

ES-4024A

Ethernet Switch

User's Guide

Version 3.60
8/2005

ZyXEL

Copyright

Copyright © 2005 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Interference Statements and Warnings

FCC Statement

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

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

FCC Warning

This equipment has been tested and found to comply with the limits for a Class A digital switch, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE Mark Warning:

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Taiwanese BSMI (Bureau of Standards, Metrology and Inspection) A Warning:

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

Notice 1

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Certifications

- 1 Go to www.zyxel.com

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

Registration

Register your product online for free future product updates and information at www.zyxel.com for global products, or at 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.

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 5 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 (0)4 72 52 97 97	www.zyxel.fr	ZyXEL France 1 rue des Vergers Bat. 1 / C 69760 Limonest France
		+33 (0)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		
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		
SPAIN	support@zyxel.es	+34 902 195 420	www.zyxel.es	ZyXEL Communications Alejandro Villegas 33 1º, 28043 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		

METHOD	SUPPORT E-MAIL	TELEPHONE*	WEB SITE	REGULAR MAIL
LOCATION	SALES E-MAIL	FAX	FTP SITE	
UNITED KINGDOM	support@zyxel.co.uk	+44 (0) 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 (0) 1344 303034	ftp.zyxel.co.uk	

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

Table of Contents

Copyright	1
Interference Statements and Warnings	2
ZyXEL Limited Warranty	4
Customer Support	5
Table of Contents	7
List of Figures	17
List of Tables	23
Preface	27
Chapter 1	
Getting to Know Your Switch	29
1.1 Introduction	29
1.2 Software Features	29
1.3 Hardware Features	32
1.4 Applications	33
1.4.1 Backbone Application	33
1.4.2 Bridging Example	33
1.4.3 High Performance Switched Example	34
1.4.4 IEEE 802.1Q VLAN Application Examples	34
1.4.4.1 Tag-based VLAN Example	35
1.4.4.2 VLAN Shared Server Example	35
Chapter 2	
Hardware Installation and Connection	37
2.1 Freestanding Installation	37
2.2 Mounting the ES-4024A on a Rack	38
2.2.1 Rack-mounted Installation Requirements	38
2.2.1.1 Precautions	38
2.2.2 Attaching the Mounting Brackets to the ES-4024A	38
2.2.3 Mounting the ES-4024A on a Rack	38
Chapter 3	
Hardware Overview	41
3.1 Front Panel Connection	41

3.1.1 Console Port	41
3.1.2 Ethernet Ports	42
3.1.2.1 Default Ethernet Settings	42
3.1.3 Mini GBIC Slots	42
3.1.3.1 Transceiver Installation	43
3.1.3.2 Transceiver Removal	43
3.2 Rear Panel	44
3.2.1 Power Connector	44
3.2.2 External Backup Power Supply Connector	45
3.3 Front Panel LEDs	45
3.4 Stacking Scenario Examples	46
3.5 Uplink Scenario Example	47
Chapter 4	
The Web Configurator	49
4.1 Introduction	49
4.2 System Login	49
4.3 The Status Screen	50
4.3.1 Change Your Password	54
4.4 Switch Lockout	54
4.5 Resetting the Switch	55
4.5.1 Reload the Configuration File	55
4.6 Logging Out of the Web Configurator	56
4.7 Help	56
Chapter 5	
Initial Setup Example	57
5.1 Overview	57
5.1.1 Configuring an IP Interface	57
5.1.2 Configuring DHCP Server Settings	58
5.1.3 Creating a VLAN	59
5.1.4 Setting Port VID	60
Chapter 6	
System Status and Port Statistics	63
6.1 Overview	63
6.2 Port Status Summary	63
6.2.1 Port Details	64
Chapter 7	
Basic Setting	69
7.1 Overview	69
7.2 System Information	69

7.3 General Setup	71
7.4 Introduction to VLANs	73
7.5 IGMP Snooping	73
7.6 Switch Setup Screen	74
7.7 IP Setup	75
7.7.1 IP Interfaces	76
7.8 Port Setup	77
Chapter 8	
VLAN	79
8.1 Introduction to IEEE 802.1Q Tagged VLAN	79
8.1.1 Forwarding Tagged and Untagged Frames	79
8.2 Automatic VLAN Registration	80
8.2.1 GARP	80
8.2.1.1 GARP Timers	80
8.2.2 GVRP	80
8.3 Port VLAN Trunking	81
8.4 Select the VLAN Type	81
8.5 Static VLAN	82
8.5.1 Static VLAN Status	82
8.5.2 Configure a Static VLAN	83
8.5.3 Configure VLAN Port Settings	85
8.6 Port-based VLANs	86
8.6.1 Configure a Port-based VLAN	86
Chapter 9	
Static MAC Forwarding.....	91
9.1 Overview	91
9.2 Configuring Static MAC Forwarding	91
Chapter 10	
Filtering.....	93
10.1 Overview	93
10.2 Configure a Filtering Rule	93
Chapter 11	
Spanning Tree Protocol.....	95
11.1 Overview	95
11.1.1 STP Terminology	95
11.1.2 How STP Works	96
11.1.3 STP Port States	96
11.2 STP Status	96
11.3 Configure STP	98

Chapter 12	
Bandwidth Control	101
12.1 Bandwidth Control Setup	101
Chapter 13	
Broadcast Storm Control	103
13.1 Overview	103
13.2 Broadcast Storm Control Setup	103
Chapter 14	
Mirroring	105
14.1 Overview	105
14.2 Port Mirroring Setup	105
Chapter 15	
Link Aggregation	107
15.1 Overview	107
15.1.1 Dynamic Link Aggregation	107
15.1.2 Link Aggregation ID	108
15.2 Link Aggregation Status	108
15.3 Link Aggregation Setup	109
Chapter 16	
Port Authentication	111
16.1 Overview	111
16.1.1 RADIUS	111
16.2 Port Authentication Configuration	111
16.2.1 Activate IEEE 802.1x Security	112
16.2.2 Configuring RADIUS Server Settings	113
Chapter 17	
Port Security	115
17.1 Overview	115
17.2 Port Security Setup	115
Chapter 18	
DHCP	117
18.1 Overview	117
18.1.1 DHCP modes	117
18.2 Configuring DHCP Server	117
18.2.1 DHCP Server Configuration Example	119
18.3 Configuring DHCP Relay	120
18.3.1 DHCP Relay Configuration Example	122

Chapter 19	
Access Control.....	125
19.1 Overview	125
19.2 The Access Control Main Screen	125
19.3 About SNMP	126
19.3.1 Supported MIBs	127
19.3.2 SNMP Traps	127
19.3.3 Configuring SNMP	128
19.3.4 Setting Up Login Accounts	128
19.4 Service Port Access Control	129
19.5 Remote Management	130
Chapter 20	
Classifier.....	133
20.1 Overview	133
20.2 Configuring the Classifier	133
20.3 Classifier Configuration Example	136
Chapter 21	
Differentiated Services.....	139
21.1 Overview	139
21.1.1 DSCP and Per-Hop Behavior	139
21.1.2 DiffServ Network Example	139
21.2 Activating DiffServ	140
21.3 Configuring Marking Rules	141
21.4 DSCP-to-IEEE802.1p Priority Mapping	142
21.4.1 Configuring DSCP Settings	142
Chapter 22	
Queuing Method.....	145
22.1 Overview	145
22.1.1 Strict Priority Queuing (SPQ)	145
22.1.2 Weighted Fair Queuing (WFQ)	145
22.2 Configuring Queuing	145
Chapter 23	
VRRP.....	147
23.1 Overview	147
23.2 Viewing VRRP Status	148
23.3 Configuring VRRP	149
23.3.1 IP Interface Setup	149
23.3.2 VRRP Parameters	150
23.3.2.1 Advertisement Interval	150

23.3.2.2 Priority	150
23.3.2.3 Preempt Mode	150
23.3.3 Configuring VRRP Parameters	151
23.4 VRRP Configuration Summary	152
23.5 VRRP Configuration Examples	152
23.5.1 One Subnet Network Example	152
23.5.2 Two Subnets Example	154
Chapter 24	
Static Route	157
24.1 Configuring Static Routes	157
Chapter 25	
RIP	159
25.1 Overview	159
25.2 Configuring RIP	159
Chapter 26	
IGMP	161
26.1 Overview	161
26.2 Configuring IGMP	161
Chapter 27	
DVMRP	163
27.1 Overview	163
27.2 How DVMRP Works	163
27.2.1 DVMRP Terminology	164
27.3 Configuring DVMRP	164
27.3.1 DVMRP Configuration Error Messages	165
27.4 Default DVMRP Timer Values	166
Chapter 28	
OSPF	167
28.1 Overview	167
28.1.1 OSPF Autonomous Systems and Areas	167
28.1.2 How OSPF Works	168
28.1.3 Interfaces and Virtual Links	168
28.1.4 Configuring OSPF	168
28.2 OSPF Status	169
28.3 Enabling OSPF and General Settings	170
28.4 Configuring OSPF Areas	172
28.4.1 Viewing OSPF Area Information Table	173
28.5 Configuring OSPF Interfaces	174

28.6 Configuring OSPF Virtual Links	175
Chapter 29	
Maintenance	177
29.1 The Maintenance Screen	177
29.2 Firmware Upgrade	177
29.3 Restore a Configuration File	178
29.4 Backing Up a Configuration File	178
29.5 Load Factory Defaults	179
29.6 Reboot System	179
29.7 FTP Command Line	180
29.7.1 Filename Conventions	180
29.7.1.1 Example FTP Commands	180
29.7.2 FTP Command Line Procedure	181
29.7.3 GUI-based FTP Clients	181
29.7.4 FTP over WAN Restrictions	182
Chapter 30	
Diagnostic.....	183
30.1 Diagnostic	183
Chapter 31	
Cluster Management.....	185
31.1 Overview	185
31.2 Cluster Management Status	186
31.2.1 Cluster Member Switch Management	187
31.2.1.1 Uploading Firmware to a Cluster Member Switch	187
31.3 Configuring Cluster Management	188
Chapter 32	
MAC Table.....	191
32.1 Overview	191
32.2 Viewing the MAC Table	192
Chapter 33	
IP Table	193
33.1 Overview	193
33.2 Viewing the IP Table	194
Chapter 34	
ARP Table	195
34.1 Overview	195
34.1.1 How ARP Works	195

34.2 Viewing ARP Table	195
Chapter 35	
Routing Table	197
35.1 Overview	197
35.2 Viewing the Routing Table	197
Chapter 36	
DHCP Server Status	199
36.1 Overview	199
36.2 Displaying DHCP Server Status	199
36.3 Displaying Detail DHCP Server Information	200
Chapter 37	
Introducing the Commands	203
37.1 Overview	203
37.1.1 Switch Configuration File	203
37.2 Accessing the CLI	203
37.2.1 Access Priority	204
37.2.2 The Console Port	204
37.2.2.1 Initial Screen	204
37.2.3 Telnet	204
37.3 The Login Screen	205
37.4 Command Syntax Conventions	205
37.5 Getting Help	205
37.5.1 List of Available Commands	206
37.5.2 Detailed Command Information	206
37.6 Command Modes	207
37.7 Using Command History	207
37.8 Saving Your Configuration	208
37.8.1 Logging Out	208
37.9 Command Summary	208
37.9.1 User Mode	209
37.9.2 Enable Mode	209
37.9.3 General Configuration Mode	212
37.9.4 interface port-channel Commands	223
37.9.5 interface route-domain Commands	225
37.9.6 config-vlan Commands	226
Chapter 38	
Command Examples	229
38.1 Overview	229
38.2 show Commands	229

38.2.1 show system-information	229
38.2.2 show hardware-monitor	230
38.2.3 show logging	230
38.2.4 show interface	231
38.2.5 show mac address-table	231
38.3 ping	232
38.4 traceroute	233
38.5 Restarting the Switch	233
38.5.1 Resetting to the Factory Default	234
38.6 no Command Examples	234
38.6.1 no mirror-port	234
38.6.2 no trunk	235
38.6.3 no port-access-authenticator	235
38.7 interface Commands	236
38.7.1 interface port-channel	236
38.7.2 interface route-domain	236
38.7.3 filter	237
38.7.4 mirror	238
38.7.5 gvrp	238
38.7.6 ingress-check	239
38.7.7 frame-type	239
38.7.8 spq	240
38.7.9 wfq	240
38.7.10 egress set	241
38.7.11 qos priority	241
38.7.12 name	242
38.7.13 speed-duplex	242
38.8 Activating RSTP on the Stacking Module	243
Chapter 39	
IEEE 802.1Q Tagged VLAN Commands	245
39.1 IEEE 802.1Q Tagged VLAN Overview	245
39.2 VLAN Databases	245
39.2.1 Static Entries (SVLAN Table)	245
39.2.2 Dynamic Entries (DVLAN Table)	246
39.3 Configuring Tagged VLAN	246
39.4 Global VLAN1Q Tagged VLAN Configuration Commands	247
39.4.1 GARP Status	247
39.4.2 GARP Timer	247
39.4.3 GVRP Timer	248
39.4.4 Enable GVRP	248
39.4.5 Disable GVRP	249
39.5 Port VLAN Commands	249

39.5.1 Set Port VID	249
39.5.2 Set Acceptable Frame Type	249
39.5.3 Enable or Disable Port GVRP	250
39.5.4 Modify Static VLAN	250
39.5.4.1 Modify a Static VLAN Table Example	251
39.5.4.2 Forwarding Process Example	251
39.5.5 Delete VLAN ID	251
39.6 Enable VLAN	252
39.7 Disable VLAN	252
39.8 Show VLAN Setting	252
Chapter 40	
Troubleshooting.....	255
40.1 Problems Starting Up the Switch	255
40.2 Problems Accessing the Switch	255
40.2.1 Pop-up Windows, JavaScripts and Java Permissions	256
40.2.1.1 Internet Explorer Pop-up Blockers	256
40.2.1.2 JavaScripts	259
40.2.1.3 Java Permissions	261
40.3 Problems with the Password	263
Appendix A	
Product Specifications.....	265
Appendix B	
IP Subnetting.....	269
Index.....	277

List of Figures

Figure 1 Backbone Application	33
Figure 2 Bridging Application	34
Figure 3 High Performance Switched Application	34
Figure 4 Tag-based VLAN Application	35
Figure 5 Shared Server Using VLAN Example	36
Figure 6 Attaching Rubber Feet	37
Figure 7 Attaching the Mounting Brackets	38
Figure 8 Mounting the ES-4024A on a Rack	39
Figure 9 Front Panel	41
Figure 10 Transceiver Installation Example	43
Figure 11 Installed Transceiver	43
Figure 12 Opening the Transceiver's Latch Example	44
Figure 13 Transceiver Removal Example	44
Figure 14 Rear Panel	44
Figure 15 Stacking Example 1	46
Figure 16 Stacking Example 2	47
Figure 17 Stacking Example 3	47
Figure 18 Uplink Example	48
Figure 19 Web Configurator: Login	49
Figure 20 Web Configurator Home Screen (Status)	50
Figure 21 Change Administrator Login Password	54
Figure 22 Resetting the Switch: Via the Console Port	56
Figure 23 Web Configurator: Logout Screen	56
Figure 24 Initial Setup Network Example: IP Interface	57
Figure 25 Initial Setup Network Example: VLAN	59
Figure 26 Initial Setup Network Example: Port VID	60
Figure 27 Status	63
Figure 28 Status: Port Details	65
Figure 29 System Info	70
Figure 30 General Setup	72
Figure 31 Switch Setup	74
Figure 32 IP Setup	76
Figure 33 Port Setup	77
Figure 34 Port VLAN Trunking	81
Figure 35 Switch Setup: Select VLAN Type	82
Figure 36 VLAN: VLAN Status	82
Figure 37 VLAN: Static VLAN	84
Figure 38 VLAN: VLAN Port Setting	85

Figure 39 Port Based VLAN Setup (All Connected)	87
Figure 40 Port Based VLAN Setup (Port Isolation)	88
Figure 41 Static MAC Forwarding	91
Figure 42 Filtering	93
Figure 43 Spanning Tree Protocol: Status	97
Figure 44 Spanning Tree Protocol: Configuration	98
Figure 45 Bandwidth Control	101
Figure 46 Broadcast Storm Control	103
Figure 47 Mirroring	105
Figure 48 Link Aggregation Control Protocol Status	109
Figure 49 Link Aggregation: Configuration	110
Figure 50 RADIUS Server	111
Figure 51 Port Authentication	112
Figure 52 Port Authentication: 802.1x	112
Figure 53 Port Authentication: RADIUS	113
Figure 54 Port Security	116
Figure 55 DHCP: Server	118
Figure 56 DHCP Server Network Example	119
Figure 57 DHCP Server Configuration Example	120
Figure 58 DHCP: Relay	121
Figure 59 DHCP Relay Network Example	122
Figure 60 DHCP Relay Configuration Example	123
Figure 61 Console Port Priority	125
Figure 62 Access Control	126
Figure 63 SNMP Management Model	126
Figure 64 Access Control: SNMP	128
Figure 65 Access Control: Logins	129
Figure 66 Access Control: Service Access Control	130
Figure 67 Access Control: Remote Management	130
Figure 68 Classifier	134
Figure 69 Classifier Example	137
Figure 70 DiffServ: Differentiated Service Field	139
Figure 71 DiffServ Network Example	140
Figure 72 DiffServ	140
Figure 73 DiffServ: Marking Rule Setting	141
Figure 74 DiffServ: DSCP Setting	143
Figure 75 Queuing Method	146
Figure 76 VRRP: Example 1	147
Figure 77 VRRP Status	148
Figure 78 VRRP Configuration: IP Interface	149
Figure 79 VRRP Configuration: VRRP Parameters	151
Figure 80 VRRP Configuration: Summary	152
Figure 81 VRRP Configuration Example: One Virtual Router Network	153

Figure 82 VRRP Example 1: VRRP Parameter Settings on Switch A	153
Figure 83 VRRP Example 1: VRRP Parameter Settings on Switch B	153
Figure 84 VRRP Example 1: VRRP Status on Switch A	154
Figure 85 VRRP Example 1: VRRP Status on Switch B	154
Figure 86 VRRP Configuration Example: Two Virtual Router Network	154
Figure 87 VRRP Example 2: VRRP Parameter Settings for VR2 on Switch A	155
Figure 88 VRRP Example 2: VRRP Parameter Settings for VR2 on Switch B	155
Figure 89 VRRP Example 2: VRRP Status on Switch A	155
Figure 90 VRRP Example 2: VRRP Status on Switch B	155
Figure 91 Static Routing	157
Figure 92 RIP	160
Figure 93 IGMP	161
Figure 94 How DVMRP Works	164
Figure 95 DVMRP	164
Figure 96 DVMRP: IGMP/RIP Not Set Error	165
Figure 97 DVMRP: Unable to Disable IGMP Error	165
Figure 98 DVMRP: Duplicate VID Error Message	166
Figure 99 OSPF Network Example	168
Figure 100 OSPF Status	169
Figure 101 OSPF Configuration: Activating and General Settings	171
Figure 102 OSPF Configuration: Area Setup	172
Figure 103 OSPF Configuration: Summary Table	173
Figure 104 OSPF Interface	174
Figure 105 OSPF Virtual Link	175
Figure 106 Maintenance	177
Figure 107 Firmware Upgrade	177
Figure 108 Restore Configuration	178
Figure 109 Backup Configuration	178
Figure 110 Load Factory Default: Conformation	179
Figure 111 Load Factory Default: Start	179
Figure 112 Reboot System: Confirmation	179
Figure 113 Reboot System: Start	180
Figure 114 Diagnostic	183
Figure 115 Clustering Application Example	185
Figure 116 Cluster Management: Status	186
Figure 117 Cluster Management: Cluster Member Web Configurator Screen	187
Figure 118 Example: Uploading Firmware to a Cluster Member Switch	188
Figure 119 Clustering Management Configuration	189
Figure 120 MAC Table Flowchart	191
Figure 121 MAC Table	192
Figure 122 IP Table Flowchart	193
Figure 123 IP Table	194
Figure 124 ARP Table	196

Figure 125 Routing Table Status	197
Figure 126 DHCP Server Status	199
Figure 127 DHCP Server Status Detail	200
Figure 128 Initial Console Port Screen	204
Figure 129 CLI: Login Screen	205
Figure 130 CLI Help: List of Commands: Example 1	206
Figure 131 CLI Help: List of Commands: Example 2	206
Figure 132 CLI Help: Detailed Command Information: Example 1	207
Figure 133 CLI: Help: Detailed Command Information: Example 2	207
Figure 134 CLI: History Command Example	208
Figure 135 CLI: write memory	208
Figure 136 show system-information Command Example	229
Figure 137 show hardware-monitor Command Example	230
Figure 138 show logging Command Example	231
Figure 139 show interface Command Example	231
Figure 140 show mac address-table Command Example	232
Figure 141 ping Command Example	232
Figure 142 traceroute Command Example	233
Figure 143 CLI: boot Command Example	233
Figure 144 CLI: reload config Command Example	234
Figure 145 CLI: Reset to the Factory Default Example	234
Figure 146 no mirror-port Command Example	235
Figure 147 no trunk Command Example	235
Figure 148 no port-access-authenticator Command Example	236
Figure 149 interface Command Example	236
Figure 150 interface Command Example	237
Figure 151 filter Command Example	238
Figure 152 mirror Command Example	238
Figure 153 gvrp Command Example	239
Figure 154 ingress-check Command Example	239
Figure 155 frame-type Command Example	240
Figure 156 spq Command Example	240
Figure 157 wfq Command Example	241
Figure 158 egress set Command Example	241
Figure 159 qos priority Command Example	242
Figure 160 name Command Example	242
Figure 161 speed-duplex Command Example	243
Figure 162 Tagged VLAN Configuration and Activation Example	246
Figure 163 CPU VLAN Configuration and Activation Example	247
Figure 164 GARP STATUS Command Example	247
Figure 165 GARP Timer Command Example	248
Figure 166 GVRP Status Command Example	248
Figure 167 vlan1q port default vid Command Example	249

Figure 168 frame type Command Example	250
Figure 169 no gvrp Example	250
Figure 170 Modifying Static VLAN Example	251
Figure 171 no vlan Command Example	252
Figure 172 show vlan Command Example	253
Figure 173 Pop-up Blocker	256
Figure 174 Internet Options	257
Figure 175 Internet Options	258
Figure 176 Pop-up Blocker Settings	259
Figure 177 Internet Options	260
Figure 178 Security Settings - Java Scripting	261
Figure 179 Security Settings - Java	262
Figure 180 Java (Sun)	263

List of Tables

Table 1 Front Panel	41
Table 2 Front Panel LEDs	45
Table 3 Navigation Panel Sub-links Overview	51
Table 4 Web Configurator Screen Sub-links Details	51
Table 5 Navigation Panel Links	52
Table 6 Status	64
Table 7 Status: Port Details	65
Table 8 System Info	70
Table 9 General Setup	72
Table 10 Switch Setup	74
Table 11 IP Setup	76
Table 12 Port Setup	78
Table 13 IEEE 802.1Q VLAN Terminology	80
Table 14 VLAN: VLAN Status	83
Table 15 VLAN: Static VLAN	84
Table 16 VLAN: VLAN Port Setting	85
Table 17 Port Based VLAN Setup	89
Table 18 Static MAC Forwarding	92
Table 19 Filtering	93
Table 20 STP Path Costs	95
Table 21 STP Port States	96
Table 22 Spanning Tree Protocol: Status	97
Table 23 Spanning Tree Protocol: Configuration	98
Table 24 Bandwidth Control	101
Table 25 Broadcast Storm Control	104
Table 26 Mirroring: Mirror Port Setting	106
Table 27 Trunk Groups	107
Table 28 Link Aggregation ID: Local Switch	108
Table 29 Link Aggregation ID: Peer Switch	108
Table 30 Link Aggregation Control Protocol Status	109
Table 31 Link Aggregation: Configuration	110
Table 32 Port Authentication: 802.1x	112
Table 33 Port Authentication: RADIUS	113
Table 34 Port Security	116
Table 35 DHCP: Server	118
Table 36 DHCP: Relay	121
Table 37 Access Control Overview	125
Table 38 SNMP Commands	127

Table 39 SNMP Traps	127
Table 40 Access Control: SNMP	128
Table 41 Access Control: Logins	129
Table 42 Access Control: Service Access Control	130
Table 43 Access Control: Remote Management	131
Table 44 Classifier	134
Table 45 Common Ethernet Types and Protocol Number	136
Table 46 Common IP Ports	136
Table 47 DiffServ	141
Table 48 DiffServ: Marking Rule Setting	141
Table 49 Default DSCP-IEEE802.1p Mapping	142
Table 50 DiffServ: DSCP Setting	143
Table 51 Queuing Method	146
Table 52 VRRP Status	148
Table 53 VRRP Configuration: IP Interface	150
Table 54 VRRP Configuration: VRRP Parameters	151
Table 55 VRRP Configuring: VRRP Parameters	152
Table 56 Static Routing	157
Table 57 RIP	160
Table 58 IGMP	161
Table 59 DVMRP	165
Table 60 DVMRP: Default Timer Values	166
Table 61 OSPF vs. RIP	167
Table 62 OSPF: Router Types	167
Table 63 OSPF Status	169
Table 64 OSPF Status: Common Output Fields	170
Table 65 OSPF Configuration: Activating and General Settings	171
Table 66 OSPF Configuration: Area Setup	172
Table 67 OSPF Configuration: Summary Table	173
Table 68 OSPF Interface	174
Table 69 OSPF Virtual Link	175
Table 70 Filename Conventions	180
Table 71 Diagnostic	183
Table 72 ZyXEL Clustering Management Specifications	185
Table 73 Cluster Management: Status	186
Table 74 FTP Upload to Cluster Member Example	188
Table 75 Clustering Management Configuration	189
Table 76 MAC Table	192
Table 77 IP Table	194
Table 78 ARP Table	196
Table 79 Routing Table Status	197
Table 80 DHCP Server Status	199
Table 81 DHCP Server Status Detail	200

Table 82 Command Summary: User Mode	209
Table 83 Command Summary: Enable Mode	209
Table 84 Command Summary: Configuration Mode	212
Table 85 interface port-channel Commands	223
Table 86 interface route-domain Commands	226
Table 87 Command Summary: config-vlan Commands	227
Table 88 Troubleshooting the Start-Up of Your Switch	255
Table 89 Troubleshooting Accessing the Switch	255
Table 90 Troubleshooting the Password	263
Table 91 General Product Specifications	265
Table 92 Management Specifications	266
Table 93 Physical and Environmental Specifications	267
Table 94 Classes of IP Addresses	269
Table 95 Allowed IP Address Range By Class	270
Table 96 "Natural" Masks	270
Table 97 Alternative Subnet Mask Notation	271
Table 98 Two Subnets Example	271
Table 99 Subnet 1	272
Table 100 Subnet 2	272
Table 101 Subnet 1	273
Table 102 Subnet 2	273
Table 103 Subnet 3	273
Table 104 Subnet 4	274
Table 105 Eight Subnets	274
Table 106 Class C Subnet Planning	274
Table 107 Class B Subnet Planning	275

Preface

Congratulations on your purchase of the ES-4024A Ethernet Switch.

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



Note: Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

About This User's Guide

This manual is designed to guide you through the installation and configuration of your ES-4024A for its various applications.










Related Documentation

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

Syntax Conventions

- “Enter” means for you to type one or more characters. “Select” or “Choose” means for you to use one of the predefined choices.
- Command and arrow keys are enclosed in square brackets. [ENTER] means the Enter, or carriage return key; [ESC] means the Escape key and [SPACE BAR] means the Space Bar.
- Mouse action sequences are denoted using a comma. For example, “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 ES-4024A Ethernet Switch may be referred to as “the ES-4024A” or “the switch” in this User's Guide.

Graphics Icons Key

ES-4024A 	Computer 	Server 
Computer 	DSLAM 	Gateway 
Central Office/ ISP 	Internet 	Hub/Switch 

User Guide Feedback

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

CHAPTER 1

Getting to Know Your Switch

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

1.1 Introduction

The ES-4024A is a stand-alone layer-3 Ethernet switch with 24 10/100Mbps ports, two Gigabit/mini-GBIC ports and one built-in stacking module.

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.

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

You can configure a classifier to categorize traffic flow and then 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 Fair Queuing (WFQ). 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.

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 Routing 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.

Ethernet Ports

The ports allow the switch to connect to another Ethernet devices.

Gigabit Ethernet Ports

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

Mini-GBIC Slots

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

Console Port

Use the console port for local management of the switch.

Stacking Module

The built-in stacking module with two Gigabit ports that allow you to stack up to eight switches.

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.

1.4 Applications

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

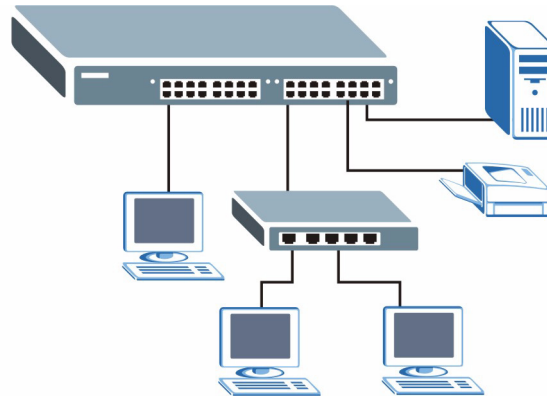
1.4.1 Backbone Application

In this application, the switch is an ideal solution for small networks where rapid growth can be expected in the near future.

The switch can be used standalone for a group of heavy traffic users. You can connect computers directly to the switch's port or connect other switches to the switch.

