

GS-2024

Gigabit Ethernet switch

User's Guide

Version 3.60

Edition 2

8/2005

ZyXEL

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.

Interference Statements and Warnings

FCC Statement

This switch complies with Part 15 of the FCC rules. Operation is subject to the following two conditions:

- 1 This switch may not cause harmful interference.
- 2 This switch must accept any interference received, including interference that may cause undesired operations.

FCC Warning

This equipment 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 equipment 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 equipment 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。

Notice 1

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.

Certifications

- 1 Go to www.zyxel.com.
- 2 Select your product from the drop-down list box on the ZyXEL home page to go to that product's page.
- 3 Select the certification you wish to view from this page.



Safety Warnings

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

- To reduce the risk of fire, use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- 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 can service the device. Please contact your vendor for further information.
- Use ONLY the dedicated power supply for your device. Connect the power cord or power adaptor to the right supply voltage (110V AC in North America or 230V AC in Europe).
- Do NOT use the device if the power supply is damaged as it might cause electrocution.
- If the power supply is damaged, remove it from the power outlet.
- Do NOT attempt to repair the power supply. Contact your local vendor to order a new power supply.
- Place connecting cables carefully so that no one will step on them or stumble over them. Do NOT allow anything to rest on the power cord and do NOT locate the product where anyone can walk on the power cord.
- If you wall mount your device, make sure that no electrical, gas or water pipes will be damaged.
- Do NOT install nor use your device during a thunderstorm. There may be a remote risk of electric shock from lightning.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Make sure to connect the cables to the correct ports.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Do NOT store things on the device.
- Connect ONLY suitable accessories to the device.

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.

- 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.

METHOD	SUPPORT E-MAIL	TELEPHONE*	WEB SITE	REGULAR MAIL
LOCATION	SALES E-MAIL	FAX	FTP SITE	
CORPORATE HEADQUARTERS (WORLDWIDE)	support@zyxel.com.tw	+886-3-578-3942	www.zyxel.com www.europe.zyxel.com	ZyXEL Communications Corp. 6 Innovation Road II Science Park Hsinchu 300 Taiwan
	sales@zyxel.com.tw	+886-3-578-2439	ftp.zyxel.com ftp.europe.zyxel.com	
CZECH REPUBLIC	info@cz.zyxel.com	+420-241-091-350	www.zyxel.cz	ZyXEL Communications Czech s.r.o. Modranská 621 143 01 Praha 4 - Modrany Ceská Republika
	info@cz.zyxel.com	+420-241-091-359		
DENMARK	support@zyxel.dk	+45-39-55-07-00	www.zyxel.dk	ZyXEL Communications A/S Columbusvej 2860 Soeborg Denmark
	sales@zyxel.dk	+45-39-55-07-07		
FINLAND	support@zyxel.fi	+358-9-4780-8411	www.zyxel.fi	ZyXEL Communications Oy Malminkaari 10 00700 Helsinki Finland
	sales@zyxel.fi	+358-9-4780 8448		
FRANCE	info@zyxel.fr	+33-4-72-52-97-97	www.zyxel.fr	ZyXEL France 1 rue des Vergers Bat. 1 / C 69760 Limonest France
		+33-4-72-52-19-20		
GERMANY	support@zyxel.de	+49-2405-6909-0	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen Germany
	sales@zyxel.de	+49-2405-6909-99		
HUNGARY	support@zyxel.hu	+36-1-3361649	www.zyxel.hu	ZyXEL Hungary 48, Zoldlomb Str. H-1025, Budapest Hungary
	info@zyxel.hu	+36-1-3259100		
KAZAKHSTAN	http://zyxel.kz/support	+7-3272-590-698	www.zyxel.kz	ZyXEL Kazakhstan 43, Dostyk ave., Office 414 Dostyk Business Centre 050010, Almaty Republic of Kazakhstan
	sales@zyxel.kz	+7-3272-590-689		
NORTH AMERICA	support@zyxel.com	1-800-255-4101 +1-714-632-0882	www.us.zyxel.com	ZyXEL Communications Inc. 1130 N. Miller St. Anaheim CA 92806-2001 U.S.A.
	sales@zyxel.com	+1-714-632-0858	ftp.us.zyxel.com	
NORWAY	support@zyxel.no	+47-22-80-61-80	www.zyxel.no	ZyXEL Communications A/S Niils Hansens vei 13 0667 Oslo Norway
	sales@zyxel.no	+47-22-80-61-81		

METHOD	SUPPORT E-MAIL	TELEPHONE*	WEB SITE	REGULAR MAIL
LOCATION	SALES E-MAIL	FAX	FTP SITE	
POLAND	info@pl.zyxel.com	+48 (22) 333 8250	www.pl.zyxel.com	ZyXEL Communications ul. Okrzei 1A 03-715 Warszawa Poland
		+48 (22) 333 8251		
RUSSIA	http://zyxel.ru/support	+7-095-542-89-29	www.zyxel.ru	ZyXEL Russia Ostrovityanova 37a Str. Moscow, 117279 Russia
	sales@zyxel.ru	+7-095-542-89-25		
SPAIN	support@zyxel.es	+34-902-195-420	www.zyxel.es	ZyXEL Communications Arte, 21 5ª planta 28033 Madrid Spain
	sales@zyxel.es	+34-913-005-345		
SWEDEN	support@zyxel.se	+46-31-744-7700	www.zyxel.se	ZyXEL Communications A/S Sjöporten 4, 41764 Göteborg Sweden
	sales@zyxel.se	+46-31-744-7701		
UKRAINE	support@ua.zyxel.com	+380-44-247-69-78	www.ua.zyxel.com	ZyXEL Ukraine 13, Pimonenko Str. Kiev, 04050 Ukraine
	sales@ua.zyxel.com	+380-44-494-49-32		
UNITED KINGDOM	support@zyxel.co.uk	+44-1344 303044 08707 555779 (UK only)	www.zyxel.co.uk	ZyXEL Communications UK Ltd., 11 The Courtyard, Eastern Road, Bracknell, Berkshire, RG12 2XB, United Kingdom (UK)
	sales@zyxel.co.uk	+44-1344 303034	ftp.zyxel.co.uk	

* "+" is the (prefix) number you enter to make an international telephone call.

Table of Contents

Copyright	3
Interference Statements and Warnings	4
ZyXEL Limited Warranty	6
Customer Support.....	7
Preface	27
Chapter 1	
Getting to Know Your Switch	29
1.1 Introduction	29
1.2 Software Features	29
1.3 Hardware Features	31
1.4 Applications	32
1.4.1 Backbone Application	32
1.4.2 Bridging Example	32
1.4.3 High Performance Switched Example	33
1.4.4 IEEE 802.1Q VLAN Application Examples	33
1.4.4.1 Tag-based VLAN Example	34
1.4.4.2 VLAN Shared Server Example	34
Chapter 2	
Hardware Installation and Connection	37
2.1 Freestanding Installation	37
2.2 Mounting the Switch on a Rack	38
2.2.1 Rack-mounted Installation Requirements	38
2.2.1.1 Precautions	38
2.2.2 Attaching the Mounting Brackets to the Switch	38
2.2.3 Mounting the Switch on a Rack	38
Chapter 3	
Hardware Overview	41
3.1 Front Panel Connection	41
3.1.1 Console Port	41
3.1.2 Ethernet Ports	42

3.1.2.1 Default Ethernet Settings	42
3.1.3 Mini-GBIC Slots	42
3.1.3.1 Transceiver Installation	43
3.1.3.2 Transceiver Removal	43
3.2 Rear Panel	44
3.2.1 Power Connector	44
3.3 Front Panel LEDs	44
Chapter 4	
The Web Configurator.....	47
4.1 Introduction	47
4.2 System Login	47
4.3 The Status Screen	48
4.3.1 Change Your Password	51
4.4 Switch Lockout	52
4.5 Resetting the Switch	53
4.5.1 Reload the Configuration File	53
4.6 Logging Out of the Web Configurator	54
4.7 Help	54
Chapter 5	
Initial Setup Example	55
5.1 Overview	55
5.1.1 Creating a VLAN	55
5.1.2 Setting Port VID	56
5.1.3 Configuring Switch Management IP Address	57
Chapter 6	
System Status and Port Statistics	59
6.1 Overview	59
6.2 Port Status Summary	59
6.2.1 Status: Port Details	61
Chapter 7	
Basic Setting	65
7.1 Overview	65
7.2 System Information	65
7.3 General Setup	67
7.4 Introduction to VLANs	69
7.5 Switch Setup Screen	70
7.6 IP Setup	71
7.6.1 Management IP Addresses	71
7.7 Port Setup	74

Chapter 8	
VLAN	77
8.1 Introduction to IEEE 802.1Q Tagged VLAN	77
8.1.1 Forwarding Tagged and Untagged Frames	77
8.2 Automatic VLAN Registration	78
8.2.1 GARP	78
8.2.1.1 GARP Timers	78
8.2.2 GVRP	78
8.3 Port VLAN Trunking	79
8.4 Select the VLAN Type	79
8.5 Static VLAN	80
8.5.1 Static VLAN Status	80
8.5.2 Configure a Static VLAN	81
8.5.3 Configure VLAN Port Settings	83
8.6 Port-based VLAN Setup	85
8.6.1 Configure a Port-based VLAN	85
Chapter 9	
Static MAC Forwarding	89
9.1 Overview	89
9.2 Configuring Static MAC Forwarding	89
Chapter 10	
Spanning Tree Protocol	93
10.1.1 STP Terminology	93
10.1.2 How STP Works	94
10.1.3 STP Port States	94
10.2 STP Status	94
10.3 Configure STP	96
Chapter 11	
Bandwidth Control	99
11.1 Bandwidth Control Setup	99
Chapter 12	
Broadcast Storm Control	103
12.1 Overview	103
12.2 Broadcast Storm Control Setup	103
Chapter 13	
Mirroring	107
13.1 Overview	107
13.2 Port Mirroring Setup	107

Chapter 14	
Link Aggregation.....	109
14.1 Overview	109
14.2 Dynamic Link Aggregation	109
14.2.1 Link Aggregation ID	110
14.3 Link Aggregation Status	110
14.4 Link Aggregation Setup	111
Chapter 15	
Port Authentication.....	115
15.1 Overview	115
15.1.1 RADIUS	115
15.2 Port Authentication Configuration	115
15.2.1 Activate IEEE 802.1x Security	116
15.2.2 Configuring RADIUS Server Settings	118
Chapter 16	
Port Security.....	121
16.1 Overview	121
16.2 Port Security Setup	121
Chapter 17	
Queuing Method.....	123
17.1 Overview	123
17.1.1 Strict Priority Queuing (SPQ)	123
17.1.2 Weighted Round Robin Scheduling (WRR)	123
17.2 Configuring Queuing	124
Chapter 18	
Multicast.....	125
18.1 Overview	125
18.1.1 IP Multicast Addresses	125
18.1.2 IGMP Filtering	125
18.1.3 IGMP Snooping	125
18.2 Multicast Status	126
18.3 Multicast Setup	126
18.4 IGMP Filtering Profile	128
18.5 MVR Overview	130
18.5.1 Types of MVR Ports	130
18.5.2 MVR Modes	130
18.5.3 How MVR Works	131
18.6 General MVR Configuration	131
18.7 MVR Group Configuration	133

18.7.1 MVR Configuration Example	135
Chapter 19	
Static Route	139
19.1 Configuring	139
Chapter 20	
Differentiated Services	141
20.1 Overview	141
20.1.1 DSCP and Per-Hop Behavior	141
20.1.2 DiffServ Network Example	141
20.2 DSCP-to-IEEE802.1p Priority Mapping	142
20.3 Configuring DSCP Settings	142
Chapter 21	
Maintenance	145
21.1 The Maintenance Screen	145
21.2 Firmware Upgrade	145
21.3 Restore a Configuration File	146
21.4 Backing Up a Configuration File	146
21.5 Load Factory Defaults	147
21.6 Reboot System	147
21.7 FTP Command Line	148
21.7.1 Filename Conventions	148
21.7.1.1 Example FTP Commands	149
21.7.2 FTP Command Line Procedure	149
21.7.3 GUI-based FTP Clients	150
21.7.4 FTP Restrictions	150
Chapter 22	
Access Control.....	151
22.1 Overview	151
22.2 The Access Control Main Screen	151
22.3 About SNMP	152
22.3.1 Supported MIBs	153
22.3.2 SNMP Traps	153
22.3.3 Configuring SNMP	154
22.3.4 Setting Up Login Accounts	155
22.4 SSH Overview	156
22.5 How SSH works	156
22.6 SSH Implementation on the Switch	157
22.6.1 Requirements for Using SSH	158
22.7 Introduction to HTTPS	158

22.8 HTTPS Example	159
22.8.1 Internet Explorer Warning Messages	159
22.8.2 Netscape Navigator Warning Messages	159
22.8.3 The Main Screen	160
22.9 Service Port Access Control	162
22.10 Remote Management	163
Chapter 23	
Diagnostic	165
23.1 Diagnostic	165
Chapter 24	
Cluster Management	167
24.1 Overview	167
24.2 Cluster Management Status	168
24.2.1 Cluster Member Switch Management	169
24.2.1.1 Uploading Firmware to a Cluster Member Switch	169
24.3 Configuring Cluster Management	170
Chapter 25	
MAC Table	173
25.1 Overview	173
25.2 Viewing the MAC Table	174
Chapter 26	
ARP Table	175
26.1 Overview	175
26.1.1 How ARP Works	175
26.2 Viewing the ARP Table	175
Chapter 27	
Introducing the Commands	177
27.1 Overview	177
27.1.1 Switch Configuration File	177
27.2 Accessing the CLI	177
27.2.1 Access Priority	178
27.2.2 The Console Port	178
27.2.2.1 Initial Screen	178
27.2.3 Telnet	178
27.3 The Login Screen	179
27.4 Command Syntax Conventions	179
27.5 Getting Help	180
27.5.1 List of Available Commands	180

27.5.2 Detailed Command Information	181
27.6 Command Modes	181
27.7 Using Command History	182
27.8 Saving Your Configuration	182
27.8.1 Logging Out	183
27.9 Command Summary	183
27.9.1 User Mode	183
27.9.2 Enable Mode	184
27.9.3 General Configuration Mode	187
27.9.4 interface port-channel Commands	195
27.9.5 config-vlan Commands	197
27.9.6 mvr Commands	199
Chapter 28	
Command Examples	201
28.1 Overview	201
28.2 show Commands	201
28.2.1 show system-information	201
28.2.2 show ip	202
28.2.3 show logging	202
28.2.4 show interface	203
28.2.5 show mac address-table	204
28.3 ping	205
28.4 traceroute	205
28.5 Enabling RSTP	206
28.6 Configuration File Maintenance	206
28.6.1 Using a Different Configuration File	207
28.6.2 Resetting to the Factory Default	207
28.7 no Command Examples	208
28.7.1 no mirror	208
28.7.2 no https timeout	208
28.7.3 no trunk	209
28.7.4 no port-access-authenticator	209
28.7.5 no ssh	210
28.8 interface Commands	210
28.8.1 interface port-channel	210
28.8.2 bandwidth-limit	211
28.8.3 mirror	212
28.8.4 gvrp	213
28.8.5 ingress-check	213
28.8.6 frame-type	213
28.8.7 queuing-method spq	214
28.8.8 queuing-method wrr	214

28.8.9 egress set	215
28.8.10 qos priority	215
28.8.11 name	216
28.8.12 speed-duplex	216

Chapter 29

IEEE 802.1Q Tagged VLAN Commands 219

29.1 IEEE 802.1Q Tagged VLAN Overview	219
29.2 VLAN Databases	219
29.2.1 Static Entries (SVLAN Table)	219
29.2.2 Dynamic Entries (DVLAN Table)	220
29.3 Configuring Tagged VLAN	220
29.4 Global VLAN1Q Tagged VLAN Configuration Commands	221
29.4.1 GARP Status	221
29.4.2 GARP Timer	221
29.4.3 GVRP Timer	222
29.4.4 Enable GVRP	222
29.4.5 Disable GVRP	223
29.5 Port VLAN Commands	223
29.5.1 Set Port VID	223
29.5.2 Set Acceptable Frame Type	223
29.5.3 Enable or Disable Port GVRP	224
29.5.4 Modify Static VLAN	224
29.5.4.1 Modify a Static VLAN Table Example	225
29.5.4.2 Forwarding Process Example	225
29.5.5 Delete VLAN ID	225
29.6 Enable VLAN	226
29.7 Disable VLAN	226
29.8 Show VLAN Setting	226

Chapter 30

Troubleshooting 229

30.1 Problems Starting Up the Switch	229
30.2 Problems Accessing the Switch	230
30.2.1 Pop-up Windows, JavaScripts and Java Permissions	230
30.2.1.1 Internet Explorer Pop-up Blockers	230
30.2.1.2 JavaScripts	233
30.2.1.3 Java Permissions	235
30.3 Problems with the Password	237

Appendix A

Product Specifications 239

Appendix B

IP Subnetting	243
Index	251

List of Figures

Figure 1 Backbone Application	32
Figure 2 Bridging Application	33
Figure 3 High Performance Switched Application	33
Figure 4 Tag-based VLAN Application	34
Figure 5 Shared Server Using VLAN Example	35
Figure 6 Attaching Rubber Feet	37
Figure 7 Attaching the Mounting Brackets	38
Figure 8 Mounting the Switch on a Rack	39
Figure 9 Front Panel	41
Figure 10 Transceiver Installation Example	43
Figure 11 Installed Transceiver	43
Figure 12 Opening the Transceiver's Latch Example	43
Figure 13 Transceiver Removal Example	44
Figure 14 Rear Panel	44
Figure 15 Web Configurator: Login	47
Figure 16 Web Configurator Home Screen (Status)	48
Figure 17 Change Administrator Login Password	52
Figure 18 Resetting the Switch: Via the Console Port	54
Figure 19 Web Configurator: Logout Screen	54
Figure 20 Initial Setup Network Example: VLAN	55
Figure 21 Initial Setup Network Example: Port VID	57
Figure 22 Initial Setup Example: Management IP Address	58
Figure 23 Status	60
Figure 24 Status: Port Details	62
Figure 25 System Info	66
Figure 26 General Setup	68
Figure 27 Switch Setup	70
Figure 28 IP Setup	72
Figure 29 Port Setup	75
Figure 30 Port VLAN Trunking	79
Figure 31 Switch Setup: Select VLAN Type	80
Figure 32 VLAN: VLAN Status	80
Figure 33 VLAN: Static VLAN	82
Figure 34 VLAN: VLAN Port Setting	84
Figure 35 Port Based VLAN Setup (All Connected)	86
Figure 36 Port Based VLAN Setup (Port Isolation)	87

Figure 37 Static MAC Forwarding	90
Figure 38 Spanning Tree Protocol: Status	95
Figure 39 Spanning Tree Protocol: Configuration	97
Figure 40 Bandwidth Control	100
Figure 41 Broadcast Storm Control	104
Figure 42 Mirroring	107
Figure 43 Link Aggregation Control Protocol Status	110
Figure 44 Link Aggregation: Configuration	112
Figure 45 RADIUS Server	115
Figure 46 Port Authentication	116
Figure 47 Port Authentication: 802.1x	117
Figure 48 Port Authentication: RADIUS	118
Figure 49 Port Security	122
Figure 50 Queuing Method	124
Figure 51 Multicast Setting	127
Figure 52 Multicast: IGMP Filtering Profile	129
Figure 53 MVR Network Example	130
Figure 54 MVR Multicast Television Example	131
Figure 55 MVR	132
Figure 56 MVR: Group Configuration	134
Figure 57 MVR Configuration Example	135
Figure 58 MVR Configuration Example	136
Figure 59 MVR Group Configuration Example	137
Figure 60 MVR Group Configuration Example	137
Figure 61 Static Routing	139
Figure 62 DiffServ: Differentiated Service Field	141
Figure 63 DiffServ Network Example	142
Figure 64 DiffServ	143
Figure 65 Maintenance	145
Figure 66 Firmware Upgrade	145
Figure 67 Restore Configuration	146
Figure 68 Backup Configuration	146
Figure 69 Load Factory Default: Conformation	147
Figure 70 Load Factory Default: Start	147
Figure 71 Reboot System: Confirmation	148
Figure 72 Reboot System: Start	148
Figure 73 Console Port Priority	151
Figure 74 Access Control	152
Figure 75 SNMP Management Model	152
Figure 76 Access Control: SNMP	154
Figure 77 Access Control: Logins	155
Figure 78 SSH Communication Example	156
Figure 79 How SSH Works	157

Figure 80 HTTPS Implementation	158
Figure 81 Security Alert Dialog Box (Internet Explorer)	159
Figure 82 Security Certificate 1 (Netscape)	160
Figure 83 Security Certificate 2 (Netscape)	160
Figure 84 Login Screen (Internet Explorer)	161
Figure 85 Login Screen (Netscape)	162
Figure 86 Access Control: Service Access Control	163
Figure 87 Access Control: Remote Management	164
Figure 88 Diagnostic	165
Figure 89 Clustering Application Example	167
Figure 90 Cluster Management: Status	168
Figure 91 Cluster Management: Cluster Member Web Configurator Screen	169
Figure 92 Example: Uploading Firmware to a Cluster Member Switch	170
Figure 93 Clustering Management Configuration	171
Figure 94 MAC Table Flowchart	173
Figure 95 MAC Table	174
Figure 96 ARP Table	176
Figure 97 Initial Console Port Screen	178
Figure 98 CLI: Login Screen	179
Figure 99 CLI Help: List of Commands: Example 1	180
Figure 100 CLI Help: List of Commands: Example 2	181
Figure 101 CLI Help: Detailed Command Information: Example 1	181
Figure 102 CLI: Help: Detailed Command Information: Example 2	181
Figure 103 CLI: History Command Example	182
Figure 104 CLI: write memory	183
Figure 105 show system-information Command Example	201
Figure 106 show ip Command Example	202
Figure 107 show logging Command Example	203
Figure 108 show interface Command Example	204
Figure 109 show mac address-table Command Example	205
Figure 110 ping Command Example	205
Figure 111 traceroute Command Example	206
Figure 112 Enable RSTP Command Example	206
Figure 113 CLI: boot config Command Example	207
Figure 114 CLI: reload config Command Example	207
Figure 115 CLI: Reset to the Factory Default Example	208
Figure 116 no mirror Command Example	208
Figure 117 no https timeout Command Example	208
Figure 118 no trunk Command Example	209
Figure 119 no port-access-authenticator Command Example	210
Figure 120 no ssh Command Example	210
Figure 121 interface Command Example	211
Figure 122 bandwidth-limit Command Example	212

Figure 123 mirror Command Example	212
Figure 124 gvrp Command Example	213
Figure 125 ingress-check Command Example	213
Figure 126 frame-type Command Example	214
Figure 127 queuing-method spq Command Example	214
Figure 128 queuing-method wrr Command Example	215
Figure 129 egress set Command Example	215
Figure 130 qos priority Command Example	216
Figure 131 name Command Example	216
Figure 132 speed-duplex Command Example	217
Figure 133 Tagged VLAN Configuration and Activation Example	220
Figure 134 CPU VLAN Configuration and Activation Example	221
Figure 135 GARP STATUS Command Example	221
Figure 136 GARP Timer Command Example	222
Figure 137 GVRP Status Command Example	222
Figure 138 vlan1q port default vid Command Example	223
Figure 139 frame type Command Example	224
Figure 140 no gvrp Command Example	224
Figure 141 Modifying Static VLAN Example	225
Figure 142 no vlan Command Example	226
Figure 143 show vlan Command Example	227
Figure 144 Pop-up Blocker	231
Figure 145 Internet Options	231
Figure 146 Internet Options	232
Figure 147 Pop-up Blocker Settings	233
Figure 148 Internet Options	234
Figure 149 Security Settings - Java Scripting	235
Figure 150 Security Settings - Java	236
Figure 151 Java (Sun)	237

List of Tables

Table 1 Front Panel	41
Table 2 Front Panel LEDs	44
Table 3 Navigation Panel Sub-links Overview	49
Table 4 Web Configurator Screen Sub-links Details	49
Table 5 Navigation Panel Links	50
Table 6 Status	60
Table 7 Status: Port Details	62
Table 8 System Info	66
Table 9 General Setup	68
Table 10 Switch Setup	70
Table 11 IP Setup	73
Table 12 Port Setup	75
Table 13 IEEE 802.1Q VLAN Terminology	78
Table 14 VLAN: VLAN Status	81
Table 15 VLAN: Static VLAN	83
Table 16 VLAN: VLAN Port Setting	84
Table 17 Port Based VLAN Setup	87
Table 18 Static MAC Forwarding	90
Table 19 STP Path Costs	93
Table 20 STP Port States	94
Table 21 Spanning Tree Protocol: Status	95
Table 22 Spanning Tree Protocol: Configuration	98
Table 23 Bandwidth Control	100
Table 24 Broadcast Storm Control	104
Table 25 Mirroring	107
Table 26 Link Aggregation ID: Local Switch	110
Table 27 Link Aggregation ID: Peer Switch	110
Table 28 Link Aggregation Control Protocol Status	111
Table 29 Link Aggregation Control Protocol: Configuration	113
Table 30 Port Authentication: 802.1x	118
Table 31 Port Authentication: RADIUS	118
Table 32 Port Security	122
Table 33 Physical Queue Priority	123
Table 34 Queuing Method	124
Table 35 Multicast Status	126
Table 36 Multicast Setting	127

Table 37 Multicast: IGMP Filtering Profile	129
Table 38 MVR	132
Table 39 MVR: Group Configuration	134
Table 40 Static Routing	139
Table 41 Default DSCP-IEEE802.1p Mapping	142
Table 42 DiffServ	143
Table 43 Filename Conventions	148
Table 44 Access Control Overview	151
Table 45 SNMP Commands	153
Table 46 SNMP Traps	153
Table 47 Access Control: SNMP	154
Table 48 Access Control: Logins	155
Table 49 Access Control: Service Access Control	163
Table 50 Access Control: Remote Management	164
Table 51 Diagnostic	165
Table 52 ZyXEL Clustering Management Specifications	167
Table 53 Cluster Management: Status	168
Table 54 FTP Upload to Cluster Member Example	170
Table 55 Clustering Management Configuration	171
Table 56 MAC Table	174
Table 57 ARP Table	176
Table 58 Command Summary: User Mode	183
Table 59 Command Summary: Enable Mode	184
Table 60 Command Summary: Configuration Mode	187
Table 61 interface port-channel Commands	195
Table 62 Command Summary: config-vlan Commands	197
Table 63 mvr Commands	199
Table 64 Troubleshooting the Start-Up of Your Switch	229
Table 65 Troubleshooting Accessing the Switch	230
Table 66 Troubleshooting the Password	237
Table 67 General Product Specifications	239
Table 68 Management Specifications	240
Table 69 Physical and Environmental Specifications	240
Table 70 Classes of IP Addresses	243
Table 71 Allowed IP Address Range By Class	244
Table 72 "Natural" Masks	244
Table 73 Alternative Subnet Mask Notation	245
Table 74 Two Subnets Example	245
Table 75 Subnet 1	246
Table 76 Subnet 2	246
Table 77 Subnet 1	247
Table 78 Subnet 2	247
Table 79 Subnet 3	247

Table 80 Subnet 4	248
Table 81 Eight Subnets	248
Table 82 Class C Subnet Planning	248
Table 83 Class B Subnet Planning	249

Preface

Congratulations on your purchase of the GS-2024 Gigabite Ethernet Switch.

This preface introduces you to the GS-2024 Gigabite Ethernet Switch and discusses the conventions of this User's Guide. It also provides information on other related documentation.

Note: 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.

About This User's Guide

This manual is designed to guide you through the installation and configuration of your GS-2024 for its various applications.










