

# **GS-4012F/4024**

*Ethernet Switch*

## ***User's Guide***

Version 3.60

1/2006

Edition 2

The logo for ZyXEL, featuring the word "ZyXEL" in a bold, blue, sans-serif font. The "Zy" is in a smaller font size than "XEL".

# 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](http://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.



## Registration

Register your product online for free future product updates and information at [www.zyxel.com](http://www.zyxel.com) for global products, or at [www.us.zyxel.com](http://www.us.zyxel.com) for North American products.

## 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 value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product is 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 of character 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](http://www.zyxel.com) for global products, or at [www.us.zyxel.com](http://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..... 2**
- Interference Statements and Warnings..... 3**
- ZyXEL Limited Warranty ..... 5**
- Customer Support ..... 6**
- Table of Contents ..... 8**
- List of Figures ..... 20**
- List of Tables ..... 26**
- Preface ..... 30**
  
- Chapter 1**
- Getting to Know Your Switch..... 32**
  - 1.1 Introduction ..... 32
  - 1.2 Software Features ..... 32
  - 1.3 Hardware Features ..... 35
  - 1.4 Applications ..... 36
    - 1.4.1 Backbone Application ..... 36
    - 1.4.2 Bridging Example ..... 37
    - 1.4.3 High Performance Switching Example ..... 37
    - 1.4.4 IEEE 802.1Q VLAN Application Examples ..... 38
      - 1.4.4.1 Tag-based VLAN Example ..... 38
      - 1.4.4.2 VLAN Shared Server Example ..... 39
  
- Chapter 2**
- Hardware Installation and Connection ..... 40**
  - 2.1 Freestanding Installation ..... 40
  - 2.2 Mounting the Switch on a Rack ..... 41
    - 2.2.1 Rack-mounted Installation Requirements ..... 41
      - 2.2.1.1 Precautions ..... 41
    - 2.2.2 Attaching the Mounting Brackets to the Switch ..... 41
    - 2.2.3 Mounting the Switch on a Rack ..... 41
  
- Chapter 3**
- Hardware Overview..... 44**
  - 3.1 Front Panel Connection ..... 44



3.1.1 Console Port .....	45
3.1.2 Gigabit Ethernet Ports .....	45
3.1.2.1 Default Ethernet Settings .....	45
3.1.3 SFP Slots .....	45
3.1.3.1 Transceiver Installation .....	46
3.1.3.2 Transceiver Removal .....	46
3.2 Rear Panel .....	47
3.2.1 Power Connector .....	47
3.2.2 External Backup Power Supply Connector .....	48
3.3 Front Panel LEDs .....	48
<b>Chapter 4</b>	
<b>The Web Configurator .....</b>	<b>50</b>
4.1 Introduction .....	50
4.2 System Login .....	50
4.3 The Status Screen .....	51
4.3.1 Change Your Password .....	55
4.4 Switch Lockout .....	56
4.5 Resetting the Switch .....	56
4.5.1 Reload the Configuration File .....	57
4.6 Logging Out of the Web Configurator .....	57
4.7 Help .....	58
<b>Chapter 5</b>	
<b>Initial Setup Example .....</b>	<b>60</b>
5.1 Overview .....	60
5.1.1 Configuring an IP Interface .....	60
5.1.2 Configuring DHCP Server Settings .....	61
5.1.3 Creating a VLAN .....	62
5.1.4 Setting Port VID .....	63
5.1.5 Enabling RIP .....	64
<b>Chapter 6</b>	
<b>System Status and Port Statistics .....</b>	<b>66</b>
6.1 Overview .....	66
6.2 Port Status Summary .....	66
6.2.1 Port Details .....	67
<b>Chapter 7</b>	
<b>Basic Setting .....</b>	<b>72</b>
7.1 Overview .....	72
7.2 System Information .....	72
7.3 General Setup .....	74

7.4 Introduction to VLANs .....	76
7.5 IGMP Snooping .....	77
7.6 Switch Setup Screen .....	77
7.7 IP Setup .....	79
7.7.1 IP Interfaces .....	79
7.8 Port Setup .....	81
<b>Chapter 8</b>	
<b>VLAN .....</b>	<b>84</b>
8.1 Introduction to IEEE 802.1Q Tagged VLANs .....	84
8.1.1 Forwarding Tagged and Untagged Frames .....	84
8.2 Automatic VLAN Registration .....	85
8.2.1 GARP .....	85
8.2.1.1 GARP Timers .....	85
8.2.2 GVRP .....	85
8.3 Port VLAN Trunking .....	86
8.4 Select the VLAN Type .....	86
8.5 Static VLAN .....	87
8.5.1 Static VLAN Status .....	87
8.5.2 Configure a Static VLAN .....	88
8.5.3 Configure VLAN Port Settings .....	90
8.6 Port-based VLANs .....	91
8.6.1 Configure a Port-based VLAN .....	91
<b>Chapter 9</b>	
<b>Static MAC Forward Setup .....</b>	<b>94</b>
9.1 Overview .....	94
9.2 Configuring Static MAC Forwarding .....	94
<b>Chapter 10</b>	
<b>Filtering .....</b>	<b>96</b>
10.1 Overview .....	96
10.2 Configure a Filtering Rule .....	96
<b>Chapter 11</b>	
<b>Spanning Tree Protocol .....</b>	<b>98</b>
11.1.1 STP Terminology .....	98
11.1.2 How STP Works .....	99
11.1.3 STP Port States .....	99
11.2 STP Status .....	99
11.2.1 Configure STP .....	101

<b>Chapter 12</b>	
<b>Bandwidth Control</b> .....	<b>104</b>
12.1 Introduction to Bandwidth Control .....	104
12.1.1 CIR and PIR .....	104
12.2 Bandwidth Control Setup .....	104
<b>Chapter 13</b>	
<b>Broadcast Storm Control</b> .....	<b>106</b>
13.1 Overview .....	106
13.2 Broadcast Storm Control Setup .....	106
<b>Chapter 14</b>	
<b>Mirroring</b> .....	<b>108</b>
14.1 Overview .....	108
14.2 Port Mirroring Configuration .....	108
<b>Chapter 15</b>	
<b>Link Aggregation</b> .....	<b>110</b>
15.1 Overview .....	110
15.1.1 Dynamic Link Aggregation .....	110
15.1.2 Link Aggregation ID .....	111
15.2 Link Aggregation Status .....	111
15.3 Link Aggregation Setup .....	112
<b>Chapter 16</b>	
<b>Port Authentication</b> .....	<b>116</b>
16.1 Overview .....	116
16.1.1 RADIUS .....	116
16.2 Configuring Port Authentication .....	116
16.2.1 Activating IEEE 802.1x Security .....	117
16.2.2 Configuring RADIUS Server Settings .....	118
<b>Chapter 17</b>	
<b>Port Security</b> .....	<b>120</b>
17.1 Overview .....	120
17.2 Port Security Setup .....	120
<b>Chapter 18</b>	
<b>Classifier</b> .....	<b>122</b>
18.1 Overview .....	122
18.2 Configuring the Classifier .....	122
18.3 Viewing and Editing Classifier Configuration .....	125
18.4 Classifier Example .....	126

<b>Chapter 19</b>	
<b>Policy Rule</b> .....	<b>128</b>
19.1 Overview .....	128
19.1.1 DiffServ .....	128
19.1.2 DSCP and Per-Hop Behavior .....	128
19.2 Configuring Policy Rules .....	128
19.3 Viewing and Editing Policy Configuration .....	131
19.4 Policy Example .....	132
<b>Chapter 20</b>	
<b>Queuing Method</b> .....	<b>134</b>
20.1 Overview .....	134
20.1.1 Strict Priority Queuing (SPQ) .....	134
20.1.2 Weighted Round Robin Scheduling (WRR) .....	135
20.2 Configuring Queuing .....	135
<b>Chapter 21</b>	
<b>VLAN Stacking</b> .....	<b>138</b>
21.1 Introduction .....	138
21.1.1 VLAN Stacking Example .....	138
21.2 VLAN Stacking Port Roles .....	139
21.3 VLAN Tag Format .....	139
21.3.1 Frame Format .....	140
21.4 Configuring VLAN Stacking .....	141
<b>Chapter 22</b>	
<b>Multicast</b> .....	<b>144</b>
22.1.1 IP Multicast Addresses .....	144
22.1.2 IGMP Filtering .....	144
22.1.3 IGMP Snooping .....	144
22.2 Multicast Status .....	145
22.2.1 Multicast Setting .....	145
22.2.2 IGMP Filtering Profile .....	147
22.3.1 Types of MVR Ports .....	149
22.3.2 MVR Modes .....	149
22.3.3 How MVR Works .....	149
22.4 General MVR Configuration .....	150
22.5.1 MVR Configuration Example .....	153
<b>Chapter 23</b>	
<b>Static Route</b> .....	<b>156</b>
23.1 Configuring .....	156

<b>Chapter 24</b>	
<b>RIP</b> .....	<b>158</b>
24.1 Overview .....	158
24.2 Configuring .....	158
<b>Chapter 25</b>	
<b>OSPF</b> .....	<b>160</b>
25.1 Overview .....	160
25.1.1 OSPF Autonomous Systems and Areas .....	160
25.1.2 How OSPF Works .....	161
25.1.3 Interfaces and Virtual Links .....	161
25.1.4 Configuring OSPF .....	161
25.2 OSPF Status .....	162
25.3 Enabling OSPF and General Settings .....	163
25.4 Configuring OSPF Areas .....	165
25.4.1 Viewing OSPF Area Information Table .....	166
25.5 Configuring OSPF Interfaces .....	167
25.6 OSPF Virtual Links .....	168
<b>Chapter 26</b>	
<b>IGMP</b> .....	<b>172</b>
26.1 Overview .....	172
26.2 Configuring .....	172
<b>Chapter 27</b>	
<b>DVMRP</b> .....	<b>174</b>
27.1 Overview .....	174
27.2 How DVMRP Works .....	174
27.2.1 DVMRP Terminology .....	175
27.3 Configuring DVMRP .....	175
27.3.1 DVMRP Configuration Error Messages .....	176
27.4 Default DVMRP Timer Values .....	177
<b>Chapter 28</b>	
<b>IP Multicast</b> .....	<b>178</b>
28.1 Overview .....	178
28.2 Configuring .....	178
<b>Chapter 29</b>	
<b>Differentiated Services</b> .....	<b>180</b>
29.1 Overview .....	180
29.1.1 DSCP and Per-Hop Behavior .....	180
29.1.2 DiffServ Network Example .....	180

- 29.2 Activating DiffServ ..... 181
- 29.3 DSCP-to-IEEE802.1p Priority Mapping ..... 182
  - 29.3.1 Configuring DSCP Settings ..... 182
  
- Chapter 30**
- DHCP ..... 184**
  
- 30.1 Overview ..... 184
  - 30.1.1 DHCP modes ..... 184
- 30.2 DHCP Server Status ..... 184
- 30.3 Configuring DHCP Server ..... 185
  - 30.3.1 DHCP Server Configuration Example ..... 187
- 30.4 DHCP Relay ..... 187
  - 30.4.1 DHCP Relay Agent Information ..... 188
  - 30.4.2 Configuring DHCP Relay ..... 188
  - 30.4.3 DHCP Relay Configuration Example ..... 189
  
- Chapter 31**
- VRRP ..... 190**
  
- 31.1 Overview ..... 190
- 31.2 Viewing VRRP Status ..... 191
- 31.3 Configuring VRRP ..... 192
  - 31.3.1 IP Interface Setup ..... 192
  - 31.3.2 VRRP Parameters ..... 193
    - 31.3.2.1 Advertisement Interval ..... 193
    - 31.3.2.2 Priority ..... 193
    - 31.3.2.3 Preempt Mode ..... 193
  - 31.3.3 Configuring VRRP Parameters ..... 194
- 31.4 VRRP Configuration Summary ..... 195
- 31.5 VRRP Configuration Examples ..... 195
  - 31.5.1 One Subnet Network Example ..... 195
  - 31.5.2 Two Subnets Example ..... 197
  
- Chapter 32**
- Maintenance ..... 200**
  
- 32.1 The Maintenance Screen ..... 200
- 32.2 Firmware Upgrade ..... 200
- 32.3 Restore a Configuration File ..... 201
- 32.4 Backing Up a Configuration File ..... 201
- 32.5 Load Factory Defaults ..... 202
- 32.6 Reboot System ..... 202
- 32.7 FTP Command Line ..... 203
  - 32.7.1 Filename Conventions ..... 203
    - 32.7.1.1 Example FTP Commands ..... 203

32.7.2 FTP Command Line Procedure .....	204
32.7.3 GUI-based FTP Clients .....	204
32.7.4 FTP Restrictions .....	205
<b>Chapter 33</b>	
<b>Access Control.....</b>	<b>206</b>
33.1 Overview .....	206
33.2 The Access Control Main Screen .....	206
33.3 About SNMP .....	207
33.3.1 Supported MIBs .....	208
33.3.2 SNMP Traps .....	208
33.3.3 Configuring SNMP .....	209
33.3.4 Setting Up Login Accounts .....	209
33.4 SSH Overview .....	211
33.5 How SSH works .....	211
33.6 SSH Implementation on the Switch .....	212
33.6.1 Requirements for Using SSH .....	212
33.7 Introduction to HTTPS .....	212
33.8 HTTPS Example .....	213
33.8.1 Internet Explorer Warning Messages .....	213
33.8.2 Netscape Navigator Warning Messages .....	214
33.8.3 The Main Screen .....	215
33.9 Service Port Access Control .....	217
33.10 Remote Management .....	217
<b>Chapter 34</b>	
<b>Diagnostic.....</b>	<b>220</b>
34.1 Diagnostic .....	220
<b>Chapter 35</b>	
<b>Cluster Management.....</b>	<b>222</b>
35.1 Overview .....	222
35.2 Cluster Management Status .....	223
35.2.1 Cluster Member Switch Management .....	224
35.2.1.1 Uploading Firmware to a Cluster Member Switch .....	224
35.3 Configuring Cluster Management .....	225
<b>Chapter 36</b>	
<b>MAC Table.....</b>	<b>228</b>
36.1 Overview .....	228
36.2 Viewing the MAC Table .....	229

---

<b>Chapter 37</b>	
<b>IP Table .....</b>	<b>230</b>
37.1 Overview .....	230
37.2 Viewing the IP Table .....	231
<b>Chapter 38</b>	
<b>ARP Table .....</b>	<b>232</b>
38.1 Overview .....	232
38.1.1 How ARP Works .....	232
38.2 Viewing the ARP Table .....	232
<b>Chapter 39</b>	
<b>Routing Table .....</b>	<b>234</b>
39.1 Overview .....	234
39.2 Viewing the Routing Table .....	234
<b>Chapter 40</b>	
<b>Introducing the Commands .....</b>	<b>236</b>
40.1 Overview .....	236
40.1.1 Switch Configuration File .....	236
40.2 Accessing the CLI .....	236
40.2.1 Access Priority .....	237
40.2.2 The Console Port .....	237
40.2.2.1 Initial Screen .....	237
40.2.3 Telnet .....	237
40.3 The Login Screen .....	238
40.4 Command Syntax Conventions .....	238
40.5 Getting Help .....	239
40.5.1 List of Available Commands .....	239
40.5.2 Detailed Command Information .....	240
40.6 Command Modes .....	240
40.7 Using Command History .....	241
40.8 Saving Your Configuration .....	241
40.8.1 Logging Out .....	242
40.9 Command Summary .....	242
40.9.1 User Mode .....	242
40.9.2 Enable Mode .....	243
40.9.3 General Configuration Mode .....	247
40.9.4 interface port-channel Commands .....	261
40.9.5 interface route-domain Commands .....	264
40.9.6 config-vlan Commands .....	265
40.10 mvr Commands .....	266



**Chapter 41**

<b>Command Examples.....</b>	<b>268</b>
41.1 Overview .....	268
41.2 show Commands .....	268
41.2.1 show system-information .....	268
41.2.2 show hardware-monitor .....	269
41.2.3 show ip .....	269
41.2.4 show logging .....	270
41.2.5 show interface .....	270
41.2.6 show mac address-table .....	271
41.3 ping .....	272
41.4 traceroute .....	273
41.5 Enabling RSTP .....	273
41.6 Configuration File Maintenance .....	274
41.6.1 Configuration Backup .....	274
41.6.2 Configuration Restoration .....	274
41.6.3 Using a Different Configuration File .....	275
41.6.4 Resetting to the Factory Default .....	275
41.7 no Command Examples .....	276
41.7.1 no mirror-port .....	276
41.7.2 no https timeout .....	276
41.7.3 no trunk .....	277
41.7.4 no port-access-authenticator .....	277
41.7.5 no ssh .....	278
41.8 interface Commands .....	278
41.8.1 interface port-channel .....	279
41.8.2 interface route-domain .....	279
41.8.3 bpdu-control .....	280
41.8.4 broadcast-limit .....	280
41.8.5 bandwidth-limit .....	281
41.8.6 mirror .....	282
41.8.7 gvrp .....	282
41.8.8 ingress-check .....	283
41.8.9 frame-type .....	283
41.8.10 spq .....	284
41.8.11 wrr .....	284
41.8.12 egress set .....	285
41.8.13 qos priority .....	285
41.8.14 name .....	286
41.8.15 speed-duplex .....	286

<b>Chapter 42</b>	
<b>IEEE 802.1Q Tagged VLAN Commands .....</b>	<b>288</b>
42.1 IEEE 802.1Q Tagged VLAN Overview .....	288
42.2 VLAN Databases .....	288
42.2.1 Static Entries (SVLAN Table) .....	288
42.2.2 Dynamic Entries (DVLAN Table) .....	289
42.3 Configuring Tagged VLAN .....	289
42.4 Global VLAN1Q Tagged VLAN Configuration Commands .....	290
42.4.1 GARP Status .....	290
42.4.2 GARP Timer .....	290
42.4.3 GVRP Timer .....	291
42.4.4 Enable GVRP .....	291
42.4.5 Disable GVRP .....	292
42.5 Port VLAN Commands .....	292
42.5.1 Set Port VID .....	292
42.5.2 Set Acceptable Frame Type .....	292
42.5.3 Enable or Disable Port GVRP .....	293
42.5.4 Modify Static VLAN .....	293
42.5.4.1 Modify a Static VLAN Table Example .....	294
42.5.4.2 Forwarding Process Example .....	294
42.5.5 Delete VLAN ID .....	294
42.6 Enable VLAN .....	295
42.7 Disable VLAN .....	295
42.8 Show VLAN Setting .....	295
<b>Chapter 43</b>	
<b>Troubleshooting.....</b>	<b>298</b>
43.1 Problems Starting Up the Switch .....	298
43.2 Problems Accessing the Switch .....	298
43.2.1 Pop-up Windows, JavaScripts and Java Permissions .....	299
43.2.1.1 Internet Explorer Pop-up Blockers .....	299
43.2.1.2 JavaScripts .....	302
43.2.1.3 Java Permissions .....	304
43.3 Problems with the Password .....	306
<b>Appendix A</b>	
<b>Product Specifications .....</b>	<b>308</b>
<b>Appendix B</b>	
<b>IP Subnetting.....</b>	<b>312</b>
<b>Index.....</b>	<b>320</b>



# List of Figures

Figure 1 Backbone Application .....	37
Figure 2 Bridging Application .....	37
Figure 3 High Performance Switched Workgroup Application .....	38
Figure 4 Tag-based VLAN Application .....	39
Figure 5 Shared Server Using VLAN Example .....	39
Figure 6 Attaching Rubber Feet .....	40
Figure 7 Attaching the Mounting Brackets .....	41
Figure 8 Mounting the Switch on a Rack .....	42
Figure 9 Front Panel: GS-4024 .....	44
Figure 10 Front Panel: GS-4012F .....	44
Figure 11 Transceiver Installation Example .....	46
Figure 12 Installed Transceiver .....	46
Figure 13 Opening the Transceiver's Latch Example .....	46
Figure 14 Transceiver Removal Example .....	47
Figure 15 Rear Panel: GS-4012F .....	47
Figure 16 Rear Panel: GS-4024 .....	47
Figure 17 Rear Panel: GS-4012F (DC Model) .....	47
Figure 18 Web Configurator: Login .....	51
Figure 19 Web Configurator Home Screen (Status) .....	51
Figure 20 Change Administrator Login Password .....	56
Figure 21 Resetting the Switch: Via the Console Port .....	57
Figure 22 Web Configurator: Logout Screen .....	58
Figure 23 Initial Setup Network Example: IP Interface .....	60
Figure 24 Initial Setup Network Example: VLAN .....	62
Figure 25 Initial Setup Network Example: Port VID .....	63
Figure 26 Status .....	66
Figure 27 Status: Port Details .....	68
Figure 28 System Info .....	73
Figure 29 General Setup .....	75
Figure 30 Switch Setup .....	77
Figure 31 IP Setup .....	80
Figure 32 Port Setup .....	82
Figure 33 Port VLAN Trunking .....	86
Figure 34 Switch Setup: Select VLAN Type .....	87
Figure 35 VLAN: VLAN Status .....	87
Figure 36 VLAN: Static VLAN .....	89
Figure 37 VLAN: VLAN Port Setting .....	90
Figure 38 Port Based VLAN Setup (All Connected) .....	92

Figure 39 Port Based VLAN Setup (Port Isolation) .....	92
Figure 40 Static MAC Forwarding .....	94
Figure 41 Filtering .....	96
Figure 42 Spanning Tree Protocol: Status .....	100
Figure 43 Spanning Tree Protocol: Configuration .....	101
Figure 44 Bandwidth Control .....	105
Figure 45 Broadcast Storm Control .....	106
Figure 46 Mirroring .....	108
Figure 47 Link Aggregation Control Protocol Status .....	111
Figure 48 Link Aggregation Control Protocol: Configuration .....	113
Figure 49 RADIUS Server .....	116
Figure 50 Port Authentication .....	117
Figure 51 Port Authentication: 802.1x .....	117
Figure 52 Port Authentication: RADIUS .....	118
Figure 53 Port Security .....	120
Figure 54 Classifier .....	123
Figure 55 Classifier: Summary Table .....	125
Figure 56 Classifier: Example .....	127
Figure 57 Policy .....	129
Figure 58 Policy: Summary Table .....	131
Figure 59 Policy Example .....	133
Figure 60 Queuing Method .....	135
Figure 61 VLAN Stacking Example .....	139
Figure 62 VLAN Stacking .....	141
Figure 63 Multicast: Status .....	145
Figure 64 Multicast: Setting .....	146
Figure 65 Multicast: Setting: IGMP Filtering Profile .....	147
Figure 66 MVR Network Example .....	149
Figure 67 MVR Multicast Television Example .....	150
Figure 68 Multicast: Setting: MVR .....	150
Figure 69 MVR: Group Configuration .....	152
Figure 70 MVR Configuration Example .....	153
Figure 71 MVR Configuration Example .....	153
Figure 72 MVR Group Configuration Example .....	154
Figure 73 MVR Group Configuration Example .....	154
Figure 74 Static Routing .....	156
Figure 75 RIP .....	159
Figure 76 OSPF Network Example .....	161
Figure 77 OSPF Status .....	162
Figure 78 OSPF Configuration: Activating and General Settings .....	164
Figure 79 OSPF Configuration: Area Setup .....	165
Figure 80 OSPF Configuration: Summary Table .....	166
Figure 81 OSPF Interface .....	167

Figure 82 OSPF Virtual Link .....	169
Figure 83 IGMP .....	172
Figure 84 How DVMRP Works .....	175
Figure 85 DVMRP .....	175
Figure 86 DVMRP: IGMP/RIP Not Set Error .....	176
Figure 87 DVMRP: Unable to Disable IGMP Error .....	176
Figure 88 DVMRP: Duplicate VID Error Message .....	177
Figure 89 IP Multicast .....	178
Figure 90 DiffServ: Differentiated Service Field .....	180
Figure 91 DiffServ Network Example .....	181
Figure 92 DiffServ .....	181
Figure 93 DiffServ: DSCP Setting .....	182
Figure 94 DHCP: DHCP Server Status .....	185
Figure 95 DHCP: Server .....	186
Figure 96 DHCP Server Network Example .....	187
Figure 97 DHCP Server Configuration Example .....	187
Figure 98 DHCP: Relay .....	188
Figure 99 DHCP Relay Network Example .....	189
Figure 100 DHCP Relay Configuration Example .....	189
Figure 101 VRRP: Example 1 .....	190
Figure 102 VRRP Status .....	191
Figure 103 VRRP Configuration: IP Interface .....	192
Figure 104 VRRP Configuration: VRRP Parameters .....	194
Figure 105 VRRP Configuration: Summary .....	195
Figure 106 VRRP Configuration Example: One Virtual Router Network .....	196
Figure 107 VRRP Example 1: VRRP Parameter Settings on Switch A .....	196
Figure 108 VRRP Example 1: VRRP Parameter Settings on Switch B .....	196
Figure 109 VRRP Example 1: VRRP Status on Switch A .....	197
Figure 110 VRRP Example 1: VRRP Status on Switch B .....	197
Figure 111 VRRP Configuration Example: Two Virtual Router Network .....	197
Figure 112 VRRP Example 2: VRRP Parameter Settings for VR2 on Switch A ....	198
Figure 113 VRRP Example 2: VRRP Parameter Settings for VR2 on Switch B ....	198
Figure 114 VRRP Example 2: VRRP Status on Switch A .....	198
Figure 115 VRRP Example 2: VRRP Status on Switch B .....	198
Figure 116 Maintenance .....	200
Figure 117 Firmware Upgrade .....	200
Figure 118 Restore Configuration .....	201
Figure 119 Backup Configuration .....	201
Figure 120 Load Factory Default: Conformation .....	202
Figure 121 Load Factory Default: Start .....	202
Figure 122 Reboot System: Confirmation .....	202
Figure 123 Reboot System: Start .....	203
Figure 124 Console Port Priority .....	206

Figure 125 Access Control .....	207
Figure 126 SNMP Management Model .....	207
Figure 127 Access Control: SNMP .....	209
Figure 128 Access Control: Logins .....	210
Figure 129 SSH Communication Example .....	211
Figure 130 How SSH Works .....	211
Figure 131 HTTPS Implementation .....	213
Figure 132 Security Alert Dialog Box (Internet Explorer) .....	214
Figure 133 Security Certificate 1 (Netscape) .....	214
Figure 134 Security Certificate 2 (Netscape) .....	215
Figure 135 Login Screen (Internet Explorer) .....	216
Figure 136 Login Screen (Netscape) .....	216
Figure 137 Access Control: Service Access Control .....	217
Figure 138 Access Control: Remote Management .....	218
Figure 139 Diagnostic .....	220
Figure 140 Clustering Application Example .....	222
Figure 141 Cluster Management: Status .....	223
Figure 142 Cluster Management: Cluster Member Web Configurator Screen .....	224
Figure 143 Example: Uploading Firmware to a Cluster Member Switch .....	225
Figure 144 Clustering Management Configuration .....	226
Figure 145 MAC Table Flowchart .....	228
Figure 146 MAC Table .....	229
Figure 147 IP Table Flowchart .....	230
Figure 148 IP Table .....	231
Figure 149 ARP Table .....	233
Figure 150 Routing Table Status .....	234
Figure 151 Initial Console Port Screen .....	237
Figure 152 CLI: Login Screen .....	238
Figure 153 CLI Help: List of Commands: Example 1 .....	239
Figure 154 CLI Help: List of Commands: Example 2 .....	240
Figure 155 CLI Help: Detailed Command Information: Example 1 .....	240
Figure 156 CLI: Help: Detailed Command Information: Example 2 .....	240
Figure 157 CLI: History Command Example .....	241
Figure 158 CLI: write memory .....	241
Figure 159 show system-information Command Example .....	268
Figure 160 show hardware-monitor Command Example .....	269
Figure 161 show ip Command Example .....	270
Figure 162 show logging Command Example .....	270
Figure 163 show interface Command Example .....	271
Figure 164 show mac address-table Command Example .....	272
Figure 165 ping Command Example .....	272
Figure 166 traceroute Command Example .....	273
Figure 167 Enable RSTP Command Example .....	274

Figure 168 CLI: Backup Configuration Example .....	274
Figure 169 CLI: Restore Configuration Example .....	275
Figure 170 CLI: boot config Command Example .....	275
Figure 171 CLI: reload config Command Example .....	275
Figure 172 CLI: Reset to the Factory Default Example .....	276
Figure 173 no mirror-port Command Example .....	276
Figure 174 no https timeout Command Example .....	276
Figure 175 no trunk Command Example .....	277
Figure 176 no port-access-authenticator Command Example .....	278
Figure 177 no ssh Command Example .....	278
Figure 178 interface Command Example .....	279
Figure 179 interface Command Example .....	280
Figure 180 interface bpdu-control Command Example .....	280
Figure 181 broadcast-limit Command Example .....	281
Figure 182 bandwidth-limit Command Example .....	281
Figure 183 mirror Command Example .....	282
Figure 184 gvrp Command Example .....	283
Figure 185 ingress-check Command Example .....	283
Figure 186 frame-type Command Example .....	284
Figure 187 spq Command Example .....	284
Figure 188 wrr Command Example .....	285
Figure 189 egress set Command Example .....	285
Figure 190 qos priority Command Example .....	286
Figure 191 name Command Example .....	286
Figure 192 speed-duplex Command Example .....	286
Figure 193 Tagged VLAN Configuration and Activation Example .....	289
Figure 194 CPU VLAN Configuration and Activation Example .....	290
Figure 195 GARP STATUS Command Example .....	290
Figure 196 GARP Timer Command Example .....	291
Figure 197 GVRP Status Command Example .....	291
Figure 198 vlan1q port default vid Command Example .....	292
Figure 199 frame type Command Example .....	293
Figure 200 no gvrp Command Example .....	293
Figure 201 Modifying Static VLAN Example .....	294
Figure 202 no vlan Command Example .....	295
Figure 203 show vlan Command Example .....	296
Figure 204 Pop-up Blocker .....	299
Figure 205 Internet Options .....	300
Figure 206 Internet Options .....	301
Figure 207 Pop-up Blocker Settings .....	302
Figure 208 Internet Options .....	303
Figure 209 Security Settings - Java Scripting .....	304
Figure 210 Security Settings - Java .....	305



Figure 211 Java (Sun) ..... 306

# List of Tables

Table 1 Front Panel .....	44
Table 2 Front Panel LEDs .....	48
Table 3 Navigation Panel Sub-links Overview .....	52
Table 4 Web Configurator Screen Sub-links Details .....	53
Table 5 Navigation Panel Links .....	53
Table 6 Status .....	67
Table 7 Status: Port Details .....	68
Table 8 System Info .....	73
Table 9 General Setup .....	75
Table 10 Switch Setup .....	78
Table 11 IP Setup .....	80
Table 12 Port Setup .....	82
Table 13 IEEE 802.1Q VLAN Terminology .....	85
Table 14 VLAN: VLAN Status .....	88
Table 15 VLAN: Static VLAN .....	89
Table 16 VLAN: VLAN Port Setting .....	90
Table 17 Port Based VLAN Setup .....	93
Table 18 Static MAC Forwarding .....	95
Table 19 Filtering .....	96
Table 20 STP Path Costs .....	98
Table 21 STP Port States .....	99
Table 22 Spanning Tree Protocol: Status .....	100
Table 23 Spanning Tree Protocol: Configuration .....	101
Table 24 Bandwidth Control .....	105
Table 25 Broadcast Storm Control .....	107
Table 26 Mirroring .....	109
Table 27 Link Aggregation ID: Local Switch .....	111
Table 28 Link Aggregation ID: Peer Switch .....	111
Table 29 Link Aggregation Control Protocol: Status .....	112
Table 30 Link Aggregation Control Protocol: Configuration .....	113
Table 31 Port Authentication: 802.1x .....	117
Table 32 Port Authentication: RADIUS .....	118
Table 33 Port Security .....	121
Table 34 Classifier .....	123
Table 35 Classifier: Summary Table .....	125
Table 36 Common Ethernet Types and Protocol Number .....	125
Table 37 Common IP Ports .....	126
Table 38 Policy .....	130

Table 39 Policy: Summary Table .....	131
Table 40 Physical Queue Priority .....	134
Table 41 Queuing Method .....	136
Table 42 VLAN Tag Format .....	139
Table 43 Single and Double Tagged 802.11Q Frame Format .....	140
Table 44 802.1Q Frame .....	140
Table 45 VLAN Stacking .....	141
Table 46 Multicast: Status .....	145
Table 47 Multicast: Setting .....	146
Table 48 Multicast: Setting: IGMP Filtering Profile .....	148
Table 49 Multicast: Setting: MVR .....	151
Table 50 Multicast: Setting: MVR: Group Configuration .....	152
Table 51 Static Routing .....	156
Table 52 RIP .....	159
Table 53 OSPF vs. RIP .....	160
Table 54 OSPF: Router Types .....	160
Table 55 OSPF Status .....	162
Table 56 OSPF Status: Common Output Fields .....	163
Table 57 OSPF Configuration: Activating and General Settings .....	164
Table 58 OSPF Configuration: Area Setup .....	165
Table 59 OSPF Configuration: Summary Table .....	166
Table 60 OSPF Interface .....	167
Table 61 OSPF Virtual Link .....	169
Table 62 IGMP .....	172
Table 63 DVMRP .....	176
Table 64 DVMRP: Default Timer Values .....	177
Table 65 IP Multicast .....	179
Table 66 DiffServ .....	181
Table 67 Default DSCP-IEEE802.1p Mapping .....	182
Table 68 DiffServ: DSCP Setting .....	183
Table 69 DHCP: DHCP Server Status .....	185
Table 70 DHCP: Server .....	186
Table 71 DHCP: Relay .....	188
Table 72 VRRP Status .....	191
Table 73 VRRP Configuration: IP Interface .....	193
Table 74 VRRP Configuration: VRRP Parameters .....	194
Table 75 VRRP Configuring: VRRP Parameters .....	195
Table 76 Filename Conventions .....	203
Table 77 Access Control Overview .....	206
Table 78 SNMP Commands .....	208
Table 79 SNMP Traps .....	208
Table 80 Access Control: SNMP .....	209
Table 81 Access Control: Logins .....	210

---

Table 82 Access Control: Service Access Control .....	217
Table 83 Access Control: Remote Management .....	218
Table 84 Diagnostic .....	220
Table 85 ZyXEL Clustering Management Specifications .....	222
Table 86 Cluster Management: Status .....	223
Table 87 FTP Upload to Cluster Member Example .....	225
Table 88 Clustering Management Configuration .....	226
Table 89 MAC Table .....	229
Table 90 IP Table .....	231
Table 91 ARP Table .....	233
Table 92 Routing Table Status .....	234
Table 93 Command Summary: User Mode .....	242
Table 94 Command Summary: Enable Mode .....	243
Table 95 Command Summary: Configuration Mode .....	247
Table 96 interface port-channel Commands .....	261
Table 97 interface route-domain Commands .....	264
Table 98 Command Summary: config-vlan Commands .....	265
Table 99 Command Summary: mvr Commands .....	266
Table 100 Troubleshooting the Start-Up of Your Switch .....	298
Table 101 Troubleshooting Accessing the Switch .....	298
Table 102 Troubleshooting the Password .....	306
Table 103 General Product Specifications .....	308
Table 104 Management Specifications .....	309
Table 105 Physical and Environmental Specifications .....	310
Table 106 Classes of IP Addresses .....	312
Table 107 Allowed IP Address Range By Class .....	313
Table 108 "Natural" Masks .....	313
Table 109 Alternative Subnet Mask Notation .....	314
Table 110 Two Subnets Example .....	314
Table 111 Subnet 1 .....	315
Table 112 Subnet 2 .....	315
Table 113 Subnet 1 .....	316
Table 114 Subnet 2 .....	316
Table 115 Subnet 3 .....	316
Table 116 Subnet 4 .....	317
Table 117 Eight Subnets .....	317
Table 118 Class C Subnet Planning .....	317
Table 119 Class B Subnet Planning .....	318



# Preface

Congratulations on your purchase of the GS-4012F/4024 Ethernet Switch.

This preface introduces you to the GS-4012F/4024 Ethernet Switch and discusses the conventions of this User's Guide. It also provides information on other related documentation.

There are two GS-4012F models. The GS-4012F DC model requires DC power supply input of -48 VDC or -60 VDC, 1.2A Max. The GS-4012F AC model requires 100~240VAC/1.5A power.

## About This User's Guide

This manual is designed to guide you through the installation and configuration of your GS-4012F/4024 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](http://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, “click the Apple icon, **Control Panels** and then **Modem**” means first click the Apple icon, then point your mouse pointer to **Control Panels** and then click **Modem**.
- For brevity's sake, we will use “e.g.,” as a shorthand for “for instance”, and “i.e.,” for “that is” or “in other words” throughout this manual.
- The GS-4012F/4024 Ethernet Switch may be referred to as “the switch” in this User's Guide.

## Graphics Icons Key

GS-4012F/4024 	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](mailto: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

Your switch is a stand-alone layer-3 Gigabit Ethernet switch. By integrating router functions, the switch performs wire-speed layer-3 routing in addition to layer-2 switching.

The GS-4024 comes with 24 Gigabit Ethernet ports and four Gigabit/mini-GBIC ports

The GS-4012F comes with with 12 min-GBIC slots and four Gigabit/mini-GBIC ports. There are two GS-4012F models. The GS-4012F DC model requires DC power supply input of -48 VDC or -60 VDC, 1.2A Max. The GS-4012F AC model requires 100~240VAC/1.5A power.

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.

#### IP Routing Domain

An IP interface (also known as an IP routing domain) is not bound to a physical port. Configure an IP routing domain to allow the switch to route traffic between different networks.

#### DHCP

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 server or disable it. When configured as a server, the switch provides the TCP/IP configuration for the clients. If you disable the DHCP service, you must have another DHCP server on your LAN, or else the computer must be manually configured.



## 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.

## VLAN Stacking

Use VLAN stacking to add an outer VLAN tag to the inner IEEE 802.1Q tagged frames that enter the network. By tagging the tagged frames (“double-tagged” frames), the service provider can manage up to 4,094 VLAN groups with each group containing up to 4,094 customer VLANs. This allows a service provider to provide different service, based on specific VLANs, for many different customers.

## 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.

## Classifier and Policy

You can create a policy to define actions to be performed on a traffic flow grouped by a classifier according to specific criteria such as the IP address, port number or protocol type, etc..

## Queuing

Queuing is used to help solve performance degradation when there is network congestion. Two scheduling services are supported: Strict Priority Queuing (SPQ) and Weighted Round Robin (WRR). This allows the switch to maintain separate queues for packets from each individual source or flow and prevent a source from monopolizing the bandwidth.

## Port Mirroring

Port mirroring allows you to copy traffic going from one or all ports to another or all ports in order that you can examine the traffic from the mirror port (the port you copy the traffic to) without interference.

## Static Route

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

## **IGMP**

IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a multicast group - it is not used to carry user data.

## **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.

## **IP Multicast**

With IP multicast, the switch delivers IP packets to a group of hosts on the network - not everybody. In addition, the switch can send packets to Ethernet devices that are not VLAN-aware by untagging (removing the VLAN tags) IP multicast packets.

## **Multicast VLAN Registration (MVR)**

Multicast VLAN Registration (MVR) is designed for applications (such as Media-on-Demand (MoD)) using multicast traffic across a network. MVR allows one single multicast VLAN to be shared among different subscriber VLANs on the network.

This improves bandwidth utilization by reducing multicast traffic in the subscriber VLANs and simplifies multicast group management.

## **RIP**

RIP (Routing Information Protocol) allows a routing device to exchange routing information with other routers.

## **OSPF**

OSPF (Open Shortest Path First) is a link-state protocol designed to distribute routing information within an autonomous system (AS). An autonomous system is a collection of networks using a common routing protocol to exchange routing information. OSPF is best suited for large networks.