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

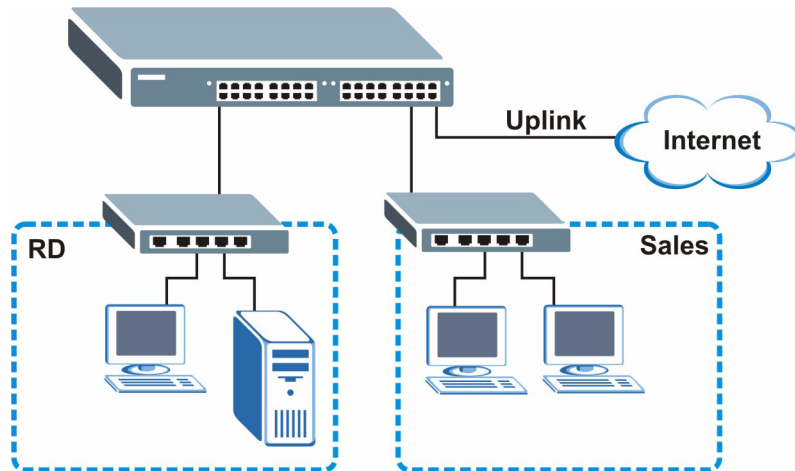
Figure 1 Backbone Application



1.4.2 Bridging Example

In this example application the switch connects different company departments (**RD** and **Sales**) to the corporate backbone. It can alleviate bandwidth contention and eliminate server and network bottlenecks. All users that need high bandwidth can connect to high-speed department servers via the switch. You can provide a super-fast uplink connection by using a Gigabit Ethernet/mini-GBIC port on the switch.

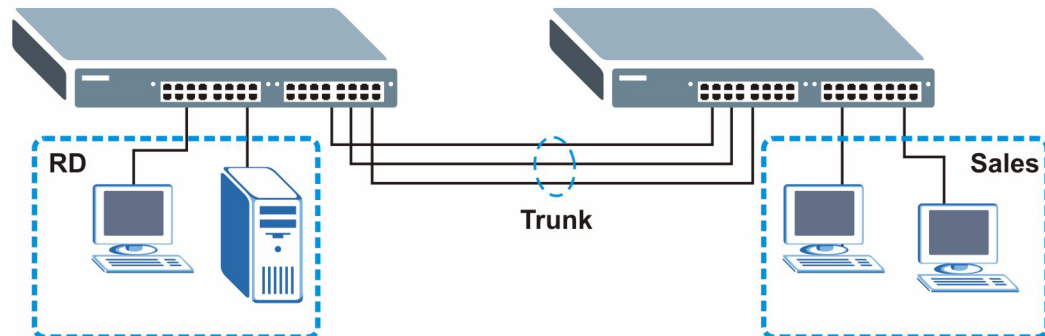
Moreover, the switch eases supervision and maintenance by allowing network managers to centralize multiple servers at a single location.

Figure 2 Bridging Application

1.4.3 High Performance Switched Example

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

Switching to higher-speed LANs such as ATM (Asynchronous Transmission Mode) is not feasible for most people due to the expense of replacing all existing Ethernet cables and adapter cards, restructuring your network and complex maintenance. The switch can provide the same bandwidth as ATM at much lower cost while still being able to use existing adapters and switches. Moreover, the current LAN structure can be retained as all ports can freely communicate with each other.

Figure 3 High Performance Switched Application

1.4.4 IEEE 802.1Q VLAN Application Examples

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

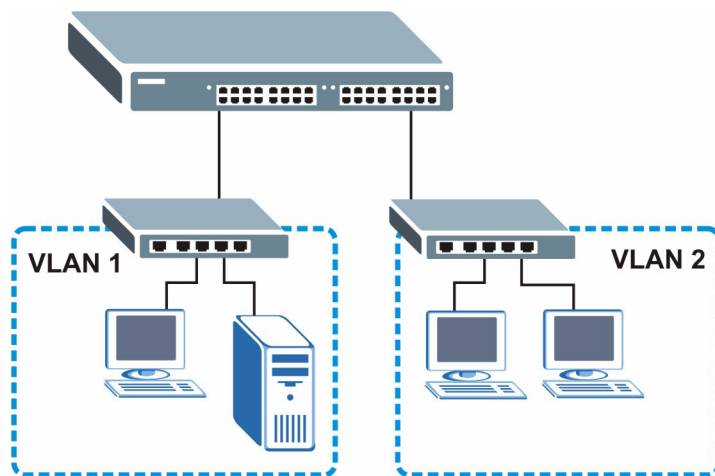
A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Stations on a logical network belong to one group. A station can belong to more than one group. With VLAN, a station cannot directly talk to or hear from stations that are not in the same group(s)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

For more information on VLANs, refer to [Chapter 8, “VLAN,” on page 79](#).

1.4.4.1 Tag-based VLAN Example

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

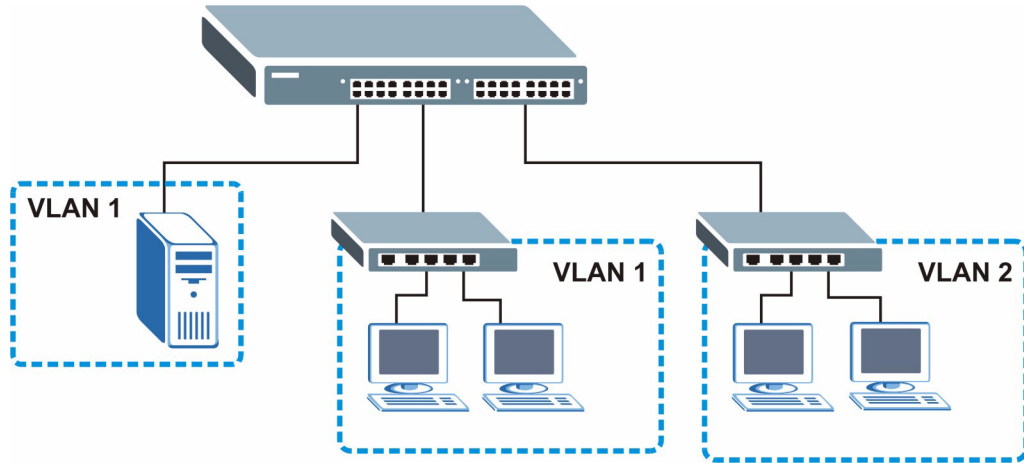
Figure 4 Tag-based VLAN Application



1.4.4.2 VLAN Shared Server Example

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

Figure 5 Shared Server Using VLAN Example



CHAPTER 2

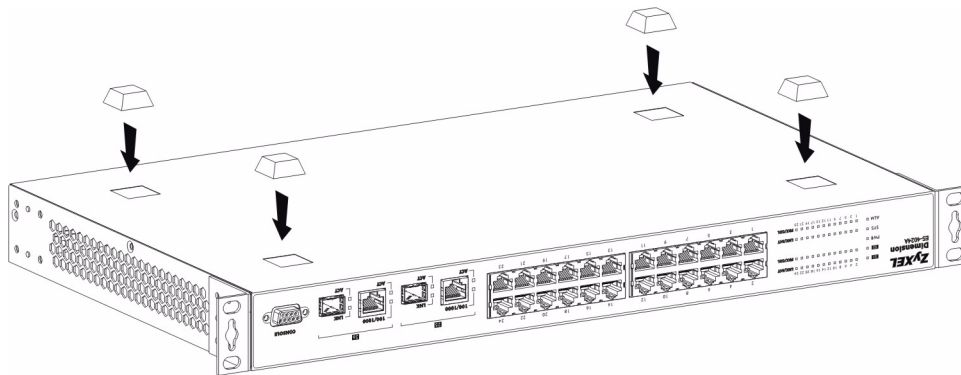
Hardware Installation and Connection

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

2.1 Freestanding Installation

- 1 Make sure the ES-4024A is clean and dry.
- 2 Set the ES-4024A on a smooth, level surface strong enough to support the weight of the ES-4024A and the connected cables. Make sure there is a power outlet nearby.
- 3 Make sure there is enough clearance around the ES-4024A 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 ES-4024A. These rubber feet help protect the ES-4024A 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 ES-4024A 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.

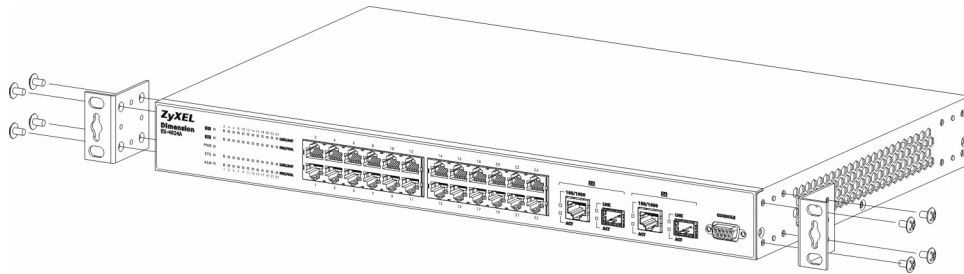
2.2.1.1 Precautions

- Make sure the rack will safely support the combined weight of all the equipment it contains.
- Make sure the position of the ES-4024A 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 ES-4024A

- 1 Position a mounting bracket on one side of the ES-4024A, lining up the four screw holes on the bracket with the screw holes on the side of the ES-4024A.

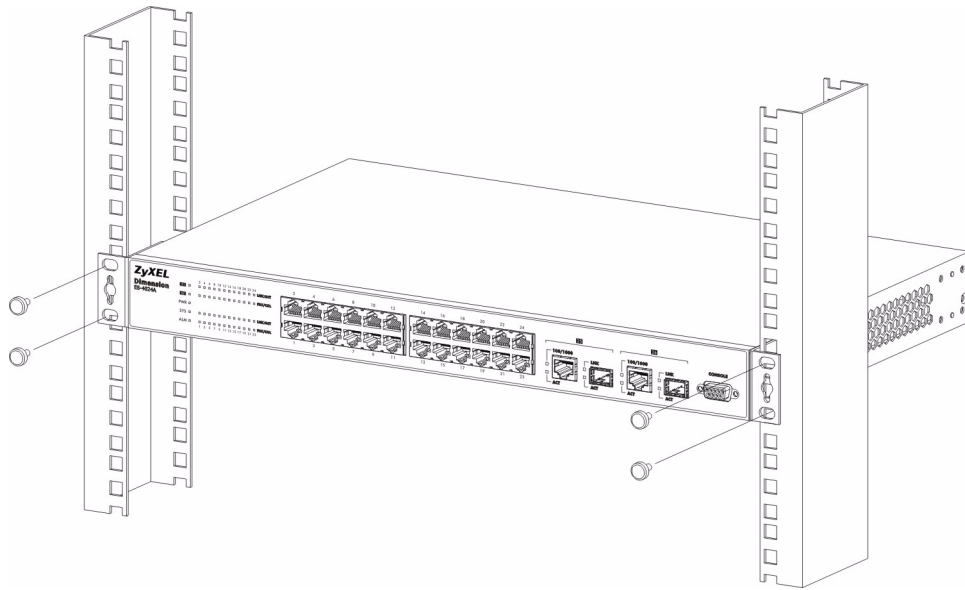
Figure 7 Attaching the Mounting Brackets



- 2 Using a #2 Philips screwdriver, install the M3 flat head screws through the mounting bracket holes into the ES-4024A.
- 3 Repeat steps 1 and 2 to install the second mounting bracket on the other side of the ES-4024A.
- 4 You may now mount the ES-4024A on a rack. Proceed to the next section.

2.2.3 Mounting the ES-4024A on a Rack

- 1 Position a mounting bracket (that is already attached to the ES-4024A) 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 ES-4024A 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

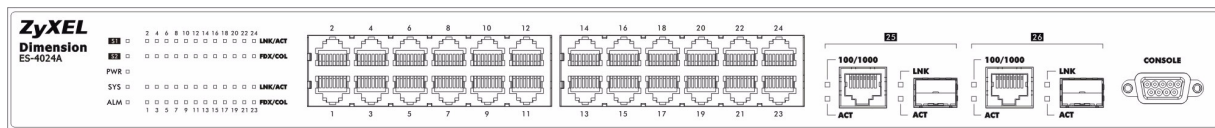
Hardware Overview

This chapter describes the front panel and rear panel of the ES-4024A and shows you how to make the hardware connections.

3.1 Front Panel Connection

The figure below shows the front panel of the ES-4024A.

Figure 9 Front Panel



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

Table 1 Front Panel

LABEL	DESCRIPTION
CONSOLE	Only connect this port if you want to configure the switch using the command line interface (CLI) via the console port.
24 10/100 Mbps RJ-45 Ethernet Ports	Connect these ports to a computer, a hub, an Ethernet switch or router.
Gigabit Ethernet/ 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

3.1.1 Console Port

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

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

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

3.1.2 Ethernet Ports

The ES-4024A has 24 10/100Mbps auto-negotiating, auto-crossover Ethernet ports. In 10/100Mbps Fast Ethernet, the speed can be 10Mbps or 100Mbps and the duplex mode can be half duplex or full duplex.

There are two pairs of Gigabit Ethernet/mini-GBIC ports. The mini-GBIC ports have priority over the Gigabit ports. This means that if a mini-GBIC port and the corresponding Gigabit port are connected at the same time, the Gigabit port will be disabled. The speed of the Gigabit Ethernet/mini-GBIC ports can be 100Mbps or 1000Mbps and the duplex mode can be half duplex (at 100 Mbps) or full duplex.

An auto-negotiating port can detect and adjust to the optimum Ethernet speed (10/100Mbps) 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 Mini GBIC Slots

These are slots for mini GBIC (Gigabit Interface Converter) transceivers. A transceiver is a single unit that houses a transmitter and a receiver. The ES-4024A 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.

There are two pairs of Gigabit Ethernet/mini-GBIC ports. The mini-GBIC ports have priority over the Gigabit ports. This means that if a mini-GBIC port and the corresponding Gigabit port are connected at the same time, the Gigabit port will be disabled.

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

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

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

3.1.3.1 Transceiver Installation

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

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

Figure 10 Transceiver Installation Example



- 2 Press the transceiver firmly until it clicks into place.
- 3 The switch automatically detects the installed transceiver. Check the LEDs to verify that it is functioning properly.

Figure 11 Installed Transceiver

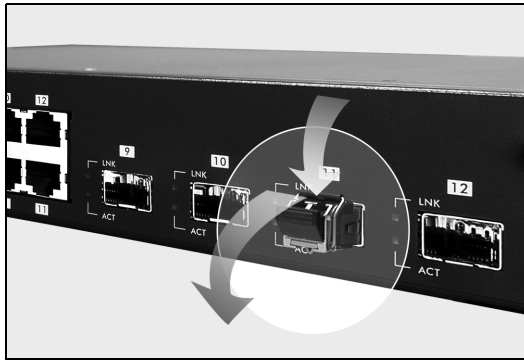


3.1.3.2 Transceiver Removal

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

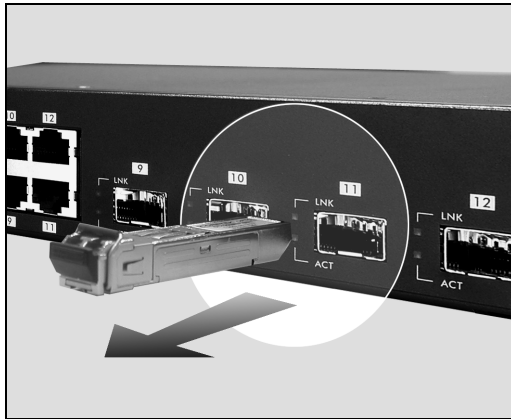
- 1 Open the transceiver's latch (latch styles vary).

Figure 12 Opening the Transceiver's Latch Example



2 Pull the transceiver out of the slot.

Figure 13 Transceiver Removal Example



3.2 Rear Panel

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

Figure 14 Rear Panel



3.2.1 Power Connector

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

To connect the power to the ES-4024A, insert the female end of power cord to the power receptacle on the rear panel. Connect the other end of the supplied power cord to a 100~240VAC/1.5A power outlet. Make sure that no objects obstruct the airflow of the fans.

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
S1 S2	Green	Blinking	The system is transmitting/receiving through the stacking port.
		On	The link through the stacking port is up.
	Off	The link through the stacking port is down.	
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.
LNK/ACT (Ethernet ports)	Green	Blinking	The system is transmitting/receiving to/from a 10 Mbps Ethernet network.
		On	The link to a 10 Mbps Ethernet network is up.
	Amber	Blinking	The system is transmitting/receiving to/from a 100 Mbps Ethernet network.
		On	The link to a 100 Mbps Ethernet network is up.
Off	The link to an Ethernet network is down.		
FDX/COL (Ethernet ports)	Amber	Blinking	The Ethernet port is negotiating in half-duplex mode and collisions are occurring; the more collisions that occur the faster the LED blinks.
		On	The Ethernet port is negotiating in full-duplex mode.
	Off	The Ethernet port is negotiating in half-duplex mode and no collisions are occurring.	

Table 2 Front Panel LEDs (continued)

LED	COLOR	STATUS	DESCRIPTION
100/1000	Green	On	The link to a 1000 Mbps Ethernet network is up.
	Amber	On	The link to a 100 Mbps Ethernet network is up.
		Off	The link to an Ethernet network is down.
ACT	Green	Blinking	The port is receiving or transmitting data.
		On	The port has a connection to an Ethernet network but not receiving or transmitting data.
		Off	The link to an Ethernet network is down.
LNK (mini GBIC Slots)	Green	On	The port has a successful connection.
		Off	No Ethernet device is connected to this port.
ACT (mini GBIC Slots)	Green	Blinking	The port is sending or receiving data.
		Off	The port is not sending or receiving data.

3.4 Stacking Scenario Examples

Use Ethernet cables when stacking the switches. See the following figures for example stacking scenarios using the stacking module. The switches must form a closed ring in all scenarios.

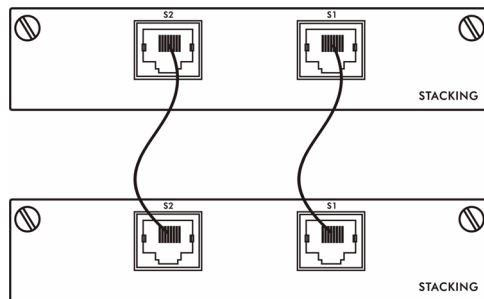
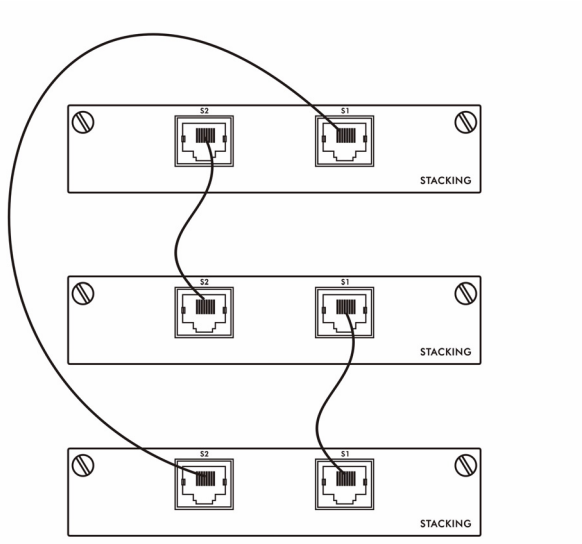
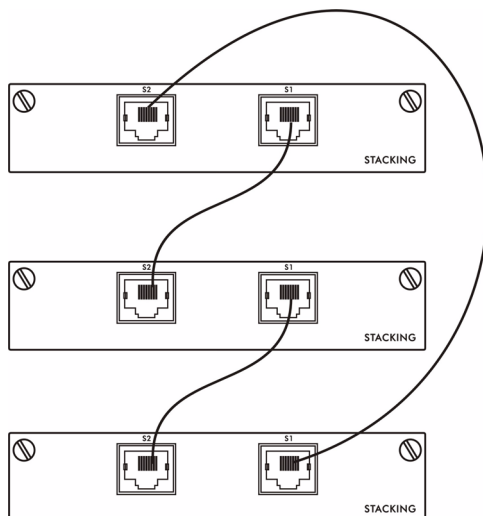
Figure 15 Stacking Example 1

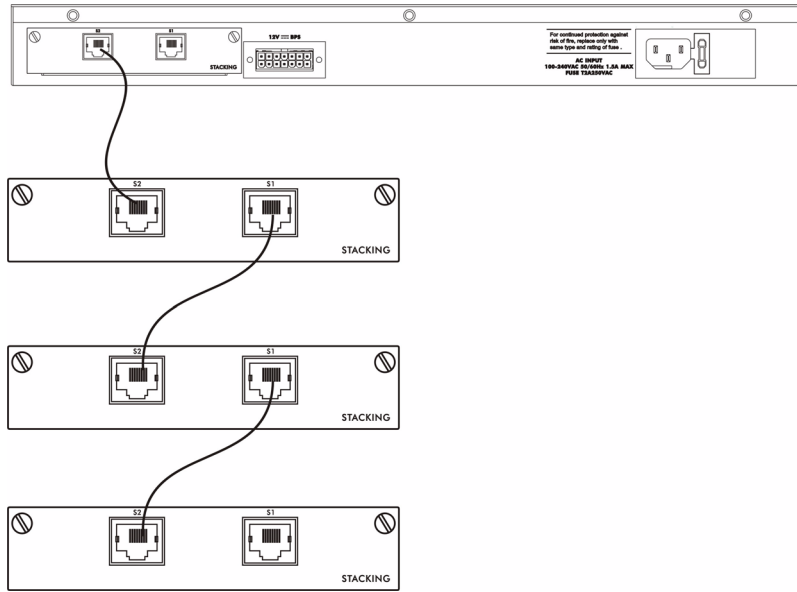
Figure 16 Stacking Example 2**Figure 17** Stacking Example 3

See the chapter on CLI for information on configuring the stacking module (as well as other ports) using line commands.

3.5 Uplink Scenario Example

Use Ethernet cables when daisy-chaining/uplinking the switches. See the following figure for an example uplink connection using the stacking module. You must uplink to a Gigabit switch using a category 5 Ethernet cable supporting Gigabit line rate when uplinking using the stacking module.

Figure 18 Uplink Example



CHAPTER 4

The Web Configurator

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

4.1 Introduction

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

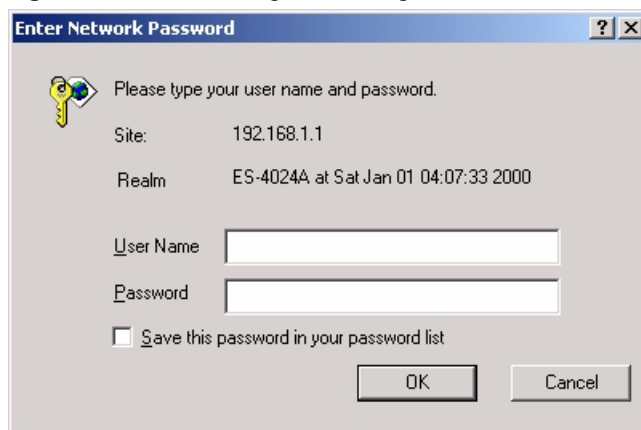
In order to use the web configurator you need to allow:

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

4.2 System Login

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

Figure 19 Web Configurator: Login



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

- A key icon on the left.
- The text "Please type your user name and password."
- Site: 192.168.1.1
- Realm: ES-4024A at Sat Jan 01 04:07:33 2000
- User Name: [text input field]
- Password: [password input field]
- Save this password in your password list
- OK and Cancel buttons at the bottom.

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 20 Web Configurator Home Screen (Status)

ZyXEL Status Logout Help

MENU
Basic Setting
Advanced Application
Routing Protocol
Management

Status
System Up Time : 0:04:01

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	100M/F	FORWARDING	Disabled	57	1273	0	13.29	4.94	0:03:08
3	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
4	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
5	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
6	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
7	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
8	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
9	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
10	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
11	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
12	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
13	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
14	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
15	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
16	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
17	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
18	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
19	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
20	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
21	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
22	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
23	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
24	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
25	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
26	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
S1	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
S2	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00

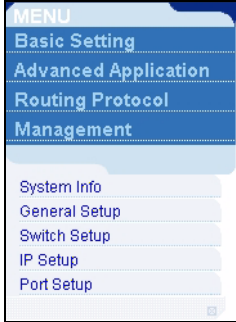

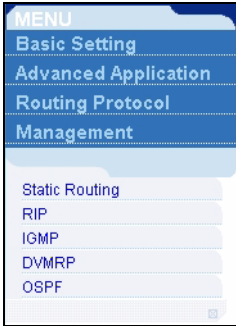
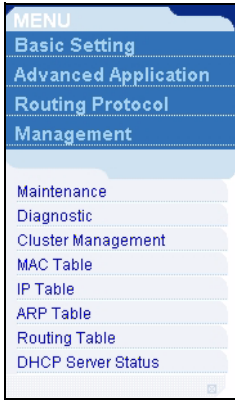
Poll Interval(s) 40 Set Interval Stop

Port ALL Clear Counter

© Copyright 1994 - 2004 by ZyXEL Communicati

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	ROUTING PROTOCOL	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	ROUTING PROTOCOL	MANAGEMENT
System Info General Setup Switch Setup IP Setup Port Setup	VLAN VLAN Status VLAN Port Setting Static VLAN Static MAC Forwarding Filtering Spanning Tree Protocol Status Spanning Tree Protocol Configuration Bandwidth Control Broadcast Storm Control Mirroring	Static Routing RIP IGMP DVMRP OSPF Status OSPF Configuration OSPF Interface OSPF Virtual Link	Maintenance Firmware Upgrade Restore Configuration Backup Configuration Load Factory Default Reboot System Diagnostic Cluster Management Status Cluster Management Configuration MAC Table

Table 4 Web Configurator Screen Sub-links Details

BASIC SETTING	ADVANCED APPLICATION	ROUTING PROTOCOL	MANAGEMENT
	Link Aggregation Link Aggregation Protocol Status Link Aggregation Port Authentication RADIUS 802.1x Port Security DHCP Access Control SNMP Logins Service Access Control Remote Management Classifier DiffServ DSCP Setting Marking Rule Setting Queuing Method VRRP Status VRRP Configuration		IP Table ARP Table Routing Table DHCP Server Status

The following table describes the links in the navigation panel.

Table 5 Navigation Panel Links

LINK	DESCRIPTION
Basic Settings	
System Info	This link takes you to a screen that displays general system and hardware monitoring information.
General Setup	This link takes you to a screen where you can configure general identification information about the switch.
Switch Setup	This link takes you to a screen where you can set up global switch parameters such as VLAN type, MAC address learning, IGMP snooping, GARP and priority queues.
IP Setup	This link takes you to a screen where you can configure the 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	

Table 5 Navigation Panel Links (continued)

LINK	DESCRIPTION
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.
DHCP	This link takes you to a screen where you can configure the DHCP settings for the network on the ES-4024A.
Access Control	This link takes you to screens where you can change the system login password and configure SNMP and remote management.
Classifier	This link takes you to a screen where you can configure the switch to group packets based on the specified criteria.
DiffServ	This link takes you to screens where you can enable DiffServ, configure marking rules and set DSCP-to-IEEE802.1p mappings.
Queuing Method	This link takes you to a screen where you can configure SPQ or WFQ with associated queue weights for each port.
VRRP	This link takes you to screens where you can configure redundant virtual router for your network.
Routing Protocol	
Static Route	This link takes you to screens where you can configure static routes. A static route defines how the ES-4024A 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.
IGMP	This link takes you to a screen where you can configure the IGMP settings.
DVMRP	This link takes you to a screen where you can configure the DVMRP (Distance Vector Multicast Routing Protocol) settings.
OSPF	This link takes you to screens where you can view the OSPF status and configure OSPF settings.
Advanced Management	

Table 5 Navigation Panel Links (continued)

LINK	DESCRIPTION
Maintenance	This link takes you to screens where you can perform firmware and configuration file maintenance as well as reboot the system.
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 in the ES-4024A.
DHCP Server Status	This link takes you to screens where you can view the general and detail DHCP server status.

4.3.1 Change Your Password

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

Figure 21 Change Administrator Login Password

The screenshot shows the 'Logins' configuration page. The 'Administrator' section has three input fields: 'Old Password', 'New Password', and 'Retype to confirm'. A red oval highlights these fields. Below them 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 the following structure:

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

At the bottom right, there are 'Apply' and 'Cancel' buttons.

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 the management VLAN (default is VLAN 1).
- 2 Deleting all IP routing domains.
- 3 Deleting all port-based VLANs with the CPU port as a member. The “CPU port” is the management port of the switch.
- 4 Filtering all traffic to the CPU port.
- 5 Disabling all ports.
- 6 Assigning minimum bandwidth to the CPU port. If you limit bandwidth to the CPU port, you may find that the switch performs sluggishly or not at all.

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 ES-4024A 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 41](#) for details.
- 2 Disconnect and reconnect the switch’s power to begin a session. When you reconnect the switch’s power, you will see the initial screen.
- 3 When you see the message “Press any key to enter Debug Mode within 3 seconds . . .” press any key to enter debug mode.
- 4 Type **atlc** after the “Enter Debug Mode” message.
- 5 Wait for the “Starting XMODEM upload” message before activating XMODEM upload on your terminal.
- 6 After a configuration file upload, type **atgo** to restart the switch.