Related Documentation

- Web Configurator Online Help
Embedded web help for descriptions of individual screens and supplementary information.
- ZyXEL Glossary and Web Site
Please refer to www.zyxel.com for an online glossary of networking terms and additional support documentation.

Syntax Conventions

- “Enter” means for you to type one or more characters. “Select” or “Choose” means for you to use one of the predefined choices.
- Command and arrow keys are enclosed in square brackets. [ENTER] means the Enter, or carriage return key; [ESC] means the Escape key and [SPACE BAR] means the Space Bar.
- Mouse action sequences are denoted using a comma. For example, “In Windows, click **Start, Settings** and then **Control Panel**” means first click the **Start** button, then point your mouse pointer to **Settings** and then click **Control Panel**.
- “e.g.,” is a shorthand for “for instance”, and “i.e.,” means “that is” or “in other words”.
- The GS-2024 Gigabite Ethernet Switch may be referred to as “the GS-2024” or “the switch” in this User's Guide.

Graphics Icons Key

GS-2024 	Computer 	Server 
Computer 	DSLAM 	Gateway 
Central Office/ ISP 	Internet 	Hub/Switch 

User Guide Feedback

Help us help you. E-mail all User Guide-related comments, questions or suggestions for improvement to techwriters@zyxel.com.tw or send regular mail to The Technical Writing Team, ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 300, Taiwan. Thank you.

CHAPTER 1

Getting to Know Your Switch

This chapter introduces the main features and applications of the switch.

1.1 Introduction

The GS-2024 is a stand-alone layer-2 Gigabit Ethernet switch with 24 100/1000Mbps ports and two mini-GBIC (Gigabit Interface Converter) slots for optical uplinking and one console port and RJ-45 port for local management.

With its built-in web configurator, managing and configuring the switch is easy. In addition, the switch can also be managed via Telnet, any terminal emulator program on the console port, or third-party SNMP management.

1.2 Software Features

This section describes the general software features of the switch.

DHCP Client

DHCP (Dynamic Host Configuration Protocol RFC 2131 and RFC 2132) allows individual computers to obtain TCP/IP configuration at start-up from a server. You can configure the switch as a DHCP client to obtain TCP/IP information (such as the IP address and subnet mask) from a DHCP server. If you disable the DHCP service, you must manually enter the TCP/IP information.

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.

Differentiated Services (DiffServ)

With DiffServ, the switch 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.

Queuing

Queuing is used to help solve performance degradation when there is network congestion. Two scheduling services are supported: Strict Priority Queuing (SPQ) and Weighted Round Robin Scheduling (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.

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.

Multicast VLAN Registration (MVR)

Multicast VLAN Registration (MVR) is designed for applications (such as Media-on-Demand (MoD)) using multicast traffic across an Ethernet ring-based service provider network. MVR allows one single multicast VLAN can be shared among different subscriber VLANs on the network.

This improves bandwidth utilization with reduced multicast traffic in the subscriber VLANs and easy multicast group management.

STP (Spanning Tree Protocol) / RSTP (Rapid STP)

(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.

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.

Maintenance and Management Features

- Access Control
You can specify the service(s) and computer IP address(es) to control access to the switch for management.
- 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.
- Configuration and Firmware Maintenance
You can backup or restore the switch configuration or upgrade the firmware on the switch.

1.3 Hardware Features

This section describes the ports on the switch.

Gigabit Ethernet Ports

The ports allow the switch to connect to another Ethernet devices or daisy-chain to other switches.

Mini-GBIC Slots

Install SFP transceivers in these slots to connect to other Ethernet switches at longer distances than the Ethernet port.

Console Port

Use the console port for local management of the switch.

One Management Port

Use the RJ-45 management port for switch management only. The management port is out-of-band, meaning that it does not carry switch traffic.

Fans

The fans cool the switch sufficiently to allow reliable operation of the switch in even poorly ventilated rooms or basements.

1.4 Applications

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

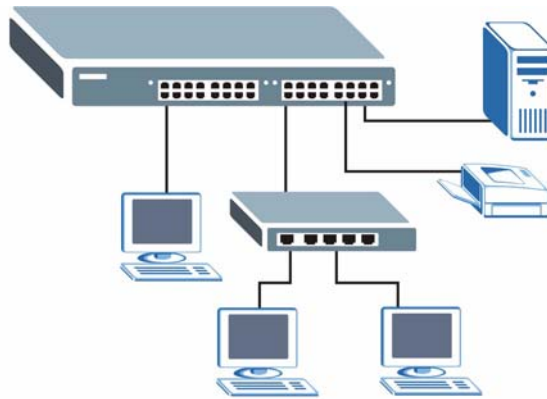
1.4.1 Backbone Application

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 port or connect other switches to the switch.

In this example, all computers can share high-speed applications on the server. To expand the network, simply add more networking devices such as switches, routers, computers, print servers etc.

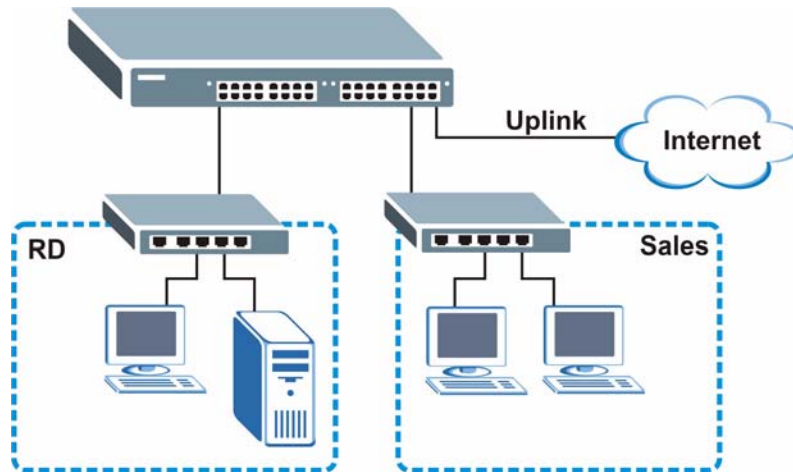
Figure 1 Backbone Application



1.4.2 Bridging Example

In this example application the switch connects different company departments (**RD** and **Sales**) 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 using a Gigabit Ethernet/mini-GBIC port on the switch.

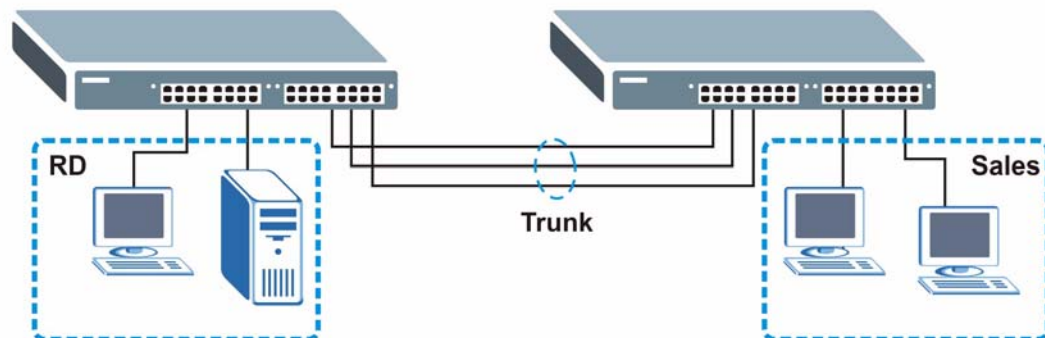
Moreover, the switch eases supervision and maintenance by allowing network managers to centralize multiple servers at a single location.

Figure 2 Bridging Application

1.4.3 High Performance Switched Example

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

Switching to higher-speed LANs such as ATM (Asynchronous Transmission Mode) 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 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

1.4.4 IEEE 802.1Q VLAN Application Examples

This section shows a workgroup and a shared server example using 802.1Q tagged VLANs.

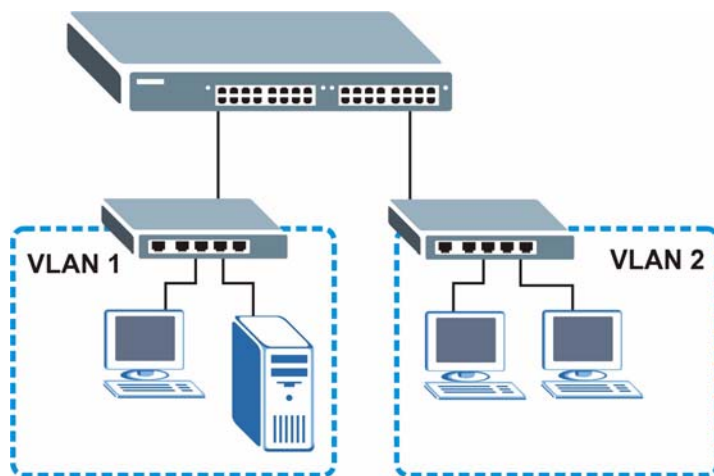
A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Stations on a logical network belong to one group. A station can belong to more than one group. With VLAN, a station cannot directly talk to or hear from stations that are not in the same group(s) unless such traffic first goes through a router.

For more information on VLANs, refer to [Chapter 8 on page 77](#).

1.4.4.1 Tag-based VLAN Example

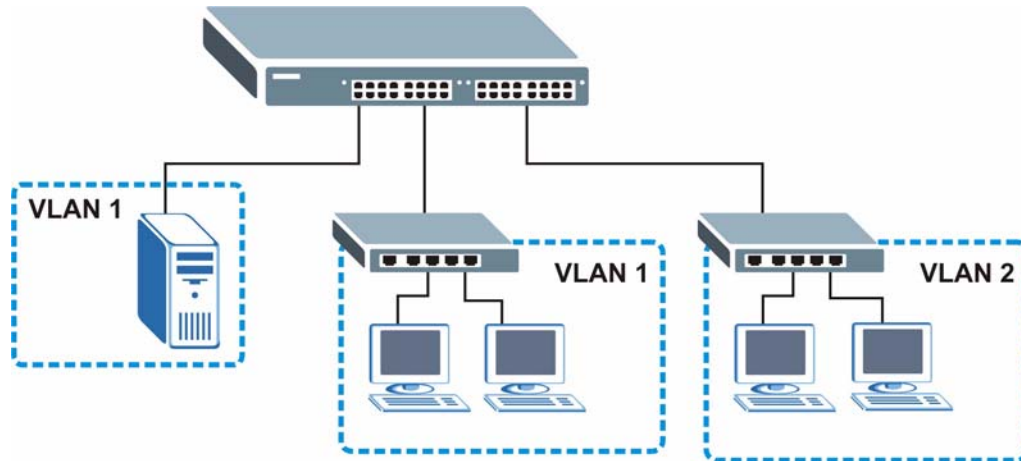
Ports in the same VLAN group share the same frame broadcast domain thus increase network performance through reduced broadcast traffic. VLAN groups can be modified at any time by adding, moving or changing ports without any re-cabling.

Figure 4 Tag-based VLAN Application



1.4.4.2 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. Ports can belong to other VLAN groups too.

Figure 5 Shared Server Using VLAN Example

CHAPTER 2

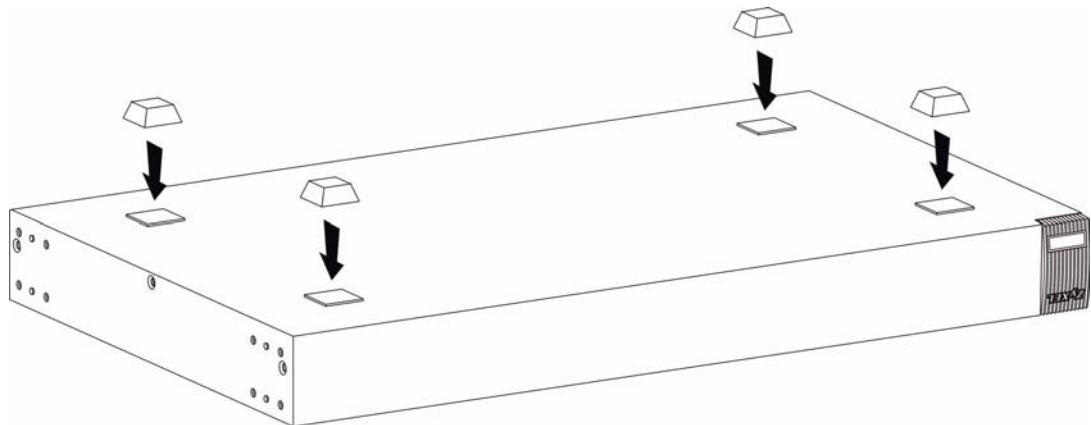
Hardware Installation and Connection

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

2.1 Freestanding Installation

- 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



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

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 Mounting the Switch on a Rack

This section lists the rack mounting requirements and precautions and describes the installation steps.

2.2.1 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.

Note: Failure to use the proper screws may damage the unit.

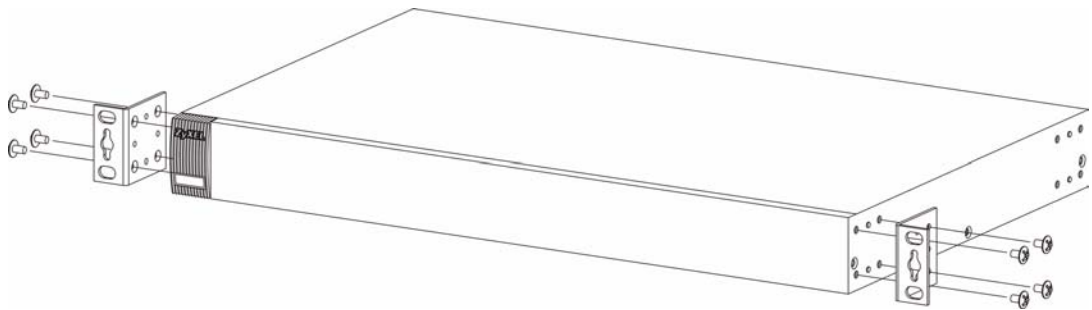
2.2.1.1 Precautions

- 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.

2.2.2 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.

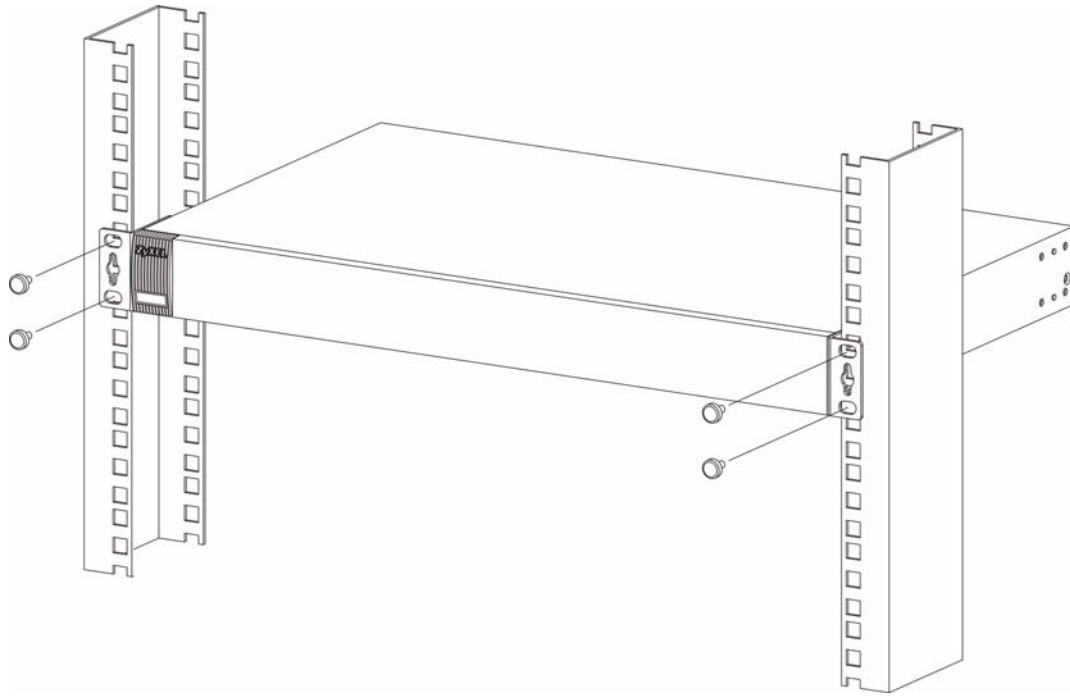
Figure 7 Attaching the Mounting Brackets



- 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.

2.2.3 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.

CHAPTER 3

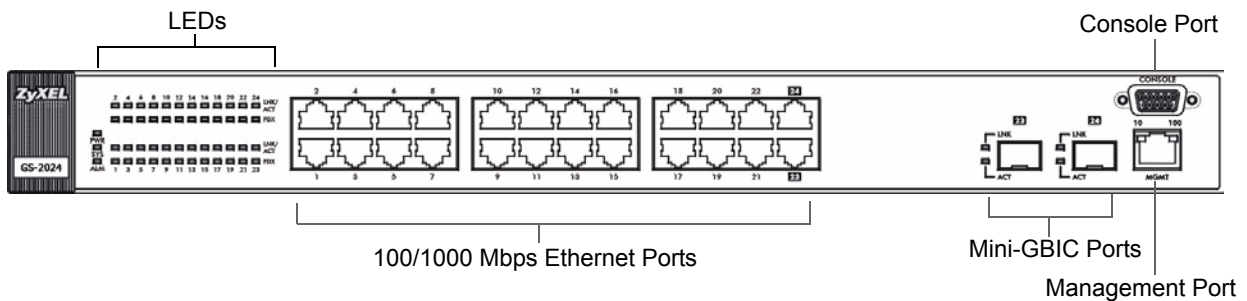
Hardware Overview

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 Connection

The figure below shows the front panel of the switch.

Figure 9 Front Panel



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

Table 1 Front Panel

CONNECTOR	DESCRIPTION
24 100/1000 Mbps RJ-45 Ethernet Ports	Connect these Gigabit Ethernet ports to high-bandwidth backbone network Ethernet switches or use them to daisy-chain other switches.
Mini-GBIC Ports	Use mini-GBIC transceivers in these slots for fiber-optical connections to backbone Ethernet switches.
Console Port	Only connect this port if you want to configure the switch using the command line interface (CLI) via the console port.
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 switch. Connect the female end to a serial port (COM1, COM2 or other COM port) of your computer.

3.1.2 Ethernet Ports

The switch has 24 100/1000Mbps 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 (at 100 Mbps) or full duplex.

An auto-negotiating port can detect and adjust to the optimum Ethernet speed (100/1000Mbps) and duplex mode (full duplex or half duplex) of the connected device.

An auto-crossover (auto-MDI/MDI-X) port automatically works with a straight-through or crossover Ethernet cable.

Two Gigabit ports are paired with the two mini GBIC slots. The switch uses up to one connection for each pair for a total of two possible Gigabit connections (one from each of the two pairs). 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.

3.1.2.1 Default Ethernet Settings

The factory default negotiation settings for the Ethernet ports on the switch are:

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

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 switch does not come with transceivers. You must use transceivers that comply with the SFP (Small Form-factor Pluggable) Transceiver MultiSource Agreement (MSA). See the SFF committee's INF-8074i specification Rev 1.0 for details.

There are two pairs of Gigabit Ethernet/mini-GBIC ports. 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.

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.

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

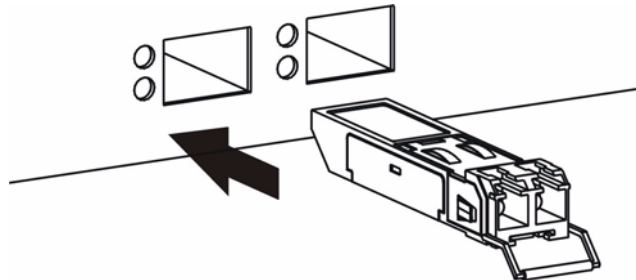
Note: To avoid possible eye injury, do not look into an operating fiber-optic module's connectors.

3.1.3.1 Transceiver Installation

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

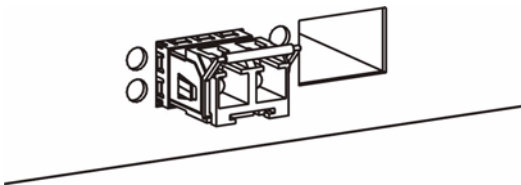
- 1 Insert the transceiver into the slot with the exposed section of PCB board facing down.

Figure 10 Transceiver Installation Example



- 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.

Figure 11 Installed Transceiver

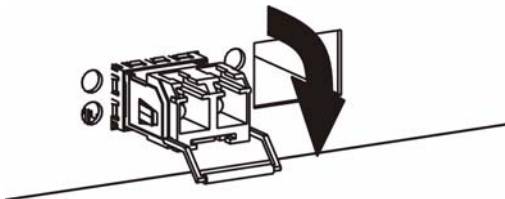


3.1.3.2 Transceiver Removal

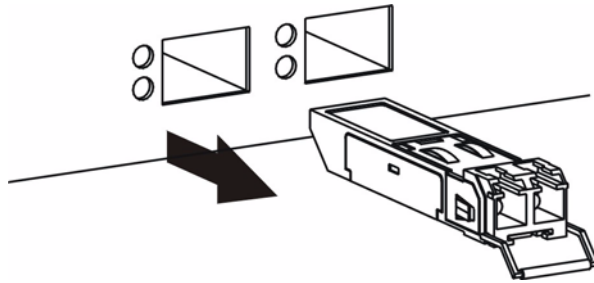
Use the following steps to remove a mini GBIC transceiver (SFP module).

- 1 Open the transceiver's latch (latch styles vary).

Figure 12 Opening the Transceiver's Latch Example

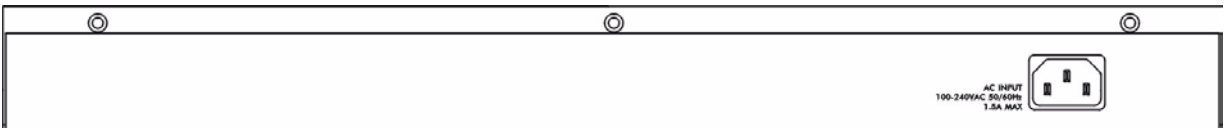


- 2 Pull the transceiver out of the slot.

Figure 13 Transceiver Removal Example

3.2 Rear Panel

The following figure shows the rear panel of the switch. The power receptacle is on the rear panel.

Figure 14 Rear Panel

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 switch, 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 the power source. Make sure that no objects obstruct the airflow of the fans.

3.3 Front Panel LEDs

The LEDs are located on the front panel. The following table describes the LEDs on the front panel.

Table 2 Front Panel LEDs

LED	COLOR	STATUS	DESCRIPTION
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.

Table 2 Front Panel LEDs (continued)

LED	COLOR	STATUS	DESCRIPTION
LNK/ACT (Gigabit ports)	Green	Blinking	The system is transmitting/receiving to/from a 1000 Mbps Ethernet network.
		On	The link to a 1000 Mbps Ethernet network is up.
	Amber	Blinking	The system is transmitting/receiving to/from a 100 Mbps Ethernet network.
		On	The link to a 100 Mbps Ethernet network is up.
		Off	The link to an Ethernet network is down.
FDX (Gigabit ports)	Amber	On	The Gigabit port is negotiating in full-duplex mode.
		Off	The Gigabit port is negotiating in half-duplex mode and no collisions are occurring.
GBIC Slots			
LNK	Green	On	The port has a successful connection.
		Off	No Ethernet device is connected to this port.
ACT	Green	Blinking	The port is receiving or transmitting data.
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.

CHAPTER 4

The Web Configurator

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

4.1 Introduction

The web configurator is an HTML-based management interface that allows easy switch setup and management via Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

4.2 System Login

- 1 Start your web browser.
- 2 Type “http://” and the IP address of the switch (for example, the default is 192.168.1.1) in the **Location** or **Address** field. Press [ENTER].
- 3 The login screen appears. The default username is **admin** and 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 15 Web Configurator: Login



The screenshot shows a dialog box titled "Enter Network Password". It contains the following information:

- Site: 192.168.1.1
- Realm: GS-2024 at Thu Jan 1 00:40:31 1970
- User Name: admin
- Password: masked with asterisks (xxxxx)
- Checkbox: Save this password in your password list
- Buttons: OK, Cancel

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

4.3 The Status Screen

The **Status** screen is the first screen that displays when you access the web configurator.

The following figure shows the navigating components of a web configurator screen.

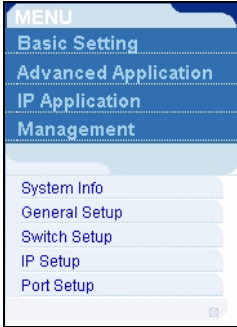

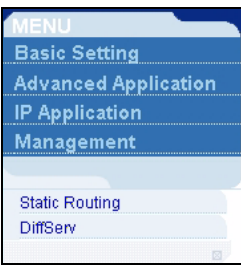

Figure 16 Web Configurator Home Screen (Status)

The screenshot shows the ZyXEL web configurator interface. On the left is a navigation menu with the following items: MENU, Basic Setting, Advanced Application, IP Application, and Management. The main content area is titled 'Status' and shows 'System Up Time : 0:42:18'. Below this is a table with the following columns: Port, Link, State, LACP, TxPkts, RxPkts, Errors, Tx KB/s, Rx KB/s, and Up Time. The table contains 17 rows, all with 'Down' link status and 'STOP' state. At the bottom of the status area, there are controls for 'Poll Interval(s)' set to 40, a 'Set Interval' button, a 'Stop' button, a 'Port' dropdown menu set to 'ALL', and a 'Clear Counter' button.

Port	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	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
12	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
13	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
14	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
15	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
16	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
17	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00

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
			

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 VLAN Status VLAN Port Setting Static VLAN Static MAC Forwarding Spanning Tree Protocol Status Spanning Tree Protocol Configuration Bandwidth Control Broadcast Storm Control Mirroring Link Aggregation Link Aggregation Protocol Status Link Aggregation	Static Routing DiffServ	Maintenance Firmware Upgrade Restore Configuration Backup Configuration Load Factory Default Reboot System Access Control SNMP Logins Service Access Control Diagnostic Cluster Management Status Configuration

Table 4 Web Configurator Screen Sub-links Details (continued)

BASIC SETTING	ADVANCED APPLICATION	IP APPLICATION	MANAGEMENT
	Port Authentication RADIUS 802.1x Port Security Queuing Method Multicast Multicast Status Multicast Setting IGMP Filtering Profile MVR		MAC Table ARP Table

The following table describes the links in the navigation panel.

Table 5 Navigation Panel Links

LINK	DESCRIPTION
Basic Settings	
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, IGMP snooping, GARP and priority queues.
IP Setup	This link takes you to a screen where you can configure the management IP address, subnet mask (necessary for switch management) and DNS (domain name server).
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.
Spanning Tree Protocol	This link takes you to screens where you can configure the STP/RSTP to prevent network loops.
Bandwidth Control	This link takes you to screens where you can cap the maximum incoming bandwidth allowed on specified port(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

Table 5 Navigation Panel Links (continued)

LINK	DESCRIPTION
Link Aggregation	This link takes you to a screen where you can logically aggregate 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 maximum port security through the use of configured static MAC addresses.
Queuing Method	This link takes you to a screen where you can configure SPQ or WRR with associated queue weights.
Multicast	This link takes you to a screen where you can configure various multicast features and create multicast VLANs.
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.
DiffServ	This link takes you to screens where you can enable DiffServ and set DSCP-to-IEEE802.1p mappings.
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).
Cluster Management	This link takes you to a screen where you can configure clustering management and view its status.
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.