## **DVMRP**

DVMRP (Distance Vector Multicast Routing Protocol) is a protocol used for routing multicast data within an autonomous system (AS). DVMRP provides multicast forwarding capability to a layer 3 switch that runs both the IPv4 protocol (with IP Multicast support) and the IGMP protocol.

## VRRP

Virtual Router Redundancy Protocol (VRRP), defined in RFC 2338, allows you to create redundant backup gateways to ensure that the default gateway of a host is always available.

## 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.

### Mini-GBIC Slots

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

## **Gigabit Ethernet Ports**

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

## **Management Port**

Connect a computer to this port for management purposes. You cannot access the network through this port.

## **Console Port**

Use the console port for local management of the switch.

## **Backup Power Supply Port**

Connect a backup power supply device to this port to ensure uninterrupted network connection in the event of a power failure.

## **Fans**

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

## **Power**

The GS-4012F AC model and GS-4024 require 100~240VAC/1.5A power. The GS-4012F DC model requires DC power supply input of -48 VDC or -60 VDC, 1.2A Max.

# **1.4 Applications**

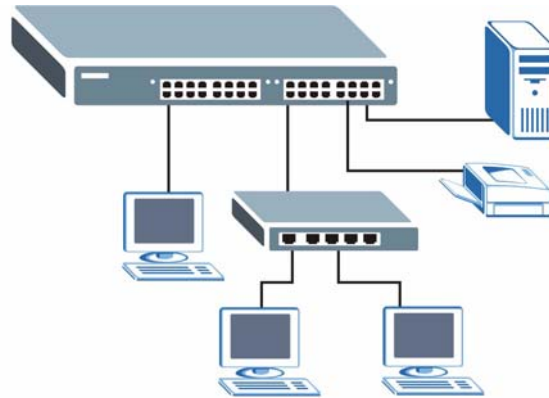
This section shows a few examples of using the switch in various network environments.

## **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.

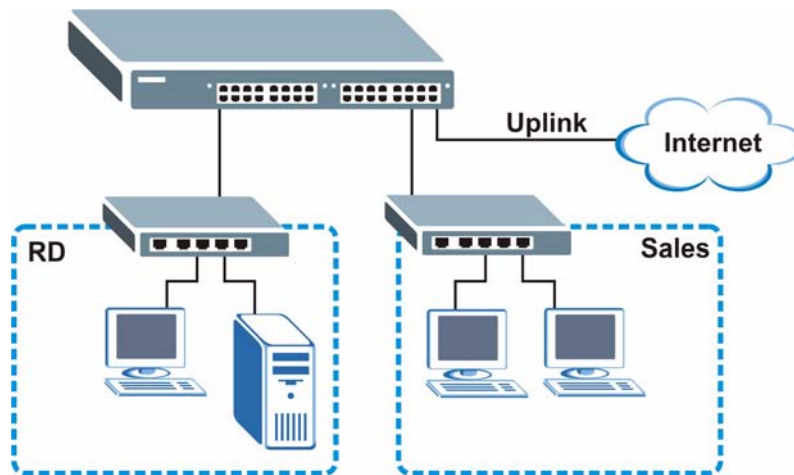
In this example, all computers can share high-speed applications on the server. To expand the network, simply add more networking devices such as switches, routers, computers, print servers etc.

**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.

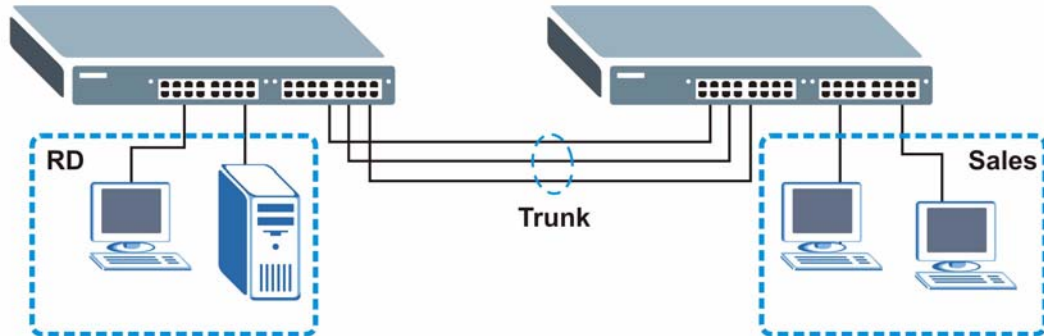
**Figure 2** Bridging Application

## 1.4.3 High Performance Switching 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 Workgroup Application



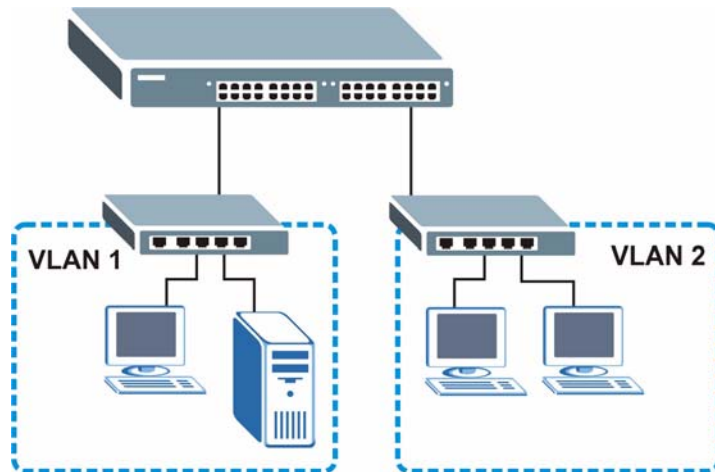
## 1.4.4 IEEE 802.1Q VLAN Application Examples

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, “VLAN,”](#) on page 84.

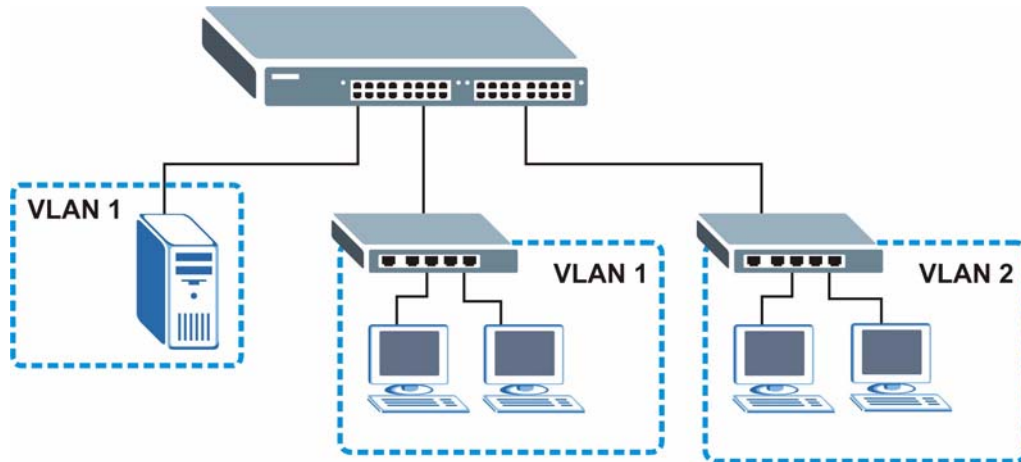
### 1.4.4.1 Tag-based VLAN Example

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

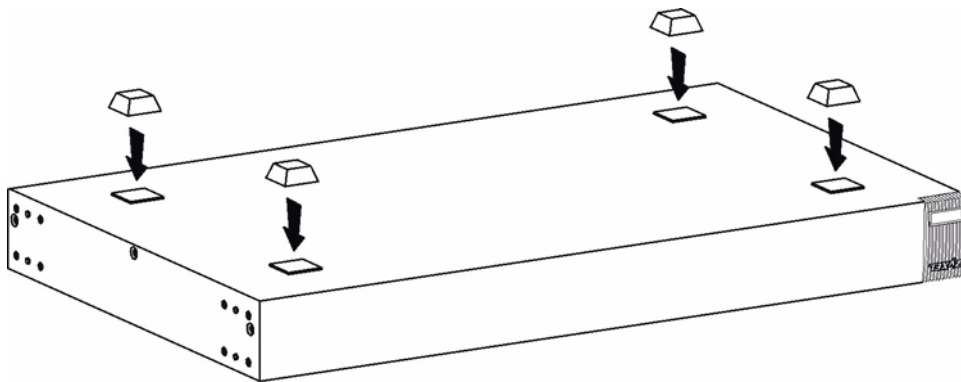
This chapter shows you how to install the hardware and make port connections.

**Note:** Example graphics are shown.

### 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.

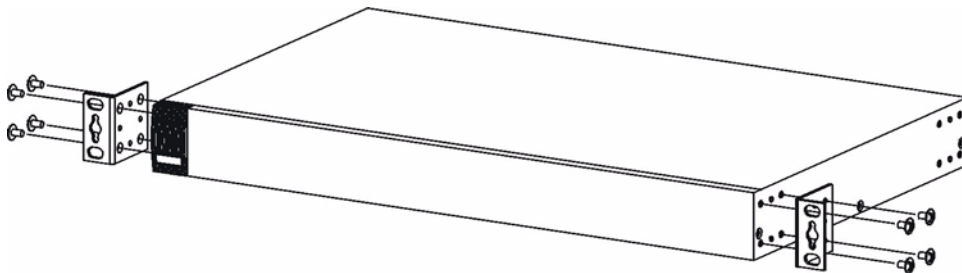
#### 2.2.1.1 Precautions

- 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.

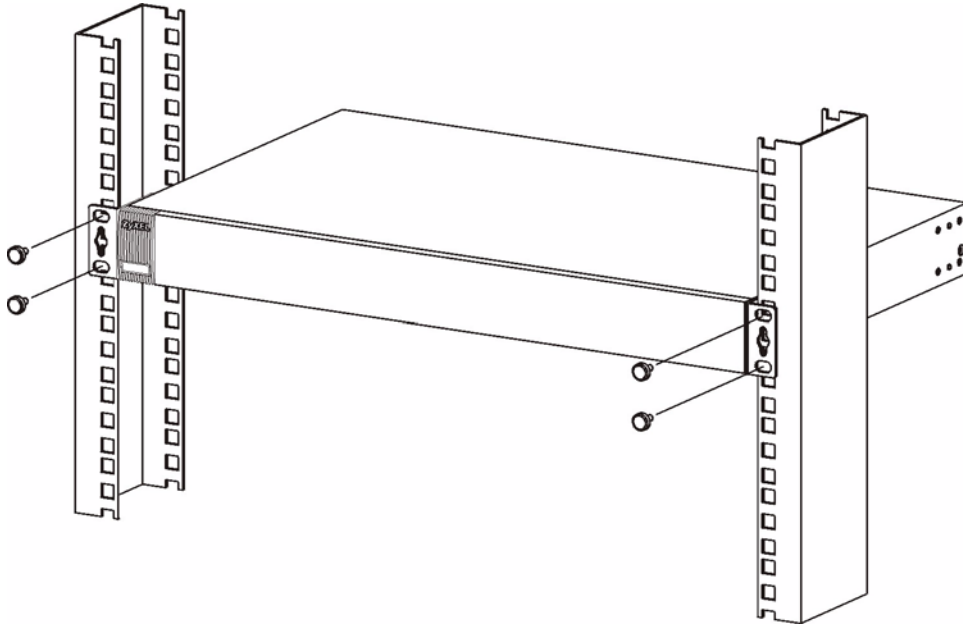
**Figure 7** Attaching the Mounting Brackets



- 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

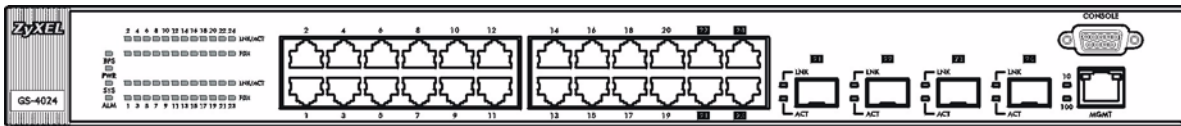
## Hardware Overview

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

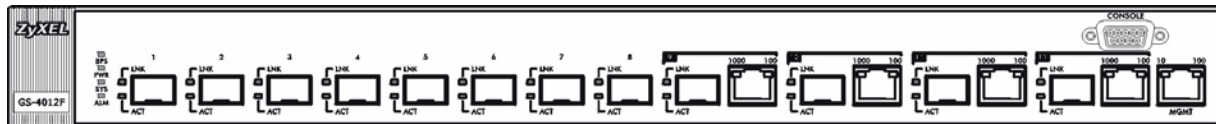
### 3.1 Front Panel Connection

The figure below shows the front panel of the switch.

**Figure 9** Front Panel: GS-4024



**Figure 10** Front Panel: GS-4012F



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

**Table 1** Front Panel

PORT	DESCRIPTION
100/1000 Mbps RJ-45 Gigabit Ethernet Ports	Connect these ports to a computer, a hub, an Ethernet switch or router.
Mini-GBIC slots	Use mini-GBIC transceivers in these slots for fiber-optical connections to backbone Ethernet switches (see <a href="#">Section 3.1.3 on page 45</a> for instructions).
Gigabit/mini-GBIC ports	Connect these Gigabit Ethernet ports to high-bandwidth backbone network Ethernet switches or use them to daisy-chain other switches. Alternatively, use mini-GBIC transceivers in these slots for fiber-optical connections to backbone Ethernet switches.
MGMT	Connect to a computer using an RJ-45 Ethernet cable for local configuration of the switch.
CONSOLE	Only connect this port if you want to configure the switch using the command line interface (CLI) via the console port.

### 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 Gigabit Ethernet Ports

The GS-4024 has 24 100/1000Mbps auto-negotiating, auto-crossover Gigabit Ethernet ports. In 10/100/1000 Mbps Gigabit Ethernet, the speed can be 100Mbps or 1000Mbps and the duplex mode can be half duplex (for 100 Mbps) or full duplex.

An auto-negotiating port can detect and adjust to the optimum Ethernet speed 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.

#### 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: on

### 3.1.3 SFP Slots

The GS-4012F comes with 12 SFP (Small Form-factor Pluggable) 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 transceiver MultiSource Agreement (MSA). See the SFF committee's INF-8074i specification Rev 1.0 for details.

The switch has four 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)

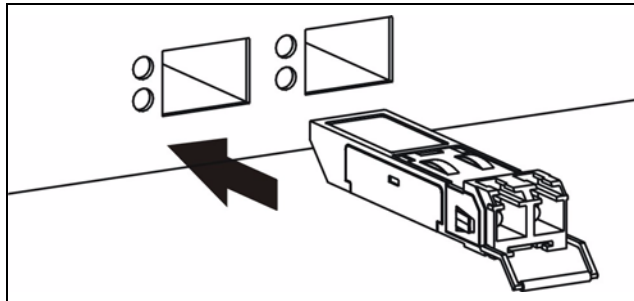
**Note:** To avoid possible eye injury, do NOT look into an operating fiber-optic module's connectors.

### 3.1.3.1 Transceiver Installation

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

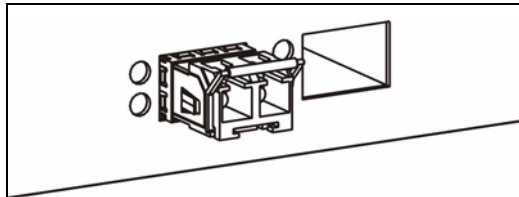
- 1 Insert the transceiver into the slot with the exposed section of PCB board facing down.

**Figure 11** 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 12** Installed Transceiver

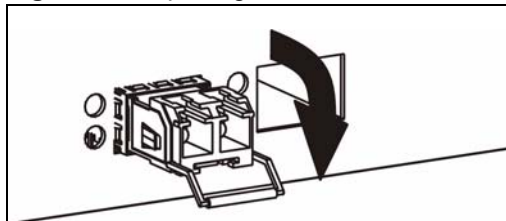


### 3.1.3.2 Transceiver Removal

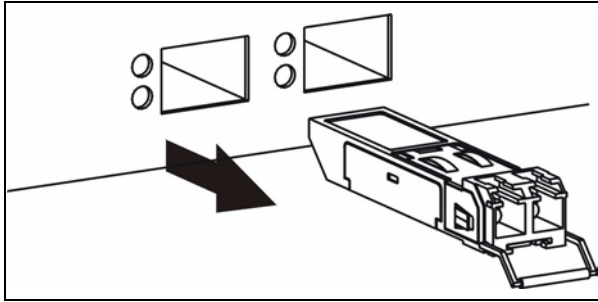
Use the following steps to remove a mini-GBIC transceiver (SFP module).

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

**Figure 13** Opening the Transceiver's Latch Example



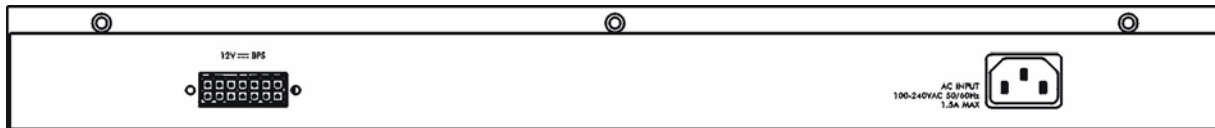
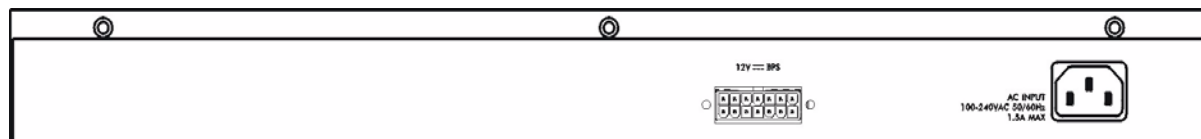
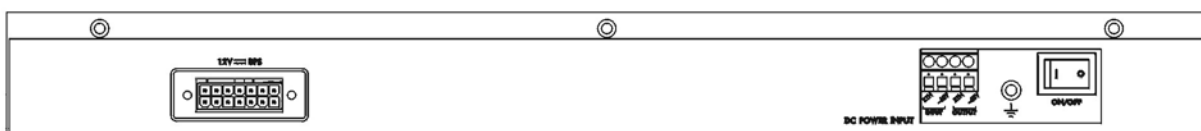
- 2 Pull the transceiver out of the slot.

**Figure 14** Transceiver Removal Example

## 3.2 Rear Panel

The following figure shows the rear panel of the switch. The rear panel contains the ventilation holes, a connector for external backup power supply (BPS), the power receptacle and the power switch (for DC model).

The following figure shows the rear panel of the switch. The rear panel contains a connector for backup power supply (BPS) and the power receptacle.

**Figure 15** Rear Panel: GS-4012F**Figure 16** Rear Panel: GS-4024**Figure 17** Rear Panel: GS-4012F (DC Model)

### 3.2.1 Power Connector

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

The GS-4012F DC unit requires DC power supply input of  $-48$  VDC or  $-60$  VDC, 1.2A Max. 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 a power outlet. Make sure that no objects obstruct the airflow of the fans.

### 3.2.2 External Backup Power Supply Connector

The backup power supply constantly monitors the status of the internal power supply. The backup power supply automatically provides power to the switch in the event of a power failure. Once the switch receives power from the backup power supply, it will not automatically switch back to using the internal power supply even when the power is resumed.

### 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
BPS	Green	Blinking	The system is receiving power from the backup power supply.
		On	The backup power supply is connected and active.
		Off	The backup power supply is not ready or not active.
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.
Gigabit Ethernet Ports			
1000	Green	Blinking	The port is sending/receiving data.
		On	The link to a 1000 Mbps Ethernet network is up. The link to a 10 Mbps Ethernet network is up when the <b>100</b> LED is on.
		Off	No Ethernet device is connected to this port or the port is transmitting at 100 Mbps.
100	Amber	Blinking	The port is sending/receiving data.
		On	The link to a 100 Mbps Ethernet network is up. The link to a 10 Mbps Ethernet network is up when the <b>1000</b> LED is on.
		Off	No Ethernet device is connected to this port or the port is transmitting at 1000 Mbps.
Mini-GBIC (SFP) 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 sending or receiving data.
		Off	The port is not sending or receiving data.



**Table 2** Front Panel LEDs (continued)

LED	COLOR	STATUS	DESCRIPTION
MGMT Port			
10	Green	On	The link to a 10 Mbps Ethernet network is up.
		Blinking	The port is receiving or transmitting data. at 10 Mbps.
		Off	The link to a 10 Mbps Ethernet network is up.
100	Amber	On	The link to a 100 Mbps Ethernet network is up.
		Blinking	The port is receiving or transmitting data. at 100 Mbps.
		Off	The link to a 100 Mbps Ethernet network is up.

# 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).

**Note:** Web configurator screens are similar for the switch models described in this guide. GS-4012F screens are shown.

### 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 18 Web Configurator: Login

Enter Network Password

Please type your user name and password.

Site: 192.168.1.1

Realm: GS-4012F at Thu Jan 1 02:12:58 1970

User Name:

Password:

Save this password in your password list

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 19 Web Configurator Home Screen (Status)

ZyXEL

STATUS Logout Help

MENU

- Basic Setting
- Advanced Application
- IP Application
- Management

Dimension GS-4012F

Status

System Up Time : 2:14:41

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	139	0	0	0.0	0.0	0:00:00
10	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
11	100MF Copper	FORWARDING	Disabled	350	408	0	0.0	0.0	2:14:30
12	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00

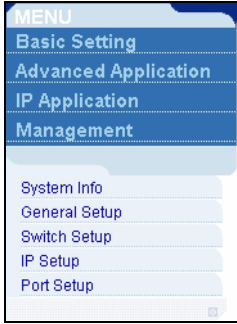

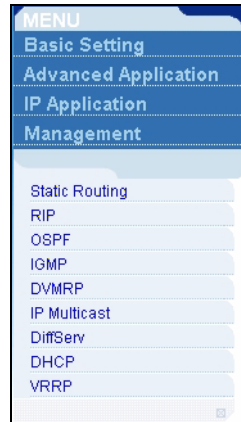

Poll Interval(s) 40 Set Interval Stop

Port ALL Clear Counter

© Copyright 1995-2005 by ZyXEL Communications Corp.

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	VLAN	Static Routing	Maintenance
General Setup	VLAN Status	RIP	Firmware Upgrade
Switch Setup	VLAN Port Setting	OSPF Status	Restore Configuration
IP Setup	Static VLAN	OSPF Configuration	Backup Configuration
Port Setup	Static MAC Forwarding	OSPF Interface	Load Factory Default
	Filtering	OSPF Virtual Link	Reboot System
	Spanning Tree Protocol	IGMP	Access Control
	Status	DVMRP	SNMP
	Spanning Tree	IP Multicast	Logins
	Protocol Configuration	DiffServ	Service Access Control
	Bandwidth Control	DSCP Setting	Remote Management
	Broadcast Storm Control	DHCP Server Status	Cluster Management Status
	Mirroring	DHCP Server	Cluster Management
	Link Aggregation	DHCP Relay	Configuration
	Link Aggregation	VRRP	MAC Table
	Protocol Status	Status	IP Table
	Link Aggregation	VRRP Configuration	ARP Table
	Port Authentication		Routing Table
	RADIUS		
	802.1x		
	Port Security		
	Classifier		
	Policy Rule		
	Queuing Method		
	VLAN Stacking		
	Multicast		
	IGMP Filtering Profile		
	MVR		
	Group Configuration		

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.

**Table 5** Navigation Panel Links (continued)

LINK	DESCRIPTION
IP Setup	This link takes you to a screen where you can configure the IP address, subnet mask (necessary for switch management) and DNS (domain name server) and set up to 64 IP routing domains.
Port Setup	This link takes you to screens where you can configure settings for individual switch ports.
Advanced Application	
VLAN	This link takes you to screens where you can configure port-based or 802.1Q VLAN (depending on what you configured in the Switch Setup menu).
Static MAC Forwarding	This link takes you to screens where you can configure static MAC addresses for a port. These static MAC addresses do not age out.
Filtering	This link takes you to a screen to set up filtering rules.
Spanning Tree Protocol	This link takes you to screens where you can configure the STP/RSTP to prevent network loops.
Bandwidth Control	This link takes you to screens where you can cap the maximum bandwidth allowed from specified source(s) to specified destination(s).
Broadcast Storm Control	This link takes you to a screen to set up broadcast filters.
Mirroring	This link takes you to screens where you can copy traffic from one port or ports to another port in order that you can examine the traffic from the first port without interference
Link Aggregation	This link takes you to a screen where you can logically 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 MAC address learning and set the maximum number of MAC addresses to learn on a port.
Classifier	This link takes you to a screen where you can configure the switch to group packets based on the specified criteria.
Policy Rule	This link takes you to a screen where you can configure the switch to perform special treatment on the grouped packets.
Queuing Method	This link takes you to a screen where you can configure queuing with associated queue weights for each port.
VLAN Stacking	This link takes you to a screen where you can configure VLAN stacking.
Multicast	This link takes you to a screen where you can configure various multicast features and create multicast VLANs.
IP Application	
Static Route	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.
RIP	This link takes you to a screen where you can configure the RIP (Routing Information Protocol) direction and versions.
OSPF	This link takes you to screens where you can view the OSPF status and configure OSPF settings.
IGMP	This link takes you to a screen where you can configure the IGMP settings.

**Table 5** Navigation Panel Links (continued)

LINK	DESCRIPTION
DVMRP	This link takes you to a screen where you can configure the DVMRP (Distance Vector Multicast Routing Protocol) settings.
IP Multicast	This link takes you to a screen where you can configure the switch to remove VLAN tags from IP multicast packets on an out-going port.
DiffServ	This link takes you to screens where you can enable DiffServ, configure marking rules and set DSCP-to-IEEE802.1p mappings.
DHCP	This link takes you to a screen where you can configure the DHCP settings.
VRRP	This link takes you to screens where you can configure redundant virtual router for your network.
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.
IP Table	This link takes you to a screen where you can view the IP 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.
Routing Table	This link takes you to a screen where you can view the routing 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 20** Change Administrator Login Password

The screenshot shows a web interface for configuring logins. At the top, there are tabs for 'Logins' 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 a table titled 'Edit Logins' with four columns: 'Login', 'User Name', 'Password', and 'Retype to confirm'. The table has four rows, numbered 1 to 4. At the bottom of the form are 'Apply' and 'Cancel' buttons.

Login	User Name	Password	Retype to confirm
1			
2			
3			
4			

## 4.4 Switch Lockout

**Note:** You cannot log into the switch using the same administrator account concurrently on different IP routing domains.

You could lock yourself (and all others) out from the switch by:

- 1 Deleting all IP routing domains.
- 2 Deleting all port-based VLANs with the CPU port as a member. The “CPU port” is the management port of the switch.
- 3 Filtering all traffic to the CPU port.
- 4 Disabling all ports.
- 5 Misconfiguring the text configuration file.
- 6 Forgetting the password and/or IP address.
- 7 Preventing all services from accessing the switch.
- 8 Changing a service port number but forgetting it.

