Vantage CNM

Centralized Network Management

User's Guide

Version 2.2
8/2005

ZyXEL

Copyright

Note: Refer also to the Open Software Announcementson page 448.

Disclaimer

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

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

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[A]	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 Nils 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		
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	

A. “+” IS THE (PREFIX) NUMBER YOU ENTER TO MAKE AN INTERNATIONAL TELEPHONE CALL.

Table of Contents

Copyright 2

ZyXEL Limited Warranty 2

Customer Support 3

Preface 34

Chapter 1
Introducing Vantage 36

1.1 Key Features 36
1.1.1 Object Tree View 36
1.1.2 Flexible Friendly Device Registration 36
1.1.3 Building Blocks 36
1.1.4 Multiple Domain Administration 36
1.1.5 Complete Device Configuration 37
1.1.6 Configuration Synchronization 37
1.1.7 Firewall 37
1.1.8 VPN Editor 37
1.1.9 Configuration File Management 37
1.1.10 Firmware Upgrade 37
1.1.11 Monitoring and Notifications 38
1.1.12 Logs 38
1.1.13 Data Maintenance 38
1.1.14 Vantage System Management 38
1.2 Vantage Requirements and Installation 38

Chapter 2
GUI Introduction 40

2.1 Overview 40
2.2 Main Menu Components 40
2.2.1 Object Pane 41
2.2.1.1 Object Tree View Types 41
2.2.1.2 Folders 42
2.2.1.3 Devices 45
2.2.2 Content Pane 46
2.2.2.1 Object Path 46

2.2.2.2 Menu Path 46
2.3 Menu Overview 46
2.4 Procedure For Configuring A Device 47
2.5 Context-Sensitive Menus 47
2.6 Icon Key 48

Chapter 3

Device Menus 52

3.1 Device Menus Overview 52
3.1.1 Device Main Screen 52
3.2 Device Status 54
3.3 Device Registration 54
3.3.1 Manual Option 56
3.3.1.1 Configuring ZyXEL Device using Commands 56
3.3.1.2 Configuring ZyXEL Device using Web Configurator 56
3.3.2 Import From an XML Registration File 57
3.3.2.1 Basic XML Syntax 58
3.3.2.2 Minimum Mandatory Device Settings 59
3.4 Device – Vantage Data Inconsistency: Synchronize 61
3.4.1 Vantage – Device Override Criteria 61
3.4.1.1 Vantage CNM Override Device 61
3.4.1.2 Device Override Vantage CNM 61
3.4.1.3 Synchronizing Device with Vantage 62
3.5 Firmware Management 62
3.5.1 Add Firmware Screen 63
3.5.2 Firmware Upgrade Select Product Line and Mode 64
3.5.3 Firmware Upgrade Process 65
3.5.4 Advisory Notes on Firmware Upgrade 65
3.5.5 Configuration File 66
3.5.6 Configuration File Management 66
3.5.7 Configuration File Backup 66
3.5.8 Configuration File Restore 67
3.6 Firmware Upgrade Scheduling 68
3.6.1 Firmware Upgrade Schedule Process 68
3.6.2 Firmware Upgrade Scheduler List 69

Chapter 4

Configuration > Select Device BB & General 72

4.1 Select Device BB 72
4.1.1 Procedure to Select and Apply a Device BB 73
4.2 Configuration General Screens 74
4.2.1 System 74
4.2.2 DDNS 75

4.2.3 Time Setting 77
4.2.4 Owner Info 78

Chapter 5
Configuration > LAN 80

5.1 LAN Overview 80
5.2 DHCP Setup 80
5.2.1 IP Pool Setup 80
5.2.2 DNS Servers 80
5.2.3 LAN TCP/IP 80
5.2.4 Factory LAN Defaults 80
5.2.5 IP Address and Subnet Mask 81
5.2.6 RIP Setup 81
5.2.7 Multicast 81
5.3 Any IP 82
5.3.1 How Any IP Works 83
5.4 Configuring LAN IP - ZyWALL 84
5.5 Configuring LAN IP - Prestige 86
5.6 Configuring LAN Static DHCP 88
5.7 Configuring LAN IP Alias - ZyWALL 90

Chapter 6
Configuration > WLAN 92

6.1 Introduction 92
6.2 Wireless Security Overview 92
6.2.1 Encryption 92
6.2.2 Authentication 92
6.2.3 Restricted Access 93
6.2.4 Hide Prestige Identity 93
6.2.5 Configuring Wireless LAN on the Prestige 93
6.3 Configuring the Wireless Screen 94
6.3.1 WEP Encryption 94
6.4 Configuring MAC Filters 96
6.5 Introduction to WPA 97
6.5.1 WPA-PSK Application Example 98
6.5.2 WPA with RADIUS Application Example 98
6.5.3 Wireless Client WPA Supplicants 99
6.6 Configuring IEEE 802.1x and WPA 99
6.6.1 Configuring 802.1x - ZyWALL 100
6.6.2 Configuring 802.1x - Prestige 100
6.6.3 Authentication Required > 802.1x 102
6.6.4 Authentication Required > WPA 104
6.6.5 Authentication Required > WPA-PSK 106

6.7 Configuring Local User Authentication 107
6.7.1 Configuring Local User Database 107
6.8 Configuring RADIUS 108

Chapter 7
Configuration > DMZ.... 110

7.1 DMZ Overview 110
7.2 DMZ Addresses 110
7.3 Configuring DMZ 110

Chapter 8
Configuration > WAN 114

8.1 WAN Overview 114
8.2 Multiple WAN - ZyWALL (ZyNOS 3.64) 114
8.3 TCP/IP Priority (Metric) 115
8.4 General WAN - ZyWALL 115
8.4.1 WAN ISP - ZyWALL 117
8.4.1.1 Ethernet Encapsulation 117
8.4.1.2 PPPoE Encapsulation 118
8.4.1.3 PPTP Encapsulation 120
8.5 WAN IP - ZyWALL 122
8.6 Dial Backup - ZyWALL 123
8.6.1 Traffic Redirect 124
8.6.2 Configuring Dial Backup - ZyWALL 124
8.6.3 Advanced Modem Setup - ZyWALL 127
8.6.3.1 AT Command Strings 127
8.6.4 Edit Dial Backup - ZyWALL 129
8.7 General WAN - Prestige 131
8.7.1 Traffic Shaping 132
8.7.2 Configuring Prestige WAN Setup 132
8.7.3 WAN Backup - Prestige 137
8.7.3.1 Traffic Redirect 137
8.7.4 Configuring WAN Backup - Prestige 137
8.7.5 Configuring Advanced WAN Backup - Prestige 140
8.7.6 Advanced Modem Setup - Prestige 143

Chapter 9
Configuration > NAT 144

9.1 NAT Overview 144
9.1.1 NAT Definitions 144
9.1.2 What NAT Does 145
9.1.3 How NAT Works 145
9.1.4 NAT Mapping Types 145

9.1.5 SUA (Single User Account) Versus NAT 146
9.2 Configuring NAT - ZyWALL 146
9.3 Configuring NAT - Prestige 148
9.4 SUA Servers 149
9.4.1 Port Forwarding: Services and Port Numbers 149
9.4.2 NAT and Multiple WAN 150
9.4.3 Port Translation 150
9.4.4 Configuring SUA Servers - ZyWALL 151
9.4.5 Configuring SUA Servers - Prestige 153
9.4.6 Full Feature Address Mapping 154
9.4.7 Edit Full Feature Address Mapping 156
9.5 Trigger Port Forwarding - ZyWALL 157
9.5.1 Configuring Trigger Port 158
9.5.2 Edit Trigger Port 160

Chapter 10
Configuration > Static Route....162

10.1 Static Route Overview 162
10.1.1 Static Route Summary 162
10.1.2 Edit Static Route 164

Chapter 11
Configuration > VPN 166

11.1 VPN Overview 166
11.1.1 IPSec 166
11.1.2 Security Association 166
11.1.3 Other Terminology 166
11.1.3.1 Encryption 166
11.1.3.2 Data Confidentiality 167
11.1.3.3 Data Integrity 167
11.1.3.4 Data Origin Authentication 167
11.1.3.5 Linking Two or More Private Networks Together 167
11.1.3.6 Accessing Network Resources When NAT Is Enabled 167
11.1.3.7 Unsupported IP Applications 167
11.2 IPSec Architecture 167
11.2.1 IPSec Algorithms 168
11.2.2 Key Management 168
11.3 Encapsulation 168
11.3.1 Transport Mode 169
11.3.2 Tunnel Mode 169
11.4 IPSec and NAT 169
11.5 IPSec Algorithms 170
11.5.1 AH (Authentication Header) Protocol 170

11.5.2 ESP (Encapsulating Security Payload) Protocol 171
11.5.3 Key Management 172
11.5.4 Encapsulation 172
11.5.4.1 Transport Mode 172
11.5.4.2 Tunnel Mode 172
11.5.5 IPSec and NAT 172
11.6 My ZyWALL 173
11.7 Remote Gateway Address 173
11.7.1 Dynamic Remote Gateway Address 174
11.7.2 Keep Alive/Nailed Up 174
11.8 NAT Traversal 174
11.8.1 NAT Traversal Configuration 175
11.9 ID Type and Content 175
11.9.1 ID Type and Content Examples 176
11.9.2 IKE Phases 177
11.9.3 Negotiation Mode 178
11.9.4 Pre-Shared Key 178
11.9.5 Diffie-Hellman (DH) Key Groups 179
11.9.6 Perfect Forward Secrecy (PFS) 179
11.10 X-Auth (Extended Authentication) 179
11.10.1 Authentication Server 179
11.11 VPN Screens 180
11.12 VPN Tunnel Summary (VPN version 1.0) 180
11.12.1 Add a VPN Tunnel 181
11.12.2 Manual VPN Tunnel 185
11.13 VPN and NetBIOS (VPN version 1.0) 188
11.14 VPN Rules (IKE) (VPN version 1.1) 188
11.14.1 VPN Rules (IKE) > Gateway Policy Add 190
11.14.2 VPN Rules (IKE) > Network Policy Edit 196
11.14.3 VPN Rules (IKE) > Network Policy Move 200
11.15 VPN Rules (Manual) (VPN version 1.1) 201
11.15.1 VPN Rules (Manual) > Edit 202
11.15.1.1 Security Parameter Index (SPI) 202
11.16 VPN Global Setting (VPN version 1.1) 206
11.17 Telecommuter VPN/IPSec Examples 207
11.17.1 Telecommuters Sharing One VPN Rule Example 207
11.17.2 Telecommuters Using Unique VPN Rules Example 208
11.18 VPN and Remote Management 210

Chapter 12
Configuration > Firewall 212

12.1 Types of DoS Attacks 212
12.1.1 ICMP Vulnerability 214

12.1.2 Illegal Commands (NetBIOS and SMTP) 215
12.1.3 Traceroute 215
12.2 Stateful Inspection 215
12.2.1 Stateful Inspection Process 216
12.2.2 Stateful Inspection and the ZyWALL 217
12.2.3 TCP Security 217
12.2.4 UDP/ICMP Security 218
12.2.5 Upper Layer Protocols 218
12.3 Guidelines For Enhancing Security With Your Firewall 219
12.4 Packet Filtering Vs Firewall 219
12.4.1 Packet Filtering: 219
12.4.1.1 When To Use Filtering 219
12.4.2 Firewall 220
12.4.2.1 When To Use The Firewall 220
12.5 Firewall Configuration Screens 220
12.5.1 Firewall Summary Screen 220
12.5.1.1 Ordering Rules 220
12.5.2 DoS Settings 222
12.5.3 Add/Edit a Firewall Rule 224
12.5.4 Add/Edit Source/Destination IP Addresses 226
12.5.5 Custom Ports 227

Chapter 13
Configuration > Device Log 228

13.1 Device Logging Options 228
13.2 Purge Logs 231

Chapter 14
Configuration > ADSL Monitor..232

14.1 Introduction 232
14.2 Configuring ADSL Monitor 232

Chapter 15
Configuration > X Auth 234

15.1 Overview 234
15.2 Configuring Local User Database 234
15.3 Configuring RADIUS 235

Chapter 16
Configuration > Device Alarms..238

16.1 Device Alarms 238
16.1.1 Alarm Classifications 238
16.1.2 Alarm States 238

16.1.3 Current Alarms Screen 239
16.1.4 Historical Alarms Screen 240

Chapter 17
Configuration > DNS 242

17.1 DNS Overview 242
17.2 DNS Server Address Assignment 242
17.3 DNS Servers 242
17.4 Address Record 243
17.4.1 DNS Wildcard 243
17.5 Name Server Record 243
17.5.1 Private DNS Server 243
17.6 DNS Screens 244
17.6.1 DNS System Configuration 244
17.6.2 Adding an Address Record 246
17.6.3 Adding a Name Server Record 247
17.7 DNS Cache 249
17.8 Configure DNS Cache 249
17.9 Dynamic DNS 250
17.9.1 DYNDNS Wildcard 250
17.9.2 High Availability 250
17.10 Configuring Dynamic DNS 251

Chapter 18
Building Blocks (BBs) 254

18.1 Categories 254
18.2 BB Properties 254
18.3 Configuring Device BB Menus 254
18.3.1 Editing an Existing BB 255
18.3.2 Device BB Configuration Select 256
18.3.3 Adding a New BB 256
18.4 Configuration BBs 257
18.4.1 Adding a Configuration BB 258
18.4.2 Editing a Configuration BB 259
18.5 Component BBs 260
18.5.1 Adding a Component BB 261
18.5.1.1 Adding a Component BB: IP Type 261
18.5.1.2 Adding a Component BB: E-mail Type 262
18.5.1.3 Adding a Component BB: VPN1.1d_IPSec Type 263
18.5.1.4 Adding a Component BB: VPN1.1d_IKE Type 265
18.5.1.5 Adding a Component BB: VPN1.0 Type 269
18.5.2 Editing a Component BB 272

Chapter 19
System > Administrators 274

19.1 Introduction to Administrators 274
19.1.1 Administrator Types 274
19.1.1.1 “Root” Administrator 274
19.1.1.2 “Super” Administrators 275
19.1.1.3 “Normal” Administrators 275
19.1.1.4 “Custom” Administrators 275
19.2 Configuring Administrators 275
19.3 Creating an Administrator Account 276
19.3.1 Administrator Details 276
19.3.2 Administrator Permissions 278

Chapter 20
Other System Screens 280

20.1 Status 280
20.2 Vantage Upgrade 281
20.2.1 Upgrade Procedure 281
20.2.2 Version Format 283
20.3 License Management 284
20.3.1 License Upgrade 284
20.4 System >Preferences 285
20.4.1 General Vantage Preferences 285
20.4.2 User Access 286
20.4.3 Servers 287
20.4.3.1 Vantage Server Public IP Address 289
20.4.4 Notifications 290
20.4.5 Vantage Permissions: User Group 291
20.4.5.1 Add User Group 292
20.5 System Maintenance 294
20.5.1 System Maintenance Management 294
20.5.2 Back Up System Maintenance 294
20.5.3 Restore System Maintenance 295
20.6 Address Book 296
20.6.1 Address Book Add/Edit 297
20.7 Vantage Logs 298
20.7.1 CNM Server 298
20.7.2 Vantage Logging Options 298
20.8 Certificate Management Overview 299
20.8.1 Advantages of Certificates 300
20.8.2 Current Certification Information 300
20.8.3 Create a Certificate 302
20.8.4 Importing Certificates 302

20.9 About Vantage 303

Chapter 21
Monitor > Alarms.. 304

21.1 Alarms 304
21.1.1 Alarm Types 304
21.1.2 Alarm Classifications 304
21.1.3 Alarm States 305
21.1.4 Current Alarms Screen 305
21.1.5 Historical Alarms 307

Chapter 22
Other Monitor Screens 308

22.1 Firmware Upgrade Report 308
22.2 Status Monitor 308
22.3 VPN Editor 309
22.3.1 VPN Editor Configuration 309
22.3.2 Tunnel Graphical Depictions 311

Chapter 23
Introduction to Reports 312

23.1 Bandwidth Reports 312
23.2 Service Reports 312
23.3 Web Filter Reports 313
23.4 Attack Reports 313
23.5 Authentication Reports 314
23.6 Log Viewer Reports 314
23.7 System Reports 315
23.8 Reports 315

Chapter 24
Bandwidth Reports 316

24.1 Introduction 316
24.1.1 Bandwidth Summary Settings 318
24.2 Bandwidth Monitoring 319
24.3 Bandwidth Top Users 319
24.3.1 Bandwidth Top Users Settings 321
24.4 Bandwidth Line Usage 321
24.4.1 Bandwidth Line Usage Settings 322
24.5 Bandwidth Line Interrupt 323
24.5.1 Bandwidth Line Interrupt Settings 324

Chapter 25
Service Reports 326

25.1 Service Monitor 326
25.2 Pre-defined and Custom Services 326
25.2.1 Creating a Custom Service 327
25.3 Configuring Service Settings 327
25.4 Service Summary Screens 329
25.4.1 All Services Summary 329
25.4.2 Service Summary Settings 330
25.4.3 Web Services Summary 330
25.4.4 FTP Services Summary 331
25.4.5 Mail Services Summary 332
25.4.6 VPN Services Summary 333
25.4.7 Custom Services Summary 334
25.5 Service Top Sites 335
25.5.1 All Services Top Sites 336
25.5.2 Top Site Service Settings 337
25.5.3 Web Service Top Sites 337
25.5.4 FTP Service Top Sites 338
25.5.5 Mail Service Top Sites 340
25.5.6 VPN Traffic Top Sites 341
25.5.7 Custom Service Top Sites 343
25.6 Top Users of Services 344
25.6.1 Top Users of All Services 344
25.6.2 Top Site Service Settings 345
25.6.3 Top Users of Web Services 346
25.6.4 Top Users of FTP Services 347
25.6.5 Top Users of Mail Services 348
25.6.6 Top Users of VPN Tunnels 349
25.6.7 Top Users of Custom Services 350

Chapter 26
Web Filter 352

26.1 Web Filter Summary 352
26.2 Web Filter Top Sites 353
26.3 Web Filter Top Users 354
26.4 Web Filter By User 355

Chapter 27
Attack Reports 358

27.1 Attack Summary 358
27.2 Attack Categories 359
27.2.1 Attack Category Settings 360

27.3 Source of Attacks 360
27.3.1 Attack Source Settings 361
27.4 Attack Errors and Exceptions 362

Chapter 28
Authentication 364

28.1 Successful Logins 364
28.2 Failed Logins 364

Chapter 29
Log Viewer 366

29.1 Log Monitor 366
29.2 Log Search 368

Chapter 30
Report System Screens 370

30.1 General Configuration 370
30.2 Schedule Reports 371
30.2.1 Schedule Daily Report 372
30.2.2 Schedule Weekly Report 373
30.3 CSV Import 375
30.4 About Reports 375

Chapter 31
Report... 376

31.1 Daily Report 376
31.2 Over Time Report 378

Appendix A
FTP Server (WFTPD) Setup Example 382

Installing WFTPD 382
Running WFTPD 385
WFTPD Main Screen 385

Appendix B
Configuring the Kiwi Syslog Daemon 388

Installing the Kiwi Syslog Daemon 388
Importing the Syslog Configuration File 389
Starting the Telnet Service 391
Setting Up the Syslog Server in Vantage 392

Appendix C
Pop-up Windows, JavaScripts and Java Permissions 394

Internet Explorer Pop-up Blockers 394
Disable pop-up Blockers.. 394
Enable pop-up Blockers with Exceptions.. 395
JavaScripts.. 397
Java Permissions 399
JAVA (Sun) 400

Appendix D
FTP and syslog Server Overview 402

Introduction 402

Appendix E
Java Console Debug Messages.. 404

Introduction 404

Appendix F
IP Subnetting 408

IP Addressing.. 408
IP Classes 408
Subnet Masks 409
Subnetting 409
Example: Two Subnets 410
Example: Four Subnets.. 412
Example Eight Subnets.. 413
Subnetting With Class A and Class B Networks. 414

Appendix G
Virtual Circuit Topology 416

Introduction 416

Appendix H
Wireless LANs 418

Wireless LAN Topologies 418
Ad-hoc Wireless LAN Configuration 418
BSS... 418
ESS... 419
Channel.. 420
RTS/CTS.. 420
Fragmentation Threshold 421
Preamble Type... 422
IEEE 802.1x 423
RADIUS.. 423

Types of RADIUS Messages 423
Types of Authentication 424
EAP-MD5 (Message-Digest Algorithm 5) 424
EAP-TLS (Transport Layer Security) 425
EAP-TTLS (Tunneled Transport Layer Service) 425
PEAP (Protected EAP) 425
LEAP 425
Dynamic WEP Key Exchange 425
WPA 426
User Authentication 426
Encryption 426
Security Parameters Summary 427
Benefits of a Wireless LAN 427
IEEE 802.11 428
Ad-hoc Wireless LAN Configuration 428
Infrastructure Wireless LAN Configuration 429

Appendix I
Log Descriptions 432

Introduction 432

Appendix J
Open Software Announcements 448

Notice 448
Copyright (C) 1999-2001 Intalio, Inc. All Rights Reserved. 448
Common Public License Version 1.0 449
Cryptix General License 453
TECHNOLOGY LICENSE FROM SUN MICROSYSTEMS, INC. TO DOUG LEA. 454
JAVA Software Technologies 455
Apache License 457
Copyright (c) 2002, 2003 Gargoyle Software Inc. All rights reserved. 462
GNU LESSER GENERAL PUBLIC LICENSE 463
GNU GENERAL PUBLIC LICENSE 470
End-User License Agreement for Vantage CNM 475

List of Figures

Figure 1 Main Screen 40
Figure 2 Object Tree View Types 41
Figure 3 Details Screen 41
Figure 4 Folder Right-Click Options 42
Figure 5 Add Devices 42
Figure 6 Remove Folder Warning 43
Figure 7 Associate Administrators 43
Figure 8 Add New Folder Group Name 44
Figure 9 Account Folder Alarm Right-Click Options 44
Figure 10 Group Configuration 44
Figure 11 Group Configuration > Firewall Example 45
Figure 12 Device Right-Click Options 45
Figure 13 Remove Device Warning 46
Figure 14 Java Applet Window 47
Figure 15 Device > Status > Main Screen 53
Figure 16 Device > Status > Single Device 54
Figure 17 Device > Registration Wizard > Account Association 55
Figure 18 Device > Registration > Owner Selection 55
Figure 19 Device > Registration > Wizard Choices 56
Figure 20 Device > Registration > Manual Registration 57
Figure 21 Registration Wizard: Configuration File 60
Figure 22 .Registration: XML File Devices 61
Figure 23 Registration Wizard: Finish 61
Figure 24 Device > Synchronize 62
Figure 25 Device > Firmware Management 63
Figure 26 Device > Firmware Management > Add Firmware 64
Figure 27 Device Firmware Upgrade 64
Figure 28 TypeView 64
Figure 29 Firmware Upgrade > Select Product Line and Model 65
Figure 30 Device > Firmware Upgrade 65
Figure 31 Device > Configuration File > Management 66
Figure 32 Device > Configuration File > Back Up 67
Figure 33 Device > Configuration File > Restore 68
Figure 34 Device > Firmware Schedule Upgrade 69
Figure 35 Device > Scheduler List 70
Figure 36 Prestige 662W-61/63 Device BB 73

Figure 37 Configuration > General > System - ZyWALL 74
Figure 38 Configuration > General > DDNS 76
Figure 39 Configuration > General > Time Setting 77
Figure 40 Configuration > General > Owner Info 79
Figure 41 Any IP Example Application 83
Figure 42 Configuration > LAN > IP - ZyWALL 84
Figure 43 Configuration > LAN > IP - Prestige 87
Figure 44 Configuration > LAN > Static DHCP 89
Figure 45 Configuration > LAN > IP Alias - ZyWALL 90
Figure 46 Wireless Security Methods 94
Figure 47 Configuration > WLAN > Wireless 95
Figure 48 Configuration > WLAN > MAC Filter 97
Figure 49 WPA - PSK Authentication 98
Figure 50 WPA with RADIUS Application Example 2 99
Figure 51 Configuration > WLAN > 802.1x - ZyWALL 100
Figure 52 Configuration > WLAN > 802.1x - Prestige 101
Figure 53 Wireless LAN > 802.1x/WPA > 802.1xl 103
Figure 54 Wireless LAN > 802.1x/WPA > WPAl 105
Figure 55 Wireless LAN > 802.1x/WPA > WPA-PSKl 106
Figure 56 Configuration > WLAN > Local User 107
Figure 57 Configuration > WLAN > RADIUS 108
Figure 58 Configuration > DMZ 111
Figure 59 Configuration > WAN > General - ZyWALL 116
Figure 60 Configuration > WAN > ISP (Ethernet) - ZyWALL 117
Figure 61 Configuration > WAN > ISP (PPPoE) - ZyWALL 119
Figure 62 Configuration > WAN > ISP (PPTP) - ZyWALL 120
Figure 63 Configuration > WAN > IP - ZyWALL 122
Figure 64 Traffic Redirect WAN Setup 124
Figure 65 Traffic Redirect LAN Setup 124
Figure 66 Configuration > WAN > Dial Backup - ZyWALL 125
Figure 67 Configuration > WAN > Dial Backup > Advanced - ZyWALL 128
Figure 68 Configuration > WAN > Dial Backup > Edit - ZyWALL 130
Figure 69 Example of Traffic Shaping 132
Figure 70 Configuration > WAN > Setup - Prestige - Bridge Mode 133
Figure 71 Configuration > WAN > Setup - Prestige - Routing Mode 135
Figure 72 Configuration > WAN > Backup - Prestige 138
Figure 73 Configuration > WAN Backup > Advanced - Prestige 141
Figure 74 Configuration > NAT - ZyWALL 147
Figure 75 Configuration > NAT - Prestige 148
Figure 76 Port Translation Example 151
Figure 77 Configuration > NAT > SUA Server - ZyWALL 152
Figure 78 Configuration > NAT > SUA Server - Prestige 154
Figure 79 Configuration > NAT > Full Feature > Address Mapping 155

Figure 80 Configuration > NAT > Full Feature > Edit Address Mapping 157
Figure 81 Configuration > NAT > Full Feature > Trigger Port 159
Figure 82 Configuration > NAT > Full Feature > Trigger Port > Edit 160
Figure 83 Configuration > Static Route 163
Figure 84 Configuration > Static Route > Edit 164
Figure 85 Encryption and Decryption 167
Figure 86 IPSec Architecture 168
Figure 87 Transport and Tunnel Mode IPSec Encapsulation 169
Figure 88 NAT Router Between IPSec Routers 175
Figure 89 Two Phases to Set Up the IPSec SA 177
Figure 90 Configuration > VPN 180
Figure 91 Configuration > VPN > Tunnel IPSec Detail 181
Figure 92 Configuration > VPN > Manual Tunnel IPSec Detail 186
Figure 93 Configuration > VPN > NetBIOS 188
Figure 94 Configuration > VPN > VPN Rules (IKE) 189
Figure 95 Gateway and Network Policies 190
Figure 96 IPSec Fields Summary 190
Figure 97 Configuration > VPN > IKE Policy 191
Figure 98 Configuration > VPN > IKE IPSec 197
Figure 99 Configuration > VPN > IKE IPSec > Move 200
Figure 100 Configuration > VPN > Manual-Key IPSec 201
Figure 101 Configuration > VPN > Manual-Key IPSec > Edit 203
Figure 102 Configuration > VPN > Global Setting 206
Figure 103 Telecommuters Sharing One VPN Rule Example 207
Figure 104 Telecommuters Using Unique VPN Rules Example 209
Figure 105 Three-Way Handshake 213
Figure 106 SYN Flood 213
Figure 107 Smurf Attack 214
Figure 108 Stateful Inspection 216
Figure 109 Configuration >Firewall 221
Figure 110 Configuration > Firewall > DoS Settings 223
Figure 111 Configuration >Firewall > Edit 225
Figure 112 Configuration >Firewall > IP Address 226
Figure 113 Configuration > Firewall > Firewall Custom Port 227
Figure 114 Configuration > Device Log > Log Settings 229
Figure 115 System > Logs > Purge Device Logs 231
Figure 116 Configuration > ADSL Monitor 233
Figure 117 Configuration > X Auth > Local User Database 235
Figure 118 Configuration > X Auth > RADIUS 236
Figure 119 Configuration > Device Alarms > Current 239
Figure 120 Configuration > Device Alarms > Historical 240
Figure 121 Private DNS Server Example 244
Figure 122 Configuration > DNS > System 245

Figure 123 Configuration > DNS > System > Add Address Record 247
Figure 124 Configuration > DNS > System > Add Name Server Record 248
Figure 125 Configuration > DNS > Cache 249
Figure 126 Configuration > DNS > DDNS 251
Figure 127 Building Block > Device BB 255
Figure 128 Building Block > Device BB > Edit 255
Figure 129 Building Block > Device BB > Edit > Configuration 256
Figure 130 Building Block > Device BB > Add 257
Figure 131 Building Block > Configuration 257
Figure 132 Building Block > Configuration BB > Add 258
Figure 133 Building Block > Configuration BB > Add > Next 259
Figure 134 Building Block > Configuration BB > Added 259
Figure 135 Building Block > Configuration BB > Edit 260
Figure 136 Building Block > Component BB 260
Figure 137 Building Block > Component BB > Add 261
Figure 138 Building Block > Component BB > Add > IP Address 262
Figure 139 Building Block > Component BB > Add > E-Mail Address 262
Figure 140 Building Block > Component BB > Add > VPN1.1d_IPSec 263
Figure 141 Building Block > Component BB > Add > VPN1.1d_IKE 266
Figure 142 Building Block > Component BB > Add > VPN1.0 270
Figure 143 Component BBs Added 272
Figure 144 Building Block > Component BB > Edit 273
Figure 145 System > View Administrator List 276
Figure 146 System > Administrator Details 277
Figure 147 System > Administrator Permissions 278
Figure 148 System > Vantage Status 280
Figure 149 System > Upgrade > Online Administrators 282
Figure 150 System > Upgrade > Vantage Upgrade 282
Figure 151 System > Upgrade > Vantage Upgrade > Next 283
Figure 152 System > Upgrading 283
Figure 153 System > License > License Management 284
Figure 154 System > License > License Management > Upgrade 285
Figure 155 System > Preferences > General System 286
Figure 156 System > Preferences > User Access 287
Figure 157 System > Preferences > Server 288
Figure 158 Vantage Icon - Stop 290
Figure 159 Figure 2-5 Vantage Icon - Start 290
Figure 160 System > Preferences > Notifications 291
Figure 161 System > Preferences > User Group 292
Figure 162 System > Preferences > Permissions > Add 293
Figure 163 System > Maintenance > Management 294
Figure 164 System > Maintenance > Backup 295
Figure 165 System > Maintenance > Restore 296

Figure 166 System > Address Book 296
Figure 167 System > Address Book Add/Edit 297
Figure 168 System > Logs > CNM Server 298
Figure 169 System > Logging Options 299
Figure 170 System > Certificate Management > Information 301
Figure 171 System > Certificate Management > Create CSR 302
Figure 172 System > Certificate Management > Import Certificate 303
Figure 173 System > About Vantage 303
Figure 174 Monitor > Current Alarms 306
Figure 175 Monitor > Historical Alarms 307
Figure 176 Monitor > Firmware Upgrade Report 308
Figure 177 Monitor > Monitor Status 309
Figure 178 Monitor > VPN Editor > Tunnel IPSec Detail 310
Figure 179 Configuration > VPN - Example Tunnel Summary 310
Figure 180 Monitor > VPN Monitor – Tunnel Graphics 311
Figure 181 Bandwidth Reports 312
Figure 182 Service Reports 313
Figure 183 Web Filter Reports 313
Figure 184 Attack Reports 314
Figure 185 Authentication Reports 314
Figure 186 Log Viewer Reports 315
Figure 187 System Reports 315
Figure 188 Schedule Reports 315
Figure 189 Bandwidth Summary 317
Figure 190 Bandwidth Summary Settings 318
Figure 191 Bandwidth Monitor 319
Figure 192 Bandwidth Top Users 320
Figure 193 Bandwidth Top Users Settings 321
Figure 194 Bandwidth Line Usage 322
Figure 195 Bandwidth Line Usage Settings 323
Figure 196 Bandwidth Line Interrupt 324
Figure 197 Bandwidth Line Interrupt Settings 325
Figure 198 Service Monitor 326
Figure 199 Pre-defined Services 327
Figure 200 Service Settings 328
Figure 201 All Services Summary 329
Figure 202 Services Summary Settings 330
Figure 203 Web Services Summary 331
Figure 204 FTP Services Summary 332
Figure 205 Mail Services Summary 333
Figure 206 VPN Services Summary 334
Figure 207 Custom Service Group 335
Figure 208 Top Sites for All Services 336

Figure 209 Top Site Service Settings ... 337
Figure 210 Web Service Top Sites ... 338
Figure 211 FTP Service Top Sites ... 339
Figure 212 Mail Service Top Sites ... 341
Figure 213 VPN Service Top Sites ... 342
Figure 214 Custom Service Top Sites ... 343
Figure 215 All Services Top Users ... 344
Figure 216 Top Site Service Settings ... 345
Figure 217 Top Users of Web Services ... 346
Figure 218 Top Users of FTP Services ... 347
Figure 219 Top Users of Mail Services ... 348
Figure 220 Top Users of VPN Tunnels ... 350
Figure 221 Top Users of Custom Services ... 351
Figure 222 Web Filter Summary ... 352
Figure 223 Web Filter Top Sites ... 353
Figure 224 Web Filter Top Users ... 355
Figure 225 Web Filter By User ... 356
Figure 226 Attack Summary ... 358
Figure 227 Attack Categories ... 359
Figure 228 Attack Category Settings ... 360
Figure 229 Source of Attacks ... 361
Figure 230 Attack Category Settings ... 362
Figure 231 Attack Errors and Exceptions ... 362
Figure 232 Successful Logins ... 364
Figure 233 Failed Logins ... 365
Figure 234 Log Monitor ... 367
Figure 235 Log Search ... 369
Figure 236 General System Configuration ... 370
Figure 237 Schedule Reports ... 371
Figure 238 Schedule Daily Reports ... 372
Figure 239 Schedule Weekly Reports ... 374
Figure 240 CSV Import ... 375
Figure 241 About Reports ... 375
Figure 242 Daily Reports ... 377
Figure 243 Over Time Report ... 379
Figure 244 Setup ... 382
Figure 245 Wizard 1 ... 382
Figure 246 Information ... 383
Figure 247 Installation Type ... 383
Figure 248 Installation Directory ... 384
Figure 249 Create Directory ... 384
Figure 250 Begin Installation ... 384
Figure 251 Run WFTPD ... 385

Figure 252 WFTPD Main Screen 385
Figure 253 Windows Services 386
Figure 254 WFTPD Properties 386
Figure 255 WFTPD Pro Log On 387
Figure 256 Kiwi Syslog Daemon Installation: License Agreement 388
Figure 257 Kiwi Installation: Installation Options 389
Figure 258 Kiwi Installation: Installation Directory 389
Figure 259 Kiwi Syslog Daemon Setup 390
Figure 260 Kiwi Syslog Daemon Setup: Import Configuration File 390
Figure 261 Windows XP: My Computer 391
Figure 262 Windows XP: Computer Management 392
Figure 263 Vantage System Servers 393
Figure 264 Pop-up Blocker 394
Figure 265 Internet Options 395
Figure 266 Internet Options 396
Figure 267 Pop-up Blocker Settings 397
Figure 268 Internet Options 398
Figure 269 Security Settings - Java Scripting 399
Figure 270 Security Settings - Java 400
Figure 271 Java (Sun) 401
Figure 272 Control Panel Java Plug-in Icon 404
Figure 273 Java Plug-in Control Panel 405
Figure 274 Java Plug-in Icon 405
Figure 275 Open Control Panel 405
Figure 276 Java Console 406
Figure 277 Virtual Circuit Topology 416
Figure 278 Peer-to-Peer Communication in an Ad-hoc Network 418
Figure 279 Basic Service Set 419
Figure 280 Infrastructure WLAN 420
Figure 281   RTS/CTS 421
Figure 282 Peer-to-Peer Communication in an Ad-hoc Network 429
Figure 283 ESS Provides Campus-Wide Coverage 430

List of Tables

Table 1 Menus Overview 47
Table 2 Object Tree Icons 48
Table 3 Pop-up Menus Icons 49
Table 4 Content Pane Icons 49
Table 5 Device > Status > Main Screen 53
Table 6 Device > Status > Single Device 54
Table 7 Device > Registration > Manual Registration 57
Table 8 Device > Firmware Management 63
Table 9 Device > Configuration File > Management 66
Table 10 Device > Configuration File > Back Up 67
Table 11 Device > Configuration File > Restore 68
Table 12 Device > Scheduler List 70
Table 13 Configuration > General > System - ZyWALL 74
Table 14 Configuration > General > DDNS 76
Table 15 Configuration > General > Time Setting 77
Table 16 Configuration > General > Owner Info 79
Table 17 Configuration > LAN > IP - ZyWALL 84
Table 18 Configuration > LAN > IP - Prestige 87
Table 19 Configuration > LAN > Static DHCP 89
Table 20 Configuration > LAN > IP Alias - ZyWALL 90
Table 21 Configuration > WLAN > Wireless 95
Table 22 Configuration > WLAN > MAC Filter 97
Table 23 Configuration > WLAN > 802.1x – ZyWALL 100
Table 24 Configuration > WLAN > 802.1x - Prestige 101
Table 25 Wireless LAN > 802.1x/WPA > 802.1x 103
Table 26 Wireless LAN > 802.1x/WPA > WPA 105
Table 27 Wireless LAN > 802.1x/WPA > WPA-PSK 106
Table 28 Configuration > WLAN > Local User 107
Table 29 Configuration > WLAN > RADIUS 108
Table 30 Configuration > DMZ 111
Table 31 Configuration > WAN > General - ZyWALL 116
Table 32 Configuration > WAN > ISP (Ethernet) - ZyWALL 117
Table 33 Configuration > WAN > ISP (PPPoE) - ZyWALL 119
Table 34 Configuration > WAN > ISP (PPTP) - ZyWALL 120
Table 35 Configuration > WAN > IP - ZyWALL 122
Table 36 Configuration > WAN > Dial Backup - ZyWALL 125

Table 37 Configuration > WAN > Dial Backup > Advanced - ZyWALL 128
Table 38 Configuration > WAN > Dial Backup > Edit - ZyWALL 130
Table 39 Configuration > WAN > Setup - Prestige - Bridge Mode 133
Table 40 Configuration > WAN > Setup - Prestige - Routing Mode 135
Table 41 Configuration > WAN > Backup - Prestige 138
Table 42 Configuration > WAN Backup > Advanced - Prestige 141
Table 43 NAT Definitions 144
Table 44 NAT Mapping Types 146
Table 45 Configuration > NAT - ZyWALL 147
Table 46 Configuration > NAT - Prestige 148
Table 47 Services and Port Numbers 150
Table 48 Configuration > NAT > SUA Server - ZyWALL 152
Table 49 Configuration > NAT > SUA Server - Prestige 154
Table 50 Configuration > NAT > Full Feature > Address Mapping 155
Table 51 Configuration > NAT > Full Feature > Edit Address Mapping 157
Table 52 Configuration > NAT > Full Feature > Trigger Port 159
Table 53 Configuration > NAT > Full Feature > Trigger Port > Edit 160
Table 54 Configuration > Static Route 163
Table 55 Configuration > Static Route > Edit 164
Table 56 VPN and NAT 170
Table 57 AH and ESP 171
Table 58 VPN and NAT 173
Table 59 Local ID Type and Content Fields 176
Table 60 Peer ID Type and Content Fields 176
Table 61 Matching ID Type and Content Configuration Example 177
Table 62 Mismatching ID Type and Content Configuration Example 177
Table 63 Configuration > VPN 180
Table 64 Configuration > VPN > Tunnel IPSec Detail 181
Table 65 Configuration > VPN >Manual Tunnel IPSec Detail 186
Table 66 Configuration > VPN > NetBIOS 188
Table 67 Configuration > VPN > VPN Rules (IKE) 189
Table 68 IPSec Fields Summary 189
Table 69 Configuration > VPN > IKE Policy 191
Table 70 Configuration > VPN > IKE IPSec 197
Table 71 Configuration > VPN > IKE IPSec > Move 200
Table 72 Configuration > VPN > Manual-Key IPSec 201
Table 73 Configuration > VPN > Manual-Key IPSec > Edit 203
Table 74 Configuration > VPN > Global Setting 206
Table 75 Telecommuters Sharing One VPN Rule Example 207
Table 76 Telecommuters Using Unique VPN Rules Example 209
Table 77 ICMP Commands That Trigger Alerts 214
Table 78 Legal NetBIOS Commands 215
Table 79 Legal SMTP Commands 215

Table 80 Configuration > Firewall 221
Table 81 Configuration > Firewall > DoS Settings 223
Table 82 Configuration >Firewall > Edit 225
Table 83 Configuration > Firewall > IP Address 226
Table 84 Configuration > Firewall > Firewall Custom Port 227
Table 85 Configuration > Device Log > Log Settings 230
Table 86 System > Logs > Purge Device Logs 231
Table 87 ADSL Standards 232
Table 88 Configuration > ADSL Monitor 233
Table 89 Configuration > X Auth > Local User Database 235
Table 90 Configuration > X Auth > RADIUS 236
Table 91 Alarm Severity 238
Table 92 Alarm States 238
Table 93 Configuration > Device Alarms > Current 239
Table 94 Configuration > Device Alarms > Historical 240
Table 95 Configuration > DNS > System 245
Table 96 Configuration > DNS > System > Add Address Record 247
Table 97 Configuration > DNS > System > Add Name Server Record 248
Table 98 Configuration > DNS > Cache 249
Table 99 Configuration > DNS > DDNS 251
Table 100 Building Block > Device BB 255
Table 101 Building Block > Device BB > Edit 255
Table 102 Building Block > Device BB > Add 257
Table 103 Building Block > Configuration 257
Table 104 Building Block > Configuration BB > Add 258
Table 105 Building Block > Configuration BB > Edit 260
Table 106 Building Block > Component BB 260
Table 107 Building Block > Component > Add 261
Table 108 Building Block > Component BB > Add > IP Address 262
Table 109 Building Block > Component BB > Add > E-Mail Address 262
Table 110 Building Block > Component BB > Add > VPN1.1d_IPSec 263
Table 111 Building Block > Component BB > Add > VPN1.1d_IKE 266
Table 112 Building Block > Component BB > Add > VPN1.0 270
Table 113 Building Block > Component BB > Edit 273
Table 114 System > View Administrator List 276
Table 115 System > Administrator Details 277
Table 116 System > Administrator Permissions 278
Table 117 System > Vantage Status 280
Table 118 Vantage Version Number 283
Table 119 System > License > License Management 284
Table 120 System > License > License Management > Upgrade 285
Table 121 System > Preferences > General System 286
Table 122 System > Preferences > User Access 287

Table 123 System > Preferences > Server 288
Table 124 System > Preferences > Notifications 291
Table 125 System > Preferences > Permissions 292
Table 126 System > Preferences > Permissions > Add 293
Table 127 System > Maintenance > Management 294
Table 128 System > Maintenance > Backup 295
Table 129 System > Maintenance > Restore 296
Table 130 System > Address Book 296
Table 131 System > Address Book Add/Edit 297
Table 132 System > Logs > CNM Server 298
Table 133 System > Certificate Management > Information 301
Table 134 System > Certificate Management > Create CSR 302
Table 135 System > Certificate Management > Import Certificate 303
Table 136 Types of Alarms 304
Table 137 Alarm Severity 304
Table 138 Alarm States 305
Table 139 Monitor > Current Alarms 306
Table 140 Monitor > Firmware Upgrade Report 308
Table 141 VPN Editor Icons 309
Table 142 Bandwidth Summary 317
Table 143 Bandwidth Summary Settings 318
Table 144 Bandwidth Top Users 320
Table 145 Bandwidth Top Users Settings 321
Table 146 Bandwidth Line Usage 322
Table 147 Bandwidth Line Usage Settings 323
Table 148 Bandwidth Line Interrupt 324
Table 149 Bandwidth Line Interrupt Settings 325
Table 150 Service Settings 328
Table 151 All Services Summary 329
Table 152 Web Services Summary 331
Table 153 FTP Services Summary 332
Table 154 Mail Services Summary 333
Table 155 VPN Services Summary 334
Table 156 Custom Service Group 335
Table 157 Top Sites for All Services 336
Table 158 Top Site Service Settings 337
Table 159 Web Service Top Sites 338
Table 160 FTP Service Top Sites 339
Table 161 Mail Service Top Sites 341
Table 162 VPN Service Top Sites 342
Table 163 Custom Service Top Sites 343
Table 164 All Services Top Users 344
Table 165 Top Site Service Settings 345

Table 166 Top Users of Web Services 346
Table 167 Top Users of FTP Services 347
Table 168 Top Users of Mail Services 348
Table 169 Top Users of VPN Tunnels 350
Table 170 Top Users of Custom Services 351
Table 171 Web Filter Summary 352
Table 172 Web Filter Top Sites 353
Table 173 Web Filter Top Users 355
Table 174 Web Filter By User 356
Table 175 Attack Summary 358
Table 176 Attack Categories 359
Table 177 Source of Attacks 361
Table 178 Attack Errors and Exceptions 362
Table 179 Successful Logins 364
Table 180 Failed Logins 365
Table 181 Log Monitor 367
Table 182 Log Search 369
Table 183 General System Configuration 370
Table 184 Schedule Reports 371
Table 185 Schedule Daily Reports 372
Table 186 Schedule Daily Reports 374
Table 187 Daily Reports 377
Table 188 Over Time Report 379
Table 189 FTP and syslog Server Overview 402
Table 190 Classes of IP Addresses 408
Table 191 Allowed IP Address Range By Class 409
Table 192 “Natural” Masks 409
Table 193 Alternative Subnet Mask Notation 410
Table 194 Two Subnets Example 410
Table 195 Subnet 1 411
Table 196 Subnet 2 411
Table 197 Subnet 1 412
Table 198 Subnet 2 412
Table 199 Subnet 3 412
Table 200 Subnet 4 413
Table 201 Eight Subnets 413
Table 202 Class C Subnet Planning 413
Table 203 Class B Subnet Planning 414
Table 204 IEEE802.11g 422
Table 205 Comparison of EAP Authentication Types 426
Table 206 Wireless Security Relational Matrix 427
Table 207 System Maintenance Logs 432
Table 208 System Error Logs 433

Table 209 Access Control Logs 433
Table 210 TCP Reset Logs 434
Table 211 Packet Filter Logs 434
Table 212 ICMP Logs 435
Table 213 CDR Logs 435
Table 214 PPP Logs 435
Table 215 UPnP Logs 436
Table 216 Content Filtering Logs 436
Table 217 Attack Logs 437
Table 218 IPSec Logs 438
Table 219 IKE Logs 438
Table 220 PKI Logs 441
Table 221 Certificate Path Verification Failure Reason Codes 442
Table 222 802.1X Logs 443
Table 223 ACL Setting Notes 444
Table 224 ICMP Notes 444
Table 225 Syslog Logs 445
Table 226 RFC-2408 ISAKMP Payload Types 445

Preface

Introducing Vantage Centralized Network Management (CNM)

Vantage Centralized Network Management is a cost-effective, browser-based global management solution that allows an administrator from any location to easily configure, manage, monitor and troubleshoot ZyXEL devices located worldwide.

Vantage CNM allows you to effectively separate usage and management of ZyXEL's comprehensive range of broadband security devices.

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 configuration of your Prestige for its various applications.

Related Documentation

- Supporting Disk

  Refer to the included CD for support documents.

- Compact Guide

  The Compact Guide is designed to help you get up and running right away. They contain connection information and instructions on getting started.

- 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.

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!

Syntax Conventions

- This manual may refer to Vantage Centralized Network Management simply as Vantage CNM or Vantage.

- The version number on the title page is the Vantage version that is documented in this User's Guide.
- Enter means for you to type one or more characters and press the carriage return. Select or Choose means for you to use one of the predefined choices.
- The choices of a menu item are in **Bold Arial** font.
- Mouse action sequences are denoted using a >. For example, click **Configuration > LAN > IP Alias** means first click **Configuration,** then click **LAN** and finally click **IP Alias**.

CHAPTER 1 Introducing Vantage

This chapter introduces Vantage key features and Vantage requirements.

1.1 Key Features

The following are the key features of Vantage CNM.

1.1.1 Object Tree View

The object tree has three defined views letting you view the devices directly as you configure them. The views are Account (arranged by customer name), Type (arranged by device type) and Main View up to seven layers deep. The object tree also allows you to create your own logical views (organizing them by geographic region etc. for example). Status icons in the tree let you know immediately if a device that has gone down, is currently being configured or there is a fatal alarm associated with the device.

1.1.2 Flexible Friendly Device Registration

Use the registration wizard to register a single device or multiple devices by importing an XML registration file. This means that any customer's network can be brought under Vantage control in the time it takes to run a wizard.

1.1.3 Building Blocks

Use BBs (building block) to rapidly configure both existing and new devices by reusing multiple configurations, a device's single configuration or a configuration component, ensuring absolute consistency across devices. As you use Vantage longer, it will become even easier to use as you build up valuable BB repositories.

1.1.4 Multiple Domain Administration

Associate administrators to domains that you specify in the object tree allowing efficient division of labor with maximum independence. Furthermore, multiple administrators may manage one domain, each with different privileges allowing autonomy while cooperatively managing the same network(s).

1.1.5 Complete Device Configuration

Use the Vantage configuration menus to configure its features including LAN, WAN, NAT, firewall, VPN, static routes, wireless etc. You may also directly access any device’s web configurator from the object tree by simply right-clicking on it, giving you total control over any device within Vantage.

1.1.6 Configuration Synchronization

Make sure a device configuration within Vantage is absolutely consistent with its actual configuration at any time by using the Vantage synchronization screen. This means that local configuration changes can be detected by selecting the Vantage Synchronize menu, therefore allowing flexibility with control.

1.1.7 Firewall

Create consistent device firewall policies by reusing successful configurations in other ZyXEL devices. Ensure consistency and compliance with all security policies as well as constantly monitor all devices and act immediately if things go wrong.

1.1.8 VPN Editor

Graphically create VPN (Virtual Private Networking) tunnels between devices by simply clicking a device and dragging a "tunnel" to another device. Pre-configured tunnel settings mean that even non-technical administrators can set up and manage tunnels with minimum effort.

1.1.9 Configuration File Management

Back up, restore and reset to factory default any device’s configuration file from one location.

1.1.10 Firmware Upgrade

Batch download device firmware from Vantage (after downloading the firmware from a website) to multiple devices located anywhere, minimizing time, effort and room for error as well as ensuring firmware consistency across devices. Batch upgrades can be scheduled using the upgrade scheduler. Device owners can be notified automatically and reports can be generated detailing any device’s firmware upload history.

1.1.11 Monitoring and Notifications

Use the **Status Monitor** to give real time messages (of who has logged in for example) and the alarm screens to know what is going on in your management domain. Alarms are warnings of hardware failure, security breaches, attacks or illegal Vantage login attempts. You can configure Vantage to notify you by e-mail in the event a device goes down or has triggered an alarm. You can also configure Vantage to automatically notify device owners and other administrators when a configuration (such as firmware upgrade) is going to take place.

1.1.12 Logs

Logs detail information pertaining to customer accounts, devices and Vantage that is essential for troubleshooting or historical analysis. Logs and alarms facilitate the secure, smooth operation of all Vantage-registered ZyXEL devices across the globe.

1.1.13 Data Maintenance

Back up all Vantage configurations including firmware uploaded to the Vantage server, creating various Vantage "snap shots" that may be restored at a later date.

1.1.14 Vantage System Management

Configure Vantage server public IP address, FTP, syslog, mail servers, set a management idle time-out and protect Vantage from brute-force password dictionary attacks in the Vantage system menus. Furthermore, you may pre-configure notification recipients and alter Administrator privileges from here, making Vantage a truly global tool.

1.2 Vantage Requirements and Installation

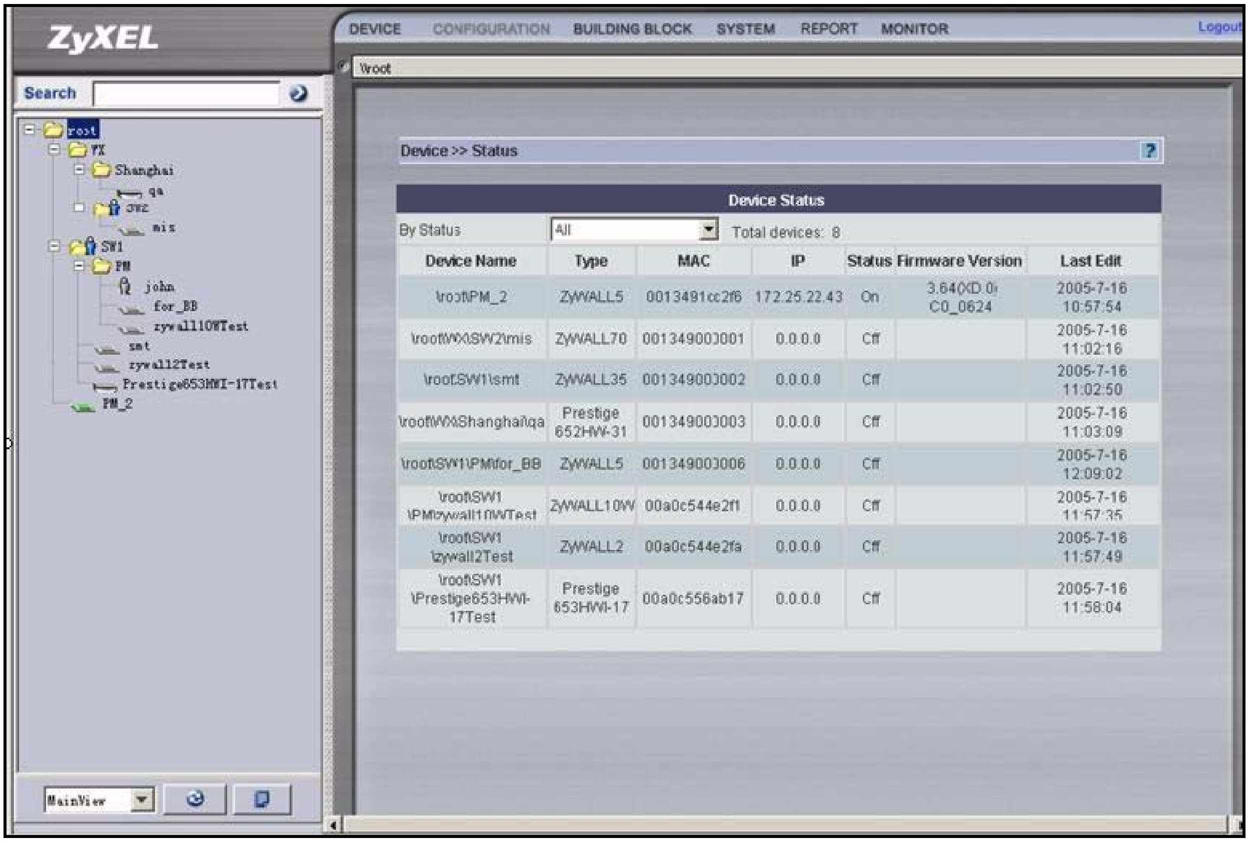
For Vantage setup requirements, access and installation, see the Quick Start Guide.

CHAPTER 2 GUI Introduction

2.1 Overview

The following figure displays an overview of the Vantage CNM graphical user interface.

Figure 1 Main Screen



Device >> Status

Device Status

By Status: All

Total devices: 8

Device Name	Type	MAC	IP	Status	Firmware Version	Last Edit
\root\PM_2	ZyWALL5	0013491cc2f6	172.25.22.43	On	3.64(XD.0) C0_0624	2005-7-16 10:57:54
\root\WX\SW2\mis	ZyWALL70	001349003001	0.0.0.0	Off		2005-7-16 11:02:16
\root\SW1\smt	ZyWALL35	001349003002	0.0.0.0	Off		2005-7-16 11:02:50
\root\WX\Shanghai\qa	Prestige 652HW-31	001349003003	0.0.0.0	Off		2005-7-16 11:03:09
\root\SW1\PM\for_BB	ZyWALL5	001349003006	0.0.0.0	Off		2005-7-16 12:09:02
\root\SW1 \PM\zywall10WTest	ZyWALL10W	00a0c544e2f1	0.0.0.0	Off		2005-7-16 11:57:35
\root\SW1 \zywall2Test	ZyWALL2	00a0c544e2fa	0.0.0.0	Off		2005-7-16 11:57:49
\root\SW1 \Prestige653HWI-17Test	Prestige 653HWI-17	00a0c556ab17	0.0.0.0	Off		2005-7-16 11:58:04

2.2 Main Menu Components

The main screen consists of two non-resizable panes; the object pane and the content pane.

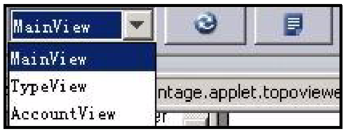
2.2.1 Object Pane

The bottom of the object pane consists of an object tree view types list box where you can select a logical view of the devices. The top of the object pane has a **Search** function where you can search for devices.

2.2.1.1 Object Tree View Types

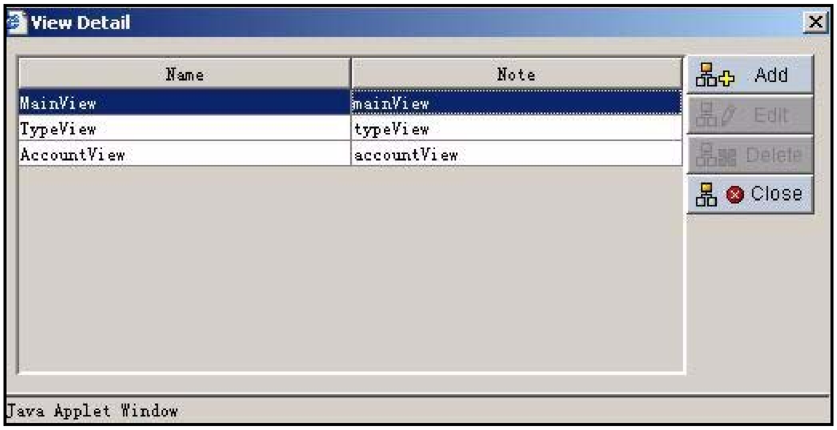
The **View** list box contains three default views called (device) **TypeView, AccountView** and **MainView.** You can also create custom views.

Figure 2 Object Tree View Types



- In the **MainView**, you may create group folders and account folders up to seven layers deep and add devices to each layer correspondingly. You can only configure devices in the main view.
- The **TypeView** view lists devices by model type.
- The **AccountView** allows for a one-layer automated view of each customer’s account and the device(s) that they own.
- You can also create custom views by clicking the detail icon to display the next screen. The custom view name then appears in this list box. In custom views, you may create group folders and account folders up to seven layers deep.

Figure 3 Details Screen



Name	Note
MainView	mainView
TypeView	typeView
AccountView	accountView

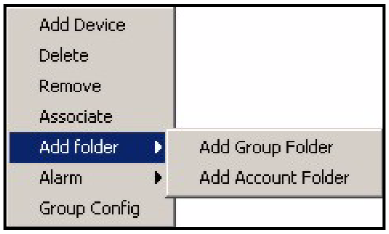
Click **Add** in this screen to create a new custom view, such as by geographic area. Give the view a unique name and write a note to further describe it. To edit or delete an existing view, select the target view in Figure 3 and then click **Edit** or **Delete**. Click **Close** to close the screen.

2.2.1.2 Folders

A folder is a logical grouping of devices. There are two types of folders, **Account** and **Group**. All devices in an **Account** folder belong to that account. When you create a folder you are requested to give a name. A device can only be owned by one customer and a customer can own many devices. A **Group** folder may contain devices belonging to different accounts.

Folder right-click options are (in **MainView** only):

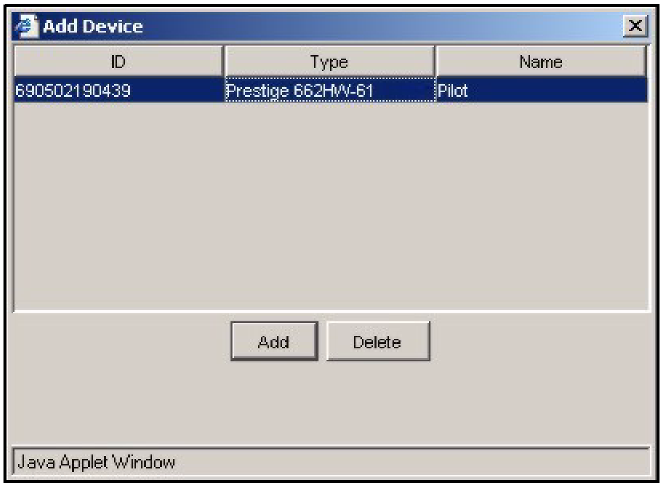
Figure 4 Folder Right-Click Options



1 **Add device.**

Displays an **Add devices** screen from which you can select devices not yet mapped to another folder.

Figure 5 Add Devices



ID	Type	Name
690502190439	Prestige 662HW-61	Pilot

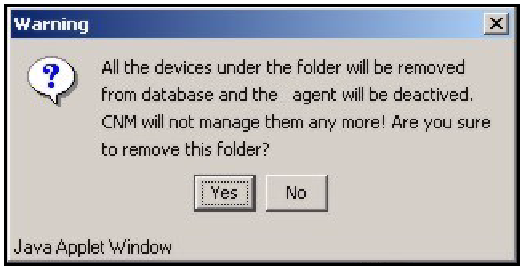
2 **Delete**.

This option displays a screen asking you if you want to delete the root folder and un-map the devices within the folder to the **Add devices** screen.

3 **Remove**.

This option displays a screen asking you if you want to remove the root folder. Removing the folder will un-map the devices within the folder. The device is still registered with Vantage but no longer associated with the folder. This action also disables Vantage within the device.

Figure 6 Remove Folder Warning



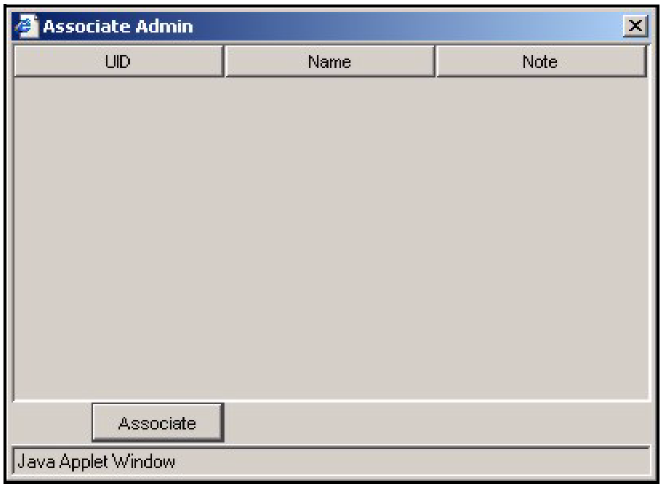
Warning

All the devices under the folder will be removed from database and the agent will be deactived. CNM will not manage them any more! Are you sure to remove this folder?

4 Associate.

Links an administrator to this folder. This folder and all sub-folders are in this administrator's domain. The administrator cannot manage nor see folders or BBs outside this domain.

Figure 7 Associate Administrators



Associate Admin

UID	Name	Note

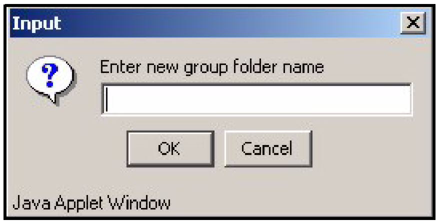
An administrator icon appears on the folder when you associate an administrator with a folder.

5 Add folder.

Add a new generic folder (**Group**) or customer folder (**Account**) where all devices within the folder belong to one customer. You can configure the **Account** folder to display the name of the customer on the folder in the object tree (see **Configuration** > **General** > **Customer Information**).

When you add a folder, you must enter a new folder group name.

Figure 8 Add New Folder Group Name



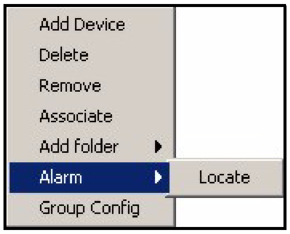
Input

Enter new group folder name

6 Alarm.

Alarms are real-time warnings of hardware failure, security breaches, attacks or illegal Vantage login attempts. Click a folder; select **Alarm** and **Locate** to find alarms associated with devices within this folder.

Figure 9 Account Folder Alarm Right-Click Options

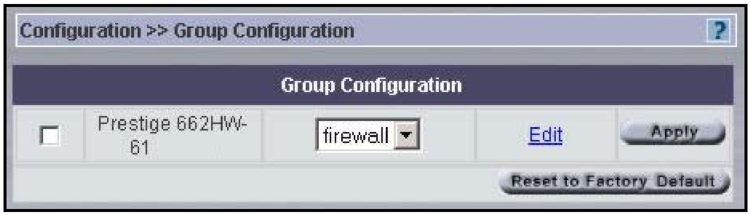


7 Group Config.

Click this to open the group configuration screen. Use Vantage CNM group configuration to configure batch devices associated to the same folder. A summary table of devices which can be batch configured is displayed.

- Select a check-box next to a listed device and click the **edit** hyperlink to proceed to a batch configuration screen for that device.

Figure 10 Group Configuration



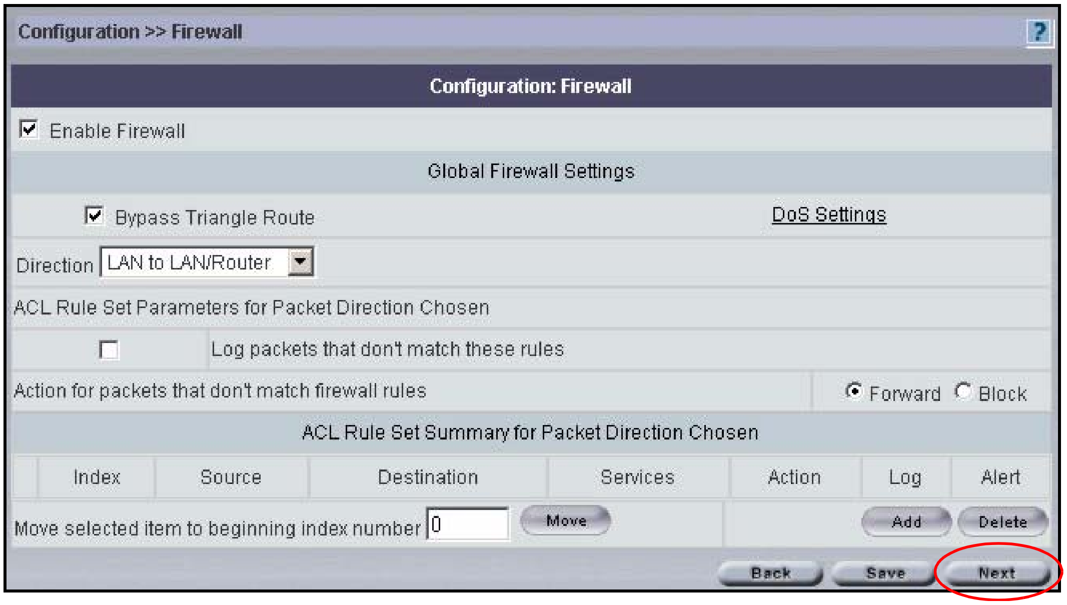
Configuration >> Group Configuration

Group Configuration

□	Prestige 662HW-61	firewall	Edit	Apply

The following screen displays a device group configuration firewall screen. See the Configuration > Firewall chapter for configuration information. When you are satisfied with the firewall configuration, click the **Next** button.

Figure 11 Group Configuration > Firewall Example



Configuration >> Firewall

Configuration: Firewall

☑ Enable Firewall

Global Firewall Settings

☑ Bypass Triangle Route — DoS Settings

Direction: LAN to LAN/Router

ACL Rule Set Parameters for Packet Direction Chosen

☐ Log packets that don't match these rules

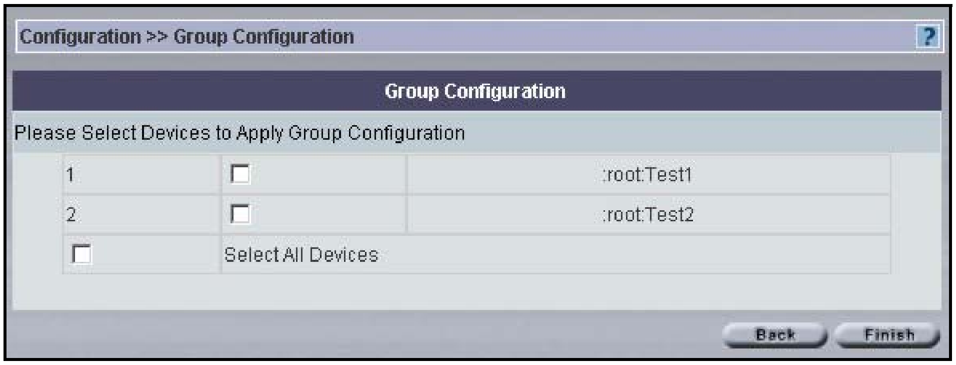
Action for packets that don't match firewall rules: ● Forward ○ Block

ACL Rule Set Summary for Packet Direction Chosen

	Index	Source	Destination	Services	Action	Log	Alert

Move selected item to beginning index number: 0

A list of devices are displayed which have already been registered to Vantage CNM. Select the checkbox next to each device that you want to include in the group configuration or select all of the devices. Click **Finish** to complete the group configuration for the device type.



Configuration >> Group Configuration

Group Configuration

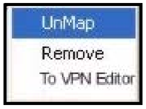
Please Select Devices to Apply Group Configuration

1	☐	:root:Test1
2	☐	:root:Test2
☐	Select All Devices	

2.2.1.3 Devices

Right-click a device options are:

Figure 12 Device Right-Click Options



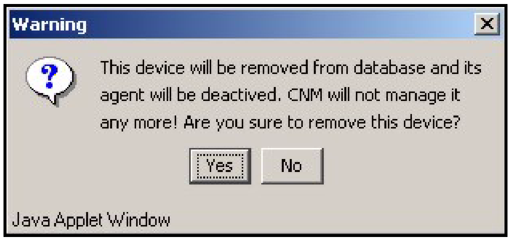
1 UnMap.

The device disappears from the tree and goes to the available pool screen from which you can map. Devices display device name, MAC address and device type.

2 Remove.

Delete the device registration from Vantage. Vantage disables CNM in the device.

Figure 13 Remove Device Warning



Warning

This device will be removed from database and its agent will be deactived. CNM will not manage it any more! Are you sure to remove this device?

3 To VPN Editor.

Create a VPN tunnel for the selected device using the VPN editor. See VPN Editor on page 309.

2.2.2 Content Pane

The content pane contains the configuration screen which also displays the object path (the folder or device you selected in the object tree) and the menu path (the screen you have open).

2.2.2.1 Object Path

The Object Path shows the folder or parent folder of the device you have clicked in the Object tree, for example \root\zywall2.

2.2.2.2 Menu Path

The Menu Path shows what menu you have clicked from the drop-down menu, for example Configuration > WAN.

2.3 Menu Overview

The following is an overview of the Vantage menus:

- All monitor menus are pop-up menus.
- You can only configure a single device at any one time.
- Some menus are not accessible because administrators do not have permission.
- Vantage can remember device and configuration menus. If for example, you select device A, then select DMZ in the **Configuration File** menu and then change to device B. The configuration DMZ will appear for device B. If device B does not have a DMZ, then the **Device > Status** screen will appear.
- If the selected device does not have a certain configuration, DMZ or wireless for example, then DMZ or WLAN will appear grayed out in the **Configuration** menu list. If this happens and you cannot access the last click menu, then you will be redirected to **Device > Status** page by default.

- If you click an administrator icon in the object tree, the **System** > **Administrators** menus will appear.

Note: You can only configure a single device at one time.

Table 1 Menus Overview

DEVICE	CONFIGURATION	BUILDING BLOCK	SYSTEM	REPORT	MONITOR	LOGOUT
Status Registration Synchronize Firmware Mgmt Firmware Upgrade Configuration File SchedulerList	Select Device BB General LAN WLAN DMZ WAN NAT Static route VPN Firewall Device Log ADSL Monitor X Auth Device Alarm DNS	Device BB Configuration BB Component BB	Administrators Status Upgrade License Preferences Maintenance Address Book Log Certificate Mgmt About	Bandwidth Service Web Filter Attack Authentication Log Viewer System Report	Alarm Firmware Report Status Monitor VPN Monitor	Logout

2.4 Procedure For Configuring A Device

The default when you first enter Vantage is the root node in the object tree and **Device >Status** menu.

1 Select a device in the object pane.

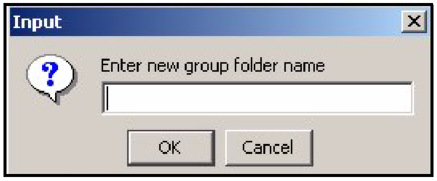
2 Select an item from a drop-down menu (Device, Configuration, Building Block, System, Monitor or Report). If the selected device does not have a certain configuration, DMZ or wireless for example, then DMZ or WLAN will appear grayed out in the Configuration menu list.

3 That menu for the selected device then appears in the Content pane.

2.5 Context-Sensitive Menus

Some context-sensitive menus appear with the words Java Applet Window as follows:

Figure 14 Java Applet Window



Input

Enter new group folder name

If you do not want to see Java Applet Window in context-sensitive menus, then do the following:

1 On the Vantage CNM server, go to Vantage CNM installation directory\utilities (the default installation path is C:\Program Files\ZyXEL\Vantage CNM\utilities) and copy the java.policy file.

2 On the Vantage CNM client computer, go to the Java plug-in installation directory\j2re1.4.1\lib\security\ (the default installation path is C:\Program Files\Java\j2re1.4.1\lib\security). You should see a (different) java.policy file there.

3 Replace the java.policy file found in step 2 with the one copied in step 1

Note: It is not advisable to replace this file if other applications use the Java plug-in. Vantage CNM functions normally whether the replacement is made or not.

2.6 Icon Key

Table 2 Object Tree Icons

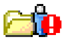
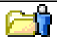
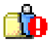
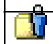
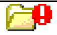
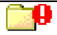
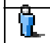
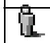
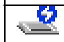
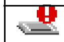
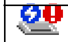
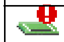
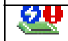
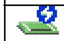
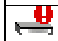
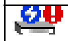
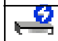
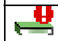
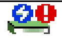
Icon	**Description**
	This is an account folder where you can see the devices and folders inside and which contain some devices with an alarm.
	This is an account folder where you can see the devices and folders inside.
	This is an account folder where you cannot see the device inside and which contains some devices with an alarm.
	This is an account folder where you cannot see the devices inside.
	This is an open group folder, which contains some devices and folders with an alarm.
	This is an open group folder.
	This is a closed group folder, which contains some devices with an alarm.
	This is an administrator currently logged in.
	This is an administrator that has logged out.
	This is a ZyWALL device turned off.
	This is a ZyWALL device that has firmware uploading.
	This is a ZyWALL device that has an alarm that is turned on.
	This is a ZyWALL device turned off with an alarm and will have a firmware upload.
	This is a ZyWALL device turned on.
	This is a ZyWALL device with an alarm.
	This is a ZyWALL device turned on with an alarm and has firmware uploading.
	This is a ZyWALL device and has firmware uploading.
	This is a Prestige device turned off.
	This is a Prestige device turned off with an alarm.
	This is a Prestige device turned off with an alarm and will have a firmware upload.
	This is a Prestige device turned off and will have a firmware upload.
	This is a Prestige device that has an alarm that is turned on.
	This is a Prestige device with an alarm.
	This is a Prestige device with an alarm and has firmware uploading.

Table 2 Object Tree Icons (continued)

Icon	Description
	This is a Prestige device with firmware uploading.
	Click this icon to refresh the current topology tree.
	Click this icon to view the topology detail information for the current user.

Table 3 Pop-up Menus Icons

ICON	DESCRIPTION
Add	Click this icon to **Add** a new topology view.
Delete	Click this icon to **Edit** the selected topology view.
Edit	Click this icon to **Delete** the selected topology view.
Close	Click this icon to **Close** the popup dialog.

Table 4 Content Pane Icons

ICON	DESCRIPTION
Apply	Click **Apply** the current configuration settings and apply to the server.
Save	Click **Save** the current configuration settings but not apply to the server. The configuration can be cancelled.
Back	Click **Back** to go to the previous page.
Next	Click **Next** to navigate to the next page.
Reset	Click to **Reset** the current page.s
OK	Click **OK** to apply the configuration.
Yes	Click **Yes** to confirm your configuration edit.
No	Click **No** to cancel the configuration edit.
Finish	Click **Finish** to complete the whole configuration.
Cancel	Click to **Cancel** the configuration and return to the previous page.
Retrieve	Click **Retrieve** to get the logs from a device.
BB	Click this icon to choose from an existing BB.
BB	Click this icon to save a new BB.
	Click this icon to choose from an existing personal profile.
	Click this icon to save as a new personal profile.
Advanced	Click **Advanced** to show more details and configure.
Check..	Click **Check** to view the status.
	This icon represents a Fatal error.
!	This icon represents a Major error.
!	This icon represents a Minor error.
!	This icon represents a Warning error.
?	This icon represents a Web Help link.

Table 4 Content Pane Icons (continued)

ICON	DESCRIPTION
□	This is a checkbox that allows you to make multiple selections from a group.
○	This is a radio button allows you to make one selection from a group.
3	Type text in a text box.
Pick One ▼	Choose from a list of pre-defined choices from a list box.
Browse...	This is a Browse icon allowing you to select a file external to Vantage.

CHAPTER 3
Device Menus

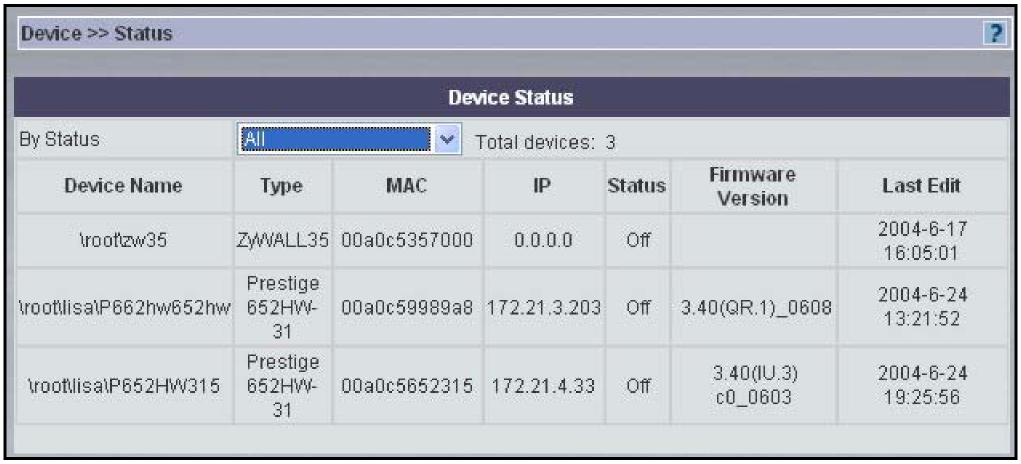
3.1 Device Menus Overview

The **Device** menus allow you to register your device, synchronize devices, and manage firmware and configuration files.

3.1.1 Device Main Screen

Device Status is the default first screen you see; the default folder in the Object pane is "root".

Figure 15 Device > Status > Main Screen



Device >> Status

Device Status

By Status: All — Total devices: 3

Device Name	Type	MAC	IP	Status	Firmware Version	Last Edit
\root\zw35	ZyWALL35	00a0c5357000	0.0.0.0	Off		2004-6-17 16:05:01
\root\lisa\P662hw652hw	Prestige 652HW-31	00a0c59989a8	172.21.3.203	Off	3.40(QR.1)_0608	2004-6-24 13:21:52
\root\lisa\P652HW315	Prestige 652HW-31	00a0c5652315	172.21.4.33	Off	3.40(IU.3) c0_0603	2004-6-24 19:25:56

The following table describes the fields in this screen.

Table 5 Device > Status > Main Screen

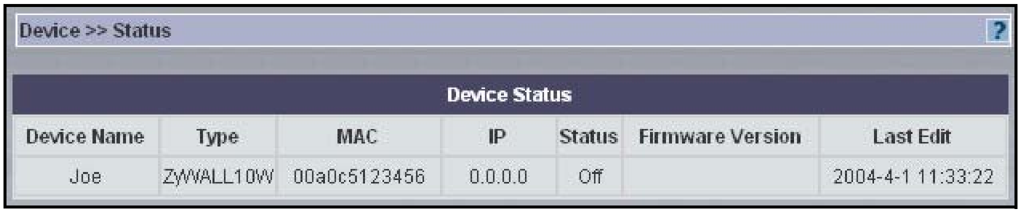
	DESCRIPTION
By Status	Select a filter status from the drop-down list box to choose which devices to view within the folder. You can view devices by: All: You can view all devices. On: You can view all devices that are online and Vantage is successfully communicating with. Off: You can view all devices that are offline. On_Alarm: You can view all devices that have an alarm that is turned on. Off_Alarm: You can view all devices that have an alarm that is turned off. On_Firmware: You can view all devices that have firmware uploading. Off_Firmware: You can view all devices that will have a firmware upload. After they are turned on Vantage will wait up to twenty minutes to upload the firmware. On_Alarm_Firmware: You can view all devices that have an alarm that is turned on and have firmware uploading. Off_Alarm_Firmware: You can view all devices that have an alarm that is turned off and will have a firmware upload.
Device Name	This field displays the user-defined name, for example, “Dev1”.
Type	This field displays the ZyXEL device model.
MAC	This field displays the LAN MAC address of the ZyXEL device.
IP	This field displays the IP address of the ZyXEL device.
Status	This field displays the operating status of the ZyXEL device. **Off** indicates the ZyXEL device is not currently connected to the network. **On** indicates the ZyXEL device is connected to the network.
Firmware Version	This field displays the device firmware network operating system (NOS) version number and date.
Last Edit	This shows the date the screen was last edited.

3.2 Device Status

In the **Device** menus, select single devices only in the Object pane when you select the **Synchronize** and **Configuration File** menu options. You may select both folders and devices for all other **Device** menu options.

Click a device, for example “test1” in the following screen and then select the Device drop down menus and click Status. This is a read-only screen showing device summary information.

Figure 16 Device > Status > Single Device



Device Name	Type	MAC	IP	Status	Firmware Version	Last Edit
Joe	ZyWALL10W	00a0c5123456	0.0.0.0	Off		2004-4-1 11:33:22

The following table describes the fields in this screen

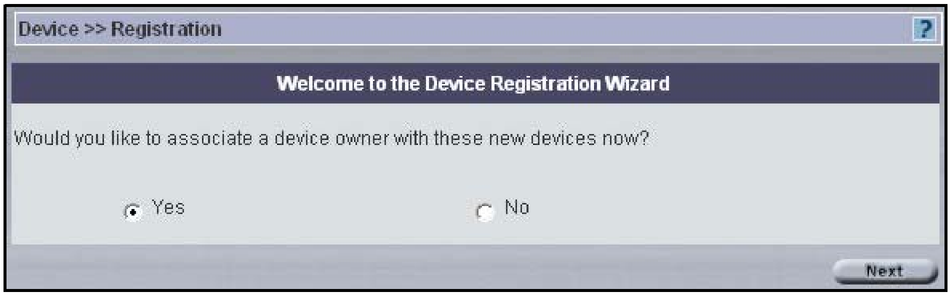
Table 6 Device > Status > Single Device

	DESCRIPTION
Device Name	This field displays the user-defined name, for example, “test1”.
Type	This field displays the ZyXEL device model.
MAC	This field displays the LAN MAC address of the ZyXEL device.
IP	This field displays the IP address of the ZyXEL device.
Status	This field displays the operating status of the ZyXEL device. **Off** indicates the ZyXEL device is not currently connected to the network. **On** indicates the ZyXEL device is connected to the network.
Firmware Version	This field displays the device firmware network operating system (NOS) version number and date.
Last Edit	This shows the date the screen was last edited.

3.3 Device Registration

Register devices with Vantage using the device registration wizard. Select a folder (not a device) in the object tree to have the new devices automatically mapped to that folder.

Figure 17 Device > Registration Wizard > Account Association



Device >> Registration

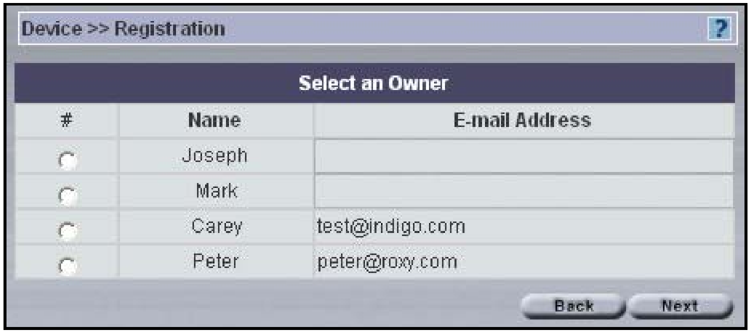
Welcome to the Device Registration Wizard

Would you like to associate a device owner with these new devices now?

● Yes ○ No

- Click **Yes** to display the next wizard screen (in the Content pane). Choose the device owner for this new device(s). This device should then appear under the correct customer in the **AccountView**.
- Click **No** to jump to see Figure 19. If you already selected an Account folder in the object tree, then the owner name is pre-selected here.

Figure 18 Device > Registration > Owner Selection



Device >> Registration

Select an Owner

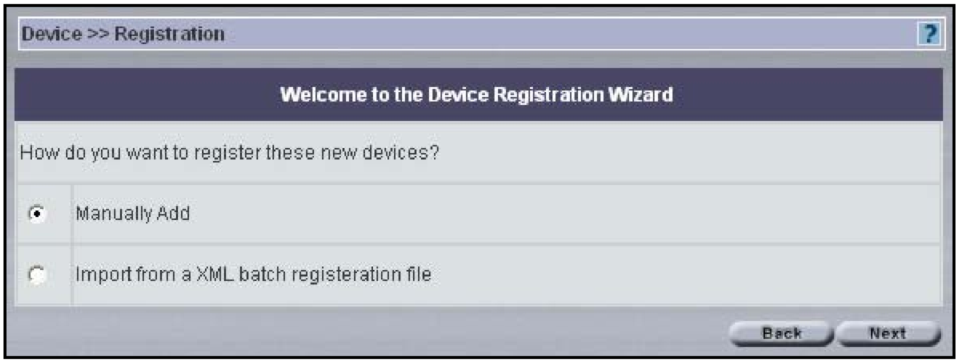
#	Name	E-mail Address
○	Joseph	
○	Mark	
○	Carey	test@indigo.com
○	Peter	peter@roxy.com

In the following screen select a radio button to either:

- Manually add: When you choose this option, you must enter the information shown in see Figure 20 for a single device at a time.
- Import from an XML batch registration file: choose this option if you want to input a batch of devices in one go. Go to the XML folder within the Vantage CNM Installation directory (C:\Program Files\ZyXEL\Vantage CNM\xml by default). Choose the 4-devices or 100-ZyWALL10W templates and modify accordingly.

Click **Next** to proceed to the next registration screen.

Figure 19 Device > Registration > Wizard Choices



Device >> Registration

Welcome to the Device Registration Wizard

How do you want to register these new devices?

● Manually Add

○ Import from a XML batch registeration file

3.3.1 Manual Option

Use the following screen to enter device information, get device configurations and set encryption options.

You do not need to add NAT or firewall rules when you encrypt this traffic.

3.3.1.1 Configuring ZyXEL Device using Commands

To set the encryption mode on the ZyXEL device, do the following:

1. Go to CI (Command Interface) mode (SMT 24.8 for devices with SMT menus).
2. Type 'CNM encrymode X' where:

Value of X	Encryption Mode
0	None
1	DES
2	3DES

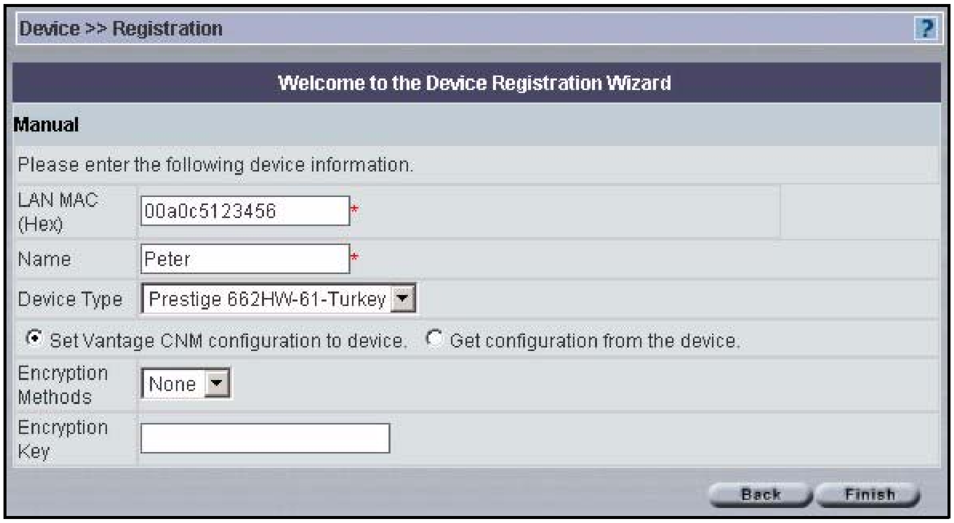
3. To set the encryption key on the ZyXEL device, type 'CNM encrykey xxxxxxxxx' where 'xxxxxxxxx' is the alphanumeric encryption key ("0" to "9", "a" to "z" or "A" to "Z") in the Vantage server.

3.3.1.2 Configuring ZyXEL Device using Web Configurator

To set the encryption mode on the ZyXEL device, do the following:

Log into the device web configurator, click **Remote Management** from the navigation panel and then click the **CNM tab**. Select **Enable**, (enter the **Vantage CNM Server** (IP) **Address**) and enter an **Encryption Algorithm** and **Encryption Key.**

Figure 20 Device > Registration > Manual Registration



Please enter the following device information.

LAN MAC (Hex): 00a0c5123456 *

Name: Peter *

Device Type: Prestige 662HW-61-Turkey

● Set Vantage CNM configuration to device. ○ Get configuration from the device.

Encryption Methods: None

Encryption Key:

The following table describes the fields in this screen

Table 7 Device > Registration > Manual Registration

LABEL	DESCRIPTION
MAC (Hex)	Enter the LAN MAC address of the ZyXEL device (without colons) in this field. Vantage uses the MAC address to identify the ZyXEL device, so make sure it is entered correctly.
Name	Enter a unique name here for the ZyXEL device for identification purposes. The device name cannot exceed ten characters.
Device Type	Select the ZyXEL device type from the pull-down menu.
Set Vantage CNM configuration to device	Select this radio button to have Vantage push all current configurations from Vantage to the device. The current device configuration is then reset to the configuration settings that Vantage contains.
Get configuration from the device	Select this radio button to have Vantage pull all current device configurations into Vantage. The current device configuration "overwrites" Vantage configurations.
Encryption Methods	The encryption options at the time of writing are DES and 3DES. Choose from None (no encryption), DES or 3DES. The ZyXEL device must be set to the same encryption mode (and have the same encryption key) as the Vantage server.
Encryption Key	Type an eight-character alphanumeric ("0" to "9", "a" to "z" or "A" to "Z") for DES encryption and a 24-character alphanumeric ("0" to "9", "a" to "z" or "A" to "Z") for 3DES encryption.
Back	Click **Back** to return to the previous screen.
Finish	Click **Finish** to go to the **Device Registration Finished** screen.

3.3.2 Import From an XML Registration File

Use this method when you want to register multiple ZyXEL devices at one time. The file should be in XML format containing the fields shown in the manual registration screen for each device.

First create an XML file. Some XML templates for each device type supported at the time may be found at “vantage installed path\xml\”. You may combine different templates into one XML file so as to import multiple devices (and of different types) in one go.

Make sure the XML syntax is correct, as there are no validation checks in Vantage. Although you may be allowed to import an XML file with incorrect syntax into Vantage, device management via Vantage may be abnormal.

When you import a device to a folder, make sure the device’s name is different from existing devices’ in that folder.

Import the XML file using Vantage device registration wizard. This may take several minutes depending on how many devices you have in your XML file. Vantage then lists all devices (if your XML file contains multiple devices), and allows you to choose which devices you want to import.

3.3.2.1 Basic XML Syntax

1 You don’t need to fill in a (blank) configuration if a device doesn’t contain that configuration.

2 Mandatory fields must be filled in or Vantage will not list that device as a device that can be imported.

3 XML fields must not contain a “return” character. For example, the format below is forbidden:

```
<mac>00a0c544e2fc
</mac>
You must write the field in one line, like this:
<mac>00a0c544e2fc</mac>
```

4 A field must contain the correct value type. You can’t write a string in a field that should contain an integer value. For example, the following is wrong, as <encryptMode> must contain integers only.

```
<encryptMode>abc</encryptMode>
```

5 In fields of type string, if the string length is 0, you also need to write zero length field to make import work correctly. For example, both the following zero length string fields are acceptable.

```
<domainName> </domainName>
```

or

```
 <domainName/>
```

6 If your XML Field contain a special character such as &,’, >, <,”, you must embrace the character with <![CDATA[and]]>, as shown next:

```
<initString><![CDATA[at&fs0=0]]></initString>
```

7 Device configuration fields needn’t be in order. For example, you can write a device’s LAN configuration fields first and then write the General configuration fields.

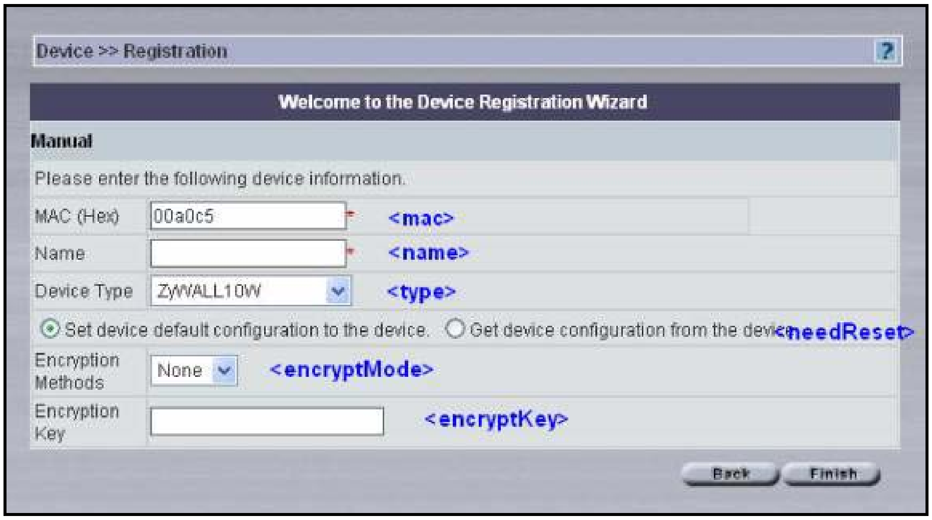
3.3.2.2 Minimum Mandatory Device Settings

You must at least fill in the MAC address, name, type, encryption mode and key fields for a device to be successfully imported into Vantage suing an XML file. Below is an example for the ZyWALL 10W.

Note: We recommend you either fill in these settings only (for each device) or fill in all configuration settings in the XML template.

```
<?xml version="1.0" encoding="UTF-8"?>
<ZyXEL xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<ZyXELDevice>
<mac>00a0c544e2fc</mac>
<name>zywall10WTest</name>
<type>ZyWALL10W</type>
<needReset>true</needReset>
<encryptMode>1</encryptMode>
<encryptKey>abcdefgh</encryptKey>
 <General/>
 <LAN/>
<ZWWAN/>
  …
</ZyXELDevice>
</ZyXEL>
```

These are the equivalent settings by using the manual device registration wizard screen.



Device >> Registration

Welcome to the Device Registration Wizard

Manual

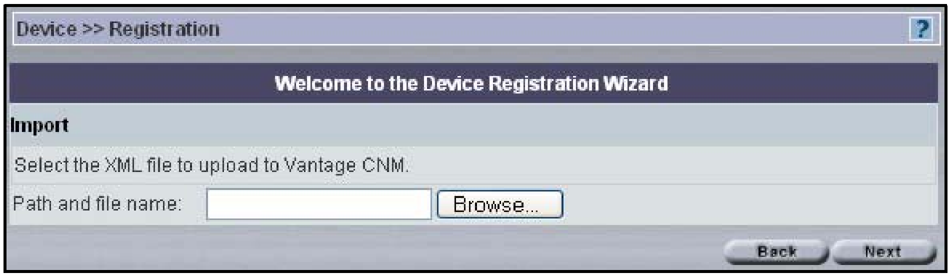
Please enter the following device information.

MAC (Hex)	00a0c5 *	<mac>
Name	*	<name>
Device Type	ZyWALL10W	<type>
● Set device default configuration to the device.	○ Get device configuration from the devi	<needReset>
Encryption Methods	None	<encryptMode>
Encryption Key		<encryptKey>

Note: For more detailed information on creating XML files for Vantage, please see the “Import Device Using XML Reference Manual” at the ZyXEL web site download library.

After you have completed the XML file, click **Browse** to locate it in the next screen and then click **Next**.

Figure 21 Registration Wizard: Configuration File



Device >> Registration

Welcome to the Device Registration Wizard

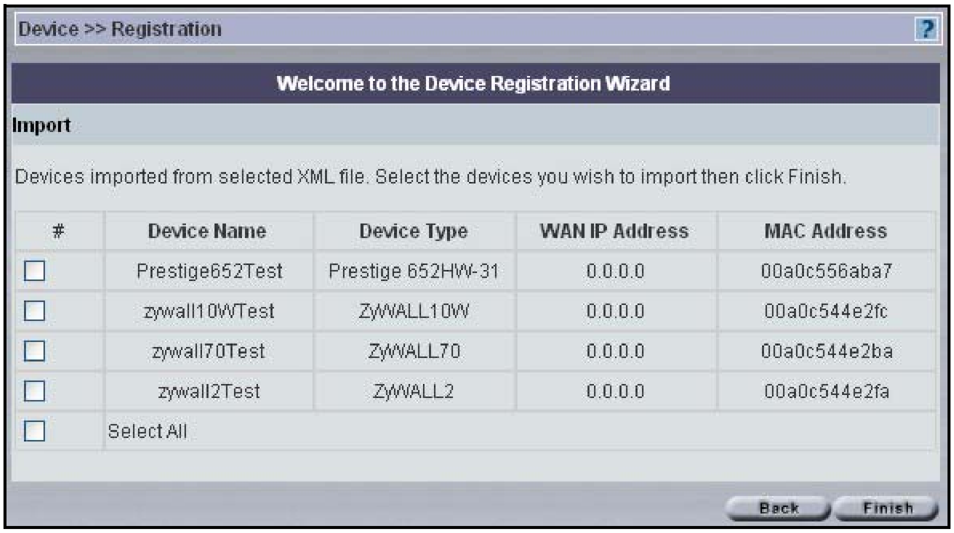
Import

Select the XML file to upload to Vantage CNM.

Path and file name:

The next screen displays all devices available in the XML file that can be imported.Select the individual devices that you wish to import or select **Select All** to import all devices that are displayed in this screen. Click **Finish** to go to a **Device Registration Finished** screen showing what files you have successfully registered.

Figure 22 .Registration: XML File Devices



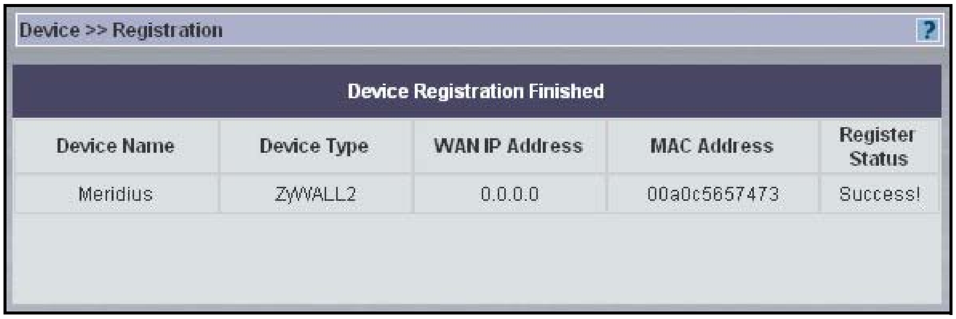
Welcome to the Device Registration Wizard

Import

Devices imported from selected XML file. Select the devices you wish to import then click Finish.

#	Device Name	Device Type	WAN IP Address	MAC Address
□	Prestige652Test	Prestige 652HW-31	0.0.0.0	00a0c556aba7
□	zywall10WTest	ZyWALL10W	0.0.0.0	00a0c544e2fc
□	zywall70Test	ZyWALL70	0.0.0.0	00a0c544e2ba
□	zywall2Test	ZyWALL2	0.0.0.0	00a0c544e2fa
□	Select All			

Figure 23 Registration Wizard: Finish



Device Registration Finished

Device Name	Device Type	WAN IP Address	MAC Address	Register Status
Meridius	ZyWALL2	0.0.0.0	00a0c5657473	Success!

3.4 Device – Vantage Data Inconsistency: Synchronize

Click **Device** > **Synchronize** to have Vantage check for data inconsistencies in the selected object. Data inconsistencies may occur if device configurations are made directly to the device instead of in Vantage.

3.4.1 Vantage – Device Override Criteria

3.4.1.1 Vantage CNM Override Device

Vantage pushes all current configurations from Vantage to the device. The current device configuration will then be reset to the configuration settings that Vantage contains.

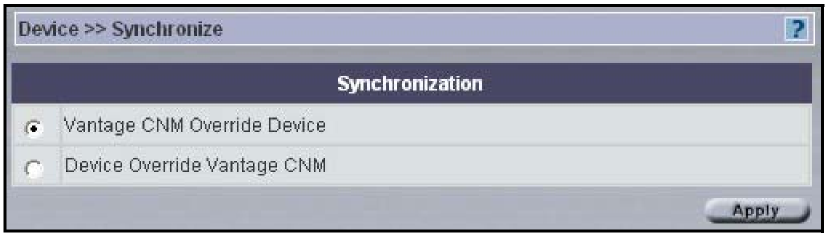
3.4.1.2 Device Override Vantage CNM

Vantage pulls all current device configurations into Vantage. The current device configuration "overwrites" Vantage configurations.

3.4.1.3 Synchronizing Device with Vantage

Select a device and then click **Device > Synchronize Settings**. A screen displays showing which configuration menus are out-of-synch. Access the device web configurator to view discrepancy details between corresponding configurations. When you understand the discrepancy, you can then decide to allow Vantage to override the device configuration or vice-versa.

Figure 24 Device > Synchronize



● Vantage CNM Override Device
○ Device Override Vantage CNM

3.5 Firmware Management

Use the **Firmware Management** screen to download ZyXEL device firmware from the ZyXEL FTP site to Vantage. After you download it to Vantage, you can then upload it from Vantage to the target devices.

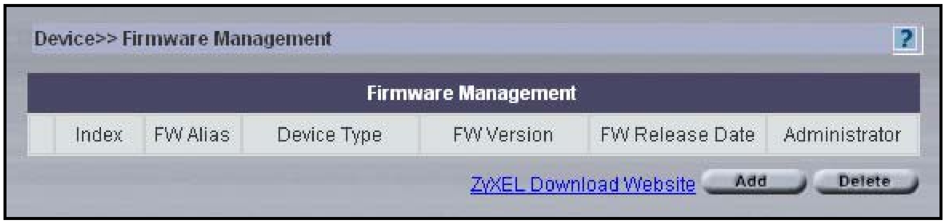
All firmware is downloaded to one repository within Vantage. There is no domain-specific repository within Vantage for firmware downloads.

You cannot edit an existing firmware in Vantage; you can only delete it.

Administrators should subscribe to the ZyXEL mailing lists to be regularly informed of new firmware versions.

Click **Device > Firmware Management** to display the next screen.

Figure 25 Device > Firmware Management



The following table describes the fields in this screen

Table 8 Device > Firmware Management

	DESCRIPTION
Index	This is the file list number.
FW Alias	This is the firmware file name.
Device Type	This field displays the model. You must upload firmware to the correct model. For example firmware for P650R-11 is not compatible with the P650R-13 model. Vantage should automatically detect firmware for the device selected. Uploading incorrect firmware may damage the device.
FW Version	This field displays ZyNOS (ZyXEL network operating System) firmware version.
FW Release Date	This field displays the date the firmware was created.
Administrator	This field displays the administrator who downloaded this firmware file to Vantage.
ZyXEL Download Website	Click this hyperlink to go to the ZyXEL Website and download firmware to your computer. Firmware is uploaded to your device in the following manner • download from the website to your computer • upload from your computer to the Vantage • upload from Vantage to your selected device.
Add	Click **Add** to proceed to the next screen.
Delete	Click to delete a selected firmware from your Vantage firmware management.

3.5.1 Add Firmware Screen

Click **Add** in **Firmware Management** to view the next screen that allows you to select a firmware zip file. Upload the firmware zip file to Vantage. This firmware zip file contains more than the firmware. It contains:

- The device firmware (bin file extension). Only this firmware file is actually downloaded to the device.
- The device default configuration file (config file extension).
- Device firmware release notes (doc file extension) highlighting.
- Boot module with bm file extension.
- A file with XML file extension. Vantage uses the XML file to gather the device type, firmware version and release date information.

Click **Add** in the screen shown in the previous figure to display the next screen. Type the file name and path or browse to where you saved the file. You may create a firmware alias for the selected zip in this screen.

Figure 26 Device > Firmware Management > Add Firmware

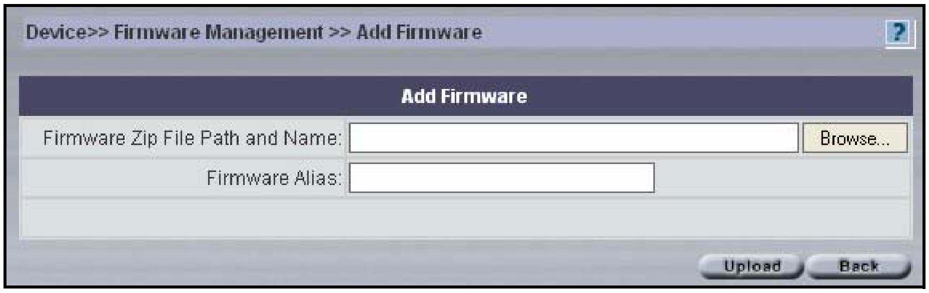
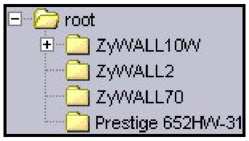

Device>> Firmware Management >> Add Firmware
?
Add Firmware
Firmware Zip File Path and Name:
Browse...
Firmware Alias:
Upload
Back

Figure 27 Device Firmware Upgrade

Use the **Device Firmware Upgrade** screen to download firmware to devices from Vantage.

You may upgrade firmware to several homogeneous devices at the same time. Vantage can upload firmware from 20 to 50 devices at a time depending on your network bandwidth. You can upload firmware in the **Main View** or in **Type View**.

Figure 28 TypeView



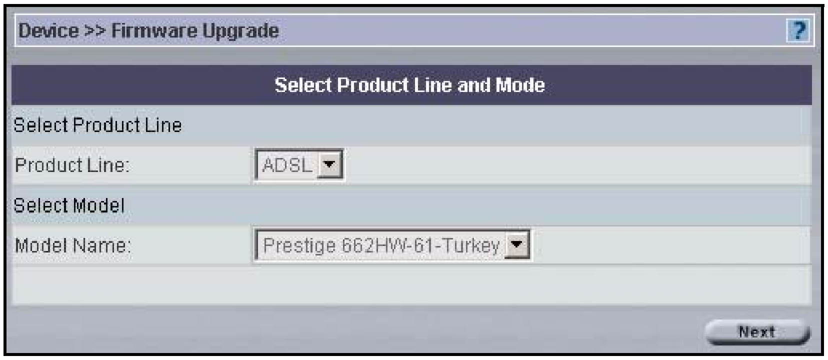
3.5.2 Firmware Upgrade Select Product Line and Mode

If you select a device in the object tree, Figure 30 on page 65 will be shown; select a folder in the object tree and the following screen will be displayed. Use this screen to select the product line and model name of devices that you want to download firmware to from Vantage.

- Pick a product line.
- Pick a model name.

Click **Next** to proceed to the **Firmware Upgrade** screen.

Figure 29 Firmware Upgrade > Select Product Line and Model



Device >> Firmware Upgrade

Select Product Line and Mode

Select Product Line

Product Line:	ADSL

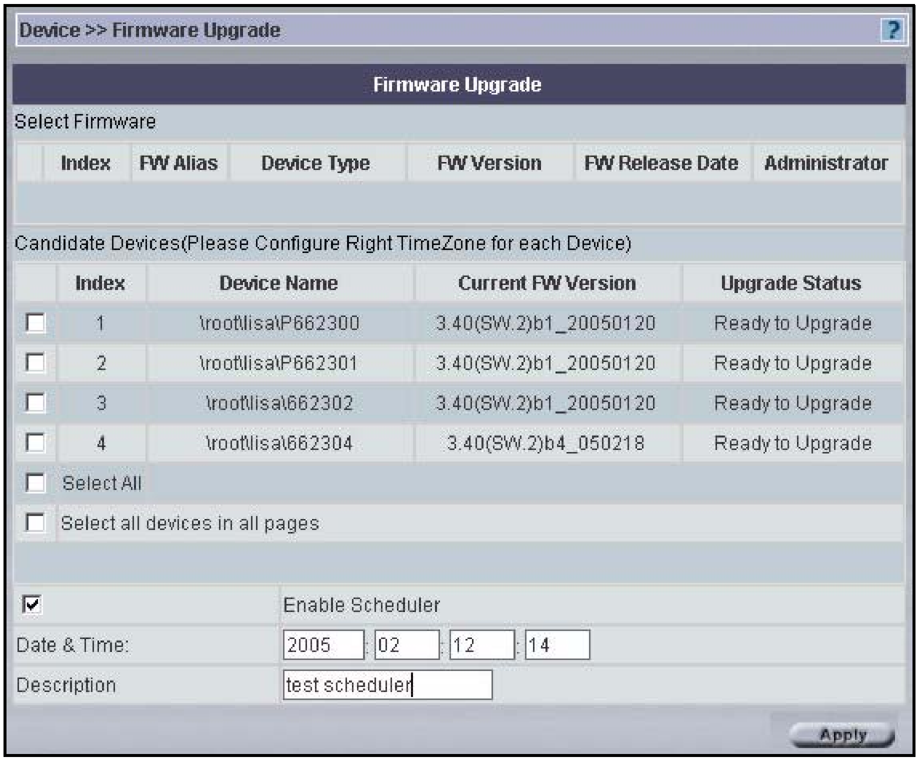
Select Model

Model Name:	Prestige 662HW-61-Turkey

3.5.3 Firmware Upgrade Process

1. Select Firmware by picking a node.
2. Select the candidate devices (of that model type for the node selected).
3. Click **Apply** to begin the device upgrade process.

Figure 30 Device > Firmware Upgrade



Device >> Firmware Upgrade

Firmware Upgrade

Select Firmware

	Index	FW Alias	Device Type	FW Version	FW Release Date	Administrator

Candidate Devices(Please Configure Right TimeZone for each Device)

	Index	Device Name	Current FW Version	Upgrade Status
□	1	\root\lisa\P662300	3.40(SW.2)b1_20050120	Ready to Upgrade
□	2	\root\lisa\P662301	3.40(SW.2)b1_20050120	Ready to Upgrade
□	3	\root\lisa\662302	3.40(SW.2)b1_20050120	Ready to Upgrade
□	4	\root\lisa\662304	3.40(SW.2)b4_050218	Ready to Upgrade

□ Select All

□ Select all devices in all pages

☑	Enable Scheduler
Date & Time:	2005 : 02 : 12 : 14
Description	test scheduler

See Table 8 on page 63 for field descriptions.

3.5.4 Advisory Notes on Firmware Upgrade

- It is advisable to upgrade firmware during periods of low network activity, since each device must restart after firmware upload.

- You should also notify device owners before you begin the upload. See the **System > Preferences > Notifications** screen.

3.5.5 Configuration File

Use these screens to manage, back up and restore configuration files.

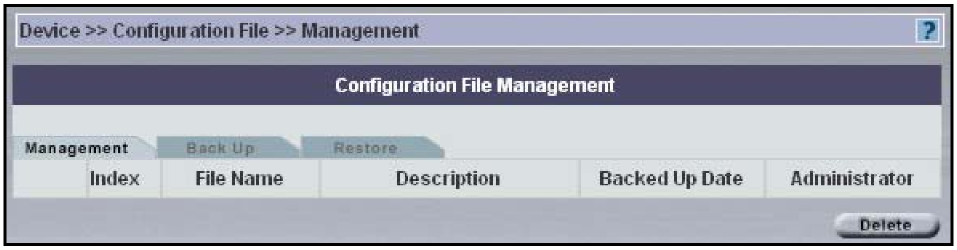
Select the device and then click **Device > Configuration File**.

You can create your own configuration file alias in Vantage. This may make it easier to distinguish multiple configuration files for the same device.

3.5.6 Configuration File Management

Use this screen to view and delete configuration files uploaded to Vantage. You can view the configuration file name, a description of it, the date it was backed up and which administrator backed it up.

Figure 31 Device > Configuration File > Management



Device >> Configuration File >> Management

Configuration File Management

Index	File Name	Description	Backed Up Date	Administrator

The following table describes the fields in this screen

Table 9 Device > Configuration File > Management

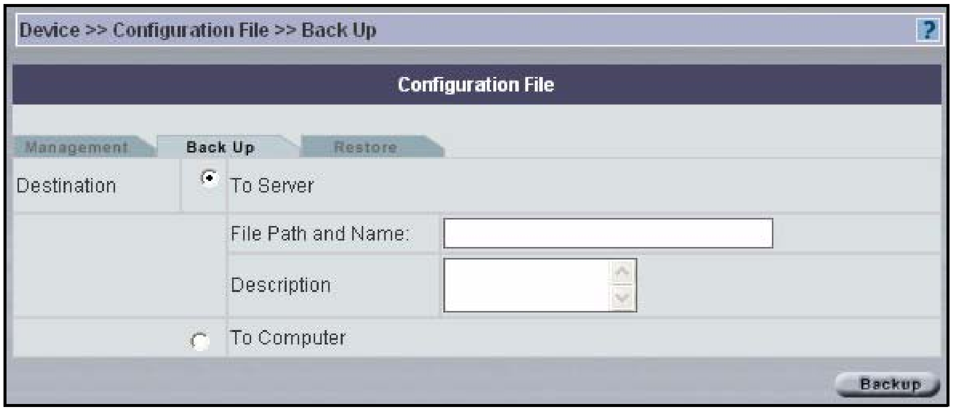
TYPE	DESCRIPTION
Index	This displays a number assigned to the file
File Name	This displays the name given to the configuration file.
Description	This displays a description that was entered at the time of file backup or file restoration.
Backed Up Date	This field displays the date of back up of a configuration file.
Administrator	This field displays the administrator who performed the backup or restoration of the configuration file.
Delete	Select the checkbox and click **Delete** to remove a selected firmware from your Vantage firmware management.

3.5.7 Configuration File Backup

Select a device and then use the **Backup** screen to save that device’s configuration file to either Vantage or your computer (from which you’re accessing Vantage).

Once your device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Figure 32 Device > Configuration File > Back Up



The following table describes the fields in this screen

Table 10 Device > Configuration File > Back Up

TYPE	DESCRIPTION
Destination	Select the radio button to give the download destination to Vantage.
File Path and Name	Type in the location of the file you want to upload in this field.
Description	Type a description of the file backup.
To Computer	Select the radio button to give the download destination to your computer.
Back Up	Click the Backup button to proceed to a dialog box where your configuration is saved to your computer.

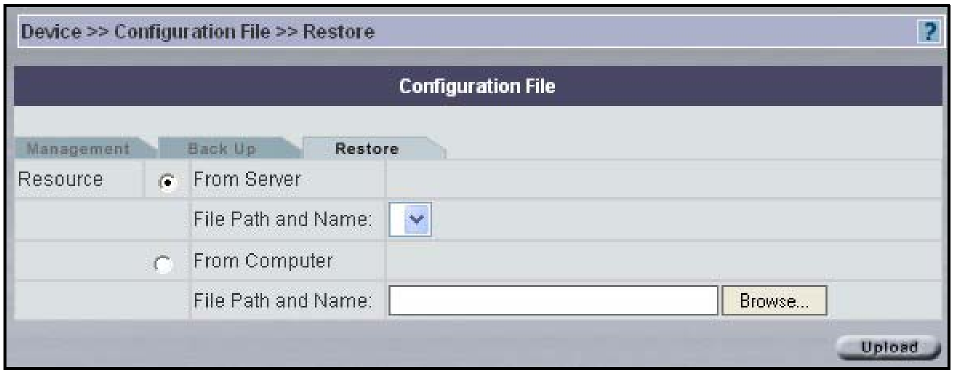
3.5.8 Configuration File Restore

Use the **Restore** screen to overwrite a devices current configuration with a previously saved backup file or the default configuration file from either Vantage or your computer (from which you're accessing Vantage). Be sure to upload the correct Configuration file for the device.

Note: Make sure you restore a configuration file to the correct model or you may damage the device.

If you restore a configuration file to a device other than the one intended, you may lock out the device. The configuration file contains the WAN configuration.

Figure 33 Device > Configuration File > Restore



Device >> Configuration File >> Restore

Configuration File

Management | Back Up | Restore

Resource ● From Server

File Path and Name:

○ From Computer

File Path and Name: Browse...

Upload

Table 11 Device > Configuration File > Restore

TYPE	DESCRIPTION
Resource	
From Server	Select this radio button to upload a configuration file From Vantage.
File Path and Name	Select a file from the drop-down list box.
From Computer	Select this radio button to upload a configuration file from your computer.
File Path and Name	Type in the location of the file you want to upload in this field or click **Browse...** to find it.
Upload	Click **Upload** to begin the upload process.