4.3.1 Change Your Password

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

Figure 17 Change Administrator Login Password

The screenshot shows a web interface for configuring logins. At the top, there are tabs for 'Logins' (selected) and 'Access Control'. Below the tabs, the 'Administrator' section is highlighted with a red oval. It contains three input fields: 'Old Password', 'New Password', and 'Retype to confirm'. Below these fields is a red warning message: 'Please record your new password whenever you change it. The system will lock you out if you have forgotten your password.' Below the warning is an 'Edit Logins' section with a table. The table has four columns: 'Login', 'User Name', 'Password', and 'Retype to confirm'. There are four rows, numbered 1 to 4, each with empty input fields. At the bottom of the form are 'Apply' and 'Cancel' buttons.

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"/>

4.4 Switch Lockout

You can be locked out from managing the switch if another administrator is currently logged in. You must wait until the other administrator has logged out before you can log in.

Any of the following could also lock you and others out from using in-band management (managing through the data ports).

- 1 Deleting the management VLAN (default is VLAN 1).
- 2 With port-based VLAN, disabling the CPU in-band switch management port option for all ports.
- 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.
- 6 Misconfiguring the text configuration file.
- 7 Forgetting the password and/or IP address.
- 8 Preventing all services from accessing the switch.
- 9 Changing a service port number but forgetting it.
- 10 Incorrectly configuring the access control settings. This could also lock you out from performing out-of-band management (managing through the console port or management port).

Note: Be careful not to lock yourself and others out of the switch.

4.5 Resetting the Switch

If you lock yourself (and others) out of the switch, you can try using out-of-band management. If you still cannot correct the situation or forgot the 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 [Section 3.1.1 on page 41](#) 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 configuration file upload, type `atgo` to restart the switch.

Figure 18 Resetting the Switch: Via the Console Port

```
Bootbase Version: V0.6 | 05/18/2004 15:28:28
AM:Size = 32 Mbytes
DRAM POST: Testing: 32768K OK
DRAM Test SUCCESS !
FLASH: Intel 32M

ZyNOS Version: V3.60(LT.0)b3 | 06/21/2005 17:00:44

Press any key to enter debug mode within 3 seconds.
.....
Enter Debug Mode

GS-2024> atlc
Starting XMODEM upload (CRC mode)....
CCCCCCCCCCCCCCCC
Total 262144 bytes received.
Erasing..
.....
OK
GS-2024> atgo
```

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

4.6 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 19 Web Configurator: Logout Screen

4.7 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.

CHAPTER 5

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:

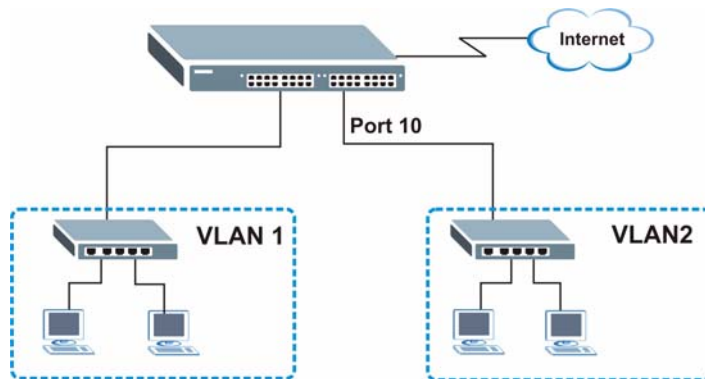
- Create a VLAN
- Set port VLAN ID
- Configure the switch IP management address

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 10 as a member of VLAN 2.

Figure 20 Initial Setup Network Example: VLAN



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

Index	VID	Port Number												Elapsed Time	Status
		2	4	6	8	10	12	14	16	18	20	22	24		
1	1	U	U	U	U	U	U	U	U	U	U	U	U	1:05:48	Static
		U	U	U	U	U	U	U	U	U	U	U	U		

Poll Interval(s):

Change Pages:

- 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 10 on the switch, select **Fixed** to configure port 10 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.

ACTIVE

Name:

VLAN Group ID:

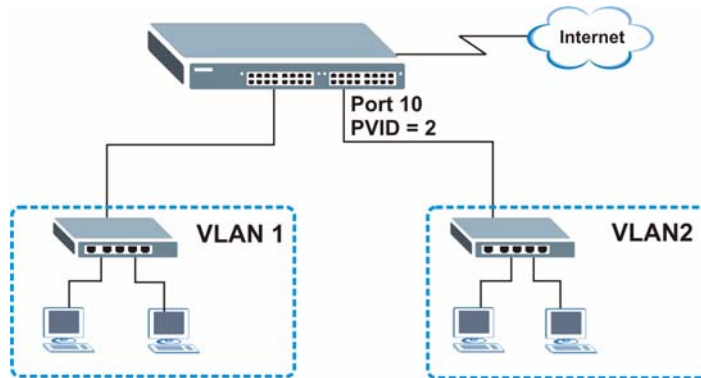
Port	Control			Tagging
1	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
2	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> 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 type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input 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
13	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
14	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
15	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
16	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
17	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
18	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
19	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
20	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
21	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
22	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
23	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
24	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging

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 10 so that any untagged frames received on that port get sent to VLAN 2.

Figure 21 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 10 and click **Apply** to save the settings.

Port	Ingress Check	PVID	GVRP	Acceptable Frame Type	VLAN Trunking
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"/>	2	<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"/>
13	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
14	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
15	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
16	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
17	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
18	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
19	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
20	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
21	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
22	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
23	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
24	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>

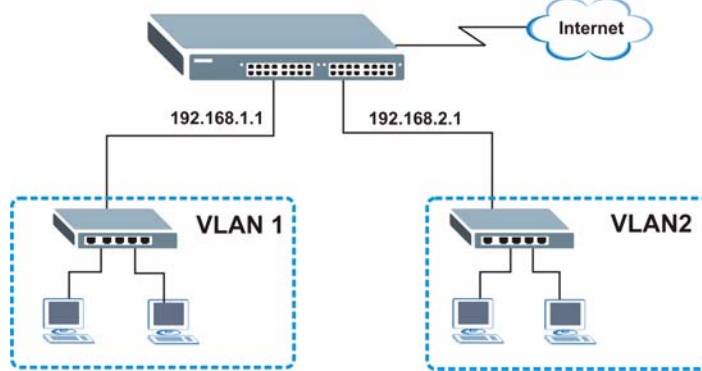
VLAN Status

GVRP

Apply Cancel

5.1.3 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 22 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 47](#) for more information.
- 3 Click **Basic Setting** and **IP Setup** in the navigation panel.
- 4 Configure the related fields in the **IP Setup** screen.

For the **VLAN2** network, enter 192.168.2.1 as the IP address and 255.255.255.0 as the subnet mask.
- 5 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.
- 6 Click **Add**.

IP Setup

Domain Name Server: 0.0.0.0
 Default Management: In-band Out-of-band

In-band Management IP Address DHCP Client Static IP Address

IP Address: 192.168.1.1
 IP Subnet Mask: 255.255.255.0
 Default Gateway: 0.0.0.0
 VID: 1

Out-of-band Management IP Address

IP Address: 192.168.0.1
 IP Subnet Mask: 255.255.255.0
 Default Gateway: 0.0.0.0

Apply Cancel

In-band IP Addresses

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

Add Cancel

Delete Cancel

CHAPTER 6

System Status and Port Statistics

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

6.1 Overview

The status screen of the web configurator displays a port statistical summary table 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 **Status** screen as shown next.

Figure 23 Status

The screenshot shows a 'Status' page with a 'System Up Time : 0:45:36' indicator. Below this is a table with 10 columns: Port, Link, State, LACP, TxPkts, RxPkts, Errors, Tx KB/s, Rx KB/s, and Up Time. The table lists 24 ports. Ports 1 through 21 are 'Down' with 'STOP' state and 'Disabled' LACP. Port 22 is '100M/F' with 'FORWARDING' state and 'Disabled' LACP, showing 1376 TxPkts and 1040 RxPkts. Ports 23 and 24 are 'Down' with 'STOP' state and 'Disabled' LACP. Below the table are control buttons: 'Poll Interval(s)' set to 40 with 'Set Interval' and 'Stop' buttons, and 'Port' set to 'ALL' with a 'Clear Counter' button.

Port	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	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
12	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
13	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
14	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
15	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
16	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
17	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
18	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
19	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
20	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
21	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
22	100M/F	FORWARDING	Disabled	1376	1040	0	0.0	0.0	0:23:58
23	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
24	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00

The following table describes the labels in this screen.

Table 6 Status

LABEL	DESCRIPTION
System up Time	This field shows how long the system has been running since the last time it was started.
Port	This identifies the Ethernet port. Click a port number to display the Port Details screen (refer to Figure 24 on page 62).
Link	This field displays the speed (either 100M for 100Mbps or 1000M for 1000Mbps) and the duplex (F for full duplex or H for half duplex).
State	This field displays the STP (Spanning Tree Protocol) state of the port. See the chapter on STP for details on STP states.
LACP	This fields displays whether LACP (Link Aggregation Control Protocol) 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.

Table 6 Status (continued)

LABEL	DESCRIPTION
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.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking Set Interval .
Stop	Click Stop to halt system statistic polling.
Clear Counter	Select a port from the Port drop-down list box and then click Clear Counter to erase the recorded statistical information for that port.

6.2.1 Status: 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 24 Status: Port Details

Port Details		Status
Port Info	Port NO.	22
	Link	100M/F
	Status	FORWARDING
	LACP	Disabled
	TxPkts	1468
	RxPkts	1104
	Errors	0
	Tx KBs/s	0.0
	Rx KBs/s	0.0
	Up Time	0:25:45
TX Packet	TX Packets	1468
	Multicast	0
	Broadcast	1
	Pause	0
RX Packet	RX Packets	1104
	Multicast	0
	Broadcast	32
	Pause	0
	Giant	0
TX Collision	Single	0
	Multiple	0
	Excessive	0
	Late	0
Error Packet	RX CRC	0
	Length	0
	Runt	0
RX Packet	64	841
	65 to 127	30
	128 to 255	4
	256 to 511	240
	512 to 1023	0
	1024 to 1518	0
Poll Interval(s) <input type="text" value="40"/> <input type="button" value="Set Interval"/> <input type="button" value="Stop"/>		

The following table describes the labels in this screen.

Table 7 Status: Port Details

LABEL	DESCRIPTION
Port Info	
Port NO.	This field identifies the Ethernet port described in this screen.
Link	This field shows whether the Ethernet connection is down, and the speed/duplex mode.
Status	This field shows the training state of the ports. The states are FORWARDING (forwarding), which means the link is functioning normally or STOP (the port is stopped to break a loop or duplicate path).
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 packets transmitted.	
TX Packets	This field shows the number of good packets (unicast, multicast and broadcast) transmitted.
Multicast	This field shows the number of good multicast packets transmitted.
Broadcast	This field shows the number of good broadcast packets transmitted.
Pause	This field shows the number of 802.3x Pause packets transmitted.
Rx Packet The following fields display detailed information about packets received.	
RX Packets	This field shows the number of good packets (unicast, multicast and broadcast) received.
Multicast	This field shows the number of good multicast packets received.
Broadcast	This field shows the number of good broadcast packets received.
Pause	This field shows the number of 802.3x Pause packets received.
Giant	This field shows the number of packets dropped because they were bigger than the maximum frame size.
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	
RX CRC	This field shows the number of packets 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 packets received that were too short (shorter than 64 octets), including the ones with CRC errors.
Rx Packet	
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.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking Set Interval .
Stop	Click Stop to stop port statistic polling.

CHAPTER 7

Basic Setting

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

7.1 Overview

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(s) and DNS (domain name server) for management purposes.

7.2 System Information

In the navigation panel, click **Basic Setting** and **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 25 System Info

System Info

System Name	GS-2024
ZyNOS F/W Version	V3.60(LT.0)b0 04/29/2005
Ethernet Address	00:a0:c5:01:23:46

Hardware Monitor
Temperature Unit | C ▾

Temperature(C)	Current	MAX	MIN	Threshold	Status
MAC	36.0	36.0	35.5	65.0	Normal
CPU	32.0	33.0	32.0	65.0	Normal
PHY	32.5	32.5	32.0	65.0	Normal

FAN Speed (RPM)	Current	MAX	MIN	Threshold	Status
FAN1	5810	5859	5763	4500	Normal
FAN2	6061	6114	6009	4500	Normal

Voltage (V)	Current	MAX	MIN	Threshold	Status
2.5	2.544	2.544	2.544	+/- 5%	Normal
1.2	1.232	1.232	1.232	+/- 10%	Normal
3.3	3.376	3.392	3.376	+/- 5%	Normal
12	12.099	12.099	12.099	+/- 10%	Normal
1.3	1.312	1.312	1.312	+/- 10%	Normal
1.8	1.904	1.904	1.888	+/- 10%	Normal

Poll Interval(s)

The following table describes the labels in this screen.

Table 8 System Info

LABEL	DESCRIPTION
System Name	This field displays the descriptive name of the switch for identification purposes.
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.

Table 8 System Info (continued)

LABEL	DESCRIPTION
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).
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). "<41" is displayed for speeds too small to measure (under 2000 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.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking Set Interval .
Stop	Click Stop to halt statistic polling.

7.3 General Setup

Click **Basic Setting** and **General Setup** in the navigation panel to display the screen as shown.

Figure 26 General Setup

General Setup

System Name: GS-2024

Location: [Empty]

Contact Person's Name: [Empty]

Login Precedence: Local Only

Use Time Server when Bootup: None

Time Server IP Address: 0.0.0.0

Current Time: 00 : 51 : 12

New Time (hh:mm:ss): 00 : 51 : 12

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 32 printable characters; spaces are allowed.
Location	Enter the geographic location of your switch. You can use up to 32 printable ASCII characters; spaces are allowed.
Contact Person's Name	Enter the name of the person in charge of this switch. You can use up to 32 printable ASCII characters; spaces are not allowed.
Login Precedence	<p>Use this drop-down list box to select which database the switch should use (first) to authenticate an administrator (user for switch management).</p> <p>Configure the local user accounts in the Access Control Logins screen. The RADIUS is an external server. 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 administrator accounts configured in the Access Control Logins screen.</p> <p>Select Local then RADIUS to have the switch check the administrator 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 Port Authentication Radius 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>

Table 9 General Setup (continued)

LABEL	DESCRIPTION
Use Time Server when Bootup	<p>Enter the time service protocol that your timeserver uses. Not all time servers 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 the settings.
Cancel	Click Cancel to reset the fields to your previous configuration.

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: VLAN is unidirectional; it only governs outgoing traffic.

See [Chapter 8 on page 77](#) 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 to 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 VLAN.

Figure 27 Switch Setup

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 Chapter 8 on page 77 for more information.
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.	

Table 10 Switch Setup (continued)

LABEL	DESCRIPTION
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 Time 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.
<p>Priority Queue Assignment</p> <p>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 the next two fields to configure the priority level-to-physical queue mapping.</p> <p>The switch has four physical queues that you can map to the 8 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.</p>	
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.
Level 0	Typically used for best-effort traffic.
Apply	Click Apply to save the settings.
Cancel	Click Cancel to reset the fields to your previous configuration.

7.6 IP Setup

Use the **IP Setup** screen to configure the default gateway device, the default domain name server and add switch IP address.

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).

Note: You must configure a VLAN first.

Figure 28 IP Setup

IP Setup

Domain Name Server

Default Management In-band Out-of-band

In-band Management IP Address DHCP Client Static IP Address

IP Address

IP Subnet Mask

Default Gateway

VID

Out-of-band Management IP Address DHCP Client Static IP Address

IP Address

IP Subnet Mask

Default Gateway

In-band IP Addresses

IP Address	<input style="width: 100%;" type="text" value="0.0.0.0"/>
IP Subnet Mask	<input style="width: 100%;" type="text" value="0.0.0.0"/>
VID	<input style="width: 100%;" type="text"/>
Default Gateway	<input style="width: 100%;" type="text" value="0.0.0.0"/>

Index	IP Address	IP Subnet Mask	VID	Default Gateway	Delete

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	
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. VID 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 switch.
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 192.168.0.254.
Apply	Click Apply to save your changes back to the switch.
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.

Table 11 IP Setup (continued)

LABEL	DESCRIPTION
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 save the new rule to the switch. It then displays in the summary table at the bottom of the screen.
Cancel	Click Cancel to reset the fields to your previous configuration.
Index	This field displays the index number of an entry.
IP Address	This field displays the IP address.
Subnet Mask	This field displays the subnet mask.
VID	This field displays the VLAN identification number of the network.
Default Gateway	This field displays the the IP address of the default outgoing gateway.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the Delete check boxes.

7.7 Port Setup

Click **Basic Setting** and then **Port Setup** in the navigation panel to enter the port configuration screen.

Figure 29 Port Setup

Port	Active	Name	Type	Speed / Duplex	Flow Control	802.1p Priority	Jumbo Frame
1	<input checked="" type="checkbox"/>	port01	100/1000M	Auto	<input type="checkbox"/>	0	<input type="checkbox"/>
2	<input checked="" type="checkbox"/>	port02	100/1000M	Auto	<input type="checkbox"/>	0	<input type="checkbox"/>
3	<input checked="" type="checkbox"/>	port03	100/1000M	Auto	<input type="checkbox"/>	0	<input type="checkbox"/>
4	<input checked="" type="checkbox"/>	port04	100/1000M	Auto	<input type="checkbox"/>	0	<input type="checkbox"/>
5	<input checked="" type="checkbox"/>	port05	100/1000M	Auto	<input type="checkbox"/>	0	<input type="checkbox"/>
6	<input checked="" type="checkbox"/>	port06	100/1000M	Auto	<input type="checkbox"/>	0	<input type="checkbox"/>
7	<input checked="" type="checkbox"/>	port07	100/1000M	Auto	<input type="checkbox"/>	0	<input type="checkbox"/>
8	<input checked="" type="checkbox"/>	port08	100/1000M	Auto	<input type="checkbox"/>	0	<input type="checkbox"/>
9	<input checked="" type="checkbox"/>	port09	100/1000M	Auto	<input type="checkbox"/>	0	<input type="checkbox"/>
10	<input checked="" type="checkbox"/>	port10	100/1000M	Auto	<input type="checkbox"/>	0	<input type="checkbox"/>
11	<input checked="" type="checkbox"/>	port11	100/1000M	Auto	<input type="checkbox"/>	0	<input type="checkbox"/>
12	<input checked="" type="checkbox"/>	port12	100/1000M	Auto	<input type="checkbox"/>	0	<input type="checkbox"/>
13	<input checked="" type="checkbox"/>	port13	100/1000M	Auto	<input type="checkbox"/>	0	<input type="checkbox"/>
14	<input checked="" type="checkbox"/>	port14	100/1000M	Auto	<input type="checkbox"/>	0	<input type="checkbox"/>
15	<input checked="" type="checkbox"/>	port15	100/1000M	Auto	<input type="checkbox"/>	0	<input type="checkbox"/>
16	<input checked="" type="checkbox"/>	port16	100/1000M	Auto	<input type="checkbox"/>	0	<input type="checkbox"/>
17	<input checked="" type="checkbox"/>	port17	100/1000M	Auto	<input type="checkbox"/>	0	<input type="checkbox"/>
18	<input checked="" type="checkbox"/>	port18	100/1000M	Auto	<input type="checkbox"/>	0	<input type="checkbox"/>
19	<input checked="" type="checkbox"/>	port19	100/1000M	Auto	<input type="checkbox"/>	0	<input type="checkbox"/>
20	<input checked="" type="checkbox"/>	port20	100/1000M	Auto	<input type="checkbox"/>	0	<input type="checkbox"/>
21	<input checked="" type="checkbox"/>	port21	100/1000M	Auto	<input type="checkbox"/>	0	<input type="checkbox"/>
22	<input checked="" type="checkbox"/>	port22	100/1000M	Auto	<input type="checkbox"/>	0	<input type="checkbox"/>
23	<input checked="" type="checkbox"/>	port23	100/1000M	Auto	<input type="checkbox"/>	0	<input type="checkbox"/>
24	<input checked="" type="checkbox"/>	port24	100/1000M	Auto	<input type="checkbox"/>	0	<input type="checkbox"/>

Apply Cancel

The following table describes the labels in this screen.

Table 12 Port Setup

LABEL	DESCRIPTION
Port	This is the port index number.
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.
Name	Enter a descriptive name that identifies this port.
Type	This field displays 100/1000M for this connection.

Table 12 Port Setup (continued)

LABEL	DESCRIPTION
Speed/Duplex	<p>Select the speed and the duplex mode of the connection on this port.</p> <p>Choices are Auto, 10M/Half Duplex, 10M/Full Duplex, 100M/Half Duplex, 100M/Full Duplex or 1000M/Full Duplex.</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 Flow Control to enable it.</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 Table 10 on page 70 for more information.</p>
Jumbo Frame	<p>Jumbo frames are used to forward non-standard packet sizes on your network. These frames can deliver frames of up to 9216 bytes instead of standard Ethernet frames of 1522 bytes. Fewer packets are required for large data transfer, improving traffic throughput on the port.</p> <p>Select this option to allow a port to send and receive jumbo frames.</p> <p>Note: The peer device must also support non-standard packet traffic.</p>
Apply	<p>Click Apply to save the settings.</p>
Cancel	<p>Click Cancel to reset the fields to your previous configuration.</p>

CHAPTER 8

VLAN

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.

8.1 Introduction to IEEE 802.1Q Tagged VLAN

A 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 (2¹²) 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	User Priority	CFI	VLAN ID
2 Bytes	3 Bits	1 Bit	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.

8.2 Automatic VLAN Registration

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

8.2.1 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.

8.2.1.1 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.

8.2.2 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 VLAN don't tag all outgoing frames transmitted.

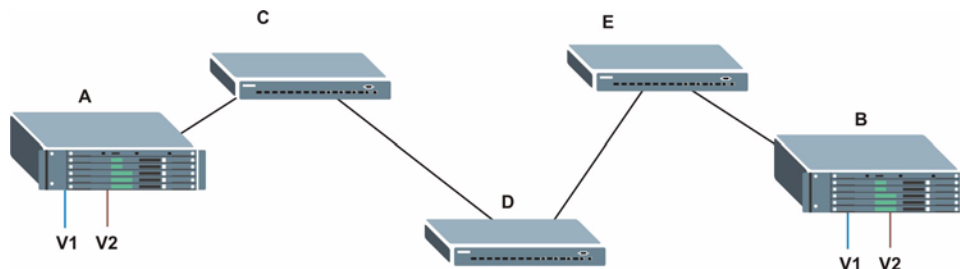
Table 13 IEEE 802.1Q VLAN Terminology (continued)

VLAN PARAMETER	TERM	DESCRIPTION
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

8.3 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 30 Port VLAN Trunking

8.4 Select the VLAN Type

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

Figure 31 Switch Setup: Select VLAN Type



8.5 Static VLAN

Use a static VLAN to decide whether an incoming frame on a port should be

- sent to a VLAN group as normal depends on its VLAN tag.
- sent to a group whether it has a VLAN tag or not.
- blocked from a VLAN group regardless of its VLAN tag.

You can also tag all outgoing frames (that were previously untagged) from a port with the specified VID.

8.5.1 Static VLAN Status

Click **Advanced Application**, **VLAN** from the navigation panel to display the **VLAN Status** screen as shown next.

Figure 32 VLAN: VLAN Status

The screenshot shows the 'VLAN Status' page. At the top, it says 'The Number Of VLAN = 1'. There are two links: 'VLAN Port Setting' and 'Static VLAN'. Below is a table with columns for Index, VID, Port Number (2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24), Elapsed Time, and Status. The table shows one VLAN with Index 1, VID 1, and all ports in 'U' (Up) status. The elapsed time is 1:05:48 and the status is 'Static'. At the bottom, there are controls for 'Poll Interval(s)' (set to 40), 'Set Interval', 'Stop', 'Change Pages', 'Previous Page', and 'Next Page'.

Index	VID	Port Number												Elapsed Time	Status	
		2	4	6	8	10	12	14	16	18	20	22	24			
1	1	U	U	U	U	U	U	U	U	U	U	U	U	U	1:05:48	Static

The following table describes the labels in this screen.

Table 14 VLAN: 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 that was configured in the Static VLAN screen.
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 are 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; dynamically using GVRP or statically, that is, added as a permanent entry.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking Set Interval .
Stop	Click Stop to halt polling statistics.
Change Pages	Click Previous Page or Next Page to show the previous/next screen if all status information cannot be seen in one screen.

8.5.2 Configure a Static VLAN

To configure a static VLAN, click **Static VLAN** in the **VLAN Status** screen to display the screen as shown next.

Figure 33 VLAN: Static VLAN

Static VLAN
VLAN Status

ACTIVE

Name

VLAN Group ID

Port	Control			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
13	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
14	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
15	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
16	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
17	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
18	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
19	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
20	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
21	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
22	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
23	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
24	<input checked="" type="radio"/> Normal	<input type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging

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

The following table describes the related labels in this screen.

Table 15 VLAN: Static VLAN

LABEL	DESCRIPTION
ACTIVE	Select this check box to activate the VLAN settings.
Name	Enter a descriptive name for the VLAN group for identification purposes.
VLAN Group ID	Enter the VLAN ID for this static entry; the valid range is between 1 and 4094.
Port	The port number identifies the port you are configuring.
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.
Add	Click Add to add the settings as a new entry in the summary table below.
Cancel	Click Cancel to reset the fields.
Clear	Click Clear to start configuring the screen again.
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	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the Delete check boxes.

8.5.3 Configure VLAN Port Settings

To configure the VLAN settings on a port, click the **VLAN Port Setting** link in the **VLAN Status** screen.

Figure 34 VLAN: VLAN Port Setting

Port	Ingress Check	PVID	GVRP	Acceptable Frame Type	VLAN Trunking
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"/>
13	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
14	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
15	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
16	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
17	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
18	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
19	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
20	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
21	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
22	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
23	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
24	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>

Apply Cancel

The following table describes the labels in this screen.

Table 16 VLAN: VLAN Port Setting

LABEL	DESCRIPTION
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. Select this check box to permit VLAN groups beyond the local switch.
Port	This field displays the port number.
Ingress Check	Select this check box to activate ingress filtering. Clear this check box to disable ingress filtering.
PVID	Enter a number between 1 and 4094 as the port VLAN ID.
GVRP	Select this check box to allow GVRP on this port.

Table 16 VLAN: VLAN Port Setting (continued)

LABEL	DESCRIPTION
Acceptable Frame Type	Specify the type of frames allowed on a port. Choices are All , Tag Only and Untag Only . Select All from the drop-down list box to accept all 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 will be dropped. Select Untag Only to accept only untagged frames on this port. All tagged frames will be 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 the changes
Cancel	Click Cancel to start configuring the screen again.

8.6 Port-based VLAN Setup

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.

Note: 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.

8.6.1 Configure a Port-based VLAN

Select **Port Based** as the **VLAN Type** in the **Switch Setup** screen (see [Figure 31 on page 80](#)) and then click **VLAN** from the navigation panel to display the next screen.

