster Member Switch Management

Go to the **Clustering Management Status** screen of the cluster manager switch and then select an **Index** hyperlink from the list of members to go to that cluster member switch's web configurator home page. This cluster member web configurator home page and the home page that you'd see if you accessed it directly are different.

Figure 112 Cluster Member Web Configuration Screen



28.2.1.1 Uploading Firmware to a Cluster Member Switch

You can use FTP to upload firmware to a cluster member switch through the cluster manager switch as shown in the following example.

Figure 113 Example: Uploading Firmware to a Cluster Member Switch

```
C:\> ftp <Cluster Manager IP address>
Connected to 192.168.0.1.
220 GS-3012F FTP version 1.0 ready at Thu Jan  1 00:31:12 1970
User (192.168.0.1:(none)): admin
331 Enter PASS command
Password:
230 Logged in
ftp> ls
200 Port command okay
150 Opening data connection for LIST
--w--w--w-  1 owner   group      3075006 Jul  01 12:00 ras
-rw-rw-rw-  1 owner   group      393216  Jul  01 12:00 config
--w--w--w-  1 owner   group           0 Jul  01 12:00 fw-00-13-49-00-00-02
-rw-rw-rw-  1 owner   group           0 Jul  01 12:00 config-00-13-49-00-00-02
226 File sent OK
ftp: 296 bytes received in 0.01Seconds 19.73Kbytes/sec.
ftp> put 370LR0.bin fw-00-13-49-00-00-02
ftp> bye
```

The following table explains some of the FTP parameters.

Table 75 FTP Upload to Cluster member Example

FTP PARAMETER	DESCRIPTION
User name	Enter "admin".
Password	The web configurator password default is 1234.
ls	Enter this command to list the name of cluster member switch's firmware and configuration file.
fw-00-13-49-00-00-02	The cluster member switch's firmware name as seen in the cluster manager switch.

Table 75 FTP Upload to Cluster member Example (continued)

FTP PARAMETER	DESCRIPTION
config-00-13-49-00-00-02	The cluster member switch's configuration file name as seen in the cluster manager switch.
370LR0.bin	The name of the firmware file you want to upload to the cluster member switch.

28.3 Clustering Management Configuration

Click **Configuration** from the **Cluster Management** screen to display the next screen. Refer to [Section 28.1 on page 193](#) for more information.

Figure 114 Configuring Cluster Management

Clustering Manager:

Active

Name

VID

Clustering Candidate:



List

Password

Index	MacAddr	Name	Model	Remove
1	00:a0:c5:3f:91:5d	ES-4024	ES-4024	<input type="checkbox"/>
2	00:a0:c5:6d:e4:77			<input type="checkbox"/>

The following table describes the labels in this screen.

Table 76 Configuring Cluster Management

LABEL	DESCRIPTION
Clustering Manager	
Active	Select Active to have this switch become the cluster manager switch. A cluster can only have one manager. Other (directly connected) switches that are set to be cluster managers will not be visible in the Clustering Candidates list. If a switch that was previously a cluster member is later set to become a cluster manager, then its Status is displayed as Error in the Cluster Management Status screen and a warning icon () appears in the member summary list below.
Name	Type a name to identify the Clustering Manager . You may use up to 32 printable characters (spaces are allowed).
VID	This is the Management VLAN ID and is only applicable if the switch is set to 802.1Q VLAN. All switches must be in the same management VLAN group to belong to the same cluster. Switches that are not in the same management VLAN group are not visible in the Clustering Candidates list. This field is ignored if the Clustering Manager is using Port-based VLAN.
Apply	Click Apply to save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this part of the screen afresh.
Clustering Candidate	The following fields relate to the switches that are potential cluster members.
List	A list of suitable candidates found by auto-discovery is shown here. The switches must be directly connected. Directly connected switches that are set to be cluster managers will not be visible in the Clustering Candidate list. Switches that are not in the same management VLAN group will not be visible in the Clustering Candidate list.
Password	Each cluster member's password is its web configurator password. Select a member in the Clustering Candidate list and then enter its web configurator password. If that switch administrator changes the web configurator password afterwards, then it cannot be managed from the Cluster Manager . Its Status is displayed as Error in the Cluster Management Status screen and a warning icon () appears in the member summary list below. If multiple devices have the same password then hold [SHIFT] and click those switches to select them. Then enter their common web configurator password.
Add	Click Add to save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this part of the screen afresh.
Refresh	Click Refresh to perform auto-discovery again to list potential cluster members.
The next summary table shows the devices selected for clustering.	
Index	This is the index number of a cluster member switch.
MAC Address	This is the cluster member switch's hardware MAC address.
Name	This is the cluster member switch's System Name .
Model	This is the cluster member switch's model name.
Remove	Select this checkbox and then click the Remove button to remove a cluster member switch from the cluster.
Cancel	Click Cancel to begin configuring this part of the screen afresh.

MAC Table

This chapter introduces MAC Table.

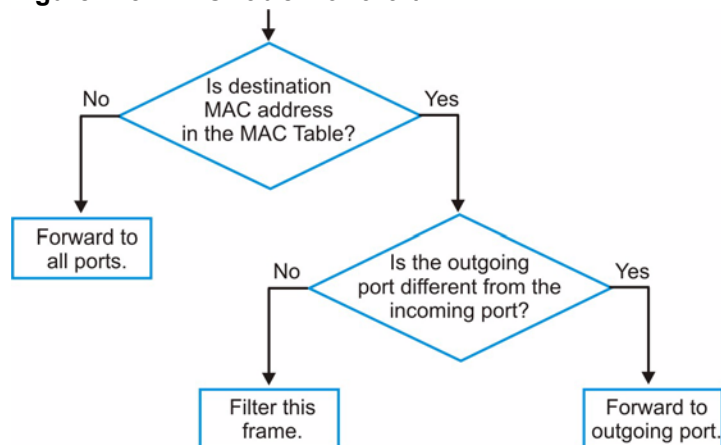
29.1 Introduction to MAC Table

The MAC table shows how frames are forwarded or filtered across the switch's ports. It shows what device MAC address, belonging to what VLAN group (if any) is forwarded to which port(s) and whether the MAC address is dynamic (learned by the switch) or static (manually entered in **Static MAC Forwarding**).

The switch uses the Filtering Database to determine how to forward frames. See the following figure.

- 1 The switch examines a received frame and learns the port on which this source MAC address came.
- 2 The switch checks to see if the frame's destination MAC address matches a source MAC address already learned in the Filtering Database.
 - If the switch has already learned the port for this MAC address, then it forwards the frame to that port.
 - If the switch has not already learned the port for this MAC address, then the frame is flooded to all ports. Too much port flooding leads to network congestion.
 - If the switch has already learned the port for this MAC address, but the destination port is the same as the port it came in on, then it filters the frame.

Figure 115 MAC Table Flowchart



29.2 Viewing MAC Table

Click **Management** in the navigation panel and then **MAC Table** to display the following screen. The MAC Table can hold up to 16K entries.

Figure 116 MAC Table

Index	MAC Address	VID	Port	Type
1	00:00:01:aa:bb:cc	1	4	dynamic
2	00:00:04:a0:00:31	1	4	dynamic
3	00:00:04:a0:00:35	1	4	dynamic
4	00:00:1c:d4:ae:04	1	4	dynamic
5	00:00:85:0b:81:30	1	4	dynamic
6	00:00:86:46:4c:0e	1	4	dynamic
7	00:00:86:46:fc:a4	1	4	dynamic
8	00:00:86:47:0c:66	1	4	dynamic
9	00:00:86:47:11:91	1	4	dynamic
10	00:00:e2:82:90:b5	1	4	dynamic

The following table describes the labels in this screen.

Table 77 MAC Table

LABEL	DESCRIPTION
Sort by	Click one of the following buttons to display and arrange the data according to that button type. The information is then displayed in the summary table below.
MAC	Click this button to display and arrange the data according to MAC address.
VID	Click this button to display and arrange the data according to VLAN group.
Port	Click this button to display and arrange the data according to port number.
Index	This is the incoming frame index number.
MAC Address	This is the MAC address of the device from which this incoming frame came.
VID	This is the VLAN group to which this frame belongs.
Port	This is the port from which the above MAC address was learned.
Type	This shows whether the MAC address is dynamic (learned by the switch) or static (manually entered in Static MAC Forwarding).

ARP Table

This chapter introduces the ARP Table.

30.1 Introduction to ARP Table

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network.

An IP (version 4) address is 32 bits long. In an Ethernet LAN, MAC addresses are 48 bits long. The ARP Table maintains an association between each MAC address and its corresponding IP address.

30.1.1 How ARP Works

When an incoming packet destined for a host device on a local area network arrives at the switch, the switch's ARP program looks in the ARP Table and, if it finds the address, sends it to the device.

If no entry is found for the IP address, ARP broadcasts the request to all the devices on the LAN. The switch fills in its own MAC and IP address in the sender address fields, and puts the known IP address of the target in the target IP address field. In addition, the switch puts all ones in the target MAC field (FF.FF.FF.FF.FF.FF is the Ethernet broadcast address). The replying device (which is either the IP address of the device being sought or the router that knows the way) replaces the broadcast address with the target's MAC address, swaps the sender and target pairs, and unicasts the answer directly back to the requesting machine. ARP updates the ARP Table for future reference and then sends the packet to the MAC address that replied.

30.2 Viewing ARP Table

Click **Management** in the navigation panel and then **ARP Table** to open the following screen. The ARP table can hold up to 500 entries.

Figure 117 ARP Table

ARP Table			
Index	IP Address	MAC Address	Type
1	127.0.0.101	00:a0:c5:32:71:95	dynamic
2	127.0.0.102	00:a0:c5:32:71:97	dynamic
3	127.0.0.103	00:a0:c5:61:28:92	dynamic
4	127.0.0.104	00:a0:c5:ff:12:6c	dynamic
5	127.0.0.105	00:a0:c5:4b:d6:67	dynamic
6	169.254.170.66	00:0b:cd:94:85:00	dynamic
7	172.17.2.1	00:60:b0:d6:e1:ad	dynamic
8	172.17.2.4	00:01:e6:61:26:d4	dynamic
9	172.17.2.6	00:10:83:95:30:a1	dynamic
10	172.17.2.254	00:01:30:b8:16:40	dynamic
11	172.21.0.2	00:05:5d:04:30:f1	dynamic
12	172.21.0.254	00:01:30:b8:16:40	dynamic
13	172.21.1.166	00:02:b3:2c:79:93	dynamic
14	172.21.2.229	00:50:8d:36:37:e2	dynamic
15	172.21.3.6	00:50:8d:36:3c:3b	dynamic
16	172.21.3.7	00:50:ba:ad:75:dd	dynamic
17	172.21.3.11	00:50:8d:af:13:31	dynamic
18	172.21.3.15	00:00:e8:89:88:06	dynamic
19	172.21.3.18	00:50:8d:af:2f:28	dynamic
20	172.21.3.19	00:a0:c5:01:23:46	dynamic
21	172.21.3.20	08:00:46:68:10:58	dynamic
22	172.21.3.21	00:0b:cd:94:89:32	dynamic
23	172.21.3.23	00:00:e2:93:68:06	dynamic
24	172.21.3.25	00:05:5d:e1:6c:cb	dynamic

The following table describes the labels in this screen.

Table 78 ARP Table

LABEL	DESCRIPTION
Index	This is the ARP Table entry number.
IP Address	This is the learned IP address of a device connected to a switch port with corresponding MAC address below.
MAC Address	This is the MAC address of the device with corresponding IP address above.
Type	This shows whether the MAC address is dynamic (learned by the switch) or static (manually entered in Static MAC Forwarding).

Configure Clone

This chapter shows you how you can copy the settings of one port onto other ports.

31.1 Configure Clone

Cloning allows you to copy the basic and advanced settings from a source port to a destination port or ports. Click **Management, Configure Clone** to open the following screen.

Figure 118 Configure Clone

The screenshot shows the 'Configure Clone' web interface. At the top, there is a title bar with a blue background and the text 'Configure Clone'. Below the title bar, there are two input fields: 'Source Port' and 'Destination'. The 'Source Port' field is currently empty. Below the input fields, there is a section titled 'Port Features' in blue text. This section is divided into two main categories: 'Basic Setting' and 'Advanced Application'. Under 'Basic Setting', there are six checkboxes: 'Active', 'Name', 'Speed / Duplex', 'BPDU Control', 'Flow Control', and 'Intrusion Lock'. Under 'Advanced Application', there are ten checkboxes: 'VLAN1 q', 'VLAN1 q Member', 'Bandwidth Control', 'Port Security', 'Broadcast Storm Control', 'Mirroring', 'Port Authentication', 'Queuing Method', 'IGMP Filtering', 'Spanning Tree Protocol', 'Multiple Rapid Spanning Tree Protocol', and 'Port-based VLAN'. At the bottom of the interface, there are two buttons: 'Apply' and 'Cancel'.

The following table describes the labels in this screen.

Table 79 Configure Clone

LABEL	DESCRIPTION
Source/ Destination Port	Enter the source port under the Source label. This port's attributes are copied. Enter the destination port or ports under the Destination label. These are the ports which are going to have the same attributes as the source port. You can enter individual ports separated by a comma or a range of ports by using a dash. Example: <ul style="list-style-type: none">• 2, 4, 6 indicates that ports 2, 4 and 6 are the destination ports.• 2-6 indicates that ports 2 through 6 are the destination ports.
Basic Setting	Select which port settings (you configured in the Basic Setting menus) should be copied to the destination port(s).
Advanced Application	Select which port settings (you configured in the Advanced Application menus) should be copied to the destination ports.
Apply	Click Apply to save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields.

PART V

Commands and Troubleshooting

Introducing the Commands (207)
Command Examples (239)
IEEE 802.1Q Tagged VLAN Commands (257)
Troubleshooting (265)

Introducing the Commands

This chapter introduces the commands and gives a summary of commands available.

32.1 Overview

In addition to the web configurator, you can use line commands to configure the switch. Use line commands for advanced switch diagnosis and troubleshooting. If you have problems with your switch, customer support may request that you issue some of these commands to assist them in troubleshooting.

32.1.1 Switch Configuration File

When you configure the switch using either the CLI or web configurator, the settings are saved as a series of commands in a configuration file on the switch. You can perform the following with a configuration file:

- Back up switch configuration once the switch is set up to work in your network.
- Restore switch configuration.
- Use the same configuration file to set all switches (of the same model) in your network to the same settings.



You may also edit a configuration file using a text editor.



Make sure you use valid commands. The switch rejects configuration files with invalid or incomplete commands.

32.2 Accessing the CLI

You can use a direct console connection or Telnet to access the CLI on the switch.



The switch automatically logs you out of the management interface after five minutes of inactivity. If this happens to you, simply log back in again.

32.2.1 Access Priority

- By default, the switch allows multiple concurrent logins. However, no more than ten concurrent login sessions are allowed.
- If you use the `no multi-login` command in the configuration mode to disallow multiple concurrent logins, only one concurrent access to the CLI is allowed via either the console port or Telnet. Console port access has higher priority.

32.2.2 The Console Port

Connect to the switch's console port using a terminal emulation software configured to the following settings:

- VT100 terminal emulation
- 9600 bps
- No parity
- 8 data bits
- 1 stop bit
- No flow control

32.2.2.1 Initial Screen

When you turn on your switch, it performs several internal tests as well as line initialization. You can view the initialization information using the console port. After the initialization, the login screen displays (refer to [Section 32.3 on page 209](#)).

Figure 119 Initial Console Port Screen

```
Copyright (c) 1994 - 2006 ZyXEL Communications Corp.
initialize mgmt, ethernet address: 00:13:49:18:00:30
initialize switch, ethernet address: 00:13:49:18:00:31
Initializing switch unit 0...
Initializing VLAN Database...
Initializing IP Interface...
Initializing Advanced Applications...
Initializing Command Line Interface...
Initializing Web Interface...
Restore System Configuration....
Press ENTER to continue...
```

32.2.3 Telnet

Use the following steps to telnet into your switch.

- 1 For local management, connect your computer to the RJ-45 management port (labeled **MGMT**) on the switch.
- 2 Make sure your computer IP address and the switch IP address are on the same subnet. In Windows, click **Start** (usually in the bottom left corner), **Run** and then type “telnet 192.168.0.1” (the default management IP address) and click **OK**.
- 3 A login screen displays (refer to [Section 32.3 on page 209](#)).

32.3 The Login Screen

After you have successfully established a connection to the switch using a direct console connection or Telnet, a login screen displays as shown below. For your first login, enter the default administrator login username “admin” and password “1234”.

Figure 120 CLI: Login Screen

```
Enter User Name : admin
Enter Password : XXXX
```

32.4 Command Syntax Conventions

The rules of the commands are listed next.

- The command keywords are in *courier new* font.
- The required fields in a command are enclosed in angle brackets <>, for instance, ping <ip> means that you must specify an IP number for this command.
- The optional fields in a command are enclosed in square brackets [], for instance, configure snmp-server [contact <system contact>] [location <system location>] means that the contact and location fields are optional.
- “Command” refers to a command used in the command line interface (CLI command).
- The | symbol means “or”.
- The entry <cr> in the command lines refers to carriage return. Press [ENTER] or carriage return after a command to execute the command.
- Use the up (↑) or down (↓) arrow key to scroll through the command history list.
- The CLI does not accept partial or incomplete commands. You may enter a unique part of a command and press [TAB] to have the switch automatically display the full command. For example, if you enter “config” and press [TAB], the full command of “configuration” automatically displays.
- Each interface refers to an Ethernet port on the switch. Commands configured after the interface command correspond to those ports.
- Type multiple ports or port ranges separated by a comma. Ranges of port numbers are typed separated by a dash.