Figure 22 Resetting the Switch: Via the Console Port

```
Bootbase Version: V1.0 | 04/25/2003 10:01:06
RAM: Size = 32768 Kbytes
FLASH: Intel 32M
ZyNOS Version: V3.50(DU.0)b6 | 07/11/2003 18:00:29
Press any key to enter debug mode within 3 seconds.
.....
Enter Debug Mode
ES-4024A> atlc
Starting XMODEM upload (CRC mode)....
CCCCCCCCCCCCCCCC
Total 262144 bytes received.
Erasing..
.....
OK
ES-4024A> atgo
```

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

4.6 Logging Out of the Web Configurator

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

Figure 23 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:

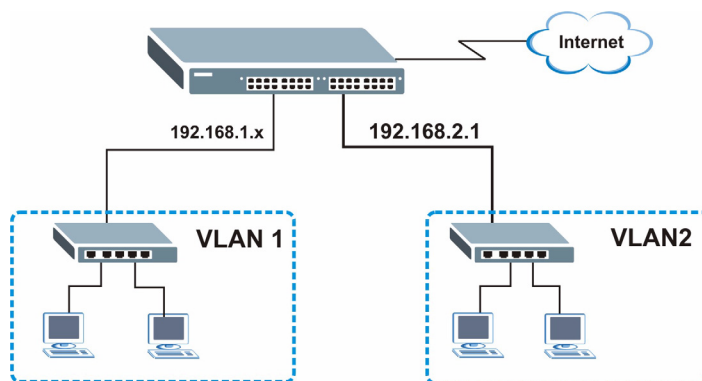
- Configure an IP interface
- Configure DHCP server settings
- Create a VLAN
- Set port VLAN ID

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 24 Initial Setup Network Example: IP Interface



- 1 Connect your computer to any Ethernet port on the switch. Make sure your computer is in the same subnet as the switch.
- 2 Open your web browser and enter 192.168.1.1 (the default IP address) in the address bar to access the web configurator. See [Section 4.2 on page 49](#) 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**.

Index	IP Address	IP Subnet Mask	VID	Delete
1	192.168.1.1	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 **Advanced Application** and **DHCP** in the navigation panel.
- 2 In the **DHCP** 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.

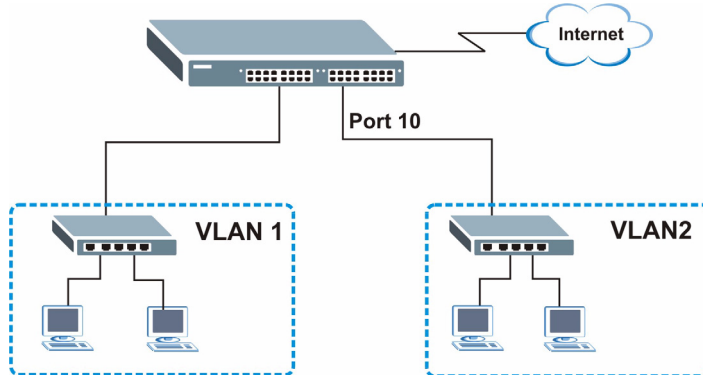
VID	Type	DHCP Status	Delete
1	Server	192.168.1.100/100	<input type="checkbox"/>

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 25 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	14	16	18	20	22	24	26	S2		
1	1	1	3	5	7	9	11	13	15	17	19	21	23	25	S1	0:27:37	Static
		U	U	U	U	U	U	U	U	U	U	U	U	U	U		
		U	U	U	U	U	U	U	U	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	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
2	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
3	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
4	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
5	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
6	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
7	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
8	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
9	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
10	<input type="radio"/> Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
11	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
12	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
13	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
26	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
31	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging
32	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging

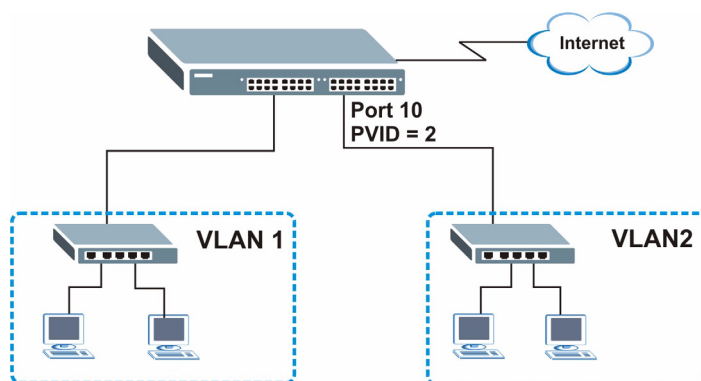
VID	Active	Name	Delete
1	Yes	1	<input type="checkbox"/>

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 26 Initial Setup Network Example: Port VID



- 1 Click **Advanced Applications** and **VLAN** in the navigation panel. Then click the **VLAN Port Setting** link.
- 2 Enter 2 in the **PVID** field for port 10 and click **Apply** to save the settings.

VLAN Port Setting VLAN Status

GVRP

Port isolation

Port	Ingress Check	PVID	GVRP	Acceptable Frame Type	VLAN Trunking
1	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
2	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
3	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
4	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
5	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
6	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
7	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
8	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
9	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
10	<input type="checkbox"/>	2	<input type="checkbox"/>	All	<input type="checkbox"/>
11	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
12	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
13	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
14	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
25	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
26	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
S1	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
S2	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>

Apply Cancel

CHAPTER 6

System Status and Port Statistics

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

6.1 Overview

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

6.2 Port Status Summary

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

Figure 27 Status

The screenshot shows the 'Status' screen with a title bar and a table of port statistics. The table has columns for Port, Link, State, LACP, TxPkts, RxPkts, Errors, Tx KB/s, Rx KB/s, and Up Time. Below the table are controls for Poll Interval (set to 40s) and Port selection (set to ALL).

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	100MF	FORWARDING	Disabled	57	1273	0	13.29	4.94	0:03:08
3	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
4	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
5	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
6	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
7	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
8	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
9	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
10	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
11	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
12	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
13	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
14	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
15	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
16	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
17	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
18	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
19	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
20	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
21	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
22	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
23	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
24	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
25	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
26	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
S1	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
S2	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00

System Up Time : 0:04:01

Poll Interval(s): 40 [Set Interval] [Stop]

Port: ALL [Clear Counter]

The following table describes the labels in this screen.

Table 6 Status

LABEL	DESCRIPTION
System up Time	This field shows how long the system has been running since the last time it was started.
Port	This identifies the Ethernet port. Click a port number to display the Port Details screen (refer to Figure 28 on page 65).
Link	This field displays the speed (either 10M for 10Mbps, 100M for 100Mbps or another value depending on the uplink module being used) and the duplex (F for full duplex or H for half duplex).
State	This field displays the STP (Spanning Tree Protocol) state of the port. See the chapter on STP for details on STP states.
LACP	This field 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 Stop to halt system statistic polling.
Clear Counter	Select a port from the Port drop-down list box and then click Clear Counter to erase the recorded statistical information for that port.

6.2.1 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 28 Status: Port Details

Port Details		Status
Port Info	Port NO.	6
	Link	100M/F
	Status	FORWARDING
	LACP	Disabled
	TxPkts	15491
	RxPkts	7784
	Errors	0
	Tx KBs/s	5.55
	Rx KBs/s	1.913
	Up Time	7:51:37
TX Packet	TX Packets	15491
	Multicast	192
	Broadcast	6258
	Pause	0
	Tagged	0
RX Packet	RX Packets	7784
	64 Byte	5676
	65-127 Byte	964
	128-255 Byte	270
	256-511 Byte	498
	512-1023 Byte	376
	1024-1518 Byte	0
	>1518 Byte	0
	Multicast	0
	Broadcast	641
	Pause	0
	Tagged	0
	Control	0
TX Collision	Single	0
	Multiple	0
	Excessive	0
	Late	0
Error Packet	RX CRC	0
	Length	0
	Alignment	0
	Runt	0
Dropped Packet	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 shows whether the Ethernet connection is down, and the speed/duplex mode.
Status	This field shows the training state of the ports. The states are FORWARDING (forwarding), which means the link is functioning normally or STOP (the port is stopped to break a loop or duplicate path).
LACP	This field shows if LACP is enabled on this port or not.
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.

Table 7 Status: Port Details (continued)

LABEL	DESCRIPTION
Rx KB/s	This field shows the number of kilobytes per second received on this port.
Up Time	This field shows the total amount of time the connection has been up.
Tx Packet The following fields display detailed information about packets transmitted.	
TX	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	This field shows the number of good packets (unicast, multicast and broadcast) received.
64	This field shows the number of packets (including bad packets) received that were 64 octets in length.
65-127	This field shows the number of packets (including bad packets) received that were between 65 and 127 octets in length.
128-255	This field shows the number of packets (including bad packets) received that were between 128 and 255 octets in length.
256-511	This field shows the number of packets (including bad packets) received that were between 256 and 511 octets in length.
512-1023	This field shows the number of packets (including bad packets) received that were between 512 and 1023 octets in length.
1024-1518	This field shows the number of packets (including bad packets) received that were between 1024 and 1518 octets in length.
>1518	This field shows the number of packets (including bad packets) transmitted that were greater than 1518 octets in length.
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.

Table 7 Status: Port Details (continued)

LABEL	DESCRIPTION
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.
Alignment	This field shows the number of packets received of proper size but with CRC error(s) and a non-integral number of octets.
Runt	This field shows the number of packets received that were too short (shorter than 64 octets), including the ones with CRC errors.
Dropped Packet	The following field indicates why packets were dropped.
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 Set Interval .
Stop	Click Stop to stop port statistic polling.

CHAPTER 7

Basic Setting

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

7.1 Overview

The **System Info** screen displays general switch information (such as firmware version number) and hardware polling information (such as fan speeds). The **General Setup** screen allows you to configure general switch identification information. The **General Setup** screen also allows you to set the system time manually or get the current time and date from an external server when you turn on your switch. The real time is then displayed in the switch logs. The **Switch Setup** screen allows you to set up and configure global switch features. The **IP Setup** screen allows you to configure a switch IP address 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 29 System Info

System Info

System Name	ES-4024A
ZyNOS F/W Version	ZyNOS F/W Version: V3.50(TV.0) 01/10/2005
Ethernet Address	00:a0:c5:00:00:01

Hardware Monitor

Temperature Unit: ▾

Temperature(C)	Current	MAX	MIN	Threshold	Status
MAC	37.0	37.0	25.0	65.0	Normal
CPU	34.5	34.5	23.5	65.0	Normal
PHY	33.5	33.5	23.5	65.0	Normal

FAN Speed (RPM)	Current	MAX	MIN	Threshold	Status
FAN1	5681	5720	5529	4500	Normal
FAN2	5529	5604	5249	4500	Normal
FAN3	5841	5967	5720	4500	Normal

Voltage (V)	Current	MAX	MIN	Threshold	Status
2.5	2.496	2.544	2.480	5	Normal
1.8	1.840	1.840	1.840	5	Normal
3.3	3.376	3.376	3.376	5	Normal
12.0	12.099	12.160	12.099	10	Normal
5.0	5.088	5.088	5.088	5	Normal
1.1	1.120	1.120	1.104	5	Normal

Poll Interval(s):

The following table describes the labels in this screen.

Table 8 System Info

LABEL	DESCRIPTION
System Name	This field displays the descriptive name of the switch for identification purposes.
ZyNOS F/W Version	This field displays the version number of the switch 's current firmware including the date created.
Ethernet Address	This field refers to the Ethernet MAC (Media Access Control) address of the switch.
Hardware Monitor	
Temperature Unit	The switch has temperature sensors that are capable of detecting and reporting if the temperature rises above the threshold. You may choose the temperature unit (Centigrade or Fahrenheit) in this field.
Temperature	MAC, CPU and PHY refer to the location of the temperature sensors on the switch printed circuit board.
Current	This 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 Normal for temperatures below the threshold and Error for those above.

Table 8 System Info (continued)

LABEL	DESCRIPTION
Fan Speed (RPM)	A properly functioning fan is an essential component (along with a sufficiently ventilated, cool operating environment) in order for the device to stay within the temperature threshold. Each fan has a sensor that is capable of detecting and reporting if the fan speed falls below the threshold shown.
Current	This field displays this fan's current speed in Revolutions Per Minute (RPM).
MAX	This field displays this fan's maximum speed measured in Revolutions Per Minute (RPM).
MIN	This field displays this fan's minimum speed measured in Revolutions Per Minute (RPM). "<41" is displayed for speeds too small to measure (under 2000 RPM).
Threshold	This field displays the minimum speed at which a normal fan should work.
Status	Normal indicates that this fan is functioning above the minimum speed. Error indicates that this fan is functioning below the minimum speed.
Voltage(V)	The power supply for each voltage has a sensor that is capable of detecting and reporting if the voltage falls out of the tolerance range.
Current	This is the current voltage reading.
MAX	This field displays the maximum voltage measured at this point.
MIN	This field displays the minimum voltage measured at this point.
Threshold	This field displays the percentage tolerance of the voltage with which the switch still works.
Status	Normal indicates that the voltage is within an acceptable operating range at this point; otherwise Error is displayed.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking Set Interval .
Stop	Click Stop to halt statistic polling.

7.3 General Setup

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

Figure 30 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.
Use Time Server when Bootup	<p>Enter the time service protocol that a timeserver sends when you turn on the switch. Not all timeservers support all protocols, so you may have to use trial and error to find a protocol that works. The main differences between them are the time format.</p> <p>When you select the Daytime (RFC 867) format, the switch displays the day, month, year and time with no time zone adjustment. When you use this format it is recommended that you use a Daytime timeserver within your geographical time zone.</p> <p>Time (RFC-868) format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0.</p> <p>NTP (RFC-1305) is similar to Time (RFC-868) .</p> <p>None is the default value. Enter the time manually. Each time you turn on the switch, the time and date will be reset to 2000-1-1 0:0.</p>
Time Server IP Address	Enter the IP address (or URL if you configure a domain name server in the IP Setup screen) of your timeserver. The switch searches for the timeserver for up to 60 seconds. If you select a timeserver that is unreachable, then this screen will appear locked for 60 seconds. Please wait.
Current Time	This field displays the time you open this menu (or refresh the menu).
New Time (hh:min:ss)	Enter the new time in hour, minute and second format. The new time then appears in the Current Time field after you click Apply .
Current Date	This field displays the date you open this menu.
New Date (yyyy-mm-dd)	Enter the new date in year, month and day format. The new date then appears in the Current Date field after you click Apply .

Table 9 General Setup (continued)

LABEL	DESCRIPTION
Time Zone	Select the time difference between UTC (Universal Time Coordinated, formerly known as GMT, Greenwich Mean Time) and your time zone from the drop-down list box.
Apply	Click Apply to save the settings.
Cancel	Click Cancel to reset the fields to your previous configuration.

7.4 Introduction to VLANs

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

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

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

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

See [Chapter 8 on page 79](#) 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 31 Switch Setup

The following table describes the labels in this screen.

Table 10 Switch Setup

LABEL	DESCRIPTION
VLAN Type	Choose 802.1Q or Port Based . The VLAN Setup screen changes depending on whether you choose 802.1Q VLAN type or Port Based VLAN type in this screen. See Chapter 8 on page 79 for more information.
IGMP Snooping	Select the Active checkbox to enable IGMP snooping have group multicast traffic only forwarded to ports that are members significantly reducing multicast traffic passing through your switch. See Section 7.5 on page 73 for more information on IGMP snooping. Note: You <i>cannot</i> enable both IGMP snooping and IGMP at the same time. Refer to Chapter 26 on page 161 for more information.
MAC Address Learning	MAC address learning reduces outgoing traffic broadcasts. For MAC address learning to occur on a port, the port must be active.
Aging Time	Enter a time from 10 to 3000 seconds. This is how long all dynamically learned MAC addresses remain in the MAC address table before they age out (and must be relearned).

Table 10 Switch Setup (continued)

LABEL	DESCRIPTION
	GARP Timer: Switches join VLANs by making a declaration. A declaration is made by issuing a Join message using GARP. Declarations are withdrawn by issuing a Leave message. A Leave All message terminates all registrations. GARP timers set declaration timeout values. See the chapter on VLAN setup for more background information.
Join Timer	Join Timer sets the duration of the Join Period timer for GVRP in milliseconds. Each port has a Join Period timer. The allowed Join Time range is between 100 and 65535 milliseconds. See the chapter on VLAN setup for more background information.
Leave Timer	Leave Time sets the duration of the Leave Period timer for GVRP in milliseconds. Each port has a single Leave Period timer. Leave Time must be two times larger than Join Timer .
Leave All Timer	Leave All Timer sets the duration of the Leave All Period timer for GVRP in milliseconds. Each port has a single Leave All Period timer. Leave All Timer must be larger than Leave Timer.
<p>Priority Queue Assignment</p> <p>IEEE 802.1p defines up to eight separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Frames without an explicit priority tag are given the default priority of the ingress port. Use the next two fields to configure the priority level-to-physical queue mapping.</p> <p>The switch has four physical queues that you can map to the 8 priority levels. On the switch, traffic assigned to higher index queues gets through faster while traffic in lower index queues is dropped if the network is congested.</p>	
Priority Level (The following descriptions are based on the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p)).	
Level 7	Typically used for network control traffic such as router configuration messages.
Level 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).
Level 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.
Level 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.
Level 3	Typically used for "excellent effort" or better than best effort and would include important business traffic that can tolerate some delay.
Level 2	This is for "spare bandwidth".
Level 1	This is typically used for non-critical "background" traffic such as bulk transfers that are allowed but that should not affect other applications and users.
Level 0	Typically used for best-effort traffic.
Apply	Click Apply to save the settings.
Cancel	Click Cancel to reset the fields to your previous configuration.

7.7 IP Setup

Use the **IP Setup** screen to configure the default gateway device, the default domain name server and add IP interface(s).

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 32 IP Setup

Index	IP Address	IP Subnet Mask	VID	Delete
1	192.168.1.1	255.255.255.0	1	<input type="checkbox"/>

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.
Apply	Click Apply to save the settings.
Cancel	Click Cancel to reset the fields to your previous configuration.
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.

Table 11 IP Setup (continued)

LABEL	DESCRIPTION
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 Add to save the new rule to the switch. It then displays in the summary table at the bottom of the screen.
Cancel	Click Cancel to reset the fields to your previous configuration.
Index	This field displays the index number of an entry.
IP Address	This field displays 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 Delete to remove the selected entry from the summary table. Note: Deleting all IP domains locks you out from the switch.
Cancel	Click Cancel to clear the Delete check boxes.

7.8 Port Setup

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

Figure 33 Port Setup

Port	Active	Name	Type	Speed / Duplex	Flow Control	802.1p Priority
1	<input checked="" type="checkbox"/>	none	10/100M	Auto	<input type="checkbox"/>	0
2	<input checked="" type="checkbox"/>	none	10/100M	Auto	<input type="checkbox"/>	0
3	<input checked="" type="checkbox"/>	none	10/100M	Auto	<input type="checkbox"/>	0
4	<input checked="" type="checkbox"/>	none	10/100M	Auto	<input type="checkbox"/>	0
5	<input checked="" type="checkbox"/>	none	10/100M	Auto	<input type="checkbox"/>	0
6	<input checked="" type="checkbox"/>	none	10/100M	Auto	<input type="checkbox"/>	0
7	<input checked="" type="checkbox"/>	none	10/100M	Auto	<input type="checkbox"/>	0
8	<input checked="" type="checkbox"/>	none	10/100M	Auto	<input type="checkbox"/>	0
24	<input checked="" type="checkbox"/>	none	10/100M	Auto	<input type="checkbox"/>	0
25	<input checked="" type="checkbox"/>	none	100/1000M	Auto	<input type="checkbox"/>	0
26	<input checked="" type="checkbox"/>	none	100/1000M	Auto	<input type="checkbox"/>	0
S1	<input checked="" type="checkbox"/>	none	1000M	Auto	<input type="checkbox"/>	0
S2	<input checked="" type="checkbox"/>	none	1000M	Auto	<input type="checkbox"/>	0

Apply Cancel

The following table describes the labels in this screen.

Table 12 Port Setup

LABEL	DESCRIPTION
Port	This is the port index number.
Active	Select this check box to enable a port. The factory default for all ports is enabled. A port must be enabled for data transmission to occur.
Name	Enter a descriptive name that identifies this port.
Type	This field displays 10/100M for an Ethernet connection and 1000M for the mini-GBIC ports.
Speed/Duplex	<p>Select the speed and the duplex mode of the Ethernet connection on this port.</p> <p>For Ethernet ports, select Auto, 10M/Half Duplex, 10M/Full Duplex, 100M/Half Duplex, 100M/Full Duplex or 1000M/Full Duplex.</p> <p>For Gigabit Ethernet/mini-GBIC ports (25 and 26), select Auto, 100M/Full Duplex or 1000M/Full Duplex.</p> <p>For stacking ports (S1 and S2), select Auto or 1000M/Full Duplex.</p> <p>Selecting Auto (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a port on the switch negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer port does not support auto-negotiation or turns off this feature, the switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the switch's auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect.</p>
Flow Control	<p>A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses. Flow Control is used to regulate transmission of signals to match the bandwidth of the receiving port.</p> <p>The ES-4024A uses IEEE802.3x flow control in full duplex mode and backpressure flow control in half duplex mode.</p> <p>IEEE802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill.</p> <p>Back Pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later. Select Flow Control to enable it.</p>
802.1P Priority	This priority value is added to incoming frames without a (802.1p) priority queue tag. See Priority Queue Assignment in Table 10 on page 74 for more information.
Apply	Click Apply to save the settings.
Cancel	Click Cancel 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 VLAN

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

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4,096 (2¹²) VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

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

8.1.1 Forwarding Tagged and Untagged Frames

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

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.

8.2 Automatic VLAN Registration

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

8.2.1 GARP

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

8.2.1.1 GARP Timers

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

8.2.2 GVRP

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

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

Table 13 IEEE 802.1Q VLAN Terminology

VLAN PARAMETER	TERM	DESCRIPTION
VLAN Type	Permanent VLAN	This is a static VLAN created manually.
	Dynamic VLAN	This is a VLAN configured by a GVRP registration/deregistration process.
VLAN Administrative Control	Registration Fixed	Fixed registration ports are permanent VLAN members.
	Registration Forbidden	Ports with registration forbidden are forbidden to join the specified VLAN.
	Normal Registration	Ports dynamically join a VLAN using GVRP.
VLAN Tag Control	Tagged	Ports belonging to the specified VLAN tag all outgoing frames transmitted.
	Untagged	Ports belonging to the specified don't tag all outgoing frames transmitted.

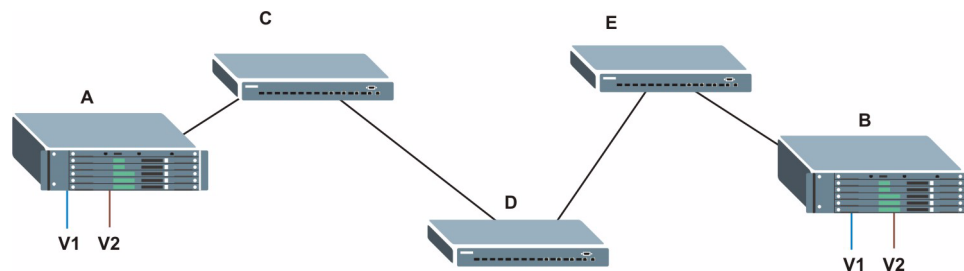
Table 13 IEEE 802.1Q VLAN Terminology (continued)

VLAN PARAMETER	TERM	DESCRIPTION
VLAN Port	Port VID	This is the VLAN ID assigned to untagged frames that this port received.
	Acceptable frame type	You may choose to accept both tagged and untagged incoming frames or just tagged incoming frames on a port.
	Ingress filtering	If set, the switch discards incoming frames for VLANs that do not have this port as a member

8.3 Port VLAN Trunking

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

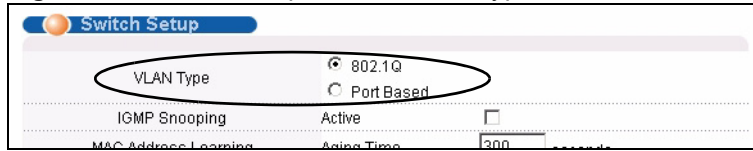
Refer to the following figure. Suppose you want to create VLAN groups 1 and 2 (V1 and V2) on devices A and B. Without **VLAN Trunking**, you must configure VLAN groups 1 and 2 on all intermediary switches C, D and E; otherwise they will drop frames with unknown VLAN group tags. However, with **VLAN Trunking**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

Figure 34 Port VLAN Trunking

8.4 Select the VLAN Type

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

Figure 35 Switch Setup: Select VLAN Type



8.5 Static VLAN

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

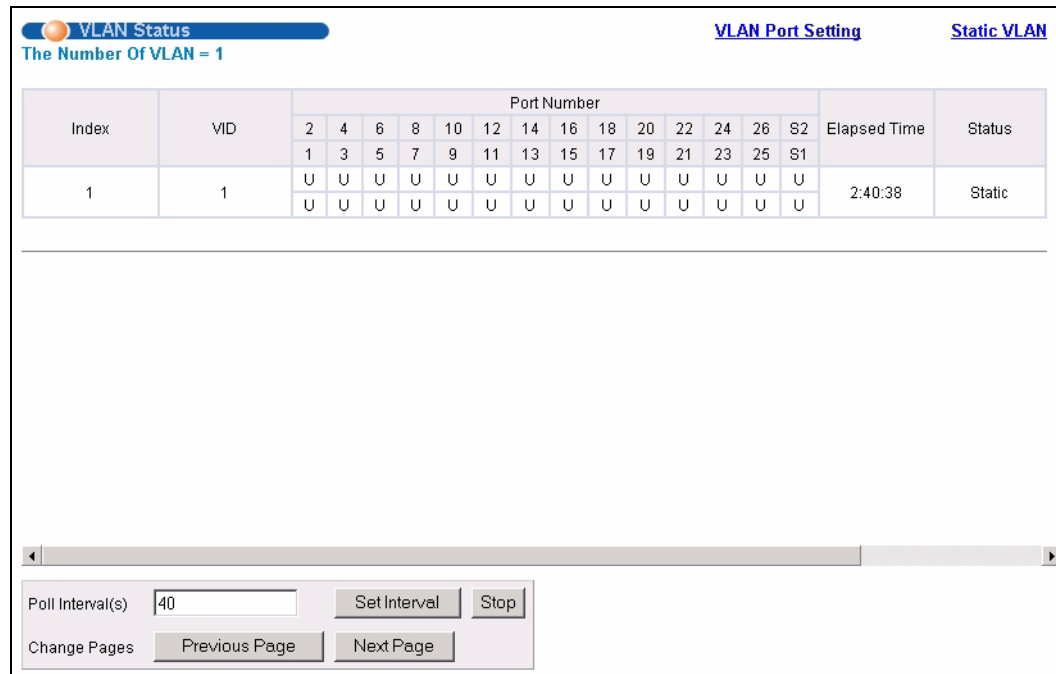
- sent to a VLAN group as normal depends on its VLAN tag.
- sent to a group whether it has a VLAN tag or not.
- blocked from a VLAN group regardless of its VLAN tag.

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 36 VLAN: VLAN Status



The following table describes the labels in this screen.

Table 14 VLAN: VLAN Status

LABEL	DESCRIPTION
The Number of VLAN	This is the number of VLANs configured on the switch.
Index	This is the VLAN index number.
VID	This is the VLAN identification number that was configured in the VLAN Setup screen.
Port Number	This column displays the ports that are participating in a VLAN. A tagged port is marked as T , an untagged port is marked as U and ports not participating in a VLAN are marked as “-”.
Elapsed Time	This field shows how long it has been since a normal VLAN was registered or a static VLAN was set up.
Status	This field shows how this VLAN was added to the switch; dynamically using GVRP or statically, that is, added as a permanent entry.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking Set Interval .
Stop	Click Stop to halt polling statistics.
Change Pages	Click Previous Page or Next Page to show the previous/next screen if all status information cannot be seen in one screen.

8.5.2 Configure a Static VLAN

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

Figure 37 VLAN: Static VLAN

The screenshot shows the 'Static VLAN' configuration screen. 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 screen 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 screen, there is a summary table with four columns: 'VID', 'Active', 'Name', and 'Delete'. The summary table shows one entry with VID '1', Active 'Yes', Name '1', and a 'Delete' 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 for the VLAN group for identification purposes.
VLAN Group ID	Enter the VLAN ID for this static entry; the valid range is between 1 and 4094.
Port	The port number identifies the port you are configuring.
Control	Select Normal for the port to dynamically join this VLAN group using GVRP. This is the default selection. Select Fixed for the port to be a permanent member of this VLAN group. Select Forbidden if you want to prohibit the port from joining this VLAN group.
Tagging	Select TX Tagging if you want the port to tag all outgoing frames transmitted with this VLAN Group ID.
Add	Click Add to add the settings as a new entry in the summary table below.
Cancel	Click Cancel to reset the fields.
Clear	Click Clear to start configuring the screen again.
VID	This field displays the ID number of the VLAN group. Click the number to edit the VLAN settings.
Active	This field indicates whether the VLAN settings are enabled (Yes) or disabled (No).
Name	This field displays the descriptive name for this VLAN group.

Table 15 VLAN: Static VLAN (continued)

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

8.5.3 Configure VLAN Port Settings

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

Figure 38 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"/>
20	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
21	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
22	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
23	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
24	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
25	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
26	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
S1	<input type="checkbox"/>	1	<input type="checkbox"/>	All	<input type="checkbox"/>
S2	<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	Port Isolation allows each port (1 to 26) 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	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	<p>Specify the type of frames allowed on a port. Choices are All, Tag Only and Untag Only.</p> <p>Select All from the drop-down list box to accept all untagged or tagged frames on this port. This is the default setting.</p> <p>Select Tag Only to accept only tagged frames on this port. All untagged frames will be dropped.</p> <p>Select Untag Only to accept only untagged frames on this port. All tagged frames will be dropped.</p>
VLAN Trunking	Enable VLAN Trunking on ports connected to other switches or routers (but not ports directly connected to end users) to allow frames belonging to unknown VLAN groups to pass through the switch.
Apply	Click Apply to save the changes
Cancel	Click Cancel to start configuring the screen again.

8.6 Port-based 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 ES-4024A uses a default VLAN ID of 1. You cannot change it.

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

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

8.6.1 Configure a Port-based VLAN

Select **Port Based** as the **VLAN Type** in the **Switch Setup** screen (see [Figure 35 on page 82](#)) and then click **VLAN** from the navigation panel to display the next screen.