Figure 35 Port Based VLAN Setup (All Connected)

Port Based VLAN Setup

Setting Wizard
All connected ▾
Apply

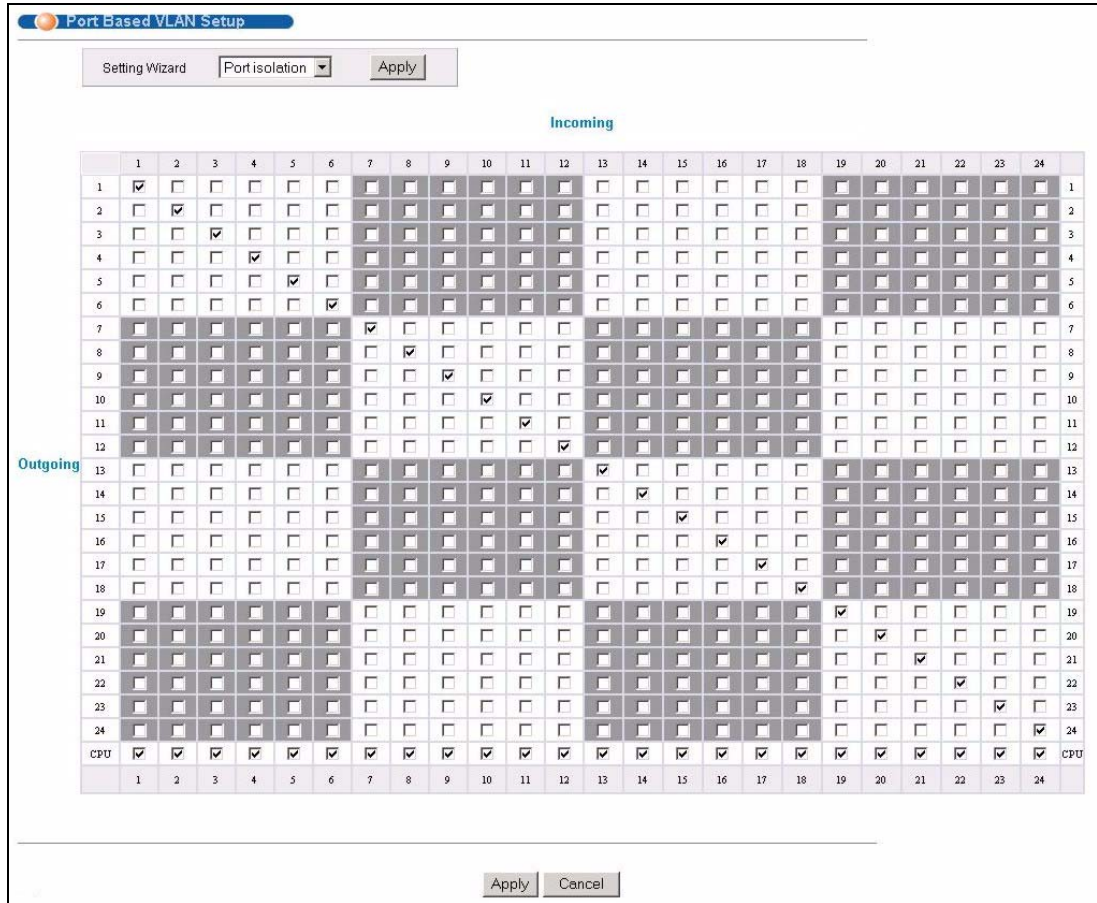
Incoming

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	
1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	1
2	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	2
3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	3
4	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	4
5	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	5
6	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	6
7	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	7
8	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	8
9	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	9
10	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	10
11	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	11
12	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	12
13	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	13
14	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	14
15	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	15
16	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	16
17	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	17
18	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	18
19	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	19
20	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	20
21	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	21
22	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	22
23	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	23
24	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	24
CPU	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	CPU

Outgoing

Apply Cancel

Figure 36 Port Based VLAN Setup (Port Isolation)



The following table describes the labels in this screen.

Table 17 Port Based VLAN Setup

LABEL	DESCRIPTION
Setting Wizard	<p>Choose 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. 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. 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 Ethernet ports. If it does not form a VLAN with a particular port then the switch cannot be managed from that port.</p>

Table 17 Port Based VLAN Setup (continued)

LABEL	DESCRIPTION
Outgoing	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 Ethernet ports. If it does not form a VLAN with a particular port then the switch cannot be managed from that port.
Apply	Click Apply to save the changes.
Cancel	Click Cancel to start configuring the screen again.

CHAPTER 9

Static MAC Forwarding

Use these screens to configure static MAC address forwarding.

9.1 Overview

A static MAC address entry is an address that has been manually entered in the MAC address learning 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. Devices that match static MAC address rules on a port can only receive traffic on that port and cannot receive traffic on other ports. This may reduce unicast flooding.

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 16 on page 121](#) for more information on port security.

9.2 Configuring Static MAC Forwarding

Click **Advanced Applications, Static MAC Forwarding** in the navigation panel to display the configuration screen as shown.

Figure 37 Static MAC Forwarding

The following table describes the labels in this screen.

Table 18 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	Select a port where the MAC address entered in the previous field will be automatically forwarded.
Add	After you set the fields above, click Add to insert a new rule.
Cancel	Click Cancel to reset the fields.
Clear	Click Clear to begin configuring this screen afresh.
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 and 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 18 Static MAC Forwarding (continued)

LABEL	DESCRIPTION
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the Delete check boxes.

CHAPTER 10

Spanning Tree Protocol

This chapter introduces the Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP).

10.1 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 allow 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.

10.1.1 STP Terminology

The root bridge is the base of the spanning tree; it is the bridge with the lowest identifier value (MAC address).

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 19 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.

10.1.2 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.

10.1.3 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 20 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.

10.2 STP Status

Click **Advanced Application, Spanning Tree Protocol** in the navigation panel to display the status screen as shown next.

Figure 38 Spanning Tree Protocol: Status

Spanning Tree Protocol Status [Configuration](#)

Spanning Tree Protocol : Running

Bridge	Root	Our Bridge
Bridge ID	8000-00a0c5012346	8000-00a0c5012346
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		0:01:04

Polling Interval

The following table describes the labels in this screen.

Table 21 Spanning Tree Protocol: Status

LABEL	DESCRIPTION
Spanning Tree Protocol	This field displays Running if STP is activated. Otherwise, it displays Down .
Configuration	Click Configuration to configure STP settings. Refer to Section 10.3 on page 96 .
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.

Table 21 Spanning Tree Protocol: Status (continued)

LABEL	DESCRIPTION
Polling Interval	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking Set Interval .
Stop	Click Stop to halt STP statistic polling.

10.3 Configure STP

To configure STP, click the **Configuration** link in the **Spanning Tree Protocol** screen as shown next.

Figure 39 Spanning Tree Protocol: Configuration

Spanning Tree Protocol
Status

Active	<input checked="" type="checkbox"/>	
Bridge Priority		32768 ▾
Hello Time		2 Seconds
Max Age		20 Seconds
Forwarding Delay		15 Seconds

Port	Active	Priority	Path Cost
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
13	<input type="checkbox"/>	128	4
14	<input type="checkbox"/>	128	4
15	<input type="checkbox"/>	128	4
16	<input type="checkbox"/>	128	4
17	<input type="checkbox"/>	128	4
18	<input type="checkbox"/>	128	4
19	<input type="checkbox"/>	128	4
20	<input type="checkbox"/>	128	4
21	<input type="checkbox"/>	128	4
22	<input type="checkbox"/>	128	4
23	<input type="checkbox"/>	128	4
24	<input type="checkbox"/>	128	4

The following table describes the labels in this screen.

Table 22 Spanning Tree Protocol: Configuration

LABEL	DESCRIPTION
Status	Click Status to display the Spanning Tree Protocol Status screen (see Figure 38 on page 95).
Active	Select this check box to activate STP. Clear this checkbox to disable STP.
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.
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> $2 * (\text{Forward Delay} - 1) \geq \text{Max Age} \geq 2 * (\text{Hello Time} + 1)$
Port	This field displays the port number.
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	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 19 on page 93 for more information.
Apply	Click Apply to save your changes back to the switch.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 11

Bandwidth Control

This chapter shows you how you can cap the maximum bandwidth using the **Bandwidth Control** screen.

11.1 Bandwidth Control Setup

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

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

Figure 40 Bandwidth Control

Port	Active	Ingress Rate	Scheme
1	<input type="checkbox"/>	64K bps	Drop
2	<input type="checkbox"/>	64K bps	Drop
3	<input type="checkbox"/>	64K bps	Drop
4	<input type="checkbox"/>	64K bps	Drop
5	<input type="checkbox"/>	64K bps	Drop
6	<input type="checkbox"/>	64K bps	Drop
7	<input type="checkbox"/>	64K bps	Drop
8	<input type="checkbox"/>	64K bps	Drop
9	<input type="checkbox"/>	64K bps	Drop
10	<input type="checkbox"/>	64K bps	Drop
11	<input type="checkbox"/>	64K bps	Drop
12	<input type="checkbox"/>	64K bps	Drop
13	<input type="checkbox"/>	64K bps	Drop
14	<input type="checkbox"/>	64K bps	Drop
15	<input type="checkbox"/>	64K bps	Drop
16	<input type="checkbox"/>	64K bps	Drop
17	<input type="checkbox"/>	64K bps	Drop
18	<input type="checkbox"/>	64K bps	Drop
19	<input type="checkbox"/>	64K bps	Drop
20	<input type="checkbox"/>	64K bps	Drop
21	<input type="checkbox"/>	64K bps	Drop
22	<input type="checkbox"/>	64K bps	Drop
23	<input type="checkbox"/>	64K bps	Drop
24	<input type="checkbox"/>	64K bps	Drop

Apply Cancel

The following table describes the related labels in this screen.

Table 23 Bandwidth Control

LABEL	DESCRIPTION
Active	Select this check box to enable bandwidth control on the switch.
Port	This field displays the port number.
Active	Make sure to select this check box to activate bandwidth control on a port.
Ingress Rate	Specify the maximum bandwidth allowed in Kilobits per second (Kbps) for the incoming traffic flow on a port. Select a number from the drop-down list box.

Table 23 Bandwidth Control (continued)

LABEL	DESCRIPTION
Scheme	<p>Select Drop (default) from the drop-down list box to discard all incoming packets that are over the maximum allowable bandwidth on a port.</p> <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.</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>
Apply	Click Apply to save the settings.
Cancel	Click Cancel to reset the fields to your previous configuration.

CHAPTER 12

Broadcast Storm Control

This chapter introduces and shows you how to configure the broadcast storm control feature.

12.1 Overview

Broadcast storm control limits the number of broadcast frames that can be stored in the switch buffer or sent out from the switch. Broadcast frames that arrive when the buffer is full are discarded. Enable this feature to reduce broadcast traffic coming into your network.

12.2 Broadcast Storm Control Setup

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

Figure 41 Broadcast Storm Control

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

The following table describes the labels in this screen.

Table 24 Broadcast Storm Control

LABEL	DESCRIPTION
Active	Select this check box to enable broadcast storm control on the switch. Clear this check box to disable the feature.
Storm Control Type	Select Broadcast Only , Broadcast and multicast , Broadcast and unknown unicast or Broadcast, multicast and unknown unicast from the drop-down list box.
Packet Limit	Select from the drop-down list box, how many packets a port receives per second based on the chosen storm control type.
Port	This field displays a port number.

Table 24 Broadcast Storm Control (continued)

LABEL	DESCRIPTION
Active	Select this check box to enable broadcast storm control on a port. Clear this check box to disable the feature.
Apply	Click Apply to save your changes back to the switch.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 13

Mirroring

This chapter discusses the Mirror setup screens.

13.1 Overview

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

13.2 Port Mirroring Setup

Click **Advanced Application, Mirroring** in the navigation panel to display the **Mirroring** screen. Use this screen to select a mirror port and specify the traffic flow to be copied to the mirror port.

Figure 42 Mirroring

The following table describes the labels in this screen.

Table 25 Mirroring

LABEL	DESCRIPTION
Active	Select this check box to activate port mirroring on the switch. Clear this check box to disable the feature.
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 a port from the drop-down list box.
Direction	Specify the direction of the traffic to mirror by selecting from the drop-down list box. Choices are Egress (outgoing), Ingress (incoming) and Both .
Mirrored Port	Select a port from the drop-down list box. Select this option to mirror the traffic on a port.

Table 25 Mirroring (continued)

LABEL	DESCRIPTION
Apply	Click Apply to save the changes.
Cancel	Click Cancel to start configuring the screen again.

CHAPTER 14

Link Aggregation

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

14.1 Overview

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.

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.

14.2 Dynamic Link Aggregation

The switch adheres to the IEEE 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. LACP also allows port redundancy, that is, if an operational port fails, then one of the “standby” ports become operational without user intervention. 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.

14.2.1 Link Aggregation ID

LACP aggregation ID consists of the following information¹:

Table 26 Link Aggregation ID: Local Switch

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

Table 27 Link Aggregation ID: Peer Switch

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

14.3 Link Aggregation Status

Click **Advanced Application**, **Link Aggregation** in the navigation panel. The **Link Aggregation Control Protocol Status** screen displays by default.

Figure 43 Link Aggregation Control 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)]	-	-

Polling Interval(s)

1. Port Priority and Port Number are 0 as it is the aggregator ID for the trunk group, not the individual port.

The following table describes the labels in this screen.

Table 28 Link Aggregation Control 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	Refer to Section 14.2.1 on page 110 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.
Polling Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking Set Interval .
Stop	Click Stop to halt statistic polling.

14.4 Link Aggregation Setup

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

Figure 44 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"/>

Port	Group	LACP Timeout
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
13	None ▾	30 ▾ seconds
14	None ▾	30 ▾ seconds
15	None ▾	30 ▾ seconds
16	None ▾	30 ▾ seconds
17	None ▾	30 ▾ seconds
18	None ▾	30 ▾ seconds
19	None ▾	30 ▾ seconds
20	None ▾	30 ▾ seconds
21	None ▾	30 ▾ seconds
22	None ▾	30 ▾ seconds
23	None ▾	30 ▾ seconds
24	None ▾	30 ▾ seconds

The following table describes the labels in this screen.

Table 29 Link Aggregation Control Protocol: Configuration

LABEL	DESCRIPTION
Link Aggregation Control Protocol	
Active	Select this checkbox to enable Link Aggregation Control Protocol (LACP).
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.
Group	Select the trunk group to which a port belongs.
LACP Timeout	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. Select either 1 second or 30 seconds.
Apply	Click Apply to save your changes back to the switch.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 15

Port Authentication

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

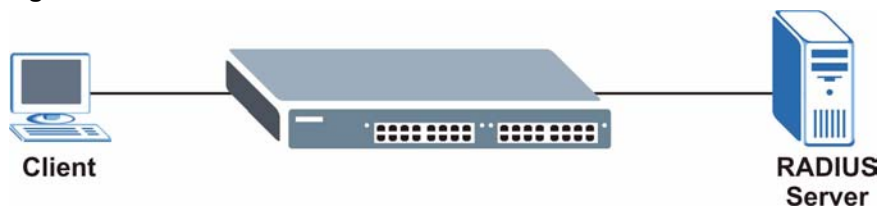
15.1 Overview

IEEE 802.1x is an extended authentication protocol² that allows support of RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.

15.1.1 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 45 RADIUS Server



15.2 Port Authentication Configuration

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

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

-
2. At the time of writing, only Windows XP of the Microsoft operating systems supports it. 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.

Figure 46 Port Authentication



15.2.1 Activate IEEE 802.1x Security

From the **Port Authentication** screen, display the configuration screen as shown.

Figure 47 Port Authentication: 802.1x

802.1x
Port Authentication

Active

Port	Active	Reauthentication	Reauthentication Timer
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
13	<input type="checkbox"/>	On ▼	3600 seconds
14	<input type="checkbox"/>	On ▼	3600 seconds
15	<input type="checkbox"/>	On ▼	3600 seconds
16	<input type="checkbox"/>	On ▼	3600 seconds
17	<input type="checkbox"/>	On ▼	3600 seconds
18	<input type="checkbox"/>	On ▼	3600 seconds
19	<input type="checkbox"/>	On ▼	3600 seconds
20	<input type="checkbox"/>	On ▼	3600 seconds
21	<input type="checkbox"/>	On ▼	3600 seconds
22	<input type="checkbox"/>	On ▼	3600 seconds
23	<input type="checkbox"/>	On ▼	3600 seconds
24	<input type="checkbox"/>	On ▼	3600 seconds

The following table describes the labels in this screen.

Table 30 Port Authentication: 802.1x

LABEL	DESCRIPTION
Active	Select this check box to permit 802.1x authentication on the switch. Note: You must first enable 802.1x authentication on the switch before configuring it on each port.
Port	This field displays a port number.
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.
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 back to the switch.
Cancel	Click Cancel to begin configuring this screen afresh.

15.2.2 Configuring RADIUS Server Settings

From the **Port Authentication** screen, click **RADIUS** to display the configuration screen as shown.

Figure 48 Port Authentication: RADIUS

The screenshot shows a configuration window for a RADIUS Authentication Server. The window title is 'RADIUS' and 'Port Authentication'. The main content area is titled 'Authentication Server' and contains three input fields: 'IP Address' with the value '0.0.0.0', 'UDP Port' with the value '1812', and 'Shared Secret' with the value '1234'. At the bottom of the window, there are two buttons: 'Apply' and 'Cancel'.

The following table describes the labels in this screen.

Table 31 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.

Table 31 Port Authentication: RADIUS (continued)

LABEL	DESCRIPTION
Apply	Click Apply to save your changes back to the switch.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 16

Port Security

This chapter shows you how to set up port security.

16.1 Overview

Port security allows only packets with configured static MAC addresses to pass through a port on the switch.

For maximum port security, enable this feature and configure static MAC address(es) for a port.

16.2 Port Security Setup

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

Figure 49 Port Security

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

The following table describes the labels in this screen.

Table 32 Port Security

LABEL	DESCRIPTION
Active	Select this option to enable port security on the switch.
Port	This field displays a port number.
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.
Apply	Click Apply to save your changes back to the switch.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 17

Queuing Method

This chapter introduces the queuing methods supported.

17.1 Overview

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.

Table 33 Physical Queue Priority

QUEUE	PRIORITY
Q3	4 (highest)
Q2	3
Q1	2
Q0	1 (lowest)

17.1.1 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, Q3 is transmitted first. When that queue empties, traffic on the next highest-priority queue, Q2 is transmitted until Q2 empties, and then traffic is transmitted on Q1 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.

17.1.2 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 queue **Weight** field) 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.

17.2 Configuring Queuing

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

Figure 50 Queuing Method

The following table describes the labels in this screen.

Table 34 Queuing Method

LABEL	DESCRIPTION
Method	Select Strictly Priority or 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. Q3 has the highest priority and Q0 the lowest. The default queuing method is Strictly Priority . Weighted Round Robin Scheduling (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 Weighted Round Robin Scheduling , use the drop-down list boxes to choose queue weights (1-15). Bandwidth is divided across the different traffic queues according to their weights.
Apply	Click Apply to save your changes back to the switch.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 18

Multicast

This chapter shows you how to configure various multicast features.

18.1 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.

18.1.1 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).

18.1.2 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.

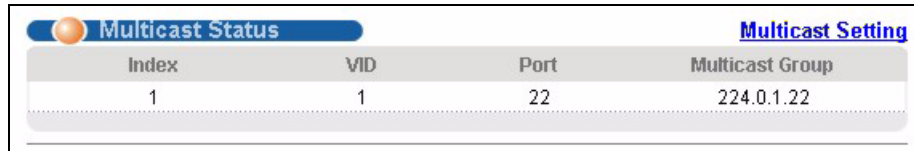
18.1.3 IGMP Snooping

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.

18.2 Multicast Status

Click **Advanced Applications** and **Multicast** to display the screen as shown. This screen shows the multicast group information.



Index	VID	Port	Multicast Group
1	1	22	224.0.1.22

The following table describes the labels in this screen.

Table 35 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.

18.3 Multicast Setup

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

Figure 51 Multicast Setting

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

IGMP Snooping Active

IGMP Filtering Active

Unknown Multicast Frame Flooding Drop

Port	Immed. Leave	Group Limited	Max Group Num.	IGMP Filtering Profile
1	<input type="checkbox"/>	<input type="checkbox"/>	0	Default ▾
2	<input type="checkbox"/>	<input type="checkbox"/>	0	Default ▾
3	<input type="checkbox"/>	<input type="checkbox"/>	0	Default ▾
4	<input type="checkbox"/>	<input type="checkbox"/>	0	Default ▾
5	<input type="checkbox"/>	<input type="checkbox"/>	0	Default ▾
6	<input type="checkbox"/>	<input type="checkbox"/>	0	Default ▾
7	<input type="checkbox"/>	<input type="checkbox"/>	0	Default ▾
8	<input type="checkbox"/>	<input type="checkbox"/>	0	Default ▾
9	<input type="checkbox"/>	<input type="checkbox"/>	0	Default ▾
10	<input type="checkbox"/>	<input type="checkbox"/>	0	Default ▾
11	<input type="checkbox"/>	<input type="checkbox"/>	0	Default ▾
12	<input type="checkbox"/>	<input type="checkbox"/>	0	Default ▾
13	<input type="checkbox"/>	<input type="checkbox"/>	0	Default ▾
14	<input type="checkbox"/>	<input type="checkbox"/>	0	Default ▾
15	<input type="checkbox"/>	<input type="checkbox"/>	0	Default ▾
16	<input type="checkbox"/>	<input type="checkbox"/>	0	Default ▾
17	<input type="checkbox"/>	<input type="checkbox"/>	0	Default ▾
18	<input type="checkbox"/>	<input type="checkbox"/>	0	Default ▾
19	<input type="checkbox"/>	<input type="checkbox"/>	0	Default ▾
20	<input type="checkbox"/>	<input type="checkbox"/>	0	Default ▾
21	<input type="checkbox"/>	<input type="checkbox"/>	0	Default ▾
22	<input type="checkbox"/>	<input type="checkbox"/>	0	Default ▾
23	<input type="checkbox"/>	<input type="checkbox"/>	0	Default ▾
24	<input type="checkbox"/>	<input type="checkbox"/>	0	Default ▾

The following table describes the labels in this screen.

Table 36 Multicast Setting

LABEL	DESCRIPTION
IGMP Snooping	Select Active to enable IGMP snooping to forward group multicast traffic only to ports that are members of that group
IGMP Filtering	Select Active to enable IGMP filtering to control which IGMP groups a subscriber on a port can join.
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.
Port	This field displays the port number.

Table 36 Multicast Setting (continued)

LABEL	DESCRIPTION
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.
Apply	Click Apply to save your changes back to the switch.
Cancel	Click Cancel to begin configuring this screen afresh.

18.4 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 52 Multicast: IGMP Filtering Profile

The screenshot shows the 'IGMP Filtering Profile' configuration interface. At the top, there's a title bar with 'IGMP Filtering Profile' and a 'Multicast Setting' link. Below that, the 'Profile Setup' section contains three input fields: 'Profile Name', 'Start Address' (with '224.0.0.0' entered), and 'End Address' (with '224.0.0.0' entered). Underneath are 'Add' and 'Clear' buttons. A table below lists existing profiles. The first row is 'Default' with 'Start Address' '0.0.0.0' and 'End Address' '0.0.0.0'. The table has columns for 'Delete Profile' and 'Delete Rule', each with a checkbox. At the bottom of the form are 'Delete' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 37 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 settings to the switch.
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.
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.

18.5 MVR Overview

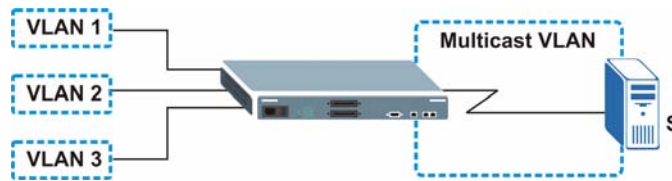
Multicast VLAN Registration (MVR) is designed for applications (such as Media-on-Demand (MoD)) that use multicast traffic across an Ethernet ring-based service provider network.

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 53 MVR Network Example



18.5.1 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.

18.5.2 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 through the source port(s) 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 through the source port(s). In this case, you must manually configure the forwarding settings on the multicast devices in the multicast VLAN.

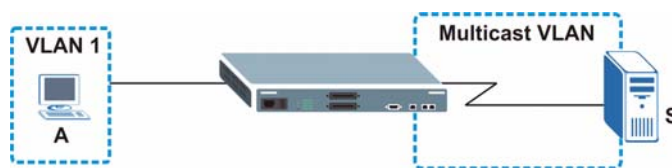
18.5.3 How MVR Works

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 54 MVR Multicast Television Example



18.6 General MVR Configuration

Use the **MVR** screen to create multicast VLANs and select the receiver port(s) and source port(s) 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.

Note: 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 55 MVR

The screenshot shows the MVR configuration page. At the top, there are three tabs: 'MVR' (selected), 'Multicast Setting', and 'Group Configuration'. Below the tabs are four configuration fields: 'Active' with a checkbox, 'Name' with a text input field, 'Multicast VLAN ID' with a text input field, and 'Mode' with two radio buttons: 'Dynamic' (selected) and 'Compatible'. Below these fields is a large table with 24 rows, one for each port. The columns are 'Port', 'Source Port', 'Receiver Port', 'None', and 'Tagging'. Each row contains radio buttons for 'Source Port', 'Receiver Port', and 'None', and a checkbox for 'Tagging'. At the bottom of the table are 'Add' and 'Cancel' buttons. Below the table is a table header with columns: 'VLAN', 'Active', 'Name', 'Mode', 'Source Port', 'Receiver Port', and 'Delete'. Below the header are 'Delete' and 'Cancel' buttons.

The following table describes the related labels in this screen.

Table 38 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.

Table 38 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.
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.
Receiver Port	Select this option to set this port as a receiver port that only receives multicast traffic.
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 the settings.
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, select the VLAN(s) that you want to remove in the Delete column, then click the Delete button.
Cancel	Click Cancel to clear the Delete check boxes.

18.7 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.

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

Figure 56 MVR: Group Configuration

The following table describes the labels in this screen.

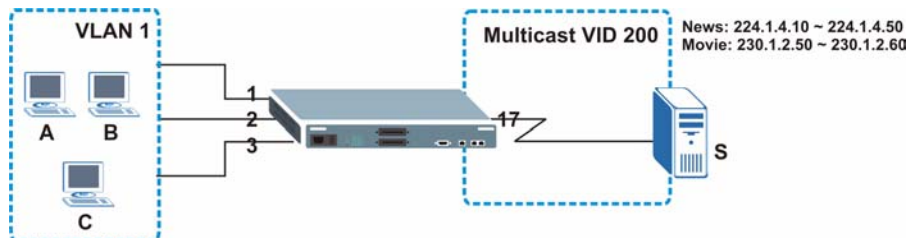
Table 39 MVR: Group Configuration

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 18.1.1 on page 125 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 18.1.1 on page 125 for more information on IP multicast addresses.
Add	Click Add to save the settings.
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.
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.

18.7.1 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 17 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 57 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 58 MVR Configuration Example

The screenshot displays the MVR configuration interface. At the top, there are two tabs: "Multicast Setting" (active) and "Group Configuration". The "Multicast Setting" tab contains the following fields:

- Active:
- Name: Premium
- Multicast VLAN ID: 200
- Mode: Dynamic Compatible

Below the settings is a table with 24 rows, each representing a port. The columns are: Port, Source Port, Receiver Port, None, and Tagging. The "Receiver Port" column has radio buttons, and the "Tagging" column has checkboxes. Red circles highlight the following rows:

- Port 1: Source Port (off), Receiver Port (on), None (off), Tagging (off)
- Port 2: Source Port (off), Receiver Port (on), None (off), Tagging (off)
- Port 3: Source Port (off), Receiver Port (on), None (off), Tagging (off)
- Port 17: Source Port (on), Receiver Port (off), None (off), Tagging (off)

At the bottom of the interface are "Add" and "Cancel" buttons.

Port	Source Port	Receiver Port	None	Tagging
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 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"/>
13	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
14	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
15	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
16	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
17	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>
18	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
19	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
20	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
21	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
22	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
23	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>
24	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>

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 59 MVR Group Configuration Example

The screenshot shows the 'Group Configuration' interface for MVR. At the top, the 'Multicast VLAN ID' is set to 200. Below this is a table for adding new groups. The table has three columns: 'Name', 'Start Address', and 'End Address'. A single row is present with 'News' in the Name column, '224.1.4.10' in the Start Address column, and '224.1.4.50' in the End Address column. This row is circled in red. Below the table are 'Add' and 'Cancel' buttons. At the bottom, there is a table for existing groups with columns: 'MVLAN', 'Name', 'Start Address', 'End Address', 'Delete All', and 'Delete Group'. The table contains one entry for MVLAN 200 with Name 'Movie', Start Address '230.1.2.50', and End Address '230.1.2.60'. Below this table are 'Delete' and 'Cancel' buttons.