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

## 4.5 Resetting the Switch

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



## 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 45](#) 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 21** Resetting the Switch: Via the Console Port

```
Bootbase Version: V1.0 | 11/26/2004 15:56:35
RAM:Size = 64 Mbytes
FLASH: Intel 32M
ZyNOS Version: V3.60(LL.0)b2 | 01/18/2005 00:39:28
Press any key to enter debug mode within 3 seconds.
.....
Enter Debug Mode
GS-4012F> atlc
Starting XMODEM upload (CRC mode)....
CCCCCCCCCCCCCCCC
Total 393216 bytes received.
Erasing..
.....
OK
GS-4012F> 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 for security reasons.

**Figure 22** 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 example network:

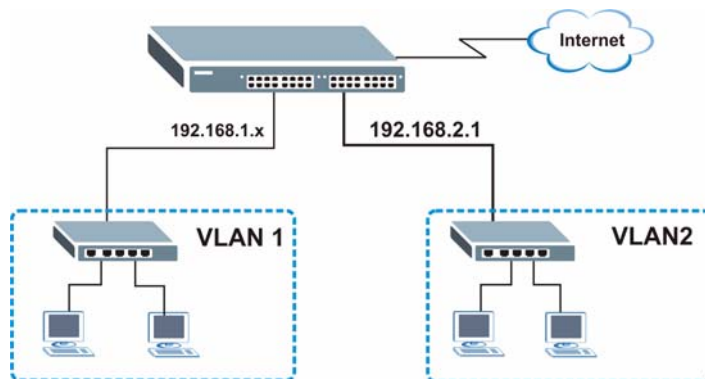
- Configure an IP interface
- Configure DHCP server settings
- Create a VLAN
- Set port VLAN ID
- Enable RIP

#### 5.1.1 Configuring an IP Interface

On a layer-3 switch, an IP interface (also known as an IP routing domain) is not bound to a physical port. The default IP address of the switch is 192.168.1.1 with a subnet mask of 255.255.255.0.

In the example network, since the **RD** network is already in the same IP interface as the switch, you don't need to create an IP interface for it. However, if you want to have the **Sales** network on a different routing domain, you need to create a new IP interface. This allows the switch to route traffic between the **RD** and **Sales** networks.

**Figure 23** Initial Setup Network Example: IP Interface



- 1 Connect your computer to the **MGMT** port that is used only for management. Make sure your computer is in the same subnet as the **MGMT** port.

- 2 Open your web browser and enter 192.168.0.1 (the default **MGMT** port IP address) in the address bar to access the web configurator. See [Section 4.2 on page 50](#) 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 **Sales** 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 IP interface to belong. This is the same as the VLAN ID you configure in the **Static VLAN** screen.
- 6 Click **Add**.

The screenshot shows the 'IP Setup' configuration page. It includes sections for 'Management IP Address' and 'IP Interface'. The 'IP Interface' section is circled in black, showing fields for IP Address (192.168.2.1), IP Subnet Mask (255.255.255.0), and VID (2). Below the form is a table with one entry and 'Add', 'Delete', and 'Cancel' buttons.

Index	IP Address	IP Subnet Mask	VID	Delete
1	192.168.1.12	255.255.255.0	1	<input type="checkbox"/>

## 5.1.2 Configuring DHCP Server Settings

You can set the switch to assign network information (such as the IP address, DNS server, etc.) to DHCP clients on the network.

For the example network, configure two DHCP client pools on the switch for the DHCP clients in the **RD** and **Sales** networks.

- 1 In the web configurator, click **IP Application** and **DHCP** in the navigation panel and click the **Server** link.
- 2 In the **DHCP Server** screen, specify the ID of the VLAN to which the DHCP clients belong, the starting IP address pool, subnet mask, default gateway address and the DNS server address(es).
- 3 Click **Add** to save the settings.

The screenshot shows the 'DHCP Server' configuration page. It includes fields for VID (2), Client IP Pool Starting Address (192.168.2.100), Size of Client IP Pool (100), IP Subnet Mask (255.255.255.0), Default Gateway (192.168.2.1), Primary DNS Server (192.168.2.120), and Secondary DNS Server (0.0.0.0). Below the form is a table with one entry and 'Add', 'Delete', and 'Cancel' buttons.

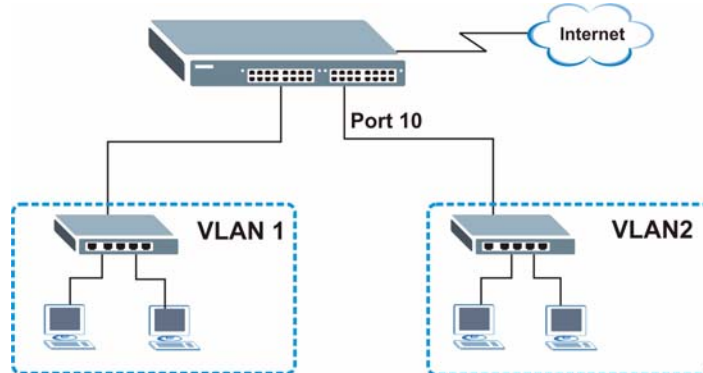
VID	Type	DHCP Status	Delete
1	Server	192.168.1.100/100	<input type="checkbox"/>

### 5.1.3 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 24** Initial Setup Network Example: VLAN



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

**VLAN Status**
[VLAN Port Setting](#)
[Static VLAN](#)

The Number Of VLAN = 1

Index	VID	Port Number						Elapsed Time	Status
		2	4	6	8	10	12		
1	1	1	3	5	7	9	11	2:54:57	Static
		U	U	U	U	U	U		

Poll Interval(s)  Set Interval Stop

Change Pages: Previous Page Next Page

- 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 **Sales** 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.

- Since the **Sales** network is connected to port 10 on the switch, select **Fixed** to configure port 10 to be a permanent member of the VLAN only.
- 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.
- Click **Add** to save the settings.

Port	Control	Tagging
1	Normal	Tx Tagging
2	Normal	Tx Tagging
3	Normal	Tx Tagging
4	Normal	Tx Tagging
5	Normal	Tx Tagging
6	Normal	Tx Tagging
7	Normal	Tx Tagging
8	Normal	Tx Tagging
9	Normal	Tx Tagging
10	Normal	Tx Tagging
11	Normal	Tx Tagging
12	Normal	Tx Tagging

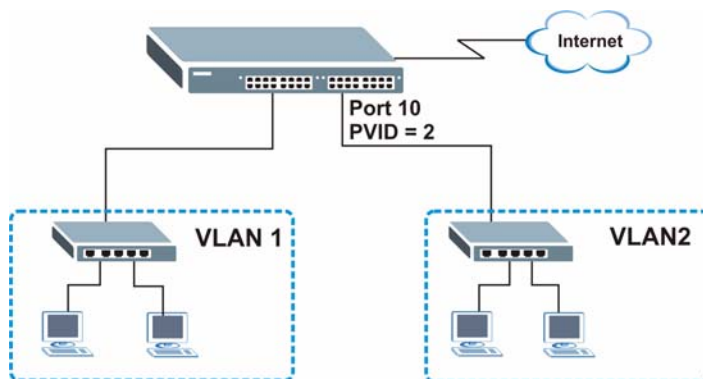
VID	Active	Name	Delete
1	Yes	1	<input type="checkbox"/>

### 5.1.4 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 25** 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"/>

### 5.1.5 Enabling RIP

To exchange routing information with other routing devices across different routing domains, enable RIP (Routing Information Protocol) in the **RIP** screen.

- 1 Click **IP Application** and **RIP** in the navigation panel.
- 2 Select **Both** in the **Direction** field to set the switch to broadcast and receive routing information.
- 3 In the **Version** field, select **RIP-1** for the RIP packet format that is universally supported.
- 4 Click **Apply** to save the settings.

Index	Network	Direction	Version
1	172.23.19.95/24	Both	RIP-1
2	192.168.1.1/24	Both	RIP-1





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

### 6.2 Port Status Summary

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

**Figure 26** Status

The screenshot shows the 'Status' screen with a title bar and a table of port statistics. Below the table are control buttons for polling interval 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	Down	STOP	Disabled	139	0	0	0.0	0.0	0:00:00
10	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
11	100M/F Copper	FORWARDING	Disabled	444	496	0	0.0	0.0	2:17:50
12	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00

System Up Time : 2:18:01

Poll Interval(s)

Port

The following table describes the labels in this screen.

**Table 6** Status

<b>LABEL</b>	<b>DESCRIPTION</b>
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 <b>Port Details</b> screen (refer to <a href="#">Figure 27 on page 68</a> ).
Link	This field displays the speed (either <b>10M</b> for 10Mbps, <b>100M</b> for 100Mbps or <b>1000M</b> for 1000Mbps) and the duplex ( <b>F</b> for full duplex or <b>H</b> for half duplex). It also shows the cable type ( <b>Copper</b> or <b>Fiber</b> ) for the Gigabit Ethernet/mini-GBIC ports.
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.
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 <b>Stop</b> to halt system statistic polling.
Clear Counter	Select a port from the Port drop-down list box and then click <b>Clear Counter</b> to erase the recorded statistical information for that port.

## 6.2.1 Port Details

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

Figure 27 Status: Port Details

Port Details		Status
Port Info	Port NO.	24
	Link	100M/F Copper
	Status	FORWARDING
	LACP	Disabled
	TxPkts	277
	RxPkts	220
	Errors	0
	Tx KBs/s	0.0
	Rx KBs/s	0.0
	Up Time	0:03:18
<b>TX Packet</b>	<b>TX Packets</b>	<b>277</b>
	Multicast	0
	Broadcast	1
	Pause	0
	Tagged	0
<b>RX Packet</b>	<b>RX Packets</b>	<b>220</b>
	Multicast	0
	Broadcast	3
	Pause	0
	Control	0
<b>TX Collision</b>	<b>Single</b>	<b>0</b>
	Multiple	0
	Excessive	0
	Late	0
<b>Error Packet</b>	<b>RX CRC</b>	<b>0</b>
	Length	0
	Runt	0
<b>Distribution</b>	<b>64</b>	<b>221</b>
	65 to 127	13
	128 to 255	5
	256 to 511	74
	512 to 1023	22
	1024 to 1518	162
	Giant	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	
Link	This field displays the speed (either <b>10M</b> for 10Mbps, <b>100M</b> for 100Mbps or <b>1000M</b> for 1000Mbps) and the duplex ( <b>F</b> for full duplex or <b>H</b> for half duplex). It also shows the cable type ( <b>Copper</b> or <b>Fiber</b> ).
Status	This field shows the training state of the ports. The states are <b>FORWARDING</b> (forwarding), which means the link is functioning normally or <b>STOP</b> (the port is stopped to break a loop or duplicate path).
LACP	This field shows if LACP is enabled on this port or not.
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.

**Table 7** Status: Port Details (continued)

<b>LABEL</b>	<b>DESCRIPTION</b>
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 Packet	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.
Tagged	This field shows the number of packets with VLAN tags transmitted.
Rx Packet The following fields display detailed information about packets received.	
RX Packet	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.
Tagged	This field shows the number of packets with VLAN tags received.
Control	This field shows the number of control packets received (including those with CRC error) but it does not include the 802.3x Pause packets.
TX Collision The following fields display information on collisions while transmitting.	
Single	This is a count of successfully transmitted packets for which transmission is inhibited by exactly one collision.
Multiple	This is a count of successfully transmitted packets for which transmission was inhibited by more than one collision.
Excessive	This is a count of packets 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 packets have already been transmitted.
Error Packet The following fields display detailed information about packets received that were in error.	
RX CRC	This field shows the number of packets received with CRC (Cyclic Redundant Check) error(s).
Length	This field shows the number of packets 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.
Distribution	
64	This field shows the number of packets (including bad packets) received that were 64 octets in length.
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.

**Table 7** Status: Port Details (continued)

LABEL	DESCRIPTION
256-511	This field shows the number of packets (including bad packets) received that were between 256 and 511 octets in length.
512-1023	This field shows the number of packets (including bad packets) received that were between 512 and 1023 octets in length.
1024-1518	This field shows the number of packets (including bad packets) received that were between 1024 and 1518 octets in length.
Giant	This field shows the number of packets dropped because they were bigger than the maximum frame size.
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 <b>Set Interval</b> .
Stop	Click <b>Stop</b> 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 in each routing domain, 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 28 System Info

**System Info**

System Name					
ZyNOS F/W Version	V3.60(TS.2) 09/26/2005				
Ethernet Address	00:13:49:1c:a2:9f				

**Hardware Monitor**

Temperature Unit:

Temperature(C)	Current	MAX	MIN	Threshold	Status
MAC	35.0	35.0	27.0	65.0	Normal
CPU	33.0	33.0	27.0	65.0	Normal
PHY	33.5	33.5	27.0	65.0	Normal

FAN Speed (RPM)	Current	MAX	MIN	Threshold	Status
FAN1	5670	5716	5536	2750	Normal
FAN2	5625	5625	5493	2750	Normal
FAN3	4815	4951	4750	2750	Normal

Voltage (V)	Current	MAX	MIN	Threshold	Status
2.5	2.592	2.592	2.592	+/- 8%	Normal
1.25	1.280	1.280	1.264	+/- 8%	Normal
3.3	3.376	3.376	3.376	+/- 8%	Normal
12	12.281	12.281	12.281	+/- 10%	Normal
5	5.053	5.053	5.053	+/- 7%	Normal
1.3	1.328	1.328	1.328	+/- 10%	Normal
1.25	1.264	1.280	1.264	+/- 8%	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	<b>MAC</b> , <b>CPU</b> and <b>PHY</b> refer to the location of the temperature sensors on the switch printed circuit board.
Current	This shows the current temperature in degrees centigrade 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 <b>Normal</b> for temperatures below the threshold and <b>Error</b> 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	<b>Normal</b> indicates that this fan is functioning above the minimum speed. <b>Error</b> 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 percentage tolerance of the voltage with which the switch still works.
Status	<b>Normal</b> indicates that the voltage is within an acceptable operating range at this point; otherwise <b>Error</b> 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 <b>Set Interval</b> .
Stop	Click <b>Stop</b> 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 29** General Setup

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 (up to 30 characters) of your switch.
Contact Person's Name	Enter the name (up to 30 characters) of the person in charge of this switch.
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 <b>Access Control Logins</b> 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 <b>Local Only</b> to have the switch just check the administrator accounts configured in the <b>Access Control Logins</b> screen.</p> <p>Select <b>Local then RADIUS</b> to have the switch check the administrator accounts configured in the <b>Access Control Logins</b> screen. If the user name is not found, the switch then checks the user database on the specified RADIUS server. You need to configure <b>Port Authentication Radius</b> first.</p> <p>Select <b>RADIUS Only</b> 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	Enter the time service protocol that a timeserver sends when you turn on the switch. 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. When you select the <b>Daytime (RFC 867)</b> 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. <b>Time (RFC-868)</b> format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. <b>NTP (RFC-1305)</b> is similar to Time (RFC-868). <b>None</b> is the default value. Enter the time manually. Each time you turn on the switch, the time and date will be reset to 2000-1-1 0:0.
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 <b>Current Time</b> field after you click <b>Apply</b> .
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 <b>Current Date</b> field after you click <b>Apply</b> .
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 <b>Apply</b> to save the settings.
Cancel	Click <b>Cancel</b> 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 84](#) for information on port-based and 802.1Q tagged VLANs.

## 7.5 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. The switch discards multicast traffic destined for multicast groups that it does not know. IGMP snooping generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through your switch.

## 7.6 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 30** Switch Setup

The screenshot shows the 'Switch Setup' configuration screen. At the top, there is a title bar with a 'Switch Setup' button. Below it, the 'VLAN Type' section has two radio buttons: '802.1Q' (selected) and 'Port Based'. The 'Bridge Control Protocol Transparency' section has a checkbox labeled 'Active' which is unchecked. The 'MAC Address Learning' section includes an 'Aging Time' field set to '300' with the unit 'seconds'. The 'GARP Timer' section includes three fields: 'Join Timer' set to '200' (milliseconds), 'Leave Timer' set to '600' (milliseconds), and 'Leave All Timer' set to '10000' (milliseconds). The 'Priority Queue Assignment' section lists levels from 'level7' to 'level0', each with a dropdown menu showing a value: level7 (7), level6 (6), level5 (5), level4 (4), level3 (3), level2 (1), level1 (0), and level0 (2). At the bottom of the screen are 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen

**Table 10** Switch Setup

LABEL	DESCRIPTION
VLAN Type	Choose <b>802.1Q</b> or <b>Port Based</b> . The <b>VLAN Setup</b> screen changes depending on whether you choose <b>802.1Q</b> VLAN type or <b>Port Based</b> VLAN type in this screen. See <a href="#">Chapter 8 on page 84</a> for more information.
Bridge Control Protocol Transparency	Select <b>Active</b> to allow the switch to handle bridging control protocols (STP for example). You also need to define how to treat a BPDU in the <b>Port Setup</b> screen.
MAC Address Learning	MAC address learning reduces outgoing traffic broadcasts. For MAC address learning to occur on a port, the port must be active.
Aging Time	Enter a time from 10 to 3000 seconds. This is how long all dynamically learned MAC addresses remain in the MAC address table before they age out (and must be relearned).
GARP Timer: Switches join VLANs by making a declaration. A declaration is made by issuing a <b>Join</b> message using GARP. Declarations are withdrawn by issuing a <b>Leave</b> message. A <b>Leave All</b> message terminates all registrations. GARP timers set declaration timeout values. See the chapter on VLAN setup for more background information.	
Join Timer	Join Timer sets the duration of the Join Period timer for GVRP in milliseconds. Each port has a <b>Join Period</b> timer. The allowed <b>Join Time</b> range is between 100 and 65535 milliseconds. See the chapter on VLAN setup for more background information.
Leave Timer	Leave Time sets the duration of the <b>Leave Period</b> timer for GVRP in milliseconds. Each port has a single <b>Leave Period</b> timer. Leave Time must be two times larger than <b>Join Timer</b> .
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 <b>Leave Timer</b> .
<p>Priority Queue Assignment</p> <p>IEEE 802.1p defines up to 8 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 eight 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.

**Table 10** Switch Setup (continued)

LABEL	DESCRIPTION
Level 0	Typically used for best-effort traffic.
Apply	Click <b>Apply</b> to save the settings.
Cancel	Click <b>Cancel</b> to reset the fields to your previous configuration.

## 7.7 IP Setup

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

### 7.7.1 IP Interfaces

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.

On the switch, as a layer-3 device, an IP address is not bound to any physical ports. Since each IP address on the switch must be in a separate subnet, the configured IP address is also known as IP interface (or routing domain). In addition, this allows routing between subnets based on the IP address without additional routers.

You can configure multiple routing domains on the same VLAN as long as the IP address ranges for the domains do not overlap. To change the IP address of the switch in a routing domain, simply add a new routing domain entry with a different IP address in the same subnet.

**Figure 31** IP Setup

**IP Setup**

Default Gateway: 0.0.0.0

Domain Name Server: 0.0.0.0

Default Management:  In-band  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

**IP Interface**

IP Address: 0.0.0.0

IP Subnet Mask: 0.0.0.0

VID:

Add Cancel

Index	IP Address	IP Subnet Mask	VID	Delete
1	192.168.1.12	255.255.255.0	1	<input type="checkbox"/>

Delete Cancel

The following table describes the labels in this screen.

**Table 11** IP Setup

LABEL	DESCRIPTION
Default Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.254.
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 ( <b>In-Band</b> or <b>Out-of-band</b> ) the switch is to send packets originating from itself (such as SNMP traps) or packets with unknown source. Select <b>Out-of-band</b> to have the switch send the packets to the management port labelled <b>MGMT</b> . This means that device(s) connected to the other port(s) do not receive these packets. Select <b>In-Band</b> to have the switch send the packets to all ports except the management port (labelled <b>MGMT</b> ) to which connected device(s) do not receive these packets.
<b>Management IP Address</b> Use these fields to set the settings for the out-of-band management port.	
IP Address	Enter the out-of-band management IP address of your switch in dotted decimal notation. For example, 192.168.0.1.
IP Subnet Mask	Enter the IP subnet mask of your switch in dotted decimal notation for example 255.255.255.0.



**Table 11** IP Setup (continued)

LABEL	DESCRIPTION
Default Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.0.254
Apply	Click <b>Apply</b> to save the settings.
Cancel	Click <b>Cancel</b> to reset the fields to your previous configuration.
IP Interface	
Use these fields to create or edit IP routing domains on the switch.	
IP Address	Enter the IP address of your switch in dotted decimal notation for example 192.168.1.1. This is the IP address of the switch in an IP routing domain.
IP Subnet Mask	Enter the IP subnet mask of an IP routing domain in dotted decimal notation. For example, 255.255.255.0.
VID	Enter the VLAN identification number to which an IP routing domain belongs.
Add	Click <b>Add</b> to save the new rule to the switch. It then displays in the summary table at the bottom of the screen.
Cancel	Click <b>Cancel</b> to reset the fields to your previous configuration.
Index	This field displays the index number of an entry.
IP Address	This field displays IP address of the switch in the IP domain.
Subnet Mask	This field displays the subnet mask of the switch in the IP domain.
VID	This field displays the VLAN identification number of the IP domain on the switch.
Delete	Click <b>Delete</b> to remove the selected entry from the summary table.  <b>Note:</b> Deleting all IP subnets locks you out from the switch.
Cancel	Click <b>Cancel</b> to clear the <b>Delete</b> check boxes.

## 7.8 Port Setup

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

Figure 32 Port Setup

Port	Active	Name	Type	Speed / Duplex	Flow Control	802.1p Priority	BPDU Control
1	<input checked="" type="checkbox"/>	port01	1000M	Auto	<input type="checkbox"/>	0	Peer
2	<input checked="" type="checkbox"/>	port02	1000M	Auto	<input type="checkbox"/>	0	Peer
3	<input checked="" type="checkbox"/>	port03	1000M	Auto	<input type="checkbox"/>	0	Peer
4	<input checked="" type="checkbox"/>	port04	1000M	Auto	<input type="checkbox"/>	0	Peer
5	<input checked="" type="checkbox"/>	port05	1000M	Auto	<input type="checkbox"/>	0	Peer
6	<input checked="" type="checkbox"/>	port06	1000M	Auto	<input type="checkbox"/>	0	Peer
7	<input checked="" type="checkbox"/>	port07	1000M	Auto	<input type="checkbox"/>	0	Peer
8	<input checked="" type="checkbox"/>	port08	1000M	Auto	<input type="checkbox"/>	0	Peer
9	<input checked="" type="checkbox"/>	port09	10/100/1000M	Auto	<input type="checkbox"/>	0	Peer
10	<input checked="" type="checkbox"/>	port10	10/100/1000M	Auto	<input type="checkbox"/>	0	Peer
11	<input checked="" type="checkbox"/>	port11	10/100/1000M	Auto	<input type="checkbox"/>	0	Peer
12	<input checked="" type="checkbox"/>	port12	10/100/1000M	Auto	<input type="checkbox"/>	0	Peer

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 (up to nine printable characters) that identifies this port.
Type	This field displays <b>10/100/1000M</b> for the Gigabit Ethernet/ mini-GBIC ports or <b>1000M</b> for the mini-GBIC ports.
Speed/Duplex	<p>Select the speed and the duplex mode of the connection on this port. Choices are <b>Auto</b>, <b>10M/Half Duplex</b>, <b>10M/Full Duplex</b>, <b>100M/Half Duplex</b>, <b>100M/Full Duplex</b> and <b>1000M/Full Duplex</b>.</p> <p>Selecting <b>Auto</b> (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. <b>Flow Control</b> 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 back pressure 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 <b>Flow Control</b> to enable it.</p>

**Table 12** Port Setup (continued)

LABEL	DESCRIPTION
802.1P Priority	This priority value is added to incoming frames without a (802.1p) priority queue tag. See <b>Priority Queue Assignment</b> in <a href="#">Table 10 on page 78</a> for more information.
BPDU Control	Configure the way to treat BPDUs received on this port. You must activate bridging control protocol transparency in the <b>Switch Setup</b> screen first. Select <b>Peer</b> to process any BPDU (Bridge Protocol Data Units) received on this port. Select <b>Tunnel</b> to forward BPDUs received on this port. Select <b>Discard</b> to drop any BPDU received on this port. Select <b>Network</b> to process a BPDU with no VLAN tag and forward a tagged BPDU.
Apply	Click <b>Apply</b> to save the settings.
Cancel	Click <b>Cancel</b> to reset the fields to your previous configuration.

# 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 VLANs

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 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

VLAN group ID (or VID) is a unique number that identifies a VLAN. A port VID (PVID) is the VID associated to a physical port. A PVID defines the VLAN group to which a port belongs.

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.

The egress (outgoing) port(s) of a frame is determined on the combination of the destination MAC address and the VID of the frame. For a unicast frame, the egress port (based on the destination MAC address) must be a member of the VID, also; otherwise, the frame is blocked. A broadcast frame (or a multicast frame for a multicast group that is known by the system) is duplicated only on ports that are members of the VID (except the ingress port itself), thus confining the broadcast to a specific domain.

Whether to tag an outgoing frame depends on the setting of the egress port on an individual VLAN and port basis (remember 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.

## 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.

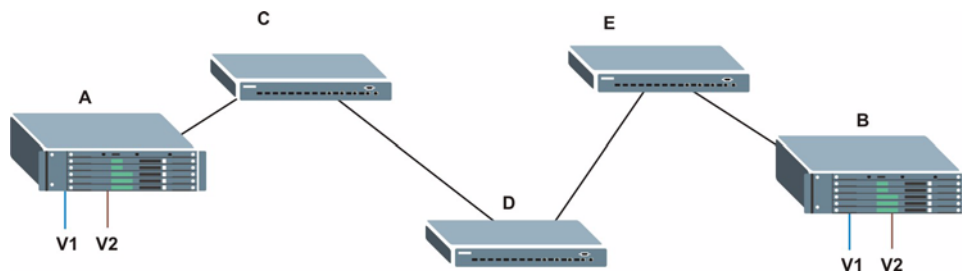
**Table 13** IEEE 802.1Q VLAN Terminology (continued)

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

## 8.3 Port VLAN Trunking

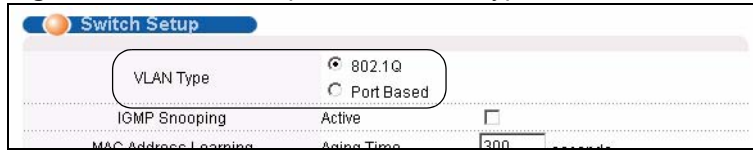
Enable **VLAN Trunking** on a port to allow frames belonging to unknown VLAN groups to pass through that port. This is useful if you want to set up VLAN groups on end devices without having to configure the same VLAN groups on intermediary devices.

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 33** Port VLAN Trunking

## 8.4 Select the VLAN Type

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

**Figure 34** 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 35** VLAN: VLAN Status

**VLAN Status** [VLAN Port Setting](#) [Static VLAN](#)

The Number Of VLAN = 1

Index	VID	Port Number						Elapsed Time	Status
		2	4	6	8	10	12		
1	1	U	U	U	U	U	U	2:54:57	Static
		U	U	U	U	U	U		

Poll Interval(s)

Change Pages

The following table describes the labels in this screen.

**Table 14** VLAN: VLAN Status

<b>LABEL</b>	<b>DESCRIPTION</b>
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 <b>VLAN Setup</b> screen.
Port Number	This column displays the ports that are participating in a VLAN. A tagged port is marked as <b>T</b> , an untagged port is marked as <b>U</b> 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 <b>Set Interval</b> .
Stop	Click <b>Stop</b> to halt polling statistics.
Change Pages	Click <b>Previous Page</b> or <b>Next Page</b> 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 36** VLAN: Static VLAN

The screenshot shows the 'Static VLAN' configuration page. At the top, there is a title bar with 'Static VLAN' and 'VLAN Status'. Below the title bar, there is an 'ACTIVE' checkbox. Underneath, there are two input fields: 'Name' and 'VLAN Group ID'. The main part of the page is a table with three columns: 'Port', 'Control', and 'Tagging'. The 'Control' column has three radio button options: 'Normal', 'Fixed', and 'Forbidden'. The 'Tagging' column has a checkbox for 'Tx Tagging'. Below the table, there are three buttons: 'Add', 'Cancel', and 'Clear'. At the bottom of the page, there is a summary table with four columns: 'VID', 'Active', 'Name', and 'Delete'. The 'VID' column has the value '1', 'Active' is 'Yes', 'Name' is '1', and 'Delete' is a checkbox. Below the summary table, there are two buttons: 'Delete' and 'Cancel'.

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 (up to 12 printable ASCII characters) for the VLAN group for identification purposes.
VLAN Group ID	Enter the VLAN ID for this VLAN group; the valid range is between 1 and 4094.
Port	The port number identifies the port you are configuring.
Control	Select <b>Normal</b> for the port to dynamically join this VLAN group using GVRP. This is the default selection. Select <b>Fixed</b> for the port to be a permanent member of this VLAN group. Select <b>Forbidden</b> if you want to prohibit the port from joining this VLAN group.
Tagging	Select <b>TX Tagging</b> if you want the port to tag all outgoing frames (that were previously untagged) transmitted with this VLAN Group ID.
Add	Click <b>Add</b> to add the settings as a new entry in the summary table below.
Cancel	Click <b>Cancel</b> to reset the fields.
Clear	Click <b>Clear</b> 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 ( <b>Yes</b> ) or disabled ( <b>No</b> ).
Name	This field displays the descriptive name for this VLAN group.

**Table 15** VLAN: Static VLAN (continued)

LABEL	DESCRIPTION
Delete	Click <b>Delete</b> to remove the selected entry from the summary table.
Cancel	Click <b>Cancel</b> to clear the <b>Delete</b> 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 37** 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"/>

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 Isolation	<b>Port Isolation</b> allows each port to communicate only with the CPU management port but not 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.
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.

**Table 16** VLAN: VLAN Port Setting (continued)

LABEL	DESCRIPTION
PVID	Specify the VLAN group ID (or VID) that will be added to untagged packets on the port. For example, if port 10's PVID is 2, then all untagged traffic on port 10 will belong to (and be sent to) VLAN 2. Enter a number between 1 and 4094 as the port VLAN ID.
GVRP	Select this check box to allow GVRP on this port.
Acceptable Frame Type	Specify the type of frames allowed on a port. Choices are <b>All</b> and <b>Tag Only</b> . Select <b>All</b> from the drop-down list box to accept all untagged or tagged frames on this port. This is the default setting. Select <b>Tag Only</b> to accept only tagged frames on this port. All untagged frames will be dropped.
VLAN Trunking	Enable <b>VLAN Trunking</b> 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 <b>Apply</b> to save the changes
Cancel	Click <b>Cancel</b> to start configuring the screen again.

## 8.6 Port-based VLANs

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

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

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

**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 and then click **VLAN** from the navigation panel to display the next screen.

**Figure 38** Port Based VLAN Setup (All Connected)

Setting Wizard: All connected [Apply]

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

[Apply] [Cancel]

**Figure 39** Port Based VLAN Setup (Port Isolation)

Setting Wizard: Port isolation [Apply]

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

[Apply] [Cancel]

The following table describes the labels in this screen.

]

**Table 17** Port Based VLAN Setup

LABEL	DESCRIPTION
Setting Wizard	<p>Choose <b>All connected</b> or <b>Port isolation</b>.</p> <p><b>All connected</b> 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><b>Port isolation</b> 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 <b>Apply</b> (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 <b>Apply</b> 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). <b>CPU</b> 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>
Outgoing	<p>These are the egress ports; an egress port is an outgoing port, that is, a port through which a data packet leaves. If you wish to allow two subscriber ports to talk to each other, you must define the egress port for both ports. <b>CPU</b> 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>
Apply	Click <b>Apply</b> to save the changes.
Cancel	Click <b>Cancel</b> to start configuring the screen again.

# CHAPTER 9

## Static MAC Forward Setup

Use these screens to configure static MAC address forwarding.

### 9.1 Overview

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

Static MAC address forwarding together with port security allow only computers in the MAC address table on a port to access the switch. See [Chapter 17 on page 120](#) 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. Scroll down to the bottom of the screen to view the summary table for the settings.

**Figure 40** Static MAC Forwarding

Index	Active	Name	MAC Address	Port	Delete
1	No	Example	00:b2:a0:9c:f0:3c / 2	1	<input type="checkbox"/>

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 (up to 32 printable ASCII characters) for identification purposes for this rule.
MAC Address	Enter the MAC address in valid MAC address format, that is, six hexadecimal character pairs.  <b>Note:</b> 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 <b>Add</b> to insert a new rule.
Cancel	Click <b>Cancel</b> to reset the fields.
Clear	Click <b>Clear</b> to begin configuring this screen afresh.
Index	Click an index number to modify the settings.
Active	This field displays whether this static MAC address forwarding rule is active ( <b>Yes</b> ) or not ( <b>No</b> ). You may temporarily deactivate a rule without deleting it.
Name	This field displays the descriptive name for this 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.
Delete	Click <b>Delete</b> to remove the selected entry from the summary table.
Cancel	Click <b>Cancel</b> to clear the <b>Delete</b> check boxes.

# CHAPTER 10

## Filtering

This chapter discusses static MAC address filtering.

### 10.1 Overview

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

### 10.2 Configure a Filtering Rule

Click **Advanced Application, Filtering** in the navigation panel to display the screen as shown next. Scroll down to the bottom of the screen to view the summary table for the settings.

**Figure 41** Filtering

The following table describes the related labels in this screen.

**Table 19** Filtering

LABEL	DESCRIPTION
Active	Make sure to select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by deselecting this check box.
Name	Type a descriptive name (up to 32 printable ASCII characters) for this rule. This is for identification purpose only.



**Table 19** Filtering (continued)

LABEL	DESCRIPTION
Action	<p>Select <b>Discard source</b> to drop frame from the source MAC address (specified in the <b>MAC</b> field). The switch can still send frames to the MAC address.</p> <p>Select <b>Discard destination</b> to drop frames to the destination MAC address (specified in the <b>MAC</b> field). The switch can still receive frames originating from the MAC address.</p> <p>Select <b>Discard source</b> and <b>Discard destination</b> to block traffic to/from the MAC address specified in the <b>MAC</b> field.</p>
MAC	Type a MAC address in valid MAC address format, that is, six hexadecimal character pairs.
VID	Type the VLAN group identification number.
Add	Click <b>Add</b> to save the new rule to the switch. It then displays in the summary table at the bottom of the screen.
Cancel	Click <b>Cancel</b> to reset the fields to your previous configuration.
Clear	Click <b>Clear</b> to clear the fields to the factory defaults.
Index	This field displays the index number of the rule. Click an index number to change the settings.
Active	This field displays <b>Yes</b> when the rule is activated and <b>No</b> when is it deactivated.
Name	This field displays the descriptive name for this rule. This is for identification purpose only.
MAC Address	This field displays the source/destination MAC address with the VLAN identification number to which the MAC address belongs.
Action	This field displays the filter action.
Delete	Check the rule(s) that you want to remove in the <b>Delete</b> column and then click the <b>Delete</b> button.
Cancel	Click <b>Cancel</b> to clear the selected checkbox(es) in the <b>Delete</b> column.

# CHAPTER 11

## Spanning Tree Protocol

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

### 11.1 STP/RSTP Overview

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

The switch uses IEEE 802.1w RSTP (Rapid Spanning Tree Protocol) that 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.

#### 11.1.1 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 20** STP Path Costs

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

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

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

## 11.1.2 How STP Works

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

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

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

## 11.1.3 STP Port States

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

**Table 21** STP Port States

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

## 11.2 STP Status

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

**Figure 42** Spanning Tree Protocol: Status

Bridge	Root	Our Bridge
Bridge ID	8000-00a0c5feea71	8000-00a0c5feea71
Hello Time (second)	2	2
Max Age (second)	20	20
Forwarding Delay (second)	15	15
Cost to Bridge	0	
Port ID	0x0000	
Topology Changed Times		0
Time Since Last Change		0:00:12

Polling Interval:

The following table describes the labels in this screen.

**Table 22** Spanning Tree Protocol: Status

LABEL	DESCRIPTION
Spanning Tree Protocol	This field displays <b>Running</b> if STP is activated. Otherwise, it displays <b>Down</b> .
Configuration	Click <b>Configuration</b> to configure STP settings. Refer to <a href="#">Section 11.2.1 on page 101</a> .
Bridge	<b>Root</b> refers to the base of the spanning tree (the root bridge). <b>Our Bridge</b> 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 <b>Root</b> and <b>Our Bridge</b> 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 <b>Hello Time</b> , <b>Max Age</b> and <b>Forwarding Delay</b>
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 22** Spanning Tree Protocol: Status (continued)

LABEL	DESCRIPTION
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 <b>Set Interval</b> .
Stop	Click <b>Stop</b> to halt STP statistic polling.

## 11.2.1 Configure STP

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

**Figure 43** Spanning Tree Protocol: Configuration

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

The following table describes the labels in this screen.

**Table 23** Spanning Tree Protocol: Configuration

LABEL	DESCRIPTION
Status	Click <b>Status</b> to display the <b>Spanning Tree Protocol Status</b> screen (see <a href="#">Figure 42 on page 100</a> ).
Active	Select this check box to activate STP. Clear this checkbox to disable STP.

**Table 23** Spanning Tree Protocol: Configuration (continued)

LABEL	DESCRIPTION
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. Bridge Priority determines the root bridge, which in turn determines Hello Time, Max Age and Forwarding Delay.</p>
Hello Time	<p>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.</p>
Max Age	<p>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.</p>
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	<p>This field displays the port number.</p>
Active	<p>Select this check box to activate STP on this port.</p>
Priority	<p>Configure the priority for each port here.</p> <p>Priority decides which port should be disabled when more than one port forms a loop in a switch. Ports with a higher priority numeric value are disabled first. The allowed range is between 0 and 255 and the default value is 128.</p>
Path Cost	<p>Path cost is the cost of transmitting a frame on to a LAN through that port. It is assigned according to the speed of the bridge. The slower the media, the higher the cost - see <a href="#">Table 20 on page 98</a> for more information.</p>
Apply	<p>Click <b>Apply</b> to save your changes back to the switch.</p>
Cancel	<p>Click <b>Cancel</b> to begin configuring this screen afresh.</p>



# CHAPTER 12

## Bandwidth Control

This chapter shows you how you can cap the maximum bandwidth allowed from specific source(s) to specified destination(s) using the **Bandwidth Control** screen.

### 12.1 Introduction to Bandwidth Control

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

#### 12.1.1 CIR and PIR

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

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

**Note:** The CIR should be less than the PIR.

The sum of CIRs cannot be greater than or equal to the uplink bandwidth.

### 12.2 Bandwidth Control Setup

Click **Advanced Application** and then **Bandwidth Control** in the navigation panel to display the configuration screen.



**Figure 44** Bandwidth Control

Port	Active	Ingress Rate		Egress Rate
		Commit Rate	Peak Rate	
1	<input type="checkbox"/>	1 Kbps	1000 Kbps	1000 Kbps
2	<input type="checkbox"/>	1 Kbps	1000 Kbps	1000 Kbps
3	<input type="checkbox"/>	1 Kbps	1000 Kbps	1000 Kbps
4	<input type="checkbox"/>	1 Kbps	1000 Kbps	1000 Kbps
5	<input type="checkbox"/>	1 Kbps	1000 Kbps	1000 Kbps
6	<input type="checkbox"/>	1 Kbps	1000 Kbps	1000 Kbps
7	<input type="checkbox"/>	1 Kbps	1000 Kbps	1000 Kbps
8	<input type="checkbox"/>	1 Kbps	1000 Kbps	1000 Kbps
9	<input type="checkbox"/>	1 Kbps	1000 Kbps	1000 Kbps
10	<input type="checkbox"/>	1 Kbps	1000 Kbps	1000 Kbps
11	<input type="checkbox"/>	1 Kbps	1000 Kbps	1000 Kbps
12	<input type="checkbox"/>	1 Kbps	1000 Kbps	1000 Kbps

The following table describes the related labels in this screen.

**Table 24** 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.
Committed Rate	Specify the guaranteed bandwidth allowed in kilobits per second (Kbps) for the incoming traffic flow on a port. The commit rate should be less than the peak rate. The sum of commit rates cannot be greater than or equal to the uplink bandwidth.
Peak Rate	Specify the maximum bandwidth allowed in kilobits per second (Kbps) for the incoming traffic flow on a port.
Egress Rate	Specify the maximum bandwidth allowed in megabits per second (Mbps) for the outgoing traffic flow on a port. Enter a number between 1 and 1000.
Apply	Click <b>Apply</b> to save the settings.
Cancel	Click <b>Cancel</b> to reset the fields to your previous configuration.

# CHAPTER 13

## Broadcast Storm Control

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

### 13.1 Overview

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

### 13.2 Broadcast Storm Control Setup

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

**Figure 45** Broadcast Storm Control

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

The following table describes the labels in this screen.

**Table 25** Broadcast Storm Control

<b>LABEL</b>	<b>DESCRIPTION</b>
Active	Select this check box to enable broadcast storm control on the switch.
Port	This field displays a port number.
Broadcast (pkt/s)	Select this option and specify how many broadcast packets the port receives per second.
Multicast (pkt/s)	Select this option and specify how many multicast packets the port receives per second.
DLF (pkt/s)	Select this option and specify how many destination lookup failure (DLF) packets the port receives per second.
Apply	Click <b>Apply</b> to save your changes back to the switch.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

# CHAPTER 14

## Mirroring

This chapter shows you how to configure mirroring on the switch.

### 14.1 Overview

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.

### 14.2 Port Mirroring Configuration

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

You must first select a monitor port. A monitor port is a port that copies the traffic of another port. After you select a monitor port, configure a mirroring rule in the related fields

**Figure 46** Mirroring

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

The following table describes the related labels in this screen.

**Table 26** Mirroring

LABEL	DESCRIPTION
Active	Clear this check box to deactivate port mirroring on the switch.
Monitor Port	The monitor port is the port you copy the traffic to in order to examine it in more detail without interfering with the traffic flow on the original port(s). Select this port from this drop-down list box.
Port	This field displays the port number.
Mirrored	Select this option to mirror the traffic on a port.
Direction	Specify the direction of the traffic to mirror. Choices are <b>Egress</b> (outgoing), <b>Ingress</b> (incoming) and <b>Both</b> .
Apply	Click <b>Apply</b> to save the changes.
Cancel	Click <b>Cancel</b> to start configuring the screen again.

# CHAPTER 15

## Link Aggregation

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

### 15.1 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.

#### 15.1.1 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.

## 15.1.2 Link Aggregation ID

LACP aggregation ID consists of the following information<sup>1</sup>:

**Table 27** Link Aggregation ID: Local Switch

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

**Table 28** Link Aggregation ID: Peer Switch

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

## 15.2 Link Aggregation Status

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

**Figure 47** 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)]	-	-
5	[(0000,00-00-00-00-00-00,0000,00,0000)] [(0000,00-00-00-00-00-00,0000,00,0000)]	-	-
6	[(0000,00-00-00-00-00-00,0000,00,0000)] [(0000,00-00-00-00-00-00,0000,00,0000)]	-	-

Polling Interval(s)

The following table describes the labels in this screen.

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

**Table 29** 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 <a href="#">Section 15.1.2 on page 111</a> for more information on this field.
Enabled Port	These are the ports you have configured in the <b>Link Aggregation</b> 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.
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 <b>Set Interval</b> .
Stop	Click <b>Stop</b> to halt statistic polling.

## 15.3 Link Aggregation Setup

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



**Figure 48** Link Aggregation Control Protocol: Configuration

The following table describes the labels in this screen.

**Table 30** 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.

**Table 30** Link Aggregation Control Protocol: Configuration (continued)

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



# CHAPTER 16

## Port Authentication

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

### 16.1 Overview

IEEE 802.1x is an extended authentication protocol<sup>2</sup> 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.

#### 16.1.1 RADIUS

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

Figure 49 RADIUS Server



### 16.2 Configuring Port Authentication

For network security, enable port authentication to check the identity of the user before access to the network is allowed. The switch authenticates users against the remote RADIUS server you specify.

To enable port authentication:

- activate IEEE802.1x security (both on the switch and the port(s))
  - configure the RADIUS server settings.
- 
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.

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

**Figure 50** Port Authentication



## 16.2.1 Activating IEEE 802.1x Security

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

**Figure 51** Port Authentication: 802.1x

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

The following table describes the labels in this screen.

**Table 31** Port Authentication: 802.1x

LABEL	DESCRIPTION
Active	Select this check box to permit 802.1x authentication on the switch.  <b>Note:</b> 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.