Figure 39 Port Based VLAN Setup (All Connected)

Port Based VLAN Setup

Setting Wizard
All connected ▾
Apply

Incoming

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	S1	S2		
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	
2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2
3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3
4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	4
5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	5
6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	6
7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	7
8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	8
9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	9
10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	10
11	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	11
12	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	12
13	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	13
14	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	14
15	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	15
16	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	16
17	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	17
18	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	18
19	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	19
20	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	20
21	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	21
22	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	22
23	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	23
24	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	24
25	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	25
26	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	26
S1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	S1
S2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	S2
CPU	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	CPU

Outgoing

Apply Cancel

Figure 40 Port Based VLAN Setup (Port Isolation)

The screenshot displays the 'Port Based VLAN Setup' interface with 'Port isolation' selected. It features a grid for configuring traffic between 26 ports (1-24) and two switches (S1, S2). The CPU is also included in the grid. The 'Incoming' section is at the top, and the 'Outgoing' section is on the left. Checkmarks indicate connections between ports and switches. Buttons for 'Setting Wizard', 'Port isolation', 'Apply', and 'Cancel' are visible.

		Incoming																												
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	S1	S2	
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"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	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"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	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"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	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"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	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"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	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"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	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"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	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"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	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"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	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"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	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"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	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"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	13	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input 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"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	14	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input 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"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	15	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input 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"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	16	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input 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"/>	<input type="checkbox"/>	<input type="checkbox"/>
	17	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input 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"/>	<input type="checkbox"/>
	18	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input 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"/>
	19	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input 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"/>
	20	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input 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"/>
	21	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input 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"/>
	22	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	23	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	24	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	25	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	26	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
S1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
S2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
CPU	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

The following table describes the labels in this screen.

Table 17 Port Based VLAN Setup

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

CHAPTER 9

Static MAC Forwarding

Use these screens to configure static MAC address forwarding.

9.1 Overview

A static MAC address 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 115](#) for more information on port security.

9.2 Configuring Static MAC Forwarding

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

Figure 41 Static MAC Forwarding

Index	Active	Name	MAC Address	Port	Delete
1	Yes	Example	0a:b2:a0:81:f3:7e / 1	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 for identification purposes for this static MAC address forwarding rule.
MAC Address	Enter the MAC address in valid MAC address format, that is, six hexadecimal character pairs. Note: Static MAC addresses do not age out.
VID	Enter the VLAN identification number.
Port	Select a port where the MAC address entered in the previous field will be automatically forwarded.
Add	After you set the fields above, click Add to insert a new rule.
Cancel	Click Cancel to reset the fields.
Clear	Click Clear to begin configuring this screen afresh.
Index	Click an index number to modify a static MAC address rule for a port.
Active	This field displays whether this static MAC address forwarding rule is active (Yes) or not (No). You may temporarily deactivate a rule without deleting it.
Name	This field displays the descriptive name for identification purposes for this static MAC address-forwarding rule.
MAC Address	This field displays the MAC address that will be forwarded and the VLAN identification number to which the MAC address belongs.
Port	This field displays the port where the MAC address shown in the next field will be forwarded.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the Delete check boxes.

CHAPTER 10

Filtering

This chapter discusses static IP and MAC address port filtering.

10.1 Overview

Port filtering means discarding (or dropping) traffic flow based on the source and/or destination IP and/or MAC addresses and VLAN group.

You must first configure rules to classify traffic flows in the **Classifier** screen.

10.2 Configure a Filtering Rule

Activate filtering on a specified traffic flow in the Filtering screen. Click **Advanced Application** and **Filtering** in the navigation panel to display the screen as shown next.

Figure 42 Filtering

Index	Active	Name	Classifier	Delete
1	Yes	Example	Example	<input type="checkbox"/>

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	This read-only field displays the name of the classifier you select in the Classifier field.

Table 19 Filtering (continued)

LABEL	DESCRIPTION
Classifier	A classifier groups traffic flow based on the specified criteria. This field displays the name(s) of the classifier(s) you configure in the Classifier screen. Select a classifier (or traffic flow) to which the rule is to apply.
Add	Click Add to inset the entry to the summary table below.
Cancel	Click Cancel to reset the fields to your previous configuration.
Clear	Click Clear to set the above fields back to the factory defaults.
Index	This field displays the index number of a rule. Click this number to edit the rule settings.
Active	This field indicates whether the rule is enabled (Yes) or disabled (No).
Name	This field displays the descriptive name of the rule.
Classifier	This field displays the name of the classifier to which this rule applies.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the Delete check boxes.

CHAPTER 11

Spanning Tree Protocol

This chapter introduces the Spanning Tree Protocol (STP).

11.1 Overview

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

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 BPDU 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 43 Spanning Tree Protocol: Status

Bridge	Root	Our Bridge
Bridge ID	8000-00a0c5012345	8000-00a0c5012345
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		1
Time Since Last Change		0:00:05

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 Running if STP is activated. Otherwise, it displays Down .
Configuration	Click Configuration to configure STP settings. Refer to Section 11.3 on page 98 .
Bridge	Root refers to the base of the spanning tree (the root bridge). Our Bridge is this switch. This switch may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same for Root and Our Bridge if the switch is the root switch.
Hello Time (second)	This is the time interval (in seconds) at which the root switch transmits a configuration message. The root bridge determines Hello Time , Max Age and Forwarding Delay
Max Age (second)	This is the maximum time (in seconds) a switch can wait without receiving a configuration message before attempting to reconfigure.
Forwarding Delay (second)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding).
Cost to Bridge	This is the path cost from the root port on this switch to the root switch.
Port ID	This is the priority and number of the port on the switch through which this switch must communicate with the root of the Spanning Tree.
Topology Changed Times	This is the number of times the spanning tree has been reconfigured.
Time Since Last Change	This is the time since the spanning tree was last reconfigured.

Table 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 Set Interval .
Stop	Click Stop to halt STP statistic polling.

11.3 Configure STP

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

Figure 44 Spanning Tree Protocol: Configuration

Port	Active	Priority	Path Cost
1	<input type="checkbox"/>	128	19
2	<input type="checkbox"/>	128	19
3	<input type="checkbox"/>	128	19
4	<input type="checkbox"/>	128	19
5	<input type="checkbox"/>	128	19
21	<input type="checkbox"/>	128	19
22	<input type="checkbox"/>	128	4
23	<input type="checkbox"/>	128	4
24	<input type="checkbox"/>	128	4
25	<input type="checkbox"/>	128	4
26	<input type="checkbox"/>	128	4
S1	<input type="checkbox"/>	128	4
S2	<input type="checkbox"/>	128	4

The following table describes the labels in this screen.

Table 23 Spanning Tree Protocol: Configuration

LABEL	DESCRIPTION
Status	Click Status to display the Spanning Tree Protocol Status screen (see Figure 43 on page 97).
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> <p>Note: $2 * (\text{Forward Delay} - 1) \geq \text{Max Age} \geq 2 * (\text{Hello Time} + 1)$</p>
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 Table 20 on page 95 for more information.</p>
Apply	<p>Click Apply to save your changes back to the switch.</p>
Cancel	<p>Click Cancel to begin configuring this screen afresh.</p>

CHAPTER 12

Bandwidth Control

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

12.1 Bandwidth Control Setup

Bandwidth control means defining a maximum allowable bandwidth for the specified traffic flow.

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

Figure 45 Bandwidth Control

The following table describes the related labels in this screen.

Table 24 Bandwidth Control

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	This read-only field displays the name of the classifier you select in the Classifier field.
Maximal Bandwidth	Specify the maximal bandwidth allowed in kilobits per second (kbps) for this traffic flow. Enter a number between 1 and 1000000.
Classifier	This list box displays the name(s) of the classifier that you configure in the Classifier screen. Select a name to which to apply this rule.
Add	Click Add to inset the entry to the summary table below.

Table 24 Bandwidth Control (continued)

LABEL	DESCRIPTION
Cancel	Click Cancel to reset the fields back to your previous configuration.
Clear	Click Clear to reset the fields back to the factory defaults.

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

13.2 Broadcast Storm Control Setup

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

Figure 46 Broadcast Storm Control

Port	Incoming	Outgoing
1	32767 Frames	32767 Frames
2	32767 Frames	32767 Frames
3	32767 Frames	32767 Frames
4	32767 Frames	32767 Frames
5	32767 Frames	32767 Frames
6	32767 Frames	32767 Frames
7	32767 Frames	32767 Frames
8	32767 Frames	32767 Frames
9	32767 Frames	32767 Frames
10	32767 Frames	32767 Frames
11	32767 Frames	32767 Frames
12	32767 Frames	32767 Frames
13	32767 Frames	32767 Frames
14	32767 Frames	32767 Frames
15	32767 Frames	32767 Frames
16	32767 Frames	32767 Frames
17	32767 Frames	32767 Frames
18	32767 Frames	32767 Frames
19	32767 Frames	32767 Frames
20	32767 Frames	32767 Frames
21	32767 Frames	32767 Frames
22	32767 Frames	32767 Frames
23	32767 Frames	32767 Frames
24	32767 Frames	32767 Frames
25	32767 Frames	32767 Frames
26	32767 Frames	32767 Frames
S1	32767 Frames	32767 Frames
S2	32767 Frames	32767 Frames

The following table describes the labels in this screen.

Table 25 Broadcast Storm Control

LABEL	DESCRIPTION
Active	Select this check box to enable broadcast storm control. Clear this check box to disable the feature.
Monitor Interval	When the Monitor Interval time period expires, each port begins counting broadcast frames allowed in its buffers anew. Select a time period from 64, 1024, 8000, 256000 microseconds.
Direction	Choose to monitor broadcast packets coming into the switch (Incoming) or going out of the switch (Outgoing).
Port	This field displays a port number.
Incoming	From the drop-down list box, select how many broadcast frames the port can store in the switch buffer.
Outgoing	From the drop-down list box, select how many frames the port will send out
Apply	Click Apply to save your changes back to the switch.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 14

Mirroring

This chapter discusses the Mirror setup screens.

14.1 Overview

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

14.2 Port Mirroring Setup

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

Figure 47 Mirroring

Index	Active	Name	Classifier	Delete
1	Yes	Example	Example	<input type="checkbox"/>

The following table describes the labels in this screen.

Table 26 Mirroring: Mirror Port Setting

LABEL	DESCRIPTION
Active	Clear this check box to deactivate port mirroring on the switch.
Mirror Port	The mirror 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.
Apply	Click Apply to save the changes.
Cancel	Click Cancel to start configuring the screen again.
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	This read-only field displays the name of the classifier you select in the Classifier field.
Classifier	A classifier groups traffic flow based on the specified criteria. This field displays the name(s) of the classifier(s) you configure in the Classifier screen. Select a classifier to which the rule is to apply. Traffic flow (both incoming or outgoing) that matches the criteria of the classifier will be copied to the specified mirror port.
Add	Click Add to inset the entry to the summary table below.
Cancel	Click Cancel to reset the fields to your previous configuration.
Clear	Click Clear to set the above fields back to the factory defaults.
Index	This field displays the index number of a rule. Click this number to edit the rule settings.
Active	This field indicates whether the rule is enabled (Yes) or disabled (No)
Name	This field displays the descriptive name of the rule.
Classifier	This field displays the name of the classifier to which this rule applies.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the Delete check box(es).

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.

The beginning port of each trunk group must be physically connected to form a trunk group. Ports should be physically linked in consecutive order without gaps when forming trunk groups.

Table 27 Trunk Groups

TRUNK GROUP	BEGINNING PORT	PORT RANGE
1	1	1 to 8
2	9	9 to 16
3	17	17 to 24
4	25	25 and 26 (the mini GBIC ports)
5	S1	S1 and S2 (the stacking ports)

15.1.1 Dynamic Link Aggregation

The ES-4024A adheres to the IEEE 802.3ad standard for static and dynamic (LACP) port trunking.

The ES-4024A 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 information¹:

Table 28 Link Aggregation ID: Local Switch

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

Table 29 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.

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

Figure 48 Link Aggregation Control Protocol Status

Link Aggregation Control Protocol Status				Configuration
Index	Aggregator ID	Enabled Ports	Synchronized Ports	
1	{(0000,00-00-00-00-00-00,0000,00,0000)}	-	-	
2	{(0000,00-00-00-00-00-00,0000,00,0000)}	-	-	
3	{(0000,00-00-00-00-00-00,0000,00,0000)}	-	-	
4	{(0000,00-00-00-00-00-00,0000,00,0000)}	-	-	
5	{(0000,00-00-00-00-00-00,0000,00,0000)}	-	-	

Polling Interval(s)

The following table describes the labels in this screen.

Table 30 Link Aggregation Control Protocol Status

LABEL	DESCRIPTION
Index	This field displays the trunk ID to identify a trunk group, that is, one logical link containing multiple ports.
Aggregator ID	Refer to Section 15.1.2 on page 108 for more information on this field.
Enabled Port	These are the ports you have configured in the Link Aggregation screen to be in the trunk group.
Synchronized Ports	These are the ports that are currently transmitting data as one logical link in this trunk group.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking Set Interval .
Stop	Click Stop to halt statistic polling.

15.3 Link Aggregation Setup

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

Figure 49 Link Aggregation: Configuration

Index	Active	Starting Port	Ending Port	LACP	LACP Timeout
1	<input type="checkbox"/>	1	2	<input type="checkbox"/>	30 seconds
2	<input type="checkbox"/>	9	10	<input type="checkbox"/>	30 seconds
3	<input type="checkbox"/>	17	18	<input type="checkbox"/>	30 seconds
4	<input type="checkbox"/>	25	26	<input type="checkbox"/>	30 seconds
5	<input type="checkbox"/>	S1	S2	<input type="checkbox"/>	30 seconds

The following table describes the labels in this screen.

Table 31 Link Aggregation: 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 65535. 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.
Index	The index identifies the trunk group, that is, one logical link containing multiple ports
Active	Make sure to select this check box to activate the trunk group. You may temporarily deactivate a trunk group without deleting it by clearing this check box.
Starting Port	This is the beginning port in the trunk group’s port range and is not configurable (see Table 27 on page 107).
Ending Port	Select the end port in the port range from the drop-down list box if applicable (see Table 27 on page 107).
LACP	Select this check box to enable LACP for a trunk.
LACP Timeout	Timeout is the time interval between the individual port exchanges of LACP packets in order to check that the peer port in the trunk group is still up. If a port does not respond after three tries, then it is deemed to be “down” and is removed from the trunk. Set a short timeout (one second) for busy trunked links to ensure that disabled ports are removed from the trunk group as soon as possible. Select either 1 second or 30 seconds.
Apply	Click Apply to save your changes back to the switch.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 16

Port Authentication

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

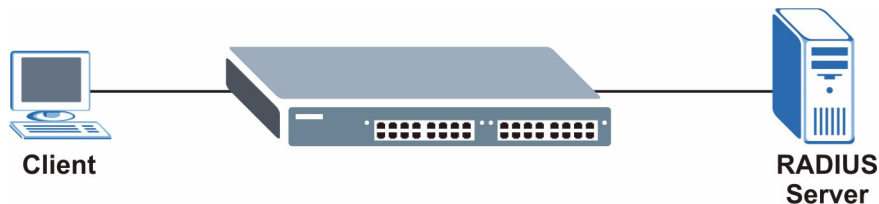
16.1 Overview

IEEE 802.1x is an extended authentication protocol² that allows support of RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting³ 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 50 RADIUS Server



16.2 Port Authentication Configuration

To enable port authentication, first activate IEEE802.1x security (both on the ES-4024A and the port(s)) then configure the RADIUS server settings.

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

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

Figure 51 Port Authentication

Port Authentication

RADIUS [Click here](#)

802.1x [Click here](#)

16.2.1 Activate IEEE 802.1x Security

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

Figure 52 Port Authentication: 802.1x

802.1x Port Authentication

Active

Port	Active	Reauthentication	Reauthentication Timer
1	<input type="checkbox"/>	Off	3600 seconds
2	<input type="checkbox"/>	Off	3600 seconds
3	<input type="checkbox"/>	Off	3600 seconds
4	<input type="checkbox"/>	Off	3600 seconds
5	<input type="checkbox"/>	Off	3600 seconds
21	<input type="checkbox"/>	Off	3600 seconds
22	<input type="checkbox"/>	Off	3600 seconds
23	<input type="checkbox"/>	Off	3600 seconds
24	<input type="checkbox"/>	Off	3600 seconds
25	<input type="checkbox"/>	Off	3600 seconds
26	<input type="checkbox"/>	Off	3600 seconds

Apply Cancel

The following table describes the labels in this screen.

Table 32 Port Authentication: 802.1x

LABEL	DESCRIPTION
Active	Select this check box to permit 802.1x authentication on the switch. Note: You must first enable 802.1x authentication on the switch before configuring it on each port.
Port	This field displays a port number.
Active	Select this checkbox to permit 802.1x authentication on this port. You must first allow 802.1x authentication on the switch before configuring it on each port.
Reauthentication	Specify if a subscriber has to periodically re-enter his or her username and password to stay connected to the port.
Reauthentication Timer	Specify how often a client has to re-enter his or her username and password to stay connected to the port.
Apply	Click Apply to save your changes back to the switch.
Cancel	Click Cancel to begin configuring this screen afresh.

16.2.2 Configuring RADIUS Server Settings

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

Figure 53 Port Authentication: RADIUS

The following table describes the labels in this screen.

Table 33 Port Authentication: RADIUS

LABEL	DESCRIPTION
Authentication Server	
IP Address	Enter the IP address of the external RADIUS server in dotted decimal notation.
UDP Port	The default port of the RADIUS server for authentication is 1812 . You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 30 alphanumeric characters) as the key to be shared between the external RADIUS server and the switch. This key is not sent over the network. This key must be the same on the external RADIUS server and the switch.
Apply	Click Apply to save your changes back to the switch.
Cancel	Click Cancel 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. The switch can learn up to 16K MAC addresses in total with no limit on individual ports other than the sum cannot exceed 16K.

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

17.2 Port Security Setup

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

Figure 54 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
...
21	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0
22	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0
23	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0
24	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0
25	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0
26	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0

Apply Cancel

The following table describes the labels in this screen.

Table 34 Port Security

LABEL	DESCRIPTION
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 Switch Setup screen. The valid range is from "0" to "254". "0" means this feature is disabled, so the switch will learn MAC addresses up to the global limit of 16K.
Apply	Click Apply to save your changes back to the switch.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 18

DHCP

This chapter shows you how to configure the DHCP feature.

18.1 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 ES-4024A as a DHCP server or disable it. When configured as a server, the ES-4024A 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.

18.1.1 DHCP modes

The ES-4024A can be configured as a DHCP server or DHCP relay agent.

- If you configure the ES-4024A 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 ES-4024A as a DHCP relay agent. When the ES-4024A 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.

18.2 Configuring DHCP Server

Click **Advanced Application**, **DHCP** in the navigation panel. Select **Server** in the **DHCP Status** field to display the screen as shown.

Figure 55 DHCP: Server

The following table describes the DHCP server related labels in this screen.

Table 35 DHCP: Server

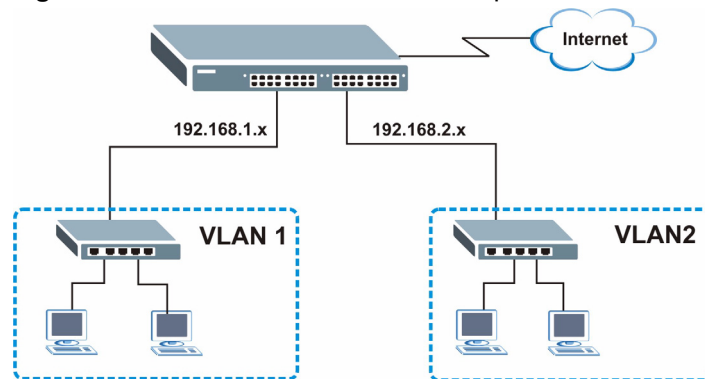
LABEL	DESCRIPTION
Active	Select this check box to enable the DHCP settings.
VID	Enter the ID number of the VLAN group to which this DHCP settings apply.
DHCP Status	Select Server to set the ES-4024A to act as a DHCP server. Select Relay to set the ES-4024A to act as a DHCP relay. Then set the corresponding fields below.
Server	The fields are editable when you select Server in the DHCP Status field.
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.
VID	This field displays the ID number of the VLAN group to which this DHCP settings apply.

Table 35 DHCP: Server (continued)

LABEL	DESCRIPTION
Type	This field displays the type of the DHCP mode (Server or Relay) for this entry. None indicates the rule is inactive.
DHCP Status	This field displays the client IP pool starting address and the size of client IP pool if the Type field displays Server . This field displays the IP address of a DHCP server if the Type field is Relay .
Delete	Click Delete to remove the selected entry.
Cancel	Click Cancel to clear the Delete check boxes.

18.2.1 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 56 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 57 DHCP Server Configuration Example

The screenshot displays the DHCP configuration interface. At the top, there is a 'DHCP' header with a status indicator. Below it, the 'Active' checkbox is checked. The 'VID' is set to 2. The 'DHCP Status' is set to 'Server'. Under the 'Server' section, the following fields are configured: 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 (192.168.1.220), and Secondary DNS Server (0.0.0.0). Under the 'Relay' section, three Remote DHCP Servers are listed, all with IP addresses of 0.0.0.0. At the bottom, there are 'Add', 'Cancel', and 'Clear' buttons. Below the configuration fields is a table with columns for VID, Type, DHCP Status, and Delete. The table contains one entry: VID 1, Type Server, DHCP Status 192.168.1.100/100, and a Delete checkbox. At the bottom of the table are 'Delete' and 'Cancel' buttons.

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

18.3 Configuring 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.

Click **Advanced Application**, **DHCP** in the navigation panel. Select **Relay** in the **DHCP Status** field to display the screen as shown.

Figure 58 DHCP: Relay

The screenshot shows the DHCP: Relay configuration interface. It includes a header 'DHCP' and a sub-header 'DHCP: Relay'. The configuration is organized into several sections:

- Active:** A checkbox that is currently unchecked.
- VID:** A text input field.
- DHCP Status:** Radio buttons for 'Server' and 'Relay'. 'Relay' is selected.
- Server:** A section with the following fields:
 - Client IP Pool Starting Address: 0.0.0.0
 - Size of Client IP Pool: [input field]
 - IP Subnet Mask: 0.0.0.0
 - Default Gateway: 0.0.0.0
 - Primary DNS Server: 0.0.0.0
 - Secondary DNS Server: 0.0.0.0
- Relay:** A section with three 'Remote DHCP Server' fields, each containing '0.0.0.0'.

Below the configuration fields are three buttons: 'Add', 'Cancel', and 'Clear'. At the bottom of the screen is a summary table:

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

Below the summary table are two buttons: 'Delete' and 'Cancel'.

The following table describes the DHCP relay related labels in this screen.

Table 36 DHCP: Relay

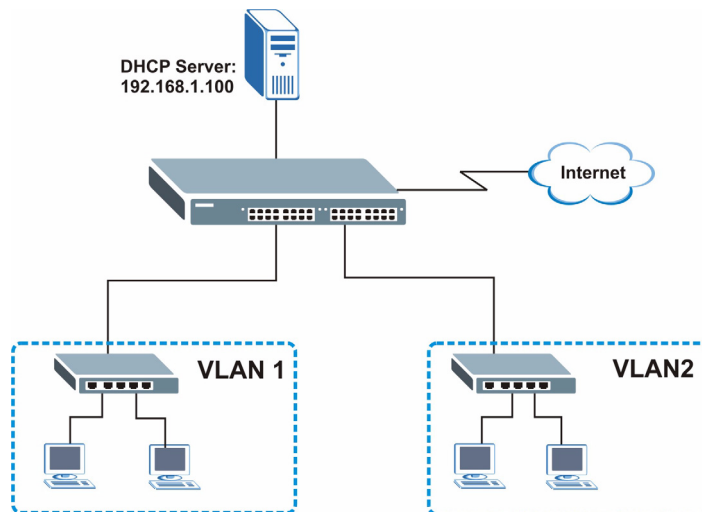
LABEL	DESCRIPTION
Active	Select this check box to enable the DHCP settings.
VID	Enter the ID number of the VLAN group to which this DHCP settings apply.
DHCP Status	Select Server to set the ES-4024A to act as a DHCP server. Select Relay to set the ES-4024A to act as a DHCP relay. Then set the corresponding fields below.
Relay	The fields are editable when you select Relay in the DHCP Status field.
Remote DHCP Server 1.. 3	Enter the IP address(es) of the DHCP server(s).
Add	Click Add to insert the settings as a new entry in the summary table.
Cancel	Click Cancel to reset the fields to your previous configurations.
Clear	Click Clear 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 the type of the DHCP mode (Server or Relay) for this entry. None indicates the rule is inactive.

Table 36 DHCP: Relay (continued)

LABEL	DESCRIPTION
DHCP Status	This field displays the client IP pool starting address and the size of client IP pool if the Type field displays Server . This field displays the IP address of a DHCP server if the Type field is Relay .
Delete	Click Delete to remove the selected entry.
Cancel	Click Cancel to clear the Delete check boxes.

18.3.1 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 59 DHCP Relay Network Example

Configure the DHCP relay settings for the two VLANs in the **DHCP Relay** screen as shown.

Figure 60 DHCP Relay Configuration Example

DHCP

Active	<input checked="" type="checkbox"/>
VID	<input type="text" value="2"/>
DHCP Status	<input type="radio"/> Server <input checked="" type="radio"/> Relay
Server	
Client IP Pool Starting Address	<input type="text" value="0.0.0.0"/>
Size of Client IP Pool	<input type="text" value=""/>
IP Subnet Mask	<input type="text" value="0.0.0.0"/>
Default Gateway	<input type="text" value="0.0.0.0"/>
Primary DNS Server	<input type="text" value="0.0.0.0"/>
Secondary DNS Server	<input type="text" value="0.0.0.0"/>
Relay	
Remote DHCP Server 1	<input type="text" value="192.168.1.100"/>
Remote DHCP Server 2	<input type="text" value="0.0.0.0"/>
Remote DHCP Server 3	<input type="text" value="0.0.0.0"/>

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

CHAPTER 19

Access Control

This chapter describes how to control access to the switch.

19.1 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 61 Console Port Priority

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

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

Table 37 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

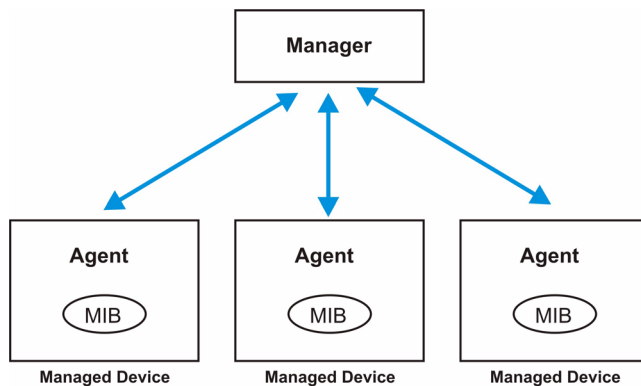
19.2 The Access Control Main Screen

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

Figure 62 Access Control

19.3 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 ES-4024A 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 63 SNMP Management Model

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

An agent is a management software module that resides in a managed switch (the ES-4024A). 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 38 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.

19.3.1 Supported MIBs

MIBs let administrators collect statistics and monitor status and performance.

The ES-4024A 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

19.3.2 SNMP Traps

The ES-4024A sends traps to an SNMP manager when an event occurs. SNMP traps supported are outlined in the following table.

Table 39 SNMP Traps

GENERIC TRAP	SPECIFIC TRAP	DESCRIPTION
0 (Cold Start)	0	This trap is sent when the ES-4024A is turned on.
1 (WarmStart)	0	This trap is sent when the ES-4024A restarts.
2 (linkDown)	0	This trap is sent when the Ethernet link is down.
3 (linkUp)	0	This trap is sent when the Ethernet link is up.
4 (authenticationFailure)	0	This trap is sent when an SNMP request comes from non-authenticated hosts.

19.3.3 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 64 Access Control: SNMP

Field	Value
Get Community	public
Set Community	public
Trap Community	public
Trap Destination	0.0.0.0
	0.0.0.0
	0.0.0.0
	0.0.0.0

The following table describes the labels in this screen.

Table 40 Access Control: SNMP

LABEL	DESCRIPTION
Get Community	Enter the get community, which is the password for the incoming Get- and GetNext-requests from the management station.
Set Community	Enter the set community, which is the password for incoming Set- requests from the management station.
Trap Community	Enter the trap community, which is the password sent with each trap to the SNMP manager.
Trap Destination	Enter the IP addresses of up to four stations to send your SNMP traps to.
Apply	Click Apply to save your changes back to the switch.
Cancel	Click Cancel to begin configuring this screen afresh.

19.3.4 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 changes.

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

Figure 65 Access Control: Logins

The screenshot shows the 'Logins' configuration screen. At the top, there's a 'Logins' header and an 'Access Control' link. Below that, the 'Administrator' section contains three password input fields: 'Old Password', 'New Password', and 'Retype to confirm'. A red warning message states: 'Please record your new password whenever you change it. The system will lock you out if you have forgotten your password.' Below this is the 'Edit Logins' section, which includes a table with four columns: 'Login', 'User Name', 'Password', and 'Retype to confirm'. The table has four rows, each with a 'Login' number (1, 2, 3, 4) and empty input fields for the other three columns. At the bottom of the screen are 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 41 Access Control: Logins

LABEL	DESCRIPTION
Administrator	This is the default administrator account with the “admin” user name. You cannot change the default administrator user name. Only the administrator has read/write access.
Old Password	Type the existing system password (1234 is the default password when shipped).
New Password	Enter your new system password.
Retype to confirm	Retype your new system password for confirmation
Edit Logins	You may configure passwords for up to four users. These people have read-only access.
User Name	Set a user name (up to 30 characters long).
Password	Enter your new system password.
Retype to confirm	Retype your new system password for confirmation
Apply	Click Apply to save your changes back to the switch.
Cancel	Click Cancel to begin configuring this screen afresh.

19.4 Service Port Access Control

Service Access Control allows you to decide what services you may use to access the ES-4024A. You may also change the default service port and configure “trusted computer(s)” for each service in the **Remote Management** screen (discussed later). Click **Access Control** to go back to the **Access Control** screen.