3.6 Firmware Upgrade Scheduling

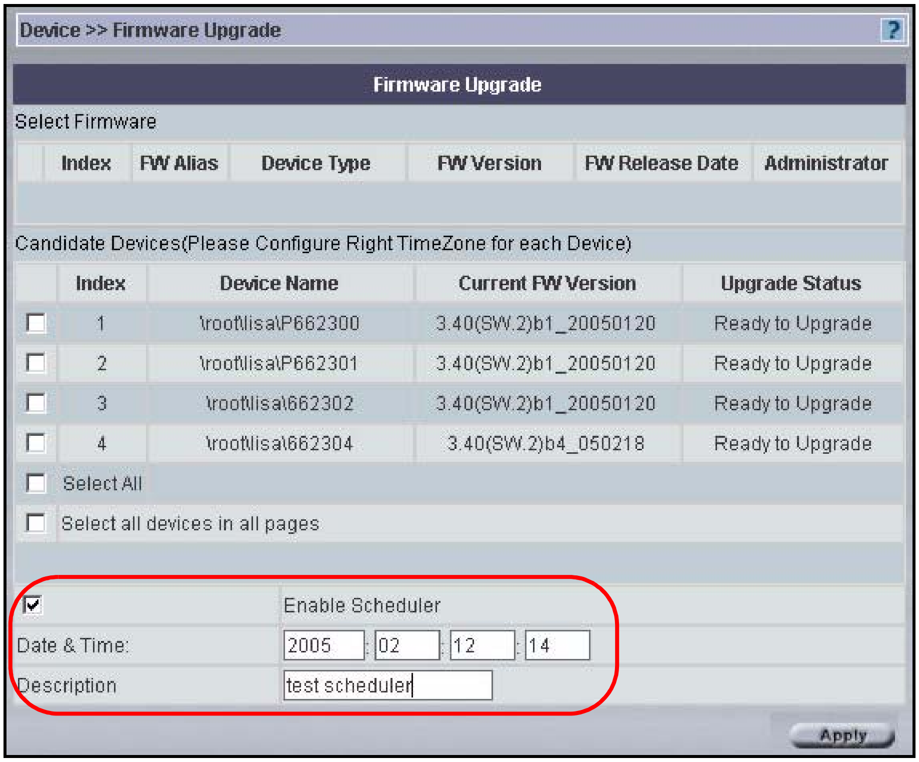
Firmware upgrade scheduling allows you to configure a schedule of firmware upgrades to specified devices to begin at a specificied date and time.

3.6.1 Firmware Upgrade Schedule Process

1 Select Firmware by picking a node.

2 Select the candidate devices (of that model type for the node selected).

Figure 34 Device > Firmware Schedule Upgrade



Device >> Firmware Upgrade

Firmware Upgrade

Select Firmware

	Index	FW Alias	Device Type	FW Version	FW Release Date	Administrator

Candidate Devices(Please Configure Right TimeZone for each Device)

	Index	Device Name	Current FW Version	Upgrade Status
□	1	\root\lisa\P662300	3.40(SW.2)b1_20050120	Ready to Upgrade
□	2	\root\lisa\P662301	3.40(SW.2)b1_20050120	Ready to Upgrade
□	3	\root\lisa\662302	3.40(SW.2)b1_20050120	Ready to Upgrade
□	4	\root\lisa\662304	3.40(SW.2)b4_050218	Ready to Upgrade

□ Select All

□ Select all devices in all pages

☑	Enable Scheduler
Date & Time:	2005 : 02 : 12 : 14
Description	test scheduler

See Table 8 on page 63 for field descriptions.

3 Select the **Enable Scheduler** checkbox.

4 Fill in the **Date & Time** fields to schedule a firmware upgrade start time. Type a date in yyyy:mm:dd format followed by the time in hh format.

5 Type some extra information in the description field. This description appears in the firmware upgrade report screen when the upgrade is logged.

6 Click **Apply** to begin the device upgrade process.

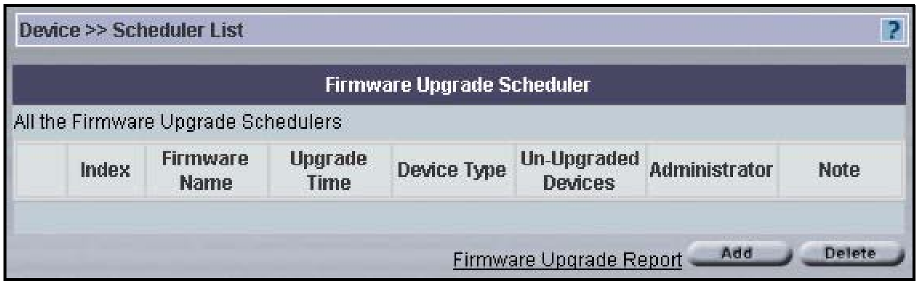
3.6.2 Firmware Upgrade Scheduler List

Use the **Firmware Upgrade Scheduler** screen to view the firmware status of ZyXEL devices managed by Vantage CNM.

View the names of firmware on each device, the time an upgrade was performed, the devices which firmware was upgraded, devices that have not been upgraded via Vantage and the names of the administrators that performed each upgrade.

Click **Device** > **Scheduler List** to display the next screen.

Figure 35 Device > Scheduler List



Device >> Scheduler List

Firmware Upgrade Scheduler

All the Firmware Upgrade Schedulers

	Index	Firmware Name	Upgrade Time	Device Type	Un-Upgraded Devices	Administrator	Note

The following table describes the fields in this screen

Table 12 Device > Scheduler List

TYPE	DESCRIPTION
Index	This field displays the firmware upgrade list number.
Firmware Name	This field displays the ZyNOS (ZyXEL network operating System) firmware version that was uploaded to a ZyXEL device.
Upgrade Time	This field displays the time a firmware upgrade was performed by an administrator.
Device Type	This field displays the device on which the firmware upgrade was performed, for example Prestige 662HW-61.
Un-Upgraded Devices	This field displays the names of ZyXEL devices that have not been upgraded by the Vantage CNM upgrade scheduler.
Administrator	This field displays the administrator who performed a firmware upgrade on a ZyXEL device(s) via the Vantage CNM scheduler.
Note	This field displays a note relating to the firmware upgrade.
Firmware Upgrade Report	Click this hyperlink to go to the **Firmware Upgrade Report** screen. See the chapter Other Monitor Screens in this User's Guide for more information.
Add	Click **Add** to proceed to the firmware upgrade screen, see Firmware Upgrade Select Product Line and Mode on page 64.
Delete	Select a check box and click **Delete** to remove an entry from the **SchedulerList**.

CHAPTER 4
Configuration > Select Device BB & General

This section shows you how to use the select device building block screen and how to configure the **General** menus.

These screens will vary depending on which model you’re configuring.

When you click a configuration menu, the screen shows the current device configuration.

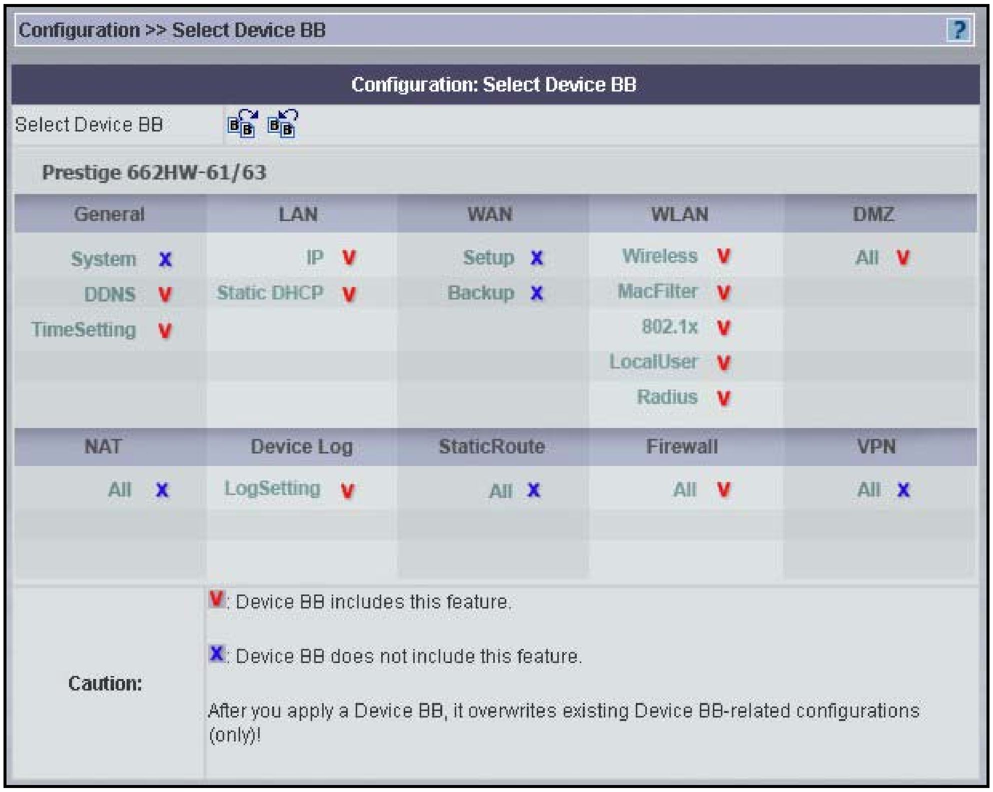
If you’re unfamiliar with ZyXEL device configurations, please consult your device User’s Guide.

Configuration > **General** can be saved as one **Configuration BB**.

4.1 Select Device BB

A device BB (Building Block) is a combination of configuration BBs. A device’s device BB varies by model type. The following figures shows a device BB for the Prestige 662W-61/63. A check mark indicates that the device BB includes this configuration and an “X” denotes that it doesn’t.

Figure 36 Prestige 662W-61/63 Device BB



Configuration >> Select Device BB

Configuration: Select Device BB

Select Device BB

Prestige 662HW-61/63

General		LAN		WAN		WLAN		DMZ	
System	X	IP	V	Setup	X	Wireless	V	All	V
DDNS	V	Static DHCP	V	Backup	X	MacFilter	V		
TimeSetting	V					802.1x	V		
						LocalUser	V		
						Radius	V		
NAT		**Device Log**		**StaticRoute**		**Firewall**		**VPN**	
All	X	LogSetting	V	All	X	All	V	All	X

Caution:

V: Device BB includes this feature.

X: Device BB does not include this feature.

After you apply a Device BB, it overwrites existing Device BB-related configurations (only)!

This **Select Device BB** screen allows you to select a device’s device BB and apply it to another device of the same type.

Note: You can only apply a device BB to another device of the same type.

4.1.1 Procedure to Select and Apply a Device BB

1 Select the device from which you want to copy its configuration.

2 Click **Configuration** > **Select Device BB** to display the next screen.

3 Click the “Save as a BB” icon () and save it as a new BB with a unique device BB name.

4 Select the device to which you want to paste this configuration.

5 Click **Configuration** > **Select Device BB** to display the next screen.

6 Click the “Load a BB” icon () and select the BB you just saved.

7 Click the **Apply** button to save that configuration to the device.

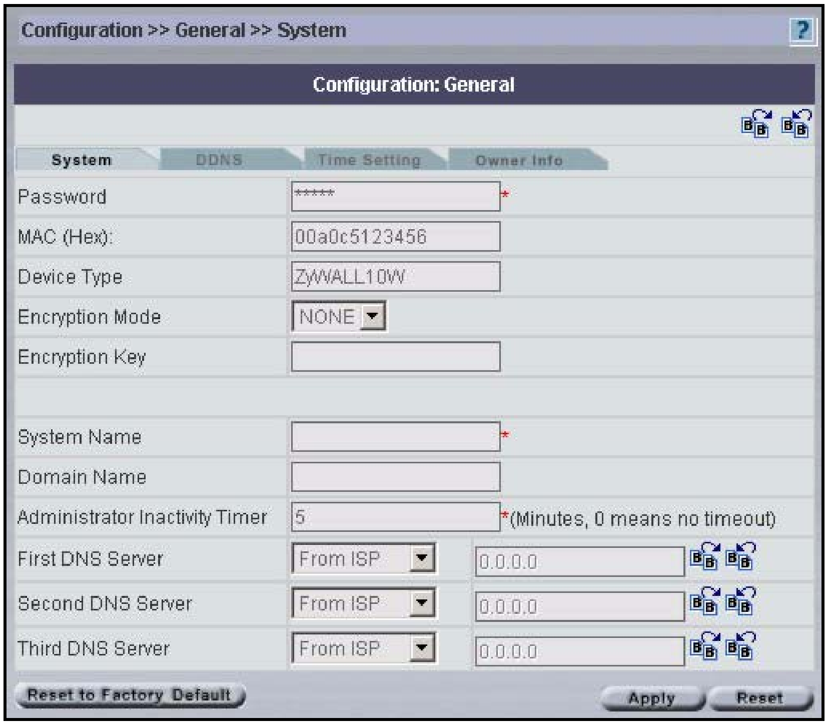
8 This device configuration can then be further fine-tuned using the regular configuration menus and saved as another new device BB.

4.2 Configuration General Screens

Click **Configuration > General** to configure **System**, **DDNS**, **Time Setting** and **Owner Info**. The **System** tab is shown next.

4.2.1 System

Figure 37 Configuration > General > System - ZyWALL



Password: ***** *
MAC (Hex): 00a0c5123456
Device Type: ZyWALL10W
Encryption Mode: NONE
Encryption Key:
System Name: *
Domain Name:
Administrator Inactivity Timer: 5 *(Minutes, 0 means no timeout)
First DNS Server: From ISP 0.0.0.0
Second DNS Server: From ISP 0.0.0.0
Third DNS Server: From ISP 0.0.0.0

The following table describes the fields in this screen

Table 13 Configuration > General > System - ZyWALL

FIELD	DESCRIPTION
Password	Enter the password used to access the device.
MAC (Hex)	This field displays the LAN MAC address of the ZyXEL device. Vantage uses the MAC address to identify the ZyXEL device. This is entered when you manually register the ZyXEL device.
Device Type	This field displays the ZyXEL device type selected in the object tree.

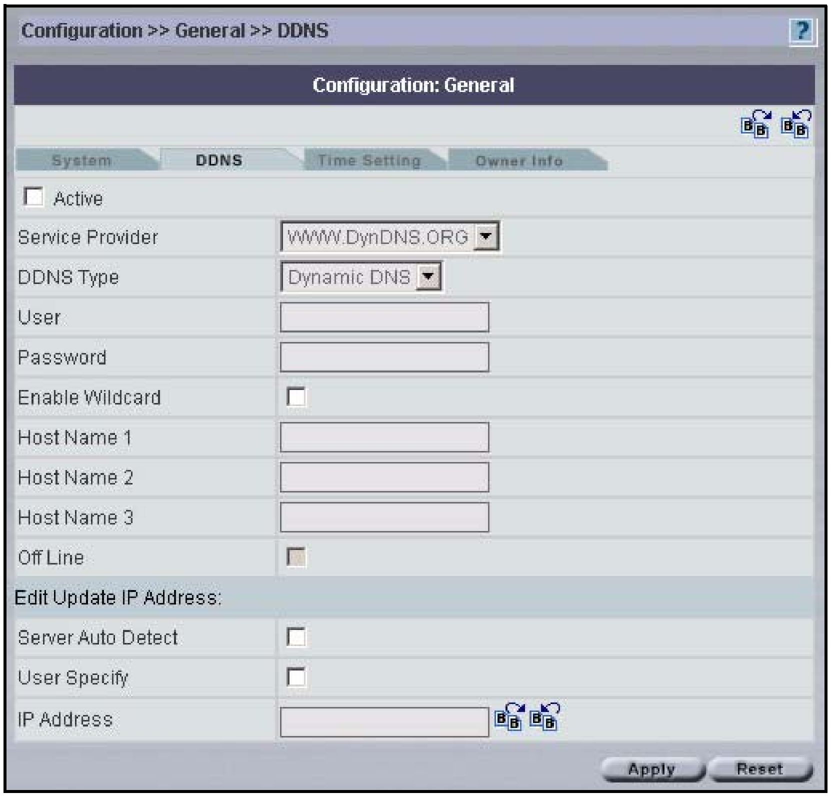
Table 13 Configuration > General > System - ZyWALL (continued)

FIELD	DESCRIPTION
Encryption Mode	You may choose to encrypt traffic between the ZyXEL device and the Vantage server here. Choose from **None** (no encryption), **DES** or **3DES**. The ZyXEL device must be set to the same encryption mode (and have the same encryption key) as the Vantage server. You do not need to add NAT or firewall rules when you encrypt this traffic. To set the encryption mode on the ZyXEL device, do the following: Go to CI mode (SMT 24.8 for devices with SMT menus) Type '`CNM encrymode X`' where: Value of X Encryption Mode 0 None 1 DES 2 3DES
Encryption Key	Type an eight-character alphanumeric ("0" to "9", "a" to "z") for **DES** encryption and a 24-character alphanumeric ("0" to "9", "a" to "z") for **3DES** encryption. To set the encryption key on the ZyXEL device, type '`CNM encrykey xxxxxxxxx`' where '`xxxxxxxxx'` is the hexadecimal secret key number you used in the Vantage server.
System Name	Enter a unique name here for the ZyXEL device for identification purposes. The device name cannot exceed 31 characters.
Domain Name	The Domain Name entry is what is propagated to the DHCP clients on the LAN side of the target device. If you leave this blank, the domain name obtained by the device via DHCP from the ISP is used.
Administrator Inactivity Timer	Set how long a management session can remain idle before it expires. After it expires, you have to (default five minutes) log back into the device.
First DNS Server Second DNS Server Third DNS Server	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. These DNS servers refer to the device system DNS server. The device uses a system DNS server (in the order you specify here) to resolve domain names for VPN, DDNS and the timeserver. Select **From ISP** if the ISP dynamically assigns the device DNS server information. The text box to the right then displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you want to assign the DNS server IP address yourself. Enter the DNS server's IP address in the field to the right or select from an IP address component BB. Select **None** if you do not want to configure device system DNS servers. If you do not configure a system DNS server, you must use IP addresses when configuring VPN and DDNS.
Reset to Factory Default	Click this button to upload the factory-default configuration file of the device.
Reset	Click **Reset** to begin configuring the screen afresh.

4.2.2 DDNS

Use this screen to configure your DNS parameters

Figure 38 Configuration > General > DDNS



Configuration >> General >> DDNS

Configuration: General

☐ Active

Service Provider	WWW.DynDNS.ORG ▾
DDNS Type	Dynamic DNS ▾
User	
Password	
Enable Wildcard	☐
Host Name 1	
Host Name 2	
Host Name 3	
Off Line	☐
Edit Update IP Address:	
Server Auto Detect	☐
User Specify	☐
IP Address	

The following table describes the fields in this screen

Table 14 Configuration > General > DDNS

LABEL	DESCRIPTION
Active	Select this check box to use dynamic DNS.
Service Provider	Select the name of your Dynamic DNS service provider.
DDNS Type	Select the type of service that you are registered for from your Dynamic DNS service provider.
User	Enter your user name.
Password	Enter the password assigned to you.
Enable Wildcard	Select the check box to enable DYNDNS Wildcard.
Host Names 1~3	Enter the host names in the three fields provided. You can specify up to two host names in each field separated by a comma (",").
Off Line	This option is available when **CustomDNS** is selected in the **DDNS Type field**. Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line.
Edit Update IP Address:	
Server Auto Detect	Select this option to update the IP address of the host name(s) automatically by the DDNS server. It is recommended that you select this option.
User Specify	Select this option to update the IP address of the host name(s) to the IP address specified below. Use this option if you have a static IP address.

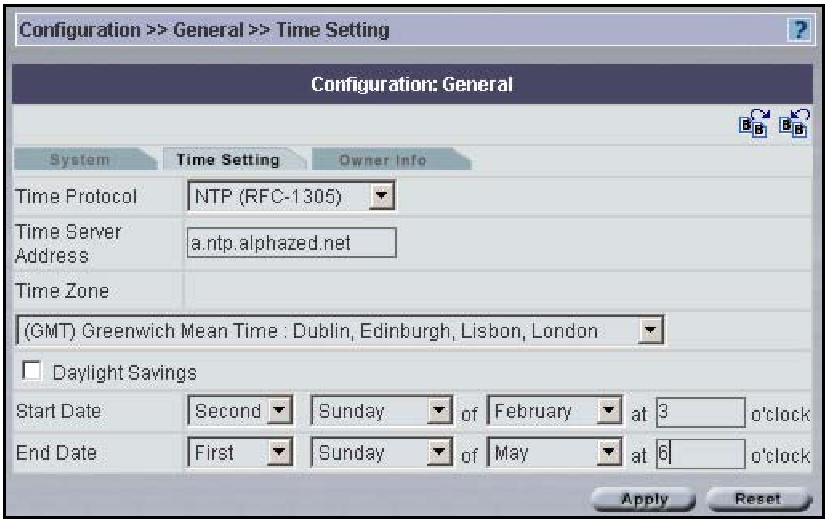
Table 14 Configuration > General > DDNS (continued)

LABEL	DESCRIPTION
IP Address	Enter the IP address if you select the **User Specify** option.
E-Mail (Prestige Only)	Type the e-mail address here or select from a previously created e-mail component BB. You may also save a newly entered e-mail address as a new e-mail component BB.
Apply	Click **Apply** to save your changes back to the device.
Reset	Click **Reset** to begin configuring this screen afresh.

4.2.3 Time Setting

Use this screen to configure your time settings.

Figure 39 Configuration > General > Time Setting



Configuration >> General >> Time Setting

Configuration: General

Time Protocol: NTP (RFC-1305)

Time Server Address: a.ntp.alphazed.net

Time Zone: (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London

□ Daylight Savings

Start Date: Second Sunday of February at 3 o'clock

End Date: First Sunday of May at 6 o'clock

The following table describes the fields in this screen

Table 15 Configuration > General > Time Setting

LABEL	DESCRIPTION
Time Protocol (or Use Time Server when Bootup)	Select the time service protocol that your timeserver sends when you turn on the device. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main difference between them is the format. **Daytime (RFC 867)** format is day/month/year/time zone of the server. **Time (RFC 868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. The default, **NTP (RFC 1305),** is similar to Time (RFC 868). Select **None** to enter the time and date manually.
Time Server Address.	Enter the IP address of your timeserver. Check with your ISP/network administrator if you are unsure of this information (the default is tick.stdtime.gov.tw)

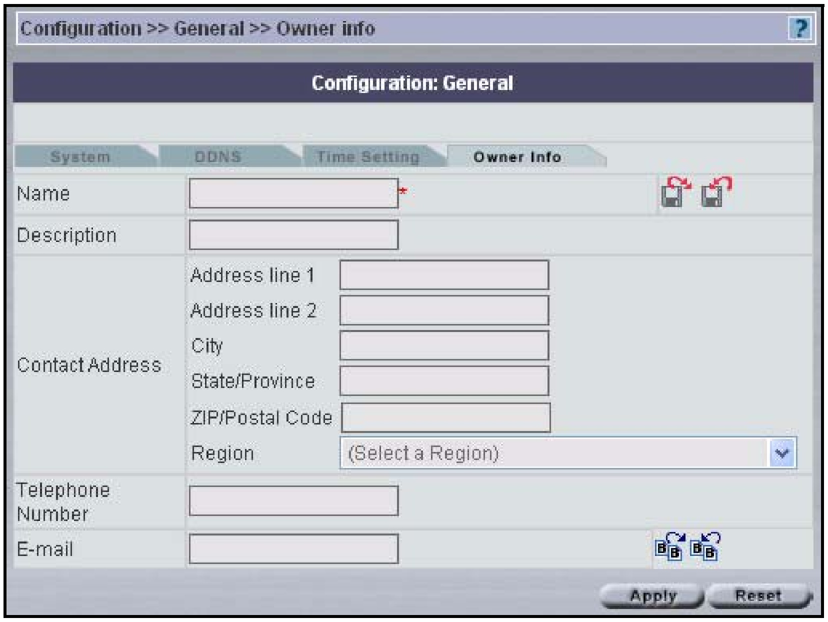
Table 15 Configuration > General > Time Setting (continued)

LABEL	DESCRIPTION
Time Zone	Choose the Time Zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected **Daylight Savings**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the first Sunday of April. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **April** and type 2 in the **o'clock** field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **March**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you selected **Daylight Savings**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the last Sunday of October. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Last**, **Sunday**, **October** and type 2 in the **o'clock** field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **October**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Calibrate now (Prestige only)	Select the check box to have your Prestige use the timeserver (that you configured above) to set its internal system clock.
Apply	Click **Apply** to save your changes back to the device.
Reset	Click **Reset** to begin configuring this screen afresh.

4.2.4 Owner Info

The address book is the equivalent of a device owner BB. You can select from previous entries or save as new entries.

Figure 40 Configuration > General > Owner Info



Name *

Description

Contact Address: Address line 1, Address line 2, City, State/Province, ZIP/Postal Code, Region (Select a Region)

Telephone Number

E-mail

The following table describes the fields in this screen.

Table 16 Configuration > General > Owner Info

	DESCRIPTION
Name	Type the full name of the owner of this device.
Description	Type some extra information about this customer.
Contact Address	Type the complete customer mailing address here.
Address 1, 2	Type the customer’s building number, street and city zone (if applicable) here.
City	Type the full city or town name.
StateProvince	Type the state or province.
ZIP/Postal Code	Type the zip or postal code here.
Region	Select the country or region from the list.
Telephone Number	Type the customer’s telephone number including country code and area code here.
E-mail	Type the customer’s e-mail address here or select from a previously created e-mail component BB. You may also save a newly entered e-mail address as a new e-mail component BB.
Apply	Click **Apply** to create the BB. This BB is then available in the BB pool for this domain.
Reset	Click **Reset** to begin configuring the screen afresh.

CHAPTER 5
Configuration > LAN

5.1 LAN Overview

The **Configuration: LAN** screen varies depending on the device type shown.

Local Area Network (LAN) is a shared communication system to which many computers are attached. Use the LAN screens to configure a LAN DHCP server, manage IP addresses, and partition a physical network into logical networks.

5.2 DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the ZyXEL device as a DHCP server or disable it. When configured as a server, the ZyXEL device provides the IP configuration for the clients. If set to **None**, DHCP service will be disabled and you must have another DHCP server on your LAN, or else the computer must be manually configured.

5.2.1 IP Pool Setup

The ZyXEL device is pre-configured with a pool of 32 IP addresses starting from 192.168.1.33 to 192.168.1.64. This configuration leaves 31 IP addresses (excluding the ZyXEL device itself) in the lower range for other server computers, for instance, servers for mail, FTP, TFTP, web, etc., that you may have.

5.2.2 DNS Servers

Use the LAN IP screen to configure the DNS server information that the ZyXEL device sends to the DHCP client devices on the LAN.

5.2.3 LAN TCP/IP

The ZyXEL device has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

5.2.4 Factory LAN Defaults

The LAN parameters of the ZyXEL device are preset in the factory with the following values:

- IP address of 192.168.1.1 with subnet mask of 255.255.255.0 (24 bits)
- DHCP server enabled with 32 client IP addresses starting from 192.168.1.33.

These parameters should work for the majority of installations. If your ISP gives you explicit DNS server address(es), read the embedded web configurator help regarding what fields need to be configured.

5.2.5 IP Address and Subnet Mask

Refer to the IP Address and Subnet Mask section in the **Wizard Setup** chapter for this information.

5.2.6 RIP Setup

RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a router to exchange routing information with other routers. **RIP Direction** controls the sending and receiving of RIP packets. When set to **Both** or **Out Only**, the ZyXEL device will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received.

RIP Version controls the format and the broadcasting method of the RIP packets that the ZyXEL device 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** send routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also.

By default, **RIP Direction** is set to **Both** and **RIP Version** to **RIP-1**.

5.2.7 Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about inter-operability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address

224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

The ZyXEL device supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the ZyXEL device queries all directly connected networks to gather group membership. After that, the ZyXEL device periodically updates this information. IP multicasting can be enabled/disabled on the ZyXEL device LAN and/or WAN interfaces in the web configurator (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

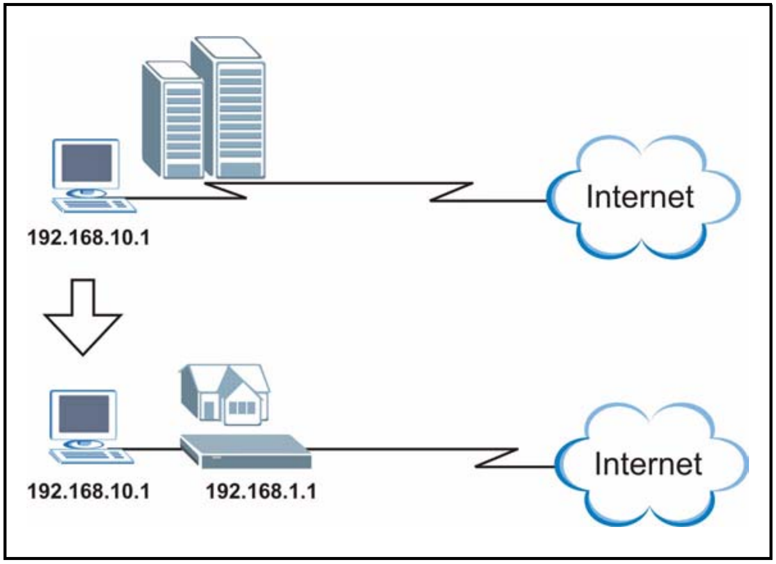
5.3 Any IP

Traditionally, you must set the IP addresses and the subnet masks of a computer and the Prestige to be in the same subnet to allow the computer to access the Internet (through the Prestige). In cases where your computer is required to use a static IP address in another network, you may need to manually configure the network settings of the computer every time you want to access the Internet via the Prestige.

With the Any IP feature and NAT enabled, the Prestige allows a computer to access the Internet without changing the network settings (such as IP address and subnet mask) of the computer, when the IP addresses of the computer and the Prestige are not in the same subnet. Whether a computer is set to use a dynamic or static (fixed) IP address, you can simply connect the computer to the Prestige and access the Internet.

The following figure depicts a scenario where a computer is set to use a static private IP address in the corporate environment. In a residential house where a Prestige is installed, you can still use the computer to access the Internet without changing the network settings, even when the IP addresses of the computer and the Prestige are not in the same subnet.

Figure 41 Any IP Example Application



The Any IP feature does not apply to a computer using either a dynamic IP address or a static IP address that is in the same subnet as the Prestige's IP address.

Note: You MUST enable NAT to use the Any IP feature on the Prestige

5.3.1 How Any IP Works

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. IP routing table is defined on IP Ethernet devices (the Prestige) to decide which hop to use, to help forward data along to its specified destination.

The following lists out the steps taken, when a computer tries to access the Internet for the first time through the Prestige.

1 When a computer (which is in a different subnet) first attempts to access the Internet, it sends packets to its default gateway (which is not the Prestige) by looking at the MAC address in its ARP table.

2 When the computer cannot locate the default gateway, an ARP request is broadcast on the LAN.

3 The Prestige receives the ARP request and replies to the computer with its own MAC address.

4 The computer updates the MAC address for the default gateway to the ARP table. Once the ARP table is updated, the computer is able to access the Internet through the Prestige.

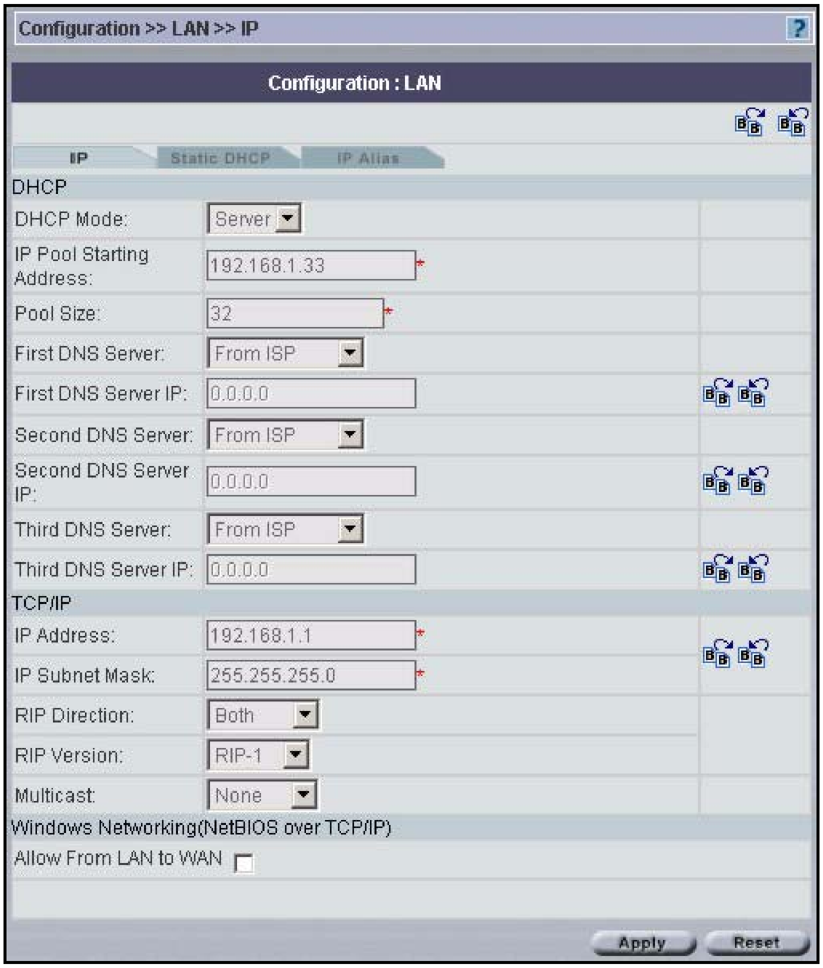
5 When the Prestige receives packets from the computer, it creates an entry in the IP routing table so it can properly forward packets intended for the computer.

After all the routing information is updated, the computer can access the Prestige and the Internet as if it is in the same subnet as the Prestige.

5.4 Configuring LAN IP - ZyWALL

Select a device and then click **Configuration** > **LAN**. **IP** is the first tab.

Figure 42 Configuration > LAN > IP - ZyWALL



DHCP

DHCP Mode:	Server
IP Pool Starting Address:	192.168.1.33 *
Pool Size:	32 *
First DNS Server:	From ISP
First DNS Server IP:	0.0.0.0
Second DNS Server:	From ISP
Second DNS Server IP:	0.0.0.0
Third DNS Server:	From ISP
Third DNS Server IP:	0.0.0.0

TCP/IP

IP Address:	192.168.1.1 *
IP Subnet Mask:	255.255.255.0 *
RIP Direction:	Both
RIP Version:	RIP-1
Multicast:	None

Windows Networking(NetBIOS over TCP/IP)

Allow From LAN to WAN □

The following table describes the fields in this screen

Table 17 Configuration > LAN > IP - ZyWALL

LABEL	DESCRIPTION
DHCP Mode	DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (computers) to obtain TCP/IP configuration at startup from a server. When configured as a server, the ZyXEL device provides TCP/IP configuration for the clients. If not, DHCP service is disabled and you must have another DHCP server on your LAN, or else the computer must be manually configured. When set as a server, fill in the rest of the DHCP setup fields.
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Pool Size	This field specifies the size, or count of the IP address pool.

Table 17 Configuration > LAN > IP - ZyWALL (continued)

LABEL	DESCRIPTION
First DNS Server Second DNS Server Third DNS Server	Domain Name System is for mapping a domain name to its corresponding IP address and vice versa. The ZyXEL device passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP clients. The ZyXEL device only passes this information to the LAN DHCP clients when you select **DHCP Server**. If you don’t select **DHCP Server**, DHCP service is disabled and you must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured. Select **From ISP** if an ISP dynamically assigns DNS server information (and the ZyXEL device’s WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **DNS Relay** to have the ZyXEL device act as a DNS proxy. The ZyXEL device’s LAN IP address displays in the field to the right (read-only). The ZyXEL device tells the DHCP clients on the LAN that the ZyXEL device itself is the DNS server. When a computer on the LAN sends a DNS query to the ZyXEL device, the ZyXEL device forwards the query to the ZyXEL device’s system DNS server (configured in the **SYSTEM General** screen) and relays the response back to the computer. You can only select **DNS Relay** for one of the three servers; if you select **DNS Relay** for a second or third DNS server, that choice changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it.
TCP/IP	
IP Address	Type the IP address of the ZyXEL device in dotted decimal notation. 192.168.1.1 is the factory default.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. The ZyXEL device automatically calculates the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyXEL device, which is 255.255.255.0.
RIP Direction	RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **Both**/**In Only**/**Out Only**/**None**. When set to **Both** or **Out Only**, the ZyXEL device broadcasts its routing table periodically. When set to **Both** or **In Only**, it incorporates the RIP information that it receives; when set to **None**, it does not send any RIP packets and ignores any RIP packets received. **Both** is the default.
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyXEL device 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. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to **Both** and the **Version** set to **RIP-1**.

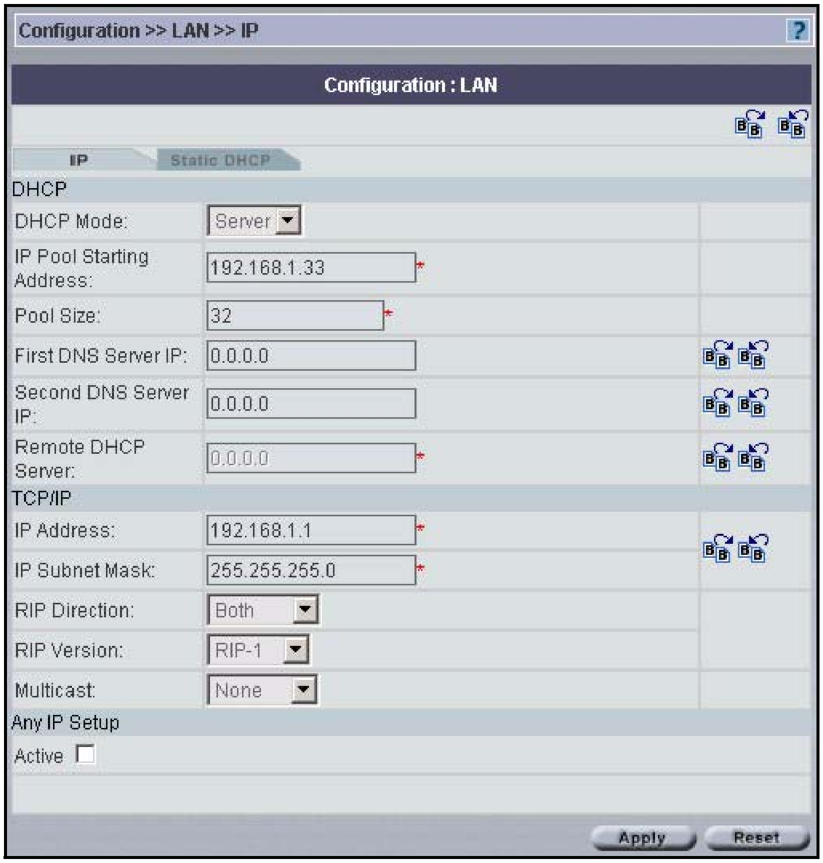
Table 17 Configuration > LAN > IP - ZyWALL (continued)

LABEL	DESCRIPTION
Multicast	Select **IGMP V-1** or **IGMP V-2** or **None**. IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about inter operability between IGMP version 2 and version 1, please see *sections 4 and 5 of RFC 2236*.
Windows Networking (NetBIOS over TCP/IP): NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls. However it may sometimes be necessary to allow NetBIOS packets to pass through to the WAN in order to find a computer on the WAN.	
Allow From LAN to WAN	Select this option to forward NetBIOS packets from the LAN port to the WAN port.
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Reset	Click **Reset** to begin configuring this screen afresh.

5.5 Configuring LAN IP - Prestige

Select a device, and then click **Configuration > LAN**. **IP** is the only tab used for an ADSL device.

Figure 43 Configuration > LAN > IP - Prestige



DHCP

DHCP Mode: Server

IP Pool Starting Address: 192.168.1.33 *

Pool Size: 32 *

First DNS Server IP: 0.0.0.0

Second DNS Server IP: 0.0.0.0

Remote DHCP Server: 0.0.0.0 *

TCP/IP

IP Address: 192.168.1.1 *

IP Subnet Mask: 255.255.255.0 *

RIP Direction: Both

RIP Version: RIP-1

Multicast: None

Any IP Setup

Active □

Table 18 Configuration > LAN > IP - Prestige

LABEL	DESCRIPTION
DHCP Mode	DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (computers) to obtain TCP/IP configuration at startup from a server. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it. When configured as a **Server**, the ZyXEL device provides TCP/IP configuration for the clients. When set as a **Server**, fill in the rest of the DHCP setup fields. Select **Relay** to have the ZyXEL device act as a DNS proxy. The ZyXEL device tells the DHCP clients on the LAN that the ZyXEL device itself is the DNS server. When a computer on the LAN sends a DNS query to the ZyXEL device, the ZyXEL device forwards the query to the ZyXEL device's system DNS server and relays the response back to the computer. You can select **Relay** and enter an IP Pool Starting Address. The First DNS Server IP and Second DNS Server IP will appear as read only fields.
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Pool Size	This field specifies the size, or count of the IP address pool.
First DNS Server IP Second DNS Server IP	The ZyWALL passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP clients. Type your First DNS Server IP and Second DNS Server IP addresses in these fields.
Remote DHCP Server	If **Relay** is selected in the DHCP field above, then type the IP address of the actual, remote DHCP server here.

Table 18 Configuration > LAN > IP - Prestige (continued)

LABEL	DESCRIPTION
TCP/IP	
IP Address	Type the IP address of the ZyXEL device in dotted decimal notation. 192.168.1.1 is the factory default.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. The ZyXEL device automatically calculates the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyXEL device, which is 255.255.255.0.
RIP Direction	RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **Both**/**In Only**/**Out Only**/**None**. When set to **Both** or **Out Only**, the ZyXEL device broadcasts its routing table periodically. When set to **Both** or **In Only**, it incorporates the RIP information that it receives; when set to **None**, it does not send any RIP packets and ignores any RIP packets received. **Both** is the default.
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyXEL device 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. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to **Both** and the **Version** set to **RIP-1**.
Multicast	Select **IGMP V-1** or **IGMP V-2** or **None**. IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interpretability between IGMP version 2 and version 1, please see *sections 4 and 5 of RFC 2236*.
Any IP Setup	
Active	Select this option to activate the Any-IP feature. This allows a computer to access the Internet without changing the network settings (such as IP address and subnet mask) of the computer, even when the IP addresses of the computer and the Prestige are not in the same subnet. When you disable the Any-IP feature, only computers with dynamic IP addresses or static IP addresses in the same subnet as the Prestige's LAN IP address can connect to the Prestige or access the Internet through the Prestige.
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Reset	Click **Reset** to begin configuring this screen afresh.

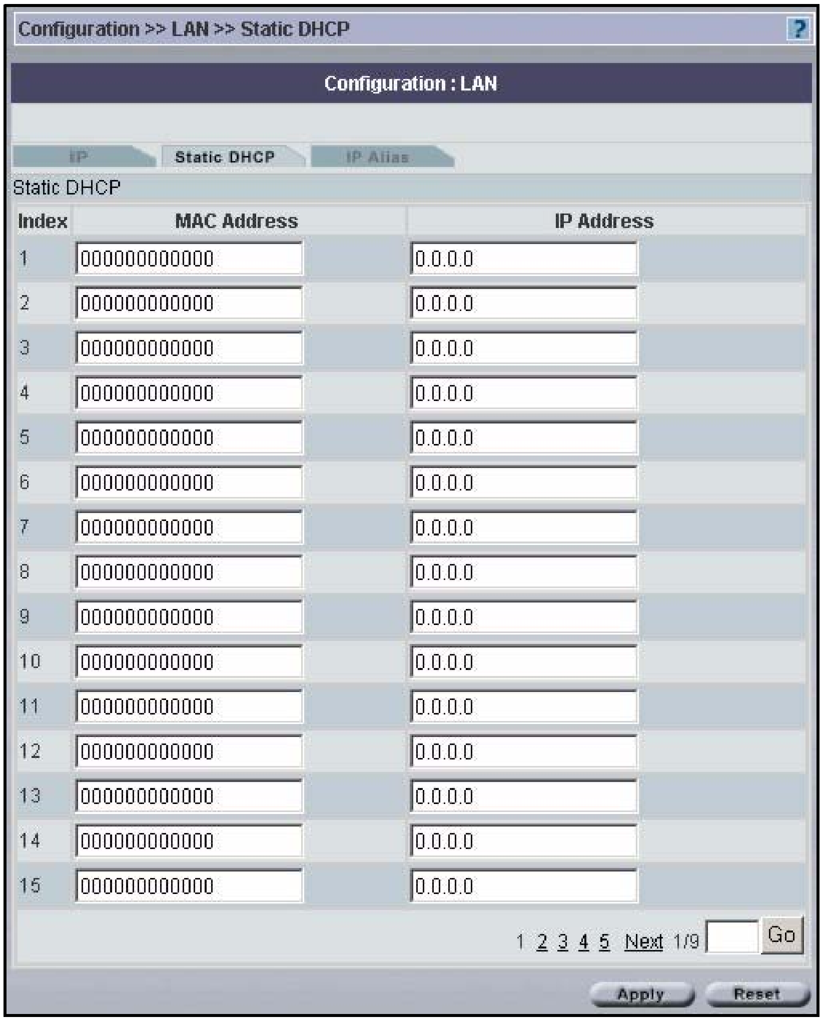
5.6 Configuring LAN Static DHCP

This table allows you to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses.

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

Select a device, and then click **Configuration > LAN > Static DHCP**.

Figure 44 Configuration > LAN > Static DHCP



Static DHCP

Index	MAC Address	IP Address
1	000000000000	0.0.0.0
2	000000000000	0.0.0.0
3	000000000000	0.0.0.0
4	000000000000	0.0.0.0
5	000000000000	0.0.0.0
6	000000000000	0.0.0.0
7	000000000000	0.0.0.0
8	000000000000	0.0.0.0
9	000000000000	0.0.0.0
10	000000000000	0.0.0.0
11	000000000000	0.0.0.0
12	000000000000	0.0.0.0
13	000000000000	0.0.0.0
14	000000000000	0.0.0.0
15	000000000000	0.0.0.0

The following table describes the fields in this screen

Table 19 Configuration > LAN > Static DHCP

LABEL	DESCRIPTION
Index	This is the index number of the Static IP table entry (row).
MAC Address	This is the MAC address of a computer on the device's LAN.
IP Address	This is the IP address to be assigned to the device with the MAC address above.
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Reset	Click **Reset** to begin configuring this screen afresh.

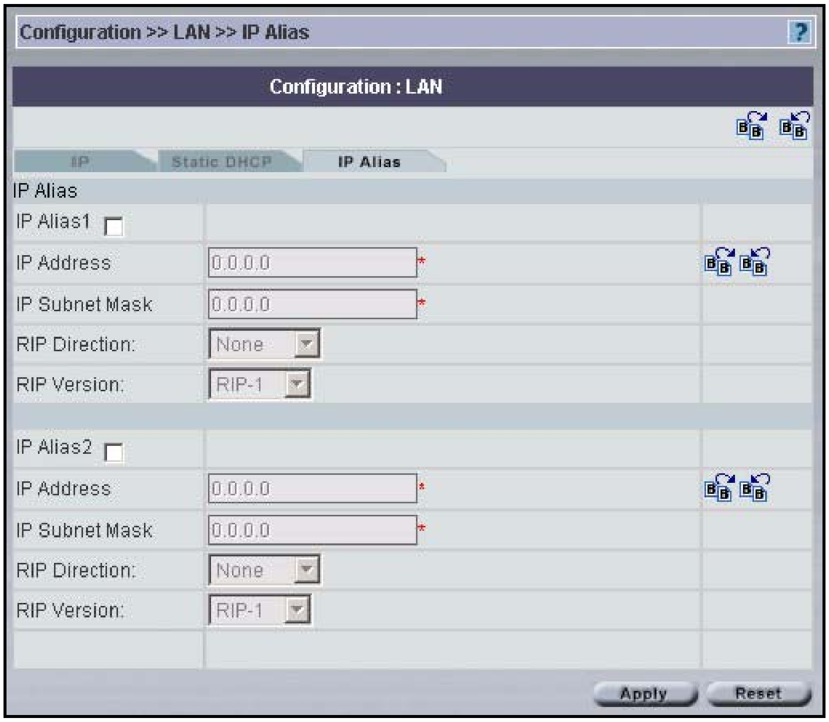
5.7 Configuring LAN IP Alias - ZyWALL

IP Alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The ZyXEL device lets you configure logical LAN interfaces via its single physical Ethernet interface with the device itself being the gateway for each LAN network.

When you use IP alias, you can also configure firewall rules to control access between the LAN's logical networks (subnets).

Select a device, and then click **Configuration > LAN > IP Alias**.

Figure 45 Configuration > LAN > IP Alias - ZyWALL



IP Alias

IP Alias1 □

IP Address: 0.0.0.0 *

IP Subnet Mask: 0.0.0.0 *

RIP Direction: None

RIP Version: RIP-1

IP Alias2 □

IP Address: 0.0.0.0 *

IP Subnet Mask: 0.0.0.0 *

RIP Direction: None

RIP Version: RIP-1

The following table describes the fields in this screen

Table 20 Configuration > LAN > IP Alias - ZyWALL

LABEL	DESCRIPTION
IP Alias 1,2	Select the check box to configure another LAN network for the ZyXEL device.
IP Address	Enter the IP address of the ZyXEL device in dotted decimal notation.
IP Subnet Mask	The ZyXEL device automatically calculates the subnet mask based how many aliases you select. See also the appendices for more information on IP subnetting.

Table 20 Configuration > LAN > IP Alias - ZyWALL (continued)

LABEL	DESCRIPTION
RIP Direction	RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **Both**/**In Only**/**Out Only**/**None**. When set to **Both** or **Out Only**, the ZyXEL device broadcasts its routing table periodically. When set to **Both** or **In Only**, it incorporates the RIP information that it receives; when set to **None**, it does not send any RIP packets and ignores any RIP packets received.
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyXEL device 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. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to **Both** and the Version set to **RIP-1**.
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Reset	Click **Reset** to begin configuring this screen afresh.

CHAPTER 6
Configuration > WLAN

This chapter discusses how to configure Wireless LAN.

6.1 Introduction

A wireless LAN can be as simple as two computers with wireless LAN adapters communicating in a peer-to-peer network or as complex as a number of computers with wireless LAN adapters communicating through access points which bridge network traffic to the wired LAN.

Note: See the WLAN appendix for more detailed information on WLANs.

6.2 Wireless Security Overview

Wireless security is vital to your network to protect wireless communication between wireless stations, access points and the wired network.

Wireless security methods available on the Prestige are data encryption, wireless client authentication, restricting access by device MAC address and hiding the Prestige identity.

6.2.1 Encryption

- Use WPA security if you have WPA-aware wireless clients and a RADIUS server. WPA has user authentication and improved data encryption over WEP.
- Use WPA-PSK if you have WPA-aware wireless clients but no RADIUS server.
- If you don't have WPA-aware wireless clients, then use WEP key encrypting. A higher bit key offers better security at a throughput trade-off. You can use Passphrase to automatically generate 64-bit or 128-bit WEP keys or manually enter 64-bit, 128-bit or 256-bit WEP keys.

6.2.2 Authentication

WPA has user authentication and you can also configure IEEE 802.1x to use the built-in database (Local User Database) or a RADIUS server to authenticate wireless clients before joining your network.

- Use RADIUS authentication if you have a RADIUS server. See the appendices for information on protocols used when a client authenticates with a RADIUS server via the Prestige.

- Use the Local User Database if you have less than 32 wireless clients in your network. The Prestige uses MD5 encryption when a client authenticates with the Local User Database

6.2.3 Restricted Access

The **MAC Filter** screen allows you to configure the AP to give exclusive access to devices (**Allow Association**) or exclude them from accessing the AP (**Deny Association**).

6.2.4 Hide Prestige Identity

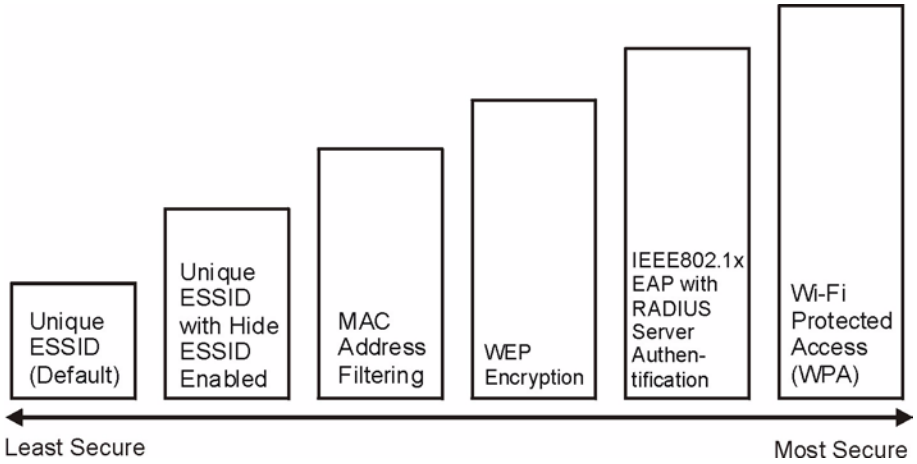
If you hide the ESSID, then the Prestige cannot be seen when a wireless client scans for local APs. The trade-off for the extra security of "hiding" the Prestige may be inconvenience for some valid WLAN clients. If you don't hide the ESSID, at least you should change the default one.

6.2.5 Configuring Wireless LAN on the Prestige

1. Configure the **ESSID** and **WEP** in the **Wireless** screen. If you configure **WEP**, you can't configure **WPA** or **WPA-PSK**.
2. Use the **MAC Filter** screen to restrict access to your wireless network by MAC address.
3. Configure **WPA** or **WPA-PSK** in the **802.1x/WPA** screen. You can also configure 802.1x wireless client authentication in the **802.1x/WPA** screen.
4. Configure the RADIUS authentication database settings in the **RADIUS** screen.
5. Configure the built-in authentication database in the **Local User Database** screen.

The following figure shows the relative effectiveness of these wireless security methods available on your Prestige.

Figure 46 Wireless Security Methods


Unique ESSID (Default)
Unique ESSID with Hide ESSID Enabled
MAC Address Filtering
WEP Encryption
IEEE802.1x EAP with RADIUS Server Authen-tification
Wi-Fi Protected Access (WPA)
Least Secure
Most Secure

Note: You must enable the same wireless security settings on the Prestige and on all wireless clients that you want to associate with it.

If you do not enable any wireless security on your Prestige, your network is accessible to any wireless networking device that is within range.

6.3 Configuring the Wireless Screen

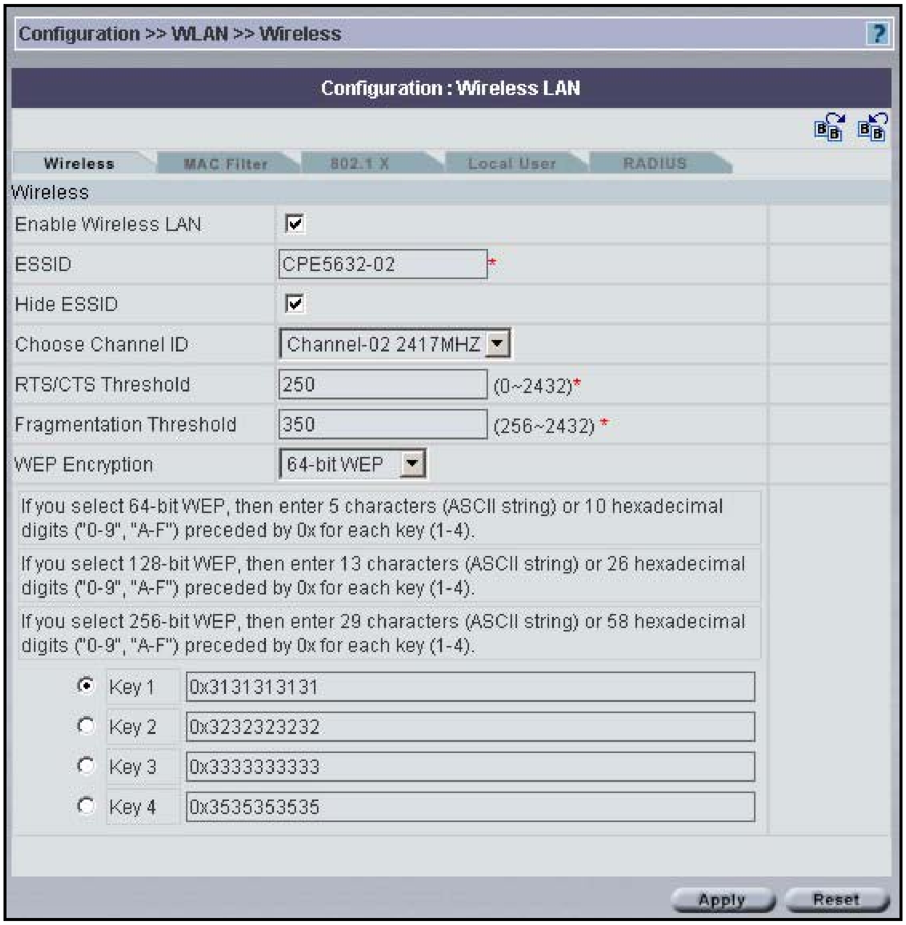
6.3.1 WEP Encryption

WEP encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private. It encrypts unicast and multicast communications in a network. Both the wireless stations and the access points must use the same WEP key.

Your Prestige allows you to configure up to four 64-bit, 128-bit or 256-bit WEP keys but only one key can be enabled at any one time.

In order to configure and enable WEP encryption; select a device, and then click **Configuration > WLAN**.

Figure 47 Configuration > WLAN > Wireless



Configuration >> WLAN >> Wireless

Configuration : Wireless LAN

Wireless

Enable Wireless LAN	☑
ESSID	CPE5632-02 *
Hide ESSID	☑
Choose Channel ID	Channel-02 2417MHZ
RTS/CTS Threshold	250 (0~2432)*
Fragmentation Threshold	350 (256~2432) *
WEP Encryption	64-bit WEP

If you select 64-bit WEP, then enter 5 characters (ASCII string) or 10 hexadecimal digits ("0-9", "A-F") preceded by 0x for each key (1-4).

If you select 128-bit WEP, then enter 13 characters (ASCII string) or 26 hexadecimal digits ("0-9", "A-F") preceded by 0x for each key (1-4).

If you select 256-bit WEP, then enter 29 characters (ASCII string) or 58 hexadecimal digits ("0-9", "A-F") preceded by 0x for each key (1-4).

●	Key 1	0x3131313131
○	Key 2	0x3232323232
○	Key 3	0x3333333333
○	Key 4	0x3535353535

The following table describes the fields in this screen

Table 21 Configuration > WLAN > Wireless

LABEL	DESCRIPTION
Enable Wireless LAN	You should configure some wireless security (see Figure 46 on page 94) when you enable the wireless LAN. Select the check box to enable the wireless LAN.
ESSID	The ESSID (Extended Service Set IDentification) is a unique name to identify the Prestige in the wireless LAN. Wireless stations associating to the Prestige must have the same ESSID. Enter a descriptive name of up to 32 printable characters (including spaces; alphabetic characters are case-sensitive).
Hide ESSID	Select **Yes** to hide the ESSID in so a station cannot obtain the ESSID through AP scanning. Select **No** to make the ESSID visible so a station can obtain the ESSID through AP scanning.
Choose Channel ID	The radio frequency used by IEEE 802.11a, b or g wireless devices is called a channel. Select a channel from the drop-down list box.

Table 21 Configuration > WLAN > Wireless (continued)

LABEL	DESCRIPTION
RTS/CTS Threshold	The RTS (Request To Send) threshold (number of bytes) is for enabling RTS/CTS. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this value to be larger than the maximum MSDU (MAC service data unit) size turns off RTS/CTS. Setting this value to zero turns on RTS/CTS. Select the check box to change the default value and enter a new value between 0 and 2432.
Fragmentation Threshold	This is the threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Select the check box to change the default value and enter a value between 256 and 2432.
You won't see the following WEP-related fields if you have **WPA** or **WPA-PSK** enabled.	
WEP Encryption	WEP (Wired Equivalent Privacy) provides data encryption to prevent unauthorized wireless stations from accessing data transmitted over the wireless network. Select Disable to allow wireless clients to communicate with the access points without any data encryption. Select **64-bit WEP** or **128-bit WEP** to enable data encryption. Although WEP is functional at 5.5 and 11 Mbps, there is significant performance degradation when using WEP at these rates.
Key 1 to Key 4	If you chose **64-bit WEP** in the **WEP Encryption** field, then enter any 5 characters (ASCII string) or 10 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key. If you chose **128-bit WEP** in the **WEP Encryption** field, then enter 13 characters (ASCII string) or 26 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key. If you chose **256-bit WEP** in the **WEP Encryption** field, then enter 29 characters (ASCII string) or 58 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key. There are four data encryption keys to secure your data from eavesdropping by unauthorized wireless users. The values for the keys must be set up exactly the same on the access points as they are on the wireless client computers.
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Reset	Click **Reset** to begin configuring this screen afresh.

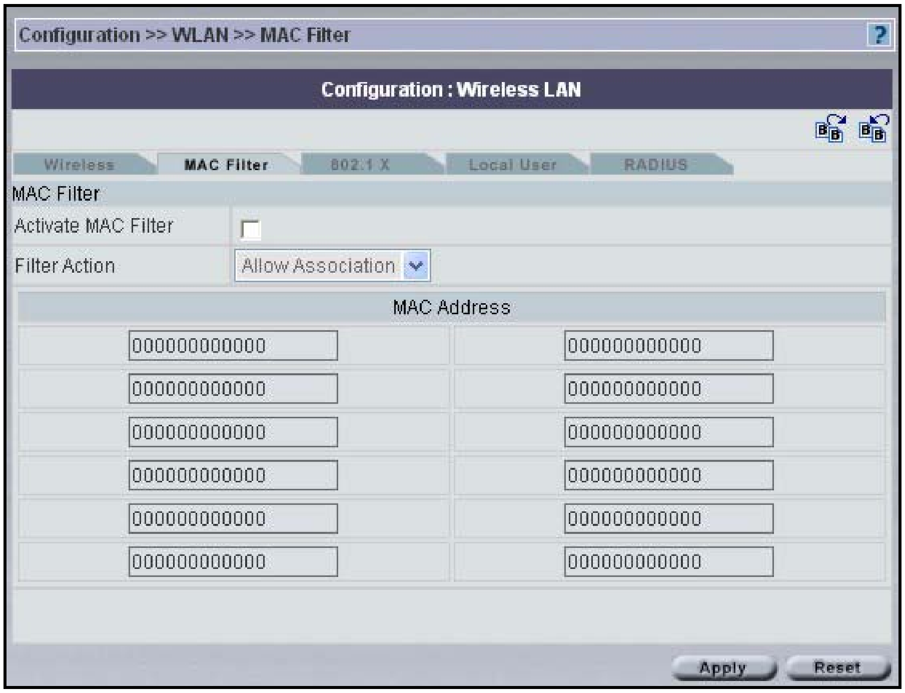
Note: If you are configuring the Prestige from a computer connected to the wireless LAN and you change the Prestige's ESSID or security settings (see Figure 46 on page 94), you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the Prestige's new settings.

6.4 Configuring MAC Filters

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of the devices to configure this screen. To change your Prestige's MAC filter settings, select a device and then click **Configuration > WLAN** > **MAC Filter**. The screen appears as shown.

Note: Be careful not to list your computer’s MAC address and set the **Action** field to **Deny Association** when managing the Prestige via a wireless connection. This would lock you out.

Figure 48 Configuration > WLAN > MAC Filter



Configuration >> WLAN >> MAC Filter

Configuration : Wireless LAN

MAC Filter

Activate MAC Filter □

Filter Action: Allow Association

MAC Address	
000000000000	000000000000
000000000000	000000000000
000000000000	000000000000
000000000000	000000000000
000000000000	000000000000
000000000000	000000000000

Table 22 Configuration > WLAN > MAC Filter

LABEL	DESCRIPTION
Active	Select **Yes** from the drop down list box to enable MAC address filtering.
Action	Define the filter action for the list of MAC addresses in the **MAC Address** table. Select **Deny Association** to block access to the router, MAC addresses not listed will be allowed to access the Prestige. Select **Allow Association** to permit access to the router, MAC addresses not listed will be denied access to the Prestige.
MAC Address	Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc of the wireless stations that are allowed or denied access to the Prestige in these address fields.
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Reset	Click **Reset** to begin configuring this screen afresh.

6.5 Introduction to WPA

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA is preferred to WEP as WPA has user authentication and improved data encryption. See the appendix for more information on WPA user authentication and WPA encryption.

If you don't have an external RADIUS server, you should use WPA-PSK (WPA -Pre-Shared Key). WPA-PSK only requires a single (identical) password entered into each WLAN member. As long as the passwords match, a client will be granted access to a WLAN.

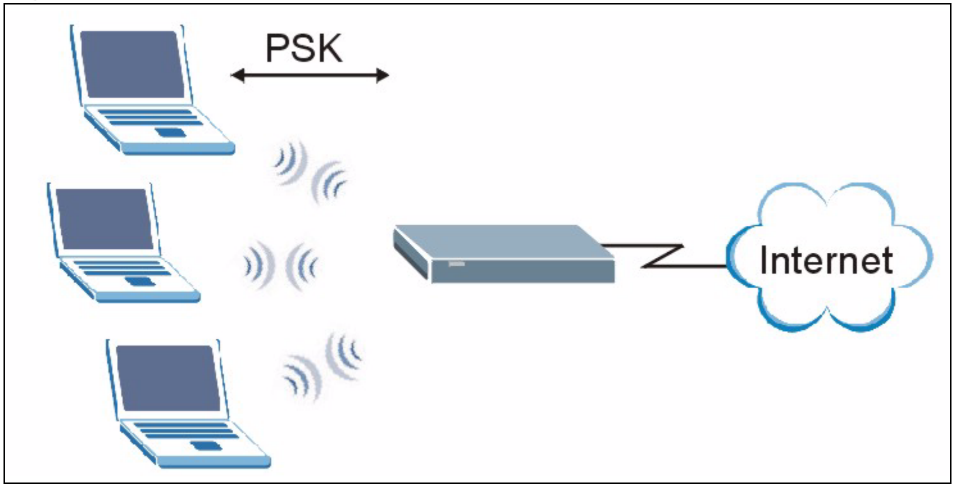
Note: You can't use the Local User Database for authentication when you select WPA.

6.5.1 WPA-PSK Application Example

A WPA-PSK application looks as follows.

1. First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must be between 8 and 63 printable characters (including spaces; alphabetic characters are case-sensitive).
2. The AP checks each client's password and (only) allows it to join the network if the passwords match.
3. The AP derives and distributes keys to the wireless clients.
4. The AP and wireless clients use the TKIP encryption process to encrypt data exchanged between them.

Figure 49 WPA - PSK Authentication



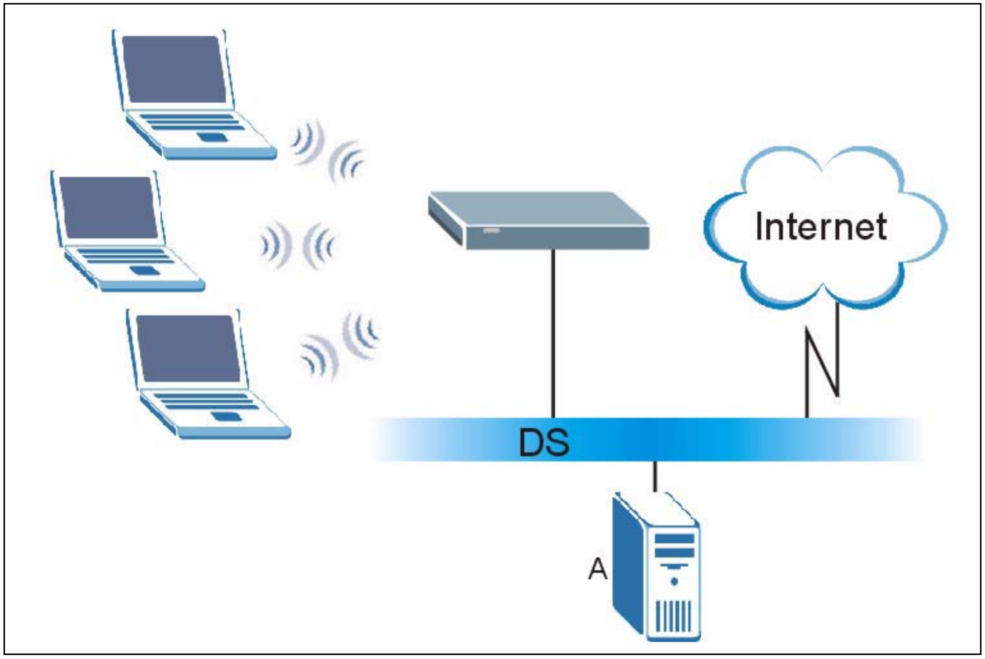
6.5.2 WPA with RADIUS Application Example

You need the IP address, port number (default is 1812) and shared secret of a RADIUS server. A WPA application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system (wired link to the LAN).

1. The AP passes the wireless client's authentication request to the RADIUS server.
2. The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.

3 The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly transmitted between the AP and the wireless clients

Figure 50 WPA with RADIUS Application Example 2



6.5.3 Wireless Client WPA Supplicants

A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicants are the WPA patch for Windows XP, Funk Software's Odyssey client, and Meetinghouse Data Communications' AEGIS client.

The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

6.6 Configuring IEEE 802.1x and WPA

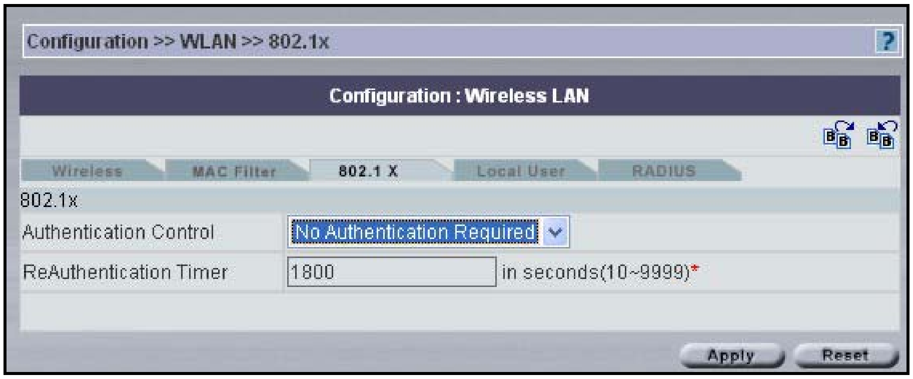
To change your Prestige's authentication settings, click the Wireless LAN link under Advanced Setup and then the 802.1x/WPA tab. The screen varies by the key management protocol you select.

You see the next screens when you select **No Access Allowed** or **No Authentication Required** in the **Wireless Port Control** field.

6.6.1 Configuring 802.1x - ZyWALL

Select a ZyWALL device and then click **Configuration > WLAN** > **802.1x**. The screen appears as shown next.

Figure 51 Configuration > WLAN > 802.1x - ZyWALL



802.1x

Authentication Control: No Authentication Required

ReAuthentication Timer: 1800 in seconds(10~9999)*

The following table describes the fields in this screen

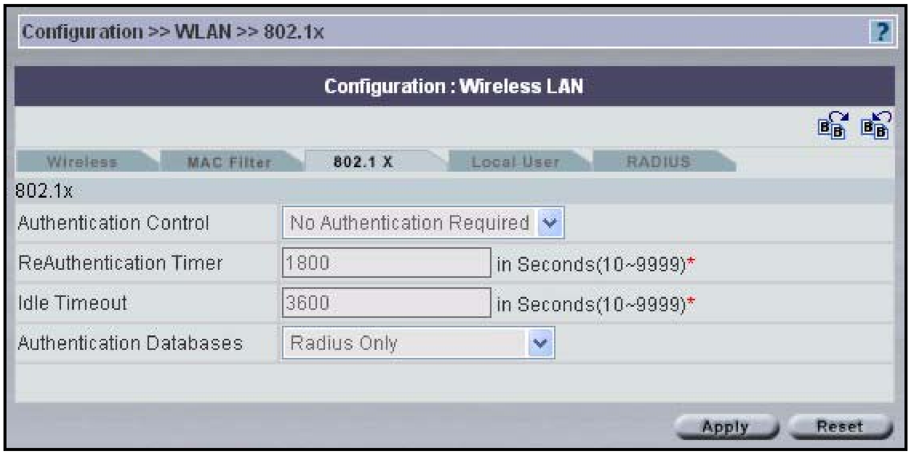
Table 23 Configuration > WLAN > 802.1x – ZyWALL

LABEL	DESCRIPTION
Authentication Control.	Select **Authentication Required** to authenticate all wireless clients before they can access the wired network. Select **No Authentication Required** to allow all wireless clients to access your wired network without authentication. Select **No Access** to deny all wireless clients access to your wired network
Reauthentication Timer	Specify the time interval between the RADIUS server’s authentication checks of wireless users connected to the network. This field is activated only when you select **Authentication Required** in the **Authentication Type** field.
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Reset	Click **Reset** to begin configuring this screen afresh.

6.6.2 Configuring 802.1x - Prestige

Select a Prestige device and then click **Configuration > WLAN** > **802.1x**. The screen appears as shown next.

Figure 52 Configuration > WLAN > 802.1x - Prestige



802.1x

Authentication Control	No Authentication Required
ReAuthentication Timer	1800 in Seconds(10~9999)*
Idle Timeout	3600 in Seconds(10~9999)*
Authentication Databases	Radius Only

The following table describes the fields in this screen

Table 24 Configuration > WLAN > 802.1x - Prestige

LABEL	DESCRIPTION
Authentication Control	Select **Authentication Required** to authenticate all wireless clients before they can access the wired network. Select **No Authentication Required** to allow all wireless clients to access your wired network without authentication. Select **No Access** to deny all wireless clients access to your wired network
Reauthentication Timer	Specify the time interval between the RADIUS server's authentication checks of wireless users connected to the network. This field is activated only when you select **Authentication Required** in the **Authentication Type** field.
Idle Timeout	The Prestige automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. The default time interval is **3600** seconds (or 1 hour).

Table 24 Configuration > WLAN > 802.1x - Prestige (continued)

LABEL	DESCRIPTION
Authentication Databases	The authentication database contains wireless station login information. The local user database is the built-in database on the Prestige. The RADIUS is an external server. Use this drop-down list box to select which database the Prestige should use (first) to authenticate a wireless station. Before you specify the priority, make sure you have set up the corresponding database correctly first. Select **Local User Database Only** to have the Prestige just check the built-in user database on the Prestige for a wireless station's username and password. Select **RADIUS Only** to have the Prestige just check the user database on the specified RADIUS server for a wireless station's username and password. Select **Local first, then RADIUS** to have the Prestige first check the user database on the Prestige for a wireless station's username and password. If the user name is not found, the Prestige then checks the user database on the specified RADIUS server. Select **RADIUS first, then Local** to have the Prestige first check the user database on the specified RADIUS server for a wireless station's username and password. If the Prestige cannot reach the RADIUS server, the Prestige then checks the local user database on the Prestige. When the user name is not found or password does not match in the RADIUS server, the Prestige will not check the local user database and the authentication fails.
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Reset	Click **Reset** to begin configuring this screen afresh.

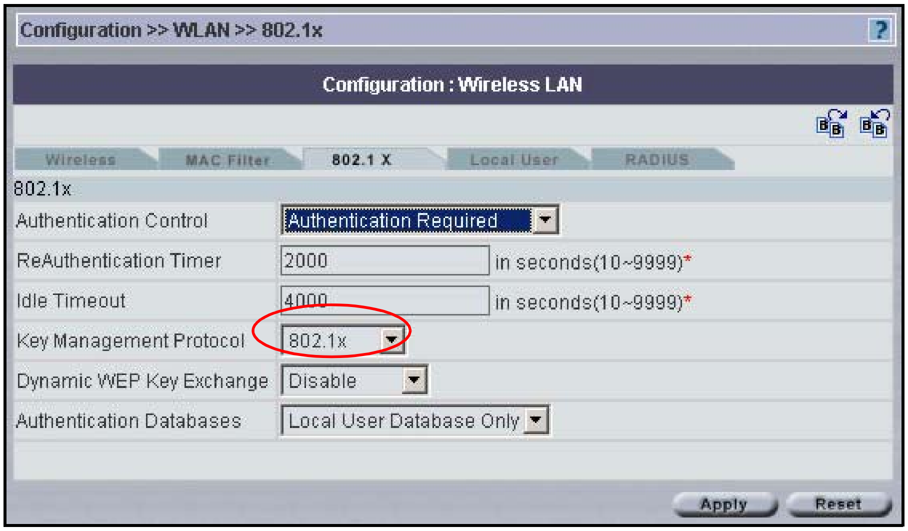
6.6.3 Authentication Required > 802.1x

You need the following for IEEE 802.1x authentication.

- A computer with an IEEE 802.11 a/b/g wireless LAN adapter and equipped with a web browser (with JavaScript enabled) and/or Telnet.
- A wireless station computer must be running IEEE 802.1x-compliant software. Not all Windows operating systems support IEEE 802.1x (see the Microsoft web site for details). For other operating systems, see their documentation. If your operating system does not support IEEE 802.1x, then you may need to install IEEE 802.1x client software.
- An optional network RADIUS server for remote user authentication and accounting.

Select **Authentication Required** in the **Authentication Control** field and **802.1x** in the **Key Management Protocol** field to display the next screen.

Figure 53 Wireless LAN > 802.1x/WPA > 802.1xl



Configuration >> WLAN >> 802.1x

Configuration : Wireless LAN

802.1x

Authentication Control	Authentication Required
ReAuthentication Timer	2000 in seconds(10~9999)*
Idle Timeout	4000 in seconds(10~9999)*
Key Management Protocol	802.1x
Dynamic WEP Key Exchange	Disable
Authentication Databases	Local User Database Only

The following table describes the labels in this screen.

Table 25 Wireless LAN > 802.1x/WPA > 802.1x

LABEL	DESCRIPTION
Authentication Control	To control wireless station access to the wired network, select a control method from the drop-down list box. Choose from **No Authentication Required**, **Authentication Required** and **No Access Allowed**. The following fields are only available when you select **Authentication Required**.
ReAuthentication Timer (in Seconds)	Specify how often wireless stations have to reenter usernames and passwords in order to stay connected. This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. Enter a time interval between 10 and 9999 seconds. The default time interval is **1800** seconds (30 minutes). **Note:** If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout (in Seconds)	The Prestige automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. The default time interval is **3600** seconds (or 1 hour).
Key Management Protocol	Choose **802.1x** from the drop-down list.

Table 25 Wireless LAN > 802.1x/WPA > 802.1x (continued)

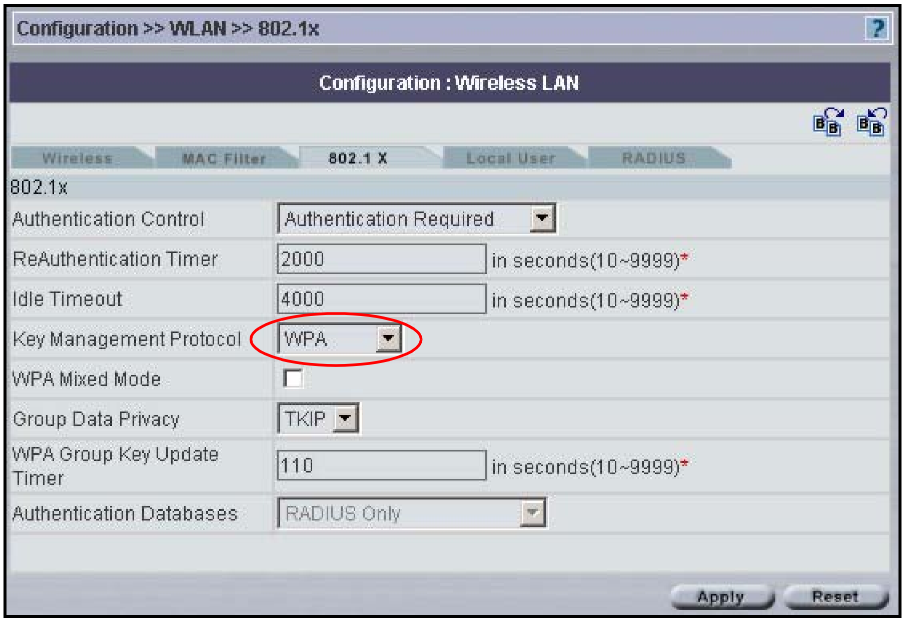
LABEL	DESCRIPTION
Dynamic WEP Key Exchange	This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. Also set the **Authentication Databases** field to **RADIUS Only**. Local user database may not be used. Select **Disable** to allow wireless stations to communicate with the access points without using dynamic WEP key exchange. Select **64-bit WEP**, **128-bit WEP** or **256-bit WEP** to enable data encryption. Up to 32 stations can access the Prestige when you configure dynamic WEP key exchange. This field is not available when you set **Key Management Protocol** to **WPA** or **WPA-PSK**.
Authentication Databases	The authentication database contains wireless station login information. The local user database is the built-in database on the Prestige. The RADIUS is an external server. Use this drop-down list box to select which database the Prestige should use (first) to authenticate a wireless station. Before you specify the priority, make sure you have set up the corresponding database correctly first. Select **Local User Database Only** to have the Prestige just check the built-in user database on the Prestige for a wireless station's username and password. Select **RADIUS Only** to have the Prestige just check the user database on the specified RADIUS server for a wireless station's username and password. Select **Local first, then RADIUS** to have the Prestige first check the user database on the Prestige for a wireless station's username and password. If the user name is not found, the Prestige then checks the user database on the specified RADIUS server. Select **RADIUS first, then Local** to have the Prestige first check the user database on the specified RADIUS server for a wireless station's username and password. If the Prestige cannot reach the RADIUS server, the Prestige then checks the local user database on the Prestige. When the user name is not found or password does not match in the RADIUS server, the Prestige will not check the local user database and the authentication fails.
Back	Click **Back** to go to the main wireless LAN setup screen.
Apply	Click **Apply** to save your changes back to the Prestige.
Cancel	Click **Cancel** to begin configuring this screen afresh.

Note: Once you enable user authentication, you need to specify an external RADIUS server or create local user accounts on the Prestige for authentication.

6.6.4 Authentication Required > WPA

Select **Authentication Required** in the **Authentication Control** field and **WPA** in the **Key Management Protocol** field to display the next screen.

Figure 54 Wireless LAN > 802.1x/WPA > WPAI



802.1x

Authentication Control	Authentication Required	
ReAuthentication Timer	2000	in seconds(10~9999)*
Idle Timeout	4000	in seconds(10~9999)*
Key Management Protocol	WPA	
WPA Mixed Mode	□	
Group Data Privacy	TKIP	
WPA Group Key Update Timer	110	in seconds(10~9999)*
Authentication Databases	RADIUS Only	

The following table describes the labels not previously discussed

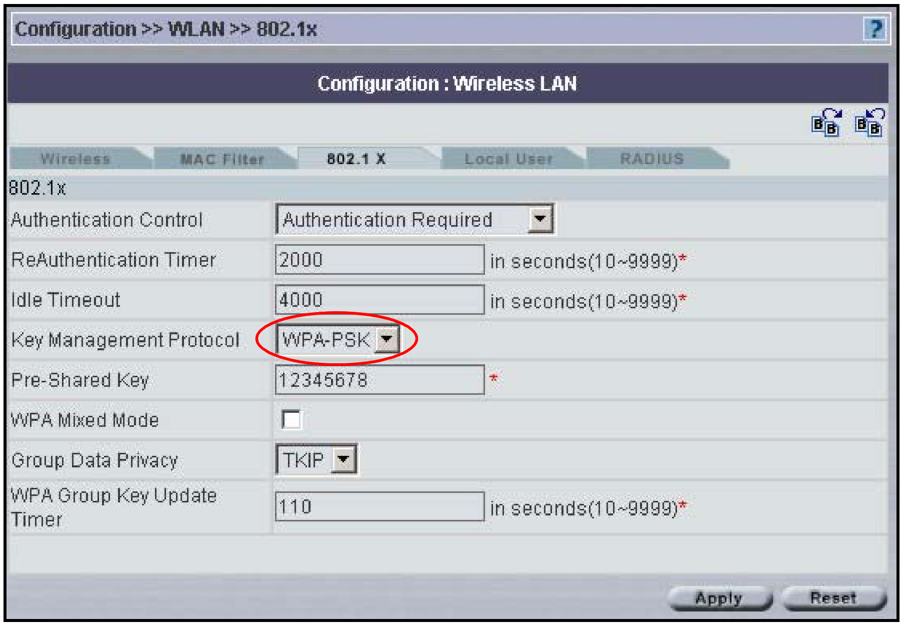
Table 26 Wireless LAN > 802.1x/WPA > WPA

	DESCRIPTION
Key Management Protocol	Choose **WPA** in this field.
WPA Mixed Mode	The Prestige can operate in **WPA Mixed Mode**, which supports both clients running WPA and clients running dynamic WEP key exchange with 802.1x in the same Wi-Fi network. Select the check box to activate WPA mixed mode. Otherwise, clear the check box and configure the **Group Data Privacy** field.
Group Data Privacy	**Group Data Privacy** allows you to choose **TKIP** (recommended) or **WEP** for broadcast and multicast ("group") traffic if the **Key Management Protocol** is **WPA** and **WPA Mixed Mode** is disabled. **WEP** is used automatically if you have enabled **WPA Mixed Mode**. All unicast traffic is automatically encrypted by **TKIP** when **WPA** or **WPA-PSK Key Management Protocol** is selected.
WPA Group Key Update Timer	The **WPA Group Key Update Timer** is the rate at which the AP (if using **WPA-PSK** key management) or RADIUS server (if using **WPA** key management) sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **WPA Group Key Update Timer** is also supported in WPA-PSK mode. The Prestige default is 1800 seconds (30 minutes).
Authentication Databases	When you configure **Key Management Protocol** to **WPA**, the **Authentication Databases** must be **RADIUS Only**. You can only use the **Local User Database Only** with **802.1x Key Management Protocol**.

6.6.5 Authentication Required > WPA-PSK

Select **Authentication Required** in the **Key Management Protocol** field and **WPA-PSK** in the **Key Management Protocol** field to display the next screen.

Figure 55 Wireless LAN > 802.1x/WPA > WPA-PSKl



802.1x

Authentication Control	Authentication Required	
ReAuthentication Timer	2000	in seconds(10~9999)*
Idle Timeout	4000	in seconds(10~9999)*
Key Management Protocol	WPA-PSK	
Pre-Shared Key	12345678	*
WPA Mixed Mode	□	
Group Data Privacy	TKIP	
WPA Group Key Update Timer	110	in seconds(10~9999)*

The following table describes the labels not previously discussed.

Table 27 Wireless LAN > 802.1x/WPA > WPA-PSK

	DESCRIPTION
Key Management Protocol	Choose **WPA-PSK** in this field.
Pre-Shared Key	The encryption mechanisms used for **WPA** and **WPA-PSK** are the same. The only difference between the two is that **WPA-PSK** uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 printable characters (including spaces; alphabetic characters are case-sensitive).
WPA Mixed Mode	The Prestige can operate in **WPA Mixed Mode**, which supports both clients running WPA and clients running dynamic WEP key exchange with 802.1x in the same Wi-Fi network. Select the check box to activate WPA mixed mode. Otherwise, clear the check box and configure the **Group Data Privacy** field.
Group Data Privacy	**Group Data Privacy** allows you to choose **TKIP** (recommended) or **WEP** for broadcast and multicast ("group") traffic if the **Key Management Protocol** is **WPA** and **WPA Mixed Mode** is disabled. **WEP** is used automatically if you have enabled **WPA Mixed Mode**. All unicast traffic is automatically encrypted by **TKIP** when **WPA** or **WPA-PSK Key Management Protocol** is selected.
Authentication Databases	This field is only visible when **WPA Mixed Mode** is enabled.

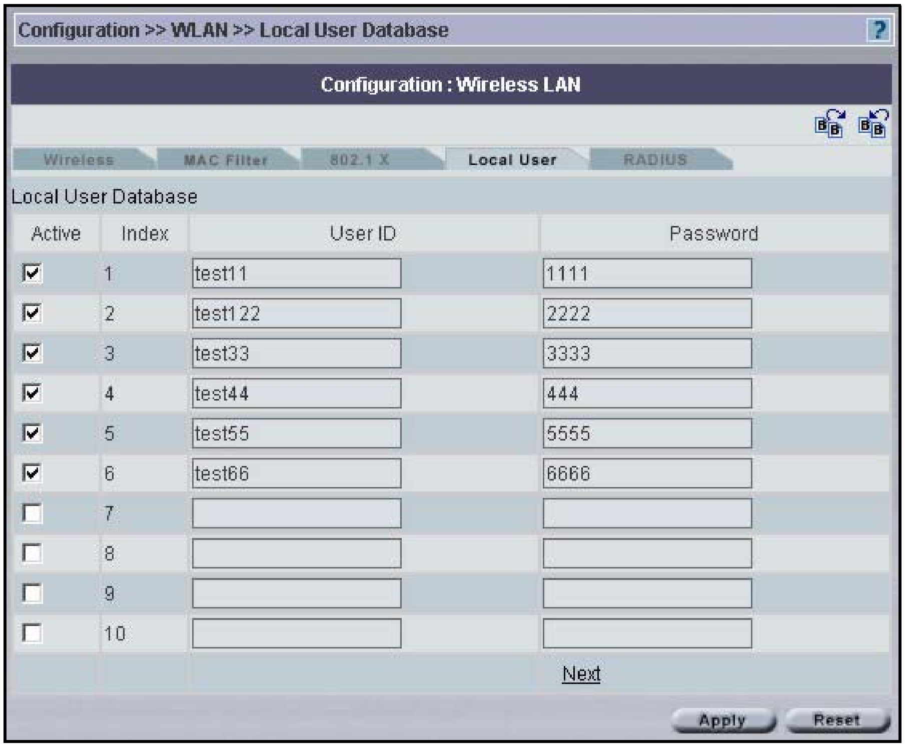
6.7 Configuring Local User Authentication

By storing user profiles locally, your Prestige is able to authenticate wireless users without interacting with a network RADIUS server. However, there is a limit on the number of users you may authenticate in this way.

6.7.1 Configuring Local User Database

Select a device and then click **Configuration > WLAN** > **Local User Database**. The screen appears as shown next.

Figure 56 Configuration > WLAN > Local User


Configuration >> WLAN >> Local User Database
?
Configuration : Wireless LAN
Wireless
MAC Filter
802.1 X
Local User
RADIUS
Next
Apply
Reset

Local User Database

Active	Index	User ID	Password
☑	1	test11	1111
☑	2	test122	2222
☑	3	test33	3333
☑	4	test44	444
☑	5	test55	5555
☑	6	test66	6666
□	7		
□	8		
□	9		
□	10		

The following table describes the labels in this screen.

Table 28 Configuration > WLAN > Local User

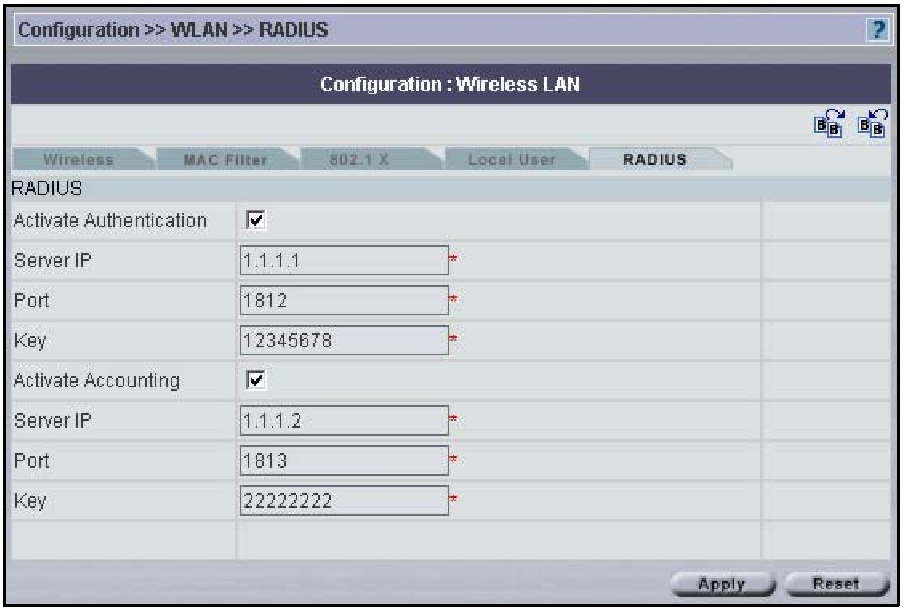
LABEL	DESCRIPTION
Active	Select this check box to enable the user profile.
Index	This is the local user index number.
User ID	Enter the user name of the user profile.
Password	Enter a password up to 31 characters long for this user profile.
Next	Select Next to view the next page of **Local User Database** entries.
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Reset	Click **Reset** to begin configuring this screen afresh.

6.8 Configuring RADIUS

Use the **RADIUS** screen if you want to use an external server to perform authentication.

Select a device, then click **Configuration > WLAN** > **RADIUS**. The screen appears as shown next.

Figure 57 Configuration > WLAN > RADIUS



RADIUS

Activate Authentication	☑
Server IP	1.1.1.1 *
Port	1812 *
Key	12345678 *
Activate Accounting	☑
Server IP	1.1.1.2 *
Port	1813 *
Key	22222222 *

The following table describes the fields in this screen

Table 29 Configuration > WLAN > RADIUS

LABEL	DESCRIPTION
Activate Authentication	Enable this feature to have the ZyXEL device use an external authentication server in performing user authentication. Disable this feature if you will not use an external authentication server. If you disable this feature, you can still set the ZyXEL device to perform user authentication using the local user database.
Server IP	Enter the IP address of the external authentication server in dotted decimal notation.
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 with additional information.
Key	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the access points. The key is not sent over the network. This key must be the same on the external authentication server and ZyXEL device.

Table 29 Configuration > WLAN > RADIUS (continued)

LABEL	DESCRIPTION
Activate Accounting	Enable this feature to do user accounting through an external authentication server.
Server IP	Enter the IP address of the external accounting server in dotted decimal notation.
Port	The default port of the RADIUS server for accounting is **1813**. You need not change this value unless your network administrator instructs you to do so with additional information.
Key	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the access points. The key is not sent over the network. This key must be the same on the external accounting server and ZyXEL device.
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Reset	Click **Reset** to begin configuring this screen afresh.

CHAPTER 7
Configuration > DMZ

7.1 DMZ Overview

The DeMilitarized Zone (DMZ) auto-negotiating 10/100 Mbps Ethernet port provides a way for public servers (Web, e-mail, FTP, etc.) to be visible to the outside world (while still being protected from DoS (Denial of Service) attacks such as SYN flooding and Ping of Death). These public servers can also still be accessed from the secure LAN.

By default the firewall allows traffic between the WAN and the DMZ, traffic from the DMZ to the LAN is denied, and traffic from the LAN to the DMZ is allowed. Internet users can have access to host servers on the DMZ but no access to the LAN, unless special filter rules allowing access were configured by the administrator or the user is an authorized remote user.

It is highly recommended that you connect all of your public servers to the DMZ port. If you have more than one public server, connect a hub to the DMZ port.

It is also highly recommended that you keep all sensitive information off of the public servers connected to the DMZ port. Store sensitive information on LAN computers.

7.2 DMZ Addresses

You can assign public or private IP addresses to computers connected to the DMZ port.

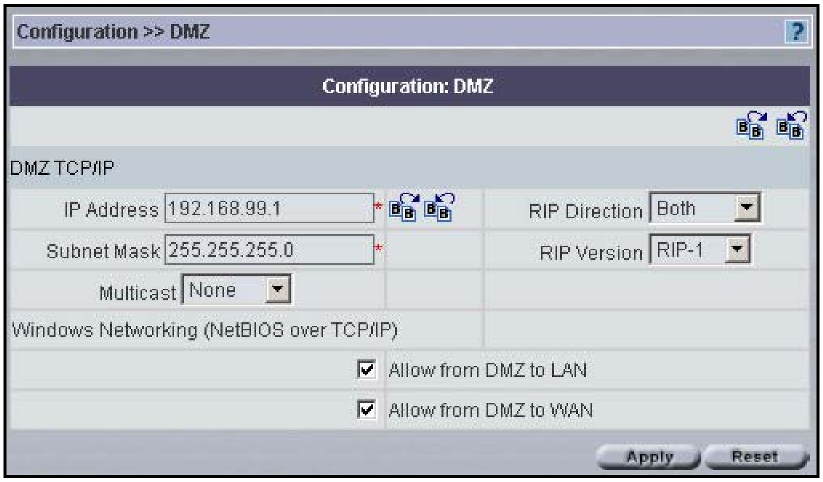
With public IP addresses, the WAN and DMZ ports must use public IP addresses that are on separate subnets. See the appendices for information on IP subnetting.

If the DMZ computers use private IP addresses, go to the **NAT** screen and select **SUA Only** or **Full Feature** in the **Network Address Translation** field. Configure NAT mapping rules for the private IP addresses of the computers on the DMZ.

7.3 Configuring DMZ

Select a ZyWALL device and from the **Configuration Screen**, click **DMZ**. The screen appears as shown next.

Figure 58 Configuration > DMZ



Configuration >> DMZ

Configuration: DMZ

DMZ TCP/IP

IP Address 192.168.99.1 *

Subnet Mask 255.255.255.0 *

Multicast None

RIP Direction Both

RIP Version RIP-1

Windows Networking (NetBIOS over TCP/IP)

☑ Allow from DMZ to LAN

☑ Allow from DMZ to WAN

The following table describes the labels in this screen.

Table 30 Configuration > DMZ

LABEL	DESCRIPTION
DMZ TCP/IP	
IP Address	Type the IP address of your ZyXEL device in dotted decimal notation 192.168.1.1 (factory default).
Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your ZyXEL device will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyXEL device 255.255.255.0.
RIP Direction	RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **Both**/**In Only**/**Out Only**/**None**. When set to **Both** or **Out Only**, the ZyXEL device will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received. Both is the default.
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyXEL device 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. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to **Both** and the Version set to **RIP-1**.
Multicast	Select **IGMP V-1** or **IGMP V-2** or **None**. IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about inter operability between IGMP version 2 and version 1, please see *sections 4 and 5 of RFC 2236*.

Table 30 Configuration > DMZ (continued)

LABEL	DESCRIPTION
Windows Networking (NetBIOS over TCP/IP)	
Allow from DMZ to LAN	Click this option to forward NetBIOS packets from the DMZ port to the LAN
Allow from DMZ to WAN	Click this option to forward NetBIOS packets from the DMZ port to the WAN port.
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Reset	Click **Reset** to refresh the current screen.

CHAPTER 8 Configuration > WAN

You will see different WAN screens depending on whether you're configuring a ZyWALL or Prestige device.

Note: Be careful when configuring a device's WAN as an incorrect configuration could result in the device being inaccessible from Vantage (or by the web configurator from the WAN) and may necessitate a site visit to correct.

8.1 WAN Overview

Use the **General** screen to configure route priority and traffic redirect properties.
Use the **WAN ISP** screen to configure the device's Internet access connection and service type.
Use the **WAN IP** screen to configure the WAN port for Internet access.
Use the **Traffic Redirect** screen to configure your traffic redirect properties and parameters.
Use the **Dial Backup** screen to configure the backup WAN dial-up connection.

The following screens relate to ZyWALL (ZyNOS 3.64):

Use the **WAN1** screen to configure the WAN1 port for Internet access.
Use the **WAN2** screen to configure the WAN2 port for Internet access.

8.2 Multiple WAN - ZyWALL (ZyNOS 3.64)

You can use a second connection for load sharing to increase overall network throughput or as a backup to enhance network reliability.

The ZyWALL has two WAN ports. You can connect one port to one ISP (or network) and connect the other to a second ISP (or network).

The ZyWALL can balance the load between the two WAN ports.

You can use policy routing to specify the WAN port that specific services go through. An ISP may give traffic from certain (more expensive) connections priority over the traffic from other accounts. You could route delay intolerant traffic (like voice over IP calls) through this kind of connection. Other traffic could be routed through a cheaper broadband Internet connection that does not provide priority service. If one WAN port's connection goes down, the ZyWALL can automatically send its traffic through the other WAN port.

The ZyWALL's NAT feature allows you to configure sets of rules for one WAN port and separate sets of rules for the other WAN port.

You can select through which WAN port you want to send out traffic from UPnP-enabled applications.

The ZyWALL's DDNS lets you select which WAN interface you want to use for each individual domain name. The DDNS high availability feature lets you have the ZyWALL use the other WAN interface for a domain name if the configured WAN interface's connection goes down.

When configuring a VPN rule, you have the option of selecting one of the ZyWALL's domain names in the **My Address** field.

8.3 TCP/IP Priority (Metric)

The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".

1 The metric sets the priority for the ZyWALL's routes to the Internet. Each route must have a unique metric.
2 The priorities of the WAN port routes must always be higher than the dial-backup and traffic redirect route priorities.

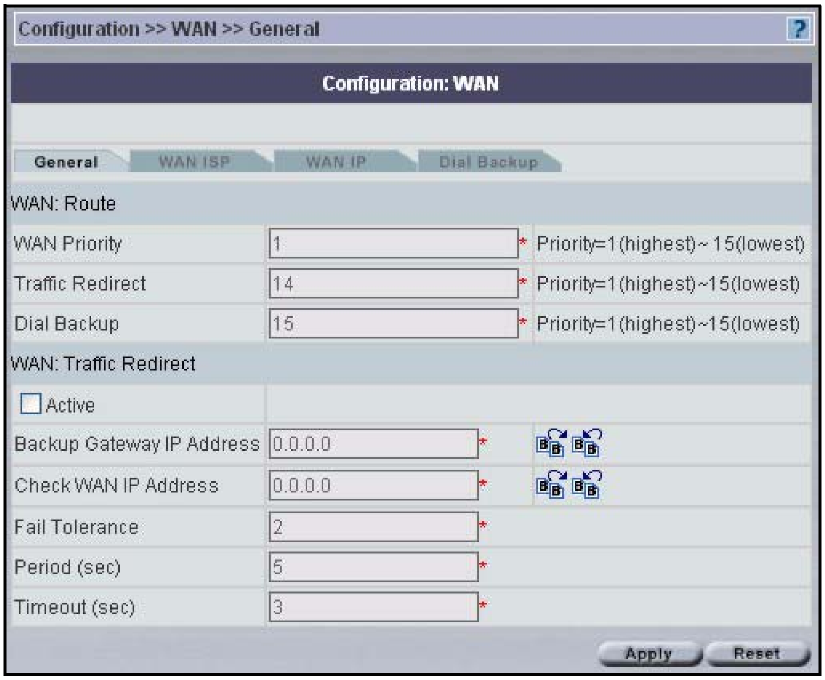
For example, lets say that you have the WAN operation mode set to active/passive and the WAN 1 route has a metric of "2", the WAN 2 route has a metric of "3", the traffic-redirect route has a metric of "14" and the dial-backup route has a metric of "15". In this case, the WAN 1 route acts as the primary default route. If the WAN 1 route fails to connect to the Internet, the ZyWALL tries the WAN 2 route next. If the WAN 2 route fails, the ZyWALL tries the traffic-redirect route. In the same manner, the ZyWALL uses the dial-backup route if the traffic-redirect route also fails.

The dial-backup or traffic redirect routes cannot take priority over the WAN 1 and WAN 2 routes.

8.4 General WAN - ZyWALL

This section gives background and configuration information on the fields displayed in this screen.

Figure 59 Configuration > WAN > General - ZyWALL



Configuration >> WAN >> General

Configuration: WAN

WAN: Route

WAN Priority	1 *	Priority=1(highest)~ 15(lowest)
Traffic Redirect	14 *	Priority=1(highest)~15(lowest)
Dial Backup	15 *	Priority=1(highest)~15(lowest)

WAN: Traffic Redirect

□ Active	
Backup Gateway IP Address	0.0.0.0 *
Check WAN IP Address	0.0.0.0 *
Fail Tolerance	2 *
Period (sec)	5 *
Timeout (sec)	3 *

The following table describes the fields in this screen

Table 31 Configuration > WAN > General - ZyWALL

LABEL	DESCRIPTION
WAN Traffic Redirect Dial Backup	The default WAN connection is "1' as your broadband connection via the WAN port should always be your preferred method of accessing the WAN. The default priority of the routes is **WAN**, **Traffic Redirect** and then **Dial Backup** (dial backup does not apply to all ZyXEL device models): You have two choices for an auxiliary connection in the event that your regular WAN connection goes down. If **Dial Backup** is preferred to **Traffic Redirect**, then type "14" in the **Dial Backup Priority (metric)** field (and leave the **Traffic Redirect Priority (metric)** at the default of "15").
Active	Select this check box to have the ZyXEL device use traffic redirect if the normal WAN connection goes down.
Backup Gateway IP Address	Type the IP address of your backup gateway in dotted decimal notation. The ZyXEL device automatically forwards traffic to this IP address if the ZyXEL device's Internet connection terminates.
Check WAN IP Address	Configuration of this field is optional. If you do not enter an IP address here, the ZyXEL device will use the default gateway IP address. Configure this field to test the ZyXEL device's WAN accessibility. Type the IP address of a reliable nearby computer (for example, your ISP's DNS server address). If you are using PPTP or PPPoE Encapsulation, type "0.0.0.0" to configure the ZyXEL device to check the PVC (Permanent Virtual Circuit) or PPTP tunnel.
Fail Tolerance	Type the number of times the ZyXEL device may attempt and fail to connect to the Internet before traffic is forwarded to the backup gateway.
Period (sec)	Type the number of seconds for the ZyXEL device to wait between checks to see if it can connect to the WAN IP address (**Check WAN IP Address** field) or default gateway. Allow more time if your destination IP address handles lots of traffic.

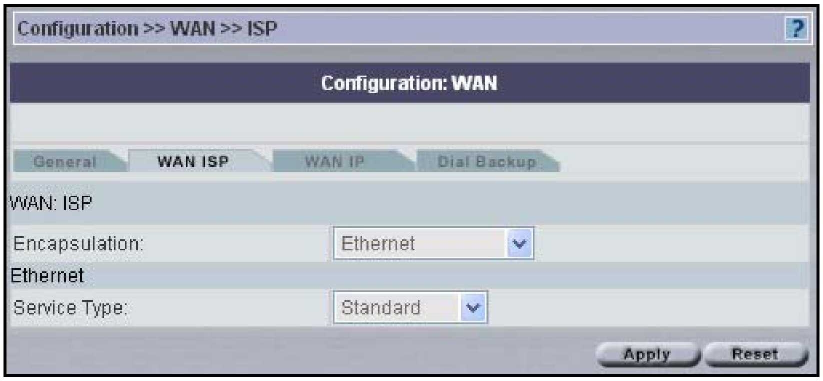
Table 31 Configuration > WAN > General - ZyWALL (continued)

LABEL	DESCRIPTION
Timeout (sec)	Type the number of seconds for the ZyXEL device to wait for a ping response from the IP Address in the **Check WAN IP Address** field before it times out. The WAN connection is considered "down" after the ZyXEL device times out the number of times specified in the **Fail Tolerance** field. Use a higher value in this field if your network is busy or congested.
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Reset	Click **Reset** to begin configuring this screen afresh.

8.4.1 WAN ISP - ZyWALL

The screen differs by the encapsulation type chosen.

Figure 60 Configuration > WAN > ISP (Ethernet) - ZyWALL



WAN: ISP

Encapsulation: Ethernet

Ethernet

Service Type: Standard

8.4.1.1 Ethernet Encapsulation

The following table describes the labels in the **Ethernet** encapsulation screen.

Table 32 Configuration > WAN > ISP (Ethernet) - ZyWALL

	DESCRIPTION
Encapsulation	You must choose the Ethernet option when the WAN port is used as a regular Ethernet.
Service Type	Choose from **Standard**, **Telstra** (RoadRunner Telstra authentication method), **RR-Manager** (Roadrunner Manager authentication method), **RR-Toshiba** (Roadrunner Toshiba authentication method) or **Telia Login**. The following fields do not appear with the **Standard** service type.
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Reset	Click **Reset** to begin configuring this screen afresh.

8.4.1.2 PPPoE Encapsulation

The ZyXEL device supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF Draft standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The **PPPoE** option is for a dial-up connection using PPPoE.

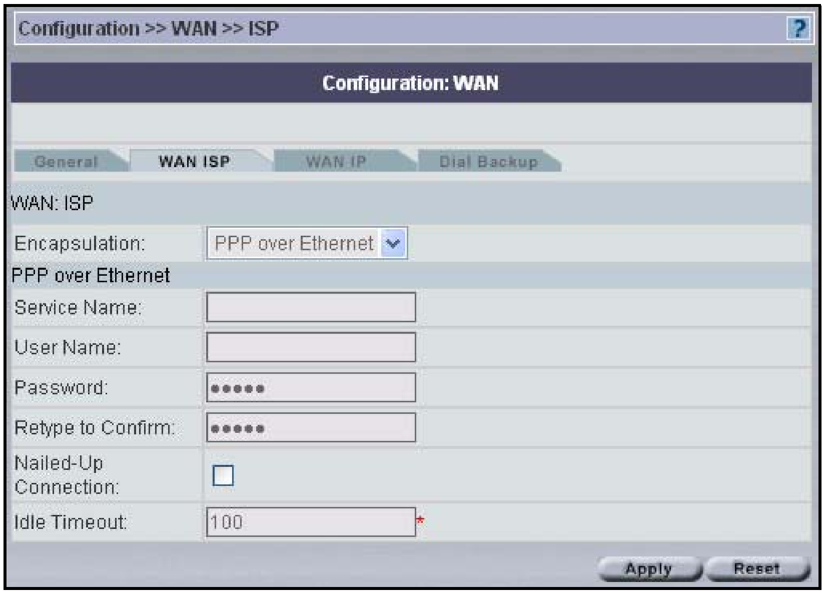
For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example Radius). PPPoE provides a login and authentication method that the existing Microsoft Dial-Up Networking software can activate, and therefore requires no new learning or procedures for Windows users.

One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the ZyXEL device (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the ZyXEL device does that part of the task. Furthermore, with NAT, all of the LANs’ computers will have access.

Figure 61 Configuration > WAN > ISP (PPPoE) - ZyWALL



WAN: ISP

Encapsulation: PPP over Ethernet

PPP over Ethernet

Service Name:

User Name:

Password: ●●●●●

Retype to Confirm: ●●●●●

Nailed-Up Connection: □

Idle Timeout: 100 *

The following table describes the labels in the **PPPoE** screen.

Table 33 Configuration > WAN > ISP (PPPoE) - ZyWALL

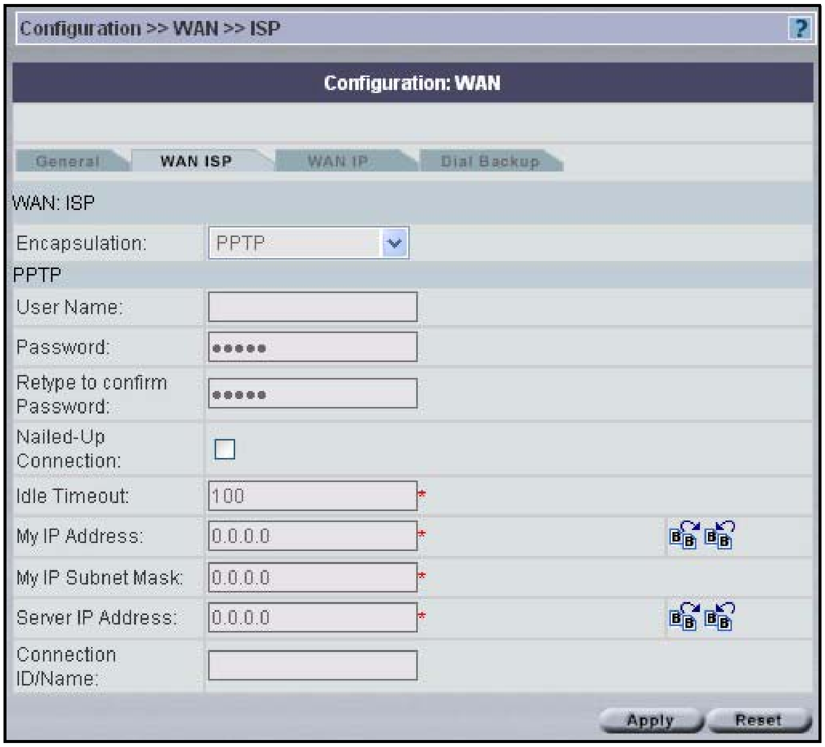
LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	The PPPoE choice is for a dial-up connection using PPPoE. The router supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF Draft standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (i.e. xDSL, cable, wireless, etc.) connection. Operationally, PPPoE saves significant effort for both the end user and ISP/carrier, as it requires no specific configuration of the broadband modem at the customer site. By implementing PPPoE directly on the router rather than individual computers, the computers on the LAN do not need PPPoE software installed, since the router does that part of the task. Further, with NAT, all of the LAN's computers will have access.
Service Name	Type the PPPoE service name provided to you. PPPoE uses a service name to identify and reach the PPPoE server.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.
Retype to Confirm	Type your password again to make sure that you have entered it correctly.
Nailed-Up Connection	Select **Nailed-Up Connection** if you do not want the connection to time out.
Idle Timeout	This value specifies the time in seconds that elapses before the router automatically disconnects from the PPPoE server.
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Reset	Click **Reset** to begin configuring this screen afresh.

8.4.1.3 PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.

PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet.

Figure 62 Configuration > WAN > ISP (PPTP) - ZyWALL



WAN: ISP

Encapsulation: PPTP

PPTP

User Name:

Password: ●●●●●

Retype to confirm Password: ●●●●●

Nailed-Up Connection: □

Idle Timeout: 100 *

My IP Address: 0.0.0.0 *

My IP Subnet Mask: 0.0.0.0 *

Server IP Address: 0.0.0.0 *

Connection ID/Name:

The following table describes the labels in the **PPTP** screen.

Table 34 Configuration > WAN > ISP (PPTP) - ZyWALL

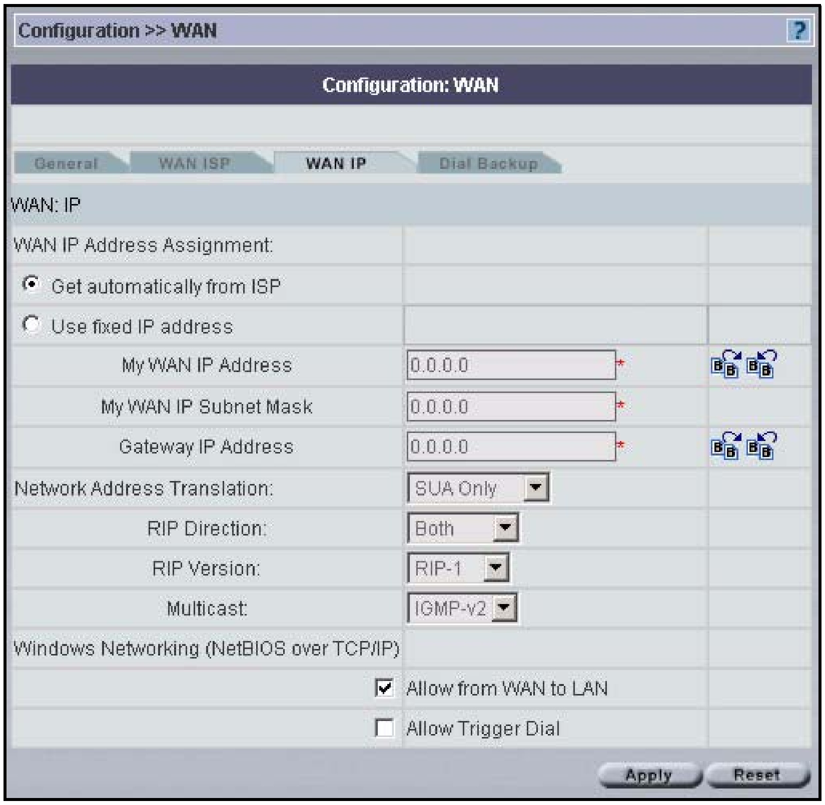
LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks. PPTP supports on-demand, multi-protocol, and virtual private networking over public networks, such as the Internet. The ZyXEL device supports only one PPTP server connection at any given time. To configure a PPTP client, you must configure the **User Name** and **Password** fields for a PPP connection and the PPTP parameters for a PPTP connection.
PPTP Configuration	
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.

Table 34 Configuration > WAN > ISP (PPTP) - ZyWALL (continued)

LABEL	DESCRIPTION
Retype to confirm Password	Type your password again to make sure that you have entered it correctly.
Nailed-up Connection	Select **Nailed-Up Connection** if you do not want the connection to time out.
Idle Timeout	This value specifies the time in seconds that elapses before the ZyXEL device automatically disconnects from the PPTP server.
My IP Address	Type the (static) IP address assigned to you by your ISP.
My IP Subnet Mask	The ZyXEL device will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyXEL device.
Server IP Address	Type the IP address of the PPTP server.
Connection ID/Name	Type your identification name for the PPTP server.
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Reset	Click **Reset** to begin configuring this screen afresh.

8.5 WAN IP - ZyWALL

Figure 63 Configuration > WAN > IP - ZyWALL



WAN: IP

WAN IP Address Assignment:

● Get automatically from ISP

○ Use fixed IP address

My WAN IP Address: 0.0.0.0 *

My WAN IP Subnet Mask: 0.0.0.0 *

Gateway IP Address: 0.0.0.0 *

Network Address Translation: SUA Only

RIP Direction: Both

RIP Version: RIP-1

Multicast: IGMP-v2

Windows Networking (NetBIOS over TCP/IP)

☑ Allow from WAN to LAN

□ Allow Trigger Dial

The following table describes the fields in this screen

Table 35 Configuration > WAN > IP - ZyWALL

LABEL	DESCRIPTION
WAN IP Address Assignment	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use fixed IP address	Select this option If the ISP assigned a fixed IP address.
My WAN IP Address	Enter your WAN IP address in this field if you selected **Use Fixed IP Address.**
My WAN IP Subnet Mask	Enter the IP subnet mask (if your ISP gave you one) in this field if you selected **Use Fixed IP Address**.
Gateway IP Address	Enter the gateway IP address (if your ISP gave you one) in this field if you selected **Use Fixed IP Address**.
Private	This parameter determines if the ZyWALL will include the route to this remote node in its RIP broadcasts. If set to Yes, this route is kept private and not included in RIP broadcast. If No, the route to this remote node will be propagated to other hosts through RIP broadcasts.