32.5 Getting Help

The system includes a help facility to provide you with the following information about the commands:

- List of available commands under a command group.
- Detailed descriptions of the commands.

32.5.1 List of Available Commands

Enter “help” to display a list of available commands and the corresponding sub commands.

Enter “?” to display a list of commands you can use.

Figure 121 CLI Help: List of Commands: Example 1

```
sysname> help
  Commands available:
  help
  logout
  exit
  history
  enable
  show ip <cr>
  show hardware-monitor <C|F>
  show system-information
  ping help
  ping <ip|host-name> [vlan <vlan-id>][..]
  ping <ip|host-name> <cr>
  traceroute help
  traceroute <ip|host-name> [vlan <vlan-id>][..]
  traceroute <ip|host-name> <cr>
  ssh <1|2> <[user@]dest-ip> [command </>]
  ssh <1|2> <[user@]dest-ip> <cr>
sysname>
```

Figure 122 CLI Help: List of Commands: Example 2

```
sysname> ?
  enable           Turn on privileged commands
  exit             Exit from the EXEC
  help             Description of the interactive help system
  history          Show a list of previously run commands
  logout           Exit from the EXEC
  ping             Exec ping
  show             Show system information
  ssh              SSH client
  traceroute       Exec traceroute
sysname>
```

32.5.2 Detailed Command Information

Enter <command> help to display detailed sub command and parameters.

Enter `<command> ?` to display detailed help information about the sub commands and parameters.

Figure 123 CLI Help: Detailed Command Information: Example 1

```
sysname> ping help
  Commands available:
  ping <ip|host-name>
    <
      [ in-band|out-of-band|vlan <vlan-id> ]
      [ size <0-1472> ]
      [ -t ]
    >
sysname>
```

Figure 124 CLI: Help: Detailed Command Information: Example 2

```
sysname> ping ?
  <ip|host-name>      destination ip address
  help                Description of ping help
```

32.6 Privilege Levels

You can use a command whose privilege level is equal to or less than that of your login account. For example, if your login account has a privilege level of 12, you can use all commands with privilege levels from 0 to 12. 0-privileged commands are available to all login accounts.



If you use an external RADIUS server to authenticate users, you can use a VSA (Vendor Specific Attribute) to configure a privilege level for an account on the RADIUS server. See [Section 16.1.1.1 on page 123](#) for more information.

32.7 Command Modes

There are three command modes: **User**, **Enable** and **Configure**. The modes (and commands) available to you depend on what level of privilege your account has. Use the `logins username` command to set up accounts and privilege levels.

When you log into the command interpreter with a read-only account (having a privilege of 0 to 12), the initial mode is User mode. The User mode commands are a subset of the Enable mode commands. The User mode command prompt ends with an angle bracket (`>`).

To enter Enable (or privileged) mode, type `enable` and enter the administrator password when prompted (the default is 1234). When you enter Enable mode, the command prompt changes to the pound sign (#). If you log into the command interpreter as an administrator (**admin**) you automatically enter Enable mode.

The following table describes command interpreter modes and how to access them.

Table 80 Command Interpreter Mode Summary

MODE	DESCRIPTION	HOW TO LOGIN/ ACCESS	PROMPT
User	Commands available in this mode are a subset of the enable mode. You can perform basic tests and display system information.	Default login level for a read-only account.	<code>sysname></code> The first part of the prompt is the system name. In the CLI examples in this User's Guide, the system name is always "sysname".
Enable	Commands available in this mode allow you to save configuration settings, reset configuration settings as well as display further system information. This mode also contains the <code>configure</code> command which takes you to config mode.	Default login level for the administrator or accounts with a privilege of 13 or 14. Read-only accounts (with a privilege of 0 to 12) need to type the <code>enable</code> command and enter the enable mode password.	<code>sysname#</code>
Config	Commands available in this mode allow you to configure settings that affect the switch globally.	Type <code>config</code> or <code>configure</code> in the enable mode prompt.	<code>sysname(config)#</code>
Command modes that follow are sub-modes of the config mode and can only be accessed from within the config mode.			
Config-vlan	This is a sub-mode of the config mode and allows you to configure VLAN settings.	Type <code>vlan</code> followed by a number (between 1 and 4094). For example, <code>vlan 10</code> to configure settings for VLAN 10.	<code>sysname(config-vlan)#</code>
Config-interface	This is a sub-mode of the config mode and allows you to configure port specific settings.	Type <code>interface port-channel</code> followed by a port number. For example, <code>interface port-channel 8</code> to configure port 8 on the switch.	<code>sysname(config-interface)#</code>
Config-mvr	This is a sub-mode of the config mode and allows you to configure multicast VLAN settings.	To enter MVR mode, enter <code>mvr</code> followed by a VLAN ID (between 1 and 4094). For example, enter <code>mvr 2</code> to configure multicast settings on VLAN 2.	<code>sysname(config-mvr)#</code>

Enter `exit` to quit from the current mode or enter `logout` to exit the command interpreter.

32.8 Using Command History

The switch keeps a list of commands you have entered for the current CLI session. You can use any commands in the history again by pressing the up (↑) or down (↓) arrow key to scroll through the previously used commands and press [ENTER]. Use the history command to display the list of commands.

Figure 125 CLI: History Command Example

```
sysname> history
  enable
  exit
  show ip
  history
sysname>
```

32.9 Saving Your Configuration

After you set the switch settings with the configuration commands, use the `write memory` command to save the changes permanently.

Figure 126 CLI: write memory

```
sysname# write memory
```



The `write memory` command is not available in User mode.



You must save your changes after each CLI session. All unsaved configuration changes are lost once you restart the switch.

32.9.1 Logging Out

In User or Enable mode, enter the `exit` or `logout` command to log out of the CLI. In Config mode, entering `exit` takes you out of Config mode and into Enable mode and entering `logout` logs you out of the CLI.

32.10 Command Summary

The following sections summarize the commands available in the switch together with a brief description of each command. Commands listed in the tables are in alphabetical order. See the related section in the User's Guide for more background information.

32.10.1 User Mode

The following table describes the commands available for User mode.

Table 81 Command Summary: User Mode

COMMAND		DESCRIPTION	PRIVILEGE
enable		Accesses Enable (or privileged) mode.	0
exit		Logs out from the CLI.	0
help		Displays help information.	0
history		Displays a list of previously command(s) that you have executed. The switch stores up to 256 commands in history.	0
logout		Exits the CLI.	0
ping	<IP host-name> [<in-band out-of-band vlan <vlan-id>] [size <0-1472>] [-t]	Sends a Ping request to an Ethernet device.	0
show	alarm-status	Displays alarm status and configuration.	0
	hardware-monitor<C F>	Displays current hardware monitor information with the specified temperature unit (Celsius C or Fahrenheit F).	0
	ip	Displays IP related information.	0
	system-information	Displays general system information.	0
ssh	<1 2> <[user@]dest-ip>	Connects to an SSH server with the specified SSH version.	0
traceroute	<ip host-name> [in-band out-of-band vlan <vlan-id>] [ttl <1-255>] [wait <1-60>] [queries <1-10>]	Determines the path a packet takes to a device.	0

32.10.2 Enable Mode

The following table describes the commands available for Enable mode.

Table 82 Command Summary: Enable Mode

COMMAND		DESCRIPTION	PRIVILEGE	
baudrate	<1 2 3 4 5>		Changes the console port speed. Choices are 1 (38400), 2 (19200), 3(9600), 4 (57600) and 5 (115200).	13
boot	config <index>		Restarts the system with the specified configuration file (1 or 2).	13
cable-diagnos- tics	<port-list>		Displays whether a cable is connected to the port (good) or not (open).	13
configure			Accesses Configuration mode.	13
copy	running-config interface port- channel <port> <port-list>		Clones (copies) the attributes from the specified port to other ports.	13
		[active] [name] [speed-duplex] [bpdu-control] [flow-control] [intrusion-lock] [vlanlq] [vlanlq-member] [bandwidth-limit] [port-security] [broadcast-storm- control] [mirroring] [port-access- authenticator] [queuing-method] [igmp-filtering] [spanning-tree] [mrstp] [port-based-vlan]	Copies the specified attributes from one port to other ports.	13
	running-config tftp <ip> <remote- file>		Backs up running configuration to the specified TFTP server with the specified file name.	13
	tftp	config <index> <ip> <remote- file>	Restores configuration with the specified filename from the specified TFTP server.	13
		flash <ip> <remote-file>	Restores firmware via TFTP.	13
disable			Exits Enable (or privileged) mode.	13
enable			Accesses Enable (or privileged) mode.	13
erase	running-config		Resets to the factory default settings.	13

Table 82 Command Summary: Enable Mode (continued)

COMMAND		DESCRIPTION	PRIVILEGE	
		interface port-channel <port-list>	Resets to the factory default settings on a per port basis.	13
		interface port-channel <port-list> [[active] [name] [speed-duplex] [bpdu-control] [flow-control] [intrusion-lock] [vlanlq] [vlanlq-member] [bandwidth-limit] [port-security] [broadcast-storm-control] [mirroring] [port-access-authenticator] [queuing-method] [igmp-filtering] [spanning-tree] [mrstp] [port-based-vlan]]	Resets to the factory default settings on a per port basis and optionally on a per feature configuration basis.	13
exit			Exits the CLI.	13
help			Displays help information.	13
history			Displays a list of command(s) that you have previously executed.	13
igmp-flush			Removes all IGMP information.	13
kick tcp	<Session ID>		Drops a TCP session.	13
logout			Exits the CLI.	13
mac-flush			Clears the MAC address table.	13
	<port-num>		Removes all learned MAC address on the specified port(s).	13
no	arp		Flushes the ARP (Address Resolution Protocol) table.	13
	interface <port-number>		Clears the interface status of the specified port(s).	13
	logging		Clears the system log.	13
ping	<ip host-name> [<i><in-band out-of-band vlan <vlan-id></i>] [size <0-1472>] [-t]		Sends a Ping request to an Ethernet device.	13

Table 82 Command Summary: Enable Mode (continued)

COMMAND		DESCRIPTION	PRIVILEGE
reload	config <index>	Restarts the system with the specified configuration file.	13
show	alarm-status	Displays alarm status and configuration.	13
	classifier	Displays all classifier related information.	13
	<name>	Displays the specified classifier related information.	13
	cluster	Displays cluster management status.	13
	candidates	Displays cluster candidate information.	13
	member	Displays the status of the cluster member(s).	13
	member config	Displays the configuration of the cluster member(s).	13
	member mac <mac-addr>	Displays the MAC address of the cluster member(s).	13
	garp	Displays GARP information.	13
	hardware-monitor <C F>	Displays current hardware monitor information with the specified temperature unit (Celsius C or Fahrenheit F).	13
	https	Displays the HTTPS information.	13
	certificate	Displays the HTTPS certificates.	13
	key <rsa dsa>	Displays the HTTPS key.	13
	session	Displays current HTTPS session(s).	13
	timeout	Displays the HTTPS session timeout.	13
	igmp-filtering profile	Displays IGMP filter profile settings.	13
	igmp-snooping	Displays IGMP snooping settings.	13
	interfaces <port-list>	Displays current interface status.	13
	interfaces config <port-list>	Displays current interface configuration.	13
	bandwidth-control	Displays bandwidth control settings.	13
	bstorm-control	Displays broadcast storm control settings.	13
	egress	Displays outgoing port information.	13
	igmp-filtering	Displays IGMP filter profile settings.	13

Table 82 Command Summary: Enable Mode (continued)

COMMAND		DESCRIPTION	PRIVILEGE
	igmp-group-limited	Displays IGMP group settings.	13
	igmp-immediate-leave	Displays IGMP immediate leave settings.	13
	igmp-query-mode	Displays IGMP query mode settings on the port(s).	13
ip		Displays IP related information.	13
	TCP	Displays the switch's current TCP sessions.	13
	UDP	Displays the switch's current UDP sessions.	13
	arp	Displays the ARP table.	13
	route	Displays IP routing information.	13
	route static	Displays IP static route information.	13
lacp		Link Aggregation Control Protocol.	13
logging		Displays system logs.	13
loginPrecedence		Displays login precedence settings.	14
logins		Displays login account information.	14
mac	address-table all [mac vid port]	Displays MAC address table. You can sort by MAC address, VID or port.	13
	address-table count	Displays the total number of MAC addresses in the MAC address table.	13
	address-table static	Displays static MAC address table. You can sort by MAC address, VID or port.	13
mac-aging-time		Displays MAC learning aging time.	13
mrstp <tree-index>		Displays the STP settings for the specific tree.	13
multicast		Displays multicast settings.	13
multi-login		Displays multi-login information	14
mvr		Displays all MVR (Multicast VLAN Registration) settings.	13
	<vlan-id>	Displays specified MVR information.	13
policy		Displays all policy related information.	13
	<name>	Displays the specified policy related information.	13
port-access-authenticator		Displays all port authentication settings.	13

Table 82 Command Summary: Enable Mode (continued)

COMMAND		DESCRIPTION	PRIVILEGE	
		<port-list>	Displays port authentication settings on the specified port(s).	13
	port-security		Displays all port security settings.	13
		<port-list>	Displays port security settings on the specified port(s).	13
	radius-server		Displays RADIUS server settings.	13
	remote-management		Displays all secured client information.	13
		<index>	Displays the specified secured client information.	13
	running-config		Displays all current operating configuration without page breaks.	13
		interface port-channel <port-list> [[active] [name] [speed-duplex] [bpdu-control] [flow-control] [intrusion-lock] [vlan1q] [vlan1q-member] [bandwidth-limit] [port-security] [broadcast-storm-control] [mirroring] [port-access-authenticator] [queuing-method] [igmp-filtering] [spanning-tree] [mrstp] [port-based-vlan]]	Displays current operating configuration on a port by port basis. Optionally specifies which settings are displayed.	13
		page	Displays current operating configuration page by page. You need to press any key to go to the next page.	13
	service-control		Displays service control settings.	13
	snmp-server		Displays SNMP settings.	13
	spanning-tree	config	Displays Spanning Tree Protocol (STP) settings.	13
	ssh		Displays general SSH settings.	13
		key <rsa rsa dsa>	Displays the SSH public and private keys	13
		known-hosts	Displays known SSH hosts information.	13
		session	Displays current SSH session(s).	13

Table 82 Command Summary: Enable Mode (continued)

COMMAND		DESCRIPTION	PRIVILEGE
	system-information		Displays general system information.
	time		Displays current system time and date.
	timesync		Displays time server information.
	trunk		Displays link aggregation information.
	vlan		Displays the status of all VLANs.
		<vlan-id>	Displays the status of the specified VLAN.
	vlanlq	gvrp	Displays GVRP setting.
		port-isolation	Displays port isolation setting.
ssh	<1 2> <[user@]dest-ip>		Connects to an SSH server with the specified SSH version.
traceroute	<ip host-name> [in-band out-of-band vlan <vlan-id>] [ttl <1-255>] [wait <1-60>] [queries <1-10>]		Determines the path a packet takes to a device.
write	memory		Saves the configuration to the configuration file the switch is currently using.
		<index>	Saves the configuration to the specified configuration file on the switch.

32.10.3 Configure Mode

The following table lists the commands in Configuration (or Config) mode.

Table 83 Command Summary: Configure Mode

COMMAND		DESCRIPTION	PRIVILEGE
admin-password	<pw-string> <confirm-string>		Changes the administrator password.
bandwidth-control			Enables bandwidth control.
bcp-transparency			Enables Bridge Control Protocol Transparency.