Figure 66 Access Control: Service Access Control

Services	Active	Service Port
Telnet	<input checked="" type="checkbox"/>	23
FTP	<input checked="" type="checkbox"/>	21
Web	<input checked="" type="checkbox"/>	80
ICMP	<input checked="" type="checkbox"/>	
SNMP	<input checked="" type="checkbox"/>	

The following table describes the fields in this screen.

Table 42 Access Control: Service Access Control

LABEL	DESCRIPTION
Services	Services you may use to access the ES-4024A are listed here.
Active	Select this option for the corresponding services that you want to allow to access the ES-4024A.
Service Port	For Telnet, FTP or web services, you may change the default service port by typing the new port number in the Service Port field. If you change the default port number then you will have to let people (who wish to use the service) know the new port number for that service.
Apply	Click Apply to save your changes back to the switch.
Cancel	Click Cancel to begin configuring this screen afresh.

19.5 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 67 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 43 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 Apply to save your changes back to the switch.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 20

Classifier

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

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

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

- 1 Configure classifiers to sort traffic into different flows.
- 2 Configure rules to define actions to be performed for a classified traffic flow (refer to the related chapters to configure the rules).

20.2 Configuring the Classifier

Use the **Classifier** screen to define the classifiers. After you define the classifier, you can specify actions (or filters) to act upon the traffic that match the rules.

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

Figure 68 Classifier

The following table describes the labels in this screen.

Table 44 Classifier

LABEL	DESCRIPTION
Active	Select this option to enable this rule.
Name	Enter a descriptive name for this rule for identifying purposes.
Layer 2	Specify the fields below to configure a layer 2 classifier.
VLAN	Select Any to classify traffic to/from any VLAN or select the second option and specify the source/destination VLAN ID in the field provided.
Ethernet Type	Select an Ethernet type or select Other and enter the Ethernet type number in hexadecimal value. Refer to Table 45 on page 136 for information.
Source	
MAC Address	Select Any to apply the rule to all MAC addresses. To specify a source, select the second choice and type a MAC address in valid MAC address format (six hexadecimal character pairs).

Table 44 Classifier (continued)

LABEL	DESCRIPTION
Port	Select the port to which the rule should be applied. You may choose one port only or all ports (All Ports).
Destination	
MAC Address	Select Any to apply the rule to all MAC addresses. To specify a destination, select the second choice and type a MAC address in valid MAC address format (six hexadecimal character pairs).
Port	Select the port to which the rule should be applied. You may choose one port only or all ports (All Ports).
Layer 3 Specify the fields below to configure a layer 3 classifier.	
IP Protocol	Select an IP protocol type or select Other and enter the protocol number in decimal value. Refer to Table 46 on page 136 for more information. You may select Establish Only for TCP protocol type. This means that the switch will pick out the packets that are sent to establish TCP connections.
Source	
IP Address/ Address Prefix	Enter a source IP address in dotted decimal notation. Specify the address prefix by entering the number of ones in the subnet mask.
Socket Number	Note: You <i>must</i> select either UDP or TCP in the IP Protocol field before you configure the socket numbers. Select Any to apply the rule to all TCP/UDP protocol port numbers or select the second option and enter a TCP/UDP protocol port number.
Destination	
IP Address/ Address Prefix	Enter a destination IP address in dotted decimal notation. Specify the address prefix by entering the number of ones in the subnet mask.
Socket Number	Note: You <i>must</i> select either UDP or TCP in the IP Protocol field before you configure the socket numbers. Select Any to apply the rule to all TCP/UDP protocol port numbers or select the second option and enter a TCP/UDP protocol port number.
Add	Click Add to insert the entry in the summary table below.
Cancel	Click Cancel to reset the fields back to your previous configuration.
Clear	Click Clear to set the above fields back to the factory defaults.
Index	This field displays the index number of the rule. Click an index number to edit the rule.
Active	This field displays Yes when the rule is activated and No when it is deactivated.
Name	This field displays the descriptive name for this rule. This is for identification purpose only.
Rule	This field displays a summary of the classifier rule's settings.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the Delete check boxes.

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

Table 45 Common Ethernet Types and Protocol Number

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

Some of the most common IP ports are:

Table 46 Common IP Ports

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

20.3 Classifier Configuration Example

The following screen shows an example where you configure a classifier that identifies all IP traffic from the MAC address 00:50:ba:00:00:01 on port 3 in VLAN 1.

After you have configured a classifier, you can define actions (such as filtering, bandwidth control) on the classified traffic flow.

Figure 69 Classifier Example

Classifier		
Active	<input checked="" type="checkbox"/>	
Name	Example	
VLAN	<input type="radio"/> Any <input checked="" type="radio"/> 1	
Ethernet Type	<input checked="" type="radio"/> IP <input type="radio"/> Others (Hex)	
Layer 2	Source MAC Address <input checked="" type="radio"/> Any <input type="radio"/> MAC	
	Port	Port 3
	Destination MAC Address <input type="radio"/> Any <input checked="" type="radio"/> MAC	
	Port	
IP Protocol	<input checked="" type="radio"/> All <input type="radio"/> Others (Dec)	
Layer 3	Source IP Address / Address Prefix 0.0.0.0 /	
	Socket Number <input checked="" type="radio"/> Any <input type="radio"/>	
	Destination IP Address / Address Prefix 0.0.0.0 /	
	Socket Number <input checked="" type="radio"/> Any <input type="radio"/>	

CHAPTER 21

Differentiated Services

This chapter shows you how to configure Differentiated Services (DiffServ) on the ES-4024A.

21.1 Overview

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

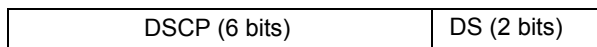
DiffServ is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired.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

21.1.1 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 70 DiffServ: Differentiated Service Field

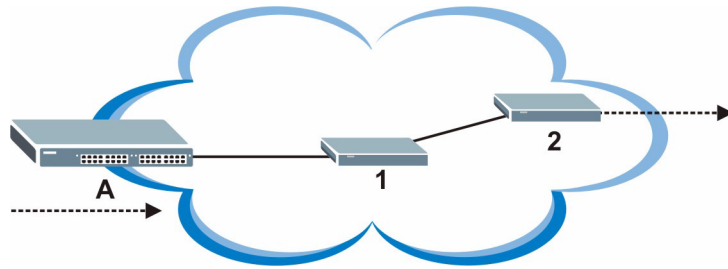


The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule different kinds of traffic can be marked for different priorities of forwarding. Resources can then be allocated according to the DSCP values and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

21.1.2 DiffServ Network Example

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

Figure 71 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.

21.2 Activating DiffServ

Activate DiffServ to allow the ES-4024A to enable DiffServ and apply marking rules and IEEE802.1p priority mapping on the selected port(s).

Click **Advanced Applications, DiffServ** in the navigation panel to display the screen as shown.

Figure 72 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"/>
13	<input checked="" type="checkbox"/>
14	<input checked="" type="checkbox"/>
15	<input checked="" type="checkbox"/>
16	<input checked="" type="checkbox"/>
17	<input checked="" type="checkbox"/>
18	<input checked="" type="checkbox"/>
19	<input checked="" type="checkbox"/>
20	<input checked="" type="checkbox"/>
21	<input checked="" type="checkbox"/>
22	<input checked="" type="checkbox"/>
23	<input checked="" type="checkbox"/>
24	<input checked="" type="checkbox"/>
25	<input checked="" type="checkbox"/>
26	<input checked="" type="checkbox"/>
31	<input checked="" type="checkbox"/>
32	<input checked="" type="checkbox"/>

The following table describes the labels in this screen.

Table 47 DiffServ

LABEL	DESCRIPTION
Active	Select this option to enable DiffServ on the switch.
Default DSCP	Enter the default DSCP value (between 0 to 63) to use if no marking rule is configured for a traffic type.
Port	This field displays the index number of a port on the ES-4024A.
Active	Select this option to apply the default DSCP value you set in the Default DSCP field on a port.
Apply	Click Apply to save the changes.
Cancel	Click Cancel to start configuring this screen again.

21.3 Configuring Marking Rules

Create DiffServ marking rules to set the DSCP values in the packets for the traffic flows.

In the **DiffServ** screen, click the **Making Rule Setting** link to display the screen as shown next.

Figure 73 DiffServ: Marking Rule Setting

The following table describes the labels in this screen.

Table 48 DiffServ: Marking Rule Setting

LABEL	DESCRIPTION
Active	Select this option to enable this rule.
Name	Enter a description name for identification purposes.
DSCP	Enter a DSCP value (between 0 and 63) for this rule.

Table 48 DiffServ: Marking Rule Setting (continued)

LABEL	DESCRIPTION
Classifier	A classifier groups traffic flow based on the specified criteria. This field displays the name(s) of the classifier(s) you configure in the Classifier screen. Select a classifier (or traffic flow) to which the rule is applied.
Add	Click Add to inset the entry to the summary table below.
Cancel	Click Cancel to reset the fields to your previous configuration.
Clear	Click Clear to reset the fields back to the factory defaults.
Index	This field displays the index number of the rule. Click an index number to edit the rule.
Active	This field displays Yes when the rule is enabled and No when is it disabled.
Name	This field displays the descriptive name for this rule. This is for identification purpose only.
DSCP	This field displays the DSCP value for this rule.
Classifier	This field displays the name of the classifier to which this rule applies.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the Delete check boxes.

21.4 DSCP-to-IEEE802.1p Priority Mapping

You can configure the DSCP to IEEE802.1p mapping to allow the ES-4024A 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 49 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

21.4.1 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 74 DiffServ: DSCP Setting

DSCP	802.1p	DSCP	802.1p	DSCP	802.1p	DSCP	802.1p
0	0	1	0	2	0	3	0
4	0	5	0	6	0	7	0
8	1	9	1	10	1	11	1
12	1	13	1	14	1	15	1
16	2	17	2	18	2	19	2
20	2	21	2	22	2	23	2
24	3	25	3	26	3	27	3
28	3	29	3	30	3	31	3
32	4	33	4	34	4	35	4
36	4	37	4	38	4	39	4
40	5	41	5	42	5	43	5
44	5	45	5	46	5	47	5
48	6	49	6	50	6	51	6
52	6	53	6	54	6	55	6
56	7	57	7	58	7	59	7
60	7	61	7	62	7	63	7

Apply Cancel

The following table describes the labels in this screen.

Table 50 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 Apply to save the changes.
Cancel	Click Cancel to discard all changes and start configuring the screen again.

CHAPTER 22

Queuing Method

This chapter introduces the queuing methods supported.

22.1 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.

22.1.1 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.

22.1.2 Weighted Fair Queuing (WFQ)

Weighted Fair Queuing (WFQ) services queues based on their priority and queue weight (the number you configure in the % field – see [Figure 75 on page 146](#)). WFQ 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.

22.2 Configuring Queuing

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

Figure 75 Queuing Method

Port	Method	Q0 Weight	Q1 Weight	Q2 Weight	Q3 Weight
1	<input checked="" type="radio"/> SPQ <input type="radio"/> WFQ	10 %	20 %	30 %	40 %
2	<input checked="" type="radio"/> SPQ <input type="radio"/> WFQ	10 %	20 %	30 %	40 %
3	<input checked="" type="radio"/> SPQ <input type="radio"/> WFQ	10 %	20 %	30 %	40 %
4	<input checked="" type="radio"/> SPQ <input type="radio"/> WFQ	10 %	20 %	30 %	40 %
5	<input checked="" type="radio"/> SPQ <input type="radio"/> WFQ	10 %	20 %	30 %	40 %
21	<input checked="" type="radio"/> SPQ <input type="radio"/> WFQ	10 %	20 %	30 %	40 %
22	<input checked="" type="radio"/> SPQ <input type="radio"/> WFQ	10 %	20 %	30 %	40 %
23	<input checked="" type="radio"/> SPQ <input type="radio"/> WFQ	10 %	20 %	30 %	40 %
24	<input checked="" type="radio"/> SPQ <input type="radio"/> WFQ	10 %	20 %	30 %	40 %
25	<input checked="" type="radio"/> SPQ <input type="radio"/> WFQ	10 %	20 %	30 %	40 %
26	<input checked="" type="radio"/> SPQ <input type="radio"/> WFQ	10 %	20 %	30 %	40 %
S1	<input checked="" type="radio"/> SPQ <input type="radio"/> WFQ	10 %	20 %	30 %	40 %
S2	<input checked="" type="radio"/> SPQ <input type="radio"/> WFQ	10 %	20 %	30 %	40 %

The following table describes the labels in this screen.

Table 51 Queuing Method

LABEL	DESCRIPTION
Port	This label shows the port you are configuring.
Method	Select SPQ (Strict Priority Queuing) or WFQ (Weighted Fair Queuing). 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. Weighted Fair Queuing (WFQ) services queues based on their priority and queue weight (the number you configure in the queue % field). Queues with larger weights get more service than queues with smaller weights.
Q0~Q3 Weight %	When you select WFQ , enter the queue weight here. Bandwidth is divided across the different traffic queues according to their weights. Queues with larger weights get more service than queues with smaller weights.
Apply	Click Apply to save your changes back to the switch.
Cancel	Click Cancel to begin configuring this screen afresh.
Calculate	Click Calculate to make sure the WFQ queuing weights total to 100%; if not an error message is displayed.

CHAPTER 23

VRRP

This chapter shows you how to configure and monitor the Virtual Routing Redundancy Protocol (VRRP) on the ES-4024A.

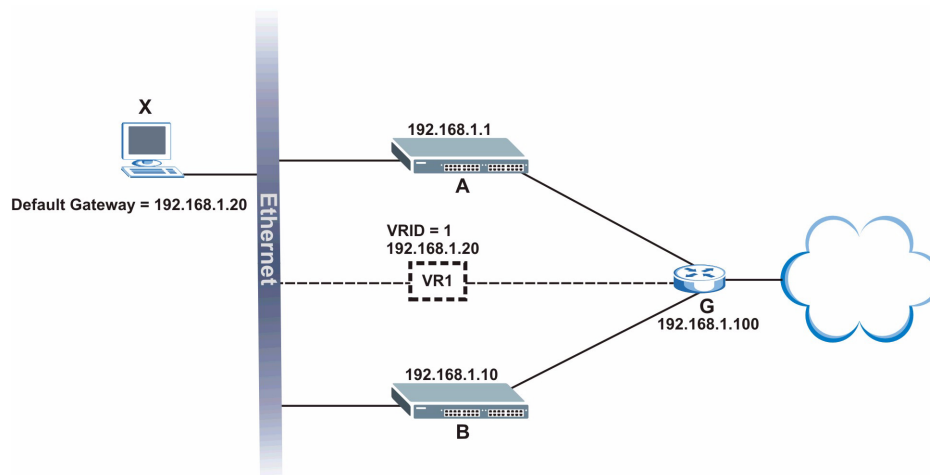
23.1 Overview

Each host on a network is configured to send packets to a statically configured default gateway (the ES-4024A). The default gateway can become a single point of failure. Virtual Routing 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 76 VRRP: Example 1



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

23.2 Viewing VRRP Status

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

Figure 77 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 52 VRRP Status

LABEL	DESCRIPTION
Index	This field displays the index number of a rule.
Active	This field displays whether a rule is enabled (Yes) or disabled (No).
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 Master indicating that the ES-4024A functions as the master router. This field is Backup indicating that the ES-4024A functions as a backup router. This field displays Init when the ES-4024A is initiating the VRRP protocol or when the Uplink Status field displays Dead .
Uplink Status	This field displays the status of the link between the ES-4024A and the uplink gateway. This field is Alive indicating that the link between the ES-4024A and the uplink gateway is up. Otherwise, this field is Dead . This field displays Probe when the ES-4024A 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 Set Interval .
Stop	Click Stop to halt system statistic polling.

23.3 Configuring VRRP

Follow the instructions in the follow sections to configure VRRP on the ES-4024A.

23.3.1 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 75](#) for more information).

Click **Advanced 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 78 VRRP Configuration: IP Interface

Index	Network	Authentication	Key	Status
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 53 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 None to disable authentication. This is the default setting. Select Simple to use a simple password to authenticate VRRP packet exchanges on this interface.
Key	When you select Simple in the Authentication field, enter a password key (up to eight printable ASCII character long) in this field.
Apply	Click Apply to save the changes.
Cancel	Click Cancel to discard all changes made in this table.

23.3.2 VRRP Parameters

This section describes the VRRP parameters.

23.3.2.1 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.

23.3.2.2 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.

23.3.2.3 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.

23.3.3 Configuring VRRP Parameters

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

Figure 79 VRRP Configuration: VRRP Parameters

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

Add Cancel Clear

The following table describes the labels in this screen.

Table 54 VRRP Configuration: VRRP Parameters

LABEL	DESCRIPTION
Active	Select this option to enable this VRRP entry.
Name	Enter a descriptive name for this VRRP entry.
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 100 by default.
Uplink Gateway	Enter the IP address of the uplink gateway in dotted decimal notation. The ES-4024A 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 0.0.0.0 .
Add	Click Add to apply the changes.
Cancel	Click Cancel to discard all changes made in this table.
Clear	Click Clear to set the above fields back to the factory defaults.

23.4 VRRP Configuration Summary

To view a summary of all VRRP configurations on the ES-4024A, scroll down to the bottom of the **VRRP Configuration** screen.

Figure 80 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 55 VRRP Configuring: VRRP Parameters

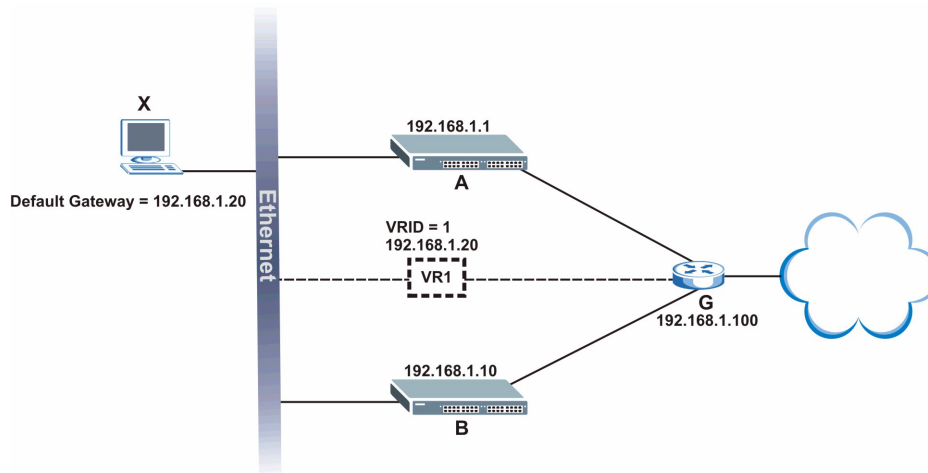
LABEL	DESCRIPTION
Index	This field displays the index number of an entry.
Active	This field shows whether a VRRP entry is enabled (Yes) or disabled (No).
Name	This field displays a descriptive name of an entry.
Network	This field displays the IP address and subnet mask of an interface.
VRID	This field 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 Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the Delete check boxes.

23.5 VRRP Configuration Examples

The following sections show two VRRP configuration examples on the ES-4024A.

23.5.1 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** (192.168.1.100). The host computer **X** is set to use **VR1** as the default gateway.

Figure 81 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 ES-4024As as shown in the figures below.

Figure 82 VRRP Example 1: VRRP Parameter Settings on Switch A

Active	<input checked="" type="checkbox"/>
Name	Example 1
Network	192.168.1.1/24
Virtual Router ID	1
Advertisement Interval	1
Preempt Mode	<input checked="" type="checkbox"/>
Priority	110
Uplink Gateway	192.168.1.100
Primary Virtual IP	192.168.1.20
Secondary Virtual IP	0.0.0.0

Figure 83 VRRP Example 1: VRRP Parameter Settings on Switch B

Active	<input checked="" type="checkbox"/>
Name	Example 1
Network	192.168.1.10/24
Virtual Router ID	1
Advertisement Interval	1
Preempt Mode	<input checked="" type="checkbox"/>
Priority	100
Uplink Gateway	192.168.1.100
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 84 VRRP Example 1: VRRP Status on Switch A

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

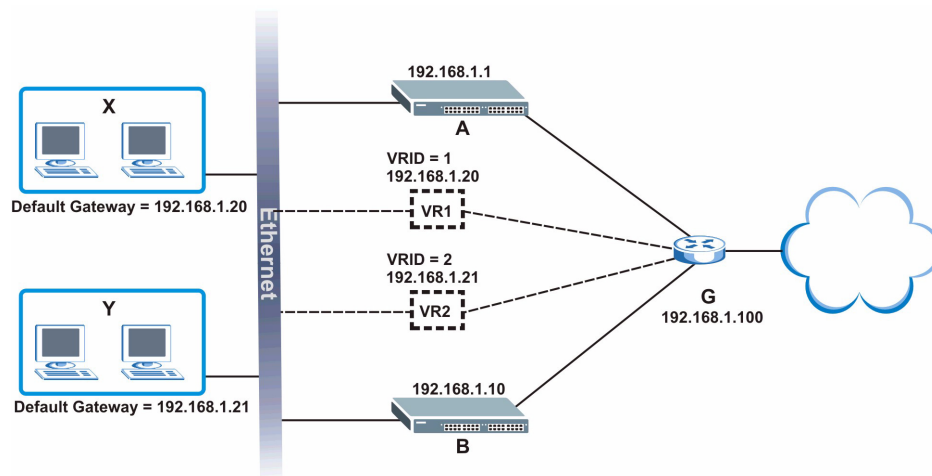
Figure 85 VRRP Example 1: VRRP Status on Switch B

VRRP Status						Configuration
Index	Active	Network	VRID	VR Status	Uplink Status	
1	Yes	192.168.1.10/24	1	Backup	Alive	

23.5.2 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 86 VRRP Configuration Example: Two Virtual Router Network

Keeping the VRRP configuration in example 1 for virtual router **VR1** (refer to [Section 23.5.2 on page 154](#)), you need to configure the **VRRP Configuration** screen for virtual router **VR2** on each switch. Configure the VRRP parameters on the ES-4024As as shown in the figures below.

Figure 87 VRRP Example 2: VRRP Parameter Settings for VR2 on Switch A

Active	<input checked="" type="checkbox"/>
Name	Example 2
Network	192.168.1.1/24
Virtual Router ID	2
Advertisement Interval	1
Preempt Mode	<input checked="" type="checkbox"/>
Priority	100
Uplink Gateway	192.168.1.100
Primary Virtual IP	192.168.1.21
Secondary Virtual IP	0.0.0.0

Figure 88 VRRP Example 2: VRRP Parameter Settings for VR2 on Switch B

Active	<input checked="" type="checkbox"/>
Name	Example 2
Network	192.168.1.10/24
Virtual Router ID	2
Advertisement Interval	1
Preempt Mode	<input checked="" type="checkbox"/>
Priority	110
Uplink Gateway	192.168.1.100
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 89 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 90 VRRP Example 2: VRRP Status on Switch B

VRRP Status						Configuration
Index	Active	Network	VRID	VR Status	Uplink Status	
1	Yes	192.168.1.10/24	2	Master	Alive	
2	Yes	192.168.1.10/24	1	Backup	Alive	

CHAPTER 24

Static Route

This chapter shows you how to configure static routes.

24.1 Configuring Static Routes

Static routes tell the ES-4024A how to forward IP traffic when you configure the TCP/IP parameters manually.

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

Figure 91 Static Routing

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

Table 56 Static Routing

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

Table 56 Static Routing (continued)

LABEL	DESCRIPTION
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your switch that will forward the packet to the destination. The gateway must be a router on the same segment as your switch.
Metric	The metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Add	Click Add to insert a new static route.
Cancel	Click Cancel to reset the above fields to your previous configuration.
Clear	Click Clear to set the above fields back to the factory defaults.
Index	This field displays the index number of the route. Click a number to edit the static route entry.
Active	This field displays Yes when the static route is activated and NO when it is deactivated.
Name	This field displays the descriptive name for this route. This is for identification purpose only.
Destination Address	This field displays the IP network address of the final destination.
Subnet Mask	This field displays the subnet mask for this destination.
Gateway Address	This field displays the IP address of the gateway. The gateway is an immediate neighbor of your switch that will forward the packet to the destination.
Metric	This field displays the cost of transmission for routing purposes.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the Delete check boxes.

CHAPTER 25

RIP

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

25.1 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 ES-4024A will broadcast its routing table periodically and incorporate the RIP information that it receives.
- **Incoming** - the ES-4024A will not send any RIP packets but will accept all RIP packets received.
- **Outgoing** - the ES-4024A will send out RIP packets but will not accept any RIP packets received.
- **None** - the ES-4024A 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 ES-4024A 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.

25.2 Configuring RIP

Click **Routing Protocol, 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 the section on IP routing domain setup).

Figure 92 RIP

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

The following table describes the labels in this screen.

Table 57 RIP

LABEL	DESCRIPTION
Active	Select this check box to enable RIP on the switch.
Index	This field displays the index number of the entry.
Network	This field displays the IP domain 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 Outgoing , Incoming , Both and None .
Version	Select the RIP version from the drop-down list box. Choices are RIP-1 , RIP-2B and RIP-2M .
Apply	Click Apply to save your changes back to the switch.
Cancel	Click Cancel to begin configuring the fields again.

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 ES-4024A supports both IGMP version 1 (**IGMP-v1**) and version 2 (**IGMP-v2**). At start up, the ES-4024A queries all directly connected networks to gather group membership. After that, the ES-4024A periodically updates this information.

26.2 Configuring IGMP

Click **Routing Protocol, 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 the section on IP routing domain setup).

Figure 93 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 58 IGMP

LABEL	DESCRIPTION
Active	Select this check box to enable IGMP on the switch. Note: You can NOT 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 58 IGMP (continued)

LABEL	DESCRIPTION
Network	This field displays the IP domain configured on the switch. Refer to the <i>IP Setup</i> section for more information on configuring IP domains.
Version	Select an IGMP version from the drop-down list box. Choices are IGMP-v1 , IGMP-v2 and None .
Apply	Click Apply to save your changes back to the switch.
Cancel	Click Cancel 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.

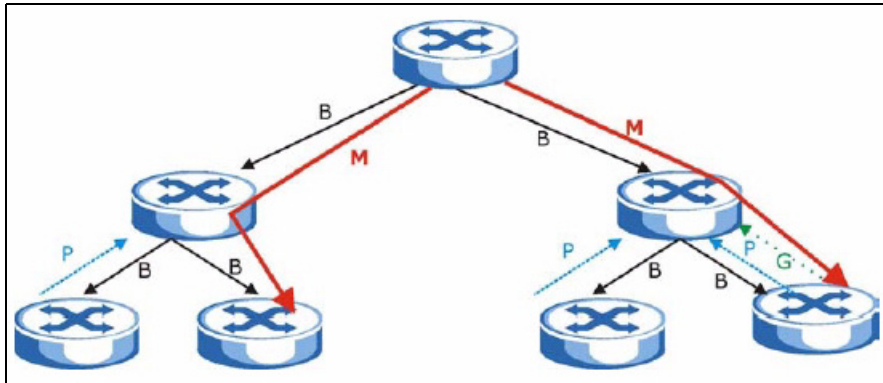
IGMP is a protocol used for joining or leaving a multicast group. You must have IGMP enabled when you enable DVMRP; otherwise you see the screen as in [Figure 96 on page 165](#).

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 94 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 **Routing Protocol, DVMRP** in the navigation panel to display the screen as shown.

Figure 95 DVMRP

Index	Network	VID	Active	Threshold
1	192.168.1.1/24	1	<input type="checkbox"/>	255

The following table describes the labels in this screen.

Table 59 DVMRP

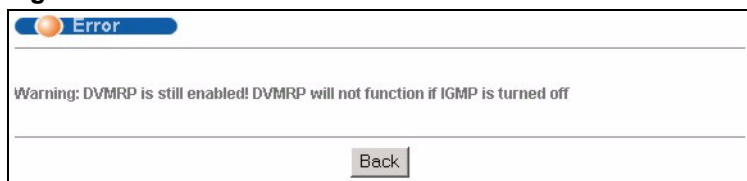
LABEL	DESCRIPTION
Active	Select Active to enable DVMRP on the switch. You should do this if you want the switch to act as a multicast router.
Index	Index is the DVMRP configuration for the IP routing domain defined under Network . The maximum number of DVMRP configurations allowed is the maximum number of IP routing domains allowed on the switch. See the IP Setup chapter for more information on IP routing domains.
Network	This is the IP routing domain IP address and subnet mask you set up in IP Setup .
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 Figure 98 on page 166).
Active	Select Active to enable DVMRP on this IP routing domain.
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.
Apply	Click Apply to save these changes to the switch.
Cancel	Click Cancel to begin configuring this part of the screen afresh.

27.3.1 DVMRP Configuration Error Messages

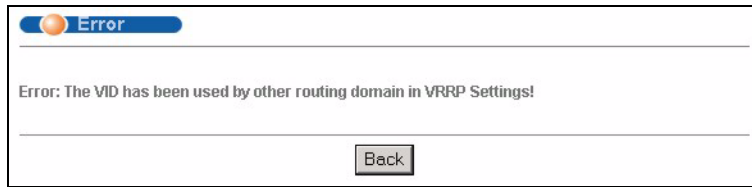
You must have IGMP/RIP enabled when you enable DVMRP; otherwise you see the screen as in the next figure.

Figure 96 DVMRP: IGMP/RIP Not Set Error

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

Figure 97 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 98 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 60 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

OSPF

This chapter describes the OSPF (Open Shortest Path First) routing protocol and shows you how to configure OSPF on the ES-4024A.

28.1 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 61 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

28.1.1 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.