Table 35 Configuration > WAN > IP - ZyWALL (continued)

LABEL	DESCRIPTION
RIP Direction	RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Choose **Both**, **None**, **In Only** or **Out Only**. When set to **Both** or **Out Only**, the ZyXEL device will broadcast its routing table periodically. When set to **Both** or **In Only**, the ZyXEL device will incorporate RIP information that it receives. When set to **None**, the ZyXEL device will not send any RIP packets and will ignore any RIP packets received. By default, **RIP Direction** is set to **Both**.
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyXEL device sends (it recognizes both formats when receiving). Choose **RIP-1**, **RIP-2B** or **RIP-2M**. **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. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, the **RIP Version** field is set to **RIP-1**.
Multicast	Choose **None** (default), **IGMP-V1** or **IGMP-V2**. IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about inter operability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236.
Windows Networking (NetBIOS over TCP/IP): NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls.	
Allow from WAN to LAN	Select this option to forward NetBIOS packets from the WAN port to the LAN port.
Allow Trigger Dial	Select this option to allow NetBIOS packets to initiate calls.
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Reset	Click **Reset** to begin configuring this screen afresh.

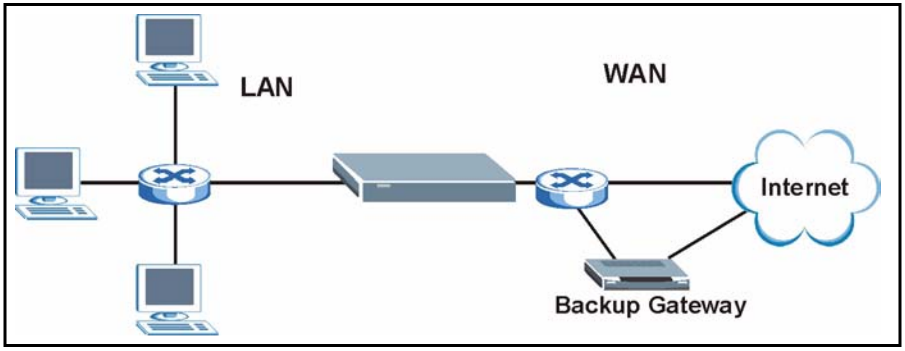
8.6 Dial Backup - ZyWALL

Vantage can communicate with the device using Dial Backup if the main WAN connection goes down.

8.6.1 Traffic Redirect

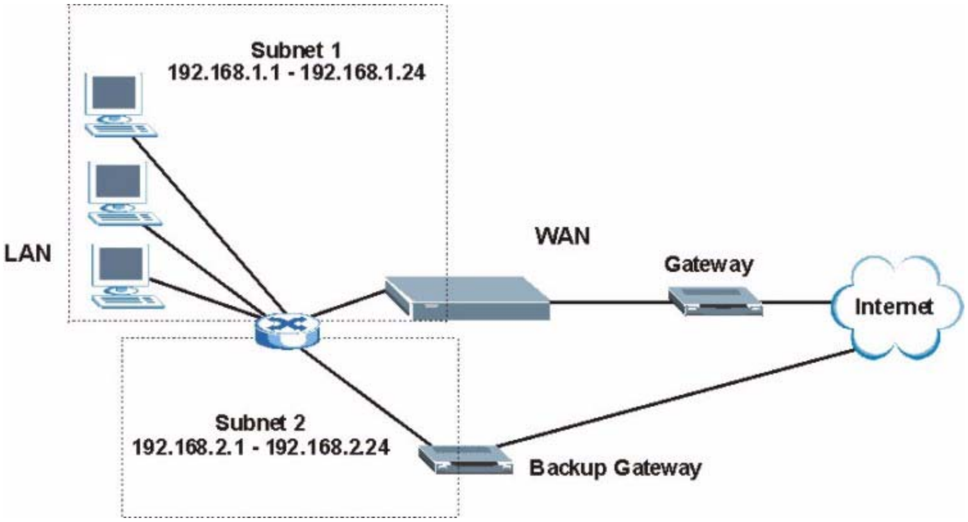
Traffic redirect forwards WAN traffic to a backup gateway when the ZyWALL cannot connect to the Internet through its normal gateway. Connect the backup gateway on the WAN so that the ZyWALL still provides firewall protection. This feature is not available on all models.

Figure 64 Traffic Redirect WAN Setup



The following network topology allows you to avoid triangle route security issues (see ZyWALL *Appendices*) when the backup gateway is connected to the LAN or DMZ. Use IP alias to configure the LAN into two or three logical networks with the ZyWALL itself as the gateway for each LAN network. Put the protected LAN in one subnet (Subnet 1 in the following figure) and the backup gateway in another subnet (Subnet 2). Configure a LAN to LAN/ZyWALL firewall rule that forwards packets from the protected LAN (Subnet 1) to the backup gateway (Subnet 2).

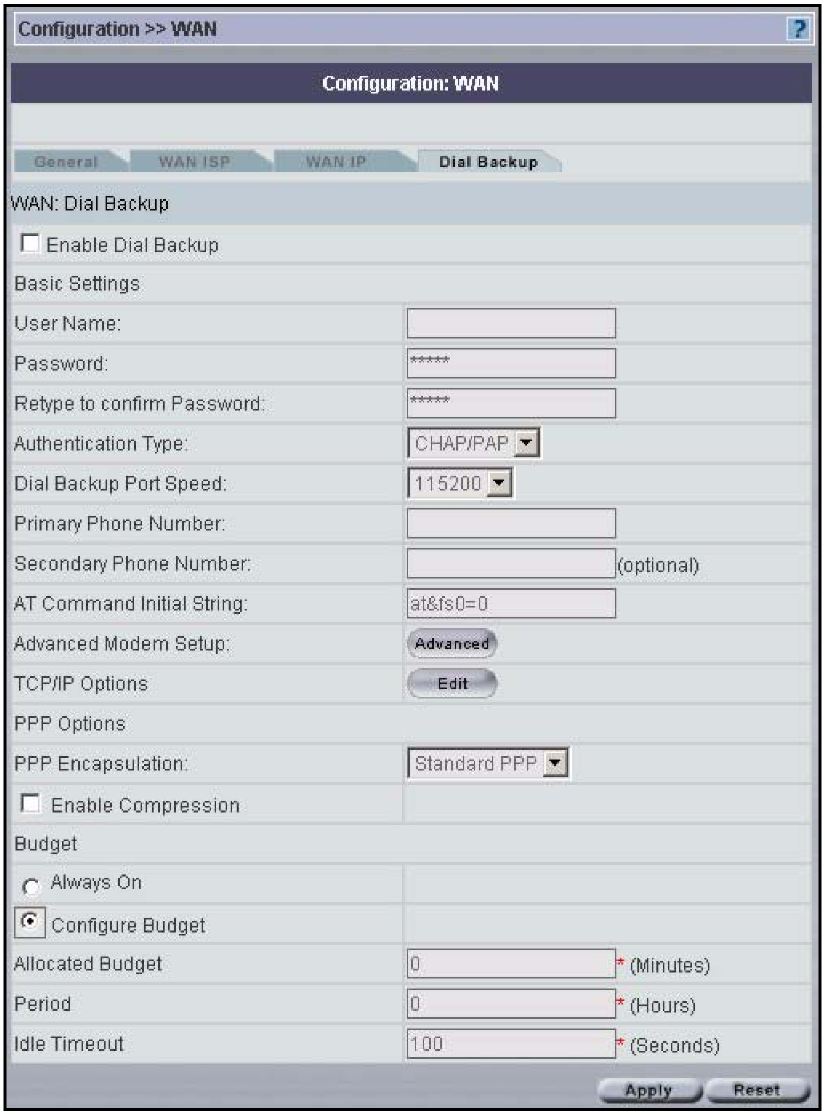
Figure 65 Traffic Redirect LAN Setup



8.6.2 Configuring Dial Backup - ZyWALL

Use the next menu to configure Dial Backup on the ZyWALL.

Figure 66 Configuration > WAN > Dial Backup - ZyWALL



WAN: Dial Backup

□ Enable Dial Backup

Basic Settings

User Name:	
Password:	*****
Retype to confirm Password:	*****
Authentication Type:	CHAP/PAP
Dial Backup Port Speed:	115200
Primary Phone Number:	
Secondary Phone Number:	(optional)
AT Command Initial String:	at&fs0=0
Advanced Modem Setup:	Advanced
TCP/IP Options	Edit
PPP Options	
PPP Encapsulation:	Standard PPP
□ Enable Compression	
Budget	
○ Always On	
● Configure Budget	
Allocated Budget	0 * (Minutes)
Period	0 * (Hours)
Idle Timeout	100 * (Seconds)

The following table describes the labels in this screen.

Table 36 Configuration > WAN > Dial Backup - ZyWALL

LABEL	DESCRIPTION
Enable Dial Backup	Select this check box to turn on dial backup.
Basic Settings	
User Name	Type the user name assigned by your ISP.
Password	Type the password assigned by your ISP.
Retype to confirm Password	Type your password again to make sure that you have entered it correctly.

Table 36 Configuration > WAN > Dial Backup - ZyWALL (continued)

LABEL	DESCRIPTION
Authentication Type	Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: **CHAP/PAP** - The ZyXEL device accepts either CHAP or PAP when requested by this remote node. **CHAP** - The ZyXEL device accepts CHAP only. **PAP** - The ZyXEL device accept PAP only.
Dial Backup Port Speed	Use the drop-down list box to select the speed of the connection between the Dial Backup port and the external device. Available speeds are: 9600, 19200, 38400, 57600, 115200 or 230400 bps.
Primary/ Secondary Phone Number	Type the first (primary) phone number from the ISP for this remote node. If the Primary Phone number is busy or does not answer, the ZyXEL device dials the Secondary Phone number if available. Some areas require dialing the pound sign # before the phone number for local calls. Include a # symbol at the beginning of the phone numbers as required.
AT Command Initial String	Type the AT command string to initialize the WAN device. Consult the manual of your WAN device connected to your Dial Backup port for specific AT commands.
Advanced Modem Setup	Click **Advanced** to display the **Advanced Modem Setup** screen and edit the details of your dial backup setup.
TCP/IP Options	Click **Edit** to display the **Dial Backup TCP/IP Options** screen.
PPP Options	
PPP Encapsulation	Select **CISCO PPP** from the drop-down list box if your dial backup WAN device uses Cisco PPP encapsulation, otherwise select **Standard PPP**.
Enable Compression	Select this check box to turn on stac compression.
Budget	
Always On	Select this check box to have the dial backup connection on all of the time.
Configure Budget	Select this check box to have the dial backup connection on during the time that you select.
Allocated Budget	Type the amount of time (in minutes) that the dial backup connection can be used during the time configured in the **Period** field. Set an amount that is less than the time period configured in the **Period** field.
Period	Type the time period (in hours) for how often the budget should be reset. For example, to allow calls to this remote node for a maximum of 10 minutes every hour, set the **Allocated Budget** to 10 (minutes) and the **Period** to 1 (hour).
Idle Timeout	Type the number of seconds of idle time (when there is no traffic from the ZyXEL device to the remote node) for the ZyXEL device to wait before it automatically disconnects the dial backup connection. This option applies only when the ZyXEL device initiates the call. The dial backup connection never times out if you set this field to "0" (it is the same as selecting **Always On**).
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Reset	Click **Reset** to begin configuring this screen afresh.

8.6.3 Advanced Modem Setup - ZyWALL

8.6.3.1 AT Command Strings

For regular telephone lines, the default Dial string tells the modem that the line uses tone dialing. `ATDT` is the command for a switch that requires tone dialing. If your switch requires pulse dialing, change the string to `ATDP`.

For ISDN lines, there are many more protocols and operational modes. Please consult the documentation of your TA. You may need additional commands in both Dial and Init strings.

8.6.3.1.1 DTR Signal

The majority of WAN devices default to hanging up the current call when the DTR (Data Terminal Ready) signal is dropped by the DTE. When the Drop DTR When Hang Up check box is selected, the ZyXEL device uses this hardware signal to force the WAN device to hang up, in addition to issuing the drop command `ATH`.

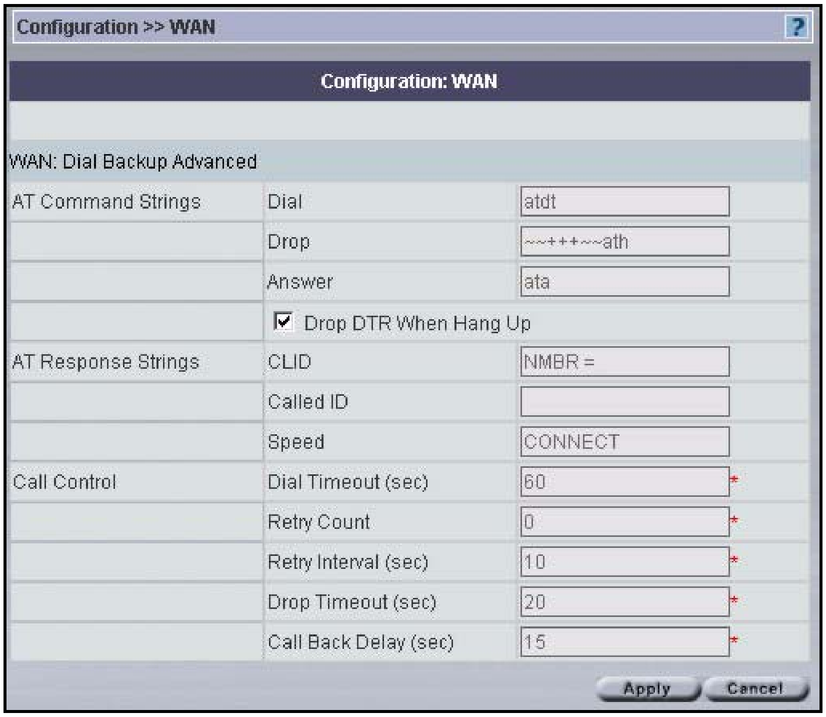
8.6.3.1.2 Response Strings

The response strings tell the ZyXEL device the tags, or labels, immediately preceding the various call parameters sent from the WAN device. The response strings have not been standardized; please consult the documentation of your WAN device to find the correct tags.

Click the **Advanced** button in the **Advanced Modem Setup** in the **Dial Backup** screen to display the **Dial Backup Advanced** screen shown next.

Note: Consult the manual of your WAN device connected to your dial backup port for specific AT commands.

Figure 67 Configuration > WAN > Dial Backup > Advanced - ZyWALL



Configuration >> WAN

Configuration: WAN

WAN: Dial Backup Advanced

AT Command Strings	Dial	atdt
	Drop	~~+++~~ath
	Answer	ata
	☑ Drop DTR When Hang Up	
AT Response Strings	CLID	NMBR =
	Called ID	
	Speed	CONNECT
Call Control	Dial Timeout (sec)	60 *
	Retry Count	0 *
	Retry Interval (sec)	10 *
	Drop Timeout (sec)	20 *
	Call Back Delay (sec)	15 *

The following table describes the labels in this screen.

Table 37 Configuration > WAN > Dial Backup > Advanced - ZyWALL

LABEL	DESCRIPTION	EXAMPLE
AT Command Strings		
Dial	Type the AT Command string to make a call.	atdt
Drop	Type the AT Command string to drop a call. "~" represents a one second wait, for example, "~~~+++~~ath" can be used if your modem has a slow response time.	~~+++~~ath
Answer	Type the AT Command string to answer a call.	ata
Drop DTR When Hang Up	Select this check box to have the ZyXEL device drop the DTR (Data Terminal Ready) signal after the "AT Command String: Drop" is sent out.	
AT Response Strings		
CLID	Type the keyword that precedes the CLID (Calling Line Identification) in the AT response string. This lets the ZyXEL device capture the CLID in the AT response string that comes from the WAN device. CLID is required for CLID authentication.	NMBR
Called ID	Type the keyword preceding the dialed number.	
Speed	Type the keyword preceding the connection speed.	CONNECT
Call Control		
Dial Timeout (sec)	Type a number of seconds for the ZyXEL device to try to set up an outgoing call before timing out (stopping).	60

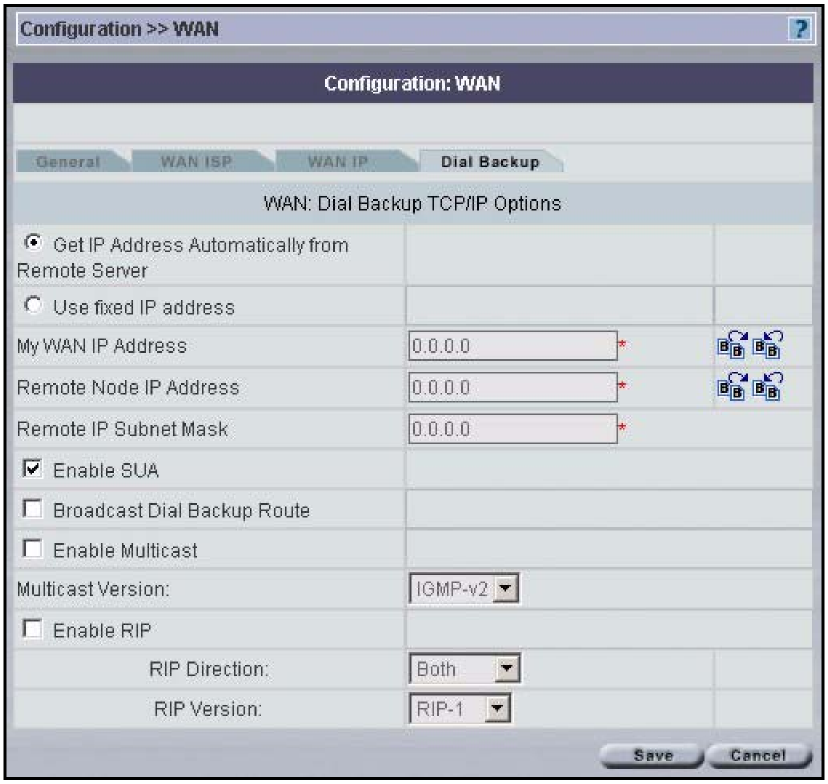
Table 37 Configuration > WAN > Dial Backup > Advanced - ZyWALL (continued)

LABEL	DESCRIPTION	EXAMPLE
Retry Count	Type a number of times for the ZyXEL device to retry a busy or no-answer phone number before blacklisting the number.	0
Retry Interval (sec)	Type a number of seconds for the ZyXEL device to wait before trying another call after a call has failed. This applies before a phone number is blacklisted.	10
Drop Timeout (sec)	Type the number of seconds for the ZyXEL device to wait before dropping the DTR signal if it does not receive a positive disconnect confirmation.	20
Call Back Delay (sec)	Type a number of seconds for the ZyXEL device to wait between dropping a callback request call and dialing the corresponding callback call.	15
Apply	Click **Apply** to save your changes back to the ZyXEL device.	
Cancel	Click **Cancel** to begin configuring this screen afresh.	

8.6.4 Edit Dial Backup - ZyWALL

Click **Edit** in the **TCP/IP** field in the screen shown in Figure 66 on page 125 to display the next screen.

Figure 68 Configuration > WAN > Dial Backup > Edit - ZyWALL



Configuration >> WAN

Configuration: WAN

WAN: Dial Backup TCP/IP Options

● Get IP Address Automatically from Remote Server	
○ Use fixed IP address	
My WAN IP Address	0.0.0.0 *
Remote Node IP Address	0.0.0.0 *
Remote IP Subnet Mask	0.0.0.0 *
☑ Enable SUA	
□ Broadcast Dial Backup Route	
□ Enable Multicast	
Multicast Version:	IGMP-v2
□ Enable RIP	
RIP Direction:	Both
RIP Version:	RIP-1

The following table describes the fields in this screen

Table 38 Configuration > WAN > Dial Backup > Edit - ZyWALL

LABEL	DESCRIPTION
Get IP Address Automatically from Remote Server	Type the login name assigned by your ISP for this remote node.
Used Fixed IP Address	Select this check box if your ISP assigned you a fixed IP address, and then enter the IP address in the following field.
My WAN IP Address	Leave the field set to 0.0.0.0 (default) to have the ISP or other remote router dynamically (automatically) assign your WAN IP address if you do not know it. Type your WAN IP address here if you know it (static). This is the address assigned to your local ZyXEL device, not the remote router.
Remote Node IP Address	Leave this field set to 0.0.0.0 (default) to have the ISP or other remote router dynamically (automatically) send its IP address if you do not know it. Type the remote gateway's IP address here if you know it (static).
Remote IP Subnet Mask	Leave this field set to 0.0.0.0 (default) to have the ISP or other remote router dynamically send its subnet mask if you do not know it. Type the remote gateway's subnet mask here if you know it (static).

Table 38 Configuration > WAN > Dial Backup > Edit - ZyWALL (continued)

LABEL	DESCRIPTION
Enable SUA	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network to a different IP address known within another network. **SUA** (Single User Account) is a subset of NAT that supports two types of mapping: Many-to-One and Server. When you select this option the ZyXEL device will use Address Mapping Set 255 in the SMT (see the section on menu 15.1 for more information). Select the check box to enable SUA. Clear the check box to disable SUA so the ZyXEL device does not perform any NAT mapping for the dial backup connection.
Broadcast Dial Backup Route	Select this check box to forward the backup route broadcasts to the WAN.
Enable Multicast	Select this check box to turn on IGMP (Internet Group Multicast Protocol). IGMP is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data.
Multicast Version	Select **IGMP-v1** or **IGMP-v2**. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about inter operability between IGMP version 2 and version 1, please see *sections 4* and *5* of *RFC 2236*.
Enable RIP	Select this check box to turn on RIP (Routing Information Protocol), which allows a router to exchange routing information with other routers.
RIP Direction	RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **Both**/**In Only**/**Out Only**/**None**. When set to **Both** or **Out Only**, the ZyXEL device broadcasts its routing table periodically. When set to **Both** or **In Only**, it incorporates the RIP information that it receives; when set to **None**, it does not send any RIP packets and ignores any RIP packets received. **Both** is the default.
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyXEL device 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. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to **Both** and the **Version** set to **RIP-1**.
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Reset	Click **Reset** to begin configuring this screen afresh.

8.7 General WAN - Prestige

This section gives background and configuration information on the fields displayed in this screen.

8.7.1 Traffic Shaping

Traffic Shaping is an agreement between the carrier and the subscriber to regulate the average rate and fluctuations of data transmission over an ATM network. This agreement helps eliminate congestion, which is important for transmission of real time data such as audio and video connections.

Peak Cell Rate (PCR) is the maximum rate at which the sender can send cells. This parameter may be lower (but not higher) than the maximum line speed. 1 ATM cell is 53 bytes (424 bits), so a maximum speed of 832Kbps gives a maximum PCR of 1962 cells/sec. This rate is not guaranteed because it is dependent on the line speed.

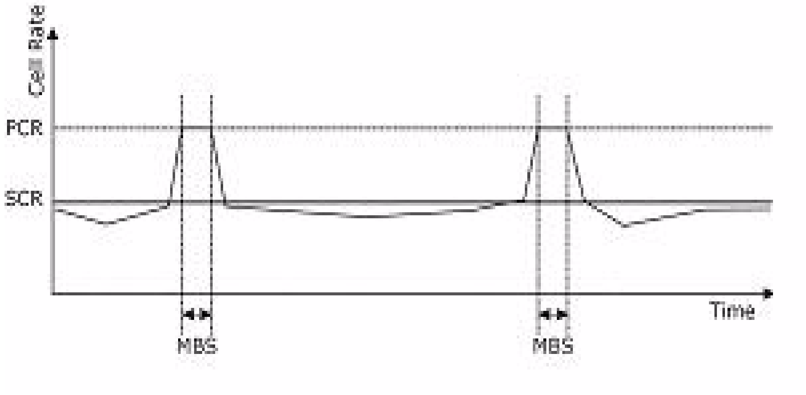
Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

Maximum Burst Size (MBS) is the maximum number of cells that can be sent at the PCR. After MBS is reached, cell rates fall below SCR until cell rate averages to the SCR again. At this time, more cells (up to the MBS) can be sent at the PCR again.

Note: If the PCR, SCR or MBS is set to the default of 0, the system will assign a maximum value that correlates to your upstream line rate.

The following figure illustrates the relationship between PCR, SCR and MBS.

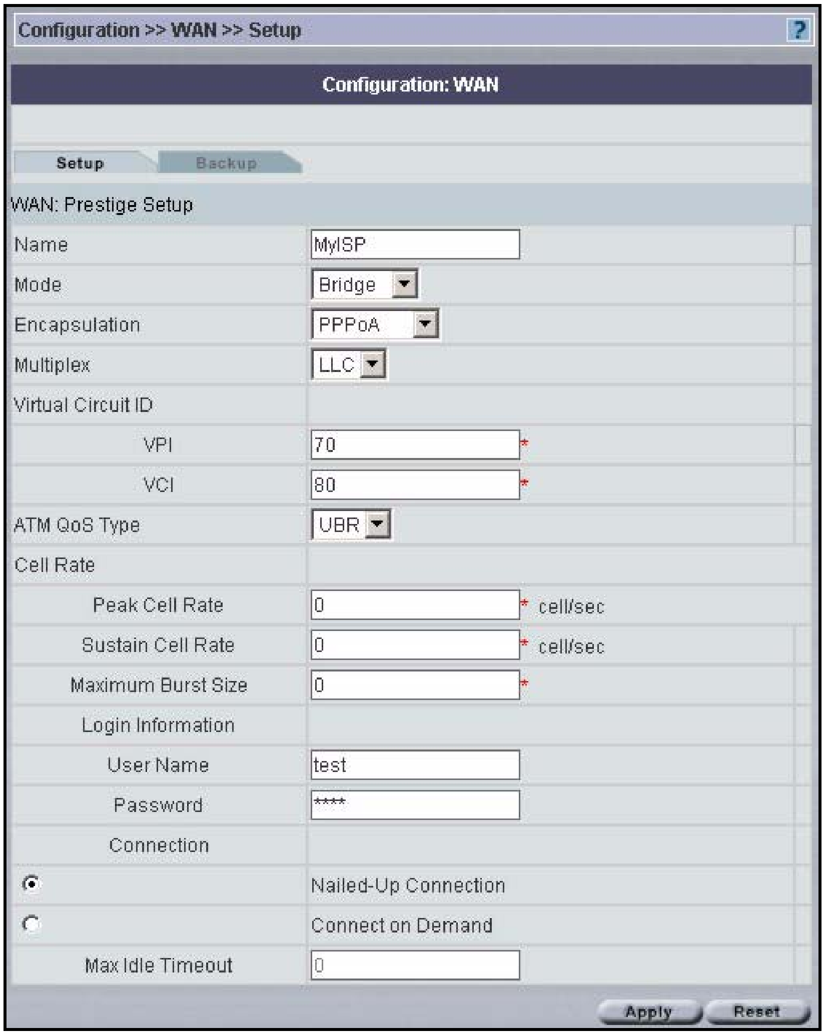
Figure 69 Example of Traffic Shaping



8.7.2 Configuring Prestige WAN Setup

Select a Prestige device in the object tree and then select **Configuration > WAN.**

Figure 70 Configuration > WAN > Setup - Prestige - Bridge Mode



WAN: Prestige Setup

Name	MyISP
Mode	Bridge
Encapsulation	PPPoA
Multiplex	LLC
Virtual Circuit ID	
VPI	70 *
VCI	80 *
ATM QoS Type	UBR
Cell Rate	
Peak Cell Rate	0 * cell/sec
Sustain Cell Rate	0 * cell/sec
Maximum Burst Size	0 *
Login Information	
User Name	test
Password	****
Connection	
●	Nailed-Up Connection
○	Connect on Demand
Max Idle Timeout	0

The following table describes the fields in this screen

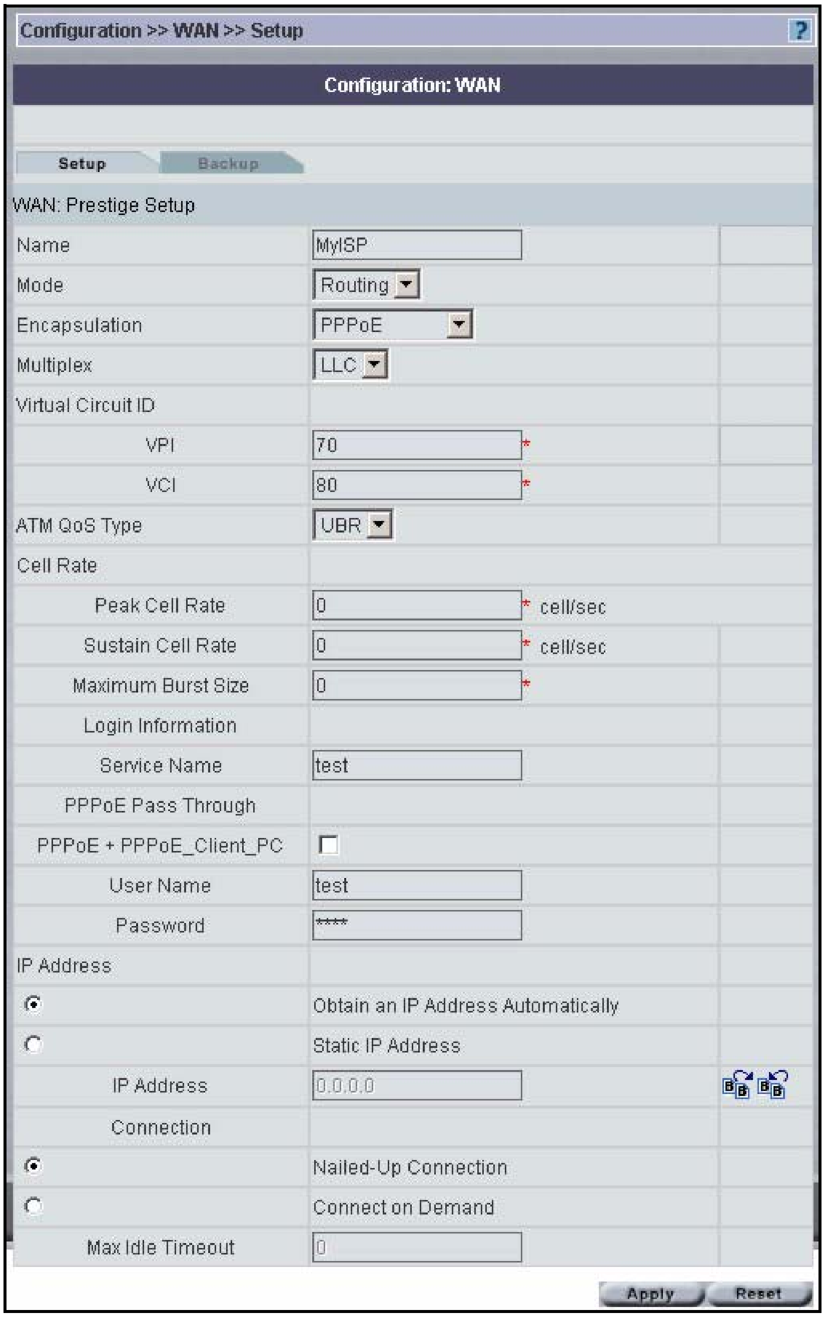
Table 39 Configuration > WAN > Setup - Prestige - Bridge Mode

LABEL	DESCRIPTION
Name	Enter the name of your Internet Service Provider, e.g., MyISP. This information is for identification purposes only.
Mode	Select **Routing** (default) from the drop-down list box if your ISP allows multiple computers to share an Internet account. Otherwise select **Bridge**.
Encapsulation	Select the method of encapsulation used by your ISP from the drop-down list box. Choices vary depending on the mode you select in the **Mode** field. If you select **Bridge** in the **Mode** field, select either **PPPoA** or **RFC 1483**. If you select **Routing** in the **Mode** field, select **PPPoA**, **RFC 1483**, **ENET ENCAP** or **PPPoE**.
Multiplex	Select the method of multiplexing used by your ISP from the drop-down list. Choices are **VC** or **LLC**.
Virtual Circuit ID	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. Refer to the appendix for more information.

Table 39 Configuration > WAN > Setup - Prestige - Bridge Mode (continued)

LABEL	DESCRIPTION
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
ATM QoS Type	Select **CBR** (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select **UBR** (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select **VBR** (Variable Bit Rate) for bursty traffic and bandwidth sharing with other applications.
Cell Rate	Cell rate configuration often helps eliminate traffic congestion that slows transmission of real time data such as audio and video connections.
Peak Cell Rate	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.
Sustain Cell Rate	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec.
Maximum Burst Size	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.
Login Information	(PPPoA and PPPoE encapsulation only)
User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	Enter the password associated with the user name above.
Connection (PPPoA and PPPoE encapsulation only)	The schedule rule(s) in the Prestige SMT menu 26 have priority over your **Connection** settings.
Nailed-Up Connection	Select **Nailed-Up Connection** when you want your connection up all the time. The Prestige will try to bring up the connection automatically if it is disconnected.
Connect on Demand	Select **Connect on Demand** when you don't want the connection up all the time and specify an idle time-out in the **Max Idle Timeout** field.
Max Idle Timeout	Specify an idle time-out in the **Max Idle Timeout** field when you select **Connect on Demand**. The default setting is 0, which means the Internet session will not timeout.
Apply	Click **Apply** to save the changes.
Reset	Click **Reset** to begin configuring this screen afresh.

Figure 71 Configuration > WAN > Setup - Prestige - Routing Mode



Configuration >> WAN >> Setup

Configuration: WAN

WAN: Prestige Setup

Name	MyISP
Mode	Routing
Encapsulation	PPPoE
Multiplex	LLC
Virtual Circuit ID	
VPI	70 *
VCI	80 *
ATM QoS Type	UBR
Cell Rate	
Peak Cell Rate	0 * cell/sec
Sustain Cell Rate	0 * cell/sec
Maximum Burst Size	0 *
Login Information	
Service Name	test
PPPoE Pass Through	
PPPoE + PPPoE_Client_PC	☐
User Name	test
Password	****
IP Address	
●	Obtain an IP Address Automatically
○	Static IP Address
IP Address	0.0.0.0
Connection	
●	Nailed-Up Connection
○	Connect on Demand
Max Idle Timeout	0

The following table describes the fields in this screen.

Table 40 Configuration > WAN > Setup - Prestige - Routing Mode

LABEL	DESCRIPTION
Name	Enter the name of your Internet Service Provider, e.g., MyISP. This information is for identification purposes only.
Mode	Select **Routing** (default) from the drop-down list box if your ISP allows multiple computers to share an Internet account. Otherwise select **Bridge**.

Table 40 Configuration > WAN > Setup - Prestige - Routing Mode (continued)

LABEL	DESCRIPTION
Encapsulation	Select the method of encapsulation used by your ISP from the drop-down list box. Choices vary depending on the mode you select in the **Mode** field. If you select **Bridge** in the **Mode** field, select either **PPPoA** or **RFC 1483**. If you select **Routing** in the **Mode** field, select **PPPoA**, **RFC 1483**, **ENET ENCAP** or **PPPoE**.
Multiplex	Select the method of multiplexing used by your ISP from the drop-down list. Choices are **VC** or **LLC**.
Virtual Circuit ID	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. Refer to the appendix for more information.
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
ATM QoS Type	Select **CBR** (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select **UBR** (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select **VBR** (Variable Bit Rate) for bursty traffic and bandwidth sharing with other applications.
Cell Rate	Cell rate configuration often helps eliminate traffic congestion that slows transmission of real time data such as audio and video connections.
Peak Cell Rate	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.
Sustain Cell Rate	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec.
Maximum Burst Size	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.
Login Information	(PPPoA and PPPoE encapsulation only)
Service Name	This field is only available when **PPPoE** encapsulation is selected. Type the **PPPoE** service name provided to you. **PPPoE** uses a service name to identify and reach the **PPPoE** server.
PPPoE + PPPoE_Client_PC(PPPoE encapsulation only)	This field is only available when **PPPoE** encapsulation is selected. Select the checkbox to enable PPPoE pass through. In addition to the Prestige's built-in PPPoE client, you can enable PPPoE pass through to allow up to ten hosts on the LAN to use PPPoE client software on their computers to connect to the ISP via the Prestige. Each host can have a separate account and a public WAN IP address. PPPoE pass through is an alternative to NAT for application where NAT is not appropriate.Disable PPPoE pass through if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP.
User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	Enter the password associated with the user name above.

Table 40 Configuration > WAN > Setup - Prestige - Routing Mode (continued)

LABEL	DESCRIPTION
IP Address	This option is available if you select **Routing** in the **Mode** field. A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. The Single User Account feature can be used with either a dynamic or static IP address. Select **Obtain an IP Address Automatically** if you have a dynamic IP address; otherwise select **Static IP Address** and type your ISP assigned IP address in the **IP Address** field below.
Connection (PPPoA and PPPoE encapsulation only)	The schedule rule(s) in SMT menu 26 have priority over your **Connection** settings.
Nailed-Up Connection	Select **Nailed-Up Connection** when you want your connection up all the time. The Prestige will try to bring up the connection automatically if it is disconnected.
Connect on Demand	Select **Connect on Demand** when you don't want the connection up all the time and specify an idle time-out in the **Max Idle Timeout** field.
Max Idle Timeout	Specify an idle time-out in the **Max Idle Timeout** field when you select **Connect on Demand**. The default setting is 0, which means the Internet session will not timeout.
Apply	Click **Apply** to save the changes.
Reset	Click **Reset** to begin configuring this screen afresh.

8.7.3 WAN Backup - Prestige

The CON/AUX port on the Prestige can be used in reserve, as a traditional dial-up connection should the WAN port connection fail. To set up the auxiliary port (AUX) for the Prestige for use in the event that the regular WAN connection is dropped, first make sure you have set up the switch and port connections.

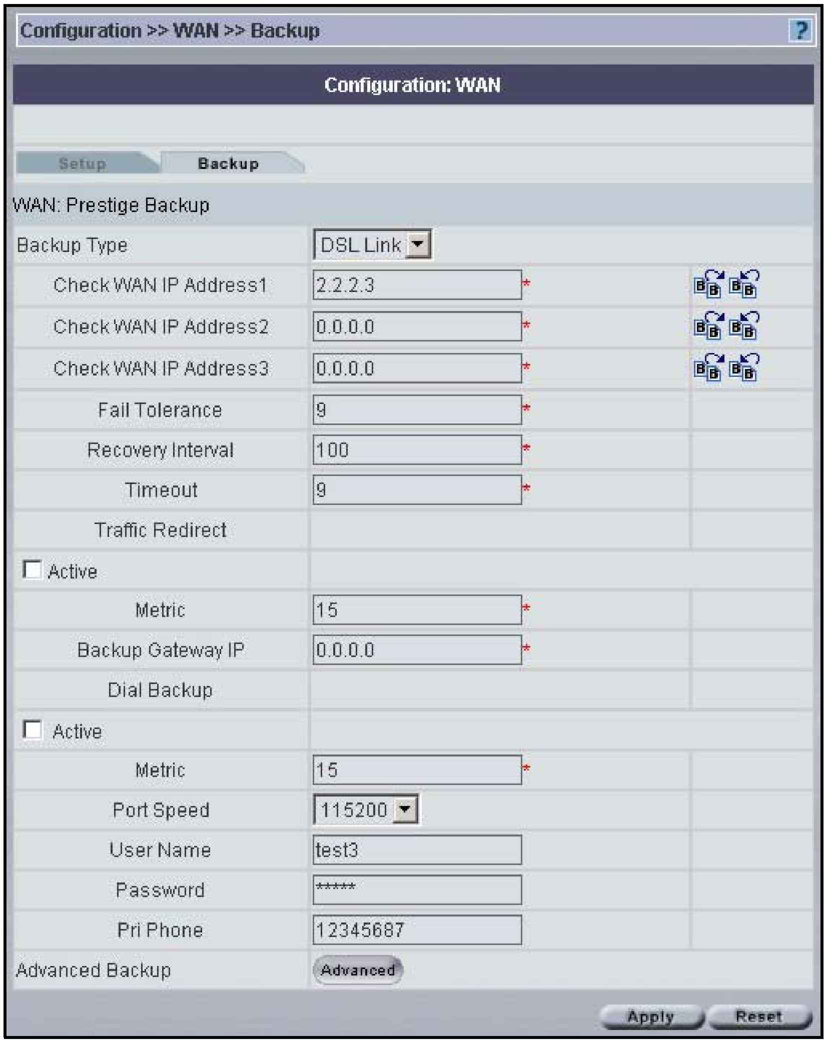
8.7.3.1 Traffic Redirect

See page 124 for more information on traffic redirect.

8.7.4 Configuring WAN Backup - Prestige

To change your Prestige's WAN backup settings, click **WAN** > **Backup**. The screen appears as shown.

Figure 72 Configuration > WAN > Backup - Prestige



Configuration >> WAN >> Backup

Configuration: WAN

WAN: Prestige Backup

Backup Type	DSL Link
Check WAN IP Address1	2.2.2.3 *
Check WAN IP Address2	0.0.0.0 *
Check WAN IP Address3	0.0.0.0 *
Fail Tolerance	9 *
Recovery Interval	100 *
Timeout	9 *
Traffic Redirect	
□ Active	
Metric	15 *
Backup Gateway IP	0.0.0.0 *
Dial Backup	
□ Active	
Metric	15 *
Port Speed	115200
User Name	test3
Password	*****
Pri Phone	12345687
Advanced Backup	Advanced

The following table describes the fields in this screen.

Table 41 Configuration > WAN > Backup - Prestige

LABEL	DESCRIPTION
Backup Type	Select the method that the Prestige uses to check the DSL connection. Select **DSL Link** to have the Prestige check if the connection to the DSLAM is up. Select **ICMP** to have the Prestige periodically ping the IP addresses configured in the **Check WAN IP Address** type fields.
Check WAN IP Address1-3	Configure this field to test your Prestige's WAN accessibility. Type the IP address of a reliable nearby computer (for example, your ISP's DNS server address). If you activate either traffic redirect or dial backup, you must configure at least one IP address here. When using a WAN backup connection, the Prestige periodically pings the addresses configured here and uses the other WAN backup connection (if configured) if there is no response.

Table 41 Configuration > WAN > Backup - Prestige (continued)

LABEL	DESCRIPTION
Fail Tolerance	Type the number of times (2 recommended) that your Prestige may ping the IP addresses configured in the **Check WAN IP Address** field without getting a response before switching to a WAN backup connection (or a different WAN backup connection).
Recovery Interval	When the Prestige is using a lower priority connection (usually a WAN backup connection), it periodically checks to whether or not it can use a higher priority connection. Type the number of seconds (30 recommended) for the Prestige to wait between checks. Allow more time if your destination IP address handles lots of traffic.
Timeout	Type the number of seconds (3 recommended) for your Prestige to wait for a ping response from one of the IP addresses in the **Check WAN IP Address** field before timing out the request. The WAN connection is considered "down" after the Prestige times out the number of times specified in the **Fail Tolerance** field. Use a higher value in this field if your network is busy or congested.
Traffic Redirect	
Active	Select this check box to have the Prestige use traffic redirect if the normal WAN connection goes down. If you activate traffic redirect, you must configure at least one Check WAN IP Address.
Metric	This field sets this route's priority among the routes the Prestige uses. The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".
Backup Gateway	Type the IP address of your backup gateway in dotted decimal notation. The Prestige automatically forwards traffic to this IP address if the Prestige's Internet connection terminates.
Dial Backup	
Active	Select this check box to turn on dial backup. If you activate dial backup, you must configure at least one Check WAN IP Address.
Metric	This field sets this route's priority among the three routes the Prestige uses (normal, traffic redirect and dial backup). Type a number (1 to 15) to set the priority of the dial backup route for data transmission. The smaller the number, the higher the priority. If the three routes have the same metrics, the priority of the routes is as follows: **WAN**, **Traffic Redirect**, **Dial Backup**.
Port Speed	Use the drop-down list box to select the speed of the connection between the dial backup port and the external device. Available speeds are: **9600**, **19200**, **38400**, **57600**, **115200** or **230400** bps.
User Name	Type the login name assigned by your ISP.
Password	Type the password assigned by your ISP.
Pri Phone #	Type the first (primary) phone number from the ISP for this remote node. Some areas require dialing the pound sign # before the phone number for local calls. Include a # symbol at the beginning of the phone numbers as required.

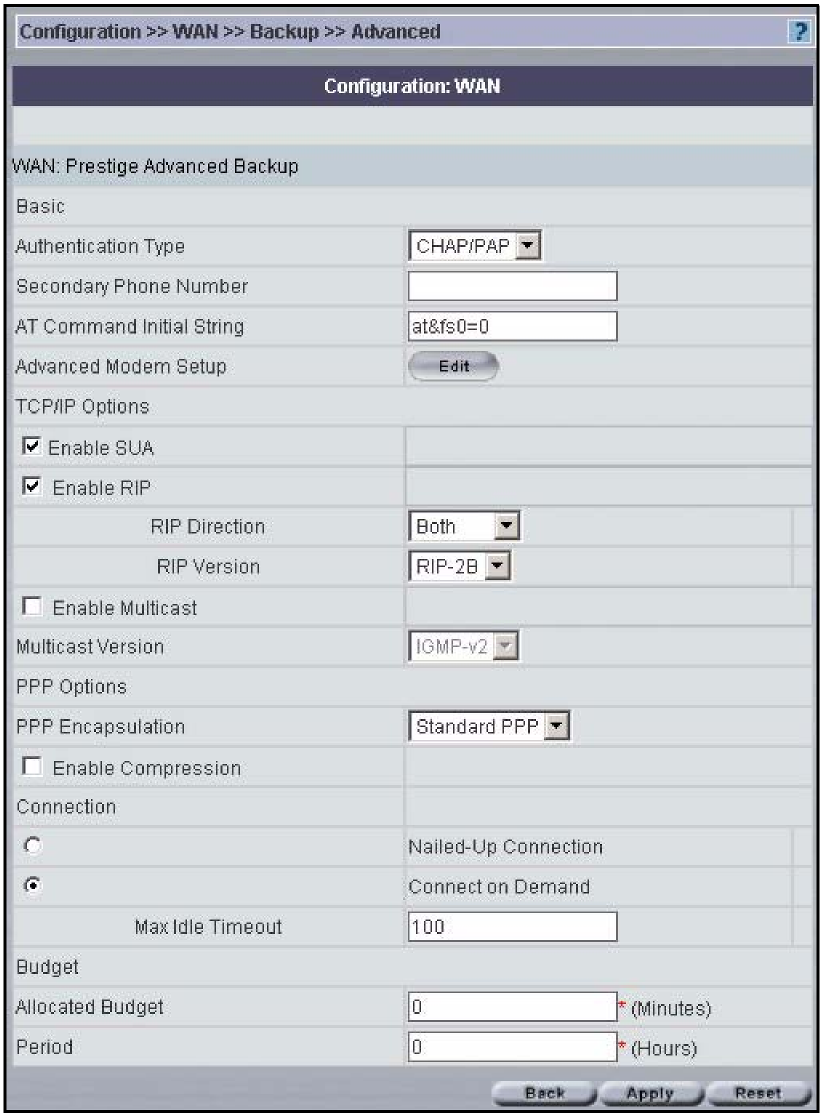
Table 41 Configuration > WAN > Backup - Prestige (continued)

LABEL	DESCRIPTION
Advanced Backup	Click this button to display the **Advanced Backup** screen and edit more details of your WAN backup setup.
Apply	Click **Apply** to save the changes.
Reset	Click **Reset** to begin configuring this screen afresh.

8.7.5 Configuring Advanced WAN Backup - Prestige

To edit your Prestige’s advanced WAN backup settings, click **WAN** > **WAN Backup** and the **Advanced Backup** button. The screen appears as shown next.

Figure 73 Configuration > WAN Backup > Advanced - Prestige



Configuration >> WAN >> Backup >> Advanced

Configuration: WAN

WAN: Prestige Advanced Backup

Basic	
Authentication Type	CHAP/PAP
Secondary Phone Number	
AT Command Initial String	at&fs0=0
Advanced Modem Setup	Edit
TCP/IP Options	
☑ Enable SUA	
☑ Enable RIP	
RIP Direction	Both
RIP Version	RIP-2B
□ Enable Multicast	
Multicast Version	IGMP-v2
PPP Options	
PPP Encapsulation	Standard PPP
□ Enable Compression	
Connection	
○	Nailed-Up Connection
●	Connect on Demand
Max Idle Timeout	100
Budget	
Allocated Budget	0 * (Minutes)
Period	0 * (Hours)

The following table describes the fields in this screen.

Table 42 Configuration > WAN Backup > Advanced - Prestige

LABEL	DESCRIPTION
Basic	
Authentication Type	Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: **CHAP/PAP** - Your Prestige accepts either CHAP or PAP when requested by this remote node. **CHAP** - Your Prestige accepts CHAP only. **PAP** - Your Prestige accept PAP only.

Table 42 Configuration > WAN Backup > Advanced - Prestige (continued)

LABEL	DESCRIPTION
Primary/ Secondary Phone Number	Type the first (primary) phone number from the ISP for this remote node. If the primary phone number is busy or does not answer, your Prestige dials the secondary phone number if available. Some areas require dialing the pound sign # before the phone number for local calls. Include a # symbol at the beginning of the phone numbers as required.
AT Command Initial String	Type the AT command string to initialize the WAN device. Consult the manual of your WAN device connected to your dial backup port for specific AT commands.
Advanced Modem Setup	Click the **Edit** button to display the **Advanced Modem Setup** screen and edit the details of your dial backup setup.
TCP/IP Options	
Enable SUA	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network to a different IP address known within another network. SUA (Single User Account) is a subset of NAT that supports two types of mapping: Many-to-One and Server. When you select this option the Prestige will use Address Mapping Set 255 in the SMT.
Enable RIP	Select this check box to turn on RIP (Routing Information Protocol), which allows a router to exchange routing information with other routers.
RIP Direction	RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Choose **Both**, **In Only** or **Out Only**. When set to **Both** or **Out Only**, the Prestige will broadcast its routing table periodically. When set to **Both** or **In Only**, the Prestige will incorporate RIP information that it receives.
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the Prestige sends (it recognizes both formats when receiving). Choose **RIP-1**, **RIP-2B** or **RIP-2M**. **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. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also.
Enable Multicast	Select this check box to turn on IGMP (Internet Group Multicast Protocol). IGMP is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data.
Multicast Version	Select **IGMP-v1** or **IGMP-v2**. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about inter operability between IGMP version 2 and version 1, please see *sections 4* and *5* of *RFC 2236*.
PPP Options	
PPP Encapsulation **Standard PPP**.	Select **CISCO PPP** from the drop-down list box if your backup WAN device uses **Cisco PPP** encapsulation; otherwise select
Enable Compression	Select this check box to enable stac compression.
Connection	

Table 42 Configuration > WAN Backup > Advanced - Prestige (continued)

LABEL	DESCRIPTION
Nailed-Up Connection	Select **Nailed-Up Connection** when you want your connection up all the time. The Prestige will try to bring up the connection automatically if it is disconnected.
Connect on Demand	Select **Connect on Demand** when you don't want the connection up all the time and specify an idle time-out in the **Max Idle Timeout** field.
Max Idle Timeout	Specify an idle time-out in the **Max Idle Timeout** field when you select **Connect on Demand**. The default setting is 0, which means the Internet session will not timeout.
Budget	The configuration in the **Budget** fields has priority over your **Connection** settings.
Allocated Budget	Type the amount of time (in minutes) that the dial backup connection can be used during the time configured in the **Period** field. Set an amount that is less than the time period configured in the **Period** field. If you set the **Allocated Budget** to 0, you will not be able to use the dial backup connection.
Period	Type the time period (in hours) for how often the budget should be reset. For example, to allow calls to this remote node for a maximum of 10 minutes every hour, set the **Allocated Budget** to 10 (minutes) and the **Period** to 1 (hour). If you set the **Period** to 0, there is no budget control and the Prestige uses the **Connection** settings.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save the changes.
Reset	Click **Reset** to begin configuring this screen afresh.

8.7.6 Advanced Modem Setup - Prestige

Click **Edit** in the **Advanced Modem Setup** field. See the section on ZyWALL advanced modem setup on page 127 for configuration of this screen.

CHAPTER 9
Configuration > NAT

9.1 NAT Overview

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet. For example, the source address of an outgoing packet, used within one network is changed to a different IP address known within another network.

9.1.1 NAT Definitions

Inside/outside denotes where a host is located relative to the ZyXEL device. For example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router. For example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

Table 43 NAT Definitions

TERM	DESCRIPTION
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

Note: NAT never changes the IP address (either local or global) of an outside host.

9.1.2 What NAT Does

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers (for example a web server and a telnet server) on your local network and make them accessible to the outside world. Although you can make designated servers on the LAN accessible to the outside world, it is strongly recommended that you attach those servers to the DMZ port instead. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping), NAT offers the additional benefit of firewall protection. With no servers defined, the ZyXEL device filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631*, *The IP Network Address Translator (NAT)*.

9.1.3 How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The ZyXEL device keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored.

9.1.4 NAT Mapping Types

NAT supports five types of IP/port mapping. They are:

- **One to One**: In One-to-One mode, the ZyXEL device maps one local IP address to one global IP address.
- **Many to One**: In Many-to-One mode, the ZyXEL device maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature (the SUA Only option).
- **Many to Many Overload**: In Many-to-Many Overload mode, the ZyXEL device maps the multiple local IP addresses to shared global IP addresses.
- **Many One to One**: In Many-One-to-One mode, the ZyXEL device maps each local IP address to a unique global IP address.
- **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world although, it is highly recommended that you use the DMZ port for these servers instead.

Note: Port numbers do not change for One-to-One and Many-One-to-One NAT mapping types.

The following table summarizes these types.

Table 44 NAT Mapping Types

TYPE	IP MAPPING	SMT ABBREVIATION
One-to-OneILA1⇓◊ IGA1 1-1		
Many-to-One (SUA/PAT)	ILA1–> IGA1 ILA2–>IGA1	M-1
Many-to-Many Overload	ILA1–> IGA1 ILA2–> IGA2 ILA3–> IGA1 ILA4–> IGA2	M-M Ov
Many-One-to-One	ILA1–> IGA1 ILA2–> IGA2 ILA3–> IGA3	M-1-1
Server	Server 1 IP–> IGA1 Server 2 IP–> IGA1 Server 3 IP–>IGA1 Server	

9.1.5 SUA (Single User Account) Versus NAT

SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. The ZyXEL device also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types. Select either **SUA Only** or **Full Feature** in **WAN IP**.

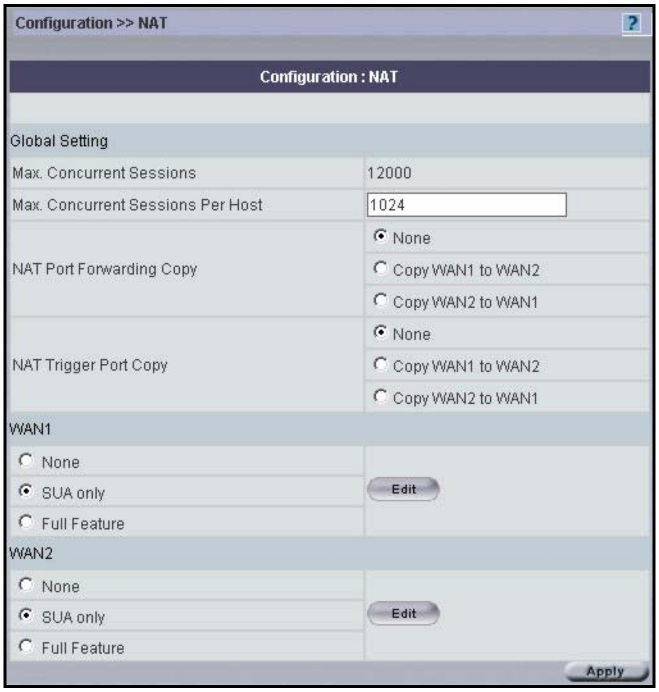
Selecting **SUA Only** means (latent) multiple WAN-to-LAN and WAN-to-DMZ multiple address translation. That means that computers on your DMZ with public IP addresses will still have to undergo NAT mapping if you’re using **SUA Only** NAT mapping. If this is not your intention, then select **Full Feature** NAT and don’t configure NAT mapping rules to those computers with public IP addresses on the DMZ.

9.2 Configuring NAT - ZyWALL

You must create a firewall rule in addition to setting up NAT, to allow traffic from the WAN to be forwarded through the ZyXEL device.

Select a device and click **Configuration > NAT**.

Figure 74 Configuration > NAT - ZyWALL



Global Setting

Max. Concurrent Sessions 12000

Max. Concurrent Sessions Per Host 1024

NAT Port Forwarding Copy ● None ○ Copy WAN1 to WAN2 ○ Copy WAN2 to WAN1

NAT Trigger Port Copy ● None ○ Copy WAN1 to WAN2 ○ Copy WAN2 to WAN1

WAN1

○ None
● SUA only
○ Full Feature

WAN2

○ None
● SUA only
○ Full Feature

The following table describes the fields in this screen.

Table 45 Configuration > NAT - ZyWALL

LABEL	DESCRIPTION
Global Setting	
Max. Concurrent Sessions	This read-only field displays the highest number of NAT sessions that the ZyWALL will permit at one time.
Max. Concurrent Sessions Per Host	Use this field to set the highest number of NAT sessions that the ZyWALL will permit a host to have at one time.
NAT Port Forwarding Copy	Click **Copy WAN1 to WAN 2** (or **Copy WAN2 to WAN 1**) to duplicate this WAN port's NAT port forwarding rules on the other WAN port. **Note:** Using the copy button overwrites the other WAN port's existing rules. The copy button is best suited for initial NAT configuration where you have configured NAT port forwarding rules for one port and want to use similar rules for the other WAN port. You can use the other NAT screens to edit the NAT rules after you copy them from one WAN port to the other.

Table 45 Configuration > NAT - ZyWALL

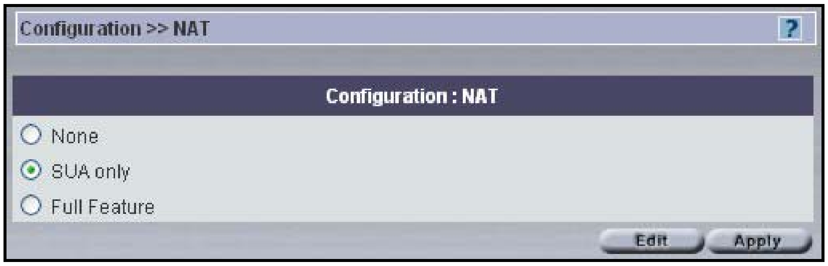
LABEL	DESCRIPTION
NAT Trigger Port Copy	Click **Copy WAN1 to WAN 2** (or **Copy WAN2 to WAN 1**) to duplicate this WAN port's NAT trigger port rules on the other WAN port. **Note:** Using the copy button overwrites the other WAN port's existing rules. The copy button is best suited for initial NAT configuration where you have configured NAT trigger port rules for one port and want to use similar rules for the other WAN port. You can use the other NAT screens to edit the NAT rules after you copy them from one WAN port to the other.
WAN 1, 2	
None	Select **None** to disable NAT on the ZyXEL device.
SUA Only	Select **SUA Only** to apply many-to-one mapping only (sufficient if the device has only one public IP address).
Full Feature	Select **Full Feature** to avail of multiple mapping types.
Edit	Click **Edit** to advance to the selected feature.
Apply	Click **Apply** to begin configuring this screen afresh.

9.3 Configuring NAT - Prestige

You must create a firewall rule in addition to setting up NAT, to allow traffic from the WAN to be forwarded through the ZyXEL device.

Select a device and then click **Configuration** > **NAT**.

Figure 75 Configuration > NAT - Prestige



Configuration >> NAT

Configuration : NAT

○ None

● SUA only

○ Full Feature

The following table describes the fields in this screen.

Table 46 Configuration > NAT - Prestige

LABEL	DESCRIPTION
None	Select **None** to disable NAT on the ZyXEL device.
SUA Only	Select **SUA Only** to apply many-to-one mapping only (sufficient if the device has only one public IP address).
Full Feature	Select **Full Feature** to avail of multiple mapping types.

Table 46 Configuration > NAT - Prestige

LABEL	DESCRIPTION
Edit	Click **Edit** to advance to the selected feature.
Apply	Click **Apply** to begin configuring this screen afresh.

9.4 SUA Servers

A SUA server set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though SUA makes your whole inside network appear as a single computer to the outside world. The ZyXEL device provides the additional safety of a DMZ port for connecting your publicly accessible servers. This makes the LAN more secure by physically separating it from your public servers.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

In addition to the servers for specified services, NAT supports a default server IP address. A default server receives packets from ports that are not specified in this screen.

Note: If you do not assign a Default Server IP Address the ZyXEL device discards all packets received for ports that are not specified here or in the remote management setup.

9.4.1 Port Forwarding: Services and Port Numbers

The most often used port numbers are shown in the following table. Please refer to RFC 1700 for further information about port numbers. Please also refer to the Supporting CD for more examples and details on SUA/NAT Services and Port Numbers

Note: Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP..

Table 47 Services and Port Numbers

SERVICES	PORT NUMBER
ECHO	
FTP (File Transfer Protocol)	21
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)1723	

9.4.2 NAT and Multiple WAN

The ZyWALL has two WAN ports. You can configure port forwarding and trigger port rule sets for the first WAN port and separate sets of rules for the second WAN port.

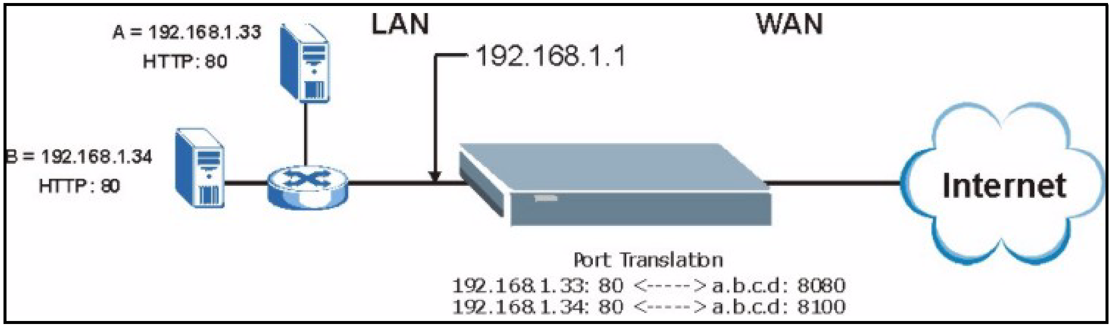
9.4.3 Port Translation

The ZyWALL can translate the destination port number or a range of port numbers of packets coming from the WAN to another destination port number or range of port numbers on the LAN (or DMZ). When you use port forwarding without port translation, a single server on the LAN or DMZ can use a specific port number and be accessible to the outside world through a single WAN IP address. When you use port translation with port forwarding, multiple servers on the LAN or DMZ can use the same port number and still be accessible to the outside world through a single WAN IP address.

The following example has two web servers on a LAN. Server **A** uses IP address 192.168.1.33 and server **B** uses 192.168.1.34. Both servers use port 80. The letters a.b.c.d represent the WAN port’s IP address. The ZyWALL translates port 8080 of traffic received on the WAN port (IP address a.b.c.d) to port 80 and sends it to server **A** (IP address 192.168.1.33). The ZyWALL also translates port 8100 of traffic received on the WAN port (also IP address a.b.c.d) to port 80, but sends it to server **B** (IP address 192.168.1.34).

Note: In this example, anyone wanting to access server A from the Internet must use port 8080. Anyone wanting to access server B from the Internet must use port 8100.

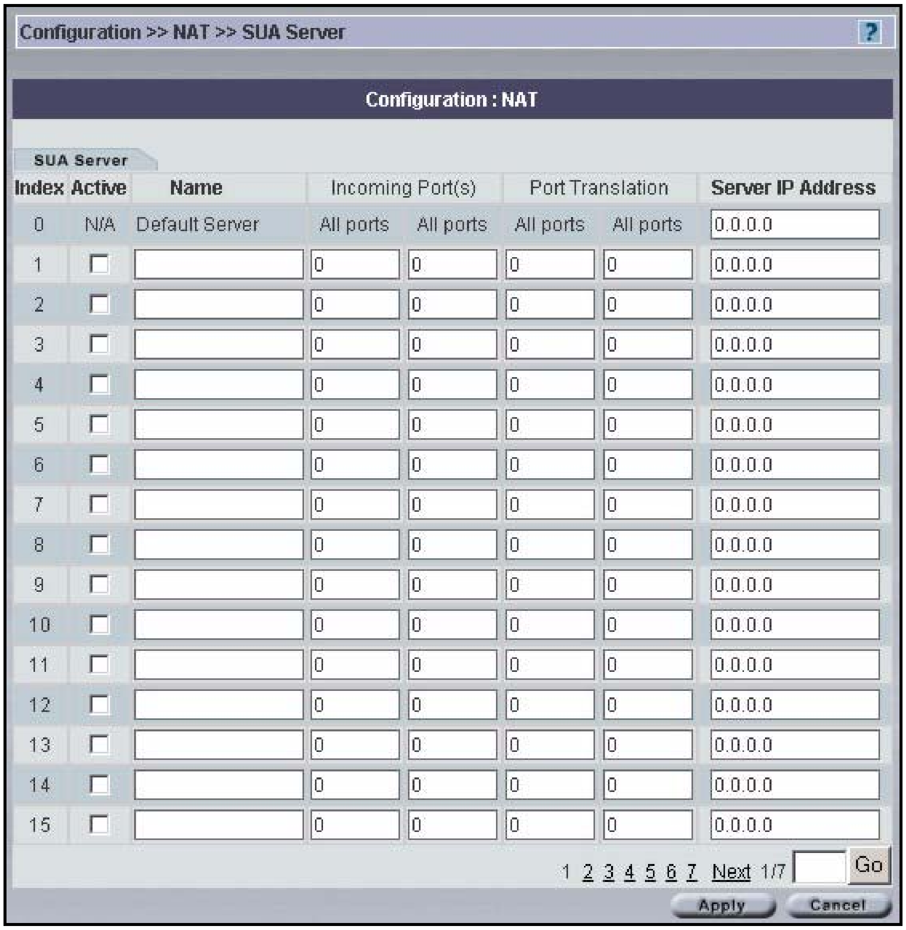
Figure 76 Port Translation Example



9.4.4 Configuring SUA Servers - ZyWALL

Select **SUA Only** in Figure 75 on page 148 and then click **Edit** to bring up the next screen.

Figure 77 Configuration > NAT > SUA Server - ZyWALL



Index	Active	Name	Incoming Port(s)		Port Translation		Server IP Address
0	N/A	Default Server	All ports	All ports	All ports	All ports	0.0.0.0
1	□		0	0	0	0	0.0.0.0
2	□		0	0	0	0	0.0.0.0
3	□		0	0	0	0	0.0.0.0
4	□		0	0	0	0	0.0.0.0
5	□		0	0	0	0	0.0.0.0
6	□		0	0	0	0	0.0.0.0
7	□		0	0	0	0	0.0.0.0
8	□		0	0	0	0	0.0.0.0
9	□		0	0	0	0	0.0.0.0
10	□		0	0	0	0	0.0.0.0
11	□		0	0	0	0	0.0.0.0
12	□		0	0	0	0	0.0.0.0
13	□		0	0	0	0	0.0.0.0
14	□		0	0	0	0	0.0.0.0
15	□		0	0	0	0	0.0.0.0

The following table describes the labels in this screen.

Table 48 Configuration > NAT > SUA Server - ZyWALL

LABEL	DESCRIPTION
Index	This is the number of an individual SUA server entry. You may select a rule to edit or delete it.
Active	Select this check box to enable the SUA server entry. Clear this checkbox to disallow forwarding of these ports to an inside server without having to delete the entry.
Name	Type a name to identify this port-forwarding rule. To delete a SUA server entry, erase the name and click **Apply**.
Default Server	In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in this screen. If you do not assign a default server IP address, then all packets received for ports not specified in this screen or remote management will be discarded.
Incoming Port(s)	Enter a port number here. To forward only one port, enter it again in the second field. To specify a range of ports, enter the last port to be forwarded in the second field.

Table 48 Configuration > NAT > SUA Server - ZyWALL

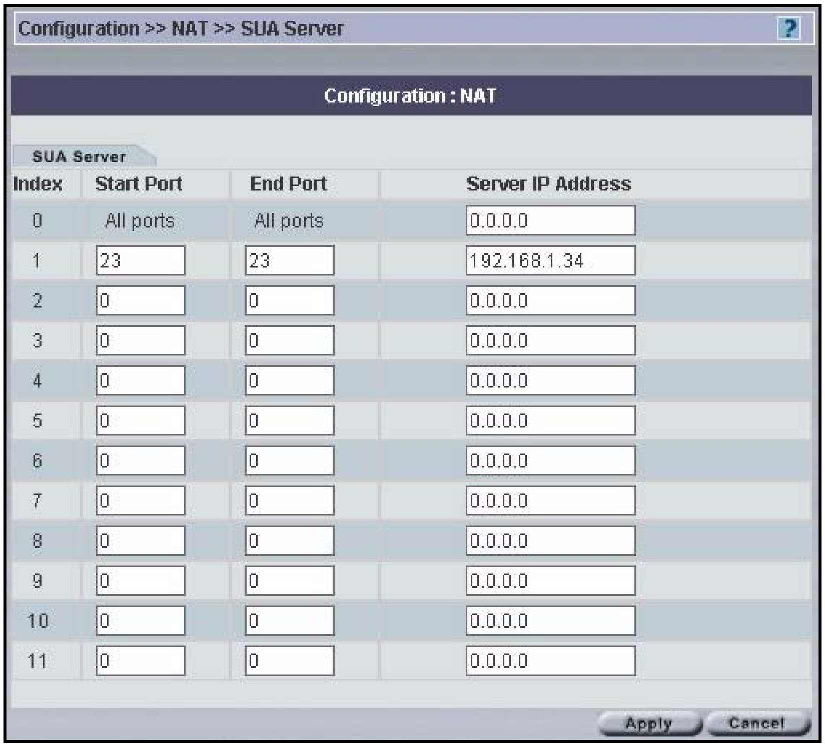
LABEL	DESCRIPTION
Port Translation	Enter the port number here to which you want the ZyWALL to translate the incoming port. For a range of ports, you only need to enter the first number of the range to which you want the incoming ports translated, the ZyWALL automatically calculates the last port of the translated port range.
Incoming Port(s)	Enter a port number here. To forward only one port, enter it again in the second field. To specify a range of ports, enter the last port to be forwarded in the second field.
Server IP Address	Type the IP address of the inside server.
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Cancel	Click **Cancel** to return to the previous screen.

Select a radio button and then click **Edit** to configure that server set.

9.4.5 Configuring SUA Servers - Prestige

Select **SUA Only** in Figure 75 on page 148 and then click **Edit** to bring up the next screen.

Figure 78 Configuration > NAT > SUA Server - Prestige



Index	Start Port	End Port	Server IP Address
0	All ports	All ports	0.0.0.0
1	23	23	192.168.1.34
2	0	0	0.0.0.0
3	0	0	0.0.0.0
4	0	0	0.0.0.0
5	0	0	0.0.0.0
6	0	0	0.0.0.0
7	0	0	0.0.0.0
8	0	0	0.0.0.0
9	0	0	0.0.0.0
10	0	0	0.0.0.0
11	0	0	0.0.0.0

The following table describes the labels in this screen.

Table 49 Configuration > NAT > SUA Server - Prestige

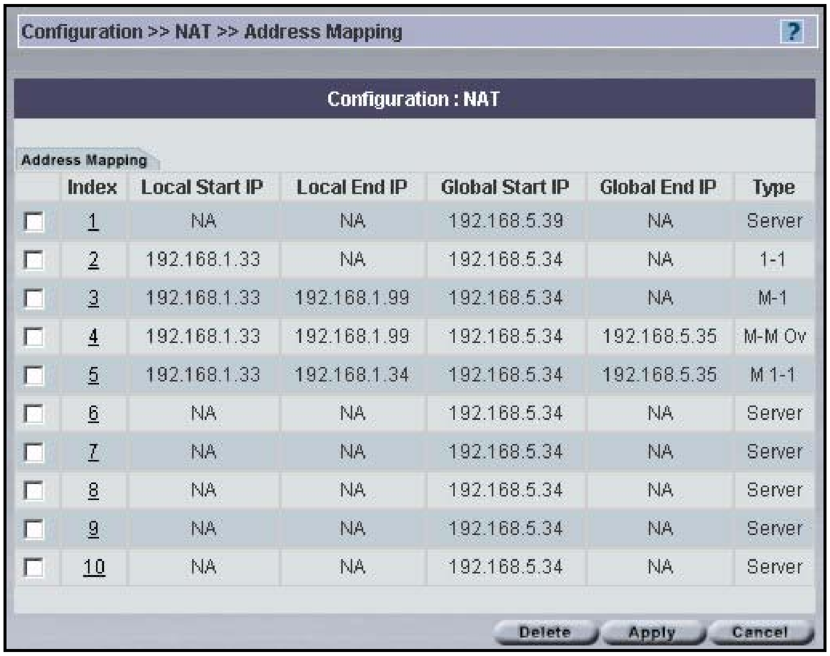
	DESCRIPTION
Index	This is the number of an individual SUA server entry.
Default Server	In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in this screen. If you do not assign a default server IP address, then all packets received for ports not specified in this screen or remote management will be discarded.
Start Port End Port	Type the start and end port numbers that define the service that will be forwarded to the inside server specified in the next field.
Server IP Address	Type the IP address of the inside server.
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Cancel	Click **Cancel** to return to the previous screen.

Select a radio button and then click **Edit** to configure that server set.

9.4.6 Full Feature Address Mapping

Select **Full Feature** in Figure 75 on page 148 and click **Edit** to bring up the next screen.

Figure 79 Configuration > NAT > Full Feature > Address Mapping



	Index	Local Start IP	Local End IP	Global Start IP	Global End IP	Type
□	1	NA	NA	192.168.5.39	NA	Server
□	2	192.168.1.33	NA	192.168.5.34	NA	1-1
□	3	192.168.1.33	192.168.1.99	192.168.5.34	NA	M-1
□	4	192.168.1.33	192.168.1.99	192.168.5.34	192.168.5.35	M-M Ov
□	5	192.168.1.33	192.168.1.34	192.168.5.34	192.168.5.35	M 1-1
□	6	NA	NA	192.168.5.34	NA	Server
□	7	NA	NA	192.168.5.34	NA	Server
□	8	NA	NA	192.168.5.34	NA	Server
□	9	NA	NA	192.168.5.34	NA	Server
□	10	NA	NA	192.168.5.34	NA	Server

The following table describes the labels in this screen.

Table 50 Configuration > NAT > Full Feature > Address Mapping

LABEL	DESCRIPTION
Index	This is the number of an individual entry. You may select a rule to edit by going to the **Edit Address Mapping** screen for that rule.
Local Start IP	This refers to the Inside Local Address (ILA), which is the starting local IP address. Local IP addresses are **N/A** for **Server** port mapping.
Local End IP	This is the end Inside Local Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 and 255.255.255.255 as the **Local End IP** address. This field is **N/A** for **One-to-One** and **Server** mapping types.
Global Start IP	This refers to the Inside Global IP Address (IGA). 0.0.0.0 is for a dynamic IP address from your ISP with **Many-to-One** and **Server** mapping types.
Global End IP	This is the ending Inside Global Address (IGA), which is the starting global IP address. This field is **N/A** for **One-to-One**, **Many-to-One** and **Server** mapping types.
Type	1. **One-to-One** mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type. 2. **Many-to-One** mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only. 3. **Many-to-Many Overload** mode maps multiple local IP addresses to shared global IP addresses. 4. **Many One-to-One** mode maps each local IP address to unique global IP addresses. 5. **Server** allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Delete	Select the radio button next to a rule and click **Delete** to delete the address-mapping rule.

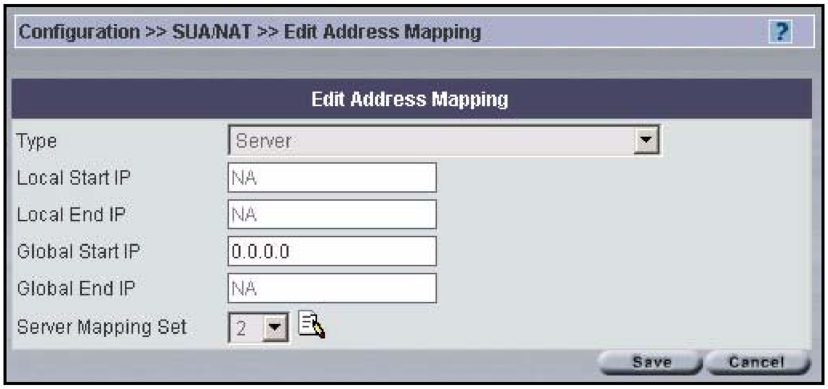
Table 50 Configuration > NAT > Full Feature > Address Mapping (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Cancel	Click **Cancel** to close this screen without applying any changes.

9.4.7 Edit Full Feature Address Mapping

Select a radio button from the **Address Mapping** screen and click **Edit**. Select the mapping type and local, remote IP address ranges here.

Figure 80 Configuration > NAT > Full Feature > Edit Address Mapping



Configuration >> SUA/NAT >> Edit Address Mapping

Edit Address Mapping

Type	Server
Local Start IP	NA
Local End IP	NA
Global Start IP	0.0.0.0
Global End IP	NA
Server Mapping Set	2

Table 51 Configuration > NAT > Full Feature > Edit Address Mapping

LABEL	DESCRIPTION
Type	When you select **Type** you can choose a server mapping set. Choose the port mapping type from one of the following. 1. **One-to-One**: One-to-one mode maps one local IP address to one global IP address. Note that port numbers do not change for One-to-one NAT mapping type. 2. **Many-to-One**: Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature. 3. **Many-to-Many Ov** (Overload): Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses. 4. **Many One-to-One**: Many One-to-one mode maps each local IP address to unique global IP addresses. 5. **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Local Start IP	This is the starting Inside Local IP Address (ILA). Local IP addresses are **N/A** for **Server** port mapping.
Local End IP	This is the end Inside Local IP Address (ILA). If your rule is for all local IP addresses, then enter 0.0.0.0 as the **Local Start IP** address and 255.255.255.255 as the **Local End IP** address. This field is **N/A** for **One-to-One** and **Server** mapping types.
Global Start IP	This is the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP.
Global End IP	This is the ending Inside Global IP Address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server** mapping types.
Server Mapping Set	This field is only available in the Prestige and when **Type** is set to **Server**. Select a number from the drop-down menu to choose a server set from the **NAT > Address Mapping** screen. Click the link to go to the **NAT > SUA Server** screen to edit a server set that you have selected in the **Server Mapping Set** field.
Save	Click **Save** to save your changes back to the ZyXEL device.
Cancel	Click **Cancel** to return to the previous screen.

9.5 Trigger Port Forwarding - ZyWALL

Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address,

Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The ZyXEL device records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the ZyXEL device's WAN port receives a response with a specific port number and protocol ("incoming" port), the ZyXEL device forwards the traffic to the LAN IP address of the computer that sent the request. After that computer’s connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

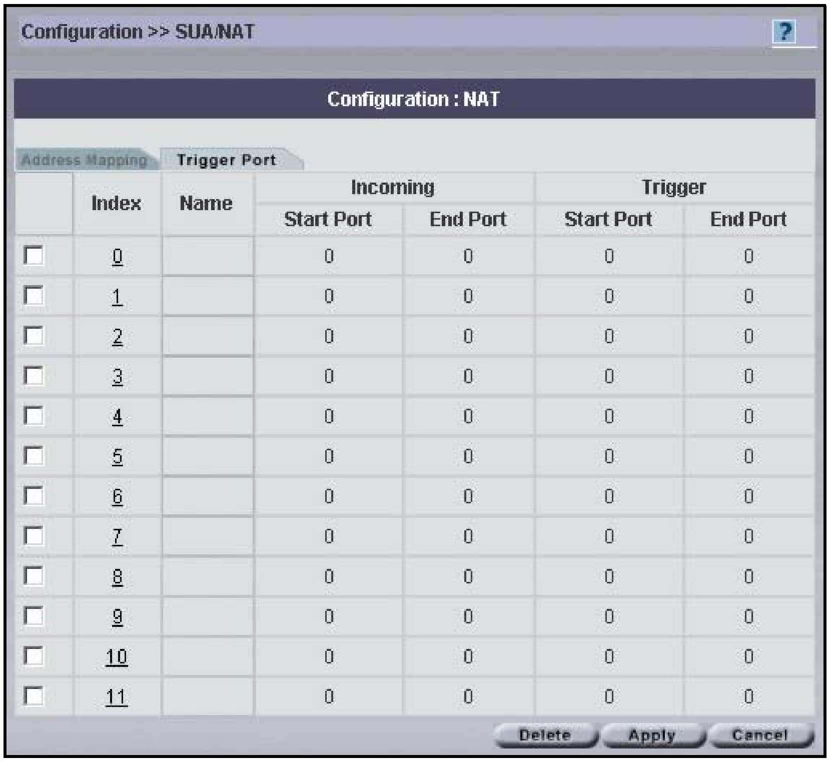
Trigger events only happen on outgoing data (from the ZyXEL device).

Only one LAN computer can use a trigger port (range) at a time. Therefore, if an application needs a continuous data stream, that port (range) will be tied up so that another computer on the LAN can’t trigger it until that stream finishes.

9.5.1 Configuring Trigger Port

Select **Full Feature** > **Edit** > **Trigger Port** tab to bring up the next screen.

Figure 81 Configuration > NAT > Full Feature > Trigger Port



	Index	Name	Incoming		Trigger	
			Start Port	End Port	Start Port	End Port
□	0		0	0	0	0
□	1		0	0	0	0
□	2		0	0	0	0
□	3		0	0	0	0
□	4		0	0	0	0
□	5		0	0	0	0
□	6		0	0	0	0
□	7		0	0	0	0
□	8		0	0	0	0
□	9		0	0	0	0
□	10		0	0	0	0
□	11		0	0	0	0

The following table describes the labels in this screen.

Table 52 Configuration > NAT > Full Feature > Trigger Port

LABEL	DESCRIPTION
Index	This is the number of an individual entry. You may select a rule to edit.
Name	This field displays a unique name (up to 15 characters) for identification purposes.
Incoming	Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The ZyXEL device forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.
Start Port	This field displays a port number or the starting port number in a range of port numbers.
End Port	This field displays a port number or the ending port number in a range of port numbers.
Trigger	The trigger port is a port (or a range of ports) that causes (or triggers) the ZyXEL device to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Start Port	This field displays a port number or the starting port number in a range of port numbers.
End Port	This field displays a port number or the ending port number in a range of port numbers.
Delete	Select a rule and then click **Delete** to erase it.

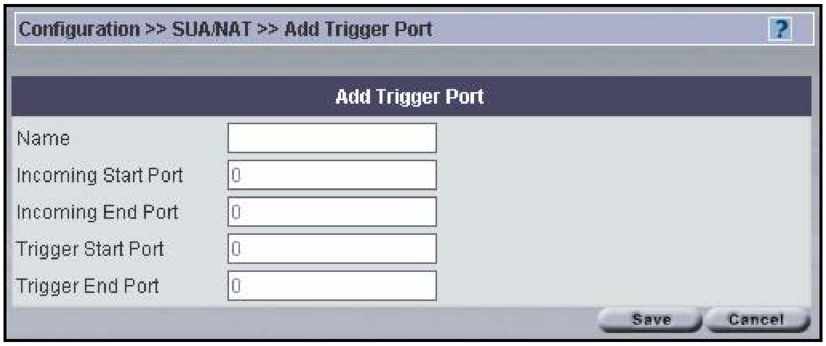
Table 52 Configuration > NAT > Full Feature > Trigger Port (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Cancel	This field displays a port number or the ending port number in a range of port numbers.

9.5.2 Edit Trigger Port

Select an index number from the **Trigger Port** screen and click **Edit**.

Figure 82 Configuration > NAT > Full Feature > Trigger Port > Edit



Configuration >> SUA/NAT >> Add Trigger Port

Add Trigger Port

Name	
Incoming Start Port	0
Incoming End Port	0
Trigger Start Port	0
Trigger End Port	0

The following table describes the labels in this screen.

Table 53 Configuration > NAT > Full Feature > Trigger Port > Edit

LABEL	DESCRIPTION
Name	Type a unique name (up to 15 characters) for identification purposes. All characters are permitted - including spaces.
Incoming	Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The ZyXEL device forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Trigger	The trigger port is a port (or a range of ports) that causes (or triggers) the ZyXEL device to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Save	Click **Save** to save your changes back to the ZyXEL device.
Cancel	Click **Cancel** to return to the previous screen.

CHAPTER 10
Configuration > Static Route

This chapter shows you how to configure static route.

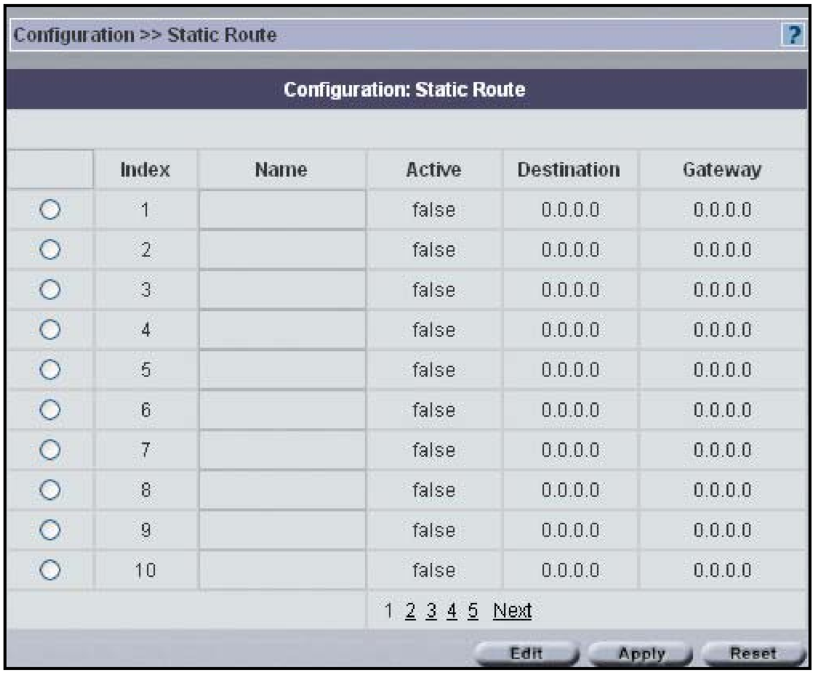
10.1 Static Route Overview

Each remote node specifies only the network to which the gateway is directly connected, and the ZyXEL device has no knowledge of the networks beyond

10.1.1 Static Route Summary

Select a device and then click **Configuration** > **Static Route**.

Figure 83 Configuration > Static Route



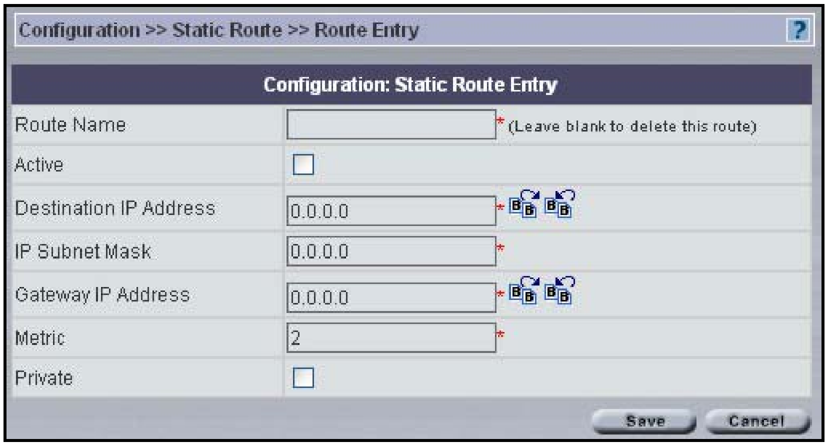
	Index	Name	Active	Destination	Gateway
○	1		false	0.0.0.0	0.0.0.0
○	2		false	0.0.0.0	0.0.0.0
○	3		false	0.0.0.0	0.0.0.0
○	4		false	0.0.0.0	0.0.0.0
○	5		false	0.0.0.0	0.0.0.0
○	6		false	0.0.0.0	0.0.0.0
○	7		false	0.0.0.0	0.0.0.0
○	8		false	0.0.0.0	0.0.0.0
○	9		false	0.0.0.0	0.0.0.0
○	10		false	0.0.0.0	0.0.0.0

Table 54 Configuration > Static Route

LABEL	DESCRIPTION
Index	This is the number of an individual entry. You may select a rule to edit or delete it.
Name	This is the name that describes or identifies this route. To delete a static route, erase the name and then click apply.
Active	This field shows whether this static route is active or not.
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Gateway	This is the IP address of the gateway. The gateway is an immediate neighbor of the ZyXEL device that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as the ZyXEL device; over the WAN, the gateway must be the IP address of one of the remote nodes.
Next	Select a page number or **Next** to view a particular page or next page of server entries respectively.
Edit	Click a static route index number and then click **Edit** to set up a static route on the ZyXEL device.
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Reset	Click **Reset** to begin configuring this screen afresh.

10.1.2 Edit Static Route

Figure 84 Configuration > Static Route > Edit



Configuration >> Static Route >> Route Entry

Configuration: Static Route Entry

Route Name	* (Leave blank to delete this route)
Active	□
Destination IP Address	0.0.0.0 *
IP Subnet Mask	0.0.0.0 *
Gateway IP Address	0.0.0.0 *
Metric	2 *
Private	□

Table 55 Configuration > Static Route > Edit

LABEL	DESCRIPTION
Route Name	Enter the name of the IP static route. Leave this field blank to delete this static route.
Active	This checkbox allows you to activate/deactivate this static route.
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 IP subnet mask here.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of the ZyXEL device that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as the ZyXEL device; over the WAN, the gateway must be the IP address of one of the Remote Nodes.
Metric	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.
Private	This parameter determines if the ZyXEL device will include this route to a remote node in its RIP broadcasts. Select this check box to keep this route private and not included in RIP broadcasts. Clear this checkbox to propagate this route to other hosts through RIP broadcasts.
Save	Click **Save** to save your changes back to the ZyXEL device.
Cancel	Click **Cancel** to return to the previous screen.

CHAPTER 11 Configuration > VPN

This chapter shows you how to configure VPNs using Vantage. Screens relate to VPN version 1.0 or 1.1 depending on the device's firmware version.

11.1 VPN Overview

A VPN (Virtual Private Network) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing technologies/services used to transport traffic over the Internet or any insecure network that uses the TCP/IP protocol suite for communication.

11.1.1 IPSec

Internet Protocol Security (IPSec) is a standards-based VPN that offers flexible solutions for secure data communications across a public network like the Internet. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer.

11.1.2 Security Association

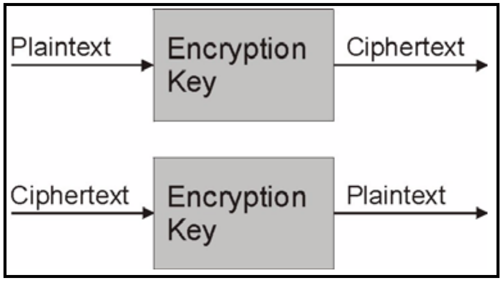
A Security Association (SA) is a contract between two parties indicating what security parameters, such as keys and algorithms they will use.

11.1.3 Other Terminology

11.1.3.1 Encryption

Encryption is a mathematical operation that transforms data from "plaintext" (readable) to "ciphertext" (scrambled text) using a "key". The key and clear text are processed by the encryption operation, which leads to the data scrambling that makes encryption secure. Decryption is the opposite of encryption: it is a mathematical operation that transforms ciphertext to plaintext. Decryption also requires a key.

Figure 85 Encryption and Decryption



11.1.3.2 Data Confidentiality

The IPSec sender can encrypt packets before transmitting them across a network.

11.1.3.3 Data Integrity

The IPSec receiver can validate packets sent by the IPSec sender to ensure that the data has not been altered during transmission.

11.1.3.4 Data Origin Authentication

The IPSec receiver can verify the source of IPSec packets. This service depends on the data integrity service.

11.1.3.5 Linking Two or More Private Networks Together

Connect branch offices and business partners over the Internet with significant cost savings and improved performance when compared to leased lines between sites.

11.1.3.6 Accessing Network Resources When NAT Is Enabled

When NAT is enabled, remote users are not able to access hosts on the LAN unless the host is designated a public LAN server for that specific protocol. Since the VPN tunnel terminates inside the LAN, remote users will be able to access all computers that use private IP addresses on the LAN.

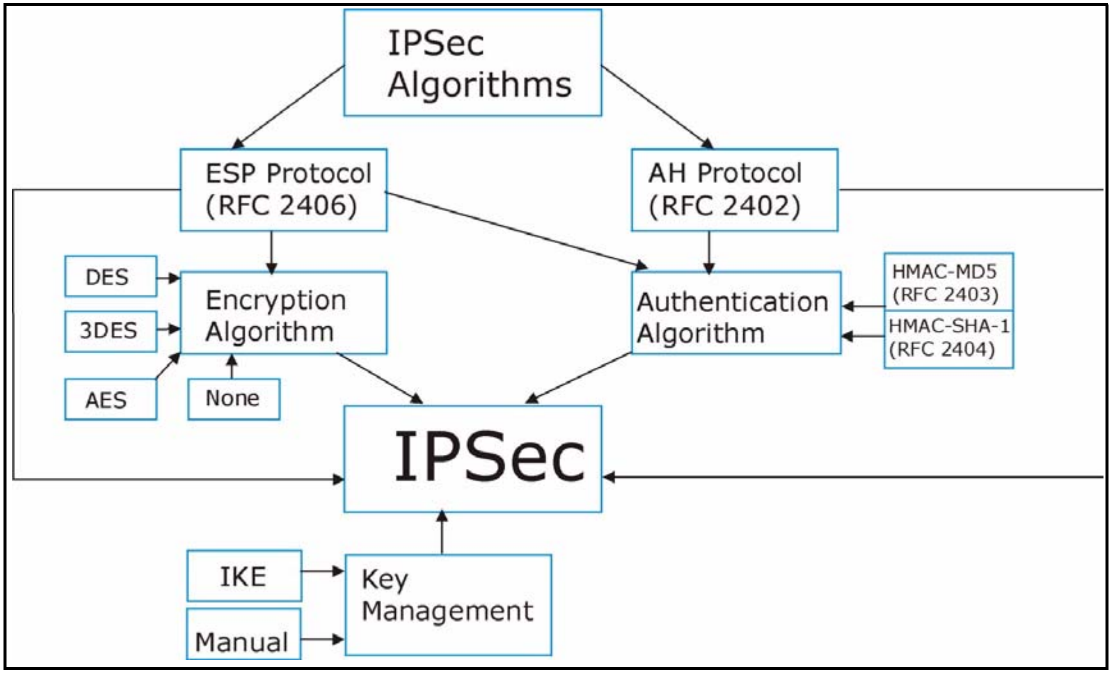
11.1.3.7 Unsupported IP Applications

A VPN tunnel may be created to add support for unsupported emerging IP applications.

11.2 IPSec Architecture

The overall IPSec architecture is shown as follows.

Figure 86 IPSec Architecture



11.2.1 IPSec Algorithms

The **ESP** (Encapsulating Security Payload) Protocol (RFC 2406) and **AH** (Authentication Header) protocol (RFC 2402) describe the packet formats and the default standards for packet structure (including implementation algorithms).

The Encryption Algorithm describes the use of encryption techniques such as DES (Data Encryption Standard), AES (Advanced Encryption Standard) and Triple DES algorithms.

The Authentication Algorithms, HMAC-MD5 (RFC 2403) and HMAC-SHA-1 (RFC 2404, provide an authentication mechanism for the **AH** and **ESP** protocols. Refer to IPSec Algorithms on page 170 for more information.

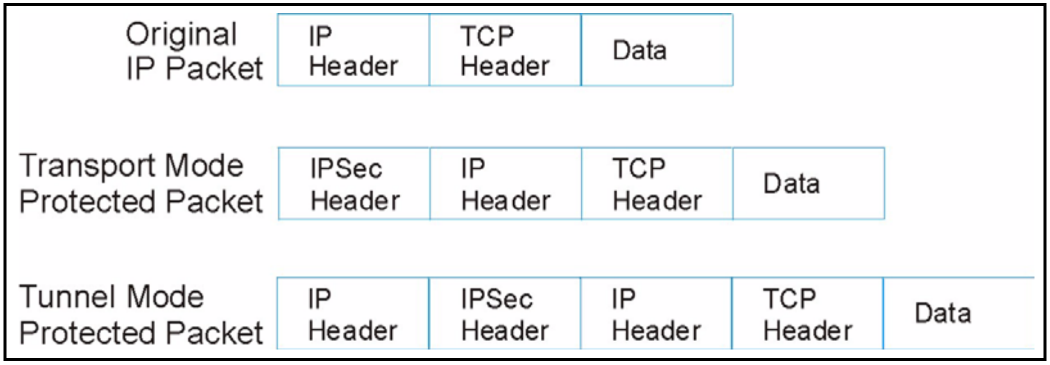
11.2.2 Key Management

Key management allows you to determine whether to use IKE (ISAKMP) or manual key configuration in order to set up a VPN.

11.3 Encapsulation

The two modes of operation for IPSec VPNs are **Transport** mode and **Tunnel** mode.

Figure 87 Transport and Tunnel Mode IPSec Encapsulation



11.3.1 Transport Mode

Transport mode is used to protect upper layer protocols and only affects the data in the IP packet. In **Transport** mode, the IP packet contains the security protocol (**AH** or **ESP**) located after the original IP header and options, but before any upper layer protocols contained in the packet (such as TCP and UDP).

With **ESP,** protection is applied only to the upper layer protocols contained in the packet. The IP header information and options are not used in the authentication process. Therefore, the originating IP address cannot be verified for integrity against the data.

With the use of **AH** as the security protocol, protection is extended forward into the IP header to verify the integrity of the entire packet by use of portions of the original IP header in the hashing process.

11.3.2 Tunnel Mode

Tunnel mode encapsulates the entire IP packet to transmit it securely. A **Tunnel** mode is required for gateway services to provide access to internal systems. **Tunnel** mode is fundamentally an IP tunnel with authentication and encryption. This is the most common mode of operation. **Tunnel** mode is required for gateway to gateway and host to gateway communications. **Tunnel** mode communications have two sets of IP headers:

- **Outside header**: The outside IP header contains the destination IP address of the VPN gateway.
- **Inside header**: The inside IP header contains the destination IP address of the final system behind the VPN gateway. The security protocol appears after the outer IP header and before the inside IP header.

11.4 IPSec and NAT

Read this section if you are running IPSec on a host computer behind the ZyWALL.

NAT is incompatible with the **AH** protocol in both **Transport** and **Tunnel** mode. An IPSec VPN using the **AH** protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet. When using **AH** protocol, packet contents (the data payload) are not encrypted.

A NAT device in between the IPSec endpoints will rewrite either the source or destination address with one of its own choosing. The VPN device at the receiving end will verify the integrity of the incoming packet by computing its own hash value, and complain that the hash value appended to the received packet doesn't match. The VPN device at the receiving end doesn't know about the NAT in the middle, so it assumes that the data has been maliciously altered.

IPSec using **ESP** in **Tunnel** mode encapsulates the entire original packet (including headers) in a new IP packet. The new IP packet's source address is the outbound address of the sending VPN gateway, and its destination address is the inbound address of the VPN device at the receiving end. When using **ESP** protocol with authentication, the packet contents (in this case, the entire original packet) are encrypted. The encrypted contents, but not the new headers, are signed with a hash value appended to the packet.

Tunnel mode **ESP** with authentication is compatible with NAT because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device. **Transport** mode **ESP** with authentication is not compatible with NAT, although NAT traversal provides a way to use **Transport** mode **ESP** when there is a NAT router between the IPSec endpoints (See NAT Traversal on page 174 for details).

Table 56 VPN and NAT

SECURITY PROTOCOL	MODE	NAT
AH	Transport	N
AH	Tunnel	N
ESP	Transport	N
ESP	Tunnel	Y

11.5 IPSec Algorithms

The **ESP** and **AH** protocols are necessary to create a Security Association (SA), the foundation of an IPSec VPN. An SA is built from the authentication provided by the **AH** and **ESP** protocols. The primary function of key management is to establish and maintain the SA between systems. Once the SA is established, the transport of data may commence.

11.5.1 AH (Authentication Header) Protocol

AH protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the **ESP** was designed.

In applications where confidentiality is not required or not sanctioned by government encryption restrictions, an **AH** can be employed to ensure integrity. This type of implementation does not protect the information from dissemination but will allow for verification of the integrity of the information and authentication of the originator.

11.5.2 ESP (Encapsulating Security Payload) Protocol

The **ESP** protocol (RFC 2406) provides encryption as well as some of the services offered by **AH**. **ESP** authenticating properties are limited compared to the **AH** due to the non-inclusion of the IP header information during the authentication process. However, **ESP** is sufficient if only the upper layer protocols need to be authenticated.

An added feature of the **ESP** is payload padding, which further protects communications by concealing the size of the packet being transmitted.

Table 57 AH and ESP

		AH
Encryption	**DES** (default) Data Encryption Standard (DES) is a widely used method of data encryption using a secret key. DES applies a 56-bit key to each 64-bit block of data.	
	3DES Triple DES (3DES) is a variant of DES, which iterates three times with three separate keys (3 x 56 = 168 bits), effectively doubling the strength of DES.	
	AES Advanced Encryption Standard is a newer method of data encryption that also uses a secret key. This implementation of AES applies a 128-bit key to 128-bit blocks of data. AES is faster than 3DES.	
	Select **NULL** to set up a phase 2 tunnel without encryption.	
Authentication	**MD5** (default) MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.	**MD5** (default) MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.
	SHA1 SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.	**SHA1** SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.
	Select **MD5** for minimal security and **SHA-1** for maximum security.	

11.5.3 Key Management

Key management allows you to determine whether to use IKE (ISAKMP) or manual key configuration in order to set up a VPN.

11.5.4 Encapsulation

The two modes of operation for IPSec VPNs are **Transport** mode and **Tunnel** mode.

11.5.4.1 Transport Mode

Transport mode is used to protect upper layer protocols and only affects the data in the IP packet. In **Transport** mode, the IP packet contains the security protocol (**AH** or **ESP**) located after the original IP header and options, but before any upper layer protocols contained in the packet (such as TCP and UDP).

With **ESP,** protection is applied only to the upper layer protocols contained in the packet. The IP header information and options are not used in the authentication process. Therefore, the originating IP address cannot be verified for integrity against the data.

With the use of **AH** as the security protocol, protection is extended forward into the IP header to verify the integrity of the entire packet by use of portions of the original IP header in the hashing process.

11.5.4.2 Tunnel Mode

Tunnel mode encapsulates the entire IP packet to transmit it securely. A **Tunnel** mode is required for gateway services to provide access to internal systems. **Tunnel** mode is fundamentally an IP tunnel with authentication and encryption. This is the most common mode of operation. **Tunnel** mode is required for gateway to gateway and host to gateway communications. **Tunnel** mode communications have two sets of IP headers:

- **Outside header**: The outside IP header contains the destination IP address of the VPN gateway.
- **Inside header**: The inside IP header contains the destination IP address of the final system behind the VPN gateway. The security protocol appears after the outer IP header and before the inside IP header.

11.5.5 IPSec and NAT

This section applies to computers running IPSec behind the ZyXEL device.

NAT is incompatible with the **AH** protocol in both **Transport** and **Tunnel** mode. An IPSec VPN using the **AH** protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet. When using **AH** protocol, packet contents (the data payload) are not encrypted.

A NAT device in between the IPSec endpoints will rewrite either the source or destination address with one of its own choosing. The VPN device at the receiving end will verify the integrity of the incoming packet by computing its own hash value, and complain that the hash value appended to the received packet doesn't match. The VPN device at the receiving end doesn't know about the NAT in the middle, so it assumes that the data has been maliciously altered.

IPSec using **ESP** in **Tunnel** mode encapsulates the entire original packet (including headers) in a new IP packet. The new IP packet's source address is the outbound address of the sending VPN gateway, and its destination address is the inbound address of the VPN device at the receiving end. When using **ESP** protocol with authentication, the packet contents (in this case, the entire original packet) are encrypted. The encrypted contents, but not the new headers, are signed with a hash value appended to the packet.

Tunnel mode **ESP** with authentication is compatible with NAT because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device. **Transport** mode **ESP** with authentication is not compatible with NAT, although NAT traversal provides a way to use **Transport** mode **ESP** when there is a NAT router between the IPSec endpoints.

Table 58 VPN and NAT

SECURITY PROTOCOL	MODE	NAT
AH	Transport	No
AH	Tunnel	No
ESP	Transport	No
ESP	Tunnel	Yes

11.6 My ZyWALL

My ZyWALL identifies the WAN IP address or domain name of the ZyWALL (if it has one) or leave the field set to **0.0.0.0**. The ZyWALL has to rebuild the VPN tunnel if the **My ZyWALL** IP address changes after setup.

11.7 Remote Gateway Address

Remote Gateway Address is the WAN IP address or domain name of the remote IPSec router (secure gateway).

If the remote secure gateway has a static WAN IP address, enter it in the **Remote Gateway Address** field. You may alternatively enter the remote secure gateway's domain name (if it has one).

You can also enter a remote secure gateway's domain name in the **Remote Gateway Address** field if the remote secure gateway has a dynamic WAN IP address and is using DDNS. The ZyWALL has to rebuild the VPN tunnel each time the remote secure gateway's WAN IP address changes (there may be a delay until the DDNS servers are updated with the remote gateway's new WAN IP address).

11.7.1 Dynamic Remote Gateway Address

If the remote secure gateway has a dynamic WAN IP address and does not use DDNS, enter 0.0.0.0 as the remote gateway's address. In this case only the remote secure gateway can initiate SAs. This may be useful for telecommuters initiating a VPN tunnel to the company network. See Telecommuter VPN/IPSec Examples on page 207 for configuration examples.

Note: The **Remote Gateway Address** may be configured as **0.0.0.0** only when using **IKE** key management and not **Manual** key management.

11.7.2 Keep Alive/Nailed Up

When you initiate an IPSec tunnel with keep alive enabled, the ZyXEL device automatically renegotiates the tunnel when the IPSec SA lifetime period expires. In effect, the IPSec tunnel becomes an always on connection after you initiate it. Both IPSec routers must have a ZyXEL device-compatible keep alive feature enabled in order for this feature to work.

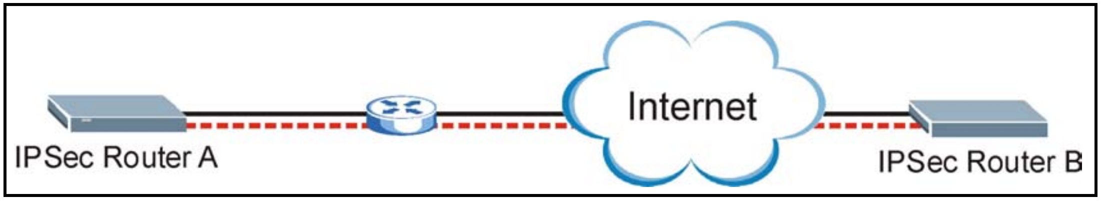
If the ZyXEL device has its maximum number of simultaneous IPSec tunnels connected to it and they all have keep alive enabled, then no other tunnels can take a turn connecting to the ZyXEL device because the ZyXEL device never drops the tunnels that are already connected.

Note: When there is outbound traffic with no inbound traffic, the ZyXEL device automatically drops the tunnel after two minutes.

11.8 NAT Traversal

NAT traversal allows you to set up a VPN connection when there are NAT routers between the two IPSec routers.

Figure 88 NAT Router Between IPSec Routers



Normally you cannot set up a VPN connection with a NAT router between the two IPSec routers because the NAT router changes the header of the IPSec packet. In the previous figure, IPSec router A sends an IPSec packet in an attempt to initiate a VPN. The NAT router changes the IPSec packet's header so it does not match the header for which IPSec router B is checking. Therefore, IPSec router B does not respond and the VPN connection cannot be built.

NAT traversal solves the problem by adding a UDP port 500 header to the IPSec packet. The NAT router forwards the IPSec packet with the UDP port 500 header unchanged. IPSec router B checks the UDP port 500 header and responds. IPSec routers A and B build a VPN connection.

11.8.1 NAT Traversal Configuration

For NAT traversal to work you must:

- Use ESP security protocol (in either transport or tunnel mode).
- Use IKE keying mode.
- Enable NAT traversal on both IPSec endpoints.

In order for IPSec router A (see Figure 88 on page 175) to receive an initiating IPSec packet from IPSec router B, set the NAT router to forward UDP port 500 to IPSec router A.

11.9 ID Type and Content

With aggressive negotiation mode, the ZyXEL device identifies incoming SAs by ID type and content since this identifying information is not encrypted. This enables the ZyXEL device to distinguish between multiple rules for SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. Telecommuters can use separate passwords to simultaneously connect to the ZyXEL device from IPSec routers with dynamic IP addresses.

Note: Regardless of the ID type and content configuration, the ZyXEL device does not allow you to save multiple active rules with overlapping local and remote IP addresses.

With main mode, the ID type and content are encrypted to provide identity protection. In this case the ZyXEL device can only distinguish between up to 12 different incoming SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. The ZyXEL device can distinguish up to 12 incoming SAs because you can select between three encryption algorithms (DES, 3DES and AES), two authentication algorithms (MD5 and SHA1) and two key groups (DH1 and DH2) when you configure a VPN rule. The ID type and content act as an extra level of identification for incoming SAs.

The type of ID can be a domain name, an IP address or an e-mail address. The content is the IP address, domain name, or e-mail address.

Table 59 Local ID Type and Content Fields

LOCAL ID TYPE	CONTENT
IP	Type the IP address of your computer or leave the field blank to have the ZyXEL device automatically use its own IP address.
DNS	Type a domain name (up to 31 characters) by which to identify this ZyXEL device.
E-mail	Type an e-mail address (up to 31 characters) by which to identify this ZyXEL device.
The domain name or e-mail address that you use in the **Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address.	

Table 60 Peer ID Type and Content Fields

PEER ID TYPE	CONTENT
IP	Type the IP address of the computer with which you will make the VPN connection or leave the field blank to have the ZyXEL device automatically use the address in the **Secure Gateway** or **Remote Gateway Address** field.
DNS	Type a domain name (up to 31 characters) by which to identify the remote IPSec router.
E-mail	Type an e-mail address (up to 31 characters) by which to identify the remote IPSec router.
Subject Name	Type the subject name (up to 255 characters) by which to identify the remote IPSec router. This option is available only when you set **Authentication Key** to **Certificate**.
The domain name or e-mail address that you use in the **Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address. The domain name also does not have to match the remote router’s IP address or what you configure in the **Secure Gateway** or **Remote Gateway Address** field.	

11.9.1 ID Type and Content Examples

Two IPSec routers must have matching ID type and content configuration in order to set up a VPN tunnel.

The two ZyWALLs in this example can complete negotiation and establish a VPN tunnel.

Table 61 Matching ID Type and Content Configuration Example

ZYWALL A	ZYWALL B
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2
Peer ID type: IP	Peer ID type: E-mail
Peer ID content: 1.1.1.2	Peer ID content: tom@yourcompany.com

The two ZyWALLs in this example cannot complete their negotiation because ZyWALL B’s **Local ID type** is **IP**, but ZyWALL A’s **Peer ID type** is set to **E-mail**. An ID mismatched message displays in the IPSec log.

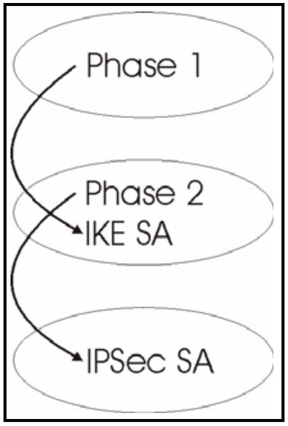
Table 62 Mismatching ID Type and Content Configuration Example

ZYWALL A	ZYWALL B
Local ID type: IP	Local ID type: IP
Local ID content: 1.1.1.10	Local ID content: 1.1.1.10
Peer ID type: E-mail	Peer ID type: IP
Peer ID content: aa@yahoo.com	Peer ID content: N/A

11.9.2 IKE Phases

There are two phases to every IKE (Internet Key Exchange) negotiation – phase 1 (Authentication) and phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA and the second one uses that SA to negotiate SAs for IPSec.

Figure 89 Two Phases to Set Up the IPSec SA



In phase 1 you must:

- Choose a negotiation mode.
- Authenticate the connection by entering a pre-shared key.

- Choose an encryption algorithm.
- Choose an authentication algorithm.
- Choose a Diffie-Hellman public-key cryptography key group (**DH1** or **DH2**).
- Set the IKE SA lifetime. This field allows you to determine how long an IKE SA should stay up before it times out. An IKE SA times out when the IKE SA lifetime period expires. If an IKE SA times out when an IPSec SA is already established, the IPSec SA stays connected.

In phase 2 you must:

- Choose which protocol to use (**ESP** or **AH**) for the IKE key exchange.
- Choose an encryption algorithm.
- Choose an authentication algorithm
- Choose whether to enable Perfect Forward Secrecy (PFS) using Diffie-Hellman public-key cryptography. Select **None** (the default) to disable PFS.
- Choose **Tunnel** mode or **Transport** mode.
- Set the IPSec SA lifetime. This field allows you to determine how long the IPSec SA should stay up before it times out. The ZyXEL device automatically renegotiates the IPSec SA if there is traffic when the IPSec SA lifetime period expires. The ZyXEL device also automatically renegotiates the IPSec SA if both IPSec routers have keep alive enabled, even if there is no traffic. If an IPSec SA times out, then the IPSec router must renegotiate the SA the next time someone attempts to send traffic.

11.9.3 Negotiation Mode

The phase 1 **Negotiation Mode** you select determines how the Security Association (SA) will be established for each connection through IKE negotiations.

- **Main Mode** ensures the highest level of security when the communicating parties are negotiating authentication (phase 1). It uses 6 messages in three round trips: SA negotiation, Diffie-Hellman exchange and an exchange of nonces (a nonce is a random number). This mode features identity protection (your identity is not revealed in the negotiation).
- **Aggressive Mode** is quicker than **Main Mode** because it eliminates several steps when the communicating parties are negotiating authentication (phase 1). However the trade-off is that faster speed limits its negotiating power and it also does not provide identity protection. It is useful in remote access situations where the address of the initiator is not know by the responder and both parties want to use pre-shared key authentication.

11.9.4 Pre-Shared Key

A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called pre-shared because you have to share it with another party before you can communicate with them over a secure connection.

11.9.5 Diffie-Hellman (DH) Key Groups

Diffie-Hellman (DH) is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communications channel. Diffie-Hellman is used within IKE SA setup to establish session keys. 768-bit (Group 1 - **DH1**) and 1024-bit (Group 2 – **DH2**) Diffie-Hellman groups are supported. Upon completion of the Diffie-Hellman exchange, the two peers have a shared secret, but the IKE SA is not authenticated. For authentication, use pre-shared keys.

11.9.6 Perfect Forward Secrecy (PFS)

Enabling PFS means that the key is transient. The key is thrown away and replaced by a brand new key using a new Diffie-Hellman exchange for each new IPSec SA setup. With PFS enabled, if one key is compromised, previous and subsequent keys are not compromised, because subsequent keys are not derived from previous keys. The (time-consuming) Diffie-Hellman exchange is the trade-off for this extra security.

This may be unnecessary for data that does not require such security, so PFS is disabled (**None**) by default in the ZyXEL device. Disabling PFS means new authentication and encryption keys are derived from the same root secret (which may have security implications in the long run) but allows faster SA setup (by bypassing the Diffie-Hellman key exchange).

11.10 X-Auth (Extended Authentication)

Extended authentication provides added security by allowing you to use usernames and passwords for VPN connections. This is especially helpful when multiple ZyWALLs use one VPN rule to connect to a single ZyWALL. An attacker cannot make a VPN connection without a valid username and password.

The extended authentication server checks the user names and passwords of the extended authentication clients before completing the IPSec connection.

A ZyWALL can be an extended authentication server for some VPN connections and an extended authentication client for other VPN connections.

11.10.1 Authentication Server

A ZyWALL set to be a VPN extended authentication server can use either the local user database internal to the ZyWALL or an external RADIUS server for an unlimited number of users. The ZyWALL uses the same local user database for VPN extended authentication and wireless LAN security.

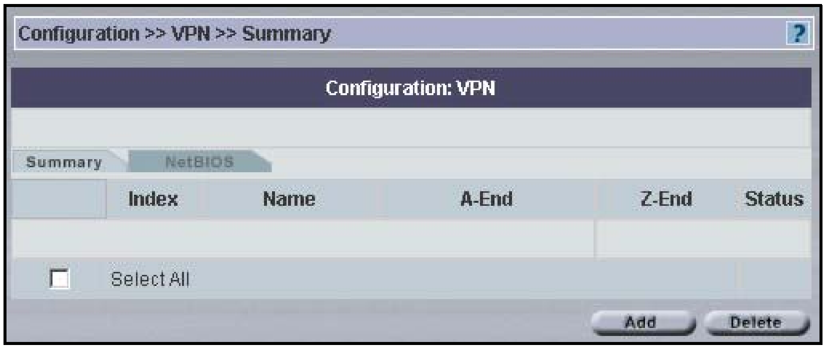
11.11 VPN Screens

Screens for VPN version 1.0 and VPN version 1.1 are explained in the following sections. The type of VPN configuration screens that display depend on the device you select.

11.12 VPN Tunnel Summary (VPN version 1.0)

Select a device and then click **Configuration** > **VPN**.

Figure 90 Configuration > VPN



The following table describes the labels in this screen.