Table 83 Command Summary: Configure Mode (continued)

COMMAND		DESCRIPTION	PRIVILEGE
classifier	<pre><name> <[packet-format <802.3untag 802.3t ag EtherIIuntag Ether IItag>] [priority <0-7>] [vlan <vlan-id>] [ethernet-type <ether-num ip ipx arp rarp appletalk decnet sna netbios dlc>] [source-mac <src- mac-addr>] [source-port <port-num>] [destination-mac <dest-mac-addr>] [dscp <0-63>] [ip-protocol <protocol- num tcp udp icmpl e gp ospf rsvp igmp igp pim ipsec>] [establish-only]] [source-ip <src- ip-addr> [mask- bits <mask-bits>]] [source-socket <socket-num>] [destination-ip <dest-ip-addr> [mask-bits <mask- bits>]] [destination- socket <socket- num>] [inactive]></pre>	Configures a classifier. A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming port number.	13
cluster	<vlan-id>	Sets the cluster management VLAN ID.	13
	member <mac-address> password <password-str>	Sets the cluster member switch's hardware MAC address and password.	13
	name <cluster name>	Configures a name to identify the cluster manager	13
	rcommand <mac-address>	Logs into a cluster member switch.	13
default-management	<in-band out-of-band>	Specifies through which traffic flow the switch is to send packets.	13
dhcp-relay		Enables DHCP relay.	13

Table 83 Command Summary: Configure Mode (continued)

COMMAND		DESCRIPTION	PRIVILEGE
	helper-address <svr_ip> [svr2_ip] [svr3_ip]	Sets the IP addresses of up to 3 DHCP servers.	13
	information	Allows the switch to add system name to agent information.	13
	option	Allows the switch to add DHCP relay agent information.	13
exit		Returns you to User mode.	13
garp	join <100-65535> leave <msec> leaveall <msec>	Configures GARP time settings.	13
help		Displays help information.	13
history		Displays a list of previously command(s) that you have executed.	13
hostname	<name_string>	Sets the switch's name for identification purposes. Note: Spaces are allowed in the CLI only when the system name is in "quotation marks". Example: <config># hostname "GS-3012"	13
https	cert-regeneration <rsa dsa>	Re-generates a certificate.	13
igmp-filtering		Enables IGMP filtering on the switch.	13
	profile <name> start-address <ip> end-address <ip>	Sets the range of multicast address(es) in a profile.	13
igmp-snooping		Enables IGMP snooping.	13
	8021p-priority <0 - 7>	Select a priority level (0-7) with which the switch replaces the priority in outgoing IGMP control packets (belonging to this multicast VLAN).	13
	host-timeout <1 - 16711450>	Sets the IGMP host timeout value.	13
	leave-timeout <1 - 16711450>	Sets the IGMP leave timeout value.	13
	reserved-multicast-group <drop flooding>	Sets how to treat a frame with a reserved multicast address.	13

Table 83 Command Summary: Configure Mode (continued)

COMMAND		DESCRIPTION	PRIVILEGE	
	unknown-multicast-frame <drop flooding>		Sets how to treat traffic from unknown multicast group.	13
interface	port-channel <port-list>		Enables a port or a list of ports for configuration. See Section 32.10.5 on page 233 for more details.	13
ip	address	<ip> <mask>	Sets the IP address and subnet mask of the out-of-band management port.	13
	address default-gateway	<ip>	Sets the default gateway's IP address for the out-of-band management port.	13
	name-server	<ip>	Sets the IP address of a domain name server.	13
	route	<ip> <mask> <next-hop-ip>	Creates a static route.	13
		<ip> <mask> <next-hop-ip> [metric <metric>] [name <name>] [inactive]	Sets the metric of a static route or deactivates a static route.	13
lACP			Enables Link Aggregation Control Protocol (LACP).	13
	system-priority	<1-65535>	Sets the priority of an active port using LACP.	13
loginPrecedence	<LocalOnly LocalRADIUS RADIUSOnly>		Select which database the switch should use (first) to authenticate a user.	14
logins	username <name> password <pwd>		Configures up to four read-only login accounts.	14
	username <name> privilege <0-14>		Sets the access privilege for the existing login accounts. The higher the value, the more commands are allowed.	14
logout			Exits the CLI.	13
mac-aging-time	<10-3000>		Sets learned MAC aging time.	13
mac-filter	name <name> mac <mac-addr> vlan <vlan-id> drop <src/dst/both>		Configures a static MAC address port filtering rule.	13
	name <name> mac <mac-addr> vlan <vlan-id> drop <src/dst/both> inactive		Disables a static MAC address port filtering rule.	13

Table 83 Command Summary: Configure Mode (continued)

COMMAND		DESCRIPTION	PRIVILEGE	
mac-forward	name <name> mac <mac-addr> vlan <vlan-id> interface <interface-id>	Configures a static MAC address forwarding rule.	13	
	name <name> mac <mac-addr> vlan <vlan-id> interface <interface-id> inactive	Disables a static MAC address forwarding rule.	13	
mirror-port		Enables port mirroring.	13	
	<port-num>	Sets a monitor port (the port to which traffic is copied for analysis).	13	
mode	zynos	Changes the CLI mode to the ZYNOS format.	13	
mrstp <tree-index>		Activates the specified STP configuration.	13	
	hello-time <1-10> maximum-age <6-40> forward-delay <4-30>	Sets Hello Time, Maximum Age and Forward Delay to the specified tree.	13	
	priority <0-61440>	Sets the priority of the switch to the specified tree.	13	
mrstp interface <port-list>		Activates MRSTP on the specified ports.	13	
	path-cost <1-65535>	Sets a path cost to the specified ports.	13	
	priority <0-255>	Sets the priority value to the specified ports for STP.	13	
	tree-index <1-2>	Assigns a specific STP configuration to the ports.	13	
multi-login		Enables multi-login.	14	
mvr <vlan-id>		Enters the MVR (Multicast VLAN Registration) configuration mode. See Section 32.10.6 on page 236 or more information.	13	
no			13	
	bandwidth-control	Disables bandwidth control.	13	
	bcp-transparency	Disables bridging control protocols such as STP.	13	
	classifier	<name>	Disables the classifier. Each classifier has one rule. If you disable a classifier you cannot use policy rule related information.	13

Table 83 Command Summary: Configure Mode (continued)

COMMAND		DESCRIPTION	PRIVILEGE
	<name> inactive	Enables a classifier.	13
cluster		Disables cluster management on the switch.	13
	member <mac-address>	Removes the cluster member.	13
dhcp-relay		Disables DHCP relay.	13
	information	System name is not appended to option 82 information field.	13
	option	Disables the relay agent information option 82.	13
igmp-filtering		Clears the IGMP filtering settings on the switch.	13
	profile <name>	Deletes the IGMP filtering profile.	13
	profile <name> start-address <ip> end-address <ip>	Deletes a rule in the IGMP filtering profile.	13
igmp-snooping		Disables IGMP snooping.	13
ip		Sets the management IP address to the default value.	13
	route <ip> <mask>	Removes a specified IP static route.	13
	route <ip> <mask> inactive	Enables a specified IP static route.	13
lACP		Disables the link aggregation control protocol (dynamic trunking) on the switch.	13
logins	username <name>	Removes the login account.	14
mac-filter	mac <mac-addr> vlan <vlan-id> inactive	Enables the specified MAC-filter rule.	13
	mac <mac-addr> vlan <vlan-id>	Disables the specified MAC filter rule.	13
mac-forward	mac <mac-addr> vlan <vlan-id> interface <interface-id> inactive	Enables the specified MAC address, belonging to a VLAN group (if any) forwarded through an interface(s).	13
	mac <mac-addr> vlan <vlan-id> interface <interface-id>	Removes the specified MAC forwarding entry, belonging to a VLAN group (if any) forwarded through an interface(s).	13
mirror-port		Disables port mirroring on the switch.	13

Table 83 Command Summary: Configure Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
	mrstp	<tree-index>	Disables the specified STP configuration. tree-index: 1 or 2	13
	mrstp interface	<port-list>	Disables the STP assignment from the specified port(s).	13
	multi-login		Disables another administrator from logging into Telnet or the CLI.	14
	mvr	<vlan-id>	Disables MVR on the switch.	13
	policy	<name>	Deletes the policy. A policy sets actions for classifier traffic.	13
		<name> inactive	Enables a policy.	13
	port-access-authenticator		Disables port authentication on the switch.	13
		<port-list>	Disables authentication on the listed ports.	13
		<port-list> reauthenticate	Disables the re-authentication mechanism on the listed port(s).	13
	port-security		Disables port security on the switch.	13
		<port-list>	Disables port security on the specified ports.	13
		<port-list> learn inactive	Enables MAC address learning on the specified ports.	13
	radius-server	<index>	Disables the use of authentication from the specified RADIUS server.	13
	remote-management	<index>	Clears a secure client set entry from the list of secure clients.	13
		<index> service < [telnet] [ftp] [http] [icmp] [snmp] [ssh] [https]>	Disables a secure client set entry number from using the selected remote management service(s).	13
	service-control	ftp	Disables FTP access to the switch.	13
		http	Disables web browser control to the switch.	13
		https	Disables secure web browser access to the switch.	13
		icmp	Disables ICMP access to the switch such as pinging and tracerouting.	13
		snmp	Disables SNMP management.	13

Table 83 Command Summary: Configure Mode (continued)

COMMAND		DESCRIPTION	PRIVILEGE
	ssh	Disables SSH (Secure Shell) server access to the switch.	13
	telnet	Disables telnet access to the switch.	13
snmp-server	trap-destination <ip>	Removes a configured trap destination IP address.	13
spanning-tree		Disables STP.	13
	<port-list>	Disables STP on listed ports.	13
ssh	key <rsa1 rsa dsa>	Disables the secure shell server encryption key. Your switch supports SSH versions 1 and 2 using RSA and DSA authentication.	13
	known-hosts	Removes all remote hosts.	13
	known-hosts <host-ip>	Removes the specified remote hosts from the list of all known hosts.	13
	known-hosts <host-ip> [1024 ssh- rsa ssh-dsa]	Removes remote known hosts with the specified public key (1024-bit RSA1, RSA or DSA).	13
storm-control		Disables broadcast storm control.	13
syslog		Disables syslog.	13
	server <ip>	Disables a syslog server entry.	13
	server <ip> inactive	Enables a syslog server entry.	13
	type <system, interface, switch, authentication, ip>	Sets the device to not generate a category of logs.	13
timesync		Disables the time setting on the timeserver.	13
trunk	<T1 T2 T3 T4 T5 T6>	Disables the specified trunk group.	13
	<T1 T2 T3 T4 T5 T6> interface <port-list>	Removes ports from the specified trunk group.	13
	<T1 T2 T3 T4 T5 T6> lacp	Disables LACP in the specified trunk group.	13
vlan	<vlan-id>	Deletes the static VLAN entry.	13
vlan1q	gvrp	Disables GVRP on the switch.	13
	port-isolation	Disables port isolation.	13

Table 83 Command Summary: Configure Mode (continued)

COMMAND		DESCRIPTION	PRIVILEGE
password	<password>	Change the password for Enable mode.	14
policy	<name> classifier <classifier-list> <[vlan<vlan-id>] [egress-port <port-num>] [priority <0-7>] [dscp <0-63>] [tos <0-7>] [bandwidth <bandwidth>] [outgoing-packet- format <tagged untagged>] [out-of-profile- dscp <0-63>] [forward-action <drop forward>] [queue-action <prio-set prio- queue prio- replace-tos>] [diffserv-action <diff-set- tos diff-replace- priority diff- set-dscp>] [outgoing-mirror] [outgoing-eport] [outgoing-non- unicast-eport] [outgoing-set- vlan] [metering] [out-of-profile- action <[change- dscp][drop][forward] [set- drop-prec]>] [inactive]>	Configures a policy. A classifier distinguishes traffic into flows based on the configured criteria. A policy rule ensures that a traffic flow gets the requested treatment in the network.	13
port-access- authenticator		Enables 802.1x authentication on the switch.	13
	<port-list>	Enables 802.1x authentication on the specified port(s).	13
	<port-list> reauthenticate	Sets a subscriber to periodically re-enter his or her username and password to stay connected to a specified port.	13

Table 83 Command Summary: Configure Mode (continued)

COMMAND		DESCRIPTION	PRIVILEGE	
	<port-list> reauth-period <reauth-period>		Specifies how often a client has to re-enter the username and password to stay connected to the specified port(s).	13
port-security			Enables port security on the switch.	13
	<port-list>		Enables the port security feature on the specified port(s).	13
	<port-list> address-limit <number>		Limits the number of (dynamic) MAC addresses that may be learned on a port.	13
	<port-list> learn inactive		Disables MAC address learning on the specified port(s).	13
	<port-list> MAC- freeze		Disables MAC address learning and enables port security. Note: All previously learned dynamic MAC addresses are saved to the static MAC address table.	13
queue	priority <0-7> level <0-7>		Sets the priority level-to-physical queue mapping.	13
radius-server	host <index> <ip>		Specifies the IP address of RADIUS server 1 or RADIUS server 2 (index =1 or index =2).	13
		[auth-port <socket-number>] [key <key- string>	Sets the UDP port and shared key of the external RADIUS server.	13
	mode <priority round- robin>		Specifies the mode for RADIUS server selection.	13
	timeout <1-1000>		Specifies the RADIUS server timeout value.	13
remote- management	<index>		Enables a specified secured client set.	13
	<index> start-addr <ip> end-addr <ip> service <[telnet] [ftp] [http] [icmp] [snmp] [ssh] [https] >		Specifies a group of trusted computer(s) from which an administrator may use a service to manage the switch.	13

Table 83 Command Summary: Configure Mode (continued)

COMMAND		DESCRIPTION	PRIVILEGE
service-control	ftp <socket-number>	Allows FTP access on the specified service port.	13
	http <socket-number> <timeout>	Allows HTTP access on the specified service port and defines the timeout period.	13
	https <socket-number>	Allows HTTPS access on the specified service port.	13
	icmp	Allows ICMP access to the switch such as pinging and tracerouting.	13
	snmp	Allows SNMP management.	13
	ssh <socket-number>	Allows SSH access on the specified service port.	13
	telnet <socket-number>	Allows Telnet access on the specified service port.	13
snmp-server	[contact <system contact>] [location <system location>]	Sets the geographic location and the name of the person in charge of this switch.	13
	get-community <property>	Sets the get community.	13
	set-community <property>	Sets the set community.	13
	trap-community <property>	Sets the trap community.	13
	trap-destination <ip>	Sets the IP addresses of up to four stations to send your SNMP traps to.	13
spanning-tree		Enables STP on the switch.	13
	<port-list>	Enables STP on a specified port.	13
	<port-list> path-cost <1-65535>	Sets the STP path cost for a specified port.	13
	<port-list> priority <0-255>	Sets the priority for a specified port.	13
	hello-time <1-10> maximum-age <6-40> forward-delay <4-30>	Sets Hello Time, Maximum Age and Forward Delay.	13
	priority <0-61440>	Sets the bridge priority of the switch.	13
ssh	known-hosts <host-ip> <1024 ssh-rsa ssh-dsa> <key>	Adds a remote host to which the switch can access using SSH service.	13
storm-control		Enables broadcast storm control on the switch.	13
syslog	<cr>	Enables syslog.	13

Table 83 Command Summary: Configure Mode (continued)

COMMAND		DESCRIPTION	PRIVILEGE	
	server <ip>	inactive	Disables a syslog server entry.	13
		level <0-7>	Sets which severity level(s) of logs are sent to this syslog server. A lower number is more critical.	13
	type <system, interface, switch, authentication, ip>		Sets the device to generate a category of logs.	13
	type <system, interface, switch, authentication, ip>	facility <0-7>	Sets the facility (file) on the syslog server to which the switch sends a category of logs.	13
time	<Hour:Min:Sec>		Sets the time in hour, minute and second format.	13
	date <month/day/year>		Sets the date in year, month and day format.	13
	timezone <-1200 ... 1200>		Selects the time difference between UTC (formerly known as GMT) and your time zone.	13
timesync	<daytime time ntp>		Sets the time server protocol.	13
	server <ip>		Sets the IP address of your time server.	13
trunk	<T1 T2 T3 T4 T5 T6>		Activates a trunk group.	13
	<T1 T2 T3 T4 T5 T6> >interface <port-list>		Adds a port(s) to the specified trunk group.	13
	<T1 T2 T3 T4 T5 T6> >lacp		Enables LACP for a trunk group.	13
	interface <port-list> timeout <lacp-timeout>		Defines the port number and LACP timeout period.	13
vlan <1-4094>			Enters the VLAN configuration mode. See Section 32.10.4 on page 232 for more information.	13
vlan-type	<802.1q port-based>		Specifies the VLAN type.	13
vlanlq	gvrp		Allows VLAN groups beyond the local switch.	13
	port-isolation		Enables port isolation.	13

32.10.4 config-vlan Commands

The following table lists the `vlan` commands in configuration mode.

Table 84 Command Summary: config-vlan Commands

COMMAND			DESCRIPTION	PRIVILEGE
<code>vlan <1-4094></code>			Creates a new VLAN group.	13
	<code>exit</code>		Leaves the VLAN configuration mode.	13
	<code>fixed <port-list></code>		Specifies the port(s) to be a permanent member of this VLAN group.	13
	<code>forbidden <port-list></code>		Specifies the port(s) you want to prohibit from joining this VLAN group.	13
	<code>help</code>		Displays a list of available VLAN commands.	13
	<code>inactive</code>		Disables the specified VLAN.	13
	<code>ip address</code>	<code><ip-address></code> <code><mask></code>	Sets the IP address and subnet mask of the switch in the specified VLAN for packet loopback test.	13
		<code><ip-address></code> <code><mask></code> <code>manageable</code>	Allows the switch to be managed using this specified IP address.	13
		<code>default-gateway <ip-address></code>	Sets a default gateway IP address for this VLAN.	13
		<code>inband-default <ip-address></code> <code><mask></code>	Sets a static in-band IP address and subnet mask.	13
		<code>inband-default dhcp-bootp</code>	Sets the dynamic in-band IP address.	13
		<code>inband-default dhcp-bootp release</code>	Releases the dynamic in-band IP address.	13
		<code>inband-default dhcp-bootp renew</code>	Updates the dynamic in-band IP address.	13
	<code>name <name-str></code>		Specifies a name for identification purposes.	13
	<code>no</code>	<code>fixed <port-list></code>	Sets fixed port(s) to normal port(s).	13
		<code>forbidden <port-list></code>	Sets forbidden port(s) to normal port(s).	13
		<code>inactive</code>	Enables the specified VLAN.	13
		<code>ip address <ip-address> <mask></code>	Deletes the IP address and subnet mask from this VLAN.	13
		<code>ip address default-gateway</code>	Deletes the default gateway from this VLAN.	13

Table 84 Command Summary: config-vlan Commands (continued)

COMMAND		DESCRIPTION	PRIVILEGE
		ip address inband-default dhcp-bootp	13
		untagged <port-list>	13
	normal <port-list>		13
	untagged <port-list>		13

32.10.5 interface port-channel Commands

The following table lists the `interface port-channel` commands in configuration mode. Use these commands to configure the ports.