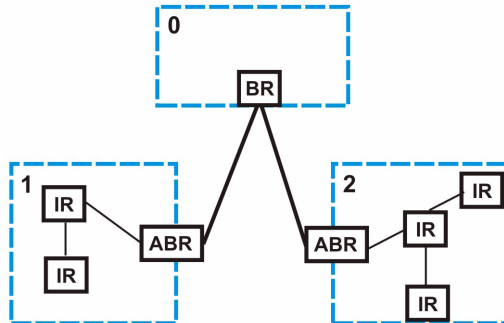
The following table describes the four classes of OSPF routers.

Table 62 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 99 OSPF Network Example



28.1.2 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.

28.1.3 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.

28.1.4 Configuring OSPF

To configure OSPF on the ES-4024A, 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.

28.2 OSPF Status

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

Figure 100 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 63 OSPF Status

LABEL	DESCRIPTION
OSPF	This field displays whether OSPF is activated (Running) or not (Down).
Interface	The text box displays the OSPF status of the interface(s) on the ES-4024A.
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 Set Interval .
Stop	Click Stop to end OSPF status polling.

The following table describes some common output fields.

Table 64 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 ES-4024A.
Transmit Delay	This field displays the transmission delay in seconds.
State	This field displays the state of the ES-4024A (backup or DR (designated router)).
Priority	This field displays the priority of the ES-4024A. 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 ES-4024A.
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 (backup or DR (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.

28.3 Enabling OSPF and General Settings

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

Figure 101 OSPF Configuration: Activating and General Settings

The screenshot shows the OSPF Configuration interface with the following fields and options:

- Active:**
- Router ID:** 0.0.0.0
- Redistribute Route:**
 - RIP:** Type: 1 Metric value: 15
 - Static:** Type: 1 Metric value: 15
- Buttons:** Apply, Cancel
- Area Settings:**
 - Active:**
 - Name:** name
 - Area ID:** 0.0.0.0
 - Authentication:** None
 - Stub Network:**
 - No Summary:**
 - Default route cost:** 15
- Buttons:** Add, Cancel, Clear
- Table Headers:** Index, Active, Name, Area ID, Authentication, Stub Network, Delete
- Buttons:** Delete, Cancel

The follow table describes the related labels in this screen.

Table 65 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 ES-4024A in an OSPF. Enter a unique ID (that uses the format of an IP address in dotted decimal notation) for the ES-4024A.
Redistribute Route	Route redistribution allows your ES-4024A to import and translate external routes learned through other routing protocols (RIP and Static) into the OSPF network transparently.
Active	Select this option to activate route redistribution for routes learn through the selected protocol.
Type	Select 1 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 2 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 Apply to save the changes.
Cancel	Click Cancel to start configuring the above fields again.

28.4 Configuring OSPF Areas

To ensure that the ES-4024A 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 102 OSPF Configuration: Area Setup

The following table describes the related labels in this screen.

Table 66 OSPF Configuration: Area Setup

LABEL	DESCRIPTION
Active	Select this option to enable an area.
Name	Enter a descriptive name for an area.

Table 66 OSPF Configuration: Area Setup (continued)

LABEL	DESCRIPTION
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 0.0.0.0 indicates that this is a backbone (also known as Area 0). You can create only one backbone area on the ES-4024A.
Authentication	Select an authentication method (Simple or MD5) to activate authentication. Select None 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 0.0.0.0 in the Area ID field, the settings in the Stub Area fields are ignored.
No Summary	Select this option to set the ES-4024A 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 Add to apply the changes.
Cancel	Click Cancel to start configuring the above fields again.
Clear	Click Clear to set the above fields back to the factory defaults.

28.4.1 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 103 OSPF Configuration: Summary Table

Index	Active	Name	Area ID	Authentication	Stub Network	Delete
1	Yes	Example	192.168.1.1	None	Yes	<input type="checkbox"/>

The following table describes the related labels in this screen.

Table 67 OSPF Configuration: Summary Table

LABEL	DESCRIPTION
Index	This field displays the index number of an area.
Active	This field displays whether an area is enabled (Yes) or not (No).
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 0.0.0.0 indicates the backbone.
Authentication	This field displays the authentication method used (None , Simple or MD5).
Stub Network	This field displays whether an area is a stub network (Yes) or not (No).

Table 67 OSPF Configuration: Summary Table (continued)

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

28.5 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 75](#) 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 104 OSPF Interface

Index	Active	Network	Area ID	Authentication	Key ID	Key	Cost
1	<input type="checkbox"/>	172.21.4.73/16	0.0.0.0	Same-as-Area	1		15
2	<input type="checkbox"/>	192.168.1.1/24	0.0.0.0	Same-as-Area	1		15

Apply Cancel

The following table describes the labels in this screen.

Table 68 OSPF Interface

LABEL	DESCRIPTION
Index	This field displays the index number for an interface.
Active	Select this option to enable an interface.
Network	This field displays the IP interface information.
Area-ID	Enter 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>Note: OSPF Interface(s) must use the same authentication method within the same area.</p> <p>Select an authentication method. Choices are Same-as-Area, None (default), Simple and MD5.</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 Same-as-Area to use the same authentication method within the area and set the related fields when necessary.</p> <p>Select None to disable authentication. This is the default setting.</p> <p>Select Simple and set the Key field to authenticate OSPF packets transmitted through this interface using simple password authentication.</p> <p>Select MD5 and set the Key ID and Key fields to authenticate OSPF packets transmitted through this interface using MD5 authentication.</p>

Table 68 OSPF Interface (continued)

LABEL	DESCRIPTION
Key ID	When you select MD5 in the Authentication field, specify the identification number of the authentication you want to use.
Key	When you select Simple in the Authentication field, enter a password eight-character long. Characters after the eighth character will be ignored. When you select MD5 in the Authentication 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.
Apply	Click Apply to save the changes.
Cancel	Click Cancel to start configuring the above fields again.

28.6 Configuring OSPF Virtual Links

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

Figure 105 OSPF Virtual Link

The following table describes the labels in this screen.

Table 69 OSPF Virtual Link

LABEL	DESCRIPTION
Active	Select this option to enable this virtual link.
Name	Enter a descriptive name for this virtual link.
Area ID	Enter the ID of a transit area in dotted decimal notation.
Peer Router ID	Enter the ID of a peer border router.

Table 69 OSPF Virtual Link (continued)

LABEL	DESCRIPTION
Authentication	<p>Note: Virtual interface(s) must use the same authentication method within the same area.</p> <p>Select an authentication method. Choices are Same-as-Area, None (default), Simple and MD5.</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 Same-as-Area to use the same authentication method within the area and set the related fields when necessary.</p> <p>Select None to disable authentication. This is the default setting.</p> <p>Select Simple to authenticate OSPF packets transmitted through this interface using a simple password.</p> <p>Select MD5 to authenticate OSPF packets transmitted through this interface using MD5 authentication.</p>
Key ID	When you select MD5 in the Authentication field, specify the identification number of the authenticate you want to use.
Key	<p>When you select Simple in the Authentication field, enter a password eight-character long.</p> <p>When you select MD5 in the Authentication field, enter a password 16-character long.</p>
Add	Click Add to apply the changes.
Cancel	Click Cancel to start configuring the above fields again.
Clear	Click Clear to set the above fields back to the factory defaults.
Index	This field displays an index number of an entry.
Active	This field displays whether a virtual link is enabled (Yes) or disabled (No).
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 (Same-as-Area , None , Simple or MD5).
Key ID	When the Authentication field displays MD5 , this field displays the identification number of the key used.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the Delete check boxes.

CHAPTER 29

Maintenance

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

29.1 The Maintenance Screen

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

Figure 106 Maintenance



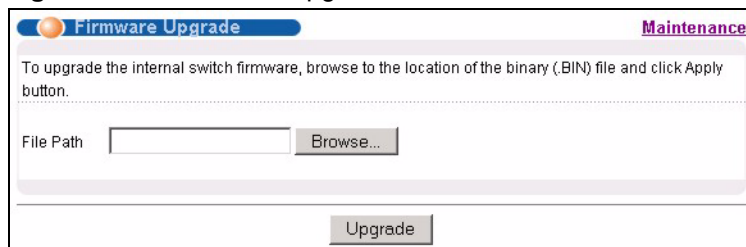
29.2 Firmware Upgrade

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 107 Firmware Upgrade



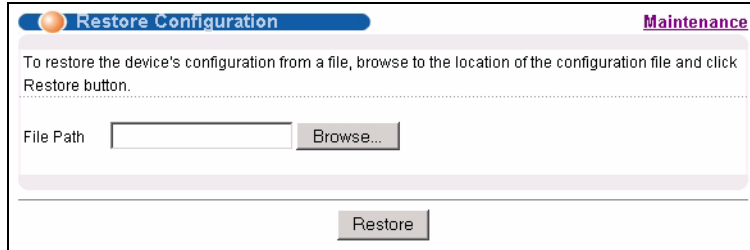
Type the path and file name of the firmware file you wish to upload to the switch in the **File Path** text box or click **Browse** to locate it. After you have specified the file, click **Upgrade**.

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

29.3 Restore a Configuration File

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

Figure 108 Restore Configuration



The screenshot shows a web interface for restoring configuration. At the top, there is a blue header with 'Restore Configuration' and a purple 'Maintenance' link. Below the header, a text 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, there is a 'File Path' label, an empty text input field, and a 'Browse...' button. At the bottom of the form is a 'Restore' button.

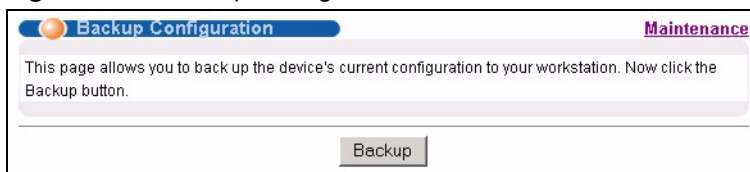
Type the path and file name of the configuration file you wish to restore in the **File Path** text box or click **Browse** to display the **Choose File** screen (below) from which you can locate it. After you have specified the file, click **Restore**. "config" is the name of the configuration file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

29.4 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 109 Backup Configuration



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

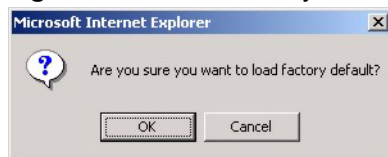
- 3 Choose a location to save the file on your computer from the **Save in** drop-down list box and type a descriptive name for it in the **File name** list box. Click **Save** to save the configuration file to your computer.

29.5 Load Factory Defaults

Follow the steps below to reset the ES-4024A back to the factory defaults.

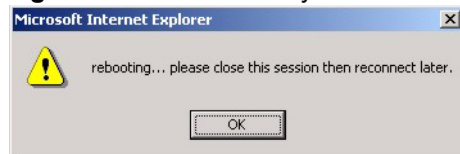
- 1 In the **Maintenance** screen, click the **Click Here** button next to **Load Factory Defaults** to clear all switch configuration information you configured and return to the factory defaults. The following message appears.

Figure 110 Load Factory Default: Conformation



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

Figure 111 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).

29.6 Reboot System

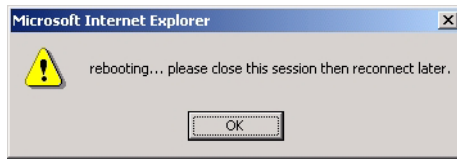
Reboot System allows you to restart the switch without physically turning the power off. Follow the steps below to reboot the ES-4024A.

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

Figure 112 Reboot System: Confirmation



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

Figure 113 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.

29.7 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.

29.7.1 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 70 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.

29.7.1.1 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.

29.7.2 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 70 on page 180](#) for more information on filename conventions.
- 7 Enter “quit” to exit the ftp prompt.

29.7.3 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).

29.7.4 FTP over WAN Restrictions

FTP over WAN will not work when:

- Telnet service is disabled in **Secured Client Sets**.
- The IP address(es) in the **Secured Client Sets** menu does not match the client IP address. If it does not match, the switch will disconnect the Telnet session immediately.

CHAPTER 30

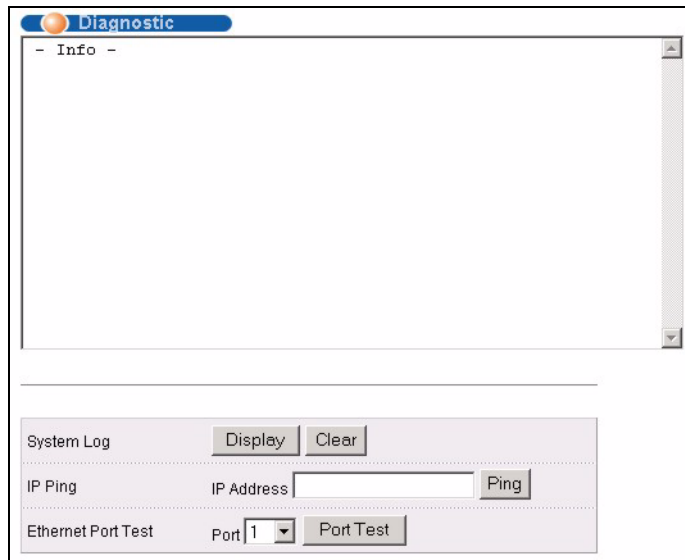
Diagnostic

This chapter explains the **Diagnostic** screen.

30.1 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 114 Diagnostic



The following table describes the labels in this screen.

Table 71 Diagnostic

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

CHAPTER 31

Cluster Management

This chapter introduces cluster management.

31.1 Overview

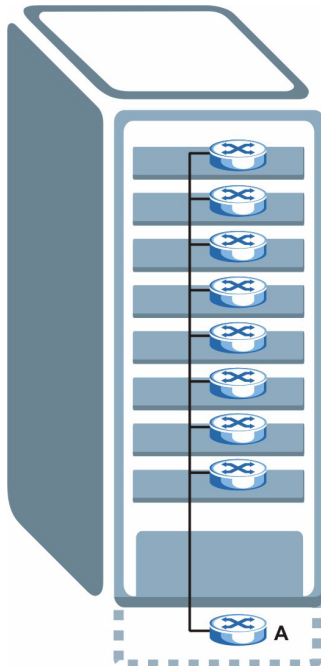
Cluster Management allows you to manage switches through one switch, called the cluster manager. The switches must be directly connected and be in the same VLAN group so as to be able to communicate with one another.

Table 72 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 115 Clustering Application Example



31.2 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 116 Cluster Management: Status

Index	HwAddr	Name	Model	Status
1	00:a0:c5:5e:df:f9	Cluster Memeber 1	ES-4024	OnLine

The following table describes the labels in this screen.

Table 73 Cluster Management: Status

LABEL	DESCRIPTION
Status	This field displays the role of this switch within the cluster. Manager Member (you see this if you access this screen in the cluster member switch directly and not via the cluster manager) None (neither a manager nor a member of a cluster)
Manager	This field displays the cluster manager switch's hardware MAC address.
The Number of Member	This field displays the number of switches that make up this cluster. The following fields describe the cluster member switches.
Index	You can manage cluster member switches via the cluster manager switch. Each number in the Index column is a hyperlink leading to the cluster member switch's web configurator (see Figure 117 on page 187).
HwAddr	This is the cluster member switch's hardware MAC address.
Name	This is the cluster member switch's System Name .
Model	This field displays the model name.
Status	This field displays: Online (the cluster member switch is accessible) Error (for example the cluster member switch password was changed or the switch was set as the manager and so left the member list, etc.) Offline (the switch is disconnected - Offline shows approximately 1.5 minutes after the link between cluster member and manager goes down)

31.2.1 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 117 Cluster Management: Cluster Member Web Configurator Screen



31.2.1.1 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 118 Example: Uploading Firmware to a Cluster Member Switch

```

ftp 192.168.1.1
Connected to 192.168.1.1.
220 ES-4024A FTP version 1.0 ready at Sat Jan 01 00:11:33 2000
User (192.168.1.1:(none)):
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           1810050 Jul 01 12:00 ras
-rw-rw-rw-  1 owner   group           262144 Jul 01 12:00 rom-0
--w--w--w-  1 owner   group              0 Jul 01 12:00 fw-00-a0-c5-5e-df-f9
-rw-rw-rw-  1 owner   group           0 Jul 01 12:00 config-00-a0-c5-5e-df-f9
-f9
226 File sent OK
ftp: 296 bytes received in 0.00Seconds 296000.00Kbytes/sec.
ftp> bin
200 Type I OK
ftp> put 350dulb2.rom config-00-a0-c5-5e-df-f9
200 Port command okay
150 Opening data connection for STOR config-00-a0-c5-5e-df-f9
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 74 FTP Upload to Cluster Member Example

FTP PARAMETER	DESCRIPTION
User	Press [ENTER].
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.
350dulb2.bin	The name of the firmware file you want to upload to the cluster member switch.
fw-00-a0-c5-5e-df-f9	The cluster member switch's firmware name as seen in the cluster manager switch.
config-00-a0-c5-5e-df-f9	The cluster member switch's configuration file name as seen in the cluster manager switch.

31.3 Configuring Cluster Management

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

Figure 119 Clustering Management Configuration

The following table describes the labels in this screen.

Table 75 Clustering Management Configuration



LABEL	DESCRIPTION
Clustering Manager	
Active	Select Active to have this switch become the cluster manager switch. A cluster can only have one manager. Other (directly connected) switches that are set to be cluster managers will not be visible in the Clustering Candidates list. If a switch that was previously a cluster member is later set to become a cluster manager, then its Status is displayed as Error in the Cluster Management Status screen and a warning icon () appears in the member summary list below.
Name	Type a name to identify the Clustering Manager . You may use up to 20 printable characters (no spaces are allowed).
VID	This is the Management VLAN ID and is only applicable if the switch is set to 802.1Q VLAN. All switches must be in the same management VLAN group to belong to the same cluster. Switches that are not in the same management VLAN group are not visible in the Clustering Candidates list. This field is ignored if the Clustering Manager is using Port-based VLAN.
Apply	Click Apply to save the changes.
Cancel	Click Cancel to begin configuring this part of the screen afresh.
Clustering Candidate	The following fields relate to the switches that are potential cluster members.

Table 75 Clustering Management Configuration (continued)

LABEL	DESCRIPTION
List	A list of suitable candidates found by auto-discovery is shown here. The switches must be directly connected. Directly connected switches that are set to be cluster managers will not be visible in the Clustering Candidate list. Switches that are not in the same management VLAN group will not be visible in the Clustering Candidate list.
Password	Each cluster member's password is its web configurator password. Select a member in the Clustering Candidate list and then enter its web configurator password. If that switch administrator changes the web configurator password afterwards, then it cannot be managed from the Cluster Manager . Its Status is displayed as Error in the Cluster Management Status screen and a warning icon () appears in the member summary list below. If multiple devices have the same password then hold [SHIFT] and click those switches to select them. Then enter their common web configurator password.
Add	Click Add to save this part of the screen to the switch.
Cancel	Click Cancel to begin configuring this part of the screen afresh.
Refresh	Click Refresh to perform auto-discovery again to list potential cluster members.
The next summary table shows the information for the clustering members configured.	
Index	This is the index number of a cluster member switch.
HwAddr	This is the cluster member switch's hardware MAC address.
Name	This is the cluster member switch's System Name .
Model	This is the cluster member switch's model name.
Remove	Select this checkbox and then click the Remove button to remove a cluster member switch from the cluster.
Cancel	Click Cancel to begin configuring this part of the screen afresh.

CHAPTER 32

MAC Table

This chapter introduces the MAC Table screen.

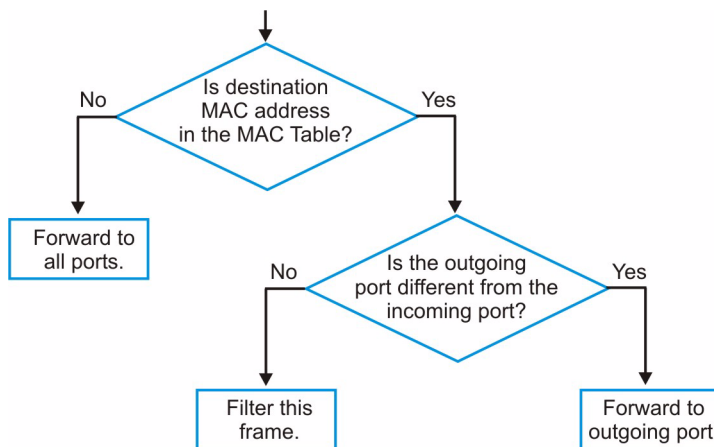
32.1 Overview

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.

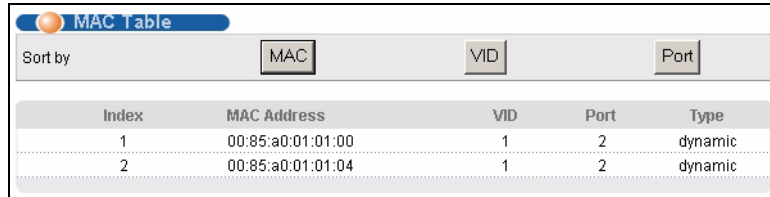
Figure 120 MAC Table Flowchart



32.2 Viewing the MAC Table

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

Figure 121 MAC Table



Index	MAC Address	VID	Port	Type
1	00:85:a0:01:01:00	1	2	dynamic
2	00:85:a0:01:01:04	1	2	dynamic

The following table describes the labels in this screen.

Table 76 MAC Table

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

CHAPTER 33

IP Table

This chapter introduces the IP table.

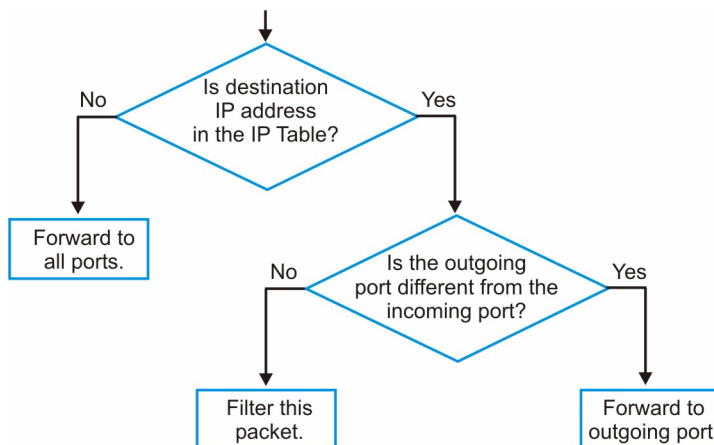
33.1 Overview

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 122 IP Table Flowchart



33.2 Viewing the IP Table

Click **Management, IP Table** in the navigation panel to display the following screen. The IP table can hold up to 16K entries.

Figure 123 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 77 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 CPU to indicate the IP address belongs to the switch.
Type	This shows whether the IP address is dynamic (learned by the switch) or static (belonging to the switch).

CHAPTER 34

ARP Table

This chapter introduces ARP Table.

34.1 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.

34.1.1 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.

34.2 Viewing 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 124 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 78 ARP Table

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

CHAPTER 35

Routing Table

This chapter introduces the routing table.

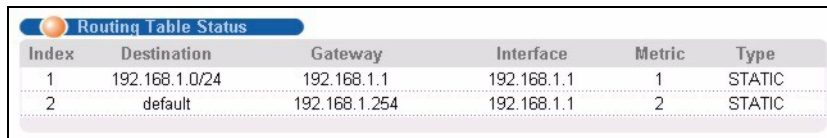
35.1 Overview

The routing table contains the route information to the network(s) that the ES-4024A can reach. The ES-4024A automatically updates the routing table with the RIP information received from other Ethernet devices.

35.2 Viewing the Routing Table

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

Figure 125 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	default	192.168.1.254	192.168.1.1	2	STATIC

The following table describes the labels in this screen.

Table 79 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 36

DHCP Server Status

This chapter shows you how to view the DHCP server status.

36.1 Overview

The **DHCP Server Status** screen displays the summary table about the DHCP server(s) you configured in the **DHCP** screen. You can also view detail DHCP server information in the **Server Status Detail** screen.

36.2 Displaying DHCP Server Status

Click **Management, DHCP Server Status** in the navigation panel to display the screen as shown.

Figure 126 DHCP Server Status

Index	VID	Server Status	IP Pool Size
1	1	192.168.1.20	100
2	2	172.21.1.10	100

Polling Interval(s)

The following table describes the labels in this screen.

Table 80 DHCP Server Status

LABEL	DESCRIPTION
Index	This field displays the index number.
VID	This field displays the ID of the VLAN to which the DHCP server belongs. Click on a VID to display detail server information (refer to Section 36.3 on page 200).

Table 80 DHCP Server Status (continued)

LABEL	DESCRIPTION
Server Status	This field displays the starting IP address of the client address pool.
IP Pool Size	This field displays the count 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 Set Interval .
Stop	Click Stop to halt polling statistics.

36.3 Displaying Detail DHCP Server Information

To view detail DHCP server information (such as client addresses and IP address lease time), click a VID in the **DHCP Server Status** screen.

Figure 127 DHCP Server Status Detail

Server Status Detail		DHCP Server Status		
Start IP Address	192.168.1.20			
End IP Address	192.168.1.119			
Subnet Mask	255.255.255.0			
Default Gateway	192.168.1.1			
Primary DNS Server	0.0.0.0			
Secondary DNS Server	0.0.0.0			
Address Leases				
Index	IP Address	Timer	Hardware Address	Hostname
1	192.168.1.20	259899	00:85:a0:01:01:04	TW1808
Polling 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 81 DHCP Server Status Detail

LABEL	DESCRIPTION
Start IP Address	The field displays the first of the contiguous addresses in the IP address pool
End IP Address	The field displays the last of the contiguous addresses in the IP address pool
Subnet Mask	This field displays the subnet mask in dotted decimal notation.
Default Gateway	This field displays the IP address (in dotted decimal notation) of the default gateway device.
Primary DNS Server	This field displays the IP address (in dotted decimal notation) of the primary DNS server.
Secondary DNS Server	This field displays the IP address (in dotted decimal notation) of the secondary DNS server.

Table 81 DHCP Server Status Detail (continued)

LABEL	DESCRIPTION
Address Leases	
Index	This field displays the index number.
IP Address	This field displays the IP address assigned to a DHCP client device.
Timer	This field displays the time (in seconds) the DHCP client is allowed to use the assigned IP address.
Hardware Address	This field displays the MAC address (in hexadecimal notation) of the DHCP client device.
Hostname	This field displays the DHCP client device name.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking Set Interval .
Stop	Click Stop to halt polling statistics.

CHAPTER 37

Introducing the Commands

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

37.1 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.

37.1.1 Switch Configuration File

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

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

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.

37.2 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.

37.2.1 Access Priority

- You can only access the CLI with the administrator account (the default password is **1234**).
- By default, only one concurrent access to the CLI is allowed via either the console port or Telnet. Console port access has higher priority.

37.2.2 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

37.2.2.1 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 37.3 on page 205](#)).

Figure 128 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...
```

37.2.3 Telnet

Use the following steps to telnet into your switch.

- 1** 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 IP address) and click **OK**.
- 2** A login screen displays (refer to [Section 37.3 on page 205](#)).

37.3 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, and enter the password (“1234” is the default for the default administrator login with the “admin” username).

Figure 129 CLI: Login Screen

```
Enter Password : XXXX
```

37.4 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.

37.5 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.