**Table 31** Port Authentication: 802.1x (continued)

LABEL	DESCRIPTION
Reauthentication Timer	Specify how often a client has to re-enter his or her username and password to stay connected to the port.
Apply	Click <b>Apply</b> to save your changes back to the switch.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 16.2.2 Configuring RADIUS Server Settings

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

**Figure 52** Port Authentication: RADIUS

The following table describes the labels in this screen.

**Table 32** 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 <b>1812</b> . You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external RADIUS server and the switch. This key is not sent over the network. This key must be the same on the external RADIUS server and the switch.
Apply	Click <b>Apply</b> to save your changes back to the switch.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.



# CHAPTER 17

## Port Security

This chapter shows you how to set up port security.

### 17.1 Overview

Port security allows only packets with dynamically learned MAC addresses and/or configured static MAC addresses to pass through a port on the switch.

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

### 17.2 Port Security Setup

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

**Figure 53** Port Security

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

The following table describes the labels in this screen.



**Table 33** Port Security

LABEL	DESCRIPTION
Active	Select this check box 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.
Address Learning	MAC address learning reduces outgoing broadcast traffic. For MAC address learning to occur on a port, the port itself must be active with address learning enabled.
Limited Number of Learned MAC Address	Use this field to limit the number of (dynamic) MAC addresses that may be learned on a port. For example, if you set this field to "5" on port 2, then only the devices with these five learned MAC addresses may access port 2 at any one time. A sixth device would have to wait until one of the five learned MAC addresses aged out. MAC address aging out time can be set in the <b>Switch Setup</b> screen. The valid range is from 0 to 16K. "0" means this feature is disabled, so the switch will learn MAC addresses up to the global limit of 16K.
Apply	Click <b>Apply</b> to save your changes back to the switch.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

# CHAPTER 18

## Classifier

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

### 18.1 Overview

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

A layer-2 classifier groups traffic according to the Ethernet type, VLAN group, MAC address and/or port number. A layer-3 classifier groups traffic according to the IP address and/or TCP/UDP protocol number.

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

- 1 Configure classifiers to sort traffic into different flows.
- 2 Configure policy rules to define actions to be performed for a classified traffic flow (refer to [Chapter 19 on page 128](#) to configure policy rules).

### 18.2 Configuring the Classifier

Use the **Classifier** screen to define the classifiers. After you define the classifier, you can specify actions (or policy) to act upon the traffic that match the rules. To configure policy rules, refer to [Chapter 19 on page 128](#).

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

**Figure 54** Classifier

**Classifier**

Active

Name

Packet Format

**Layer 2**

VLAN  Any

Priority  Any

Ethernet Type  All  
 Others  (Hex)

Source MAC Address  Any  
 MAC

Port

Destination MAC Address  Any  
 MAC

**Layer 3**

DSCP  Any

IP Protocol  All  Establish Only  
 Others  (Dec)

Source IP Address / Address Prefix  /

Socket Number  Any

Destination IP Address / Address Prefix  /

Socket Number  Any

Add Cancel Clear

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

Delete Cancel

The following table describes the related labels in this screen.

**Table 34** Classifier

LABEL	DESCRIPTION
Active	Select this option to enable this rule.
Name	Type a descriptive name (up to 32 printable ASCII characters) for this rule. This is for identification purpose only.
Packet Format	Specify the format of the packet. Choices are <b>All</b> , <b>802.3 tagged</b> , <b>802.3 untagged</b> , <b>Ethernet II tagged</b> and <b>Ethernet II untagged</b> . A value of <b>802.3</b> indicates that the packets are formatted according to the IEEE 802.3 standards. A value of <b>Ethernet II</b> indicates that the packets are formatted according to RFC 894, Ethernet II encapsulation.

**Table 34** Classifier (continued)

LABEL	DESCRIPTION
Layer 2 Specify the fields below to configure a layer-2 classifier.	
VLAN	Select <b>Any</b> to classify traffic from any VLAN or select the second option and specify the source VLAN ID in the field provided.
Priority	Select <b>Any</b> to classify traffic from any priority level or select <b>MAC</b> and specify a priority level in the field provided.
Ethernet Type	Select an Ethernet type or select <b>Other</b> and enter the Ethernet type number in hexadecimal value. Refer to <a href="#">Table 36 on page 125</a> for information. Select <b>All</b> if you don't know.
Source	
MAC Address	Select <b>Any</b> to apply the rule to all MAC addresses. To specify a source, select <b>MAC</b> and type a MAC address in valid MAC address format (six hexadecimal character pairs).
Port	Select the port to which the rule should be applied. You may choose one port only or all ports ( <b>All Ports</b> ).
Destination	
MAC Address	Select <b>Any</b> to apply the rule to all MAC addresses. To specify a destination, select the second choice and type a MAC address in valid MAC address format (six hexadecimal character pairs).
Layer 3 Specify the fields below to configure a layer 3 classifier.	
DSCP	Select <b>Any</b> to classify traffic from any DSCP or select the second option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.
IP Protocol	Select an IP protocol type or select <b>Other</b> and enter the protocol number in decimal value. Refer to <a href="#">Table 37 on page 126</a> for more information. You may select <b>Establish Only</b> for <b>TCP</b> protocol type. This means that the switch will pick out the packets that are sent to establish TCP connections.
Source	
IP Address/ Address Prefix	Enter a source IP address in dotted decimal notation. Specify the address prefix by entering the number of ones in the subnet mask.
Socket Number	<b>Note:</b> You <i>must</i> select either UDP or TCP in the IP Protocol field before you configure the socket numbers.  Select <b>Any</b> to apply the rule to all TCP/UDP protocol port numbers or select the second option and enter a TCP/UDP protocol port number.
Destination	
IP Address/ Address Prefix	Enter a destination IP address in dotted decimal notation. Specify the address prefix by entering the number of ones in the subnet mask.
Socket Number	<b>Note:</b> You <i>must</i> select either UDP or TCP in the IP Protocol field before you configure the socket numbers.  Select <b>Any</b> to apply the rule to all TCP/UDP protocol port numbers or select the second option and enter a TCP/UDP protocol port number.
Add	Click <b>Add</b> to save the changes.

**Table 34** Classifier (continued)

LABEL	DESCRIPTION
Cancel	Click <b>Cancel</b> to reset the fields back to your previous configuration.
Clear	Click <b>Clear</b> to set the above fields back to the factory defaults.

## 18.3 Viewing and Editing Classifier Configuration

To view a summary of the classifier configuration, scroll down to the summary table at the bottom of the **Classifier** screen. To change the settings of a rule, click a number in the **Index** field. When two rules conflict with each other, a higher layer rule has priority over lower layer rule.

**Figure 55** Classifier: Summary Table

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

The following table describes the labels in this screen.

**Table 35** Classifier: Summary Table

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

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

**Table 36** Common Ethernet Types and Protocol Number

ETHERNET TYPE	PROTOCOL NUMBER
IP ETHII	0800
X.75 Internet	0801
NBS Internet	0802
ECMA Internet	0803
Chaosnet	0804
X.25 Level 3	0805

**Table 36** Common Ethernet Types and Protocol Number (continued)

ETHERNET TYPE	PROTOCOL NUMBER
XNS Compat	0807
Banyan Systems	0BAD
BBN Simnet	5208
IBM SNA	80D5
AppleTalk AARP	80F3

Some of the most common IP ports are:

**Table 37** Common IP Ports

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

## 18.4 Classifier Example

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

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

**Figure 56** Classifier: Example

Classifier	
Active	<input checked="" type="checkbox"/>
Name	Example
Packet Format	All
VLAN	<input checked="" type="radio"/> Any <input type="radio"/> <input type="text"/>
Priority	<input checked="" type="radio"/> Any <input type="radio"/> 0
Ethernet Type	<input checked="" type="radio"/> IP <input type="radio"/> Others <input type="text"/> (Hex)
Layer 2	Source MAC Address <input checked="" type="radio"/> MAC <input type="text"/> 00 : 50 : ba : ad : 4f : 81 <input type="text"/> Port <input type="text"/> Port 2
Destination	<input checked="" type="radio"/> Any <input type="radio"/> MAC <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>
DSCP	<input checked="" type="radio"/> Any <input type="radio"/> <input type="text"/>
IP Protocol	<input checked="" type="radio"/> All <input type="checkbox"/> Establish Only <input type="radio"/> Others <input type="text"/> (Dec)
Layer 3	Source IP Address / Address Prefix <input type="text"/> 0.0.0.0 / <input type="text"/> Socket Number <input checked="" type="radio"/> Any <input type="radio"/> <input type="text"/>
Destination	IP Address / Address Prefix <input type="text"/> 0.0.0.0 / <input type="text"/> Socket Number <input checked="" type="radio"/> Any <input type="radio"/> <input type="text"/>
<input type="button" value="Add"/> <input type="button" value="Cancel"/> <input type="button" value="Clear"/>	

# CHAPTER 19

## Policy Rule

This chapter shows you how to configure policy rules.

### 19.1 Overview

A classifier distinguishes traffic into flows based on the configured criteria (refer to [Chapter 18 on page 122](#) for more information). A policy rule ensures that a traffic flow gets the requested treatment in the network.

#### 19.1.1 DiffServ

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

#### 19.1.2 DSCP and Per-Hop Behavior

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

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

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

### 19.2 Configuring Policy Rules

**Note:** You must first configure a classifier in the **Classifier** screen. Refer to [Chapter 18 on page 122](#) for more information.



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

**Figure 57** Policy

The screenshot shows a web-based configuration interface for a Policy Rule. At the top, there is a 'Policy' header with a blue bar. Below it, the 'Active' checkbox is unchecked. The 'Name' field is empty. The 'Classifier(s)' field is also empty. The 'Parameters' section is divided into 'General' and 'Metering' sub-sections. Under 'General', there are fields for 'VLAN ID', 'EgressPort' (set to 'Port1'), 'Outgoing packet format for Egress port' (radio buttons for 'Tag' and 'Untag'), 'Priority' (set to '0'), 'DSCP', and 'TOS' (set to '0'). Under 'Metering', there are fields for 'Bandwidth' (with 'Kbps' unit), 'Out-of-Profile', and 'DSCP'. The 'Action' section contains several sub-sections: 'Forwarding' with radio buttons for 'No change', 'Discard the packet', and 'Do not drop the matching frame previously marked for dropping'; 'Priority' with radio buttons for 'No change', 'Set the packet's 802.1 priority', 'Send the packet to priority queue', and 'Replace the 802.1 priority field with the IP TOS value'; 'Diffserv' with radio buttons for 'No change', 'Set the packet's TOS field', 'Replace the IP TOS field with the 802.1 priority value', and 'Set the Diffserv Codepoint field in the frame'; 'Outgoing' with checkboxes for 'Send the packet to the mirror port', 'Send the packet to the egress port', 'Send the matching frames(broadcast or DLF, multicast, marked for dropping or to be sent to the CPU) to the egress port', and 'Set the packet's VLAN ID'; 'Metering' with a checkbox for 'Enable'; and 'Out-of-profile action' with checkboxes for 'Drop the packet', 'Change the DSCP value', 'Set Out-Drop Precedence', and 'Do not drop the matching frame previously marked for dropping'. At the bottom, there are three buttons: 'Add', 'Cancel', and 'Clear'.

The following table describes the labels in this screen.

**Table 38** Policy

LABEL	DESCRIPTION
Active	Select this option to enable the policy.
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
Classifier(s)	This field displays the active classifier(s) you configure in the <b>Classifier</b> screen (refer to <a href="#">Chapter 18 on page 122</a> ). Select the classifier(s) to which this policy rule applies. To select more than one classifier, press [SHIFT] and select the choices at the same time.
Parameters Set the fields below for this policy. You only have to set the field(s) that is related to the action(s) you configure in the <b>Action</b> field.	
General	
VLAN ID	Specify a VLAN ID number.
Egress Port	Select an outgoing port.
Outgoing packet format for Egress Port	Select <b>Tag</b> to add the specified VID to packets on the specified outgoing port. Otherwise, select <b>Untag</b> . The switch removes the VLAN tag from the packets.
Priority	Specify a priority level.
DSCP	Specify a DSCP (DiffServ Code Point) number between 0 and 63.
TOS	Specify the type of service (TOS) priority level.
Metering	You can configure the desired bandwidth available to a traffic flow. Traffic that exceeds the maximum bandwidth allocated (in cases where the network is congested) is called out-of-profile traffic.
Bandwidth	Specify the bandwidth in mega bits per second (Mbps). Enter a number between 1 and 1023.
Out-of-Profile DSCP	Specify a new DSCP number (between 0 and 63) if you want to replace or remark the DSCP number for out-of-profile traffic.
Action Specify the action(s) the switch takes on the associated classified traffic flow.	
Forwarding	Select <b>No change</b> to forward the packets. Select <b>Discard packet</b> to drop the packets. Select <b>Do not drop the matching frame previously marked for dropping</b> to retain the frames that were marked to be dropped before.
Priority	Select <b>No change</b> to keep the priority setting of the frames. Select <b>Set the packet's 802.1 priority</b> to replace the 802.1 priority field with the value you set in the <b>Priority</b> field. Select <b>Send the packet to priority queue</b> to put the packets in the designated queue. Select <b>Replace the 802.1 priority field with IP TOS value</b> to replace the 802.1 priority field with the value you set in the <b>TOS</b> field.

**Table 38** Policy (continued)

LABEL	DESCRIPTION
DiffServ	Select <b>No change</b> to keep the TOS and/or DSCP fields in the packets. Select <b>Set the packet's TOS field</b> to set the TOS field with the value you configure in the <b>TOS</b> field. Select <b>Replace the IP TOS with the 802.1 priority value</b> to replace the TOS field with the value you configure in the <b>Priority</b> field. Select <b>Set the Diffserv Codepoint field in the frame</b> to set the DSCP field with the value you configure in the <b>DSCP</b> field.
Outgoing	Select <b>Send the packet to the mirror port</b> to send the packet to the mirror port. Select <b>Send the packet to the egress port</b> to send the packet to the egress port. Select <b>Send the matching frames (broadcast or DLF, multicast, marked for dropping or to be sent to the CPU) to the egress port</b> to send the broadcast, multicast, DLF, marked-to-drop or CPU frames to the egress port. Select <b>Set the packet's VLANID</b> to set the VLAN ID of the packet with the value you configure in the <b>VLANID</b> field.
Metering	Select <b>Enable</b> to activate bandwidth limitation on the traffic flow(s) then set the actions to be taken on out-of-profile packets.
Out-of-profile Action	Select the action(s) to be performed for out-of-profile traffic. Select <b>Drop the packet</b> to discard the out-of-profile traffic. Select <b>Change the DSCP Value</b> to replace the DSCP field with the value specified in the <b>Out-of-Profile DSCP</b> field above. Select <b>Do not drop the matching frame previously marked for dropping</b> to queue the frames that are marked to be dropped.
Add	Click <b>Add</b> to inset the entry to the summary table below.
Cancel	Click <b>Cancel</b> to reset the fields back to your previous configuration.
Clear	Click <b>Clear</b> to set the above fields back to the factory defaults.

## 19.3 Viewing and Editing Policy Configuration

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

**Figure 58** Policy: Summary Table

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

Delete Cancel

The following table describes the labels in this screen.

**Table 39** Policy: Summary Table

LABEL	DESCRIPTION
Index	This field displays the policy index number. Click an index number to edit the policy.
Active	This field displays <b>Yes</b> when policy is activated and <b>No</b> when is it deactivated.

**Table 39** Policy: Summary Table (continued)

LABEL	DESCRIPTION
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
Classifier(s)	This field displays the name(s) of the classifier to which this policy applies.
Delete	Click <b>Delete</b> to remove the selected entry from the summary table.
Cancel	Click <b>Cancel</b> to clear the <b>Delete</b> check boxes.

## 19.4 Policy Example

The figure below shows an example **Policy** screen where you configure a policy to limit bandwidth and discard out-of-profile traffic on a traffic flow classified using the **Example** classifier (refer to [Section 18.4 on page 126](#)).

**Figure 59** Policy Example

Policy																																					
Active	<input checked="" type="checkbox"/>																																				
Name	Test																																				
Classifier(s)	Example																																				
Parameters	<table border="0"> <tr> <td>VLAN ID</td> <td>1</td> <td>General</td> <td>Bandwidth</td> <td>1000</td> <td>Mbps</td> </tr> <tr> <td>EgressPort</td> <td>Port 1</td> <td></td> <td>Out-of-Profile DSCP</td> <td>63</td> <td></td> </tr> <tr> <td>Outgoing packet format for Egress port</td> <td><input checked="" type="radio"/> Tag <input type="radio"/> Untag</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Priority</td> <td>0</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>DSCP</td> <td>0</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>TOS</td> <td>0</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	VLAN ID	1	General	Bandwidth	1000	Mbps	EgressPort	Port 1		Out-of-Profile DSCP	63		Outgoing packet format for Egress port	<input checked="" type="radio"/> Tag <input type="radio"/> Untag					Priority	0					DSCP	0					TOS	0				
	VLAN ID	1	General	Bandwidth	1000	Mbps																															
	EgressPort	Port 1		Out-of-Profile DSCP	63																																
	Outgoing packet format for Egress port	<input checked="" type="radio"/> Tag <input type="radio"/> Untag																																			
	Priority	0																																			
	DSCP	0																																			
	TOS	0																																			
Action	<b>Forwarding</b> <input checked="" type="radio"/> No change <input type="radio"/> Discard the packet <input type="radio"/> Do not drop the matching frame previously marked for dropping																																				
	<b>Priority</b> <input checked="" type="radio"/> No change <input type="radio"/> Set the packet's 802.1 priority <input type="radio"/> Send the packet to priority queue <input type="radio"/> Replace the 802.1 priority field with the IP TOS value																																				
	<b>Diffserv</b> <input checked="" type="radio"/> No change <input type="radio"/> Set the packet's TOS field <input type="radio"/> Replace the IP TOS field with the 802.1 priority value <input type="radio"/> Set the Diffserv Codepoint field in the frame																																				
	<b>Outgoing</b> <input type="checkbox"/> Send the packet to the mirror port <input type="checkbox"/> Send the packet to the egress port <input type="checkbox"/> Send the matching frames(broadcast or DLF, multicast, marked for dropping or to be sent to the CPU) to the egress port <input type="checkbox"/> Set the packet's VLAN ID																																				
	<b>Metering</b> <input type="checkbox"/> Enable																																				
	<b>Out-of-profile action</b> <input checked="" type="checkbox"/> Drop the packet <input type="checkbox"/> Change the DSCP value <input type="checkbox"/> Do not drop the matching frame previously marked for dropping																																				
	<input type="button" value="Add"/> <input type="button" value="Cancel"/> <input type="button" value="Clear"/>																																				

# CHAPTER 20

## Queuing Method

This chapter introduces the queuing methods supported.

### 20.1 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.

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

**Table 40** Physical Queue Priority

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

#### 20.1.1 Strict Priority Queuing (SPQ)

Strict Priority Queuing (SPQ) services queues based on priority only. As traffic comes into the switch, traffic on the highest priority queue, 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.

## 20.1.2 Weighted Round Robin Scheduling (WRR)

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

Weighted Round Robin Scheduling (WRR) uses the same algorithm as round robin scheduling, but services queues based on their priority and queue weight (the number you configure in the 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.

## 20.2 Configuring Queuing

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

**Figure 60** Queuing Method

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

The following table describes the labels in this screen.

**Table 41** Queuing Method

LABEL	DESCRIPTION
Port	This label shows the port you are configuring.
Method	<p>Select <b>SPQ</b> (Strict Priority Queuing) or <b>WRR</b> (Weighted Round Robin).</p> <p>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.</p> <p>Weighted Round Robin Scheduling (WRR) services queues on a rotating basis based on their queue weight (the number you configure in the queue <b>Weight</b> field). Queues with larger weights get more service than queues with smaller weights.</p>
Q0~Q7 Weight %	When you select <b>WRR</b> , enter the queue weight here. Bandwidth is divided across the different traffic queues according to their weights. Queues with larger weights get more service than queues with smaller weights.
Apply	Click <b>Apply</b> to save your changes back to the switch.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.
Calculate	Click <b>Calculate</b> to make sure the WFQ queuing weights total to 100%; if not an error message is displayed.





# CHAPTER 21

## VLAN Stacking

This chapter shows you how to configure VLAN stacking on your switch. See the chapter on VLANs for more background information on Virtual LAN

### 21.1 Introduction

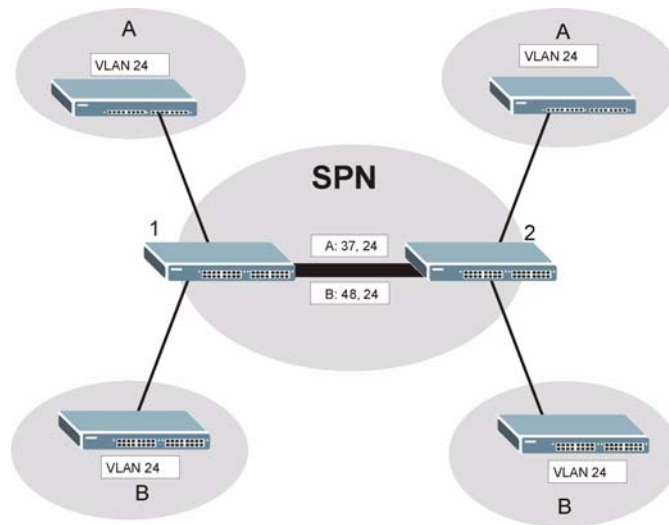
A service provider can use VLAN stacking to allow it to distinguish multiple customers VLANs, even those with the same (customer-assigned) VLAN ID, within its network.

Use VLAN stacking to add an outer VLAN tag to the inner IEEE 802.1Q tagged frames that enter the network. By tagging the tagged frames (“double-tagged” frames), the service provider can manage up to 4,094 VLAN groups with each group containing up to 4,094 customer VLANs. This allows a service provider to provide different service, based on specific VLANs, for many different customers.

A service provider's customers may require a range of VLANs to handle multiple applications. A service provider's customers can assign their own inner VLAN tags on ports for these applications. The service provider can assign an outer VLAN tag for each customer. Therefore, there is no VLAN tag overlap among customers, so traffic from different customers is kept separate.

#### 21.1.1 VLAN Stacking Example

In the following example figure, both A and B are Service Provider's Network (SPN) customers with VPN tunnels between their head offices and branch offices respectively. Both have an identical VLAN tag for their VLAN group. The service provider can separate these two VLANs within its network by adding tag 37 to distinguish customer A and tag 48 to distinguish customer B at edge device 1 and then stripping those tags at edge device 2 as the data frames leave the network.

**Figure 61** VLAN Stacking Example

## 21.2 VLAN Stacking Port Roles

Each port can have three VLAN stacking “roles”, **Normal**, **Access Port** and **Tunnel** (the latter is for Gigabit ports only).

- Select **Normal** for “regular” (non-VLAN stacking) IEEE 802.1Q frame switching.
- Select **Access Port** for ingress ports on the service provider's edge devices (1 and 2 in the VLAN stacking example figure). The incoming frame is treated as "untagged", so a second VLAN tag (outer VLAN tag) can be added.

**Note:** Static VLAN Tx Tagging **MUST** be disabled on a port where you choose Normal or Access Port.

- Select **Tunnel** (available for Gigabit ports only) for egress ports at the edge of the service provider's network. All VLANs belonging to a customer can be aggregated into a single service provider's VLAN (using the outer VLAN tag defined by SP VID).

**Note:** Static VLAN Tx Tagging **MUST** be enabled on a port where you choose Tunnel.

## 21.3 VLAN Tag Format

A VLAN tag (service provider VLAN stacking or customer IEEE 802.1Q) consists of the following three fields.

**Table 42** VLAN Tag Format

Type	Priority	VID
------	----------	-----

**Type** is a standard Ethernet type code identifying the frame and indicates that whether the frame carries IEEE 802.1Q tag information. **SP TPID** (Service Provider Tag Protocol Identifier) is the service provider VLAN stacking tag type. Many vendors use 0x8100 or 0x9100.

**TPID** (Tag Protocol Identifier) is the customer IEEE 802.1Q tag.

- If the VLAN stacking port role is **Access Port**, then the switch adds the **SP TPID** tag to all incoming frames on the service provider's edge devices (1 and 2 in the VLAN stacking example figure).
- If the VLAN stacking port role is **Tunnel**, then the switch only adds the **SP TPID** tag to all incoming frames on the service provider's edge devices (1 and 2 in the VLAN stacking example figure) that have an **SP TPID** different to the one configured on the switch. (If an incoming frame's **SP TPID** is the same as the one configured on the switch, then the switch will not add the tag.)

**Priority** refers to the IEEE 802.1p standard that allows the service provider to prioritize traffic based on the class of service (CoS) the customer has paid for.

- On the switch, configure priority level of inner IEEE 802.1Q tag in the **Port Setup** screen.
- "0" is the lowest priority level and "7" is the highest.

**VID** is the VLAN ID. **SP VID** is the VID for the second (service provider's) VLAN tag.

### 21.3.1 Frame Format

The frame format for an untagged Ethernet frame, a single-tagged 802.1Q frame (customer) and a "double-tagged" 802.1Q frame (service provider) is shown next.

Configure the fields as circled in the switch **VLAN Stacking** screen.

**Table 43** Single and Double Tagged 802.11Q Frame Format

						DA	SA	Len/Etype	Data	FCS	Untagged Ethernet frame
			DA	SA	<b>TPID</b>	<b>Priority</b>	<b>VID</b>	Len/Etype	Data	FCS	IEEE 802.1Q customer tagged frame
DA	SA	<b>SPTPID</b>	<b>Priority</b>	<b>VID</b>	<b>TPID</b>	<b>Priority</b>	<b>VID</b>	Len/Etype	Data	FCS	Double-tagged frame

**Table 44** 802.1Q Frame

DA	Destination Address	Priority	802.1p Priority
SA	Source Address	Len/Etype	Length and type of Ethernet frame
(SP)TPID	(Service Provider) Tag Protocol IDentifier	Data	Frame data
VID	VLAN ID	FCS	Frame Check Sequence

## 21.4 Configuring VLAN Stacking

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

**Figure 62** VLAN Stacking

Port	Role	SPVID	Priority
1	Access Port	1	0
2	Access Port	1	0
3	Access Port	1	0
4	Access Port	1	0
5	Access Port	1	0
6	Access Port	1	0
7	Access Port	1	0
8	Access Port	1	0
9	Access Port	1	0
10	Access Port	1	0
11	Access Port	1	0
12	Access Port	1	0

The following table describes the labels in this screen.

**Table 45** VLAN Stacking

LABEL	DESCRIPTION
Active	Select this checkbox to enable VLAN stacking on the switch.
SP TPID	<b>SP TPID</b> is a standard Ethernet type code identifying the frame and indicates whether the frame carries IEEE 802.1Q tag information. Choose <b>0x8100</b> or <b>0x9100</b> from the drop-down list box or select <b>Others</b> and then enter a four-digit hexadecimal number from 0x0000 to 0xFFFF. 0x denotes a hexadecimal number. It does not have to be typed in the <b>Others</b> text field.
Port	The port number identifies the port you are configuring.
Role	Select <b>Normal</b> to have the switch ignore frames received (or transmitted) on this port with VLAN stacking tags. Anything you configure in <b>SPVID</b> and <b>Priority</b> are ignored. Select <b>Access Port</b> to have the switch add the <b>SP TPID</b> tag to all incoming frames received on this port. Select <b>Access Port</b> for ingress ports at the edge of the service provider's network. Select <b>Tunnel</b> (available for Gigabit ports only) for egress ports at the edge of the service provider's network. In order to support VLAN stacking on a port, the port must be able to allow frames of 1526 Bytes (1522 Bytes + 4 Bytes for the second tag) to pass through it.
SPVID	<b>SPVID</b> is the service provider's VLAN ID (the outer VLAN tag). Enter the service provider ID (from 1 to 4094) for frames received on this port. See <a href="#">Chapter 8 on page 84</a> for more background information on VLAN ID.

**Table 45** VLAN Stacking (continued)

LABEL	DESCRIPTION
Priority	Select a number from the drop-down list box to configure the priority level of the outer tag. "0" is the lowest priority level and "7" is the highest.  <b>Note:</b> Configure the priority level of the inner IEEE 802.1Q tag in the <b>Port Setup</b> screen.
Apply	Click <b>Apply</b> to save your changes back to the switch.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.



# CHAPTER 22

## Multicast

This chapter shows you how to configure various multicast features.

### 22.1 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 session-layer protocol used to establish membership in a multicast group - it is not used to carry user data. Refer to RFC 1112 and RFC 2236 for information on IGMP versions 1 and 2 respectively.

#### 22.1.1 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).

#### 22.1.2 IGMP Filtering

With IGMP filtering, 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.

#### 22.1.3 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.

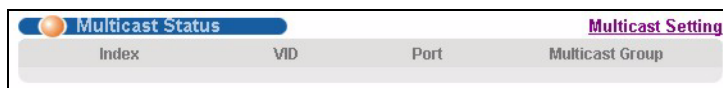


The switch forwards multicast traffic destined for multicast groups (that it has learned from IGMP snooping) to ports that are members of that group. The switch discards multicast traffic destined for multicast groups that it does not know. IGMP snooping generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through your switch.

## 22.2 Multicast Status

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

**Figure 63** Multicast: Status



The following table describes the labels in this screen.

**Table 46** 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.

### 22.2.1 Multicast Setting

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

**Figure 64** Multicast: Setting

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

The following table describes the labels in this screen.

**Table 47** Multicast: Setting

LABEL	DESCRIPTION
IGMP Snooping	Select <b>Active</b> to enable IGMP snooping to forward group multicast traffic only to ports that are members of that group
IGMP Filtering	Select <b>Active</b> to enable IGMP filtering to limit the 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 <b>Drop</b> to discard the frame(s). Select <b>Forwarding</b> to send the frame(s) to the destination device.
Port	This field displays the port number.
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 No.	Select this option and enter a number to limit 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 <b>Default</b> to prohibit the port from joining any multicast group.

**Table 47** Multicast: Setting (continued)

LABEL	DESCRIPTION
IGMP Querier Mode	<p>The switch treats an IGMP query port as being connected to an IGMP multicast router (or server). The switch forwards IGMP join or leave packets to an IGMP query port.</p> <p>Select <b>Auto</b> to have the switch dynamically change to using the port as an IGMP query port after it receives IGMP query packets.</p> <p>Select <b>Fixed</b> to have the switch always use the port as an IGMP query port. Select this when you connect an IGMP multicast server to the port.</p> <p>Select <b>Edge</b> to stop the switch from using the port as an IGMP query port. The switch will not keep any record of an IGMP router being connected to this port. The switch does not forward IGMP join or leave packets to this port.</p>
Apply	Click <b>Apply</b> to save your changes back to the switch.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 22.2.2 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 65** Multicast: Setting: IGMP Filtering Profile

The screenshot shows the 'IGMP Filtering Profile' configuration interface. At the top, there is a title bar with 'IGMP Filtering Profile' and a 'Multicast Setting' link. Below the title bar, there is a 'Profile Setup' section. This section contains a table with three columns: 'Profile Name', 'Start Address', and 'End Address'. The first row of the table has an empty 'Profile Name' field, '224.0.0.0' in the 'Start Address' field, and '224.0.0.0' in the 'End Address' field. Below the table, there are 'Add' and 'Clear' buttons. At the bottom of the screen, there are 'Delete' and 'Cancel' buttons.

The following table describes the labels in this screen.

**Table 48** Multicast: Setting: IGMP Filtering Profile

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name for the profile for identification purposes.  <b>Note:</b> To configure additional rule(s) for a profile that you have already added, enter the same 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 <b>Start Address</b> and <b>End Address</b> fields.
Add	Click <b>Add</b> to save the settings to the switch.
Clear	Click <b>Clear</b> 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 <b>Delete Profile</b> column, then click the <b>Delete</b> button.  To delete a rule(s) from a profile, select the rule(s) that you want to remove in the <b>Delete Rule</b> column, then click the <b>Delete</b> button.
Cancel	Click <b>Cancel</b> to clear the <b>Delete Profile/Delete Rule</b> check boxes.

## 22.3 MVR Overview

Multicast VLAN Registration (MVR) is designed for applications (such as Media-on-Demand (MoD)) that use multicast traffic across a 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 66** MVR Network Example

### 22.3.1 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 traffic. Once configured, the switch maintains a forwarding table that matches the multicast stream to the associated multicast group.

### 22.3.2 MVR Modes

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

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

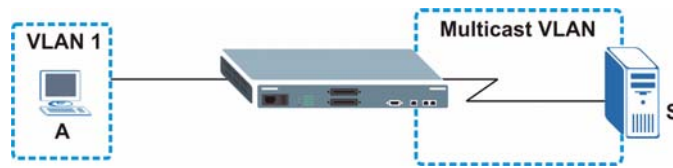
In compatible mode, the switch does not send any IGMP reports. In this case, you must manually configure the forwarding settings on the multicast devices in the multicast VLAN.

### 22.3.3 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 67** MVR Multicast Television Example

## 22.4 General MVR Configuration

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

Click **Advanced Applications** and **Multicast** in the navigation panel. Click the **Multicast Setting** link and then the **MVR** link to display the screen as shown next.

**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 68** Multicast: Setting: MVR

MVR
Multicast Setting [Group Configuration](#)

Active

Name

Multicast VLAN ID

Mode  Dynamic  Compatible

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

VLAN	Active	Name	Mode	Source Port	Receiver Port	Delete

The following table describes the related labels in this screen.

**Table 49** Multicast: Setting: 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.
Mode	Specify the MVR mode on the switch. Choices are <b>Dynamic</b> and <b>Compatible</b> . Select <b>Dynamic</b> to send IGMP reports to all MVR source ports in the multicast VLAN. Select <b>Compatible</b> 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 <b>Ethernet</b> 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 <b>Add</b> to save the settings.
Cancel	Click <b>Cancel</b> 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 the group(s) and all the accompanying rules, select the group(s) that you want to remove in the <b>Delete</b> column, then click the <b>Delete</b> button.
Cancel	Click <b>Cancel</b> to clear the <b>Delete</b> check boxes.

## 22.5 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 69** MVR: Group Configuration

The following table describes the labels in this screen.

**Table 50** Multicast: Setting: MVR: Group Configuration

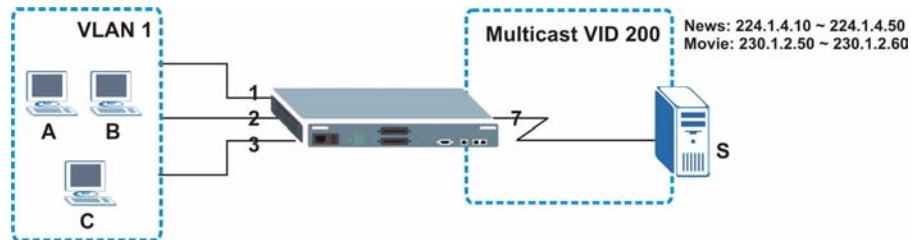
LABEL	DESCRIPTION
Multicast VLAN ID	Select a multicast VLAN ID (that you configured in the <b>MVR</b> screen) from the drop-down list box.
Name	Enter a descriptive name for identification purposes.
Start Address	Enter the starting IP multicast address of the multicast group in dotted decimal notation. Refer to <a href="#">Section 22.1.1 on page 144</a> 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 <b>Start Address</b> field if you want to configure only one IP address for a multicast group. Refer to <a href="#">Section 22.1.1 on page 144</a> for more information on IP multicast addresses.
Add	Click <b>Add</b> to save the settings.
Cancel	Click <b>Cancel</b> 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 <b>Delete All</b> and click <b>Delete</b> to remove all entries from the table. Select <b>Delete Group</b> and click <b>Delete</b> to remove the selected entry(ies) from the table.
Cancel	Select <b>Cancel</b> to clear the checkbox(es) in the table.



## 22.5.1 MVR Configuration Example

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

**Figure 70** 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 71** MVR Configuration Example

**MVR** Multicast Setting   Group Configuration

Active

Name

Multicast VLAN ID

Mode  Dynamic  Compatible

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 checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" 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"/>

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 72** MVR Group Configuration Example

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

Name	Start Address	End Address
Movie	230.1.2.50	230.1.2.60

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"/>

**Figure 73** MVR Group Configuration Example

The screenshot shows the 'Group Configuration' interface for MVR. At the top, there is a 'Multicast VLAN ID' dropdown menu set to '200'. Below this is a table for adding new groups. The table has three columns: 'Name', 'Start Address', and 'End Address'. One row is present with 'Name' as an empty field, 'Start Address' as '0.0.0.0', and 'End Address' as '0.0.0.0'. Below the table are 'Add' and 'Cancel' buttons. At the bottom, there is a table showing existing groups for MVLAN 200. It has columns for 'Name', 'Start Address', 'End Address', 'Delete All', and 'Delete Group'. Two rows are present: one with 'Name' as 'Movie', 'Start Address' as '230.1.2.50', and 'End Address' as '230.1.2.60'; and another with 'Name' as 'News', 'Start Address' as '224.1.4.10', and 'End Address' as '224.1.4.50'. This entire table is circled in red. Below this table are 'Delete' and 'Cancel' buttons.

Name	Start Address	End Address
	0.0.0.0	0.0.0.0

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"/>
200	News	224.1.4.10	224.1.4.50	<input type="checkbox"/>	<input type="checkbox"/>



# CHAPTER 23

## Static Route

This chapter shows you how to configure static routes.

### 23.1 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 74** Static Routing

Index	Active	Name	Destination Address	Subnet Mask	Gateway Address	Metric	Delete
1	Yes	Example	172.21.1.1	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 51** 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.
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.

**Table 51** Static Routing (continued)

LABEL	DESCRIPTION
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 <b>Add</b> to insert a new static route.
Cancel	Click <b>Cancel</b> to reset the above fields to your previous configuration.
Clear	Click <b>Clear</b> 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 <b>Yes</b> when the static route is activated and <b>NO</b> 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 <b>Delete</b> to remove the selected entry from the summary table.
Cancel	Click <b>Cancel</b> to clear the <b>Delete</b> check boxes.

# CHAPTER 24

## RIP

This chapter shows you how to configure RIP (Routing Information Protocol).

### 24.1 Overview

RIP (Routing Information Protocol) allows a routing device to exchange routing information with other routers. The **Direction** field controls the sending and receiving of RIP packets. When set to:

- **Both** - the switch will broadcast its routing table periodically and incorporate the RIP information that it receives.
- **Incoming** - the switch will not send any RIP packets but will accept all RIP packets received.
- **Outgoing** - the switch will send out RIP packets but will not accept any RIP packets received.
- **None** - the switch will not send any RIP packets and will ignore any RIP packets received.

The **Version** field controls the format and the broadcasting method of the RIP packets that the switch sends (it recognizes both formats when receiving). **RIP-1** is universally supported; but RIP-2 carries more information. **RIP-1** is probably adequate for most networks, unless you have an unusual network topology.

Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting.

### 24.2 Configuring

Click **IP Application, RIP** in the navigation panel to display the screen as shown. You cannot manually configure a new entry. Each entry in the table is automatically created when you configure a new IP domain in the **IP Setup** screen (refer to [Section 7.7 on page 79](#)).

**Figure 75** RIP

Index	Network	Direction	Version
1	192.168.1.1/24	None	RIP-1

The following table describes the labels in this screen.

**Table 52** RIP

LABEL	DESCRIPTION
Active	Select this check box to enable RIP on the switch.
Index	This field displays the index number of an IP interface.
Network	This field displays the IP interface configured on the switch. Refer to the section on IP Setup for more information on configuring IP domains.
Direction	Select the RIP direction from the drop-down list box. Choices are <b>Outgoing</b> , <b>Incoming</b> , <b>Both</b> and <b>None</b> .
Version	Select the RIP version from the drop-down list box. Choices are <b>RIP-1</b> , <b>RIP-2B</b> and <b>RIP-2M</b> .
Apply	Click <b>Apply</b> to save your changes back to the switch.
Cancel	Click <b>Cancel</b> to begin configuring the fields again.

# CHAPTER 25

## OSPF

This chapter describes the OSPF (Open Shortest Path First) routing protocol and shows you how to configure OSPF.

### 25.1 Overview

OSPF (Open Shortest Path First) is a link-state protocol designed to distribute routing information within an autonomous system (AS). An autonomous system is a collection of networks using a common routing protocol to exchange routing information.

OSPF offers some advantages over traditional vector-space routing protocols (such as RIP). The following table summarizes some of the major differences between OSPF and RIP.

**Table 53** OSPF vs. RIP

	OSPF	RIP
Network Size	Large	Small (with up to 15 routers)
Metrics	Bandwidth, hop count, throughput, round trip time and reliability.	Hop count
Convergence	Fast	Slow

#### 25.1.1 OSPF Autonomous Systems and Areas

An OSPF autonomous system can be divided into logical areas. Each area represents a group of adjacent networks. All areas are connected to a backbone (also known as area 0). The backbone is the transit area to route packets between two areas. A stub area, at the edge of an AS, is not a transit area since there is only one connection to the stub area.

The following table describes the four classes of OSPF routers.

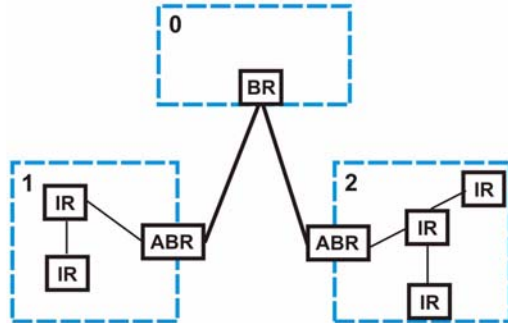
**Table 54** OSPF: Router Types

TYPE	DESCRIPTION
Internal Router (IR)	An Internal or intra-area router is a router in an area.
Area Border Router (ABR)	An Area Border Router connects two or more areas.
Backbone Router (BR)	A backbone router has an interface to the backbone.
AS Boundary Router	An AS boundary router exchanges routing information with routers in other ASes.



The following figure depicts an OSPF network example. The backbone is area 0 with a backbone router. The internal routers are in area 1 and 2. The area border routers connect area 1 and 2 to the backbone.

**Figure 76** OSPF Network Example



## 25.1.2 How OSPF Works

Layer 3 devices exchange routing information to build synchronized link state database within the same AS or area. They do this by exchanging Hello messages to confirm which neighbor (layer 3) devices exist and then they exchange database descriptions (DDs) to create the link state database. The link state database is constantly updated through LSAs (Link State Advertisements).

The link state database contains records of router IDs, their associated links and path costs. Each device can then use the link state database and Dijkstra algorithm to compute the least cost paths to network destinations.

## 25.1.3 Interfaces and Virtual Links

An OSPF interface is a link between a layer 3 device and an OSPF network. An interface has state information, an IP address and subnet mask associated with it. When you configure an OSPF interface, you first set an interface to transmit OSPF traffic and add the interface to an area.

You can configure a virtual link to establish/maintain connectivity between a non-backbone area and the backbone. The virtual link must be configured on both layer 3 devices in the non-backbone area and the backbone.

## 25.1.4 Configuring OSPF

To configure OSPF on the switch, do the following tasks

- 1 Enable OSPF
- 2 Create OSPF areas
- 3 Create and associate interface(s) to an area
- 4 Create virtual links to maintain backbone connectivity.

## 25.2 OSPF Status

To view current OSPF status, click **IP Application**, **OSPF** in the navigation panel to display the screen as shown next.

**Figure 77** OSPF Status

**OSPF Status** Configuration

OSPF: Running

**Interface:**