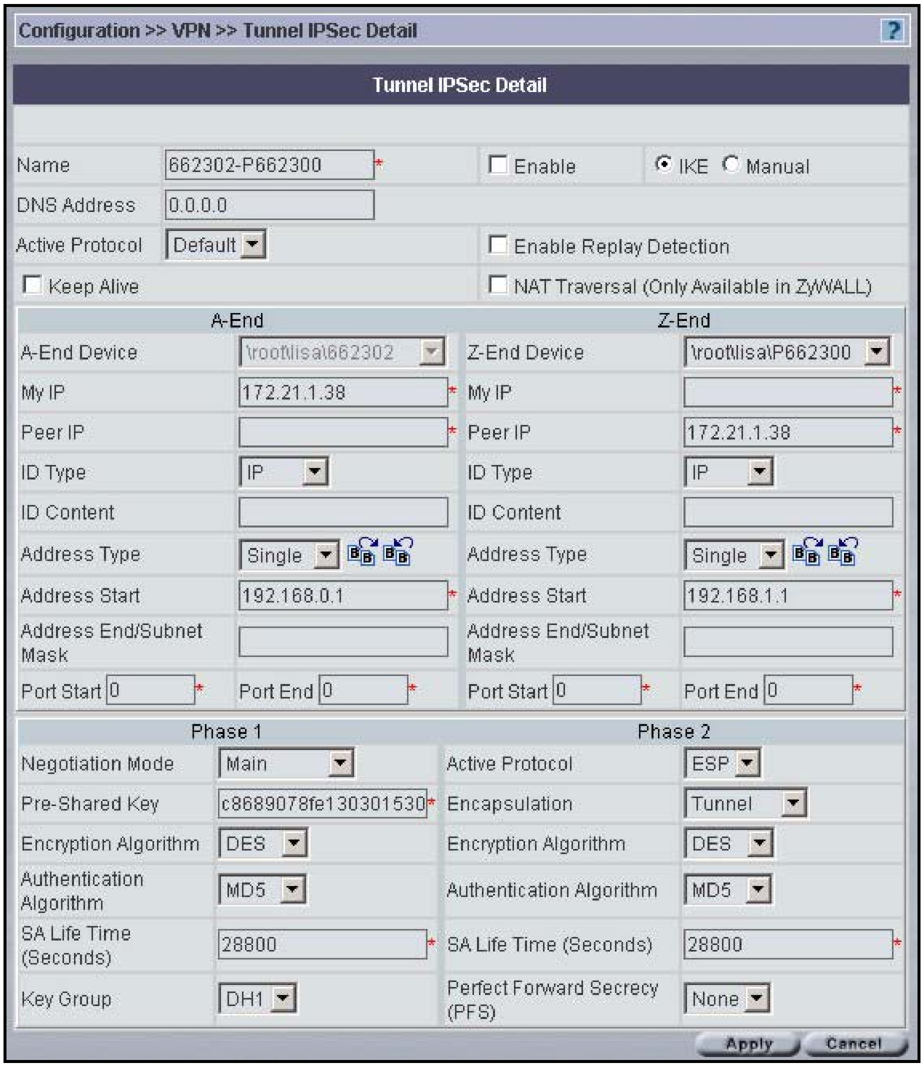
Table 63 Configuration > VPN

	DESCRIPTION
Index	This is the VPN policy index number.
Name	This field displays the identification name for this VPN policy.
A-End/Z-End	For the Vantage manager there is no local or remote. A-End and Z-End are the end devices where the VPN tunnel terminates. These fields display the device administrators at both ends of a VPN tunnel respectively. **Note:** If one end of the tunnel cannot be managed (the device exists in another administrators domain and cannot be seen), **Unknown-ZyXEL-Device** is displayed in this field. If you configure a Single-Side-VPN tunnel then a Non-ZyXEL-Device is supported at the Z-End.
Status	This field displays whether the VPN tunnel is active or not.
Add	Click **Add** to create a new VPN tunnel or to modify an existing one.
Delete	Select a rule and then click **Delete** to erase it. All rules can be deleted if you check the **Select All** checkbox and click **Delete**.

11.12.1 Add a VPN Tunnel

You can create a single-ended VPN tunnel using Vantage by selecting **N/A** from the **Remote Device** field. This allows you to create a VPN tunnel between a ZyXEL device and another IPSec router. You must make sure the remote IPSec router VPN settings correspond to the ZyXEL device VPN settings.

Figure 91 Configuration > VPN > Tunnel IPSec Detail



Configuration >> VPN >> Tunnel IPSec Detail

Tunnel IPSec Detail

Name	662302-P662300 *	□ Enable	● IKE ○ Manual
DNS Address	0.0.0.0		
Active Protocol	Default	□ Enable Replay Detection	
□ Keep Alive		□ NAT Traversal (Only Available in ZyWALL)	

A-End		Z-End	
A-End Device	\root\lisa\662302	Z-End Device	\root\lisa\P662300
My IP	172.21.1.38 *	My IP	*
Peer IP	*	Peer IP	172.21.1.38 *
ID Type	IP	ID Type	IP
ID Content		ID Content	
Address Type	Single	Address Type	Single
Address Start	192.168.0.1 *	Address Start	192.168.1.1 *
Address End/Subnet Mask		Address End/Subnet Mask	
Port Start 0 *	Port End 0 *	Port Start 0 *	Port End 0 *

Phase 1		Phase 2	
Negotiation Mode	Main	Active Protocol	ESP
Pre-Shared Key	c8689078fe130301530 *	Encapsulation	Tunnel
Encryption Algorithm	DES	Encryption Algorithm	DES
Authentication Algorithm	MD5	Authentication Algorithm	MD5
SA Life Time (Seconds)	28800 *	SA Life Time (Seconds)	28800 *
Key Group	DH1	Perfect Forward Secrecy (PFS)	None

The following table describes the labels in this screen.

Table 64 Configuration > VPN > Tunnel IPSec Detail

LABEL	DESCRIPTION
Name	This is a VPN name for identification purposes.
Enable	Select this checkbox to make the VPN rule active.

Table 64 Configuration > VPN > Tunnel IPSec Detail (continued)

LABEL	DESCRIPTION
IKE/Manual	Select either **IKE** or **Manual** to manage encryption keys. If you select the **IKE** method, you must configure the IKE fields. **Manual** is useful for troubleshooting if you have problems using **IKE** key management.
DNS Address	Type a domain name (up to 31 characters) by which to identify the local or remote IPSec router.
Active Protocol	The **ESP** and **AH** protocols are necessary to create a Security Association (SA), the foundation of an IPSec VPN. **AH** protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the **ESP** was designed. The **ESP** protocol (RFC 2406) provides encryption as well as some of the services offered by **AH**. **ESP** authenticating properties are limited compared to the **AH** due to the non-inclusion of the IP header information during the authentication process.
Enable Replay Detection	
Keep Alive	When you initiate an IPSec tunnel with keep alive enabled, the ZyXEL device automatically renegotiates the tunnel when the IPSec SA lifetime period expires. In effect, the IPSec tunnel becomes an always on connection after you initiate it. Both IPSec routers must have a ZyXEL device-compatible keep alive feature enabled in order for this feature to work. If the ZyXEL device has its maximum number of simultaneous IPSec tunnels connected to it and they all have keep alive enabled, then no other tunnels can take a turn connecting to the ZyXEL device because the ZyXEL
A-End/Z-End	
NAT Traversal (Only Available in ZyWALL)	Select this check box to enable NAT traversal. NAT traversal allows you to set up a VPN connection when there are NAT routers between the two IPSec routers. The remote IPSec router must also have NAT traversal enabled. You can use NAT traversal with ESP protocol using Transport or Tunnel mode, but not with AH protocol nor with manual key management. In order for an IPSec router behind a NAT router to receive an initiating IPSec packet, set the NAT router to forward UDP port 500 to the IPSec router behind the NAT router.
A-End/Z-End Device	Select the name of the ZyXEL device from the pull-down list.
My IP	This is the IP address of the local and remote computer(s) of the VPN tunnel.
Peer IP	Type the IP address of the computer with which you will make the VPN connection or leave the field blank to have the ZyXEL device automatically use the address in the **Secure Gateway** field.
ID Type	Select **IP** to identify this ZyXEL device by its IP address. Select **DNS** to identify this ZyXEL device by a domain name. Select **E-mail** to identify this ZyXEL device by an e-mail address. You do not configure the local ID type and content when you set **Authentication Method** to **Certificate**. The ZyXEL device takes them from the certificate you select.

Table 64 Configuration > VPN > Tunnel IPSec Detail (continued)

LABEL	DESCRIPTION
ID Content	When you select **IP** in the **Local ID Type** field, type the IP address of your computer. The ZyXEL device uses the IP address in the **My IP Address** field if you configure the local **Content** field to **0.0.0.0** or leave it blank. It is recommended that you type an IP address other than **0.0.0.0** in the local **Content** field or use the **DNS** or **E-mail** ID type in the following situations. ➢ When there is a NAT router between the two IPSec routers. ➢ When you want the remote IPSec router to be able to distinguish between VPN connection requests that come in from IPSec routers with dynamic WAN IP addresses. ➢ With **DNS** or **E-mail** in the **Local ID Type** field, type a domain name or e-mail address by which to identify this ZyXEL device. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string.
Address Type	This is the IP address(es) of computer(s) the A-end or Z-end of the VPN tunnel. The same (static) IP address is displayed twice in the **Address Start** and **Address End** fields when the **Address Type** field is configured to **Single**. The beginning and ending (static) IP addresses, in a range of computers are displayed when the **Address Type** is configured to **Range**. A (static) IP address and a subnet mask are displayed when the **Address** Type field is configured to Subnet. These addresses cannot be automatically generated by Vantage.
Address Start	Enter the beginning IP address of the computers behind the ZyXEL device.
Address End	Enter the ending IP address of the computers behind the ZyXEL device.
Port Start	**0** is the default and signifies any port. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3 Type a port number from 0 to 65535 for the starting port in a range.
Port End	Type the same port number as above to specify a single port. Type a port number greater than the start port number to specify the end port in a port range.
Phase 1	There are two phases to every IKE (Internet Key Exchange) negotiation – phase 1 (Authentication) and phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA and the second one uses that SA to negotiate SAs for IPSec.
Negotiation Mode	Select either **Main** or **Aggressive**. Aggressive mode is quicker than Main mode because it eliminates several steps when the communicating parties are negotiating authentication (phase 1). However the trade-off is that faster speed limits its negotiating power and it also does not provide identity protection. It is useful in remote access situations where the address of the initiator is not know by the responder and both parties want to use pre-shared key authentication.

Table 64 Configuration > VPN > Tunnel IPSec Detail (continued)

LABEL	DESCRIPTION
Pre-Shared key	A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called pre-shared because you have to share it with another party before you can communicate with them over a secure connection. ZyXEL gateways authenticate an IKE VPN session by matching pre-shared keys. Enter from 8 up to 31 characters. Any character may be used, including spaces, but trailing spaces are truncated. Multiple SAs connecting through a secure gateway must have the same pre-shared key.
Encryption Algorithm	Select an encryption algorithm from the pull-down menu. You can select either **DES** or **3DES**. **3DES** is more powerful but increases latency.
Authentication Algorithm	The Authentication Algorithms, HMAC-MD5 (RFC 2403) and HMAC-SHA-1 (RFC 2404, provide an authentication mechanism for the AH and ESP protocols. Select **MD5** for minimal security and **SHA-1** for maximum security. **MD5** (Message Digest 5) produces a 128-bit digest to authenticate packet data. **SHA-1** (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.
SA Life Time (Seconds)	Define the length of time before an IKE Security Association automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days). A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Key Group	Diffie-Hellman (DH) is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communications channel. Diffie-Hellman is used within IKE SA setup to establish session keys. 768-bit (Group 1 - DH1) and 1024-bit (Group 2 - DH2) Diffie-Hellman groups are supported. Upon completion of the Diffie-Hellman exchange, the two peers have a shared secret, but the IKE SA is not authenticated. For authentication, use pre-shared keys.
Phase 2	There are two phases to every IKE (Internet Key Exchange) negotiation – phase 1 (Authentication) and phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA and the second one uses that SA to negotiate SAs for IPSec.
Active Protocol	The **ESP** and **AH** protocols are necessary to create a Security Association (SA), the foundation of an IPSec VPN. **AH** protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the **ESP** was designed. The **ESP** protocol (RFC 2406) provides encryption as well as some of the services offered by **AH**. **ESP** authenticating properties are limited compared to the **AH** due to the non-inclusion of the IP header information during the authentication process.

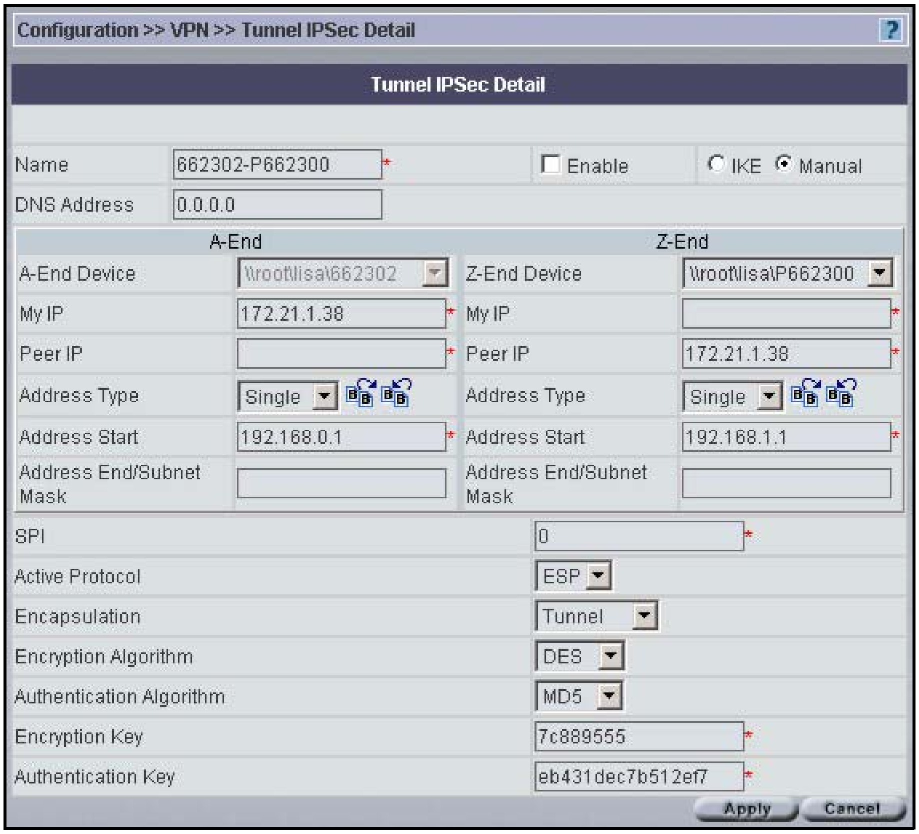
Table 64 Configuration > VPN > Tunnel IPSec Detail (continued)

LABEL	DESCRIPTION
Encapsulation	In **Transport** mode, the IP packet contains the security protocol (**AH** or **ESP**) located after the original IP header and options, but before any upper layer protocols contained in the packet (such as TCP and UDP). With ESP, protection is applied only to the upper layer protocols contained in the packet. The IP header information and options are not used in the authentication process. Therefore, the originating IP address cannot be verified for integrity against the data. With the use of **AH** as the security protocol, protection is extended forward into the IP header to verify the integrity of the entire packet by use of portions of the original IP header in the hashing process. **Tunnel** mode encapsulates the entire IP packet to transmit it securely. **Tunnel** mode is required for gateway services to provide access to internal systems. **Tunnel** mode is fundamentally an IP tunnel with authentication and encryption. This is the most common mode of operation
Encryption Algorithm	Select an encryption algorithm from the pull-down menu. You can select either **DES** or **3DES**. **3DES** is more powerful but increases latency.
Authentication Algorithm	The Authentication Algorithms, HMAC-MD5 (RFC 2403) and HMAC-SHA-1 (RFC 2404, provide an authentication mechanism for the **AH** and **ESP** protocols. Select **MD5** for minimal security and **SHA-1** for maximum security. **MD5** (Message Digest 5) produces a 128-bit digest to authenticate packet data. **SHA-1** (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.
SA Life Time (Seconds)	Define the length of time before an IKE Security Association automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days). A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Perfect Forward Secrecy (PFS)	Choose whether to enable Perfect Forward Secrecy (**PFS**) using Diffie-Hellman public-key cryptography. Enabling **PFS** means that the key is transient. A brand new key using a new Diffie-Hellman exchange replaces the key for each new IPSec SA. With PFS enabled, if one key is compromised, previous and subsequent keys are not compromised, because subsequent keys are not derived from previous keys. The (time-consuming) Diffie-Hellman exchange is the trade-off for this extra security. Disabling PFS means new authentication and encryption keys are derived from the same root secret (which may have security implications in the long run) but allows faster SA setup (by bypassing the Diffie-Hellman key exchange).
Apply	Click **Apply** to apply your changes in this screen.
Cancel	Click **Cancel** to close this screen without applying any changes.

11.12.2 Manual VPN Tunnel

Select **Manual** from Figure 91 on page 181 to proceed to the next screen.

Figure 92 Configuration > VPN > Manual Tunnel IPSec Detail



Configuration >> VPN >> Tunnel IPSec Detail

Tunnel IPSec Detail

Name	662302-P662300 *	□ Enable	○ IKE ● Manual
DNS Address	0.0.0.0		

A-End		Z-End	
A-End Device	\\root\lisa\662302	Z-End Device	\\root\lisa\P662300
My IP	172.21.1.38 *	My IP	*
Peer IP	*	Peer IP	172.21.1.38 *
Address Type	Single	Address Type	Single
Address Start	192.168.0.1 *	Address Start	192.168.1.1 *
Address End/Subnet Mask		Address End/Subnet Mask	

SPI	0 *
Active Protocol	ESP
Encapsulation	Tunnel
Encryption Algorithm	DES
Authentication Algorithm	MD5
Encryption Key	7c889555 *
Authentication Key	eb431dec7b512ef7 *

The following table describes the labels in this screen.

Table 65 Configuration > VPN >Manual Tunnel IPSec Detail

LABEL	DESCRIPTION
Name	Type up to 32 characters to identify this VPN policy. You may use any character, including spaces, but the ZyXEL device drops trailing spaces.
Enable	Select this check box to activate this VPN policy.
IKE / Manual	Select **IKE** or **Manual**. **Manual** is a useful option for troubleshooting if you have problems using **IKE** key management.
DNS Address	Type a domain name (up to 31 characters) by which to identify the local or remote IPSec router.
A-End / Z-End	Local / Remote IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
A-End / Z-End Device	Select the name of the ZyXEL device from the pull-down list.
My IP	This is the IP address of the local and remote computer(s) of the VPN tunnel.

Table 65 Configuration > VPN >Manual Tunnel IPSec Detail (continued)

LABEL	DESCRIPTION
Peer IP	Type the IP address of the computer with which you will make the VPN connection or leave the field blank to have the ZyXEL device automatically use the address in the **Secure Gateway** field.
Address Start	When the **Address Type** field is configured to **Single**, enter a (static) IP address on the LAN behind the ZyXEL device. When the **Address Type** field is configured to **Range**, enter the beginning (static) IP address, in a range of computers on the LAN behind the ZyXEL device. When the **Address Type** field is configured to **Subnet**, this is a (static) IP address on the LAN behind the ZyXEL device.
Address End	When the **Address Type** field is configured to **Single**, this field is N/A. When the **Address Type** field is configured to **Range**, enter the end (static) IP address, in a range of computers on the LAN behind the ZyXEL device. When the **Address Type** field is configured to **Subnet**, this is a subnet mask on the LAN behind the ZyXEL device.
SPI	Type a number (base 10) from 1 to 999999 for the Security Parameter Index.
Active Protocol	Select ESP if you want to use ESP (Encapsulation Security Payload). The ESP protocol (RFC 2406) provides encryption as well as some of the services offered by AH. If you select ESP here, you must select options from the **Encryption Algorithm** and **Authentication Algorithm** fields. Select **AH** if you want to use AH (Authentication Header Protocol). The AH protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the ESP was designed. If you select **AH** here, you must select options from the **Authentication Algorithm** field.
Encapsulation	Select **Tunnel** mode or **Transport** mode from the drop-down list box.
Encryption Algorithm	Select **DES**, **3DES** or **NULL** from the drop-down list box. When you use **DES** or **3DES**, both sender and receiver must know the **Encryption Key**, which can be used to encrypt and decrypt the messages. The DES encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on DES that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. Select **NULL** to set up a tunnel without encryption. When you select **NULL**, you do not enter an encryption key.
Authentication Algorithm	When you use **SHA1** or **MD5**, both sender and receiver must know the **Authentication Key**, which can be used to generate and verify a message authentication code. Select **SHA1** or **MD5** from the drop-down list box. **MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slower. Select **MD5** for minimal security and **SHA-1** for maximum security.
Encryption Key	This field only applies when you select **ESP**. With **DES**, type a unique key 8 ASCII characters long. With **3DES**, type a unique key 24 ASCII characters long. Any characters may be used, including spaces, but trailing spaces are truncated.
Authentication Key	Type a unique authentication key to be used by IPSec if applicable. Enter 16 characters for **MD5** authentication or 20 characters for **SHA-1** authentication. Any characters may be used, including spaces, but trailing spaces are truncated.

Table 65 Configuration > VPN >Manual Tunnel IPSec Detail (continued)

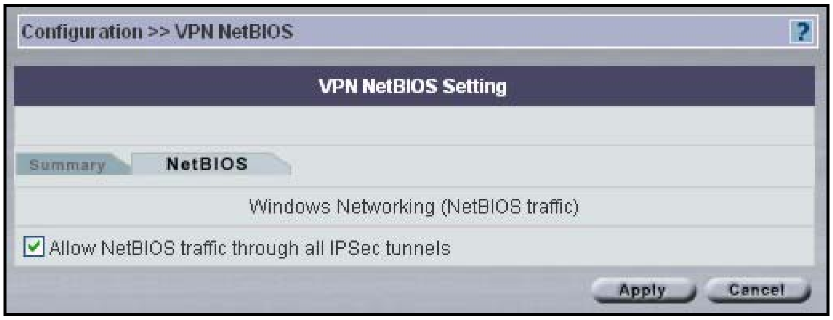
LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

11.13 VPN and NetBIOS (VPN version 1.0)

NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to find other computers. It may sometimes be necessary to allow NetBIOS packets to pass through VPN tunnels in order to allow local computers to find computers on the remote network and vice versa.

Select a device, click **Configuration > VPN** and then click the NetBIOS tab to bring up the next screen.

Figure 93 Configuration > VPN > NetBIOS



Configuration >> VPN NetBIOS

VPN NetBIOS Setting

Windows Networking (NetBIOS traffic)

☑ Allow NetBIOS traffic through all IPSec tunnels

The following table describes the labels in this screen.

Table 66 Configuration > VPN > NetBIOS

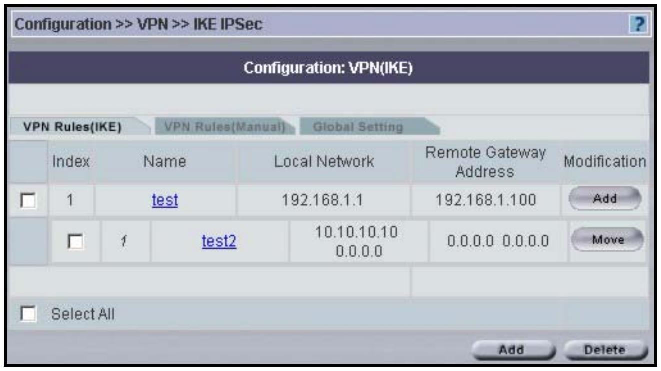
	DESCRIPTION
Windows Networking (NetBIOS traffic)	
Allow NetBIOS traffic through all IPSec tunnels	Select the check box to permit NetBIOS packets through the VPN connection.
Apply	Click **Apply** to save your changes back to the ZyXEL device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

11.14 VPN Rules (IKE) (VPN version 1.1)

Select a device and then click **Configuration** > **VPN**.

This is a read-only menu of your IPSec rule (tunnel). To add an IPSec rule (or gateway policy), click the **Add** button in the **Modification** column. Edit an IPSec rule by clicking the **Name** hyperlink to configure the associated submenus.

Figure 94 Configuration > VPN > VPN Rules (IKE)



Configuration >> VPN >> IKE IPSec

Configuration: VPN(IKE)

	Index	Name	Local Network	Remote Gateway Address	Modification
□	1	test	192.168.1.1	192.168.1.100	Add
□	1	test2	10.10.10.10 0.0.0.0	0.0.0.0 0.0.0.0	Move

□ Select All

The following table describes the labels in this screen.

Table 67 Configuration > VPN > VPN Rules (IKE)

	DESCRIPTION
Index	This field displays the VPN policy index number.
Name	This field identifies a VPN policy gateway. Click the hyperlink to go open a screen where you can edit the gateway policy.
Local Network	This field displays one or a range of IP address(es) of the computer(s) behind the ZyWALL.
Remote Gateway Address	This is the WAN IP address of the IPSec router with which you are making the VPN connection.
Modification	Click the **Add** button in this field to go to a screen where you can configure an IKE IPSec rule. Click the **Move** button to change the order in which the IPSec rules display.
Select All	Select this checkbox to select the check boxes for all VPN rules.
Add	Click the **Add** button to go to a screen where you can configure a VPN gateway policy.
Delete	Select a checkbox(es) next to a rule and click **Delete** to remove a VPN rule(s).

The following table introduces some of the general IPSec terms used in the VPN screens.

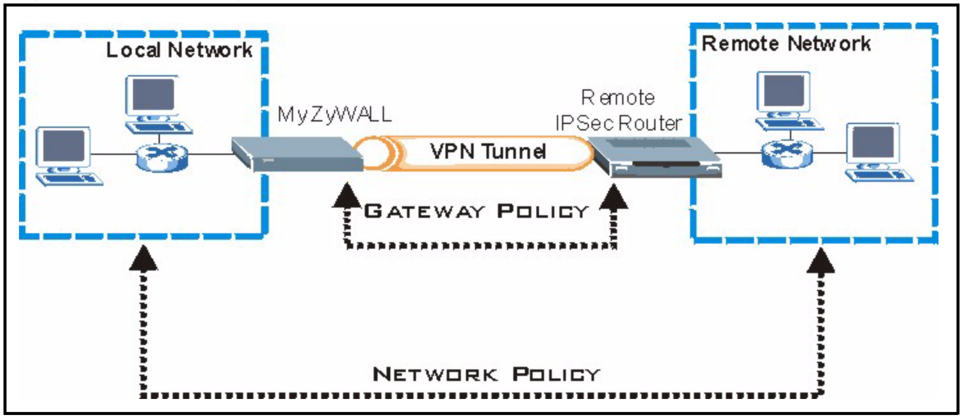
Table 68 IPSec Fields Summary

LABEL	DESCRIPTION
VPN Tunnel	A VPN (Virtual Private Network) tunnel gives you a secure connection to another computer or network.
Gateway Policy	A gateway policy identifies the IPSec routers at either end of a VPN tunnel and specifies the authentication, encryption and other settings needed to negotiate a phase 1 IKE SA.

Table 68 IPSec Fields Summary

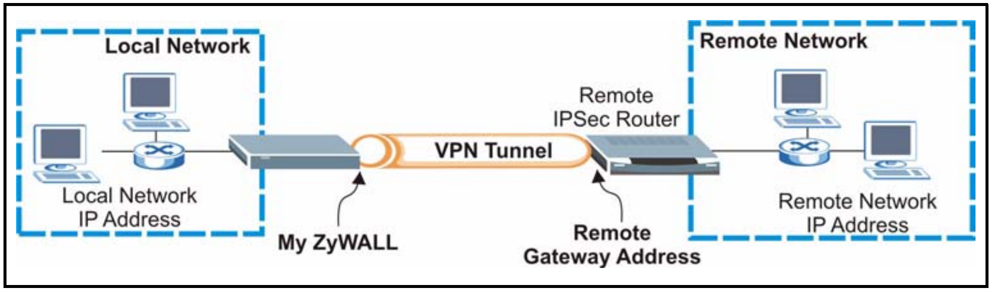
LABEL	DESCRIPTION
Network Policy	A network policy identifies the devices behind the IPSec routers at either end of a VPN tunnel and specifies the authentication, encryption and other settings needed to negotiate a phase 2 IPSec SA.
My ZyWALL	This is the ZyWALL's WAN IP address or domain name.
Local Network	This is the network behind the ZyWALL.
Remote Gateway Address	This is the WAN IP address or domain name of the IPSec router with which you're making the VPN connection.
Remote Network	This is the remote network behind the remote IPsec router.

Figure 95 Gateway and Network Policies



This figure helps explain the main fields in the VPN setup.

Figure 96 IPSec Fields Summary

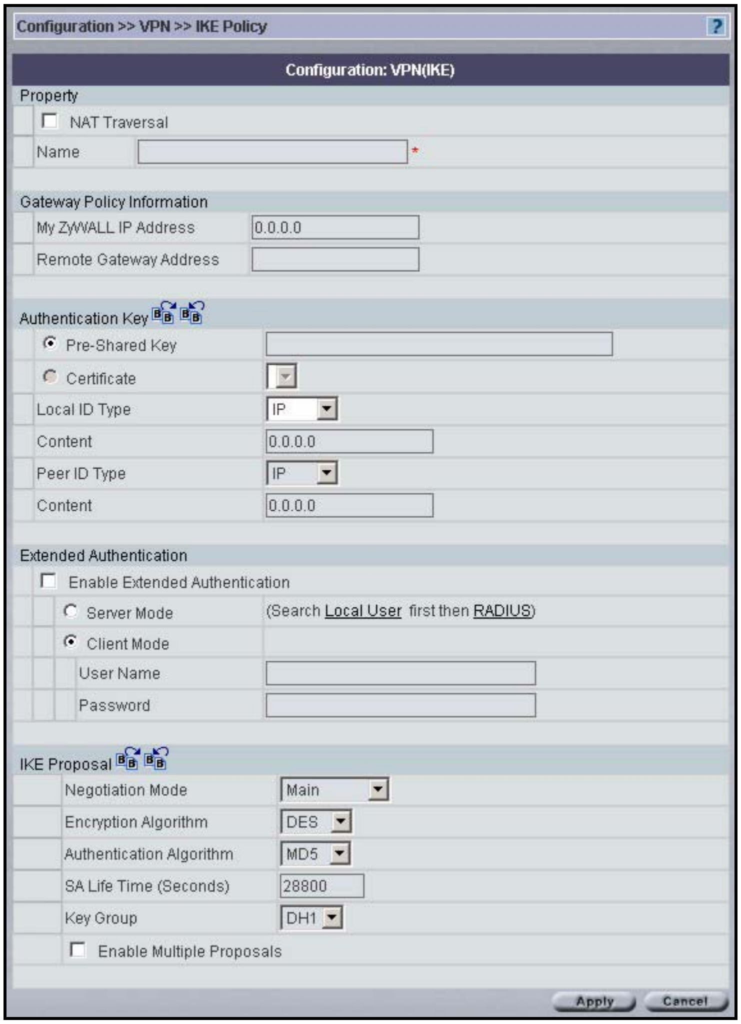


Note: Local and remote network IP addresses must be static.

11.14.1 VPN Rules (IKE) > Gateway Policy Add

In the **VPN Rule (IKE)** screen, click the **Add** button to display the **IKE Policy** screen.

Figure 97 Configuration > VPN > IKE Policy



Configuration >> VPN >> IKE Policy

Configuration: VPN(IKE)

Property

□ NAT Traversal

Name *

Gateway Policy Information

My ZyWALL IP Address: 0.0.0.0

Remote Gateway Address

Authentication Key

● Pre-Shared Key

○ Certificate

Local ID Type: IP

Content: 0.0.0.0

Peer ID Type: IP

Content: 0.0.0.0

Extended Authentication

□ Enable Extended Authentication

○ Server Mode (Search Local User first then RADIUS)

● Client Mode

User Name

Password

IKE Proposal

Negotiation Mode: Main

Encryption Algorithm: DES

Authentication Algorithm: MD5

SA Life Time (Seconds): 28800

Key Group: DH1

□ Enable Multiple Proposals

The following table describes the labels in this screen..

Table 69 Configuration > VPN > IKE Policy

LABEL	DESCRIPTION
Property	
Name	Type up to 32 characters to identify this VPN gateway policy. You may use any character, including spaces, but the ZyWALL drops trailing spaces.

Table 69 Configuration > VPN > IKE Policy (continued)

LABEL	DESCRIPTION
NAT Traversal	Select this check box to enable NAT traversal. NAT traversal allows you to set up a VPN connection when there are NAT routers between the two IPSec routers. **Note:** The remote IPSec router must also have NAT traversal enabled. You can use NAT traversal with **ESP** protocol using **Transport** or **Tunnel** mode, but not with **AH** protocol nor with manual key management. In order for an IPSec router behind a NAT router to receive an initiating IPSec packet, set the NAT router to forward UDP port 500 to the IPSec router behind the NAT router.
Gateway Policy Information	
My ZyWALL	This field identifies the WAN IP address or domain name of the ZyWALL. You can select **My Address** and enter the ZyWALL's static WAN IP address (if it has one) or leave the field set to 0.0.0.0. The following applies if the **My ZyWALL** field is configured as **0.0.0.0**: • When the WAN port operation mode is set to **Active/Passive**, the ZyWALL uses the IP address (static or dynamic) of the WAN port that is in use. • When the WAN port operation mode is set to **Active/Active**, the ZyWALL uses the IP address (static or dynamic) of the primary (highest priority) WAN port to set up the VPN tunnel as long as the corresponding WAN1 or WAN2 connection is up. If the corresponding WAN1 or WAN2 connection goes down, the ZyWALL uses the IP address of the other WAN port. • If both WAN connections go down, the ZyWALL uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect. See the chapter on WAN for details on dial backup and traffic redirect. Otherwise you can select **My Domain Name** and choose one of the dynamic domain names that you have configured (in the **DDNS** screen) to have the ZyWALL use that dynamic domain name's IP address. The VPN tunnel has to be rebuilt if the **My ZyWALL** IP address changes after setup.
Remote Gateway Address	Type the WAN IP address or the domain name (up to 31 characters) of the IPSec router with which you're making the VPN connection. Set this field to **0.0.0.0** if the remote IPSec router has a dynamic WAN IP address. In order to have more than one active rule with the **Remote Gateway Address** field set to **0.0.0.0**, the ranges of the local IP addresses cannot overlap between rules. If you configure an active rule with **0.0.0.0** in the **Remote Gateway Address** field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the **Remote Gateway Address** field set to **0.0.0.0**.
Authentication Key	

Table 69 Configuration > VPN > IKE Policy (continued)

LABEL	DESCRIPTION
Pre-Shared Key	Select the **Pre-Shared Key** radio button and type your pre-shared key in this field. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection. Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. You must precede a hexadecimal key with a "0x (zero x), which is not counted as part of the 16 to 62 character range for the key. For example, in "0x0123456789ABCDEF", 0x denotes that the key is hexadecimal and 0123456789ABCDEF is the key itself. Both ends of the VPN tunnel must use the same pre-shared key. You will receive a PYLD_MALFORMED (payload malformed) packet if the same pre-shared key is not used on both ends.
Certificate	Select the **Certificate** radio button to identify the ZyWALL by a certificate. Use the drop-down list box to select the certificate to use for this VPN tunnel. You must have certificates already configured in the **My Certificates** screen. Click **My Certificates** to go to the **My Certificates** screen where you can view the ZyWALL's list of certificates.
Local ID Type	Select **IP** to identify this ZyWALL by its IP address. Select **DNS** to identify this ZyWALL by a domain name. Select **E-mail** to identify this ZyWALL by an e-mail address. You do not configure the local ID type and content when you set **Authentication Key** to **Certificate**. The ZyWALL takes them from the certificate you select.
Content	When you select **IP** in the **Local ID Type** field, type the IP address of your computer in the local **Content** field. The ZyWALL automatically uses the IP address in the **My ZyWALL** field (refer to the **My ZyWALL** field description) if you configure the local **Content** field to **0.0.0.0** or leave it blank. It is recommended that you type an IP address other than **0.0.0.0** in the local **Content** field or use the **DNS** or **E-mail** ID type in the following situations. • When there is a NAT router between the two IPSec routers. • When you want the remote IPSec router to be able to distinguish between VPN connection requests that come in from IPSec routers with dynamic WAN IP addresses. When you select **DNS** or **E-mail** in the **Local ID Type** field, type a domain name or e-mail address by which to identify this ZyWALL in the local **Content** field. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string.

Table 69 Configuration > VPN > IKE Policy (continued)

LABEL	DESCRIPTION
Peer ID Type	Select from the following when you set **Authentication Key** to **Pre-shared Key**. • Select **IP** to identify the remote IPSec router by its IP address. • Select **DNS** to identify the remote IPSec router by a domain name. • Select **E-mail** to identify the remote IPSec router by an e-mail address. Select from the following when you set **Authentication Key** to **Certificate**. • Select **IP** to identify the remote IPSec router by the IP address in the subject alternative name field of the certificate it uses for this VPN connection. • Select **DNS** to identify the remote IPSec router by the domain name in the subject alternative name field of the certificate it uses for this VPN connection. • Select **E-mail** to identify the remote IPSec router by the e-mail address in the subject alternative name field of the certificate it uses for this VPN connection. • Select **Subject Name** to identify the remote IPSec router by the subject name of the certificate it uses for this VPN connection. • Select **Any** to have the ZyWALL not check the remote IPSec router's ID.
Content	The configuration of the peer content depends on the peer ID type. Do the following when you set **Authentication Key** to **Pre-shared Key**. • For **IP**, type the IP address of the computer with which you will make the VPN connection. If you configure this field to **0.0.0.0** or leave it blank, the ZyWALL will use the address in the **Remote Gateway Address** field (refer to the **Remote Gateway Address** field description). • For **DNS** or **E-mail**, type a domain name or e-mail address by which to identify the remote IPSec router. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string. It is recommended that you type an IP address other than **0.0.0.0** or use the **DNS** or **E-mail** ID type in the following situations: • When there is a NAT router between the two IPSec routers. • When you want the ZyWALL to distinguish between VPN connection requests that come in from remote IPSec routers with dynamic WAN IP addresses. Do the following when you set **Authentication Key** to **Certificate**. • For **IP**, type the IP address from the subject alternative name field of the certificate the remote IPSec router will use for this VPN connection. If you configure this field to **0.0.0.0** or leave it blank, the ZyWALL will use the address in the **Remote Gateway Address** field (refer to the **Remote Gateway Address** field description). • For **DNS** or **E-mail**, type the domain name or e-mail address from the subject alternative name field of the certificate the remote IPSec router will use for this VPN connection. • For **Subject Name**, type the subject name of the certificate the remote IPSec router will use for this VPN connection. Use up to255 ASCII characters including spaces. • For **Any**, the peer **Content** field is not available. • Regardless of how you configure the **ID Type** and **Content** fields, two active SAs cannot have both the local and remote IP address ranges overlap between rules.
Extended Authentication	

Table 69 Configuration > VPN > IKE Policy (continued)

LABEL	DESCRIPTION
Enable Extended Authentication	Select this check box to activate extended authentication.
Server Mode	Select **Server Mode** to have this ZyWALL authenticate extended authentication clients that request this VPN connection. You must also configure the extended authentication clients' usernames and passwords in the authentication server's local user database or a RADIUS server. Click **Local User** to go to the **Local User Database** screen where you can view and/or edit the list of user names and passwords. Click **RADIUS** to go to the **RADIUS** screen where you can configure the ZyWALL to check an external RADIUS server. During authentication, if the ZyWALL (in server mode) does not find the extended authentication clients' user name in its internal user database and an external RADIUS server has been enabled, it attempts to authenticate the client through the RADIUS server.
Client Mode	Select **Client Mode** to have your ZyWALL use a username and password when initiating this VPN connection to the extended authentication server ZyWALL. Only a VPN extended authentication client can initiate this VPN connection.
User Name	Enter a user name for your ZyWALL to be authenticated by the VPN peer (in server mode). The user name can be up to 31 case-sensitive ASCII characters, but spaces are not allowed. You must enter a user name and password when you select client mode.
Password	Enter the corresponding password for the above user name. The password can be up to 31 case-sensitive ASCII characters, but spaces are not allowed.
IKE Proposal	
Negotiation Mode	Select **Main** or **Aggressive** from the drop-down list box. Multiple SAs connecting through a secure gateway must have the same negotiation mode.
Encryption Algorithm	Select **DES**, **3DES** or **AES** from the drop-down list box. When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on DES that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of AES uses a 128-bit key. **AES** is faster than **3DES**.
Authentication Algorithm	Select **SHA1** or **MD5** from the drop-down list box. **MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slower. Select **MD5** for minimal security and **SHA-1** for maximum security.
SA Life Time (Seconds)	Define the length of time before an IKE SA automatically renegotiates in this field. It may range from 180 to 3,000,000 seconds (almost 35 days). A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Key Group	You must choose a key group for phase 1 IKE setup. **DH1** (default) refers to Diffie-Hellman Group 1 a 768 bit random number. **DH2** refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number.

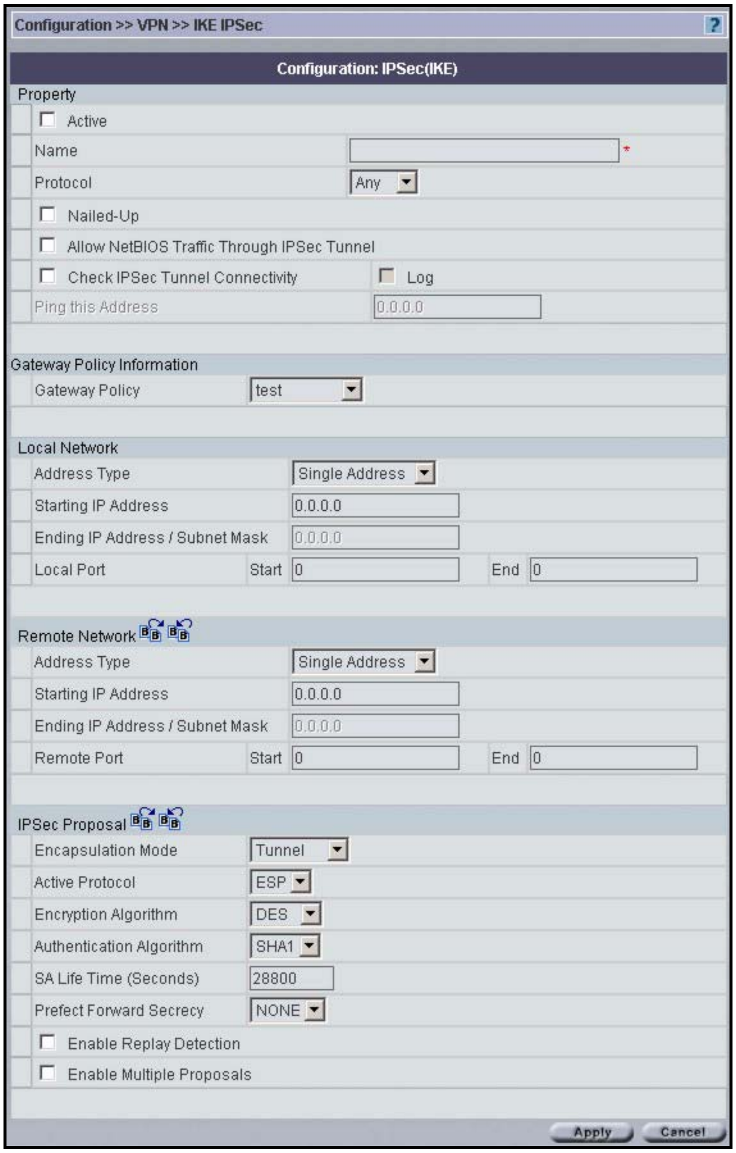
Table 69 Configuration > VPN > IKE Policy (continued)

LABEL	DESCRIPTION
Enable Multiple Proposals	Select this check box to allow the ZyWALL to use any of its phase 1 or phase 2 encryption and authentication algorithms when negotiating an IPSec SA. When you enable multiple proposals, the ZyWALL allows the remote IPSec router to select which encryption and authentication algorithms to use for the VPN tunnel, even if they are less secure than the ones you configure for the VPN rule. Clear this check box to have the ZyWALL use only the phase 1 or phase 2 encryption and authentication algorithms configured below when negotiating an IPSec SA.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving.

11.14.2 VPN Rules (IKE) > Network Policy Edit

In the **VPN Rule (IKE)** screen, click the **Add** button in the **Modification** field or a **Name** hyperlink to display the **IKE IPSec** screen.

Figure 98 Configuration > VPN > IKE IPSec



Configuration >> VPN >> IKE IPSec

Configuration: IPSec(IKE)

Property

☐ Active

Name *

Protocol: Any

☐ Nailed-Up

☐ Allow NetBIOS Traffic Through IPSec Tunnel

☐ Check IPSec Tunnel Connectivity ☐ Log

Ping this Address: 0.0.0.0

Gateway Policy Information

Gateway Policy: test

Local Network

Address Type: Single Address

Starting IP Address: 0.0.0.0

Ending IP Address / Subnet Mask: 0.0.0.0

Local Port Start: 0 End: 0

Remote Network

Address Type: Single Address

Starting IP Address: 0.0.0.0

Ending IP Address / Subnet Mask: 0.0.0.0

Remote Port Start: 0 End: 0

IPSec Proposal

Encapsulation Mode: Tunnel

Active Protocol: ESP

Encryption Algorithm: DES

Authentication Algorithm: SHA1

SA Life Time (Seconds): 28800

Prefect Forward Secrecy: NONE

☐ Enable Replay Detection

☐ Enable Multiple Proposals

The following table describes the labels in this screen.

Table 70 Configuration > VPN > IKE IPSec

LABEL	DESCRIPTION
Active	If the **Active** check box is selected, packets for the tunnel trigger the ZyWALL to build the tunnel. Clear the **Active** check box to turn the network policy off. The ZyWALL does not apply the policy. Packets for the tunnel do not trigger the tunnel. If you clear the **Active** check box while the tunnel is up (and click **Apply**), you turn off the network policy and the tunnel goes down.
Name	Type a name to identify this VPN network policy. You may use any character, including spaces, but the ZyWALL drops trailing spaces.
Protocol	Enter 1 for ICMP, 6 for TCP, 17 for UDP, etc. 0 is the default and signifies any protocol.

Table 70 Configuration > VPN > IKE IPSec (continued)

LABEL	DESCRIPTION
Nailed-Up	Select this check box to turn on the nailed up feature for this SA. Turn on nailed up to have the ZyWALL automatically reinitiate the SA after the SA lifetime times out, even if there is no traffic. The ZyWALL also reinitiates the SA when it restarts. The ZyWALL also rebuilds the tunnel if it was disconnected due to the output or input idle timer.
Allow NetBIOS Traffic Through IPSec Tunnel	NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to connect to and communicate with a LAN. It may sometimes be necessary to allow NetBIOS packets to pass through VPN tunnels in order to allow local computers to find computers on the remote network and vice versa. Select this check box to send NetBIOS packets through the VPN connection.
Check IPSec Tunnel Connectivity	Select the check box and configure an IP address in the **Ping this Address** field to have the ZyWALL periodically test the VPN tunnel to the remote IPSec router. The ZyWALL pings the IP address every minute. The ZyWALL starts the IPSec connection idle timeout timer when it sends the ping packet. If there is no traffic from the remote IPSec router by the time the timeout period expires, the ZyWALL disconnects the VPN tunnel.
Log	Select this check box to set the ZyWALL to create logs when it cannot ping the remote device.
Ping this Address	If you select **Check IPSec Tunnel Connectivity**, enter the IP address of a computer at the remote IPSec network. The computer's IP address must be in this IP policy's remote range (see the **Remote Network** fields).
Gateway Policy Information	
Gateway Policy	Select the gateway policy with which you want to use the VPN policy.
Local Network	Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Address Type	Use the drop-down list box to choose **Single Address**, **Range Address**, or **Subnet Address**. Select **Single Address** for a single IP address. Select **Range Address** for a specific range of IP addresses. Select **Subnet Address** to specify IP addresses on a network by their subnet mask.
Starting IP Address	When the **Address Type** field is configured to **Single Address**, enter a (static) IP address on the LAN behind your ZyWALL. When the **Address Type** field is configured to **Range Address**, enter the beginning (static) IP address, in a range of computers on the LAN behind your ZyWALL. When the **Address Type** field is configured to **Subnet Address**, this is a (static) IP address on the LAN behind your ZyWALL.
Ending IP Address/ Subnet Mask	When the **Address Type** field is configured to **Single Address**, this field is N/A. When the **Address Type** field is configured to **Range Address**, enter the end (static) IP address, in a range of computers on the LAN behind your ZyWALL. When the **Address Type** field is configured to **Subnet Address**, this is a subnet mask on the LAN behind your ZyWALL.
Local Port	0 is the default and signifies any port. Type a port number from 0 to 65535 in the **Start** and **End** fields. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.

Table 70 Configuration > VPN > IKE IPSec (continued)

LABEL	DESCRIPTION
Remote Network	Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Address Type	Use the drop-down list box to choose **Single Address**, **Range Address**, or **Subnet Address**. Select **Single Address** with a single IP address. Select **Range Address** for a specific range of IP addresses. Select **Subnet Address** to specify IP addresses on a network by their subnet mask.
Starting IP Address	When the **Address Type** field is configured to **Single Address**, enter a (static) IP address on the network behind the remote IPSec router. When the **Address Type** field is configured to **Range Address**, enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Address Type** field is configured to **Subnet Address**, enter a (static) IP address on the network behind the remote IPSec router.
Ending IP Address/ Subnet Mask	When the **Address Type** field is configured to **Single Address**, this field is N/A. When the **Address Type** field is configured to **Range Address**, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Address Type** field is configured to **Subnet Address**, enter a subnet mask on the network behind the remote IPSec router.
Remote Port	0 is the default and signifies any port. Type a port number from 0 to 65535 in the **Start** and **End** fields. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.
IPSec Proposal	
Encapsulation Mode	Select **Tunnel** mode or **Transport** mode.
Active Protocol	Select the security protocols used for an SA. Both **AH** and **ESP** increase Prestige processing requirements and communications latency (delay).
Encryption Algorithm	When **DES** is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on DES that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of **AES** uses a 128-bit key. **AES** is faster than **3DES**. Select **NULL** to set up a tunnel without encryption. When you select **NULL**, you do not enter an encryption key.
Authentication Algorithm	**MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slower. Select **MD5** for minimal security and **SHA-1** for maximum security.
SA Life Time (Seconds)	Define the length of time before an IKE SA automatically renegotiates in this field. The minimum value is 180 seconds. A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.

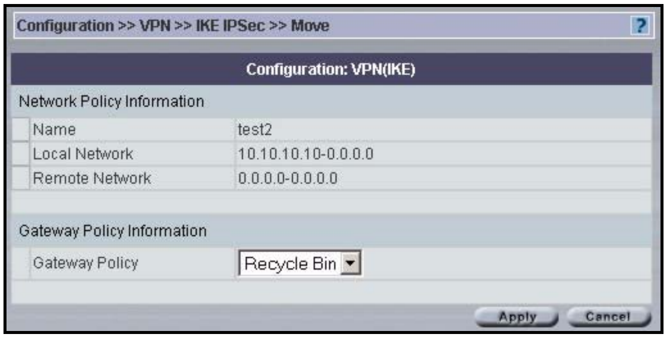
Table 70 Configuration > VPN > IKE IPSec (continued)

LABEL	DESCRIPTION
Perfect Forward Secret (PFS)	Perfect Forward Secret (PFS) is disabled (**NONE**) by default in phase 2 IPSec SA setup. This allows faster IPSec setup, but is not so secure. Select **DH1** or **DH2** to enable PFS. **DH1** refers to Diffie-Hellman Group 1 a 768 bit random number. **DH2** refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number (more secure, yet slower).
Enable Replay Detection	As a VPN setup is processing intensive, the system is vulnerable to Denial of Service (DOS) attacks. The IPSec receiver can detect and reject old or duplicate packets to protect against replay attacks. Enable replay detection by selecting this check box.
Enable Multiple Proposals	Select this check box to allow the ZyWALL to use any of its phase 1 or phase 2 encryption and authentication algorithms when negotiating an IPSec SA. When you enable multiple proposals, the ZyWALL allows the remote IPSec router to select which encryption and authentication algorithms to use for the VPN tunnel, even if they are less secure than the ones you configure for the VPN rule. Clear this check box to have the ZyWALL use only the phase 1 or phase 2 encryption and authentication algorithms configured below when negotiating an IPSec SA.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard all changes and return to the main VPN screen.

11.14.3 VPN Rules (IKE) > Network Policy Move

Click the **Move** button icon in the VPN Rules (IKE) screen to display the screen shown next. Use this screen to associate a network policy to a gateway policy.

Figure 99 Configuration > VPN > IKE IPSec > Move



Configuration >> VPN >> IKE IPSec >> Move

Configuration: VPN(IKE)

Network Policy Information

Name	test2
Local Network	10.10.10.10-0.0.0.0
Remote Network	0.0.0.0-0.0.0.0

Gateway Policy Information

Gateway Policy	Recycle Bin

The following table describes the labels in this screen.

Table 71 Configuration > VPN > IKE IPSec > Move

LABEL	DESCRIPTION
Network Policy Information	The following fields display the general network settings of this VPN policy.
Name	This field displays the policy name.

Table 71 Configuration > VPN > IKE IPSec > Move (continued)

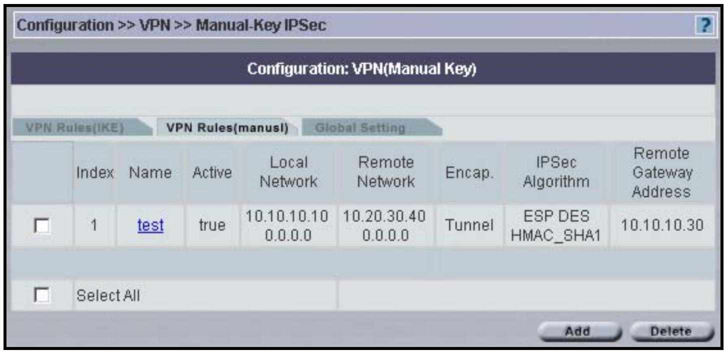
LABEL	DESCRIPTION
Local Network	This field displays one or a range of IP address(es) of the computer(s) behind the ZyWALL.
Remote Network	This field displays one or a range of IP address(es) of the remote network behind the remote IPsec router.
Gateway Policy Information	
Gateway Policy	Select the name of a VPN rule (or gateway policy) to which you want to associate this VPN network policy. If you do not want to associate a network policy to any gateway policy, select **Recycle Bin** from the drop-down list box. The **Recycle Bin** gateway policy is a virtual placeholder for any network policy(ies) without an associated gateway policy. When there is a network policy in **Recycle Bin**, the **Recycle Bin** gateway policy automatically displays in the **VPN Rules (IKE)** screen.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard all changes and return to the main VPN screen.

11.15 VPN Rules (Manual) (VPN version 1.1)

Select a device, click **Configuration > VPN** > **VPN Rules(manual)** tab to open the VPN Rules screen. This is a read-only menu of your IPSec rules (tunnels). Edit an IPSec rule by clicking the edit icon to configure the associated submenus.

You may want to configure a VPN rule that uses manual key management if you are having problems with IKE key management.

Figure 100 Configuration > VPN > Manual-Key IPSec



Configuration >> VPN >> Manual-Key IPSec

Configuration: VPN(Manual Key)

	Index	Name	Active	Local Network	Remote Network	Encap.	IPSec Algorithm	Remote Gateway Address
□	1	test	true	10.10.10.10 0.0.0.0	10.20.30.40 0.0.0.0	Tunnel	ESP DES HMAC_SHA1	10.10.10.30
□	Select All							

The following table describes the labels in this screen.

Table 72 Configuration > VPN > Manual-Key IPSec

LABEL	DESCRIPTION
Index	This is the VPN policy index number.
Name	This field displays the identification name for this VPN policy. Click the hyperlink to edit the VPN policy.

Table 72 Configuration > VPN > Manual-Key IPSec (continued)

LABEL	DESCRIPTION
Active	This field displays whether the VPN policy is active or not. A **true** signifies that this VPN policy is active; **false** signifies that this VPN policy is not active.
Local Network	This is the IP address(es) of computer(s) on your local network behind your ZyWALL. The same (static) IP address is displayed twice when the **Local Network Address Type** field in the **VPN - Manual Key - Edit** screen is configured to **Single Address**. The beginning and ending (static) IP addresses, in a range of computers are displayed when the **Local Network Address Type** field in the **VPN - Manual Key - Edit** screen is configured to **Range Address**. A (static) IP address and a subnet mask are displayed when the **Local Network Address Type** field in the **VPN - Manual Key - Edit** screen is configured to **Subnet Address**.
Remote Network	This is the IP address(es) of computer(s) on the remote network behind the remote IPSec router. This field displays **N/A** when the **Remote Gateway Address** field displays **0.0.0.0**. In this case only the remote IPSec router can initiate the VPN. The same (static) IP address is displayed twice when the **Remote Network Address Type** field in the **VPN - Manual Key - Edit** screen is configured to **Single Address**. The beginning and ending (static) IP addresses, in a range of computers are displayed when the **Remote Network Address Type** field in the **VPN - Manual Key - Edit** screen is configured to **Range Address**. A (static) IP address and a subnet mask are displayed when the **Remote Network Address Type** field in the **VPN - Manual Key - Edit** screen is configured to **Subnet Address**.
Encap.	This field displays **Tunnel** or **Transport** mode (**Tunnel** is the default selection).
IPSec Algorithm	This field displays the security protocols used for an SA. Both **AH** and **ESP** increase ZyWALL processing requirements and communications latency (delay).
Remote Gateway Address	This is the static WAN IP address or domain name of the remote IPSec router.
Add	Click **Add** to add a new VPN policy.
Delete	Select a policy and click **Delete** to remove the VPN policy. A window displays asking you to confirm that you want to delete the VPN rule. When a VPN policy is deleted, subsequent policies move up in the page list.

11.15.1 VPN Rules (Manual) > Edit

Manual key management is useful if you have problems with IKE key management.

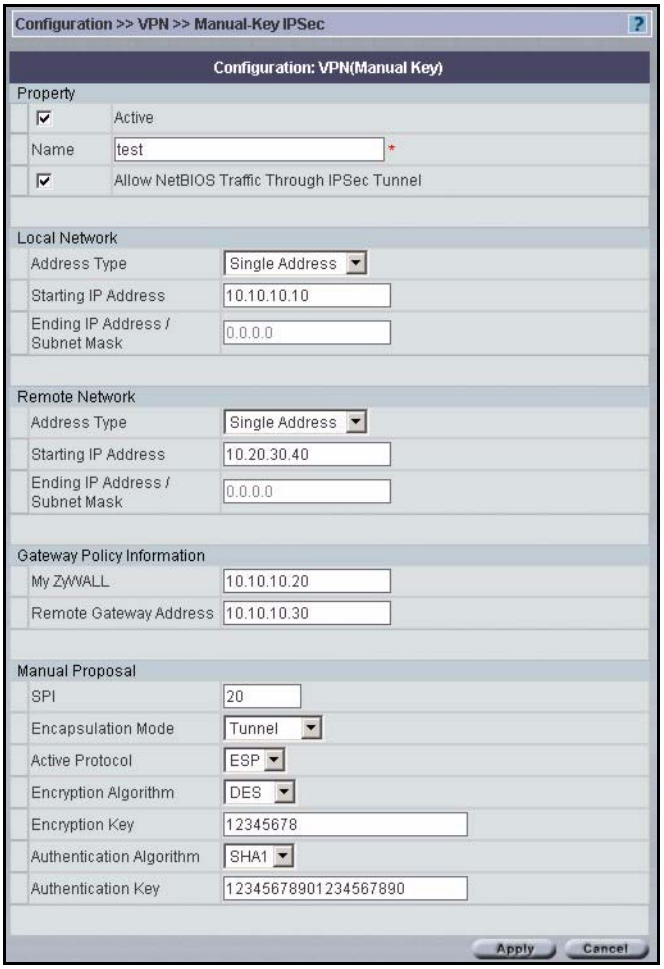
11.15.1.1 Security Parameter Index (SPI)

An SPI is used to distinguish different SAs terminating at the same destination and using the same IPSec protocol. This data allows for the multiplexing of SAs to a single gateway. The **SPI** (Security Parameter Index) along with a destination IP address uniquely identify a particular Security Association (SA). The **SPI** is transmitted from the remote VPN gateway to the local VPN gateway. The local VPN gateway then uses the network, encryption and key values that the administrator associated with the SPI to establish the tunnel.

Note: Current ZyXEL implementation assumes identical outgoing and incoming SPIs.

Click a **Name** hyperlink in the **VPN Rules (Manual)** screen to edit VPN rules.

Figure 101 Configuration > VPN > Manual-Key IPSec > Edit



Configuration >> VPN >> Manual-Key IPSec

Configuration: VPN(Manual Key)

Property

☑	Active
Name	test *
☑	Allow NetBIOS Traffic Through IPSec Tunnel

Local Network

Address Type	Single Address
Starting IP Address	10.10.10.10
Ending IP Address / Subnet Mask	0.0.0.0

Remote Network

Address Type	Single Address
Starting IP Address	10.20.30.40
Ending IP Address / Subnet Mask	0.0.0.0

Gateway Policy Information

My ZyWALL	10.10.10.20
Remote Gateway Address	10.10.10.30

Manual Proposal

SPI	20
Encapsulation Mode	Tunnel
Active Protocol	ESP
Encryption Algorithm	DES
Encryption Key	12345678
Authentication Algorithm	SHA1
Authentication Key	12345678901234567890

The following table describes the labels in this screen.

Table 73 Configuration > VPN > Manual-Key IPSec > Edit

LABEL	DESCRIPTION
Property	
Active	Select this check box to activate this VPN policy.
Name	Type up to 32 characters to identify this VPN policy. You may use any character, including spaces, but the ZyWALL drops trailing spaces.
Allow NetBIOS Traffic Through IPSec Tunnel	NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to find other computers. It may sometimes be necessary to allow NetBIOS packets to pass through VPN tunnels in order to allow local computers to find computers on the remote network and vice versa. Select this check box to send NetBIOS packets through the VPN connection.

Table 73 Configuration > VPN > Manual-Key IPSec > Edit (continued)

LABEL	DESCRIPTION
Local Network	Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Address Type	Use the drop-down list box to choose **Single Address**, **Range Address**, or **Subnet Address**. Select **Single Address** for a single IP address. Select **Range Address** for a specific range of IP addresses. Select **Subnet Address** to specify IP addresses on a network by their subnet mask.
Starting IP Address	When the **Address Type** field is configured to **Single Address**, enter a (static) IP address on the LAN behind your ZyWALL. When the **Address Type** field is configured to **Range Address**, enter the beginning (static) IP address, in a range of computers on the LAN behind your ZyWALL. When the **Address Type** field is configured to **Subnet Address**, this is a (static) IP address on the LAN behind your ZyWALL.
Ending IP Address/Subnet Mask	When the **Address Type** field is configured to **Single Address**, this field is N/A. When the **Address Type** field is configured to **Range Address**, enter the end (static) IP address, in a range of computers on the LAN behind your ZyWALL. When the **Address Type** field is configured to **Subnet Address**, this is a subnet mask on the LAN behind your ZyWALL.
Remote Network	Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Address Type	Use the drop-down list box to choose **Single Address**, **Range Address**, or **Subnet Address**. Select **Single Address** with a single IP address. Select **Range Address** for a specific range of IP addresses. Select **Subnet Address** to specify IP addresses on a network by their subnet mask.
Starting IP Address	When the **Address Type** field is configured to **Single Address**, enter a (static) IP address on the network behind the remote IPSec router. When the **Address Type** field is configured to **Range Address**, enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Address Type** field is configured to **Subnet Address**, enter a (static) IP address on the network behind the remote IPSec router.
Ending IP Address/Subnet Mask	When the **Address Type** field is configured to **Single Address**, this field is N/A. When the **Address Type** field is configured to **Range Address**, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Address Type** field is configured to **Subnet Address**, enter a subnet mask on the network behind the remote IPSec router.
Gateway Policy Information	

Table 73 Configuration > VPN > Manual-Key IPSec > Edit (continued)

LABEL	DESCRIPTION
My ZyWALL	Enter the WAN IP address or domain name of your ZyWALL or leave the field set to **0.0.0.0**. The VPN tunnel has to be rebuilt if the **My ZyWALL** IP address changes after setup. The following applies if the **My ZyWALL** field is configured as **0.0.0.0**: • When the WAN port operation mode is set to Active/Passive, the ZyWALL uses the IP address (static or dynamic) of the WAN port that is in use. • When the WAN port operation mode is set to Active/Active, the ZyWALL uses the IP address (static or dynamic) of the primary (highest priority) WAN port to set up the VPN tunnel as long as the corresponding WAN1 or WAN2 connection is up. If the corresponding WAN1 or WAN2 connection goes down, the ZyWALL uses the IP address of the other WAN port. • If both WAN connections go down, the ZyWALL uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect. See the chapter on WAN for details on dial backup and traffic redirect.
Remote Gateway Addr	Type the WAN IP address or the domain name (up to 31 characters) of the IPSec router with which you're making the VPN connection.
Manual Proposal	
SPI	Type a unique **SPI** (Security Parameter Index) from one to four characters long. Valid Characters are "0, 1, 2, 3, 4, 5, 6, 7, 8, and 9".
Encapsulation Mode	Select **Tunnel** mode or **Transport** mode from the drop-down list box.
Active Protocol	Select **ESP** if you want to use ESP (Encapsulation Security Payload). The ESP protocol (RFC 2406) provides encryption as well as some of the services offered by **AH**. If you select **ESP** here, you must select options from the **Encryption Algorithm** and **Authentication Algorithm** fields (described next). Select **AH** if you want to use AH (Authentication Header Protocol). The AH protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the ESP was designed. If you select **AH** here, you must select options from the **Authentication Algorithm** field (described next).
Encryption Algorithm	Select **DES**, **3DES** or **NULL** from the drop-down list box. When **DES** is used for data communications, both sender and receiver must know the **Encryption Key**, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on DES that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. Select **NULL** to set up a tunnel without encryption. When you select **NULL**, you do not enter an encryption key.
Authentication Algorithm	Select **SHA1** or **MD5** from the drop-down list box. **MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slower. Select **MD5** for minimal security and **SHA1** for maximum security.
Encryption Key	This field is applicable when you select **ESP** in the **Active Protocol** field above. With **DES**, type a unique key 8 characters long. With **3DES**, type a unique key 24 characters long. Any characters may be used, including spaces, but trailing spaces are truncated.
Authentication Key	Type a unique authentication key to be used by IPSec if applicable. Enter 16 characters for **MD5** authentication or 20 characters for **SHA1** authentication. Any characters may be used, including spaces, but trailing spaces are truncated.

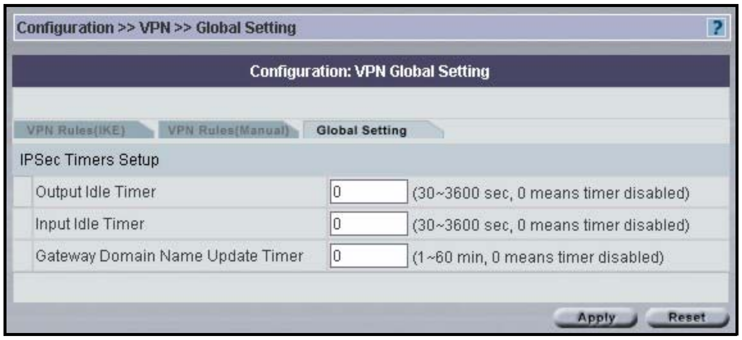
Table 73 Configuration > VPN > Manual-Key IPSec > Edit (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving.

11.16 VPN Global Setting (VPN version 1.1)

Select a device, click **Configuration > VPN** > **Global Setting** tab to open the screen shown next. Use this screen to change your ZyWALL's global settings.

Figure 102 Configuration > VPN > Global Setting



Configuration >> VPN >> Global Setting

Configuration: VPN Global Setting

IPSec Timers Setup

Output Idle Timer 0 (30~3600 sec, 0 means timer disabled)

Input Idle Timer 0 (30~3600 sec, 0 means timer disabled)

Gateway Domain Name Update Timer 0 (1~60 min, 0 means timer disabled)

The following table describes the labels in this screen.

Table 74 Configuration > VPN > Global Setting

LABEL	DESCRIPTION
Output Idle Timer	When traffic is sent to a remote IPSec router from which no reply is received after the specified time period, the ZyWALL checks the VPN connectivity. If the remote IPSec router does not reply, the ZyWALL automatically disconnects the VPN tunnel. Enter the time period (between 30 and 3600 seconds) to wait before the ZyWALL checks all of the VPN connections to remote IPSec routers. Enter **0** to disable this feature.
Input Idle Timer	When no traffic is received from a remote IPSec router after the specified time period, the ZyWALL checks the VPN connectivity. If the remote IPSec router does not reply, the ZyWALL automatically disconnects the VPN tunnel. Enter the time period (between 30 and 3600 seconds) to wait before the ZyWALL checks all of the VPN connections to remote IPSec routers. Enter **0** to disable this feature.
Gateway Domain Name Update Timer	This field is applicable when you enter a domain name to identify the ZyWALL and/or the remote secure gateway. Enter the time period (between 2 and 60 minutes) to wait before the ZyWALL updates the domain name and IP address mapping through a DNS server. The ZyWALL rebuilds the VPN tunnel if it finds that the domain name is now using a different IP address (any users of the VPN tunnel will be temporarily disconnected). Enter **0** to disable this feature.

Table 74 Configuration > VPN > Global Setting (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

11.17 Telecommuter VPN/IPSec Examples

The following examples show how multiple telecommuters can make VPN connections to a single ZyWALL at headquarters. The telecommuters use IPSec routers with dynamic WAN IP addresses. The ZyWALL at headquarters has a static public IP address.

11.17.1 Telecommuters Sharing One VPN Rule Example

See the following figure and table for an example configuration that allows multiple telecommuters (**A**, **B** and **C** in the figure) to use one VPN rule to simultaneously access a ZyWALL at headquarters (**HQ** in the figure). The telecommuters do not have domain names mapped to the WAN IP addresses of their IPSec routers. The telecommuters must all use the same IPSec parameters but the local IP addresses (or ranges of addresses) should not overlap.

Figure 103 Telecommuters Sharing One VPN Rule Example

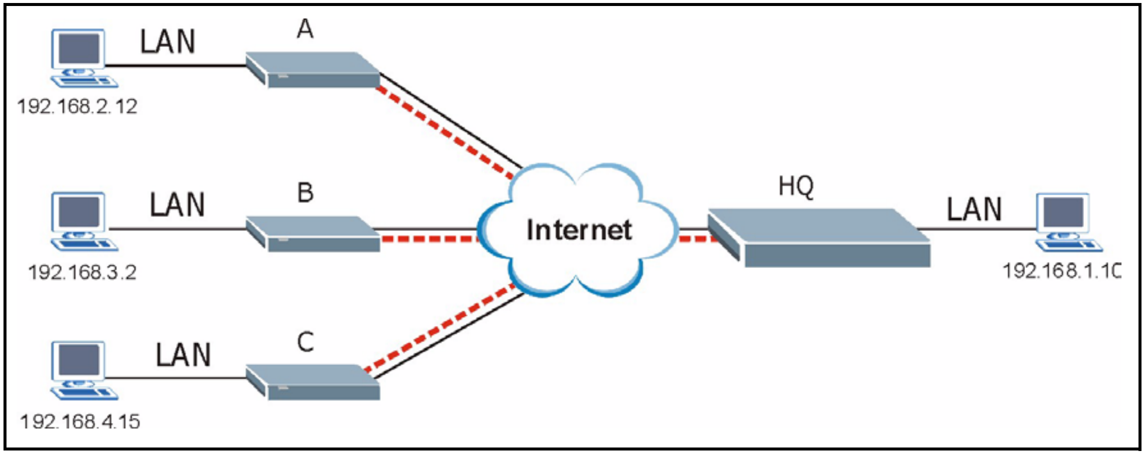


Table 75 Telecommuters Sharing One VPN Rule Example

FIELDS	TELECOMMUTERS	HEADQUARTERS
My ZyWALL:	0.0.0.0 (dynamic IP address assigned by the ISP)	Public static IP address
Remote Gateway Address:	Public static IP address	0.0.0.0 With this IP address only the telecommuter can initiate the IPSec tunnel.

Table 75 Telecommuters Sharing One VPN Rule Example

FIELDS	TELECOMMUTERS	HEADQUARTERS
Local Network - Single IP Address:	Telecommuter A: 192.168.2.12 Telecommuter B: 192.168.3.2 Telecommuter C: 192.168.4.15	192.168.1.10
Remote Network - Single IP Address:	192.168.1.10	Not Applicable

11.17.2 Telecommuters Using Unique VPN Rules Example

In this example the telecommuters (A, B and C in the figure) use IPSec routers with domain names that are mapped to their dynamic WAN IP addresses (use Dynamic DNS to do this).

With aggressive negotiation mode, the ZyWALL can use the ID types and contents to distinguish between VPN rules. Telecommuters can each use a separate VPN rule to simultaneously access a ZyWALL at headquarters. They can use different IPSec parameters. The local IP addresses (or ranges of addresses) of the rules configured on the ZyWALL at headquarters can overlap. The local IP addresses of the rules configured on the telecommuters’ IPSec routers should not overlap.

See the following table and figure for an example where three telecommuters each use a different VPN rule for a VPN connection with a ZyWALL located at headquarters. The ZyWALL at headquarters (HQ in the figure) identifies each incoming SA by its ID type and content and uses the appropriate VPN rule to establish the VPN connection.

The ZyWALL at headquarters can also initiate VPN connections to the telecommuters since it can find the telecommuters by resolving their domain names.

Figure 104 Telecommuters Using Unique VPN Rules Example

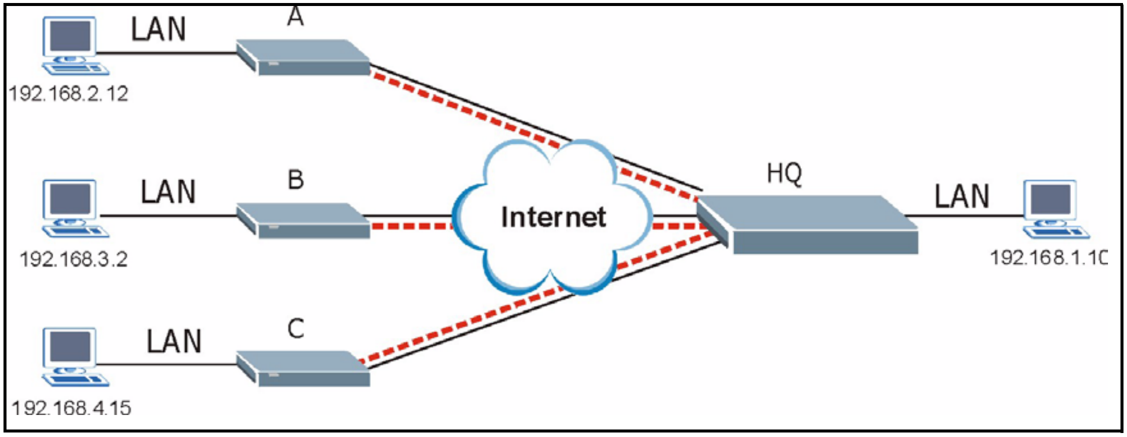


Table 76 Telecommuters Using Unique VPN Rules Example

TELECOMMUTERS	HEADQUARTERS
All Telecommuter Rules:	All Headquarters Rules:
My ZyWALL 0.0.0.0	My ZyWALL: bigcompanyhq.com
Remote Gateway Address: bigcompanyhq.com	Local Network - Single IP Address: 192.168.1.10
Remote Network - Single IP Address: 192.168.1.10	Local ID Type: E-mail
Peer ID Type: E-mail	Local ID Content: bob@bigcompanyhq.com
Peer ID Content: bob@bigcompanyhq.com	
Telecommuter A (telecommutera.dydns.org)	Headquarters ZyWALL Rule 1:
Local ID Type: IP	Peer ID Type: IP
Local ID Content: 192.168.2.12	Peer ID Content: 192.168.2.12
Local IP Address: 192.168.2.12	Remote Gateway Address: telecommutera.dydns.org
	Remote Address 192.168.2.12
Telecommuter B (telecommuterb.dydns.org)	Headquarters [Product Name (short)] Rule 2:
Local ID Type: DNS	Peer ID Type: DNS
Local ID Content: telecommuterb.com	Peer ID Content: telecommuterb.com
Local IP Address: 192.168.3.2	Remote Gateway Address: telecommuterb.dydns.org
	Remote Address 192.168.3.2
Telecommuter C (telecommuterc.dydns.org)	Headquarters [Product Name (short)] Rule 3:
Local ID Type: E-mail	Peer ID Type: E-mail
Local ID Content: myVPN@myplace.com	Peer ID Content: myVPN@myplace.com

Table 76 Telecommuters Using Unique VPN Rules Example

TELECOMMUTERS	HEADQUARTERS
Local IP Address: 192.168.4.15	Remote Gateway Address: telecommuterc.dydns.org
	Remote Address 192.168.4.15

11.18 VPN and Remote Management

If a VPN tunnel uses Telnet, FTP, WWW, SNMP, DNS or ICMP, then you should configure remote management to allow access for that service.

CHAPTER 12
Configuration > Firewall

This chapter shows you how to configure firewall for your devices.

12.1 Types of DoS Attacks

There are four types of DoS attacks:

1. Those that exploit bugs in a TCP/IP implementation.
2. Those that exploit weaknesses in the TCP/IP specification.
3. Brute-force attacks that flood a network with useless data.
4. IP Spoofing.

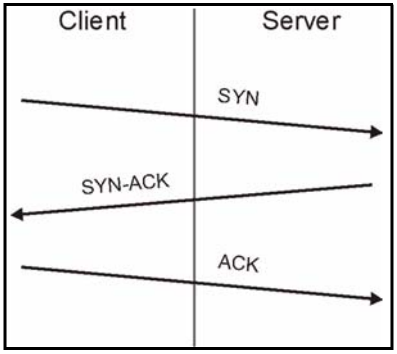
- "**Ping of Death**" and "**Teardrop**" attacks exploit bugs in the TCP/IP implementations of various computer and host systems.

    a. Ping of Death uses a "ping" utility to create an IP packet that exceeds the maximum 65,536 bytes of data allowed by the IP specification. The oversize packet is then sent to an unsuspecting system. Systems may crash, hang or reboot.

    b. Teardrop attack exploits weaknesses in the reassembly of IP packet fragments. As data is transmitted through a network, IP packets are often broken up into smaller chunks. Each fragment looks like the original IP packet except that it contains an offset field that says, for instance, "This fragment is carrying bytes 200 through 400 of the original (non fragmented) IP packet." The Teardrop program creates a series of IP fragments with overlapping offset fields. When these fragments are reassembled at the destination, some systems will crash, hang, or reboot.

- Weaknesses in the TCP/IP specification leave it open to "**SYN Flood**" and "**LAND**" attacks. These attacks are executed during the handshake that initiates a communication session between two applications.

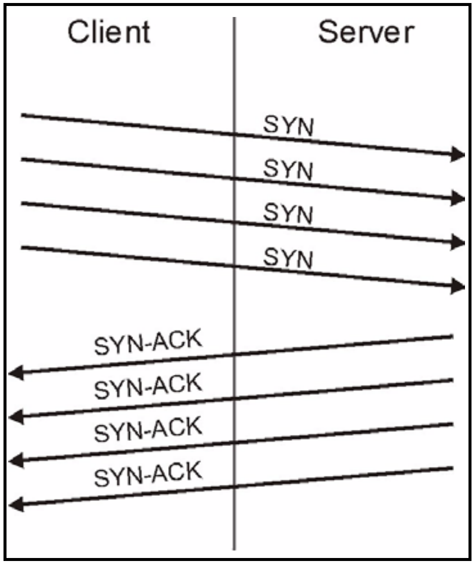
Figure 105 Three-Way Handshake



Under normal circumstances, the application that initiates a session sends a SYN (synchronize) packet to the receiving server. The receiver sends back an ACK (acknowledgment) packet and its own SYN, and then the initiator responds with an ACK (acknowledgment). After this handshake, a connection is established.

a **SYN Attack** floods a targeted system with a series of SYN packets. Each packet causes the targeted system to issue a SYN-ACK response. While the targeted system waits for the ACK that follows the SYN-ACK, it queues up all outstanding SYN-ACK responses on what is known as a backlog queue. SYN-ACKs are moved off the queue only when an ACK comes back or when an internal timer (which is set at relatively long intervals) terminates the three-way handshake. Once the queue is full, the system will ignore all incoming SYN requests, making the system unavailable for legitimate users.

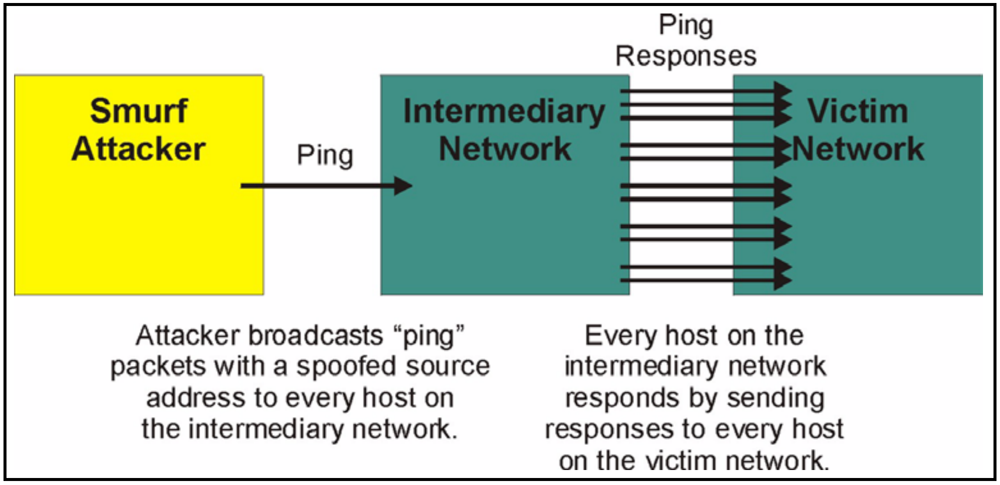
Figure 106 SYN Flood



b In a **LAND Attack**, hackers flood SYN packets into the network with a spoofed source IP address of the targeted system. This makes it appear as if the host computer sent the packets to itself, making the system unavailable while the target system tries to respond to itself.

- A **brute-force** attack, such as a "Smurf" attack, targets a feature in the IP specification known as directed or subnet broadcasting, to quickly flood the target network with useless data. A Smurf hacker floods a router with Internet Control Message Protocol (ICMP) echo request packets (pings). Since the destination IP address of each packet is the broadcast address of the network, the router will broadcast the ICMP echo request packet to all hosts on the network. If there are numerous hosts, this will create a large amount of ICMP echo request and response traffic. If a hacker chooses to spoof the source IP address of the ICMP echo request packet, the resulting ICMP traffic will not only clog up the "intermediary" network, but will also congest the network of the spoofed source IP address, known as the "victim" network. This flood of broadcast traffic consumes all available bandwidth, making communications impossible.

Figure 107 Smurf Attack


Ping
Responses
Smurf
Attacker
Ping
Intermediary
Network
Victim
Network
Attacker broadcasts "ping" packets with a spoofed source address to every host on the intermediary network.
Every host on the intermediary network responds by sending responses to every host on the victim network.

12.1.1 ICMP Vulnerability

ICMP is an error-reporting protocol that works in concert with IP. The following ICMP types trigger an alert:

Table 77 ICMP Commands That Trigger Alerts

5	REDIRECT
13	TIMESTAMP_REQUEST
14	TIMESTAMP_REPLY
17	ADDRESS_MASK_REQUEST
18	ADDRESS_MASK_REPLY

12.1.2 Illegal Commands (NetBIOS and SMTP)

The only legal NetBIOS commands are the following - all others are illegal.

Table 78 Legal NetBIOS Commands

MESSAGE:
REQUEST:
POSITIVE:
NEGATIVE:
RETARGET:
KEEPALIVE:

All SMTP commands are illegal except for those displayed in the following tables.

Table 79 Legal SMTP Commands

AUTH	DATA	EHLO	ETRN	EXPN	HELO	HELP	MAIL	NOOP
QUIT	RCPT	RSET	SAML	SEND	SOML	TURN	VRFY	

12.1.3 Traceroute

Traceroute is a utility used to determine the path a packet takes between two endpoints. Sometimes when a packet filter firewall is configured incorrectly an attacker can traceroute the firewall gaining knowledge of the network topology inside the firewall.

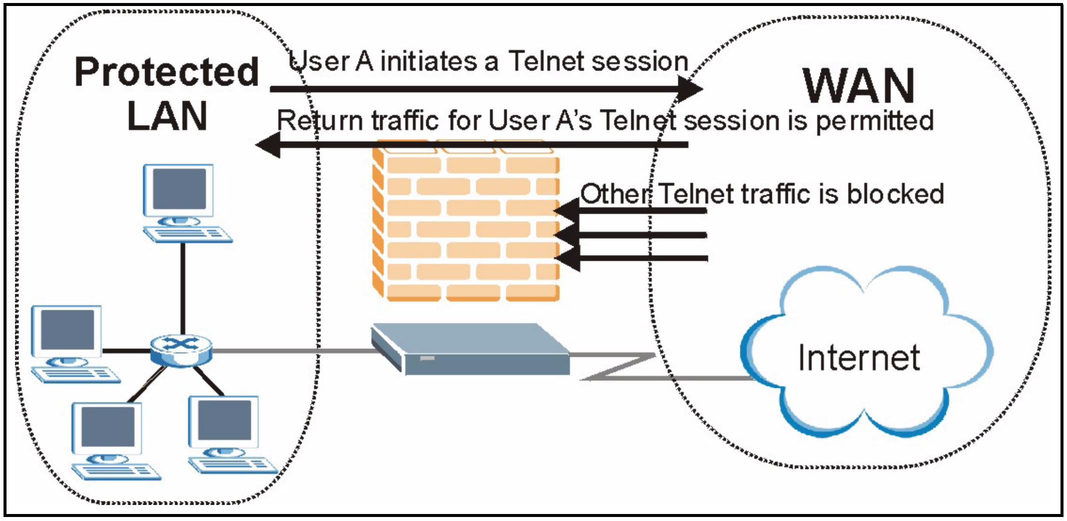
Often, many DoS attacks also employ a technique known as "**IP Spoofing**" as part of their attack. IP Spoofing may be used to break into systems, to hide the hacker's identity, or to magnify the effect of the DoS attack. IP Spoofing is a technique used to gain unauthorized access to computers by tricking a router or firewall into thinking that the communications are coming from within the trusted network. To engage in IP spoofing, a hacker must modify the packet headers so that it appears that the packets originate from a trusted host and should be allowed through the router or firewall. The ZyWALL blocks all IP Spoofing attempts.

12.2 Stateful Inspection

With stateful inspection, fields of the packets are compared to packets that are already known to be trusted. For example, if you access some outside service, the proxy server remembers things about your original request, like the port number and source and destination addresses. This remembering is called *saving the state.* When the outside system responds to your request, the firewall compares the received packets with the saved state to determine if they are allowed in. The ZyWALL uses stateful packet inspection to protect the private LAN from hackers and vandals on the Internet. By default, the ZyWALL’s stateful inspection allows all communications to the Internet that originate from the LAN, and blocks all traffic to the LAN that originates from the Internet. In summary, stateful inspection:

- Allows all sessions originating from the LAN (local network) to the WAN (Internet). Denies all sessions originating from the WAN to the LAN.

Figure 108 Stateful Inspection


Protected LAN
User A initiates a Telnet session
WAN
Return traffic for User A's Telnet session is permitted
Other Telnet traffic is blocked
Internet

The previous figure shows the ZyWALL's default firewall rules in action as well as demonstrates how stateful inspection works. User A can initiate a Telnet session from within the LAN and responses to this request are allowed. However other Telnet traffic initiated from the WAN is blocked.

12.2.1 Stateful Inspection Process

In this example, the following sequence of events occurs when a TCP packet leaves the LAN network through the firewall's WAN interface. The TCP packet is the first in a session, and the packet's application layer protocol is configured for a firewall rule inspection:

1 The packet travels from the firewall's LAN to the WAN.

2 The packet is evaluated against the interface's existing outbound access list, and the packet is permitted (a denied packet would simply be dropped at this point).

3 The firewall inspects packets to determine and record information about the state of the packet's connection. This information is recorded in a new state table entry created for the new connection. If there is not a firewall rule for this packet and it is not an attack, then the setting in the **Firewall Default Rule** screen determines the action for this packet.

4 Based on the obtained state information, a firewall rule creates a temporary access list entry that is inserted at the beginning of the WAN interface's inbound extended access list. This temporary access list entry is designed to permit inbound packets of the same connection as the outbound packet just inspected.

5 The outbound packet is forwarded out through the interface.

6 Later, an inbound packet reaches the interface. This packet is part of the connection previously established with the outbound packet. The inbound packet is evaluated against the inbound access list, and is permitted because of the temporary access list entry previously created.

7 The packet is inspected by a firewall rule, and the connection's state table entry is updated as necessary. Based on the updated state information, the inbound extended access list temporary entries might be modified, in order to permit only packets that are valid for the current state of the connection.

8 Any additional inbound or outbound packets that belong to the connection are inspected to update the state table entry and to modify the temporary inbound access list entries as required, and are forwarded through the interface.

9 When the connection terminates or times out, the connection's state table entry is deleted and the connection's temporary inbound access list entries are deleted.

12.2.2 Stateful Inspection and the ZyWALL

Additional rules may be defined to extend or override the default rules. For example, a rule may be created which will:

1 Block all traffic of a certain type, such as IRC (Internet Relay Chat), from the LAN to the Internet.

2 Allow certain types of traffic from the Internet to specific hosts on the LAN.

3 Allow access to a Web server to everyone but competitors.

4 Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

These custom rules work by evaluating the network traffic’s Source IP address, Destination IP address, IP protocol type, and comparing these to rules set by the administrator.

Note: The ability to define firewall rules is a very powerful tool. Using custom rules, it is possible to disable all firewall protection or block all access to the Internet. Use extreme caution when creating or deleting firewall rules. Test changes after creating them to make sure they work correctly.

Below is a brief technical description of how these connections are tracked. Connections may either be defined by the upper protocols (for instance, TCP), or by the ZyWALL itself (as with the "virtual connections" created for UDP and ICMP).

12.2.3 TCP Security

The ZyWALL uses state information embedded in TCP packets. The first packet of any new connection has its SYN flag set and its ACK flag cleared; these are "initiation" packets. All packets that do not have this flag structure are called "subsequent" packets, since they represent data that occurs later in the TCP stream.

If an initiation packet originates on the WAN, this means that someone is trying to make a connection from the Internet into the LAN. Except in a few special cases (see "Upper Layer Protocols" shown next), these packets are dropped and logged.

If an initiation packet originates on the LAN, this means that someone is trying to make a connection from the LAN to the Internet. Assuming that this is an acceptable part of the security policy (as is the case with the default policy), the connection will be allowed. A cache entry is added which includes connection information such as IP addresses, TCP ports, sequence numbers, etc.

When the ZyWALL receives any subsequent packet (from the Internet or from the LAN), its connection information is extracted and checked against the cache. A packet is only allowed to pass through if it corresponds to a valid connection (that is, if it is a response to a connection which originated on the LAN).

12.2.4 UDP/ICMP Security

UDP and ICMP do not themselves contain any connection information (such as sequence numbers). However, at the very minimum, they contain an IP address pair (source and destination). UDP also contains port pairs, and ICMP has type and code information. All of this data can be analyzed in order to build "virtual connections" in the cache.

For instance, any UDP packet that originates on the LAN will create a cache entry. Its IP address and port pairs will be stored. For a short period of time, UDP packets from the WAN that have matching IP and UDP information will be allowed back in through the firewall.

A similar situation exists for ICMP, except that the ZyWALL is even more restrictive. Specifically, only outgoing echoes will allow incoming echo replies, outgoing address mask requests will allow incoming address mask replies, and outgoing timestamp requests will allow incoming timestamp replies. No other ICMP packets are allowed in through the firewall, simply because they are too dangerous and contain too little tracking information. For instance, ICMP redirect packets are never allowed in, since they could be used to reroute traffic through attacking machines.

12.2.5 Upper Layer Protocols

Some higher layer protocols (such as FTP and RealAudio) utilize multiple network connections simultaneously. In general terms, they usually have a "control connection" which is used for sending commands between endpoints, and then "data connections" which are used for transmitting bulk information.

Consider the FTP protocol. A user on the LAN opens a control connection to a server on the Internet and requests a file. At this point, the remote server will open a data connection from the Internet. For FTP to work properly, this connection must be allowed to pass through even though a connection from the Internet would normally be rejected.

In order to achieve this, the ZyWALL inspects the application-level FTP data. Specifically, it searches for outgoing "PORT" commands, and when it sees these; it adds a cache entry for the anticipated data connection. This can be done safely, since the PORT command contains address and port information, which can be used to uniquely identify the connection.

Any protocol that operates in this way must be supported on a case-by-case basis. You can use the web configurator's **Custom Services** feature to do this.

12.3 Guidelines For Enhancing Security With Your Firewall

1 Change the default password via SMT or web configurator.

2 Think about access control before you connect a console port to the network in any way, including attaching a modem to the port. Be aware that a break on the console port might give unauthorized individuals total control of the firewall, even with access control configured.

3 Limit who can telnet into your router.

4 Don't enable any local service (such as SNMP or NTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.

5 For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.

6 Protect against IP spoofing by making sure the firewall is active.

7 Keep the firewall in a secured (locked) room.

12.4 Packet Filtering Vs Firewall

Below are some comparisons between the ZyWALL's filtering and firewall functions.

12.4.1 Packet Filtering:

- The router filters packets as they pass through the router's interface according to the filter rules you designed.
- Packet filtering is a powerful tool, yet can be complex to configure and maintain, especially if you need a chain of rules to filter a service.
- Packet filtering only checks the header portion of an IP packet.

12.4.1.1 When To Use Filtering

1 To block/allow LAN packets by their MAC addresses.

2 To block/allow special IP packets which are neither TCP nor UDP, nor ICMP packets.

3 To block/allow both inbound (WAN to LAN) and outbound (LAN to WAN) traffic between the specific inside host/network "A" and outside host/network "B". If the filter blocks the traffic from A to B, it also blocks the traffic from B to A. Filters cannot distinguish traffic originating from an inside host or an outside host by IP address.

4 To block/allow IP trace route.

12.4.2 Firewall

- The firewall inspects packet contents as well as their source and destination addresses. Firewalls of this type employ an inspection module, applicable to all protocols, that understands data in the packet is intended for other layers, from the network layer (IP headers) up to the application layer.
- The firewall performs stateful inspection. It takes into account the state of connections it handles so that, for example, a legitimate incoming packet can be matched with the outbound request for that packet and allowed in. Conversely, an incoming packet masquerading as a response to a nonexistent outbound request can be blocked.
- The firewall uses session filtering, i.e., smart rules, that enhance the filtering process and control the network session rather than control individual packets in a session.
- The firewall provides e-mail service to notify you of routine reports and when alerts occur.

12.4.2.1 When To Use The Firewall

1. To prevent DoS attacks and prevent hackers cracking your network.
2. A range of source and destination IP addresses as well as port numbers can be specified within one firewall rule making the firewall a better choice when complex rules are required.
3. To selectively block/allow inbound or outbound traffic between inside host/networks and outside host/networks. Remember that filters cannot distinguish traffic originating from an inside host or an outside host by IP address.
4. The firewall performs better than filtering if you need to check many rules.
5. Use the firewall if you need routine e-mail reports about your system or need to be alerted when attacks occur.
6. The firewall can block specific URL traffic that might occur in the future. The URL can be saved in an Access Control List (ACL) database.

12.5 Firewall Configuration Screens

This section shows you how to configure each Firewall screen.

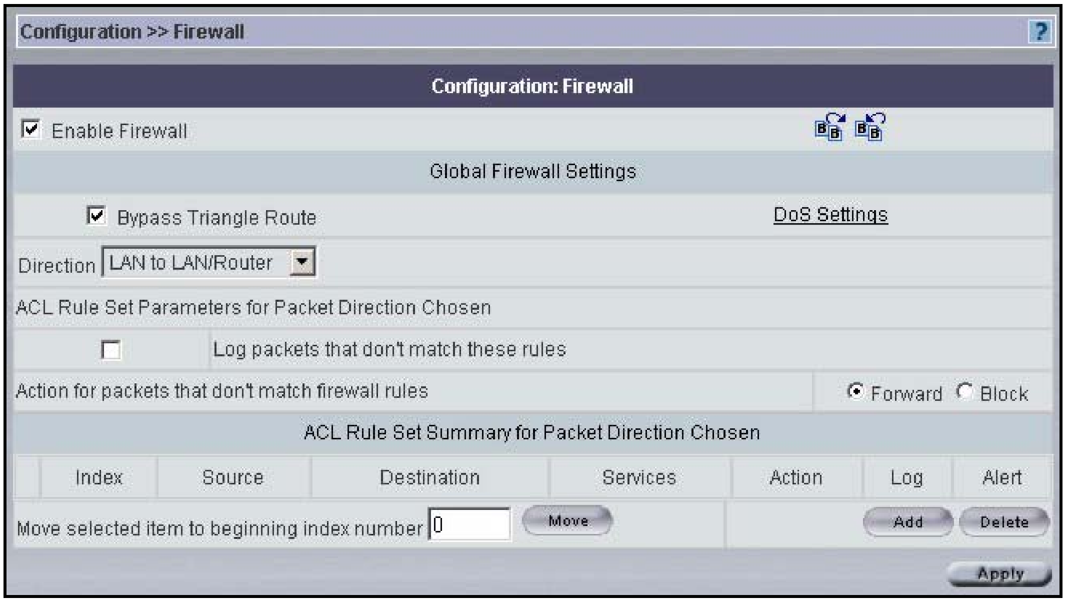
12.5.1 Firewall Summary Screen

12.5.1.1 Ordering Rules

When you click Add, a new rule is always appended to the end of the list. Use the **Move selected item to beginning index number** textbox and **Move** button to put a single rule in a different place.

Select a device and then click **Configuration** > **Firewall**.

Figure 109 Configuration >Firewall



Configuration >> Firewall

Configuration: Firewall

☑ Enable Firewall

Global Firewall Settings

☑ Bypass Triangle Route

Direction: LAN to LAN/Router

ACL Rule Set Parameters for Packet Direction Chosen

☐ Log packets that don't match these rules

Action for packets that don't match firewall rules: ● Forward ○ Block

ACL Rule Set Summary for Packet Direction Chosen

	Index	Source	Destination	Services	Action	Log	Alert

Move selected item to beginning index number: 0

The following table describes the labels in this screen.

Table 80 Configuration > Firewall

LABEL	DESCRIPTION
Enable Firewall	Select this check box to activate the firewall. The ZyXEL device performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Bypass Triangle Route	Select this check box to have the ZyXEL device firewall ignore the use of triangle route topology on the network. See the *Appendices* for more on triangle route topology.
Direction	Firewall rules are grouped based on the direction of travel of packets to which they apply. Select a direction from the drop-down list box.
DoS Settings	Click the DoS settings link to configure global firewall Denial of Services settings.
Packet Direction	Use the drop-down list box to select a direction of travel of packets for which you want to configure firewall rules.
Log packets that don't match these rules.	Select the check box to create a log (when the above action is taken) for packets that are traveling in the selected direction and do not match any of the rules below.
Action for packets that don't match firewall rules	Select whether to **Block** (silently discard) or **Forward** (allow the passage of) packets that don't match any of the firewall rules you configured.
The following read-only fields summarize the rules you have created that apply to traffic traveling in the selected packet direction. The firewall rules that you configure (summarized below) take priority over the general firewall action settings above. Select an ACL hyperlink to edit that ACL rule.	
Index	This is your firewall rule number. Select a rule hyperlink to edit that rule. The ordering of your rules is important as rules are applied in turn. The **Move** field below allows you to reorder your rules.
Source	This field lists the source IP address of the incoming packet.
Destination	This field lists the destination IP address of the outgoing packet.

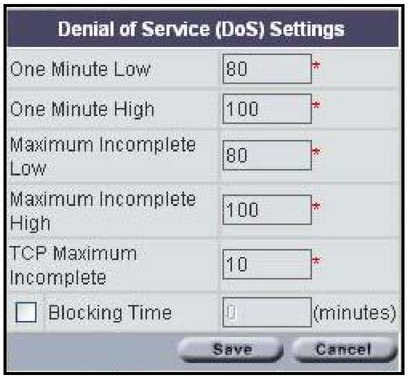
Table 80 Configuration > Firewall (continued)

LABEL	DESCRIPTION
Services	This field displays the services to which this firewall rule applies. See Figure 111 on page 225 for more information.
Action	This field displays whether the rule allows (**Forward**) or discards (**Block**) packets that match this rule.
Log	This field shows you if a log is created for packets that match the rule (**Match**), don't match the rule (**Not Match**), both (**Both**) or no log is created (**None**).
Alert	This field tells you whether this rule generates an alert (**Yes**) or not (**No**) when the rule is matched.
Move	Select a rule's Index option button and type a number for where you want to put that rule. Click **Move** to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering.
Add	Click **Add** to create a new firewall rule.
Delete	Select a rule index and then click **Delete** to delete an existing firewall rule. Note that subsequent firewall rules move up by one when you take this action.
Apply	Click **Apply** to save your changes back to the ZyXEL device.

12.5.2 DoS Settings

Click the DoS settings link to configure global firewall Denial of Services settings.

Figure 110 Configuration > Firewall > DoS Settings



Denial of Service (DoS) Settings

One Minute Low	80 *
One Minute High	100 *
Maximum Incomplete Low	80 *
Maximum Incomplete High	100 *
TCP Maximum Incomplete	10 *
□ Blocking Time	0 (minutes)

The following table describes the labels in this screen.

Table 81 Configuration > Firewall > DoS Settings

LABEL	DESCRIPTION	EXAMPLE VALUES
One Minute Low	This is the rate of new half-open sessions that causes the firewall to stop deleting half-open sessions. The ZyXEL device continues to delete half-open sessions as necessary, until the rate of new connection attempts drops below this number.	80 existing half-open sessions.
One Minute High	This is the rate of new half-open sessions that causes the firewall to start deleting half-open sessions. When the rate of new connection attempts rises above this number, the ZyXEL device deletes half-open sessions as required to accommodate new connection attempts.	100 half-open sessions per minute. The above numbers cause the ZyXEL device to start deleting half-open sessions when more than 100 session establishment attempts have been detected in the last minute, and to stop deleting half-open sessions when fewer than 80 session establishment attempts have been detected in the last minute.
Maximum Incomplete Low	This is the number of existing half-open sessions that causes the firewall to stop deleting half-open sessions. The ZyXEL device continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below this number.	80 existing half-open sessions.
Maximum Incomplete High	This is the number of existing half-open sessions that causes the firewall to start deleting half-open sessions. When the number of existing half-open sessions rises above this number, the ZyXEL device deletes half-open sessions as required to accommodate new connection requests. Do not set **Maximum Incomplete High** to lower than the current **Maximum Incomplete Low** number.	100 existing half-open sessions. The above values causes the ZyXEL device to start deleting half-open sessions when the number of existing half-open sessions rises above 100, and to stop deleting half-open sessions with the number of existing half-open sessions drops below 80.

Table 81 Configuration > Firewall > DoS Settings (continued)

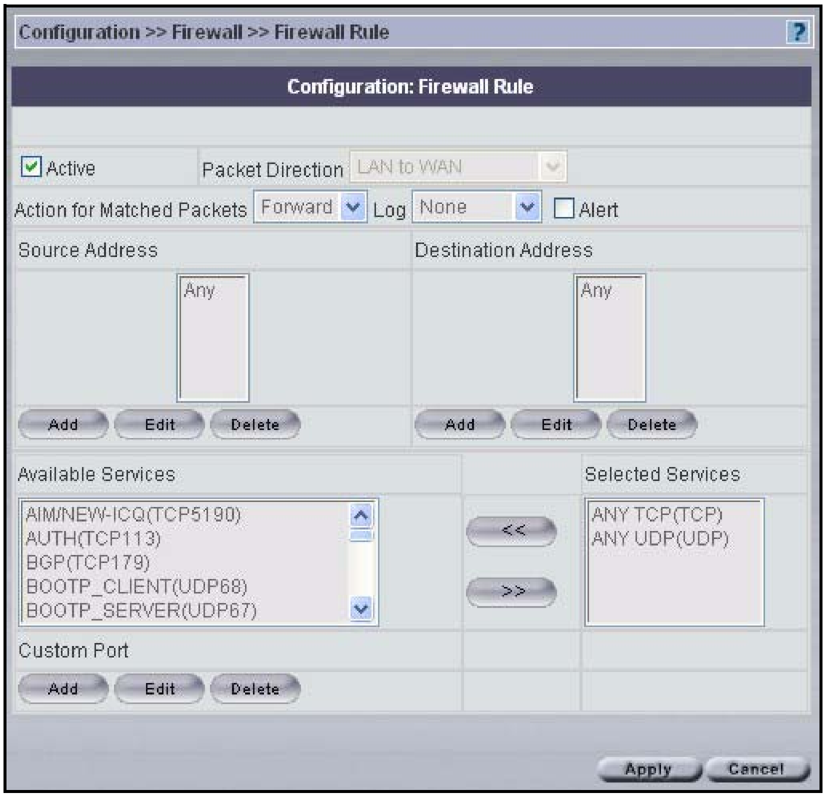
LABEL	DESCRIPTION	EXAMPLE VALUES
TCP Maximum Incomplete	This is the number of existing half-open TCP sessions with the same destination host IP address that causes the firewall to start dropping half-open sessions to that same destination host IP address. Enter a number between 1 and 256. As a general rule, you should choose a smaller number for a smaller network, a slower system or limited bandwidth	10 existing half-open TCP sessions
Blocking Time	When **TCP Maximum Incomplete** is reached you can choose if the next session should be allowed or blocked. If you check **Blocking Time** any new sessions will be blocked for the length of time you specify in the next field (min) and all old incomplete sessions will be cleared during this period. If you want strong security, it is better to block the traffic for a short time, as it will give the server some time to digest the loading.	Select this check box to specify a number in minutes (min) text box.
(minutes)	Enter the length of **Blocking Time** in minutes.	0
Save	Click **Save** to save your changes and return to the previous screen.	
Cancel	Click **Cancel** to return to the previous screen.	

12.5.3 Add/Edit a Firewall Rule

Each device has a different number of rules and custom ports; see the device User Guide for more details.

In Figure 112 on page 226, select an existing rule to edit it or click **Add** to create a new firewall rule.

Figure 111 Configuration >Firewall > Edit



Configuration >> Firewall >> Firewall Rule

Configuration: Firewall Rule

☑ Active

Packet Direction: LAN to WAN

Action for Matched Packets: Forward

Log: None

□ Alert

Source Address: Any

Destination Address: Any

Available Services:
AIM/NEW-ICQ(TCP5190)
AUTH(TCP113)
BGP(TCP179)
BOOTP_CLIENT(UDP68)
BOOTP_SERVER(UDP67)

Selected Services:
ANY TCP(TCP)
ANY UDP(UDP)

Custom Port

The following table describes the labels in this screen.

Table 82 Configuration >Firewall > Edit

LABEL	DESCRIPTION
Active	Check the **Active** check box to have the ZyXEL device use this rule. Leave it unchecked if you do not want the ZyXEL device to use the rule after you apply it
Packet Direction	Use the drop-down list box to select the direction of packet travel to which you want to apply this firewall rule.
Action for matched packets	Select whether to **Block** (silently discard) or **Forward** (allow the passage of) packets that are traveling in the selected direction.
Log	This field determines if a log is created for packets that match the rule (**Match**), don't match the rule (**Not Match**), both (**Both**) or no log is created (**None**). Go to the **Log Settings** page and select the **Access Control** logs category to have the ZyXEL device record these logs.
Alert	Check the **Alert** check box to determine that this rule generates an alert when the rule is matched.
Source Address	Click **Add** to add a new address, **Edit** to edit an existing one or **Delete** to delete one. Please see the next section for more information on adding and editing source addresses.
Destination Address	Click **Add** to add a new address, **Edit** to edit an existing one or **Delete** to delete one. Please see the following section on adding and editing destination addresses.
Available/ Selected Services	Highlight a service from the **Available Services** box on the left, then click **>>** to add it to the **Selected Services** box on the right. To remove a service, highlight it in the **Selected Services** box on the right, then click **<<**.
Custom Port	

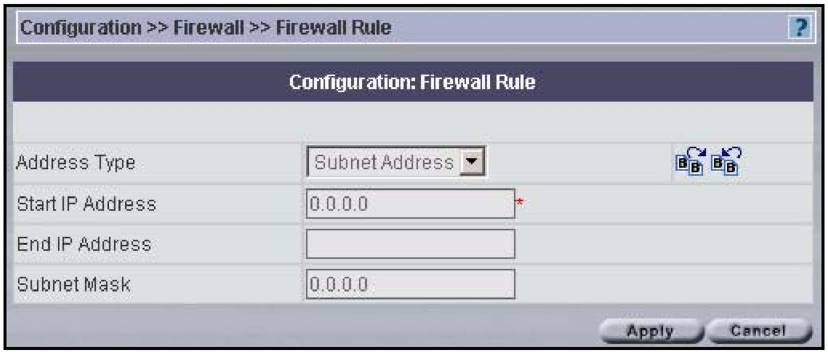
Table 82 Configuration >Firewall > Edit (continued)

LABEL	DESCRIPTION
Add	Click this button to bring up the screen that you use to configure a new custom service that is not in the predefined list of services.
Edit	Select a custom service (denoted by an *) from the **Available Services** list and click this button to edit the service.
Delete	Select a custom service (denoted by an *) from the **Available Services** list and click this button to remove the service.
Apply	Click **Apply** to save the current rule setting to the device.
Cancel	Click **Cancel** to exit this screen without saving,

12.5.4 Add/Edit Source/Destination IP Addresses

Click **Add** or **Edit** under **Source Address** or **Destination Address** to add or edit a source or destination IP address.

Figure 112 Configuration >Firewall > IP Address



Configuration >> Firewall >> Firewall Rule

Configuration: Firewall Rule

Address Type	Subnet Address
Start IP Address	0.0.0.0 *
End IP Address	
Subnet Mask	0.0.0.0

The following table describes the labels in this screen.

Table 83 Configuration > Firewall > IP Address

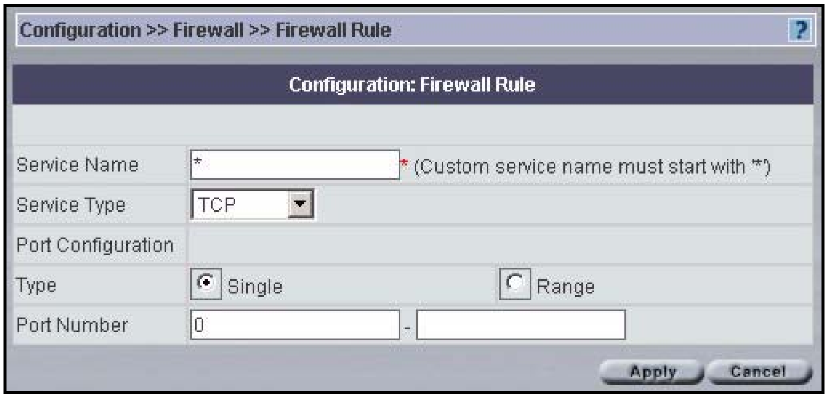
	DESCRIPTION
Address Type	Do you want your rule to apply to packets with a particular (single) IP, a range of IP addresses (e.g., 192.168.1.10 to 192.169.1.50), a subnet or any IP address? Select an option from the drop-down list box that includes: **Single Address**, **Range Address**, **Subnet Address** and **Any Address**.
Start IP Address	Enter the single IP address or the starting IP address in a range here.
End IP Address	Enter the ending IP address in a range here.
Subnet Mask	Enter the subnet mask here, if applicable.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

12.5.5 Custom Ports

Configure customized ports for services not predefined by the ZyXEL device. For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

Click **Add** or **Edit** under **Custom Port** to add or edit a custom port.

Figure 113 Configuration > Firewall > Firewall Custom Port



Configuration >> Firewall >> Firewall Rule

Configuration: Firewall Rule

Service Name: * * (Custom service name must start with "*")

Service Type: TCP

Port Configuration

Type: ● Single ○ Range

Port Number: 0 -

The following table describes the labels in this screen.

Table 84 Configuration > Firewall > Firewall Custom Port

LABEL	DESCRIPTION
Service Name	Enter a unique name for your custom port. All custom ports must begin with * to identify it as such in the Available Services list box in Figure 111 on page 225.
Service Type	Choose the IP port (**TCP**, **UDP** or **Both**) that defines your customized port from the drop down list box.
Port Configuration	
Type	Click **Single** to specify one port only or **Range** to specify a span of ports that define your customized service
Port Number	Enter a single port number or the range of port numbers that define your customized service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving,

CHAPTER 13 Configuration > Device Log

Use these screens to configure device logs. Not all devices have the centralized feature.

13.1 Device Logging Options

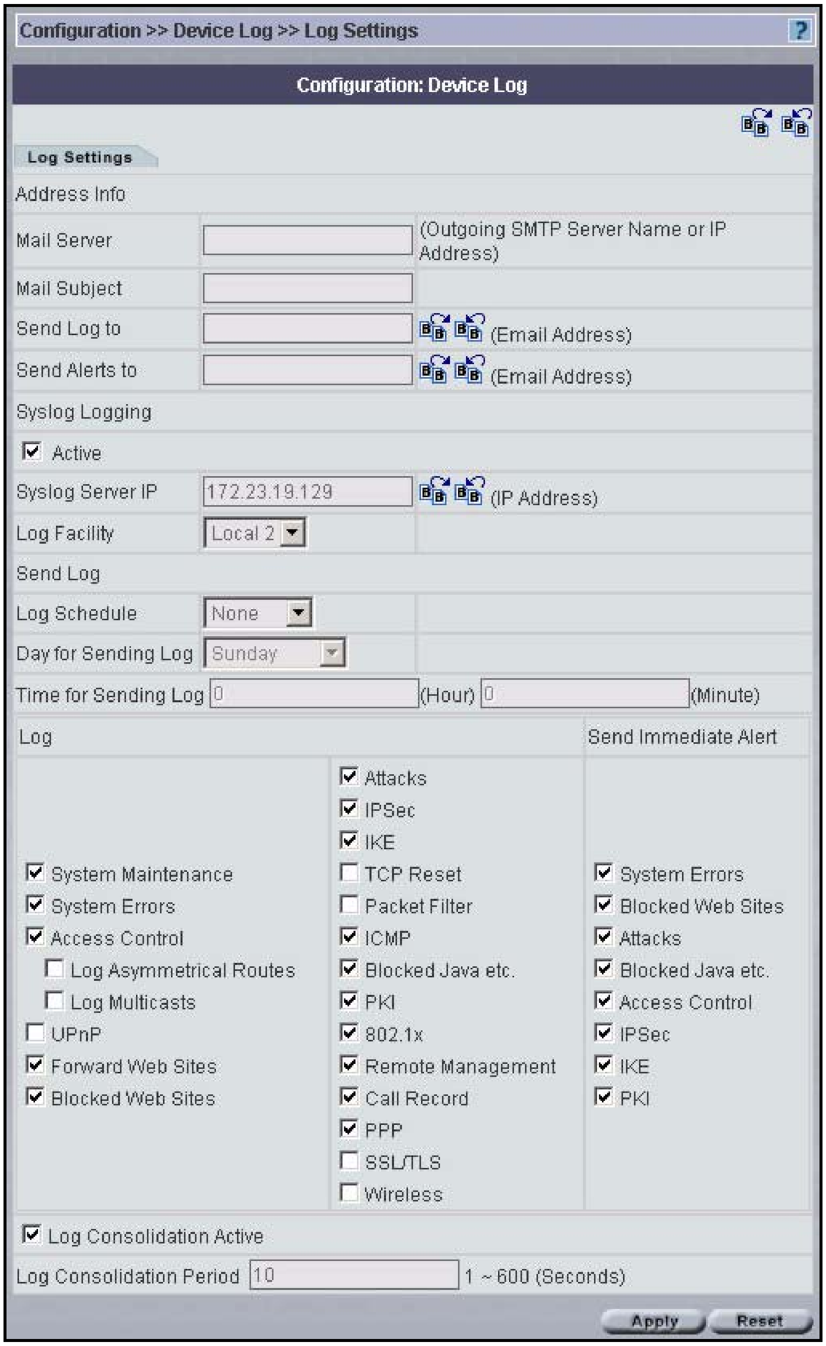
Use the **Logging Options** screen to configure to where the ZyXEL device is to send logs; the schedule for when the ZyXEL device is to send the logs and which logs and/or immediate alerts the ZyXEL device is to send.

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites or web sites with restricted web features such as cookies, active X and so on. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **Device** screen. Alerts display in red and logs display in black.

Alerts are e-mailed as soon as they happen. Logs may be e-mailed as soon as the log is full (see Log Schedule). Selecting many alert and/or log categories (especially Access Control) may result in many e-mails being sent.

To change a ZyXEL devices log settings, select a device, click **Configuration** > **Device Log**. The screen appears as shown next.

Figure 114 Configuration > Device Log > Log Settings



Configuration >> Device Log >> Log Settings

Configuration: Device Log

Log Settings

Address Info

Mail Server		(Outgoing SMTP Server Name or IP Address)
Mail Subject		
Send Log to		(Email Address)
Send Alerts to		(Email Address)

Syslog Logging

☑ Active

Syslog Server IP	172.23.19.129	(IP Address)
Log Facility	Local 2	

Send Log

Log Schedule	None
Day for Sending Log	Sunday
Time for Sending Log	0 (Hour) 0 (Minute)

Log

☑ System Maintenance
☑ System Errors
☑ Access Control
□ Log Asymmetrical Routes
□ Log Multicasts
□ UPnP
☑ Forward Web Sites
☑ Blocked Web Sites

☑ Attacks
☑ IPSec
☑ IKE
□ TCP Reset
□ Packet Filter
☑ ICMP
☑ Blocked Java etc.
☑ PKI
☑ 802.1x
☑ Remote Management
☑ Call Record
☑ PPP
□ SSL/TLS
□ Wireless

Send Immediate Alert

☑ System Errors
☑ Blocked Web Sites
☑ Attacks
☑ Blocked Java etc.
☑ Access Control
☑ IPSec
☑ IKE
☑ PKI

☑ Log Consolidation Active

Log Consolidation Period 10 1 ~ 600 (Seconds)

The following table describes the labels in this screen.