37.5.1 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 130 CLI Help: List of Commands: Example 1

```
ras> help
  Commands available:

  help
  logout
  exit
  history
  enable
  show hardware-monitor <C|F>
  show system-information
  ping <ip|host-name> <cr>
  traceroute <ip|host-name> <cr>
  traceroute <ip|host-name> [ttl <1-255>[..]]
  traceroute help
ras>
```

Figure 131 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
  traceroute     Exec traceroute
ras>
```

37.5.2 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 132 CLI Help: Detailed Command Information: Example 1

```

ras> ping help
Usage: ping <hostid>
ras>

```

Figure 133 CLI: Help: Detailed Command Information: Example 2

```

ras> ping ?
      <ip|host-name>          destination ip address
ras>

```

37.6 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, `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.

37.7 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 134 CLI: History Command Example

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

37.8 Saving Your Configuration

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

Figure 135 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.

37.8.1 Logging Out

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

37.9 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.

37.9.1 User Mode

The following table describes the commands available for User mode.

Table 82 Command Summary: User Mode

COMMAND		DESCRIPTION
enable		Accesses Enable (or privileged) mode. See Section 37.9.2 on page 209 .
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>	Sends a Ping request to an Ethernet device.
show	hardware-monitor <C F>	Displays current hardware monitor information with the specified temperature unit (Celsius C or Fahrenheit F).
	system-information	Displays general system information.
traceroute	<ip host-name> [ttl <1-255>] [wait <1-60>] [queries <1-10>]	Determines the path a packet takes to a device.

37.9.2 Enable Mode

The following table describes the commands available for Enable mode.

Table 83 Command Summary: Enable Mode

COMMAND		DESCRIPTION
baudrate	<1 2 3 4 5>	Changes the console port speed. Choices are 1 (9600), 2 (19200), 3(38400), 4 (57600) and 5 (115200).
boot		Restarts the switch.
configure		Accesses Configuration mode. See Section 37.9.3 on page 212 .
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.
logout		Exits Enable (or privileged) mode.

Table 83 Command Summary: Enable Mode (continued)

COMMAND			DESCRIPTION
no	logging		Disables syslog logging.
ping	<IP host-name>		Sends Ping request to an Ethernet device.
reload			Restarts the system.
show			
	bandwidth-control		Displays bandwidth control settings.
	broadcast-storm-control		Displays broadcast storm control settings.
	classifier		Displays all classifier related information.
		[name]	Displays the specified classifier related information.
	cluster		Displays cluster management status.
		candidates	Displays cluster candidate information.
		member	Displays the MAC address of the cluster member(s).
		member mac <mac-addr>	Displays the status of the cluster member(s).
		members config	Displays the configuration of the cluster member(s).
	dhcp	relay	Displays DHCP relay settings.
		server	Displays DHCP server settings.
		server <vlan-id>	Displays DHCP server settings in a specified VLAN.
	diffserv		Displays general DiffServ settings.
	filter		Displays filter settings.
	garp		Displays GARP information.
	hardware-monitor	<C F>	Displays current hardware monitor information with the specified temperature unit (Celsius C or Fahrenheit F).
	interface <port-number>		Displays current interface status.
	interfaces config <port-list>		Displays current interface configuration.
		egress	Displays outgoing port information.
		broadcast-storm-control	Displays broadcast storm control settings.
		port-access-authentication	Displays port authentication settings.
		port-security	Displays port MAC address learning settings.
		spanning-tree	Displays STP settings on the port.

Table 83 Command Summary: Enable Mode (continued)

COMMAND		DESCRIPTION	
	ip arp	Displays the ARP table.	
	ip dvmrp	Displays DVMRP settings.	
	ip igmp	Displays IGMP settings.	
	ip iptable	static	Displays static IP address table.
		all <sort>	Displays the IP address table. You can sort by MAC address, VID or port.
	ip route		Displays IP route information.
		static	Displays static IP route information.
	ip ospf	database	Displays OSPF link state database information.
		interface	Displays OSPF interface settings.
		neighbor	Displays OSPF neighbor information.
	lacp		Displays LACP (Link Aggregation Control Protocol) settings.
	logging		Displays system logs.
	mac	address-table all <sort>	Displays MAC address table. You can sort by MAC address, VID or port.
		static	Displays static MAC address table.
	mac-aging-time		Displays MAC learning aging time.
	marking-rule		Displays the OSCP-IEEE802.11q mappings.
	mirror		Displays port mirroring settings.
	port-access-authenticator		Displays all port authentication settings.
	radius-server		Displays RADIUS server settings.
	remote-management		Displays all secured client information.
		[index]	Displays the specified secured client information.
	router		
		dvmrp	Displays DVMRP settings.
		igmp	Displays IGMP settings.
		rip	Displays RIP settings.
		ospf	Displays OSPF settings.
		ospf area	Displays OSPF area settings.
		ospf network	Displays OSPF network (or interface) settings.
		ospf redistribute	Displays OSPF redistribution settings.

Table 83 Command Summary: Enable Mode (continued)

COMMAND		DESCRIPTION	
	ospf virtual-link	Displays OSPF virtual link settings.	
	vrrp	Displays VRRP settings.	
	running-config	Displays current operating configuration.	
	service-control	Displays service control settings.	
	snmp-server	Displays SNMP settings.	
	spanning-tree	config	Displays Spanning Tree Protocol (STP) settings.
	system-information		Displays general system information.
	time		Displays current system time and date.
	timesync		Displays time server information.
	trunk		Displays link aggregation information.
	vlan		Displays the status of all VLANs.
		<vlan-id>	Displays the status of the specified VLAN.
	vlanlq	gvrp	Displays GVRP settings.
		port-isolation	Displays port isolation settings.
traceroute	<ip host-name> [ttl <1-255>] [wait <1-60>] [queries <1-10>]		Determines the path a packet takes to a device.
	help		Displays command information.
write	memory		Saves current configuration to the configuration file the switch is currently using.

37.9.3 General Configuration Mode

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

Table 84 Command Summary: Configuration Mode

COMMAND		DESCRIPTION	
admin-password	<pw-string> <confirm-string>	Changes the administrator password.	
bandwidth-control	classifier <classifier-name> maximal-bandwidth <kbps>	Enables bandwidth control for a traffic flow.	
		inactive	Disables bandwidth control for a traffic flow.
broadcast-storm-control			Enables broadcast storm control on the switch.

Table 84 Command Summary: Configuration Mode (continued)

COMMAND		DESCRIPTION
	direction <incoming outgoing>	Sets broadcast storm control direction.
	monitor-interval <64 1024 8000 256000 >	Sets monitor interval in microseconds.
classifier	<name> < [ethernet-type <ether- num ip ipx arp rarp appletalk decnet sna netbios dlc>] [vlan<vlan-id>] [source-mac <src- mac-addr>] [source- port <port-num>] [destination-mac <dest-mac-addr>] [destination-port <port-num>] [ip-protocol <protocol- num tcp udp icmp egg ospf rsvp igmp igp pim dvmrp ipsec>] [source-ip <src-ip- addr> [mask-bits <mask-bits>]] [source-socket <socket-num>] [destination-ip <dest-ip-addr> [mask-bits <mask- bits>]] [destination-socket <socket-num>] [inactive] >	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 command information.
cluster	<vlan-id>	Sets the management VID for the cluster.
	name <cluster name>	Sets the name to identify the cluster manager.
	member <mac-address> password <password- str>	Adds a member to the cluster.
	rcommand <mac- address>	Removes a member from the cluster.

Table 84 Command Summary: Configuration Mode (continued)

COMMAND		DESCRIPTION
dhcp	relay <vlan-id> helper-address <remote-dhcp- server1>	Enables and sets the DHCP server settings for DHCP relay in the VLAN.
		inactive
	relay <vlan-id> helper-address <remote-dhcp- server2>	Enables and sets the DHCP server settings for DHCP relay in the VLAN.
		inactive
	relay <vlan-id> helper-address <remote-dhcp- server3>	Enables and sets the DHCP server settings for DHCP relay in the VLAN.
		inactive
	server <vlan-id> starting-address <ip-addr> <subnet- mask> size-of- client-ip-pool <1- 253> [default- gateway <ip-addr>] [primary-dns <ip- addr>] [secondary- dns <ip-addr>]	Enables DHCP server for the specified DHCP client IP address pool.
diffserv		Enables DiffServ.
	default-dscp <0-63>	Sets the default DSCP.
	dscp <0-63> priority <0-7>	Sets the DSCP-to-IEEE 802.1q mappings.
exit		Exits from the CLI.
filter	classifier <classifier-name>	Enables filtering to drop the classified traffic flow.
		inactive
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.
igmp-snooping		Enables IGMP snooping.

Table 84 Command Summary: Configuration Mode (continued)

COMMAND		DESCRIPTION
interface	port-channel <port-list>	Enables a port or a list of ports for configuration. See Section 37.9.4 on page 223 for more details.
	route-domain <ip-address>/<mask-bits>	Enables a routing domain for configuration. See Section 37.9.5 on page 225 for more details.
ip	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.
logins	username <name> password <pwd>	Configures up to four read-only login accounts to log into the web configurator.
logout		Exits from the CLI.
mac-aging-time	<10-3000>	Sets learned MAC aging time.
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.
marking-rule	classifier <classifier-name> dscp <0-63>	Enables DSCP marking rule for the specified classifier.
		inactive Disables DSCP marking rule for the specified classifier.
mirror	classifier <classifier-name>	Enables port mirroring on a traffic flow.
		inactive Disables port mirroring on a traffic flow.
mirror-port		Enables port mirroring.
	<port-num>	Enables port mirroring on a specified port.

Table 84 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION
mode	zynos		Changes the CLI mode to the ZyNOS format.
no	bandwidth-control		Disable bandwidth control on the switch.
	broadcast-storm-control		Disables broadcast storm control on the switch.
	classifier <name>		Disables the classifier. Each classifier has one rule. If you disable a classifier you cannot use rule related information.
		inactive	Enables a classifier.
	cluster		Disables cluster management on the switch.
		member <mac-address>	Removes the cluster member.
	dhcp	relay	Disables DHCP relay.
		server <vlan-id>	Disables DHCP server settings.
		server default-gateway	Disables DHCP server default gateway settings.
		server primary-dns	Disables DHCP primary DNS server settings.
		server secondary-gateway	Disables DHCP server secondary gateway settings.
	diffserv		Disables the DiffServ settings.
	filter classifier <classifier-name>		Disables filtering (traffic blocking) for a classifier.
		inactive	Enables filtering (traffic blocking) for a classifier.
	igmp-snooping		Disables IGMP snooping.
	ip route <ip> <mask>		Removes a specified IP static route.
		inactive	Enables a specified IP static route.
	lACP		Disables the link aggregation control protocol (dynamic trunking) on the switch.
	logins <name>		Disables login access to the specified name.
	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).

Table 84 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION
		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).
	marking-rule classifier <classifier-name>		Disables DSCP marking rule on a classifier.
		inactive	Enables DSCP marking rule on a classifier.
	mirror classifier <classifier-name>		Disables port mirroring on a traffic flow.
		inactive	Enables port mirroring on a traffic flow.
	mirror-port		Disables port mirroring on the switch.
	port-access- authenticator		Disables port authentication on the switch.
	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.
		service <telnet ftp http icmp snmp>	Disables a secure client set entry number from using the selected remote management service(s).
	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.
		icmp	Disables ICMP access to the switch such as pinging and tracerouting.
		snmp	Disables SNMP management.
		telnet	Disables telnet access to the switch.

Table 84 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION
	snmp-server	trap-destination <ip>	Disables sending of SNMP traps to a station.
	spanning-tree		Disables STP.
	timesync		Disables timeserver settings.
	trunk	<T1 T2 T3 T4 T5>	Disables the specified trunk group.
		lacp	Disables LACP in the trunk groups.
	vlan	<vlan-id>	Deletes the static VLAN entry.
	vlanlq	gvrp	Disables GVRP on the switch.
		port-isolation	Disables port isolation.
password	<password>		Change the password for Enable mode.
port-access-authenticator			Enables 802.1x authentication on the switch.
queue	level <0-7> priority <0-3>		Sets the priority level-to-physical queue mapping.
radius-server	host <ip> [acct-port <socket-number>] [key <key-string>]		Sets the IP address of the external RADIUS server, UDP port and shared key.
remote-management	<index>		Enables a remote management setting.
		start-addr <ip> end-addr <ip> service <telnet ftp http icmp snmp>	Specifies a group of trusted computer(s) from which an administrator may use a service to manage the switch.
router	dvmrp		Enables and enters the DVMRP configuration mode.
		exit	Leaves the DVMRP configuration mode.
		threshold <t1- value>	Sets the DVMRP threshold value.
	igmp		Enables and enters the IGMP configuration mode.
		exit	Leaves the IGMP configuration mode.
	ospf <router-id>		Enables and enters the OSPF configuration mode.
		area <area-id>	Enables and sets the area ID.
		area <area-id> authentication	Enables simple authentication for the area.

Table 84 Command Summary: Configuration Mode (continued)

COMMAND		DESCRIPTION
	<code>area <area-id> authentication message-digest</code>	Enables MD5 authentication for the area.
	<code>area <area-id> default-cost <0- 65535></code>	Sets the cost to the area.
	<code>area <area-id> name <name></code>	Sets a descriptive name for the area for identification purposes.
	<code>area <area-id> stub</code>	Enables and sets the area as a stub area.
	<code>area <area-id> stub no-summary</code>	Sets the stub area not to send any LSA (Link State Advertisement).
	<code>area <area-id> virtual-link <router-id></code>	Sets the virtual link ID information for the area.
	<code>area <area-id> virtual-link <router-id> authentication- key <key></code>	Enables simple authentication and sets the authentication key for the specified virtual link in the area.
	<code>area <area-id> virtual-link <router-id> authentication- same-as-area</code>	Sets the virtual link to use the same authentication method as the area.
	<code>area <area-id> virtual-link <router-id> message-digest- key <keyid> md5 <key></code>	Enables MD5 authentication and sets the key ID and key for the virtual link in the area.
	<code>area <area-id> virtual-link <router-id> name <name></code>	Sets a descriptive name for the virtual link for identification purposes.
	<code>exit</code>	Leaves the router OSPF configuration mode.
	<code>network <ip-addr/ bits> area <area- id></code>	Creates an OSPF area.
	<code>no area <area-id></code>	Removes the specified area.
	<code>no area <area-id> authentication</code>	Sets the area to use no authentication (None).
	<code>no area <area-id> default-cost</code>	Sets the area to use the default cost (15).

Table 84 Command Summary: Configuration Mode (continued)

COMMAND		DESCRIPTION	
		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.
		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	Sets the switch to learn RIP 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	Sets the switch to learn static routing 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.

Table 84 Command Summary: Configuration Mode (continued)

COMMAND		DESCRIPTION
	vrrp network <ip-address>/<mask-bits> vr-id <1-7> uplink-gateway <ip>	Adds a new VRRP network and enters the VRRP configuration 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).
	preempt	Enables preemption mode.
	primary-virtual-ip <ip>	Sets the primary VRRP virtual gateway IP address.
	priority <1 .. 254>	Sets the priority of the switch in the VRRP network.
	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>	Allows HTTP access on the specified service port.
	igmp	Allows IGMP management for Ping, traceroute, etc..
	snmp	Allows SNMP management.
	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.

Table 84 Command Summary: Configuration Mode (continued)

COMMAND		DESCRIPTION
	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.
	hello-time <1-10> maximum-age <6 .. 40> forward-delay <4 .. 30>	Sets Hello Time.
	help	Displays help information.
	priority <0-61440>	Sets the bridge priority of the switch. Note: The priority value MUST be a multiple of 4096.
broadcast storm-control		Enables broadcast storm control on the switch.
	direction <incoming outgoing>	Sets the direction of the traffic.
	monitor-interval <64 1024 8000 256000>	Sets the monitoring interval (in microseconds).
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>	Activates a trunk group.
	<T1 T2 T3 T4 T5>lacp	Enables LACP for a trunk group.
	<T1 T2 T3 T4 T5> end-port <port>	Sets the last port in 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 Section 37.9.6 on page 226 for more information.
vlan-type	<802.1q port-based>	Specifies the VLAN type.

Table 84 Command Summary: Configuration Mode (continued)

COMMAND		DESCRIPTION
vlan1q	gvrp	Enables GVRP.
	port-isolation	Enables port-isolation.

37.9.4 interface port-channel Commands

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

Table 85 interface port-channel Commands

COMMAND		DESCRIPTION
interface port-channel <port-list>		Enables a port or a list of ports for configuration.
	broadcast-storm-control	incoming <frames> Limits the number of incoming broadcast frame the switch store. frames = 1, 2, 3 4, 6, 8, 12, 16, 24, 32, 48, 64, 96, 128, 192, 256, 384, 512, 768, 1024, 1536, 2048, 3072, 4096, 6144, 8192, 12288, 16384, 24576 or 32767.
		help Displays command information.
	diffserv	Enables DiffServ on the port(s).
	egress set <port-list>	Sets the outgoing traffic port list for a port-based VLAN.
	exit	Exits from the interface port-channel command mode.
	flow-control	Enables interface flow control. Flow control regulates transmissions to match the bandwidth of the receiving port.
	frame-type <all tagged untagged>	Choose to accept both tagged and untagged incoming frames or just tagged/untagged incoming frames on a port.
	gvrp	Enables this function to permit VLAN groups beyond the local switch.
	help	Displays a description of the interface port-channel commands.
	inactive	Disables the specified port(s) on the switch.

Table 85 interface port-channel Commands (continued)

COMMAND		DESCRIPTION
	ingress-check	Enables the device to discard incoming frames for VLANs that are not included in a port member set.
	name <port-name-string>	Sets a name for the port(s). Enter a descriptive name (up to nine printable ASCII characters).
	no	egress set <port-list>
		exit
		flow-control
		gvrp
		inactive
		ingress-check
		port-access-authenticator
		port-access-authenticator reauthenticate
		port-security
		port-security learn inactive
		spanning-tree
		vlan-trunking
	port-access-authenticator	
		reauthenticate
		reauth-period <reauth-period>
	port-security	
		learn inactive
		address-limit <number>
	pvid <1-4094>	

Table 85 interface port-channel Commands (continued)

COMMAND			DESCRIPTION
	qos priority	<0 .. 7>	Sets the quality of service priority for an interface.
	spanning-tree		Enables STP on the port(s).
		path-cost <1-65535>	Sets the STP path cost for the specified port(s).
		priority <0-255>	Sets the priority for the specified port(s).
	speed-duplex	<auto 10-half 10-full 100-half 100-full 1000-full>	Sets the duplex mode (half or full) and speed (10, 100 or 1000 Mbps) of the connection on the interface. Selecting auto (auto-negotiation) makes one port able to negotiate with a peer automatically to obtain the connection speed and duplex mode that both ends support.
	spq		Sets the port(s) to use Strict Priority Queuing.
	test		Performs an interface loopback test.
	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.
	wfq		Sets the port(s) to use Weighted Fair Queuing (WFQ).
		<wt0> <wt1> <wt2> <wt3>	Sets the interface to use WFQ. A weight value of one to eight is given to each variable from wt1 to wt3.

37.9.5 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 86 interface route-domain Commands

COMMAND			DESCRIPTION
interface route-domain <ip-address>/ <mask-bits>			Enables a routing domain for configuration.
	exit		Exits from the interface routing-domain command mode.
	ip	dvmrp	Enables this function to permit VLAN groups beyond the local switch.
		igmp <v1 v2>	Enables IGMP in this routing domain.
		ospf authentication-key <keyid> md5 <key>	Enables OSPF authentication in this routing domain and sets the security key.
		ospf authentication-same-as-area	Sets the same OSPF authentication settings in the routing domain as the associated area.
		ospf cost <1-65535>	Sets the OSPF cost in this routing domain.
		ospf message-digest-key <k>	Sets the OSPF authentication key in this routing domain.
		rip direction <Outgoing Incoming Both None> version <v1 v2b v2m>	Sets the RIP direction and version 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-same-as-area	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.

37.9.6 config-vlan Commands

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

Table 87 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 management IP address and subnet mask of the switch in the specified VLAN.
	name <name-str>		Specifies a name for identification purposes.
	no	fixed <port-list>	Sets fixed port(s) to normal port(s).
		forbidden <port-list>	Sets forbidden port(s) to normal port(s).
		untagged <port-list>	Specifies the port(s) you want to tag all outgoing frames transmitted with this VLAN Group ID.
		inactive	Enables the specified VLAN.
		ip address <ip-address> <mask>	Deletes the IP address and subnet mask from this VLAN.
	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.

CHAPTER 38

Command Examples

This chapter describes some commands in more detail.

38.1 Overview

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

38.2 show Commands

These are the commonly used `show` commands.

38.2.1 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 136 show system-information Command Example

```
ras> show system-information
System Name       : ES-4024A
System Contact   :
System Location  :
Ethernet Address  : 00:a0:c5:01:23:45
ZyNOS F/W Version : V3.60(TV.0) | 04/13/2005
RomRasSize       : 1975760
System up Time   : 3:24:45 (12bf25 ticks)
Bootbase Version : V1.01 | 03/09/2005
ZyNOS CODE       : RAS Apr 13 2005 21:27:18
Product Model    : ES-4024A
ras>
```

38.2.2 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 137 show hardware-monitor Command Example

```
ras> show hardware-monitor c
Temperature Unit : (c)
Temperature      Current  MAX    MIN    Threshold  Status
MAC              41.0   41.0   27.0    65.0       Normal
CPU              37.5   37.5   26.5    65.0       Normal
PHY              36.5   36.5   26.5    65.0       Normal

FAN Speed (RPM)  Current  MAX    MIN    Threshold  Status
FAN1             5681    5720   5529   4500       Normal
FAN2             5760    5800   5642   4500       Normal
FAN3             5882    5924   5760   4500       Normal
FAN4             5720    5720   5566   4500       Normal

Voltage (V)      Current  MAX    MIN    Threshold  Status
2.5              2.496   2.512   2.480   +/-5       Normal
1.8              1.824   1.824   1.824   +/-5       Normal
3.3              3.328   3.328   3.312   +/-5       Normal
12.0             12.099  12.099  12.099  +/-5       Normal
5.0              5.024   5.024   5.024   +/-5       Normal
1.1              1.104   1.120   1.088   +/-10      Normal
ras>
```

38.2.3 show logging

Note: This command is not available in User mode.

Syntax:

```
show logging
```

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

Figure 138 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.

38.2.4 show interface

Syntax:

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

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

Figure 139 show interface Command Example

```

ras# show interface 2
ES-4024A# show interface 2
Port Info      Port NO.      :2
                Link           :100M/F
                Status        :FORWARDING
                LACP           :Disabled
                TxPkts         :1244
                RxPkts         :6220
                Errors         :0
                Tx KBs/s       :0.0
                Rx KBs/s       :0.0
                Up Time        :   3:27:15
ras#

```

38.2.5 show mac address-table

Syntax:

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

Where

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

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

Figure 140 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#
```

38.3 ping

Syntax:

```
ping <ip|host-name>
```

where

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

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 141 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#
```

38.4 traceroute

Syntax:

```
traceroute <ip|host-name> [<ttl <1-255>] [wait <1-60>] [queries  
<1-10>]>
```

where

<code><ip hostname></code>	=	The IP address or hostname of an Ethernet device.
<code>[ttl <1-255>]</code>	=	Specifies the Time To Live (TTL) period.
<code>[wait <1-60>]</code>	=	Specifies the time period to wait.
<code>[quesries <1-10>]</code>	=	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 142 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:
```

38.5 Restarting the Switch

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` command to restart the switch. The following example restarts the switch to use the second configuration file.

Figure 143 CLI: boot Command Example

```
ras# boot
```

Use the `reload` command to restart the system. The following example restarts the system to use the second configuration file.

Figure 144 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.

38.5.1 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 configuration file.

The following example resets configuration file to the factory default settings.

Figure 145 CLI: Reset to the Factory Default Example

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

38.6 no Command Examples

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

38.6.1 no mirror-port

Syntax:

```
no mirror-port
```

Disables port mirroring on the switch.

An example is shown next.

Figure 146 no mirror-port Command Example

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

38.6.2 no trunk

Syntax:

```
no trunk <T1|T2|T3|T4|T5>
no trunk <T1|T2|T3|T4|T5> lacp
```

where

<T1 T2 T3 T4 T5>	Disables the trunk group.
<T1 T2 T3 T4 T5> lacp	Disables LACP in the trunk group.

- An example is shown next.
- Disable trunk one (T1).
- Disable LAPC on trunk three (T3).

Figure 147 no trunk Command Example

```
ras(config)# no trunk T1
ras(config)# no trunk T3 lacp
```

38.6.3 no port-access-authenticator

Syntax:

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

where

	= Disables port authentication on the switch.
<port-list>	= Specifies the port(s).

An example is shown next.

- Disable port access authentication on the switch.
- Disable port access authentication on ports 10 to 15.
- Disable reauthentication on the ports.

Figure 148 no port-access-authenticator Command Example

```
ras(config)# no port-access-authenticator
ras(config)# interface port-channel 10-15
ras(config-interface)# no port-access-authenticator
ras(config-interface)# no port-access-authenticator reauthenticate
```

38.7 interface Commands

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

38.7.1 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 149 interface Command Example

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

38.7.2 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 150 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)#

```

38.7.3 filter

Syntax:

```
filter classifier <classifier-name>
```

where

<classifier-name> Specifies the name of the classifier to which this rule applies.

This command sets the switch to drop the traffic flow defined by a classifier.

An example is shown next.

- Create a classifier to define all IP traffic in VLAN 1 from port 3 to the destination device with a MAC address of 00:a0:c5:00:00:01.
- Enable filtering on that traffic flow.

Figure 151 filter Command Example

```
ras(config)# classifier Example ethernet-type ip vlan 1 source-port 3
destination-mac 00:a0:c5:00:00:01
ras(config)# filter classifier Example
```

38.7.4 mirror

Syntax:

```
mirror classifier <classifier-name>
mirror-port <port-num>
```

where

<classifier-name> Specifies the name of the classifier to which this rule applies.
<port-num> This is the mirror port number.

This command sets the switch to copy the incoming/outgoing traffic flow defined by a classifier to the specified mirror port.

An example is shown next.

- Create a classifier to define all IP traffic in VLAN 1 from port 3 to the destination device with a MAC address of 00:a0:c5:00:00:01.
- Enable mirroring on the classifier.
- Enable the monitor port three.

Figure 152 mirror Command Example

```
ras(config)# mirror classifier Example
ras(config)# mirror-port 3
```

38.7.5 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 153 gvrp Command Example

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

38.7.6 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 154 ingress-check Command Example

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

38.7.7 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 155 frame-type Command Example

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

38.7.8 spq

Syntax:

```
spq
```

Sets the interface to use Strict Priority Queuing (SPQ).

An example is shown next.

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

Figure 156 spq Command Example

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

38.7.9 wfq

Syntax:

```
wfq <wt0> <wt1> <wt2> <wt3>
```

where

Enables WFQ (Weighted Fair Queuing) queuing method on the switch.

<wt0> <wt1>
<wt2> <wt3> Sets the interface to use WFQ queuing. A weight value of one to eight is given to each variable from wt0 to wt3.

An example is shown next.

- Enable port two and ports six to twelve for configuration.
- Enable Weighted Fair Queuing method on the ports.
- Set the queue weights from Q0 to Q3.

Note: Make sure the WFQ queuing weights total to 100.

Figure 157 wfq Command Example

```

ras# configure
ras(config)# interface port-channel 2,6-12
ras(config-interface)# wfq
ras(config-interface)# wfq 40 30 20 10

```

38.7.10 egress set

Syntax:

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

where

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

An example is shown next.

- Enable port-based VLAN tagging on the switch.
- Enable ports one, three, four and five for configuration.
- Set the outgoing traffic ports as the CPU (0), seven (7), eight (8) and nine (9).

Figure 158 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

```

38.7.11 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 159 qos priority Command Example

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

38.7.12 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 160 name Command Example

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

38.7.13 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 161 speed-duplex Command Example

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

38.8 Activating RSTP on the Stacking Module

The following procedure shows you how to activate RSTP on the stacking module (port 25 and 26).

- 1 Access the port interface commands for ports 25 and 26.

```
interface port-channel 25,26
```

- 2 Enabling RSTP on the ports.

```
spanning-tree
```


CHAPTER 39

IEEE 802.1Q Tagged VLAN Commands

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

39.1 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.

39.2 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).

39.2.1 Static Entries (SVLAN Table)

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

39.2.2 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.

39.3 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 162 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 163 CPU VLAN Configuration and Activation Example

```

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

```

39.4 Global VLAN1Q Tagged VLAN Configuration Commands

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

39.4.1 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 164 GARP STATUS Command Example

```

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

```

39.4.2 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 165 GARP Timer Command Example

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

39.4.3 GVRP Timer

Syntax:

```
show vlan1q gvrp
```

This command shows the switch's GVRP settings.

An example is shown next.

Figure 166 GVRP Status Command Example

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

39.4.4 Enable GVRP

Syntax:

```
vlan1q gvrp
```

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

39.4.5 Disable GVRP

Syntax:

```
no vlan1q gvrp
```

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

39.5 Port VLAN Commands

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

39.5.1 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 167 vlan1q port default vid Command Example

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

39.5.2 Set Acceptable Frame Type

Syntax:

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

where

<all|tagged|untagged> = Specifies the Ethernet frames (tagged, untagged or all) the switch accepts.

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 168 frame type Command Example

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

39.5.3 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 169 no gvrp Example

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

39.5.4 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.

39.5.4.1 Modify a Static VLAN Table Example

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

Figure 170 Modifying Static VLAN Example

```

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

```

39.5.4.2 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.

39.5.5 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 171 no vlan Command Example

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

39.6 Enable VLAN

Syntax:

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

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

39.7 Disable VLAN

Syntax:

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

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

39.8 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 172 show vlan Command Example

```
ras# show vlan
802.1Q VLAN Static Entry:
idx. Name          VID  Active  AdCtl / TagCtl
-----
  0             1   1 active  FFFFFFFFFFFFFFFFFFFFFFFFFF
                1   1 active  UUUUUUUUUUUUUUUUUUUUUUUUU
  1      Example   2   active  -----F-----
                2   1 active  TTTTTTTTTTTTTTTTTTTTTTTT
ras#
```


CHAPTER 40

Troubleshooting

This chapter covers potential problems and possible remedies.

40.1 Problems Starting Up the Switch

Table 88 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.

40.2 Problems Accessing the Switch

Table 89 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.

40.2.1 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.

40.2.1.1 Internet Explorer Pop-up Blockers

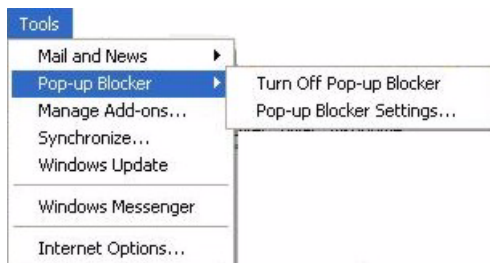
You may have to disable pop-up blocking to log into your device.

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.

40.2.1.1.1 Disable pop-up Blockers

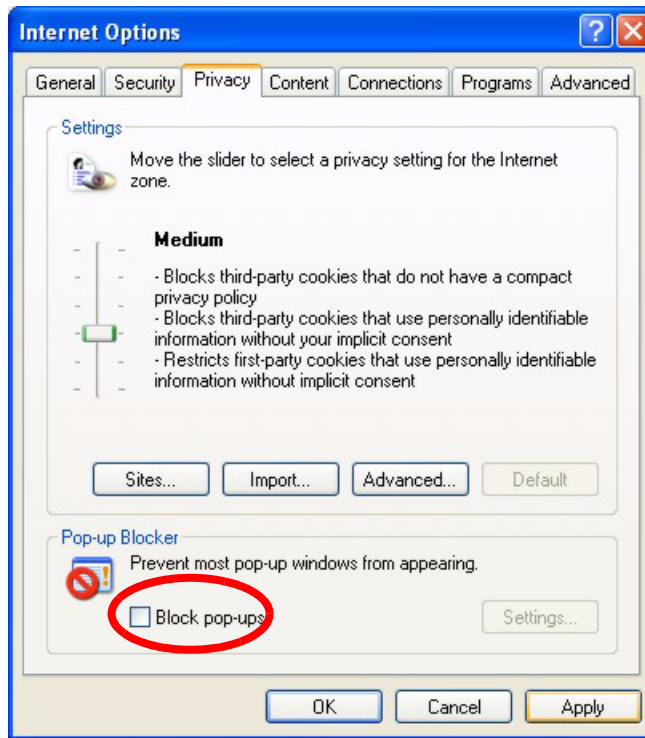
- 1 In Internet Explorer, select **Tools, Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 173 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.