Table 85 Command Summary: Interface

COMMAND		DESCRIPTION	PRIVILEGE
interface port-channel <port-list>		Enables a port or a list of ports for configuration.	13
	bandwidth-limit		13
		cir	13
		cir <Kbps>	13
		egress	13
		egress <Kbps>	13
		pir	13
		pir <Kbps>	13
	bpdu-control	<peer tunnel discard network>	13
	broadcast-limit		13
		<pkt/s>	13
	dlf-limit		13
		<pkt/s>	13

Table 85 Command Summary: Interface (continued)

COMMAND		DESCRIPTION	PRIVILEGE
	egress set	<port-list>	13
	exit		13
	flow-control		13
	frame-type	<all tagged>	13
	gvrp		13
	help		13
	igmp-filtering profile <name>		13
	igmp-group- limited		13
	igmp-group- limited number <number>		13
	igmp-immediate- leave		13
	igmp-querier- mode <auto fixed edge >		13
	inactive		13
	ingress-check		13
	intrusion-lock		13
	mirror		13
		dir <ingress egress both>	13
	multicast-limit		13
		<pkt/s>	13

Table 85 Command Summary: Interface (continued)

COMMAND		DESCRIPTION	PRIVILEGE	
	name	<port-name-string>	Sets a name for your interface. Enter a descriptive name (up to nine printable ASCII characters).	13
	no			
		bandwidth-limit cir	Disables CIR bandwidth limits on the port(s).	13
		bandwidth-limit egress	Disables egress bandwidth limits on the port(s).	13
		bandwidth-limit pir	Disables PIR bandwidth limits on the port(s).	13
		broadcast-limit	Disables broadcast storm control limit on the port(s).	13
		dlf-limit	Disables destination lookup failure (DLF) on the port(s).	13
		egress set <port-list>	Disables the outgoing traffic port list for a port-based VLAN.	13
		flow-control	Disables flow control on the port(s).	13
		gvrp	Disables GVRP on the port(s).	13
		igmp-filtering profile	Disables IGMP filtering on the port.	13
		igmp-group- limited	Disables IGMP group limitation.	13
		igmp-immediate- leave	Disables IGMP immediate leave on the port.	13
		inactive	Enables the specified interface on the switch.	13
		ingress-check	Incoming traffic on the port(s) is not checked for VLAN tags.	13
		intrusion-lock	Disables intrusion-lock on a port so that a port can be connected again after you disconnected the cable.	13
		mirror	Disables port mirroring on the port(s).	13
		multicast-limit	Disables multicast limit on the port(s).	13
		vlan-trunking	Disables VLAN trunking on the port(s).	13
	pvid	<1-4094>	The default PVID is VLAN 1 for all ports. Sets a PVID in the range 1 to 4094 for the specified interface.	13
	qos priority	<0 .. 7>	Sets the quality of service priority for an interface.	13
	speed-duplex	<auto 10- half 10- full 100- half 100- full 1000- full>	Sets the duplex mode (half, full) and speed (10/100/1000 Mbps) of the connection on the interface. Selecting auto (auto-negotiation) makes one port able to negotiate with a peer automatically to obtain the connection speed and duplex mode that both ends support.	13

Table 85 Command Summary: Interface (continued)

COMMAND		DESCRIPTION	PRIVILEGE
	spq	Sets the interface to use Strict Priority Queuing.	13
	test	Performs an interface loopback test.	13
	vlan-trunking	Enables VLAN Trunking on ports connected to other switches or routers (but not ports directly connected to end users) to allow frames belonging to unknown VLAN groups to pass through the switch.	13
	wrr	Sets the interface to use Weighted Round Robin queuing (WRR).	13
	wt1> <wt2> ... <wt8>	Sets the WRR weight. A weight value of one to eight is given to each variable from wt1 to wt8.	13

32.10.6 mvr Commands

The following table lists the `mvr` commands in configuration mode.

Table 86 Command Summary: mvr Commands

COMMAND		DESCRIPTION	PRIVILEGE
	mvr <1-4094>	Enters the MVR (Multicast VLAN Registration) configuration mode.	13
	8021p-priority <0 - 7>	Select a priority level (0-7) with which the switch replaces the priority in outgoing IGMP control packets (belonging to this multicast VLAN).	13
	exit	Exist from the MVR configuration mode.	13
	group <name-str> start-address <ip> end-address <ip>	Sets the multicast group range for the MVR.	13
	inactive	Disables MVR settings.	13
	mode <dynamic compatible>	Sets the MVR mode (dynamic or compatible).	13
	name <name-str>	Sets the MVR name for identification purposes.	13
	no group	Disables all MVR group settings.	13
	no group <name-str>	Disables the specified MVR group setting.	13
	no inactive	Enables MVR.	13
	no receiver-port <port-list>	Disables the receiver port(s). An MVR receiver port can only receive multicast traffic in a multicast VLAN.	13
	no source-port <port-list>	Disables the source port(s). An MVR source port can send and receive multicast traffic in a multicast VLAN.	13
	no tagged <port-list>	Sets the port(s) to untag VLAN tags.	13

Table 86 Command Summary: mvr Commands (continued)

COMMAND		DESCRIPTION	PRIVILEGE
	receiver-port <port-list>	Sets the receiver port(s). An MVR receiver port can only receive multicast traffic in a multicast VLAN.	13
	source-port <port-list>	Sets the source port(s). An MVR source port can send and receive multicast traffic in a multicast VLAN.	13
	tagged <port-list>	Sets the port(s) to tag VLAN tags.	13

Command Examples

This chapter describes some commands in more detail.

33.1 Overview

These are commands that you may use frequently in maintaining your switch.

33.2 show Commands

These are the commonly used `show` commands.

33.2.1 show system-information

Syntax:

```
show system-information
```

This command shows the general system information (such as the firmware version and system up time).

An example is shown next.

Figure 127 show system-information Command Example

```
sysname> show system-information

System Name           : GS-3012
System Contact        :
System Location       :
Ethernet Address      : 00:a0:c5:da:d3:17
ZyNOS F/W Version     : V3.70(LR.0)b4 | 10/13/2006
RomRasSize            : 2453896
System up Time        : 0:01:03 (18db ticks)
Bootbase Version      : V0.6 | 03/02/2004
ZyNOS CODE            : RAS Oct 13 2006 09:58:56
Product Model         : GS-3012
sysname>
```

33.2.2 show hardware-monitor

Syntax:

```
show hardware-monitor [c|f]
```

This command displays the current hardware status (such as temperature and voltage levels).

Figure 128 how hardware-monitor Command Example

```
sysname> show hardware-monitor c

Temperature Unit : (c)
Temperature(%c)  Current    Max    Min  Threshold  Status
-----
                MAC      30.0   30.0   27.0    65.0  Normal
                CPU      29.5   29.5   27.0    65.0  Normal
                PHY      28.5   28.5   27.0    65.0  Normal

FAN Speed(RPM)  Current    Max    Min  Threshold  Status
-----
                FAN1     5716   5716   5625    4500  Normal
                FAN2     5625   5763   5536    4500  Normal
                FAN3     5625   5716   5580    4500  Normal

Voltage (V)     Current    Max    Min  Threshold  Status
-----
                2.5      2.560   2.560   2.560   +/-8%  Normal
                1.25     1.232   1.232   1.232   +/-11% Normal
                3.3      3.312   3.312   3.296   +/-7%  Normal
                12       11.977  11.977  11.977  +/-11% Normal
                5        4.999   4.999   4.999   +/-7%  Normal
                1.3      1.296   1.296   1.296   +/-10% Normal
                1.25     1.232   1.232   1.232   +/-8%  Normal
                BPS_12VIN  --      --      --      --      Absent
sysname>
```

33.2.3 show ip

Syntax:

```
show ip
```

This command displays the IP related information (such as IP address and subnet mask) on all switch interfaces.

Figure 129 show ip Command Example

```
sysname> show ip
Out-of-band Management IP Address = 192.168.0.1
Management IP Address
    IP[192.168.0.1], Netmask[255.255.255.0], VID[0]
IP Interface
    IP[192.168.1.1], Netmask[255.255.255.0], VID[1]
sysname>
```


33.2.4 show logging



This command is not available in User mode.

Syntax:

```
show logging
```

This command displays the system logs. The following figure shows an example.

Figure 130 show logging Command Example

```
sysname# show logging
 57 Thu Jan  1 00:00:05 1970 PINI  INFO  main: init completed
 58 Thu Jan  1 00:00:02 1970 PP0c -WARN  SNMP TRAP 3: link up
 59 Thu Jan  1 00:00:05 1970 PINI -WARN  SNMP TRAP 0: cold start
 60 Thu Jan  1 00:00:05 1970 PINI -WARN  SNMP TRAP 3: link up
 61 Thu Jan  1 00:00:05 1970 PINI  INFO  main: init completed
 62 Thu Jan  1 00:00:10 1970 PP24  INFO  adjtime task pause 1 day
 63 Thu Jan  1 00:14:36 1970 PP0c -WARN  SNMP TRAP 2: link down
Clear Error Log (y/n):
```



If you clear a log (by entering `y` at the “Clear Error Log (y/n):” prompt), you cannot view it again.

33.2.5 show interface

Syntax:

```
show interface [port-number]
```

This command displays statistics of a port. The following example shows that port 2 is up and the related information.

Figure 131 show interface Command Example

```

sysname# show interface 2
  Port Info      Port NO.      :2
                Link          :100M/F
                Statuss       :FORWARDING
                LACP          :Disabled
                TxPkts        :69
                RxPkts        :4
                Errors         :0
                Tx KBs/s       :1.684
                Rx KBs/s       :1.684
                Up Time        :0:02:12
TX Packet       Tx Packets    :69
                Multicast     :0
                Broadcast     :0
                Pause         :0
                Tagged        :0
RX Packet       Rx Packets    :4
                Multicast     :0
                Broadcast     :4
                Pause         :0
                Control       :0
TX Collison     Single         :0
                Multiple      :0
                Excessive     :0
                Late          :0
Error Packet    RX CRC         :0
                Length        :0
                Runt          :0
Distribution    64           :4
                65 to 127     :74
                128 to 255    :18
                256 to 511    :0
                512 to 1023   :0
                1024 to 1518  :44
                Giant         :0
sysname#

```

33.2.6 show mac address-table

Syntax:

```
show mac address-table <all <sort>|static>
```

where

<sort> = Specifies the sorting criteria (MAC, VID or port).

This command displays the MAC address(es) stored in the switch. The following example shows a static MAC address table.

Figure 132 show mac address-table Command Example

```

sysname# show mac address-table static
Port      VLAN ID      MAC Address      Type
CPU       1            00:a0:c5:01:23:46  Static
sysname#

```

33.3 ping

Syntax:

```
ping <ip> < [in-band|out-of-band|vlan <vlan-id> ] [ size <0-8024> ] [ -t ]>
```

where

<ip> = The IP address of an Ethernet device.

[in-band|out-of-band|vlan <vlan-id>] = Specifies the network interface or the VLAN ID to which the Ethernet device belongs.
 out-of-band refers the management port while in-band means the other ports on the switch.

[size <0-8024>] = Specifies the packet size to send.

[-t] = Sends Ping packets to the Ethernet device indefinitely. Click [CTRL]+ C to terminate the Ping process.

This command sends Ping packets to an Ethernet device. The following example sends Ping requests to and displays the replies from an Ethernet device with an IP address of 192.168.1.100.

Figure 133 ping Command Example

```

sysname# ping 192.168.1.100
sent  rcvd  rate   rtt    avg    mdev    max    min  reply from
  1     1    100     0     0     0     0     0   192.168.1.100
  2     2    100     0     0     0     0     0   192.168.1.100
  3     3    100     0     0     0     0     0   192.168.1.100
sysname#

```

33.4 traceroute

Syntax:

```
traceroute <ip> [in-band|out-of-band|vlan <vlan-id>][ttl <1-255>] [wait <1-60>] [queries <1-10>]
```

where

<ip> = The IP address of an Ethernet device.

[in-band|out-of-band|vlan <vlan-id>] = Specifies the network interface or the VLAN ID to which the Ethernet device belongs.

[ttl <1-255>] = Specifies the Time To Live (TTL) period.

[wait <1-60>] = Specifies the time period to wait.

[queries <1-10>] = Specifies how many tries the switch performs the traceroute function.

This command displays information about the route to an Ethernet device. The following example displays route information to an Ethernet device with an IP address of 192.168.1.100.

Figure 134 traceroute Command Example

```
sysname> traceroute 192.168.1.100
traceroute to 192.168.1.100, 30 hops max, 40 byte packet
 1:192.168.1.100 (10 ms) (10 ms) (0 ms)
traceroute done:
```

33.5 Enabling RSTP

To enable RSTP on a port, enter `spanning-tree` followed by the port number. You also need to use “`spanning-tree`” to enable RSTP on the switch. The following example enables RSTP on port 3.

Figure 135 Enable RSTP Command Example

```
sysname(config)# spanning-tree 3
sysname(config)# spanning-tree
```

33.6 Configuration File Maintenance

This section shows you how to backup or restore the configuration file on the switch using TFTP.

33.6.1 Backing up Configuration

Syntax:

```
copy running-config tftp <ip> <remote-file>
```

where

<ip> = The IP address of a TFTP server on which you want to store the backup configuration file.

<remote-file> = Specifies the name of the configuration file.

This command backs up the current configuration file on a TFTP server. The following example backs up the current configuration to a file (`test.cfg`) on the TFTP server (172.23.19.96).

Figure 136 CLI: Backup Configuration Example

```
sysname# copy running-config tftp 172.23.19.96 test.cfg
Backuping
. (599)Bytes Done!
sysname#
```

33.6.2 Restoring Configuration

This command allows you to restore a configuration file to the currently running configuration on the switch.

Syntax:

```
copy tftp config <index> <ip> <remote-file>
```

where

- <index> = Note: At the time of writing, regardless of the value entered for this parameter (1 or 2), this command restores the configuration file to the currently running configuration on the switch.
- <ip> = The IP address of a TFTP server from which you want to get the backup configuration file.
- <remote-file> = Specified the name of the configuration file.

This command restores a configuration file on the switch. The following example uploads the configuration file (`test.cfg`) from the TFTP server (172.23.19.96) to the currently running configuration on the switch.

Figure 137 CLI: Restore Configuration Example

```
sysname# copy tftp config 1 172.23.19.96 test.cfg
Restoring
. (599)Bytes Done!
sysname#
```

33.6.3 Using a Different Configuration File

You can store up to two configuration files on the switch. Only one configuration file is used at a time. By default the switch uses the first configuration file (with an index number of 1). You can set the switch to use a different configuration file. There are two ways in which you can set the switch to use a different configuration file: restart the switch (cold reboot) and restart the system (warm reboot).

Use the `boot config` command to restart the switch and use a different configuration file (if specified). The following example reboots the switch to use the second configuration file.

Figure 138 boot config Command Example

```
sysname# boot config 2
```

Use the `reload config` command to restart the system and use a different configuration file (if specified). The following example restarts the system to use the second configuration file.

Figure 139 CLI: reload config Command Example

```
sysname# reload config 2
```



When you use the `write memory` command without specifying a configuration file index number, the switch saves the changes to the configuration file the switch is currently using.

33.6.4 Resetting to the Factory Default

Follow the steps below to reset the switch back to the factory defaults.

- 1 Enter “erase running config” to reset the current running configuration.
- 2 Enter “write memory” to save the changes to the current configuration file. If you want to reset the second configuration file, use the write memory command again with the specified index number.

The following example resets both configuration files to the factory default settings.

Figure 140 CLI: Reset to the Factory Default Example

```
sysname# erase running-config
sysname# write memory
sysname# write memory 2
```

33.7 Example no Commands

These are the commonly used command examples that belong to the “no” group of commands.

33.7.1 no mirror-port

Syntax:

```
no mirror-port
```

Disables port mirroring on the switch. An example is shown next.

Figure 141 no mirror-port Command Example

```
sysname(config)# no mirror-port
```

33.7.2 no trunk

Syntax:

```
no trunk <T1|T2|T3|T4|T5|T6>
no trunk <T1|T2|T3|T4|T5|T6> lacp
no trunk <T1|T2|T3|T4|T5|T6> interface <port-list>
```

where

<T1 T2 T3 T4 T5 T6>	Disables the trunk group.
<T1 T2 T3 T4 T5 T6> lacp	Disables LACP in the trunk group.
<T1 T2 T3 T4 T5 T6> interface <port-list>	Removes ports from the trunk group.

An example is shown next.

- Disable trunk one (T1).
- Disable LACP on trunk three (T3).
- Remove ports one, three, four and five from trunk five (T5).