Table 85 Configuration > Device Log > Log Settings

LABEL	DESCRIPTION
Address Info	
Mail Server	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via e-mail.
Mail Subject	Type a title that you want to be in the subject line of the log e-mail message that the ZyXEL device sends.
Send Log To	Logs are sent to the e-mail address specified in this field. If this field is left blank, logs will not be sent via e-mail.
Send Alerts To	Alerts are sent to the e-mail address specified in this field. If this field is left blank, alerts will not be sent via e-mail.
Syslog Logging	Syslog logging sends a log to an external syslog server used to store logs.
Active	Click **Active** to enable syslog logging.
Syslog Server IP Address	Enter the server IP address of the syslog server that will log the selected categories of logs. The device syslog server must be the same as the Vantage syslog server.
Log Facility	Select a location from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Send Log	
Log Schedule	This drop-down menu is used to configure the frequency of log messages being sent as E-mail: • Daily • Weekly • Hourly • When Log is Full • None. If you select **Weekly** or **Daily**, specify a time of day when the E-mail should be sent. If you select **Weekly**, then also specify which day of the week the E-mail should be sent. If you select **When Log is Full**, an alert is sent when the log fills up. If you select **None**, no log messages are sent
Day for Sending Log	Use the drop down list box to select which day of the week to send the logs.
Time for Sending Log	Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.
Log	Select the categories of logs that you want to record. Logs include alerts.
Send Immediate Alert	Select the categories of alerts for which you want the ZyXEL device to instantly e-mail alerts to the e-mail address specified in the **Send Alerts To** field.
Log Consolidation	
Active	Some logs (such as the Attacks logs) may be so numerous that it becomes easy to ignore other important log messages. Select this check box to merge logs with identical messages into one log.
Log Consolidation Period	Specify the time interval during which the ZyWALL merges logs with identical messages into one log.

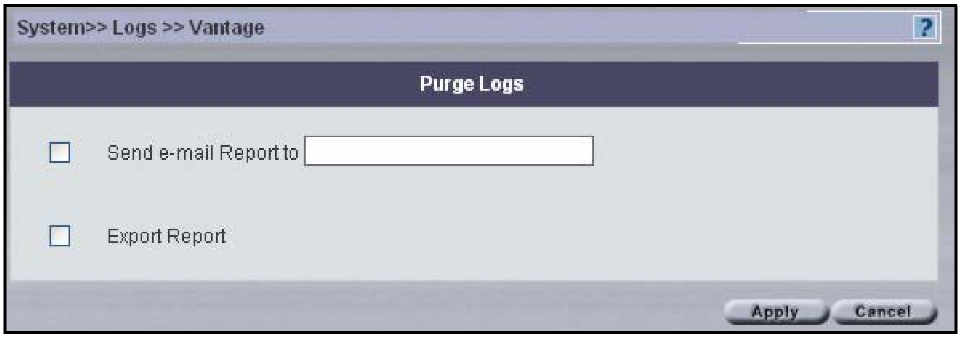
Table 85 Configuration > Device Log > Log Settings (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

13.2 Purge Logs

Click **Purge** to remove logs from the Vantage database. A report of purged logs can be e-mailed and/or downloaded to your computer.

Figure 115 System > Logs > Purge Device Logs



The following table describes the labels in this screen.

Table 86 System > Logs > Purge Device Logs

	DESCRIPTION
Send e-mail report to	Select the checkbox and enter valid e-mail address(es) of those who should receive a report on logs that have been purged. Separate more than one E-mail address by a comma.
Export Report	Select this checkbox to send a report on logs that have been purged, to the e-mail addresses defined in notifications.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to begin configuring this screen afresh.

CHAPTER 14
Configuration > ADSL Monitor

Use this screen to monitor your ADSL link.

14.1 Introduction

The Prestige is an ADSL device compatible with the ADSL/ADSL2/ADSL2+ standards. Maximum data rates attainable by the Prestige for each standard are shown in the next table.

Table 87 ADSL Standards

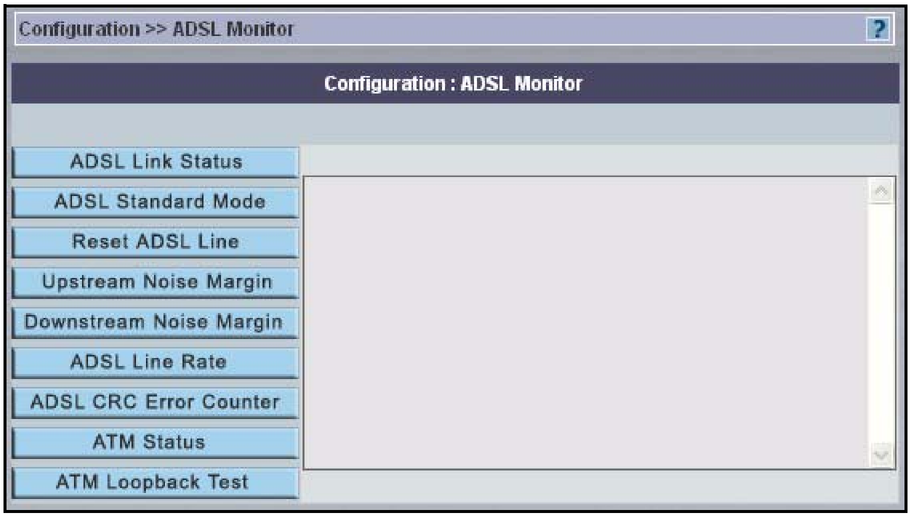
DATA RATE/STANDARD	UPSTREAM	DOWNSTREAM
ADSL	832 Kips	8Mbps
ADSL2	3.5Mbps	12Mbps
ADSL2+	3.5Mbps	24Mbps

14.2 Configuring ADSL Monitor

Select an ADSL device and click **Configuration** > **ADSL Monitor**.

Click a label to have the information displayed in the text box.

Figure 116 Configuration > ADSL Monitor



The following table describes the labels in this screen.

Table 88 Configuration > ADSL Monitor

LABEL	DESCRIPTION
ADSL Link Status	This is the status of your ADSL link.
ADSL Standard Mode	This refers to the operational protocol the Prestige and the DSLAM (Digital Subscriber Line Access Multiplexer) are using. The standard the ISP supports determines the maximum upstream and downstream speeds attainable. Actual speeds attained also depend on the distance from your ISP, noise, line quality, etc.
Reset ADSL Line	Click this button to reinitialize the ADSL line. The large text box above then displays the progress and results of this operation, for example: "Start to reset ADSL Loading ADSL modem F/W... Reset ADSL Line Successfully!"
Upstream Noise Margin	Click this button to display the upstream noise margin.
Downstream Noise Margin	Click this button to display the downstream noise margin.
ADSL Line Rate	Click this button to display the upstream and downstream rates of your ADSL link.
ADSL CRC Error Counter	Click this computer to have your device perform a Cyclic Redundancy Checksum. The Prestige sends a sequence of bits to every block of data or frame. This is called a frame check sequence (FCS). The receiving computer uses a predetermined number to divide the frame. If there is a remainder, then the frame is considered corrupted and a retransmission is requested.
ATM Status	Click this button to view ATM status.
ATM Loopback Test	Click this button to start the ATM loopback test. Make sure you have configured at least one PVC with proper VPIs/VCIs before you begin this test. The Prestige sends an OAM F5 packet to the DSLAM/ATM switch and then returns it (loops it back) to the Prestige. The ATM loopback test is useful for troubleshooting problems with the DSLAM and ATM network.

CHAPTER 15 Configuration > X Auth

This chapter shows you how to configure the authentication server using Vantage.

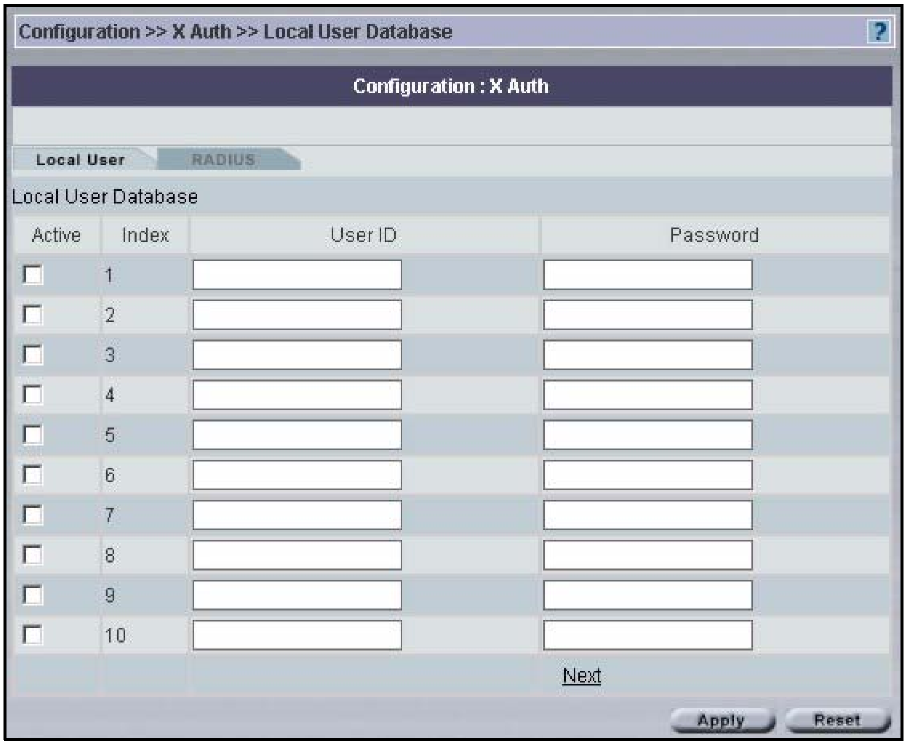
15.1 Overview

A ZyWALL set to be a VPN extended authentication server can use either the local user database internal to the ZyWALL or an external RADIUS server for an unlimited number of users. The ZyWALL uses the same local user database for VPN extended authentication and wireless LAN security.

15.2 Configuring Local User Database

To change your ZyWALL's local user list, click **Configuration**, **X-Auth**. The **Local User Database** screen appears as shown.

Figure 117 Configuration > X Auth > Local User Database



Configuration >> X Auth >> Local User Database

Configuration : X Auth

Local User Database

Active	Index	User ID	Password
□	1		
□	2		
□	3		
□	4		
□	5		
□	6		
□	7		
□	8		
□	9		
□	10		

The following table describes the labels in this screen.

Table 89 Configuration > X Auth > Local User Database

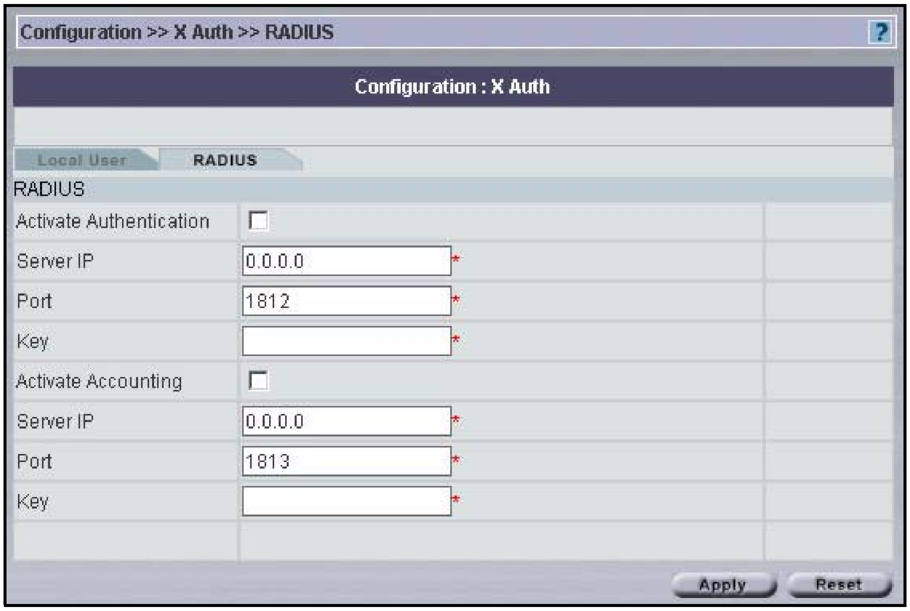
LABEL	DESCRIPTION
Active	Select this check box to enable the user profile.
Index	This is the index number of the **Local User Database** entry (row).
User ID	Enter the user name of the user profile.
Password	Enter a password up to 31 characters long for this user profile.
Next	Click **Next** to view the next page of **Local User Database** entries.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

15.3 Configuring RADIUS

Use RADIUS if you want to authenticate wireless users using an external server.

To set up your ZyWALL’s RADIUS Server settings, click **Configuration**, **X Auth**, then the **RADIUS** tab. The screen appears as shown.

Figure 118 Configuration > X Auth > RADIUS



RADIUS

Activate Authentication	□
Server IP	0.0.0.0 *
Port	1812 *
Key	*
Activate Accounting	□
Server IP	0.0.0.0 *
Port	1813 *
Key	*

The following table describes the labels in this screen.

Table 90 Configuration > X Auth > RADIUS

LABEL	DESCRIPTION
Activate Authentication	Select the check box to enable user authentication through an external authentication server. Clear the check box to enable user authentication using the local user profile on the ZyWALL.
Server IP	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	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 with additional information.
Key	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the ZyWALL. The key is not sent over the network. This key must be the same on the external authentication server and ZyWALL.
Activate Accounting	Select the check box to enable user accounting through an external authentication server.
Server IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Port Number	The default port of the RADIUS server for accounting is **1813**. You need not change this value unless your network administrator instructs you to do so with additional information.
Key	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the ZyWALL. The key is not sent over the network. This key must be the same on the external accounting server and ZyWALL.

Table 90 Configuration > X Auth > RADIUS

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

CHAPTER 16 Configuration > Device Alarms

Use these screens to view and manage device alarms.

16.1 Device Alarms

Select a domain in the object tree to view alarms for that domain.

Alarms are time-critical information that the ZyXEL device automatically sends out at the time of occurrence.

16.1.1 Alarm Classifications

There are four alarm severity classifications.

Table 91 Alarm Severity

SEVERITY	DESCRIPTION
All	This displays all alarm severities.
Fatal	This is an alarm such as unrecoverable hardware failure.
Major	This is an alarm such as an attack.
Minor	This is an alarm such as a recoverable hardware error.
Warning	This is an alarm such as an illegal Vantage login attempt.

16.1.2 Alarm States

When an alarm is received by Vantage, it can be in one of three states:

Table 92 Alarm States

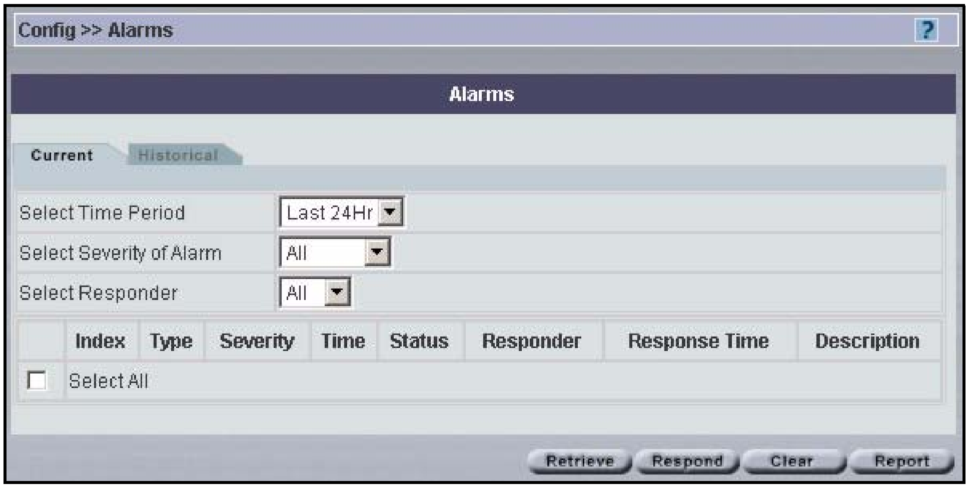
STATE	DESCRIPTION
Active	This is the initial state of an alarm, which means this alarm is new and no one has assumed responsibility for handling it yet.
Acknowledged	This means that one administrator has decided to respond to the cause of this alarm. Other administrators see that person's name in their alarm screen and so duplicate effort in solving the same problem is avoided.
Cleared	After the administrator has solved the cause of the alarm, he/she can clear the alarm. When an alarm is cleared, it is removed from the current alarm screen and becomes an historical alarm.

16.1.3 Current Alarms Screen

This screen includes filters for time, alarm type, alarm severity type and the administrator who responded to the alarm.

You may also configure to have administrators automatically e-mailed when an alarm occurs in the **System > Preferences > Notifications** screen. Alarm becomes historical after selecting **Clear**.

Figure 119 Configuration > Device Alarms > Current



Select Time Period: Last 24Hr

Select Severity of Alarm: All

Select Responder: All

	Index	Type	Severity	Time	Status	Responder	Response Time	Description
☐	Select All							

The following table describes the labels in this screen.

Table 93 Configuration > Device Alarms > Current

LABEL	DESCRIPTION
Select Time Period	Select the time period (24, 48 or 72 hours) for which you wish to view logs.
Select Severity of Alarm.	Select the severity of the alarm (see above) for which you wish to view logs
Select Responder	Select **All** or **root** to display all of the administrators or root administrators that have responded to the cause of this alarm. Other administrators see that person’s name in their alarm screen and so duplicate effort in solving the same problem is avoided.
Index	This is a number assigned to an alarm record.
Type	The field displays the categories that you select in the **Log Settings** page.
Severity	This field displays the alarm severity. See the alarm classifications above.
Time	This field displays the time the log was recorded.
Status	This field states the reason for the log.
Responder	This field displays the administrator who has responded to the alarm.
Response Time	This field displays the time of response since an administrator first received the alarm.
Description	This field displays a brief explanation of the administrator’s response.

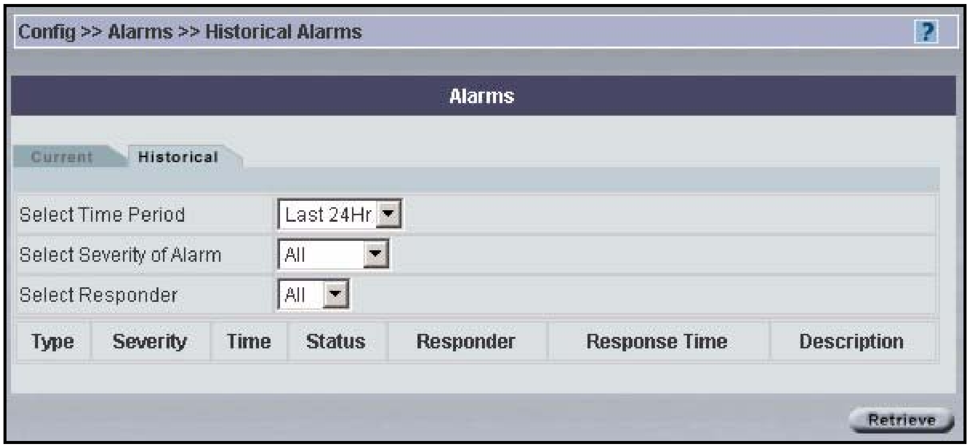
Table 93 Configuration > Device Alarms > Current (continued)

LABEL	DESCRIPTION
Retrieve	Click **Retrieve** to renew the logs displayed for the selected device.
Respond	Click **Respond** to create a response to an alarm.
Clear	Click **Clear** to erase the logs displayed for the selected device. Only the root administrator can clear logs.
Report	Click **Report** to generate a report on the logs for the time period selected.

16.1.4 Historical Alarms Screen

This screen displays a history of device alarm logs.

Figure 120 Configuration > Device Alarms > Historical



Config >> Alarms >> Historical Alarms

Alarms

Current | Historical

Select Time Period	Last 24Hr
Select Severity of Alarm	All
Select Responder	All

Type	Severity	Time	Status	Responder	Response Time	Description

The following table describes the labels in this screen.

Table 94 Configuration > Device Alarms > Historical

LABEL	DESCRIPTION
Select Time Period	Select the time period (24, 48 or 72 hours) for which you wish to view logs.
Select Severity of Alarm	Select the severity of the alarm (see above) for which you wish to view logs.
Select Responder	Select **All** or **root** to display all of the administrators or root administrators that have responded to the cause of this alarm. Other administrators see that person's name in their alarm screen and so duplicate effort in solving the same problem is avoided.
Index	This is a number assigned to an alarm record.
Type	The field displays the categories that you select in the **Log Settings** page.
Severity	This field displays the alarm severity. See the alarm classifications above.
Time	This field displays the time the log was recorded.
Status	This field states the reason for the log.
Responder	This field displays the administrator who has responded to the alarm.

Table 94 Configuration > Device Alarms > Historical (continued)

LABEL	DESCRIPTION
Response Time	This field displays the time of response since an administrator first received the alarm.
Description	This field displays a brief explanation of the administrator’s response.
Retrieve	Click **Retrieve** for Vantage to pull the selected logs from the selected device.

CHAPTER 17
Configuration > DNS

This chapter shows you how to configure the DNS screens.

17.1 DNS Overview

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it. The ZyWALL uses a system DNS server (in the order you specify in the **DNS System** screen) to resolve domain names, for example, VPN, DDNS and the time server.

17.2 DNS Server Address Assignment

The ZyWALL can get the DNS server addresses in the following ways.

1. The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.
2. If your ISP dynamically assigns the DNS server IP addresses (along with the ZyWALL's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.
3. You can manually enter the IP addresses of other DNS servers. These servers can be public or private. A DNS server could even be behind a remote IPSec router (see Private DNS Server on page 243.).

17.3 DNS Servers

There are three places where you can configure DNS setup on the ZyWALL.

1. Use the **DNS System** screen to configure the ZyWALL to use a DNS server to resolve domain names for ZyWALL system features like VPN, DDNS and the time server.
2. Use the **DNS LAN** screen to configure the DNS server information that the ZyWALL sends to the DHCP client devices on the LAN.
3. Use the **REMOTE MGMT DNS** screen to configure the ZyWALL (in router mode) to accept or discard DNS queries.

17.4 Address Record

An address record contains the mapping of a fully qualified domain name (FQDN) to an IP address. An FQDN consists of a host and domain name and includes the top-level domain. For example, www.zyxel.com.tw is a fully qualified domain name, where "www" is the host, "zyxel" is the second-level domain, and "com.tw" is the top level domain. mail.myZyXEL.com.tw is also a FQDN, where "mail" is the host, "myZyXEL" is the second-level domain, and "com.tw" is the top level domain.

The ZyWALL allows you to configure address records about the ZyWALL itself or another device. This way you can keep a record of DNS names and addresses that people on your network may use frequently. If the ZyWALL receives a DNS query for an FQDN for which the ZyWALL has an address record, the ZyWALL can send the IP address in a DNS response without having to query a DNS name server.

17.4.1 DNS Wildcard

Enabling the wildcard feature for your host causes *.yourhost.com to be aliased to the same IP address as yourhost.com. This feature is useful if you want to be able to use, for example, www.yourhost.com and still reach your hostname.

17.5 Name Server Record

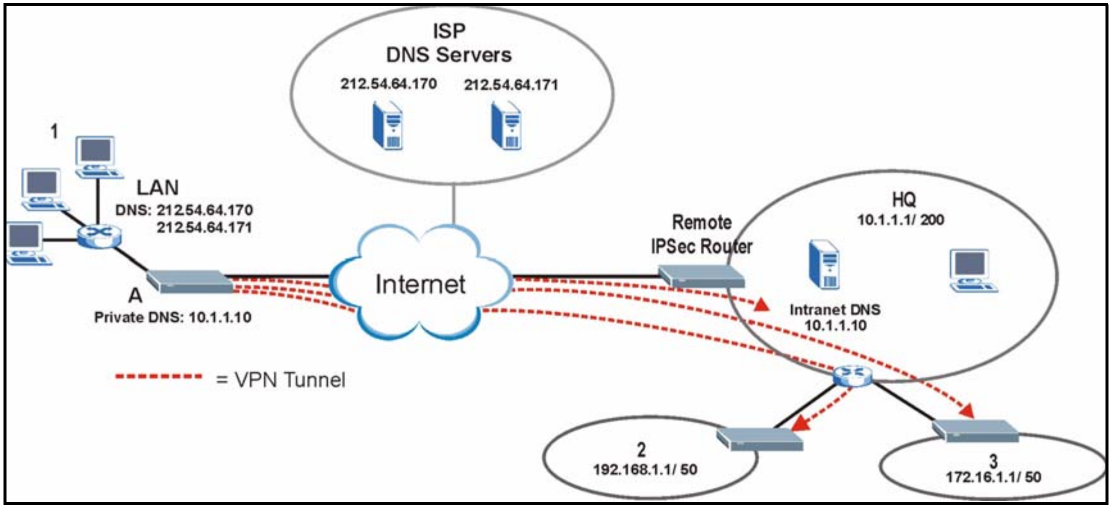
A name server record contains a DNS server's IP address. The ZyWALL can query the DNS server to resolve domain names for features like VPN, DDNS and the time server. A domain zone may also be included. A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name.

17.5.1 Private DNS Server

In cases where you want to use domain names to access Intranet servers on a remote private network that has a DNS server, you must identify that DNS server. You cannot use DNS servers on the LAN or from the ISP since these DNS servers cannot resolve domain names to private IP addresses on the remote private network.

The following figure depicts an example where three VPN tunnels are created from ZyWALL A; one to branch office **2**, one to branch office **3** and another to headquarters (**HQ**). In order to access computers that use private domain names on the **HQ** network, the ZyWALL at branch office **1** uses the Intranet DNS server in headquarters.

Figure 121 Private DNS Server Example



Note: If you do not specify an Intranet DNS server on the remote network, then the VPN host must use IP addresses to access the computers on the remote private network.

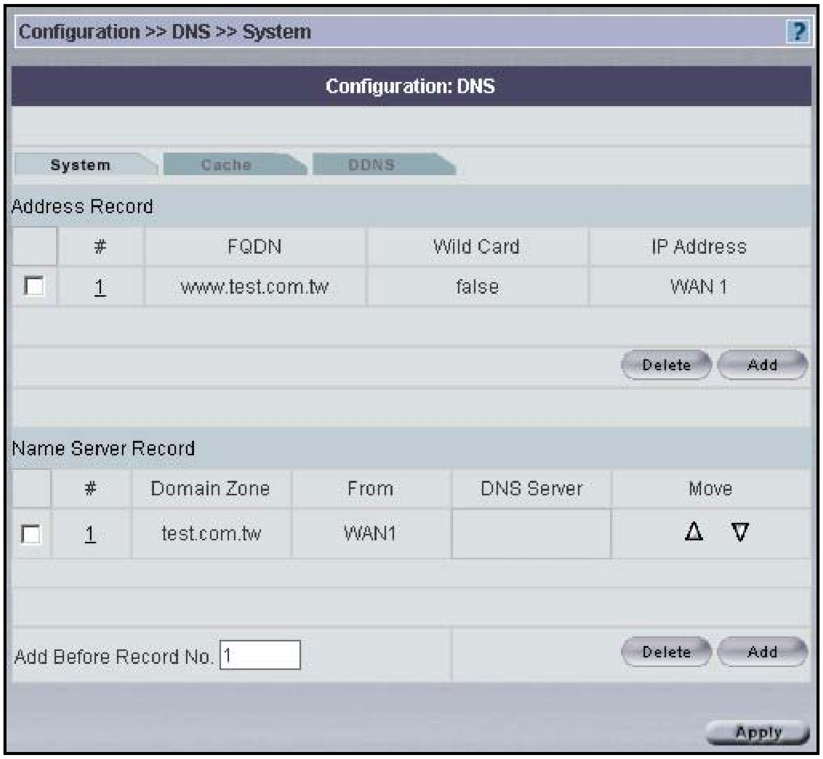
17.6 DNS Screens

Click **Configuration**, **DNS** to configure **System**, **Cache** and **DDNS**. The **System** tab is shown next.

17.6.1 DNS System Configuration

To configure your device's DNS address and name server records, click the **System** tab in **DNS**. The screen appears as shown.

Figure 122 Configuration > DNS > System



Address Record

	#	FQDN	Wild Card	IP Address
□	1	www.test.com.tw	false	WAN 1

Name Server Record

	#	Domain Zone	From	DNS Server	Move
□	1	test.com.tw	WAN1		∆ ∇

Add Before Record No. 1

The following table describes the labels in this screen.

Table 95 Configuration > DNS > System

LABEL	DESCRIPTION
Address Record	An address record specifies the mapping of a fully qualified domain name (FQDN) to an IP address. An FQDN consists of a host and domain name and includes the top-level domain. For example, www.zyxel.com.tw is a fully qualified domain name, where "www" is the host, "zyxel" is the second-level domain, and "com.tw" is the top level domain.
#	This is the index number of the address record. Click the hyperlink to go to the screen where you can edit the record.
FQDN	This is a host's fully qualified domain name.
Wildcard	This column displays whether or not the DNS wildcard feature is enabled for this domain name.
IP Address	This is the IP address of a host.
Delete	Select an address record and then click the **Delete** button to remove an existing record. A window display asking you to confirm that you want to delete the record. Note that subsequent records move up by one when you take this action.
Add	Click the **Add** button to open a screen where you can add a new address record. Refer to Table 96 on page 247 for information on the fields.

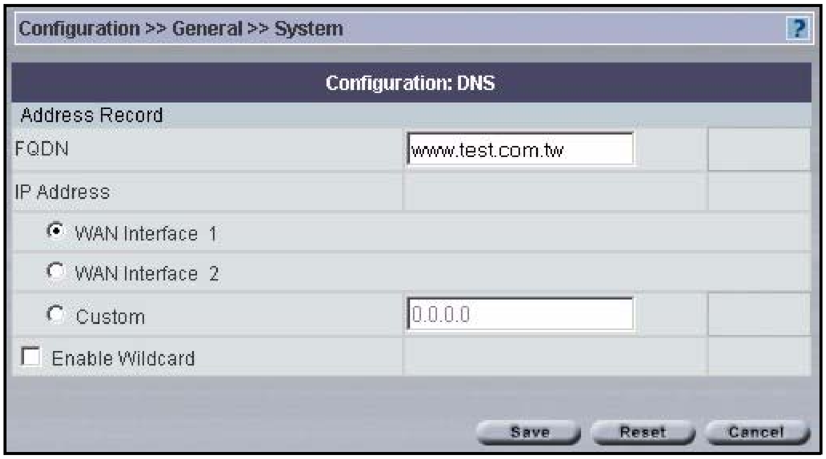
Table 95 Configuration > DNS > System (continued)

LABEL	DESCRIPTION
Name Server Record	A name server record contains a DNS server's IP address. The ZyWALL can query the DNS server to resolve domain names for features like VPN, DDNS and the time server. When the ZyWALL needs to resolve a domain name, it checks it against the name server record entries in the order that they appear in this list. A "*" indicates a name server record without a domain zone. The default record is grayed out. The ZyWALL uses this default record if the domain name that needs to be resolved does not match any of the other name server records.
#	This is the index number of the name server record. Click the hyperlink to go to the screen where you can edit the record.
Domain Zone	A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name.
From	This field displays whether the IP address of a DNS server is from a WAN interface (and which it is) or specified by the user.
DNS Server	This is the IP address of a DNS server.
Move	Click the icon to move the record up or down in the list.
Delete	Select a server record and then click the **Delete** button to remove an existing record. A window display asking you to confirm that you want to delete the record. Note that subsequent records move up by one when you take this action.
Add	Click the **Add** button to open a screen where you can create a new name server record. Enter the record number to which you want to insert the new server record below.

17.6.2 Adding an Address Record

Click **Add** in the **System** screen **Address Record** section to add an address record.

Figure 123 Configuration > DNS > System > Add Address Record



FQDN	www.test.com.tw
IP Address	
● WAN Interface 1	
○ WAN Interface 2	
○ Custom	0.0.0.0
□ Enable Wildcard	

The following table describes the labels in this screen.

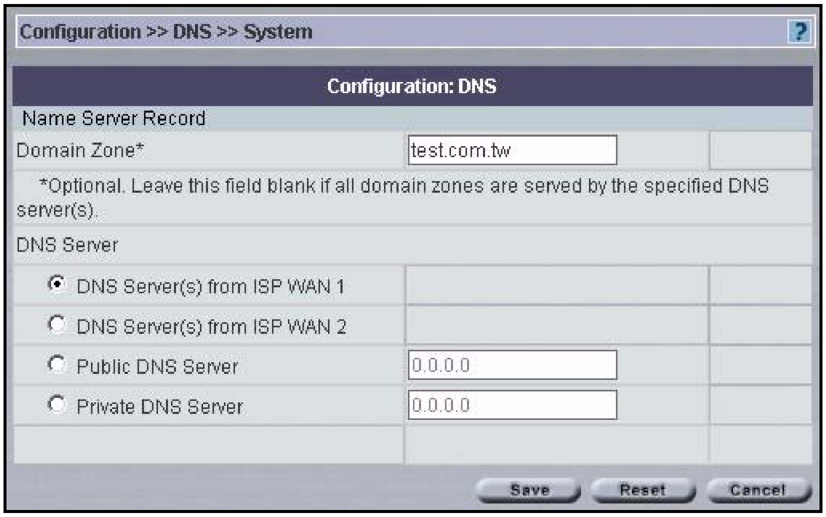
Table 96 Configuration > DNS > System > Add Address Record

LABEL	DESCRIPTION
FQDN	Type a fully qualified domain name (FQDN) of a server. An FQDN starts with a host name and continues all the way up to the top-level domain name. For example, www.zyxel.com.tw is a fully qualified domain name, where "www" is the host, "zyxel" is the second-level domain, and "com.tw" is the top level domain.
IP Address	If this entry is for one of the WAN ports, select **WAN Interface 1** or **WAN Interface 2**. For entries that are not for one of the WAN ports, select **Custom** and enter the IP address of the host in dotted decimal notation.
Enable Wildcard	Select the check box to enable DNS wildcard.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.
Cancel	Click **Cancel** to exit this screen without saving.

17.6.3 Adding a Name Server Record

Click **Add** in the **System** screen **Name Server Record** section to insert a name server record.

Figure 124 Configuration > DNS > System > Add Name Server Record



Configuration >> DNS >> System

Configuration: DNS

Name Server Record

Domain Zone* test.com.tw

*Optional. Leave this field blank if all domain zones are served by the specified DNS server(s).

DNS Server

● DNS Server(s) from ISP WAN 1

○ DNS Server(s) from ISP WAN 2

○ Public DNS Server 0.0.0.0

○ Private DNS Server 0.0.0.0

The following table describes the labels in this screen.

Table 97 Configuration > DNS > System > Add Name Server Record

LABEL	DESCRIPTION
Domain Zone	This field is optional. A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name. For example, whenever the ZyWALL receives needs to resolve a zyxel.com.tw domain name, it can send a query to the recorded name server IP address. Leave this field blank if all domain zones are served by the specified DNS server(s).
DNS Server	Select the **DNS Server(s) from ISP WAN 1** or **DNS Server(s) from ISP WAN 2** radio button if your ISP dynamically assigns DNS server information. The fields below display the (read-only) DNS server IP address(es) that the ISP assigns. **N/A** displays for any DNS server IP address fields for which the ISP does not assign an IP address. **N/A** displays for all of the DNS server IP address fields if the ZyWALL has a fixed WAN IP address. Select **Public DNS Server** if you have the IP address of a DNS server. The IP address must be public or a private address on your local LAN. Enter the DNS server's IP address in the field to the right. **Public DNS Server** entries with the IP address set to 0.0.0.0 are not allowed. Select **Private DNS Server** if the DNS server has a private IP address and is located behind a VPN peer. Enter the DNS server's IP address in the field to the right. With a private DNS server, you must also configure the first DNS server entry in the **DNS LAN** screen to use **DNS Relay**. You must also configure a VPN rule since the ZyWALL uses a VPN tunnel when it relays DNS queries to the private DNS server. The rule must include the LAN IP address of the ZyWALL as a local IP address and the IP address of the DNS server as a remote IP address. **Private DNS Server** entries with the IP address set to 0.0.0.0 are not allowed.
Save	Click **Save** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.
Cancel	Click **Cancel** to exit this screen without saving.

17.7 DNS Cache

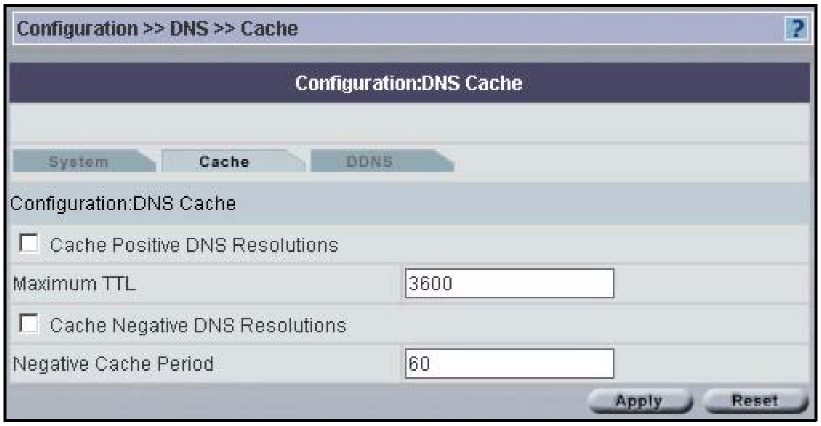
DNS cache is the temporary storage area where a router stores responses from DNS servers. When the ZyWALL receives a positive or negative response for a DNS query, it records the response in the DNS cache. A positive response means that the ZyWALL received the IP address for a domain name that it checked with a DNS server within the five second DNS timeout period. A negative response means that the ZyWALL did not receive a response for a query it sent to a DNS server within the five second DNS timeout period.

When the ZyWALL receives DNS queries, it compares them against the DNS cache before querying a DNS server. If the DNS query matches a positive entry, the ZyWALL responses with the IP address from the entry. If the DNS query matches a negative entry, the ZyWALL replies that the DNS query failed.

17.8 Configure DNS Cache

To configure a device's DNS caching, click **Configuration** > **DNS** > **Cache**. The screen appears as shown.

Figure 125 Configuration > DNS > Cache



Configuration >> DNS >> Cache

Configuration:DNS Cache

Configuration:DNS Cache

☐ Cache Positive DNS Resolutions

Maximum TTL: 3600

☐ Cache Negative DNS Resolutions

Negative Cache Period: 60

The following table describes the labels in this screen.

Table 98 Configuration > DNS > Cache

LABEL	DESCRIPTION
DNS Cache Setup	
Cache Positive DNS Resolutions	Select the check box to record the positive DNS resolutions in the cache. Caching positive DNS resolutions helps speed up the ZyWALL's processing of commonly queried domain names and reduces the amount of traffic that the ZyWALL sends out to the WAN.
Maximum TTL	Type the maximum time to live (TTL) (60 to 3600 seconds). This sets how long the ZyWALL is to allow a positive resolution entry to remain in the DNS cache before discarding it.

Table 98 Configuration > DNS > Cache

LABEL	DESCRIPTION
Cache Negative DNS Resolutions	Caching negative DNS resolutions helps speed up the ZyWALL’s processing of commonly queried domain names (for which DNS resolution has failed) and reduces the amount of traffic that the ZyWALL sends out to the WAN.
Negative Cache Period	Type the time (60 to 3600 seconds) that the ZyWALL is to allow a negative resolution entry to remain in the DNS cache before discarding it.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

17.9 Dynamic DNS

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

Note: You must go to the Dynamic DNS service provider’s website and register a user account and a domain name before you can use the Dynamic DNS service with your ZyWALL.

17.9.1 DYNDNS Wildcard

Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

Note: If you have a private WAN IP address, then you cannot use Dynamic DNS.

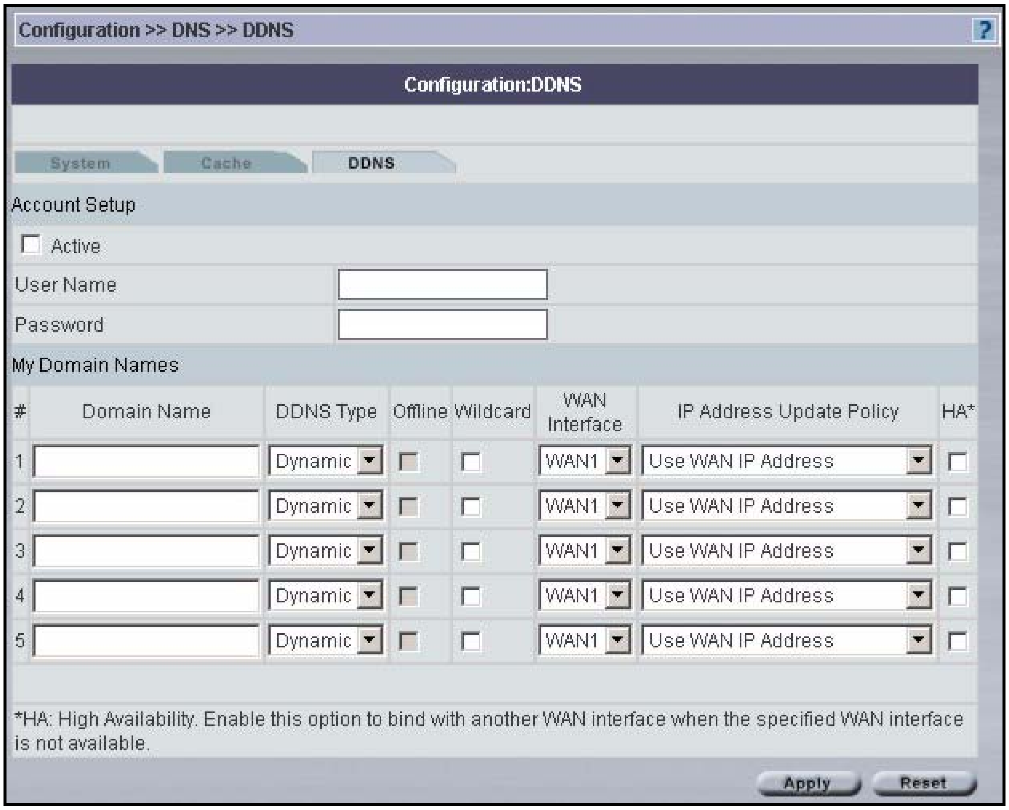
17.9.2 High Availability

A DNS server maps a domain name to a port's IP address. If that WAN port loses its connection, high availability allows the router to substitute another port's IP address for the domain name mapping.

17.10 Configuring Dynamic DNS

To change a device's DDNS, click **Configuration** > **DNS > DDNS**. The screen appears as shown.

Figure 126 Configuration > DNS > DDNS



□ Active

User Name	
Password	

#	Domain Name	DDNS Type	Offline	Wildcard	WAN Interface	IP Address Update Policy	HA*
1		Dynamic	□	□	WAN1	Use WAN IP Address	□
2		Dynamic	□	□	WAN1	Use WAN IP Address	□
3		Dynamic	□	□	WAN1	Use WAN IP Address	□
4		Dynamic	□	□	WAN1	Use WAN IP Address	□
5		Dynamic	□	□	WAN1	Use WAN IP Address	□

*HA: High Availability. Enable this option to bind with another WAN interface when the specified WAN interface is not available.

The following table describes the labels in this screen.

Table 99 Configuration > DNS > DDNS

LABEL	DESCRIPTION
Account Setup	
Active	Select this check box to use dynamic DNS.
Username	Enter your user name. You can use up to 31 alphanumeric characters (and the underscore). Spaces are not allowed.
Password	Enter the password associated with the user name above. You can use up to 31 alphanumeric characters (and the underscore). Spaces are not allowed.
My Domain Names	
Domain Name 1~5	Enter the host names in these fields.
DDNS Type	Select the type of service that you are registered for from your Dynamic DNS service provider. Select **Dynamic** if you have the Dynamic DNS service. Select **Static** if you have the Static DNS service. Select **Custom** if you have the Custom DNS service.

Table 99 Configuration > DNS > DDNS (continued)

LABEL	DESCRIPTION
Offline	This option is available when **Custom** is selected in the **DDNS Type** field. Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line.
Wildcard	Select the check box to enable DYNDNS Wildcard.
WAN Interface	Select the WAN port to use for updating the IP address of the domain name.
IP Address Update Policy	Select **Use WAN IP Address** to have the ZyWALL update the domain name with the WAN port's IP address. Select **Use User-Defined** and enter the IP address if you have a static IP address. Select **Let DDNS Server Auto Detect** only when there are one or more NAT routers between the ZyWALL and the DDNS server. This feature has the DDNS server automatically detect and use the IP address of the NAT router that has a public IP address. **Note:** The DDNS server may not be able to detect the proper IP address if there is an HTTP proxy server between the ZyWALL and the DDNS server.
HA	Select this check box to enable the high availability (HA) feature. High availability has the ZyWALL update a domain name with another port's IP address when the normal WAN port does not have a connection. If the WAN port specified in the **WAN Interface** field does not have a connection, the ZyWALL will attempt to use the IP address of another WAN port to update the domain name. When the WAN ports are in the active/passive operating mode, the ZyWALL will update the domain name with the IP address of whichever WAN port has a connection, regardless of the setting in the **WAN Interface** field. Disable this feature and the ZyWALL will only update the domain name with an IP address of the WAN port specified in the **WAN Interface** field. If that WAN port does not have a connection, the ZyWALL will not update the domain name with another port's IP address. **Note:** If you enable high availability, DDNS can also function when the ZyWALL uses the dial backup port. DDNS does not function when the ZyWALL uses traffic redirect.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

CHAPTER 18
Building Blocks (BBs)

18.1 Categories

A BB is a building block used to build a device configuration using Vantage CNM.

- A device BB is a combination of configuration BBs, which vary by model. A device can have only one Device BB. You can select any device and save its configuration as a BB ready to be applied to another device (of the same model type). This allows rapid configuration of new devices as you can essentially copy one device's configuration to another.
- A configuration BB is the template of a single configuration menu item, such as **Configuration** > **General** or **Configuration** > **Firewall**. You can create a new configuration BB or save an existing configuration item as a BB and it is then available to apply to other devices of the same model type. Configuration BBs may vary by model type. For example, you should not apply a ZyWALL 10W firewall configuration BB to a ZyWALL 70.
- A component BB is the template a portion of a configuration menu item, such as IP address, e-mail address, etc.

18.2 BB Properties

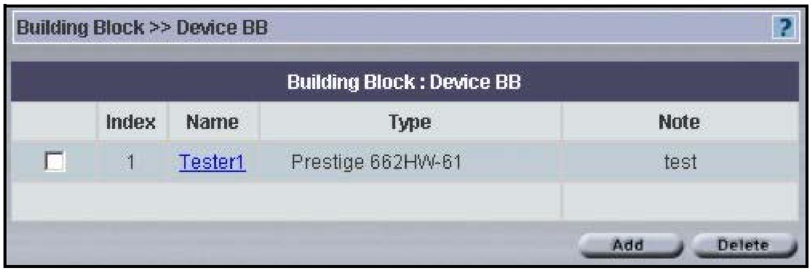
You can only view (and use) BBs in your own domain. You cannot view other administrator's BBs, including BBs created by the root administrator. When creating new BBs from old ones use the save as icon to save as a new BB.

If you modify a BB, changes only affect new device configurations that use this BB and not previous ones.

18.3 Configuring Device BB Menus

You don't have to select a folder or device in the object tree first; click a BB category such as **Building Block** > **Device BB**.

Figure 127 Building Block > Device BB



Building Block >> Device BB

	Index	Name	Type	Note
☐	1	Tester1	Prestige 662HW-61	test

The following table describes the fields in this screen

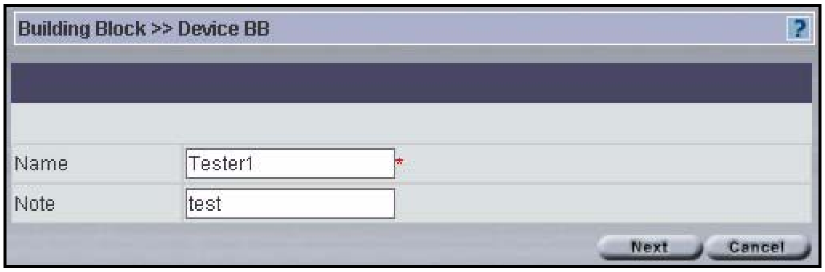
Table 100 Building Block > Device BB

TYPE	DESCRIPTION
Index	This is the building block list number.
Name	A building block should have a unique name. Click this hyperlink to go to a BB info screen that allows you to edit the name and add some extra description of the BB.
Type	This field displays the device model, for example, ZyWALL70.
Note	This field displays some extra description of the BB
Add	Click to proceed to the next screen.
Delete	Click to delete a selected device BB.

18.3.1 Editing an Existing BB

Editing an existing does not influence devices already configured with that BB. Click a **Name** hyperlink to go to that Device BB. Change the name and type some extra description of the BB.

Figure 128 Building Block > Device BB > Edit



Building Block >> Device BB

Name	Tester1 *
Note	test

The following table describes the fields in this screen

Table 101 Building Block > Device BB > Edit

TYPE	DESCRIPTION
Name	Type a unique name for the building block.
Note	Type some extra description of the BB

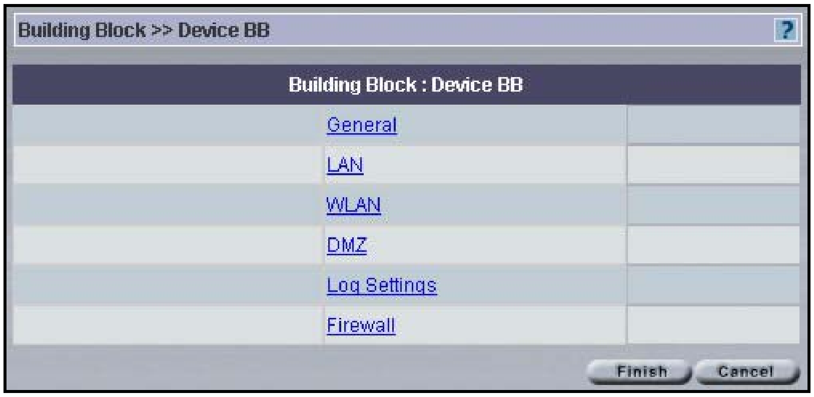
Table 101 Building Block > Device BB > Edit (continued)

TYPE	DESCRIPTION
Next	Click to proceed to the following screen
Cancel	Click to return to the previous screen.

18.3.2 Device BB Configuration Select

Select one of the hyperlink configuration menus to configure your BB Device LAN, WLAN etc. Click **Finish** to complete the setup. Click **Cancel** to return to the previous screen.

Figure 129 Building Block > Device BB > Edit > Configuration



18.3.3 Adding a New BB

Click **Add** from Figure 127 on page 255.The next screen asks you what model type BB you want to add. This should be the same as the model types supported by Vantage.

Figure 130 Building Block > Device BB > Add

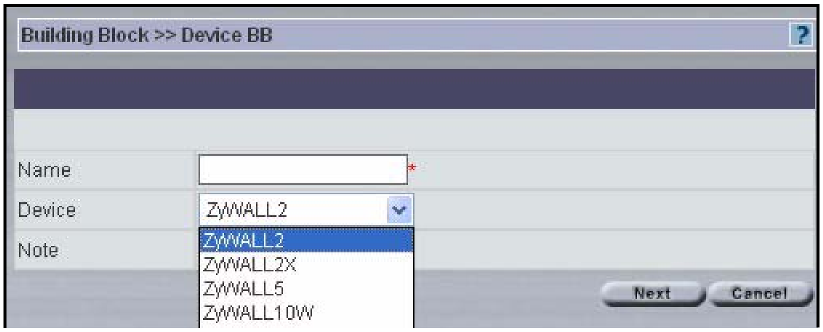


Table 102 Building Block > Device BB > Add

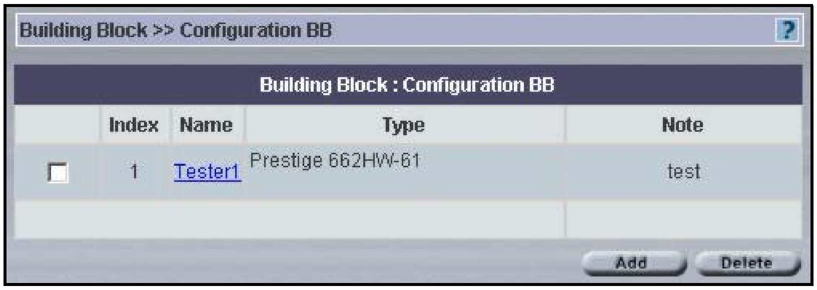
TYPE	DESCRIPTION
Name	Type a unique name for the building block.
Device	Select the device model.
Note	Type some extra description of the BB
Next	Click to proceed to the following screen
Cancel	Click to return to the previous screen.

18.4 Configuration BBs

Configuration building blocks depend on the device type.

Click **Building Block** > **Configuration BB**.

Figure 131 Building Block > Configuration



Building Block >> Configuration BB
?
Building Block : Configuration BB
Add
Delete

	Index	Name	Type	Note
□	1	Tester1	Prestige 662HW-61	test

The following table describes the fields in this screen

Table 103 Building Block > Configuration

TYPE	DESCRIPTION
Index	This is the building block list number.
Name	A building block should have a unique name. Click this hyperlink to go to a BB info screen that allows you to edit the name and add some extra description of the BB.
Type	This field displays the configuration type, for example, ZyWALL LAN.

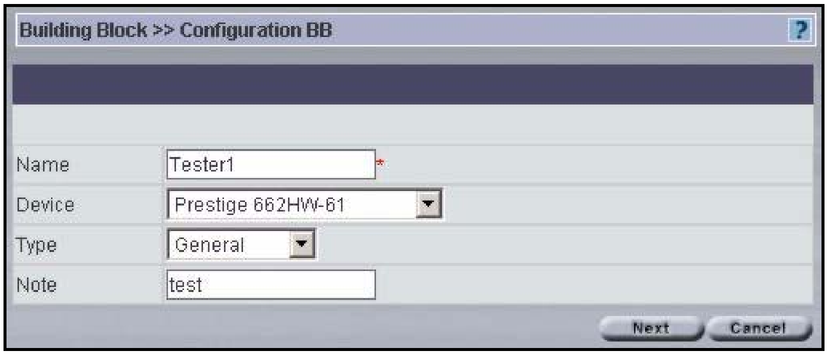
Table 103 Building Block > Configuration (continued)

TYPE	DESCRIPTION
Note	This field displays some extra description of the BB
Add	Click to proceed to the next screen.
Delete	Click to delete a selected device BB.

18.4.1 Adding a Configuration BB

Click **Add** from Figure 131 on page 257. Type a **Name** to identify your existing or new **Configuration BB**. When you add a new Configuration BB, you must choose what device type and BB configuration type you wish to add, from the **Device** and **Type** list boxes respectively.

Figure 132 Building Block > Configuration BB > Add



Building Block >> Configuration BB

Name	Tester1 *
Device	Prestige 662HW-61
Type	General
Note	test

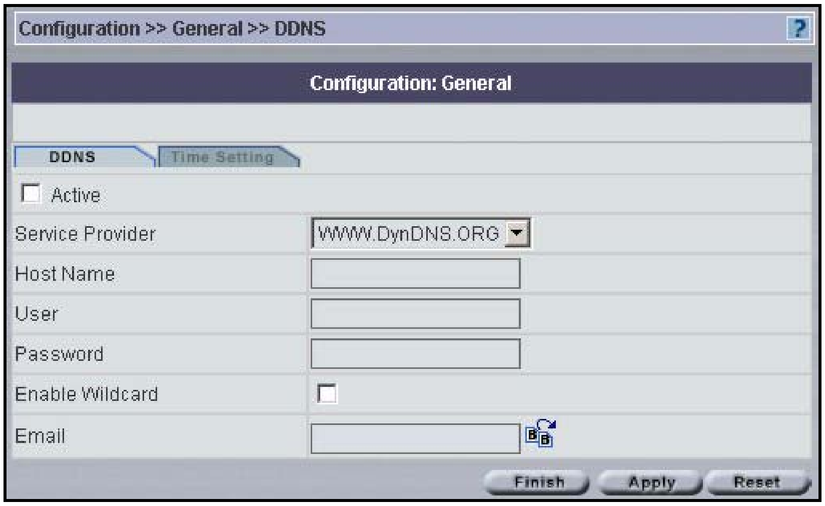
The following table describes the fields in this screen

Table 104 Building Block > Configuration BB > Add

TYPE	DESCRIPTION
Name	Type a unique name for the building block.
Device	Select the device type. The configuration BB's available differ for each device.
Type	Select the configuration. Choices available depend on the device selected.
Note	Type some extra description of the BB
Next	Click **Next** to continue to the configuration BB details for the device type selected.
Cancel	Click **Cancel** to return to the **Building Block > Configuration BB** summary screen.

After you click **Next in** Figure 132 on page 258, the next screen that appears depends on the **Device** and **Type** fields you selected in Figure 132. Figure 132 and Figure 133 show the **General** configuration BB for a ZyWALL 10 device. Create the BB as shown in the screen. Refer to the corresponding **Configuration** chapter for details on fields in the screen. Click **Apply** to save BB changes (you may click **Reset** to begin configuring the screen afresh) and then click **Finish** to complete the BB.

Figure 133 Building Block > Configuration BB > Add > Next



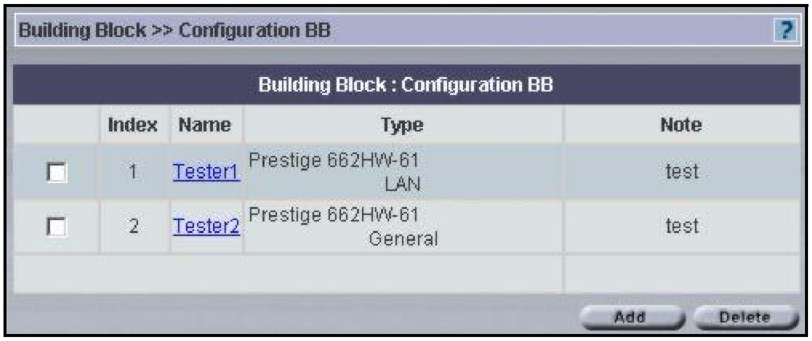
Configuration >> General >> DDNS

Configuration: General

□ Active	
Service Provider	WWW.DynDNS.ORG
Host Name	
User	
Password	
Enable Wildcard	□
Email	

The completed configuration BB is shown next. You may edit this BB by clicking the **Name** hyperlink.

Figure 134 Building Block > Configuration BB > Added



Building Block >> Configuration BB

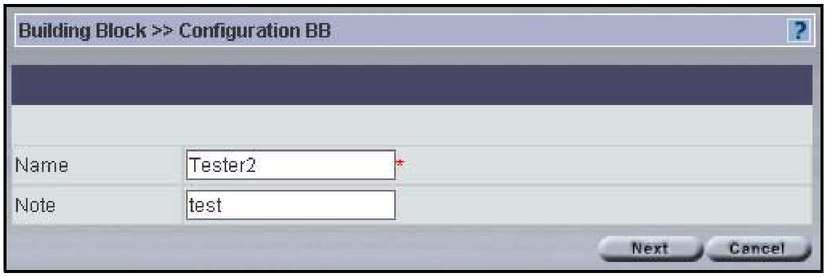
Building Block : Configuration BB

	Index	Name	Type	Note
□	1	Tester1	Prestige 662HW-61 LAN	test
□	2	Tester2	Prestige 662HW-61 General	test

18.4.2 Editing a Configuration BB

Click the **Name** hyperlink in the **Building Block > Configuration BB** screen (as shown in Figure 134 on page 259 for example) to edit an existing configuration. What you can edit in a configuration building block depends on the configuration type and device.

Figure 135 Building Block > Configuration BB > Edit



Name	Tester2
Note	test

The following table describes the fields in this screen

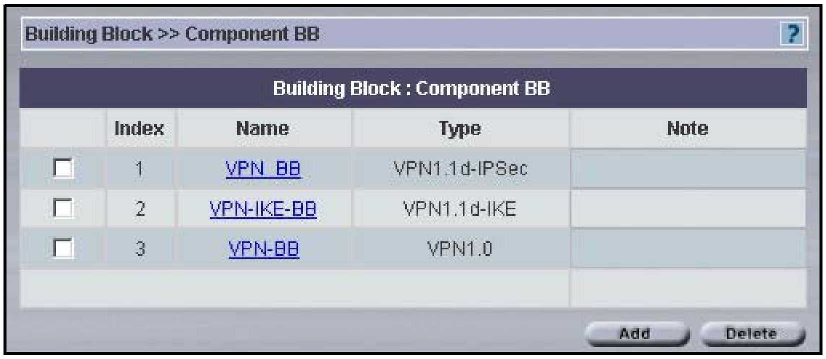
Table 105 Building Block > Configuration BB > Edit

TYPE	DESCRIPTION
Name	You may change the name for this configuration building block.
Note	You may change the description of the BB here.
Next	Click **Next** to continue to edit the configuration BB details for the device type selected as shown in Figure 133 on page 259.
Cancel	Click **Cancel** to return to the previous screen.

18.5 Component BBs

Current (at the time of writing) component BB types are IP address and e-mail address. Click **Building Block > Component BB** to see the following screen.

Figure 136 Building Block > Component BB



Building Block : Component BB

	Index	Name	Type	Note
□	1	VPN_BB	VPN1.1d-IPSec	
□	2	VPN-IKE-BB	VPN1.1d-IKE	
□	3	VPN-BB	VPN1.0	

The following table describes the fields in this screen

Table 106 Building Block > Component BB

TYPE	DESCRIPTION
Index	This is the building block list number.
Name	A building block should have a unique name. Click this hyperlink to go to a BB info screen that allows you to edit the name, type and add some extra description of the BB.

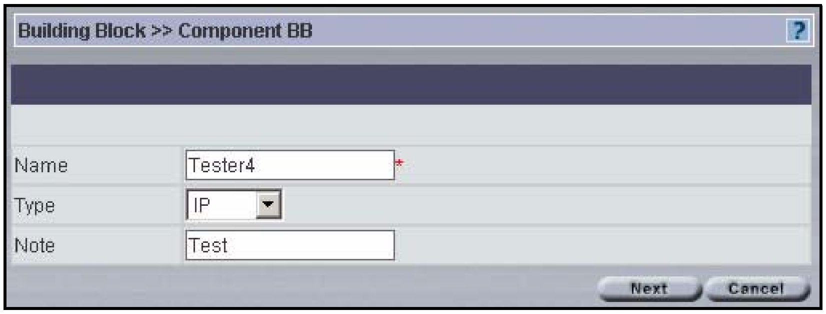
Table 106 Building Block > Component BB (continued)

TYPE	DESCRIPTION
Type	This field displays the component type, for example, E-mail.
Note	This field displays some extra description of the BB
Add	Click Add to create a new configuration BB. Alternatively, create new component BBs directly from the configuration menus by using the "save as new BB" icon.
Delete	Click to delete a selected device BB.

18.5.1 Adding a Component BB

Click **Add** in Figure 136 on page 260 to create a brand new component BB.

Figure 137 Building Block > Component BB > Add



Building Block >> Component BB

Name: Tester4 *

Type: IP

Note: Test

The following table describes the fields in this screen

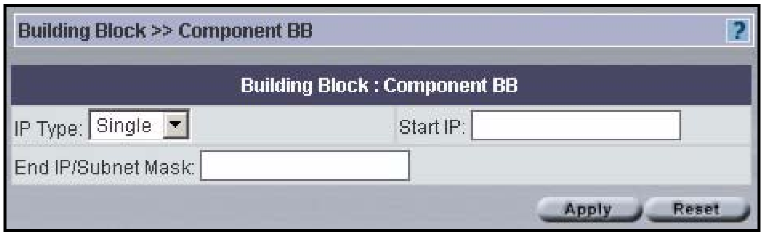
Table 107 Building Block > Component > Add

TYPE	DESCRIPTION
Name	Type a unique name for the building block.
Type	Select from **IP**, **E-mail**, **VPN1.1d_IPSec**, **VPN1.1d_IKE** or **VPN1.0**..
Note	Type some extra description of the BB
Next	Click **Next** to proceed to the next screen.
Cancel	Click **Cancel** to return to the previous screen without saving any changes.

18.5.1.1 Adding a Component BB: IP Type

If you select **IP** in the **Type** field in the **BB Info** screen and select **Next,** you will to the next screen, where you must enter your **IP Type, Start** and **End IP/Subnet Mask** details.

Figure 138   Building Block > Component BB > Add > IP Address


Building Block >> Component BB

Building Block : Component BB

IP Type: Single

Start IP:

End IP/Subnet Mask:

The following table describes the fields in this screen

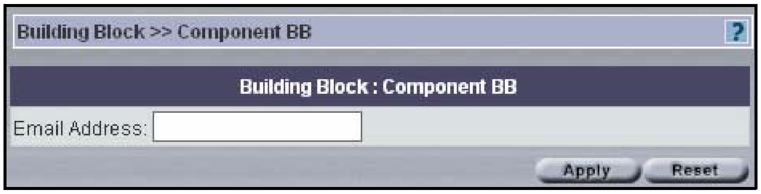
Table 108   Building Block > Component BB > Add > IP Address

TYPE	DESCRIPTION
IP Type	Select from **Single, Range** or **Subnet**.
Start IP	Type the IP address or the first IP address in a range.
End IP/Subnet Mask	Type the last IP address in a range or the subnet mask. See the appendices for information on IP subnetting
Apply	Click **Apply** to create the BB. This BB is then displayed in the component BB summary screen.
Reset	Click **Reset** to begin configuring the screen afresh.

18.5.1.2 Adding a Component BB: E-mail Type

If you select **E-mail** in the **Type** field in the **BB Info** screen and select **Next,** you will to the next screen, where you must enter your **E-Mail Address**.

Figure 139   Building Block > Component BB > Add > E-Mail Address


Building Block >> Component BB

Building Block : Component BB

Email Address:

The following table describes the fields in this screen

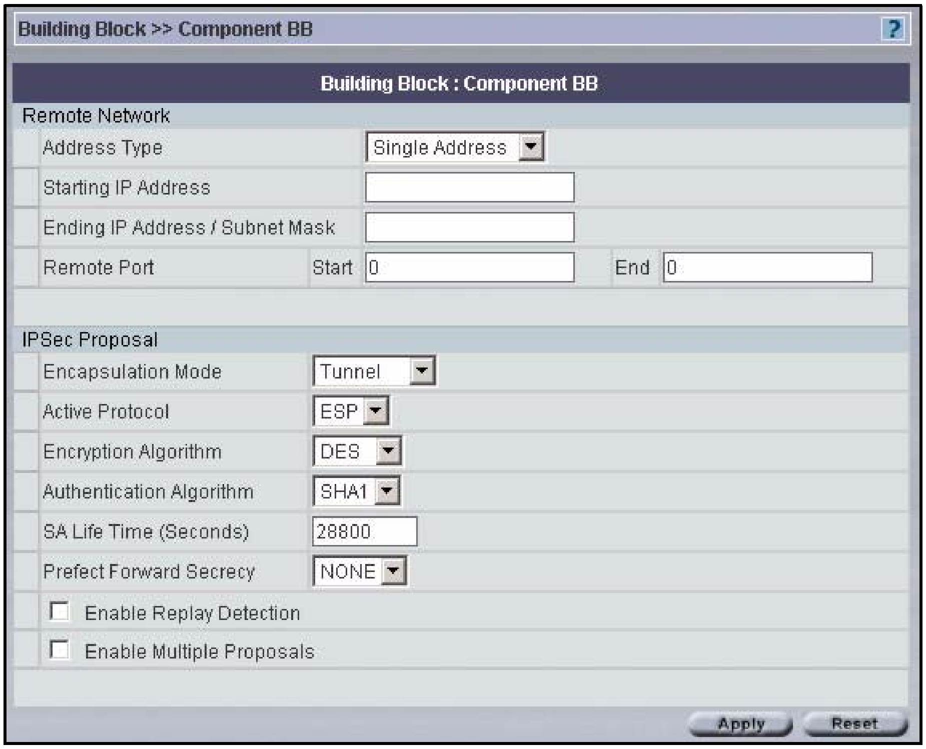
Table 109   Building Block > Component BB > Add > E-Mail Address

TYPE	DESCRIPTION
E-mail Address	Type the e-mail address in standard you@here.xx format.
Apply	Click **Apply** to create the BB. This BB is then displayed in the component BB summary screen.
Reset	Click **Reset** to begin configuring the screen afresh.

18.5.1.3 Adding a Component BB: VPN1.1d_IPSec Type

If you select **VPN1.1d_IPSec** in the **Type** field in the **BB Info** screen and select **Next,** you will to the next screen, where you must enter VPN information.

Figure 140 Building Block > Component BB > Add > VPN1.1d_IPSec



Building Block >> Component BB

Building Block : Component BB

Remote Network

Address Type	Single Address		
Starting IP Address			
Ending IP Address / Subnet Mask			
Remote Port	Start 0	End	0

IPSec Proposal

Encapsulation Mode	Tunnel
Active Protocol	ESP
Encryption Algorithm	DES
Authentication Algorithm	SHA1
SA Life Time (Seconds)	28800
Prefect Forward Secrecy	NONE

☐ Enable Replay Detection

☐ Enable Multiple Proposals

The following table describes the fields in this screen

Table 110 Building Block > Component BB > Add > VPN1.1d_IPSec

TYPE	DESCRIPTION
Remote Network	Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Address Type	Use the drop-down list box to choose **Single Address**, **Range Address**, or **Subnet Address**. Select **Single Address** with a single IP address. Select **Range Address** for a specific range of IP addresses. Select **Subnet Address** to specify IP addresses on a network by their subnet mask.
Starting IP Address	When the **Address Type** field is configured to **Single Address**, enter a (static) IP address on the network behind the remote IPSec router. When the **Address Type** field is configured to **Range Address**, enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Address Type** field is configured to **Subnet Address**, enter a (static) IP address on the network behind the remote IPSec router.

Table 110 Building Block > Component BB > Add > VPN1.1d_IPSec

TYPE	DESCRIPTION
Ending IP Address/Subnet Mask	When the **Address Type** field is configured to **Single Address**, this field is N/A. When the **Address Type** field is configured to **Range Address**, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Address Type** field is configured to **Subnet Address**, enter a subnet mask on the network behind the remote IPSec router.
Remote Port	0 is the default and signifies any port. Type a port number from 0 to 65535 in the **Start** and **End** fields. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.
IPSec Proposal	
Encapsulation Mode	Select **Tunnel** mode or **Transport** mode.
Active Protocol	Select the security protocols used for an SA. Both **AH** and **ESP** increase Prestige processing requirements and communications latency (delay).
Encryption Algorithm	When **DES** is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on DES that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of **AES** uses a 128-bit key. **AES** is faster than **3DES**. Select **NULL** to set up a tunnel without encryption. When you select **NULL**, you do not enter an encryption key.
Authentication Algorithm	**MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slower. Select **MD5** for minimal security and **SHA-1** for maximum security.
SA Life Time (Seconds)	Define the length of time before an IKE SA automatically renegotiates in this field. The minimum value is 180 seconds. A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Perfect Forward Secret (PFS)	Perfect Forward Secret (PFS) is disabled (**NONE**) by default in phase 2 IPSec SA setup. This allows faster IPSec setup, but is not so secure. Select **DH1** or **DH2** to enable PFS. **DH1** refers to Diffie-Hellman Group 1 a 768 bit random number. **DH2** refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number (more secure, yet slower).
Enable Replay Detection	As a VPN setup is processing intensive, the system is vulnerable to Denial of Service (DOS) attacks. The IPSec receiver can detect and reject old or duplicate packets to protect against replay attacks. Enable replay detection by selecting this check box.
Enable Multiple Proposals	Select this check box to allow the ZyWALL to use any of its phase 1 or phase 2 encryption and authentication algorithms when negotiating an IPSec SA. When you enable multiple proposals, the ZyWALL allows the remote IPSec router to select which encryption and authentication algorithms to use for the VPN tunnel, even if they are less secure than the ones you configure for the VPN rule. Clear this check box to have the ZyWALL use only the phase 1 or phase 2 encryption and authentication algorithms configured below when negotiating an IPSec SA.

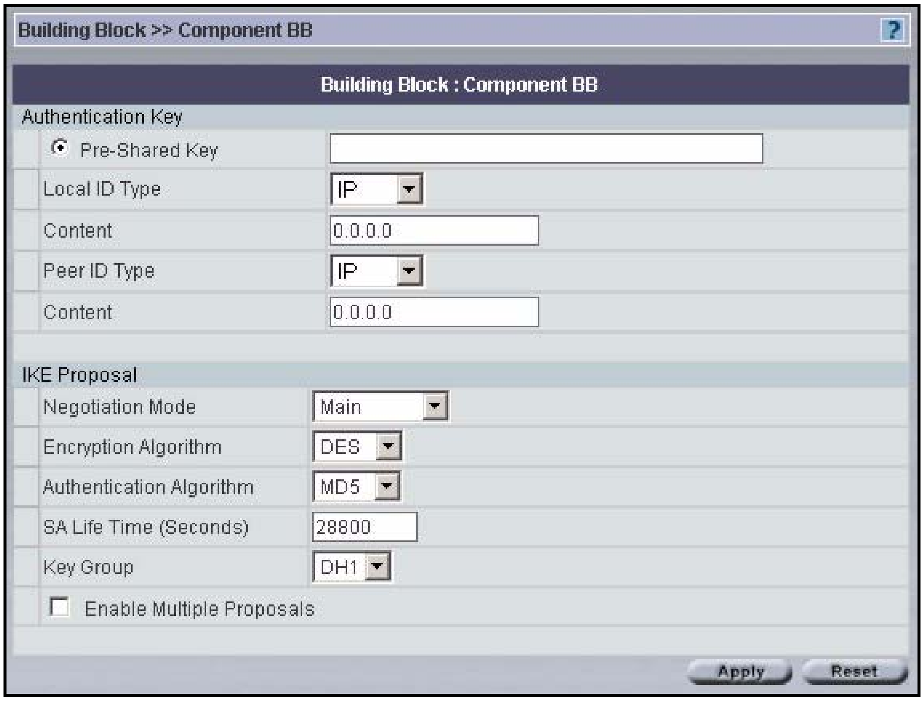
Table 110 Building Block > Component BB > Add > VPN1.1d_IPSec

TYPE	DESCRIPTION
Apply	Click **Apply** to create the BB. This BB is then displayed in the component BB summary screen.
Reset	Click **Reset** to begin configuring the screen afresh.

18.5.1.4 Adding a Component BB: VPN1.1d_IKE Type

If you select **VPN1.1d_IKE** in the **Type** field in the **BB Info** screen and select **Next,** you will to the next screen, where you must enter VPN information.

Figure 141 Building Block > Component BB > Add > VPN1.1d_IKE



Building Block : Component BB

Authentication Key

● Pre-Shared Key	
Local ID Type	IP
Content	0.0.0.0
Peer ID Type	IP
Content	0.0.0.0

IKE Proposal

Negotiation Mode	Main
Encryption Algorithm	DES
Authentication Algorithm	MD5
SA Life Time (Seconds)	28800
Key Group	DH1

□ Enable Multiple Proposals

The following table describes the fields in this screen

Table 111 Building Block > Component BB > Add > VPN1.1d_IKE

TYPE	DESCRIPTION
Authentication Key	
Pre-Shared Key	Select the **Pre-Shared Key** radio button and type your pre-shared key in this field. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection. Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. You must precede a hexadecimal key with a "0x (zero x), which is not counted as part of the 16 to 62 character range for the key. For example, in "0x0123456789ABCDEF", 0x denotes that the key is hexadecimal and 0123456789ABCDEF is the key itself. Both ends of the VPN tunnel must use the same pre-shared key. You will receive a PYLD_MALFORMED (payload malformed) packet if the same pre-shared key is not used on both ends.
Local ID Type	Select **IP** to identify this ZyWALL by its IP address. Select **DNS** to identify this ZyWALL by a domain name. Select **E-mail** to identify this ZyWALL by an e-mail address. You do not configure the local ID type and content when you set **Authentication Key** to **Certificate**. The ZyWALL takes them from the certificate you select.

Table 111 Building Block > Component BB > Add > VPN1.1d_IKE

TYPE	DESCRIPTION
Content	When you select **IP** in the **Local ID Type** field, type the IP address of your computer in the local **Content** field. The ZyWALL automatically uses the IP address in the **My ZyWALL** field (refer to the **My ZyWALL** field description) if you configure the local **Content** field to **0.0.0.0** or leave it blank. It is recommended that you type an IP address other than **0.0.0.0** in the local **Content** field or use the **DNS** or **E-mail** ID type in the following situations. • When there is a NAT router between the two IPSec routers. • When you want the remote IPSec router to be able to distinguish between VPN connection requests that come in from IPSec routers with dynamic WAN IP addresses. When you select **DNS** or **E-mail** in the **Local ID Type** field, type a domain name or e-mail address by which to identify this ZyWALL in the local **Content** field. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string.
Peer ID Type	Select from the following when you set **Authentication Key** to **Pre-shared Key**. • Select **IP** to identify the remote IPSec router by its IP address. • Select **DNS** to identify the remote IPSec router by a domain name. • Select **E-mail** to identify the remote IPSec router by an e-mail address. Select from the following when you set **Authentication Key** to **Certificate**. • Select **IP** to identify the remote IPSec router by the IP address in the subject alternative name field of the certificate it uses for this VPN connection. • Select **DNS** to identify the remote IPSec router by the domain name in the subject alternative name field of the certificate it uses for this VPN connection. • Select **E-mail** to identify the remote IPSec router by the e-mail address in the subject alternative name field of the certificate it uses for this VPN connection. • Select **Subject Name** to identify the remote IPSec router by the subject name of the certificate it uses for this VPN connection. • Select **Any** to have the ZyWALL not check the remote IPSec router's ID.

Table 111 Building Block > Component BB > Add > VPN1.1d_IKE

TYPE	DESCRIPTION
Content	The configuration of the peer content depends on the peer ID type. Do the following when you set **Authentication Key** to **Pre-shared Key**. • For **IP**, type the IP address of the computer with which you will make the VPN connection. If you configure this field to **0.0.0.0** or leave it blank, the ZyWALL will use the address in the **Remote Gateway Address** field (refer to the **Remote Gateway Address** field description). • For **DNS** or **E-mail**, type a domain name or e-mail address by which to identify the remote IPSec router. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string. It is recommended that you type an IP address other than **0.0.0.0** or use the **DNS** or **E-mail** ID type in the following situations: • When there is a NAT router between the two IPSec routers. • When you want the ZyWALL to distinguish between VPN connection requests that come in from remote IPSec routers with dynamic WAN IP addresses. Do the following when you set **Authentication Key** to **Certificate**. • For **IP**, type the IP address from the subject alternative name field of the certificate the remote IPSec router will use for this VPN connection. If you configure this field to **0.0.0.0** or leave it blank, the ZyWALL will use the address in the **Remote Gateway Address** field (refer to the **Remote Gateway Address** field description). • For **DNS** or **E-mail**, type the domain name or e-mail address from the subject alternative name field of the certificate the remote IPSec router will use for this VPN connection. • For **Subject Name**, type the subject name of the certificate the remote IPSec router will use for this VPN connection. Use up to255 ASCII characters including spaces. • For **Any**, the peer **Content** field is not available. • Regardless of how you configure the **ID Type** and **Content** fields, two active SAs cannot have both the local and remote IP address ranges overlap between rules.
IKE Proposal	
Negotiation Mode	Select **Main** or **Aggressive** from the drop-down list box. Multiple SAs connecting through a secure gateway must have the same negotiation mode.
Encryption Algorithm	Select **DES**, **3DES** or **AES** from the drop-down list box. When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on DES that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of AES uses a 128-bit key. **AES** is faster than **3DES**.
Authentication Algorithm	Select **SHA1** or **MD5** from the drop-down list box. **MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slower. Select **MD5** for minimal security and **SHA-1** for maximum security.

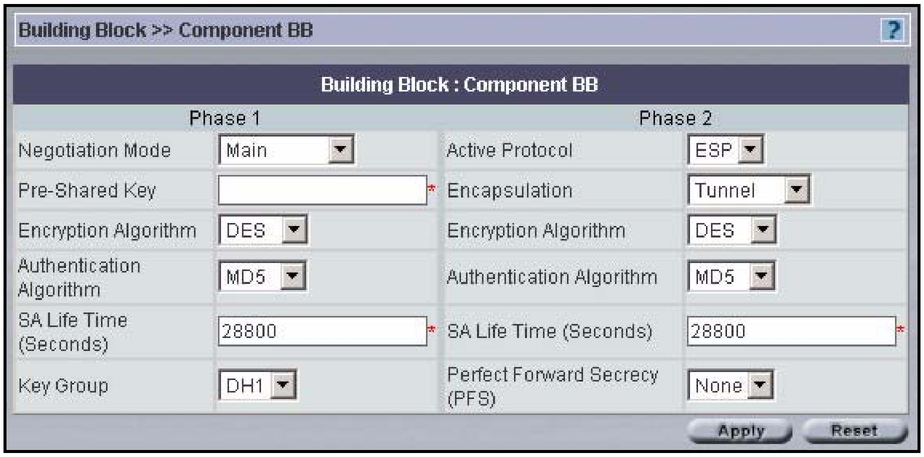
Table 111 Building Block > Component BB > Add > VPN1.1d_IKE

TYPE	DESCRIPTION
SA Life Time (Seconds)	Define the length of time before an IKE SA automatically renegotiates in this field. It may range from 180 to 3,000,000 seconds (almost 35 days). A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Key Group	You must choose a key group for phase 1 IKE setup. **DH1** (default) refers to Diffie-Hellman Group 1 a 768 bit random number. **DH2** refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number.
Enable Multiple Proposals	Select this check box to allow the ZyWALL to use any of its phase 1 or phase 2 encryption and authentication algorithms when negotiating an IPSec SA. When you enable multiple proposals, the ZyWALL allows the remote IPSec router to select which encryption and authentication algorithms to use for the VPN tunnel, even if they are less secure than the ones you configure for the VPN rule. Clear this check box to have the ZyWALL use only the phase 1 or phase 2 encryption and authentication algorithms configured below when negotiating an IPSec SA.
Apply	Click **Apply** to create the BB. This BB is then displayed in the component BB summary screen.
Reset	Click **Reset** to begin configuring the screen afresh.

18.5.1.5 Adding a Component BB: VPN1.0 Type

If you select **VPN1.0** in the **Type** field in the **BB Info** screen and select **Next,** you will to the next screen, where you must enter VPN information.

Figure 142 Building Block > Component BB > Add > VPN1.0



Building Block >> Component BB

Building Block : Component BB

Phase 1		Phase 2	
Negotiation Mode	Main	Active Protocol	ESP
Pre-Shared Key	*	Encapsulation	Tunnel
Encryption Algorithm	DES	Encryption Algorithm	DES
Authentication Algorithm	MD5	Authentication Algorithm	MD5
SA Life Time (Seconds)	28800 *	SA Life Time (Seconds)	28800 *
Key Group	DH1	Perfect Forward Secrecy (PFS)	None

The following table describes the fields in this screen

Table 112 Building Block > Component BB > Add > VPN1.0

TYPE	DESCRIPTION
Phase 1	There are two phases to every IKE (Internet Key Exchange) negotiation – phase 1 (Authentication) and phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA and the second one uses that SA to negotiate SAs for IPSec.
Negotiation Mode	Select either **Main** or **Aggressive**. Aggressive mode is quicker than Main mode because it eliminates several steps when the communicating parties are negotiating authentication (phase 1). However the trade-off is that faster speed limits its negotiating power and it also does not provide identity protection. It is useful in remote access situations where the address of the initiator is not know by the responder and both parties want to use pre-shared key authentication.
Pre-Shared key	A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called pre-shared because you have to share it with another party before you can communicate with them over a secure connection. ZyXEL gateways authenticate an IKE VPN session by matching pre-shared keys. Enter from 8 up to 31 characters. Any character may be used, including spaces, but trailing spaces are truncated. Multiple SAs connecting through a secure gateway must have the same pre-shared key.
Encryption Algorithm	Select an encryption algorithm from the pull-down menu. You can select either **DES** or **3DES**. **3DES** is more powerful but increases latency.
Authentication Algorithm	The Authentication Algorithms, HMAC-MD5 (RFC 2403) and HMAC-SHA-1 (RFC 2404, provide an authentication mechanism for the AH and ESP protocols. Select **MD5** for minimal security and **SHA-1** for maximum security. **MD5** (Message Digest 5) produces a 128-bit digest to authenticate packet data. **SHA-1** (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.
SA Life Time (Seconds)	Define the length of time before an IKE Security Association automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days). A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.

Table 112 Building Block > Component BB > Add > VPN1.0

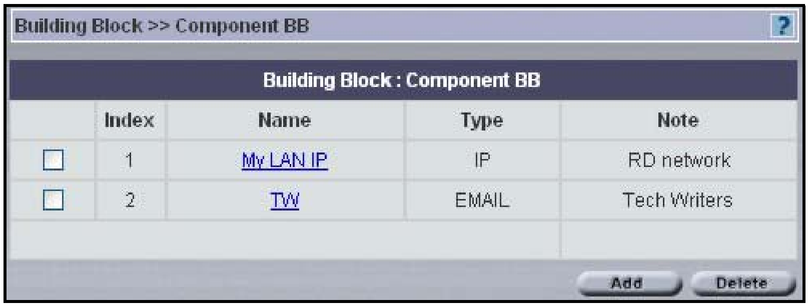
TYPE	DESCRIPTION
Key Group	Diffie-Hellman (DH) is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communications channel. Diffie-Hellman is used within IKE SA setup to establish session keys. 768-bit (Group 1 - DH1) and 1024-bit (Group 2 – DH2) Diffie-Hellman groups are supported. Upon completion of the Diffie-Hellman exchange, the two peers have a shared secret, but the IKE SA is not authenticated. For authentication, use pre-shared keys.
Phase 2	There are two phases to every IKE (Internet Key Exchange) negotiation – phase 1 (Authentication) and phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA and the second one uses that SA to negotiate SAs for IPSec.
Active Protocol	The **ESP** and **AH** protocols are necessary to create a Security Association (SA), the foundation of an IPSec VPN. **AH** protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the **ESP** was designed. The **ESP** protocol (RFC 2406) provides encryption as well as some of the services offered by **AH**. **ESP** authenticating properties are limited compared to the **AH** due to the non-inclusion of the IP header information during the authentication process.
Encapsulation	In **Transport** mode, the IP packet contains the security protocol (**AH** or **ESP**) located after the original IP header and options, but before any upper layer protocols contained in the packet (such as TCP and UDP). With ESP, protection is applied only to the upper layer protocols contained in the packet. The IP header information and options are not used in the authentication process. Therefore, the originating IP address cannot be verified for integrity against the data. With the use of **AH** as the security protocol, protection is extended forward into the IP header to verify the integrity of the entire packet by use of portions of the original IP header in the hashing process. **Tunnel** mode encapsulates the entire IP packet to transmit it securely. **Tunnel** mode is required for gateway services to provide access to internal systems. **Tunnel** mode is fundamentally an IP tunnel with authentication and encryption. This is the most common mode of operation
Encryption Algorithm	Select an encryption algorithm from the pull-down menu. You can select either **DES** or **3DES**. **3DES** is more powerful but increases latency.
Authentication Algorithm	The Authentication Algorithms, HMAC-MD5 (RFC 2403) and HMAC-SHA-1 (RFC 2404, provide an authentication mechanism for the **AH** and **ESP** protocols. Select **MD5** for minimal security and **SHA-1** for maximum security. **MD5** (Message Digest 5) produces a 128-bit digest to authenticate packet data. **SHA-1** (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.
SA Life Time (Seconds)	Define the length of time before an IKE Security Association automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days). A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.

Table 112 Building Block > Component BB > Add > VPN1.0

TYPE	DESCRIPTION
Perfect Forward Secrecy (PFS)	Choose whether to enable Perfect Forward Secrecy (**PFS**) using Diffie-Hellman public-key cryptography. Enabling **PFS** means that the key is transient. A brand new key using a new Diffie-Hellman exchange replaces the key for each new IPSec SA. With PFS enabled, if one key is compromised, previous and subsequent keys are not compromised, because subsequent keys are not derived from previous keys. The (time-consuming) Diffie-Hellman exchange is the trade-off for this extra security. Disabling PFS means new authentication and encryption keys are derived from the same root secret (which may have security implications in the long run) but allows faster SA setup (by bypassing the Diffie-Hellman key exchange).
Apply	Click **Apply** to create the BB. This BB is then displayed in the component BB summary screen.
Reset	Click **Reset** to begin configuring the screen afresh.

The following screen then shows the component BBs you added. Click a **Name** hyperlink to edit the BB.

Figure 143 Component BBs Added



Building Block >> Component BB

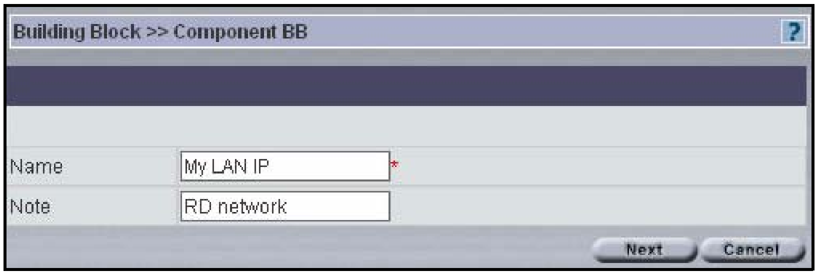
Building Block : Component BB

	Index	Name	Type	Note
□	1	My LAN IP	IP	RD network
□	2	TW	EMAIL	Tech Writers

18.5.2 Editing a Component BB

Click the **Name** hyperlink in the component BB summary screen as shown in Figure 143 on page 272 to edit a component BB.

Figure 144 Building Block > Component BB > Edit



Building Block >> Component BB

Name	My LAN IP *
Note	RD network

The following table describes the fields in this screen

Table 113 Building Block > Component BB > Edit

TYPE	DESCRIPTION
Name	You may change the name for the building block.
Note	You may change the description of the BB.
Next	Click **Next** to proceed to a screen to edit the component BB details as shown above.
Cancel	Click **Cancel** to return to the previous screen.

CHAPTER 19 System > Administrators

Use these screens to manage Vantage administrators.

19.1 Introduction to Administrators

An Administrator can only be associated to one management domain. To change an Administrator's management domain, you must first disassociate him or her from an existing domain before associating to the new domain.

Once an Administrator account has been created, his or her account name (UID) cannot be changed, but the password can. New administrators must change their password after first login and then regularly at three month intervals. Administrators should periodically change their passwords. The "root" Administrator can enforce periodic Administrator password changes in the **Force Administrator Password Change every 90 Days** in the **System Preferences > User Access** screen.

You can create (and manage) administrators within your domain. You cannot delete an Administrator if that Administrator has "child Administrators" (you will see a warning message). You must first delete the "child Administrators".

19.1.1 Administrator Types

There are four types of administrators, root, super, normal and custom. Only "root" can do everything including managing the Vantage system. Super and normal are predefined administrator profiles that come with a default set of permissions. You can alter normal permissions but not super permissions in the **System > Preferences** screen. Custom administrators have no predefined permissions. Permissions allow for efficient division of labor without the danger of overlap or conflict.

Predefined permissions can only be re-defined by the Administrator who created the Administrator account. An Administrator's details cannot be changed while logged in, unless "root" forcibly logs him or her out first.

19.1.1.1 "Root" Administrator

The default system name (and password) when you first log in is "root". This is a default system Administrator account. "root's" details are viewable by others, but not editable.

1 Only one "root" administrator can exist.

2 Only "root" can change her own personal information except for UID (User Identification).

3 Only "root" can see all other Administrators. Other Administrators can only see Administrators within their domain.

19.1.1.1.1 Change the "Root" Administrator Password

1 You should change the "root" password for security resons.

2 If you change the "root" password and cannot remember the new password, you must access the MySQL database directly.

19.1.1.2 "Super" Administrators

"Super" Administrators are Administrators created using the "Super" User Group. They are the next most powerful type Administrator next to "root".

1 Super users have all permissions except System Management. System Management is defined as follows:

- Vantage Upgrade
- License
- Preference
- Log option and purge log
- Maintenance

2 Super permissions are pre-defined in Vantage and are not editable by Vantage Administrators.

3 A "super" Administrator cannot edit any Vantage system settings, but can view (read only) Vantage system status and Vantage logs (but cannot purge or change log options).

4 "Super" Administrators at same management level can't disassociate each other from that management level.

19.1.1.3 "Normal" Administrators

These administrators have default permissions enabled as shown on the screen. Some permissions are not allowed. The Administrator who creates the "Normal" Administrator determines which of the enabled permissions to disable. Normal Administrators cannot associate nor disassociate other Administrators.

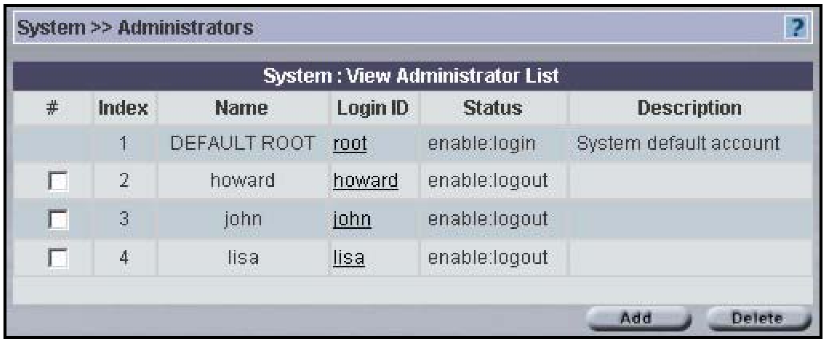
19.1.1.4 "Custom" Administrators

These administrators have no privileges enabled by default. Some permissions are not allowed. The Administrator who creates the "custom administrator" determines which of the allowable permissions to enable.

19.2 Configuring Administrators

Select a folder in the object pane and then click **System** > **Administrators** to display a list of all administrators configured for this domain and root.

Figure 145 System > View Administrator List



System : View Administrator List

#	Index	Name	Login ID	Status	Description
	1	DEFAULT ROOT	root	enable:login	System default account
□	2	howard	howard	enable:logout	
□	3	john	john	enable:logout	
□	4	lisa	lisa	enable:logout	

The following table describes the fields in this screen.

Table 114 System > View Administrator List

LABEL	DESCRIPTION
#	Select the checkbox and enter a valid e-mail address of the person who should receive a report on logs that have been purged.
Index	This is the administrator index number.
Name	This is the administrator name for identification purposes.
Login ID	This is the administrator login name associated with the password that you log into Vantage with. The Login ID is displayed in the object tree when you associate an administrator to a folder. The Login ID cannot be changed after an Administrator account is created but her name can be. Click the hyperlink to change the administrator name, password and contact information.
Status	This field displays if this Administrator is currently logged in or not.
Description	This field displays extra information on this Administrator.
Add	Click **Add** to create a new Administrator if you have this permission.
Delete	Select an Administrator(s) and then click **Delete** to erase that Administrator account from Vantage.

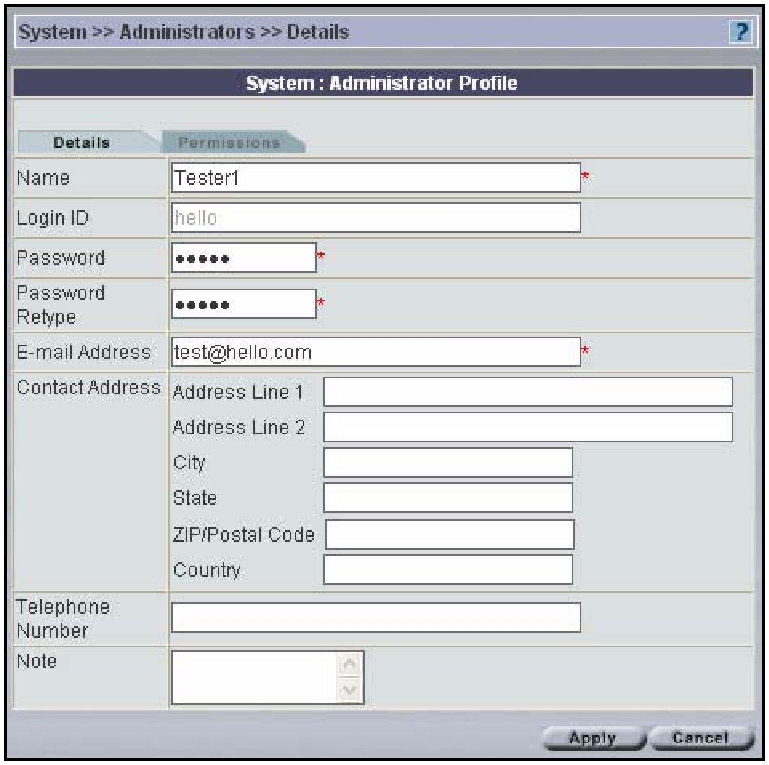
19.3 Creating an Administrator Account

Click **Add** to create a new Administrator account or select and existing Administrator account to edit it.

19.3.1 Administrator Details

Only root may create or edit her administrator details and create other administrators at the same (root) level. Other administrators can only create administrators for a level below them.

Figure 146 System > Administrator Details


System >> Administrators >> Details
?
System : Administrator Profile
Details
Permissions
Apply
Cancel

Name	Tester1 *
Login ID	hello
Password	●●●●● *
Password Retype	●●●●● *
E-mail Address	test@hello.com *
Contact Address	Address Line 1 Address Line 2 City State ZIP/Postal Code Country
Telephone Number	
Note	

The following table describes the fields in this screen.

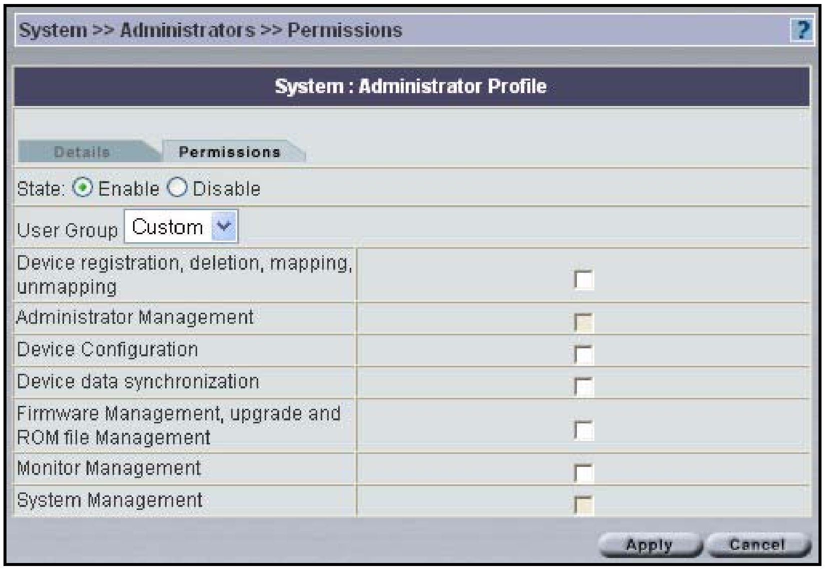
Table 115 System > Administrator Details

LABEL	DESCRIPTION
Name	Type the administrator name used for identification purposes.
Login ID	Type the administrator login name associated with the password that you log into Vantage with. The Login ID is displayed in the object tree when you associate an administrator to a folder. The Login ID cannot be changed after an Administrator account is created but her name can be.
Password	Type a password associated with the Login ID above up to a maximum of 12 characters in length.
Password Retype	Type the same password again here to make sure that the one you typed above was typed as intended.
E-mail Address	Type a valid e-mail address for this Administrator.
Contact Address	Type a mailing address for this Administrator.
Telephone Number	Type the complete telephone number including area codes for this Administrator.
Note	Type some extra information about this Administrator here.
Apply	Click **Apply** to save your settings in Vantage.
Cancel	Click **Cancel** to go back to the previous screen without saving any changes.

19.3.2 Administrator Permissions

You may select which permissions (privileges) an administrator may have from the next screen.

Figure 147 System > Administrator Permissions



System >> Administrators >> Permissions

System : Administrator Profile

State: ● Enable ○ Disable

User Group: Custom

Device registration, deletion, mapping, unmapping	□
Administrator Management	□
Device Configuration	□
Device data synchronization	□
Firmware Management, upgrade and ROM file Management	□
Monitor Management	□
System Management	□

The following table describes the fields in this screen.

Table 116 System > Administrator Permissions

LABEL	DESCRIPTION
State	Select **Disable** to prohibit Administrator access to Vantage without deleting her profile.
User Group	A user group is a pre-defined Administrator permission set. Select from **Custom**, **Super** and **Normal**. **Super** and **Normal** user groups permission sets are not editable, **Custom** user group permissions are editable. See *section 1.1* for more information. You may select the following permissions for **Custom**.
Device registration, deletion, mapping, unmapping	This permission allows the Administrator to register and delete devices as well as associate and disassociate devices to a folder.
Administrator Management	This permission allows the Administrator to create, edit and delete Administrators as well as associate and disassociate Administrators to a folder.
Device Configuration	This permission allows the Administrator access to all the **System > Configuration** screens.
Device data synchronization	This permission allows the Administrator access to the Device > Synchronize screen. See that screen information in this User’s Guide for more details.
Firmware Management, upgrade and ROM file Management	This permission allows the Administrator to upload device firmware and configuration files to Vantage, download device firmware and configuration files as well as remove them from Vantage.
Monitor Management	This permission allows the Administrator access to the Monitor screens.

Table 116 System > Administrator Permissions (continued)

LABEL	DESCRIPTION
System Management	System Management is defined as follows: ➢ Vantage Upgrade ➢ License ➢ Preference ➢ Log option and purge log ➢ Maintenance
Apply	Click **Apply** to save your settings in Vantage.
Cancel	Click **Cancel** to begin configuring the screen afresh.

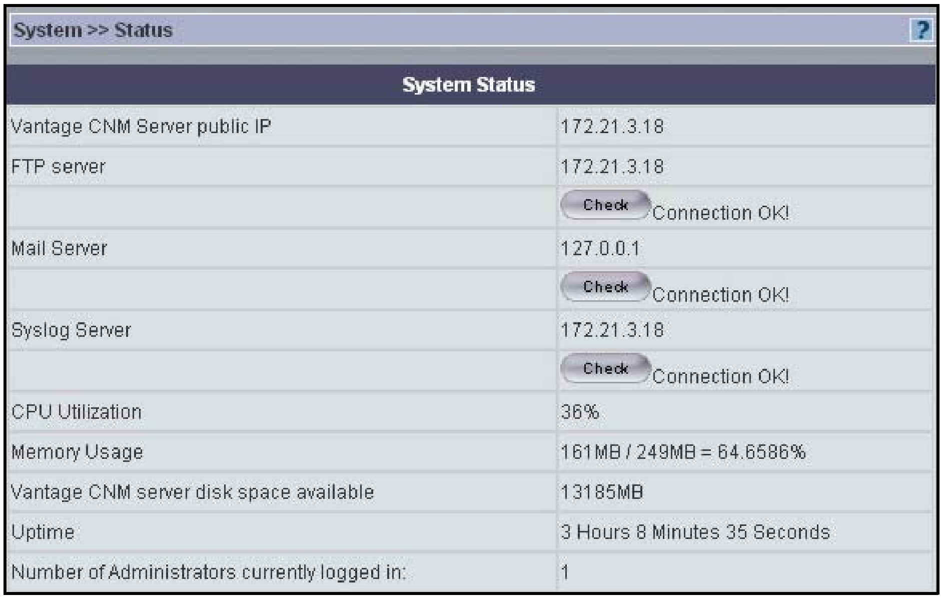
CHAPTER 20
Other System Screens

Only the root administrator can view the **System** > **Upgrade** to **System** > **Data Maintenance** screens as only the root administrator can perform these duties.

20.1 Status

Click **System** > **Status** to view the current Vantage system status. This is a read-only screen.

Figure 148 System > Vantage Status



System >> Status

System Status

Vantage CNM Server public IP	172.21.3.18
FTP server	172.21.3.18
	Check Connection OK!
Mail Server	127.0.0.1
	Check Connection OK!
Syslog Server	172.21.3.18
	Check Connection OK!
CPU Utilization	36%
Memory Usage	161MB / 249MB = 64.6586%
Vantage CNM server disk space available	13185MB
Uptime	3 Hours 8 Minutes 35 Seconds
Number of Administrators currently logged in:	1

The following table describes the fields in this screen.

Table 117 System > Vantage Status

LABEL	DESCRIPTION
Vantage CNM Server public IP	This field displays the IP address of the communications server. If the COM server is on the same computer as Vantage, then this address is the same IP address as that of the Vantage server computer.
FTP server	This field displays the IP address of the FTP server. Click the **Check** button to test if the connection to the server is up.
Mail Server	This field displays the IP address of the Mail Server. Click the **Check** button to test if the connection to the server is up.
Syslog Server	This field displays the IP address of the Syslog Server. Click the **Check** button to test if the connection to the server is up.

Table 117 System > Vantage Status (continued)

LABEL	DESCRIPTION
CPU Utilization	This field displays the Vantage server CPU processing power usage. Heavy usage may necessitate upgrading to a more powerful CPU.
Memory Usage	This field displays the Vantage server memory usage. Heavy usage may necessitate installing more RAM.
Vantage CNM server disk space available	This field displays the Vantage server computer hard drive free space. Heavy usage may necessitate buying another hard drive or purging old logs and alerts.
Uptime	This field displays how long Vantage has been on since the last start up.
Number of Administrators currently logged in	This field displays the number of Administrators currently logged into Vantage.

20.2 Vantage Upgrade

Upgraded Vantage software may be for bug fixes, increased ZyXEL device support or new Vantage modules. You should perform system maintenance (backup) before upgrading software.

20.2.1 Upgrade Procedure

1 Click **System > Upgrade** to start the upgrade procedure.

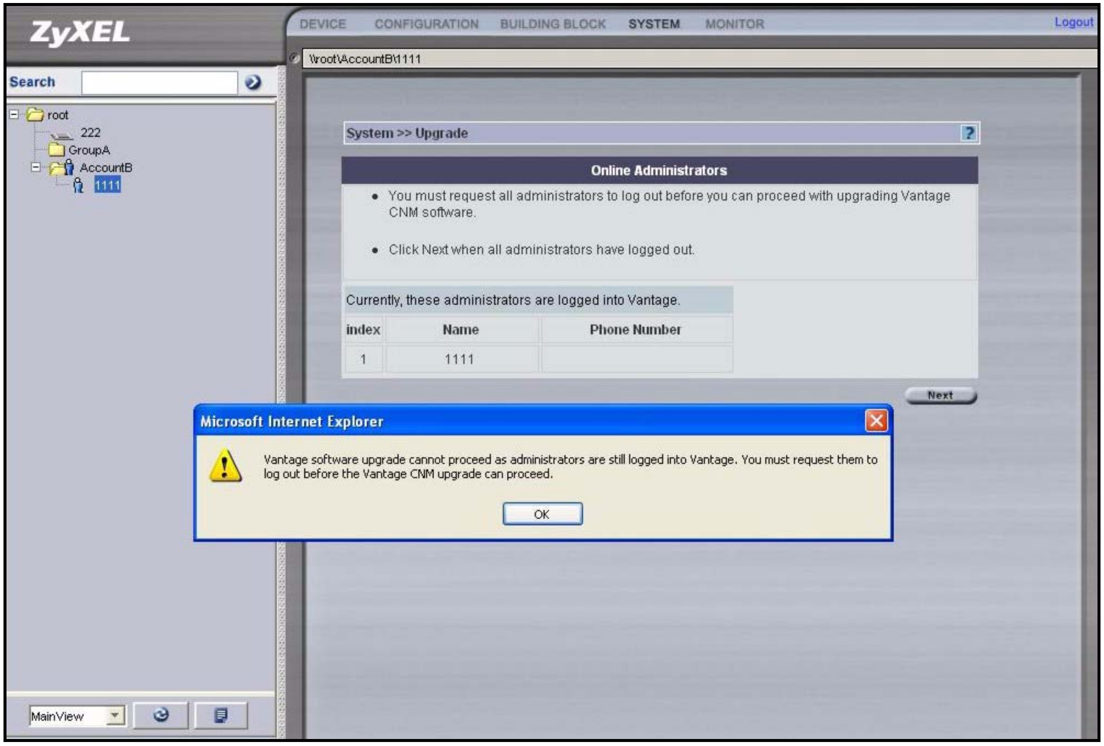
A warning screen appears if there are administrators logged into Vantage. Click **OK** to view the **Online Administrators** screen.

Note: You must request all administrators to log out before you can proceed with upgrading Vantage CNM software.

A list of Vantage administrators that are logged into Vantage is shown.

The administrator details include an administrator **Index** number, **Name** and **Phone** number (if configured).

Figure 149 System > Upgrade > Online Administrators



System >> Upgrade

Online Administrators

- You must request all administrators to log out before you can proceed with upgrading Vantage CNM software.
- Click Next when all administrators have logged out.

Currently, these administrators are logged into Vantage.

index	Name	Phone Number
1	1111	

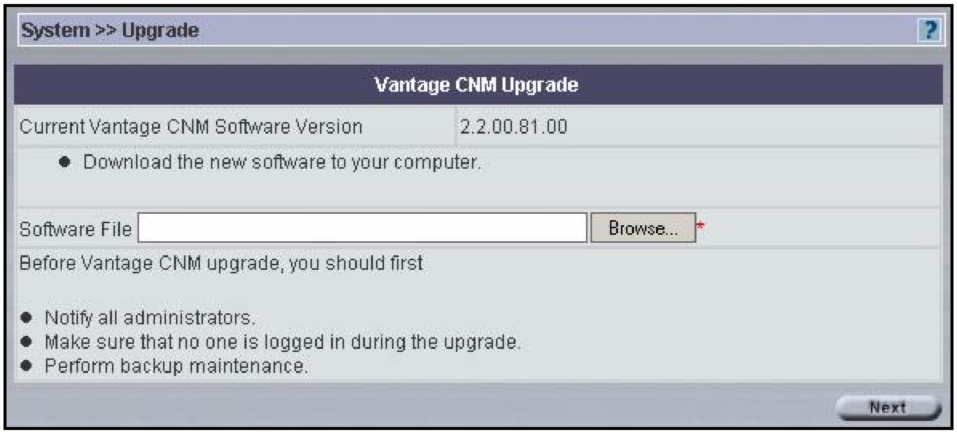
Vantage software upgrade cannot proceed as administrators are still logged into Vantage. You must request them to log out before the Vantage CNM upgrade can proceed.

2 Click **Next** when all administrators have logged out.

If an administrator has not logged out, Vantage will not let you continue. A warning screen will re-appear reminding you to notify them to log out.

You should have already downloaded the upgraded Vantage software from the ZyXEL website. The next screen asks you to **Browse** to the location on your computer where you have previously downloaded the software upgrade file. The software upgrade file has a .zip extension. Click **Next** to proceed.

Figure 150 System > Upgrade > Vantage Upgrade



System >> Upgrade

Vantage CNM Upgrade

Current Vantage CNM Software Version	2.2.00.81.00

- Download the new software to your computer.

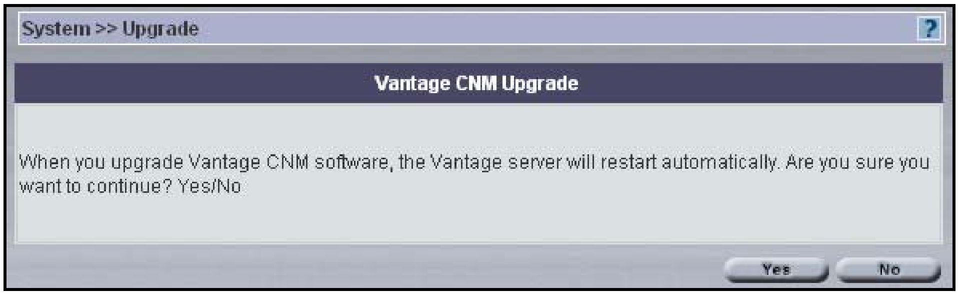
Software File

Before Vantage CNM upgrade, you should first

- Notify all administrators.
- Make sure that no one is logged in during the upgrade.
- Perform backup maintenance.

3 The next screen reminds you that Vantage will restart automatically after you start the upgrade and asks you if you are sure you want to continue with the Vantage upgrade now. Click **Yes** to continue.

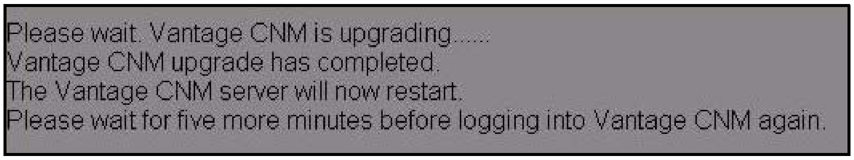
Figure 151 System > Upgrade > Vantage Upgrade > Next



When you upgrade Vantage CNM software, the Vantage server will restart automatically. Are you sure you want to continue? Yes/No

You must wait while Vantage CNM is upgrading.

Figure 152 System > Upgrading



Please wait. Vantage CNM is upgrading......
Vantage CNM upgrade has completed.
The Vantage CNM server will now restart.
Please wait for five more minutes before logging into Vantage CNM again.

After you upgrade Vantage CNM software, the Vantage CNM server will restart automatically. Wait for about five more minutes before you log into Vantage again.

20.2.2 Version Format

The Vantage CNM software version format is as follows:

A.B.CD.EF.GH

The following table details the format of this version code.

Table 118 Vantage Version Number

CODE	DESCRIPTION
A	This represents a major upgrade such as major new features or upgrade modules.
B	This represents a non-major upgrade such as new features and increased ZyXEL device support.
CD	This is the project code number.
EF	This represents the code for the operating system on which you can install this version of Vantage.
GH	This number changes for patch upgrades.

The version code of Vantage CNM for Windows XP with reporting menus is **2.2.00.81.00.**

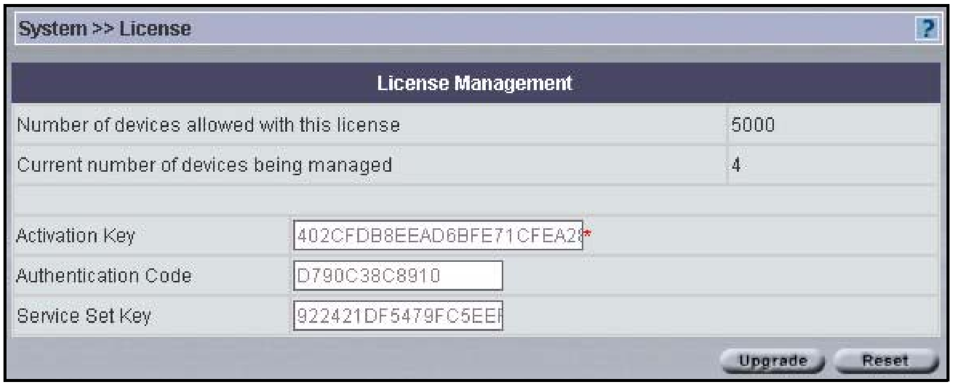
20.3 License Management

You need a license key to generate an **Activation Key** and **Server Set Key** in order to be able to use Vantage. See the *Quick Start Guide* for more information on generating keys at www.myZyXEL.com.

You get an initial license key when you first buy Vantage and after that you may buy expansion license keys in order to be able to manage more ZyXEL devices with Vantage.

Click **Vantage** > **License** to display the next screen.

Figure 153 System > License > License Management



System >> License

License Management

Number of devices allowed with this license	5000
Current number of devices being managed	4
Activation Key	402CFDB8EEAD6BFE71CFEA2*
Authentication Code	D790C38C8910
Service Set Key	922421DF5479FC5EEI

The following table describes the fields in this screen.

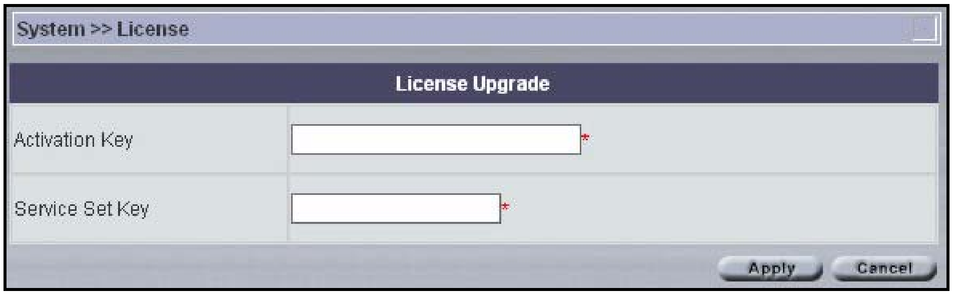
Table 119 System > License > License Management

LABEL	DESCRIPTION
Number of devices allowed with this license	This field displays the number of devices you are allowed to manage with this license. If you want to manage more devices, you need to purchase another license.
Current number of devices being managed	This field displays the number of devices currently registered with Vantage.
Activation Key	This key is generated in the myZyXEL.com website from the **Authentication Code**.
Authentication Code	This read-only field displays an automatically generated code after you have installed Vantage. Use this key to obtain an **Activation Key** and a **Service Set Key** from the myZyXEL.com website.
Service Set Key	This key is generated in the myZyXEL.com website. It identifies the set of licenses activated on a product.
Upgrade	Click **Upgrade** to proceed to the next screen.
Reset	Click **Reset** to begin configuring the screen afresh.

20.3.1 License Upgrade

Click **Upgrade** in Figure 153 on page 284 to display this screen.

Figure 154 System > License > License Management > Upgrade



The following table describes the fields in this screen.

Table 120 System > License > License Management > Upgrade

LABEL	DESCRIPTION
Activation Key	Copy and paste or type the **Activation Key** that is generated in the myZyXEL.com website.
Service Set Key	Copy and paste or type the **Service Set Key** that is generated in the myZyXEL.com website.
Apply	Click **Apply** to begin the license upgrade process. Vantage must have an Internet connection.
Cancel	Click **Cancel** to return to the previous screen.

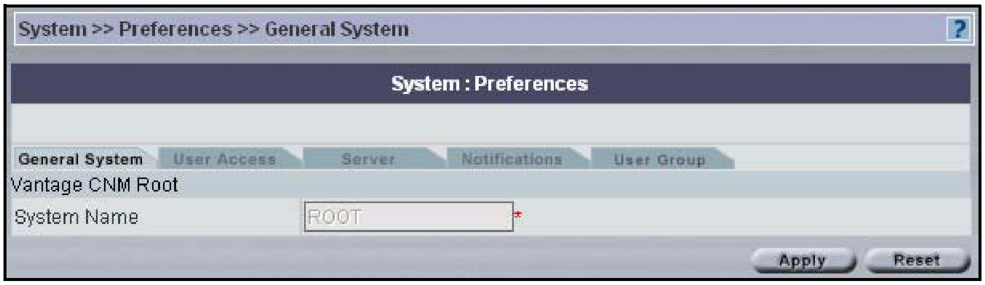
20.4 System >Preferences

System preferences are global Vantage server settings.

20.4.1 General Vantage Preferences

This is a read only screen.

Figure 155 System > Preferences > General System



Vantage CNM Root

System Name: ROOT *

The following table describes the fields in this screen.