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

Figure 60 MVR Group Configuration Example

The screenshot shows the 'Group Configuration' interface for MVR. At the top, the 'Multicast VLAN ID' is set to 200. Below this is a table for adding new groups. The table has three columns: 'Name', 'Start Address', and 'End Address'. A single row is present with empty fields for Name, '0.0.0.0' for Start Address, and '0.0.0.0' for End Address. Below the table are 'Add' and 'Cancel' buttons. At the bottom, there is a table for existing groups with columns: 'MVLAN', 'Name', 'Start Address', 'End Address', 'Delete All', and 'Delete Group'. The table contains two entries for MVLAN 200: 'Movie' (Start Address: 230.1.2.50, End Address: 230.1.2.60) and 'News' (Start Address: 224.1.4.10, End Address: 224.1.4.50). This table is circled in red. Below this table are 'Delete' and 'Cancel' buttons.

MVLAN	Name	Start Address	End Address	Delete All	Delete Group
200	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"/>

CHAPTER 19

Static Route

This chapter shows you how to configure static routes.

19.1 Configuring

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

Click **IP Application**, **Static Routing** in the navigation panel to display the screen as shown.

Figure 61 Static Routing

Index	Active	Name	Destination Address	Subnet Mask	Gateway Address	Metric	Delete
1	Yes	example	172.21.1.104	255.255.0.0	192.168.1.2	2	<input type="checkbox"/>

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

Table 40 Static Routing

LABEL	DESCRIPTION
Active	This field allows you to activate/deactivate this static route.
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.

Table 40 Static Routing (continued)

LABEL	DESCRIPTION
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.
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.
Cancel	Click Cancel to reset the above fields to your previous configuration.
Clear	Click Clear to set the above fields back to the factory defaults.
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 it is 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	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the Delete check boxes.

CHAPTER 20

Differentiated Services

This chapter shows you how to configure Differentiated Services (DiffServ) on the switch.

20.1 Overview

Quality of Service (QoS) mechanisms provide the best service on a per-flow guarantee. To fine-tune the levels of services on the priority of the traffic flow using QoS places a heavy burden on the network infrastructure.

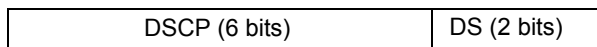
DiffServ is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. 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.

20.1.1 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.

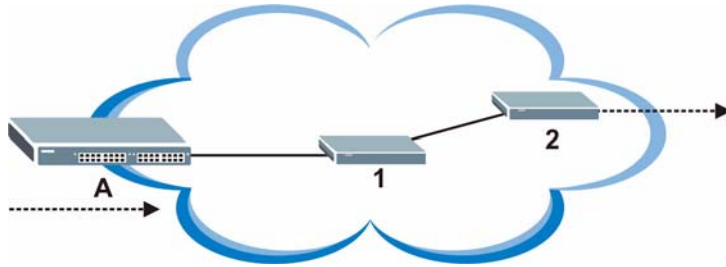
Figure 62 DiffServ: Differentiated Service Field



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 priorities of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

20.1.2 DiffServ Network Example

The following figure depicts a simple DiffServ network consisting of a group of contiguous DiffServ-compliant network devices.

Figure 63 DiffServ Network Example

Switch **A** marks traffic flowing into the network based on the configured marking rules. Intermediary network devices **1** and **2** allocate network resources (such as bandwidth) by mapping the DSCP values and the associated policies.

20.2 DSCP-to-IEEE802.1p Priority Mapping

You can configure the DSCP to IEEE802.1p mapping to allow the switch to prioritize all traffic based on the incoming DSCP value according to the DiffServ to IEEE802.1p mapping table.

The following table shows the default DSCP-to-IEEE802.1P mapping.

Table 41 Default DSCP-IEEE802.1p Mapping

DSCP VALUE	0 – 7	8 – 15	16 – 23	24 – 31	32 – 39	40 – 47	48 – 55	56 – 63
IEEE802.1P	0	1	2	3	4	5	6	7

20.3 Configuring DSCP Settings

Click **IP Application**, **DiffServ** in the navigation panel to display the screen as shown.

Figure 64 DiffServ

The following table describes the labels in this screen.

Table 42 DiffServ

LABEL	DESCRIPTION
Active	Select this option to activate DiffServ and apply IEEE802.1p priority mapping on the switch.
0 ... 63	This is the DSCP classification identification number. To set the IEEE802.1p priority mapping, select the priority level from the drop-down list box.
Apply	Click Apply to save the changes.
Cancel	Click Cancel to discard all changes and start configuring the screen again.

CHAPTER 21

Maintenance

This chapter explains how to configure the maintenance screens that let you maintain the firmware and configuration files.

21.1 The Maintenance Screen

Click **Management, Maintenance** in the navigation panel to open the following screen.

Figure 65 Maintenance



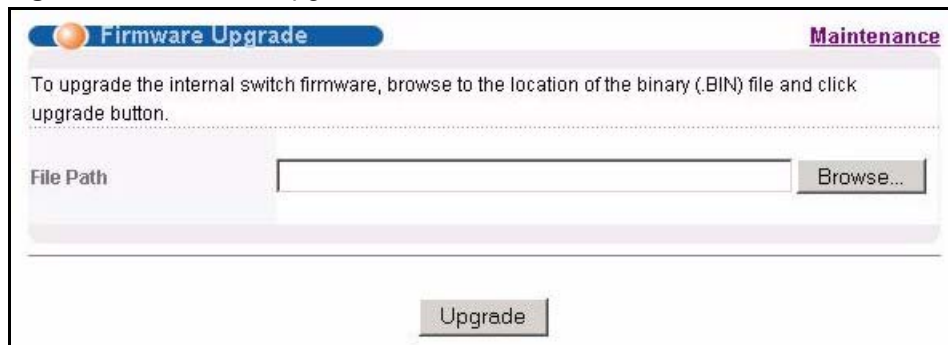
21.2 Firmware Upgrade

Make sure you have downloaded (and unzipped) the correct model firmware and version to your computer before uploading to the device.

Note: 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 66 Firmware Upgrade



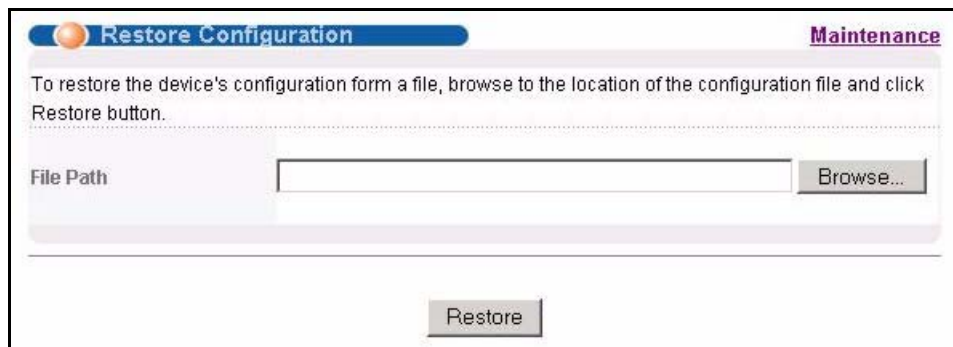
Type the path and file name of the firmware file you wish to upload to the switch in the **File Path** text box or click **Browse** to locate it. After you have specified the file, click **Upgrade**.

After the firmware upgrade process is complete, see the **System Info** screen to verify your current firmware version number.

21.3 Restore a Configuration File

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

Figure 67 Restore Configuration



The screenshot shows a web interface for restoring a configuration. At the top, there is a blue header with an orange circle icon, the text "Restore Configuration", and a "Maintenance" link. Below the header is a light purple box containing the instruction: "To restore the device's configuration from a file, browse to the location of the configuration file and click Restore button." Underneath this box is a "File Path" label, a text input field, and a "Browse..." button. At the bottom center of the page is a "Restore" button.

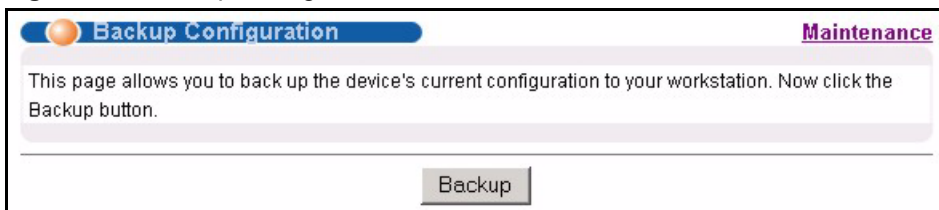
Type the path and file name of the configuration file you wish to restore in the **File Path** text box or click **Browse** to display the **Choose File** screen (below) from which you can locate it. After you have specified the file, click **Restore**. "config" is the name of the configuration file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

21.4 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 **Backup Configuration** screen.

Figure 68 Backup Configuration



The screenshot shows a web interface for backing up a configuration. At the top, there is a blue header with an orange circle icon, the text "Backup Configuration", and a "Maintenance" link. Below the header is a light purple box containing the instruction: "This page allows you to back up the device's current configuration to your workstation. Now click the Backup button." At the bottom center of the page is a "Backup" button.

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.

21.5 Load Factory Defaults

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

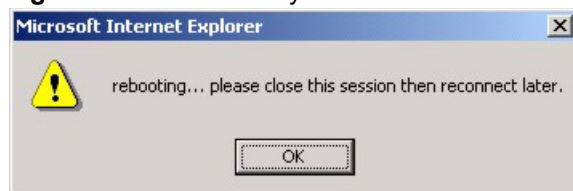
- 1 In the **Maintenance** screen, click the **Click Here** button next to **Load Factory Defaults** to clear all switch configuration information you configured and return to the factory defaults. The following message appears.

Figure 69 Load Factory Default: Conformation



- 2 Click **OK** to display the screen shown next.

Figure 70 Load Factory Default: Start



- 3 Click **OK** to begin resetting all switch configurations to the factory defaults and then wait for the switch to restart. This takes up to two minutes. If you want 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).

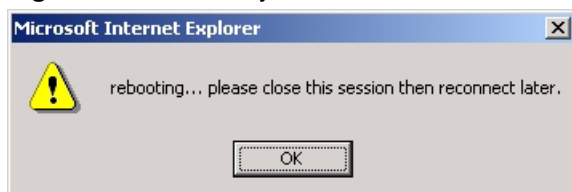
21.6 Reboot System

Reboot System allows you to restart the switch without physically turning the power off. Follow the steps below to reboot the switch.

- 1 In the **Maintenance** screen, click the **Click Here** button next to **Reboot System** to display the next screen.

Figure 71 Reboot System: Confirmation

2 Click **OK** to display the screen shown next.

Figure 72 Reboot System: Start

3 Click **OK** again and then wait for the switch to restart. This takes up to two minutes. This does not affect the switch's configuration.

21.7 FTP Command Line

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

21.7.1 Filename Conventions

The configuration file (also known as the romfile or ROM) 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.

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

Table 43 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, system-related data (including the default password), the error log and the trace log.
Firmware	Ras	*.bin	This is the generic name for the ZyNOS firmware on the switch.

21.7.1.1 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.

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

21.7.2 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 to "ras". Similarly, `put config.cfg config` transfers the configuration file on your computer (`config.cfg`) to the switch and renames it to "config". Likewise `get config config.cfg` transfers the configuration file on the switch to your computer and renames it to "config.cfg". See [Table 43 on page 148](#) for more information on filename conventions.
- 7 Enter `quit` to exit the ftp prompt.

21.7.3 GUI-based FTP Clients

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

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).

21.7.4 FTP Restrictions

FTP will not work when:

- FTP service is disabled in the **Service Access Control** screen.
- The IP address(es) 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.

CHAPTER 22

Access Control

This chapter describes how to control access to the switch.

22.1 Overview

- 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 73 Console Port Priority

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

- A console port or Telnet session can coexist with one FTP session, up to five Web sessions (five different usernames and passwords) and/or limitless SNMP access control sessions.

Table 44 Access Control Overview

Console Port	SSH	Telnet	FTP	Web	SNMP
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

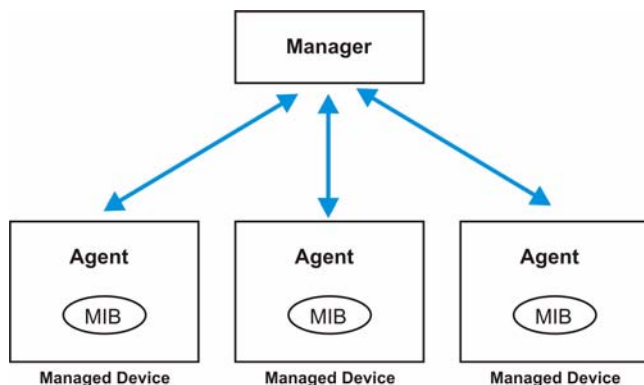
22.2 The Access Control Main Screen

Click **Management, Access Control** in the navigation panel to display the main screen as shown.

Figure 74 Access Control

22.3 About SNMP

Simple Network Management Protocol (SNMP) is an application layer protocol used to manage and monitor TCP/IP-based devices. SNMP is used to exchange management information between the network management system (NMS) and a network element (NE). 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 75 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-2024). 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 45 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.
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.
GetBulk	Allows the manager to retrieve voluminous data from a large table by giving one or more object identifiers (OIDs) and performing a continuous GetNext operation. This operation is not available in SNMP v1.

22.3.1 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

22.3.2 SNMP Traps

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

Table 46 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.

Table 46 SNMP Traps (continued)

OBJECT LABEL	OBJECT ID	DESCRIPTION
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 topology changes.
topology change	1.3.6.1.2.1.17.0.2	This trap is sent when the STP root switch changes.

22.3.3 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 76 Access Control: SNMP

The screenshot shows the 'SNMP' configuration screen within the 'Access Control' interface. The screen features a title bar with an orange circle icon, the text 'SNMP', and a link to 'Access Control'. Below the title bar, there are several input fields: 'Get Community' with the value 'public', 'Set Community' with the value 'public', and 'Trap Community' with the value 'public'. Under the 'Trap Destination' label, there are three input fields, each containing the IP address '0.0.0.0'. At the bottom of the screen, there are two buttons: 'Apply' and 'Cancel'.

The following table describes the labels in this screen.

Table 47 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 back to the switch.
Cancel	Click Cancel to begin configuring this screen afresh.

22.3.4 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.

- 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**.

Note: It is highly recommended that you change the default administrator password (**1234**).

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

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

Figure 77 Access Control: Logins

The following table describes the labels in this screen.

Table 48 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).

Table 48 Access Control: Logins (continued)

LABEL	DESCRIPTION
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 people have read-only access.	
User Name	Set a user name (up to 30 characters long).
Password	Enter your new system password.
Retype to confirm	Retype your new system password for confirmation
Apply	Click Apply to save your changes back to the switch.
Cancel	Click Cancel to begin configuring this screen afresh.

22.4 SSH Overview

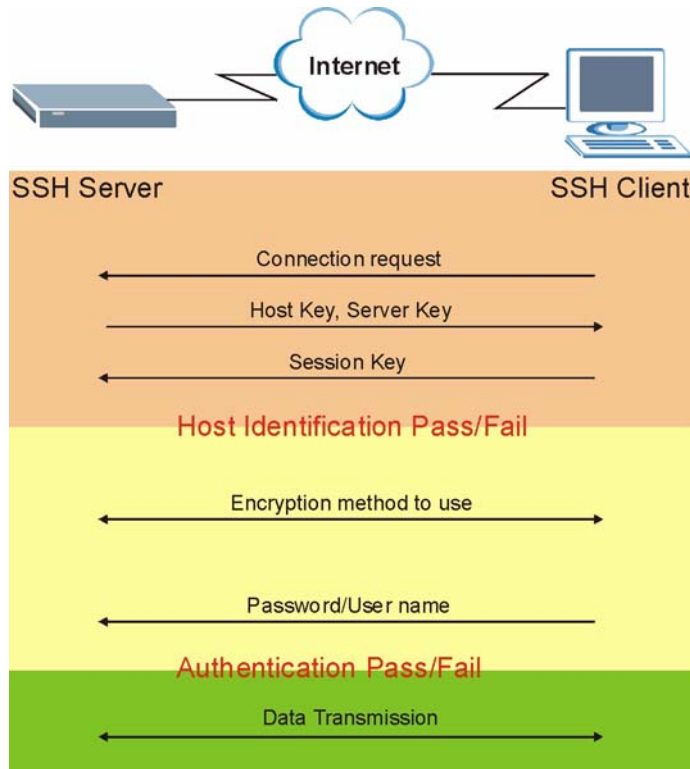
Unlike Telnet or FTP, which transmit data in clear text, SSH (Secure Shell) is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication

between two hosts over an unsecured network.

Figure 78 SSH Communication Example

22.5 How SSH works

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

Figure 79 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.

22.6 SSH Implementation on the Switch

Your switch supports SSH version 2 using RSA authentication and three encryption methods (DES, 3DES and Blowfish). The SSH server is implemented on the switch for remote management and file transfer on port 22. Only one SSH connection is allowed at a time.

22.6.1 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.

22.7 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).

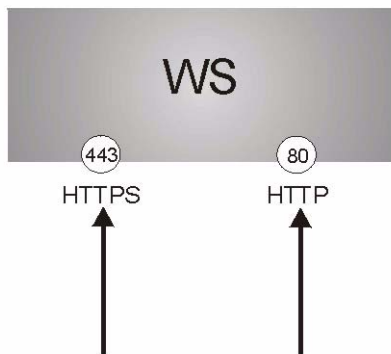
It relies upon certificates, public keys, and private keys.

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. Authenticating client certificates is optional and if selected means the SSL-client must send the switch a certificate. You must apply for a certificate for the browser from a CA that is a trusted CA on the switch.

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 80 HTTPS Implementation



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

22.8 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.

22.8.1 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 81 Security Alert Dialog Box (Internet Explorer)

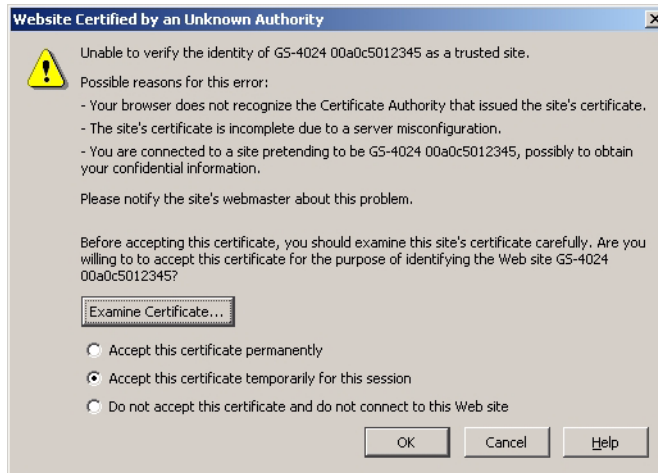


22.8.2 Netscape Navigator Warning Messages

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 82 Security Certificate 1 (Netscape)**Figure 83** Security Certificate 2 (Netscape)

22.8.3 The Main Screen

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

Figure 84 Login Screen (Internet Explorer)

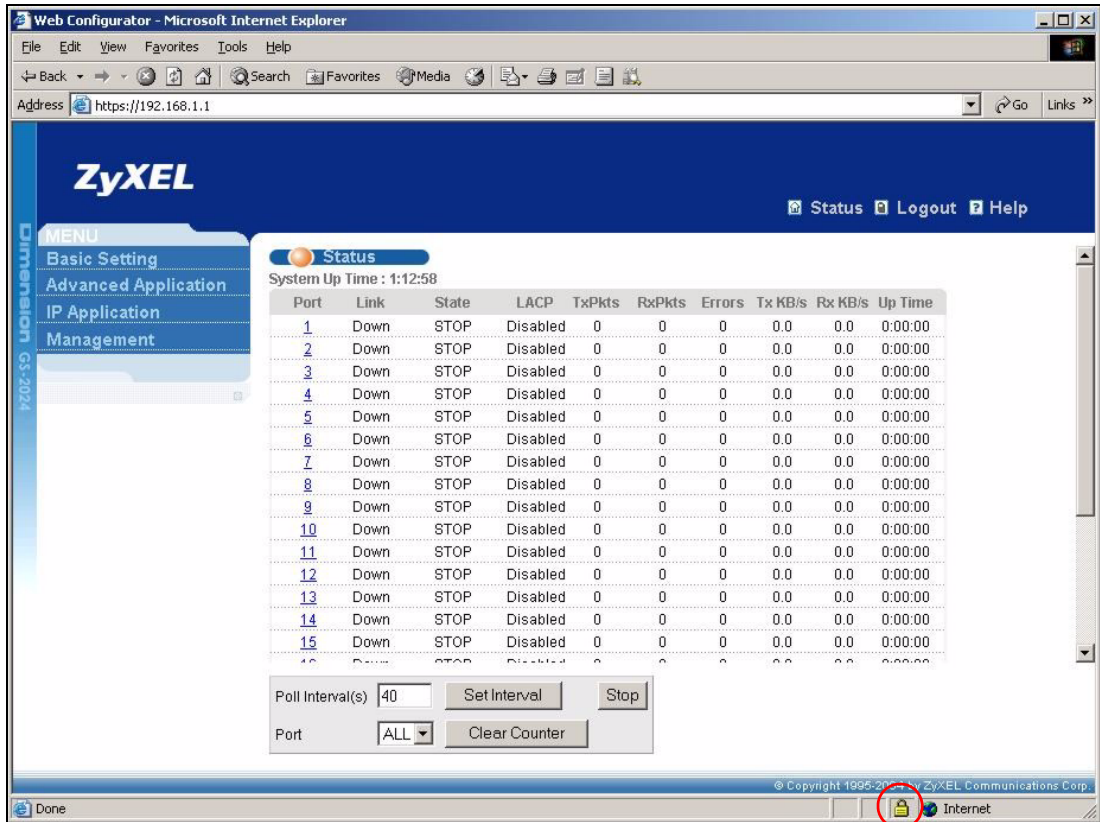


Figure 85 Login Screen (Netscape)

The screenshot shows the ZyXEL Web Configurator interface in Netscape. The browser address bar shows `https://192.168.1.1`. The page features the ZyXEL logo and a navigation menu on the left. The main content area displays the 'Status' section, which includes a table of port statistics and control buttons for polling intervals and port selection.

Port	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	100M/F	Copper	FORWARDING	1673	1509	0	0.0	0.0	3:01:42
10	100M/F	Copper	FORWARDING	2565	2466	0	32.545	8.95	3:01:42
11	100M/F	Copper	FORWARDING	41457	3843	0	0.0	0.0	3:01:42
12	100M/F	Copper	FORWARDING	4373	41647	0	0.0	0.0	3:01:42

Below the table, there are controls for 'Poll Interval(s)' (set to 40) and 'Port' (set to ALL). Buttons for 'Set Interval', 'Stop', and 'Clear Counter' are also present.

22.9 Service Port 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 main **Access Control** screen.

Figure 86 Access Control: Service Access Control

Services	Active	Service Port	Timeout
Telnet	<input checked="" type="checkbox"/>	23	
SSH	<input checked="" type="checkbox"/>	22	
FTP	<input checked="" type="checkbox"/>	21	
HTTP	<input checked="" type="checkbox"/>	80	3 Minutes
HTTPS	<input checked="" type="checkbox"/>	443	
ICMP	<input checked="" type="checkbox"/>		
SNMP	<input checked="" type="checkbox"/>		

The following table describes the fields in this screen.

Table 49 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 Server 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.
Apply	Click Apply to save your changes back to the switch.
Cancel	Click Cancel to begin configuring this screen afresh.

22.10 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 87 Access Control: Remote Management

Entry	Active	Start Address	End Address	Telnet	FTP	HTTP	ICMP	SNMP
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"/>
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"/>
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"/>
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"/>

The following table describes the labels in this screen.

Table 50 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.
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	Select services that may be used for managing the switch from the specified trusted computers.
Apply	Click Apply to save your changes back to the switch.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 23

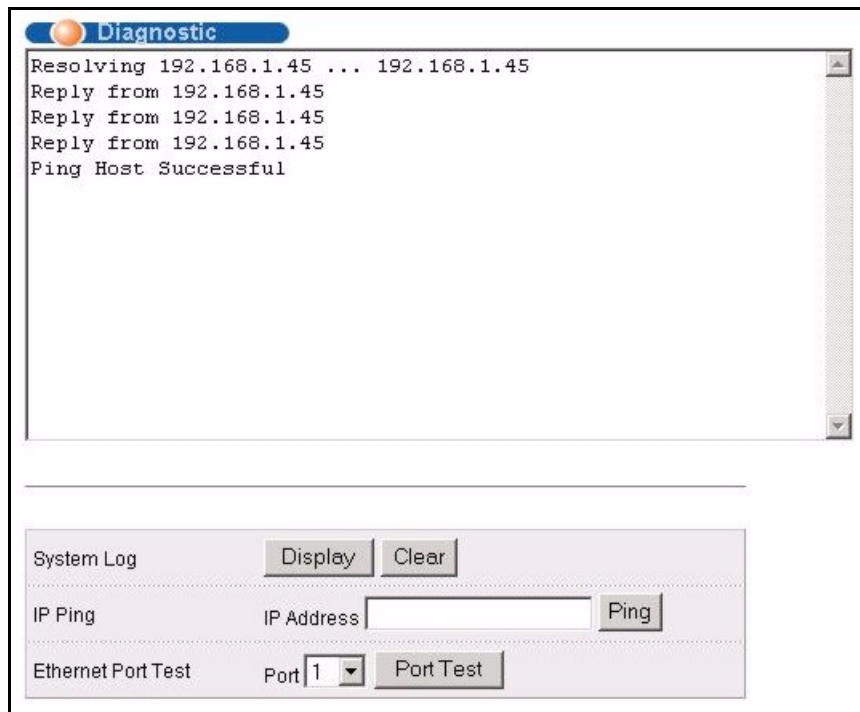
Diagnostic

This chapter explains the **Diagnostic** screen.

23.1 Diagnostic

Click **Management, Diagnostic** in the navigation panel to open this screen. Use this screen to check system logs, reset the system or ping IP addresses.

Figure 88 Diagnostic



The following table describes the labels in this screen.

Table 51 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.

CHAPTER 24

Cluster Management

This chapter introduces cluster management.

24.1 Overview

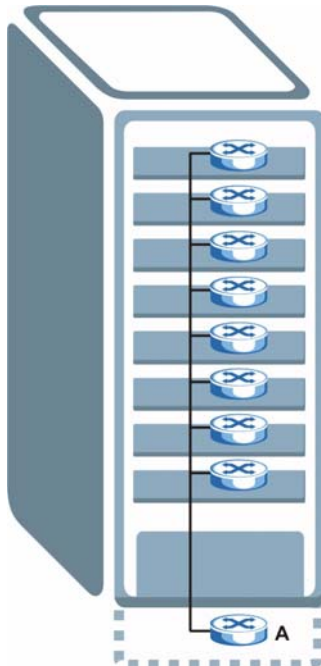
Cluster Management allows you to manage switches through one switch, called the cluster manager. The switches must be directly connected and be in the same VLAN group so as to be able to communicate with one another.

Table 52 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 89 Clustering Application Example



24.2 Cluster Management Status

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

Note: A cluster can only have one manager.

Figure 90 Cluster Management: Status

Clustering Management Status		Configuration		
Status	Manager			
Manager	00:a0:c5:01:23:46			
The Number Of Member = 1				
Index	MacAddr	Name	Model	Status
1	00:13:49:00:00:02	ES-3148	ES-3148	Online

The following table describes the labels in this screen.