```
VLINK0 is down, line protocol is down
  OSPF is enabled, but not running on this interface
swif2 is up, line protocol is up
  Internet Address 192.168.1.10/24, Area 192.168.1.1
  Router ID 192.168.1.10, Network Type BROADCAST, Cost: 15
  Transmit Delay is 1 sec, State Backup, Priority 1
```

**Neighbor:**

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.1.1	1	Full/DR	00:00:34	192.168.1.1	swif2:192.168.1.10

**Link State Database:**

```
OSPF Router with ID (192.168.1.10)
  Router Link States (Area 0.0.0.0)
Link ID      ADV Router    Age  Seq#    CkSum  Link count
```

Poll Interval(s)

The following table describes the labels in this screen.

**Table 55** OSPF Status

LABEL	DESCRIPTION
OSPF	This field displays whether OSPF is activated ( <b>Running</b> ) or not ( <b>Down</b> ).
Interface	The text box displays the OSPF status of the interface(s) on the switch.
Neighbor	The text box displays the status of the neighboring router participating in the OSPF network.
Link State Database	The text box displays information in the link state database which contains data in the LSAs.
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 <b>Set Interval</b> .
Stop	Click <b>Stop</b> to end OSPF status polling.

The following table describes some common output fields.

**Table 56** OSPF Status: Common Output Fields

FIELD	DESCRIPTION
Interface	
Internet Address	This field displays the IP address and subnet bits of an IP routing domain.
Area	This field displays the area ID.
Router ID	This field displays the unique ID of the switch.
Transmit Delay	This field displays the transmission delay in seconds.
State	This field displays the state of the switch ( <b>backup</b> or <b>DR</b> (designated router)).
Priority	This field displays the priority of the switch. This number is used in the designated router election.
Designated Router	This field displays the router ID of the designated router.
Backup Designated Router	This field displays the router ID of a backup designated router.
Time Intervals Configured	This field displays the time intervals (in seconds) configured.
Neighbor Count	This field displays the number of neighbor routers.
Adjacent Neighbor Count	This field displays the number of neighbor router(s) that is adjacent to the switch.
Neighbor	
Neighbor ID	This field displays the router ID of the neighbor.
Pri	This field displays the priority of the neighbor. This number is used in the designated router election.
State	This field displays the state of the neighbor ( <b>backup</b> or <b>DR</b> (designated router)).
Dead Time	This field displays the dead time in seconds.
Address	This field displays the IP address of a neighbor.
Interface	This field displays the MAC address of a device.
Link State Database	
Link ID	This field displays the ID of a router or subnet.
ADV Router	This field displays the IP address of the layer-3 device that sends the LSAs.
Age	This field displays the time (in seconds) since the last LSA was sent.
Seq #	This field displays the link sequence number of the LSA.
Checksum	This field displays the checksum value of the LSA.
Link Count	This field displays the number of links in the LSA.

## 25.3 Enabling OSPF and General Settings

To activate OSPF and set general settings, click **IP Application**, **OSPF** and the **Configuration** link to display the **OSPF Configuration** screen.

**Figure 78** OSPF Configuration: Activating and General Settings

The screenshot shows the OSPF Configuration interface. The top section, titled 'OSPF Configuration', has tabs for 'Interface', 'Virtual-Link', and 'Status'. The 'Active' checkbox is unchecked. The 'Router ID' is set to 0.0.0.0. Below this, the 'Redistribute Route' section has a table with columns: 'Redistribute Route', 'Active', 'Type', and 'Metric value'. The 'RIP' and 'Static' rows are checked, with 'Type' set to 1 and 'Metric value' set to 15. 'Apply' and 'Cancel' buttons are below. The 'General Settings' section has fields for 'Name' (name), 'Area ID' (0.0.0.0), 'Authentication' (None), 'Stub Network' (unchecked), 'No Summary' (unchecked), and 'Default route cost' (15). 'Add', 'Cancel', and 'Clear' buttons are below. At the bottom, a table with columns 'Index', 'Name', 'Area ID', 'Authentication', 'Stub Network', and 'Delete' is shown, with 'Delete' and 'Cancel' buttons below it.

The follow table describes the related labels in this screen.

**Table 57** OSPF Configuration: Activating and General Settings

LABEL	DESCRIPTION
Active	OSPF is disabled by default. Select this option to enable it.
Router ID	Router ID uniquely identifies the switch in an OSPF. Enter a unique ID (that uses the format of an IP address in dotted decimal notation) for the switch.
Redistribute Route	Route redistribution allows your switch to import and translate external routes learned through other routing protocols ( <b>RIP</b> and <b>Static</b> ) into the OSPF network transparently.
Active	Select this option to activate route redistribution for routes learn through the selected protocol.
Type	Select <b>1</b> for routing protocols (such as RIP) whose external metrics are directly comparable to the internal OSPF cost. When selecting a path, the internal OSPF cost is added to the AB boundary router to the external metrics. Select <b>2</b> for routing protocols whose external metrics are not comparable to the OSPF cost. In this case, the external cost of the AB boundary router is used in path decision to a destination.
Metric Value	Enter a route cost (between 0 and 16777214).
Apply	Click <b>Apply</b> to save the changes.
Cancel	Click <b>Cancel</b> to start configuring the above fields again.

## 25.4 Configuring OSPF Areas

To ensure that the switch receives only routing information from a trusted layer 3 devices, activate authentication. The OSPF supports three authentication methods:

- None – no authentication is used.
- Simple – authenticate link state updates using an 8 printable ASCII character password.
- MD5 – authenticate link state updates using a 16 printable ASCII character password.

To configure an area, set the related fields in the **OSPF Configuration** screen.

**Figure 79** OSPF Configuration: Area Setup

The screenshot shows the 'OSPF Configuration' screen with the following details:

- General Configuration:**
  - Active:
  - Router ID: 0.0.0.0
- Redistribute Route Table:**

Redistribute Route	Active	Type	Metric value
RIP	<input checked="" type="checkbox"/>	1	15
Static	<input checked="" type="checkbox"/>	1	15
- Area Configuration (Circled):**
  - Name: name
  - Area ID: 0.0.0.0
  - Authentication: None
  - Stub Network:
  - No Summary:
  - Default route cost: 15
- Area List Table:**

Index	Name	Area ID	Authentication	Stub Network	Delete

The following table describes the related labels in this screen.

**Table 58** OSPF Configuration: Area Setup

LABEL	DESCRIPTION
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
Area ID	Enter a 32-bit ID (that uses the format of an IP address in dotted decimal notation) that uniquely identifies an area. A value of <b>0.0.0.0</b> indicates that this is a backbone (also known as Area 0). You can create only one backbone area on the switch.

**Table 58** OSPF Configuration: Area Setup (continued)

LABEL	DESCRIPTION
Authentication	Select an authentication method ( <b>Simple</b> or <b>MD5</b> ) to activate authentication. Select <b>None</b> to disable authentication. Interface(s) and virtual interface(s) must use the same authentication method as the associated area.
Stub Area	Select this option to set the area as a stub area. If you enter <b>0.0.0.0</b> in the <b>Area ID</b> field, the settings in the <b>Stub Area</b> fields are ignored.
No Summary	Select this option to set the switch to not send/receive LSAs.
Default Route Cost	Specify a cost (between 0 and 16777214) used to add a default route into a stub area for routes which are external to an OSPF domain. If you do not set a route cost, no default route is added.
Add	Click <b>Add</b> to apply the changes.
Cancel	Click <b>Cancel</b> to start configuring the above fields again.
Clear	Click <b>Clear</b> to set the above fields back to the factory defaults.

### 25.4.1 Viewing OSPF Area Information Table

The bottom of the **OSPF Configuration** screen displays a summary table of all the OSPF areas you have configured.

**Figure 80** OSPF Configuration: Summary Table

Index	Name	Area ID	Authentication	Stub Network	Delete
1	Example	192.168.1.1	None	No	<input type="checkbox"/>

The following table describes the related labels in this screen.

**Table 59** OSPF Configuration: Summary Table

LABEL	DESCRIPTION
Index	This field displays the index number of an area.
Name	This field displays the descriptive name of an area.
Area ID	This field displays the area ID (that uses the format of an IP address in dotted decimal notation) that uniquely identifies an area. An area ID of <b>0.0.0.0</b> indicates the backbone.
Authentication	This field displays the authentication method used ( <b>None</b> , <b>Simple</b> or <b>MD5</b> ).
Stub Network	This field displays whether an area is a stub network ( <b>Yes</b> ) or not ( <b>No</b> ).
Delete	Click <b>Delete</b> to remove the selected entry from the summary table.
Cancel	Click <b>Cancel</b> to clear the <b>Delete</b> check boxes.

## 25.5 Configuring OSPF Interfaces

To configure an OSPF interface, first create an IP routing domain in the **IP Setup** screen (see [Section 7.7 on page 79](#) for more information). Once you create an IP routing domain, an OSPF interface entry is automatically created.

In the **OSPF Configuration** screen, click **Interface** to display the **OSPF Interface** screen.

**Figure 81** OSPF Interface

The following table describes the labels in this screen.

**Table 60** OSPF Interface

LABEL	DESCRIPTION
Network	Select an IP interface.
Area ID	Select the area ID (that uses the format of an IP address in dotted decimal notation) of an area to associate the interface to that area.
Authentication	<p><b>Note:</b> OSPF Interface(s) must use the same authentication method within the same area.</p> <p>Select an authentication method. Choices are <b>Same-as-Area</b>, <b>None</b> (default), <b>Simple</b> and <b>MD5</b>.</p> <p>To participate in an OSPF network, you must set the authentication method and/or password the same as the associated area.</p> <p>Select <b>Same-as-Area</b> to use the same authentication method within the area and set the related fields when necessary.</p> <p>Select <b>None</b> to disable authentication. This is the default setting.</p> <p>Select <b>Simple</b> and set the <b>Key</b> field to authenticate OSPF packets transmitted through this interface using simple password authentication.</p> <p>Select <b>MD5</b> and set the <b>Key ID</b> and <b>Key</b> fields to authenticate OSPF packets transmitted through this interface using MD5 authentication.</p>
Key ID	When you select <b>MD5</b> in the <b>Authentication</b> field, specify the identification number of the authentication you want to use.

**Table 60** OSPF Interface (continued)

LABEL	DESCRIPTION
Key	When you select <b>Simple</b> in the <b>Authentication</b> field, enter a password eight-character long. Characters after the eighth character will be ignored. When you select <b>MD5</b> in the <b>Authentication</b> field, enter a password 16-character long.
Cost	The interface cost is used for calculating the routing table. Enter a number between 0 and 65535.
Add	Click <b>Add</b> to apply the changes.
Cancel	Click <b>Cancel</b> to start configuring the above fields again.
Clear	Click <b>Clear</b> to set the above fields back to the factory defaults.
Index	This field displays the index number for an interface.
Network	This field displays the IP interface information.
Area ID	This field displays the area ID (that uses the format of an IP address in dotted decimal notation) of an area to associate the interface to that area.
Authentication	This field displays the authentication method used ( <b>Same-as-Area</b> , <b>None</b> , <b>Simple</b> or <b>MD5</b> ).
Key ID	When the <b>Authentication</b> field displays <b>MD5</b> , this field displays the identification number of the key used.
Cost	This field displays the interface cost used for calculating the routing table.
Apply	Click <b>Apply</b> to save the changes.
Cancel	Click <b>Cancel</b> to start configuring the above fields again.

## 25.6 OSPF Virtual Links

Configure and view virtual link settings in the **OSPF Virtual Link** screen.

In the **OSPF Configuration** screen, click **Virtual Link** to display the screen as shown next.



**Figure 82** OSPF Virtual Link

The following table describes the related labels in this screen.

**Table 61** OSPF Virtual Link

LABEL	DESCRIPTION
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
Area ID	Select the area ID (that uses the format of an IP address in dotted decimal notation) of an area to associate the interface to that area.
Peer Router ID	Enter the ID of a peer border router.
Authentication	<p><b>Note:</b> Virtual interface(s) must use the same authentication method within the same area.</p> <p>Select an authentication method. Choices are <b>Same-as-Area</b>, <b>None</b> (default), <b>Simple</b> and <b>MD5</b>.</p> <p>To exchange OSPF packets with peer border router, you must set the authentication method and/or password the same as the peer border router.</p> <p>Select <b>Same-as-Area</b> to use the same authentication method within the area and set the related fields when necessary.</p> <p>Select <b>None</b> to disable authentication. This is the default setting.</p> <p>Select <b>Simple</b> to authenticate OSPF packets transmitted through this interface using a simple password.</p> <p>Select <b>MD5</b> to authenticate OSPF packets transmitted through this interface using MD5 authentication.</p>
Key ID	When you select <b>MD5</b> in the <b>Authentication</b> field, specify the identification number of the authentication you want to use.
Key	<p>When you select <b>Simple</b> in the <b>Authentication</b> field, enter a password eight-character long.</p> <p>When you select <b>MD5</b> in the <b>Authentication</b> field, enter a password 16-character long.</p>
Add	Click <b>Add</b> to apply the changes.
Cancel	Click <b>Cancel</b> to start configuring the above fields again.
Clear	Click <b>Clear</b> to set the above fields back to the factory defaults.
Index	This field displays an index number of an entry.

**Table 61** OSPF Virtual Link (continued)

LABEL	DESCRIPTION
Name	This field displays a descriptive name of a virtual link.
Peer Router ID	This field displays the ID (that uses the format of an IP address in dotted decimal notation) of a peer border router.
Authentication	This field displays the authentication method used ( <b>Same-as-Area</b> , <b>None</b> , <b>Simple</b> or <b>MD5</b> ).
Key ID	When the <b>Authentication</b> field displays <b>MD5</b> , this field displays the identification number of the key used.
Delete	Click <b>Delete</b> to remove the selected entry from the summary table.
Cancel	Click <b>Cancel</b> to clear the <b>Delete</b> check boxes.



# CHAPTER 26

## IGMP

This chapter shows you how to configure IGMP.

### 26.1 Overview

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

The switch supports both IGMP version 1 (**IGMP-v1**) and version 2 (**IGMP-v2**). At start up, the switch queries all directly connected networks to gather group membership. After that, the switch periodically updates this information.

### 26.2 Configuring

Click **IP Application**, **IGMP** in the navigation panel to display the screen as shown next. Each entry in the table is automatically created when you configure a new IP domain in the **IP Setup** screen (refer to [Section 7.7 on page 79](#)).

**Figure 83** IGMP

Index	Network	Version
1	172.21.4.73/16	None
2	192.168.1.1/24	None

The following table describes the labels in this screen.

**Table 62** IGMP

LABEL	DESCRIPTION
Active	Select this check box to enable IGMP on the switch.  <b>Note:</b> You <i>cannot</i> enable both IGMP snooping and IGMP at the same time. Refer to the section on IGMP snooping.
Index	This field displays an index number of an entry.

**Table 62** IGMP (continued)

LABEL	DESCRIPTION
Network	This field displays the IP domain configured on the switch. Refer to <a href="#">Section 7.7 on page 79</a> for more information on configuring IP domains.
Version	Select an IGMP version from the drop-down list box. Choices are <b>IGMP-v1</b> , <b>IGMP-v2</b> and <b>None</b> .
Apply	Click <b>Apply</b> to save your changes back to the switch.
Cancel	Click <b>Cancel</b> to begin configuring the fields again.

# CHAPTER 27

## DVMRP

This chapter introduces DVMRP and tells you how to configure it.

### 27.1 Overview

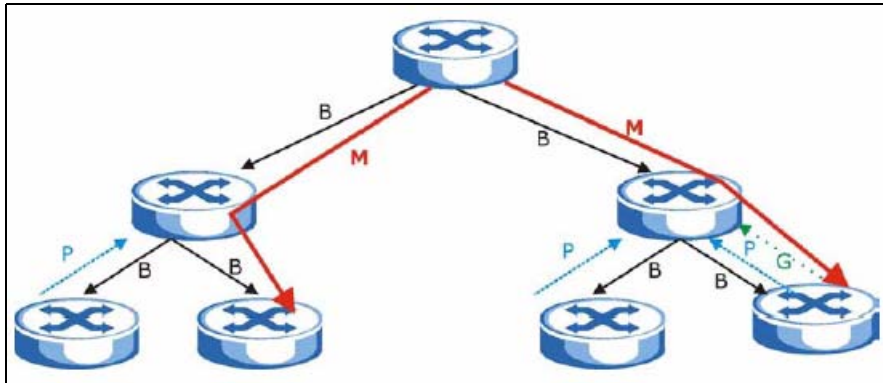
DVMRP (Distance Vector Multicast Routing Protocol) is a protocol used for routing multicast data within an autonomous system (AS). This DVMRP implementation is based on draft-ietf-idmr-dvmrp-v3-10. DVMRP provides multicast forwarding capability to a layer 3 switch that runs both the IPv4 protocol (with IP Multicast support) and the IGMP protocol. The DVMRP metric is a hop count of 32.

IGMP is a protocol used for joining or leaving a multicast group. You must have IGMP enabled when you enable DVMRP; otherwise you see the screen as in [Figure 86 on page 176](#).

### 27.2 How DVMRP Works

DVMRP uses the Reverse Path Multicasting (RPM) algorithm to generate an IP Multicast delivery tree. Multicast packets are forwarded along these multicast tree branches. DVMRP dynamically learns host membership information using Internet Group Multicast Protocol (IGMP). The trees are updated dynamically to track the membership of individual groups.

- 1 Initially an advertisement multicast packet is broadcast (“B” in the following figure).
- 2 DVMRP-enabled Layer 3 devices that do not have any hosts in their networks that belong to this multicast group send back a prune message (“P”).
- 3 If hosts later join the multicast group, a graft message (“G”) to undo the prune is sent to the parent.
- 4 The final multicast (“M”) after pruning and grafting is shown in the next figure.

**Figure 84** How DVMRP Works

## 27.2.1 DVMRP Terminology

DVMRP probes are used to discover other DVMRP Neighbors on a network.

DVMRP reports are used to exchange DVMRP source routing information. These packets are used to build the DVMRP multicast routing table that is used to build source trees and also perform Reverse Path Forwarding (RPF) checks on incoming multicast packets. RPF checks prevent duplicate packets being filtered when loops exist in the network topology.

DVMRP prunes trim the multicast delivery tree(s). DVMRP grafts attach a branch back onto the multicast delivery tree.

## 27.3 Configuring DVMRP

Configure DVMRP on the switch when you wish it to act as a multicast router (“mrouter”). Click **IP Application**, **DVMRP** in the navigation panel to display the screen as shown.

**Figure 85** DVMRP

DVMRP			
Active	<input type="checkbox"/>		
Threshold	255		
Index	Network	VID	Active
1	10.10.10.1/24	2	<input type="checkbox"/>
2	192.168.1.1/24	1	<input type="checkbox"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

The following table describes the labels in this screen.

**Table 63** DVMRP

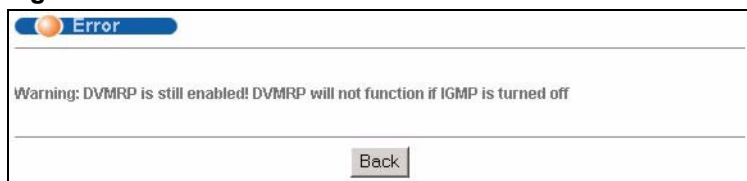
LABEL	DESCRIPTION
Active	Select <b>Active</b> to enable DVMRP on the switch. You should do this if you want the switch to act as a multicast router.
Threshold	Threshold is the maximum time to live (TTL) value. TTL is used to limit the scope of multicasting. You should reduce this value if you do not wish to flood Layer 3 devices many hops away with multicast traffic. This applies only to multicast traffic this switch sends out.
Index	Index is the DVMRP configuration for the IP routing domain defined under <b>Network</b> . The maximum number of DVMRP configurations allowed is the maximum number of IP routing domains allowed on the switch. See <a href="#">Section 7.7 on page 79</a> for more information on IP routing domains.
Network	This is the IP routing domain IP address and subnet mask you set up in <b>IP Setup</b> .
VID	DVMRP cannot be enabled on the same VLAN group across different IP routing domains, that is, you cannot have duplicate VIDs for different DVMRP configurations (see <a href="#">Figure 88 on page 177</a> ).
Active	Select <b>Active</b> to enable DVMRP on this IP routing domain.
Apply	Click <b>Apply</b> to save these changes to the switch.
Cancel	Click <b>Cancel</b> to begin configuring this part of the screen afresh.

### 27.3.1 DVMRP Configuration Error Messages

You must have IGMP/RIP enabled when you enable DVMRP; otherwise you see the screen as in the next figure.

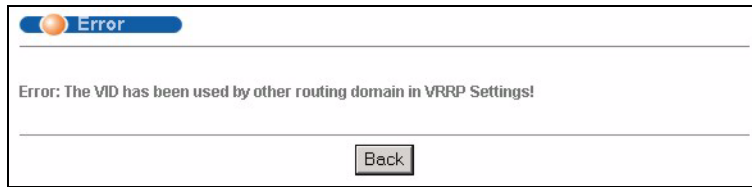
**Figure 86** DVMRP: IGMP/RIP Not Set Error

When you disable IGMP, but DVMRP is still active you also see another warning screen.

**Figure 87** DVMRP: Unable to Disable IGMP Error

Each IP routing domain DVMRP configuration must be in a different VLAN group; otherwise you see the following screen.



**Figure 88** DVMRP: Duplicate VID Error Message

## 27.4 Default DVMRP Timer Values

The following are some default DVMRP timer values. These may be changed using line commands. Please see the commands chapter later in this User's Guide.

**Table 64** DVMRP: Default Timer Values

DVMRP FIELD	DEFAULT VALUE
Probe interval	10 sec
Report interval	35 sec
Route expiration time	140 sec
Prune lifetime	Variable (less than two hours)
Prune retransmission time	3 sec with exponential back off
Graft retransmission time	5 sec with exponential back off

# CHAPTER 28

## IP Multicast

This chapter shows you how to configure the **IP Multicast** screen.

### 28.1 Overview

Traditionally, IP packets are transmitted in one of either two ways - Unicast (one sender to one recipient) or Broadcast (one sender to everybody on the network). IP Multicast is a third way to deliver IP packets to a group of hosts on the network - not everybody.

You can configure the switch to untag (remove the VLAN tags from) IP multicast packets that the switch forwards. This allows the switch to send packets to Ethernet devices that are not VLAN-aware.

### 28.2 Configuring

Click **IP Application** and **IP Multicast** in the navigation panel to display the screen as shown next.

**Figure 89** IP Multicast

Port	IP Multicast Egress Untag Vlan ID
1	<input type="text" value="0"/>
2	<input type="text" value="0"/>
3	<input type="text" value="0"/>
4	<input type="text" value="0"/>
5	<input type="text" value="0"/>
6	<input type="text" value="0"/>
7	<input type="text" value="0"/>
8	<input type="text" value="0"/>
9	<input type="text" value="0"/>
10	<input type="text" value="0"/>
11	<input type="text" value="0"/>
12	<input type="text" value="0"/>

The following table describes the labels in this screen.

**Table 65** IP Multicast

LABEL	DESCRIPTION
Port	This read-only field displays the port number.
IP Multicast Egress Untag Vlan ID	The switch removes the VLAN tag from IP multicast packets belonging to the specified VLAN before transmission on this port. Enter a VLAN group ID in this field. Enter <b>0</b> to set the switch not to remove any VLAN tags from the packets.
Apply	Click <b>Apply</b> to save the settings.
Cancel	Click <b>Cancel</b> to reset the fields to your previous configuration.

# CHAPTER 29

## Differentiated Services

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

### 29.1 Overview

Quality of Service (QoS) is used to prioritize source-to-destination traffic flows. All packets in the flow are given the same priority. You can use CoS (class of service) to give different priorities to different packet types.

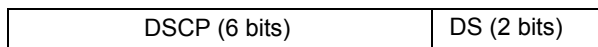
DiffServ is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired.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

#### 29.1.1 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.

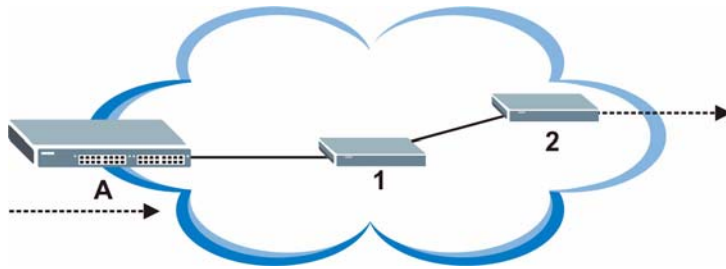
**Figure 90** DiffServ: Differentiated Service Field



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.

#### 29.1.2 DiffServ Network Example

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

**Figure 91** 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.

## 29.2 Activating DiffServ

Activate DiffServ to allow the switch to enable DiffServ and apply marking rules and IEEE802.1p priority mapping on the selected port(s).

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

**Figure 92** DiffServ

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

The following table describes the labels in this screen.

**Table 66** DiffServ

LABEL	DESCRIPTION
Active	Select this option to enable DiffServ on the switch.
Port	This field displays the index number of a port on the switch.
Active	Select this option to enable DiffServ on the port.

**Table 66** DiffServ (continued)

LABEL	DESCRIPTION
Apply	Click <b>Apply</b> to save the changes.
Cancel	Click <b>Cancel</b> to start configuring this screen again.

## 29.3 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 67** 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

### 29.3.1 Configuring DSCP Settings

To change the DSCP-IEEE 802.1p mapping click the **DSCP Setting** link in the **DiffServ** screen to display the screen as shown next.

**Figure 93** DiffServ: DSCP Setting

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

The following table describes the labels in this screen.

**Table 68** DiffServ: DSCP Setting

LABEL	DESCRIPTION
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 <b>Apply</b> to save the changes.
Cancel	Click <b>Cancel</b> to discard all changes and start configuring the screen again.

# CHAPTER 30

## DHCP

This chapter shows you how to configure the DHCP feature.

### 30.1 Overview

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 server or disable it. When configured as a server, the switch provides the TCP/IP configuration for the clients. If you disable the DHCP service, you must have another DHCP server on your LAN, or else the computer must be manually configured.

#### 30.1.1 DHCP modes

The switch can be configured as a DHCP server or DHCP relay agent.

- If you configure the switch as a DHCP server, it will maintain the pool of addresses and distribute them to your LAN computers.
- If there is an Ethernet device that performs the DHCP server function for your network, then you can configure the switch as a DHCP relay agent. When the switch receives a request from a computer on your network, it contacts the Ethernet device (the DHCP server) for the necessary IP information, and then relays the assigned information back to the computer.

### 30.2 DHCP Server Status

Click **IP Application**, **DHCP** in the navigation panel. The **DHCP Server Status** screen displays.



**Figure 94** DHCP: DHCP Server Status

Index	VID	Server Status	IP Pool Size
1	2	10.10.10.100	100

Polling Interval(s)

The following table describes the labels in this screen.

**Table 69** DHCP: DHCP Server Status

LABEL	DESCRIPTION
Index	This is the index number.
VID	This field displays the ID number of the VLAN group to which this DHCP settings apply.
Server Status	This field displays the starting DHCP client IP address.
Client Pool Size	This field displays the size of the DHCP client IP address pool.
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 <b>Set Interval</b> .
Stop	Click <b>Stop</b> to end status polling.

### 30.3 Configuring DHCP Server

Click **IP Application**, **DHCP** in the navigation panel. Click the **Server** link In the **DHCP Server Status** screen that displays.

**Figure 95** DHCP: Server

VID	Type	DHCP Status	Delete
2	Server	10.10.10.100/100	<input type="checkbox"/>

The following table describes the labels in this screen.

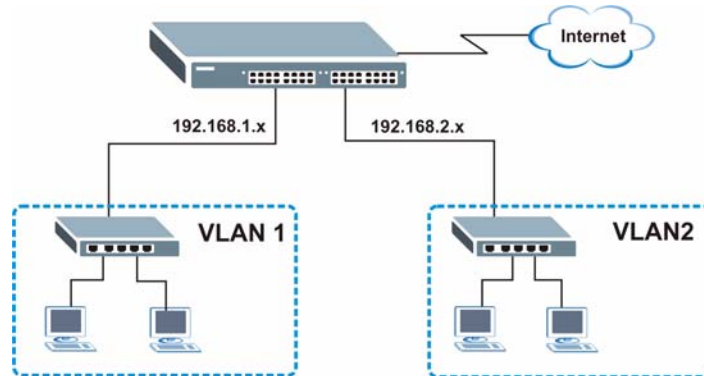
**Table 70** DHCP: Server

LABEL	DESCRIPTION
VID	Enter the ID number of the VLAN group to which this DHCP settings apply.
Client IP Pool Starting Address	Specify the first of the contiguous addresses in the IP address pool.
Size of Client IP Pool	Specify the size, or count of the IP address pool.
IP Subnet Mask	Enter the subnet mask of the DHCP server.
Default Gateway	Enter the IP address of the default gateway device.
Primary/Secondary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.
Add	Click <b>Add</b> to insert the settings as a new entry in the summary table.
Cancel	Click <b>Cancel</b> to reset the fields to your previous configurations.
Clear	Click <b>Clear</b> to reset the fields back to the factory defaults.
VID	This field displays the ID number of the VLAN group to which this DHCP settings apply.
Type	This field displays <b>Server</b> for the DHCP mode.
DHCP Status	This field displays the starting and the size of DHCP client IP address.
Delete	Click <b>Delete</b> to remove the selected entry.
Cancel	Click <b>Cancel</b> to clear the <b>Delete</b> check boxes.

### 30.3.1 DHCP Server Configuration Example

The follow figure shows a network example where the switch is used to assign network information to the DHCP clients in the **RD** and **Sales** network.

**Figure 96** DHCP Server Network Example



In the **DHCP Server** screen, configure two DHCP client IP address pools for the two networks. The following shows an example.

**Figure 97** DHCP Server Configuration Example

**DHCP Server**
Status

VID	2
Client IP Pool Starting Address	192.168.2.100
Size of Client IP Pool	100
IP Subnet Mask	255.255.255.0
Default Gateway	192.168.2.1
Primary DNS Server	192.168.2.120
Secondary DNS Server	0.0.0.0

Add Cancel Clear

VID	Type	DHCP Status	Delete
1	Server	192.168.1.100/100	<input type="checkbox"/>

Delete Cancel

## 30.4 DHCP Relay

Configure DHCP relay on the switch if the DHCP clients and the DHCP server are not in the same subnet. During the initial IP address leasing, the switch helps to relay network information (such as the IP address and subnet mask) between a DHCP client and a DHCP server. Once the DHCP client obtains an IP address and can connect to the network, network information renewal is done between the DHCP client and the DHCP server without the help of the switch.

### 30.4.1 DHCP Relay Agent Information

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

The DHCP relay agent information feature adds an Agent Information field to the option 82 field of the DHCP headers of client DHCP request frames that the switch relays to a DHCP server. The following lists the DHCP relay agent option 82 information that the switch sends to the DHCP server:

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

### 30.4.2 Configuring DHCP Relay

Configure DHCP relay in the **DHCP Relay** screen. Click **IP Application**, **DHCP** in the navigation panel and click the **Relay** link to display the screen as shown.

**Figure 98** DHCP: Relay

The following table describes the labels in this screen.

**Table 71** DHCP: Relay

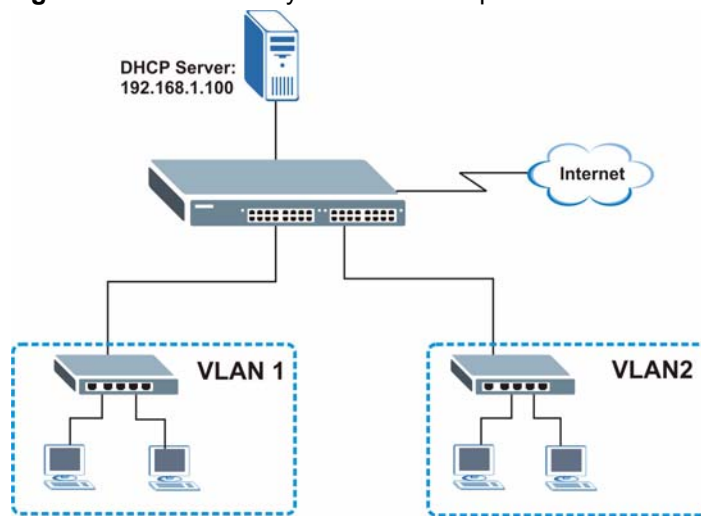
LABEL	DESCRIPTION
Active	Select this check box to enable DHCP relay.
Remote DHCP Server 1 .. 3	Enter the IP address of a DHCP server in dotted decimal notation.
Relay Agent Information	Select the <b>Option 82</b> check box to have the switch add information (slot number, port number and VLAN ID) to client DHCP requests that it relays to a DHCP server.
Information	This read-only field displays the system name you configure in the <b>General Setup</b> screen. Select the check box for the switch to add the system name to the client DHCP requests that it relays to a DHCP server.

**Table 71** DHCP: Relay (continued)

LABEL	DESCRIPTION
Apply	Click <b>Apply</b> to save the changes.
Cancel	Click <b>Cancel</b> to discard all changes and start configuring the screen again.

### 30.4.3 DHCP Relay Configuration Example

The follow figure shows a network example where the switch is used to relay DHCP requests for the **RD** and **Sales** network. There is only one DHCP server that services the DHCP clients in both networks.

**Figure 99** DHCP Relay Network Example

Configure the **DHCP Relay** screen as shown. Make sure you select the **Option 82** check box to set the switch to send additional information (such as the VLAN ID) together with the DHCP requests to the DHCP server. This allows the DHCP server to assign the appropriate IP address according to the VLAN ID.

**Figure 100** DHCP Relay Configuration Example

The screenshot shows the DHCP Relay configuration interface. The 'Active' checkbox is checked. The 'Remote DHCP Server 1' field is set to 192.168.1.100. The 'Remote DHCP Server 2' and 'Remote DHCP Server 3' fields are set to 0.0.0.0. The 'Relay Agent Information' section has the 'Option 82' checkbox checked and the 'Information' field set to GS-4012F. The 'Apply' and 'Cancel' buttons are visible at the bottom.

Field	Value
Active	<input checked="" type="checkbox"/>
Remote DHCP Server 1	192.168.1.100
Remote DHCP Server 2	0.0.0.0
Remote DHCP Server 3	0.0.0.0
Relay Agent Information	<input checked="" type="checkbox"/> Option 82
Information	<input type="checkbox"/> GS-4012F

# CHAPTER 31

## VRRP

This chapter shows you how to configure and monitor the Virtual Router Redundancy Protocol (VRRP) on the switch.

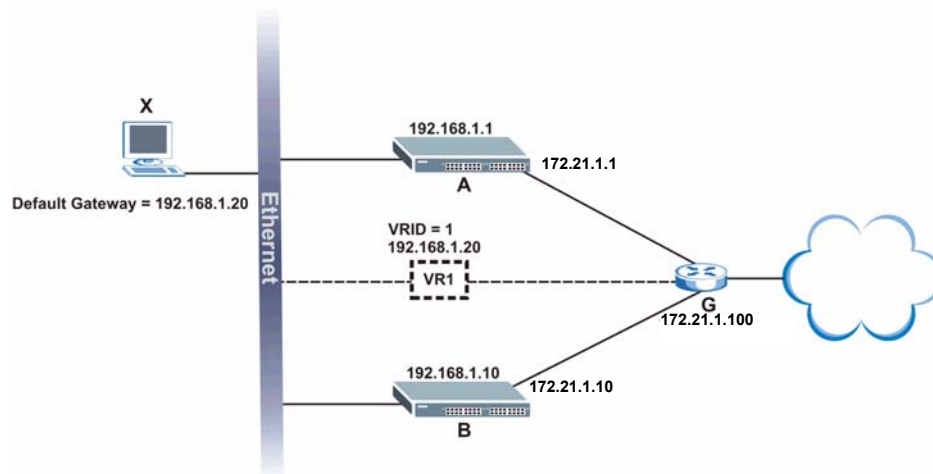
### 31.1 Overview

Each host on a network is configured to send packets to a statically configured default gateway (this switch). The default gateway can become a single point of failure. Virtual Router Redundancy Protocol (VRRP), defined in RFC 2338, allows you to create redundant backup gateways to ensure that the default gateway of a host is always available.

In VRRP, a virtual router (VR) represents a number of physical layer-3 devices. An IP address is associated with the virtual router. A layer-3 device having the same IP address is the preferred master router while the other Layer-3 devices are the backup routers. The master router forwards traffic for the virtual router. When the master router becomes unavailable, a backup router assumes the role of the master router until the master router comes back up and takes over.

The following figure shows a VRRP network example with the switches (**A** and **B**) implementing one virtual router **VR1** to ensure the link between the host **X** and the uplink gateway **G**. Host **X** is configured to use **VR1** (192.168.1.20) as the default gateway. If switch **A** has a higher priority, it is the master router. Switch **B**, having a lower priority, is the backup router.

**Figure 101** VRRP: Example 1



If switch **A** (the master router) is unavailable, switch **B** takes over. Traffic is then processed by switch **B**.

## 31.2 Viewing VRRP Status

Click **IP Application**, **VRRP** in the navigation panel to display the **VRRP Status** screen as shown next.

**Figure 102** VRRP Status

Index	Active	Network	VRID	VR Status	Uplink Status
1	Yes	192.168.1.1/24	1	Master	Alive

Poll Interval(s)

The following table describes the labels in this screen.

**Table 72** VRRP Status

LABEL	DESCRIPTION
Index	This field displays the index number of a rule.
Active	This field displays whether a rule is enabled ( <b>Yes</b> ) or disabled ( <b>No</b> ).
Network	This field displays the IP address and the subnet mask bits of an IP routing domain that is associated to a virtual router.
VRID	This field displays the ID number of the virtual router.
VR Status	This field displays the status of the virtual router. This field is <b>Master</b> indicating that this switch functions as the master router. This field is <b>Backup</b> indicating that this switch functions as a backup router. This field displays <b>Init</b> when this switch is initiating the VRRP protocol or when the <b>Uplink Status</b> field displays <b>Dead</b> .
Uplink Status	This field displays the status of the link between this switch and the uplink gateway. This field is <b>Alive</b> indicating that the link between this switch and the uplink gateway is up. Otherwise, this field is <b>Dead</b> . This field displays <b>Probe</b> when this switch is check for the link state.
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 <b>Set Interval</b> .
Stop	Click <b>Stop</b> to halt system statistic polling.

## 31.3 Configuring VRRP

Follow the instructions in the follow sections to configure VRRP on the switch.

### 31.3.1 IP Interface Setup

Before configuring VRRP, first create an IP interface (or routing domain) in the **IP Setup** screen (see the [Section 7.7 on page 79](#) for more information).

Click **IP Application**, **VRRP** and click the **Configuration** link to display the **VRRP Configuration** screen as shown next.

**Note:** You can only configure VRRP on interfaces with unique VLAN IDs.

Routing domains with the same VLAN ID are not displayed in the table indicated.

**Figure 103** VRRP Configuration: IP Interface

Index	Network	Authentication	Key
1	192.168.1.10/24	None	

Apply Cancel

Active

Name

Network

Virtual Router ID

Advertisement Interval

Preempt Mode

Priority

Uplink Gateway

Primary Virtual IP

Secondary Virtual IP

Add Cancel Clear

Index	Active	Name	Network	VRID	Primary VIP	Uplink Gateway	Priority	Delete
1	Yes	Example	192.168.1.10/24	1	192.168.1.1	192.168.1.100	110	<input type="checkbox"/>

Delete Cancel

The following table describes the labels in this screen.



**Table 73** VRRP Configuration: IP Interface

LABEL	DESCRIPTION
Index	This field displays the index number of an entry.
Network	This field displays the IP address and number of subnet mask bit of an IP domain.
Authentication	Select <b>None</b> to disable authentication. This is the default setting. Select <b>Simple</b> to use a simple password to authenticate VRRP packet exchanges on this interface.
Key	When you select <b>Simple</b> in the <b>Authentication</b> field, enter a password key (up to eight printable ASCII character long) in this field.
Apply	Click <b>Apply</b> to save the changes.
Cancel	Click <b>Cancel</b> to discard all changes made in this table.

## 31.3.2 VRRP Parameters

This section describes the VRRP parameters.

### 31.3.2.1 Advertisement Interval

The master router sends out Hello messages to let the other backup routers know that it is still up and running. The time interval between sending the Hello messages is the advertisement interval. By default, a Hello message is sent out every second.

If the backup routers do not receive a Hello message from the master router after this interval expires, it is assumed that the master router is down. Then the backup router with the highest priority becomes the master router.

**Note:** All routers participating in the virtual router must use the same advertisement interval.

### 31.3.2.2 Priority

Configure the priority level (1 to 254) to set which backup router to take over in case the master router goes down. The backup router with the highest priority will take over. The priority of the VRRP router that owns the IP address(es) associated with the virtual router is 255.

### 31.3.2.3 Preempt Mode

If the master router is unavailable, a backup router assumes the role of the master router. However, when another backup router with a higher priority joins the network, it will preempt the lower priority backup router that is the master. Disable preempt mode to prevent this from happening.

By default, a layer 3 device with the same IP address as the virtual router will become the master router regardless of the preempt mode.

### 31.3.3 Configuring VRRP Parameters

After you set up an IP interface, configure the VRRP parameters in the **VRRP Configuration** screen.

**Figure 104** VRRP Configuration: VRRP Parameters

The screenshot shows a configuration form for VRRP parameters. The fields and their values are as follows:

Active	<input type="checkbox"/>
Name	name
Network	192.168.1.10/24
Virtual Router ID	1
Advertisement Interval	1
Preempt Mode	<input checked="" type="checkbox"/>
Priority	100
Uplink Gateway	0.0.0.0
Primary Virtual IP	0.0.0.0
Secondary Virtual IP	0.0.0.0

At the bottom of the form are three buttons: **Add**, **Cancel**, and **Clear**.

The following table describes the labels in this screen.

**Table 74** VRRP Configuration: VRRP Parameters

LABEL	DESCRIPTION
Active	Select this option to enable this VRRP entry.
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
Network	Select an IP domain to which this VRRP entry applies.
Virtual Router ID	Select a virtual router number (1 to 7) for which this VRRP entry is created. You can configure up to seven virtual routers for one network.
Advertisement Interval	Specify the number of seconds between Hello message transmissions. The default is 1.
Preempt Mode	Select this option to activate preempt mode.
Priority	Enter a number (between 1 and 254) to set the priority level. The bigger the number, the higher the priority. This field is <b>100</b> by default.
Uplink Gateway	Enter the IP address of the uplink gateway in dotted decimal notation. The switch checks the link to the uplink gateway.
Primary Virtual IP	Enter the IP address of the primary virtual router in dotted decimal notation.
Secondary Virtual IP	This field is optional. Enter the IP address of a secondary virtual router in dotted decimal notation. This field is ignored when you enter <b>0.0.0.0</b> .
Add	Click <b>Add</b> to apply the changes.
Cancel	Click <b>Cancel</b> to discard all changes made in this table.
Clear	Click <b>Clear</b> to set the above fields back to the factory defaults.

## 31.4 VRRP Configuration Summary

To view a summary of all VRRP configurations on the switch, scroll down to the bottom of the **VRRP Configuration** screen.

**Figure 105** VRRP Configuration: Summary

Index	Active	Name	Network	VRID	Primary VIP	Uplink Gateway	Priority	Delete
1	Yes	Example	192.168.1.10/24	1	192.168.1.1	192.168.1.100	110	<input type="checkbox"/>

The following table describes the labels in this screen.

**Table 75** VRRP Configuring: VRRP Parameters

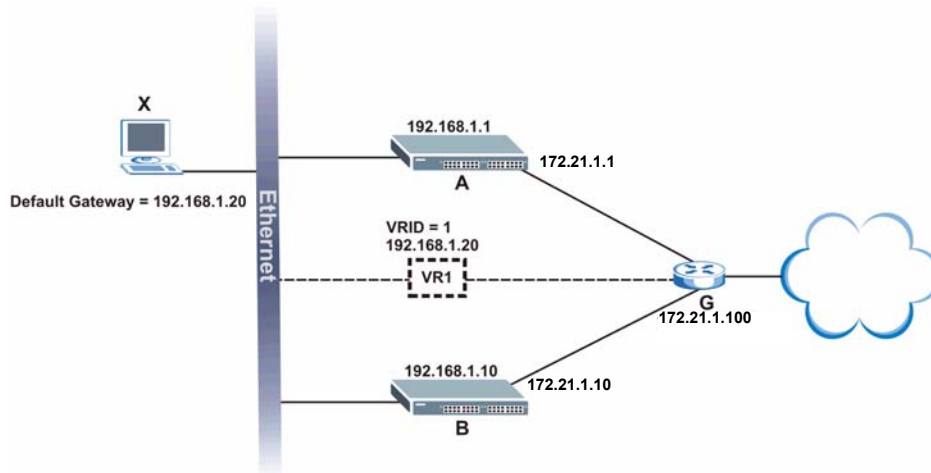
LABEL	DESCRIPTION
Index	This field displays the index number of an entry.
Active	This field shows whether a VRRP entry is enabled ( <b>Yes</b> ) or disabled ( <b>No</b> ).
Name	This field displays a descriptive name of an entry.
Network	This field displays the IP address and subnet mask of an interface.
VRID	This field displays the ID number of a virtual router.
Primary VIP	This field displays the IP address of the primary virtual router.
Uplink Gateway	This field displays the IP address of the uplink gateway.
Priority	This field displays the priority level (1 to 255) of the entry.
Delete	Click <b>Delete</b> to remove the selected entry from the summary table.
Cancel	Click <b>Cancel</b> to clear the <b>Delete</b> check boxes.

## 31.5 VRRP Configuration Examples

The following sections show two VRRP configuration examples on the switch.

### 31.5.1 One Subnet Network Example

The figure below shows a simple VRRP network with only one virtual router **VR1** (VRID =1) and two switches. The network is connected to the WAN via an uplink gateway **G** (172.21.1.100). The host computer **X** is set to use **VR1** as the default gateway.

**Figure 106** VRRP Configuration Example: One Virtual Router Network

You want to set switch **A** as the master router. Configure the VRRP parameters in the **VRRP Configuration** screens on the switches as shown in the figures below.

**Figure 107** VRRP Example 1: VRRP Parameter Settings on Switch A

Active	<input checked="" type="checkbox"/>
Name	Example1
Network	192.168.1.1/24
Virtual Router ID	1
Advertisement Interval	1
Preempt Mode	<input checked="" type="checkbox"/>
Priority	110
Uplink Gateway	172.21.1.100
Primary Virtual IP	192.168.1.20
Secondary Virtual IP	0.0.0.0

**Figure 108** VRRP Example 1: VRRP Parameter Settings on Switch B

Active	<input checked="" type="checkbox"/>
Name	Example1
Network	192.168.10.1/24
Virtual Router ID	1
Advertisement Interval	1
Preempt Mode	<input checked="" type="checkbox"/>
Priority	100
Uplink Gateway	172.21.1.100
Primary Virtual IP	192.168.1.20
Secondary Virtual IP	0.0.0.0

After configuring and saving the VRRP configuration, the **VRRP Status** screens for both switches are shown next.

**Figure 109** VRRP Example 1: VRRP Status on Switch A

VRRP Status						<a href="#">Configuration</a>
Index	Active	Network	VRID	VR Status	Uplink Status	
1	Yes	192.168.1.1/24	1	Master	Alive	

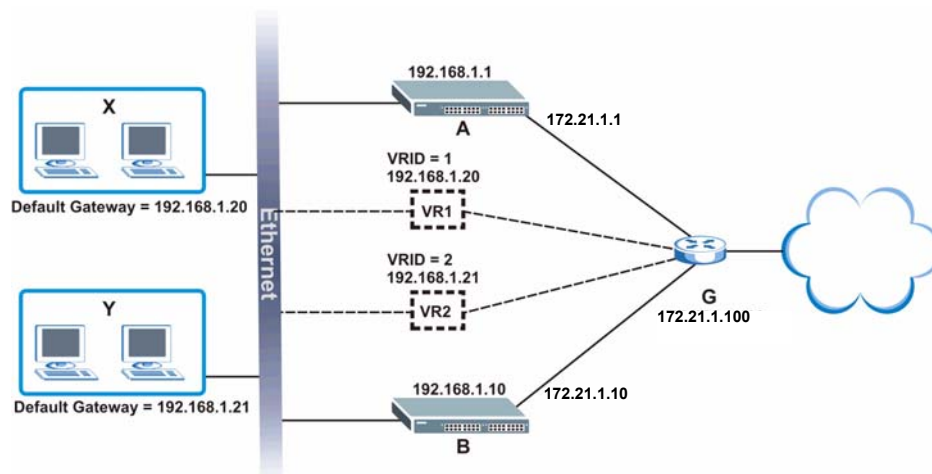
**Figure 110** VRRP Example 1: VRRP Status on Switch B

VRRP Status						<a href="#">Configuration</a>
Index	Active	Network	VRID	VR Status	Uplink Status	
1	Yes	192.168.1.10/24	1	Backup	Alive	

### 31.5.2 Two Subnets Example

The following figure depicts an example in which two switches share the network traffic. Hosts in the two network groups use different default gateways. Each switch is configured to backup a virtual router using VRRP.

You wish to configure switch **A** as the master router for virtual router **VR1** and as a backup for virtual router **VR2**. On the other hand, switch **B** is the master for **VR2** and a backup for **VR1**.

**Figure 111** VRRP Configuration Example: Two Virtual Router Network

Keeping the VRRP configuration in example 1 for virtual router **VR1** (refer to [Section 31.5.2 on page 197](#)), you need to configure the **VRRP Configuration** screen for virtual router **VR2** on each switch. Configure the VRRP parameters on the switches as shown in the figures below.

**Figure 112** VRRP Example 2: VRRP Parameter Settings for VR2 on Switch A

Active	<input checked="" type="checkbox"/>
Name	Example2
Network	192.168.1.1/24
Virtual Router ID	1
Advertisement Interval	1
Preempt Mode	<input checked="" type="checkbox"/>
Priority	100
Uplink Gateway	172.21.1.100
Primary Virtual IP	192.168.1.21
Secondary Virtual IP	0.0.0.0

**Figure 113** VRRP Example 2: VRRP Parameter Settings for VR2 on Switch B

Active	<input checked="" type="checkbox"/>
Name	Example2
Network	192.168.10.1/24
Virtual Router ID	1
Advertisement Interval	1
Preempt Mode	<input checked="" type="checkbox"/>
Priority	110
Uplink Gateway	172.21.1.100
Primary Virtual IP	192.168.1.21
Secondary Virtual IP	0.0.0.0

After configuring and saving the VRRP configuration, the **VRRP Status** screens for both switches are shown next.

**Figure 114** VRRP Example 2: VRRP Status on Switch A

VRRP Status						Configuration
Index	Active	Network	VRID	VR Status	Uplink Status	
1	Yes	192.168.1.1/24	2	Backup	Alive	
2	Yes	192.168.1.1/24	1	Master	Alive	

**Figure 115** VRRP Example 2: VRRP Status on Switch B

VRRP Status						Configuration
Index	Active	Network	VRID	VR Status	Uplink Status	
1	Yes	192.168.10.1/24	2	Master	Alive	
2	Yes	192.168.10.1/24	1	Backup	Alive	



# CHAPTER 32

## Maintenance

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

### 32.1 The Maintenance Screen

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

**Figure 116** Maintenance



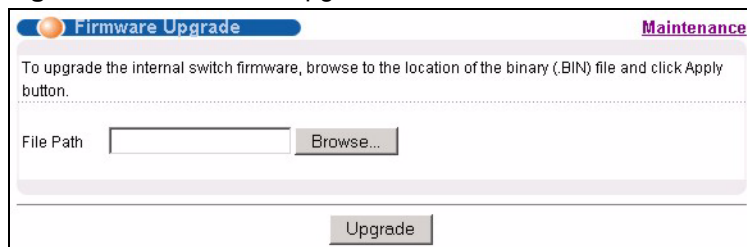
### 32.2 Firmware Upgrade

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 117** 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**.

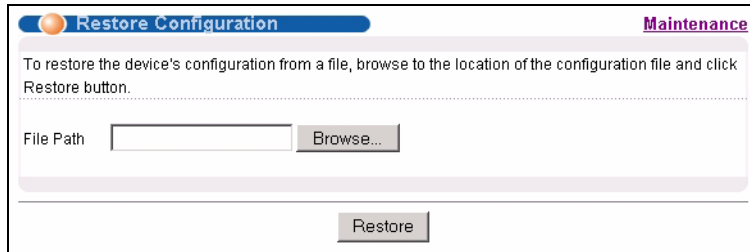


After the firmware upgrade process is complete, see the **System Info** screen to verify your current firmware version number.

## 32.3 Restore a Configuration File

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

**Figure 118** Restore Configuration



The screenshot shows a web interface for restoring a configuration file. At the top, there is a blue header with 'Restore Configuration' and a purple 'Maintenance' link. Below the header, a light gray box contains 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 instruction is a 'File Path' text input field and a 'Browse...' button. At the bottom of the interface is a 'Restore' button.

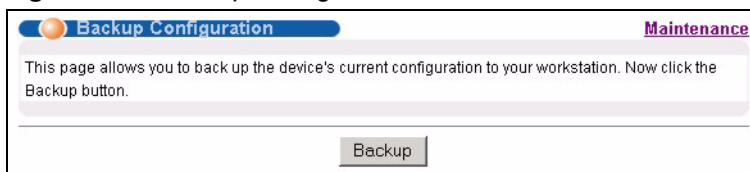
Type the path and file name of the configuration file you wish to restore in the **File Path** text box or click **Browse** to display the **Choose File** screen (below) from which you can locate it. After you have specified the file, click **Restore**. "config" is the name of the configuration file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

## 32.4 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 119** Backup Configuration



The screenshot shows a web interface for backing up the configuration. At the top, there is a blue header with 'Backup Configuration' and a purple 'Maintenance' link. Below the header, a light gray box contains 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 of the interface 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.

## 32.5 Load Factory Defaults

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

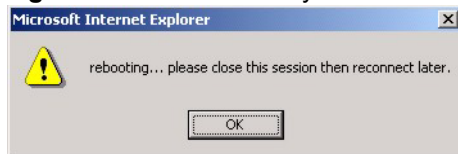
- 1 In the **Maintenance** screen, click the **Click Here** button next to **Load Factory Defaults** to clear all switch configuration information you configured and return to the factory defaults. The following message appears.

**Figure 120** Load Factory Default: Conformation



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

**Figure 121** Load Factory Default: Start



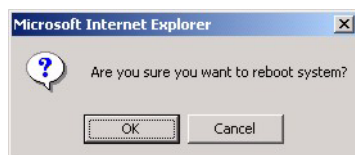
- 3 Click **OK** to begin resetting all switch configurations to the factory defaults and then wait for the switch to restart. This takes up to two minutes. If you want to access the switch web configurator again, you may need to change the IP address of your computer to be in the same subnet as that of the default switch IP address (192.168.1.1).

## 32.6 Reboot System

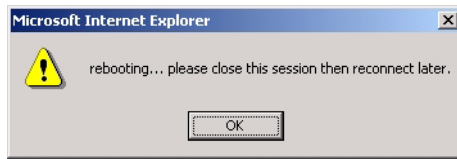
**Reboot System** allows you to restart the switch without physically turning the power off. Follow the steps below to reboot the switch.

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

**Figure 122** Reboot System: Confirmation



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

**Figure 123** 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.

## 32.7 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.

### 32.7.1 Filename Conventions

The configuration file 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 76** 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.

#### 32.7.1.1 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.

### 32.7.2 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 76 on page 203](#) for more information on filename conventions.
- 7 Enter `quit` to exit the ftp prompt.

### 32.7.3 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).

## 32.7.4 FTP Restrictions

FTP will not work when:

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

# CHAPTER 33

## Access Control

This chapter describes how to control access to the switch.

### 33.1 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 124** Console Port Priority

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

- A console port, SSH 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 77** 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

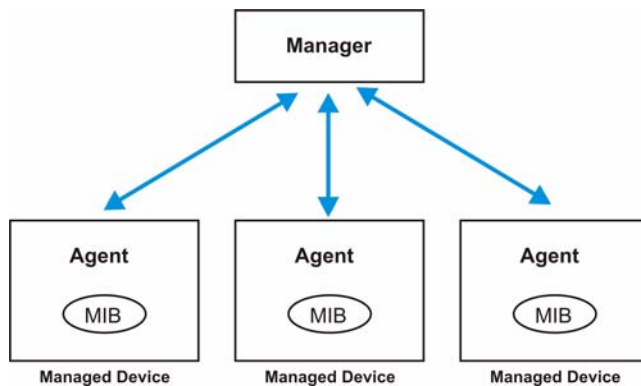
### 33.2 The Access Control Main Screen

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

**Figure 125** Access Control

### 33.3 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 126** 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 (this switch). 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 78** 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.

### 33.3.1 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
- RFC 1253 OSPF MIBs
- 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

### 33.3.2 SNMP Traps

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

**Table 79** SNMP Traps

OBJECT LABEL	OBJECT ID	DESCRIPTION
SNMPv2 Traps		
Cold Start	1.3.6.1.6.3.1.1.5.1	This trap is sent when the switch is turned on.
WarmStart	1.3.6.1.6.3.1.1.5.2	This trap is sent when the switch restarts.
linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.
linkUp	1.3.6.1.6.3.1.1.5.4	This trap is sent when the Ethernet link is up.



**Table 79** SNMP Traps (continued)

OBJECT LABEL	OBJECT ID	DESCRIPTION
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.

### 33.3.3 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 127** Access Control: SNMP

The following table describes the labels in this screen.

**Table 80** 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 <b>Apply</b> to save your changes back to the switch.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

### 33.3.4 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 128** Access Control: Logins

The screenshot shows the 'Logins' configuration page. At the top, there's a 'Logins' header and a 'Administrator' sub-header. Below this are three input fields for 'Old Password', 'New Password', and 'Retype to confirm'. A red warning message is displayed: '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 a section titled 'Edit Logins' which contains a table with four rows and four columns: 'Login', 'User Name', 'Password', and 'Retype to confirm'. At the bottom of the page are 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen.

**Table 81** 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 ( <b>1234</b> is the default password when shipped).
New Password	Enter your new system password.
Retype to confirm	Retype your new system password for confirmation
Edit Logins	You may configure passwords for up to four users. These 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 <b>Apply</b> to save your changes back to the switch.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 33.4 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.

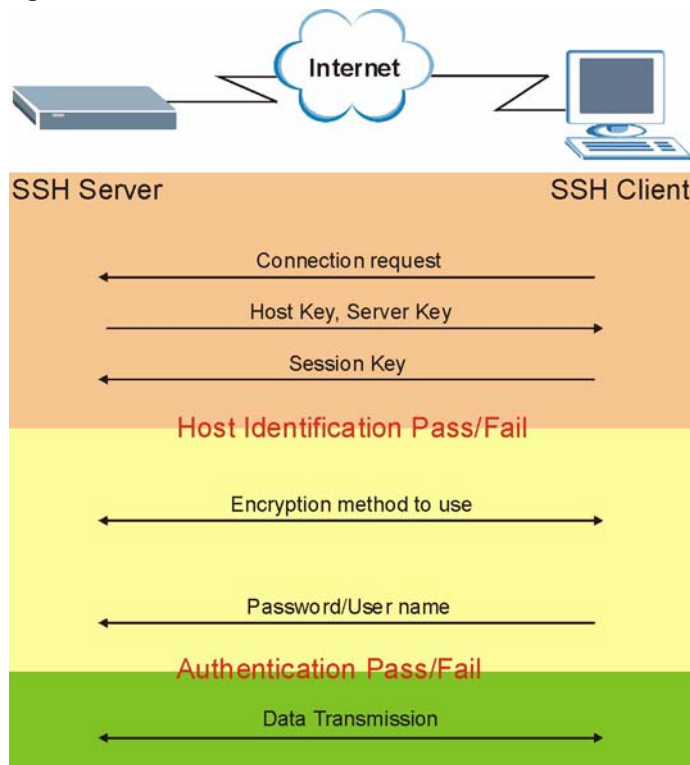
**Figure 129** SSH Communication Example



## 33.5 How SSH works

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

**Figure 130** 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.

## **33.6 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.

### **33.6.1 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.

## **33.7 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.

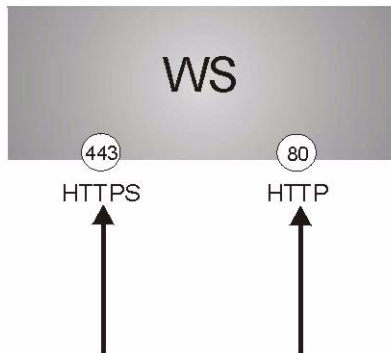
HTTPS on the switch is used so that you may securely access the switch using the web configurator. The SSL protocol specifies that the SSL server (the switch) must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the switch), whereas the SSL client only 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 131** HTTPS Implementation



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

## 33.8 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.

### 33.8.1 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.

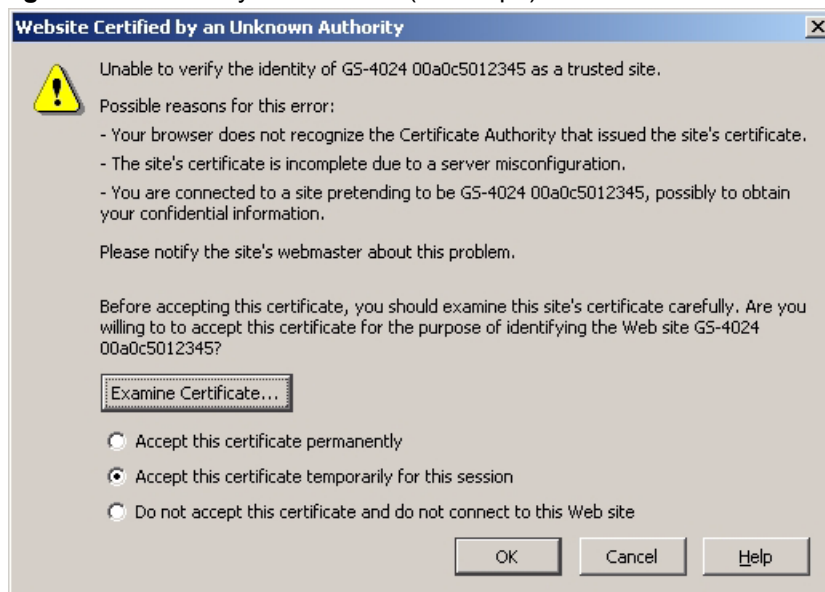
**Figure 132** Security Alert Dialog Box (Internet Explorer)

### 33.8.2 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 133** Security Certificate 1 (Netscape)

**Figure 134** Security Certificate 2 (Netscape)

### 33.8.3 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 135 Login Screen (Internet Explorer)

Web Configurator - Microsoft Internet Explorer

Address: https://192.168.1.1

**ZyXEL** Status Logout Help

MENU  
Basic Setting  
Advanced Application  
IP Application  
Management

**Status**  
System Up Time : 2:59:52

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	100MF Copper	FORWARDING	Disabled	1673	1509	0	0.0	0.0	2:59:41
10	100MF Copper	FORWARDING	Disabled	2394	2346	0	17.837	3.822	2:59:41
11	100MF Copper	FORWARDING	Disabled	41246	3802	0	0.128	0.0	2:59:41
12	100MF Copper	FORWARDING	Disabled	4322	41406	0	0.0	0.128	2:59:41

Poll Interval(s) 40 Set Interval Stop

Port ALL Clear Counter

© Copyright 1995-2005 by ZyXEL Communications Corp.

Figure 136 Login Screen (Netscape)

Web Configurator - Netscape

Address: https://192.168.1.1

**ZyXEL** Status Logout Help

MENU  
Basic Setting  
Advanced Application  
IP Application  
Management

**Status**  
System Up Time : 3:01:53

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	100MF Copper	FORWARDING	Disabled	1673	1509	0	0.0	0.0	3:01:42
10	100MF Copper	FORWARDING	Disabled	2565	2466	0	32.545	8.95	3:01:42
11	100MF Copper	FORWARDING	Disabled	41457	3843	0	0.0	0.0	3:01:42
12	100MF Copper	FORWARDING	Disabled	4373	41647	0	0.0	0.0	3:01:42

Poll Interval(s) 40 Set Interval Stop

Port ALL Clear Counter

© Copyright 1995-2005 by ZyXEL Communications Corp.



## 33.9 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 137** 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"/>		

Apply Cancel

The following table describes the fields in this screen.

**Table 82** 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 <b>Server Port</b> 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 (between 1 and 255) 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 <b>Apply</b> to save your changes back to the switch.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 33.10 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 138** Access Control: Remote Management

Entry	Active	Start Address	End Address	Telnet	FTP	Web	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 83** 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/ Web/ICMP/ SNMP	Select services that may be used for managing the switch from the specified trusted computers.
Apply	Click <b>Apply</b> to save your changes back to the switch.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.



# CHAPTER 34

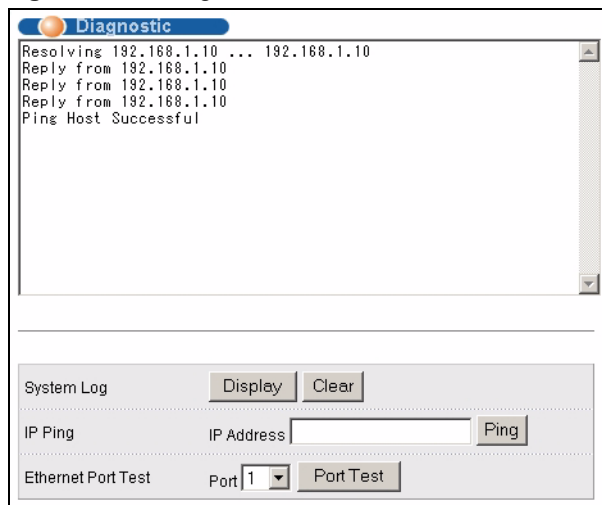
## Diagnostic

This chapter explains the **Diagnostic** screen.

### 34.1 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 139** Diagnostic



The following table describes the labels in this screen.

**Table 84** Diagnostic

LABEL	DESCRIPTION
System Log	Click <b>Display</b> to display a log of events in the multi-line text box. Click <b>Clear</b> 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 <b>Ping</b> to have the switch ping the IP address (in the field to the left).
Ethernet Port Test	From the <b>Port</b> drop-down list box, select a port number and click <b>Port Test</b> to perform internal loopback test.



# CHAPTER 35

## Cluster Management

This chapter introduces cluster management.

### 35.1 Overview

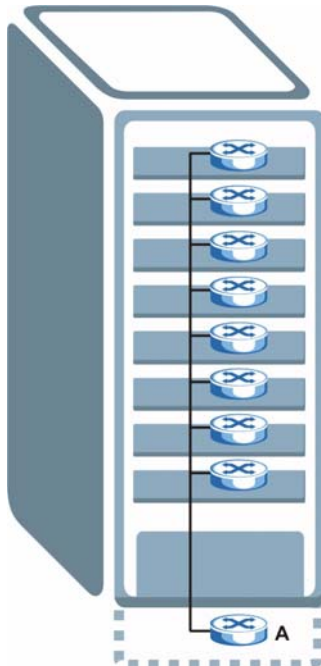
Cluster Management allows you to manage switches through one switch, called the cluster manager. The switches must be directly connected and be in the same VLAN group so as to be able to communicate with one another.

**Table 85** 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 140** Clustering Application Example



## 35.2 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 141** Cluster Management: Status

Index	MacAddr	Name	Model	Status
1	00:a0:c5:01:23:45	ES-4024A	ES-4024A	Online
2	00:a0:c5:5f:a2:b9	ES-3024	ES-3024	Online

The following table describes the labels in this screen.

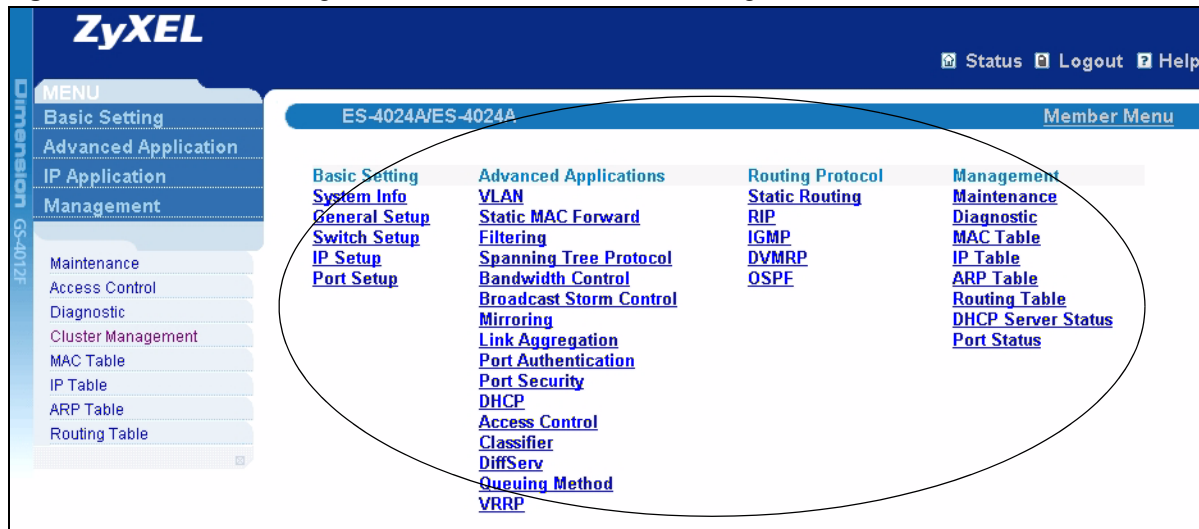
**Table 86** Cluster Management: Status

LABEL	DESCRIPTION
Status	This field displays the role of this switch within the cluster. <b>Manager</b> <b>Member</b> (you see this if you access this screen in the cluster member switch directly and not via the cluster manager) <b>None</b> (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 <b>Index</b> column is a hyperlink leading to the cluster member switch's web configurator (see <a href="#">Figure 142 on page 224</a> ).
HwAddr	This is the cluster member switch's hardware MAC address.
Name	This is the cluster member switch's <b>System Name</b> .
Model	This field displays the model name.
Status	This field displays: <b>Online</b> (the cluster member switch is accessible) <b>Error</b> (for example the cluster member switch password was changed or the switch was set as the manager and so left the member list, etc.) <b>Offline</b> (the switch is disconnected - <b>Offline</b> shows approximately 1.5 minutes after the link between cluster member and manager goes down)

## 35.2.1 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 142** Cluster Management: Cluster Member Web Configurator Screen



### 35.2.1.1 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 143** 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 00:47:52 1970
User (192.168.1.1:(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           3209434 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-a0-c5-d4-88-bf
-rw-rw-rw-  1 owner   group              0 Jul  01 12:00 config-00-a0-c5-d4-88-bf
226 File sent OK
ftp: 463 bytes received in 0.00Seconds 463000.00Kbytes/sec.
ftp> bin
200 Type I OK
ftp> put 350du1.bin fw-00-a0-c5-d4-88-bf
200 Port command okay
150 Opening data connection for STOR fw-00-a0-c5-d4-88-bf
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 87** 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.
350du1.bin	This is the name of the firmware file you want to upload to the cluster member switch.
fw-00-a0-c5-d4-88-bf	This is the cluster member switch's firmware name as seen in the cluster manager switch.
config-00-a0-c5-d4-88-bf	This is the cluster member switch's configuration file name as seen in the cluster manager switch.

## 35.3 Configuring Cluster Management

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

**Figure 144** Clustering Management Configuration

**Clustering Management Configuration** Status

**Clustering Manager:**

Active

Name

VID

Apply Cancel

**Clustering Candidate:**

List

Password

Add Cancel Refresh

Index	MacAddr	Name	Model	Remove


Remove Cancel

The following table describes the labels in this screen.

**Table 88** Clustering Management Configuration

LABEL	DESCRIPTION
Clustering Manager	
Active	Select <b>Active</b> 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 <b>Clustering Candidates</b> list. If a switch that was previously a cluster member is later set to become a cluster manager, then its <b>Status</b> is displayed as <b>Error</b> in the <b>Cluster Management Status</b> screen and a warning icon (  ) appears in the member summary list below.
Name	Type a name to identify the <b>Clustering Manager</b> . 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 <b>802.1Q</b> 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 <b>Clustering Candidates</b> list. This field is ignored if the <b>Clustering Manager</b> is using <b>Port-based</b> VLAN.
Apply	Click <b>Apply</b> to save these changes to the switch.
Cancel	Click <b>Cancel</b> to begin configuring this part of the screen afresh.
Clustering Candidate	The following fields relate to the switches that are potential cluster members.
List	A list of suitable candidates found by auto-discovery is shown here. The switches must be directly connected. Directly connected switches that are set to be cluster managers will not be visible in the <b>Clustering Candidate</b> list. Switches that are not in the same management VLAN group will not be visible in the <b>Clustering Candidate</b> list.

**Table 88** Clustering Management Configuration (continued)

LABEL	DESCRIPTION
Password	<p>Each cluster member's password is its web configurator password. Select a member in the <b>Clustering Candidate</b> 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 <b>Cluster Manager</b>. Its <b>Status</b> is displayed as <b>Error</b> in the <b>Cluster Management Status</b> screen and a warning icon (  ) appears in the member summary list below.</p> <p>If multiple devices have the same password then hold [SHIFT] and click those switches to select them. Then enter their common web configurator password.</p>
Add	Click <b>Add</b> to save this part of the screen to the switch.
Cancel	Click <b>Cancel</b> to begin configuring this part of the screen afresh.
Refresh	Click <b>Refresh</b> 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.
HwAddr	This is the cluster member switch's hardware MAC address.
Name	This is the cluster member switch's <b>System Name</b> .
Model	This is the cluster member switch's model name.
Remove	Select this checkbox and then click the <b>Remove</b> button to remove a cluster member switch from the cluster.
Cancel	Click <b>Cancel</b> to begin configuring this part of the screen afresh.

# CHAPTER 36

## MAC Table

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

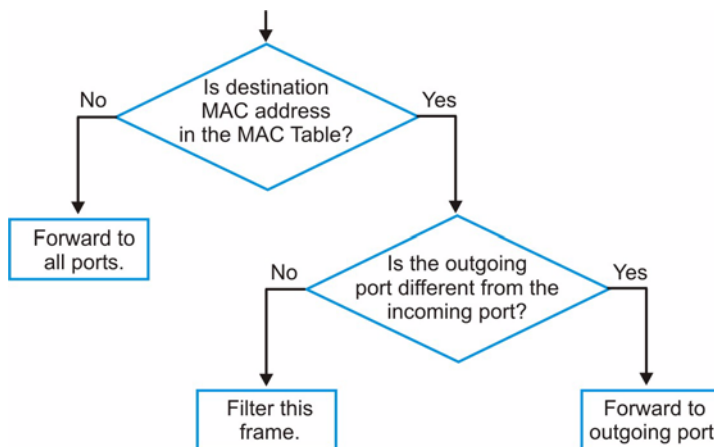
### 36.1 Overview

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.

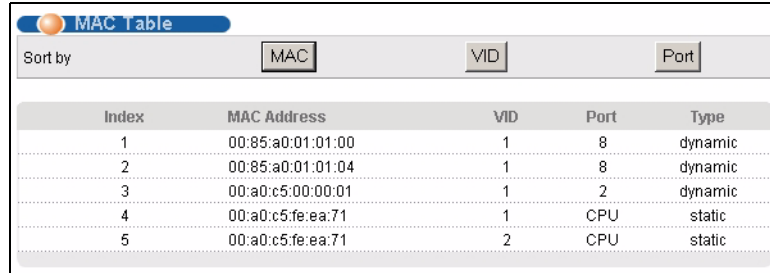
**Figure 145** MAC Table Flowchart



## 36.2 Viewing the MAC Table

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

**Figure 146** MAC Table



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 89** 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 <b>dynamic</b> (learned by the switch) or <b>static</b> (manually entered in the <b>Static MAC Forwarding</b> screen).

# CHAPTER 37

## IP Table

This chapter introduces the IP table.

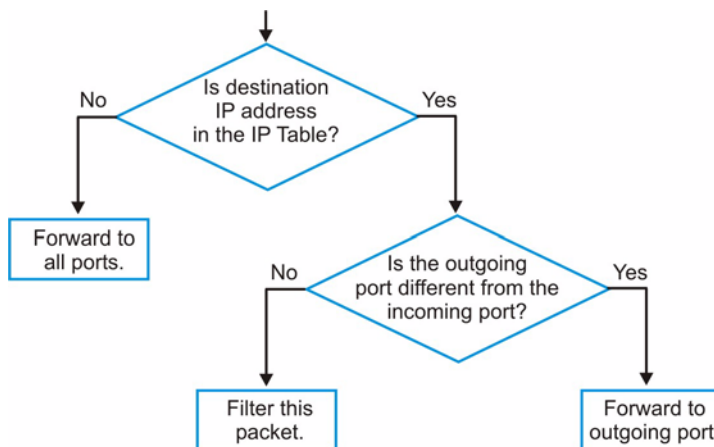
### 37.1 Overview

The **IP Table** screen shows how packets are forwarded or filtered across the switch's ports. It shows what device IP address, belonging to what VLAN group (if any) is forwarded to which port(s) and whether the IP address is dynamic (learned by the switch) or static (belonging to the switch).

The switch uses the IP table to determine how to forward packets. See the following figure.

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

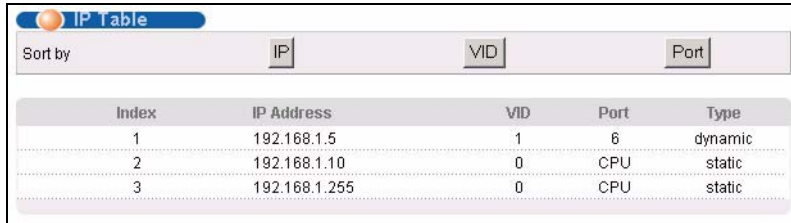
**Figure 147** IP Table Flowchart



## 37.2 Viewing the IP Table

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

**Figure 148** IP Table



Index	IP Address	VID	Port	Type
1	192.168.1.5	1	6	dynamic
2	192.168.1.10	0	CPU	static
3	192.168.1.255	0	CPU	static

The following table describes the labels in this screen.

**Table 90** IP 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.
IP	Click this button to display and arrange the data according to IP 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 field displays the index number.
IP Address	This is the IP address of the device from which the incoming packets came.
VID	This is the VLAN group to which the packet belongs.
Port	This is the port from which the above IP address was learned. This field displays <b>CPU</b> to indicate the IP address belongs to the switch.
Type	This shows whether the IP address is <b>dynamic</b> (learned by the switch) or <b>static</b> (belonging to the switch).

# CHAPTER 38

## ARP Table

This chapter introduces ARP Table.

### 38.1 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.

#### 38.1.1 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.

### 38.2 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 149** 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 91** 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 <b>Static MAC Forwarding</b> screen).

# CHAPTER 39

## Routing Table

This chapter introduces the routing table.

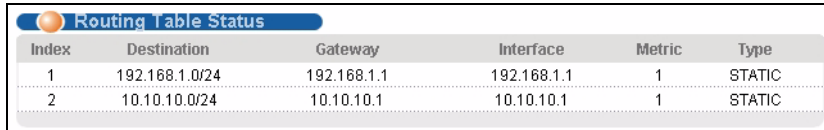
### 39.1 Overview

The routing table contains the route information to the network(s) that the switch can reach. The switch automatically updates the routing table with the RIP information received from other Ethernet devices.

### 39.2 Viewing the Routing Table

Click **Management, Routing Table** in the navigation panel to display the screen as shown.

**Figure 150** Routing Table Status



Index	Destination	Gateway	Interface	Metric	Type
1	192.168.1.0/24	192.168.1.1	192.168.1.1	1	STATIC
2	10.10.10.0/24	10.10.10.1	10.10.10.1	1	STATIC

The following table describes the labels in this screen.

**Table 92** Routing Table Status

LABEL	DESCRIPTION
Index	This field displays the index number.
Destination	This field displays the destination IP routing domain.
Gateway	This field displays the IP address of the gateway device.
Metric	This field displays the cost of the route.
Type	This field displays the method used to learn the route.



# CHAPTER 40

## Introducing the Commands

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

### 40.1 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.

#### 40.1.1 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.

### 40.2 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.

## 40.2.1 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.

## 40.2.2 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

### 40.2.2.1 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 40.3 on page 238](#)).

**Figure 151** Initial Console Port Screen