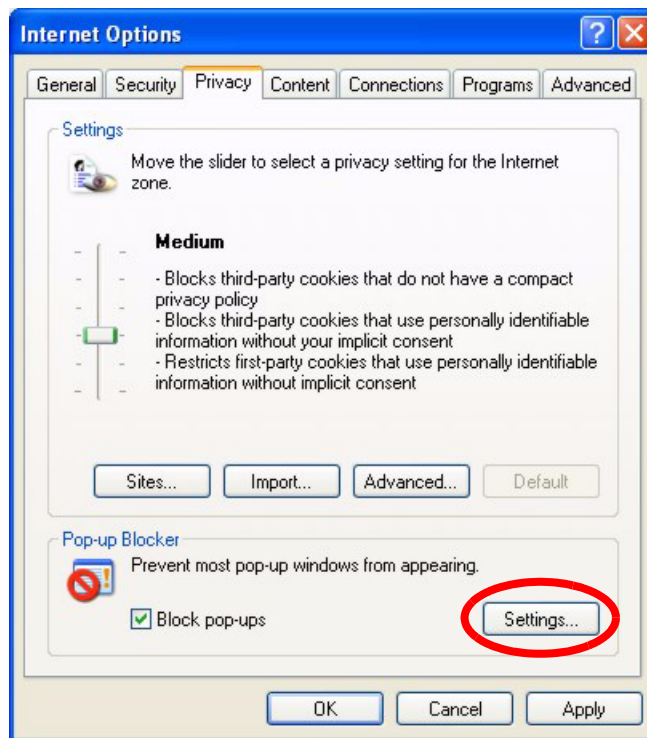
Figure 174 Internet Options

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

40.2.1.1.2 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 175 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 176 Pop-up Blocker Settings

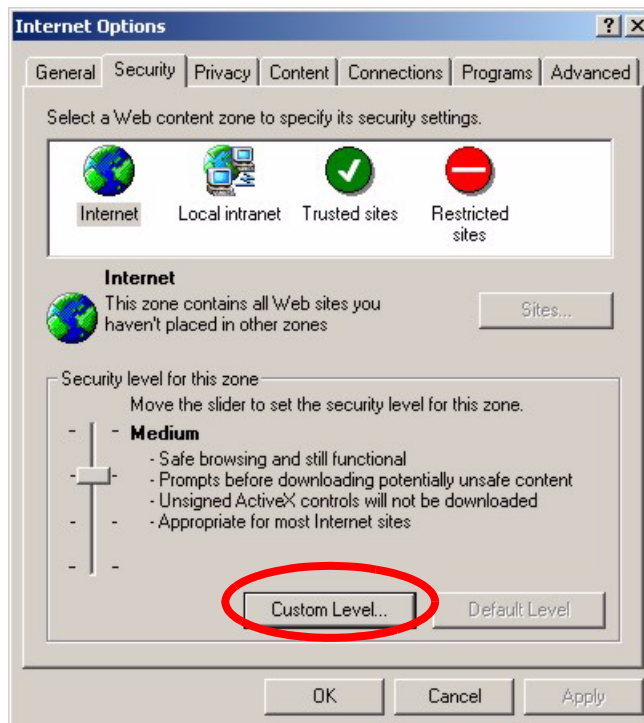
5 Click **Close** to return to the **Privacy** screen.

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

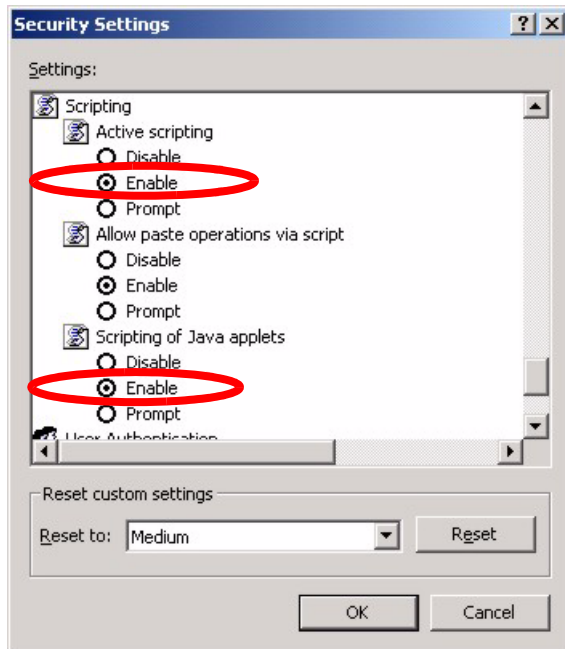
40.2.1.2 JavaScripts

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.

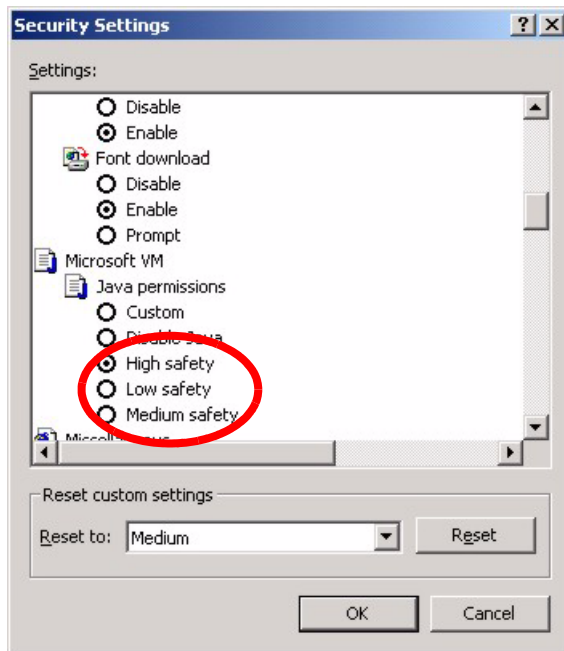
Figure 177 Internet Options

- 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 178 Security Settings - Java Scripting

40.2.1.3 Java Permissions

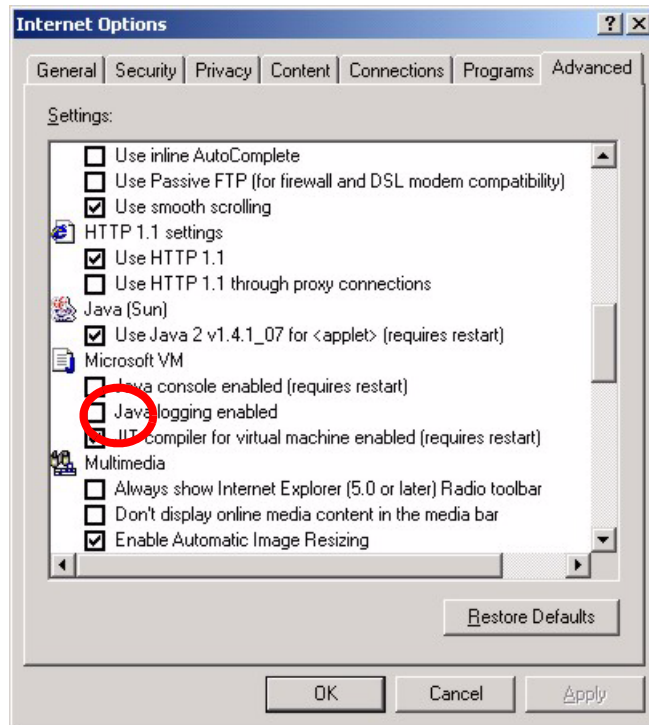
- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Security** tab.
- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Microsoft VM**.
- 4 Under **Java permissions** make sure that a safety level is selected.
- 5 Click **OK** to close the window.

Figure 179 Security Settings - Java

40.2.1.3.1 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 180 Java (Sun)



40.3 Problems with the Password

Table 90 Troubleshooting the Password

PROBLEM	CORRECTIVE ACTION
Cannot access the switch.	The password field is case sensitive. Make sure that you enter the correct password using the proper casing.
	The administrator username is "admin". The default administrator password is "1234". The username and password are case-sensitive. Make sure that you enter the correct password and username using the proper casing. If you have changed the password and have now forgotten it, you will need to upload the default configuration file. This restores all of the factory defaults including the password.

APPENDIX A

Product Specifications

These are the ES-4024A product specifications.

Table 91 General Product Specifications

Ethernet Interface		24 10/100 Base-TX interfaces Auto-negotiation Auto-MDI/MDIX Compliant with IEEE 802.3/3u Back pressure flow control for half duplex Flow control for full duplex (IEEE 802.3x) RJ-45 Ethernet cable connector Rate limiting at 1Kbps steps
Uplink Interface		Two Gigabit/mini-GBIC ports
Stacking Interface		One stacking module with two 1000Base-T ports
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: 12.8Gbps, non-blocking Max. Frame size: 1522 bytes Forwarding frame: IEEE 802.3, IEEE 802.1q, Ethernet II, PPPoE Prevent the forwarding of corrupted packets
	STP	IEEE 802.1d spanning tree protocol IEEE 802.1w, rapid reconfiguration to recover network failure
	QoS	IEEE 802.1p Four 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 Fast Ethernet: three groups (up to 8 ports for each group) Gigabit: one group Stacking: one group
	Port mirroring	All ports support port mirroring
	Bandwidth control	Supports rate limiting at 1Kbps increment Supports IGMP snooping

Table 91 General Product Specifications (continued)

Layer 3 Features	IP forwarding	Wire-speed 16K 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 92 Management Specifications

System Control	Alarm/Status surveillance LED indication for alarm and system status Performance monitoring Line speed Four RMON groups (history, statistics, alarms, and events) Throughput monitoring CMP packet transmission Port mirroring and aggregation Spanning Tree Protocol IGMP snooping Firmware upgrade and download through FTP/TFTP 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 SNMP HP OpenView interface (version 6.1 and above) RMON groups (history, statistics, alarms and events)
MIB	RFC1213 MIB II RFC1493 Bridge MIB RFC1643 Ethernet MIB RFC1757 Four groups of RMON RFC2674 Bridge MIB extension

Table 93 Physical and Environmental Specifications

LEDs	Per switch: S1, S2, PWR, SYS, ALARM Per Ethernet port: LNK/ACT, FDX/COL
Dimension	438 mm (W) x 270 mm (D) x 44.45 mm (H) Standard 19" rack mountable
Weight	3.6Kg
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 input: 100-240VAC, 50/60Hz, 1.5A 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 94 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 95 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 96 “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 97 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 98 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 99 Subnet 1

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

Table 100 Subnet 2

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

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

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

Example: Four Subnets

The above example illustrated using a 25-bit subnet mask to divide a class “C” address space into two subnets. Similarly to divide a class “C” address into four subnets, you need to “borrow” two host ID bits to give four possible combinations of 00, 01, 10 and 11. The subnet mask is 26 bits (11111111.11111111.11111111.11000000) or 255.255.255.192. Each subnet contains 6 host ID bits, giving 2^6-2 or 62 hosts for each subnet (all 0’s is the subnet itself, all 1’s is the broadcast address on the subnet).

Table 101 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 102 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 103 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 104 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 105 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	223	254	255

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

Table 106 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 94 on page 269](#)) available for subnetting.

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

Table 107 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 [107](#)

Numerics

110V AC [3](#)
 230V AC [3](#)
 802.1P priority [78](#)

A

AC [3](#)
 Access control [125](#)
 Access priority [125](#)
 Limitation [125](#)
 Login account [128](#)
 Remote management [130](#)
 Service port [129](#)
 SNMP [126](#)
 Accessories [3](#)
 Address Resolution Protocol (ARP) [195](#)
 Administrator password [129](#)
 Aggregator ID [109](#)
 Aging time [74](#)
 Airflow [3](#)
 Alternative Subnet Mask Notation [271](#)
 American Wire Gauge [3](#)
 Application [33](#)
 Backbone [33](#)
 Bridging [33](#)
 IEEE 802.1Q VLAN [34](#)
 Switched workgroup [34](#)
 Area 0 [167](#)
 Area Border Router (ABR) [167](#)
 Area ID [173](#), [174](#)
 ARP [195](#)
 How it works [195](#)
 View [195](#)
 AS Boundary Router [167](#)
 Authentication [172](#), [173](#), [174](#), [176](#)
 Authority [2](#)

Automatic VLAN registration [80](#)
 Autonomous system (AS) [31](#), [163](#), [167](#)
 AWG [3](#)

B

Backbone [167](#)
 Backbone Router (BR) [167](#)
 Bandwidth control
 Maximum bandwidth [101](#)
 Basement [3](#)
 Basic setting [69](#)
 BPDUs (Bridge Protocol Data Units) [96](#)
 Bridge Protocol Data Units (BPDUs) [96](#)
 Broadcast frames [104](#)
 Broadcast storm control [103](#)
 Direction [104](#)

C

Cables, Connecting [3](#)
 CFI (Canonical Format Indicator) [79](#)
 Change password [54](#)
 Changes or Modifications [2](#)
 CLI Commands [205](#)
 Class of Service (CoS) [139](#)
 Classifier [133](#)
 Ethernet Type [134](#)
 CLI Command
 Configure tagged VLAN example [246](#)
 Static VLAN Table example [251](#)
 Cluster management [32](#), [185](#)
 Cluster manager [185](#), [189](#)
 Cluster member [185](#), [189](#)
 Cluster member firmware upgrade [187](#)
 Network example [185](#)
 Setup [188](#)
 Specification [185](#)
 Status [186](#)
 Switch models [185](#)
 VID [189](#)
 Web configurator [187](#)
 Cluster manager [185](#)

- Cluster member [185](#)
- Command
 - Forwarding Process Example [251](#)
 - Summary [208](#)
 - Syntax conventions [205](#)
- Command Line Interface
 - Accessing [203](#)
 - Introduction [203](#)
- Configuration file [55](#)
 - Backup [178](#)
 - Restore [55, 178](#)
- Configure QoS [133](#)
- Connecting Cables [3](#)
- Console port [32](#)
 - Settings [41](#)
- Copyright [1](#)
- Corrosive Liquids [3](#)
- Covers [3](#)
- CPU management port [86](#)
- CRC (Cyclic Redundant Check) [67](#)
- Current date [72](#)
- Current time [72](#)
- Customer Support [5](#)

D

- Damage [3](#)
- Dampness [3](#)
- Danger [3](#)
- Database Description (DD) [168](#)
- Default gateway [118](#)
- Denmark, Contact Information [5](#)
- DHCP [29, 117, 199](#)
 - Client IP pool [118](#)
 - Modes [117](#)
 - Relay agent [117, 121](#)
 - Remote DHCP server [121](#)
 - Server [117, 118](#)
 - Setup [117](#)
 - Status [118, 119, 121, 122, 199](#)
- DHCP (Dynamic Host Configuration Protocol) [29, 117](#)
- Diagnostic [183](#)
 - Ethernet port test [183](#)
 - Ping [183](#)
 - System log [183](#)
- Differentiated Service (DiffServ) [139](#)
- DiffServ [139](#)
 - Activate [140](#)
 - Default DSCP value [141](#)
 - DS field [139](#)
 - DSCP [139](#)

- DSCP-to-IEEE802.1p mapping [142](#)
 - Marking rule [141](#)
 - Network example [139](#)
 - PHB [139](#)
- DNS server [200](#)
- DS (Differentiated Services) [139](#)
- DSCP
 - Default value [141](#)
 - DSCP-to-IEEE802.1p mapping [142](#)
 - Service level [139](#)
 - What it does [139](#)
- DSCP (DiffServ Code Point) [139](#)
- Dust [3](#)
- DVLAN Table [245](#)
- DVMRP
 - Autonomous system [31, 163](#)
 - Default timer setting [166](#)
 - Error message [165](#)
 - Graft [164](#)
 - How it works [163](#)
 - Implementation [163](#)
 - Probe [164](#)
 - Prune [164](#)
 - Report [164](#)
 - Setup [164](#)
 - Terminology [164](#)
 - Threshold [165](#)
- DVMRP (Distance Vector Multicast Routing Protocol) [31, 163](#)
- Dynamic link aggregation [107](#)

E

- Egress port [89](#)
- Electric Shock [3](#)
- Electrical Pipes [3](#)
- Electrocution [3](#)
- Ethernet broadcast address [195](#)
- Ethernet port test [183](#)
- Ethernet ports [42](#)
 - Default settings [42](#)
- Europe [3](#)
- Exposure [3](#)
- Extended authentication protocol [111](#)
- External authentication server [111](#)

F

- Fan speed [71](#)

FCC
 Compliance [2](#)
 Feature
 Hardware [32](#)
 File Transfer using FTP
 command example [180](#)
 Filename convention [180](#)
 Filtering [93](#)
 Filtering database [191](#)
 Finland, Contact Information [5](#)
 Firmware [70](#)
 Upgrade [177](#), [187](#)
 Flow control [78](#)
 Back pressure [78](#)
 IEEE802.3x [78](#)
 France, Contact Information [5](#)
 Front panel [41](#)
 FTP [180](#)
 File transfer procedure [181](#)
 Restrictions over WAN [182](#)

G

GARP [80](#), [246](#)
 GARP (Generic Attribute Registration Protocol) [80](#)
 garp status [247](#)
 GARP Status Command [247](#)
 GARP timer [75](#), [80](#)
 Gas Pipes [3](#)
 General setup [71](#)
 Germany, Contact Information [5](#)
 Getting help [56](#)
 GMT (Greenwich Mean Time) [73](#)
 GVRP [80](#), [85](#), [86](#), [246](#)
 GVRP (GARP VLAN Registration Protocol) [80](#), [238](#)
 gvrp disable [249](#)
 gvrp enable [248](#)
 gvrp status [248](#)

H

Hardware address [201](#)
 Hardware installation [37](#)
 Hardware monitor [70](#)
 Hardware overview [41](#)
 High Voltage Points [3](#)
 Host IDs [269](#)

HTTP [136](#)

I

IEEE 802.1p [75](#)
 IEEE 802.1Q Tagged VLAN [245](#)
 IEEE 802.1x [111](#)
 Activate [112](#)
 Note [111](#)
 Reauthentication [112](#)
 IGMP [30](#), [161](#), [163](#)
 Setup [161](#)
 Version [161](#)
 IGMP snooping [73](#), [74](#)
 Ingress port [89](#)
 Installation
 Freestanding [37](#)
 Precautions [38](#)
 Rack-mounting [38](#)
 Interface [168](#), [169](#), [174](#)
 Internal Router (IR) [167](#)
 Introduction [29](#)
 IP Addressing [269](#)
 IP Classes [269](#)
 IP interface [76](#), [149](#)
 IP Ports [136](#)
 IP routing domain [76](#)
 IP setup [75](#)
 IP table [193](#)
 How it works [193](#)
 View [194](#)
 iStacking [32](#)

K

Key [175](#)

L

LACP [107](#)
 System priority [110](#)
 Timeout [110](#)
 LEDs [45](#)
 Lightning [3](#)
 Limit MAC address learning [116](#)
 Link Aggregate Control Protocol (LACP) [107](#)

Link aggregation [31](#), [107](#)
 Dynamic [107](#)
 ID information [108](#)
 Setup [109](#)
 Status [109](#)

Link state database [168](#), [169](#)

Liquids, Corrosive [3](#)

Lockout [54](#)

Log [183](#)

Login [49](#)
 Password [54](#)

Login account [128](#)
 Administrator [128](#)
 Non-administrator [128](#)
 Number of [128](#)

Login password [129](#)

LSA (Link State Advertisement) [168](#)

M

MAC (Media Access Control) [70](#)

MAC address [70](#), [195](#)
 Global MAC address table size [115](#)
 Maximum number per port [116](#)

MAC address learning [31](#), [74](#), [91](#), [115](#), [116](#)
 Specify limit [116](#)

MAC table [191](#)
 How it works [191](#)
 View [192](#)

Maintenance [177](#)

Management Information Base (MIB) [126](#)

Management port [89](#)

MD5 [172](#)

Metric [171](#)

MIB [126](#)
 Supported MIBs [127](#)

Mini GBIC ports [42](#)
 Connection speed [42](#)
 Connector type [42](#)
 Transceiver installation [43](#)
 Transceiver removal [43](#)

Mirror port [105](#)

Modifications [2](#)

Mounting brackets [38](#)

MSA (Multi-Source Agreement) [42](#)

MTU (Multi-Tenant Unit) [73](#)

Multicast delivery tree [164](#)

Multicast router (“mrouter”) [164](#)

N

Network management system (NMS) [126](#)

North America [3](#)

North America Contact Information [5](#)

Norway, Contact Information [5](#)

NTP (RFC-1305) [72](#)

O

Opening [3](#)

OSPF [31](#), [167](#)
 Advantage [167](#)
 Area [167](#), [172](#)
 Area 0 [167](#)
 Area ID [173](#), [174](#)
 Authentication [172](#), [173](#), [174](#), [176](#)
 Autonomous system [167](#)
 Backbone [167](#)
 Configuration steps [168](#)
 General settings [170](#)
 How it works [168](#)
 Interface [168](#), [169](#), [174](#)
 Link state database [168](#), [169](#)
 Network example [168](#)
 Redistribute route [171](#)
 Route cost [173](#)
 Router ID [171](#)
 Router types [167](#)
 Status [169](#)
 Stub area [167](#), [173](#)
 Virtual link [168](#), [175](#)

OSPF (Open Shortest Path First) [31](#), [167](#)

OSPF vs RIP [167](#)

P

Password [54](#), [190](#)

PHB (Per-Hop Behavior) [139](#)

Ping [183](#)

Pipes [3](#)

Pool [3](#)

POP3 [136](#)

Port authentication [111](#)
 IEEE802.1x [112](#)
 RADIUS server [113](#)

Port Based VLAN Type [74](#)

Port details [64](#)

Port isolation [85](#), [89](#)

Port mirroring [30, 105](#)
 Mirror port [105](#)
 Port redundancy [107](#)
 Port security [31, 115](#)
 Limit MAC address learning [116](#)
 Port setup [77](#)
 Port speed/duplex [78](#)
 Port status [63](#)
 Port VID
 Default for all ports [224](#)
 Port VLAN trunking [81](#)
 Port-based VLAN [86](#)
 All connected [89](#)
 Port isolation [89](#)
 Setting Wizard [89](#)
 Power [71](#)
 Backup power supply connector [45](#)
 Voltage [71](#)
 Power Adaptor [3](#)
 Power Cord [3](#)
 Power Outlet [3](#)
 Power Supply [3](#)
 Power Supply, repair [3](#)
 Priority [75](#)
 Priority level [75](#)
 Priority queue assignment [75](#)
 Product specification [265](#)
 PVID [79, 86](#)
 PVID (Priority Frame) [79](#)

Q

Qualified Service Personnel [3](#)
 Quality of Service (QoS) [133, 139](#)
 Queue priority [146](#)
 Queue weight [146](#)
 Queuing [30, 145](#)
 Queuing algorithm [145, 146](#)
 Queuing method [145, 146](#)
 Calculate [146](#)

R

RADIUS [111](#)
 RADIUS (Remote Authentication Dial In User Service)
 [111](#)
 RADIUS server [111](#)
 Advantages [111](#)

 Network example [111](#)
 Settings [113](#)
 Rear panel [44](#)
 Redistribute route [171](#)
 Regular Mail [5](#)
 Related Documentation [27](#)
 Remote DHCP server [121](#)
 Remote management [130](#)
 Service [131](#)
 Trusted computers [131](#)
 Removing [3](#)
 Repair [3](#)
 Reset [55](#)
 Reset to factory default settings [179](#)
 Restore configuration [55](#)
 Reverse Path Forwarding (RPF) [164](#)
 Reverse Path Multicasting (RPM) [163](#)
 Revolutions Per Minute (RPM) [71](#)
 Risk [3](#)
 Risks [3](#)
 Router ID [171](#)
 Routing domain [76, 149](#)
 Routing protocol [171](#)
 Routing table [197](#)
 RSTP (Rapid STP) [31](#)
 Rubber feet [37](#)

S

Safety Warnings [3](#)
 Service [3, 4](#)
 Service access control [129](#)
 Service port [130](#)
 Service Personnel [3](#)
 Shock, Electric [3](#)
 Simple Network Management Protocol (SNMP) [126](#)
 SNMP [126](#)
 Agent [126](#)
 Communities [128](#)
 Management model [126](#)
 Manager [126](#)
 MIB [126, 127](#)
 Network components [126](#)
 Object variables [126](#)
 Protocol operations [127](#)
 Setup [128](#)
 Traps [127](#)
 Versions supported [126](#)
 Spain, Contact Information [5](#)
 Spanning Tree Protocol (STP) [95](#)

- Stacking module [32](#)
- Stacking port [46](#)
 - Stacking examples [46](#)
 - Uplink example [47](#)
- Static MAC address [31](#), [91](#), [115](#)
- Static MAC forwarding [91](#)
- Static VLAN [83](#)
 - Control [84](#)
 - Tagging [84](#)
- Status [50](#), [63](#)
 - LED [45](#)
 - Link aggregation [109](#)
 - OSPF [169](#)
 - Port [63](#)
 - Port details [64](#)
 - STP [96](#)
 - VLAN [82](#)
 - VRRP [148](#)
- STP [95](#)
 - Bridge ID [97](#)
 - Bridge priority [99](#)
 - Configuration [98](#)
 - Designated bridge [95](#)
 - Forwarding Delay [99](#)
 - Hello BPDU [96](#)
 - Hello Time [97](#), [99](#)
 - How it works [96](#)
 - Max Age [97](#), [99](#)
 - Path cost [95](#), [99](#)
 - Port priority [99](#)
 - Port state [96](#)
 - Root port [95](#)
 - Status [96](#)
 - Terminology [95](#)
- STP (Spanning Tree Protocol) [31](#)
- Strict Priority Queuing (SPQ) [145](#), [240](#)
- Stub area [167](#), [173](#)
- Subnet Masks [270](#)
- Subnetting [270](#)
- Supply Voltage [3](#)
- Support E-mail [5](#)
- SVLAN Table [245](#)
- Sweden, Contact Information [5](#)
- Swimming Pool [3](#)
- Switch lockout [54](#)
- Switch reset [55](#)
- Switch setup [74](#)
- Syntax Conventions [27](#)
- sys Commands
 - examples [229](#), [234](#), [236](#)
- sys log disp [230](#), [234](#), [236](#)
- sys sw mac list [231](#)
- System information [69](#)
- System log [183](#)

- System reboot [179](#)
- System up time [64](#)

T

- Tagged VLAN [79](#)
- TCP/UDP protocol port numbers [135](#)
- Telecommunication Line Cord. [3](#)
- Telephone [5](#)
- Temperature [70](#)
- Thunderstorm [3](#)
- Time
 - Current [72](#)
 - Time zone [73](#)
 - Timeserver [72](#)
- Time (RFC-868) [72](#)
- Time service protocol [72](#)
 - Time format [72](#)
- Time To Live (TTL) [165](#)
- Time zone [73](#)
- Timeserver [72](#)
- Transceiver
 - Installation [43](#)
 - Removal [43](#)
- Trap
 - Destination [128](#)
- Traps [127](#)
- Trunk group [107](#)
- Trunking [31](#), [107](#)
- Type of Service (ToS) [139](#)

U

- UTC (Universal Time Coordinated) [73](#)

V

- Vendor [3](#)
- Ventilation [37](#)
- Ventilation holes [37](#)
- Ventilation Slots [3](#)
- VID [77](#), [79](#), [83](#)
 - Number of possible VIDs [79](#)
 - Priority frame [79](#)
- VID (VLAN Identifier) [79](#)
- Virtual link [168](#), [175](#)

Virtual router
 Status [148](#)
 Virtual router (VR) [147](#)
 Virtual Routing Redundancy Protocol (VRRP) [147](#)
 VLAN [73](#), [79](#)
 Acceptable frame type [86](#)
 Automatic registration [80](#)
 Explicit Tagging [245](#)
 ID [79](#)
 ID (VID) [246](#)
 Implicit Tagging [245](#)
 Ingress filtering [85](#)
 Introduction [73](#)
 Number of VLANs [83](#)
 Port isolation [85](#)
 Port number [83](#)
 Port settings [85](#)
 Port-based VLAN [86](#)
 Registration Information [245](#)
 Static VLAN [83](#)
 Status [82](#), [83](#)
 Tagged [79](#)
 Trunking [81](#)
 Type [74](#), [81](#)
 VLAN (Virtual Local Area Network) [29](#), [73](#)
 VLAN Databases [245](#)
 VLAN number [77](#)
 VLAN trunking [86](#)
 vlan1q port accept [249](#)
 vlan1q port grp [250](#)
 vlan1q svlan active [252](#)
 vlan1q svlan delentry [251](#)
 vlan1q svlan inactive [252](#)
 vlan1q svlan list [252](#)
 vlan1q svlan setentry [250](#)
 Voltage Supply [3](#)
 Voltage, High [3](#)
 VRID (Virtual Router ID) [148](#)
 VRRP [147](#)
 Advertisement interval [150](#)
 Authentication [150](#)
 Backup router [147](#)
 Configuration example [152](#)
 Hello message [150](#)
 How it works [147](#)
 Interface setup [149](#)
 Master router [147](#)
 Network example [147](#), [152](#)
 Parameter [150](#)
 Preempt mode [150](#), [151](#)
 Priority [150](#), [151](#)
 Status [148](#)
 Uplink gateway [151](#)
 Uplink status [148](#)
 Virtual IP [151](#)

Virtual router [147](#)
 Virtual Router ID [151](#)
 VRID [148](#)

W

Wall Mount [3](#)
 Warnings [3](#)
 Water [3](#)
 Water Pipes [3](#)
 Web configuration
 Screen summary [51](#)
 Web configurator
 Getting help [56](#)
 Home [50](#)
 Login [49](#)
 Logout [56](#)
 Navigation panel [50](#)
 Web Site [5](#)
 Weighted Fair Queuing (WFQ) [145](#), [240](#)
 Weight [146](#)
 Wet Basement [3](#)
 Worldwide Contact Information [5](#)

Z

ZyNOS (ZyXEL Network Operating System) [180](#)
 ZyXEL Limited Warranty
 Note [4](#)