Table 53 Cluster Management: Status

LABEL	DESCRIPTION
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 91 on page 169).
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)

24.2.1 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 91 Cluster Management: Cluster Member Web Configurator Screen



24.2.1.1 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 92 Example: Uploading Firmware to a Cluster Member Switch

```

C:\>ftp 192.168.1.1
Connected to 192.168.1.1.
220  FTP version 1.0 ready at Thu Jan  1 01:06:19 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      2603856 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: 297 bytes received in 0.00Seconds 297000.00Kbytes/sec.
ftp> bin
200 Type I OK
ftp> put 360tz0.bin fw-00-13-49-00-00-02
200 Port command okay
150 Opening data connection for STOR fw-00-13-49-00-00-02
226 File received OK
ftp: 262144 bytes sent in 0.63Seconds 415.44Kbytes/sec.
ftp>

```

The following table explains some of the FTP parameters.

Table 54 FTP Upload to Cluster Member Example

FTP PARAMETER	DESCRIPTION
User	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.
360tz0.bin	This is the name of the firmware file you want to upload to the cluster member switch.
fw-00-13-49-00-00-02	This is the cluster member switch's firmware name as seen in the cluster manager switch.
config-00-13-49-00-00-02	This is the cluster member switch's configuration file name as seen in the cluster manager switch.

24.3 Configuring Cluster Management

Click **Configuration** from the **Cluster Management** screen to display the next screen.

Figure 93 Clustering Management Configuration

Clustering Management Configuration [Status](#)

Clustering Manager:

Active

Name

VID

Clustering Candidate:

List

Password

Index	MacAddr	Name	Model	Remove
<input type="button" value="Remove"/> <input type="button" value="Cancel"/>				

The following table describes the labels in this screen.

Table 55 Clustering Management Configuration



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 20 printable characters (no spaces are allowed).
VID	This is the VLAN ID and is only applicable if the switch is set to 802.1Q VLAN. All switches must be directly connected and in the same VLAN group to belong to the same cluster. Switches that are not in the same 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 these changes to the switch.
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.

Table 55 Clustering Management Configuration (continued)

LABEL	DESCRIPTION
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 this part of the screen to the switch.
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 information for the clustering members configured.	
Index	This is the index number of a cluster member switch.
MacAddr	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.

CHAPTER 25

MAC Table

This chapter introduces the **MAC Table** screen.

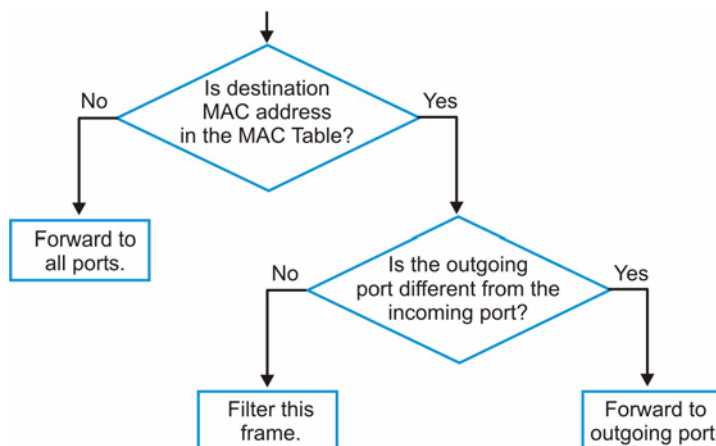
25.1 Overview

The **MAC Table** screen (a MAC table is also known as a filtering database) 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 the **Static MAC Forwarding** screen).

The switch uses the MAC table 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 MAC table.
 - 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.

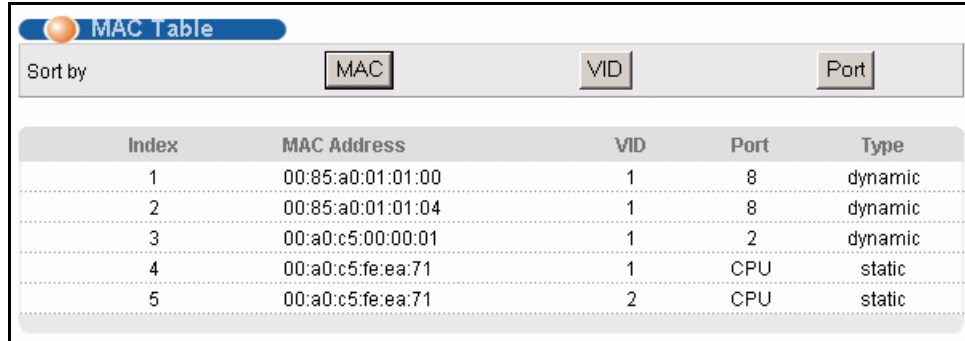
Figure 94 MAC Table Flowchart



25.2 Viewing the MAC Table

Click **Management, MAC Table** in the navigation panel to display the following screen.

Figure 95 MAC Table



MAC Table					
Sort by					
		MAC	VID	Port	
Index	MAC Address	VID	Port	Type	
1	00:85:a0:01:01:00	1	8	dynamic	
2	00:85:a0:01:01:04	1	8	dynamic	
3	00:a0:c5:00:00:01	1	2	dynamic	
4	00:a0:c5:fe:ea:71	1	CPU	static	
5	00:a0:c5:fe:ea:71	2	CPU	static	

The following table describes the labels in this screen.

Table 56 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 the Static MAC Forwarding screen).

CHAPTER 26

ARP Table

This chapter introduces ARP Table.

26.1 Overview

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.

26.1.1 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.

26.2 Viewing the ARP Table

Click **Management, ARP Table** in the navigation panel to open the following screen. Use the ARP table to view IP-to-MAC address mapping(s).

Figure 96 ARP Table

ARP Table			
Index	IP Address	MAC Address	Type
1	172.21.0.2	00:05:5d:04:30:f1	dynamic
2	172.21.3.16	00:05:1c:15:08:71	dynamic
3	172.21.3.19	00:0b:cd:8c:6d:ed	dynamic
4	172.21.3.40	00:0c:76:07:41:0d	dynamic
5	172.21.3.66	00:50:8d:47:73:4f	dynamic
6	172.21.3.90	00:05:5d:f4:49:20	dynamic
7	172.21.3.91	00:50:ba:ad:56:7c	dynamic
8	172.21.3.95	00:10:b5:ae:56:97	dynamic
9	172.21.3.120	00:10:b5:ae:62:32	dynamic
10	172.21.3.138	00:a0:c5:b2:62:26	dynamic
11	172.21.4.99	00:0c:76:09:cf:88	dynamic
12	172.21.10.11	08:00:20:ad:f6:88	dynamic
13	172.21.100.153	00:90:27:be:a2:8c	dynamic
14	172.21.207.247	00:0c:76:09:17:1a	dynamic
15	192.168.1.1	00:a0:c5:3f:91:56	dynamic
16	192.168.1.5	00:85:a0:01:01:04	dynamic
17	192.168.1.10	00:a0:c5:5e:df:f9	static
18	192.168.1.100	00:85:a0:01:01:00	dynamic

The following table describes the labels in this screen.

Table 57 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 the Static MAC Forwarding screen).

CHAPTER 27

Introducing the Commands

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

27.1 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.

Note: See the web configurator parts of this User's Guide for background information on features configurable by the web configurator.

27.1.1 Switch Configuration File

When you configure the switch using either the CLI (Command Line Interface) 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.

Note: 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.

27.2 Accessing the CLI

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

Note: 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.

27.2.1 Access Priority

- You can only access the CLI with the administrator account (the default username is **admin** and password is **1234**).
- By default, only one CLI management session is allowed via either the console port or Telnet. Console port access has higher priority.
- Use the `configure multi-login` command in the configuration mode to allow multiple concurrent logins. However, no more than five concurrent login sessions are allowed.

27.2.2 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

27.2.2.1 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 27.3 on page 179](#)).

Figure 97 Initial Console Port Screen

```
Copyright (c) 1994 - 2005 ZyXEL Communications Corp.
initialize mgmt, ethernet address: 00:a0:c5:01:23:45
initialize switch, ethernet address: 00:a0:c5:01:23:46
Initializing switch unit 0...
Initializing switch unit 1...
Press ENTER to continue...
```

27.2.3 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 192.168.1.1` (the default management IP address) and click **OK**.

- 3 A login screen displays (refer to [Section 27.3 on page 179](#)).

27.3 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 98 CLI: Login Screen

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

27.4 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.
- 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 “`configure`” 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.

27.5 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.

27.5.1 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 99 CLI Help: List of Commands: Example 1

```
ras> help
  Commands available:

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

Figure 100 CLI Help: List of Commands: Example 2

```

ras> ?
  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
ras>

```

27.5.2 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 101 CLI Help: Detailed Command Information: Example 1

```

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

```

Figure 102 CLI: Help: Detailed Command Information: Example 2

```

ras> ping ?
  <ip>           destination ip address
  help          Description of ping help

```

27.6 Command Modes

There are three CLI command modes: User, Enable and Configure.

When you first log into the CLI, the initial command mode is the 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 a password when prompted (the default is 1234). When you enter the Enable mode, the command prompt changes to the pound sign (#).

To enter the configuration mode, type `configure` or `config`. The Configure mode command prompt consists of the word “`config`” and the pound sign (#). There are various sub configuration modes: interface, MVR and VLAN.

- To enter config-vlan mode, type `vlan` followed by a number (between 1 to 4094). For example, `vlan 10` to configure settings for VLAN 10.
- To enter config-interface mode and configure the ports, enter `interface port-channel` followed by a port number. For example, `interface port-channel 10`.
- To enter MVR mode, enter `mvr` followed by a VLAN ID (between 1 and 4094). For example, enter `mvr 2` to configure multicast settings on VLAN 2.

Enter `exit` or `logout` to quit from the current mode or log out from the CLI.

27.7 Using Command History

The switch keeps a list of up to 256 commands(s) 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 103 CLI: History Command Example

```
ras> history
  enable
  exit
  show ip
  history
ras>
```

27.8 Saving Your Configuration

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

Figure 104 CLI: write memory

```

ras# write memory

```

Note: 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.

27.8.1 Logging Out

In User mode, enter the `exit` or `logout` command to log out of the CLI.

27.9 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 the same order as they are displayed in the CLI. See the related section in the User's Guide for more background information.

27.9.1 User Mode

The following table describes the commands available for User mode.

Table 58 Command Summary: User Mode

COMMAND		DESCRIPTION
help		Displays help information.
logout		Exits from the CLI.
exit		Logs out from the CLI.
history		Displays a list of previously command(s) that you have executed. The switch stores up to 256 commands in history.
enable		Accesses Enable (or privileged) mode. See Section 27.9.2 on page 184 .
show	ip	Displays IP related information.
	hardware-monitor <C F>	Displays current hardware monitor information with the specified temperature unit (Celsius C or Fahrenheit F).
	system-information	Displays general system information.
	mirror	Displays port mirroring information.
ping	<IP host-name>	Sends Ping request to an Ethernet device.

Table 58 Command Summary: User Mode (continued)

COMMAND		DESCRIPTION
	<IP host-name> [vlan <vlan-id>] [size <0-1472>] [-t]	Sends Ping request to an Ethernet device in the specified VLAN(s) with the specified parameters.
	help	Displays command help information.
traceroute	<ip host-name>	Determines the path a packet takes to a device.
	<ip host-name> [vlan <vlan-id>] [ttl <1-255>] [wait <1-60>] [queries <1-10>]	Determines the path a packet takes to a device in a VLAN.
	help	Displays command help information.
ssh	<1 2> <[user@]dest-ip>	Connects to an SSH server with the specified SSH version.

27.9.2 Enable Mode

The following table describes the commands available for Enable mode.

Table 59 Command Summary: Enable Mode

COMMAND		DESCRIPTION	
help		Displays help information.	
logout		Exits Enable (or privileged) mode.	
exit		Exits Enable (or privileged) mode.	
history		Displays a list of command(s) that you have previously executed.	
enable		Accesses Enable (or privileged) mode.	
disable		Exits Enable (or privileged) mode.	
configure		Accesses Configuration mode. See Section 27.9.3 on page 187 .	
no	logging	Disables syslog logging.	
show	ip	Displays IP related information.	
	arp	Displays the ARP table.	
	route	Displays IP routing information.	
	route static	Displays IP static route information.	
	hardware-monitor <C F>	Displays current hardware monitor information with the specified temperature unit (Celsius C or Fahrenheit F).	
	system-information	Displays general system information.	
	vlanlq	gvrp	Displays GVRP settings.
	spanning-tree	config	Displays Spanning Tree Protocol (STP) settings.

Table 59 Command Summary: Enable Mode (continued)

COMMAND			DESCRIPTION
	diffserv		Displays general DiffServ settings.
	mac	address-table <all [mac vid port]>	Displays MAC address table. You can sort by MAC address, VID or port.
		address-table static	Displays static MAC address table.
	lacp		Displays LACP (Link Aggregation Control Protocol) settings.
	trunk		Displays link aggregation information.
	mirror		Displays port mirroring information.
	radius-server		Displays RADIUS server settings.
	port-access- authenticator		Displays all port authentication settings.
		<port-list>	Displays port authentication settings on the specified port(s).
	port-security		Displays all port security settings.
	snmp-server		Displays SNMP settings.
	logins		Displays login account information.
	service-control		Displays service control settings.
	remote-management		Displays all secured client information.
		[index]	Displays the specified secured client information.
	interface <port- number>		Displays current interface status.
	interfaces config <port-list>		Displays current interface configuration.
		bandwidth- control	Displays bandwidth control settings.
		egress	Displays outgoing port information.
		bstorm-control	Displays broadcast storm control settings.
		igmp-immediate- leave	Displays IGMP immediate leave settings.
		igmp-filtering	Displays IGMP filter profile settings.
		igmp-group- limited	Displays IGMP group settings.
		igmp-query-mode	Displays IGMP query mode settings on the port(s).
	vlan		Displays the status of all VLANs.
		<vlan-id>	Displays the status of the specified VLAN.
	running-config		Displays current operating configuration.
	timesync		Displays time server information.

Table 59 Command Summary: Enable Mode (continued)

COMMAND		DESCRIPTION	
	time	Displays current system time and date.	
	garp	Displays GARP information.	
	loginPrecedence	Displays login precedence settings.	
	logging	Displays system logs.	
	ssh	Displays general SSH settings.	
		known-hosts	Displays known SSH hosts information.
		key <rsa1 rsa dsa>	Displays internal SSH public and private key information.
		session	Displays current SSH session(s).
	https		Displays the HTTPS information.
		session	Displays current HTTPS session(s).
		certificate	Displays the HTTPS certificates.
		key <rsa dsa>	Displays the HTTPS key.
		timeout	Displays the HTTPS session timeout.
	multi-login		Displays multi-login information
	mac-aging-time		Displays MAC learning aging time.
	cluster		Displays cluster management status.
		candidates	Displays cluster candidate information.
		member	Displays the MAC address of the cluster member(s).
		member mac <mac-addr>	Displays the status of the cluster member(s).
		member config	Displays the configuration of the cluster member(s).
	igmp-filtering profile		Displays IGMP filter profile settings.
	igmp-snooping		Displays IGMP snooping settings.
	multicast		Displays multicast settings.
	mvr		Displays all MVR (Multicast VLAN Registration) settings.
		<vlan-id>	Displays specified MVR information.
igmp-flush			Removes all IGMP information.
mac-flush			Clears the MAC address table.
	<port-num>		Removes all learned MAC address on the specified port(s).
erase	running-config		Resets to the factory default settings.
baudrate	<1 2 3 4 5>		Changes the console port speed. Choices are 1 (9600), 2 (19200), 3(38400), 4 (57600) and 5 (115200).

Table 59 Command Summary: Enable Mode (continued)

COMMAND		DESCRIPTION
boot	config <index>	Restarts the system with the specified configuration file.
reload	config <index>	Restarts the system and use the specified configuration file.
write	memory	Saves current configuration to the configuration file the switch is currently using.
		<index>
		Saves current configuration to the specified configuration file on the switch.
ping	<ip host-name>	Sends Ping request to an Ethernet device.
		[vlan <vlan-id>][..]
		Sends Ping request to an Ethernet device in the specified VLAN(s).
	help	Displays command help information.
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.
	help	Displays command help information.
ssh	<1 2> <[user@]dest-ip>	Connects to an SSH server with the specified SSH version.
		[command </>]
		Connects to an SSH server with the specified SSH version and addition commands to be executed on the server.

27.9.3 General Configuration Mode

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

Table 60 Command Summary: Configuration Mode

COMMAND		DESCRIPTION
help		Displays help information.
logout		Exits from the CLI.
history		Displays a list of previous command(s) that you have executed.
exit		Exits from the CLI.
mode	zynos	Changes the CLI mode to the ZyNOS format.
password		Change the password for Enable mode.

Table 60 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION
no	ip		Sets the management IP address to the default value.
		route <ip> <mask>	Removes a specified IP static route.
		route <ip> <mask> inactive	Enables a specified IP static route.
	igmp-filtering		Clears the IGMP filtering settings on the switch.
		profile <name>	Deletes the IGMP filtering profile.
		profile <name> start-address <ip> end-address <ip>	Deletes a rule in the IGMP filtering profile.
	igmp-snooping		Disables IGMP snooping on the switch.
	mac-forward	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).
		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).
	mirror		Disables port mirroring on the switch.
	lacp		Disables the link aggregation control protocol (dynamic trunking) on the switch.
	trunk	<T1 T2 T3 T4>	Disables the specified trunk group.
		<T1 T2 T3 T4> lacp	Disables LACP in the specified trunk group.
		<T1 T2 T3 T4> interface <port-list>	Removes ports from the specified trunk group.
	bandwidth-control		Disable bandwidth control on the switch.
	vlanlq	gvrp	Disables GVRP on the switch.
	diffserv		Disables the DiffServ settings.
	spanning-tree		Disables STP.
		<port-list>	Disables STP on listed ports.
	timesync		Disables timeserver settings.

Table 60 Command Summary: Configuration Mode (continued)

COMMAND		DESCRIPTION	
	radius-server	Disables the use of authentication from the RADIUS server.	
	port-access-authenticator	Disables port authentication on the switch.	
		<port-list>	Disables authentication on the listed ports.
		<port-list> reauthenticate	Disables the re-authentication mechanism on the listed port(s).
	port-security		Disables port security on the switch.
		<port-list>	Disables port security on the specified port(s).
		<port-list> learn inactive	Enables MAC address learning on the specified ports.
	snmp-server	trap-destination <ip>	Disables sending of SNMP traps to a station.
	logins	<name>	Disables login access to the specified name.
	service-control	telnet	Disables telnet access to the switch.
		ftp	Disables FTP access to the switch.
		http	Disables web browser control to the switch.
		ssh	Disables SSH (Secure Shell) server access to the switch.
		https	Disables secure web browser access to the switch.
		icmp	Disables ICMP access to the switch such as pinging and tracerouting.
		snmp	Disables SNMP management.
	remote-management	<index>	Clears a secure client set entry from the list of secure clients.
		<index> service <[telnet] [ftp] [http] [icmp] [snmp] [ssh] [https]>	Disables a secure client set entry number from using the selected remote management service(s).
	vlan	<vlan-id>	Deletes the static VLAN entry.
	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.
		known-hosts	Removes all remote hosts.

Table 60 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION
		known-hosts <host-ip>	Removes the specified remote hosts from the list of all known hosts.
		known-hosts <host-ip> [1024 ssh- rsa ssh-dsa]	Removes remote known hosts with the specified public key (1024-bit RSA1, RSA or DSA).
	https	timeout	Resets the session timeout to the default of 300 seconds.
	multi-login		Disables another administrator from logging into Telnet or the CLI.
	cluster		Disables cluster management on the switch.
	cluster member	<mac-address>	Removes the cluster member.
	storm-control		Disables broadcast storm control.
		<port-list>	Disables broadcast storm control on the specified port(s).
	mvr	<vlan-id>	Disables MVR on the switch.
vlan	<1-4094>		Enters the VLAN configuration mode. See Section 27.9.5 on page 197 for more information.
vlan-type	<802.1q port-based>		Specifies the VLAN type.
igmp-snooping			Enables IGMP snooping.
	unknown-multicast- frame <drop flooding>		Sets actions on traffic from unknown multicast group.
igmp-filtering			Enables IGMP filtering on the switch.
	profile <name> start-address <ip> end-address <ip>		Sets the range of multicast address(es) in a profile.
interface	port-channel <port- list>		Enables a port or a list of ports for configuration. See Section 27.9.4 on page 195 for more details.
ip	route	<ip> <mask> <next-hop-ip>	Creates a static route.
		<ip> <mask> <next-hop-ip> [metric <metric>] [name <name>] [inactive]	Sets the metric of a static route or deactivates a static route.
	name-server	<ip>	Sets the IP address of a domain name server.

Table 60 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION
	address default-gateway	<ip>	Sets the default gateway's IP address for the out-of-band management port.
	address	<ip> <mask>	Sets the IP address and subnet mask of the out-of-band management port.
mac-forward	name <name> mac <mac-addr> vlan <vlan-id> interface <interface-id>		Configures a static MAC address forwarding rule.
		inactive	Disables a static MAC address forwarding rule.
mirror			Enables port mirroring.
	monitor-port <port-num> mirrored-port <port-num>		Sets a monitor port (the port you copy the traffic to) and on which port you mirror the traffic.
	direction <ingress egress both>		Specifies the direction of the traffic to mirror.
lacp			Enables Link Aggregation Control Protocol (LACP).
	system-priority	<1-65535>	Sets the priority of an active port using LACP.
trunk	<T1 T2 T3 T4>		Activates a trunk group.
	<T1 T2 T3 T4>lacp		Enables LACP for a trunk group.
	<T1 T2 T3 T4>interface <port-list>		Adds a port(s) to the specified trunk group.
	interface <port-list> timeout <lacp-timeout>		Defines the port number and LACP timeout period.
queuing-method	spq		Sets the switch to use Strictly Priority Queuing (SPQ).
	wrr		Sets the switch to use Weighted Round Robin queuing (WRR).
		<wt1><wt2><wt3><wt4>	Sets the WRR weight. A weight value of one to eight is given to each variable from wt1 to wt4.
radius-server	host <ip> [acct-port <socket-number>] [key <key-string>]		Sets the IP address and/or the port number and key of the external RADIUS server.
port-access-authenticator			Enables 802.1x authentication on the switch.
	<port-list>		Enables 802.1x authentication on the specified port(s).

Table 60 Command Summary: Configuration Mode (continued)

COMMAND		DESCRIPTION	
		reauthenticate	Sets a subscriber to periodically re-enter his or her username and password to stay connected to a specified port.
		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).
port-security			Enables port security on the switch.
	<port-list>		Enables the port security feature on the specified port(s).
		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.
vlanlq	gvrp		Enables GVRP.
garp	join <100-65535> leave <msec> leaveall <msec>		Configures GARP time settings.
spanning-tree			Enables STP on the switch.
	priority <0-61440>		Sets the bridge priority of the switch.
	hello-time <1-10> maximum-age <6-40> forward-delay <4-30>		Sets Hello Time, Maximum Age and Forward Delay.
	<port-list>		Enables STP on a specified port.
	<port-list> path-cost <1-65535>		Sets the STP path cost for a specified port.
	<port-list> priority <0-255>		Sets the priority for a specified port.
	help		Displays help information.
hostname	<name_string>		Sets the switch's name for identification purposes.
time	<Hour:Min:Sec>		Sets the time in hour, minute and second format.
	timezone <-1200 ... 1200>		Selects the time difference between UTC (formerly known as GMT) and your time zone.
	date <month/day/year>		Sets the date in year, month and day format.

Table 60 Command Summary: Configuration Mode (continued)

COMMAND		DESCRIPTION	
	help	Displays help information.	
timesync	<daytime time ntp>	Sets the time server protocol.	
	server <ip>	Sets the IP address of your time server.	
loginPrecedence	<LocalOnly LocalRADIUS RADIUSOnly>	Select which database the switch should use (first) to authenticate a user.	
queue	level <0-7> priority <0-3>	Sets the priority level-to-physical queue mapping.	
bandwidth-control		Enables bandwidth control.	
mac-aging-time	<10-3000>	Sets learned MAC aging time.	
snmp-server	get-community <property>	Sets the get community.	
	set-community <property>	Sets the set community.	
	trap-community <property>	Sets the trap community.	
	trap-destination <ip>	Sets the IP addresses of up to four stations to send your SNMP traps to.	
	[contact <system contact>] [location <system location>]	Sets the geographic location and the name of the person in charge of this switch.	
logins	username <name> password <pwd>	Configures up to four read-only login accounts.	
service-control	icmp	Allows ICMP access for services such as Ping.	
	snmp	Allows SNMP management.	
	http <socket-number> <timeout>	Allows HTTP access on the specified service port and defines the timeout period.	
	telnet <socket-number>	Allows Telnet access on the specified service port.	
	ftp <socket-number>	Allows FTP access on the specified service port.	
	ssh <socket-number>	Allows SSH access on the specified service port.	
	https <socket-number>	Allows HTTPS access on the specified service port.	
	remote-management	<index>	Enables a specified secured client set.

Table 60 Command Summary: Configuration Mode (continued)

COMMAND		DESCRIPTION
	<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.
admin-password	<pw-string> <confirm-string>	Changes the administrator password.
default-management	<in-band out-of-band>	Specifies through which traffic flow the switch is to send packets.
ssh	known-hosts <host-ip> <1024 ssh-rsa ssh-dsa> <key>	Adds a remote host to which the switch can access using SSH service.
https	cert-regeneration <rsa dsa>	Re-generates a certificate.
	timeout <0-65535>	Sets the HTTPS timeout period.
multi-login		Enables multi-login.
cluster	<vlan-id>	Sets the cluster management VLAN ID.
	name <cluster name>	Configures a name to identify the cluster manager.
	member <mac-address> password <password-str>	Sets the cluster member switch's hardware MAC address and password.
	rcommand <mac-address>	Logs into a cluster member switch.
diffserv		Enables DiffServ.
	dscp <0-63> priority <0-7>	Sets the DSCP-to-IEEE 802.1q mappings.
mvr <vlan-id>		Enters the MVR (Multicast VLAN Registration) configuration mode. See Section 27.9.6 on page 199 for more information.
storm-control		Enables broadcast storm control on the switch.
	<port-list>	Enables broadcast storm control on a port.
	type broadcast	[multicast] [unknown-unicast]
	packet-limit <number>	Sets how many packets a port receives per second based on the chosen storm control type.

27.9.4 interface port-channel Commands

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

Table 61 interface port-channel Commands

COMMAND		DESCRIPTION
<code>interface port-channel <port-list></code>		Enables a port or a list of ports for configuration.
	<code>egress set <port-list></code>	Sets the outgoing traffic port list for a port-based VLAN.
	<code>igmp-immediate-leave</code>	Enables IGMP immediate leave on the port.
	<code>igmp-filtering profile <name></code>	Sets the IGMP filtering profile for this port.
	<code>igmp-group-limited</code>	Limits the number of multicast groups.
	<code>igmp-group-limited number <number></code>	Sets the number of multicast groups this port is allowed to join.
	<code>igmp-querier-mode <auto fixed edge></code>	Sets the IGMP querier mode of a port. Selects <code>auto</code> to treat the IGMP queries normally, <code>fixed</code> to always treat the port as a querier port no matter there is a query or <code>edge</code> to treat the port as a non-querier port which drops any IGMP queries received.
	<code>pvid <1-4094></code>	The default PVID is VLAN 1 for all ports. Sets a PVID in the range 1 to 4094 for the specified interface.
	<code>ingress-check</code>	Enables the device to discard incoming frames for VLANs that are not included in a port member set.
	<code>gvrp</code>	Enables this function to permit VLAN groups beyond the local switch.
	<code>frame-type <all tagged untagged></code>	Choose to accept both tagged and untagged incoming frames or just tagged incoming frames on a port.
	<code>name <port-name-string></code>	Sets a name for the port(s). Enter a descriptive name (up to nine printable ASCII characters).

Table 61 interface port-channel Commands (continued)

COMMAND		DESCRIPTION	
	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.	
	flow-control	Enables interface flow control. Flow control regulates transmissions to match the bandwidth of the receiving port.	
	bandwidth-limit	Enables bandwidth control on the port(s).	
		scheme <drop flow-control>	Sets the bandwidth control action on individual ports.
		ingress <Kbps>	Sets the maximum bandwidth allowed for incoming traffic on the port(s).
	qos priority	<0 .. 7>	Sets the quality of service priority for an interface.
	speed-duplex	<auto 10-half 10-full 100-half 100-full 1000-full>	Sets the duplex mode (half or full) and speed (10, 100 or 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.
	jumbo-frame		Enables sending and receiving jumbo frames on the port.
	no	egress set <port-list>	Disables outgoing traffic on the port for a port-based VLAN.
		igmp-immediate-leave	Disables IGMP immediate leave on the port.
		igmp-filtering profile	Disables IGMP filtering on the port.
		igmp-group-limited	Disables IGMP group limitation.
		ingress-check	Disables ingress checking on the port(s).
		gvrp	Disable GVRP on the port(s).
		flow-control	Disables flow control on the port(s).
		vlan-trunking	Disables VLAN trunking on the port(s).
		bandwidth-limit	Disables bandwidth limit on the port(s).

Table 61 interface port-channel Commands (continued)

COMMAND		DESCRIPTION
	jumbo-frame	Disables sending and receiving jumbo frames on the port.
	inactive	Enables the port(s) on the switch.
	intrusion-lock	Disables intrusion-lock on a port so that a port can be connected again after you disconnected the cable.
	inactive	Disables the specified port(s) on the switch.
	help	Displays a description of the interface port-channel commands.
	exit	Exits from the interface port-channel command mode.
	cable_diagnostics	Displays whether a cable is connected to the port (good) or not (open).
	intrusion-lock	Enables intrusion lock on a port. A port is disabled and cannot be connected again after you disconnected the Ethernet cable to the port. No traffic can pass through the port after it is disabled. If you want to use this port again you must access the switch through another port (or the management port) and disable intrusion lock.
	test	Performs an interface loopback test.

27.9.5 config-vlan Commands

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

Table 62 Command Summary: config-vlan Commands

COMMAND		DESCRIPTION
vlan <1-4094>		Creates a new VLAN group.
	name <name-str>	Specifies a name for identification purposes.
	normal <port-list>	Specifies the port(s) to dynamically join this VLAN group using GVRP
	fixed <port-list>	Specifies the port(s) to be a permanent member of this VLAN group.

Table 62 Command Summary: config-vlan Commands (continued)

COMMAND			DESCRIPTION
	forbidden <port-list>		Specifies the port(s) you want to prohibit from joining this VLAN group.
	untagged <port-list>		Specifies the port(s) you don't want to tag all outgoing frames transmitted with this VLAN Group ID.
	inactive		Disables the specified VLAN.
	help		Displays a list of available VLAN commands.
	no	fixed <port-list>	Sets fixed port(s) to normal port(s).
		forbidden <port-list>	Sets forbidden port(s) to normal port(s).
		untagged <port-list>	Enables VLAN tagging for outgoing traffic on the specified port(s).
		inactive	Enables the specified VLAN.
		ip address inband-default dhcp-bootp	Sets the default in-band interface to use a static IP address in this VLAN. The switch will use the default IP address of 0.0.0.0 if you do not configure a static IP address.
		ip address <ip-address> <mask>	Deletes the IP address and subnet mask from this VLAN.
		ip address default-gateway	Deletes the default gateway from this VLAN.
	exit		Leaves the VLAN configuration mode.
	ip address	inband-default dhcp-bootp	Sets the dynamic in-band IP address
		inband-default dhcp-bootp release	Releases the dynamic in-band IP address.
		inband-default dhcp-bootp renew	Updates the dynamic in-band IP address.
		inband-default <ip-address> <mask>	Sets a static in-band IP address and subnet mask.
		<ip-address> <mask> manageable	Sets the management IP address and subnet mask of the switch in the specified VLAN.
		<ip-address> <mask>	Sets the IP address and subnet mask of the switch in the specified VLAN.
		default-gateway <ip-address>	Sets a default gateway IP address for this VLAN.

27.9.6 mvr Commands

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

Table 63 mvr Commands

COMMAND		DESCRIPTION
<code>mvr <1-4094></code>		Enters the MVR (Multicast VLAN Registration) configuration mode.
	<code>source-port <port-list></code>	Sets the source port(s). An MVR source port can send and receive multicast traffic in a multicast VLAN
	<code>receiver-port <port-list></code>	Sets the receiver port(s). An MVR receiver port can only receive multicast traffic in a multicast VLAN
	<code>inactive</code>	Disables MVR settings.
	<code>mode <dynamic compatible></code>	Sets the MVR mode (dynamic or compatible).
	<code>name <name-str></code>	Sets the MVR name for identification purposes.
	<code>tagged <port-list></code>	Sets the port(s) to tag VLAN tags.
	<code>group <name-str></code> <code>start-address <ip></code> <code>end-address <ip></code>	Sets the multicast group range for the MVR.
	<code>exit</code>	Exist from the MVR configuration mode.
	<code>no source-port <port-list></code>	Disables the source port(s). An MVR source port can send and receive multicast traffic in a multicast VLAN
	<code>no receiver-port <port-list></code>	Disables the receiver port(s). An MVR receiver port can only receive multicast traffic in a multicast VLAN
	<code>no tagged <port-list></code>	Sets the port(s) to untag VLAN tags.
	<code>no inactive</code>	Enables MVR.
	<code>no group</code>	Disables all MVR group settings.
	<code>no group <name-str></code>	Disables the specified MVR group setting.

CHAPTER 28

Command Examples

This chapter describes some commands in more detail.

28.1 Overview

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

28.2 show Commands

These are the commonly used `show` commands.

28.2.1 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 105 show system-information Command Example