```
Copyright (c) 1994 - 2004 ZyXEL Communications Corp.
initialize mgmt, ethernet address: 00:a0:c5:fe:ea:70
initialize switch, ethernet address: 00:a0:c5:fe:ea:71
Initializing switch unit 0...
Initializing switch unit 1...
Press ENTER to continue...
```

## 40.2.3 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 40.3 on page 238](#)).

## 40.3 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 152** CLI: Login Screen

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

## 40.4 Command Syntax Conventions

The rules of the commands are listed next.

- The command keywords are in *courier new* font.
- The required fields in a command are enclosed in angle brackets <>, for instance, ping <ip> means that you must specify an IP number for this command.
- The optional fields in a command are enclosed in square brackets [], for instance,

```
configure snmp-server [contact <system contact>] [location
<system location>]
```

means that the `contact` and `location` fields are optional.

- “Command” refers to a command used in the command line interface (CLI command).
- The | symbol means “or”.
- The entry <cr> in the command lines refers to carriage return. Press [ENTER] or carriage return after a command to execute the command.
- Use the up (▲) or down (▼) arrow key to scroll through the command history list.
- The CLI does not accept partial or incomplete commands. You may enter a unique part of a command and press [TAB] to have the switch automatically display the full command. For example, if you enter “config” and press [TAB], the full command of “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.

## 40.5 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.

### 40.5.1 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 153** 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
  ping <ip|host-name> <cr>
  ping <ip|host-name> [..]
  ping help
  traceroute <ip|host-name> <cr>
  traceroute <ip|host-name> [..]
  traceroute help
  ssh <1|2> <[user@]dest-ip> <cr>
  ssh <1|2> <[user@]dest-ip> [command </>]
ras>
```

**Figure 154** 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>

```

## 40.5.2 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 155** 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 156** CLI: Help: Detailed Command Information: Example 2