Figure 142 no trunk Command Example

```
sysname(config)# no trunk T1
sysname(config)# no trunk T3 lacp
sysname(config)# no trunk T5 interface 1,3-5
```

33.7.3 no port-access-authenticator

Syntax:

```
no port-access-authenticator
no port-access-authenticator <port-list> reauthenticate
no port-access-authenticator <port-list>
```

where

	Disables port authentication on the switch.
<port-list> reauthenticate	Disables the re-authentication mechanism on the listed ports.
<port-list>	Disables authentication on the listed ports.

An example is shown next.

- Disable authentication on the switch.
- Disable re-authentication on ports one, three, four and five.
- Disable authentication on ports one, six and seven.

Figure 143 no port-access-authenticator Command Example

```
sysname(config)# no port-access-authenticator
sysname(config)# no port-access-authenticator 1,3-5 reauthenticate
sysname(config)# no port-access-authenticator 1,6-7
```

33.7.4 no ssh

Syntax:

```
no ssh key <rsa1|rsa|dsa>
no ssh known-hosts <host-ip> <cr>
no ssh known-hosts <host-ip> [1024|ssh-rsa|ssh-dsa]
```

where

key <rsa1 rsa dsa>	Disables the secure shell server encryption key. Your switch supports SSH versions 1 and 2 using RSA and DSA authentication.
known-hosts <host-ip>	Remove specific remote hosts from the list of all known hosts.
known-hosts <host-ip> [1024 ssh- rsa ssh-dsa]	Remove remote known hosts with a specified public key (1024-bit RSA1, RSA or DSA).

An example is shown next.

- Disable the secure shell RSA1 encryption key.
- Remove the remote host with IP address 172.165.1.8 from the list of known hosts.

- Remove the remote host with IP address 172.165.1.9 and with an SSH-RSA encryption key from the list of known hosts.

Figure 144 no ssh Command Example

```
sysname(config)# no ssh key rsa1
sysname(config)# no ssh known-hosts 172.165.1.8
sysname(config)# no ssh known-hosts 172.165.1.9 ssh-rsa
```

33.8 interface Commands

These are some commonly used commands that belong to the interface group of commands.

33.8.1 interface port-channel

Syntax:

```
interface port-channel
```

Each interface refers to an Ethernet port on the switch. Commands configured after the interface command correspond to those ports. Type multiple ports or port ranges separated by a comma. Ranges of port numbers are typed separated by a dash.

An example is shown next.

- Enter the configuration command set.
- Enable ports one, three, four and five for configuration.
- Begin configuring for those ports.

Figure 145 interface port-channel Command Example

```
sysname# config
sysname(config)# interface port-channel 1,3-5
sysname(config-interface)#
```

33.8.2 bpd-control

Syntax:

```
bpd-control <peer|tunnel|discard|network>
```

where

<peer tunnel d	Type peer to process any BPDUs received on these ports.
iscard network	Type tunnel to forward BPDUs received on these ports.
>=	Type discard to drop any BPDUs received on these ports.
	Type network to process a BPDU with no VLAN tag and forward a tagged BPDU.

An example is shown next.

- Enable ports one, three, four and five for configuration.
- Set the BPDU control to tunnel, to forward BPDUs received on ports one, three, four and five.

Figure 146 interface bpdu-control Command Example

```

sysname(config)# interface port-channel 1,3-5
sysname(config-interface)# bpdu-control tunnel
sysname(config-interface)#

```

33.8.3 broadcast-limit

Syntax:

```

broadcast-limit
broadcast-limit <pkt/s>

```

where

	Enables broadcast storm control limit on the switch.
<pkt/s>	Sets how many broadcast packets the interface receives per second.

An example is shown next.

- Enable port one for configuration.
- Enable broadcast control.
- Set the number of broadband packets the interface receives per second

Figure 147 broadcast-limit Command Example

```

sysname(config)# interface port-channel 1
sysname(config-interface)# broadcast-limit
sysname(config-interface)# broadcast-limit 21

```

33.8.4 bandwidth-limit

Syntax:

```

bandwidth-limit
bandwidth-limit pir <Kbps>
bandwidth-limit cir <Kbps>
bandwidth-limit egress <Kbps>

```

where

	Enables bandwidth control on the switch.
<Kbps>	Sets the maximum bandwidth allowed for outgoing traffic (egress) or incoming traffic (ingress) on the switch.

An example is shown next.

- Enable port one for configuration.
- Enable bandwidth control.
- Set the outgoing traffic bandwidth limit to 5000Kbps.
- Set the guaranteed bandwidth allowed for incoming traffic to 4000Kbps.
- Set the maximum bandwidth allowed for incoming traffic to 8000Kbps.

Figure 148 bandwidth-limit Command Example

```

sysname(config)# interface port-channel 1
sysname(config-interface)# bandwidth-limit
sysname(config-interface)# bandwidth-limit egress 5000
sysname(config-interface)# bandwidth-limit cir 4000
sysname(config-interface)# bandwidth-limit pir 8000

```

33.8.5 mirror

Syntax:

```

mirror
mirror dir <ingress|egress|both>

```

where

	Enables port mirroring on the interface.
<ingress egress both>	Enables port mirroring for incoming, outgoing or both incoming and outgoing traffic.

Port mirroring copies traffic from one or all ports to another or all ports for external analysis. An example is shown next.

- Enable port mirroring.
- Enable the monitor port three.
- Enable ports one, four, five and six for configuration.
- Enable port mirroring on the interface.
- Enable port mirroring for outgoing traffic. Traffic is copied from ports one, four, five and six to port three in order to examine it in more detail without interfering with the traffic flow on the original port(s).

Figure 149 mirror Command Example

```

sysname(config)# mirror-port
sysname(config)# mirror-port 3
sysname(config)# interface port-channel 1,4-6
sysname(config-interface)# mirror
sysname(config-interface)# mirror dir egress

```

33.8.6 gvrp

Syntax:

```

gvrp

```

GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way for switches to register necessary VLAN members on ports across the network. Enable this function to permit VLANs groups beyond the local switch.

An example is shown next.

- Enable the IEEE 802.1Q tagged VLAN command to configure tagged VLAN for the switch.
- Enable ports one, three, four and five for configuration.
- Enable GVRP on the interface.

Figure 150 gvrp Command Example

```
sysname(config)# vlan1q gvrp
sysname(config)# interface port-channel 1,3-5
sysname(config-interface)# gvrp
```

33.8.7 ingress-check

Syntax:

```
ingress-check
```

Enables the device to discard incoming frames for VLANs that are not included in a port member set.

An example is shown next.

- Enable ports one, three, four and five for configuration.
- Enable ingress checking on the interface.

Figure 151 ingress-check Command Example

```
sysname(config)# interface port-channel 1,3-5
sysname(config-interface)# ingress-check
```

33.8.8 vlan-trunking

Syntax:

```
vlan-trunking
```

Enable VLAN Trunking on ports connected to other switches or routers (but not ports directly connected to end users) to allow frames belonging to unknown VLAN groups to pass through the switch.

An example is shown next.

- Enable ports one, three, four and five for configuration.
- Enable VLAN Trunking on the interface.

Figure 152 vlan-trunking Command Example

```
sysname(config)# interface port-channel 1,3-5
sysname(config-interface)# vlan-trunking
```

33.8.9 weight

Syntax:

```
weight <wt1> <wt2> ... <wt8>
```

where

```
<wt1> <wt2> ... <wt8> Sets the interface WFQ weighting. A weight value of one to
eight is given to each variable from wt1 to wt8.
```

An example is shown next.

- Enable port two and ports six to eight for configuration.
- Set the queue weights from Q0 to Q7.

Figure 153 weight Command Example

```
sysname# configure
sysname(config)# interface port-channel 2,6-8
sysname(config-interface)# weight 8 7 6 5 4 3 2 1
```

33.8.10 egress set

Syntax:

```
egress set <port-list>
```

where

```
<port-list> Sets the outgoing traffic port list for a port-based VLAN.
```

An example is shown next.

- Enable port-based VLAN tagging on the switch.
- Enable ports one, three, four and five for configuration.
- Set the outgoing traffic ports as the CPU (0) six (6), seven (7) and eight (8).

Figure 154 egress set Command Example

```
sysname(config)# vlan-type port-based
sysname(config)# interface port-channel 1,3-5
sysname(config-interface)# egress set 0,6-8
```

33.8.11 qos priority

Syntax:

```
qos priority <0 .. 7>
```

where

```
<0 .. 7> Sets the quality of service priority for an interface(s).
```

An example is shown next.

- Enable ports one, three, four and five for configuration.
- Set the IEEE 802.1p quality of service priority as four (4).

Figure 155 qos priority Command Example

```
sysname(config)# interface port-channel 1,3-5
sysname(config-interface)# qos priority 4
```

33.8.12 name

Syntax:

```
name <port-name-string>
```

where

```
<port-name-    Sets a name for your port interface(s).
string>
```

An example is shown next.

- Enable ports one, three, four and five for configuration.
- Set a name for the interfaces.

Figure 156 name Command Example

```
sysname(config)# interface port-channel 1,3-5
sysname(config-interface)# name Test
```

33.8.13 speed-duplex

Syntax:

```
speed-duplex <auto|10-half|10-full|100-half|100-full|1000-full>
```

where

```
<auto|10-    Sets the duplex mode (half, full) and speed (10/100/1000
half|10-    Mbps) of the connection on the interface. Selecting auto
full|100-    (auto-negotiation) makes one port able to negotiate with a
half|100-    peer automatically to obtain the connection speed and
full|1000-    duplex mode that both ends support.
full>
```

An example is shown next.

- Enable ports one, three, four and five for configuration.
- Set the speed to 10 Mbps in half duplex mode.

Figure 157 speed-duplex Command Example

```
sysname(config)# interface port-channel 1,3-5
sysname(config-interface)# speed-duplex 10-half
```


IEEE 802.1Q Tagged VLAN Commands

This chapter describes the IEEE 802.1Q Tagged VLAN and associated commands.

34.1 IEEE 802.1Q Tagged VLAN Overview

See the *VLAN* chapter for more information on VLANs. There are two kinds of tagging:

- 1 Explicit Tagging
A VLAN identifier is added to the frame header that identifies the source VLAN.
- 2 Implicit Tagging
The MAC (Media Access Control) number, the port or other information is used to identify the source of a VLAN frame.

The IEEE 802.1Q Tagged VLAN uses both explicit and implicit tagging.

Whether to tag an outgoing frame depends on the setting of the egress port on a per-LAN, per-port basis (recall that a port can belong to multiple VLANs). If the tagging on the egress port is enabled for the VID of a frame, then the frame is transmitted as a tagged frame; otherwise, it is transmitted as an untagged frame.

34.2 VLAN Databases

A VLAN database stores and organizes VLAN registration information useful for switching frames to and from a switch. A VLAN database consists of a static entries (Static VLAN or SVLAN table) and dynamic entries (Dynamic VLAN or DVLAN table).

34.2.1 Static Entries (SVLAN Table)

Static entry registration information is added, modified and removed by administrators only.

34.2.2 Dynamic Entries (DVLAN Table)

Dynamic entries are learned by the switch and cannot be created or updated by administrators. The switch learns this information by observing what port, source address and VLAN ID (or VID) is associated with a frame. Entries are added and deleted using GARP VLAN Registration Protocol (GVRP), where GARP is the Generic Attribute Registration Protocol.

34.3 Configuring Tagged VLAN

The following procedure shows you how to configure tagged VLAN.

- 1 Use the IEEE 802.1Q tagged VLAN commands to configure tagged VLAN for the switch.
- 2 Use the `vlan <vlan-id>` command to configure or create a VLAN on the switch. The switch automatically enters the config-vlan mode.
- 3 Use the `exit` command when you are finished configuring the VLAN.
- 4 Use the `interface port-channel <port-list>` command to enter the config-interface mode to set the VLAN settings on a port, then use the `pvid <vlan-id>` command to set the VLAN ID you created for the port-list to that specific port in the PVID table.
- 5 Use the `inactive` command to deactivate the VLAN(s).

Example:

Figure 158 Tagged VLAN Configuration and Activation Example

```
sysname(config)# vlan 2000
sysname(config-vlan)# name upl
sysname(config-vlan)# fixed 5-7
sysname(config-vlan)# no untagged 5-7
sysname(config-vlan)# exit
sysname(config)# interface port-channel 5-7
sysname(config-interface)# pvid 2000
sysname(config-interface)# exit
sysname(config)#
```

- 6 Configure your management VLAN.
 - Use the `vlan <vlan-id>` command to create a VLAN (VID 3 in this example) for managing the switch, and the switch will activate the new management VLAN.
 - Use the `inactive` command to disable the new management VLAN.

Example:

Figure 159 CPU VLAN Configuration and Activation Example

```
sysname(config)# vlan 3
sysname(config-vlan)# inactive
sysname(config-vlan)#
```

34.4 Global VLAN1Q Tagged VLAN Configuration Commands

This section shows you how to configure and monitor the IEEE 802.1Q Tagged VLAN.

34.4.1 GARP Status

Syntax:

```
show garp
```

This command shows the switch's GARP timer settings, including the join, leave and leave all timers.

An example is shown next.

Figure 160 garp status Command Example

```
sysname# show garp
GARP Timer
-----
Join Timer      :200
Leave Timer      :600
Leave All Timer  :10000
sysname#
```

34.4.2 GARP Timer

Syntax:

```
garp join <msec> leave <msec> leaveall <msec>
```

where

<pre>join <msec> =</pre>	<p>This sets the duration of the Join Period timer for GVRP in milliseconds. Each port has a Join Period timer. The allowed Join Time range is between 100 and 32767 milliseconds; the default is 200 milliseconds.</p>
<pre>leave <msec> =</pre>	<p>This sets the duration of the Leave Period timer for GVRP in milliseconds. Each port has a single Leave Period timer. Leave Time must be two times larger than Join Timer; the default is 600 milliseconds.</p>
<pre>leaveall <msec> =</pre>	<p>This sets the duration of the Leave All Period timer for GVRP in milliseconds. Each port has a single Leave All Period timer. Leave All Timer must be larger than Leave Timer; the default is 10000 milliseconds.</p>

This command sets the switch's GARP timer settings, including the join, leave and leave all timers.

Switches join VLANs by making a declaration. A declaration is made by issuing a Join message using GARP. Declarations are withdrawn by issuing a Leave message. A Leave All message terminates all registrations. GARP timers set declaration timeout values.

The following example sets the Join Timer to 300 milliseconds, the Leave Timer to 800 milliseconds and the Leave All Timer to 11000 milliseconds.

```
sysname(config)# garp join 300 leave 800 leaveall 11000
```

34.4.3 Show GVRP

Syntax:

```
show vlan1q gvrp
```

This command shows the switch's GVRP settings.

An example is shown next.

Figure 161 show gvrp Command Example

```
sysname# show vlan1q gvrp
GVRP Support
-----
gvrpEnable = YES
```

34.4.4 Enable GVRP

Syntax:

```
vlan1q gvrp
```

This command turns on GVRP in order to propagate VLAN information beyond the switch.

34.4.5 Disable GVRP

Syntax:

```
no vlan1q gvrp
```

This command turns off GVRP so that the switch does not propagate VLAN information to other switches.

34.5 Port VLAN Commands

You must configure the switch port VLAN settings in config-interface mode.

34.5.1 Set Port VID

Syntax:

```
pvid <VID>
```

where

<VID> = Specifies the VLAN number between 1 and 4094

This command sets the default VLAN ID on the port(s).

The following example sets the default VID to 200 on ports 1 to 5.

Figure 162 port default vid Command Example

```

sysname(config)# interface port-channel 1-5
sysname(config-interface)# pvid 200

```

34.5.2 Set Acceptable Frame Type

Syntax:

```
frame-type <all|tagged>
```

where

<all|tagged> = Specifies all Ethernet frames (tagged and untagged) or only tagged Ethernet frames.

This command sets the specified port to accept all Ethernet frames or only those with an IEEE 802.1Q VLAN tag.

The following example sets ports 1 to 5 to accept only tagged frames.

Figure 163 frame type Command Example

```

sysname(config)# interface port-channel 1-5
sysname(config-interface)# frame-type tagged

```

34.5.3 Enable or Disable Port GVRP

Use the `gvrp` command to enable GVRP on the port(s). Use the `no gvrp` command to disable GVRP.

The following example turns off GVRP for ports 1 to 5.

Figure 164 no gvrp Command Example

```

sysname(config)# interface port-channel 1-5
sysname(config-interface)# no gvrp

```

34.5.4 Modify Static VLAN

Use the following commands in the `config-vlan` mode to configure the static VLAN table.

Syntax:

```
vlan <vlan-id>
fixed <port-list>
forbidden <port-list>
name <name-str>
normal <port-list>
untagged <port-list>
no fixed <port-list>
no forbidden <port-list>
no untagged <port-list>
```

where

<vlan-id> = The VLAN ID [1 – 4094].
 <name-str> = A name to identify the SVLAN entry.
 <port-list> = This is the switch port list.

- Enter `fixed` to register the <port-list> to the static VLAN table with <vlan-id>.
- Enter `normal` to confirm registration of the <port-list> to the static VLAN table with <vlan-id>.
- Enter `forbidden` to block a <port-list> from joining the static VLAN table with <vlan-id>.
- Enter `no fixed` or `no forbidden` to change <port-list> to normal status.
- Enter `untagged` to send outgoing frames without a tag.
- Enter `no untagged` to tag outgoing frames.