```
ras> show system-information
System Name           :
System Contact        :
System Location       :
Ethernet Address      : 00:a0:c5:01:23:46
ZyNOS F/W Version     : V3.60(LT.0)b3 | 06/21/2005
RomRasSize           : 2603856
System up Time        : 0:36:42 (35c65 ticks)
Bootbase Version      : V0.6 | 05/18/2004
ZyNOS CODE            : RAS Jun 21 2005 18:12:15
Product Model         : GS-2024
ras>
```

28.2.2 show ip

Syntax:

```
show ip
```

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

The following figure shows the default interface settings.

Figure 106 show ip Command Example

```
ras> 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]
ras>
```

28.2.3 show logging

Note: This command is not available in User mode.

Syntax:

```
show logging
```

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

Figure 107 show logging Command Example

```
ras# show logging
 50 Thu Jan  1 00:00:04 1970 PP05 -WARN  SNMP TRAP 3: link up
 51 Thu Jan  1 00:00:10 1970 PP0f -WARN  SNMP TRAP 26: Event On Trap
 52 Thu Jan  1 00:00:10 1970 PINI -WARN  SNMP TRAP 0: cold start
 53 Thu Jan  1 00:00:10 1970 PINI  INFO  main: init completed
 54 Thu Jan  1 00:00:10 1970 PP0f -WARN  SNMP TRAP 26: Event On Trap
 55 Thu Jan  1 00:00:10 1970 PINI -WARN  SNMP TRAP 0: cold start
 56 Thu Jan  1 00:00:10 1970 PINI  INFO  main: init completed
 57 Thu Jan  1 00:00:10 1970 PP0f -WARN  SNMP TRAP 26: Event On Trap
 58 Thu Jan  1 00:00:10 1970 PINI -WARN  SNMP TRAP 0: cold start
 59 Thu Jan  1 00:00:10 1970 PINI  INFO  main: init completed
 60 Thu Jan  1 00:00:10 1970 PP0f -WARN  SNMP TRAP 26: Event On Trap
 61 Thu Jan  1 00:00:10 1970 PINI -WARN  SNMP TRAP 0: cold start
 62 Thu Jan  1 00:00:10 1970 PINI  INFO  main: init completed
 63 Thu Jan  1 00:00:11 1970 PP27  INFO  adjtime task pause 1 day
Clear Error Log (y/n):
```

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

28.2.4 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 108 show interface Command Example

```

ras# show interface 2
  Port Info      Port NO.      :2
                 Link          :100M/F
                 Status        :FORWARDING
                 LACP          :Disabled
                 TxPkts        :0
                 RxPkts        :63
                 Errors        :0
                 Tx KBs/s      :0.0
                 Rx KBs/s      :0.0
                 Up Time       :0:02:33
TX Packet      Tx Packets      :0
                Multicast      :0
                Broadcast      :0
                Pause          :0
                Tagged         :0
RX Packet      Rx Packets      :63
                Multicast      :0
                Broadcast      :63
                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             :3
                65 to 127     :44
                128 to 255    :14
                256 to 511    :2
                512 to 1023   :0
                1024 to 1518  :0
                Giant         :0
ras#

```

28.2.5 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 the static MAC address table.

Figure 109 show mac address-table Command Example

```

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

```

28.3 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 110 ping Command Example

```

ras# 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
ras#

```

28.4 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.
[quesries <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 111 traceroute Command Example

```
ras> 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:
ras>
```

28.5 Enabling RSTP

To enable RSTP on a port. Enter `spanning-tree` followed by the port number and press [ENTER].

An example is shown next.

- Enable RSTP on the switch.
- Enable RSTP on port 10.

Figure 112 Enable RSTP Command Example

```
ras(config)# spanning-tree
ras(config)# spanning-tree 10
```

28.6 Configuration File Maintenance

The following sections shows how to manage the configuration files.

28.6.1 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 restarts the switch to use the second configuration file.

Figure 113 CLI: boot config Command Example

```
ras# 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 114 CLI: reload config Command Example

```
ras# reload config 2
```

Note: 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.

28.6.2 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 115 CLI: Reset to the Factory Default Example

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

28.7 no Command Examples

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

28.7.1 no mirror

Syntax:

```
no mirror
```

Disables port mirroring on the switch.

An example is shown next.

Figure 116 no mirror Command Example

```
ras(config)# no mirror
```

28.7.2 no https timeout

Syntax:

```
no https timeout
```

Resets the https session timeout to default.

An example is shown next. The session timeout is reset to 300 seconds.

Figure 117 no https timeout Command Example

```
ras(config)# no https timeout
Cache timeout 300
```


28.7.3 no trunk

Syntax:

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

where

<T1 T2 T3 T4>	Disables the trunk group.
<T1 T2 T3 T4> lacp	Disables LACP in the trunk group.
<T1 T2 T3 T4> 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 two (T2).

Figure 118 no trunk Command Example

```
ras(config)# no trunk T1
ras(config)# no trunk T3 lacp
ras(config)# no trunk T2 interface 1,3-5
```

28.7.4 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 port(s).
<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 119 no port-access-authenticator Command Example

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

28.7.5 no ssh

Syntax:

```
no ssh key <rsa1|rsa|dsa>
no ssh known-hosts <host-ip>
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 120 no ssh Command Example

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

28.8 interface Commands

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

28.8.1 interface port-channel

Syntax:

```
interface port-channel <port-list>
```

Use this command to enable the specified ports for configuration. 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 mode.
- Enable ports one, three, four and five for configuration.
- Begin configuring for those ports.

Figure 121 interface Command Example

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

28.8.2 bandwidth-limit

Syntax:

```
bandwidth-limit
bandwidth-limit ingress <Kbps>
bandwidth-limit scheme <drop|flow-control>
```

where

bandwidth-limit Enables bandwidth control on the switch.

scheme <drop|flow-control> Sets the bandwidth control action on individual ports.

<Kbps> Sets the maximum bandwidth allowed for incoming traffic (ingress) on the switch.

An example is shown next.

- Enable port one for configuration.
- Enable bandwidth control.
- Set the incoming traffic bandwidth limit to 16000 Kbps.
- Sets the control scheme to discard all incoming packets that are over the maximum allowable bandwidth on a port.

Figure 122 bandwidth-limit Command Example

```
ras(config)# interface port-channel 1
ras(config-interface)# bandwidth-limit
ras(config-interface)# bandwidth-limit ingress 16000
ras(config-interface)# bandwidth-limit scheme drop
```

28.8.3 mirror

Syntax:

```
mirror
mirror monitor-port <port-num> mirrored-port <port-num>
mirror direction <ingress|egress|both>
```

where

	Enables port mirroring on the interface.
monitor-port <port-num> mirrored-port <port-num>	Sets a monitor port (the port you copy the traffic to) and on which port you mirror the traffic.
<ingress egress both> =	Enables port mirroring for incoming, outgoing or both incoming and outgoing traffic.

Port mirroring is copying 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 two.
- Traffic is copied from port ten to port two in order to examine it in more detail without interfering with the traffic flow on the original port(s).
- Enable port mirroring for outgoing traffic.

Figure 123 mirror Command Example

```
ras(config)# mirror
ras(config)# mirror monitor-port 2 mirrored-port 10
ras(config)# mirror direction egress
```

28.8.4 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 124 gvrp Command Example

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

28.8.5 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 125 ingress-check Command Example

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

28.8.6 frame-type

Syntax:

```
frame-type <all|tagged|untagged>
```

where

`<all|tagged|untagged>` Choose to accept both tagged and untagged incoming frames or just tagged incoming frames on a port.

An example is shown next.

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

Figure 126 frame-type Command Example

```
ras(config)# interface port-channel 1,3-5
ras(config-interface)# ingress-check
ras(config-interface)# frame-type tagged
```

28.8.7 queuing-method spq

Syntax:

```
queuing-method spq
```

Set the switch to use Strictly Priority Queuing (SPQ).

An example is shown next.

Figure 127 queuing-method spq Command Example

```
ras(config)# queuing-method spq
```

28.8.8 queuing-method wrr

Syntax:

```
queuing-method wrr <wt1><wt2><wt3><wt4>
```

where

Enables WRR (Weighted Round Robin) queuing method on the switch.

`<wt1> .. <wt4>` Sets the interface to use WRR queuing. A weight value of one to eight is given to each variable from `wt1` to `wt4`.

An example is shown next. Enable Weighted Round Robin queuing on the switch and set the queue weights from Q0 to Q3.

Figure 128 queuing-method wrr Command Example

```
ras# configure
ras(config)# queuing-method wrr 4 3 2 1
```

28.8.9 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), seven (7), eight (8) and nine (9).

Figure 129 egress set Command Example

```
ras(config)# vlan-type port-based
ras(config)# interface port-channel 1,3-5
ras(config-interface)# egress set 0,7-9
```

28.8.10 qos priority

Syntax:

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

where

<0 .. 7> Sets the quality of service priority for a port.

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 130 qos priority Command Example

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

28.8.11 name

Syntax:

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

where

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

An example is shown next.

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

Figure 131 name Command Example

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

28.8.12 speed-duplex

Syntax:

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

where

<auto|10-half|10-full|100-half|100-full|1000-full> Sets the duplex mode (half or full) and speed (10, 100 or 1000 Mbps) of the connection on the port. 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.

An example is shown next.

- Enable ports one, three, four and five for configuration.
- Set the speed to 100 Mbps in half duplex mode.

Figure 132 speed-duplex Command Example

```
ras(config)# interface port-channel 1,3-5
ras(config-interface)# speed-duplex 100-half
```


CHAPTER 29

IEEE 802.1Q Tagged VLAN Commands

This chapter describes the IEEE 802.1Q Tagged VLAN and associated commands.

29.1 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.

29.2 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).

29.2.1 Static Entries (SVLAN Table)

Static entry registration information is added, modified and removed by administrators only.

29.2.2 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.

29.3 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.
 - Use the `vlan <vlan-id>` command to configure or create a VLAN on the switch. The switch automatically enters the `config-vlan` mode. Use the `inactive` command to deactivate the VLAN(s).
 - 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.
 - Use the `exit` command when you are finished configuring the VLAN.

Example:

Figure 133 Tagged VLAN Configuration and Activation Example

```
ras (config)# vlan 2000
ras (config-vlan)# name up1
ras (config-vlan)# fixed 10-12
ras (config-vlan)# no untagged 10-12
ras (config-vlan)# exit
ras (config)# interface port-channel 10-12
ras (config-interface)# pvid 2000
ras (config-interface)# exit
```

- 2 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 134 CPU VLAN Configuration and Activation Example

```

ras (config)# vlan 3
ras (config-vlan)# inactive

```

29.4 Global VLAN1Q Tagged VLAN Configuration Commands

This section shows you how to configure and monitor the IEEE 802.1Q Tagged VLAN.

29.4.1 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 135 GARP STATUS Command Example

```

ras # show garp
GARP Timer
-----
Join Timer = 200
Leave Timer = 600
Leave All Timer = 10000
ras#

```

29.4.2 GARP Timer

Syntax:

```
garp join <msec> leave <msec> leaveall <msec>
```

where

`join <msec>` = 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.

- `leave <msec>` = 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.
- `leaveall <msec>` = 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.

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.

Figure 136 GARP Timer Command Example

```
ras (config)# garp join 300 leave 800 leaveall 11000
```

29.4.3 GVRP Timer

Syntax:

```
show vlan1q gvrp
```

This command shows the switch's GVRP settings.

An example is shown next.

Figure 137 GVRP Status Command Example

```
ras # show vlan1q gvrp
GVRP Support
-----
gvrpEnable = YES
ras #
```

29.4.4 Enable GVRP

Syntax:

```
vlan1q gvrp
```

This command turns on GVRP in order to propagate VLAN information beyond the switch.

29.4.5 Disable GVRP

Syntax:

```
no vlan1q gvrp
```

This command turns off GVRP so that the switch does not propagate VLAN information to other switches.

29.5 Port VLAN Commands

You must configure the switch port VLAN settings in config-interface mode.

29.5.1 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 138 vlan1q port default vid Command Example

```

ras (config)# interface port-channel 1-5
ras (config-interface)# pvid 200

```

29.5.2 Set Acceptable Frame Type

Syntax:

```
frame-type <all|tagged|untagged>
```

where

<all|tagged|untagged> = 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 139 frame type Command Example

```
ras (config)# interface port-channel 1-5
ras (config-interface)# frame-type tagged
```

29.5.3 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 140 no gvrp Command Example

```
ras (config)# interface port-channel 1-5
ras (config-interface)# no gvrp
```

29.5.4 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.

29.5.4.1 Modify a Static VLAN Table Example

The following example configures ports 1 to 5 as fixed and untagged ports in VLAN 2000.

Figure 141 Modifying Static VLAN Example

```

ras (config)# vlan 2000
ras (config-vlan)# fixed 1-5
ras (config-vlan)# untagged 1-5

```

29.5.4.2 Forwarding Process Example

29.5.4.2.1 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.

29.5.4.2.2 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.

29.5.5 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 142 no vlan Command Example

```
ras (config)# no vlan 2
```

29.6 Enable VLAN

Syntax:

```
vlan <vlan-id>
```

This command enables the specified VLAN ID in the SVLAN (Static VLAN) table.

29.7 Disable VLAN

Syntax:

```
vlan <vlan-id> inactive
```

This command disables the specified VLAN ID in the SVLAN (Static VLAN) table.

29.8 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 143 show vlan Command Example