```

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

```

## 40.6 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, router and VLAN.

- To enter config-vlan mode, type `vlan` followed by a number (between 1 to 4094). For example, enter `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 configure the routing domain, enter `interface route-domain` followed by the domain IP address and subnet mask bits (for example, `interface route-domain 192.168.1.1/24`).
- Use the `router` commands to configure the routing protocol settings.

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

## 40.7 Using Command History

The switch keeps a list of up to 256 commands you have entered for the current CLI session. You can use any commands in the history again by pressing the up (▲) or down (▼) arrow key to scroll through the previously used commands and press [ENTER]. Use the history command to display the list of commands.

**Figure 157** CLI: History Command Example

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

## 40.8 Saving Your Configuration

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

**Figure 158** 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.

## 40.8.1 Logging Out

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

## 40.9 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.

### 40.9.1 User Mode

The following table describes the commands available for User mode.

**Table 93** Command Summary: User Mode

COMMAND		DESCRIPTION
enable		Accesses Enable (or privileged) mode. See <a href="#">Section 40.9.2 on page 243</a> .
exit		Logs out from the CLI.
help		Displays help information.
history		Displays a list of previously command(s) that you have executed. The switch stores up to 256 commands in history.
logout		Exits from the CLI.
ping	<IP host-name> [<in-band out-of-band vlan <vlan-id>] [size <0-1472>] [-t]	Sends a Ping request to an Ethernet device.
	help	Displays help information for this command.
show	hardware-monitor <C F>	Displays current hardware monitor information with the specified temperature unit (Celsius C or Fahrenheit F).
	ip	Displays IP related information.
	system-information	Displays general system information.
ssh	<1 2> <[user@]dest-ip>	Connects to an SSH server with the specified SSH version.

**Table 93** Command Summary: User Mode (continued)

COMMAND		DESCRIPTION
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 help information for this command.

## 40.9.2 Enable Mode

The following table describes the commands available for Enable mode.

**Table 94** Command Summary: Enable Mode

COMMAND		DESCRIPTION
baudrate <1 2 3 4 5 >		Sets the console port baud rate. 1:38400 2:19200 3:9600 4:57600 5:115200
boot	config <index>	Restarts the system with the specified configuration file.
configure		Accesses Configuration mode. See <a href="#">Section 40.9.3 on page 247</a> .
copy	running-config tftp <ip><remote-file>	Backs up running configuration to the specified TFTP server with the specified file name.
	tftp	config <ip> <remote-file>
		flash <ip> <remote-file>
disable		Exits Enable (or privileged) mode.
enable		Accesses Enable (or privileged) mode.
erase	running-config	Resets to the factory default settings.
exit		Exits Enable (or privileged) mode.
help		Displays help information.
history		Displays a list of command(s) that you have previously executed.
igmp-flush		Removes all IGMP information.
kick	<tcp session>	Disconnects the specified TCP session.
logout		Exits Enable (or privileged) mode.
mac-flush		Clears the MAC address table.

**Table 94** Command Summary: Enable Mode (continued)

COMMAND		DESCRIPTION
	<port-num>	Removes all learned MAC address on the specified port(s).
no	logging	Disables syslog logging.
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).
reload	config <index>	Restarts the system and use the specified configuration file.
show	classifier	Displays all classifier related information.
		[name]
	cluster	Displays the specified classifier related information.
		cluster
		candidates
		member
		members config
		member mac <mac-addr>
	dhcp	relay
		server
		server <vlnid-id>
	diffserv	
	garp	
	hardware-monitor	<C F>
	https	
		certificate
		key <rsa dsa>
		session
		timeout
	igmp-filtering	profile [name]
	igmp-snooping	
	interface <port-number>	
	interfaces config <port-list>	

**Table 94** Command Summary: Enable Mode (continued)

COMMAND			DESCRIPTION
		bandwidth-control	Displays bandwidth control settings.
		bstorm-control	Displays broadcast storm control settings.
		egress	Displays outgoing port information.
		igmp-filtering	Displays IGMP filtering settings.
		igmp-group-limited	Displays the IGMP group limit.
		igmp-immediate-leave	Displays the IGMP Immediate Leave setting.
	ip		Displays IP related information.
		arp	Displays the ARP table.
		dvmrp group	Displays DVMRP group information.
		dvmrp interface	Displays DVMRP interface information.
		dvmrp neighbour	Displays DVMRP neighbour information.
		dvmrp prune	Displays the DVMRP prune information.
		dvmrp route	Displays the DVMRP routes.
		igmp	Displays the IGMP setting.
		iptable all [IP VID PORT]	Displays the IP address table. You can sort the table based on the IP address, VLAN ID or the port number.
		iptable static	Displays the static IP address table.
		ospf database	Displays OSPF link state database information.
		ospf interface	Displays OSPF interface settings.
		ospf neighbor	Displays OSPF neighbor information.
		route	Displays IP routing information.
		route static	Displays IP static route information.
		tcp	Displays IP TCP information.
		udp	Displays IP UDP information.
	lACP		Displays LACP (Link Aggregation Control Protocol) settings.
	logging		Displays system logs.
	loginPrecedence		Displays login precedence settings.
	logins		Displays login account information.
	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.

**Table 94** Command Summary: Enable Mode (continued)

COMMAND		DESCRIPTION
	mac-aging-time	Displays MAC learning aging time.
	mac-count	Displays the count of MAC addresses learnt.
	multicast	Displays multicast settings.
	multi-login	Displays multi-login information
	mvr	Displays all MVR settings.
		<VID>
	policy	Displays the specified MVR group settings.
		[name]
	port-access-authenticator	Displays all policy related information.
		[port-list]
	port-security	Displays port authentication settings on the specified port(s).
		[port-list]
	radius-server	Displays all port security settings.
	remote-management	Displays RADIUS server settings.
		[index]
	router	Displays all secured client information.
		dvmrp
		igmp
		ospf
		ospf area
		ospf network
		ospf redistribute
		ospf virtual-link
		rip
		vrrp
	running-config	Displays DVMRP settings.
	service-control	Displays global IGMP settings.
	snmp-server	Displays OSPF settings.
	spanning-tree	Displays OSPF area settings.
	ssh	Displays OSPF network (or interface) settings.
		config
		ospf redistribute
		ospf virtual-link
		rip
		vrrp
	running-config	Displays current operating configuration.
	service-control	Displays service control settings.
	snmp-server	Displays SNMP settings.
	spanning-tree	Displays Spanning Tree Protocol (STP) settings.
	ssh	Displays general SSH settings.

**Table 94** Command Summary: Enable Mode (continued)

COMMAND		DESCRIPTION	
		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).
	system-information		Displays general system information.
	time		Displays current system time and date.
	timesync		Displays time server information.
	trunk		Displays link aggregation information.
	vlan		Displays the status of all VLANs.
		<vlan-id>	Displays the status of the specified VLAN.
	vlan-stacking		Displays VLAN stacking settings.
	vlanlq	gvrp	Displays GVRP settings.
		port-isolation	Displays port isolation settings.
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.
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 help information for this command.
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.

### 40.9.3 General Configuration Mode

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

**Table 95** Command Summary: Configuration Mode

COMMAND		DESCRIPTION
admin-password	<pw-string> <confirm-string>	Changes the administrator password.
bandwidth-control		Enables bandwidth control.

**Table 95** Command Summary: Configuration Mode (continued)

COMMAND		DESCRIPTION
bcp-transparency		Enables Bridge Control Protocol (BCP) transparency.
classifier	<pre> &lt;name&gt; &lt;[packet-format &lt;802.3untag 802.3tag   EtherIIuntag  EtherIItag&gt;] [priority &lt;0-7&gt;] [vlan &lt;vlan-id&gt;] [ethernet-type &lt;ether-num ip ipx  arp rarp  appletalk decnet  sna netbios dlc&gt;] [source-mac &lt;src- mac-addr&gt;] [source- port &lt;port-num&gt;] [destination-mac &lt;dest-mac-addr&gt;] [dscp &lt;0-63&gt; ] [ip- protocol &lt;protocol- num tcp udp icmp egp   ospf rsvp igmp  igp pim ipsec&gt;] [establish-only]] [source-ip &lt;src-ip- addr&gt; [mask-bits &lt;mask-bits&gt;]] [source-socket &lt;socket-num&gt;] [destination-ip &lt;dest-ip-addr&gt; [mask-bits &lt;mask- bits&gt;]] [destination-socket &lt;socket-num&gt;] [inactive]&gt; </pre>	Configures a classifier. A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming port number.
	help	Displays help information for this command.
cluster	<vlan-id>	Enables clustering in the specified VLAN group.
	member <mac-address> password <password-str>	Sets the cluster member.
	name <cluster name>	Sets a descriptive name for the cluster.
	rcommand <mac-address>	Logs into the CLI of the specified cluster member.
default-management	<in-band out-of-band>	Specifies through which traffic flow the switch is to send packets.



**Table 95** Command Summary: Configuration Mode (continued)

COMMAND		DESCRIPTION	
dhcp	relay	Enables DHCP relay.	
		helper-address <remote-dhcp-server1> <remote-dhcp-server2> <remote-dhcp-server3>	Sets the IP addresses of up to 3 DHCP servers.
		information	Allows the switch to add system name to agent information.
		option	Allows the switch to add DHCP relay agent information.
	server <vlan-id>	starting-address <ip-addr> <subnet-mask> <size-of-client>	
diffserv			Enables DiffServ.
	dscp <0-63> priority <0-7>		Sets the DSCP-to-IEEE 802.1q mappings.
exit			Exits from the CLI.
garp	join <100-65535> leave <msec> leaveall <msec>		Configures GARP time settings.
help			Displays help information.
history			Displays a list of previous command(s) that you have executed.
hostname	<name_string>		Sets the switch's name for identification purposes.
https	cert-regeneration <rsa dsa>		Re-generates a certificate.
	timeout <0-65535>		Sets the HTTPS timeout period.
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.
igmp-snooping			Enables IGMP snooping.
	unknown-multicast-frame <drop flooding>		Sets how to treat traffic from unknown multicast group.
interface	port-channel <port-list>		Enables a port or a list of ports for configuration. See <a href="#">Section 40.9.4 on page 261</a> for more details.

**Table 95** Command Summary: Configuration Mode (continued)

COMMAND		DESCRIPTION	
	route-domain <ip-address>/<mask-bits>	Enables a routing domain for configuration. See <a href="#">Section 40.9.5 on page 264</a> for more details.	
ip	address	<ip> <mask>	Sets the IP address and subnet mask of the out-of-band management port.
		default-gateway <ip>	Sets the default gateway's IP address for the out-of-band management port.
	name-server	<ip>	Sets the IP address of a domain name server.
	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.
lACP			Enables Link Aggregation Control Protocol (LACP).
	system-priority	<1-65535>	Sets the priority of an active port using LACP.
loginPrecedence	<LocalOnly   LocalRADIUS   RADIUSOnly>		Select which database the switch should use (first) to authenticate a user.
logins	username <name> password <pwd>		Configures up to four read-only login accounts.
logout			Exits from the CLI.
mac-aging-time	<10-3000>		Sets learned MAC aging time.
mac-filter	name <name> mac <mac-addr> vlan <vlan-id> drop <src/ dst/both>		Configures a static MAC address port filtering rule.
		inactive	Disables a static MAC address port filtering rule.
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-port			Enables port mirroring.
	<port-num>		Enables port mirroring on a specified port.
mode	zynos		Changes the CLI mode to the Zynos format.

**Table 95** Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION
multi-login			Enables multi-login.
mvr	<vlan-id>		Enters the MVR (Multicast VLAN Registration) configuration mode. Refer to <a href="#">Section 40.10 on page 266</a> for more information.
no	bandwidth-control		Disable bandwidth control on the switch.
	bcp-transparency		
	classifier	<name>	Disables the classifier. Each classifier has one rule. If you disable a classifier you cannot use policy rule related information.
		<name> inactive	Enables a classifier.
	cluster		Disables cluster management on the switch.
		member <mac-address>	Removes the cluster member.
	dhcp relay		Disables DHCP relay.
		information	Disables the relay agent information option 82.
		option	System name is not appended to option 82 information field.
	dhcp server <vlan-id>		Disables DHCP server settings.
		default-gateway	Disables DHCP server default gateway settings.
		primary-dns	Disables DHCP primary DNS server settings.
		secondary-dns	Disables DHCP server secondary DNS settings.
	diffserv		Disables the DiffServ settings.
	https	timeout	Resets the session timeout to the default of 300 seconds.
	igmp-filtering		Disables IGMP filtering on the switch.
		profile <name>	Disables the specified IGMP filtering profile.
		profile <name> start-address <ip> end-address <ip>	Clears the settings of the specified IGMP filtering profile.
	igmp-snooping		Disables IGMP snooping.
	ip		Sets the management IP address to the default value.

**Table 95** Command Summary: Configuration Mode (continued)

COMMAND		DESCRIPTION
	route <ip> <mask>	Removes a specified IP static route.
	route <ip> <mask> inactive	Enables a specified IP static route.
lacp		Disables the link aggregation control protocol (dynamic trunking) on the switch.
logins		Disables login access to the specified name.
mac-filter	name <name> mac <mac-addr> vlan <vlan-id> drop <src dst both> inactive	Enables the specified MAC-filter rule.
	name <name> mac <mac-addr> vlan <vlan-id> drop <src dst both>	Disables the specified MAC filter rule.
mac-forward	name <name> 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).
	name <name> 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-port		Disables port mirroring on the switch.
multi-login		Disables another administrator from logging into Telnet or the CLI.
mvr		Displays MVR on the switch.
policy <name>		Deletes the policy. A policy sets actions for the classified traffic.
	inactive	Enables a policy.
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 device.

**Table 95** Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION
		<port-list>	Disables port security on the specified ports.
		<port-list> learn inactive	Enables MAC address learning on the specified ports.
	radius-server		Disables the use of authentication from the RADIUS server.
	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.
	router	dvmrp	Disables DVMRP on the switch.
		igmp	Disables IGMP on the switch.
		ospf	Disables OSPF on the switch.
		rip	Disable RIP on the switch.
		vrrp network <ip-address>/<mask-bits> vr-id <1-7>	Deletes VRRP settings.
	service-control	ftp	Disables FTP access to the switch.
		http	Disables web browser control 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.
		ssh	Disables SSH (Secure Shell) server access to the switch.
		telnet	Disables telnet access to the switch.
	snmp-server	trap-destination <ip>	Disables sending of SNMP traps to a station.
	spanning-tree		Disables STP.
		<port-list>	Disables STP on listed ports.
	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 <host-ip>	Removes the specified remote hosts from the list of all known hosts.

**Table 95** Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION
		known-hosts <host-ip> [1024 ssh- rsa ssh-dsa]	Removes remote known hosts with the specified public key (1024-bit RSA1, RSA or DSA).
	storm-control		Disables broadcast storm control.
	timesync		Disables timeserver settings.
	trunk	<T1 T2 T3 T4 T5 T6>	Disables the specified trunk group.
		<T1 T2 T3 T4 T5 T6> interface <port-list>	Removes ports from the specified trunk group.
		<T1 T2 T3 T4 T5 T6> lacp	Disables LACP in the specified trunk group.
	vlan	<vlan-id>	Deletes the static VLAN entry.
	vlanlq	gvrp	Disables GVRP on the switch.
		port-isolation	Disables port isolation.
	vlan-stacking		Disables VLAN stacking.
password			Change the password for Enable mode.

**Table 95** Command Summary: Configuration Mode (continued)

COMMAND		DESCRIPTION	
policy	<pre> &lt;name&gt; classifier &lt;classifier-list&gt; &lt; [vlan&lt;vlan-id&gt;] [egress-port &lt;port- num&gt;] [priority &lt;0-7&gt;] [dscp &lt;0-63&gt;] [tos &lt;0-7&gt;] [bandwidth &lt;bandwidth&gt;] [outgoing-packet- format &lt;tagged untagged&gt;] [out-of-profile-dscp &lt;0-63&gt;] [forward-action &lt;drop forward&gt;] [queue-action &lt;prio- set prio-queue prio- replace-tos&gt;] [diffserv-action &lt;diff-set-tos diff- replace- priority diff-set- dscp&gt;] [outgoing-mirror] [outgoing-eport] [outgoing-non- unicast-eport] [outgoing-set-vlan] [metering] [out-of-profile- action &lt;[change- dscp] [drop] [ forward]&gt;] [inactive]&gt; </pre>	<p>Configures a policy. A classifier distinguishes traffic into flows based on the configured criteria. A policy rule ensures that a traffic flow gets the requested treatment in the network.</p>	
port-access-authenticator		Enables 802.1x authentication on the switch.	
	<port-list>	Enables 802.1x authentication on the specified port(s).	
		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 device.
	<port-list>		Enables port security on the specified port(s).

**Table 95** Command Summary: Configuration Mode (continued)

COMMAND		DESCRIPTION
		<code>learn inactive</code>
		<code>address-limit &lt;number&gt;</code>
<code>queue</code>	<code>level &lt;0-7&gt; priority &lt;0-7&gt;</code>	
<code>radius-server</code>	<code>host &lt;ip&gt; [acct-port &lt;socket-number&gt;] [key &lt;key-string&gt;]</code>	
<code>remote-management</code>	<code>&lt;index&gt; start-addr &lt;ip&gt; end-addr &lt;ip&gt; service &lt;telnet ftp http icmp snmp&gt;</code>	
<code>router</code>	<code>dvmrp</code>	
		<code>exit</code>
		<code>threshold &lt;ttl-value&gt;</code>
	<code>igmp</code>	
		<code>exit</code>
	<code>ospf &lt;router-id&gt;</code>	
		<code>area &lt;area-id&gt;</code>
		<code>area &lt;area-id&gt; authentication</code>
		<code>area &lt;area-id&gt; authentication message-digest</code>
		<code>area &lt;area-id&gt; default-cost &lt;0-65535&gt;</code>
		<code>area &lt;area-id&gt; name &lt;name&gt;</code>
		<code>area &lt;area-id&gt; stub</code>
		<code>area &lt;area-id&gt; stub no-summary</code>
		<code>area &lt;area-id&gt; virtual-link &lt;router-id&gt;</code>



**Table 95** Command Summary: Configuration Mode (continued)

COMMAND		DESCRIPTION
	area <area-id> virtual-link <router-id> authentication- key <key>	Enables simple authentication and sets the authentication key for the specified virtual link in the area.
	area <area-id> virtual-link <router-id> authentication- same-as-area	Sets the virtual link to use the same authentication method as the area.
	area <area-id> virtual-link <router-id> message-digest- key <keyid> md5 <key>	Enables MD5 authentication and sets the key ID and key for the virtual link in the area.
	area <area-id> virtual-link <router-id> name <name>	Sets a descriptive name for the virtual link for identification purposes.
	exit	Leaves the router OSPF configuration mode.
	network <ip-addr/ bits> area <area- id>	Creates an OSPF area.
	no area <area-id>	Removes the specified area.
	no area <area-id> authentication	Sets the area to use no authentication (None).
	no area <area-id> default-cost	Sets the area to use the default cost (15).
	no area <area-id> stub	Disables stub network settings in the area.
	no area <area-id> stub no-summary	Sets the area to send LSAs (Link State Advertisements).
	no area <area-id> virtual-link <router-id> authentication- key	Resets the authentication settings on this virtual link.
	no area <area-id> virtual-link <router-id> message-digest- key	Resets the authentication settings on this virtual link.

**Table 95** Command Summary: Configuration Mode (continued)

COMMAND		DESCRIPTION	
		no area <area-id> virtual-link <router-id> authentication- same-as-area	Resets the authentication settings on this virtual area.
		no area <area-id> virtual-link <router-id>	Deletes the virtual link from the area.
		no network <ip- addr/bits>	Deletes the OSPF network.
		no redistribute rip	Sets the switch not to learn RIP routing information.
		no redistribute static	Sets the switch not to learn static routing information.
		redistribute rip metric-type <1 2> metric <0-65535>	Sets the switch to learn RIP routing information which will use the specified metric information.
		redistribute static metric- type <1 2> metric <0-65535>	Sets the switch to learn static routing information which will use the specified metric information.
	rip		Enables and enters the RIP configuration mode.
		exit	Leaves the RIP configuration mode.
	vrrp network <ip- address>/<mask-bits> vr-id <1-7> uplink- gateway <ip>		Adds a new VRRP network and enters the VRRP configuration mode.
		exit	Exits from the VRRP command mode.
		inactive	Disables the VRRP settings.
		interval <1..255>	Sets the time interval (in seconds) between Hello message transmissions.
		name <name string>	Sets a descriptive name of the VRRP setting for identification purposes.
		no inactive	Activates this VRRP.
		no preempt	Disables VRRP preemption mode.
		no primary- virtual-ip	Resets the network to use the default primary virtual gateway (interface IP address).
		no secondary- virtual-ip	Sets the network to use the default secondary virtual gateway (0.0.0.0).

**Table 95** Command Summary: Configuration Mode (continued)

COMMAND		DESCRIPTION
	preempt	Enables preemption mode.
	primary-virtual-ip <ip>	Sets the primary VRRP virtual gateway IP address.
	priority <1-254>	Sets the priority of the uplink-gateway.
	secondary-virtual-ip <ip>	Sets the secondary VRRP virtual gateway IP address.
service-control	ftp <socket-number>	Allows FTP access on the specified service port.
	http <socket-number> <timeout>	Allows HTTP access on the specified service port and defines the timeout period.
	https <socket-number>	Allows HTTPS access on the specified service port.
	icmp	Allows ICMP management packets.
	snmp	Allows SNMP management.
	ssh <socket-number>	Allows SSH access on the specified service port.
	telnet <socket-number>	Allows Telnet access on the specified service port.
snmp-server	[contact <system contact>] [location <system location>]	Sets the geographic location and the name of the person in charge of this switch.
	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.
spanning-tree		Enables STP on the switch.
	<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.
	hello-time <1-10> maximum-age <6-40> forward-delay <4-30>	Sets Hello Time, Maximum Age and Forward Delay.
	help	Displays help information.

**Table 95** Command Summary: Configuration Mode (continued)

COMMAND		DESCRIPTION
	priority <0-61440>	Sets the bridge priority of the switch.
ssh	known-hosts <host-ip> <1024 ssh-rsa ssh-dsa> <key>	Adds a remote host to which the switch can access using SSH service.
storm-control		Enables broadcast storm control on the switch.
time	<Hour:Min:Sec>	Sets the time in hour, minute and second format.
	date <month/day/year>	Sets the date in year, month and day format.
	help	Displays help information.
	timezone <-1200 ... 1200>	Selects the time difference between UTC (formerly known as GMT) and your time zone.
timesync	<daytime time ntp>	Sets the time server protocol.
	server <ip>	Sets the IP address of your time server.
trunk	<T1 T2 T3 T4 T5 T6>	Activates a trunk group.
	<T1 T2 T3 T4 T5 T6>lacp	Enables LACP for a trunk group.
	<T1 T2 T3 T4 T5 T6>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.
vlan	<1-4094>	Enters the VLAN configuration mode. See <a href="#">Section 40.9.6 on page 265</a> for more information.
vlanlq	gvrp	Enables GVRP.
	port-isolation	Enables port-isolation.
vlan-stacking		Enables VLAN stacking on the switch.
	<SPTPID>	Sets the SP TPID (Service Provider Tag Protocol Identifier).
vlan-type	<802.1q port-based>	Specifies the VLAN type.

## 40.9.4 interface port-channel Commands

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

**Table 96** interface port-channel Commands

COMMAND			DESCRIPTION
<code>interface port-channel &lt;port-list&gt;</code>			Enables a port or a list of ports for configuration.
	<code>bandwidth-limit</code>		Enables bandwidth control on the port(s).
		<code>cir &lt;Kbps&gt;</code>	Sets the guaranteed bandwidth allowed for incoming traffic on the port(s).
		<code>egress &lt;Kbps&gt;</code>	Sets the maximum bandwidth allowed for outgoing traffic on the port(s).
		<code>ingress &lt;Kbps&gt;</code>	Sets the maximum bandwidth allowed for incoming traffic on the port(s).
		<code>pir &lt;Kbps&gt;</code>	Sets the maximum bandwidth allowed for incoming traffic on the port(s).
	<code>bpdu-control &lt;peer tunnel discard network&gt;</code>		Sets how Bridge Protocol Data Units (BPDUs) are used in STP port states.
	<code>broadcast-limit</code>		Enables broadcast storm control limit on the switch.
	<code>diffserv</code>		Enables DiffServ on the port(s).
		<code>&lt;pkt/s&gt;</code>	Sets how many broadcast packets the interface receives per second.
	<code>dlf-limit</code>		Enables the Destination Lookup Failure (DLF) limit.
		<code>&lt;pkt/s&gt;</code>	Sets the interface DLF limit in packets per second (pps).
	<code>egress set &lt;port-list&gt;</code>		Sets the outgoing traffic port list for a port-based VLAN.
	<code>exit</code>		Exits from the interface port-channel command mode.
	<code>flow-control</code>		Enables interface flow control. Flow control regulates transmissions to match the bandwidth of the receiving port.
	<code>frame-type &lt;all tagged&gt;</code>		Choose to accept both tagged and untagged incoming frames or just tagged incoming frames on a port.

**Table 96** interface port-channel Commands (continued)

COMMAND		DESCRIPTION
	<code>gvrp</code>	Enables this function to permit VLAN groups beyond the local switch.
	<code>help</code>	Displays a description of the interface port-channel commands.
	<code>igmp-filtering</code>	<code>profile &lt;profile&gt;</code> Applies the specified IGMP filtering profile.
	<code>igmp-group-limit</code>	Enables the IGMP group limiting feature.
		<code>number &lt;number&gt;</code> Sets the maximum number IGMP groups allowed.
	<code>igmp-immediate-leave</code>	Enables the IGMP immediate leave function.
	<code>igmp-querier-mode &lt;auto fixed edge&gt;</code>	Sets the IGMP query mode for the port.
	<code>inactive</code>	Disables the specified port(s) on the switch.
	<code>ingress-check</code>	Enables the device to discard incoming frames for VLANs that are not included in a port member set.
	<code>intrusion-lock</code>	Enables intrusion lock on the port(s) and a port cannot be connected again after you disconnected the cable.
	<code>ipmc egress-untag-vlan &lt;1-4094&gt;</code>	Enables the port(s) to remove specified VLAN tag from IP multicasting packets before forwarding.
	<code>mirror</code>	Enables port mirroring in the interface.
		<code>dir &lt;ingress egress both&gt;</code> Enables port mirroring for incoming, outgoing or both incoming and outgoing traffic. Port mirroring copies traffic from one or all ports to another or all ports for external analysis.
	<code>multicast-limit</code>	Enables the port(s) multicast limit.
		<code>&lt;pkt/s&gt;</code> Sets how many multicast packets the port(s) receives per second.
	<code>name &lt;port-name-string&gt;</code>	Sets a name for the port(s). Enter a descriptive name (up to nine printable ASCII characters).
	<code>no</code>	<code>bandwidth-limit</code> Disables bandwidth limit on the port(s).

**Table 96** interface port-channel Commands (continued)

COMMAND		DESCRIPTION
	<code>broadcast-limit</code>	Disables broadcast storm control limit on the port(s).
	<code>diffserv</code>	Disables DiffServ on the port(s).
	<code>dlf-limit</code>	Disables destination lookup failure (DLF) on the switch.
	<code>egress-set &lt;port-list&gt;</code>	Disables the egress port setting.
	<code>flow-control</code>	Disables flow control on the port(s).
	<code>gvrp</code>	Disable GVRP on the port(s).
	<code>igmp-filtering profile</code>	Disables IGMP filtering.
	<code>igmp-group-limit</code>	Disables IGMP group limitation.
	<code>igmp-immediate-leave</code>	Disables the IGMP immediate leave function.
	<code>inactive</code>	Enables the port(s) on the switch.
	<code>ingress-check</code>	Disables ingress checking on the port(s).
	<code>intrusion-lock</code>	Disables intrusion-lock on a port so that a port can be connected again after you disconnected the cable.
	<code>mirror</code>	Disables port mirroring on the port(s).
	<code>multicast-limit</code>	Disables multicast limit on the port(s).
	<code>vlan-trunking</code>	Disables VLAN trunking on the port(s).
	<code>pvid &lt;1-4094&gt;</code>	The default PVID is VLAN 1 for all ports. Sets a PVID in the range 1 to 4094 for the specified interface.
	<code>qos</code>	<code>priority &lt;0 .. 7&gt;</code> Sets the quality of service priority for an interface.
	<code>speed-duplex</code>	<code>&lt;auto 10-half 10-full 100-half 100-full 1000-full&gt;</code> Sets the duplex mode (half or full) and speed (10, 100 or 1000 Mbps) of the connection on the interface. Selecting <code>auto</code> (auto-negotiation) makes one port able to negotiate with a peer automatically to obtain the connection speed and duplex mode that both ends support.
	<code>spq</code>	Sets the port(s) to use Strict Priority Queuing.
	<code>test</code>	Performs an interface loopback test.

**Table 96** interface port-channel Commands (continued)

COMMAND			DESCRIPTION
	vlan-stacking	priority <0-7>	Sets the priority of the specified port(s) in VLAN stacking.
		role <access   tunnel>	Sets the VLAN stacking port roles of the specified port(s).
		SPVID <1-4094>	Sets the service provider VID of the specified port(s).
	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.
	wrr		Sets the port(s) to use Weighted Round Robin queuing (WRR).
		<wt1> <wt2> ... <wt8>	Sets the interface to use WRR queuing. A weight value of one to eight is given to each variable from wt1 to wt8.

## 40.9.5 interface route-domain Commands

The following table lists the `interface route-domain` commands in configuration mode.

Use these commands to configure the IP routing domains.

**Table 97** interface route-domain Commands

COMMAND			DESCRIPTION
<code>interface route-domain &lt;ip-address&gt;/&lt;mask-bits&gt;</code>			Enables a routing domain for configuration.
	<code>exit</code>		Exits from the interface routing-domain command mode.
	<code>ip</code>	<code>dvmrp</code>	Enables this function to permit VLAN groups beyond the local switch.
		<code>igmp &lt;v1 v2&gt;</code>	Enables IGMP in this routing domain.
		<code>ospf authentication-key &lt;k&gt;</code>	Enables OSPF authentication in this routing domain.
		<code>ospf authentication-same-aa</code>	Sets the same OSPF authentication settings in the routing domain as the associated area.
		<code>ospf cost &lt;1-65535&gt;</code>	Sets the OSPF cost in this routing domain.
		<code>ospf message-digest-key &lt;k&gt;</code>	Sets the OSPF authentication key in this routing domain.



**Table 97** interface route-domain Commands (continued)

COMMAND			DESCRIPTION
		rip direction <Outgoing In>	Sets the RIP direction in this routing domain.
		vrrp authentication- key <k>	Sets the VRRP authentication key in the routing domain.
	no	ip dvmrp	Disables DVMRP in this routing domain.
		ip igmp	Disables IP IGMP in this routing domain.
		ip ospf authentication-key	Disables OSPF authentication key settings in this routing domain.
		ip ospf authentication-sama	Sets the routing domain not to use the same OSPF authentication settings as the area.
		ip ospf cost	Disables the OSPF cost in the routing domain.
		ip ospf message- digest-key	Sets the routing domain not to use a security key in OSPF.
		ip vrrp authentication-key	Resets the VRRP authentication settings.

## 40.9.6 config-vlan Commands

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

**Table 98** Command Summary: config-vlan Commands

COMMAND			DESCRIPTION
vlan <1-4094>			Creates a new VLAN group.
	exit		Leaves the VLAN configuration mode.
	fixed <port-list>		Specifies the port(s) to be a permanent member of this VLAN group.
	forbidden <port- list>		Specifies the port(s) you want to prohibit from joining this VLAN group.
	help		Displays a list of available VLAN commands.
	inactive		Disables the specified VLAN.
	ip address	<ip-address> <mask>	Sets the IP address of the switch in the VLAN.
		<ip-address> <mask> manageable	Sets the IP address of the switch in the VLAN and allow remote management to this IP address.
		default gateway <ip-address>	Sets the default gateway IP address in this VLAN.
	name <name-str>		Specifies a name for identification purposes.
	no	fixed <port-list>	Sets fixed port(s) to normal port(s).

**Table 98** Command Summary: config-vlan Commands (continued)

COMMAND		DESCRIPTION
	forbidden <port-list>	Sets forbidden port(s) to normal port(s).
	inactive	Enables the specified VLAN.
	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.
	untagged <port-list>	Specifies the port(s) you want to tag all outgoing frames transmitted with this VLAN Group ID.
	normal <port-list>	Specifies the port(s) to dynamically join this VLAN group using GVRP
	untagged <port-list>	Specifies the port(s) you don't want to tag all outgoing frames transmitted with this VLAN Group ID.

## 40.10 mvr Commands

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

**Table 99** Command Summary: mvr Commands

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

**Table 99** Command Summary: mvr Commands (continued)

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

# CHAPTER 41

## Command Examples

This chapter describes some commands in more detail.

### 41.1 Overview

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

### 41.2 show Commands

These are the commonly used `show` commands.

#### 41.2.1 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 159** show system-information Command Example

```
ras> show system-information

System Name           :
System Contact        :
System Location       :
Ethernet Address      : 00:13:49:1c:a2:9f
ZyNOS F/W Version     : V3.60(TS.2) | 10/11/2005
RomRasSize            : 3430448
System up Time        :      3:18:31 (122ce8 ticks)
Bootbase Version      : V3.0 | 04/08/2005

ras>
```

## 41.2.2 show hardware-monitor

Syntax:

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

This command displays the current hardware status (such as temperature and voltage levels). The following figure shows an example using degree Celsius as the temperature unit.

**Figure 160** show hardware-monitor Command Example

```
ras> show hardware-monitor c
Temperature Unit : (c)
Temperature      Current  MAX    MIN    Threshold  Status
MAC              33.0   34.0   32.0    65.0      Normal
CPU              32.0   32.0   31.0    65.0      Normal
PHY              37.0   37.5   35.5    65.0      Normal

FAN Speed (RPM) Current  MAX    MIN    Threshold  Status
FAN1             5958   6009   5908    4500      Normal
FAN2             6061   6114   6009    4500      Normal
FAN3             6222   6222   6114    4500      Normal
FAN4             6061   6114   6009    4500      Normal

Voltage (V)      Current  MAX    MIN    Threshold  Status
2.5              2.576   2.576   2.576   +/-5%      Normal
1.25             1.216   1.216   1.216   +/-10%     Normal
3.3              3.360   3.360   3.344   +/-5%      Normal
12               12.220  12.281  12.220  +/-10%     Normal
5                5.080   5.080   5.080   +/-5%      Normal
1.3              1.328   1.328   1.328   +/-5%      Normal
1.25             1.248   1.248   1.248   +/-5%      Normal
ras>
```

## 41.2.3 show ip

Syntax:

```
show ip
```

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

The following figure shows the default interface settings.

**Figure 161** show ip Command Example

```

ras> show ip
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>

```

## 41.2.4 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 162** show logging Command Example

```

ras# show logging
 0 Thu Jan  1 00:00:11 1970 PP2b  INFO  adjtime task pause 1 day
 7 Thu Jan  1 01:06:26 1970 PP23  ERROR ospfReadConf: can't get spOSPFArea_t
10 Thu Jan  1 01:06:38 1970 PP23  ERROR ospfReadConf: can't get spOSPFArea_t
13 Thu Jan  1 01:06:50 1970 PP23  ERROR ospfReadConf: can't get spOSPFArea_t
16 Thu Jan  1 01:07:05 1970 PP23  ERROR ospfReadConf: can't get spOSPFArea_t
20 Thu Jan  1 00:00:04 1970 PP0c -WARN  SNMP TRAP 3: link up
21 Thu Jan  1 00:00:06 1970 PINI -WARN  SNMP TRAP 1: warm start
22 Thu Jan  1 00:00:06 1970 PINI -WARN  SNMP TRAP 3: link up
22 Thu Jan  1 00:00:06 1970 PINI -WARN  SNMP TRAP 3: link up
24 Thu Jan  1 00:00:07 1970 PP23  ERROR ospfReadConf: can't get spOSPFArea_t
25 Thu Jan  1 00:00:11 1970 PP2b  INFO  adjtime task pause 1 day
30 Thu Jan  1 00:00:04 1970 PP0c -WARN  SNMP TRAP 3: link up
31 Thu Jan  1 00:00:06 1970 PINI -WARN  SNMP TRAP 1: warm start
32 Thu Jan  1 00:00:06 1970 PINI -WARN  SNMP TRAP 3: link up
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.

## 41.2.5 show interface

Syntax:

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

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

**Figure 163** show interface Command Example

```

ras# show interface 2
  Port Info   Port NO.           :2
              Link           :100M/F
              Statuss        :FORWARDING
              LACP            :Disabled
              TxPkts          :2778
              RxPkts          :2043
              Errors          :0
              Tx KBs/s        :0.0
              Rx KBs/s        :0.0
              Up Time         :   4:29:36
TX Packet     Tx Packets      :2778
              Multicast      :0
              Broadcast       :542
              Pause           :0
              Tagged           :0
RX Packet     Rx Packets      :2043
              Multicast      :0
              Broadcast       :256
              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             :2355
              65 to 127      :463
              128 to 255     :435
              256 to 511     :593
              512 to 1023    :154
              1024 to 1518   :821
              Giant          :0
ras#

```

## 41.2.6 show mac address-table

Syntax:

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

Where

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

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

**Figure 164** show mac address-table Command Example

```

ras# show mac address-table static
  Vid           Mac Port           Status
  1 01:a0:c5:aa:aa:aa    1      Permanent
  2 00:50:ba:ad:4f:81    1      Permanent
  1 00:a0:c5:fe:ea:71   CPU      Permanent
  2 00:a0:c5:fe:ea:71   CPU      Permanent
ras#

```

## 41.3 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 165** 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#

```



## 41.4 traceroute

Syntax:

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

where

<ip>	=	The IP address of an Ethernet device.
[in-band out-of-band vlan <vlan-id> ]	=	Specifies the network interface or the VLAN ID to which the Ethernet device belongs.
[ttl <1-255>]	=	Specifies the Time To Live (TTL) period.
[wait <1-60>]	=	Specifies the time period to wait.
[queries <1-10>]	=	Specifies how many tries the switch performs the traceroute function.

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

**Figure 166** 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:
```

## 41.5 Enabling RSTP

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

The following example enables RSTP on port 10.

**Figure 167** Enable RSTP Command Example

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

## 41.6 Configuration File Maintenance

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

### 41.6.1 Configuration Backup

Syntax:

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

where

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

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

**Figure 168** CLI: Backup Configuration Example

```
ras# copy running-config tftp 172.23.19.96 test.cfg
Backupping
. (683)Bytes Done!
ras#
```

### 41.6.2 Configuration Restoration

Syntax:

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

where

- <index> = Specifies to restore which configuration file (1 or 2) on the switch.
- <ip> = The IP address of a TFTP server from which you want to get the backup configuration file.
- <remote-file> = Specified the name of the configuration file.

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

**Figure 169** CLI: Restore Configuration Example

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

### 41.6.3 Using a Different Configuration File

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

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

**Figure 170** 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 171** 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.

### 41.6.4 Resetting to the Factory Default

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

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

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

**Figure 172** CLI: Reset to the Factory Default Example

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

## 41.7 no Command Examples

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

### 41.7.1 no mirror-port

Syntax:

```
no mirror-port
```

Disables port mirroring on the switch.

An example is shown next.

**Figure 173** no mirror-port Command Example

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

### 41.7.2 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 174** no https timeout Command Example

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

### 41.7.3 no trunk

Syntax:

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

where

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

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

**Figure 175** no trunk Command Example

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

### 41.7.4 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 176** 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

```

## 41.7.5 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 177** 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

```

## 41.8 interface Commands

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

## 41.8.1 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 178** interface Command Example

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

## 41.8.2 interface route-domain

Syntax:

```
interface route-domain <ip-address>/<mask-bits>
```

where

- <ip-address> = This is the IP address of the switch in the routing domain. Specify the IP address in dotted decimal notation. For example, 192.168.1.1.
- <mask-bits> = The number of bits in the subnet mask. Enter the subnet mask number preceded with a "/". To find the bit number, convert the subnet mask to binary and add all of the 1's together. Take "255.255.255.0" for example. 255 converts to eight 1's in binary. There are three 255's, so add three eights together and you get the bit number (24).

Use this command to enable/create the specified routing domain for configuration.

An example is shown next.

- Enter the configuration mode.
- Enable default routing domain (the 192.168.1.1 subnet) for configuration.
- Begin configuring for this domain.

**Figure 179** interface Command Example

```

ras# config
ras(config)# interface route-domain 192.168.1.1/24
cmd interface route domain
  192.168.1.1 255.255.255.0
ras(config-if)#

```

### 41.8.3 bpdu-control

Syntax:

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

where

`peer|tunnel|discard|network` = Type `peer` to process any BPDUs received on these ports.

Type `tunnel` to forward BPDUs received on these ports.

Type `discard` to drop any BPDUs received on these ports.

Type `network` to process and forward BPDUs with a VLAN tag and to process untagged BPDUs.

An example is shown next.

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

**Figure 180** interface bpdu-control Command Example

```

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

```

### 41.8.4 broadcast-limit

Syntax:

```

broadcast-limit
broadcast-limit <pkt/s>

```



where

Enables broadcast storm control limit on the switch.

<pkt/s> Sets how many broadcast packets the interface receives per second.