Table 121 System > Preferences > General System

LABEL	DESCRIPTION
Vantage CNM Root	This refers to the root of the object tree.
System Name	The root of the object tree is called root by default.
Apply	You cannot edit this screen.
Reset	You cannot edit this screen.

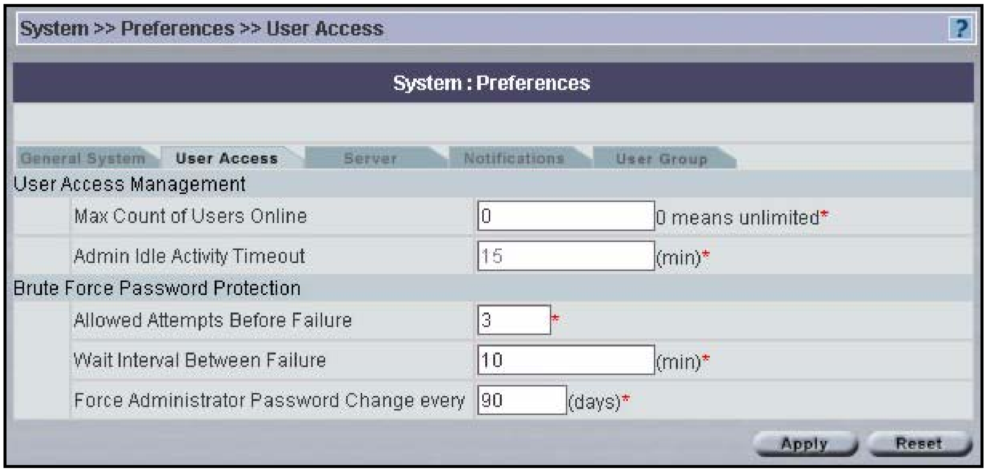
20.4.2 User Access

A User is an administrator. Set the maximum number of administrators allowed to log into Vantage at one time, Vantage idle time-out (so one administrator does not unwittingly hog resources by not logging out) and a brute force password protection mechanism in this screen.

Brute-Force Password Guessing Protection is a protection mechanism to discourage brute-force password guessing attacks on a device’s management interface. You can specify a wait-time that must expire before entering a fourth password after three incorrect passwords have been entered.

You can also force all administrators to periodically change their passwords in this screen.

Figure 156 System > Preferences > User Access



User Access Management

Max Count of Users Online	0	0 means unlimited*
Admin Idle Activity Timeout	15	(min)*

Brute Force Password Protection

Allowed Attempts Before Failure	3	*
Wait Interval Between Failure	10	(min)*
Force Administrator Password Change every	90	(days)*

The following table describes the fields in this screen.

Table 122 System > Preferences > User Access

	DESCRIPTION
Max Count of Users Online	Type the maximum number of administrators allowed to log into Vantage at any one time.
Admin Idle Activity Timeout	Type the length of time an Administrator can leave the Vantage web configurator idle before he is automatically logged out.
Brute Force Password Protection	Configure the next two fields to apply this.
Allowed Attempts Before Failure	Type the number of times an incorrect password may be entered before a login failure is returned.
Wait Interval Between Failure	Type the wait time before allowing another login in after a login failure is returned.
Force Administrator Password Change every	Type how often all Administrators must change their Vantage login passwords. If an Administrator does not change her password within this time, then the old password expires.
Apply	Click **Apply** to save your settings in Vantage.
Reset	Click **Reset** to begin configuring the screen afresh.

20.4.3 Servers

You can configure these servers as you install Vantage (in the installation wizard) or after you install it in this screen.

Configure the Vantage CNM public IP server address, FTP server (for firmware upload), syslog server (for logs) and mail server (for Vantage notifications and reports) in this screen. These IP addresses will be the same as the Vantage server computer if they are all on the same computer.

The FTP server is used for file transfers, such as firmware upgrade.

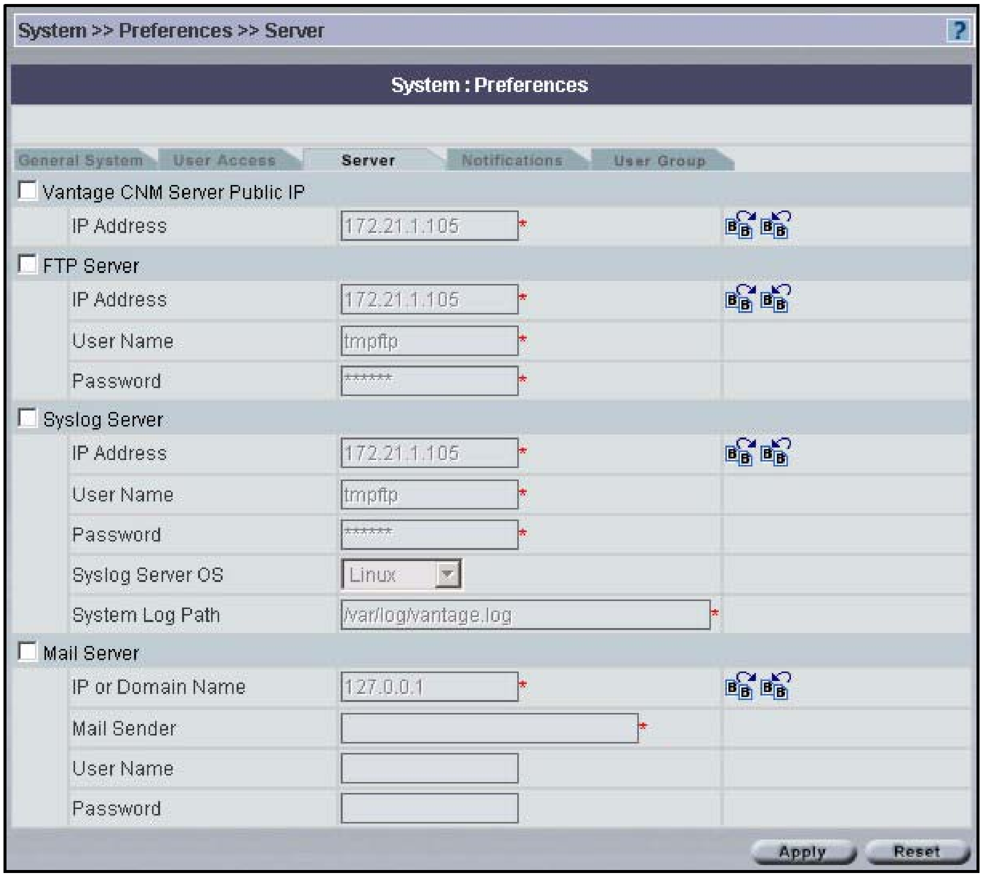
The SMTP server is used for e-mail notifications.

The syslog server is used to receive logs. The syslog server you configure for a device and the syslog server you configure for Vantage MUST be the same.

You should know each server's IP address, username and password. File transfers (FTP), e-mail notifications (SMTP) or log reports (syslog) will not work in Vantage if these are incorrectly configured.

See the Quick Start Guide for information on configuring the Linux syslog server to send logs to Vantage.

Figure 157 System > Preferences > Server



☐ Vantage CNM Server Public IP
IP Address: 172.21.1.105 *

☐ FTP Server
IP Address: 172.21.1.105 *
User Name: tmpftp *
Password: ****** *

☐ Syslog Server
IP Address: 172.21.1.105 *
User Name: tmpftp *
Password: ****** *
Syslog Server OS: Linux
System Log Path: /var/log/vantage.log *

☐ Mail Server
IP or Domain Name: 127.0.0.1 *
Mail Sender: *
User Name:
Password:

The following table describes the fields in this screen.

Table 123 System > Preferences > Server

LABEL	DESCRIPTION
Vantage CNM Server Public IP	Select the check box to make the IP address editable.
IP Address	Type the IP address of the communications server.
FTP Server	The FTP server is used for file uploads to and from Vantage. Select the checkbox to activate the fields below.

Table 123 System > Preferences > Server (continued)

LABEL	DESCRIPTION
IP Address	Type the IP address of the FTP server here.
User Name	Type your login name to this FTP server.
Password	Type the FTP server password associated with the login name.
Syslog Server	The FTP server is used for Vantage logs. Select the checkbox to activate the fields below.
IP Address	Type the IP address of the syslog server here.
User Name	Type your login name to this syslog server.
Password	Type the syslog server password associated with the login name.
Syslog Server OS	Choose Linux if your syslog server is Linux-based and choose Windows if your syslog server is Windows-based.
System Log Path	This displays the file path of your syslog server.
Mail Server	The mail (SMTP) server is used to send Vantage notifications. Select the checkbox to activate the fields below.
IP or Domain Name	Type the IP address or the domain name of the mail server here.
Mail Sender	Type a name to identify the mail server.
User Name	Type your login name to this mail server.
Password	Type the mail server password associated with the login name.
Apply	Click **Apply** to save your settings in Vantage.
Reset	Click **Reset** to begin configuring the screen afresh.

20.4.3.1 Vantage Server Public IP Address

If you change the Vantage server public IP address, then each (Vantage-registered) device's Manager IP address must change too.

1 Go to the **System** > **Preferences** > **Server** screen.

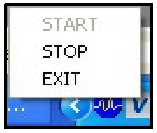
2 Enter the new IP address in the **Vantage CNM Public IP** field and **Apply**.

3 To change all registered devices' Manager IP address to the new IP address, you must do *one* of the following:

- Manually restart each device and wait about 5 minutes until the device registers with Vantage.
- Access each device's command line interface and enter "CNM managerIp x.x.x.x" where "x.x.x.x" is the new Vantage CNM public IP address.

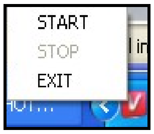
4 Restart Vantage CNM; you don't have to restart the computer on which Vantage CNM is installed. Right-click the Vantage icon in the system tray and select **STOP**.

Figure 158 Vantage Icon - Stop



Right-click the icon again and select **START**.

Figure 159 Figure 2-5 Vantage Icon - Start



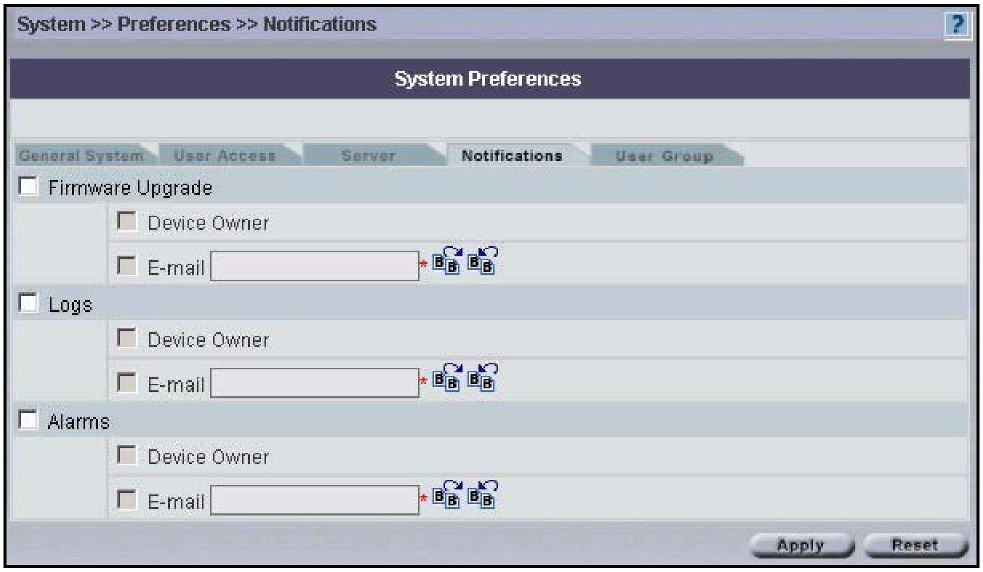
5 When you register new devices with Vantage, make sure the new device can ping the Vantage server (the new **Vantage CNM Public IP** address) and then set the device’s Manager IP address correspondingly.

20.4.4 Notifications

Use this screen to decide who should receive e-mails for events that may warrant immediate attention such as firmware upgrade or device logs and/or alarms. **Device Owner** is a variable that refers to the e-mail address of the device owner (configured in **Configuration > General > Owner Info** screen).

Use e-mail component BBs (building block) to rapidly configure both existing and new system notification entries.

Figure 160 System > Preferences > Notifications



The following table describes the fields in this screen.

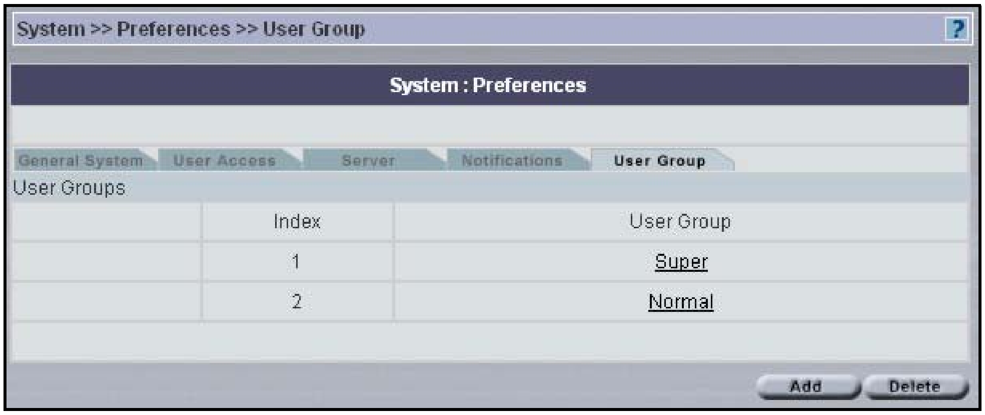
Table 124 System > Preferences > Notifications

	DESCRIPTION
Firmware Upgrade	Set who should be notified when you upload firmware to a device.
Device Owner	Select to have an e-mail automatically sent to the selected device owner e-mail address (configured in **Configuration > General > Owner Info**).
E-mail	Select a BB or enter multiple e-mail addresses separated by commas.
Logs	Set who should receive e-mailed logs.
Device Owner	Select to have an e-mail automatically sent to the selected device owner e-mail address (configured in **Configuration > General > Owner Info**).
E-mail	Select a BB or enter multiple e-mail addresses separated by commas.
Alarms	Set who should receive e-mailed alarms.
Device Owner	Select to have an e-mail automatically sent to the selected device owner e-mail address (configured in **Configuration > General > Owner Info**).
E-mail	Select a BB or enter multiple e-mail addresses separated by commas.
Apply	Click **Apply** to save your settings in Vantage.
Reset	Click **Reset** to begin configuring the screen afresh.

20.4.5 Vantage Permissions: User Group

A "user group" is a pre-defined set of administrator permissions. **Super** pre-defined permissions are not editable. Root may choose what default permissions are associated with the **Normal** permissions template here. Root can also create and delete new permission templates here.

Figure 161 System > Preferences > User Group



System >> Preferences >> User Group

System : Preferences

User Groups

	Index	User Group
	1	Super
	2	Normal

The following table describes the fields in this screen.

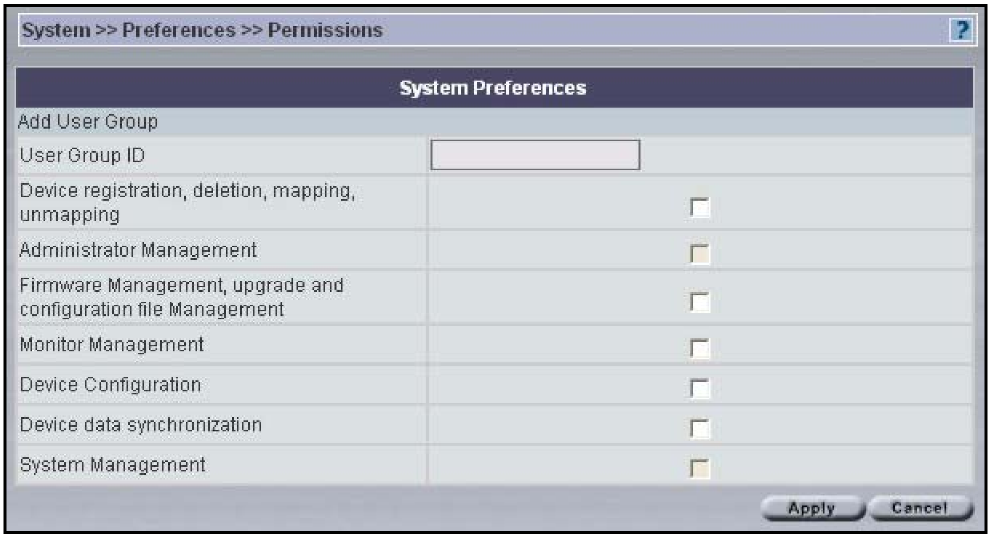
Table 125 System > Preferences > Permissions

LABEL	DESCRIPTION
Index	This is the template index number. 1 and 2 are default templates.
User Group	This field displays the template name (**User Group**).
Add	Click **Add** to create a new template.
Delete	Click **Delete** to remove a newly created template.

20.4.5.1 Add User Group

Create a new "user group" (administrator permission template) by clicking **Add** in the previous screen to display the next one as shown.

Figure 162 System > Preferences > Permissions > Add



System >> Preferences >> Permissions

System Preferences

Add User Group

User Group ID	
Device registration, deletion, mapping, unmapping	□
Administrator Management	□
Firmware Management, upgrade and configuration file Management	□
Monitor Management	□
Device Configuration	□
Device data synchronization	□
System Management	□

The following table describes the fields in this screen.

Table 126 System > Preferences > Permissions > Add

	DESCRIPTION
Add User Group	
User Group ID	Enter the new template name (**User Group**) in this field.
Device registration, deletion, mapping, unmapping	This field allows the Administrator to register and delete devices as well as associate and disassociate devices to a folder.
Firmware Management, upgrade and configuration file Management	This field allows the Administrator to upload device firmware and configuration files to Vantage, download device firmware and configuration files as well as remove them from Vantage.
Monitor Management	This field allows the Administrator access to the Monitor screens.
Device Configuration	This field allows the Administrator access to all the **System > Configuration** screens.
Device data synchronization	This field allows the Administrator access to the Device > Synchronize screen. See that screen information in this User's Guide for more details.
System Management	System Management is defined as follows: ➢ Vantage Upgrade ➢ License ➢ Preference ➢ Log option and purge log ➢ Maintenance
Apply	Click **Apply** to save your settings in Vantage.
Cancel	Click **Cancel** to begin configuring the screen afresh.

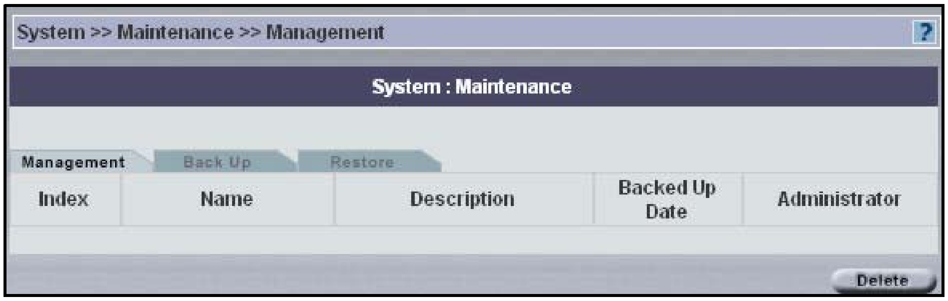
20.5 System Maintenance

Use the **Maintenance** screens to manage, back up and restore Vantage system backup files. Data maintenance includes device firmware and configuration files you have uploaded to the Vantage server. You can back up or restore to your computer or Vantage. You can choose what domain to back up by selecting a folder in the object tree.

20.5.1 System Maintenance Management

Use this screen to delete previous (old) system backups.

Figure 163 System > Maintenance > Management



The following table describes the fields in this screen.

Table 127 System > Maintenance > Management

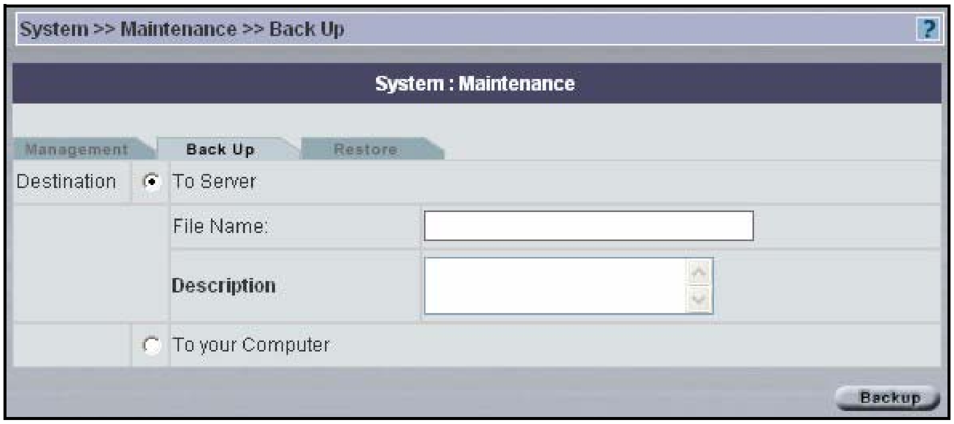
LABEL	DESCRIPTION
Index	This field displays the system backup file index number.
Name	This field displays the system backup file name.
Description	This field displays some extra description of the system backup file.
Backed Up Date	This field displays the date the system backup file was created.
Administrator	This field displays who created the system backup file.
Delete	Select a system backup file and then click **Delete** to remove it from Vantage.

20.5.2 Back Up System Maintenance

Use this screen to save your current Vantage system to the Vantage server or your computer. You can enter extra information on the file in the **Description** text box.

Backup configuration allows you to back up (save) the current configuration to a file on your computer. Once your device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings. You should perform system backup before you upgrade Vantage software.

Figure 164 System > Maintenance > Backup


System >> Maintenance >> Back Up

System : Maintenance

Destination ● To Server

File Name:

Description

○ To your Computer

The following table describes the fields in this screen.

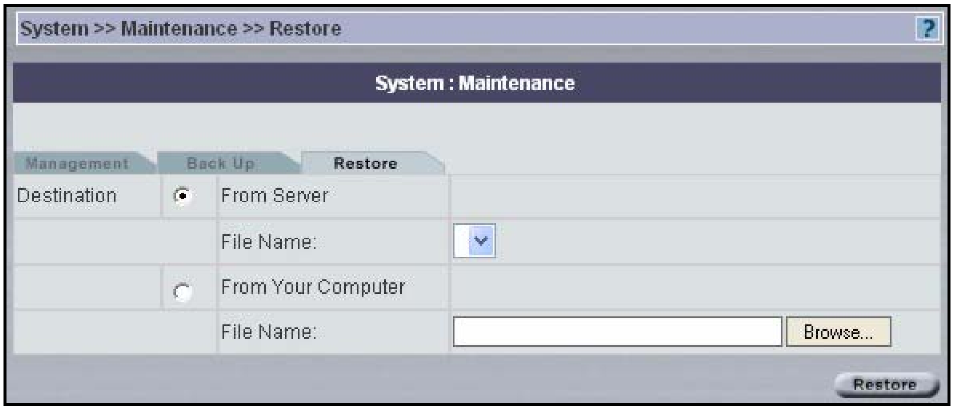
Table 128 System > Maintenance > Backup

LABEL	DESCRIPTION
Destination	Select the radio button to give the download destination to server.
To Server	Select this option to back up the file to the Vantage CNM server.
File Name	Type in the location of the file you want to upload in this field.
Description	Type a description of the file backup.
To your Computer	Select the radio button to give the download destination to your computer.
Backup	Click this button to perform the file backup.

20.5.3 Restore System Maintenance

Use this screen to restore a previously saved system backup (from your computer or Vantage) to Vantage.

Figure 165 System > Maintenance > Restore



The following table describes the fields in this screen.

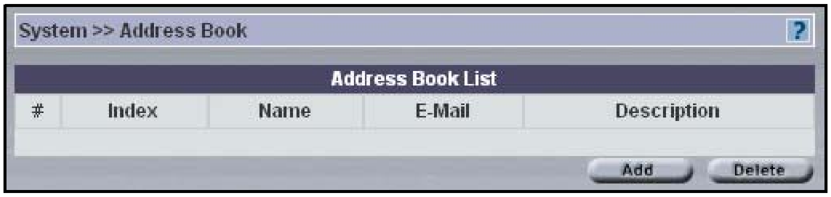
Table 129 System > Maintenance > Restore

LABEL	DESCRIPTION
Destination	Select this radio button to upload a configuration file **From Server**.
From Server	Select this option to restore the file from the Vantage CNM server.
File Name	Select a file from the drop-down list box.
From Your Computer	Select this radio button to upload a configuration file From **Your Computer**.
File Name	Type in the location of the file you want to upload in this field or click **Browse** ... to find it.
Restore	Click **Restore** to begin the upload process.

20.6 Address Book

An address book is a list of personal details of people such as device owners and administrators. Click **System** > **Address Book** to display the next screen.

Figure 166 System > Address Book



The following table describes the labels in this screen.

Table 130 System > Address Book

LABEL	DESCRIPTION
#	This is a number defining an address book entry.
Index	This field displays the address book entry index number.

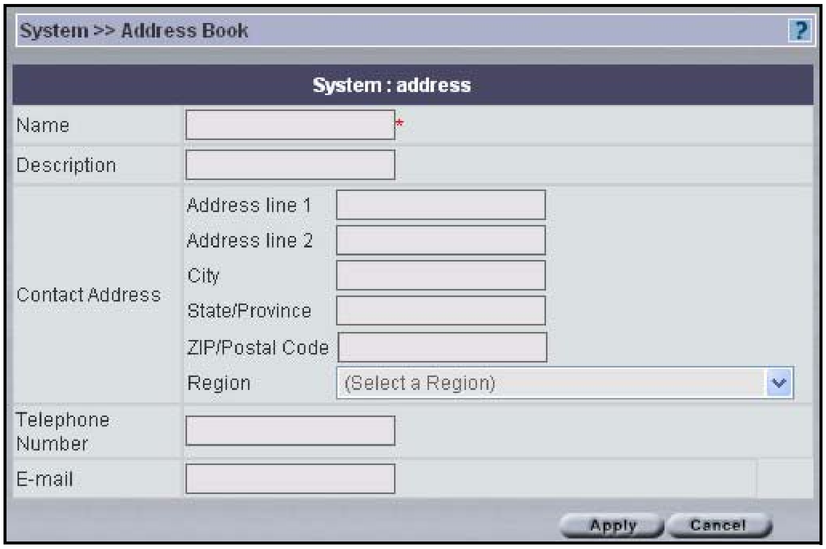
Table 130 System > Address Book

LABEL	DESCRIPTION
Name	This field displays the person’s name.
Email	This field displays the person’s e-mail address.
Description	This field displays some extra information about the person.
Add	Click **Add** to create a new customer record.
Delete	Select a system backup file and then click **Delete** to remove it from Vantage.

20.6.1 Address Book Add/Edit

From Figure 166 on page 296, click **Add** to create a new entry or click an existing entry hyperlink to edit it.

Figure 167 System > Address Book Add/Edit



The following table describes the labels in this screen.

Table 131 System > Address Book Add/Edit

LABEL	DESCRIPTION
Name	Type the person’s name.
Description	Type some extra information about the person.
Contact Address	Type a mailing address for this person.
Telephone Number	Type the complete telephone number including area codes for this person.
E-mail	Type the person’s e-mail address.
Apply	Click **Apply** to create a new address book record.
Cancel	Click **Cancel** to return to the previous screen.

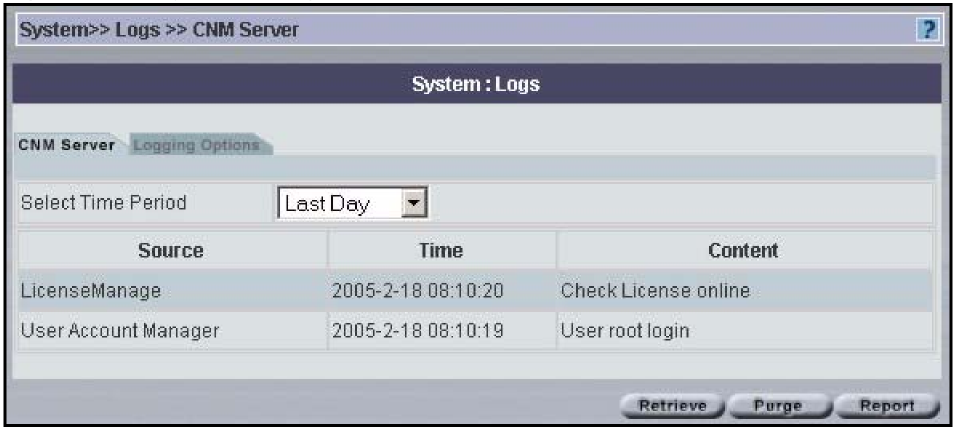
20.7 Vantage Logs

Use these screens to view and configure Vantage system log preferences.

20.7.1 CNM Server

You can view system logs for previous day, the last two days or up to one week here.

Figure 168 System > Logs > CNM Server



Select Time Period: Last Day

Source	Time	Content
LicenseManage	2005-2-18 08:10:20	Check License online
User Account Manager	2005-2-18 08:10:19	User root login

The following table describes the labels in this screen.

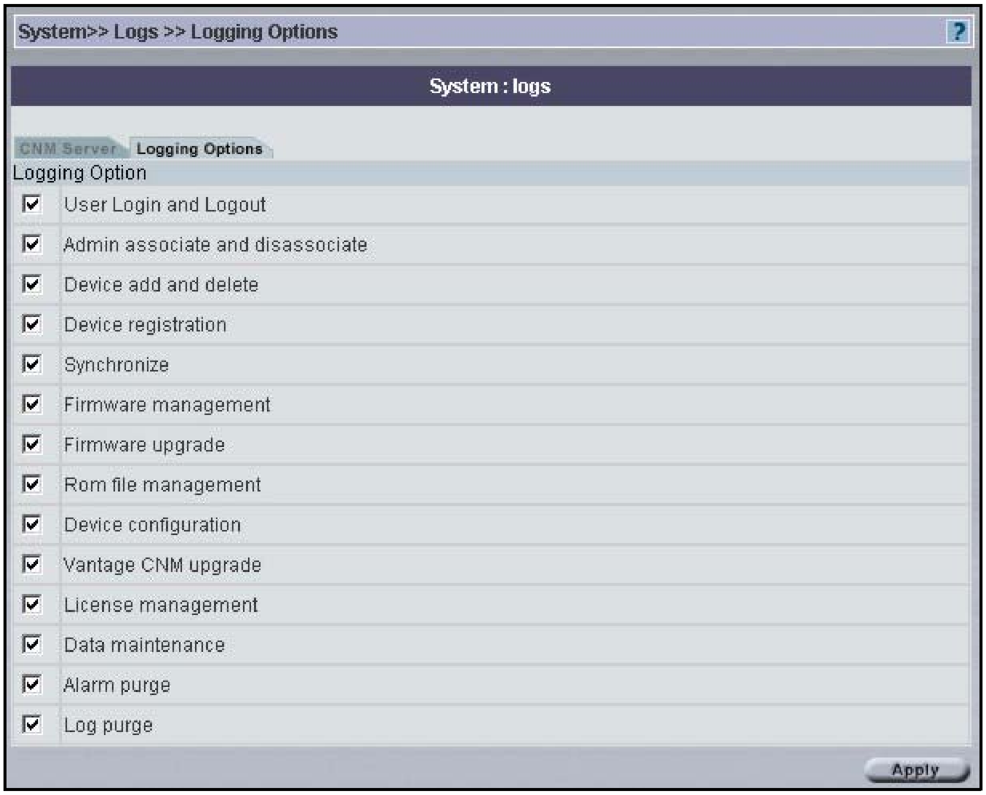
Table 132 System > Logs > CNM Server

LABEL	DESCRIPTION
Select Time Period	Select the time period for which you wish to view Vantage logs
Source	This field displays the source of the Vantage log.
Time	This field displays the date the Vantage log occurred.
Content	This field displays a message describing for the log.
Retrieve	Click **Retrieve** for Vantage to pull the logs from the selected device.
Purge	Select **Purge** to delete system logs from the Vantage server.
Report	Click **Report** to generate a report on the logs for the time period selected.

20.7.2 Vantage Logging Options

Select what type of system logs you wish to log as shown in the following screen.

Figure 169 System > Logging Options



Logging Option

☑ User Login and Logout
☑ Admin associate and disassociate
☑ Device add and delete
☑ Device registration
☑ Synchronize
☑ Firmware management
☑ Firmware upgrade
☑ Rom file management
☑ Device configuration
☑ Vantage CNM upgrade
☑ License management
☑ Data maintenance
☑ Alarm purge
☑ Log purge

20.8 Certificate Management Overview

Vantage CNM can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. You can use Vantage CNM to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

In public-key encryption and decryption, each host has two keys. One key is public and can be made openly available; the other key is private and must be kept secure. Public-key encryption in general works as follows.

1 Tim wants to send a private message to Jenny. Tim generates a public key pair. What is encrypted with one key can only be decrypted using the other.

2 Tim keeps the private key and makes the public key openly available.

3 Tim uses his private key to encrypt the message and sends it to Jenny.

4 Jenny receives the message and uses Tim's public key to decrypt it.

5 Additionally, Jenny uses her own private key to encrypt a message and Tim uses Jenny's public key to decrypt the message.

Vantage CNM uses certificates based on public-key cryptology to authenticate users attempting to establish a connection, not to encrypt the data that you send after establishing a connection. The method used to secure the data that you send through an established connection depends on the type of connection. For example, a VPN tunnel might use the triple DES encryption algorithm.

The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates.

A certification path is the hierarchy of certification authority certificates that validate a certificate. The ZyXEL device does not trust a certificate if any certificate on its path has expired or been revoked.

Certification authorities maintain directory servers with databases of valid and revoked certificates. A directory of certificates that have been revoked before the scheduled expiration is called a CRL (Certificate Revocation List). The ZyXEL device can check a peer's certificate against a directory server's list of revoked certificates. The framework of servers, software, procedures and policies that handles keys is called PKI (public-key infrastructure).

20.8.1 Advantages of Certificates

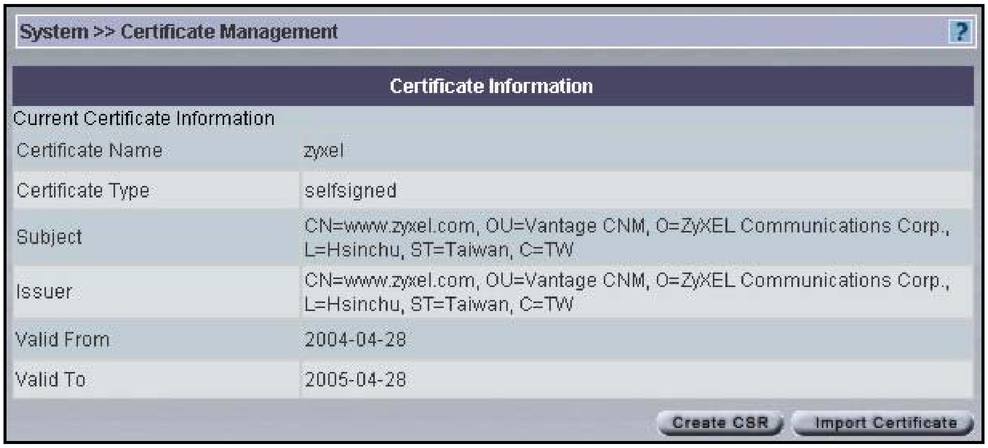
The ZyXEL device only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.

Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

20.8.2 Current Certification Information

You can view your current certificate information in the following screen, including certificate name, type, origin and duration of validity.

Figure 170 System > Certificate Management > Information



System >> Certificate Management

Certificate Information

Current Certificate Information

Certificate Name	zyxel
Certificate Type	selfsigned
Subject	CN=www.zyxel.com, OU=Vantage CNM, O=ZyXEL Communications Corp., L=Hsinchu, ST=Taiwan, C=TW
Issuer	CN=www.zyxel.com, OU=Vantage CNM, O=ZyXEL Communications Corp., L=Hsinchu, ST=Taiwan, C=TW
Valid From	2004-04-28
Valid To	2005-04-28

The following table describes the labels in this screen.

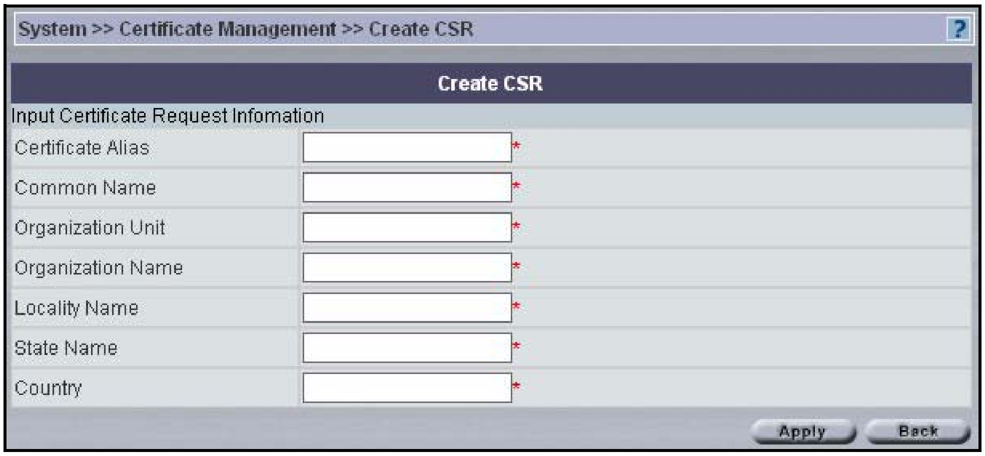
Table 133 System > Certificate Management > Information

LABEL	DESCRIPTION
Current Certificate Information	
Certificate Name	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Certificate Type	This field displays what kind of certificate this is. **selfsigned** represents the default self-signed certificate. Use the **Create CSR** to create a new certificate also called **selfsigned**. The new certificate only becomes valid after you restart Vantage. **CATrust** represents a certificate issued by a certification authority. Use the **Import Certificate** screen to import the certificate and replace the old certificate. The new certificate only becomes valid after you restart Vantage.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country such as CN (China), UK (United Kingdom), US (United States)). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the **Subject** field.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a "Not Yet Valid!" message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an "Expiring!" or "Expired!" message if the certificate is about to expire or has already expired.
Create CSR	Click **Create CSR** to go create a certificate.
Import Certificate	Click **Import Certificate** to go to the Import Certificate screen.

20.8.3 Create a Certificate

You can create certificates by entering the requested information into the fields below. Then click **Apply**.

Figure 171 System > Certificate Management > Create CSR



The following table describes the labels in this screen.

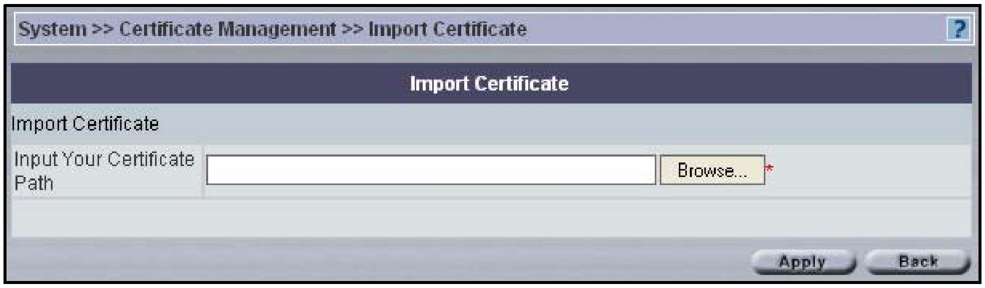
Table 134 System > Certificate Management > Create CSR

LABEL	DESCRIPTION
Input Certificate Request Information	
Certificate Alias	Type a name to identify the certificate.
Common Name	Type a name to identify the certificates owner.
Organization Unit	Type the organization unit or department in this field.
Organization Name	Type the organization name or company in this field.
Locality Name	Type your company location; number, street etc.
State Name	Type the **State** or county where your company is located.
Country	Type the **Country** where your company is located.
Apply	Click **Apply** to save these changes.
Back	Click **Back** to return to the previous screen.

20.8.4 Importing Certificates

In the following screen, you can **Browse** for a certificate that has already been downloaded to your computer. Select **Apply** to complete the certificate import.

Figure 172 System > Certificate Management > Import Certificate



System >> Certificate Management >> Import Certificate

Import Certificate

Import Certificate

Input Your Certificate Path

The following table describes the labels in this screen.

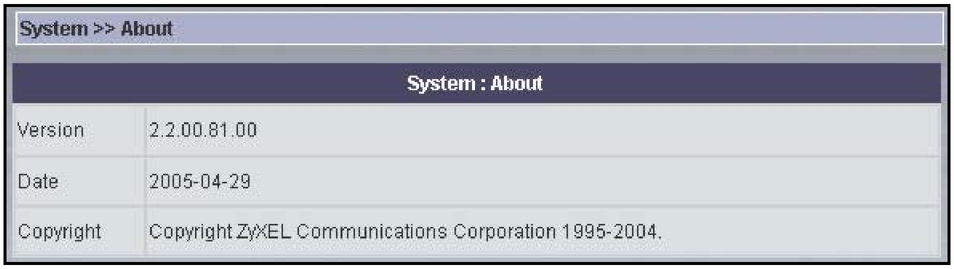
Table 135 System > Certificate Management > Import Certificate

LABEL	DESCRIPTION
Input Certificate	
Input Your Certificate Path	Type in the location of the certificate you want to upload in this field or click **Browse** ... to find it.
Apply	Click **Apply** to save these changes.
Back	Click **Back** to return to the previous screen.

20.9 About Vantage

The **About** screen provides some basic information about Vantage as shown in the following screen.

Figure 173 System > About Vantage



System >> About

System : About

Version	2.2.00.81.00
Date	2005-04-29
Copyright	Copyright ZyXEL Communications Corporation 1995-2004.

CHAPTER 21
Monitor > Alarms

This chapter describes the monitor alarms.

21.1 Alarms

Select a domain in the object tree to view alarms for that domain.

Alarms are time-critical information that the ZyXEL device automatically sends out at the time of occurrence.

21.1.1 Alarm Types

There are three types of alarms.

Table 136 Types of Alarms

TYPE	DESCRIPTION
All	This displays all types of alarms.
Device	This is an alarm such as hardware failure or the network connection is down.
CNM	This is an alarm such as server communication error or illegal Vantage login attempt.

21.1.2 Alarm Classifications

There are four alarm severity classifications.

Table 137 Alarm Severity

SEVERITY	DESCRIPTION
All	This displays all alarm severities.
Fatal	This is an alarm such as unrecoverable hardware failure.
Major	This is an alarm such as an attack.
Minor	This is an alarm such as a recoverable hardware error.
Warning	This is an alarm such as an illegal Vantage login attempt.

21.1.3 Alarm States

When an alarm is received by Vantage, it can be in one of three states:

Table 138 Alarm States

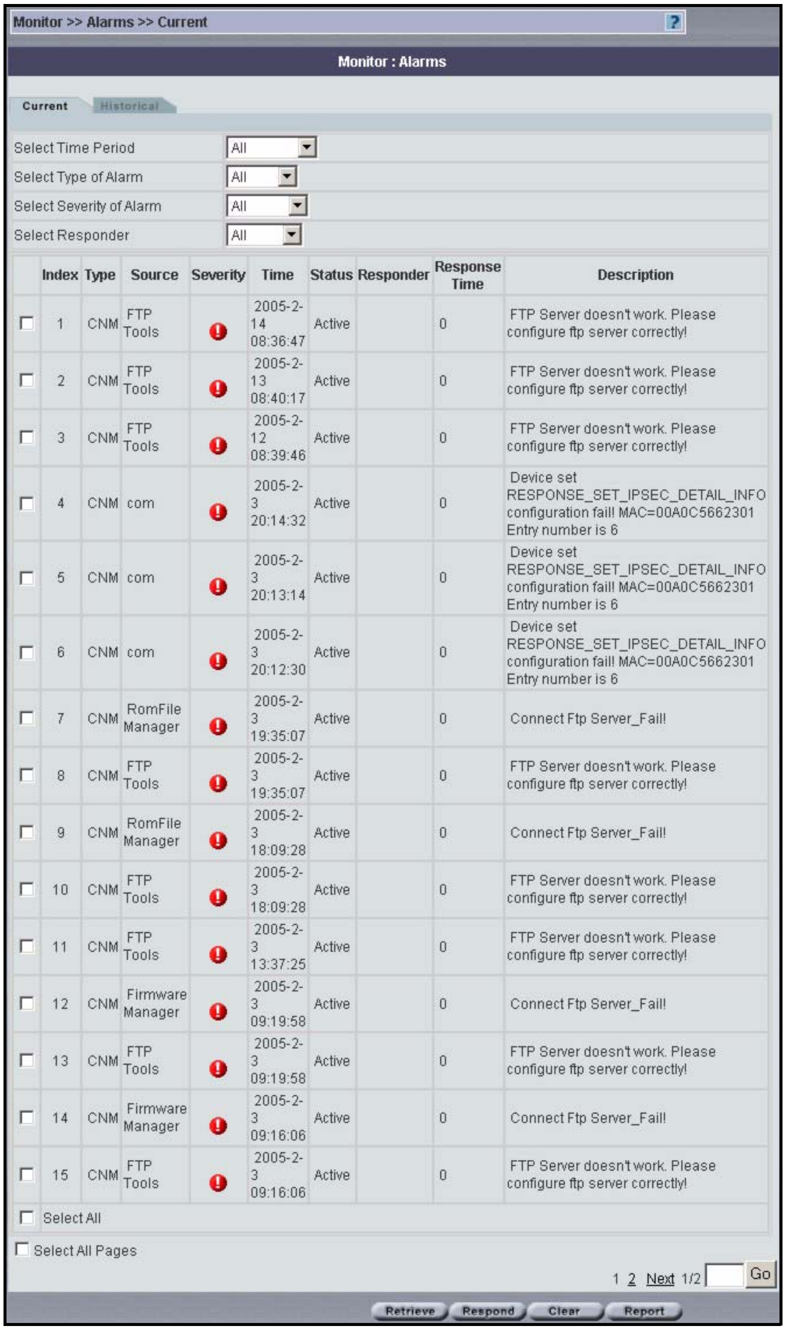
STATE	DESCRIPTION
Active	This is the initial state of an alarm, which means this alarm is new and no one has assumed responsibility for handling it yet.
Acknowledged	This means that one administrator has decided to respond to the cause of this alarm. Other administrators see that person’s name in their alarm screen and so duplicate effort in solving the same problem is avoided.
Cleared	After the administrator has solved the cause of the alarm, he/she can clear the alarm. When an alarm is cleared, it is removed from the current alarm screen and becomes an historical alarm.

21.1.4 Current Alarms Screen

View recent alarms and who has taken care of or is taking care of them in this screen.

You may also configure to have administrators automatically e-mailed when an alarm occurs in the **System > Preferences >Notifications** screen. Alarm becomes historical after selecting **Clear**.

Figure 174 Monitor > Current Alarms



Monitor >> Alarms >> Current

Monitor : Alarms

Select Time Period	All
Select Type of Alarm	All
Select Severity of Alarm	All
Select Responder	All

	Index	Type	Source	Severity	Time	Status	Responder	Response Time	Description
□	1	CNM	FTP Tools	❗	2005-2-14 08:36:47	Active		0	FTP Server doesn't work. Please configure ftp server correctly!
□	2	CNM	FTP Tools	❗	2005-2-13 08:40:17	Active		0	FTP Server doesn't work. Please configure ftp server correctly!
□	3	CNM	FTP Tools	❗	2005-2-12 08:39:46	Active		0	FTP Server doesn't work. Please configure ftp server correctly!
□	4	CNM	com	❗	2005-2-3 20:14:32	Active		0	Device set RESPONSE_SET_IPSEC_DETAIL_INFO configuration fail! MAC=00A0C5662301 Entry number is 6
□	5	CNM	com	❗	2005-2-3 20:13:14	Active		0	Device set RESPONSE_SET_IPSEC_DETAIL_INFO configuration fail! MAC=00A0C5662301 Entry number is 6
□	6	CNM	com	❗	2005-2-3 20:12:30	Active		0	Device set RESPONSE_SET_IPSEC_DETAIL_INFO configuration fail! MAC=00A0C5662301 Entry number is 6
□	7	CNM	RomFile Manager	❗	2005-2-3 19:35:07	Active		0	Connect Ftp Server_Fail!
□	8	CNM	FTP Tools	❗	2005-2-3 19:35:07	Active		0	FTP Server doesn't work. Please configure ftp server correctly!
□	9	CNM	RomFile Manager	❗	2005-2-3 18:09:28	Active		0	Connect Ftp Server_Fail!
□	10	CNM	FTP Tools	❗	2005-2-3 18:09:28	Active		0	FTP Server doesn't work. Please configure ftp server correctly!
□	11	CNM	FTP Tools	❗	2005-2-3 13:37:25	Active		0	FTP Server doesn't work. Please configure ftp server correctly!
□	12	CNM	Firmware Manager	❗	2005-2-3 09:19:58	Active		0	Connect Ftp Server_Fail!
□	13	CNM	FTP Tools	❗	2005-2-3 09:19:58	Active		0	FTP Server doesn't work. Please configure ftp server correctly!
□	14	CNM	Firmware Manager	❗	2005-2-3 09:16:06	Active		0	Connect Ftp Server_Fail!
□	15	CNM	FTP Tools	❗	2005-2-3 09:16:06	Active		0	FTP Server doesn't work. Please configure ftp server correctly!

□ Select All

□ Select All Pages

Table 139 Monitor > Current Alarms

STATE	DESCRIPTION
Select Time Period	Select the time period for which you wish to view alarms.
Select Type of Alarm	Select the type of alarm you wish to view.
Select Severity of Alarm	Select the type of alarm you wish to view.
Select Responder	Select the administrator to view the alarms that administrator has responded to.

Table 139 Monitor > Current Alarms

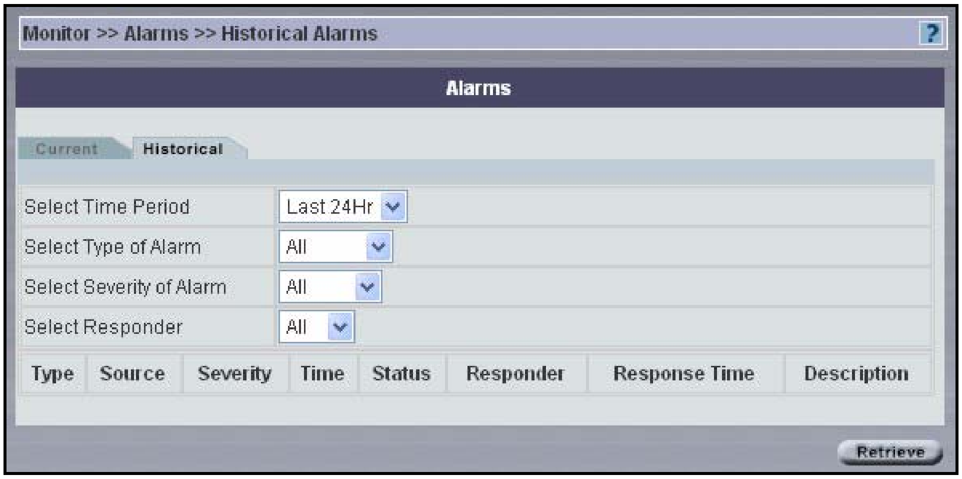
STATE	DESCRIPTION
Checkbox/Select All	Select a checkbox(es) and then click **Clear** to erase those alarms.
Index	This is the alarm index number.
Type	This is the type of alarm.
Severity	This is the alarm severity.
Time	This is the time the alarm occurred.
Status	This is the state of the alarm.
Responder	This is the administrator who responded to the alarm.
Response Time	This is the time the alarm occurred.
Description	This is the reason the alarm occurred.
Retrieve	Click **Retrieve** for Vantage to display the most recent alarms. These alarms may be displayed in another page.
Respond	Select an alarm and then click **Respond** to take responsibility for finding the cause of this alarm.
Clear	Select an alarm(s) and click **Clear** to erase this alarm(s).
Report	Click **Report** to generate a report on the alarms currently being viewed.

21.1.5 Historical Alarms

Historical alarms are alarms that have been cleared by an administrator.

This screen includes viewing filters for time, alarm type, alarm severity type and the administrator who responded to the alarm here.

Figure 175 Monitor > Historical Alarms



Select Time Period	Last 24Hr
Select Type of Alarm	All
Select Severity of Alarm	All
Select Responder	All

Type	Source	Severity	Time	Status	Responder	Response Time	Description

See Table 139 on page 306 for more information on fields in this table.

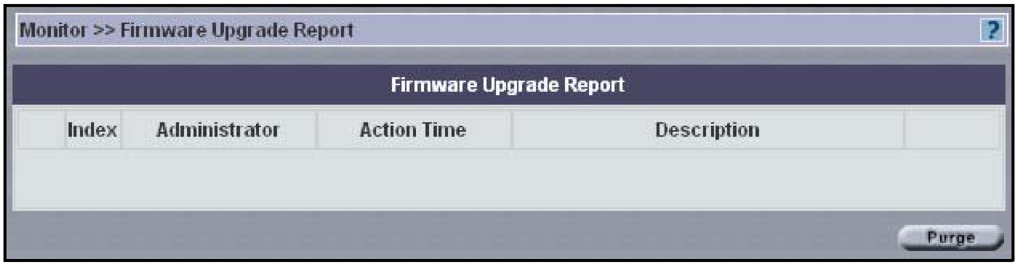
CHAPTER 22
Other Monitor Screens

Firmware Upgrade means that Vantage signals the device to request a firmware FTP upload from Vantage.

22.1 Firmware Upgrade Report

Details of firmware uploaded to Vantage are shown as in the next screen.

Figure 176 Monitor > Firmware Upgrade Report



The following table describes the labels in this screen.

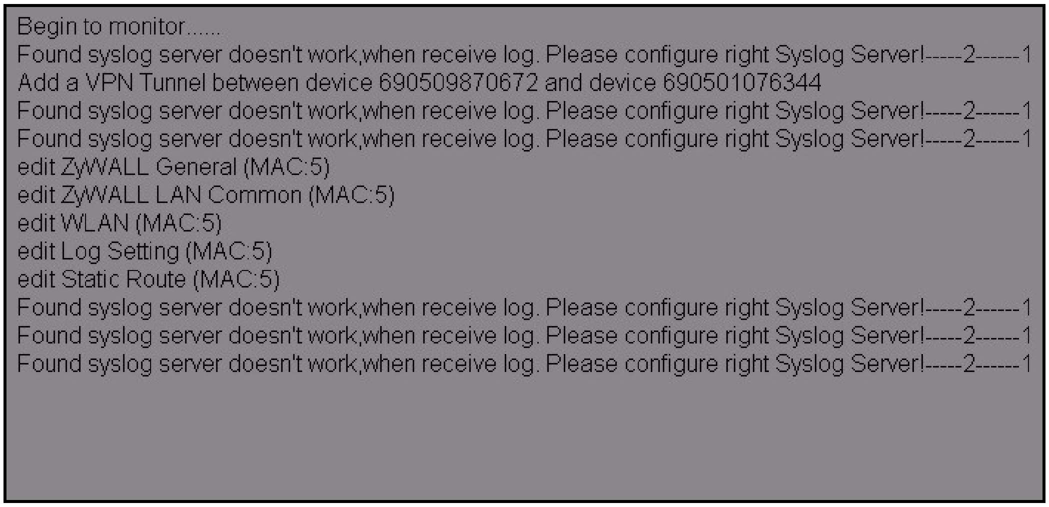
Table 140 Monitor > Firmware Upgrade Report

LABEL	DESCRIPTION
Index	This is the upgrade list number.
Administrator	This displays the administrator who performed the upgrade.
Action Time	This displays the time at which the upgrade was performed.
Description	This displays a description entered in **Firmware Upgrade** prior to uploading.
Purge	Select **Purge** to delete selected reports from the Vantage server.

22.2 Status Monitor

This is a real time message monitor that displays messages such as urgent alerts and when an administrator has logged in or logged out. Click **Monitor > Status Monitor** and wait for Vantage to retrieve information and display it.

Figure 177 Monitor > Monitor Status



```
Begin to monitor......
Found syslog server doesn't work,when receive log. Please configure right Syslog Server!-----2------1
Add a VPN Tunnel between device 690509870672 and device 690501076344
Found syslog server doesn't work,when receive log. Please configure right Syslog Server!-----2------1
Found syslog server doesn't work,when receive log. Please configure right Syslog Server!-----2------1
edit ZyWALL General (MAC:5)
edit ZyWALL LAN Common (MAC:5)
edit WLAN (MAC:5)
edit Log Setting (MAC:5)
edit Static Route (MAC:5)
Found syslog server doesn't work,when receive log. Please configure right Syslog Server!-----2------1
Found syslog server doesn't work,when receive log. Please configure right Syslog Server!-----2------1
Found syslog server doesn't work,when receive log. Please configure right Syslog Server!-----2------1
```

22.3 VPN Editor

This is a graphical VPN editor screen where you can click and drag VPN tunnels (single-click VPN) and also view individual tunnel details.

The following table lists the icons that are used in the **Monitor**, **VPN Editor** screens.

Table 141 VPN Editor Icons

ICON	DESCRIPTION
Edit	Edit the selected tunnel.
Delete	Delete the selected tunnel.
Save	Save a devices topology.
Force	Force delete the selected tunnel.
Refresh	Refresh the VPN monitor.
	A turned On ZyXEL device.
	A turned Off ZyXEL device.

22.3.1 VPN Editor Configuration

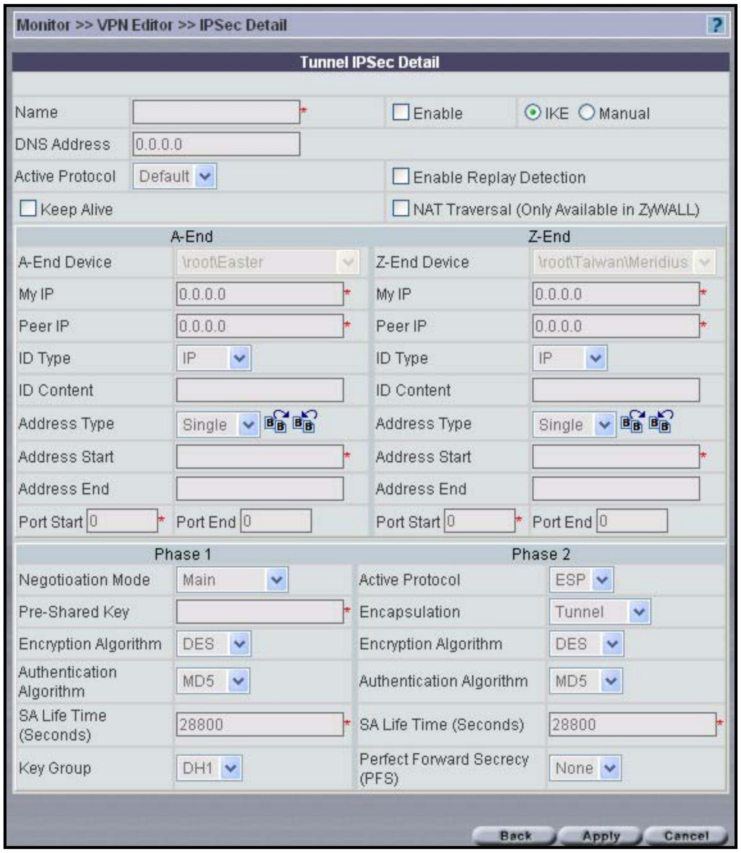
Configure IPSec tunnels graphically by doing the following

1 Right-click the **To VPN Editor** option on a device node in the object tree view. See Devices on page 45.

2 You see the **Tunnel IPSec Detail** screen as shown next. Note that information in some fields has been automatically generated for you when you configure VPN this way. See Section 11.12.1 on page 181 for information on configuring this screen. At minimum,

you must fill in the fields with the red asterisks. You can accept (or change) the automatically configured information in the other fields to set up the tunnel.

Figure 178 Monitor > VPN Editor > Tunnel IPSec Detail



Monitor >> VPN Editor >> IPSec Detail

Tunnel IPSec Detail

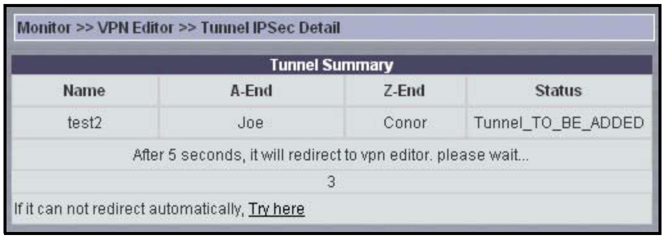
Name	*	□ Enable	● IKE ○ Manual
DNS Address	0.0.0.0		
Active Protocol	Default	□ Enable Replay Detection	
□ Keep Alive		□ NAT Traversal (Only Available in ZyWALL)	

A-End		Z-End	
A-End Device	\root\Easter	Z-End Device	\root\Taiwan\Meridius
My IP	0.0.0.0 *	My IP	0.0.0.0 *
Peer IP	0.0.0.0 *	Peer IP	0.0.0.0 *
ID Type	IP	ID Type	IP
ID Content		ID Content	
Address Type	Single	Address Type	Single
Address Start	*	Address Start	*
Address End		Address End	
Port Start 0 *	Port End 0	Port Start 0 *	Port End 0

Phase 1		Phase 2	
Negotioation Mode	Main	Active Protocol	ESP
Pre-Shared Key	*	Encapsulation	Tunnel
Encryption Algorithm	DES	Encryption Algorithm	DES
Authentication Algorithm	MD5	Authentication Algorithm	MD5
SA Life Time (Seconds)	28800 *	SA Life Time (Seconds)	28800 *
Key Group	DH1	Perfect Forward Secrecy (PFS)	None

3 Click **Apply** to go to a tunnel summary screen. The **Tunnel Summary** shows the **Name** of your tunnel, A-End and Z-End devices and the current tunnel Status.

Figure 179 Configuration > VPN - Example Tunnel Summary



Monitor >> VPN Editor >> Tunnel IPSec Detail

Tunnel Summary

Name	A-End	Z-End	Status
test2	Joe	Conor	Tunnel_TO_BE_ADDED

After 5 seconds, it will redirect to vpn editor. please wait...

3

If it can not redirect automatically, Try here

4 If you are not redirected, click the **Try here** hyperlink to go to the next screen.

Note: The Tunnel Summary details are added to the top of the IPSec Summary, see Figure 180 in the order they are configured (last tunnel appears last in the list).

5 Drag the ZyXEL device icons around the screen as you please (the icons are on top of each other in the top left corner of the screen in the beginning. Drag them apart to view each of them). Save this view by clicking **Save**.

6 Right-click a ZyXEL device (A-End) and select **VPN** in the popup menu. Click the ZyXEL device again and drag (you should see a red line) to another ZyXEL device (Z-End), then release the mouse button.

22.3.2 Tunnel Graphical Depictions

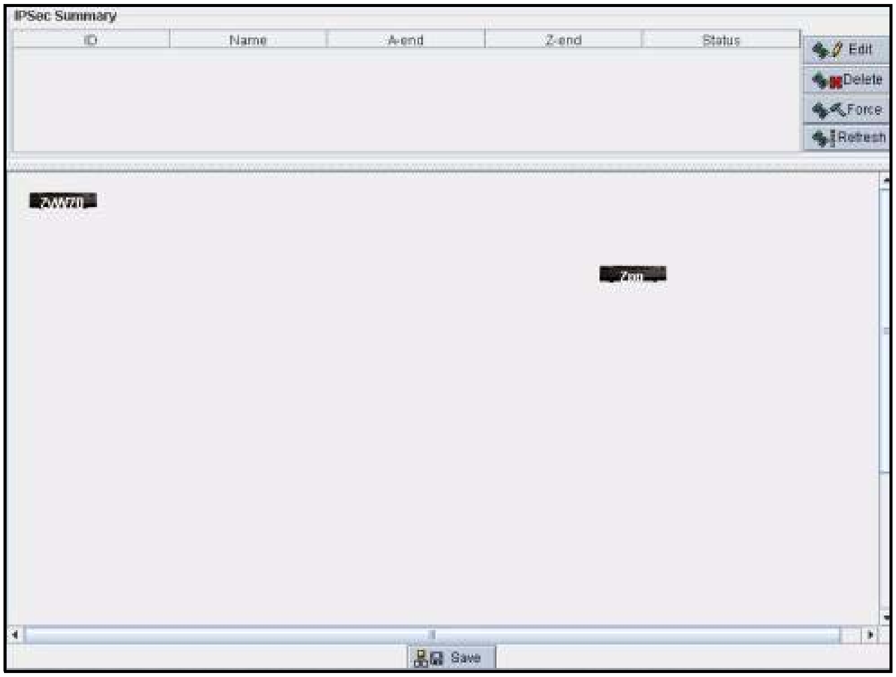
A gray dashed line means that the Vantage server has not yet synchronized VPN tunnel information with both devices. This may be because Vantage has not so far communicated with one of the devices.

A gray solid line means that the VPN tunnel is set up between the devices but the tunnel is not active yet (no traffic).

A green solid line means an active tunnel (with traffic) between the ZyXEL devices.

The icons are dragged apart and dashed lines indicating VPN Tunnels are created after configuring the **Tunnel IPSec Detail** screen.

Figure 180 Monitor > VPN Monitor – Tunnel Graphics



IPSec Summary

ID	Name	A-end	Z-end	Status

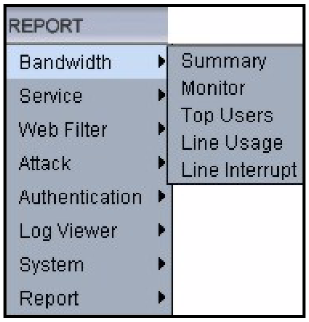
CHAPTER 23 Introduction to Reports

Vantage CNM can collect and analyze logs from the ZyXEL devices that you select in the object tree. Use the report screens to create graphical representations of data gathered from the logs over a period of time (that you configure) and send scheduled e-mail reports. Use these reports to monitor network access, enhance security, and anticipate future bandwidth needs.

23.1 Bandwidth Reports

Use the bandwidth reports to view bandwidth handled by selected ZyXEL device(s), view real time bandwidth usage and who used the most bandwidth over the specified time period.

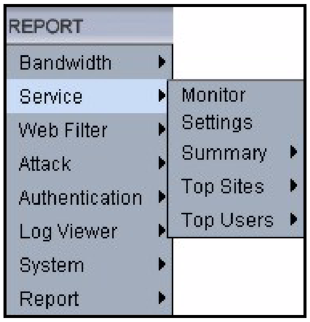
Figure 181 Bandwidth Reports



23.2 Service Reports

Use the service reports to monitor service usage over time handled by the selected ZyXEL devices, create TCP/UDP custom services, view bandwidth consumed by a service, what sites were accessed using the service and who used a service.

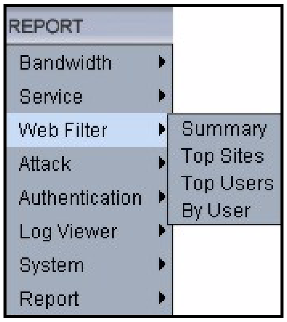
Figure 182 Service Reports



23.3 Web Filter Reports

Use the web filter reports to view statistics on who attempted to access what blocked sites and when via the selected ZyXEL device(s).

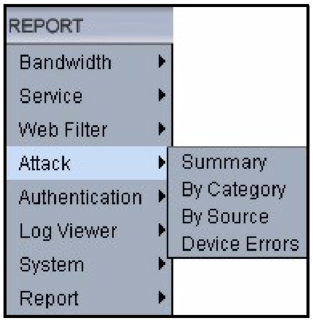
Figure 183 Web Filter Reports



23.4 Attack Reports

Use the attack reports to view statistics on who performed what kind of attacks on selected ZyXEL devices and information on packets dropped by those ZyXEL devices.

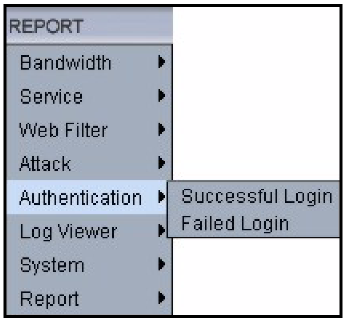
Figure 184 Attack Reports



23.5 Authentication Reports

Use the authentication reports screens to view successful and failed logins to selected ZyXEL devices over the specified period of time.

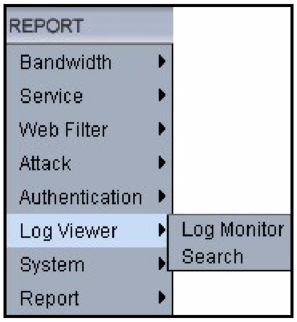
Figure 185 Authentication Reports



23.6 Log Viewer Reports

Use these reports to view, purge and search for logs from the selected ZyXEL device(s).

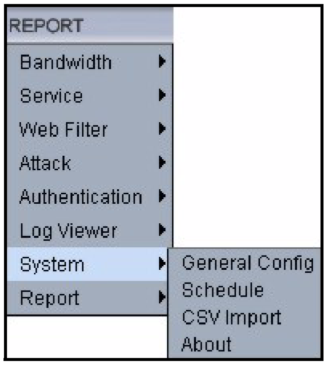
Figure 186 Log Viewer Reports



23.7 System Reports

Use these screens to configure global reporting parameters such as refresh intervals, syslog retrieval intervals, days to keep logs and default chart types (pie or chart). You can also schedule reports to be sent by e-mail and import a Comma-Separated Value (CSV) text file (of purged logs).

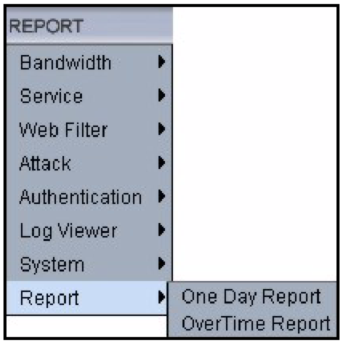
Figure 187 System Reports



23.8 Reports

Use these screens to configure e-mail details, report types to be sent and report sending schedule.

Figure 188 Schedule Reports



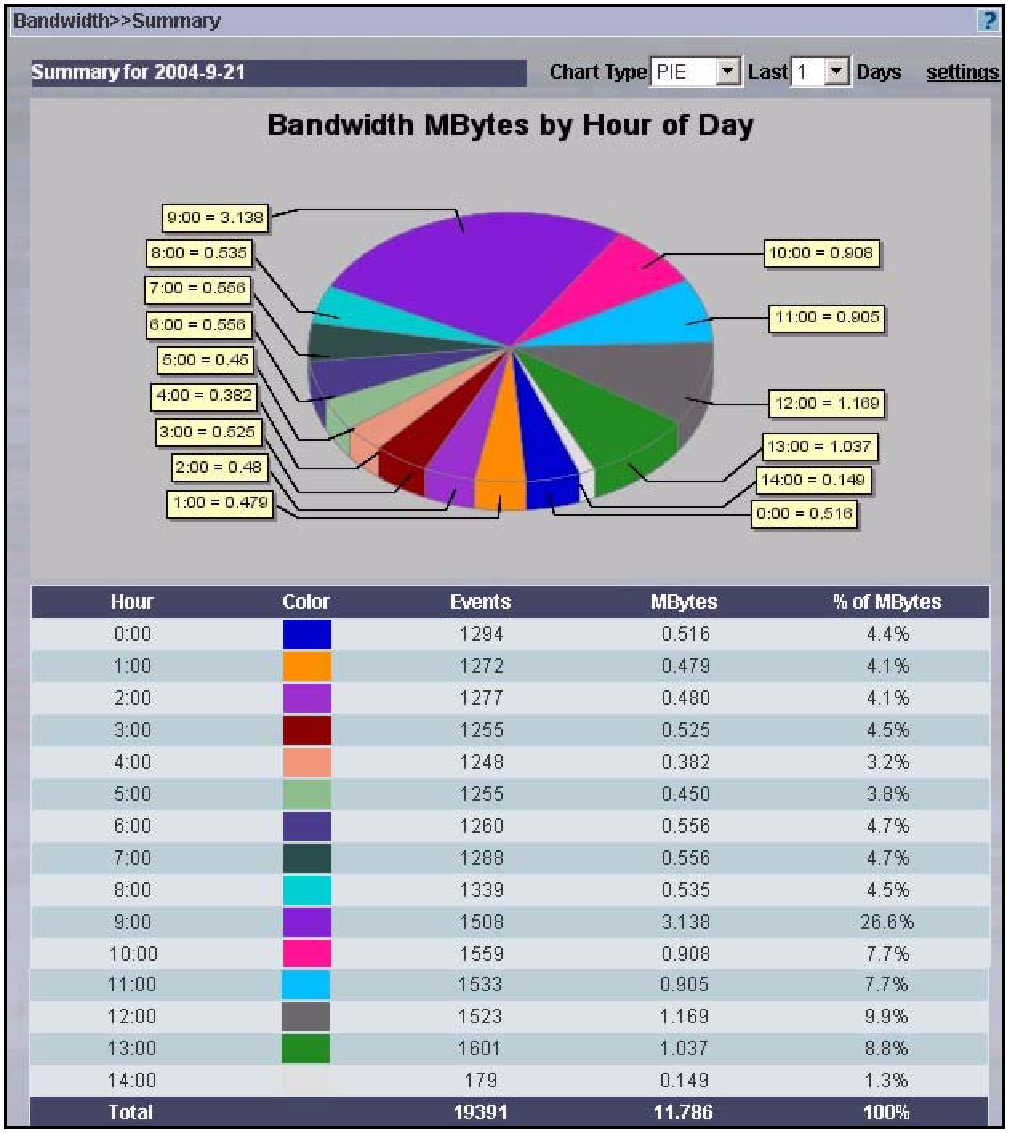
CHAPTER 24
Bandwidth Reports

24.1 Introduction

The Bandwidth Summary report contains information on the amount of traffic handled by a selected ZyXEL device(s) over the specified time period.

To view the Bandwidth Summary report, select ZyXEL device(s) and click **Report, Bandwidth**, **Summary**.

Figure 189 Bandwidth Summary



Summary for 2004-9-21

Chart Type PIE ▼ Last 1 ▼ Days settings

Hour	Color	Events	MBytes	% of MBytes
0:00	🟦	1294	0.516	4.4%
1:00	🟧	1272	0.479	4.1%
2:00	🟪	1277	0.480	4.1%
3:00	🟥	1255	0.525	4.5%
4:00	🟧	1248	0.382	3.2%
5:00	🟩	1255	0.450	3.8%
6:00	🟪	1260	0.556	4.7%
7:00	⬛	1288	0.556	4.7%
8:00	🟦	1339	0.535	4.5%
9:00	🟪	1508	3.138	26.6%
10:00	🟥	1559	0.908	7.7%
11:00	🟦	1533	0.905	7.7%
12:00	⬛	1523	1.169	9.9%
13:00	🟩	1601	1.037	8.8%
14:00	⬜	179	0.149	1.3%
Total		19391	11.786	100%

Table 142 Bandwidth Summary

LABEL	DESCRIPTION
Chart Type	Select **PIE** or **BAR** chart from the **Chart Type** list box. You can select the default for all screens in the **Report, System, General Config** screen.
Last Days	The report displays information per hour when you select one day and information per day when you select more than one day.
Settings	Click **Settings** to view reports for more days (up to 31 days) than the previous list box allows or for an earlier time range.
Hour (Date)	This field displays the hour the event happened when one day is selected and the date the event happened when more than one day is selected (**Date** replaces **Hour**).
Total	This field displays totals for measurable items in this screen.

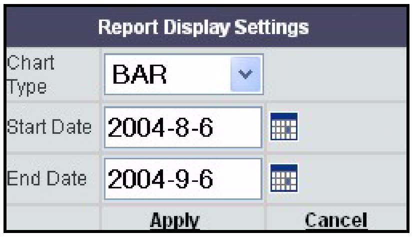
Table 142 Bandwidth Summary (continued)

LABEL	DESCRIPTION
Events	This field displays the number of events that occurred on the selected devices during each hour of the current day or each day for a range of days (up to 31 days).
Color	Use the color field to distinguish parameters in the graph.
MBytes	This field shows the number of megabytes transferred through the selected ZyXEL device(s) in the last hour or day.
% of MBytes	This field shows the percentage of megabytes transferred during this hour, compared to the whole day when one day is selected. It shows the percentage of megabytes transferred during this day, compared to the total number of days selected when more than one day is selected.

24.1.1 Bandwidth Summary Settings

Click **Settings** in the previous screen to display this screen. You only need to do this to view reports for more days (up to 31 days) than the main screen list box allows or for an earlier time range.

Figure 190 Bandwidth Summary Settings



Report Display Settings

Chart Type: BAR

Start Date: 2004-8-6

End Date: 2004-9-6

Table 143 Bandwidth Summary Settings

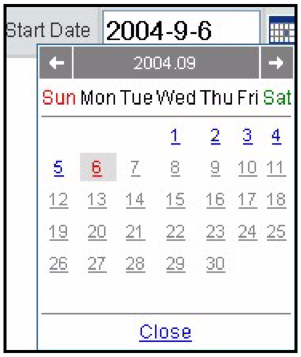
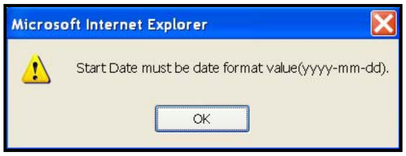
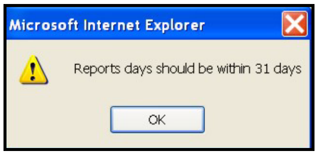
LABEL	DESCRIPTION
Chart Type	Select **PIE** or **BAR** chart from the **Chart Type** list box. You can select the default for all screens in the **Report, System, General Config** screen.
Start Date	Click the calendar icon to select a beginning year-month-date or manually enter the date in year-month-date format.  Start Date 2004-9-6 2004.09 Sun Mon Tue Wed Thu Fri Sat 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 27 28 29 30 Close  Microsoft Internet Explorer Start Date must be date format value(yyyy-mm-dd).

Table 143 Bandwidth Summary Settings (continued)

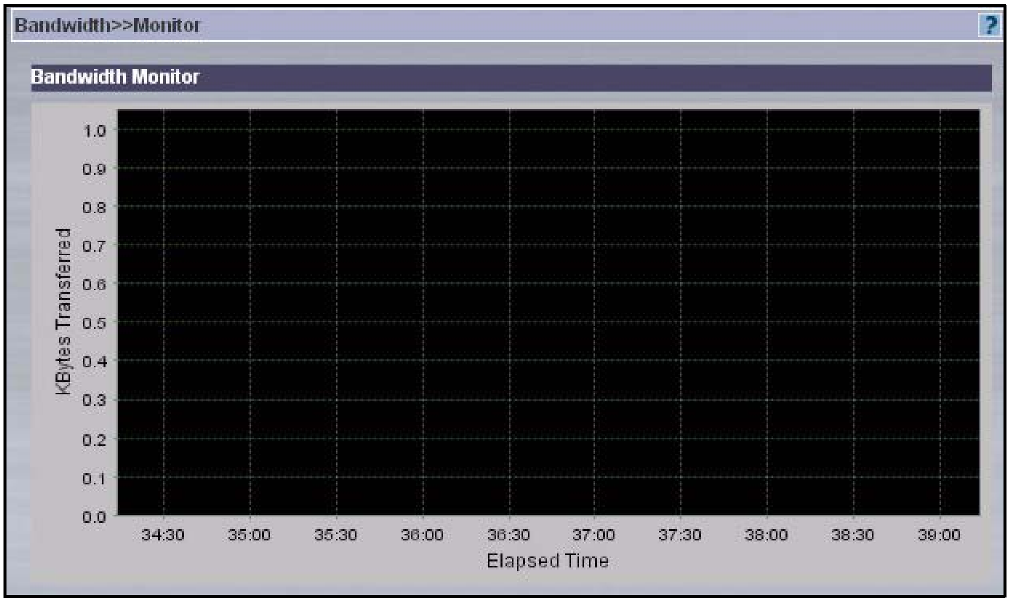
LABEL	DESCRIPTION
End Date	Click the calendar icon to select an ending year-month-date or manually enter the date in year-month-date format. The end date must come after the start date but not after the current date. The total range must not exceed 31 days.  Microsoft Internet Explorer Reports days should be within 31 days
Apply	Click **Apply** to create a report based on the settings you configured in this screen.
Cancel	Click **Cancel** to close this screen without saving your settings.

24.2 Bandwidth Monitoring

The **Bandwidth Monitor** displays bandwidth usage (kilobytes transferred) for the selected ZyXEL device(s) in real time.

To view the **Bandwidth Monitor**, select ZyXEL device(s) and click **Report, Bandwidth, Monitor**.

Figure 191 Bandwidth Monitor

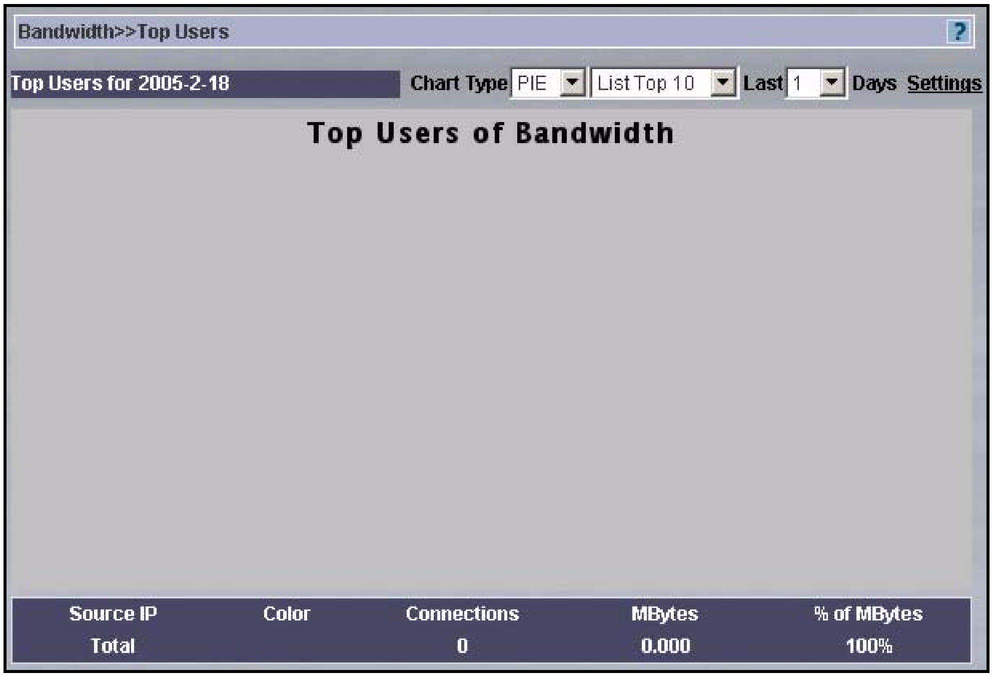


24.3 Bandwidth Top Users

This report displays the users who used the most bandwidth on selected ZyXEL devices(s) over the specified time period. The chart displays the percentage of bandwidth transferred by each user.

To view the **Bandwidth Top Users** report, select ZyXEL device(s) and click **Report, Bandwidth**, **Top Users**.

Figure 192 Bandwidth Top Users



Top Users for 2005-2-18

Chart Type PIE

List Top 10

Last 1 Days

Top Users of Bandwidth

Source IP	Color	Connections	MBytes	% of MBytes
Total		0	0.000	100%

Table 144 Bandwidth Top Users

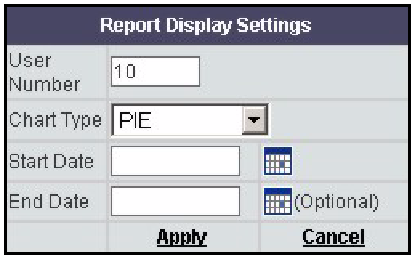
	DESCRIPTION
Chart Type	Select **PIE** or **BAR** chart from the **Chart Type** list box. You can select the default for all screens in the **Report, System, General Config** screen.
List Top 10	Select the number of users for which you want to create this report.
Last Days	The report displays information per hour when you select one day and information per day when you select more than one day.
Settings	Click **Settings** to view reports for more users than the **List Top 10** box allows, to view reports for more days (up to 31 days) than the **Last Days** list box allows or for an earlier time range.
Source IP	This field displays the IP address of the user who consumed this bandwidth on the selected device.
Color	You can color code individual items for better graphical representation.
Connections	This field displays the number of TCP connections that occurred on the selected devices during each hour of the current day or each day for a range of days (up to 31 days).
MBytes	This field shows the number of megabytes transferred through the selected ZyXEL device(s) in the last hour or day.
% of MBytes	This field shows the percentage of megabytes transferred during this hour, compared to the whole day when one day is is selected. It shows the percentage of megabytes transferred during this day, compared to the total number of days selected when more than one day is selected.
Total	This field displays totals for measurable items in this screen.

24.3.1 Bandwidth Top Users Settings

Click **Settings** in the previous screen to display this screen. You only need to do this:

- To view reports for more days (up to 31 days) than the main screen list box allows
- For an earlier time range
- To view the screen for a specific number of users. Enter that number in the **User Number** field.

Figure 193 Bandwidth Top Users Settings



User Number: 10
Chart Type: PIE
Start Date:
End Date: (Optional)

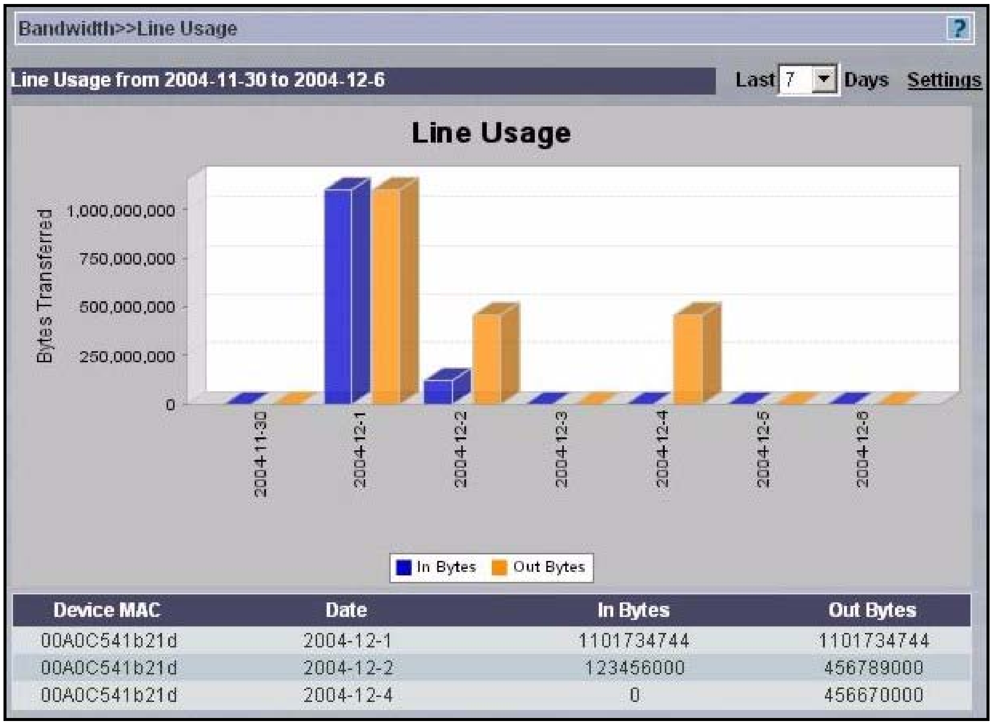
Table 145 Bandwidth Top Users Settings

LABEL	DESCRIPTION
User Number	Select the number of users for which you want to create the report.
Chart Type	Select **PIE** or **BAR** chart from the **Chart Type** list box. You can select the default for all screens in the **Report, System, General Config** screen.
Start Date	Click the calendar icon to select a beginning year-month-date or manually enter the date in year-month-date format.
End Date	The **End Date** selection is optional. Click the calendar icon to select an ending year-month-date or manually enter the date in year-month-date format. The end date must come after the start date but not after the current date. The total range must not exceed 31 days.
Apply	Click **Apply** to create a report based on the settings you configured in this screen.
Cancel	Click **Cancel** to close this screen without saving your settings.

24.4 Bandwidth Line Usage

This report displays the amount of bandwidth transferred to and from ZyXEL devices(s) during the specified day(s). The chart displays the amount of bandwidth transferred by each user, click **Report**, **Bandwidth**, **Line Usage**.

Figure 194 Bandwidth Line Usage



Bandwidth>>Line Usage

Line Usage from 2004-11-30 to 2004-12-6 Last 7 Days Settings

Device MAC	Date	In Bytes	Out Bytes
00A0C541b21d	2004-12-1	1101734744	1101734744
00A0C541b21d	2004-12-2	123456000	456789000
00A0C541b21d	2004-12-4	0	456670000

Table 146 Bandwidth Line Usage

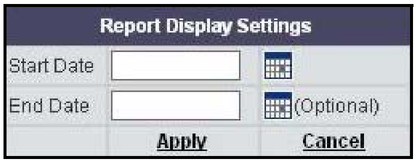
LABEL	DESCRIPTION
Last Days	The report displays information per hour for one day selected and information per day for more than one day selected.
Settings	Click Settings to view reports for more MAC addresses, or for more days (up to 31 days) than the previous list box allows or for an earlier time range.
Device MAC	This field displays the WAN MAC address of the device that caused the ZyXEL device to generate a log.
Date	This field displays the date the ZyXEL device generated the log.
In Bytes	This field shows the number of megabytes transferred through the ADSL connection to the ZyXEL device(s) during this hour when one day is selected or transferred during this day when more than one day is selected.
Out Bytes	This field shows the number of megabytes transferred through the ADSL connection from the ZyXEL device(s) during this hour when one day is selected or transferred during this day when more than one day is selected.

24.4.1 Bandwidth Line Usage Settings

Click **Settings** in the previous screen to display this screen. You only need to do this:

- To view reports for more days (up to 31 days) than the main screen list box allows for an earlier time range

Figure 195 Bandwidth Line Usage Settings



Report Display Settings

Start Date

End Date (Optional)

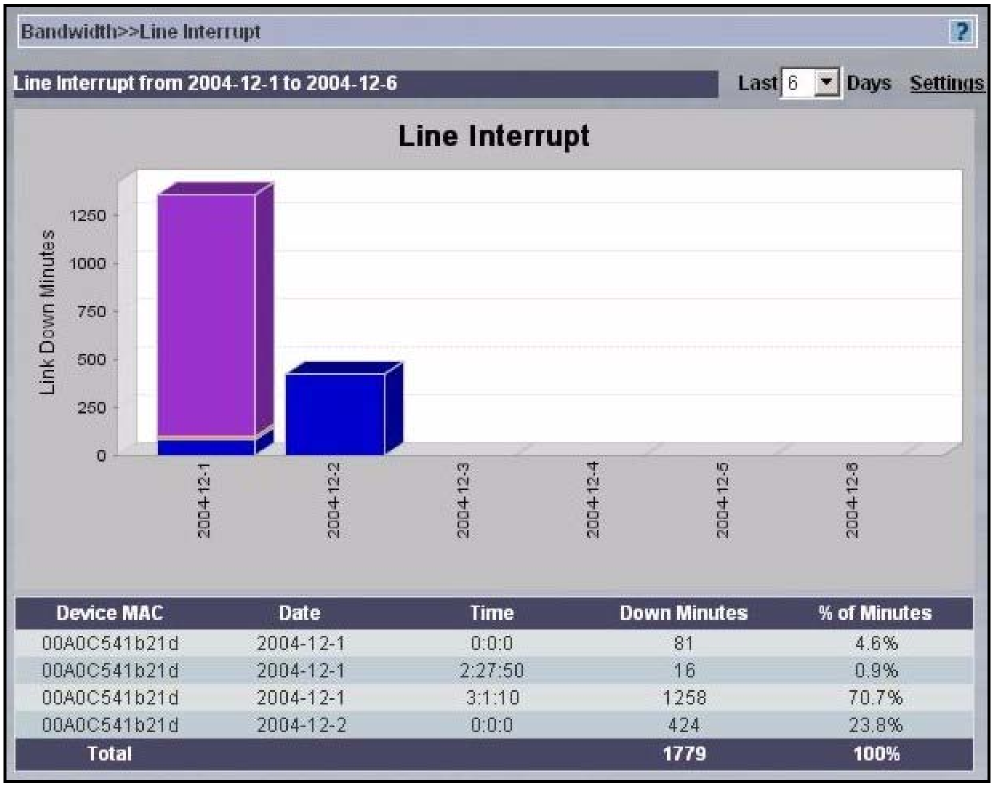
Table 147 Bandwidth Line Usage Settings

LABEL	DESCRIPTION
Start Date	Click the calendar icon to select a beginning year-month-date or manually enter the date in year-month-date format.
End Date	The **End Date** selection is optional. Click the calendar icon to select an ending year-month-date or manually enter the date in year-month-date format. The end date must come after the start date but not after the current date. The total range must not exceed 31 days.
Apply	Click **Apply** to create a report based on the settings you configured in this screen.
Cancel	Click **Cancel** to close this screen without saving your settings.

24.5 Bandwidth Line Interrupt

This report displays the time in minutes the ADSL link went down for ZyXEL device(s) during the specified day(s). The chart displays the number of minutes of down time for each time the connection went down, click **Report**, **Bandwidth**, **Line Interrupt**.

Figure 196 Bandwidth Line Interrupt



Device MAC	Date	Time	Down Minutes	% of Minutes
00A0C541b21d	2004-12-1	0:0:0	81	4.6%
00A0C541b21d	2004-12-1	2:27:50	16	0.9%
00A0C541b21d	2004-12-1	3:1:10	1258	70.7%
00A0C541b21d	2004-12-2	0:0:0	424	23.8%
Total			1779	100%

Table 148 Bandwidth Line Interrupt

LABEL	DESCRIPTION
Last Days	The report displays information per hour for one day selected and information per day for more than one day selected.
Settings	Click **Settings** to view reports for more MAC addresses, or for more days (up to 31 days) than the previous list box allows or for an earlier time range.
Device MAC	This field displays the WAN MAC address of the device that caused the ZyXEL device to generate a log.
Date	This field displays the date the ZyXEL device generated the log.
Time	This field displays the time the ADSL connection went down.
Down Minutes	This field shows the number of minutes that the ADSL connection to the ZyXEL device(s) was down.
% of Minute	This field shows the percentage of ADSL interruption time for a ZyXEL device.

24.5.1 Bandwidth Line Interrupt Settings

Click **Settings** in the previous screen to display this screen. You only need to do this:

- To view reports for more days (up to 31 days) than the main screen list box allows for an earlier time range

Figure 197 Bandwidth Line Interrupt Settings

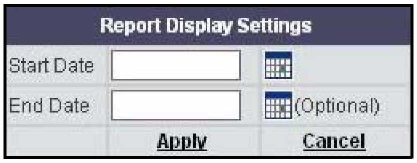


Table 149 Bandwidth Line Interrupt Settings

LABEL	DESCRIPTION
Start Date	Click the calendar icon to select a beginning year-month-date or manually enter the date in year-month-date format.
End Date	The **End Date** selection is optional. Click the calendar icon to select an ending year-month-date or manually enter the date in year-month-date format. The end date must come after the start date but not after the current date. The total range must not exceed 31 days.
Apply	Click **Apply** to create a report based on the settings you configured in this screen.
Cancel	Click **Cancel** to close this screen without saving your settings.

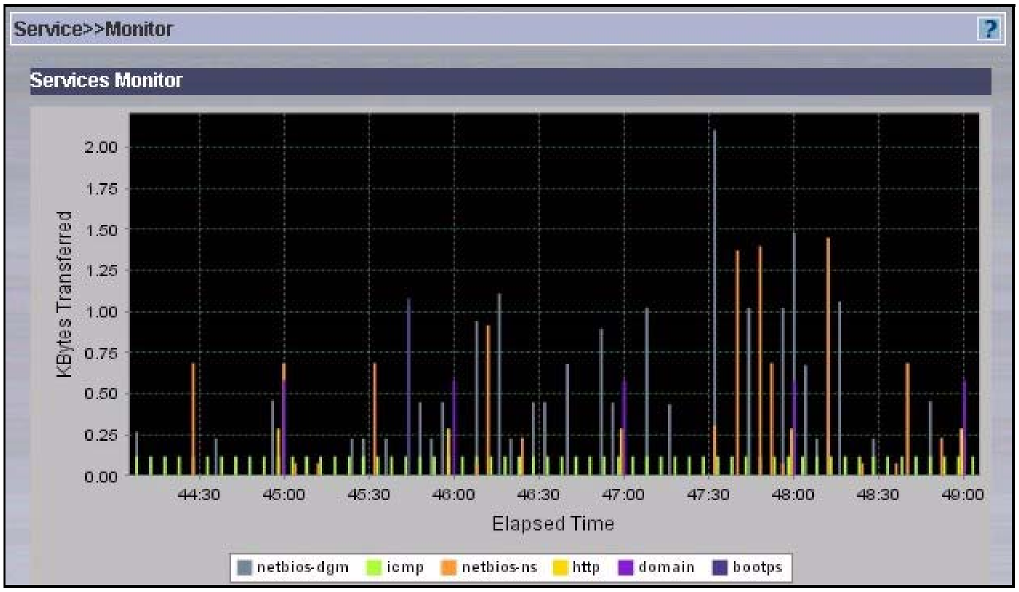
CHAPTER 25 Service Reports

25.1 Service Monitor

The **Service Monitor** displays service usage (kilobytes transferred) for the selected ZyXEL device(s) within the sampling period. To change the sampling period, go to **Report, System, General Config**.

To view the **Service Monitor** select a ZyXEL device(s) and then click **Report, Service, Monitor**.

Figure 198 Service Monitor

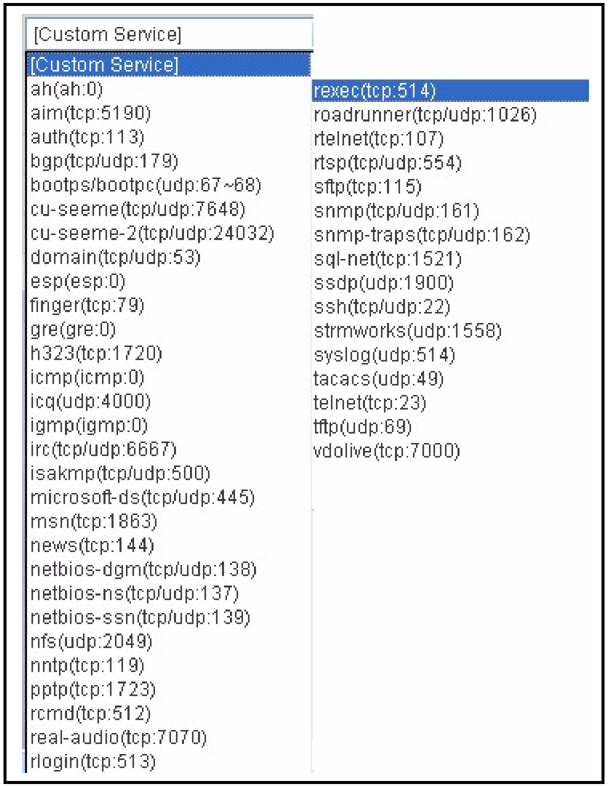


25.2 Pre-defined and Custom Services

This page list all pre-defined services and allows you to create (or delete) custom services.

The pre-defined services (at the time of writing) are shown in the following figure.

Figure 199 Pre-defined Services



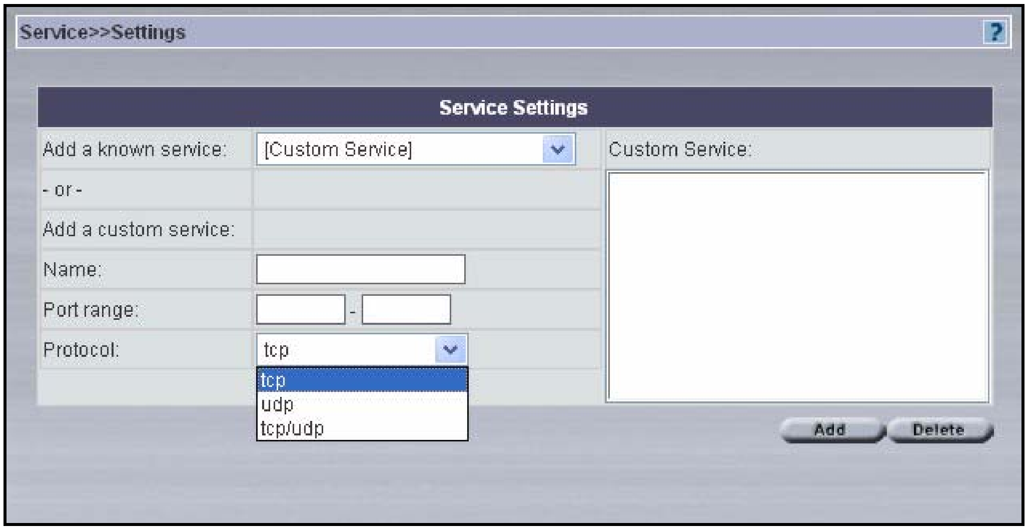
25.2.1 Creating a Custom Service

To create a custom service, select **Custom Service** from the **Add a known service** field and then fill in the **Add a custom service** fields.

25.3 Configuring Service Settings

To view **Service Settings** select a ZyXEL device(s) and then click **Report, Service**, **Settings**.

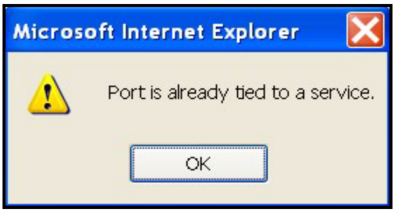
Figure 200 Service Settings



Add a known service: [Custom Service]

Protocol: tcp

Table 150 Service Settings

LABEL	DESCRIPTION
Add a known service	Select a pre-defined service from the drop-down list box or select **Custom Service** and then fill in the **Add a custom service** fields to create a custom service.
Add a custom service	Fill in the following fields to specify a TCP/UDP service that is not pre-defined.
Name	Enter a unique name to identify this service.
Port range	Enter a port range (start port to end port in ascending order) that is not already in use to define your service. Enter the same start and end port if the service is defined by one port. If you select a port range already in use, you see the following screen.  Microsoft Internet Explorer Port is already tied to a service. OK
	Select from **tcp**, **udp** or **tcp/udp** to define your service.
Custom service	This text box lists all pre-defined and custom services. These are the services that then display in the **Service Monitor** screen. You can edit a custom port by selecting it here and then modifying the **Port range** and **Protocol** fields. You cannot edit a pre-defined service.
Add	Click either a pre-defined service or create a custom port and then click this button to add it to the “Custom service” list box.
Delete	Click a service in the “Custom service” list box and then click this button to remove it. If you remove a custom port, you will have to recreate it later if you need it again.

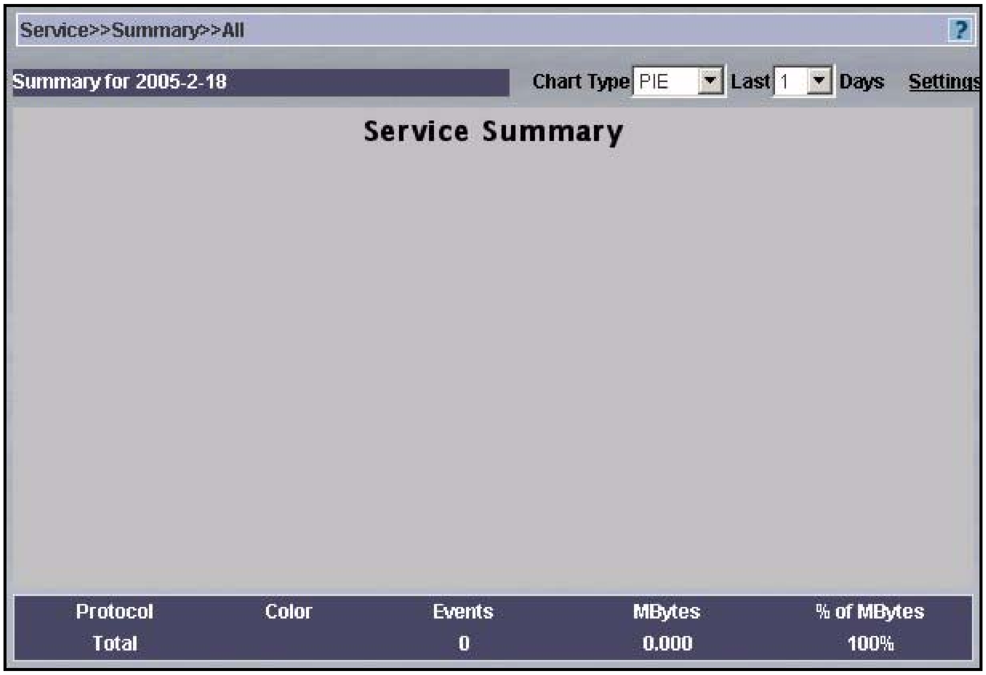
25.4 Service Summary Screens

Use these screens to view bandwidth consumed by a service(s), through a ZyXEL device(s) during the specified time.

25.4.1 All Services Summary

To view the amount of traffic handled by selected ZyXEL device(s), consumed by services defined in the **Service, Settings** screen, click **Report, Service**, **Summary, All**.

Figure 201 All Services Summary



Service>>Summary>>All

Summary for 2005-2-18

Chart Type: PIE, Last: 1 Days

Protocol	Color	Events	MBytes	% of MBytes
Total		0	0.000	100%

Table 151 All Services Summary

LABEL	DESCRIPTION
Chart Type	Select **PIE** or **BAR** chart from the **Chart Type** list box. You can select the default for all screens in the **Report, System, General Config** screen.
Last Days	The report displays information per hour when you select one day and information per day when you select more than one day.
Settings	Click **Settings** to view reports for more days (up to 31 days) than the previous list box allows or for an earlier time range.
Protocol	This field displays the protocol(s) that define the service.
Total	This field displays totals for measurable items in this screen.
Color	You can color code individual items for better graphical representation.
Events	This field displays the number of events or "hits."

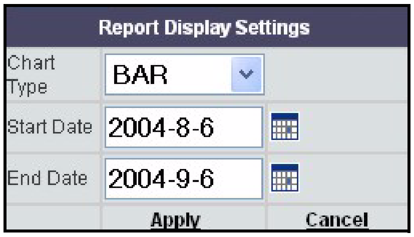
Table 151 All Services Summary (continued)

LABEL	DESCRIPTION
MBytes	This field displays the number of megabytes consumed by the service(s).through the selected ZyXEL device(s) in the last hour or day.
% of MBytes	This field shows the percentage of megabytes consumed by the service(s) during this hour, compared to the whole day when one day is is selected. It shows the percentage of megabytes consumed by the service(s) during this day, compared to the total number of days selected when more than one day is selected.

25.4.2 Service Summary Settings

Click **Settings** from a service summary screen, to view reports for an earlier time range or for more days (up to 31 days) than the previous list box allows.

Figure 202 Services Summary Settings



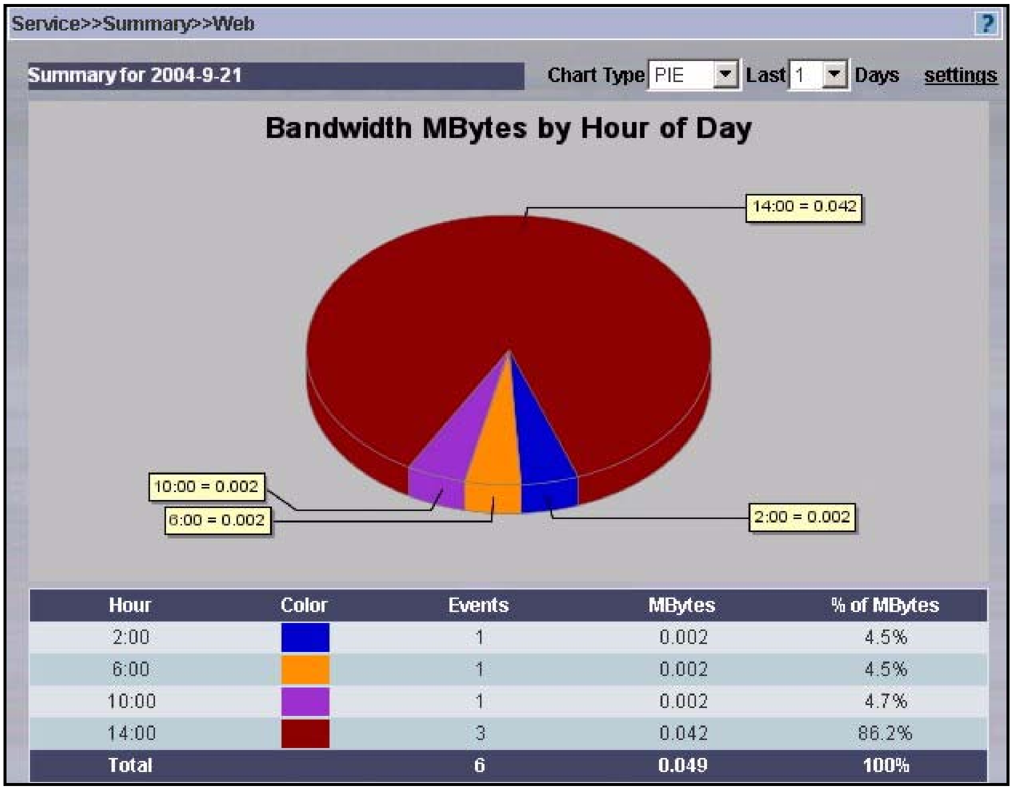
Report Display Settings

Chart Type	BAR
Start Date	2004-8-6
End Date	2004-9-6

25.4.3 Web Services Summary

To view the amount of web traffic handled by selected ZyXEL device(s), during the selected time, select a ZyXEL device(s) and then click **Report, Service**, **Summary, Web**.

Figure 203 Web Services Summary



Service>>Summary>>Web

Summary for 2004-9-21 Chart Type PIE Last 1 Days settings

Bandwidth MBytes by Hour of Day

Hour	Color	Events	MBytes	% of MBytes
2:00	🟦	1	0.002	4.5%
6:00	🟧	1	0.002	4.5%
10:00	🟪	1	0.002	4.7%
14:00	🟥	3	0.042	86.2%
Total		6	0.049	100%

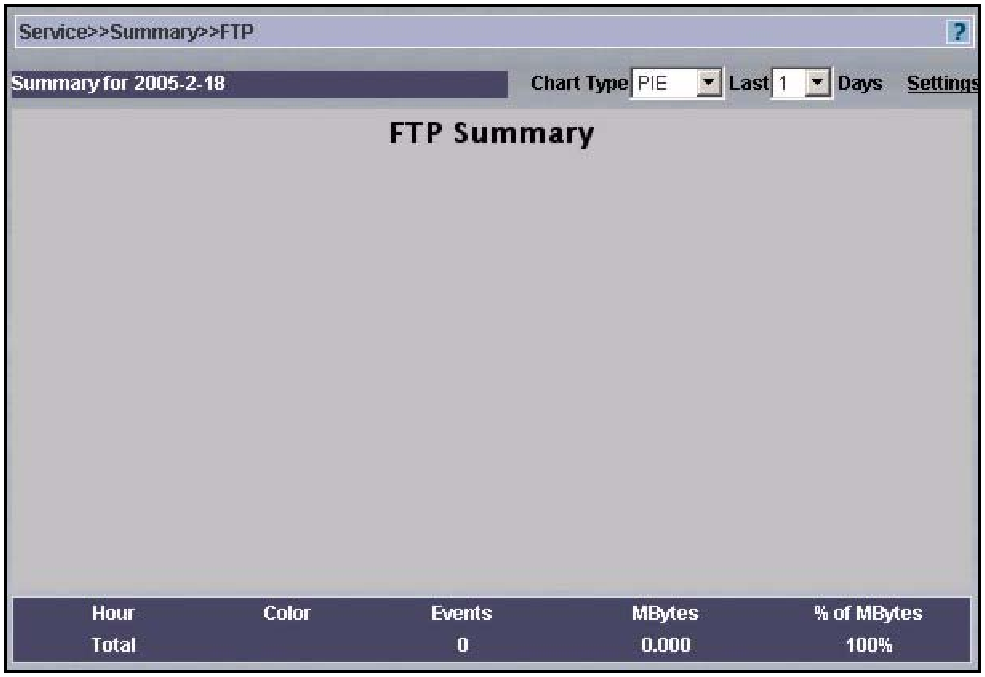
Table 152 Web Services Summary

LABEL	DESCRIPTION
Chart Type	Select **PIE** or **BAR** chart from the **Chart Type** list box. You can select the default for all screens in the **Report, System, General Config** screen.
Last Days	The report displays information per hour when you select one day and information per day when you select more than one day.
Settings	Click **Settings** to view reports for more days (up to 31 days) than the previous list box allows or for an earlier time range.
Hour (Date)	This field displays the hour the event happened when one day is selected and the date the event happened when more than one day is selected (**Date** replaces **Hour**).
Total	This field displays totals for measurable items in this screen.
Color	You can color code individual items for better graphical representation.
Events	This field displays the number of events or "hits."
MBytes	This field displays the number of megabytes consumed by web services through the selected ZyXEL device(s) in the last hour or day.
% of MBytes	This field shows the percentage of megabytes consumed by web services during this hour, compared to the whole day when one day is is selected. It shows the percentage of megabytes consumed by the service(s) during this day, compared to the total number of days selected when more than one day is selected.

25.4.4 FTP Services Summary

To view the amount of FTP traffic handled by selected ZyXEL device(s), during the specified time, select a ZyXEL device(s) and then click **Report, Service**, **Summary, FTP**.

Figure 204 FTP Services Summary



Hour	Color	Events	MBytes	% of MBytes
Total		0	0.000	100%

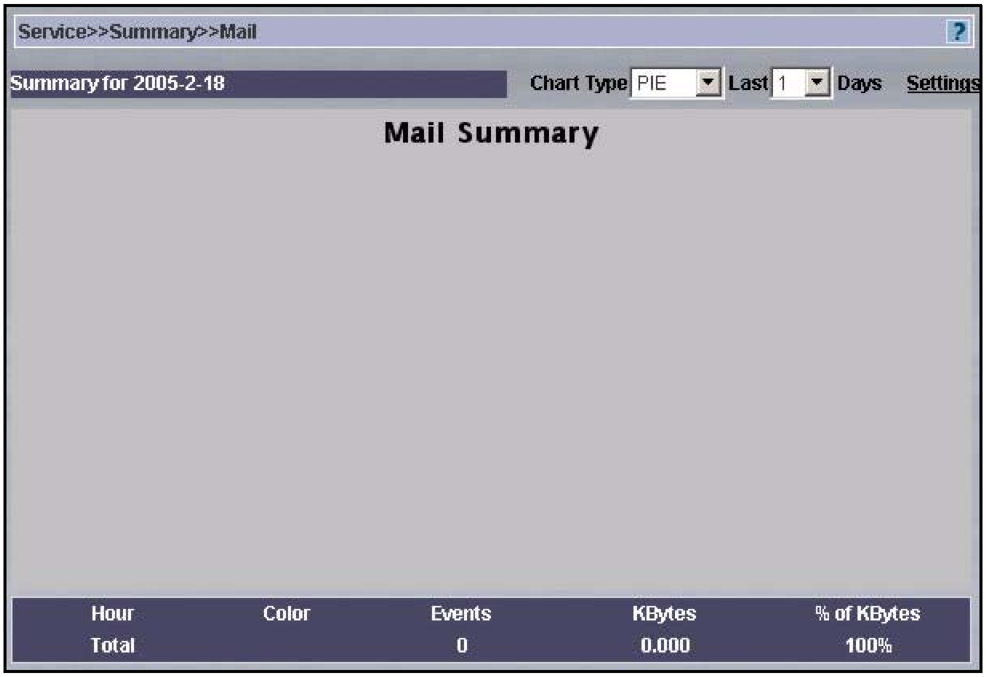
Table 153 FTP Services Summary

LABEL	DESCRIPTION
Chart Type	Select **PIE** or **BAR** chart from the **Chart Type** list box. You can select the default for all screens in the **Report, System, General Config** screen.
Last Days	The report displays information per hour when you select one day and information per day when you select more than one day.
Settings	Click **Settings** to view reports for more days (up to 31 days) than the previous list box allows or for an earlier time range.
Hour (Date)	This field displays the hour the event happened when one day is selected and the date the event happened when more than one day is selected (**Date** replaces **Hour**).
Color	You can color code individual items for better graphical representation.
Events	This field displays the number of events or "hits."
MBytes	This field displays the number of megabytes consumed by FTP services through the selected ZyXEL device(s) in the last hour or day.
% of MBytes	This field shows the percentage of megabytes consumed by FTP services during this hour, compared to the whole day when one day is is selected. It shows the percentage of megabytes consumed by the service(s) during this day, compared to the total number of days selected when more than one day is selected.
Total	This field displays totals for measurable items in this screen.

25.4.5 Mail Services Summary

To view the amount of mail traffic handled by selected ZyXEL device(s), during the specified time, select a ZyXEL device(s) and then click **Report, Service**, **Summary, Mail**.