34.5.4.1 Modify a Static VLAN Table Example

The following example configures ports 1 to 5 as fixed and untagged ports in VLAN 2000.

Figure 165 Modifying Static VLAN Example

```
sysname(config)# vlan 2000
sysname(config-vlan)# fixed 1-5
sysname(config-vlan)# untagged 1-5
```

34.5.4.2 Forwarding Process Example**Tagged Frames**

- 1 First the switch checks the VLAN ID (VID) of tagged frames or assigns temporary VIDs to untagged frames.
- 2 The switch then checks the VID in a frame's tag against the SVLAN table.
- 3 The switch notes what the SVLAN table says (that is, the SVLAN tells the switch whether or not to forward a frame and if the forwarded frames should have tags).
- 4 Then the switch applies the port filter to finish the forwarding decision. This means that frames may be dropped even if the SVLAN says to forward them. Frames might also be dropped if they are sent to a CPE (customer premises equipment) DSL device that does not accept tagged frames.

Untagged Frames

- 1 An untagged frame comes in from the LAN.
- 2 The switch checks the PVID table and assigns a temporary VID of 1.
- 3 The switch ignores the port from which the frame came, because the switch does not send a frame to the port from which it came. The switch also does not forward frames to “forbidden” ports.
- 4 If after looking at the SVLAN, the switch does not have any ports to which it will send the frame, it won’t check the port filter.

34.5.5 Delete VLAN ID

Syntax:

```
no vlan <vlan-id>
```

where

`<vlan-id>` The VLAN ID [1 – 4094].
=

This command deletes the specified VLAN ID entry from the static VLAN table. The following example deletes entry 2 in the static VLAN table.

Figure 166 no vlan Command Example

```
sysname(config)# no vlan 2
```

34.6 Enable VLAN

Syntax:

```
vlan <vlan-id>
```

This command enables the specified VLAN ID in the SVLAN (Static VLAN) table.

34.7 Disable VLAN

Syntax:

```
vlan <vlan-id> inactive
```

This command disables the specified VLAN ID in the SVLAN (Static VLAN) table.

34.8 Show VLAN Setting

Syntax:

```
show vlan
```

This command shows the IEEE 802.1Q Tagged SVLAN (Static VLAN) table.

An example is shown next.

For the AdCtl section of the last column, “-“ is a port set to normal, “x” is a forbidden port and “F” is a fixed port.

For the TagCtl section of the last column, “T“ is a tagged port, “U” is an untagged port.

Figure 167 show vlan Command Example

```

sysname# show vlan

802.1Q VLAN Static Entry:
idx. Name          VID  Active  AdCtl / TagCtl
-----
 0          1    1  active  FFFFFFFFFFFFFFFFFFFFFFFFFF
          UUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUU
 1          up1 2000  active  -----F-----
          TTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTT
 2          up1 2001  active  -----F----
          TTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTT
 3          example 3    active  -----F-----
          TTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTT

sysname#

```


Troubleshooting

This chapter covers potential problems and possible remedies.



Problems Starting Up the Switch

Table 87 Troubleshooting the Start-Up of Your Switch

PROBLEM	CORRECTIVE ACTION
None of the LEDs turn on when you turn on the switch.	Check the power connection and make sure the power source is turned on. If the error persists, you may have a hardware problem. In this case, you should contact your vendor.



Problems Accessing the Switch

Table 88 Troubleshooting Accessing the Switch

PROBLEM	CORRECTIVE ACTION
I cannot access the switch using Telnet.	Make sure the ports are properly connected. You may have exceeded the maximum number of concurrent Telnet sessions. Close other Telnet session(s) or try connecting again later. Check that you have enabled Telnet service access. If you have configured a secured client IP address, your computer's IP address must match it. Refer to the chapter on access control for details.
I cannot access the web configurator.	The administrator username is "admin". The default administrator password is "1234". The username and password are case-sensitive. Make sure that you enter the correct password and username using the proper casing. If you have changed the password and have now forgotten it, you will need to upload the default configuration file. This restores all of the factory defaults including the password. Check that you have enabled web service access. If you have configured a secured client IP address, your computer's IP address must match it. Refer to the chapter on access control for details. Your computer's and the switch's IP addresses must be on the same subnet. See the following section to check that pop-up windows, JavaScripts and Java permissions are allowed.



Problems with the Password

Table 89 Troubleshooting the Password

PROBLEM	CORRECTIVE ACTION
Cannot access the switch.	The password field is case sensitive. Make sure that you enter the correct password using the proper casing. The administrator username is "admin". The default administrator password is "1234". The username and password are case-sensitive. Make sure that you enter the correct password and username using the proper casing. If you have changed the password and have now forgotten it, you will need to upload the default configuration file. This restores all of the factory defaults including the password.

PART VI

Appendices and Index

Product Specifications (269)
Browser Setup (273)
IP Addresses and Subnetting (279)
Legal Information (287)
Customer Support (291)
Index (295)

Product Specifications

These are the GS-3012 and GS-3012F product specifications.

Table 90 General Product Specifications

Standards	IEEE802.3 10BASE-T Ethernet (twisted-pair copper) IEEE802.3u 100BASE-TX Fast Ethernet (twisted-pair copper) ANSI/IEEE802.3 Auto-negotiation IEEE802.3x Flow Control IEEE802.1p Priority Queues IEEE802.1q VLAN IEEE802.1d Spanning Tree IEEE 802.1x Authentication IEEE 802.3 ad Link Aggregation IEEE 802.1w Rapid reconfiguration
Protocol	CSMA/CD
Interface GS-3012	GS-3012: 12 10/100/1000BASE-T Gigabit ports (with four paired Gigabit/mini-GBIC ports) Four mini-GBIC slots for uplinking One console port One RJ-45 management port
Interface GS-3012F	GS-3012F: 12 mini-GBIC slots for uplinking (with four paired Gigabit/mini-GBIC ports) Four 100/1000BASE-T Gigabit ports One console port One RJ-45 management port
Data Transfer Rate	Ethernet (GS-3012): 10Mbps (half duplex), 20Mbps (full duplex) Fast Ethernet: 100Mbps (half duplex), 200Mbps(full duplex) Gigabit: 1000Mbps (half duplex), 2000Mbps (full duplex) Uplink rates depend on the uplink module used (see your module manual).
Network Cables	10BASE-T: 2-pair Unshielded Twisted Pair (UTP) Cat.3, 4, 5 (100 meters) EIA/TIA-586 100-ohm Shielded Twisted Pair (STP) (100 meters) 100BASE-TX, 1000BASE-T: UTP Cat.5 (100 m max.) EIA/TIA-568 100-ohm STP (100 m max.) Uplink cables depend on the uplink module used (see your module manual).
Full/Half Duplex	Full/half duplex for 100 Mbps speeds Full duplex 1000 Mbps speed
Media Interface Exchange	All ports are auto-crossover (auto-MDI-X) and auto-negotiating.

Table 91 Performance and Management Specifications

Back plane	12.8 Gbps
Packet Forwarding Rate	148800 PPS for 100BASE-TX 1488000PPS for 1000Base-X Uplink packet forwarding rate depends on the uplink module used (see your module manual)
Switching Method	Store-and-forward
MAC Address Table	16 K entries
Data Buffer	1MB (excluding optional modules) Uplink data buffers depend on the uplink module used (see your module manual)
VLAN	Port-based VLAN setting Tag-based (IEEE 802.1Q) VLAN Number of VLAN: 4K, 1000 static maximum Supports GVRP
IEEE 802.1p Priority Queues	Eight CoS queues
Port Link Aggregation	Static port trunking IEEE802.3ad dynamic port trunking
Port Security	Static MAC address filtering MAC address learning limit
Multicasting	Support IGMP snooping
Broadcast Storm	Support broadcast storm control
Port Mirroring	All Gigabit and uplink ports support port mirroring
Management	Web-based management Console Telnet SNMP Syslog
Management Security	User ID/Password for console, Telnet and Web-based management authentication Up to four administrators allowed
MIBs	SNMP MIB II (RFC 1213) RFC 1157 SNMP v1 SNMPv2 or SNMPv2c RFC 1643 Ethernet MIBs RFC 1493 Bridge MIBs RFC 1155 SMI RFC 1757 RMON Bridge extension MIBs RFC 2674 RFC 2863 Interface MIB RFC 2925 Ping and Trace Route

Table 92 Physical and Environmental Specifications

Weight	GS-3012 Main switch: 4 Kg GS-3012F Main switch: 3.1 Kg
LED	Main switch: PWR, SYS, ALM Per Port: LNK/ACT, FDX (GS-3012) Per Port: 1000, 100 (GS-3012F) Per GBIC Slot: LNK, ACT Per Management Port: 10, 100
Dimensions	Main switch: GS-3012: 438(W) x 300(D) x 45(H) mm GS-3012F: 438(W) x 225(D) x 45(H) mm 19-inch rack-mount width, 1 U height
Power Supply (AC Unit)	100 - 240VAC 50/60Hz 1.5A maximum internal universal power supply
Power Supply (DC Unit)	DC input of -48VDC — -60VDC 1.5A maximum for the GS-3012 1.25A maximum for the GS-3012F
Power Consumption	GS-3012 AC unit: 50W maximum GS-3012 DC unit: 48W maximum GS-3012F AC unit: 36W maximum GS-3012F DC unit: 38W maximum
Wire Gauge Specifications	Ground Wire: 18 AWG or larger Power Wire: 18 AWG or larger
Operating Temperature	0° C ~45° C
Storage Temperature	-25° C ~70° C
Operational Humidity	10% to 90% (Non-condensing)
Safety	UL 60950-1 CSA 60950-1 EN60950-1 IEC60950-1
EMC	FCC Part15 (Class A) CE EMC (Class A)

Table 93 Firmware Features

FEATURE	DESCRIPTION
VLAN	A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.
MAC Address Filter	Filter traffic based on the source and/or destination MAC address and VLAN group (ID).
IGMP Snooping	The switch supports IGMP snooping enabling group multicast traffic to be only forwarded to ports that are members of that group; thus allowing you to significantly reduce multicast traffic passing through your switch.

Table 93 Firmware Features

FEATURE	DESCRIPTION
Classifier and Policy	You can create a policy to define actions to be performed on a traffic flow grouped by a classifier according to specific criteria such as the IP address, port number or protocol type, etc.
Queuing	Queuing is used to help solve performance degradation when there is network congestion. Three scheduling services are supported: Strict Priority Queuing (SPQ) and Weighted Round Robin (WRR). This allows the switch to maintain separate queues for packets from each individual source or flow and prevent a source from monopolizing the bandwidth.
Port Mirroring	Port mirroring allows you to copy traffic going from one or all ports to another or all ports in order that you can examine the traffic from the mirror port (the port you copy the traffic to) without interference.
Static Route	Static routes tell the switch how to forward IP traffic when you configure the TCP/IP parameters manually.
Multicast VLAN Registration (MVR)	Multicast VLAN Registration (MVR) is designed for applications (such as Media-on-Demand (MoD)) using multicast traffic across a network. MVR allows one single multicast VLAN to be shared among different subscriber VLANs on the network. This improves bandwidth utilization by reducing multicast traffic in the subscriber VLANs and simplifies multicast group management.
RSTP (Rapid Spanning Tree Protocol) / MRSTP (Multiple RSTP)	RSTP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a switch to interact with other RSTP -compliant switches in your network to ensure that only one path exists between any two stations on the network. MRSTP allows you to configure multiple RSTP configurations and assign ports to each tree.
Link Aggregation	Link aggregation (trunking) is the grouping of physical ports into one logical higher-capacity link. You may want to trunk ports if for example, it is cheaper to use multiple lower-speed links than to under-utilize a high-speed, but more costly, single-port link.
Port Authentication and Security	For security, the switch allows authentication using IEEE 802.1x with an external RADIUS server and port security that allows only packets with dynamically learned MAC addresses and/or configured static MAC addresses to pass through a port on the switch. For redundancy, multiple RADIUS servers can be configured.
Device Management	Use the web configurator to easily configure the rich range of features on the switch.
Firmware Upgrade	Download new firmware (when available) from the ZyXEL web site and use the web configurator, CLI or an FTP/TFTP tool to put it on the switch. Note: Only upload firmware for your specific model!
Configuration Backup & Restoration	Make a copy of the switch's configuration and put it back on the switch later if you decide you want to revert back to an earlier configuration.
Cluster Management	Cluster management (also known as iStacking) allows you to manage switches through one switch, called the cluster manager. The switches must be directly connected and be in the same VLAN group so as to be able to communicate with one another.
Configure Clone	The switch allows you to copy multiple attributes of one port and apply them to other ports on the switch.

Browser Setup

This appendix helps you configure your browser for working with the web configurator.

Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).



Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

Internet Explorer Pop-up Blockers

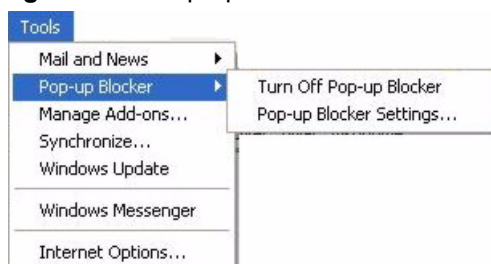
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

Disable pop-up Blockers

- 1 In Internet Explorer, select **Tools, Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

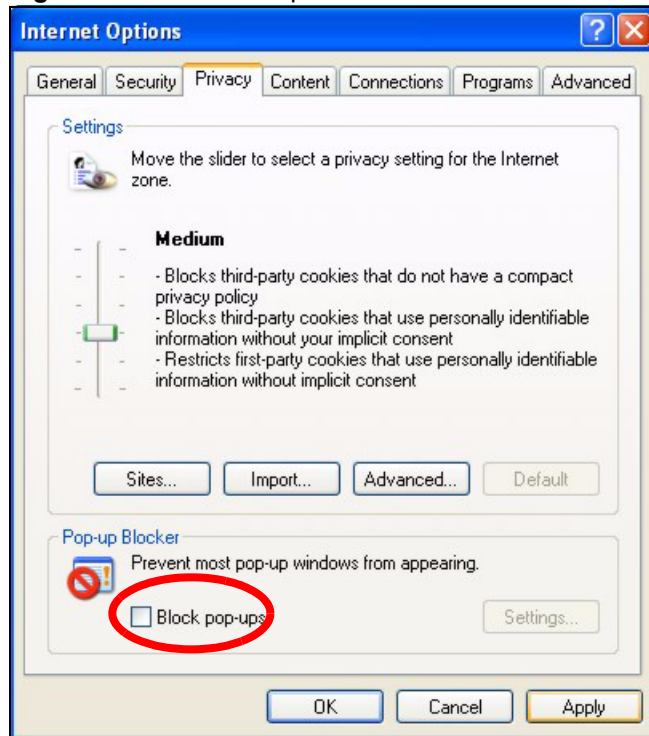
Figure 168 Pop-up Blocker



You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

- 1 In Internet Explorer, select **Tools, Internet Options, Privacy**.
- 2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 169 Internet Options



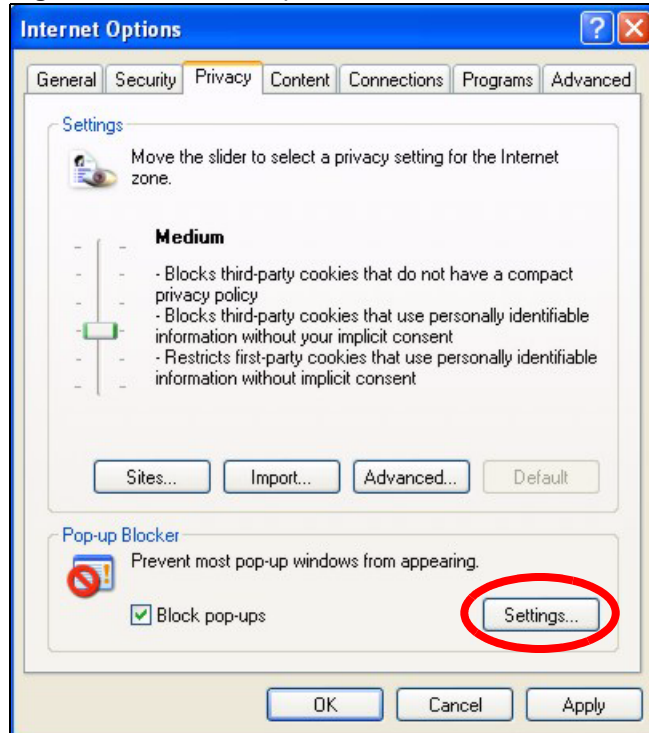
- 3 Click **Apply** to save this setting.