An example is shown next.

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

**Figure 181** broadcast-limit Command Example

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

## 41.8.5 bandwidth-limit

Syntax:

```
bandwidth-limit
bandwidth-limit egress <Mbps>
bandwidth-limit ingress <Mbps>
```

where

Enables bandwidth control on the switch.

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

An example is shown next.

- Enable port one for configuration.
- Enable bandwidth control.
- Set the outgoing traffic bandwidth limit to 7Mbps.
- Set the incoming traffic bandwidth limit to 9Mbps.

**Figure 182** bandwidth-limit Command Example

```
ras(config)# interface port-channel 1
ras(config-interface)# bandwidth-limit
ras(config-interface)# bandwidth-limit egress 7
ras(config-interface)# bandwidth-limit ingress 9
```

## 41.8.6 mirror

Syntax:

```
mirror
mirror dir <ingress|egress|both>
```

where

Enables port mirroring on the interface.

<ingress|egress|both> = Enables port mirroring for incoming, outgoing or both incoming and outgoing traffic.

Port mirroring copies traffic from one or all ports to another or all ports for external analysis.

An example is shown next.

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

**Figure 183** mirror Command Example

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

## 41.8.7 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 184** gvrp Command Example

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

### 41.8.8 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 185** ingress-check Command Example

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

### 41.8.9 frame-type

Syntax:

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

where

<all|tagged> 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 186** frame-type Command Example

```

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

```

### 41.8.10 spq

Syntax:

```
spq
```

Sets the interface to use Strict Priority Queuing.

An example is shown next.

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

**Figure 187** spq Command Example

```

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

```

### 41.8.11 wrr

Syntax:

```
wrr <wt1> <wt2> ... <wt8>
```

where

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

<wt1> <wt2> ... Sets the interface to use WRR queuing. A weight value of one to eight is given to each variable from wt1 to wt8.

An example is shown next.

- Enable port two and ports six to twelve for configuration.
- Enable Weighted Round Robin queuing on the ports.
- Set the queue weights from Q0 to Q7.

**Figure 188** wrp Command Example

```
ras# configure
ras(config)# interface port-channel 2,6-12
ras(config-interface)# wrp
ras(config-interface)# wrp 8 7 6 5 4 3 2 1
```

### 41.8.12 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 189** 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
```

### 41.8.13 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 190** qos priority Command Example

```

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

```

### 41.8.14 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 191** name Command Example

```

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

```

### 41.8.15 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 10 Mbps in half duplex mode.

**Figure 192** speed-duplex Command Example

```

ras(config)# interface port-channel 1,3-5
ras(config-interface)# speed-duplex 10-half

```



# CHAPTER 42

## IEEE 802.1Q Tagged VLAN Commands

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

### 42.1 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.

### 42.2 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).

#### 42.2.1 Static Entries (SVLAN Table)

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



## 42.2.2 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.

## 42.3 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 193** 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 194** CPU VLAN Configuration and Activation Example

```

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

```

## 42.4 Global VLAN1Q Tagged VLAN Configuration Commands

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

### 42.4.1 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 195** GARP STATUS Command Example

```

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

```

### 42.4.2 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 196** GARP Timer Command Example

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

### 42.4.3 GVRP Timer

Syntax:

```
show vlan1q gvrp
```

This command shows the switch's GVRP settings.

An example is shown next.

**Figure 197** GVRP Status Command Example

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

### 42.4.4 Enable GVRP

Syntax:

```
vlan1q gvrp
```

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

### 42.4.5 Disable GVRP

Syntax:

```
no vlan1q gvrp
```

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

## 42.5 Port VLAN Commands

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

### 42.5.1 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 198** vlan1q port default vid Command Example

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

### 42.5.2 Set Acceptable Frame Type

Syntax:

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

where

<all|tagged> = Specifies all Ethernet frames (tagged and untagged) or only tagged Ethernet frames.

This command sets the specified port to accept all Ethernet frames or only those with an IEEE 802.1Q VLAN tag.

The following example sets ports 1 to 5 to accept only tagged frames.

**Figure 199** frame type Command Example

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

### 42.5.3 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 200** no gvrp Command Example

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

### 42.5.4 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.

#### 42.5.4.1 Modify a Static VLAN Table Example

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

**Figure 201** Modifying Static VLAN Example

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

#### 42.5.4.2 Forwarding Process Example

##### Tagged Frames

- 1 First the switch checks the VLAN ID (VID) of tagged frames or assigns temporary VIDs to untagged frames.
- 2 The switch then checks the VID in a frame's tag against the SVLAN table.
- 3 The switch notes what the SVLAN table says (that is, the SVLAN tells the switch whether or not to forward a frame and if the forwarded frames should have tags).
- 4 Then the switch applies the port filter to finish the forwarding decision. This means that frames may be dropped even if the SVLAN says to forward them. Frames might also be dropped if they are sent to a CPE (customer premises equipment) DSL device that does not accept tagged frames.

##### Untagged Frames

- 1 An untagged frame comes in from the LAN.
- 2 The switch checks the PVID table and assigns a temporary VID of 1.
- 3 The switch ignores the port from which the frame came, because the switch does not send a frame to the port from which it came. The switch also does not forward frames to "forbidden" ports.
- 4 If after looking at the SVLAN, the switch does not have any ports to which it will send the frame, it won't check the port filter.

#### 42.5.5 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 202** no vlan Command Example

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

## 42.6 Enable VLAN

Syntax:

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

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

## 42.7 Disable VLAN

Syntax:

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

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

## 42.8 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 203** show vlan Command Example

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





# CHAPTER 43

## Troubleshooting

This chapter covers potential problems and possible remedies.

### 43.1 Problems Starting Up the Switch

**Table 100** 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.

### 43.2 Problems Accessing the Switch

**Table 101** Troubleshooting Accessing the Switch

PROBLEM	CORRECTIVE ACTION
I cannot access the switch using Telnet.	Make sure the ports are properly connected. You may have exceeded the maximum number of concurrent Telnet sessions. Close other Telnet session(s) or try connecting again later. Check that you have enabled Telnet service access. If you have configured a secured client IP address, your computer's IP address must match it. Refer to the chapter on access control for details.
I cannot access the web configurator.	The administrator username is "admin". The default administrator password is "1234". The username and password are case-sensitive. Make sure that you enter the correct password and username using the proper casing. If you have changed the password and have now forgotten it, you will need to upload the default configuration file. This restores all of the factory defaults including the password. If you have configured more than one IP interface, make sure another administrator is NOT logged into the web configurator on a different IP interface using the same account. Check that you have enabled web service access. If you have configured a secured client IP address, your computer's IP address must match it. Refer to the chapter on access control for details. Your computer's and the switch's IP addresses must be on the same subnet. See the following section to check that pop-up windows, JavaScripts and Java permissions are allowed.

## 43.2.1 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.

### 43.2.1.1 Internet Explorer Pop-up Blockers

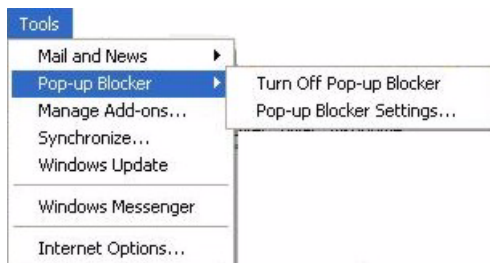
You may have to disable pop-up blocking to log into your device.

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.

#### 43.2.1.1.1 Disable pop-up Blockers

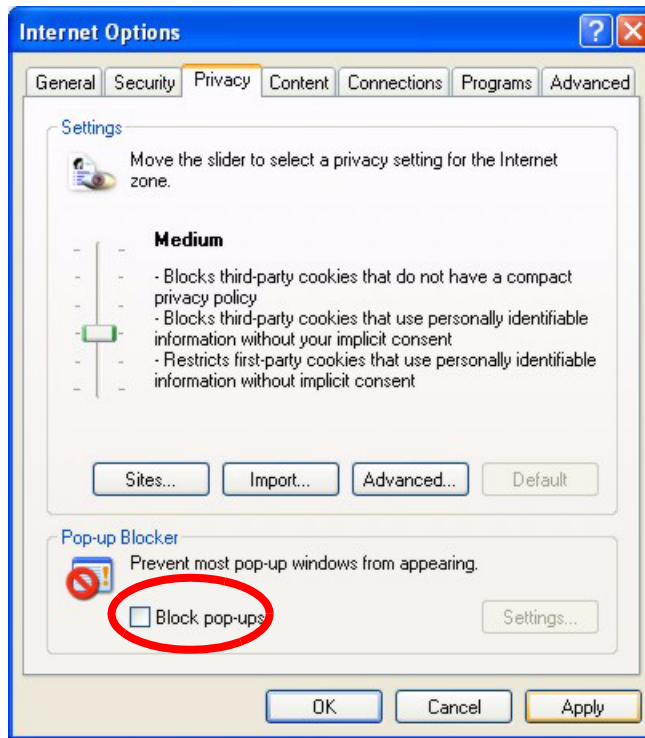
- 1 In Internet Explorer, select **Tools, Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

**Figure 204** 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.

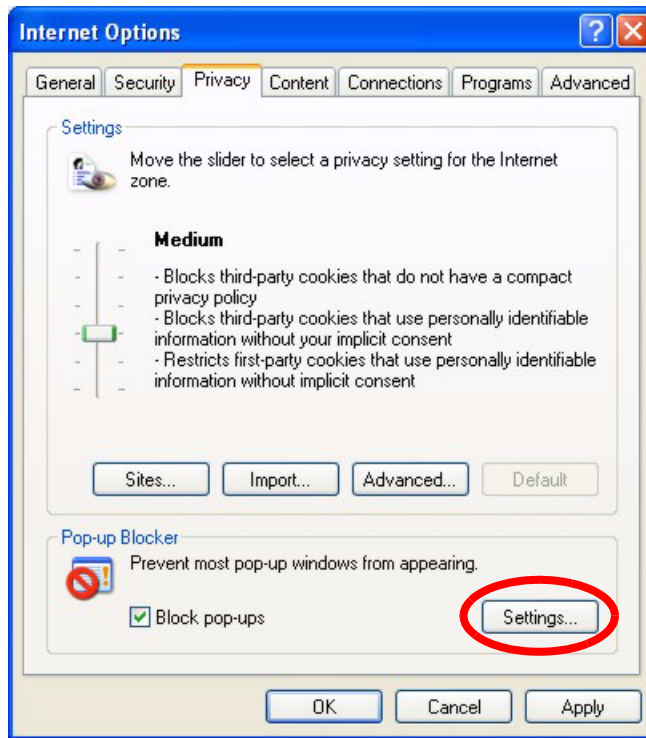
**Figure 205** Internet Options

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

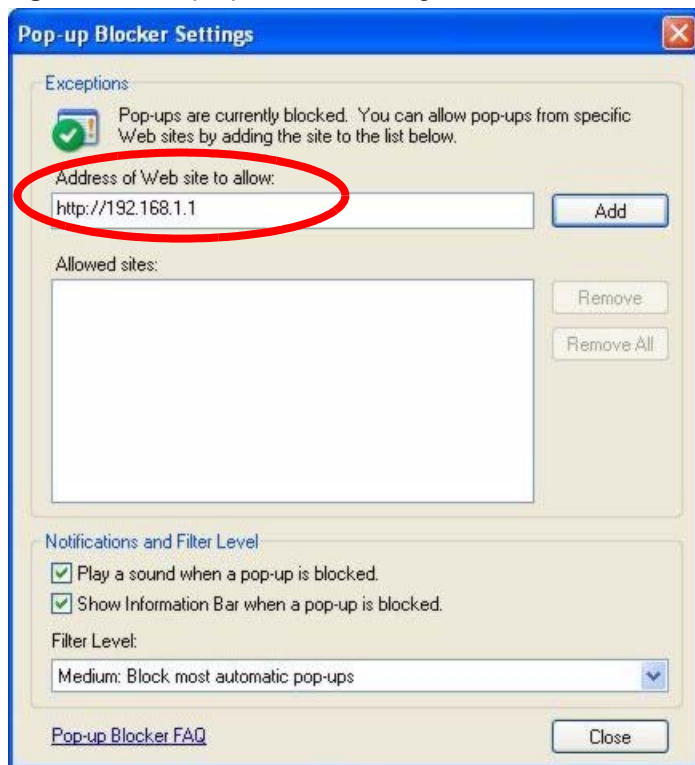
#### 43.2.1.1.2 Enable pop-up Blockers with Exceptions

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 206** 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 207** Pop-up Blocker Settings

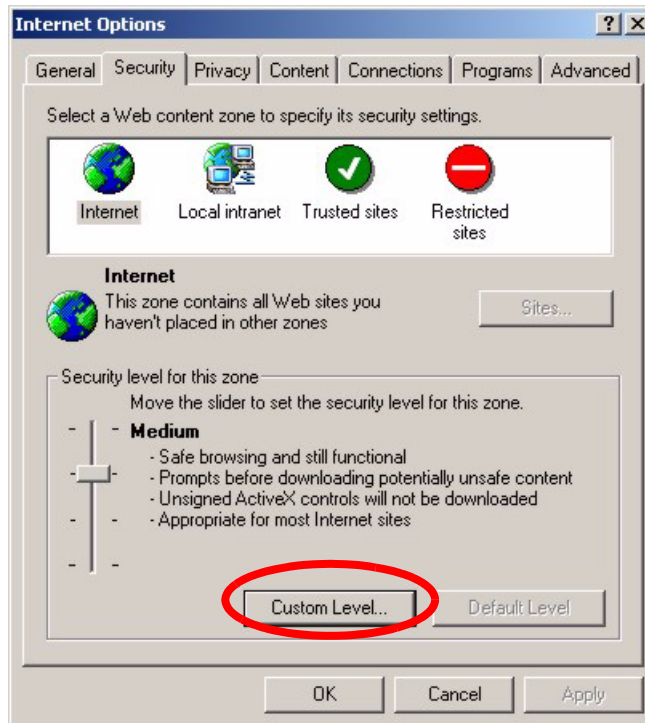
**5** Click **Close** to return to the **Privacy** screen.

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

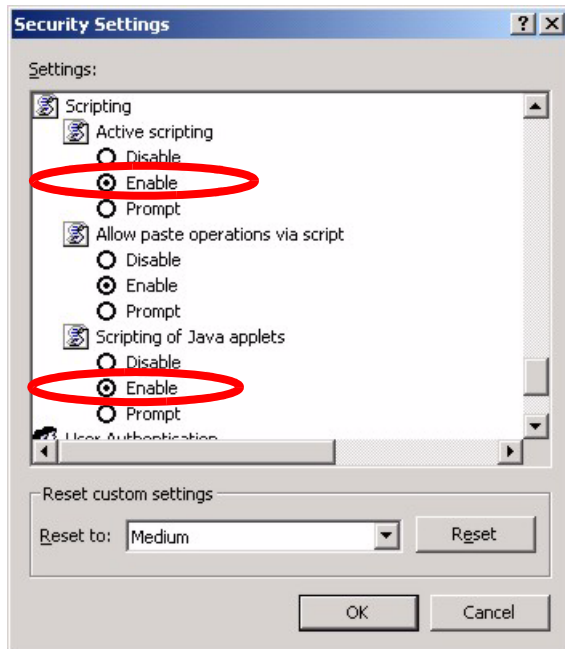
### 43.2.1.2 JavaScripts

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 208** Internet Options

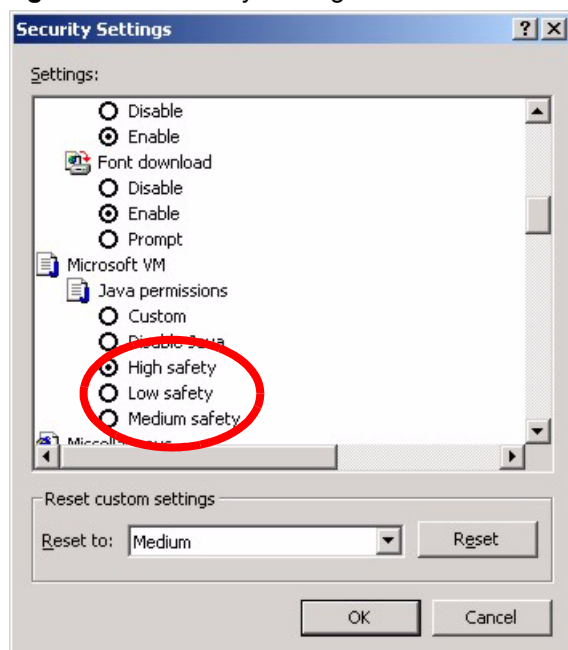
- 2** Click the **Custom Level...** button.
- 3** Scroll down to **Scripting**.
- 4** Under **Active scripting** make sure that **Enable** is selected (the default).
- 5** Under **Scripting of Java applets** make sure that **Enable** is selected (the default).
- 6** Click **OK** to close the window.

**Figure 209** Security Settings - Java Scripting

### 43.2.1.3 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.

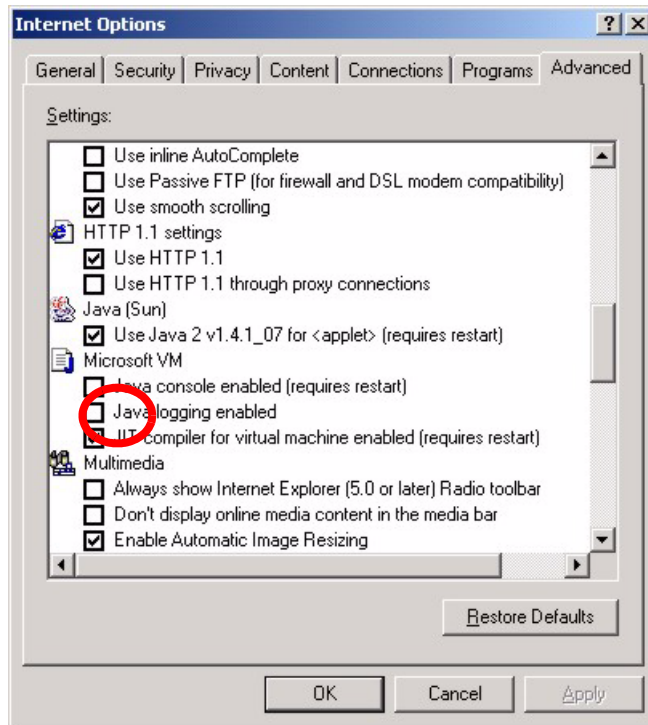


**Figure 210** Security Settings - Java

#### 43.2.1.3.1 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 211 Java (Sun)



### 43.3 Problems with the Password

Table 102 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

The following table lists the product specifications.

**Table 103** General Product Specifications

Interface		GS-4012F: 12 mini-GBIC (SFP) slots GS-4024: 24 10/100/1000 Base-Tx ports 4 Gigabit/mini-GBIC ports One local management Ethernet port Auto-negotiation Auto-MDIX Compliant with IEEE 802.3ad/u/x Back pressure flow control for half duplex Flow control for full duplex (IEEE 802.3x) RJ-45 Ethernet cable connector Rate limiting at 64Kbps steps
Layer 2 Features	Bridging	16K MAC addresses Static MAC address filtering (port lock) Broadcast storm control Limited maximum number of MAC addresses per port
	Switching	Switching fabric: 48Gbps (GS-4024)/ 24Gbps (GS-4012F), 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	IEEE 802.1d spanning tree protocol IEEE 802.1w, rapid reconfiguration to recover network failure
	QoS	IEEE 802.1p Eight priority queues Supports RFC 2475 DiffServ, DSCP to IEEE 802.1p priority mapping
	Security	IEEE 802.1x port-based authentication
	VLAN	Port-based VLAN setting Tag-based (IEEE 802.1Q) VLAN Number of VLAN: 4K Supports GVRP
	Link aggregation	Supports IEEE 802.3ad; static and dynamic (LACP) port trunking Six groups (up to 8 ports each)
	Port mirroring	All ports support port mirroring
	Bandwidth control	Supports rate limiting at 1Mbps increment Supports IGMP snooping

**Table 103** General Product Specifications (continued)

Layer 3 Features	IP forwarding	Wire-speed 8K IP address table Filtering based on the source/destination IP address
	Routing protocols	Unicast: RIP-V1/V2, OSPF V2 Multicast: DVMRP VRRP
	IP services	DHCP server/relay
Layer 4 Features	TCP/UDP port-based filtering Bandwidth management	

**Table 104** 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 ICMP packet transmission Port mirroring and aggregation Spanning Tree Protocol IGMP snooping Firmware upgrade and download through FTP/TFTP DHCP server/relay 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 address SNMP RMON groups (history, statistics, alarms and events)
MIB	RFC1213 MIB II RFC1253 OSPF MIBs RFC1493 Bridge MIB RFC1643 Ethernet MIB RFC1757 Four groups of RMON RFC2674 Bridge MIB extension

**Table 105** Physical and Environmental Specifications

LEDs	Per switch: BPS, PWR, SYS, ALM Per Gigabit Ethernet/mini-GBIC port: 100, 1000/LNK, ACT Per mini-GBIC port: LNK, ACT Per Management port: 10, 100
Dimension	Standard 19" rack mountable GS-4012F: 438 mm (W) x 225 mm (D) x 44.45 mm (H) GS-4024: 438 mm (W) x 300 mm (D) x 44.45 mm (H)
Weight	GS-4012F: 3.1 Kg GS-4024: 4.2 Kg
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 AC model:100 - 240VAC 50/60Hz 1.5A max internal universal power supply DC model: -48VDC--60VDC, 1.2A Max.
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 106** 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 107** 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 108** “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 109** 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 110** 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 111** Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	<b>00000000</b>
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	<b>10000000</b>
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 112** Subnet 2

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	<b>10000000</b>
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	<b>10000000</b>
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 113** 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 114** 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 115** 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 116** 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 117** 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	225	254	255

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

**Table 118** 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 106 on page 312](#)) available for subnetting.

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

**Table 119** 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 [110](#)

## Numerics

802.1P priority [83](#)

## A

Access control [206](#)  
 Access priority [206](#)  
 Limitation [206](#)  
 Login account [209](#)  
 Remote management [217](#)  
 Service port [217](#)  
 SNMP [207](#)

Address Resolution Protocol (ARP) [232](#)

Administrator password [210](#)

Aggregator ID [112](#)

Aging time [78](#)

Alternative Subnet Mask Notation [314](#)

Application [36](#)  
 Backbone [36](#)  
 Bridging [37](#)  
 IEEE 802.1Q VLAN [38](#)  
 Switched workgroup [37](#)

Area 0 [160](#)

Area Border Router (ABR) [160](#)

Area ID [165](#), [168](#)

ARP [232](#)  
 How it works [232](#)  
 View [232](#)

AS Boundary Router [160](#)

Authentication [165](#), [166](#), [167](#), [168](#), [169](#)

Authority [3](#)

Automatic VLAN registration [85](#)

Autonomous system (AS) [34](#), [160](#), [174](#)

## B

Backbone [160](#)

Backbone Router (BR) [160](#)

Basic setting [72](#)

BPDUs (Bridge Protocol Data Units) [99](#)

Bridge Protocol Data Units (BPDUs) [99](#)

## C

CFI (Canonical Format Indicator) [84](#)

Change password [55](#)

Changes or Modifications [3](#)

CLI Commands [238](#)

Class of Service (CoS) [128](#), [180](#)

Classifier  
 Ethernet Type [124](#)  
 Example [126](#)  
 Packet Format [123](#)  
 View summary [125](#)

CLI Command  
 Configure tagged VLAN example [289](#)  
 Static VLAN Table example [294](#)

Cluster management [35](#), [222](#)  
 Cluster manager [222](#), [226](#)  
 Cluster member [222](#), [226](#)  
 Cluster member firmware upgrade [224](#)  
 Network example [222](#)  
 Setup [225](#)  
 Specification [222](#)  
 Status [223](#)  
 Switch models [222](#)  
 VID [226](#)  
 Web configurator [224](#)

Cluster manager [222](#)

Cluster member [222](#)

Command  
 Forwarding Process Example [294](#)  
 Summary [242](#)  
 Syntax conventions [238](#)

Command Line Interface  
 Accessing [236](#)  
 Introduction [236](#)

Configuration file [57](#)  
 Backup [201](#)  
 Restore [57](#), [201](#)



Configure QoS [122](#)  
Console port [36](#)  
  Settings [45](#)  
Copyright [2](#)  
CPU management port [91](#)  
CRC (Cyclic Redundant Check) [69](#)  
Current date [76](#)  
Current time [76](#)  
Customer Support [6](#)

## D

Database Description (DD) [161](#)  
Default gateway [186](#)  
DHCP [32](#), [184](#)  
  Client IP pool [186](#)  
  Modes [184](#)  
  Relay agent [184](#)  
  Server [184](#)  
  Setup [185](#)  
DHCP (Dynamic Host Configuration Protocol) [32](#), [184](#)  
Diagnostic [220](#)  
  Ethernet port test [220](#)  
  Ping [220](#)  
  System log [220](#)  
Differentiated Service (DiffServ) [180](#)  
DiffServ [180](#)  
  Activate [181](#)  
  DS field [180](#)  
  DSCP [180](#)  
  DSCP-to-IEEE802.1p mapping [182](#)  
  Network example [180](#)  
  PHB [180](#)  
DiffServ (Differentiated Services) [128](#)  
DiffServ Code Point (DSCP) [128](#)  
DiffServ marking rule [128](#)  
Double-tagged Frames [33](#), [138](#)  
DS (Differentiated Services) [180](#)  
DS field [128](#)  
DS See Differentiated Services  
DSCP  
  DSCP-to-IEEE802.1p mapping [182](#)  
  Service level [180](#)  
  What it does [180](#)  
DSCP (DiffServ Code Point) [180](#)  
DVLAN Table [288](#)  
DVMRP  
  Autonomous system [34](#), [174](#)  
  Default timer setting [177](#)  
  Error message [176](#)  
  Graft [175](#)

  How it works [174](#)  
  Implementation [174](#)  
  Probe [175](#)  
  Prune [175](#)  
  Report [175](#)  
  Setup [175](#)  
  Terminology [175](#)  
  Threshold [176](#)  
DVMRP (Distance Vector Multicast Routing Protocol) [34](#),  
[174](#)  
Dynamic link aggregation [110](#)

## E

Egress port [93](#)  
Ethernet broadcast address [232](#)  
Ethernet port test [220](#)  
Ethernet ports  
  Default settings [45](#)  
Extended authentication protocol [116](#)  
External authentication server [116](#)

## F

Fan speed [74](#)  
FCC  
  Compliance [3](#)  
Feature  
  Hardware [35](#)  
File Transfer using FTP  
  command example [203](#)  
Filename convention [203](#)  
Filtering [96](#)  
Filtering database [228](#)  
Firmware [73](#)  
  Upgrade [200](#), [224](#)  
Flow control [82](#)  
  Back pressure [82](#)  
  IEEE802.3x [82](#)  
Front panel [44](#)  
FTP [203](#)  
  File transfer procedure [204](#)  
  Restrictions over WAN [205](#)

## G

GARP [85](#), [289](#)

GARP (Generic Attribute Registration Protocol) [85](#)  
 garp status [290](#)  
 GARP Status Command [290](#)  
 GARP timer [78, 85](#)  
 General setup [74](#)  
 Getting help [58](#)  
 Gigabit Ethernet ports [45](#)  
 GMT (Greenwich Mean Time) [76](#)  
 GVRP [85, 90, 91, 289](#)  
 GVRP (GARP VLAN Registration Protocol) [85, 282](#)  
 gvrp disable [292](#)  
 gvrp enable [291](#)  
 gvrp status [291](#)

## H

Hardware installation [40](#)  
 Hardware monitor [73](#)  
 Hardware overview [44](#)  
 Host IDs [312](#)  
 How SSH works [211](#)  
 HTTP [126](#)  
 HTTPS [212](#)  
 HTTPS Example [213](#)

## I

IEEE 802.1p [78](#)  
 IEEE 802.1Q Tagged VLAN [288](#)  
 IEEE 802.1x [116](#)  
   Activate [117](#)  
   Note [116](#)  
   Reauthentication [117](#)  
 IGMP [34, 172, 174](#)  
   Setup [172](#)  
   Version [172](#)  
 IGMP snooping [77, 144](#)  
 Ingress port [93](#)  
 Installation  
   Freestanding [40](#)  
   Precautions [41](#)  
   Rack-mounting [41](#)  
 Interface [161, 162, 167](#)  
 Internal Router (IR) [160](#)  
 Introduction [32](#)  
 IP Addressing [312](#)  
 IP Classes [312](#)

IP interface [79, 192](#)  
 IP Ports [126](#)  
 IP routing domain [79](#)  
 IP setup [79](#)  
 IP table [230](#)  
   How it works [230](#)  
   View [231](#)  
 iStacking [35](#)

## K

Key [168](#)

## L

LACP [110](#)  
   System priority [113](#)  
   Timeout [114](#)  
 LEDs [48](#)  
 Limit MAC address learning [121](#)  
 Link Aggregate Control Protocol (LACP) [110](#)  
 Link aggregation [35, 110](#)  
   Dynamic [110](#)  
   ID information [111](#)  
   Setup [112](#)  
   Status [112](#)  
 Link state database [161, 162](#)  
 Lockout [56](#)  
 Log [220](#)  
 Login [50](#)  
   Password [55](#)  
 Login account [209](#)  
   Administrator [210](#)  
   Non-administrator [210](#)  
   Number of [209](#)  
 Login password [210](#)  
 LSA (Link State Advertisement) [161](#)

## M

MAC (Media Access Control) [73](#)  
 MAC address [73, 232](#)  
   Maximum number per port [121](#)  
 MAC address learning [35, 78, 94, 120, 121](#)  
   Specify limit [121](#)  
 MAC table [228](#)

- How it works [228](#)
- View [229](#)
- Maintenance [200](#)
- Management Information Base (MIB) [207](#)
- Management port [93](#)
- MD5 [165](#)
- Metric [164](#)
- MIB [207](#)
  - Supported MIBs [208](#)
- Mini GBIC ports [45](#)
  - Connection speed [46](#)
  - Connector type [46](#)
  - Transceiver installation [46](#)
  - Transceiver removal [46](#)
- Modifications [3](#)
- Mounting brackets [41](#)
- MSA (MultiSource Agreement) [45](#)
- MTU (Multi-Tenant Unit) [76](#)
- Multicast delivery tree [175](#)
- Multicast router ("mrouter") [175](#)

## N

- Network management system (NMS) [207](#)
- NTP (RFC-1305) [76](#)

## O

- OSPF [34](#), [160](#)
  - Advantage [160](#)
  - Area [160](#), [165](#)
  - Area 0 [160](#)
  - Area ID [165](#), [168](#)
  - Authentication [165](#), [166](#), [167](#), [168](#), [169](#)
  - Autonomous system [160](#)
  - Backbone [160](#)
  - Configuration steps [161](#)
  - General settings [163](#)
  - How it works [161](#)
  - Interface [161](#), [162](#), [167](#)
  - Link state database [161](#), [162](#)
  - Network example [161](#)
  - Redistribute route [164](#)
  - Route cost [166](#)
  - Router ID [164](#)
  - Router types [160](#)
  - Status [162](#)
  - Stub area [160](#), [166](#)
  - Virtual link [161](#), [168](#)
- OSPF (Open Shortest Path First) [34](#), [160](#)

- OSPF vs RIP [160](#)
- Out of Profile Action [131](#)
- Out-of-profile traffic [130](#)

## P

- Password [55](#), [227](#)
- PHB (Per-Hop Behavior) [128](#), [180](#)
- Physical queue [134](#)
- Ping [220](#)
- Policy
  - Actions [130](#)
  - Example [132](#)
  - Metering [130](#)
  - View summary [131](#)
- Policy Rules [128](#)
- POP3 [126](#)
- Port authentication [116](#)
  - IEEE802.1x [117](#)
  - RADIUS server [118](#)
- Port Based VLAN Type [78](#)
- Port details [67](#)
- Port isolation [90](#), [93](#)
- Port Mirroring [262](#), [282](#)
- Port mirroring [33](#), [108](#)
- Port redundancy [110](#)
- Port security [35](#), [120](#)
  - Limit MAC address learning [121](#)
- Port setup [81](#)
- Port speed/duplex [82](#)
- Port status [66](#)
- Port VID
  - Default for all ports [263](#)
- Port VLAN trunking [86](#)
- Port-based VLAN [91](#)
  - All connected [93](#)
  - Port isolation [93](#)
  - Setting Wizard [93](#)
- Power [74](#)
  - Backup power supply connector [48](#)
  - Voltage [74](#)
- Priority [78](#)
- Priority level [78](#)
- Priority queue assignment [78](#)
- Product specification [308](#)
- PVID [91](#)

**Q**

Quality of Service (QoS) [122](#)  
 Queue priority [136](#)  
 Queue weight [135](#), [136](#)  
 Queuing [33](#), [134](#)  
 Queuing algorithm [134](#), [136](#)  
 Queuing method [134](#), [136](#)  
   Calculate [136](#)

**R**

RADIUS [116](#)  
 RADIUS (Remote Authentication Dial In User Service) [116](#)  
 RADIUS server [116](#)  
   Advantages [116](#)  
   Network example [116](#)  
   Settings [118](#)  
 Rear panel [47](#)  
 Redistribute route [164](#)  
 Related Documentation [30](#)  
 Remote management [217](#)  
   Service [218](#)  
   Trusted computers [218](#)  
 Reset [56](#)  
 Reset to factory default settings [202](#)  
 Restore configuration [56](#)  
 Return Material Authorization number (RMA) [5](#)  
 Reverse Path Forwarding (RPF) [175](#)  
 Reverse Path Multicasting (RPM) [174](#)  
 Revolutions Per Minute (RPM) [74](#)  
 Round Robin Scheduling [135](#)  
 Router ID [164](#)  
 Routing domain [79](#), [192](#)  
 Routing protocol [164](#)  
 Routing table [234](#)  
 RSTP (Rapid STP) [35](#)  
 Rubber feet [40](#)

**S**

Safety warnings [4](#)  
 Service access control [217](#)  
   Service port [217](#)  
 Service Provider Tag Protocol Identifier [140](#)  
 Service Provider's Network [138](#)

SFP (Small Form-factor Pluggable) [45](#)  
 Simple Network Management Protocol (SNMP) [207](#)  
 SNMP [207](#)  
   Agent [207](#)  
   Communities [209](#)  
   Management model [207](#)  
   Manager [207](#)  
   MIB [207](#), [208](#)  
   Network components [207](#)  
   Object variables [207](#)  
   Protocol operations [208](#)  
   Setup [209](#)  
   Traps [208](#)  
   Versions supported [207](#)  
 SP TPID [140](#)  
 Spanning Tree Protocol (STP) [98](#)  
 SPN [138](#)  
 SSH [211](#)  
 SSH Implementation [212](#)  
 Static MAC address [35](#), [94](#), [120](#)  
 Static MAC forwarding [94](#)  
 Static VLAN [88](#)  
   Control [89](#)  
   Tagging [89](#)  
 Status [51](#), [66](#)  
   LED [48](#)  
   Link aggregation [112](#)  
   OSPF [162](#)  
   Port [66](#)  
   Port details [67](#)  
   STP [99](#)  
   VLAN [87](#)  
   VRRP [191](#)  
 STP [98](#)  
   Bridge ID [100](#)  
   Bridge priority [102](#)  
   Configuration [101](#)  
   Designated bridge [99](#)  
   Forwarding Delay [102](#)  
   Hello BPDU [99](#)  
   Hello Time [100](#), [102](#)  
   How it works [99](#)  
   Max Age [100](#), [102](#)  
   Path cost [98](#), [102](#)  
   Port priority [102](#)  
   Port state [99](#)  
   Root port [99](#)  
   Status [99](#)  
   Terminology [98](#)  
 STP (Spanning Tree Protocol) [35](#)  
 Strict Priority Queuing (SPQ) [134](#)  
 Stub area [160](#), [166](#)  
 Subnet Masks [313](#)  
 Subnetting [313](#)  
 SVLAN Table [288](#)

- Switch lockout [56](#)
- Switch reset [56](#)
- Switch setup [77](#)
- Syntax Conventions [30](#)
- sys Commands
  - examples [268](#), [276](#), [278](#)
- sys log disp [270](#), [276](#), [279](#)
- sys sw mac list [271](#)
- System information [72](#)
- System log [220](#)
- System reboot [202](#)
- System up time [67](#)

## T

- Tagged VLAN [84](#)
- TCP/UDP protocol port numbers [124](#)
- Temperature [73](#)
- Time
  - Current [76](#)
  - Time zone [76](#)
  - Timeserver [76](#)
- Time (RFC-868) [76](#)
- Time service protocol [76](#)
  - Time format [76](#)
- Time To Live (TTL) [176](#)
- Time zone [76](#)
- Timeserver [76](#)
- Transceiver
  - Installation [46](#)
  - Removal [46](#)
- Trap
  - Destination [209](#)
- Traps [208](#)
- Trunk group [110](#)
- Trunking [35](#), [110](#)
- Type of Service (ToS) [180](#)

## U

- UTC (Universal Time Coordinated) [76](#)

## V

- Ventilation [40](#)

- Ventilation holes [40](#)
- VID [81](#), [84](#), [88](#), [140](#)
  - Number of possible VIDs [84](#)
  - Priority frame [84](#)
- VID (VLAN Identifier) [84](#)
- Virtual link [161](#), [168](#)
- Virtual router
  - Status [191](#)
- Virtual router (VR) [190](#)
- Virtual Router Redundancy Protocol (VRRP) [190](#)
- VLAN [76](#), [84](#)
  - Acceptable frame type [91](#)
  - Automatic registration [85](#)
  - Explicit Tagging [288](#)
  - ID [84](#)
  - ID (VID) [289](#)
  - Implicit Tagging [288](#)
  - Ingress filtering [90](#)
  - Introduction [76](#)
  - Number of VLANs [88](#)
  - Port isolation [90](#)
  - Port number [88](#)
  - Port settings [90](#)
  - Port-based VLAN [91](#)
  - Registration Information [288](#)
  - Static VLAN [88](#)
  - Status [87](#), [88](#)
  - Tagged [84](#)
  - Trunking [86](#)
  - Type [78](#), [86](#)
- VLAN (Virtual Local Area Network) [33](#), [76](#)
- VLAN Databases [288](#)
- VLAN number [81](#)
- VLAN Stacking [33](#), [138](#)
- VLAN trunking [91](#)
- vlan1q port accept [292](#)
- vlan1q port gvrp [293](#)
- vlan1q svlan active [295](#)
- vlan1q svlan delentry [294](#)
- vlan1q svlan inactive [295](#)
- vlan1q svlan list [295](#)
- vlan1q svlan setentry [293](#)
- VRID (Virtual Router ID) [191](#)
- VRRP [190](#)
  - Advertisement interval [193](#)
  - Authentication [193](#)
  - Backup router [190](#)
  - Configuration example [195](#)
  - Hello message [193](#)
  - How it works [190](#)
  - Interface setup [192](#)
  - Master router [190](#)
  - Network example [190](#), [195](#)
  - Parameter [193](#)
  - Preempt mode [193](#), [194](#)

Priority [193](#), [194](#)  
Status [191](#)  
Uplink gateway [194](#)  
Uplink status [191](#)  
Virtual IP [194](#)  
Virtual router [190](#)  
Virtual Router ID [194](#)  
VRID [191](#)

## W

Web configuration  
  Screen summary [53](#)  
Web configurator  
  Getting help [58](#)  
  Home [51](#)  
  Login [50](#)  
  Logout [57](#)  
  Navigation panel [52](#)  
Weighted Fair Queuing (WFQ)  
  Weight [136](#)  
Weighted Round Robin Scheduling (WRR) [135](#)

## Z

ZyNOS (ZyXEL Network Operating System) [203](#)  
ZyXEL Limited Warranty  
  Note [5](#)