```
ras# show vlan
802.1Q VLAN Static Entry:
idx. Name          VID  Active  AdCtl / TagCtl
-----
  0             1    1 active  FFFFFFFFFFFFFFFFFFFFFFFF
                1    1 active  UUUUUUUUUUUUUUUUUUUUUUU
  2             test2  2 active  FFXFXFXFXFXFXFXFXFXFXFX
                2    2 active  UUUUUUUUUUUUUUUUUUUUUUU
ras#
```


CHAPTER 30

Troubleshooting

This chapter covers potential problems and possible remedies.

30.1 Problems Starting Up the Switch

Table 64 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.

30.2 Problems Accessing the Switch

Table 65 Troubleshooting Accessing the Switch

PROBLEM	CORRECTIVE ACTION
I cannot access the switch using Telnet.	<p>Make sure the ports are properly connected.</p> <p>You may have exceeded the maximum number of concurrent Telnet sessions. Close other Telnet session(s) or try connecting again later.</p> <p>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.</p>
I cannot access the web configurator.	<p>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.</p> <p>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.</p> <p>Your computer's and the switch's IP addresses must be on the same subnet.</p> <p>See the following section to check that pop-up windows, JavaScripts and Java permissions are allowed.</p> <p>You may also need to clear your Internet browser's cache.</p> <p>In Internet Explorer, click Tools and then Internet Options to open the Internet Options screen.</p> <p>In the General tab, click Delete Files. In the pop-up window, select the Delete all offline content check box and click OK. Click OK in the Internet Options screen to close it.</p> <p>If you disconnect your computer from one device and connect it to another device that has the same IP address, your computer's ARP (Address Resolution Protocol) table may contain an entry that maps the management IP address to the previous device's MAC address).</p> <p>In Windows, use arp -d at the command prompt to delete all entries in your computer's ARP table.</p>

30.2.1 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).

Note: Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

30.2.1.1 Internet Explorer Pop-up Blockers

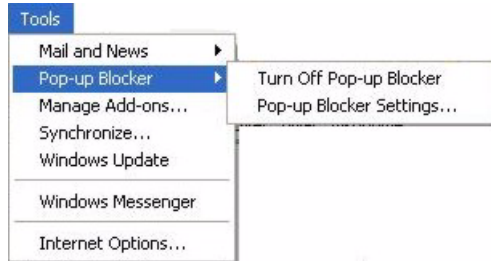
You may have to disable pop-up blocking to log into your device.

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.

30.2.1.1.1 Disable pop-up Blockers

- 1 In Internet Explorer, select **Tools, Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

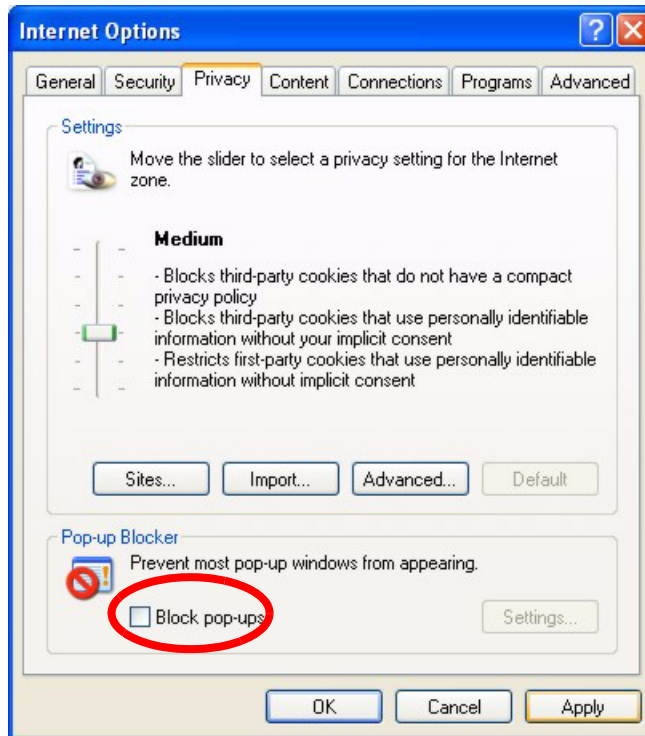
Figure 144 Pop-up Blocker



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 145 Internet Options



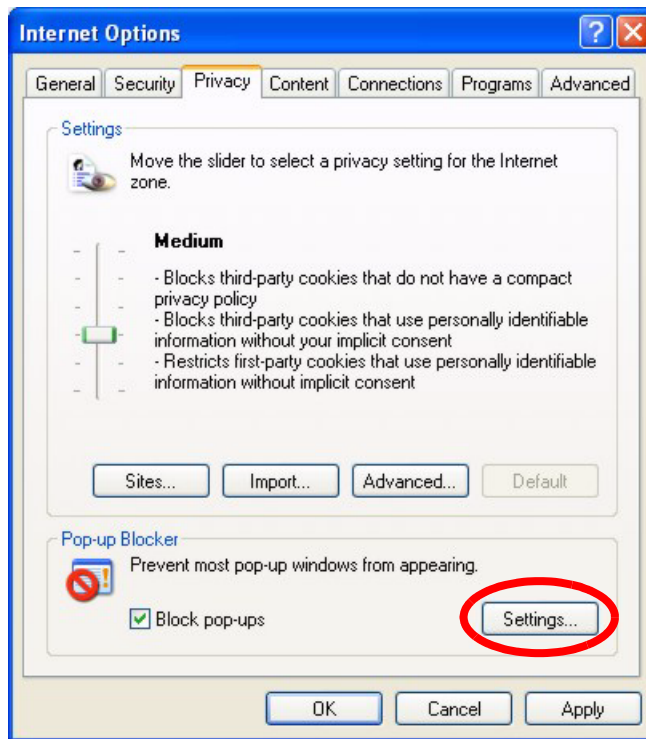
- 3 Click **Apply** to save this setting.

30.2.1.1.2 Enable pop-up Blockers with Exceptions

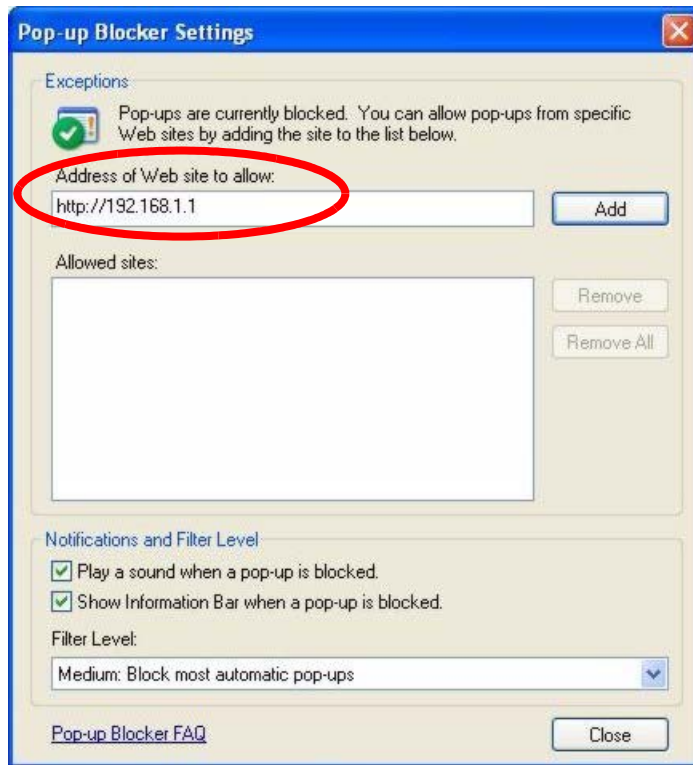
Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

- 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 146 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 147 Pop-up Blocker Settings

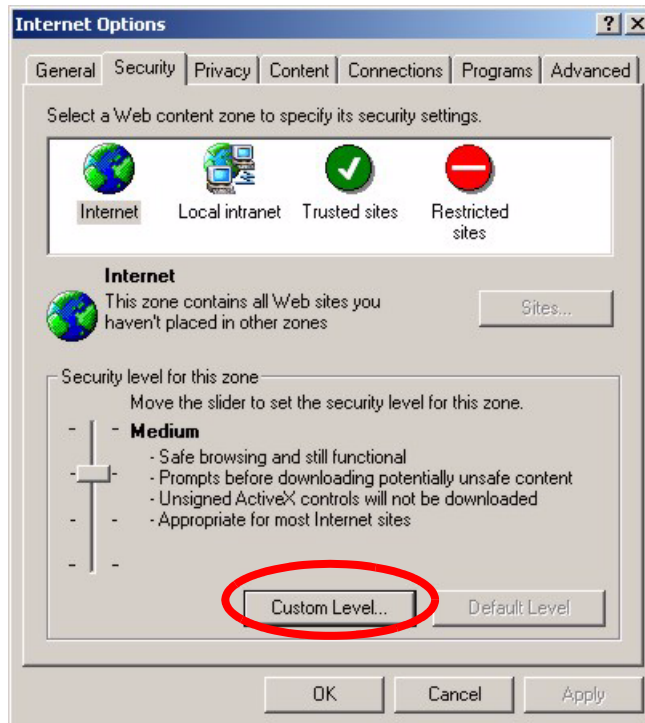
5 Click **Close** to return to the **Privacy** screen.

6 Click **Apply** to save this setting.

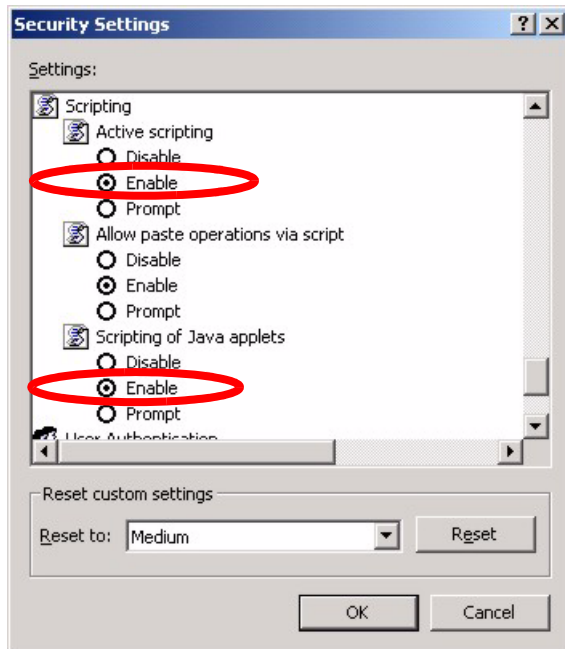
30.2.1.2 JavaScripts

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.

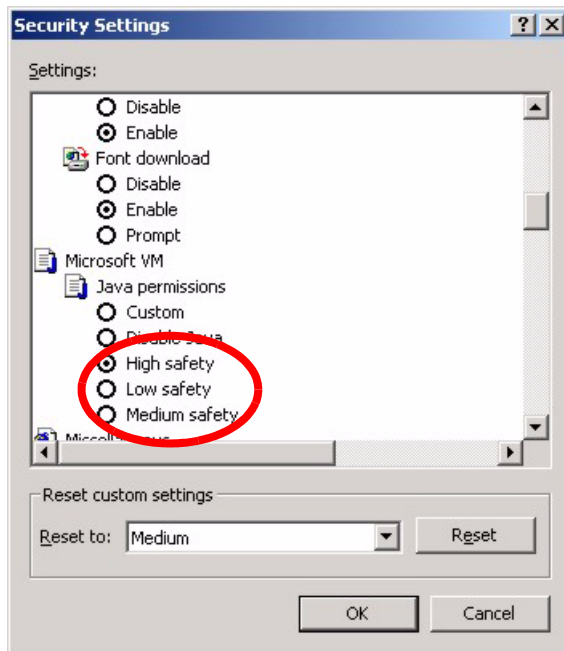
Figure 148 Internet Options

- 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 149 Security Settings - Java Scripting

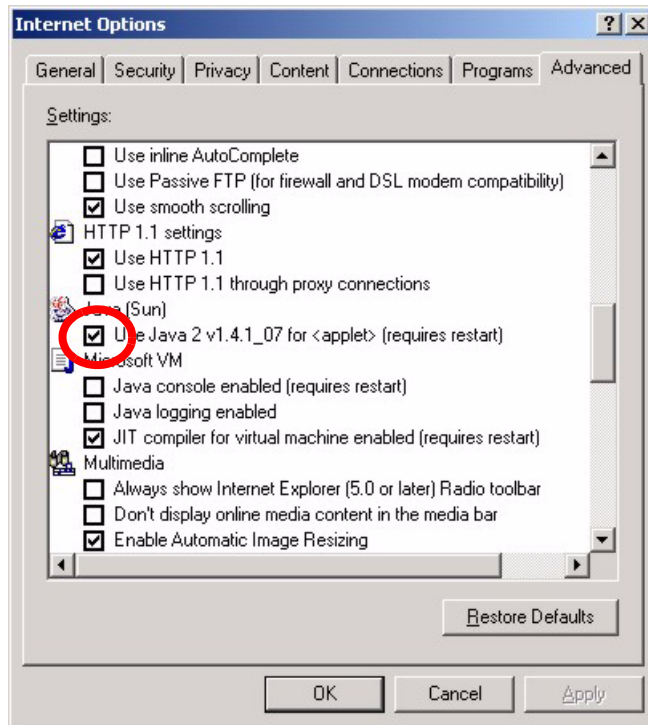
30.2.1.3 Java Permissions

- 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 150 Security Settings - Java

30.2.1.3.1 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 151 Java (Sun)

30.3 Problems with the Password

Table 66 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.

APPENDIX A

Product Specifications

These are the switch product specifications.

Table 67 General Product Specifications

Interface	<ul style="list-style-type: none"> 24 10/100/1000 Base-TX interfaces Two mini-GBIC ports Auto-negotiation Auto-MDI/MDIX Compliant with IEEE 802.3/3u Back pressure flow control for half duplex Flow control for full duplex (IEEE 802.3x) RJ-45 Ethernet cable connector Rate limiting at 1Kbps steps
Bridging	<ul style="list-style-type: none"> 8K MAC addresses Static MAC address filtering (port lock) Broadcast storm control Limited maximum number of MAC addresses per port
Switching	<ul style="list-style-type: none"> Switching fabric: 8.8Gbps, non-blocking Max. Frame size: 1522 bytes Forwarding frame: IEEE 802.3, IEEE 802.1q, Ethernet II, PPPoE Prevent the forwarding of corrupted packets
STP	<ul style="list-style-type: none"> IEEE 802.1d spanning tree protocol IEEE 802.1w, rapid reconfiguration to recover network failure
QoS	<ul style="list-style-type: none"> IEEE 802.1p Four priority queues Supports RFC 2475 DiffServ, DSCP to IEEE 802.1p priority mapping
Security	<ul style="list-style-type: none"> IEEE 802.1x port-based authentication Static MAC Address Forward (up to 24 enteries per port)
VLAN	<ul style="list-style-type: none"> Port-based VLAN setting Tag-based (IEEE 802.1Q) VLAN Number of VLAN: 4K (64 static VLANs) Supports GVRP
Link aggregation	<ul style="list-style-type: none"> Supports IEEE 802.3ad; static and dynamic (LACP) port trunking Up to six groups and each group can aggregate up to eight ports
Port mirroring	<ul style="list-style-type: none"> All ports support port mirroring
Bandwidth control	<ul style="list-style-type: none"> Supports rate limiting at 64Kbps increment Supports IGMP snooping

Table 68 Management Specifications

System Control	Alarm/Status surveillance LED indication for alarm and system status Performance monitoring Line speed Four RMON groups (history, statistics, alarms, and events) Throughput monitoring CMP packet transmission Port mirroring and aggregation Spanning Tree Protocol IGMP snooping Firmware upgrade and download through FTP/TFTP Login authorization and security levels (read only and read/write) Self diagnostics FLASH memory
Network Management	CLI through console port and telnet Web-based management Clustering: up to 24 switches can be manage by one IP SNMP RMON groups (history, statistics, alarms and events)
MIB	RFC1213 MIB II RFC1493 Bridge MIB RFC1643 Ethernet MIB RFC1757 Four groups of RMON RFC1155 SMI RFC2674 Bridge MIB extension (for IEEE 802.1Q)

Table 69 Physical and Environmental Specifications

LEDs	Main switch: BPS, PWR, SYS, ALM, Per Port: LNK/ACT, FDX Per Mini-GBIC Slot: LNK, ACT Per Management Port: 10, 100
Dimension	Main switch: 438(W) x 270(D) x 44.45(H) mm (17.2(W) x 10.6(D) x 1.75(H) inches), 19-inch rack-mount width, 1 U height
Weight	3.8Kg
Temperature	Operating: 0° C ~ 45° C (32° F ~ 113° F) Storage: -25° C ~ 70° C (13° F ~ 158° F)
Humidity	10 ~ 90% (non-condensing)
Power Supply	Overload protection 100 - 240VAC 50/60Hz 1.5A max internal universal power supply

Table 69 Physical and Environmental Specifications (continued)

Safety	UL 60950-1 CSA 60950-1 EN 60950-1 IEC 60950-1
EMC	FCC Part 15 (Class A) CE EMC (Class A)

APPENDIX B

IP Subnetting

IP Addressing

Routers “route” based on the network number. The router that delivers the data packet to the correct destination host uses the host ID.

IP Classes

An IP address is made up of four octets (eight bits), written in dotted decimal notation, for example, 192.168.1.1. IP addresses are categorized into different classes. The class of an address depends on the value of its first octet.

- Class “A” addresses have a 0 in the left most bit. In a class “A” address the first octet is the network number and the remaining three octets make up the host ID.
- Class “B” addresses have a 1 in the left most bit and a 0 in the next left most bit. In a class “B” address the first two octets make up the network number and the two remaining octets make up the host ID.
- Class “C” addresses begin (starting from the left) with 1 1 0. In a class “C” address the first three octets make up the network number and the last octet is the host ID.
- Class “D” addresses begin with 1 1 1 0. Class “D” addresses are used for multicasting. (There is also a class “E” address. It is reserved for future use.)

Table 70 Classes of IP Addresses

IP ADDRESS:		OCTET 1	OCTET 2	OCTET 3	OCTET 4
Class A	0	Network number	Host ID	Host ID	Host ID
Class B	10	Network number	Network number	Host ID	Host ID
Class C	110	Network number	Network number	Network number	Host ID

Note: Host IDs of all zeros or all ones are not allowed.

Therefore:

A class “C” network (8 host bits) can have $2^8 - 2$ or 254 hosts.

A class “B” address (16 host bits) can have $2^{16} - 2$ or 65534 hosts.

A class “A” address (24 host bits) can have $2^{24} - 2$ hosts (approximately 16 million hosts).

Since the first octet of a class “A” IP address must contain a “0”, the first octet of a class “A” address can have a value of 0 to 127.

Similarly the first octet of a class “B” must begin with “10”, therefore the first octet of a class “B” address has a valid range of 128 to 191. The first octet of a class “C” address begins with “110”, and therefore has a range of 192 to 223.

Table 71 Allowed IP Address Range By Class

CLASS	ALLOWED RANGE OF FIRST OCTET (BINARY)	ALLOWED RANGE OF FIRST OCTET (DECIMAL)
Class A	00000000 to 01111111	0 to 127
Class B	10000000 to 10111111	128 to 191
Class C	11000000 to 11011111	192 to 223
Class D	11100000 to 11101111	224 to 239

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). A subnet mask has 32 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.

Subnet masks are expressed in dotted decimal notation just as IP addresses are. The “natural” masks for class A, B and C IP addresses are as follows.

Table 72 “Natural” Masks

CLASS	NATURAL MASK
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Subnetting

With subnetting, the class arrangement of an IP address is ignored. For example, a class C address no longer has to have 24 bits of network number and 8 bits of host ID. With subnetting, some of the host ID bits are converted into network number bits. By convention, subnet masks always consist of a continuous sequence of ones beginning from the left most bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

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 mask 255.255.255.128.

The following table shows all possible subnet masks for a class “C” address using both notations.

Table 73 Alternative Subnet Mask Notation

SUBNET MASK IP ADDRESS	SUBNET MASK “1” BITS	LAST OCTET BIT VALUE
255.255.255.0	/24	0000 0000
255.255.255.128	/25	1000 0000
255.255.255.192	/26	1100 0000
255.255.255.224	/27	1110 0000
255.255.255.240	/28	1111 0000
255.255.255.248	/29	1111 1000
255.255.255.252	/30	1111 1100

The first mask shown is the class “C” natural mask. Normally if no mask is specified it is understood that the natural mask is being used.

Example: Two Subnets

As an example, you have a class “C” address 192.168.1.0 with subnet mask of 255.255.255.0.

Table 74 Two Subnets Example

	NETWORK NUMBER	HOST ID
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask	255.255.255.	0
Subnet Mask (Binary)	11111111.11111111.11111111.	00000000

The first three octets of the address make up the network number (class “C”). You want to have two separate networks.

Divide the network 192.168.1.0 into two separate subnets by converting one of the host ID bits of the IP address to a network number bit. The “borrowed” host ID bit can be either “0” or “1” thus giving two subnets; 192.168.1.0 with mask 255.255.255.128 and 192.168.1.128 with mask 255.255.255.128.

Note: In the following charts, shaded/bolded last octet bit values indicate host ID bits “borrowed” to form network ID bits. The number of “borrowed” host ID bits determines the number of subnets you can have. The remaining number of host ID bits (after “borrowing”) determines the number of hosts you can have on each subnet.

Table 75 Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	10000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 76 Subnet 2

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	10000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	10000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

The remaining 7 bits determine the number of hosts each subnet can have. Host IDs of all zeros represent the subnet itself and host IDs of all ones are the broadcast address for that subnet, so the actual number of hosts available on each subnet in the example above is $2^7 - 2$ or 126 hosts for each subnet.

192.168.1.0 with mask 255.255.255.128 is the subnet itself, and 192.168.1.127 with mask 255.255.255.128 is the directed broadcast address for the first subnet. Therefore, the lowest IP address that can be assigned to an actual host for the first subnet is 192.168.1.1 and the highest is 192.168.1.126. Similarly the host ID range for the second subnet is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The above example illustrated using a 25-bit subnet mask to divide a class “C” address space into two subnets. Similarly to divide a class “C” address into four subnets, you need to “borrow” two host ID bits to give four possible combinations of 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 (all 0’s is the subnet itself, all 1’s is the broadcast address on the subnet).

Table 77 Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	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 78 Subnet 2

	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 79 Subnet 3

	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 80 Subnet 4

	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 8 subnets (001, 010, 011, 100, 101, 110).

The following table shows class C IP address last octet values for each subnet.

Table 81 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
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	223	254	255

The following table is a summary for class “C” subnet planning.

Table 82 Class C 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

Subnetting With Class A and Class B Networks.

For class “A” and class “B” addresses the subnet mask also determines which bits are part of the network number and which are part of the host ID.

A class “B” address has two host ID octets available for subnetting and a class “A” address has three host ID octets (see [Table 70 on page 243](#)) available for subnetting.

The following table is a summary for class “B” subnet planning.

Table 83 Class B 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
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Index

Symbols

“standby” ports [109](#)

Numerics

110V AC [5](#)

230V AC [5](#)

802.1P priority [76](#)

A

AC [5](#)

Access control [151](#)

 Access priority [151](#)

 Limitation [151](#)

 Login account [155](#)

 Remote management [163](#)

 Service port [162](#)

 SNMP [152](#)

Accessories [5](#)

Address Resolution Protocol (ARP) [175](#)

Administrator password [155](#)

Aggregator ID [111](#)

Aging time [70](#)

Airflow [5](#)

Alternative Subnet Mask Notation [245](#)

American Wire Gauge [5](#)

Application [32](#)

 Backbone [32](#)

 Bridging [32](#)

 IEEE 802.1Q VLAN [33](#)

 Switched workgroup [33](#)

ARP [175](#)

 How it works [175](#)

 View [175](#)

Authority [4](#)

Automatic VLAN registration [78](#)

AWG [5](#)

B

Basement [5](#)

Basic setting [65](#)

BPDUs (Bridge Protocol Data Units) [94](#)

Bridge Protocol Data Units (BPDUs) [94](#)

Broadcast storm control [103](#)

C

Cables, Connecting [5](#)

CFI (Canonical Format Indicator) [77](#)

Change password [51](#)

Changes or Modifications [4](#)

CI Commands [179](#)

Class of Service (CoS) [141](#)

CLI Command

 Configure tagged VLAN example [220](#)

 Static VLAN Table example [225](#)

Cluster management [31](#), [167](#)

 Cluster manager [167](#), [171](#)

 Cluster member [167](#), [171](#)

 Cluster member firmware upgrade [169](#)

 Network example [167](#)

 Setup [170](#)

 Specification [167](#)

 Status [168](#)

 Switch models [167](#)

 VID [171](#)

 Web configurator [169](#)

Cluster manager [167](#)

Cluster member [167](#)

Command

 Forwarding Process Example [225](#)

 Summary [183](#)

 Syntax conventions [179](#)

Command Line Interface

 Accessing [177](#)

 Introduction [177](#)

Configuration file [53](#)

 Backup [146](#)

 Restore [53](#), [146](#)

Connecting Cables [5](#)

Console port [31](#)

 Settings [41](#)

Copyright [3](#)
Corrosive Liquids [5](#)
Covers [5](#)
CPU management port [85](#)
CRC (Cyclic Redundant Check) [63](#)
Current date [69](#)
Current time [69](#)
Customer Support [7](#)

D

Damage [5](#)
Dampness [5](#)
Danger [5](#)
DHCP [29](#)
DHCP (Dynamic Host Configuration Protocol) [29](#)
Diagnostic [165](#)

- Ethernet port test [165](#)
- Ping [165](#)
- System log [165](#)

Differentiated Service (DiffServ) [141](#)
Differentiated Services [29](#)
DiffServ [29](#), [141](#)

- Activate [142](#)
- DS field [141](#)
- DSCP [141](#)
- DSCP-to-IEEE802.1p mapping [142](#)
- Network example [141](#)
- PHB [141](#)

DS (Differentiated Services) [141](#)
DSCP

- DSCP-to-IEEE802.1p mapping [142](#)
- Service level [141](#)
- What it does [141](#)

DSCP (DiffServ Code Point) [141](#)
Dust [5](#)
DVLAN Table [219](#)
Dynamic link aggregation [109](#)

E

Egress port [88](#)
Electric Shock [5](#)
Electrical Pipes [5](#)
Electrocution [5](#)
Ethernet broadcast address [175](#)
Ethernet port test [165](#)
Ethernet ports [42](#)

Default settings [42](#)
Europe [5](#)
Exposure [5](#)
Extended authentication protocol [115](#)
External authentication server [115](#)

F

FCC

- Compliance [4](#)

Feature

- Hardware [31](#)

File Transfer using FTP

- command example [149](#)

Filename convention [148](#)
Filtering database [173](#)
Firmware [66](#)

- Upgrade [145](#), [169](#)

Flow control [76](#)

- Back pressure [76](#)
- IEEE802.3x [76](#)

Front panel [41](#)
FTP [148](#)

- File transfer procedure [149](#)
- Restrictions over WAN [150](#)

G

GARP [78](#), [220](#)
GARP (Generic Attribute Registration Protocol) [78](#)
garp status [221](#)
GARP Status Command [221](#)
GARP terminology [78](#)
GARP timer [70](#), [78](#)
Gas Pipes [5](#)
General setup [67](#)
Getting help [54](#)
GMT (Greenwich Mean Time) [69](#)
GVRP [78](#), [84](#), [220](#)
GVRP (GARP VLAN Registration Protocol) [78](#), [213](#)
gvrp disable [223](#)
gvrp enable [222](#)
gvrp status [222](#)

H

Hardware installation [37](#)
Hardware overview [41](#)
High Voltage Points [5](#)
Host IDs [243](#)
How SSH works [156](#)
HTTPS [158](#)
HTTPS Example [159](#)

I

IEEE 802.1p [71](#)
IEEE 802.1Q Tagged VLAN [219](#)
IEEE 802.1x [115](#)
 Activate [116](#)
 Note [115](#)
 Reauthentication [118](#)
IGMP snooping [125](#)
Ingress port [87](#)
Installation
 Freestanding [37](#)
 Precautions [38](#)
 Rack-mounting [38](#)
Introduction [29](#)
IP Addressing [243](#)
IP Classes [243](#)
IP interface [71](#)
IP setup [71](#)
iStacking [31](#)

L

LACP [109](#)
 System priority [113](#)
 Timeout [113](#)
LEDs [44](#)
Lightning [5](#)
Link Aggregate Control Protocol (LACP) [109](#)
Link aggregation [30](#), [109](#)
 Dynamic [109](#)
 ID information [110](#)
 Setup [111](#)
 Status [111](#)
Liquids, Corrosive [5](#)
Lockout [52](#)
Log [165](#)

Login [47](#)
 Password [51](#)
Login account [155](#)
 Administrator [155](#)
 Non-administrator [155](#)
 Number of [155](#)
Login password [156](#)

M

MAC (Media Access Control) [66](#)
MAC address [66](#), [175](#)
MAC address learning [31](#), [70](#), [89](#)
MAC table [173](#)
 How it works [173](#)
 View [174](#)
Maintenance [145](#)
Management Information Base (MIB) [152](#)
Management port [88](#)
MIB [152](#)
 Supported MIBs [153](#)
Mini GBIC ports [42](#)
 Connection speed [43](#)
 Connector type [43](#)
 Transceiver installation [43](#)
 Transceiver removal [43](#)
Mirror port [107](#)
Modifications [4](#)
Mounting brackets [38](#)
MSA (MultiSource Agreement) [42](#)
MTU (Multi-Tenant Unit) [69](#)

N

Network management system (NMS) [152](#)
North America [5](#)
NTP (RFC-1305) [69](#)

O

Opening [5](#)

P

Password [51](#), [172](#)
PHB (Per-Hop Behavior) [141](#)
Ping [165](#)
Pipes [5](#)
Pool [5](#)
Port authentication [115](#)
 IEEE802.1x [116](#)
 RADIUS server [118](#)
Port Based VLAN Type [70](#)
Port details [61](#)
Port isolation [87](#)
Port mirroring [30](#), [107](#)
 Mirror port [107](#)
Port redundancy [109](#)
Port security [31](#), [121](#)
Port setup [74](#)
Port speed/duplex [76](#)
Port status [59](#)
Port VID
 Default for all ports [195](#)
Port VLAN trunking [79](#)
Port-based VLAN [85](#)
 All connected [87](#)
 Port isolation [87](#)
 Setting Wizard [87](#)
Power Adaptor [5](#)
Power Cord [5](#)
Power Outlet [5](#)
Power Supply [5](#)
Power Supply, repair [5](#)
Priority [71](#)
Priority level [71](#)
Priority queue assignment [71](#)
Product specification [239](#)
PVID [77](#), [84](#)
PVID (Priority Frame) [77](#)

Q

Qualified Service Personnel [5](#)
Quality of Service (QoS) [141](#)
Queue weight [124](#)
Queuing [30](#), [123](#)
Queuing algorithm [123](#), [124](#)
Queuing method [123](#), [124](#)

R

RADIUS [115](#)
RADIUS (Remote Authentication Dial In User Service) [115](#)
RADIUS server [115](#)
 Advantages [115](#)
 Network example [115](#)
 Settings [118](#)
Rear panel [44](#)
Related Documentation [27](#)
Remote management [163](#)
 Service [164](#)
 Trusted computers [164](#)
Removing [5](#)
Repair [5](#)
Reset [53](#)
Reset to factory default settings [147](#)
Restore configuration [53](#)
Risk [5](#)
Risks [5](#)
Round Robin Scheduling [123](#)
RSTP (Rapid STP) [30](#)
Rubber feet [37](#)

S

Safety Warnings [5](#)
Service [5](#), [6](#)
Service access control [162](#)
 Service port [163](#)
Service Personnel [5](#)
Shock, Electric [5](#)
Simple Network Management Protocol (SNMP) [152](#)
SNMP [152](#)
 Agent [152](#)
 Communities [154](#)
 Management model [152](#)
 Manager [152](#)
 MIB [152](#), [153](#)
 Network components [152](#)
 Object variables [152](#)
 Protocol operations [153](#)
 Setup [154](#)
 Traps [153](#)
 Versions supported [152](#)
Spanning Tree Protocol (STP) [93](#)
SSH [156](#)
SSH Implementation [157](#)
Static MAC address [31](#), [121](#)

- Static MAC forwarding [89](#)
- Static VLAN [81](#)
 - Control [83](#)
 - Tagging [83](#)
- Status [48, 59](#)
 - LED [44](#)
 - Link aggregation [111](#)
 - Port [59](#)
 - Port details [61](#)
 - STP [94](#)
 - VLAN [80](#)
- STP [93](#)
 - Bridge ID [95](#)
 - Bridge priority [98](#)
 - Configuration [96](#)
 - Designated bridge [94](#)
 - Forwarding Delay [98](#)
 - Hello BPDU [94](#)
 - Hello Time [95, 98](#)
 - How it works [94](#)
 - Max Age [95, 98](#)
 - Path cost [93, 98](#)
 - Port priority [98](#)
 - Port state [94](#)
 - Root port [94](#)
 - Status [94](#)
 - Terminology [93](#)
- STP (Spanning Tree Protocol) [30](#)
- Strict Priority Queuing (SPQ) [123](#)
- Subnet Masks [244](#)
- Subnetting [244](#)
- Supply Voltage [5](#)
- SVLAN Table [219](#)
- Swimming Pool [5](#)
- Switch lockout [52](#)
- Switch reset [53](#)
- Switch setup [70](#)
- Syntax Conventions [27](#)
- sys Commands
 - examples [201, 208, 210](#)
- sys log disp [202, 208, 210](#)
- sys sw mac list [204](#)
- System information [65](#)
- System log [165](#)
- System reboot [147](#)
- System up time [60](#)

T

- Tagged VLAN [77](#)
- Telecommunication Line Cord. [5](#)
- Thunderstorm [5](#)

- Time
 - Current [69](#)
 - Time zone [69](#)
 - Timeserver [69](#)
- Time (RFC-868) [69](#)
- Time service protocol [69](#)
 - Time format [69](#)
- Time zone [69](#)
- Timeserver [69](#)
- Transceiver
 - Installation [43](#)
 - Removal [43](#)
- Trap
 - Destination [154](#)
- Traps [153](#)
- Trunk group [109](#)
- Trunking [30, 109](#)
- Type of Service (ToS) [141](#)

U

- UTC (Universal Time Coordinated) [69](#)

V

- Vendor [5](#)
- Ventilation [37](#)
- Ventilation holes [37](#)
- Ventilation Slots [5](#)
- VID [77, 81](#)
 - Number of possible VIDs [77](#)
 - Priority frame [77](#)
- VID (VLAN Identifier) [77](#)
- VLAN [69, 77](#)
 - Acceptable frame type [85](#)
 - Automatic registration [78](#)
 - Explicit Tagging [219](#)
 - ID [77](#)
 - ID (VID) [220](#)
 - Implicit Tagging [219](#)
 - Ingress filtering [84](#)
 - Introduction [69](#)
 - Number of VLANs [81](#)
 - Port number [81](#)
 - Port settings [83](#)
 - Port-based VLAN [85](#)
 - Registration Information [219](#)
 - Static VLAN [81](#)
 - Status [80, 81](#)
 - Tagged [77](#)

- Trunking [79](#)
- Type [70](#), [79](#)
- VLAN (Virtual Local Area Network) [29](#), [69](#)
- VLAN Databases [219](#)
- VLAN trunking [85](#)
- vlan1q port accept [223](#)
- vlan1q port gvrp [224](#)
- vlan1q svlan active [226](#)
- vlan1q svlan delentry [225](#)
- vlan1q svlan inactive [226](#)
- vlan1q svlan list [226](#)
- vlan1q svlan setentry [224](#)
- Voltage Supply [5](#)
- Voltage, High [5](#)

W

- Wall Mount [5](#)
- Warnings [5](#)
- Water [5](#)
- Water Pipes [5](#)
- Web configuration
 - Screen summary [49](#)
- Web configurator
 - Getting help [54](#)
 - Home [48](#)
 - Login [47](#)
 - Logout [54](#)
 - Navigation panel [48](#)
- Weighted Round Robin Scheduling (WRR) [124](#)
- Wet Basement [5](#)

Z

- ZyNOS (ZyXEL Network Operating System) [148](#)
- ZyXEL Limited Warranty
 - Note [6](#)