Enable pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

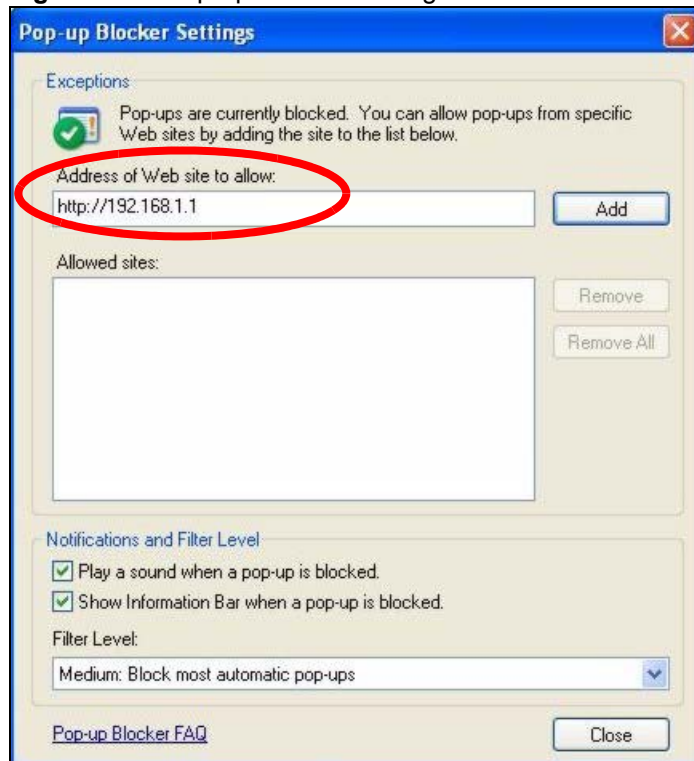
- 1 In Internet Explorer, select **Tools, Internet Options** and then the **Privacy** tab.
- 2 Select **Settings...** to open the **Pop-up Blocker Settings** screen.

Figure 170 Internet Options



- 3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.1.1.
- 4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 171 Pop-up Blocker Settings



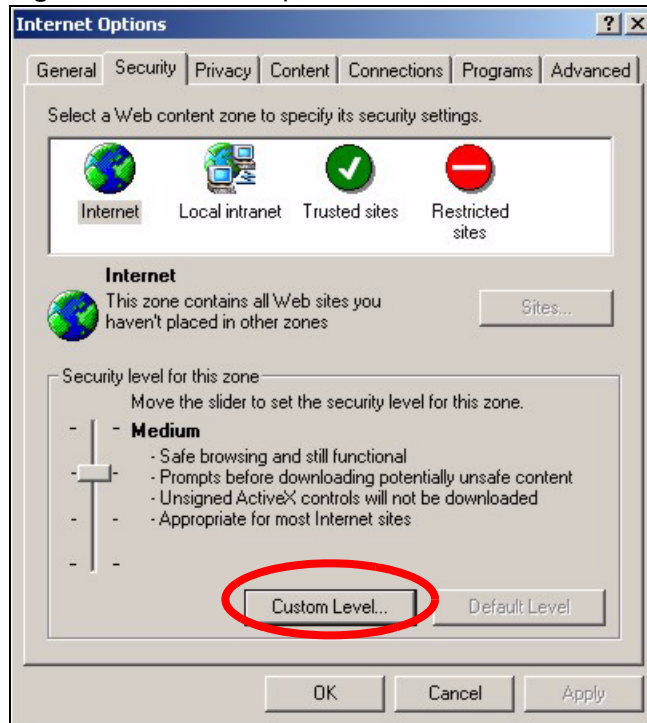
- 5 Click **Close** to return to the **Privacy** screen.
- 6 Click **Apply** to save this setting.

JavaScripts

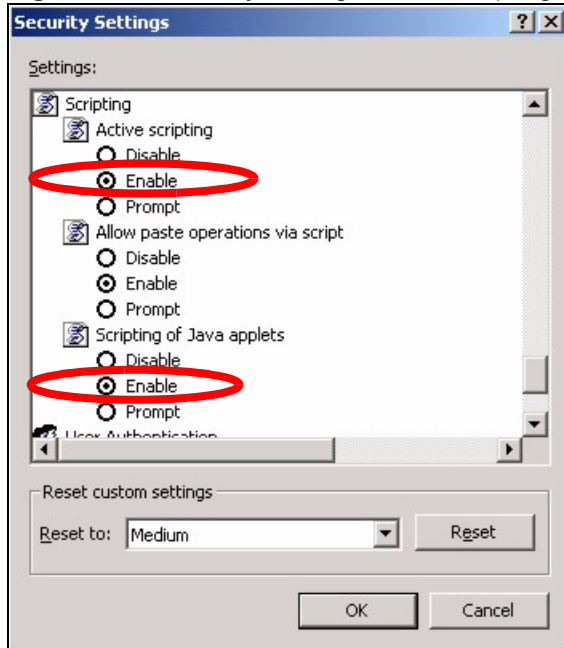
If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

- 1 In Internet Explorer, click **Tools, Internet Options** and then the **Security** tab.

Figure 172 Internet Options

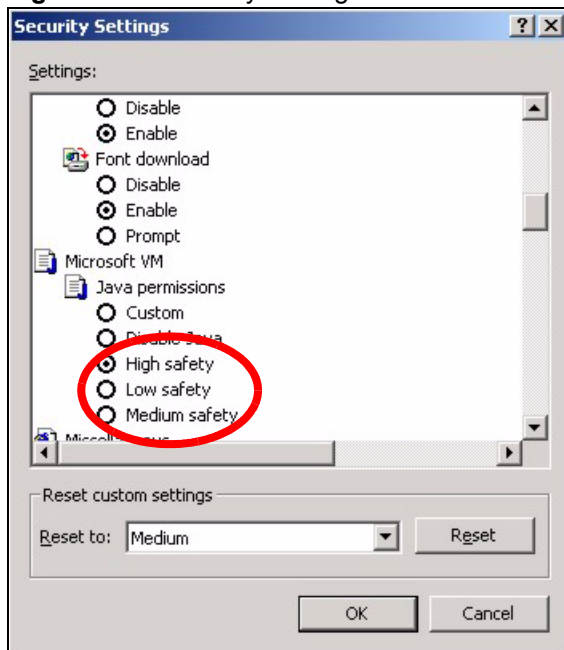


- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Scripting**.
- 4 Under **Active scripting** make sure that **Enable** is selected (the default).
- 5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).
- 6 Click **OK** to close the window.

Figure 173 Security Settings - Java Scripting

Java Permissions

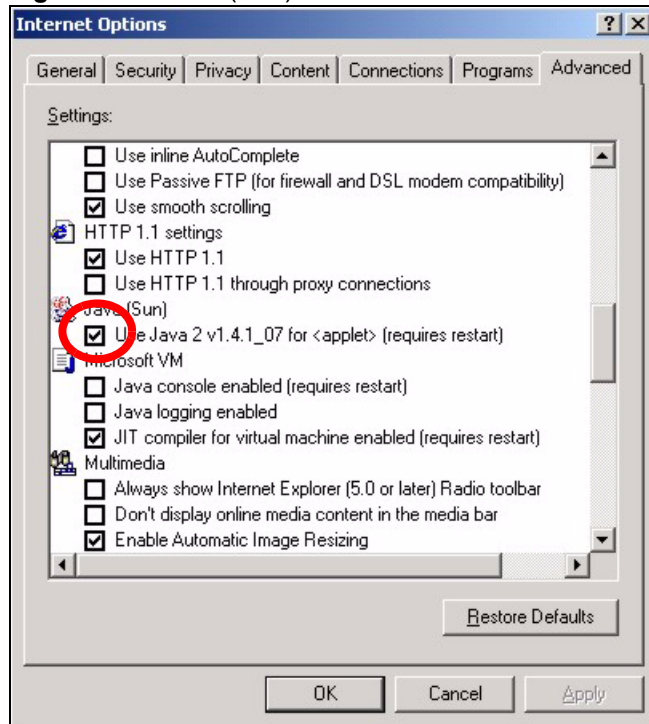
- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Security** tab.
- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Microsoft VM**.
- 4 Under **Java permissions** make sure that a safety level is selected.
- 5 Click **OK** to close the window.

Figure 174 Security Settings - Java

JAVA (Sun)

- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Advanced** tab.
- 2 make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.
- 3 Click **OK** to close the window.

Figure 175 Java (Sun)



IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

Introduction to IP Addresses

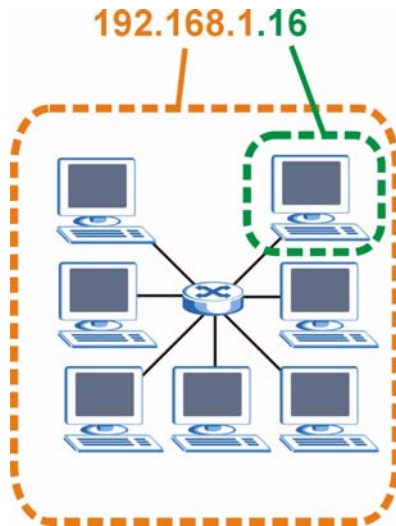
One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

Figure 176 Network Number and Host ID

How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term “subnet” is short for “sub-network”.

A subnet mask has 32 bits. If a bit in the subnet mask is a “1” then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is “0” then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

Table 94 Subnet Mask Example

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	11111111	11111111	11111111	00000000
Network Number	11000000	10101000	00000001	
Host ID				00000010

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a “1” value). For example, an “8-bit mask” means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

Table 95 Subnet Masks

	BINARY				DECIMAL
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.0
16-bit mask	11111111	11111111	00000000	00000000	255.255.0.0
24-bit mask	11111111	11111111	11111111	00000000	255.255.255.0
29-bit mask	11111111	11111111	11111111	11111000	255.255.255.248

Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

Table 96 Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} - 2$	16777214
16 bits	255.255.0.0	16 bits	$2^{16} - 2$	65534
24 bits	255.255.255.0	8 bits	$2^8 - 2$	254
29 bits	255.255.255.248	3 bits	$2^3 - 2$	6

Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a “/” followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

Table 97 Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128

Table 97 Alternative Subnet Mask Notation (continued)

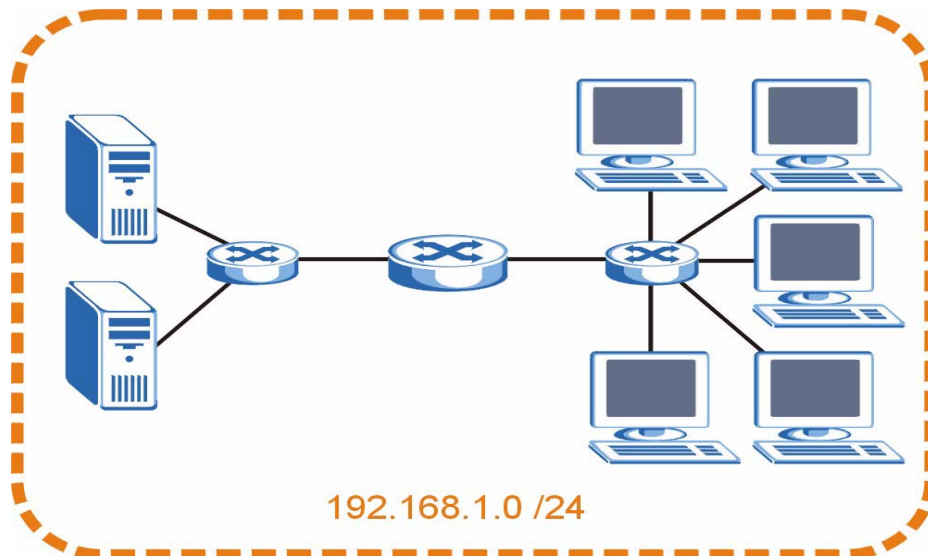
SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of $2^8 - 2$ or 254 possible hosts.

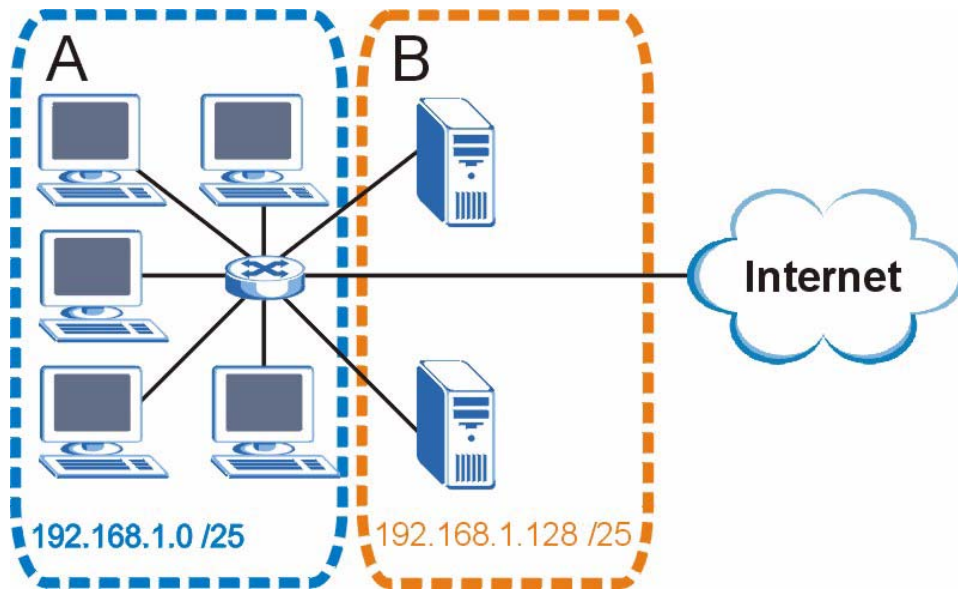
The following figure shows the company network before subnetting.

Figure 177 Subnetting Example: Before Subnetting

You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The “borrowed” host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

Figure 178 Subnetting Example: After Subnetting

In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of $2^7 - 2$ or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to “borrow” two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.11000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving $2^6 - 2$ or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

Table 98 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 99 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	01000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 100 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	10000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 101 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	11000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

Table 102 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127

Table 102 Eight Subnets (continued)

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

Table 103 24-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

The following table is a summary for subnet planning on a network with a 16-bit network number.

Table 104 16-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6

Table 104 16-bit Network Number Subnet Planning (continued)

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Configuring IP Addresses

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the switch.

Once you have decided on the network number, pick an IP address for your switch that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your switch will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the switch unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, *Address Allocation for Private Internets* and RFC 1466, *Guidelines for Management of IP Address Space*.

Legal Information

Copyright

Copyright © 2006 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

FCC Warning

This device has been tested and found to comply with the limits for a Class A digital switch, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This device generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this device in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE Mark Warning:

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Taiwanese BSMI (Bureau of Standards, Metrology and Inspection) A Warning:

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

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

CLASS 1 LASER PRODUCT

APPAREIL A LASER DE CLASS 1

PRODUCT COMPLIES WITH 21 CFR 1040.10 AND 1040.11.

PRODUIT CONFORME SELON 21 CFR 1040.10 ET 1040.11.

Viewing Certifications

- 1 Go to <http://www.zyxel.com>.
- 2 Select your product on the ZyXEL home page to go to that product's page.
- 3 Select the certification you wish to view from this page.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating

condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Customer Support

Please have the following information ready when you contact customer support.

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Corporate Headquarters (Worldwide)

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-3-578-3942
- Fax: +886-3-578-2439
- Web Site: www.zyxel.com, www.europe.zyxel.com
- FTP Site: [ftp.zyxel.com](ftp://ftp.zyxel.com), [ftp.europe.zyxel.com](ftp://ftp.europe.zyxel.com)
- Regular Mail: ZyXEL Communications Corp., 6 Innovation Road II, Science Park, Hsinchu 300, Taiwan

Costa Rica

- Support E-mail: soporte@zyxel.co.cr
- Sales E-mail: sales@zyxel.co.cr
- Telephone: +506-2017878
- Fax: +506-2015098
- Web Site: www.zyxel.co.cr
- FTP Site: [ftp.zyxel.co.cr](ftp://ftp.zyxel.co.cr)
- Regular Mail: ZyXEL Costa Rica, Plaza Roble Escazú, Etapa El Patio, Tercer Piso, San José, Costa Rica

Czech Republic

- E-mail: info@cz.zyxel.com
- Telephone: +420-241-091-350
- Fax: +420-241-091-359
- Web Site: www.zyxel.cz
- Regular Mail: ZyXEL Communications, Czech s.r.o., Modranská 621, 143 01 Praha 4 - Modrany, Česká Republika

Denmark

- Support E-mail: support@zyxel.dk
- Sales E-mail: sales@zyxel.dk
- Telephone: +45-39-55-07-00
- Fax: +45-39-55-07-07
- Web Site: www.zyxel.dk
- Regular Mail: ZyXEL Communications A/S, Columbusvej, 2860 Soeborg, Denmark

Finland

- Support E-mail: support@zyxel.fi
- Sales E-mail: sales@zyxel.fi
- Telephone: +358-9-4780-8411
- Fax: +358-9-4780 8448
- Web Site: www.zyxel.fi
- Regular Mail: ZyXEL Communications Oy, Malminkaari 10, 00700 Helsinki, Finland

France

- E-mail: info@zyxel.fr
- Telephone: +33-4-72-52-97-97
- Fax: +33-4-72-52-19-20
- Web Site: www.zyxel.fr
- Regular Mail: ZyXEL France, 1 rue des Vergers, Bat. 1 / C, 69760 Limonest, France

Germany

- Support E-mail: support@zyxel.de
- Sales E-mail: sales@zyxel.de
- Telephone: +49-2405-6909-0
- Fax: +49-2405-6909-99
- Web Site: www.zyxel.de
- Regular Mail: ZyXEL Deutschland GmbH., Adenauerstr. 20/A2 D-52146, Wuerselen, Germany

Hungary

- Support E-mail: support@zyxel.hu
- Sales E-mail: info@zyxel.hu
- Telephone: +36-1-3361649
- Fax: +36-1-3259100
- Web Site: www.zyxel.hu
- Regular Mail: ZyXEL Hungary, 48, Zoldlomb Str., H-1025, Budapest, Hungary

Kazakhstan

- Support: <http://zyxel.kz/support>
- Sales E-mail: sales@zyxel.kz

- Telephone: +7-3272-590-698
- Fax: +7-3272-590-689
- Web Site: www.zyxel.kz
- Regular Mail: ZyXEL Kazakhstan, 43, Dostyk ave., Office 414, Dostyk Business Centre, 050010, Almaty, Republic of Kazakhstan

North America

- Support E-mail: support@zyxel.com
- Sales E-mail: sales@zyxel.com
- Telephone: +1-800-255-4101, +1-714-632-0882
- Fax: +1-714-632-0858
- Web Site: www.us.zyxel.com
- FTP Site: <ftp.us.zyxel.com>
- Regular Mail: ZyXEL Communications Inc., 1130 N. Miller St., Anaheim, CA 92806-2001, U.S.A.