Figure 205 Mail Services Summary



Service>>Summary>>Mail

Summary for 2005-2-18 Chart Type PIE Last 1 Days Settings

Mail Summary

Hour	Color	Events	KBytes	% of KBytes
Total		0	0.000	100%

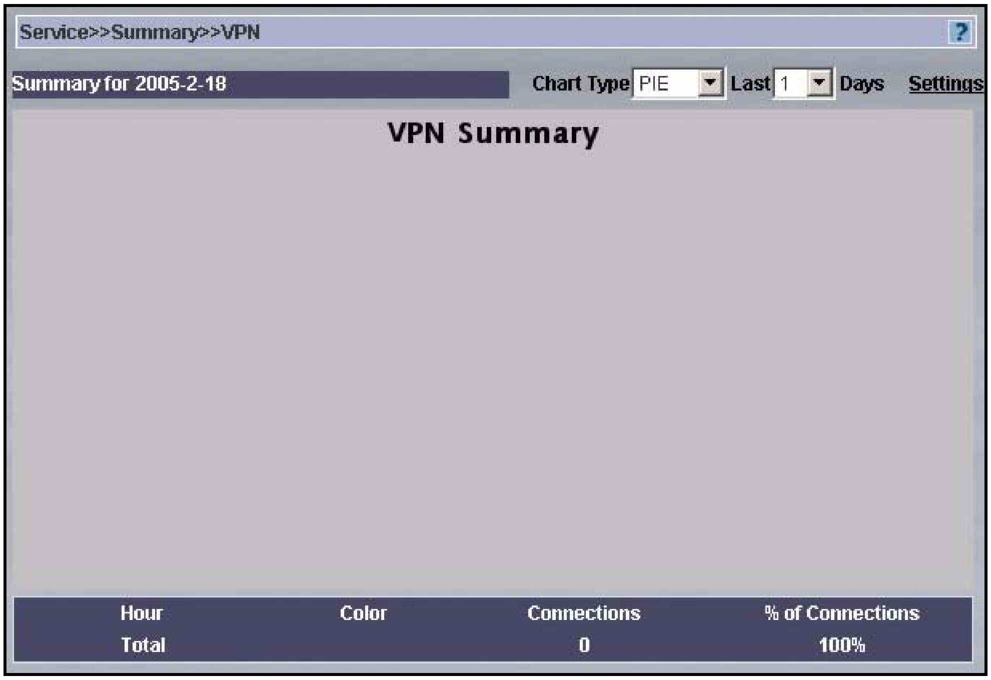
Table 154 Mail Services Summary

LABEL	DESCRIPTION
Chart Type	Select **PIE** or **BAR** chart from the **Chart Type** list box. You can select the default for all screens in the **Report, System, General Config** screen.
Last Days	The report displays information per hour when you select one day and information per day when you select more than one day.
Settings	Click **Settings** to view reports for more days (up to 31 days) than the previous list box allows or for an earlier time range.
Hour (Date)	This field displays the hour the event happened when one day is selected and the date the event happened when more than one day is selected (**Date** replaces **Hour**).
Color	You can color code individual items for better graphical representation.
Events	This field displays the number of events or "hits."
KBytes	This field displays the number of kilobytes consumed by mail services through the selected ZyXEL device(s) in the last hour or day.
% of KBytes	This field shows the percentage of kilobytes consumed by mail services during this hour, compared to the whole day when one day is is selected. It shows the percentage of kilobytes consumed by the service(s) during this day, compared to the total number of days selected when more than one day is selected.
Total	This field displays totals for measurable items in this screen.

25.4.6 VPN Services Summary

To view the amount of VPN traffic handled by selected ZyXEL device(s), during the specified time, select a ZyXEL device(s) and then click **Report, Service**, **Summary, VPN**.

Figure 206 VPN Services Summary



Summary for 2005-2-18

Hour	Color	Connections	% of Connections
Total		0	100%

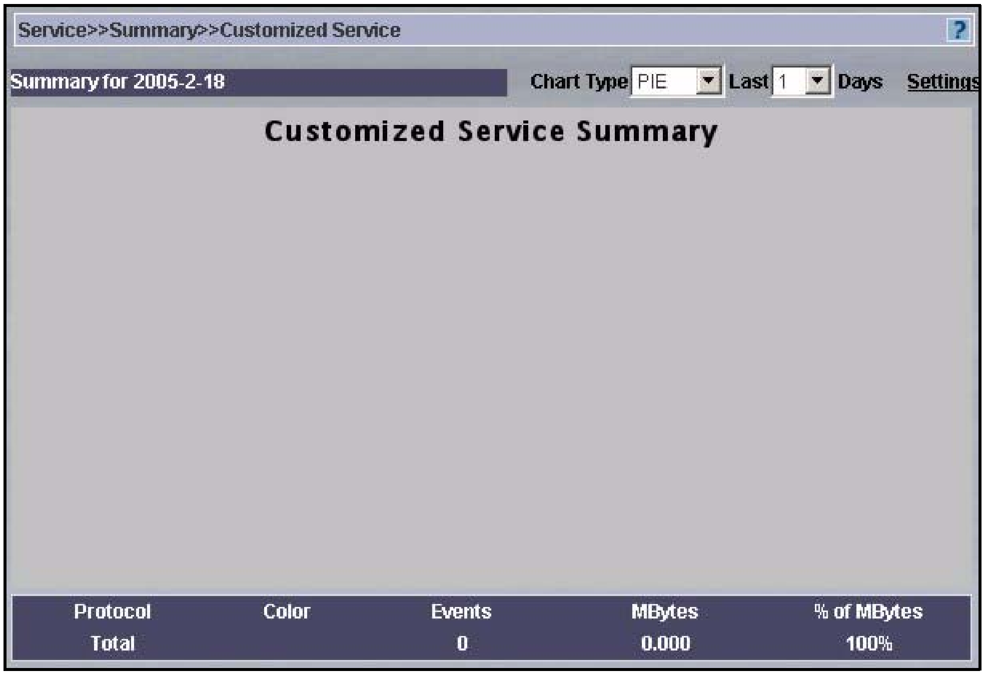
Table 155 VPN Services Summary

LABEL	DESCRIPTION
Chart Type	Select **PIE** or **BAR** chart from the **Chart Type** list box. You can select the default for all screens in the **Report, System, General Config** screen.
Last Days	The report displays information per hour when you select one day and information per day when you select more than one day.
Settings	Click **Settings** to view reports for more days (up to 31 days) than the previous list box allows or for an earlier time range.
Hour (Date)	This field displays the hour the event happened when one day is selected and the date the event happened when more than one day is selected (**Date** replaces **Hour**).
Color	You can color code individual items for better graphical representation.
Connections	This field displays the number of VPN connections.
% of Connections	This field shows the percentage of connections in use during this hour, compared to the whole day when one day is is selected. It shows the percentage of connections in use during this day, compared to the total number of days selected when more than one day is selected.
Total	This field displays totals for measurable items in this screen.

25.4.7 Custom Services Summary

To view the amount of custom traffic defined in the **Service, Settings** screen, handled by selected ZyXEL device(s), during the specified time, select a ZyXEL device(s) and then click **Report, Service**, **Summary, Customized Service Group**.

Figure 207 Custom Service Group



Service>>Summary>>Customized Service
?
Summary for 2005-2-18
Chart Type PIE
Last 1
Days
Settings
Customized Service Summary

Protocol	Color	Events	MBytes	% of MBytes
Total		0	0.000	100%

Table 156 Custom Service Group

LABEL	DESCRIPTION
Chart Type	Select **PIE** or **BAR** chart from the **Chart Type** list box. You can select the default for all screens in the **Report, System, General Config** screen.
Last Days	The report displays information per hour when you select one day and information per day when you select more than one day.
Settings	Click **Settings** to view reports for more days (up to 31 days) than the previous list box allows or for an earlier time range.
Protocol	This field displays the service (defined by port protocol) that consumed bandwidth via the selected ZyXEL devices.
Color	You can color code individual items for better graphical representation.
Events	This field displays the number of events or "hits."
MBytes	This field displays the number of megabytes consumed by custom services defined in the **Service, Settings** screen through the selected ZyXEL device(s) in the last hour or day.
% of MBytes	This field shows the percentage of megabytes consumed by custom services defined in the **Service, Settings** screen during this hour, compared to the whole day when one day is is selected. It shows the percentage of megabytes consumed by the service(s) during this day, compared to the total number of days selected when more than one day is selected.
Total	This field displays totals for measurable items in this screen.

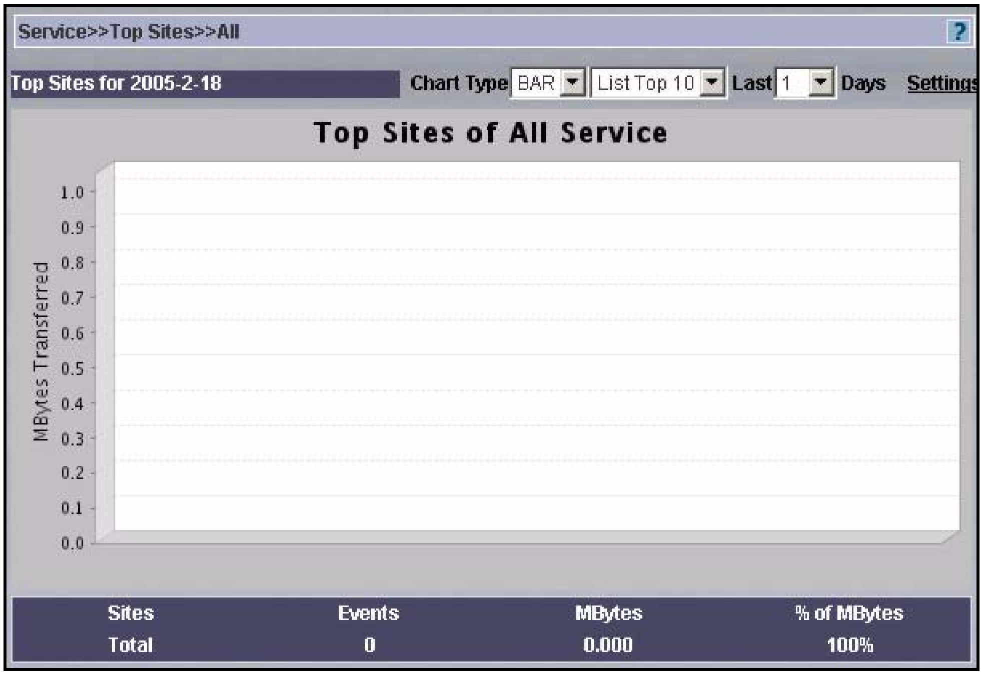
25.5 Service Top Sites

Use these screens to view web sites visited when using a service(s), through a ZyXEL device(s) during the specified time.

25.5.1 All Services Top Sites

To view web sites visited when using all services defined in the **Service, Settings** screen, during the specified time, select a ZyXEL device(s) and then click **Report, Service**, **Top Sites, All**.

Figure 208 Top Sites for All Services



Sites	Events	MBytes	% of MBytes
Total	0	0.000	100%

Table 157 Top Sites for All Services

LABEL	DESCRIPTION
Chart Type	Select **PIE** or **BAR** chart from the **Chart Type** list box. You can select the default for all screens in the **Report, System, General Config** screen.
List Top 10	Select the number of sites to view from the drop-down list box
Last Days	The report displays information per hour when you select one day and information per day when you select more than one day.
Settings	Click **Settings** to view reports for more sites visited, or for days (up to 31 days) than the previous list box allows or for an earlier time range.
Sites	This field displays the URL or IP address of the site visited.
Events	This field displays the number of events or "hits."
MBytes	This field displays the number of megabytes consumed by the service(s) through the selected ZyXEL device(s) in the last hour or day.

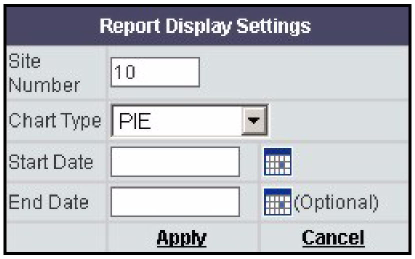
Table 157 Top Sites for All Services (continued)

LABEL	DESCRIPTION
% of MBytes	This field shows the percentage of megabytes consumed by the service(s) during this hour, compared to the whole day when one day is is selected. It shows the percentage of megabytes consumed by the service(s) during this day, compared to the total number of days selected when more than one day is selected.
Total	This field displays totals for measurable items in this screen.

25.5.2 Top Site Service Settings

Click **Settings** in the previous screen to view reports for more sites visited, or for days (up to 31 days) than the previous list box allows or for an earlier time range.

Figure 209 Top Site Service Settings



Report Display Settings

Site Number	10
Chart Type	PIE
Start Date	
End Date	(Optional)

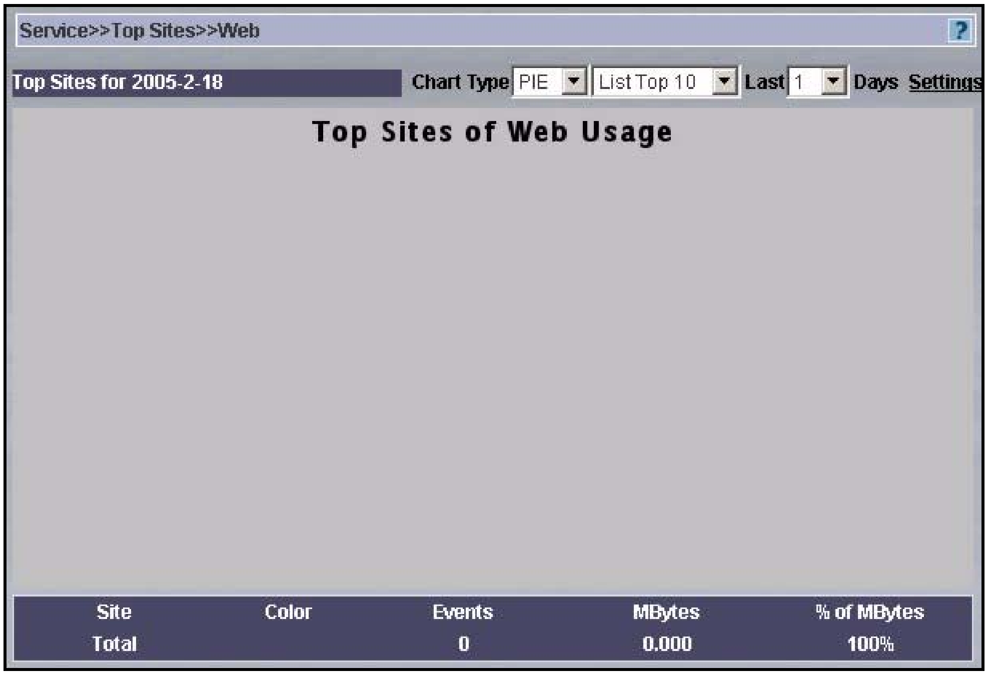
Table 158 Top Site Service Settings

LABEL	DESCRIPTION
Site Number	Type the number of sites you'd like to view here.
Chart Type	Select **PIE** or **BAR** chart from the **Chart Type** list box. You can select the default for all screens in the **Report, System, General Config** screen.
Start Date	Click the calendar icon to select a beginning year-month-date or manually enter the date in year-month-date format.
End Date	The **End Date** selection is optional. Click the calendar icon to select an ending year-month-date or manually enter the date in year-month-date format. The end date must come after the start date but not after the current date. The total range must not exceed 31 days.
Apply	Click **Apply** to create a report based on the settings you configured in this screen.
Cancel	Click **Cancel** to close this screen without saving your settings.

25.5.3 Web Service Top Sites

To view web sites visited when using web services through selected ZyXEL device(s), during the specified time, select a ZyXEL device(s) and then click **Report, Service**, **Top Sites, Web**.

Figure 210 Web Service Top Sites



Service>>Top Sites>>Web

Top Sites for 2005-2-18

Chart Type PIE List Top 10 Last 1 Days Settings

Top Sites of Web Usage

Site	Color	Events	MBytes	% of MBytes
Total		0	0.000	100%

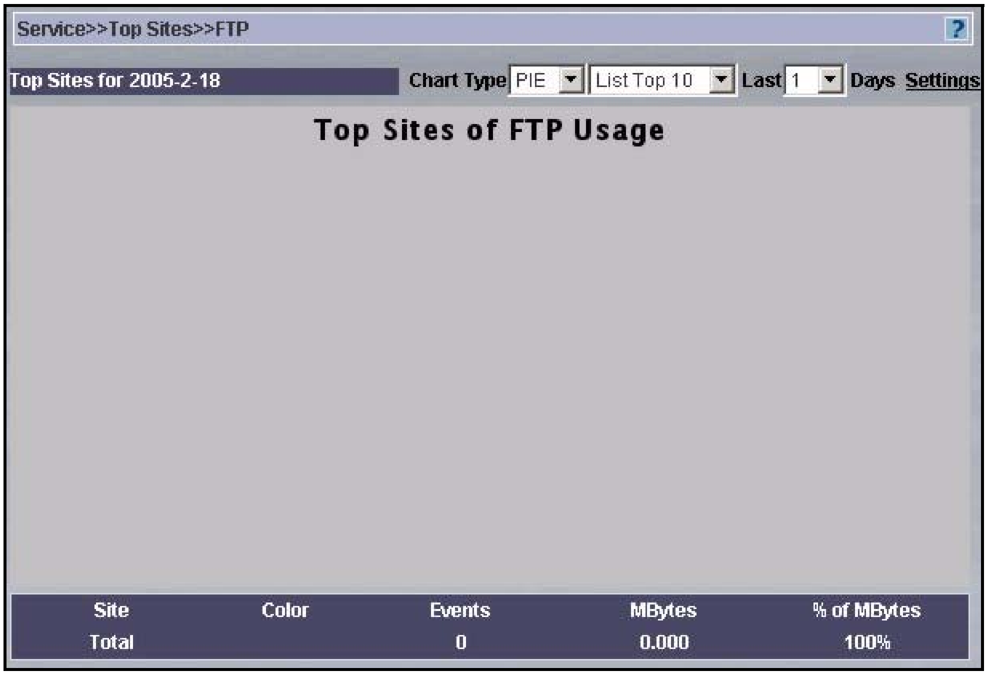
Table 159 Web Service Top Sites

LABEL	DESCRIPTION
Chart Type	Select **PIE** or **BAR** chart from the **Chart Type** list box. You can select the default for all screens in the **Report, System, General Config** screen.
List Top 10	Select the number of sites to view from the drop-down list box
Last Days	The report displays information per hour when you select one day and information per day when you select more than one day.
Settings	Click **Settings** to view reports for more sites visited, or for days (up to 31 days) than the previous list box allows or for an earlier time range.
Site	This field displays the URL or IP address of the site visited.
Color	You can color code individual items for better graphical representation.
Events	This field displays the number of events or "hits."
MBytes	This field displays the number of megabytes consumed by the web service through the selected ZyXEL device(s) in the last hour or day.
% of MBytes	This field shows the percentage of megabytes consumed by the web service during this hour, compared to the whole day when one day is is selected. It shows the percentage of megabytes consumed by the service(s) during this day, compared to the total number of days selected when more than one day is selected.
Total	This field displays totals for measurable items in this screen.

25.5.4 FTP Service Top Sites

To view sites visited when using FTP services through selected ZyXEL device(s), during the specified time, select a ZyXEL device(s) and then click **Report, Service**, **Top Sites, FTP**.

Figure 211   FTP Service Top Sites



Service>>Top Sites>>FTP

Top Sites for 2005-2-18

Chart Type PIE ▼ List Top 10 ▼ Last 1 ▼ Days Settings

Top Sites of FTP Usage

Site	Color	Events	MBytes	% of MBytes
Total		0	0.000	100%

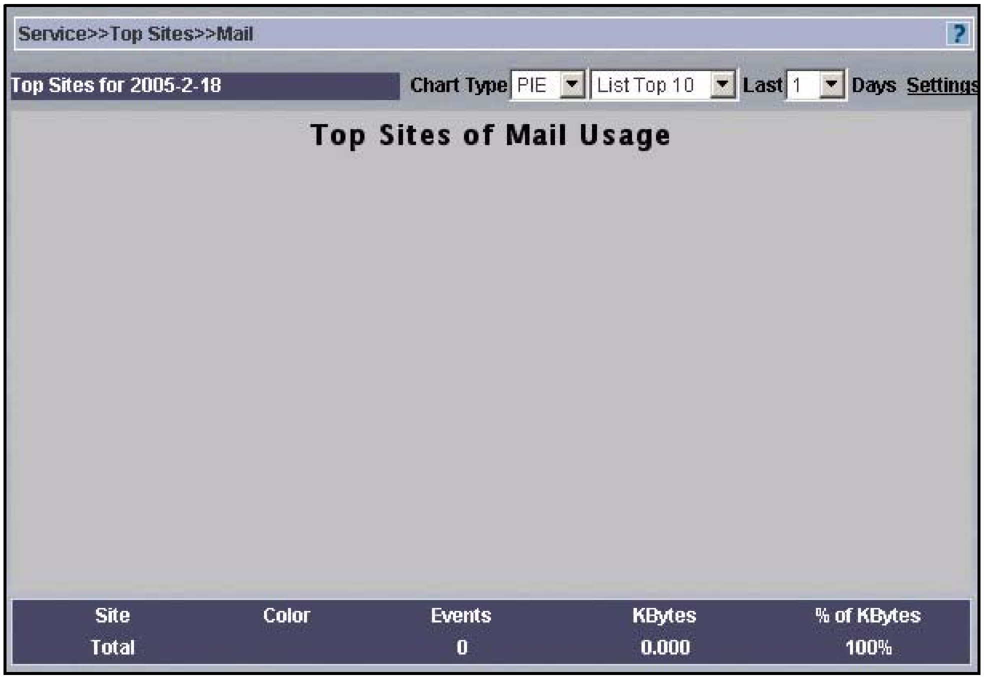
Table 160   FTP Service Top Sites

	DESCRIPTION
Chart Type	Select **PIE** or **BAR** chart from the **Chart Type** list box. You can select the default for all screens in the **Report, System, General Config** screen.
List Top 10	Select the number of sites to view from the drop-down list box
Last Days	The report displays information per hour when you select one day and information per day when you select more than one day.
Settings	Click **Settings** to view reports for more sites visited, or for days (up to 31 days) than the previous list box allows or for an earlier time range.
Site	This field displays the URL or IP address of the site visited.
Color	You can color code individual items for better graphical representation.
Events	This field displays the number of events or "hits."
MBytes	This field displays the number of megabytes consumed by the FTP service through the selected ZyXEL device(s) in the last hour or day.
% of MBytes	This field shows the percentage of megabytes consumed by the FTP service during this hour, compared to the whole day when one day is is selected. It shows the percentage of megabytes consumed by the service(s) during this day, compared to the total number of days selected when more than one day is selected.
Total	This field displays totals for measurable items in this screen.

25.5.5 Mail Service Top Sites

To view sites visited when using mail services through selected ZyXEL device(s), during the specified time, select a ZyXEL device(s) and then click **Report, Service**, **Top Sites, Mail**.

Figure 212 Mail Service Top Sites



Service>>Top Sites>>Mail

Top Sites for 2005-2-18 Chart Type PIE List Top 10 Last 1 Days Settings

Top Sites of Mail Usage

Site	Color	Events	KBytes	% of KBytes
Total		0	0.000	100%

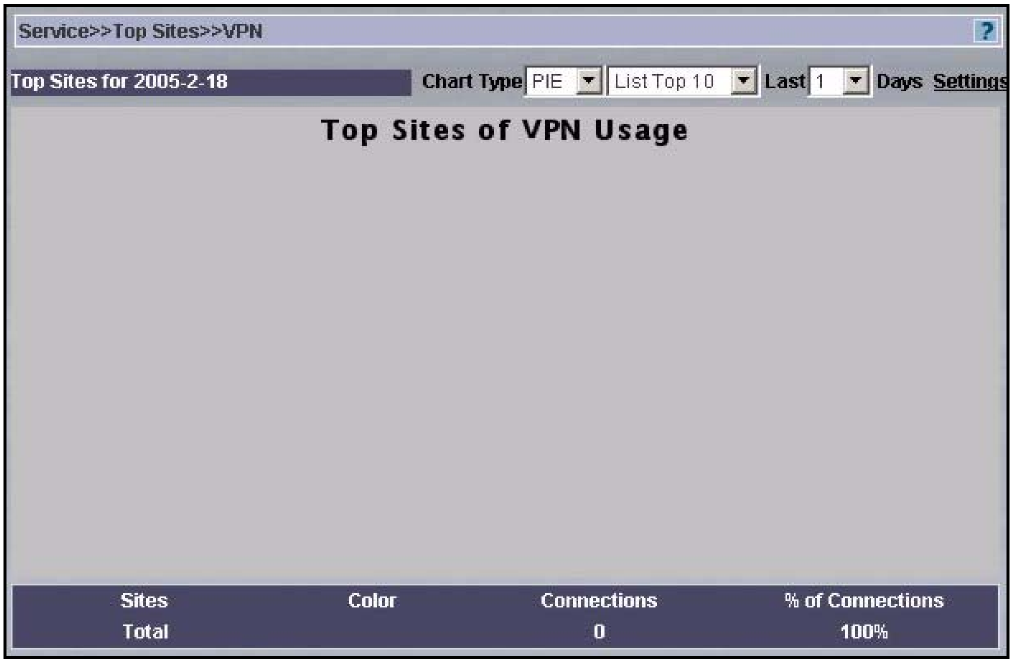
Table 161 Mail Service Top Sites

LABEL	DESCRIPTION
Chart Type	Select **PIE** or **BAR** chart from the **Chart Type** list box. You can select the default for all screens in the **Report, System, General Config** screen.
List Top 10	Select the number of sites to view from the drop-down list box
Last Days	The report displays information per hour when you select one day and information per day when you select more than one day.
Settings	Click **Settings** to view reports for more sites visited, or for days (up to 31 days) than the previous list box allows or for an earlier time range.
Site	This field displays the URL or IP address of the site visited.
Color	You can color code individual items for better graphical representation.
Events	This field displays the number of events or "hits."
KBytes	This field displays the number of kilobytes consumed by the mail service through the selected ZyXEL device(s) in the last hour or day.
% of KBytes	This field shows the percentage of kilobytes consumed by the mail service during this hour, compared to the whole day when one day is is selected. It shows the percentage of kilobytes consumed by the service(s) during this day, compared to the total number of days selected when more than one day is selected.
Total	This field displays totals for measurable items in this screen.

25.5.6 VPN Traffic Top Sites

To view sites visited via VPN tunnels through selected ZyXEL device(s), during the specified time, select a ZyXEL device(s) and then click **Report, Service**, **Top Sites, VPN**.

Figure 213 VPN Service Top Sites



Sites	Color	Connections	% of Connections
Total		0	100%

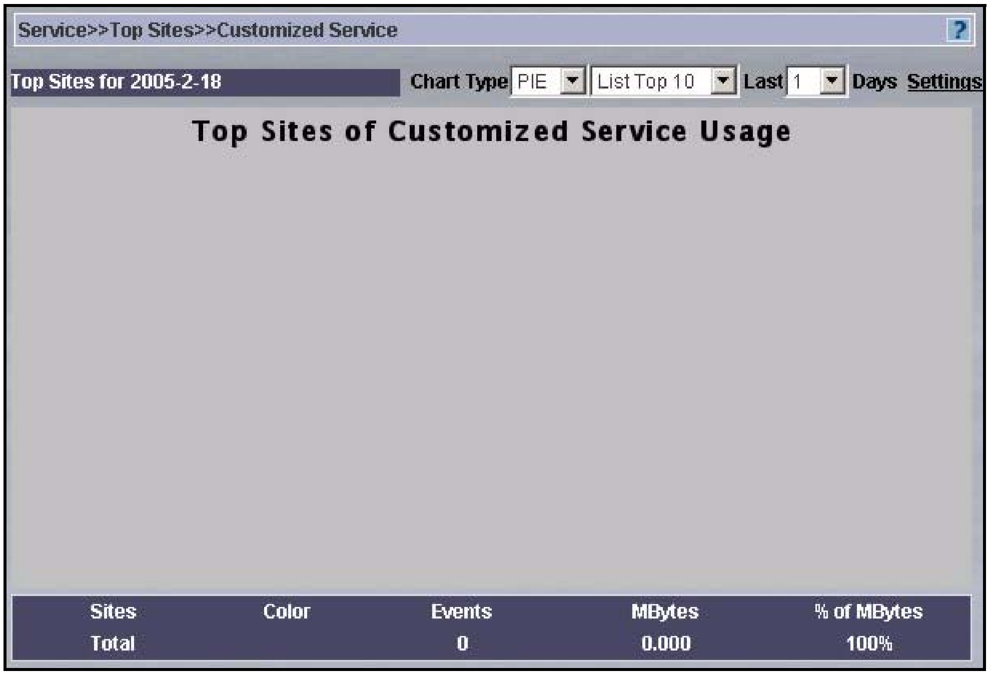
Table 162 VPN Service Top Sites

LABEL	DESCRIPTION
Chart Type	Select **PIE** or **BAR** chart from the **Chart Type** list box. You can select the default for all screens in the **Report, System, General Config** screen.
List Top 10	Select the number of sites to view from the drop-down list box
Last Days	The report displays information per hour when you select one day and information per day when you select more than one day.
Settings	Click **Settings** to view reports for more sites visited, or for days (up to 31 days) than the previous list box allows or for an earlier time range.
Sites	This field displays the destination IP address of the VPN tunnel through the selected ZyXEL devices.
Color	You can color code individual items for better graphical representation.
Connections	This field displays the number of VPN connections through the selected ZyXEL device(s).
% of Connections	This field shows the percentage of connections in use during this hour, compared to the whole day when one day is is selected. It shows the percentage of connections in use during this day, compared to the total number of days selected when more than one day is selected.
Total	This field displays totals for measurable items in this screen.

25.5.7 Custom Service Top Sites

To view sites visited when using custom services defined in the **Service, Settings** screen, through selected ZyXEL device(s), during the specified time, select a ZyXEL device(s) and then click **Report, Service**, **Top Sites, Customized Service Group**.

Figure 214 Custom Service Top Sites



Service>>Top Sites>>Customized Service

Top Sites for 2005-2-18

Chart Type PIE | List Top 10 | Last 1 Days | Settings

Top Sites of Customized Service Usage

Sites	Color	Events	MBytes	% of MBytes
Total		0	0.000	100%

Table 163 Custom Service Top Sites

LABEL	DESCRIPTION
Chart Type	Select **PIE** or **BAR** chart from the **Chart Type** list box. You can select the default for all screens in the **Report, System, General Config** screen.
List Top 10	Select the number of sites to view from the drop-down list box
Last Days	The report displays information per hour when you select one day and information per day when you select more than one day.
Settings	Click **Settings** to view reports for more sites visited, or for days (up to 31 days) than the previous list box allows or for an earlier time range.
Sites	This field displays the URL or IP address of the site visited.
Color	You can color code individual items for better graphical representation.
Events	This field displays the number of events or "hits."
MBytes	This field displays the number of megabytes consumed by the custom services defined in the **Service, Settings** screen, through the selected ZyXEL device(s) in the last hour or day.

Table 163 Custom Service Top Sites

% of MBytes	This field shows the percentage of megabytes consumed by the custom services defined in the **Service, Settings** screen, during this hour, compared to the whole day when one day is is selected. It shows the percentage of megabytes consumed by the service(s) during this day, compared to the total number of days selected when more than one day is selected.
Total	This field displays totals for measurable items in this screen.

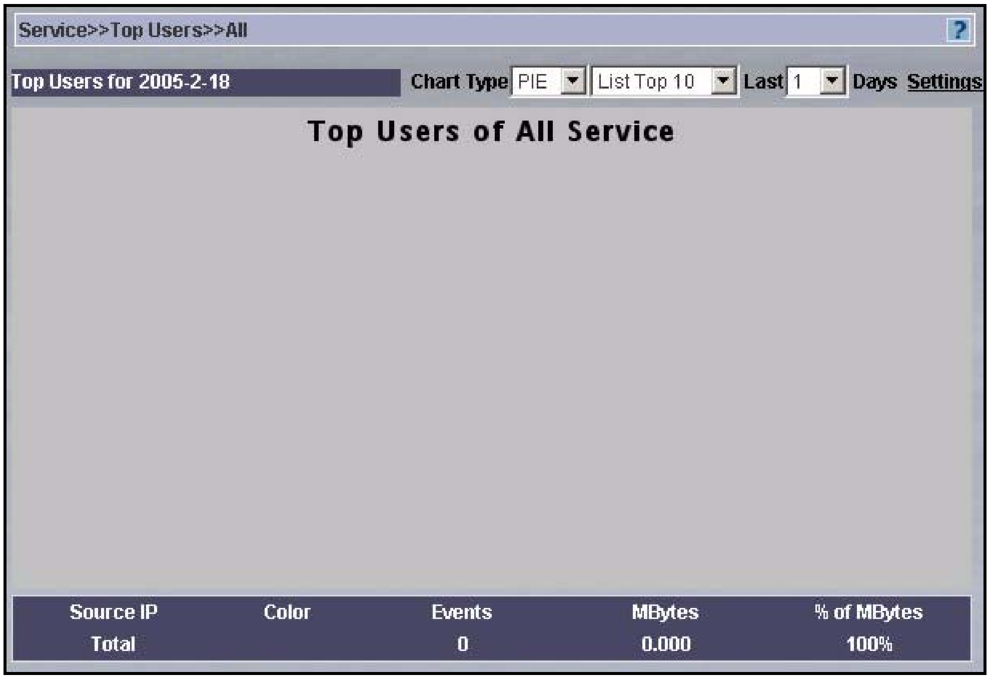
25.6 Top Users of Services

Use these screens to view top users (source IP addresses) that used a service(s), through a ZyXEL device(s) during the specified time.

25.6.1 Top Users of All Services

To view top users (source IP addresses) of all services defined in the **Service, Settings** screen, through selected ZyXEL device(s), during the specified time, select a ZyXEL device(s) and then click **Report, Service**, **Top Users, All**.

Figure 215 All Services Top Users



Service>>Top Users>>All

Top Users for 2005-2-18

Chart Type PIE | List Top 10 | Last 1 Days | Settings

Top Users of All Service

Source IP	Color	Events	MBytes	% of MBytes
Total		0	0.000	100%

Table 164 All Services Top Users

LABEL	DESCRIPTION
Chart Type	Select **PIE** or **BAR** chart from the **Chart Type** list box. You can select the default for all screens in the **Report, System, General Config** screen.

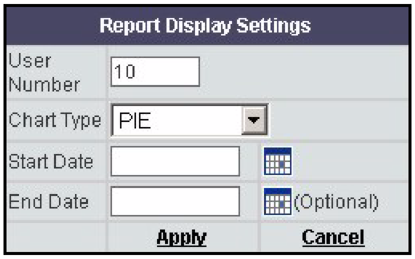
Table 164 All Services Top Users (continued)

List Top 10	Select the number of users to view from the drop-down list box
Last Days	The report displays information per hour when you select one day and information per day when you select more than one day.
Settings	Click **Settings** to view reports for more users, or for days (up to 31 days) than the previous list box allows or for an earlier time range.
Source IP	This field displays the source IP address (user) that used a service(s), through a ZyXEL device(s) during each hour of the current day or each day for a range of days (up to 31 days).
Color	You can color code individual items for better graphical representation.
Events	This field displays the number of events or "hits."
MBytes	This field displays the number of megabytes consumed by the service(s).through the selected ZyXEL device(s) in the last hour or day.
% of MBytes	This field shows the percentage of megabytes consumed by the service(s) during this hour, compared to the whole day when one day is is selected. It shows the percentage of megabytes consumed by the service(s) during this day, compared to the total number of days selected when more than one day is selected.
Total	This field displays totals for measurable items in this screen.

25.6.2 Top Site Service Settings

Click **Settings** in the previous screen to view reports for more sites visited, or for days (up to 31 days) than the previous list box allows or for an earlier time range.

Figure 216 Top Site Service Settings



Report Display Settings

User Number: 10

Chart Type: PIE

Start Date:

End Date: (Optional)

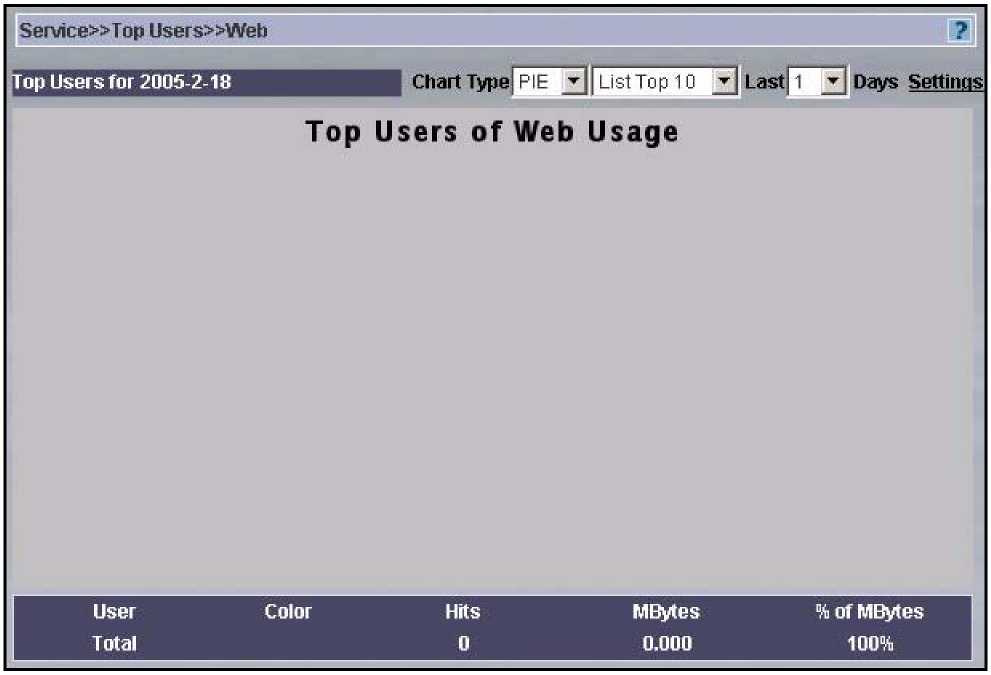
Table 165 Top Site Service Settings

LABEL	DESCRIPTION
User Number	Type the number of users you'd like to view here.
Chart Type	Select **PIE** or **BAR** chart from the **Chart Type** list box. You can select the default for all screens in the **Report, System, General Config** screen.
Start Date	Click the calendar icon to select a beginning year-month-date or manually enter the date in year-month-date format.
End Date	Click the calendar icon to select an ending year-month-date or manually enter the date in year-month-date format. The end date must come after the start date but not after the current date. The total range must not exceed 31 days.
Apply	Click **Apply** to create a report based on the settings you configured in this screen.
Cancel	Click **Cancel** to close this screen without saving your settings.

25.6.3 Top Users of Web Services

To view top users (source IP addresses) of web services through selected ZyXEL device(s), during the specified time, select a ZyXEL device(s) and then click **Report, Service**, **Top Users, Web.**

Figure 217 Top Users of Web Services



User	Color	Hits	MBytes	% of MBytes
Total		0	0.000	100%

Table 166 Top Users of Web Services

LABEL	DESCRIPTION
Chart Type	Select **PIE** or **BAR** chart from the **Chart Type** list box. You can select the default for all screens in the **Report, System, General Config** screen.
List Top 10	Select the number of users to view from the drop-down list box
Last Days	The report displays information per hour when you select one day and information per day when you select more than one day.
Settings	Click **Settings** to view reports for more users, or for days (up to 31 days) than the previous list box allows or for an earlier time range.
Users	This field displays the source IP address (user) that used web service, through a ZyXEL device(s) during each hour of the current day or each day for a range of days (up to 31 days).
Color	You can color code individual items for better graphical representation.
Hits	This field displays the number of events or "hits."
MBytes	This field displays the number of megabytes consumed by the service(s) through the selected ZyXEL device(s) in the last hour or day.

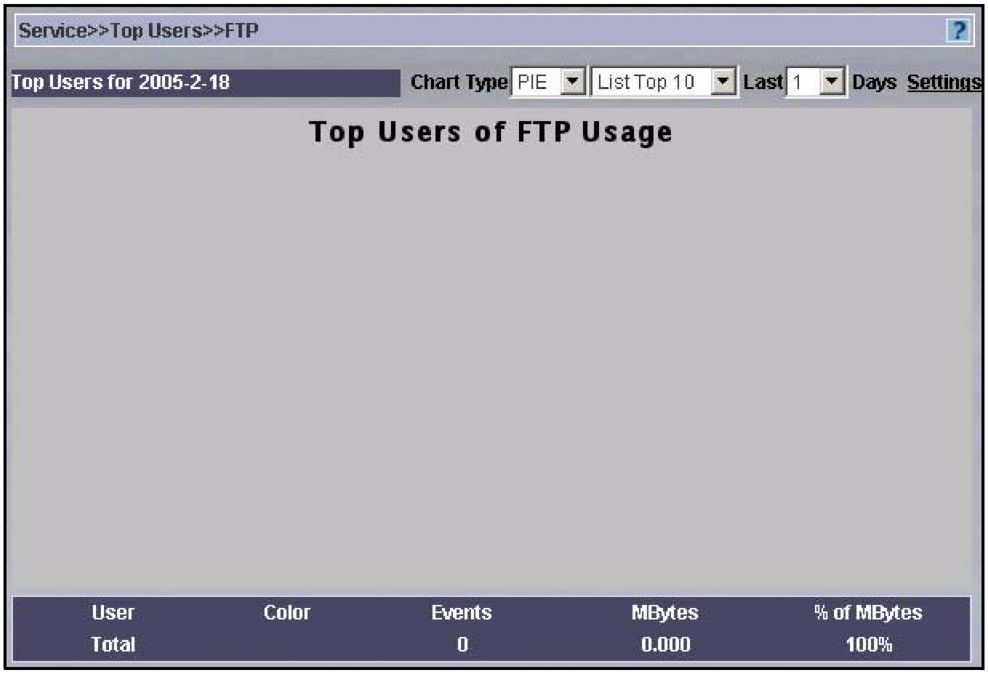
Table 166 Top Users of Web Services (continued)

% of MBytes	This field shows the percentage of megabytes consumed by the service(s) during this hour, compared to the whole day when one day is is selected. It shows the percentage of megabytes consumed by the service(s) during this day, compared to the total number of days selected when more than one day is selected.
Total	This field displays totals for measurable items in this screen.

25.6.4 Top Users of FTP Services

To view top users (source IP addresses) of FTP services through selected ZyXEL device(s), during the specified time, select a ZyXEL device(s) and then click **Report, Service**, **Top Users, FTP**.

Figure 218 Top Users of FTP Services



Service>>Top Users>>FTP

Top Users for 2005-2-18 Chart Type PIE List Top 10 Last 1 Days Settings

Top Users of FTP Usage

User	Color	Events	MBytes	% of MBytes
Total		0	0.000	100%

Table 167 Top Users of FTP Services

LABEL	DESCRIPTION
Chart Type	Select **PIE** or **BAR** chart from the **Chart Type** list box. You can select the default for all screens in the **Report, System, General Config** screen.
List Top 10	Select the number of users to view from the drop-down list box
Last Days	The report displays information per hour when you select one day and information per day when you select more than one day.
Settings	Click **Settings** to view reports for more users, or for days (up to 31 days) than the previous list box allows or for an earlier time range.
User	This field displays the source IP address (user) that used FTP service, through a ZyXEL device(s) during each hour of the current day or each day for a range of days (up to 31 days).

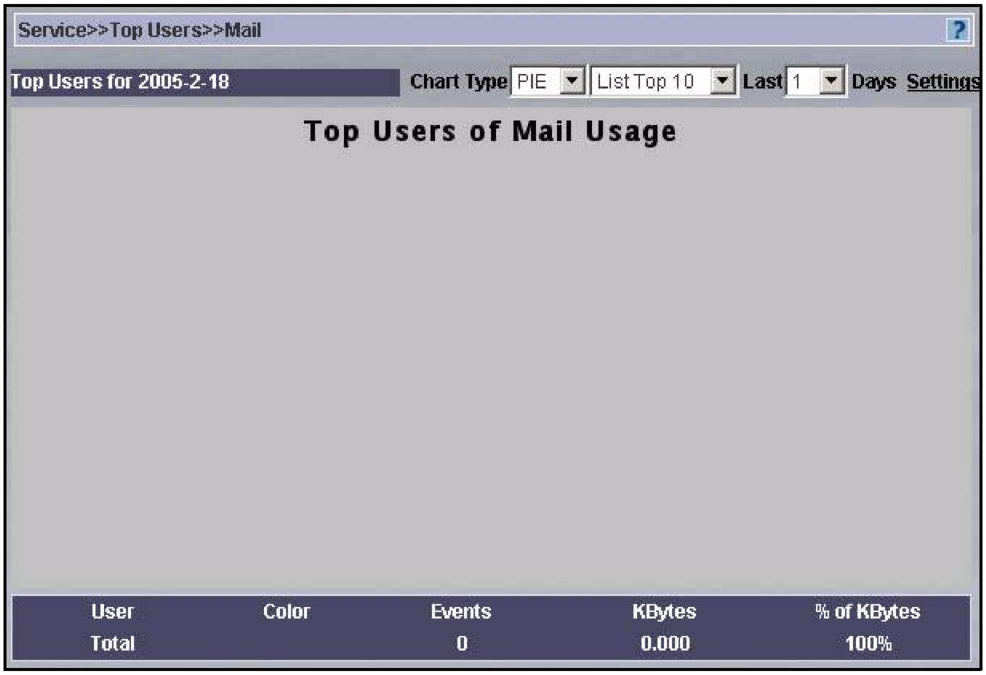
Table 167 Top Users of FTP Services (continued)

LABEL	DESCRIPTION
Color	You can color code individual items for better graphical representation.
Events	This field displays the number of events or "hits."
MBytes	This field displays the number of megabytes consumed by the service(s) through the selected ZyXEL device(s) in the last hour or day.
% of MBytes	This field shows the percentage of megabytes consumed by the service(s) during this hour, compared to the whole day when one day is is selected. It shows the percentage of megabytes consumed by the service(s) during this day, compared to the total number of days selected when more than one day is selected.
Total	This field displays totals for measurable items in this screen.

25.6.5 Top Users of Mail Services

To view top users (source IP addresses) of mail services through selected ZyXEL device(s), during the specified time, select a ZyXEL device(s) and then click **Report, Service**, **Top Users, MAIL**.

Figure 219 Top Users of Mail Services



User	Color	Events	KBytes	% of KBytes
Total		0	0.000	100%

Table 168 Top Users of Mail Services

LABEL	DESCRIPTION
Chart Type	Select **PIE** or **BAR** chart from the **Chart Type** list box. You can select the default for all screens in the **Report, System, General Config** screen.
List Top 10	Select the number of users to view from the drop-down list box

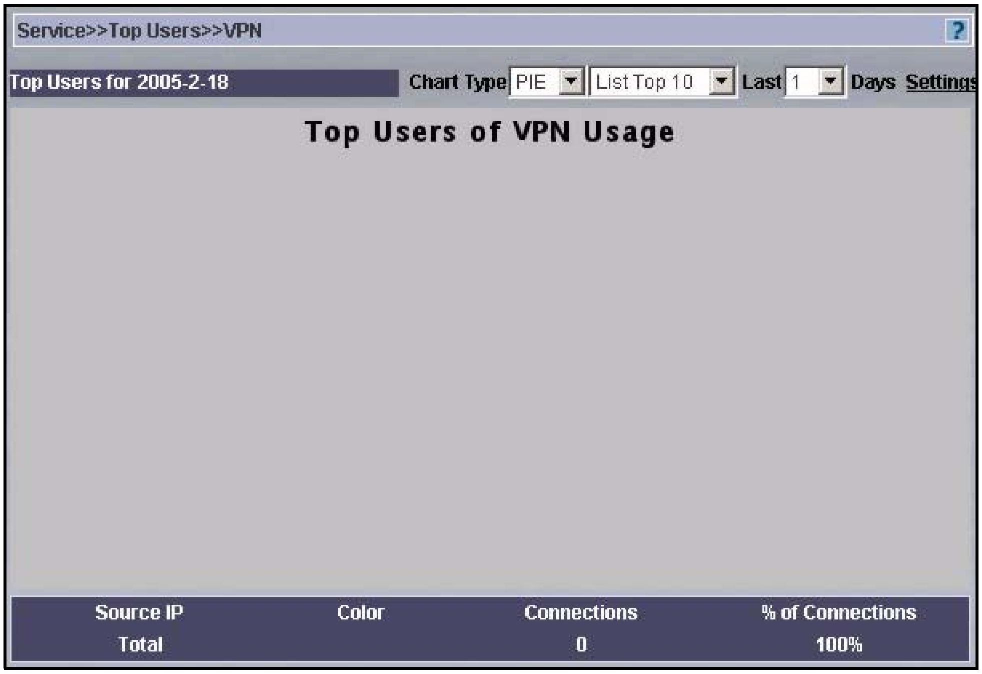
Table 168 Top Users of Mail Services (continued)

LABEL	DESCRIPTION
Last Days	The report displays information per hour when you select one day and information per day when you select more than one day.
Settings	Click **Settings** to view reports for more users, or for days (up to 31 days) than the previous list box allows or for an earlier time range.
User	This field displays the source IP address (user) that used mail service, through a ZyXEL device(s) during each hour of the current day or each day for a range of days (up to 31 days).
Color	You can color code individual items for better graphical representation.
Events	This field displays the number of events or "hits."
KBytes	This field displays the number of megabytes consumed by the service(s) through the selected ZyXEL device(s) in the last hour or day.
% of KBytes	This field shows the percentage of kilobytes consumed by the service(s) during this hour, compared to the whole day when one day is is selected. It shows the percentage of kilobytes consumed by the service(s) during this day, compared to the total number of days selected when more than one day is selected.
Total	This field displays totals for measurable items in this screen.

25.6.6 Top Users of VPN Tunnels

To view top users (source IP addresses) of VPN tunnels through selected ZyXEL device(s), during the specified time, select a ZyXEL device(s) and then click **Report, Service**, **Top Users, VPN**.

Figure 220 Top Users of VPN Tunnels



Top Users for 2005-2-18

Top Users of VPN Usage

Source IP	Color	Connections	% of Connections
Total		0	100%

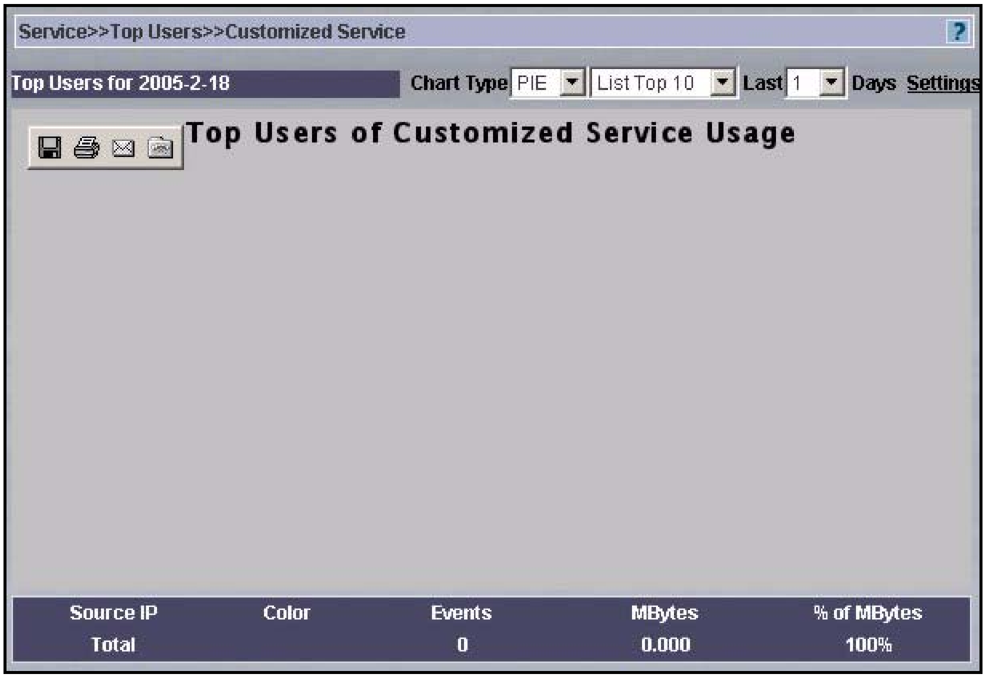
Table 169 Top Users of VPN Tunnels

	DESCRIPTION
Chart Type	Select **PIE** or **BAR** chart from the **Chart Type** list box. You can select the default for all screens in the **Report, System, General Config** screen.
List Top 10	Select the number of users to view from the drop-down list box
Last Days	The report displays information per hour when you select one day and information per day when you select more than one day.
Settings	Click **Settings** to view reports for more users, or for days (up to 31 days) than the previous list box allows or for an earlier time range.
Source IP	This field displays the source IP address (user) that used VPN service, through a ZyXEL device(s) during each hour of the current day or each day for a range of days (up to 31 days).
Color	You can color code individual items for better graphical representation.
Connections	This field displays the number of connections.
% of Connections	This field shows the percentage of connections in use during this hour, compared to the whole day when one day is is selected. It shows the percentage of connections in use during this day, compared to the total number of days selected when more than one day is selected.
Total	This field displays totals for measurable items in this screen.

25.6.7 Top Users of Custom Services

To view top users (source IP addresses) of custom services defined in the **Service, Settings** screen, through selected ZyXEL device(s), during the specified time, select a ZyXEL device(s) and then click **Report, Service**, **Top Users, Customized Service Group**.

Figure 221 Top Users of Custom Services



Service>>Top Users>>Customized Service

Top Users for 2005-2-18 Chart Type PIE List Top 10 Last 1 Days Settings

Top Users of Customized Service Usage

Source IP	Color	Events	MBytes	% of MBytes
Total		0	0.000	100%

Table 170 Top Users of Custom Services

LABEL	DESCRIPTION
Chart Type	Select **PIE** or **BAR** chart from the **Chart Type** list box. You can select the default for all screens in the **Report, System, General Config** screen.
List Top 10	Select the number of users to view from the drop-down list box
Last Days	The report displays information per hour when you select one day and information per day when you select more than one day.
Settings	Click **Settings** to view reports for more users, or for days (up to 31 days) than the previous list box allows or for an earlier time range.
Source IP	This field displays the source IP address (user) that used custom services defined in the **Service, Settings** screen, through a ZyXEL device(s) during each hour of the current day or each day for a range of days (up to 31 days).
Color	You can color code individual items for better graphical representation.
Events	This field displays the number of events or "hits."
MBytes	This field displays the number of megabytes consumed by the service(s) through the selected ZyXEL device(s) in the last hour or day.
% of MBytes	This field shows the percentage of megabytes consumed by the service(s) during this hour, compared to the whole day when one day is is selected. It shows the percentage of megabytes consumed by the service(s) during this day, compared to the total number of days selected when more than one day is selected.
Total	This field displays totals for measurable items in this screen.

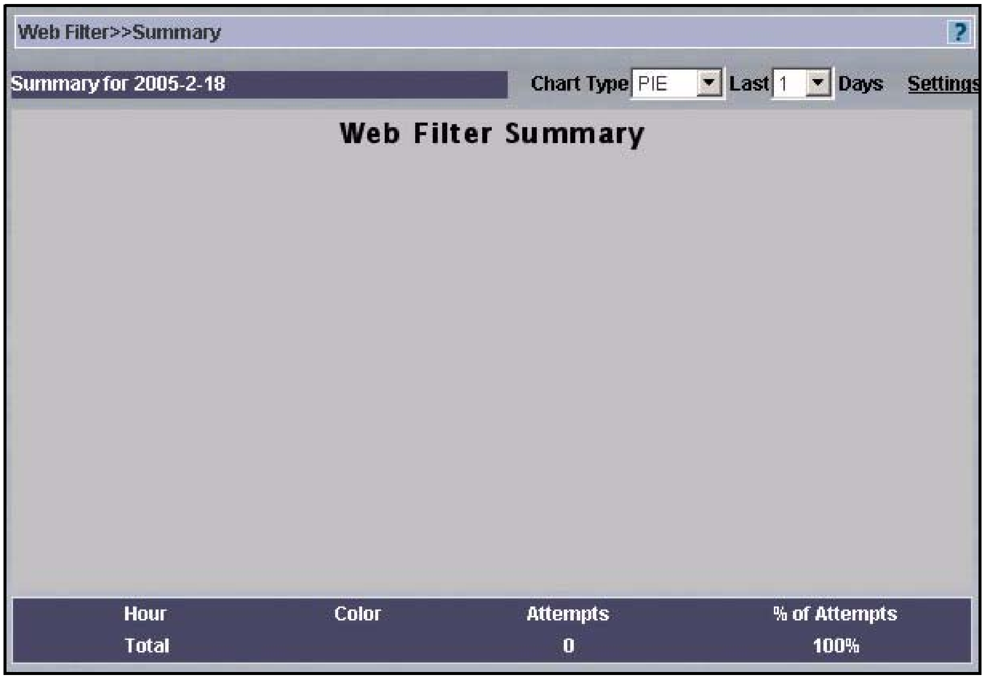
CHAPTER 26
Web Filter

A blocked site is a site blocked by a ZyXEL device(s) content filtering feature. Use these screens to view information on attempts to access a blocked site, through the selected ZyXEL device(s), during the specified timeduring.

26.1 Web Filter Summary

Use this screen to view the number of attempts to access a blocked site, through the selected ZyXEL device(s), during the specified time. Select **Report, Web Filter, Summary**.

Figure 222 Web Filter Summary



Web Filter>>Summary

Summary for 2005-2-18

Chart Type PIE ▾ Last 1 ▾ Days Settings

Web Filter Summary

Hour	Color	Attempts	% of Attempts
Total		0	100%

Table 171 Web Filter Summary

LABEL	DESCRIPTION
Chart Type	Select **PIE** or **BAR** chart from the **Chart Type** list box. You can select the default for all screens in the **Report, System, General Config** screen.
Last Days	The report displays information per hour when you select one day and information per day when you select more than one day.
Settings	Click **Settings** to view reports for days (up to 31 days) than the previous list box allows or for an earlier time range.

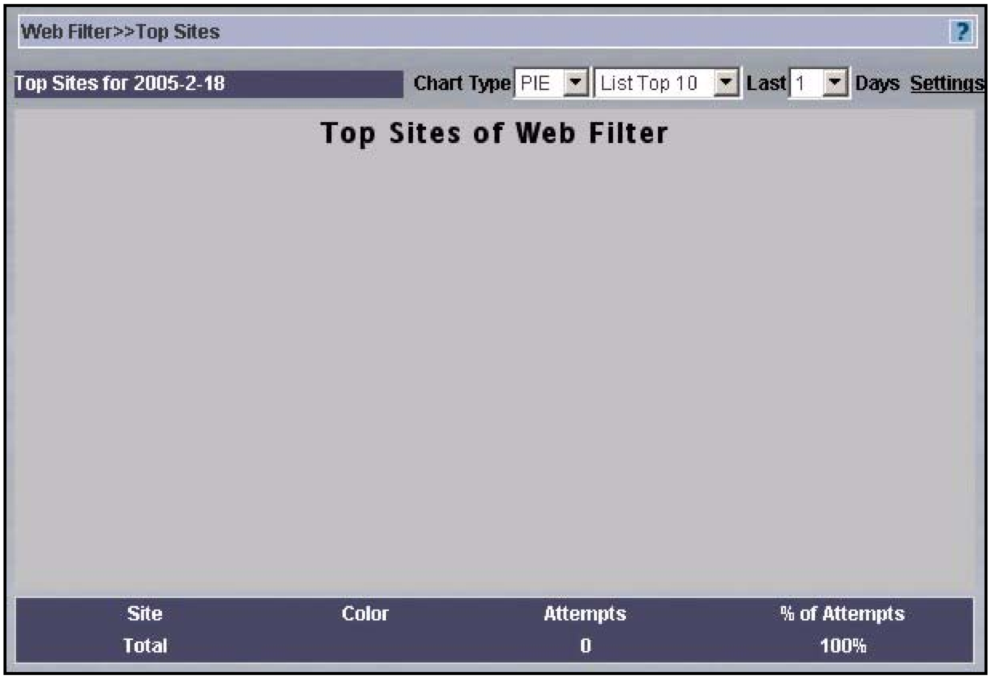
Table 171 Web Filter Summary (continued)

LABEL	DESCRIPTION
Hour	This field displays the time the (blocked) access attempt was made.
Color	You can color code individual items for better graphical representation.
Attempts	This field displays the number of attempts to access a blocked site.
% of Attempts	This field shows the percentage of attempts to access a blocked site during this hour, compared to the whole day when one day is is selected. It shows the percentage of attempts to access a blocked site during this day, compared to the total number of days selected when more than one day is selected.
Total	This field displays totals for measurable items in this screen.

26.2 Web Filter Top Sites

Use this screen to view the top blocked sites by attempts to access a blocked site, through the selected ZyXEL device(s), during the specified time. Select **Report, Web Filter, Top Sites**.

Figure 223 Web Filter Top Sites



Top Sites for 2005-2-18

Chart Type PIE

List Top 10

Last 1 Days

Top Sites of Web Filter

Site	Color	Attempts	% of Attempts
Total		0	100%

Table 172 Web Filter Top Sites

LABEL	DESCRIPTION
Chart Type	Select **PIE** or **BAR** chart from the **Chart Type** list box. You can select the default for all screens in the **Report, System, General Config** screen.
Last Days	The report displays information per hour when you select one day and information per day when you select more than one day.

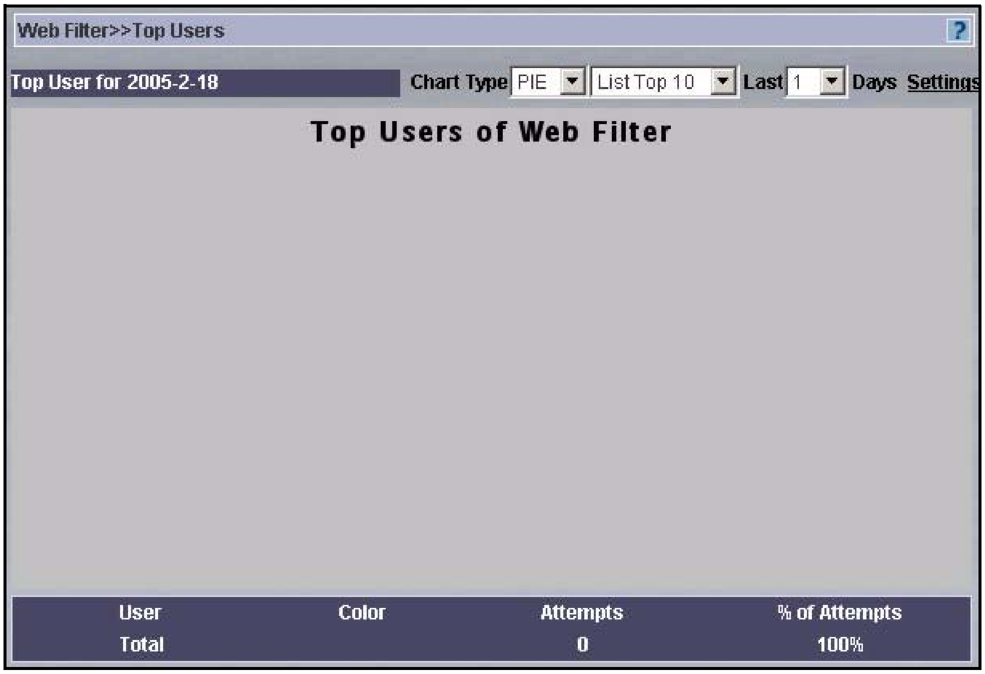
Table 172 Web Filter Top Sites (continued)

LABEL	DESCRIPTION
Settings	Click **Settings** to view reports for days (up to 31 days) than the previous list box allows or for an earlier time range.
Site	This field displays the blocked sites by attempts to access a blocked site, through the selected ZyXEL device(s).
Color	You can color code individual items for better graphical representation.
Attempts	This field displays the number of attempts to access a blocked site.
% of Attempts	This field shows the percentage of attempts to access a blocked site during this hour, compared to the whole day when one day is is selected. It shows the percentage of attempts to access a blocked site during this day, compared to the total number of days selected when more than one day is selected.
Total	This field displays totals for measurable items in this screen.

26.3 Web Filter Top Users

Use this screen to view the top users who attempted to access a blocked site, through the selected ZyXEL device(s), during the specified time.

Figure 224 Web Filter Top Users



Web Filter>>Top Users

Top User for 2005-2-18

Top Users of Web Filter

User	Color	Attempts	% of Attempts
Total		0	100%

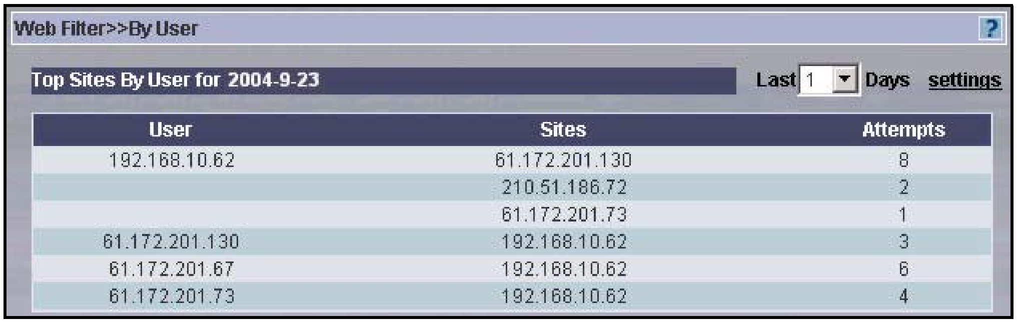
Table 173 Web Filter Top Users

LABEL	DESCRIPTION
Chart Type	Select **PIE** or **BAR** chart from the **Chart Type** list box. You can select the default for all screens in the **Report, System, General Config** screen.
Last Days	The report displays information per hour when you select one day and information per day when you select more than one day.
Settings	Click **Settings** to view reports for days (up to 31 days) than the previous list box allows or for an earlier time range.
Users	This field displays the users who attempted to access a blocked site, through the selected ZyXEL device(s).
Color	You can color code individual items for better graphical representation.
Attempts	This field displays the number of attempts to access a blocked site.
% of Attempts	This field shows the percentage of attempts to access a blocked site during this hour, compared to the whole day when one day is is selected. It shows the percentage of attempts to access a blocked site during this day, compared to the total number of days selected when more than one day is selected.
Total	This field displays totals for measurable items in this screen.

26.4 Web Filter By User

Use this screen to view the number of attempts a user made to access a blocked site, through the selected ZyXEL device(s), during the specified time.

Figure 225 Web Filter By User



Web Filter>>By User

Top Sites By User for 2004-9-23

Last 1 Days settings

User	Sites	Attempts
192.168.10.62	61.172.201.130	8
	210.51.186.72	2
	61.172.201.73	1
61.172.201.130	192.168.10.62	3
61.172.201.67	192.168.10.62	6
61.172.201.73	192.168.10.62	4

Table 174 Web Filter By User

LABEL	
	The report displays information per hour when you select one day and information per day when you select more than one day.
Settings	Click **Settings** to view reports for days (up to 31 days) than the previous list box allows or for an earlier time range.
User	This field displays the user who attempted to access a blocked site, through the selected ZyXEL device(s).
Sites	This field displays the blocked sites by attempts to access a blocked site by this user, through the selected ZyXEL device(s).
Attempts	This field displays the number of attempts to access a blocked site.

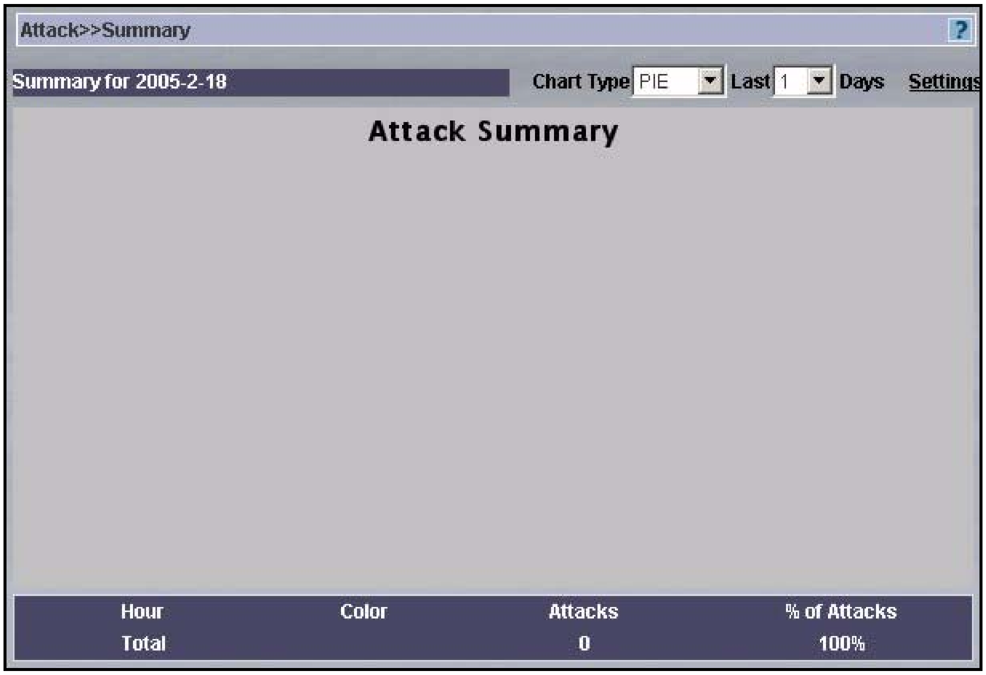
CHAPTER 27
Attack Reports

Use these screens to create reports on attacks detected by a ZyXEL device's firewall during the specified time.

27.1 Attack Summary

To view the number of attacks on the selected ZyXEL device(s), during the specified time, select a ZyXEL device(s) and then click **Report, Attack**, **Summary**.

Figure 226 Attack Summary



Hour	Color	Attacks	% of Attacks
Total		0	100%

Table 175 Attack Summary

LABEL	DESCRIPTION
Chart Type	Select **PIE** or **BAR** chart from the **Chart Type** list box. You can select the default for all screens in the **Report, System, General Config** screen.
Last Days	The report displays information per hour when you select one day and information per day when you select more than one day.
Settings	Click **Settings** to view reports for more days (up to 31 days) than the previous list box allows or for an earlier time range.
Hour	This field displays the time the attack occurred.

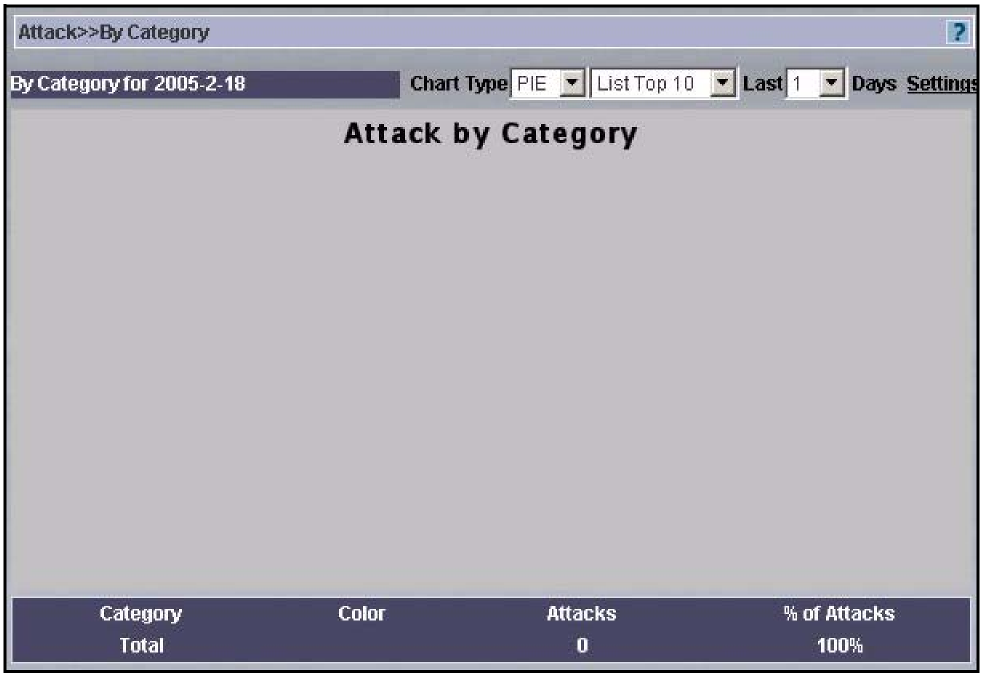
Table 175 Attack Summary (continued)

LABEL	DESCRIPTION
Color	You can color code individual items for better graphical representation.
Attacks	This field displays the number of attacks on the selected ZyXEL devices.
% of Attacks	This field shows the percentage of attacks on the selected ZyXEL devices during this hour, compared to the whole day when one day is is selected. It shows the percentage of attacks on the selected ZyXEL devices during this day, compared to the total number of days selected when more than one day is selected.
Total	This field displays totals for measurable items in this screen.

27.2 Attack Categories

To view the types of attacks on the selected ZyXEL device(s), during the specified time, select a ZyXEL device(s) and then click **Report, Attack**, **By Category**.

Figure 227 Attack Categories



Attack>>By Category

By Category for 2005-2-18

Chart Type PIE | List Top 10 | Last 1 Days

Attack by Category

Category	Color	Attacks	% of Attacks
Total		0	100%

Table 176 Attack Categories

LABEL	DESCRIPTION
Chart Type	Select **PIE** or **BAR** chart from the **Chart Type** list box. You can select the default for all screens in the **Report, System, General Config** screen.
List Top 10	Select the number of categories to view from the drop-down list box
Last Days	The report displays information per hour when you select one day and information per day when you select more than one day.

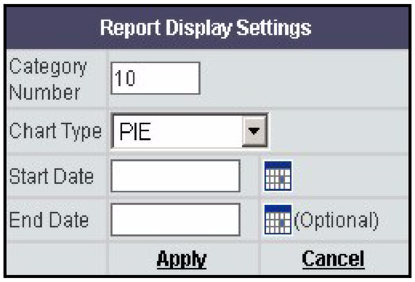
Table 176 Attack Categories (continued)

LABEL	DESCRIPTION
Settings	Click **Settings** to view reports for more categories, or for more days (up to 31 days) than the previous list box allows or for an earlier time range.
Category	This field displays the types of attacks that occurred.
Color	You can color code individual items for better graphical representation.
Attacks	This field displays the number of attacks on the selected ZyXEL devices.
% of Attacks	This field shows the percentage of attacks on the selected ZyXEL devices during this hour, compared to the whole day when one day is is selected. It shows the percentage of attacks on the selected ZyXEL devices during this day, compared to the total number of days selected when more than one day is selected.
Total	This field displays totals for measurable items in this screen.

27.2.1 Attack Category Settings

Enter the number of categories you want to view in the **Category Number** text field.

Figure 228 Attack Category Settings



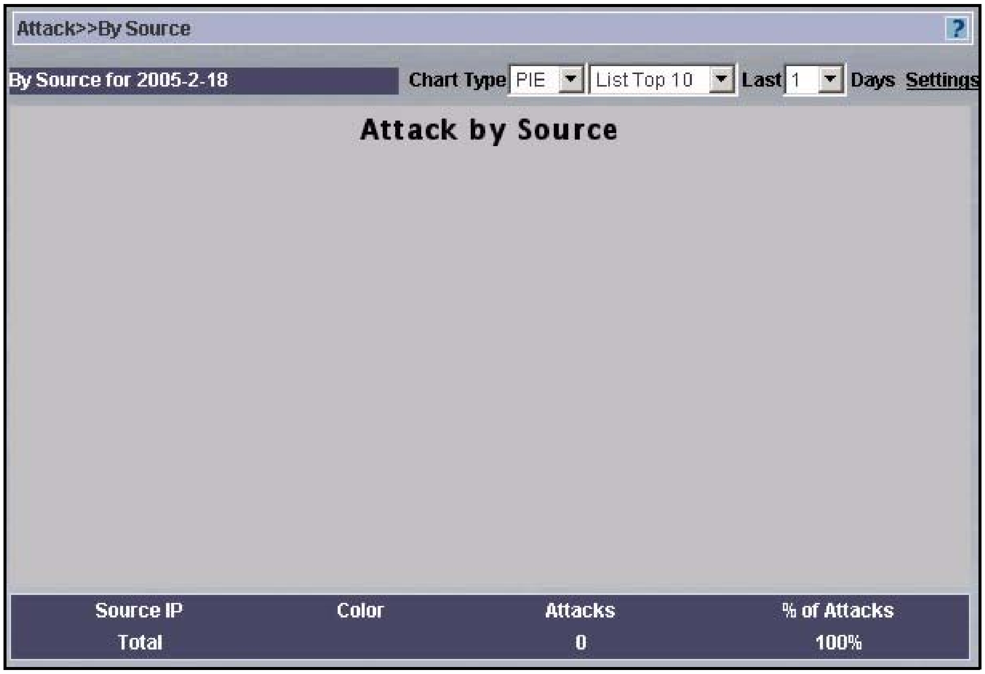
Report Display Settings

Category Number	10
Chart Type	PIE
Start Date	
End Date	(Optional)

27.3 Source of Attacks

To view the source IP addresses of attacks on the selected ZyXEL device(s), during the specified time, select a ZyXEL device(s) and then click **Report, Attack**, **By Source**.

Figure 229 Source of Attacks



By Source for 2005-2-18

Chart Type PIE | List Top 10 | Last 1 Days

Attack by Source

Source IP	Color	Attacks	% of Attacks
Total		0	100%

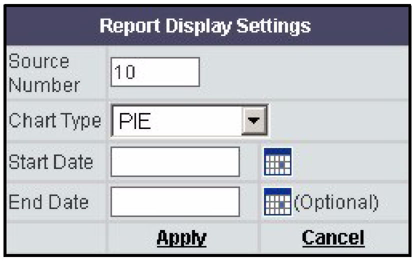
Table 177 Source of Attacks

LABEL	DESCRIPTION
Chart Type	Select **PIE** or **BAR** chart from the **Chart Type** list box. You can select the default for all screens in the **Report, System, General Config** screen.
List Top 10	Select the number of sources to view from the drop-down list box
Last Days	The report displays information per hour when you select one day and information per day when you select more than one day.
Settings	Click **Settings** to view reports for more source IP addresses, or for more days (up to 31 days) than the previous list box allows or for an earlier time range.
Source IP	This field displays the source IP addresses of attacks that occurred on the selected ZyXEL devices.
Color	You can color code individual items for better graphical representation.
Attacks	This field displays the number of attacks on the selected ZyXEL devices.
% of Attacks	This field shows the percentage of attacks on the selected ZyXEL devices during this hour, compared to the whole day when one day is is selected. It shows the percentage of attacks on the selected ZyXEL devices during this day, compared to the total number of days selected when more than one day is selected.
Total	This field displays totals for measurable items in this screen.

27.3.1 Attack Source Settings

Enter the number of attack source IP addresses that you want to view in the **Source Number** text field.

Figure 230 Attack Category Settings

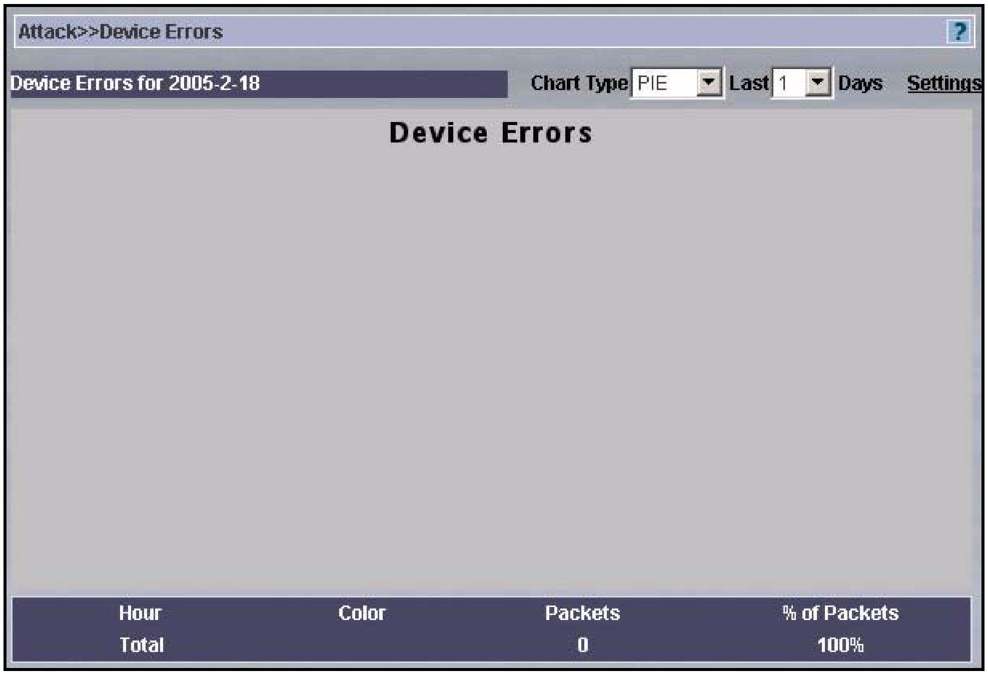


Report Display Settings	
Source Number	10
Chart Type	PIE
Start Date	
End Date	(Optional)

27.4 Attack Errors and Exceptions

To view information on the number of dropped packets by the selected ZyXEL device(s), during the specified time, select a ZyXEL device(s) and then click **Report, Attack**, **Errors & Exceptions**.

Figure 231 Attack Errors and Exceptions



Attack>>Device Errors

Device Errors for 2005-2-18

Chart Type PIE Last 1 Days

Hour	Color	Packets	% of Packets
Total		0	100%

Table 178 Attack Errors and Exceptions

LABEL	DESCRIPTION
Chart Type	Select **PIE** or **BAR** chart from the **Chart Type** list box. You can select the default for all screens in the **Report, System, General Config** screen.
Last Days	The report displays information per hour when you select one day and information per day when you select more than one day.
Settings	Click **Settings** to view reports for more days (up to 31 days) than the previous list box allows or for an earlier time range.
Hour	This field displays the time the packets were dropped.

Table 178 Attack Errors and Exceptions (continued)

LABEL	DESCRIPTION
Color	You can color code individual items for better graphical representation.
Packets	This field displays the number of packets that were dropped by the selected ZyXEL devices.
% of Packets	This field shows the percentage of packets on the selected ZyXEL devices during this hour, compared to the whole day when one day is is selected. It shows the percentage of packets on the selected ZyXEL devices during this day, compared to the total number of days selected when more than one day is selected.
Total	This field displays totals for measurable items in this screen.

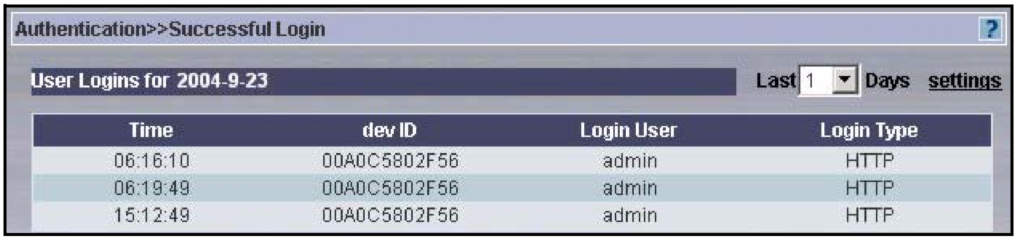
CHAPTER 28 Authentication

Use these screens to view information on who successfully logged into the selected ZyXEL devices (for management or monitoring purposes) and also on those who tried to log in, but failed.

28.1 Successful Logins

To view information on who successfully logged into the selected ZyXEL device(s), during the specified time, select a ZyXEL device(s) and then click **Report, Authentication, Successful Login**.

Figure 232 Successful Logins



User Logins for 2004-9-23

Last 1 Days

Time	dev ID	Login User	Login Type
06:16:10	00A0C5802F56	admin	HTTP
06:19:49	00A0C5802F56	admin	HTTP
15:12:49	00A0C5802F56	admin	HTTP

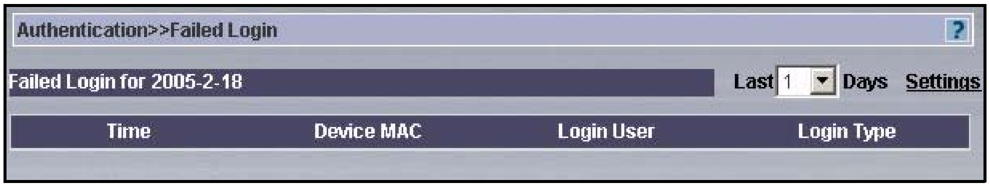
Table 179 Successful Logins

LABEL	DESCRIPTION
Last Days	The report displays information per hour when you select one day and information per day when you select more than one day.
Settings	Click **Settings** to view reports for more days (up to 31 days) than the previous list box allows or for an earlier time range.
Time	This field displays the time the person logged into a selected ZyXEL device.
dev ID	This field displays the LAN MAC address of the device the administrator logged into.
Login User	This field displays who logged into a selected ZyXEL device.
Login Type	This field shows whether the login was a web or Telnet connection.

28.2 Failed Logins

To view information on who failed to log into the selected ZyXEL device(s), during the specified time, select a ZyXEL device(s) and then click **Report, Authentication, Failed Login**.

Figure 233 Failed Logins



Authentication>>Failed Login

Failed Login for 2005-2-18

Last 1 Days Settings

Time	Device MAC	Login User	Login Type

Table 180 Failed Logins

LABEL	DESCRIPTION
Last Days	The report displays information per hour when you select one day and information per day when you select more than one day.
Settings	Click **Settings** to view reports for more days (up to 31 days) than the previous list box allows or for an earlier time range.
Time	This field displays the time the person attempted (and failed) to log into a selected ZyXEL device.
Device MAC	This field displays the LAN MAC address of the device the administrator failed to log into.
Login User	This field displays who failed to log into a selected ZyXEL device.
Login Type	This field shows whether the login attempt was a web or Telnet connection.

CHAPTER 29 Log Viewer

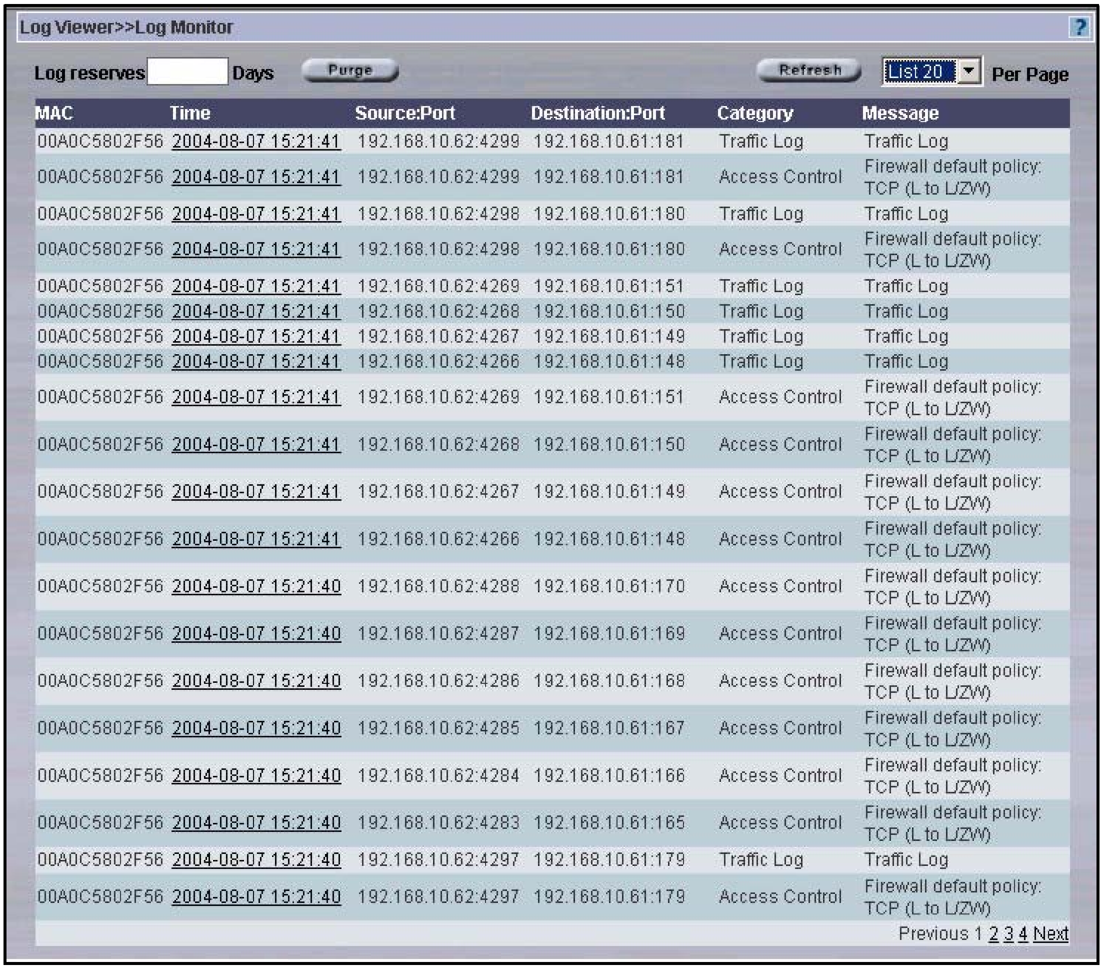
Use these screens to view and purge information on logs that the selected ZyXEL devices generated.

29.1 Log Monitor

To view (and purge information) on logs that the selected ZyXEL devices generated during the specified time, select a ZyXEL device(s) and then click **Report, Log Viewer, Log Monitor**.

Purged logs are saved as CSV (Comma-Separated Value) files. If you purge logs and then later discover you need to view them later, then use the **Report, System, CSV Import** screen to import the purged log CSV file.

Figure 234 Log Monitor



Log Viewer>>Log Monitor

Log reserves [ ] Days Purge Refresh List 20 Per Page

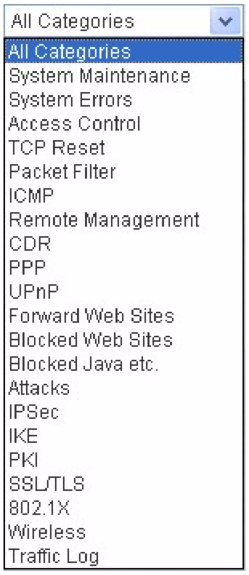
MAC	Time	Source:Port	Destination:Port	Category	Message
00A0C5802F56	2004-08-07 15:21:41	192.168.10.62:4299	192.168.10.61:181	Traffic Log	Traffic Log
00A0C5802F56	2004-08-07 15:21:41	192.168.10.62:4299	192.168.10.61:181	Access Control	Firewall default policy: TCP (L to L/ZW)
00A0C5802F56	2004-08-07 15:21:41	192.168.10.62:4298	192.168.10.61:180	Traffic Log	Traffic Log
00A0C5802F56	2004-08-07 15:21:41	192.168.10.62:4298	192.168.10.61:180	Access Control	Firewall default policy: TCP (L to L/ZW)
00A0C5802F56	2004-08-07 15:21:41	192.168.10.62:4269	192.168.10.61:151	Traffic Log	Traffic Log
00A0C5802F56	2004-08-07 15:21:41	192.168.10.62:4268	192.168.10.61:150	Traffic Log	Traffic Log
00A0C5802F56	2004-08-07 15:21:41	192.168.10.62:4267	192.168.10.61:149	Traffic Log	Traffic Log
00A0C5802F56	2004-08-07 15:21:41	192.168.10.62:4266	192.168.10.61:148	Traffic Log	Traffic Log
00A0C5802F56	2004-08-07 15:21:41	192.168.10.62:4269	192.168.10.61:151	Access Control	Firewall default policy: TCP (L to L/ZW)
00A0C5802F56	2004-08-07 15:21:41	192.168.10.62:4268	192.168.10.61:150	Access Control	Firewall default policy: TCP (L to L/ZW)
00A0C5802F56	2004-08-07 15:21:41	192.168.10.62:4267	192.168.10.61:149	Access Control	Firewall default policy: TCP (L to L/ZW)
00A0C5802F56	2004-08-07 15:21:41	192.168.10.62:4266	192.168.10.61:148	Access Control	Firewall default policy: TCP (L to L/ZW)
00A0C5802F56	2004-08-07 15:21:40	192.168.10.62:4288	192.168.10.61:170	Access Control	Firewall default policy: TCP (L to L/ZW)
00A0C5802F56	2004-08-07 15:21:40	192.168.10.62:4287	192.168.10.61:169	Access Control	Firewall default policy: TCP (L to L/ZW)
00A0C5802F56	2004-08-07 15:21:40	192.168.10.62:4286	192.168.10.61:168	Access Control	Firewall default policy: TCP (L to L/ZW)
00A0C5802F56	2004-08-07 15:21:40	192.168.10.62:4285	192.168.10.61:167	Access Control	Firewall default policy: TCP (L to L/ZW)
00A0C5802F56	2004-08-07 15:21:40	192.168.10.62:4284	192.168.10.61:166	Access Control	Firewall default policy: TCP (L to L/ZW)
00A0C5802F56	2004-08-07 15:21:40	192.168.10.62:4283	192.168.10.61:165	Access Control	Firewall default policy: TCP (L to L/ZW)
00A0C5802F56	2004-08-07 15:21:40	192.168.10.62:4297	192.168.10.61:179	Traffic Log	Traffic Log
00A0C5802F56	2004-08-07 15:21:40	192.168.10.62:4297	192.168.10.61:179	Access Control	Firewall default policy: TCP (L to L/ZW)

Previous 1 2 3 4 Next

Table 181 Log Monitor

LABEL	DESCRIPTION
Log reserves	Type the number of days you want to keep logs in Vantage. Logs older that this are then deleted from Vantage after you click the **Purge** button. For example, if you type “5”, all logs older than five days will be deleted. If you type “0”, all logs will be deleted.
Purge	Click this button to delete logs older than defined in the Log reserves text field from Vantage. You see this screen when logs have been successfully purged. Microsoft Internet Explorer Purge log successfully. OK
Refresh	Click this button to redisplay the screen with the latest logs that the selected ZyXEL devices generated.
List Per Page	Select the number of logs that you wish to display per page here.

Table 181 Log Monitor (continued)

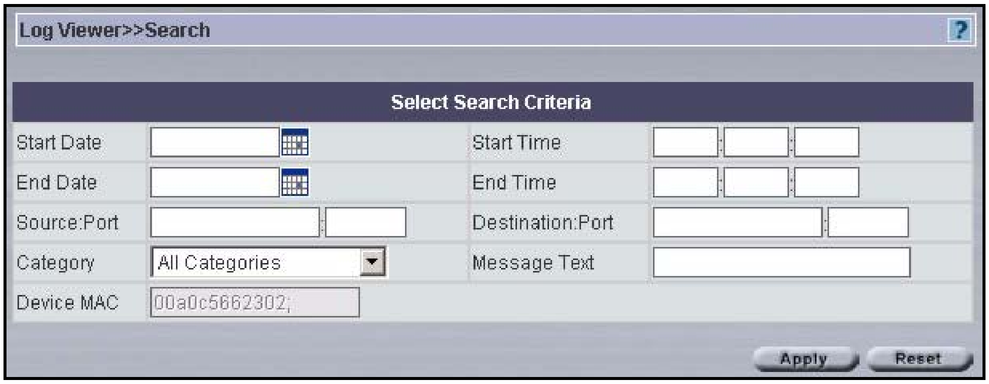
LABEL	DESCRIPTION
MAC	This field displays the LAN MAC address of the device that caused the ZyXEL device to generate a log.
Time	This field displays the time the ZyXEL device generated the log.
Source:Port	This field displays the source port of the (ZyXEL device) generated log.
Destination:Port	This field displays the destination port of the (ZyXEL device) generated log.
Category	This field displays the type of log generated. The log type depends on the ZyXEL device model. Some example log categories are:  All Categories All Categories System Maintenance System Errors Access Control TCP Reset Packet Filter ICMP Remote Management CDR PPP UPnP Forward Web Sites Blocked Web Sites Blocked Java etc. Attacks IPSec IKE PKI SSL/TLS 802.1X Wireless Traffic Log
Message	This field displays additional information on the reason the log was generated.
Previous 1, 2, 3…Next	Use these hyperlinks to go to a specific log page.

29.2 Log Search

You can search for logs by specific criteria (date, time, port, category, log message or device LAN MAC address) select a ZyXEL device(s) and then click **Report, Log Viewer, Search**.

Fill in the search criteria as shown in this screen.

Figure 235 Log Search



Category: All Categories

Device MAC: 00a0c5662302;

Table 182 Log Search

LABEL	DESCRIPTION
Start Date	Click the calendar icon to select a beginning year-month-date or manually enter the date in year-month-date format.
Start Time	Enter the time from which to start searching for logs in hour-minute-second format in this screen.
End Date	Click the calendar icon to select an ending year-month-date or manually enter the date in year-month-date format. The end date must come after the start date but not after the current date.
End Time	Enter the time to which to start searching for logs in hour-minute-second format in this screen.
Source: Port	Enter the source port of the (ZyXEL device) generated log.
Destination: Port	Enter the destination port of the (ZyXEL device) generated log.
Category	Select the type of log generated from the drop-down list box (see Table 181).
Message Text	Select key log message text for which to search additional information on the reason the log was generated.
Device MAC	This field displays the LAN MAC address of the device that caused the ZyXEL device to generate a log.
Apply	Click **Apply** to begin your log search. The search result is then displayed.
Reset	Click **Reset** to begin configuring the screen afresh.

Chapter 30 Report System Screens

Use these screens to:

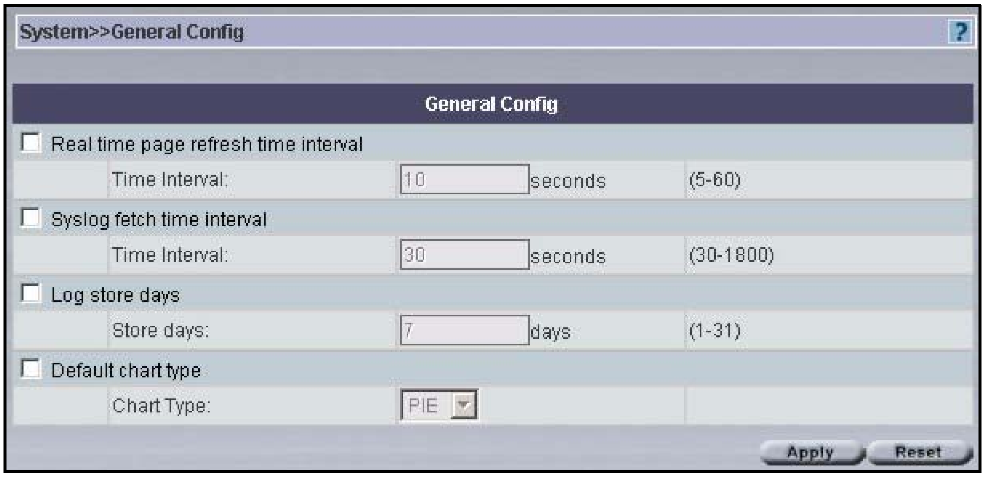
- Set default reporting parameters such as refresh intervals, syslog retrieval intervals, log storage within Vantage and default chart types.
- Schedule daily or weekly reports.
- Import a CSV (Comma-Separated Value) file of previously purged logs.
- View information on the Vantage reporting module.

30.1 General Configuration

Use this screen to set default reporting parameters such as refresh intervals, syslog retrieval intervals, log storage within Vantage and default chart types.

Click **Report, System, General Config** to display the next screen. Select a check box to make the corresponding item configurable.

Figure 236 General System Configuration



System>>General Config

General Config

□ Real time page refresh time interval			
Time Interval:	10	seconds	(5-60)
□ Syslog fetch time interval			
Time Interval:	30	seconds	(30-1800)
□ Log store days			
Store days:	7	days	(1-31)
□ Default chart type			
Chart Type:	PIE		

Table 183 General System Configuration

LABEL	DESCRIPTION
Real Time page Refresh Interval	Select the checkbox and then type the number of seconds a reporting monitoring screen should redisplay.
Syslog Fetch Time Interval	Select the checkbox and then type the number of seconds defining how often Vantage should retrieve logs from the syslog server.

Table 183 General System Configuration (continued)

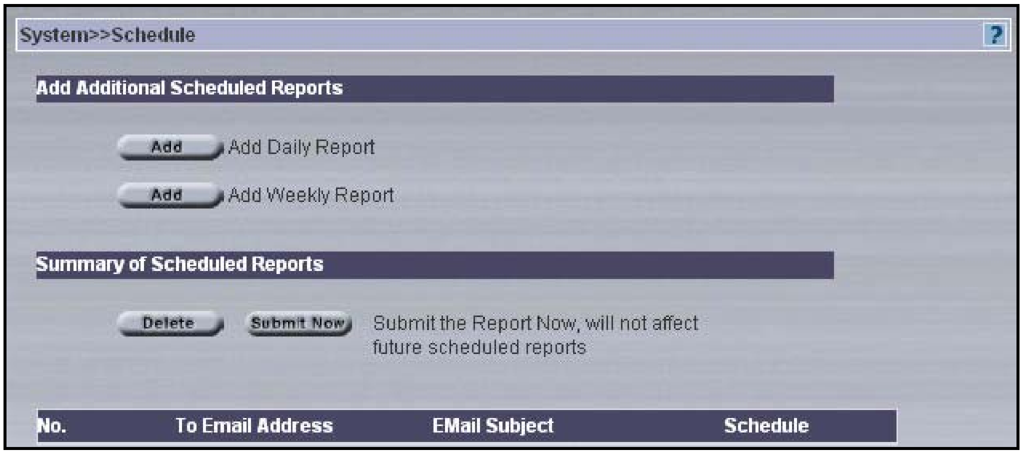
LABEL	DESCRIPTION
Log Store Days	Select the checkbox and then type the number of days Vantage should store logs.
Default Chart Type	Select the checkbox and then choose the default chart type that should display in report screens.
Apply	Click **Apply** to save your changes to the Vantage reporting module.
Reset	Click **Reset** to begin configuring the screen afresh.

30.2 Schedule Reports

Use this screen to schedule daily or weekly reports.

Click **Report, System, Schedule** to display the next screen.

Figure 237 Schedule Reports



System>>Schedule
?
Add Additional Scheduled Reports
Add
Add Daily Report
Add
Add Weekly Report
Summary of Scheduled Reports
Delete
Submit Now
Submit the Report Now, will not affect future scheduled reports
No.
To Email Address
EMail Subject
Schedule

Table 184 Schedule Reports

LABEL	DESCRIPTION
Add Additional Scheduled Reports	Use the next two buttons to schedule and configure daily or weekly reports.
Add (Add Daily Report)	Use this button to schedule and configure daily reports.
Add (Add Weekly Report)	Use this button to schedule and configure weekly reports.
Summary of Scheduled Reports	Use the next two buttons to delete scheduled reports or send a scheduled report immediately.
Delete	Select a report and then use this button to delete that scheduled report.
Submit Now (Submit the Report Now, will not affect future scheduled reports)	Select a report and then use this button to send that scheduled report immediately. Submitting a report immediately does not affect future scheduled reports.
No.	This is a previously created scheduled report index number.

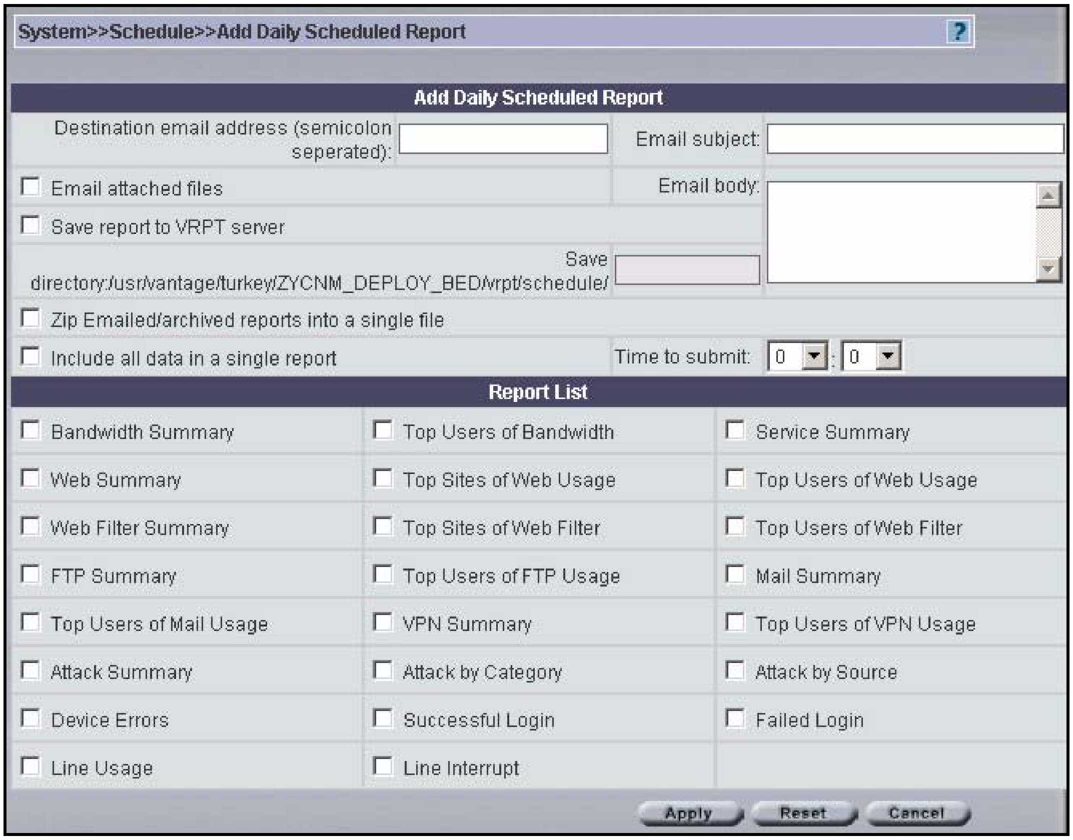
Table 184 Schedule Reports (continued)

LABEL	DESCRIPTION
To Email Address	This is the e-mail address(es) to which a previously created scheduled report sends reports.
EMail Subject	This is the e-mail subject a previously created scheduled report uses.
Schedule	This is the time of day or the day of the week a previously created report has been scheduled.

30.2.1 Schedule Daily Report

Click **Add** (Add Daily Report) in the System Schedule screen to display the next screen. Use this screen to send reports each day. In this screen, you can configure e-mail details, report types and times to send.

Figure 238 Schedule Daily Reports



System>>Schedule>>Add Daily Scheduled Report

Add Daily Scheduled Report

Destination email address (semicolon seperated):

Email subject:

□ Email attached files

Email body:

□ Save report to VRPT server

Save directory:/usr/vantage/turkey/ZYCNM_DEPLOY_BED/vrpt/schedule/

□ Zip Emailed/archived reports into a single file

□ Include all data in a single report

Time to submit: 0 : 0

Report List

□ Bandwidth Summary	□ Top Users of Bandwidth	□ Service Summary
□ Web Summary	□ Top Sites of Web Usage	□ Top Users of Web Usage
□ Web Filter Summary	□ Top Sites of Web Filter	□ Top Users of Web Filter
□ FTP Summary	□ Top Users of FTP Usage	□ Mail Summary
□ Top Users of Mail Usage	□ VPN Summary	□ Top Users of VPN Usage
□ Attack Summary	□ Attack by Category	□ Attack by Source
□ Device Errors	□ Successful Login	□ Failed Login
□ Line Usage	□ Line Interrupt	

Table 185 Schedule Daily Reports

LABEL	DESCRIPTION
Add Daily Scheduled Report	
Destination Email Address (Semicolon seperated):	Type e-mail addresses to where e-mailed reports should be sent separated by semicolons.

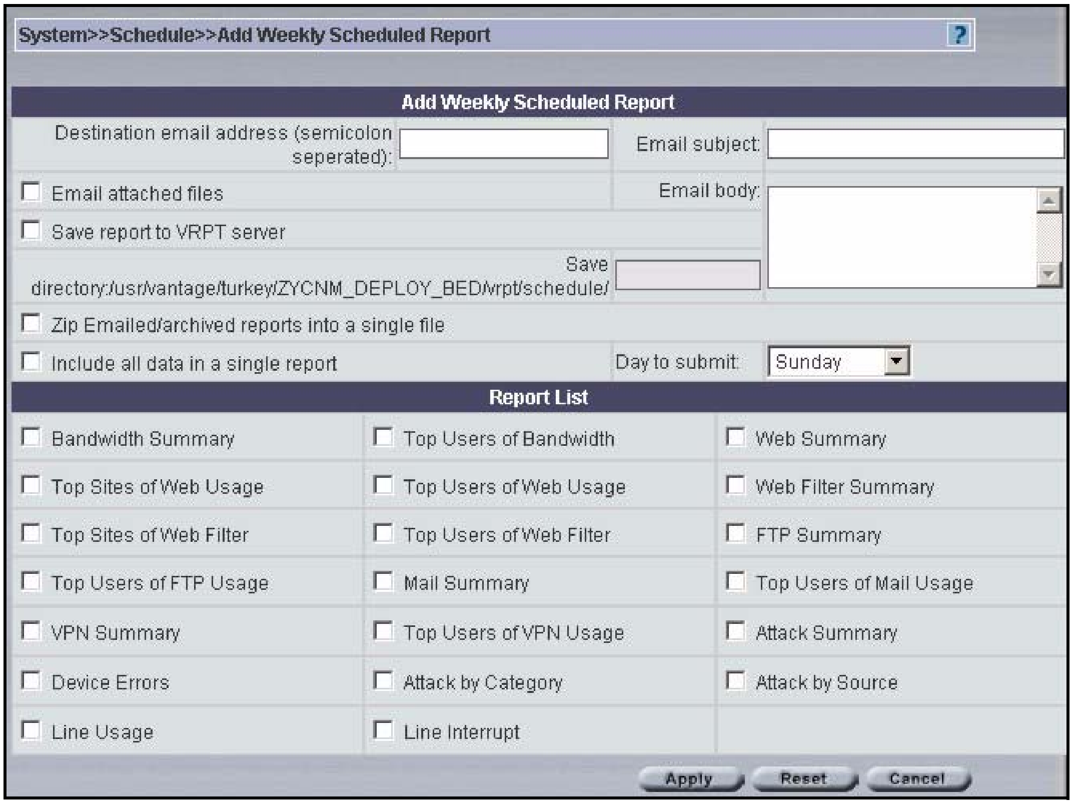
Table 185 Schedule Daily Reports (continued)

LABEL	DESCRIPTION
Email Subject:	Type a meaningful e-mail subject here.
Email Attached Files	Select this checkbox to have Vantage e-mail the attached reports.
Email Body:	Type a meaningful message that you want to appear in the e-mail body here.
Save Report to VRPT Server	Select this checkbox to save the selected reports within the Vantage server.
Save directory:/usr/vantage/ ZYCNM_DEPLOY_BED/vrpt/schedule/	Type the name of the report here. The report will be saved to this path on the Vantage server.
Zip Emailed/Archived Reports into a Single File	Select this checkbox to zip selected reports into a single file when e-mailing them.
Include All Data In a Single Report	Select this checkbox to merge all selected reports into a single report when e-mailing them
time to submit	Select the hour and minute from the respective drop-down list boxes at which to send these daily reports.
Report List	Select the report type from this list. Each report type corresponds to a report screen in Vantage.
Apply	Click **Apply** to save your changes and exit this screen.
Reset	Click **Reset** to revert to last-saved screen settings.
Cancel	Click **Cancel** to close this screen without saving any setting changes.

30.2.2 Schedule Weekly Report

Click **Add** (**Add Weekly Report**) in the **System Schedule** screen to display the next screen. Use this screen to send reports once a week. In this screen, you can configure e-mail details, report types and days of the week to send.

Figure 239 Schedule Weekly Reports



System>>Schedule>>Add Weekly Scheduled Report

Add Weekly Scheduled Report

Destination email address (semicolon seperated):		Email subject:	
☐ Email attached files		Email body:	
☐ Save report to VRPT server			
Save directory:/usr/vantage/turkey/ZYCNM_DEPLOY_BED/vrpt/schedule/			
☐ Zip Emailed/archived reports into a single file			
☐ Include all data in a single report		Day to submit:	Sunday

Report List

☐ Bandwidth Summary	☐ Top Users of Bandwidth	☐ Web Summary
☐ Top Sites of Web Usage	☐ Top Users of Web Usage	☐ Web Filter Summary
☐ Top Sites of Web Filter	☐ Top Users of Web Filter	☐ FTP Summary
☐ Top Users of FTP Usage	☐ Mail Summary	☐ Top Users of Mail Usage
☐ VPN Summary	☐ Top Users of VPN Usage	☐ Attack Summary
☐ Device Errors	☐ Attack by Category	☐ Attack by Source
☐ Line Usage	☐ Line Interrupt	

Table 186 Schedule Daily Reports

LABEL	DESCRIPTION
Add Weekly Scheduled Report	
Destination Email Address (Semicolon seperated):	Type e-mail addresses to where e-mailed reports should be sent separated by semicolons.
Email Subject:	Type a meaningful e-mail subject here.
Email Attached Files	Select this checkbox to have Vantage e-mail the attached reports.
Email Body:	Type a meaningful message that you want to appear in the e-mail body here.
Save Report to VRPT Server	Select this checkbox to save the selected reports within the Vantage server.
Save directory:/usr/vantage/ ZYCNM_DEPLOY_BED/vrpt/schedule	Type the name of the report here. The report will be saved to this path on the Vantage server.
Zip Emailed/Archived Reports into a Single File	Select this checkbox to zip selected reports into a single file when e-mailing them.
Include All Data In a Single Report	Select this checkbox to merge all selected reports into a single report when e-mailing them
day to submit	Select the day from the drop-down list box at which to send these daily reports.
Report List	Select the report type from this list. Each report type corresponds to a report screen in Vantage.

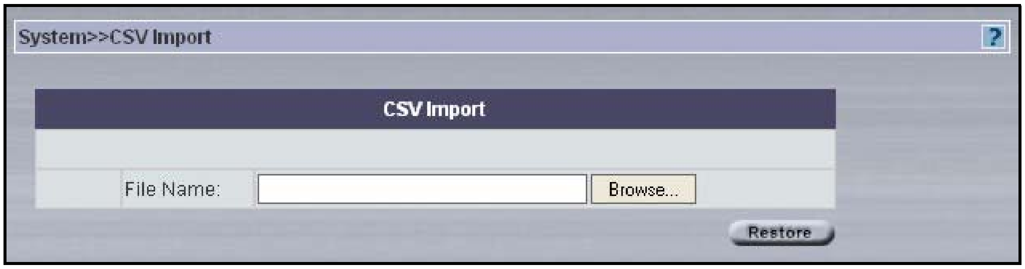
Table 186 Schedule Daily Reports (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes and exit this screen.
Reset	Click **Reset** to revert to last-saved screen settings.
Cancel	Click **Cancel** to close this screen without saving any setting changes.

30.3 CSV Import

Purged logs are saved as CSV (Comma-Separated Value) files. If you purge logs and then later discover you need to view them later, then use this screen to import the purged log CSV file. Click **Report, System, CSV Import** to display the next screen. Click **Browse** to navigate to the CSV file on your computer or type the file name and path in the text box and then click **Restore** to bring the file into the Vantage reporting module.

Figure 240 CSV Import



System>>CSV Import

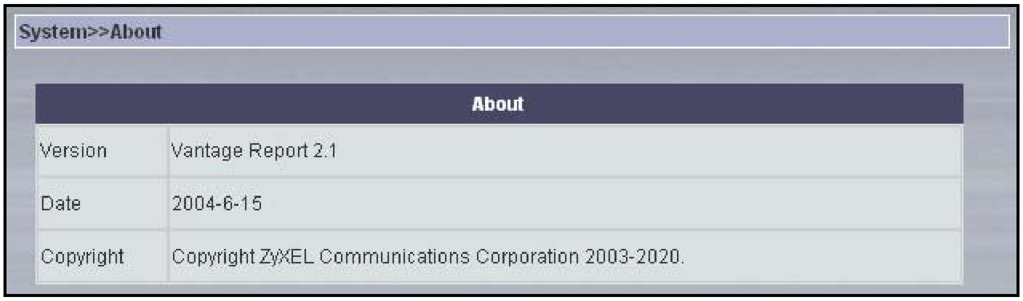
CSV Import

File Name:

30.4 About Reports

Use this screen to view version, date and copyright information about the Vantage reporting module. Click **Report, System, About** to display the next screen.

Figure 241 About Reports



System>>About

About

Version	Vantage Report 2.1
Date	2004-6-15
Copyright	Copyright ZyXEL Communications Corporation 2003-2020.

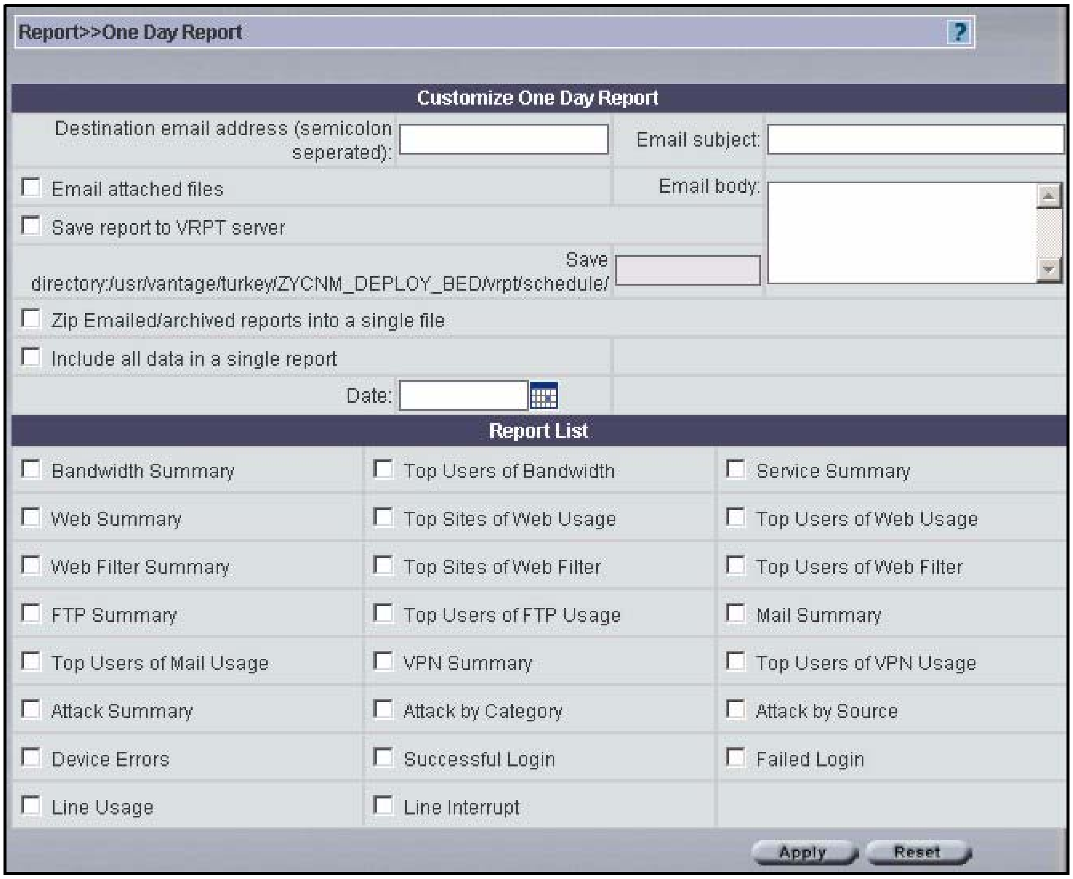
CHAPTER 31
Report

Use these screens to configure reports for a single day or multiple days to be e-mailed or saved in Vantage.