Norway

- Support E-mail: support@zyxel.no
- Sales E-mail: sales@zyxel.no
- Telephone: +47-22-80-61-80
- Fax: +47-22-80-61-81
- Web Site: www.zyxel.no
- Regular Mail: ZyXEL Communications A/S, Nils Hansens vei 13, 0667 Oslo, Norway

Poland

- E-mail: info@pl.zyxel.com
- Telephone: +48 (22) 333 8250
- Fax: +48 (22) 333 8251
- Web Site: www.pl.zyxel.com
- Regular Mail: ZyXEL Communications, ul. Okrzei 1A, 03-715 Warszawa, Poland

Russia

- Support: <http://zyxel.ru/support>
- Sales E-mail: sales@zyxel.ru
- Telephone: +7-095-542-89-29
- Fax: +7-095-542-89-25
- Web Site: www.zyxel.ru
- Regular Mail: ZyXEL Russia, Ostrovityanova 37a Str., Moscow, 117279, Russia

Spain

- Support E-mail: support@zyxel.es
- Sales E-mail: sales@zyxel.es
- Telephone: +34-902-195-420
- Fax: +34-913-005-345

- Web Site: www.zyxel.es
- Regular Mail: ZyXEL Communications, Arte, 21 5ª planta, 28033 Madrid, Spain

Sweden

- Support E-mail: support@zyxel.se
- Sales E-mail: sales@zyxel.se
- Telephone: +46-31-744-7700
- Fax: +46-31-744-7701
- Web Site: www.zyxel.se
- Regular Mail: ZyXEL Communications A/S, Sjöporten 4, 41764 Göteborg, Sweden

Ukraine

- Support E-mail: support@ua.zyxel.com
- Sales E-mail: sales@ua.zyxel.com
- Telephone: +380-44-247-69-78
- Fax: +380-44-494-49-32
- Web Site: www.ua.zyxel.com
- Regular Mail: ZyXEL Ukraine, 13, Pimonenko Str., Kiev, 04050, Ukraine

United Kingdom

- Support E-mail: support@zyxel.co.uk
- Sales E-mail: sales@zyxel.co.uk
- Telephone: +44-1344 303044, 08707 555779 (UK only)
- Fax: +44-1344 303034
- Web Site: www.zyxel.co.uk
- FTP Site: [ftp.zyxel.co.uk](ftp://ftp.zyxel.co.uk)
- Regular Mail: ZyXEL Communications UK, Ltd., 11 The Courtyard, Eastern Road, Bracknell, Berkshire, RG12 2XB, United Kingdom (UK)

“+” is the (prefix) number you dial to make an international telephone call.

Index

Numerics

802.1Q VLAN type [76](#)

A

acceptable frame type [90](#)
 access control [175](#)
 address learning [130](#)
 Address Resolution Protocol (ARP) [201](#)
 aging time [76](#)
 airflow [48](#)
 all connected [95](#)
 ALM LED [48](#)
 alternative subnet mask notation [281](#)
 ARP
 how it works [201](#)
 learned IP addresses [202](#)
 viewing entries [201](#)
 ARP (Address Resolution Protocol) [201](#)
 ARP table [201](#)
 auto-crossover [45](#)

B

back plane [270](#)
 backup configuration [169](#)
 Backup Power Supply (BPS) [47](#)
 bandwidth control setup [113](#)
 BPDUs (Bridge Protocol Data Units) [104](#)
 BPS LED [48](#)
 Bridge Protocol Data Units (BPDUs) [104](#)
 broadcast storm control [115](#)

C

Canonical Format Indicator (CFI) [85](#)
 certifications [287](#)
 notices [288](#)

 viewing [288](#)
 CFI (Canonical Format Indicator) [85](#)
 change login password [57](#)
 Class of Service (CoS) [139](#)
 classifier [133](#)
 Ethernet type [135](#)
 example [137](#)
 packet format [134](#)
 view summary [136](#)
 CLI [209](#)
 accessing [207](#)
 configure tagged VLAN example [258](#)
 examples [239](#), [247](#)
 forwarding process example [262](#)
 IEEE 802.1Q tagged VLAN commands example [257](#)
 introduction [207](#)
 privilege levels [211](#)
 static VLAN table example [262](#)
 summary tables [214](#)
 syntax conventions [209](#)
 CLI (Command Line Interface) [207](#)
 cloning [203](#)
 cloning a port, See also port cloning [204](#)
 cluster management [193](#)
 cluster member switch
 uploading firmware [195](#)
 web management [194](#)
 clustering management
 ZyXEL specifications [193](#)
 Command Line Interface, see also CLI [207](#)
 commands, see also CLI [207](#)
 configuration file
 saving [170](#)
 configure QoS [133](#)
 console port [44](#)
 contact information [291](#)
 contact person's name [74](#)
 copying port settings, See also port cloning [204](#)
 copyright [287](#)
 CPU management port [93](#)
 customer support [291](#)

D

data buffer [270](#)
Daytime (RFC 867) [74](#)
default Ethernet settings [45](#)
default IP address [47](#)
Destination Lookup Failure (DLF) [115](#)
DHCP [161](#)
diagnostics [187](#)
DiffServ (Differentiated Services) [139](#)
DiffServ Code Point (DSCP) [139](#)
DiffServ marking rule [139](#)
dimensions [271](#)
disclaimer [287](#)
DS (Differentiated Services) [139](#)
DS field [139](#)
DVLAN table [257](#)
dynamic link aggregation [119](#)

E

egress port [95](#)
error packet [68](#)
Ethernet address [72](#)
Ethernet port test [187](#)

F

FCC interference statement [287](#)
file transfer using FTP [171](#)
 command example [172](#)
 GUI-based [173](#)
 procedure [172](#)
 restrictions over WAN [173](#)
filename conventions [171](#)
filter setup [101](#)
filtering [101](#)
 view rules [102](#)
filtering database, See also MAC table [199](#)
firmware upgrade [168](#)
firmware version [72](#)
flow control [81](#)
front panel [43](#)
FTP [171](#)

G

GARP [257](#)
GARP (Generic Attribute Registration Protocol) [86](#)
garp status, command [259](#)
GARP timer [76](#)
general setup [71](#), [73](#), [74](#)
Generic Attribute Registration Protocol (GARP) [86](#)
Get Community command, SNMP [178](#)
GetNext command, SNMP [176](#)
Gigabit ports [44](#)
GS-3012 models [33](#)
GS-3012F models [33](#)
GVRP [90](#), [257](#)
GVRP (GARP VLAN Registration Protocol) [86](#), [90](#)
gvrp disable, command [260](#)
gvrp enable, command [260](#)
gvrp status, command [260](#)
GVRP, command [252](#)

H

hardware installation [39](#)
hardware monitor
 fans [72](#)
 temperature [72](#)
 temperature unit [72](#)
 voltage [73](#)
hardware overview [43](#)
help [59](#)
how SSH works [180](#)
HTTPS [181](#)
HTTPS example [182](#)

I

IANA [286](#)
IEEE 802.1p [76](#)
IEEE 802.1Q tagged VLAN [257](#)
IEEE 802.1x [123](#)
IGMP snooping [149](#)
ingress check [90](#)
ingress filtering [86](#)
inspecting traffic, via mirroring [117](#)
installation
 desktop [39](#)
 precautions [40](#)

- rack-mounting [40](#)
- transceivers [46](#)
- installation scenarios [39](#)
- Internet Assigned Numbers Authority, See also IANA [286](#)
- IP address [79](#)
- IP interface [77](#)
- IP Ports [137](#)
- IP setup [71](#), [77](#)
- IP subnet mask [79](#)
- iStacking [193](#)

J

- join timer [76](#)

L

- LACP
 - timeout [122](#)
- LACP status [120](#)
- leave all timer [76](#)
- leave timer [76](#)
- LEDs [48](#)
 - ALM [48](#)
 - BPS [48](#)
 - PWR [48](#)
 - SYS [48](#)
- Link Aggregate Control Protocol (LACP), [119](#)
- link aggregation [119](#)
- link aggregation ID [120](#)
- link aggregation setup [121](#)
- location [74](#)
- login accounts [178](#)

M

- MAC address [72](#)
- MAC address learning [76](#)
- MAC address table [270](#)
- MAC table [199](#)
- maintenance [167](#)
 - current configuration [167](#)
 - main screen [167](#)
- Management Information Base (MIB) [176](#)
- management port [47](#)

- default IP address [47](#)
- managing the device
 - good habits [37](#)
 - using FTP. See FTP. [36](#)
 - using Telnet. See command interface. [36](#)
 - using the command interface. See command interface. [36](#)
- MDIX (Media Dependent Interface Crossover) [45](#)
- Media Access Control (MAC) [72](#)
- media interface exchange [269](#)
- MGMT port [47](#)
- MIBs [270](#)
- mini GBIC slots [44](#)
- mini-GBIC slots [44](#)
- mirror, command [251](#)
- mirroring [117](#)
- model types [33](#)
- monitor port [117](#)
- mounting brackets [40](#)
- MTU (Multi-Tenant Unit) [75](#)
- Multiple Rapid Spanning Tree Protocol (MRSTP) [105](#)
- multiple STP [105](#)

N

- NAT (Network Address Translation) [286](#)
- network applications [33](#)
 - backbone [33](#)
 - bridging [34](#)
 - high performance switched workgroup [35](#)
 - IEEE802.1Q VLAN [35](#)
 - VLAN server [36](#)
 - VLAN workgroup [35](#)
- network cables [269](#)
- NTP (RFC-1305) [74](#)

O

- operating temperature [271](#)
- operational humidity [271](#)
- out of profile action [142](#)
- out-of-profile traffic [141](#)

P

- packet forwarding rate [270](#)

- password
 - default [53](#)
- PHB (Per-Hop Behavior) [139](#)
- ping [187](#)
- policy
 - actions [141](#)
 - example [143](#)
 - metering [141](#)
 - view summary [142](#)
- policy rules [139](#)
- port authentication
 - and VSA [124](#)
- port based VLAN type [76](#)
- port cloning [203](#), [204](#)
 - advanced settings [203](#), [204](#)
 - basic settings [203](#), [204](#)
- port details [66](#), [67](#)
- port isolation [95](#)
- port mirroring [117](#)
- port mirroring, CLI [234](#)
- port security [129](#)
- port setup [80](#)
- port statistics, See also port details [66](#)
- port status [65](#)
- port status, See also port details [66](#)
- port VID [86](#)
 - default for all ports [85](#), [235](#)
- port-based VLANs [93](#)
 - configure [94](#)
- power connector [47](#)
- power consumption [271](#)
- power supply [271](#)
- priority [76](#)
- priority level [76](#)
- priority queue assignment [76](#)
- privilege levels [211](#)
- product registration [289](#)
- product specifications [269](#)
- PVID [90](#)
- PWR LED [48](#)

Q

- Quality of Service (QoS) [133](#)
- queuing [145](#)
- queuing algorithms [145](#)

R

- rack-mounting [40](#)
- RADIUS (Remote Authentication Dial-In User Service) [123](#)
- Rapid Spanning Tree Protocol (RSTP). See STP [103](#)
- ras, firmware file extension [172](#)
- rear panel [47](#)
- rear panel connections [47](#)
- reauthentication [127](#)
- registration
 - product [289](#)
- related documentation [3](#)
- remote management [185](#)
- resetting the switch [58](#)
- restore configuration [169](#)
- Revolutions Per Minute (RPM) [72](#)
- RFC 3580 [124](#)
- Round Robin Scheduling [146](#)
- RSTP [103](#)
 - See also STP [103](#)
- rubber feet [39](#)
- runt [68](#)
- Rx KB/s [66](#), [68](#)
- Rx packet [68](#)
- RxPkts [66](#), [68](#)

S

- safety [271](#)
- safety warnings [6](#)
- save configuration [170](#)
- Secure Shell, See also SSH [181](#)
- server port, and service access control [185](#)
- service access control [184](#)
- Set Community command, SNMP [178](#)
- shared secret [125](#)
- Simple Network Management Protocol, See also SNMP [176](#)
- Small Form-factor Pluggable (SFP) [45](#)
- SNMP
 - configuring [177](#)
 - configuring traps [178](#)
 - Get command [176](#)
 - manager [176](#)
 - MIBs [177](#)
 - supported versions [176](#)
 - Trap command [177](#)
 - traps [177](#)

SNMP (Simple Network Management Protocol) **176**
 SNMP traps **177**
 source MAC address **102**
 Spanning Tree Protocol (STP) **103**
 speed/duplex **81**
 SSH (Secure Shell) **180**
 SSH implementation **181**
 standards **269**
 static MAC address **97**
 static MAC forward setup **97**
 static MAC forwarding **97**
 static route
 setup **165**
 static VLAN **90**
 control **91**
 tagging **91**
 status **65**
 STP **108, 111**
 STP **103**
 bridge ID **109, 112**
 bridge priority **107, 110**
 configuration **106, 109**
 designated bridge **104**
 forwarding delay **108, 111**
 Hello BPDU **104**
 Hello Time **107, 109, 110, 112**
 how it works **104**
 Max Age **108, 109, 110, 112**
 path cost **104, 108, 111**
 port priority **108, 111**
 port state **105**
 root port **104**
 status **108, 111**
 terminology **103**
 Strict Priority Queuing (SPQ) **145**
 subnet **279**
 subnet mask **280**
 subnetting **282**
 SVLAN table **257**
 switch lockout **57**
 switch setup **75, 87**
 switching method **270**
 synchronized ports **120**
 syntax conventions **4**
 SYS LED **48**
 sys log disp, command **241, 247**
 sys sw mac list, command **242**
 syslog **189**
 system information **65, 71**
 system log **187**
 system name **74**
 system priority **122**
 system statistics **65**

T

Tag Control Information (TCI) **85**
 Tag Protocol Identifier (TPID) **85**
 tagged VLAN **85**
 GARP **86**
 GVRP **86**
 membership registration **86**
 TCI (Tag Control Information) **85**
 TCP/UDP protocol port numbers **135**
 terminal emulation **44**
 Time (RFC-868) **74**
 time server protocol supported **74**
 TPID (Tag Protocol Identifier) **85**
 trademarks **287**
 transceiver MultiSource Agreement (MSA) **45**
 transceivers **45**
 installation **46**
 removal **46**
 traps, and SNMP **178**
 traps, SNMP **177**
 trunk group **119**
 trunking, See also link aggregation **119**
 trusted computers **185**
 tunnel protocol attribute **124**
 TX collision **68**
 Tx KB/s **66, 68**
 Tx packet **68**
 TxPkts **66, 68**

U

up time **66**
 username
 default **53**

V

Vendor Specific Attribute, See also VSA **123**
 ventilation **39**
 ventilation holes **40**
 VID **88, 89, 102**
 VID (VLAN Identifier) **85**
 VLAN **85**
 administrative control **86**
 explicit tagging **257**
 forwarding **85**

- ID (VID) [257](#)
- implicit tagging [257](#)
- introduction [75](#)
- port-based [93](#)
- priority frame [85](#)
- registration information [257](#)
- tag control [86](#)
- tagged VLAN [85](#)
- type [87](#)
- types of [76](#)
- VLAN (Virtual Local Area Network) [75](#)
- VLAN databases [257](#)
- VLAN group [91](#)
- VLAN ID [79](#), [85](#)
 - maximum number of [85](#)
- VLAN Identifier [85](#)
- VLAN port settings [89](#)
- VLAN status [88](#)
- VLAN type [87](#)
- vlan1q port accept, command [261](#)
- vlan1q port gvrp, command [261](#)
- vlan1q svlan delentry [263](#)
- VSA [123](#), [124](#)
 - and port authentication [124](#)
- VT100 [44](#)

W

- warranty [288](#)
 - note [289](#)
- web configurator
 - logging out [59](#)
 - login [53](#)
 - online help [59](#)
 - recommended browsers [53](#)
- Weighted Round Robin Scheduling [146](#)
- WRR (Weighted Round Robin Scheduling) [146](#)

X

- XMODEM upload [58](#)

Z

- ZyNOS (ZyXEL Network Operating System) [172](#)
- ZyNOS firmware version [72](#)