31.1 Daily Report

Use this screen to configure reports for a single day to be e-mailed or saved in Vantage. Click **Report, Report, Daily Report** to display the next screen.

Figure 242 Daily Reports



Report>>One Day Report

Customize One Day Report

Destination email address (semicolon seperated):

Email subject:

□ Email attached files

Email body:

□ Save report to VRPT server

Save directory:/usr/vantage/turkey/ZYCNM_DEPLOY_BED/vrpt/schedule/

□ Zip Emailed/archived reports into a single file

□ Include all data in a single report

Date:

Report List

□ Bandwidth Summary	□ Top Users of Bandwidth	□ Service Summary
□ Web Summary	□ Top Sites of Web Usage	□ Top Users of Web Usage
□ Web Filter Summary	□ Top Sites of Web Filter	□ Top Users of Web Filter
□ FTP Summary	□ Top Users of FTP Usage	□ Mail Summary
□ Top Users of Mail Usage	□ VPN Summary	□ Top Users of VPN Usage
□ Attack Summary	□ Attack by Category	□ Attack by Source
□ Device Errors	□ Successful Login	□ Failed Login
□ Line Usage	□ Line Interrupt	

Table 187 Daily Reports

LABEL	DESCRIPTION
Customize One Day Report	
Destination Email Address (Semicolon seperated):	Type e-mail addresses to where e-mailed reports should be sent separated by semicolons.
Email Subject:	Type a meaningful e-mail subject here.
Email Attached Files	Select this checkbox to have Vantage e-mail the attached reports.
Email Body:	Type a meaningful message that you want to appear in the e-mail body here.
Save Report to VRPT Server	Select this checkbox to save the selected reports within the Vantage server.
Save directory:/usr/vantage/ZYCNM_DEPLOY_BED/vrpt/schedule/	Type the name of the report here. The report will be saved to this path on the Vantage server.
Zip Emailed/Archived Reports into a Single File	Select this checkbox to zip selected reports into a single file when e-mailing them.
Include All Data In a Single Report	Select this checkbox to merge all selected reports into a single report when e-mailing them

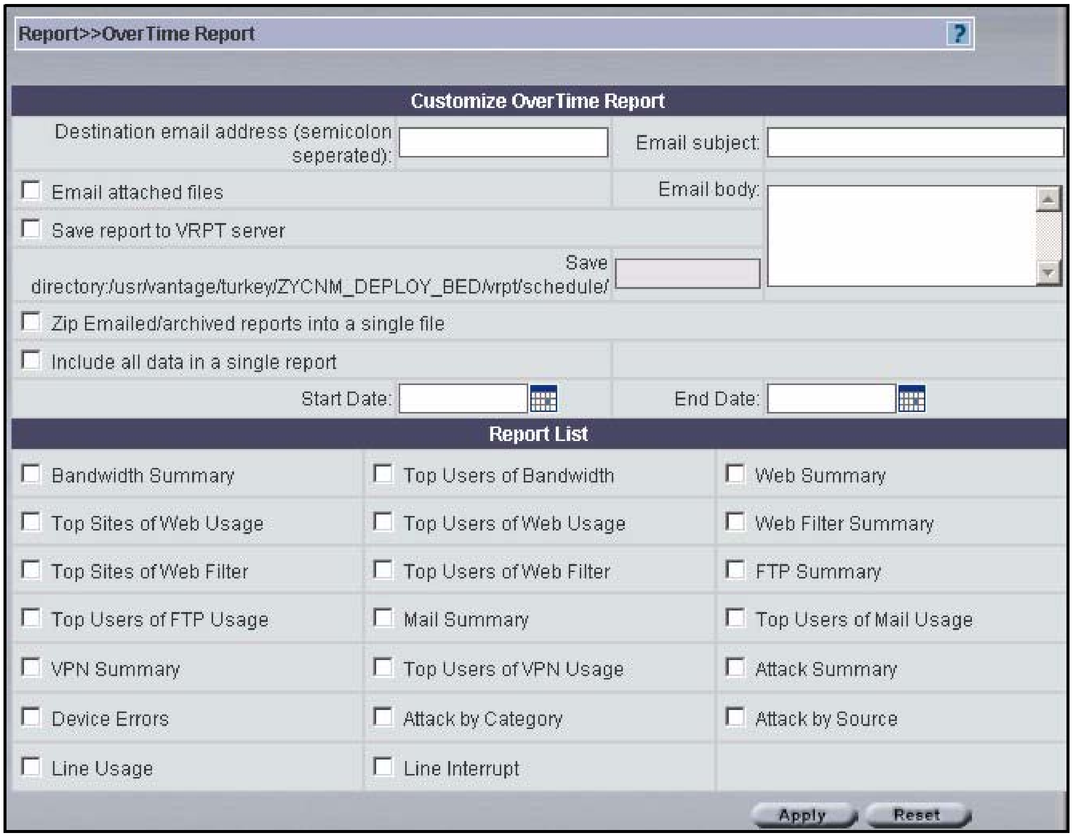
Table 187 Daily Reports (continued)

LABEL	DESCRIPTION
Date	Click the calendar icon to select a date for the report to be sent or manually enter the date in year-month-date format.
Report List	Select the report type from this list. Each report type corresponds to a report screen in Vantage.
Apply	Click **Apply** to save your changes and exit this screen.
Reset	Click **Reset** to begin configuring the screen afresh.

31.2 Over Time Report

Use this screen to configure reports for multiple days to be e-mailed or saved in Vantage. Click **Report, Report, Over Time Report** to display the next screen.

Figure 243 Over Time Report



Report>>OverTime Report

Customize OverTime Report

Destination email address (semicolon seperated):		Email subject:	
□ Email attached files		Email body:	
□ Save report to VRPT server			
Save directory:/usr/vantage/turkey/ZYCNM_DEPLOY_BED/vrpt/schedule/			
□ Zip Emailed/archived reports into a single file			
□ Include all data in a single report			
Start Date:		End Date:	

Report List

□ Bandwidth Summary	□ Top Users of Bandwidth	□ Web Summary
□ Top Sites of Web Usage	□ Top Users of Web Usage	□ Web Filter Summary
□ Top Sites of Web Filter	□ Top Users of Web Filter	□ FTP Summary
□ Top Users of FTP Usage	□ Mail Summary	□ Top Users of Mail Usage
□ VPN Summary	□ Top Users of VPN Usage	□ Attack Summary
□ Device Errors	□ Attack by Category	□ Attack by Source
□ Line Usage	□ Line Interrupt	

Table 188 Over Time Report

LABEL	DESCRIPTION
Customize Over Time Report	
Destination Email Address (Semicolon seperated):	Type e-mail addresses to where e-mailed reports should be sent separated by semicolons.
Email Subject:	Type a meaningful e-mail subject here.
Email Attached Files	Select this checkbox to have Vantage e-mail the attached reports.
Email Body:	Type a meaningful message that you want to appear in the e-mail body here.
Save Report to VRPT Server	Select this checkbox to save the selected reports within the Vantage server.
Save directory:/usr/vantage/ ZYCNM_DEPLOY_BED/vrpt/ schedule/	The reports will be saved to this path on the Vantage server.
Zip Emailed/Archived Reports into a Single File	Select this checkbox to zip selected reports into a single file when e-mailing them.
Include All Data In a Single Report	Select this checkbox to merge all selected reports into a single report when e-mailing them
Start Date	Click the calendar icon to select a beginning year-month-date or manually enter the date in year-month-date format.

Table 188 Over Time Report (continued)

LABEL	DESCRIPTION
End Date	Click the calendar icon to select an ending year-month-date or manually enter the date in year-month-date format. The end date must come after the start date but not after the current date.
Report List	Select the report type from this list. Each report type corresponds to a report screen in Vantage.
Apply	Click **Apply** to save your changes and exit this screen.
Reset	Click **Reset** to begin configuring the screen afresh.

APPENDIX A
FTP Server (WFTPD) Setup Example

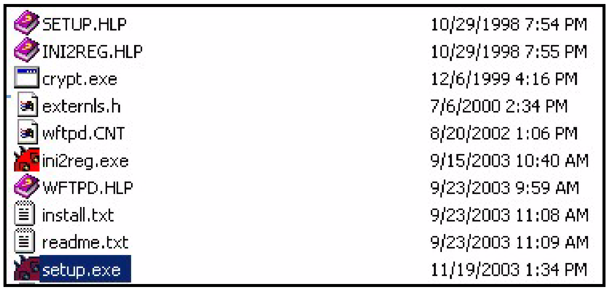
This appendix applies to the Windows version of Vantage CNM.

Installing WFTPD

1 Download the WFTPD software from www.wftpd.com to where you want to install it.

2 Double-click **setup.exe** to begin the wizard.

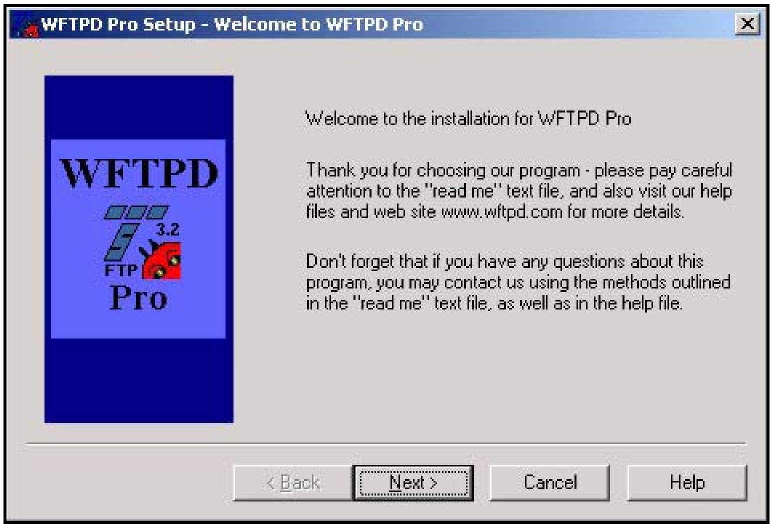
Figure 244 Setup



SETUP.HLP	10/29/1998 7:54 PM
INI2REG.HLP	10/29/1998 7:55 PM
crypt.exe	12/6/1999 4:16 PM
externls.h	7/6/2000 2:34 PM
wftpd.CNT	8/20/2002 1:06 PM
ini2reg.exe	9/15/2003 10:40 AM
WFTPD.HLP	9/23/2003 9:59 AM
install.txt	9/23/2003 11:08 AM
readme.txt	9/23/2003 11:09 AM
setup.exe	11/19/2003 1:34 PM

3 Click **Next** to begin and then follow the wizard prompts.

Figure 245 Wizard 1



WFTPD Pro Setup - Welcome to WFTPD Pro

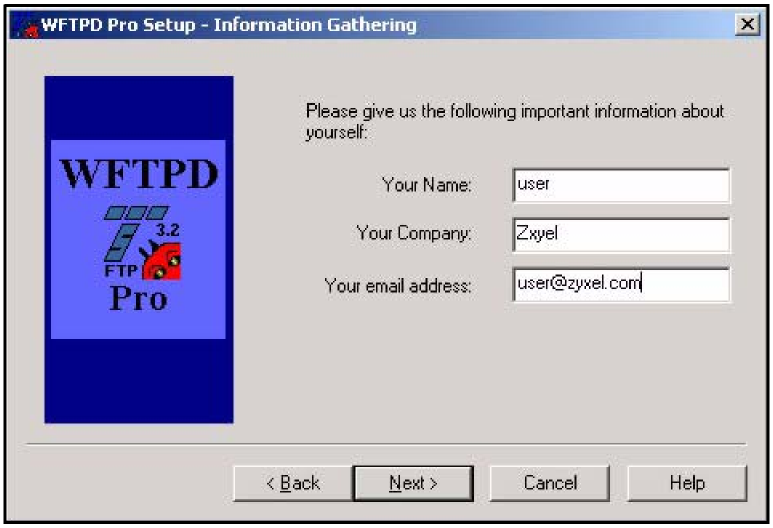
Welcome to the installation for WFTPD Pro

Thank you for choosing our program - please pay careful attention to the "read me" text file, and also visit our help files and web site www.wftpd.com for more details.

Don't forget that if you have any questions about this program, you may contact us using the methods outlined in the "read me" text file, as well as in the help file.

4 Enter your details here as shown and click **Next.**

Figure 246 Information



WFTPD Pro Setup - Information Gathering

Please give us the following important information about yourself:

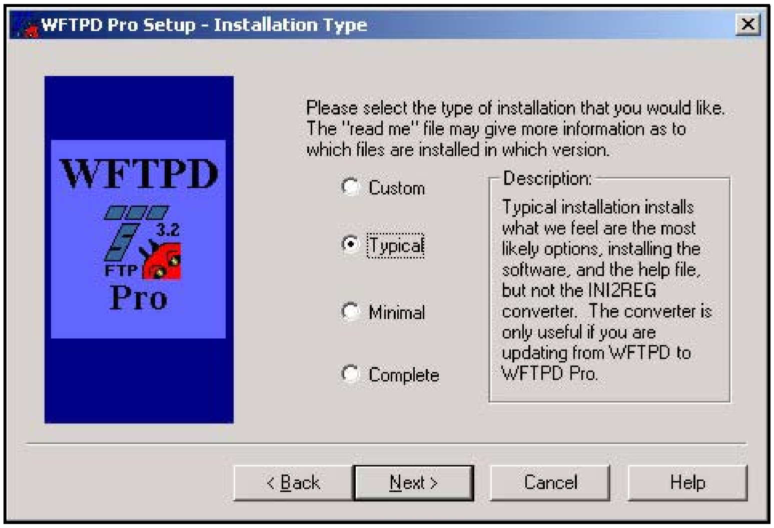
Your Name: user

Your Company: Zxyel

Your email address: user@zyxel.com

5 Select the installation type and click **Next**.

Figure 247 Installation Type



WFTPD Pro Setup - Installation Type

Please select the type of installation that you would like. The "read me" file may give more information as to which files are installed in which version.

○ Custom

● Typical

○ Minimal

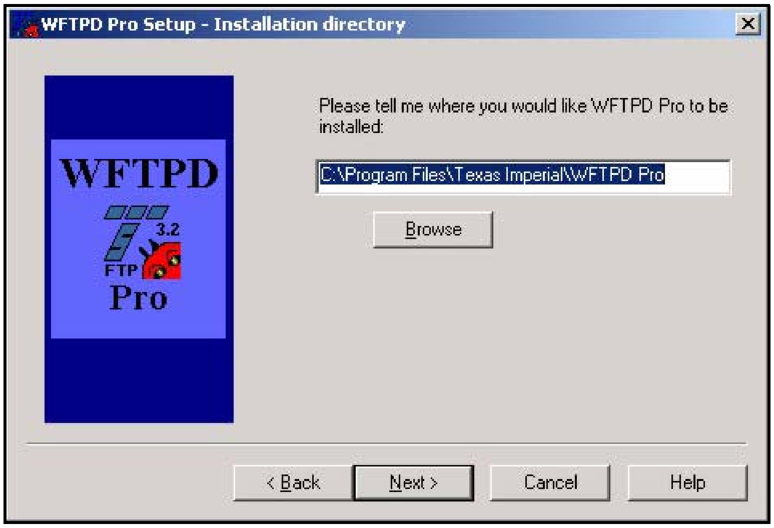
○ Complete

Description:

Typical installation installs what we feel are the most likely options, installing the software, and the help file, but not the INI2REG converter. The converter is only useful if you are updating from WFTPD to WFTPD Pro.

6 Select where to install WFTPD Pro and click **Next**.

Figure 248 Installation Directory



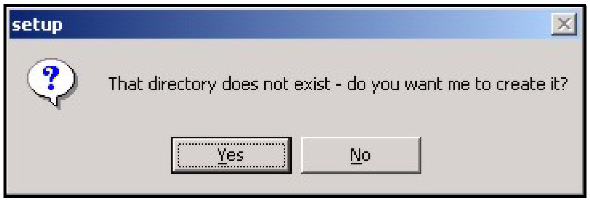
WFTPD Pro Setup - Installation directory

Please tell me where you would like WFTPD Pro to be installed:

C:\Program Files\Texas Imperial\WFTPD Pro

7 You are prompted to create the directory if it doesn't already exist. Click **Yes** to create a new directory.

Figure 249 Create Directory

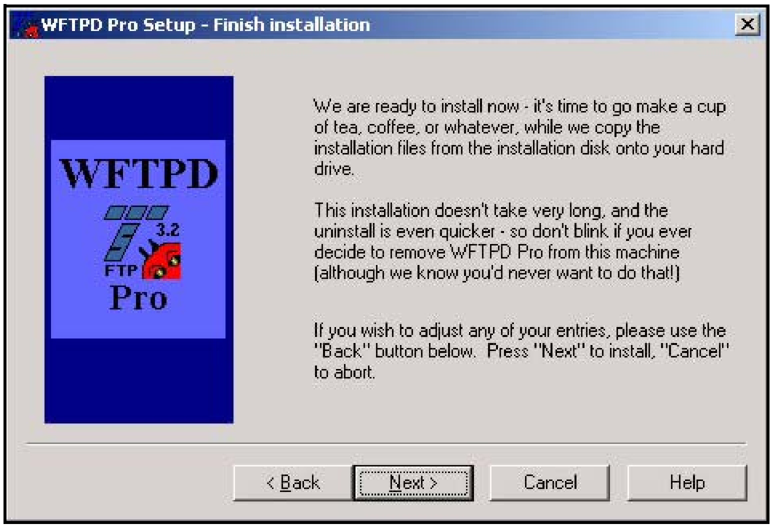


setup

That directory does not exist - do you want me to create it?

8 Click **Next** to begin the installation.

Figure 250 Begin Installation



WFTPD Pro Setup - Finish installation

We are ready to install now - it's time to go make a cup of tea, coffee, or whatever, while we copy the installation files from the installation disk onto your hard drive.

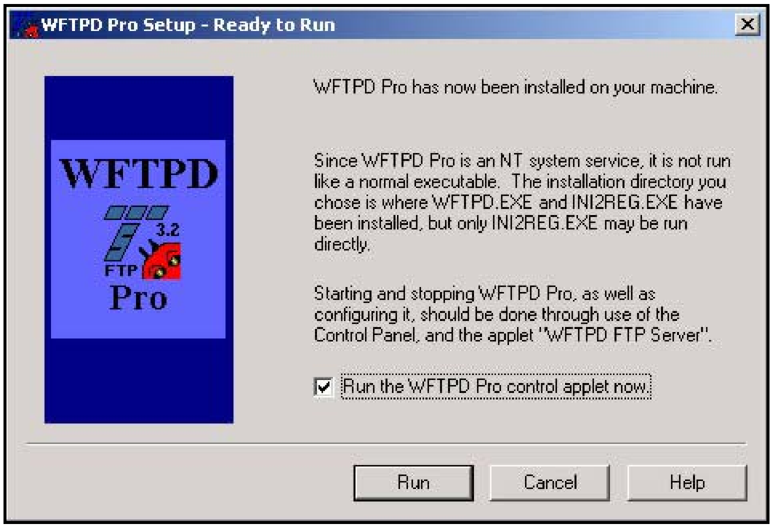
This installation doesn't take very long, and the uninstall is even quicker - so don't blink if you ever decide to remove WFTPD Pro from this machine (although we know you'd never want to do that!)

If you wish to adjust any of your entries, please use the "Back" button below. Press "Next" to install, "Cancel" to abort.

9 WFTPD has been installed. Click **Run** to start it. Make sure the check box is selected.

Running WFTPD

Figure 251 Run WFTPD



WFTPD Pro has now been installed on your machine.

Since WFTPD Pro is an NT system service, it is not run like a normal executable. The installation directory you chose is where WFTPD.EXE and INI2REG.EXE have been installed, but only INI2REG.EXE may be run directly.

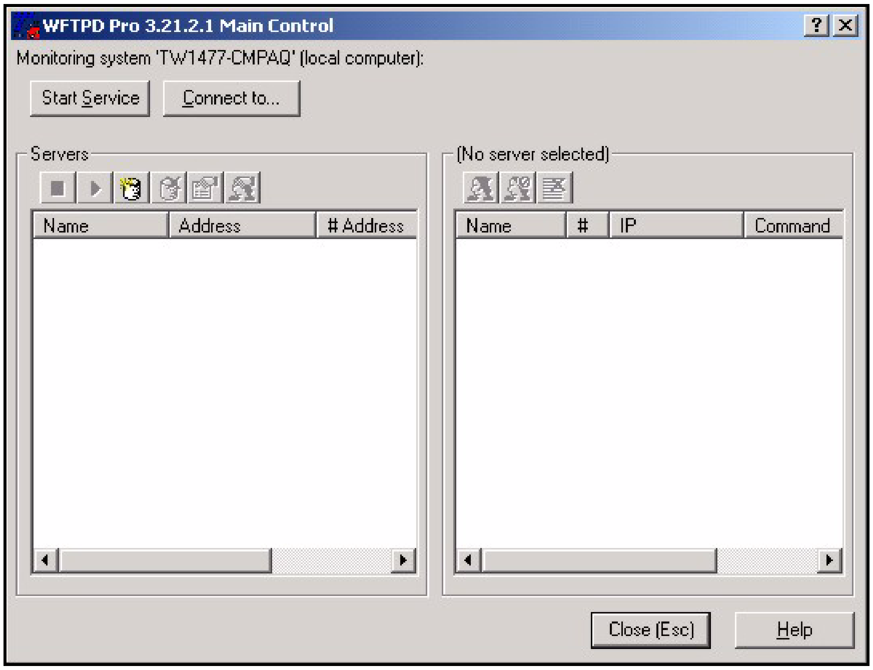
Starting and stopping WFTPD Pro, as well as configuring it, should be done through use of the Control Panel, and the applet "WFTPD FTP Server".

☑ Run the WFTPD Pro control applet now.

10 Click **Start Service** form the WFTPD main screen.

WFTPD Main Screen

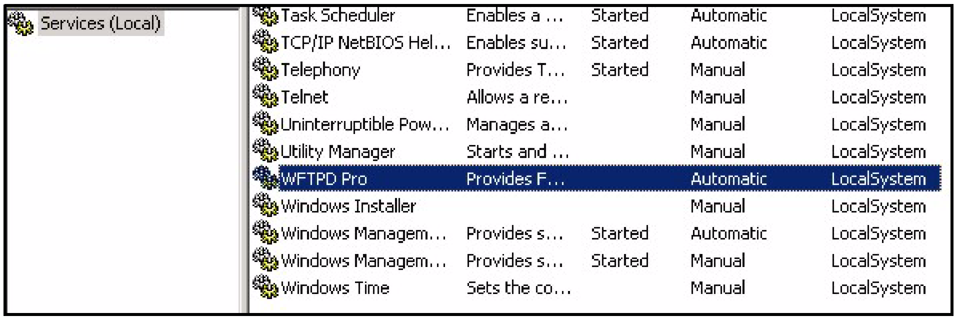
Figure 252 WFTPD Main Screen



Monitoring system 'TW1477-CMPAQ' (local computer):

11 Open **Administrative Tools** in the Windows **Control Panel** and then select **Services** to see the WFTPD Pro service.

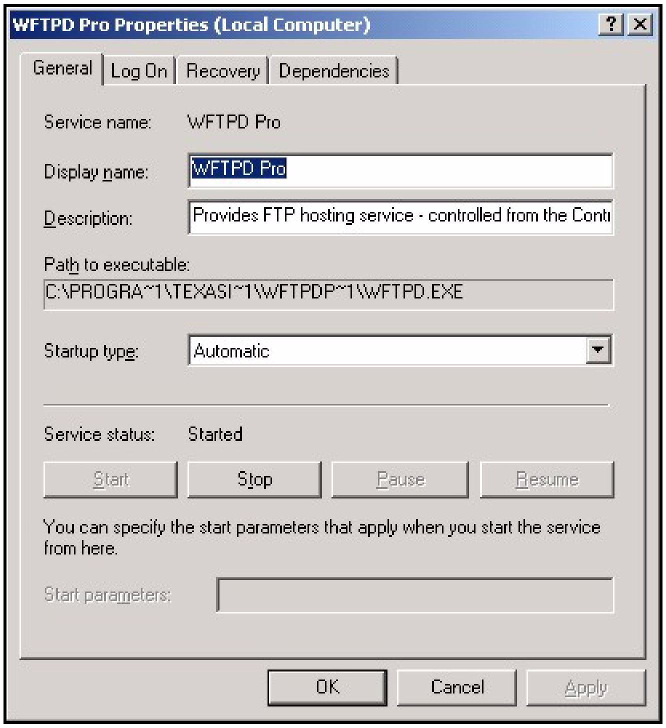
Figure 253   Windows Services



Task Scheduler	Enables a ...	Started	Automatic	LocalSystem
TCP/IP NetBIOS Hel...	Enables su...	Started	Automatic	LocalSystem
Telephony	Provides T...	Started	Manual	LocalSystem
Telnet	Allows a re...		Manual	LocalSystem
Uninterruptible Pow...	Manages a...		Manual	LocalSystem
Utility Manager	Starts and ...		Manual	LocalSystem
WFTPD Pro	Provides F...		Automatic	LocalSystem
Windows Installer			Manual	LocalSystem
Windows Managem...	Provides s...	Started	Automatic	LocalSystem
Windows Managem...	Provides s...	Started	Manual	LocalSystem
Windows Time	Sets the co...		Manual	LocalSystem

12 Right-click **WFTPD Pro** service and then click **Properties**.

Figure 254   WFTPD Properties



Service name: WFTPD Pro

Display name: WFTPD Pro

Description: Provides FTP hosting service - controlled from the Conti

Path to executable:
C:\PROGRA~1\TEXASI~1\WFTPDP~1\WFTPD.EXE

Startup type: Automatic

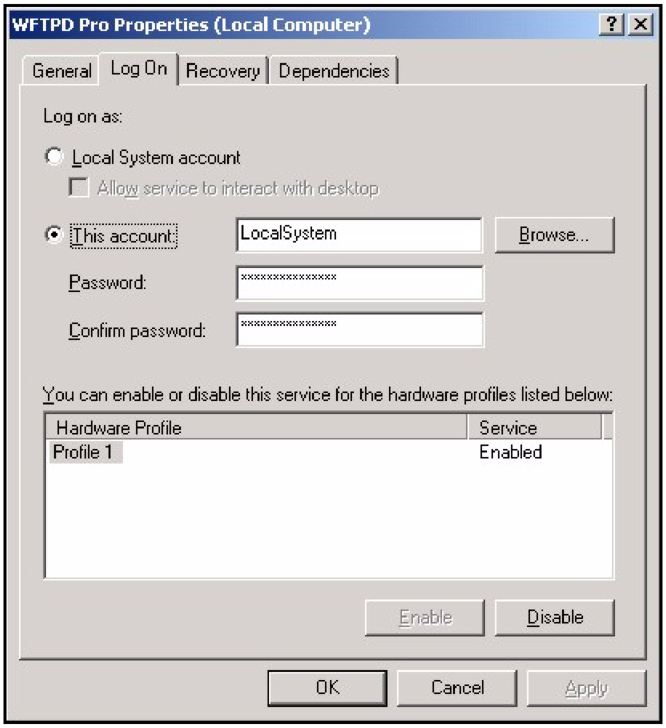
Service status: Started

You can specify the start parameters that apply when you start the service from here.

Start parameters:

13 Click the **Log On** tab to configure a user name and password for this server. This must be the same username and password that you use in Vantage.

Figure 255 WFTPD Pro Log On



Log on as:

○ Local System account

□ Allow service to interact with desktop

● This account: LocalSystem

Password: ***************

Confirm password: ***************

You can enable or disable this service for the hardware profiles listed below:

Hardware Profile	Service
Profile 1	Enabled

APPENDIX B
Configuring the Kiwi Syslog Daemon

This appendix applies to the Windows version of Vantage CNM.

This section shows you how to install and configure the KiWi Syslog Daemon for use with Vantage CNM.

Note: If you already have a Kiwi Syslog Daemon installed, you can modify the "Syslog Daemon Settings.ini" text file before you import it to the Kiwi Syslog Daemon. See the Vantage CNM release notes for information on how to do this.

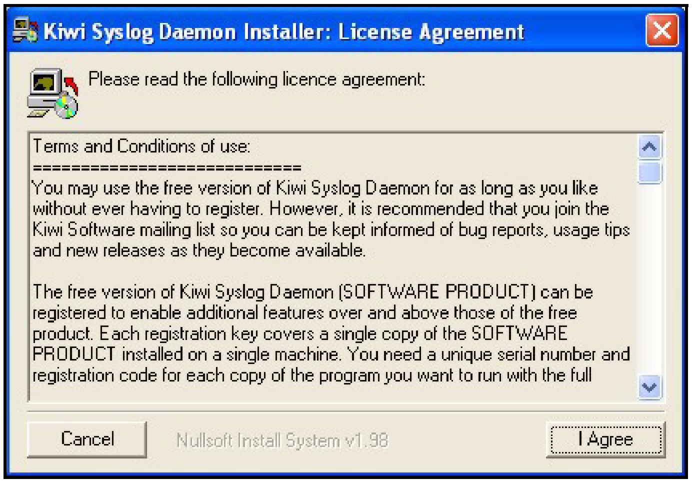
Installing the Kiwi Syslog Daemon

Follow the steps below to install the KiWi. Syslog Daemon

1 Download the latest version of the KiWi Syslog Daemon from www.kiwisyslog.com to your computer.

2 Double-click on the setup program. A screen displays as shown. Click **I Agree** to accept the license agreement.

Figure 256 Kiwi Syslog Daemon Installation: License Agreement



Kiwi Syslog Daemon Installer: License Agreement

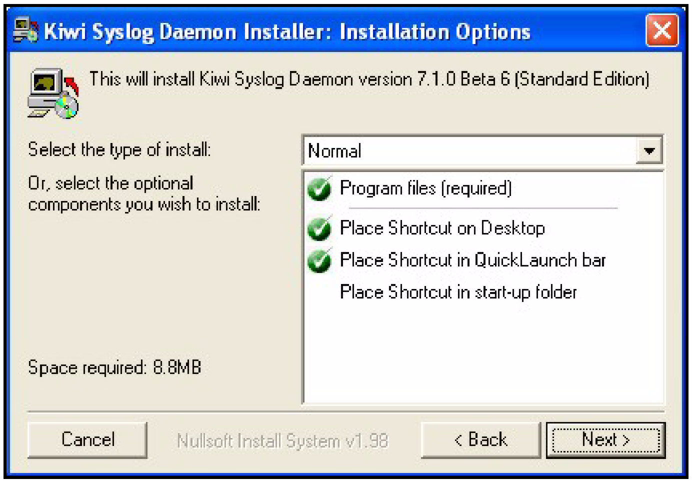
Please read the following licence agreement:

Terms and Conditions of use:
============================
You may use the free version of Kiwi Syslog Daemon for as long as you like without ever having to register. However, it is recommended that you join the Kiwi Software mailing list so you can be kept informed of bug reports, usage tips and new releases as they become available.

The free version of Kiwi Syslog Daemon (SOFTWARE PRODUCT) can be registered to enable additional features over and above those of the free product. Each registration key covers a single copy of the SOFTWARE PRODUCT installed on a single machine. You need a unique serial number and registration code for each copy of the program you want to run with the full

3 Select the installation type (the default is **Normal**) and click **Next**.

Figure 257 Kiwi Installation: Installation Options



Kiwi Syslog Daemon Installer: Installation Options

This will install Kiwi Syslog Daemon version 7.1.0 Beta 6 (Standard Edition)

Select the type of install: Normal

Or, select the optional components you wish to install:

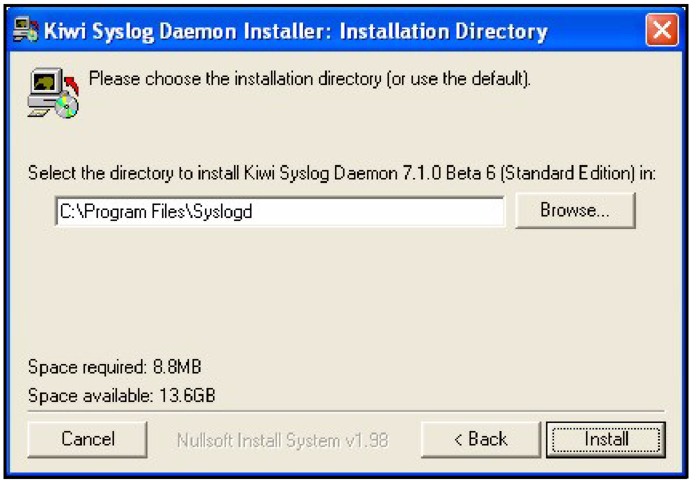
- ☑ Program files (required)
- ☑ Place Shortcut on Desktop
- ☑ Place Shortcut in QuickLaunch bar
- Place Shortcut in start-up folder

Space required: 8.8MB

4 Click **Install** to install Kiwi to the default directory.

Note: Make sure that the directory you install Kiwi is the same as the directory in the **System Log Path** field in the Vantage CNM **System > Preferences > Server** screen.

Figure 258 Kiwi Installation: Installation Directory



Kiwi Syslog Daemon Installer: Installation Directory

Please choose the installation directory (or use the default).

Select the directory to install Kiwi Syslog Daemon 7.1.0 Beta 6 (Standard Edition) in:

C:\Program Files\Syslogd

Space required: 8.8MB

Space available: 13.6GB

Wait before the installation process completes.

Importing the Syslog Configuration File

After installing the Kiwi Syslog Daemon, follow the steps below to import the configuration file.

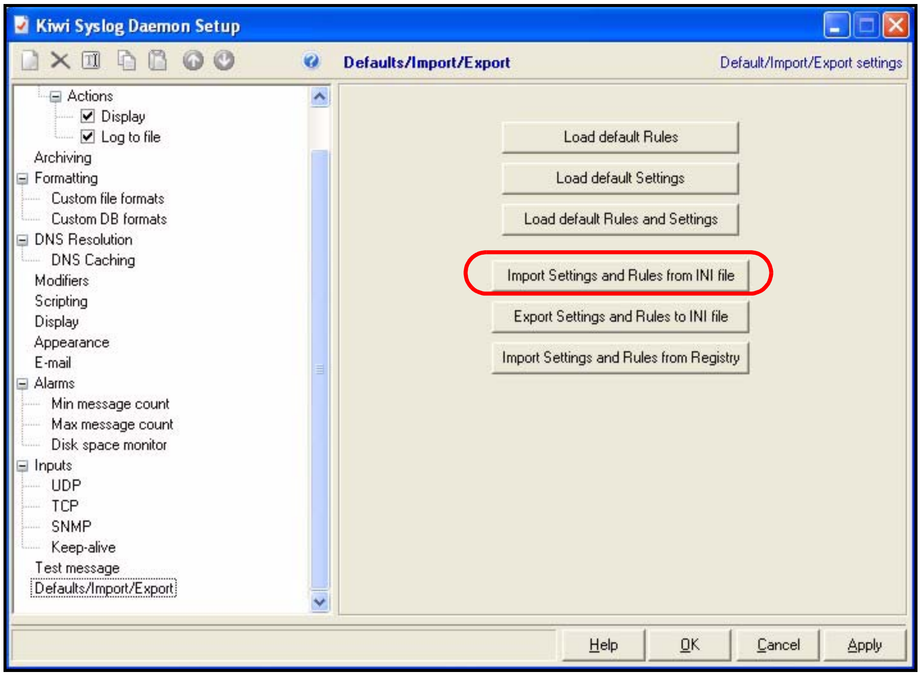
1 Copy and save the "Syslog Daemon Settings.ini" file to your computer.

2 Start the Kiwi Syslog Daemon. In the main Kiwi Syslog Daemon screen, click **File**, **Setup**. A screen displays as shown.

3 Click **Defaults/Import/Export** under **Inputs**.

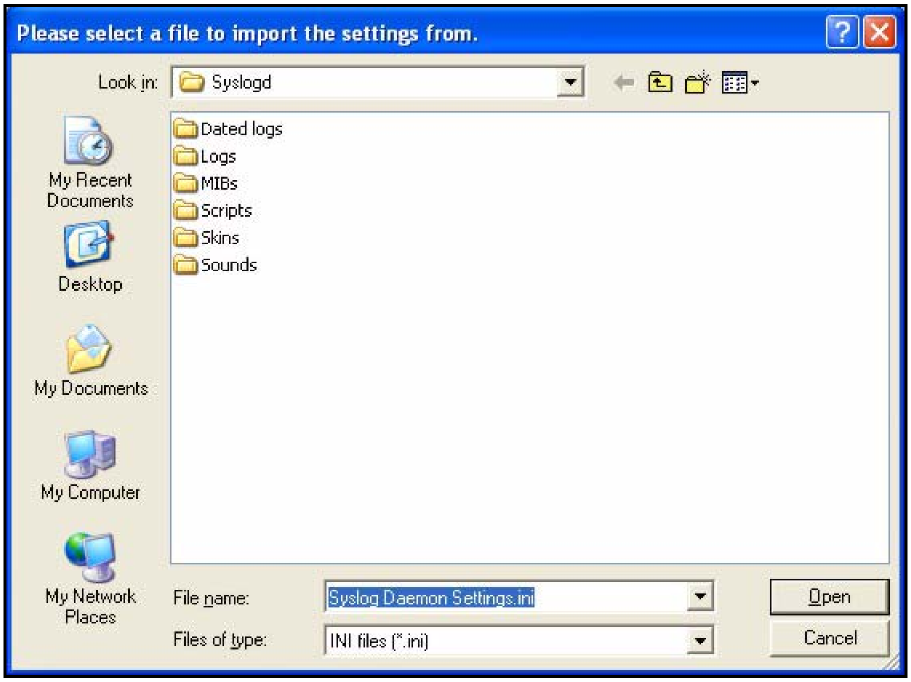
4 Click **Import Settings and Rules from INI file**.

Figure 259 Kiwi Syslog Daemon Setup



5 Locate the “.ini” syslog configuration file you saved to your computer in step 1 and click **Open**.

Figure 260 Kiwi Syslog Daemon Setup: Import Configuration File



Look in: Syslogd

File name: Syslog Daemon Settings.ini

Files of type: INI files (*.ini)

6 Click **Yes** to confirm the configuration file import.

7 In the **Kiwi Syslog Daemon Setup** screen, click **Apply** and then **OK** to close the screen.

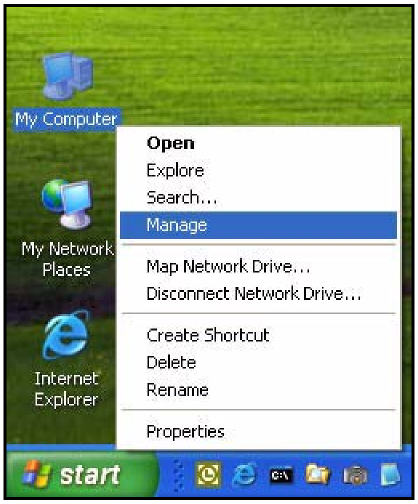
Note: You must start the Telnet service on the computer you install Kiwi.

Starting the Telnet Service

Follow the steps below to activate Telnet service for syslog logging on the computer you install Kiwi.

1 Right-click on **My Computer** on the desktop and click **Manage**.

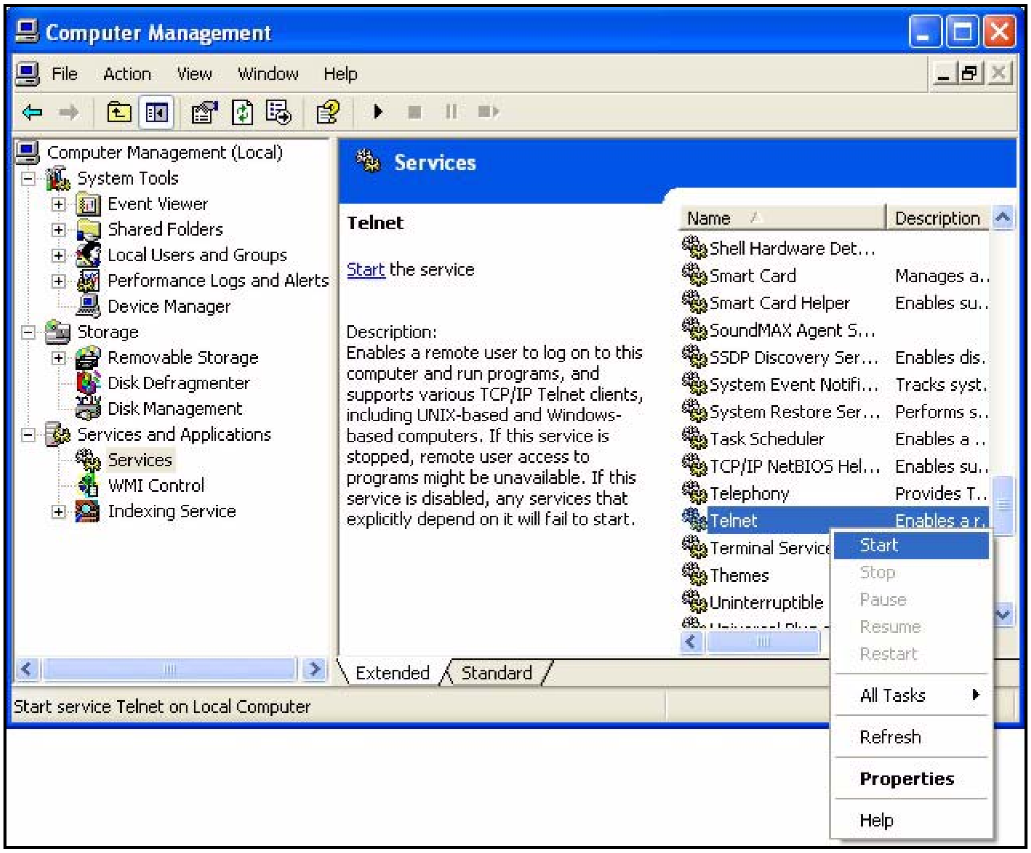
Figure 261 Windows XP: My Computer



2 A **Computer Management** screen displays as shown next. Click **Services** under **Services and Applications** on the left panel.

3 Search for the Telnet service on the right panel (you may have to scroll down the screen). Right-click on **Telnet** and click **Start** to start the Telnet service.

Figure 262 Windows XP: Computer Management



Description:
Enables a remote user to log on to this computer and run programs, and supports various TCP/IP Telnet clients, including UNIX-based and Windows-based computers. If this service is stopped, remote user access to programs might be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

Start service Telnet on Local Computer

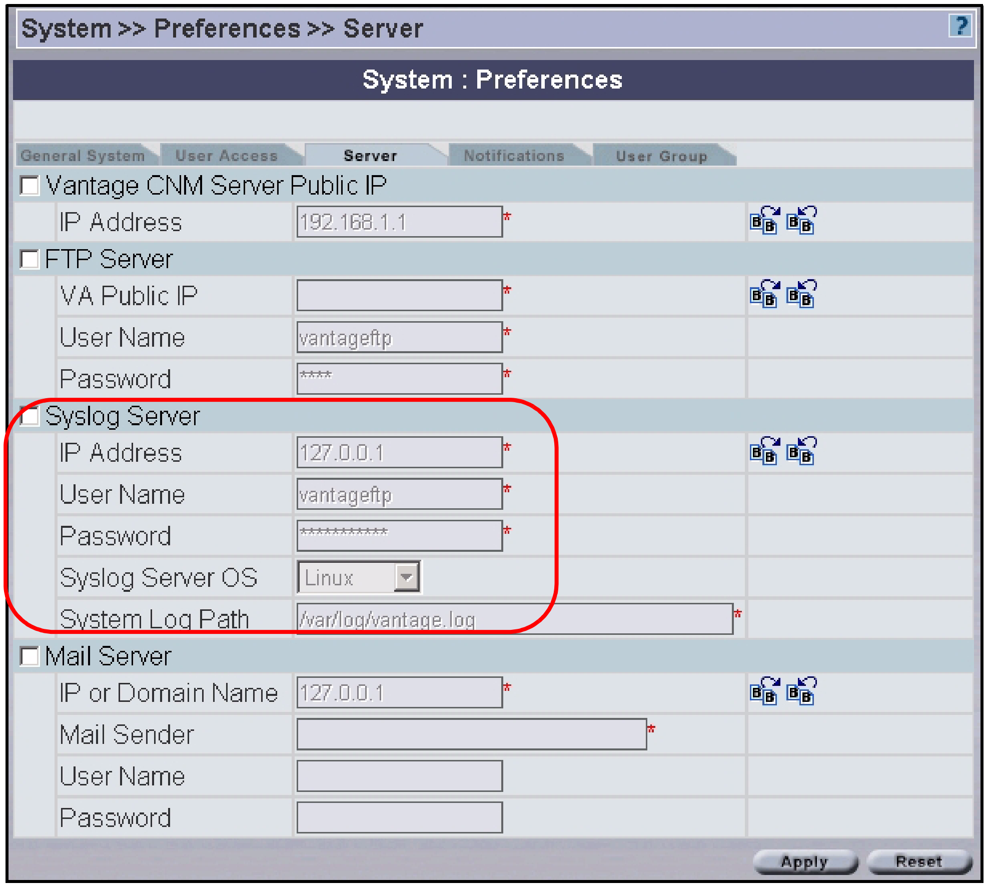
After you have installed and configure the Kiwi Syslog Daemon and started the Telnet service on the computer, configure the syslog settings in Vantage CNM. Set the syslog server username and password to be the same as the Windows username and password in the Vantage system **Server** screen.

Setting Up the Syslog Server in Vantage

1 Log in to Vantage using the root account.

2 Go to **System>Preferences>Server** screen.

Figure 263 Vantage System Servers



System >> Preferences >> Server

System : Preferences

☐ Vantage CNM Server Public IP	
IP Address	192.168.1.1 *
☐ FTP Server	
VA Public IP	*
User Name	vantageftp *
Password	**** *
☐ Syslog Server	
IP Address	127.0.0.1 *
User Name	vantageftp *
Password	*********** *
Syslog Server OS	Linux
System Log Path	/var/log/vantage.log *
☐ Mail Server	
IP or Domain Name	127.0.0.1 *
Mail Sender	*
User Name	
Password	

3 Select **Syslog Server** and enter the IP address of the computer on which you installed the Syslog server and the user name and password that you configured.

4 Click **Apply**.

APPENDIX C
Pop-up Windows, JavaScripts and Java Permissions

This appendix applies to the Windows version of Vantage CNM.

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.

Internet Explorer Pop-up Blockers

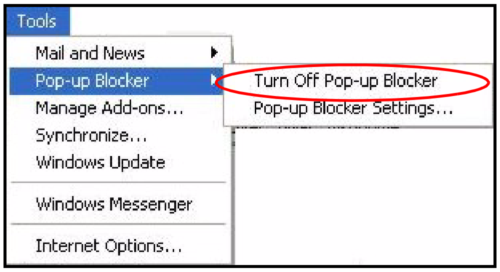
You may have to disable pop-up blocking to log into your device and to display the VPN graphic editor screen.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

Disable pop-up Blockers

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

Figure 264 Pop-up Blocker

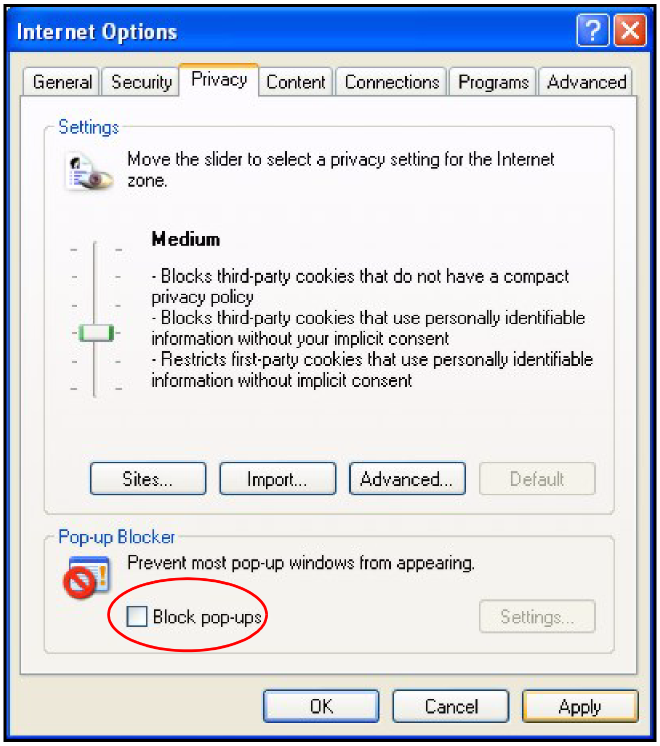


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

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 265 Internet Options



Move the slider to select a privacy setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

Prevent most pop-up windows from appearing.

□ Block pop-ups

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

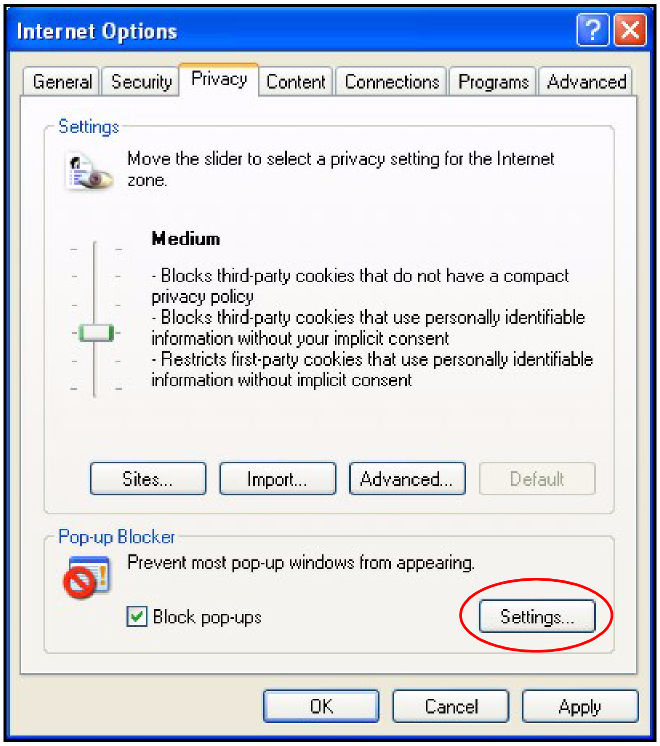
Enable pop-up Blockers with Exceptions

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

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings…**to open the **Pop-up Blocker Settings** screen.

Figure 266 Internet Options



Internet Options

Settings

Move the slider to select a privacy setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

Pop-up Blocker

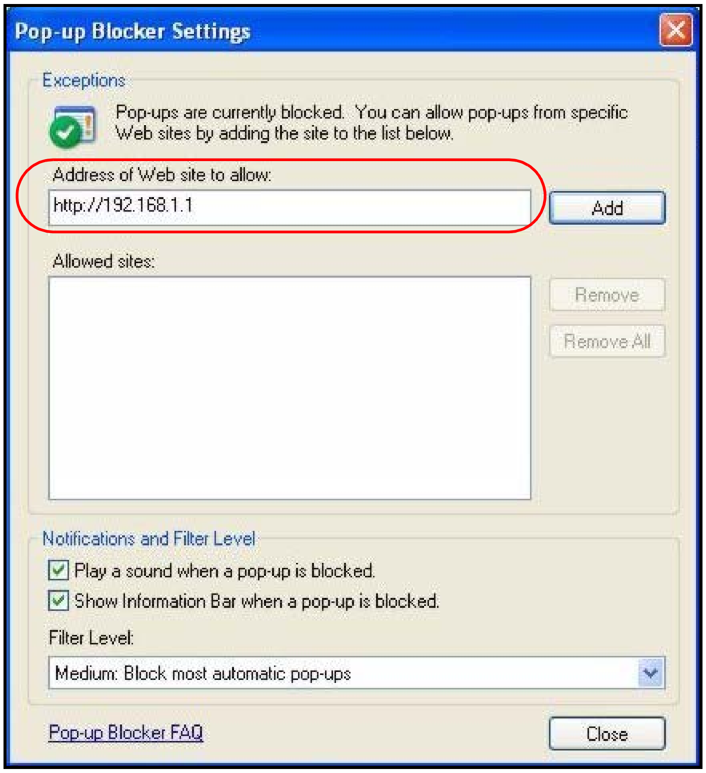
Prevent most pop-up windows from appearing.

☑ Block pop-ups

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 267 Pop-up Blocker Settings



Pop-ups are currently blocked. You can allow pop-ups from specific Web sites by adding the site to the list below.

Address of Web site to allow: http://192.168.1.1

☑ Play a sound when a pop-up is blocked.

☑ Show Information Bar when a pop-up is blocked.

Filter Level: Medium: Block most automatic pop-ups

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

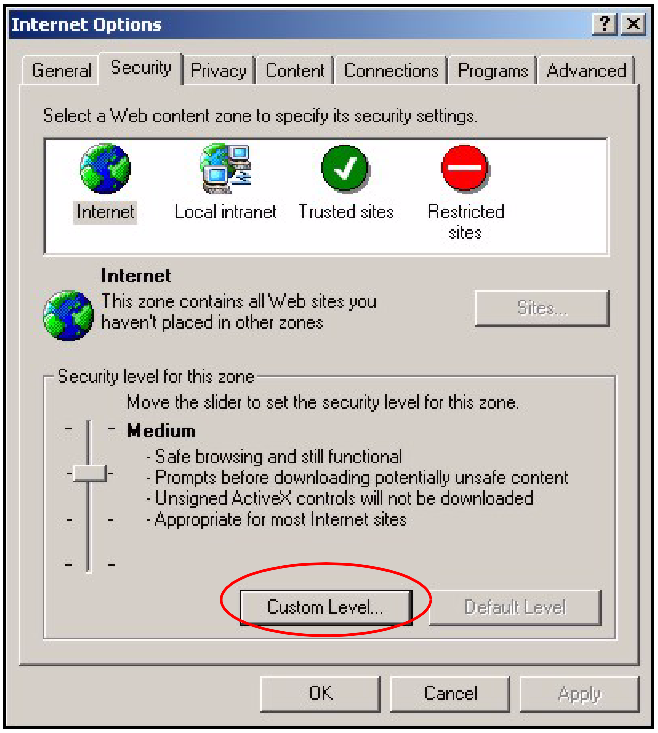
6 Click **Apply** to save this setting.

JavaScripts

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

Figure 268 Internet Options



Select a Web content zone to specify its security settings.

Internet

This zone contains all Web sites you haven't placed in other zones

Security level for this zone

Move the slider to set the security level for this zone.

Medium

- Safe browsing and still functional
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded
- Appropriate for most Internet sites

2 Click the **Custom Level...** button.

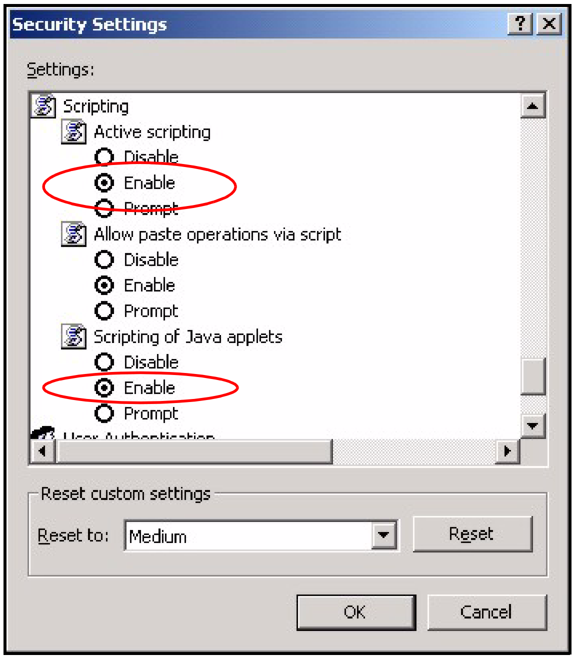
3 Scroll down to **Scripting**.

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 269 Security Settings - Java Scripting



Settings:

Scripting

Active scripting
○ Disable
● Enable
○ Prompt

Allow paste operations via script
○ Disable
● Enable
○ Prompt

Scripting of Java applets
○ Disable
● Enable
○ Prompt

User Authentication

Reset to: Medium

Java Permissions

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

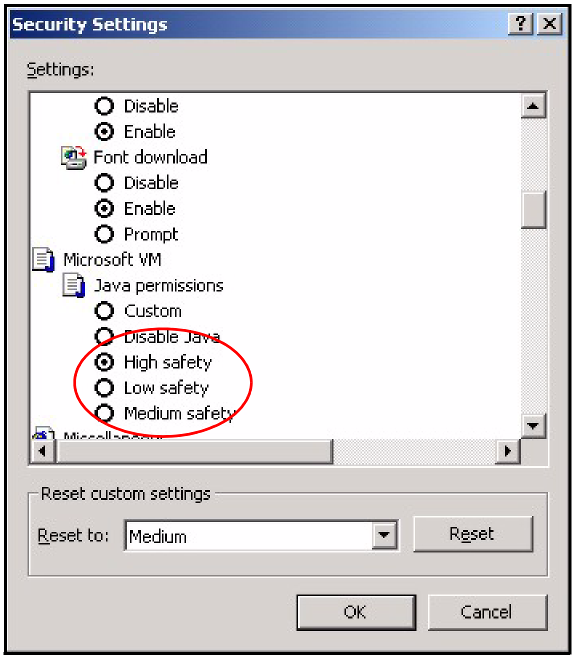
2 Click the **Custom Level...** button.

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 270 Security Settings - Java



Settings:

- ○ Disable
- ● Enable
- Font download
  - ○ Disable
  - ● Enable
  - ○ Prompt
- Microsoft VM
  - Java permissions
    - ○ Custom
    - ○ Disable Java
    - ● High safety
    - ○ Low safety
    - ○ Medium safety

Reset custom settings

Reset to: Medium

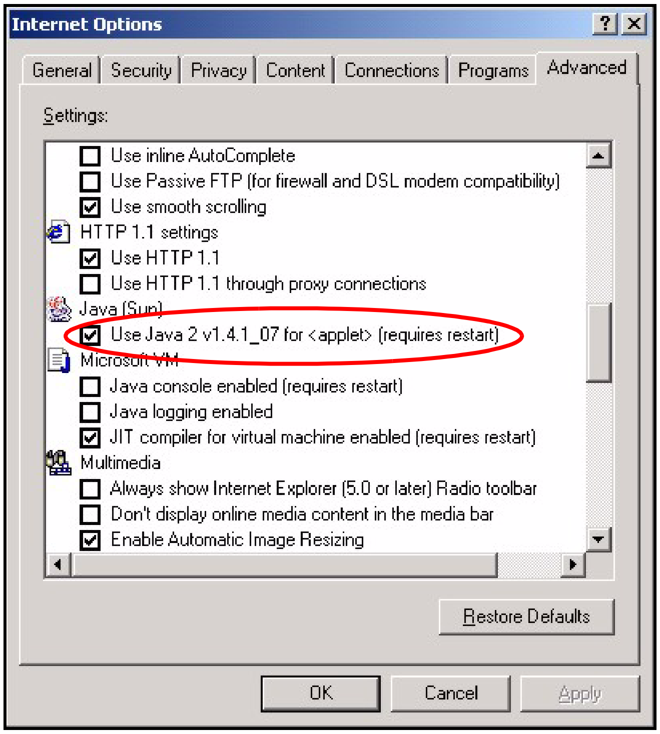
JAVA (Sun)

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 271 Java (Sun)



Settings:

- □ Use inline AutoComplete
- □ Use Passive FTP (for firewall and DSL modem compatibility)
- ☑ Use smooth scrolling

HTTP 1.1 settings

- ☑ Use HTTP 1.1
- □ Use HTTP 1.1 through proxy connections

Java (Sun)

- ☑ Use Java 2 v1.4.1_07 for <applet> (requires restart)

Microsoft VM

- □ Java console enabled (requires restart)
- □ Java logging enabled
- ☑ JIT compiler for virtual machine enabled (requires restart)

Multimedia

- □ Always show Internet Explorer (5.0 or later) Radio toolbar
- □ Don't display online media content in the media bar
- ☑ Enable Automatic Image Resizing

APPENDIX D
FTP and syslog Server Overview

Introduction

The following graphic displays the Vantage server, syslog server and FTP server interrelationships.Any combination of these servers (or all three) may be on the same computer..

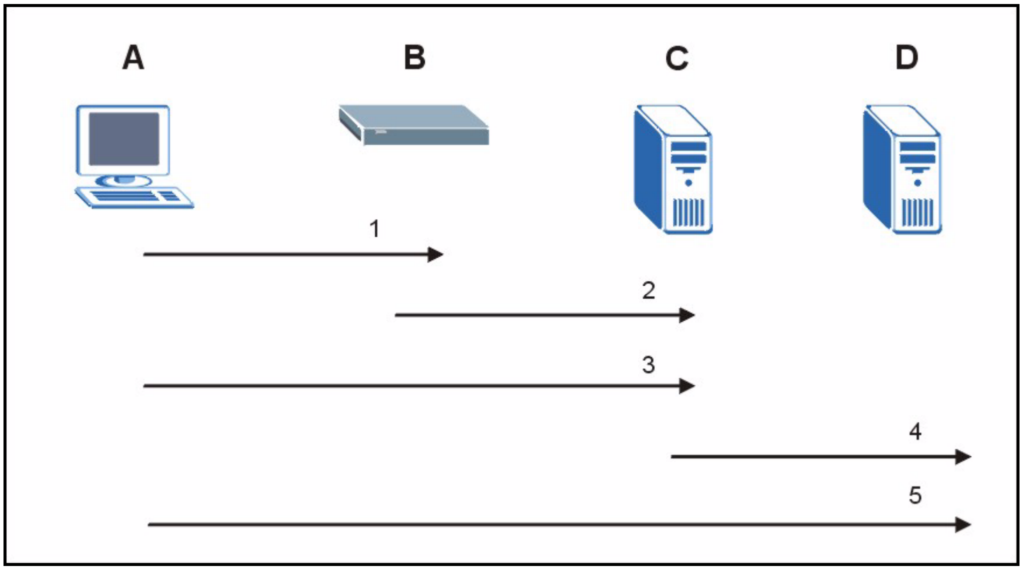


Table 189 FTP and syslog Server Overview

LABEL	DESCRIPTION
A	This is the Vantage CNM server.
B	This is any ZyXEL device.
C	This is a syslog server
D	This is an FTP server
1	Vantage sends syslog and FTP information for those servers to the device when you register the device with Vantage.
2	The syslog server must receive the log at local facility C[a] and then writes the log file to /var/log/vantage.log.
3	Vantage communicates with the syslog server using Telnet if Vantage is installed on Windows XP Professional and using SSH (SecureSHell) if Vantage is installed on Redhat Linux 9.0. In either case, you need a Telnet account with a username and password.

Table 189 FTP and syslog Server Overview

LABEL	DESCRIPTION
4	After a successful communication link has been established between Vantage and the syslog server, Vantage instructs the syslog server to send the vantage.log (ZyXEL devices’ logs) from the syslog server to an FTP server for retrieval.
5	Vantage uses the FTP protocol to retrieve the vantage.log (ZyXEL devices’ logs) from the FTP server.

[a] This is how it works at the time of writing.

Note: Vantage instructs the syslog server to send the vantage.log (ZyXEL devices’ logs) from the syslog server to an FTP server for retrieval once every ten minutes, see note a.

APPENDIX E
Java Console Debug Messages

This appendix applies to the Windows version of Vantage CNM.

Introduction

If you have problems with Vantage, customer support may ask you to find Java console debug messages. This appendix shows you how to do this.

1 Click **Start**, **Control Panel** and double-click on **Java Plug-in**.

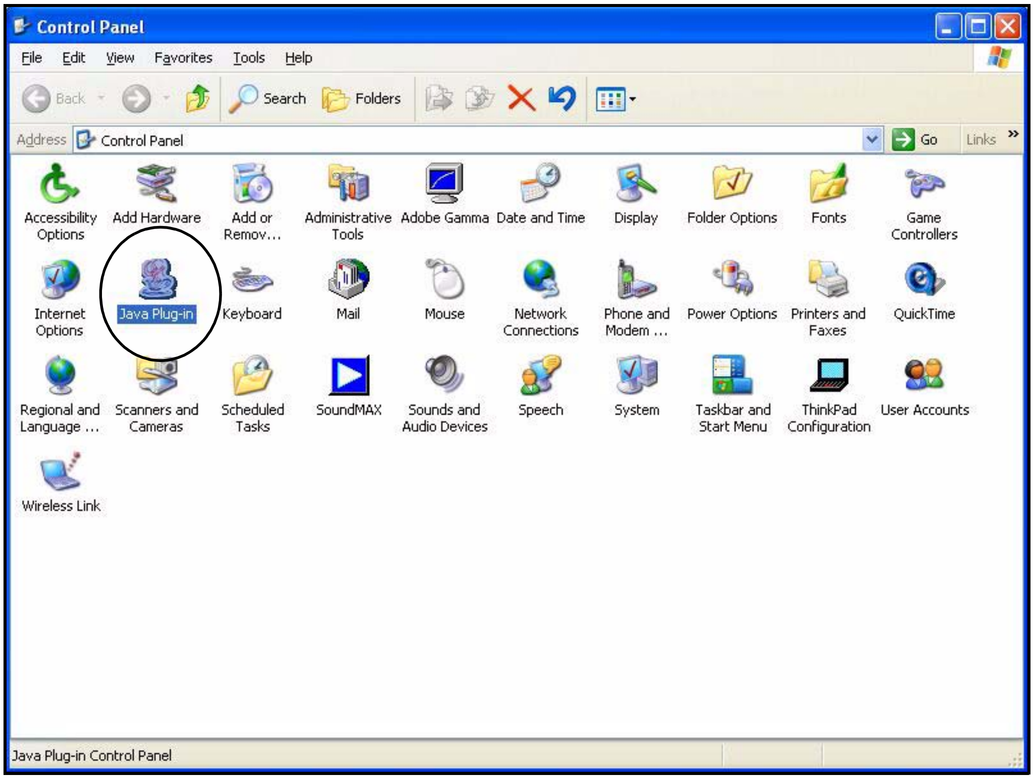
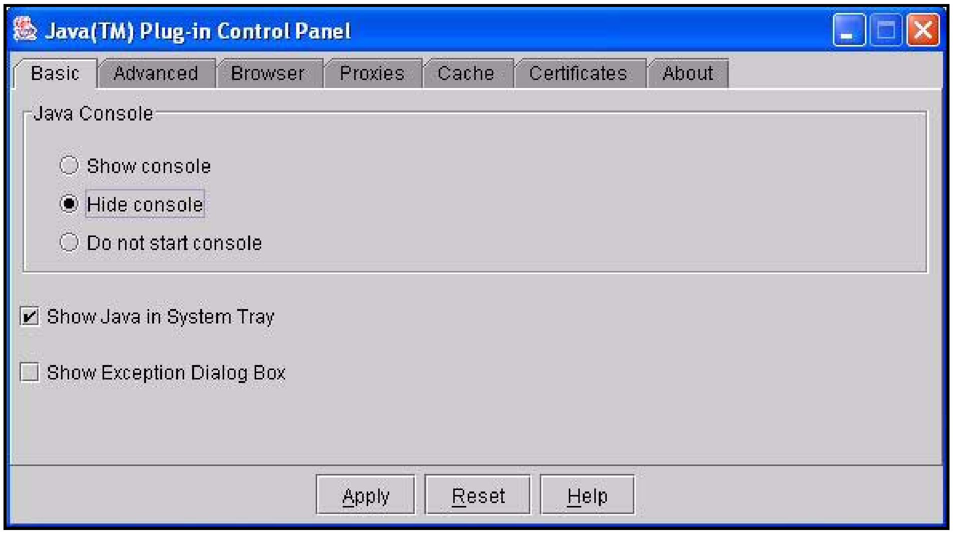


Figure 272 Control Panel Java Plug-in Icon

2 Make sure that your settings match those of the **Basic** tab in the **Java Plug-in Control Panel** as shown in the following screenshot.

Figure 273 Java Plug-in Control Panel



Java(TM) Plug-in Control Panel

Basic | Advanced | Browser | Proxies | Cache | Certificates | About

Java Console

○ Show console

● Hide console

○ Do not start console

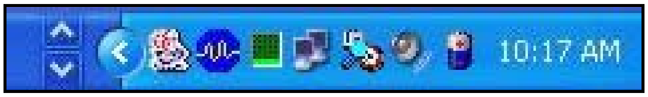
☑ Show Java in System Tray

□ Show Exception Dialog Box

Apply | Reset | Help

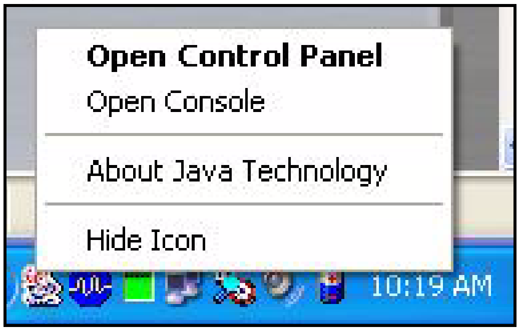
3 Open Internet Explorer and log into Vantage CNM. After successful login a Java plug-in icon should appear in your Windows system tray. If there is no icon present, return to step 2.

Figure 274 Java Plug-in Icon



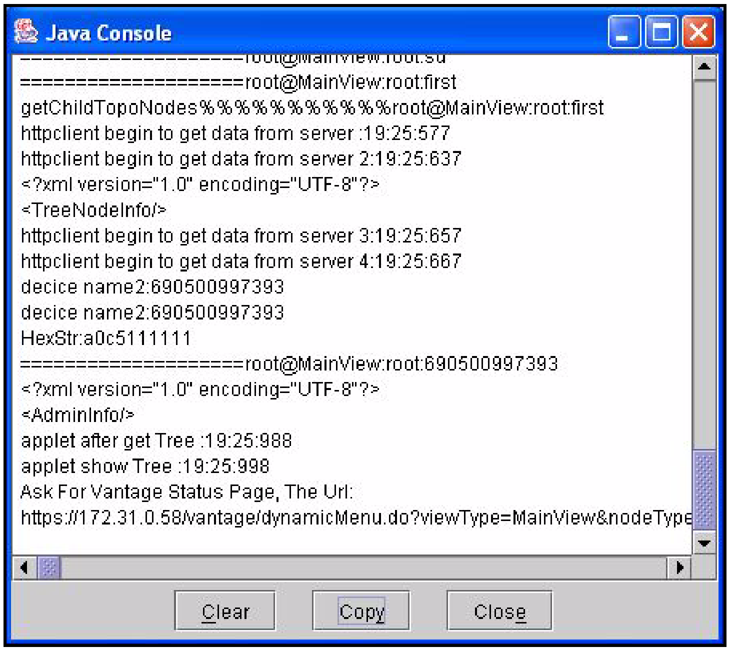
4 Right-click on the Java plug-in icon and select **Open Control Panel,** to view the Java Console screen.

Figure 275 Open Control Panel



5 In the Java Console window, click **Copy**.

Figure 276 Java Console



```
====================root@MainView:root:su
====================root@MainView:root:first
getChildTopoNodes%%%%%%%%%%root@MainView:root:first
httpclient begin to get data from server :19:25:577
httpclient begin to get data from server 2:19:25:637
<?xml version="1.0" encoding="UTF-8"?>
<TreeNodeInfo/>
httpclient begin to get data from server 3:19:25:657
httpclient begin to get data from server 4:19:25:667
decice name2:690500997393
decice name2:690500997393
HexStr:a0c5111111
====================root@MainView:root:690500997393
<?xml version="1.0" encoding="UTF-8"?>
<AdminInfo/>
applet after get Tree :19:25:988
applet show Tree :19:25:998
Ask For Vantage Status Page, The Url:
https://172.31.0.58/vantage/dynamicMenu.do?viewType=MainView&nodeType
```

6 Paste this data into an e-mail and send it to customer support.

Appendix F
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 190 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 191 Allowed IP Address Range By Class

CLASS	ALLOWED RANGE OF FIRST OCTET (BINARY)	ALLOWED RANGE OF FIRST OCTET (DECIMAL)
Class A	**0**0000000 to **0**1111111	0 to 127
Class B	**10**000000 to **10**111111	128 to 191
Class C	**110**00000 to **110**11111	192 to 223
Class D	**1110**0000 to **1110**1111	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 192 "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 193 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 194 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 195 Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**0**0000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	**1**0000000
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 196 Subnet 2

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**1**0000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	**1**0000000
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.**11**000000) 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 197 Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
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 198 Subnet 2

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
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 199 Subnet 3

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
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 200 Subnet 4

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
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 201 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

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

Table 202 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 190) available for subnetting.

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

Table 203 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

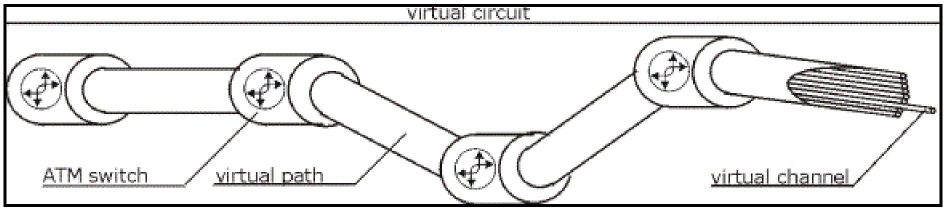
APPENDIX G
Virtual Circuit Topology

Introduction

ATM is a connection-oriented technology, meaning that it sets up virtual circuits over which end systems communicate. The terminology for virtual circuits is as follows:

- Virtual Channel: Logical connections between ATM switches
- Virtual Path: A bundle of virtual channels
- Virtual Circuit: A series of virtual paths between circuit end points

Figure 277 Virtual Circuit Topology



Think of a virtual path as a cable that contains a bundle of wires. The cable connects two points and wires within the cable provide individual circuits between the two points. In an ATM cell header, a VPI (Virtual Path Identifier) identifies a link formed by a virtual path; a VCI (Virtual Channel Identifier) identifies a channel within a virtual path.

The VPI and VCI identify a virtual path, that is, termination points between ATM switches. A series of virtual paths make up a virtual circuit.

Your ISP (Internet Service Provider) should supply you with VPI/VCI numbers.

APPENDIX H
Wireless LANs

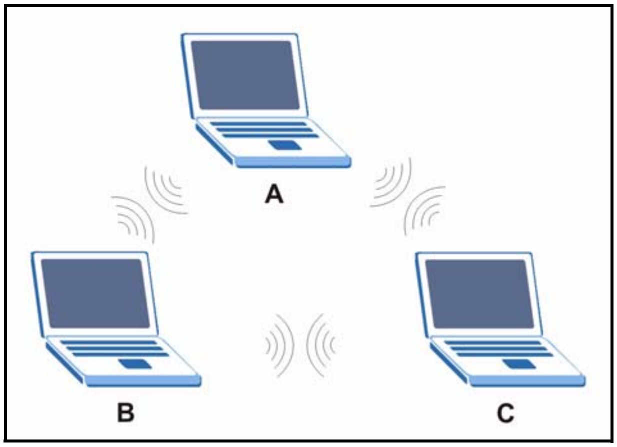
Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless stations (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an Ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an Ad-hoc wireless LAN.

Figure 278 Peer-to-Peer Communication in an Ad-hoc Network

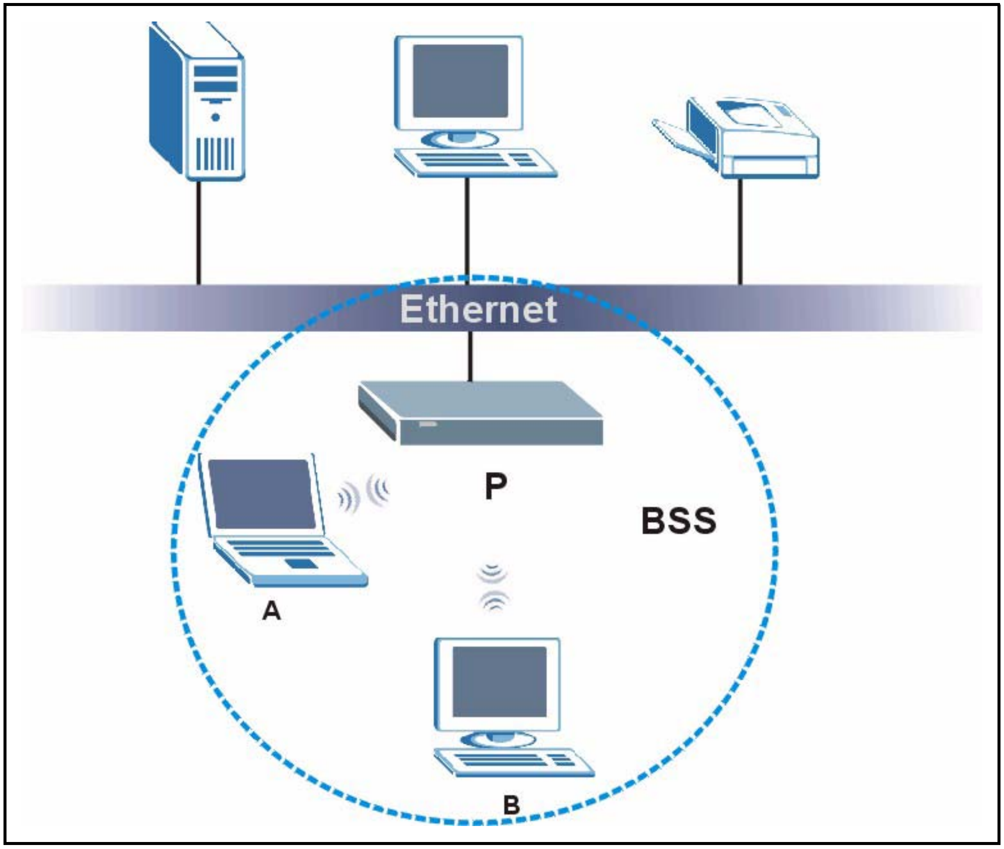


BSS

A Basic Service Set (BSS) exists when all communications between wireless stations or between a wireless station and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless stations in the BSS. When Intra-BSS is enabled, wireless station A and B can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless station A and B can still access the wired network but cannot communicate with each other.

Figure 279 Basic Service Set



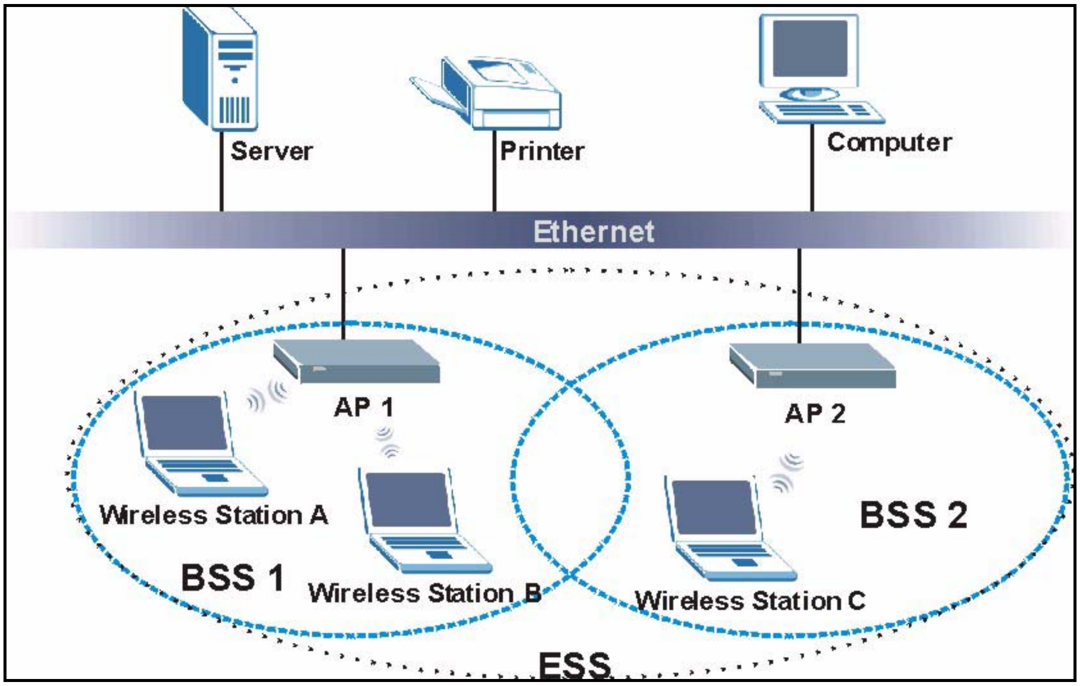
ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless stations within the same ESS must have the same ESSID in order to communicate.

Figure 280 Infrastructure WLAN



Channel

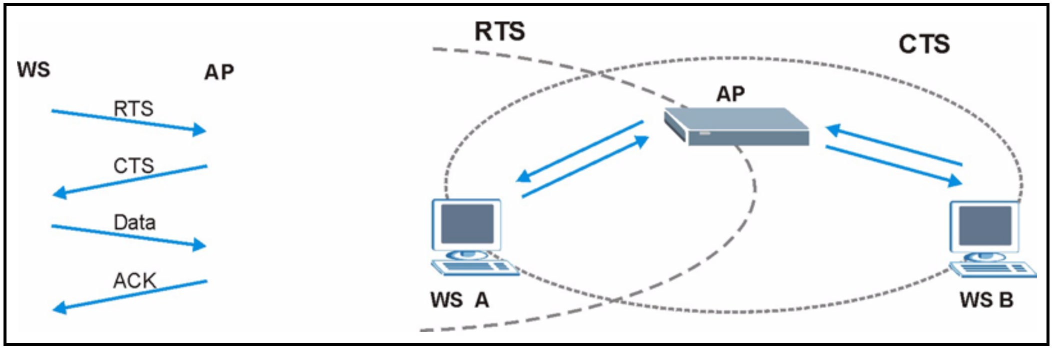
A channel is the radio frequency(ies) used by IEEE 802.11a/b/g wireless devices. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a different channel than an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

Figure 281 RTS/CTS



When station A sends data to the AP, it might not know that the station B is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS/CTS is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Note: Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Preamble Type

A preamble is used to synchronize the transmission timing in your wireless network. There are two preamble modes: **Long** and **Short**.

Short preamble takes less time to process and minimizes overhead, so it should be used in a good wireless network environment when all wireless stations support it.

Select **Long** if you have a 'noisy' network or are unsure of what preamble mode your wireless stations support as all IEEE 802.11b compliant wireless adapters must support long preamble. However, not all wireless adapters support short preamble. Use long preamble if you are unsure what preamble mode the wireless adapters support, to ensure interpretability between the AP and the wireless stations and to provide more reliable communication in 'noisy' networks.

Select **Dynamic** to have the AP automatically use short preamble when all wireless stations support it, otherwise the AP uses long preamble.

Note: The AP and the wireless stations MUST use the same preamble mode in order to communicate.

IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

Table 204 IEEE802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless stations.

RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication

  Determines the identity of the users.
- Authorization

  Determines the network services available to authenticated users once they are connected to the network.
- Accounting

  Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless station and the network RADIUS server.

Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request

  Sent by an access point requesting authentication.
- Access-Reject

  Sent by a RADIUS server rejecting access.
- Access-Accept

  Sent by a RADIUS server allowing access.

- Access-Challenge

  Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request

  Sent by the access point requesting accounting.

- Accounting-Response

  Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

Types of Authentication

This appendix discusses some popular authentication types: **EAP-MD5**, **EAP-TLS**, **EAP-TTLS**, **PEAP** and **LEAP**.

The type of authentication you use depends on the RADIUS server or the AP. Consult your network administrator for more information.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless station. The wireless station 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless stations for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the Wireless screen. You may still configure and store keys here, but they will not be used while Dynamic WEP is enabled.

Note: EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

Table 205 Comparison of EAP Authentication Types

	EAP-MD5	**EAP-TLS**	**EAP-TTLS**	**PEAP**	**LEAP**
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

WPA

User Authentication

WPA applies IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless stations using an external RADIUS database.

Encryption

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP) or Advanced Encryption Standard (AES), Message Integrity Check (MIC) and IEEE 802.1x.

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. It includes a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

TKIP regularly changes and rotates the encryption keys so that the same encryption key is never used twice.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless stations. This all happens in the background automatically.

AES (Advanced Encryption Standard) also uses a secret key. This implementation of AES applies a 128-bit key to 128-bit blocks of data.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), TKIP makes it much more difficult to decrypt data on a Wi-Fi network than WEP, making it difficult for an intruder to break into the network.

The encryption mechanisms used for WPA and WPA-PSK are the same. The only difference between the two is that WPA-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs an easier-to-use, consistent, single, alphanumeric password.

Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each Authentication Method/ key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 206 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	ENABLE IEEE 802.1X
Open	None	No	No
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	WEP	No	Yes
WPA	TKIP	No	Yes
WPA-PSK	WEP	Yes	Yes
WPA-PSK	TKIP	Yes	Yes

Benefits of a Wireless LAN

Wireless LAN offers the following benefits:

It provides you with access to network services in areas otherwise hard or expensive to wire, such as historical buildings, buildings with asbestos materials and classrooms.

It provides health care workers like doctors and nurses access to a complete patient’s profile on a handheld or notebook computer upon entering a patient’s room.

It allows flexible workgroups a lower total cost of ownership for workspaces that are frequently reconfigured.

It allows conference room users access to the network as they move from meeting to meeting, getting up-to-date access to information and the ability to communicate decisions while “on the go”.

It provides campus-wide networking mobility, allowing enterprises the roaming capability to set up easy-to-use wireless networks that cover the entire campus transparently.

IEEE 802.11

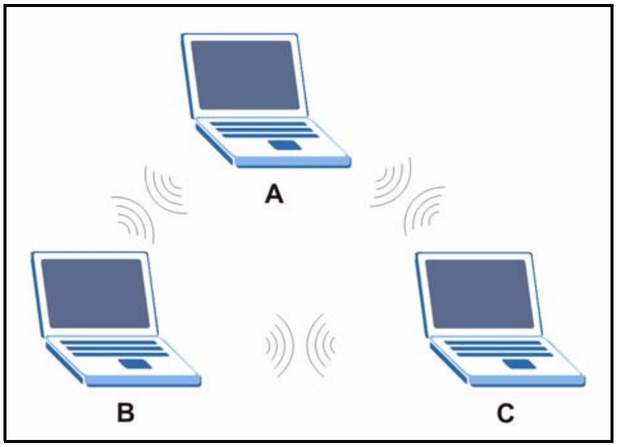
The 1997 completion of the IEEE 802.11 standard for wireless LANs (WLANs) was a first important step in the evolutionary development of wireless networking technologies. The standard was developed to maximize inter operability between differing brands of wireless LANs as well as to introduce a variety of performance improvements and benefits.

The IEEE 802.11 specifies three different transmission methods for the PHY, the layer responsible for transferring data between nodes. Two of the methods use spread spectrum RF signals, Direct Sequence Spread Spectrum (DSSS) and Frequency-Hopping Spread Spectrum (FHSS), in the 2.4 to 2.4825 GHz unlicensed ISM (Industrial, Scientific and Medical) band. The third method is infrared technology, using very high frequencies, just below visible light in the electromagnetic spectrum to carry data.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless nodes or stations (STA), which is called a Basic Service Set (BSS). In the most basic form, a wireless LAN connects a set of computers with wireless adapters. Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an Ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an Ad-hoc wireless LAN.

Figure 282 Peer-to-Peer Communication in an Ad-hoc Network

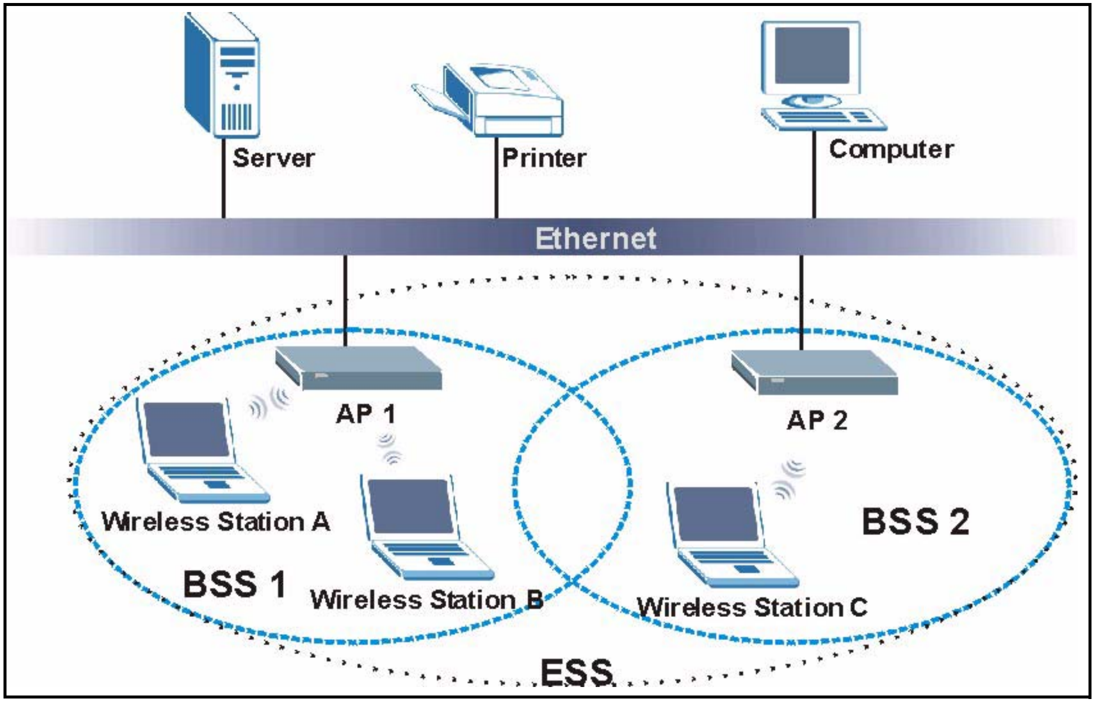


Infrastructure Wireless LAN Configuration

For Infrastructure WLANs, multiple Access Points (APs) link the WLAN to the wired network and allow users to efficiently share network resources. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood. Multiple Access Points can provide wireless coverage for an entire building or campus. All communications between stations or between a station and a wired network client go through the Access Point.

The Extended Service Set (ESS) shown in the next figure consists of a series of overlapping BSSs (each containing an Access Point) connected together by means of a Distribution System (DS). Although the DS could be any type of network, it is almost invariably an Ethernet LAN. Mobile nodes can roam between Access Points and seamless campus-wide coverage is possible.

Figure 283 ESS Provides Campus-Wide Coverage



APPENDIX I Log Descriptions

Introduction

This appendix provides descriptions of example device log messages.

Table 207 System Maintenance Logs

LOG MESSAGE	DESCRIPTION
`Time calibration is successful`	The router has adjusted its time based on information from the time server.
`Time calibration failed`	The router failed to get information from the time server.
`WAN interface gets IP:%s`	A WAN interface got a new IP address from the DHCP, PPPoE, PPTP or dial-up server.
`DHCP client IP expired`	A DHCP client's IP address has expired.
`DHCP server assigns%s`	The DHCP server assigned an IP address to a client.
`Successful SMT login`	Someone has logged on to the router's SMT interface.
`SMT login failed`	Someone has failed to log on to the router's SMT interface.
`Successful WEB login`	Someone has logged on to the router's web configurator interface.
`WEB login failed`	Someone has failed to log on to the router's web configurator interface.
`Successful TELNET login`	Someone has logged on to the router via telnet.
`TELNET login failed`	Someone has failed to log on to the router via telnet.
`Successful FTP login`	Someone has logged on to the router via ftp.
`FTP login failed`	Someone has failed to log on to the router via ftp.
`NAT Session Table is Full!`	The maximum number of NAT session table entries has been exceeded and the table is full.
`Starting Connectivity Monitor`	Starting Connectivity Monitor.
`Time initialized by Daytime Server`	The router got the time and date from the Daytime server.
`Time initialized by Time server`	The router got the time and date from the time server.
`Time initialized by NTP server`	The router got the time and date from the NTP server.
`Connect to Daytime server fail`	The router was not able to connect to the Daytime server.
`Connect to Time server fail`	The router was not able to connect to the Time server.
`Connect to NTP server fail`	The router was not able to connect to the NTP server.

Table 207 System Maintenance Logs (continued)

LOG MESSAGE	DESCRIPTION
`Too large ICMP packet has been dropped`	The router dropped an ICMP packet that was too large.
`SMT Session Begin`	An SMT management session has started.
`SMT Session End`	An SMT management session has ended.
`Configuration Change: PC = 0x%x, Task ID = 0x%x`	The router is saving configuration changes.
`Successful SSH login`	Someone has logged on to the router's SSH server.
`SSH login failed`	Someone has failed to log on to the router's SSH server.
`Successful HTTPS login`	Someone has logged on to the router's web configurator interface using HTTPS protocol.
`HTTPS login failed`	Someone has failed to log on to the router's web configurator interface using HTTPS protocol.

Table 208 System Error Logs

LOG MESSAGE	DESCRIPTION
`%s exceeds the max. number of session per host!`	This attempt to create a NAT session exceeds the maximum number of NAT session table entries allowed to be created per host.
`setNetBIOSFilter: calloc error`	The router failed to allocate memory for the NetBIOS filter settings.
`readNetBIOSFilter: calloc error`	The router failed to allocate memory for the NetBIOS filter settings.
`WAN connection is down.`	A WAN connection is down. You cannot access the network through this interface.

Table 209 Access Control Logs

LOG MESSAGE	DESCRIPTION
`Firewall default policy: [ TCP | UDP | IGMP | ESP | GRE | OSPF] <Packet Direction>`	Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched the default policy and was blocked or forwarded according to the default policy's setting.
`Firewall rule [NOT] match:[TCP | UDP | IGMP | ESP | GRE | OSPF] <Packet Direction>, <ruled>`	Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched (or did not match) a configured firewall rule (denoted by its number) and was blocked or forwarded according to the rule.
`Triangle route packet forwarded: [TCP | UDP | IGMP | ESP | GRE | OSPF]`	The firewall allowed a triangle route session to pass through.

Table 209 Access Control Logs (continued)

LOG MESSAGE	DESCRIPTION
`Packet without a NAT table entry blocked: [TCP | UDP | IGMP | ESP | GRE | OSPF]`	The router blocked a packet that didn't have a corresponding NAT table entry.
`Router sent blocked web site message: TCP`	The router sent a message to notify a user that the router blocked access to a web site that the user requested.

Table 210 TCP Reset Logs

LOG MESSAGE	DESCRIPTION
`Under SYN flood attack, sent TCP RST`	The router sent a TCP reset packet when a host was under a SYN flood attack (the TCP incomplete count is per destination host.)
`Exceed TCP MAX incomplete, sent TCP RST`	The router sent a TCP reset packet when the number of TCP incomplete connections exceeded the user configured threshold. (the TCP incomplete count is per destination host.) Note: Refer to **TCP Maximum Incomplete** in the **Firewall Attack Alerts** screen.
`Peer TCP state out of order, sent TCP RST`	The router sent a TCP reset packet when a TCP connection state was out of order.Note: The firewall refers to RFC793 Figure 6 to check the TCP state.
`Firewall session time out, sent TCP RST`	The router sent a TCP reset packet when a dynamic firewall session timed out.Default timeout values:ICMP idle timeout (s): 60UDP idle timeout (s): 60TCP connection (three way handshaking) timeout (s): 30TCP FIN-wait timeout (s): 60TCP idle (established) timeout (s): 3600
`Exceed MAX incomplete, sent TCP RST`	The router sent a TCP reset packet when the number of incomplete connections (TCP and UDP) exceeded the user-configured threshold. (Incomplete count is for all TCP and UDP connections through the firewall.)Note: When the number of incomplete connections (TCP + UDP) > “Maximum Incomplete High”, the router sends TCP RST packets for TCP connections and destroys TOS (firewall dynamic sessions) until incomplete connections < “Maximum Incomplete Low”.
`Access block, sent TCP RST`	The router sends a TCP RST packet and generates this log if you turn on the firewall TCP reset mechanism (via CI command: "sys firewall tcprst").

Table 211 Packet Filter Logs

LOG MESSAGE	DESCRIPTION
`[TCP | UDP | ICMP | IGMP | Generic] packet filter matched (set: %d, rule: %d)`	Attempted access matched a configured filter rule (denoted by its set and rule number) and was blocked or forwarded according to the rule.

Table 212 ICMP Logs

LOG MESSAGE	DESCRIPTION
`Firewall default policy: ICMP <Packet Direction>, <type:%d>, <code:%d>`	ICMP access matched the default policy and was blocked or forwarded according to the user's setting. For type and code details, see Table 224.
`Firewall rule [NOT] match: ICMP <Packet Direction>, <rule:%d>, <type:%d>, <code:%d>`	ICMP access matched (or didn't match) a firewall rule (denoted by its number) and was blocked or forwarded according to the rule. For type and code details, see Table 224.
`Triangle route packet forwarded: ICMP`	The firewall allowed a triangle route session to pass through.
`Packet without a NAT table entry blocked: ICMP`	The router blocked a packet that didn't have a corresponding NAT table entry.
`Unsupported/out-of-order ICMP: ICMP`	The firewall does not support this kind of ICMP packets or the ICMP packets are out of order.
`Router reply ICMP packet: ICMP`	The router sent an ICMP reply packet to the sender.

Table 213 CDR Logs

LOG MESSAGE	DESCRIPTION
`board %d line %d channel %d, call %d, %s C01 Outgoing Call dev=%x ch=%x %s`	The router received the setup requirements for a call. "call" is the reference (count) number of the call. "dev" is the device type (3 is for dial-up, 6 is for PPPoE, 10 is for PPTP). "channel" or "ch" is the call channel ID.For example,"board 0 line 0 channel 0, call 3, C01 Outgoing Call dev=6 ch=0 "Means the router has dialed to the PPPoE server 3 times.
`board %d line %d channel %d, call %d, %s C02 OutCall Connected %d %s`	The PPPoE, PPTP or dial-up call is connected.
`board %d line %d channel %d, call %d, %s C02 Call Terminated`	The PPPoE, PPTP or dial-up call was disconnected.

Table 214 PPP Logs

LOG MESSAGE	DESCRIPTION
`ppp:LCP Starting`	The PPP connection's Link Control Protocol stage has started.
`ppp:LCP Opening`	The PPP connection's Link Control Protocol stage is opening.
`ppp:CHAP Opening`	The PPP connection's Challenge Handshake Authentication Protocol stage is opening.
`ppp:IPCP Starting`	The PPP connection's Internet Protocol Control Protocol stage is starting.
`ppp:IPCP Opening`	The PPP connection's Internet Protocol Control Protocol stage is opening.

Table 214 PPP Logs (continued)

LOG MESSAGE	DESCRIPTION
`ppp:LCP Closing`	The PPP connection’s Link Control Protocol stage is closing.
`ppp:IPCP Closing`	The PPP connection’s Internet Protocol Control Protocol stage is closing.

Table 215 UPnP Logs

LOG MESSAGE	DESCRIPTION
`UPnP pass through Firewall`	UPnP packets can pass through the firewall.

Table 216 Content Filtering Logs

LOG MESSAGE	DESCRIPTION
`%s: Keyword blocking`	The content of a requested web page matched a user defined keyword.
`%s: Not in trusted web list`	The web site is not in a trusted domain, and the router blocks all traffic except trusted domain sites.
`%s: Forbidden Web site`	The web site is in the forbidden web site list.
`%s: Contains ActiveX`	The web site contains ActiveX.
`%s: Contains Java applet`	The web site contains a Java applet.
`%s: Contains cookie`	The web site contains a cookie.
`%s: Proxy mode detected`	The router detected proxy mode in the packet.
`%s`	The content filter server responded that the web site is in the blocked category list, but it did not return the category type.
`%s: %s`	The content filter server responded that the web site is in the blocked category list, and returned the category type.
`%s(cache hit)`	The system detected that the web site is in the blocked list from the local cache, but does not know the category type.
`%s :%s(cache hit)`	The system detected that the web site is in blocked list from the local cache, and knows the category type.
`%s: Trusted Web site`	The web site is in a trusted domain.
`%s`	When the content filter is not on according to the time schedule or you didn't select the "Block Matched Web Site” checkbox, the system forwards the web content.
`Waiting content filter server timeout`	The external content filtering server did not respond within the timeout period.
`DNS resolving failed`	The ZyWALL cannot get the IP address of the external content filtering via DNS query.
`Creating socket failed`	The ZyWALL cannot issue a query because TCP/IP socket creation failed, port:port number.

Table 216 Content Filtering Logs (continued)

LOG MESSAGE	DESCRIPTION
`Connecting to content filter server fail`	The connection to the external content filtering server failed.
`License key is invalid`	The external content filtering license key is invalid.

Table 217 Attack Logs

LOG MESSAGE	DESCRIPTION
`attack [ TCP | UDP | IGMP | ESP | GRE | OSPF]`	The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF attack.
`attack ICMP (type:%d, code:%d)`	The firewall detected an ICMP attack. For type and code details, see Table 224.
`land [TCP | UDP | IGMP | ESP | GRE | OSPF ]`	The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF land attack.
`land ICMP (type:%d, code:%d)`	The firewall detected an ICMP land attack. For type and code details, see Table 224.
`ip spoofing - WAN [ TCP | UDP | IGMP | ESP | GRE | OSPF]`	The firewall detected an IP spoofing attack on the WAN port.
`ip spoofing - WAN ICMP (type:%d, code:%d)`	The firewall detected an ICMP IP spoofing attack on the WAN port. For type and code details, see Table 224.
`icmp echo : ICMP (type:%d, code:%d)`	The firewall detected an ICMP echo attack. For type and code details, see Table 224.
`syn flood TCP`	The firewall detected a TCP syn flood attack.
`ports scan TCP`	The firewall detected a TCP port scan attack.
`teardrop TCP`	The firewall detected a TCP teardrop attack.
`teardrop UDP`	The firewall detected an UDP teardrop attack.
`teardrop ICMP (type:%d, code:%d)`	The firewall detected an ICMP teardrop attack. For type and code details, see Table 224.
`illegal command TCP`	The firewall detected a TCP illegal command attack.
`NetBIOS TCP`	The firewall detected a TCP NetBIOS attack.
`ip spoofing - no routing entry [TCP | UDP | IGMP | ESP | GRE | OSPF]`	The firewall classified a packet with no source routing entry as an IP spoofing attack.
`ip spoofing - no routing entry ICMP (type:%d, code:%d)`	The firewall classified an ICMP packet with no source routing entry as an IP spoofing attack.
`vulnerability ICMP (type:%d, code:%d)`	The firewall detected an ICMP vulnerability attack. For type and code details, see Table 224.
`traceroute ICMP (type:%d, code:%d)`	The firewall detected an ICMP traceroute attack. For type and code details, see Table 224.

Table 218 IPSec Logs

LOG MESSAGE	DESCRIPTION
`Discard REPLAY packet`	The router received and discarded a packet with an incorrect sequence number.
`Inbound packet authentication failed`	The router received a packet that has been altered. A third party may have altered or tampered with the packet.
`Receive IPSec packet, but no corresponding tunnel exists`	The router dropped an inbound packet for which SPI could not find a corresponding phase 2 SA.
`Rule <%d> idle time out, disconnect`	The router dropped a connection that had outbound traffic and no inbound traffic for a certain time period. You can use the "ipsec timer chk_conn" CI command to set the time period. The default value is 2 minutes.
`WAN IP changed to <IP>`	The router dropped all connections with the “MyIP” configured as “0.0.0.0” when the WAN IP address changed.

Table 219 IKE Logs

LOG MESSAGE	DESCRIPTION
`Active connection allowed exceeded`	The IKE process for a new connection failed because the limit of simultaneous phase 2 SAs has been reached.
`Start Phase 2: Quick Mode`	Phase 2 Quick Mode has started.
`Verifying Remote ID failed:`	The connection failed during IKE phase 2 because the router and the peer’s Local/Remote Addresses don’t match.
`Verifying Local ID failed:`	The connection failed during IKE phase 2 because the router and the peer’s Local/Remote Addresses don’t match.
`IKE Packet Retransmit`	The router retransmitted the last packet sent because there was no response from the peer.
`Failed to send IKE Packet`	An Ethernet error stopped the router from sending IKE packets.
`Too many errors! Deleting SA`	An SA was deleted because there were too many errors.
`Phase 1 IKE SA process done`	The phase 1 IKE SA process has been completed.
`Duplicate requests with the same cookie`	The router received multiple requests from the same peer while still processing the first IKE packet from the peer.
`IKE Negotiation is in process`	The router has already started negotiating with the peer for the connection, but the IKE process has not finished yet.
`No proposal chosen`	Phase 1 or phase 2 parameters don’t match. Please check all protocols / settings. Ex. One device being configured for 3DES and the other being configured for DES causes the connection to fail.
`Local / remote IPs of incoming request conflict with rule <%d>`	The security gateway is set to “0.0.0.0” and the router used the peer’s “Local Address” as the router’s “Remote Address”. This information conflicted with static rule #d; thus the connection is not allowed.

Table 219 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
`Cannot resolve Secure Gateway Addr for rule <%d>`	The router couldn’t resolve the IP address from the domain name that was used for the secure gateway address.
`Peer ID: <peer id> <My remote type> -<My local type>`	The displayed ID information did not match between the two ends of the connection.
`vs. My Remote <My remote> -<My remote>`	The displayed ID information did not match between the two ends of the connection.
`vs. My Local <My local>-<My local>`	The displayed ID information did not match between the two ends of the connection.
`Send <packet>`	A packet was sent.
`Recv <packet>`	IKE uses ISAKMP to transmit data. Each ISAKMP packet contains many different types of payloads. All of them show in the LOG. Refer to RFC2408 – ISAKMP for a list of all ISAKMP payload types.
`Recv <Main or Aggressive> Mode request from <IP>`	The router received an IKE negotiation request from the peer address specified.
`Send <Main or Aggressive> Mode request to <IP>`	The router started negotiation with the peer.
`Invalid IP <Peer local> / <Peer local>`	The peer’s “Local IP Address” is invalid.
`Remote IP <Remote IP> / <Remote IP> conflicts`	The security gateway is set to “0.0.0.0” and the router used the peer’s “Local Address” as the router’s “Remote Address”. This information conflicted with static rule #d; thus the connection is not allowed.
`Phase 1 ID type mismatch`	This router’s "Peer ID Type" is different from the peer IPSec router's "Local ID Type".
`Phase 1 ID content mismatch`	This router’s "Peer ID Content" is different from the peer IPSec router's "Local ID Content".
`No known phase 1 ID type found`	The router could not find a known phase 1 ID in the connection attempt.
`ID type mismatch. Local / Peer: <Local ID type/Peer ID type>`	The phase 1 ID types do not match.
`ID content mismatch`	The phase 1 ID contents do not match.
`Configured Peer ID Content: <Configured Peer ID Content>`	The phase 1 ID contents do not match and the configured "Peer ID Content" is displayed.
`Incoming ID Content: <Incoming Peer ID Content>`	The phase 1 ID contents do not match and the incoming packet's ID content is displayed.
`Unsupported local ID Type: <%d>`	The phase 1 ID type is not supported by the router.
`Build Phase 1 ID`	The router has started to build the phase 1 ID.
`Adjust TCP MSS to %d`	The router automatically changed the TCP Maximum Segment Size value after establishing a tunnel.
`Rule <%d> input idle time out, disconnect`	The tunnel for the listed rule was dropped because there was no inbound traffic within the idle timeout period.
`XAUTH succeed! Username: <Username>`	The router used extended authentication to authenticate the listed username.

Table 219 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
`XAUTH fail! Username: <Username>`	The router was not able to use extended authentication to authenticate the listed username.
`Rule[%d] Phase 1 negotiation mode mismatch`	The listed rule's IKE phase 1 negotiation mode did not match between the router and the peer.
`Rule [%d] Phase 1 encryption algorithm mismatch`	The listed rule's IKE phase 1 encryption algorithm did not match between the router and the peer.
`Rule [%d] Phase 1 authentication algorithm mismatch`	The listed rule's IKE phase 1 authentication algorithm did not match between the router and the peer.
`Rule [%d] Phase 1 authentication method mismatch`	The listed rule's IKE phase 1 authentication method did not match between the router and the peer.
`Rule [%d] Phase 1 key group mismatch`	The listed rule's IKE phase 1 key group did not match between the router and the peer.
`Rule [%d] Phase 2 protocol mismatch`	The listed rule's IKE phase 2 protocol did not match between the router and the peer.
`Rule [%d] Phase 2 encryption algorithm mismatch`	The listed rule's IKE phase 2 encryption algorithm did not match between the router and the peer.
`Rule [%d] Phase 2 authentication algorithm mismatch`	The listed rule's IKE phase 2 authentication algorithm did not match between the router and the peer.
`Rule [%d] Phase 2 encapsulation mismatch`	The listed rule's IKE phase 2 encapsulation did not match between the router and the peer.
`Rule [%d]> Phase 2 pfs mismatch`	The listed rule's IKE phase 2 perfect forward secret (pfs) setting did not match between the router and the peer.
`Rule [%d] Phase 1 ID mismatch`	The listed rule's IKE phase 1 ID did not match between the router and the peer.
`Rule [%d] Phase 1 hash mismatch`	The listed rule's IKE phase 1 hash did not match between the router and the peer.
`Rule [%d] Phase 1 preshared key mismatch`	The listed rule's IKE phase 1 pre-shared key did not match between the router and the peer.
`Rule [%d] Tunnel built successfully`	The listed rule's IPSec tunnel has been built successfully.
`Rule [%d] Peer's public key not found`	The listed rule's IKE phase 1 peer's public key was not found.
`Rule [%d] Verify peer's signature failed`	The listed rule's IKE phase 1verification of the peer's signature failed.
`Rule [%d] Sending IKE request`	IKE sent an IKE request for the listed rule.
`Rule [%d] Receiving IKE request`	IKE received an IKE request for the listed rule.
`Swap rule to rule [%d]`	The router changed to using the listed rule.
`Rule [%d] Phase 1 key length mismatch`	The listed rule's IKE phase 1 key length (with the AES encryption algorithm) did not match between the router and the peer.
`Rule [%d] phase 1 mismatch`	The listed rule's IKE phase 1 did not match between the router and the peer.

Table 219 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
`Rule [%d] phase 2 mismatch`	The listed rule's IKE phase 2 did not match between the router and the peer.
`Rule [%d] Phase 2 key length mismatch`	The listed rule's IKE phase 2 key lengths (with the AES encryption algorithm) did not match between the router and the peer.

Table 220 PKI Logs

LOG MESSAGE	DESCRIPTION
`Enrollment successful`	The SCEP online certificate enrollment was successful. The Destination field records the certification authority server IP address and port.
`Enrollment failed`	The SCEP online certificate enrollment failed. The Destination field records the certification authority server's IP address and port.
`Failed to resolve <SCEP CA server url>`	The SCEP online certificate enrollment failed because the certification authority server's address cannot be resolved.
`Enrollment successful`	The CMP online certificate enrollment was successful. The Destination field records the certification authority server's IP address and port.
`Enrollment failed`	The CMP online certificate enrollment failed. The Destination field records the certification authority server's IP address and port.
`Failed to resolve <CMP CA server url>`	The CMP online certificate enrollment failed because the certification authority server's IP address cannot be resolved.
`Rcvd ca cert: <subject name>`	The router received a certification authority certificate, with subject name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.
`Rcvd user cert: <subject name>`	The router received a user certificate, with subject name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.
`Rcvd CRL <size>: <issuer name>`	The router received a CRL (Certificate Revocation List), with size and issuer name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.
`Rcvd ARL <size>: <issuer name>`	The router received an ARL (Authority Revocation List), with size and issuer name as recorded, from the LDAP server whose address and port are recorded in the Source field.
`Failed to decode the received ca cert`	The router received a corrupted certification authority certificate from the LDAP server whose address and port are recorded in the Source field.
`Failed to decode the received user cert`	The router received a corrupted user certificate from the LDAP server whose address and port are recorded in the Source field.
`Failed to decode the received CRL`	The router received a corrupted CRL (Certificate Revocation List) from the LDAP server whose address and port are recorded in the Source field.
`Failed to decode the received ARL`	The router received a corrupted ARL (Authority Revocation List) from the LDAP server whose address and port are recorded in the Source field.

Table 220 PKI Logs (continued)

LOG MESSAGE	DESCRIPTION
`Rcvd data <size> too large! Max size allowed: <max size>`	The router received directory data that was too large (the size is listed) from the LDAP server whose address and port are recorded in the Source field. The maximum size of directory data that the router allows is also recorded.
`Cert trusted: <subject name>`	The router has verified the path of the certificate with the listed subject name.
`Due to <reason codes>, cert not trusted: <subject name>`	Due to the reasons listed, the certificate with the listed subject name has not passed the path verification. The recorded reason codes are only approximate reasons for not trusting the certificate. Please see Table 221 for the corresponding descriptions of the codes.

Table 221 Certificate Path Verification Failure Reason Codes

CODE	DESCRIPTION
1	Algorithm mismatch between the certificate and the search constraints.
2	Key usage mismatch between the certificate and the search constraints.
3	Certificate was not valid in the time interval.
4	(Not used)
5	Certificate is not valid.
6	Certificate signature was not verified correctly.
7	Certificate was revoked by a CRL.
8	Certificate was not added to the cache.
9	Certificate decoding failed.
10	Certificate was not found (anywhere).
11	Certificate chain looped (did not find trusted root).
12	Certificate contains critical extension that was not handled.
13	Certificate issuer was not valid (CA specific information missing).
14	(Not used)
15	CRL is too old.
16	CRL is not valid.
17	CRL signature was not verified correctly.
18	CRL was not found (anywhere).
19	CRL was not added to the cache.
20	CRL decoding failed.
21	CRL is not currently valid, but in the future.
22	CRL contains duplicate serial numbers.
23	Time interval is not continuous.
24	Time information not available.
25	Database method failed due to timeout.

Table 221 Certificate Path Verification Failure Reason Codes (continued)

CODE	DESCRIPTION
26	Database method failed.
27	Path was not verified.
28	Maximum path length reached.

Table 222 802.1X Logs

LOG MESSAGE	DESCRIPTION
`Local User Database accepts user.`	A user was authenticated by the local user database.
`Local User Database reports user credential error.`	A user was not authenticated by the local user database because of an incorrect user password.
``Local User Database does not find user`s credential.``	A user was not authenticated by the local user database because the user is not listed in the local user database.
`RADIUS accepts user.`	A user was authenticated by the RADIUS Server.
`RADIUS rejects user. Pls check RADIUS Server.`	A user was not authenticated by the RADIUS Server. Please check the RADIUS Server.
`Local User Database does not support authentication method.`	The local user database only supports the EAP-MD5 method. A user tried to use another authentication method and was not authenticated.
`User logout because of session timeout expired.`	The router logged out a user whose session expired.
`User logout because of user deassociation.`	The router logged out a user who ended the session.
`User logout because of no authentication response from user.`	The router logged out a user from which there was no authentication response.
`User logout because of idle timeout expired.`	The router logged out a user whose idle timeout period expired.
`User logout because of user request.`	A user logged out.
`Local User Database does not support authentication mothed.`	A user tried to use an authentication method that the local user database does not support (it only supports EAP-MD5).
`No response from RADIUS. Pls check RADIUS Server.`	There is no response message from the RADIUS server, please check the RADIUS server.
`Use Local User Database to authenticate user.`	The local user database is operating as the authentication server.
`Use RADIUS to authenticate user.`	The RADIUS server is operating as the authentication server.
`No Server to authenticate user.`	There is no authentication server to authenticate a user.
``Local User Database does not find user`s credential.``	A user was not authenticated by the local user database because the user is not listed in the local user database.

Table 223 ACL Setting Notes

PACKET DIRECTION	DIRECTION	DESCRIPTION
(L to W)	LAN to WAN	ACL set for packets traveling from the LAN to the WAN.
(W to L)	WAN to LAN	ACL set for packets traveling from the WAN to the LAN.
(D to L)	DMZ to LAN	ACL set for packets traveling from the DMZ to the LAN.
(D to W)	DMZ to WAN	ACL set for packets traveling from the DMZ to the WAN.
(W to D)	WAN to DMZ	ACL set for packets traveling from the WAN to the DMZ.
(L to D)	LAN to DMZ	ACL set for packets traveling from the LAN to the DMZ.
(L to L/ZW)	LAN to LAN/ ZyWALL	ACL set for packets traveling from the LAN to the LAN or the ZyWALL.
(W to W/ZW)	WAN to WAN/ ZyWALL	ACL set for packets traveling from the WAN to the WAN or the ZyWALL.
(D to D/ZW)	DMZ to DMZ/ ZyWALL	ACL set for packets traveling from the DMZ to the DM or the ZyWALL.

Table 224 ICMP Notes

TYPE	CODE	DESCRIPTION
0		Echo Reply
	0	Echo reply message
3		Destination Unreachable
	0	Net unreachable
	1	Host unreachable
	2	Protocol unreachable
	3	Port unreachable
	4	A packet that needed fragmentation was dropped because it was set to Don't Fragment (DF)
	5	Source route failed
4		Source Quench
	0	A gateway may discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network.
5		Redirect
	0	Redirect datagrams for the Network
	1	Redirect datagrams for the Host
	2	Redirect datagrams for the Type of Service and Network
	3	Redirect datagrams for the Type of Service and Host
8		Echo
	0	Echo message

Table 224 ICMP Notes (continued)

TYPE	CODE	DESCRIPTION
11		Time Exceeded
	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
12		Parameter Problem
	0	Pointer indicates the error
13		Timestamp
	0	Timestamp request message
14		Timestamp Reply
	0	Timestamp reply message
15		Information Request
	0	Information request message
16		Information Reply
	0	Information reply message

Table 225 Syslog Logs

LOG MESSAGE	DESCRIPTION
`<Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="<msg>" note="<note>" devID="<mac address last three numbers>" cat="<category>`	"This message is sent by the system ("RAS" displays as the system name if you haven't configured one) when the router generates a syslog. The facility is defined in the web MAIN MENU->LOGS->Log Settings page. The severity is the log's syslog class. The definition of messages and notes are defined in the various log charts throughout this appendix. The "devID" is the last three characters of the MAC address of the router's LAN port. The "cat" is the same as the category in the router's logs.

The following table shows RFC-2408 ISAKMP payload types that the log displays. Please refer to the RFC for detailed information on each type.

Table 226 RFC-2408 ISAKMP Payload Types

LOG DISPLAY	PAYLOAD TYPE
SA	Security Association
PROP	Proposal
TRANS	Transform
KE	Key Exchange
ID	Identification
CER	Certificate
CER_REQ	Certificate Request
HASH	Hash

Table 226 RFC-2408 ISAKMP Payload Types (continued)

LOG DISPLAY	PAYLOAD TYPE
`SIG`	Signature
`NONCE`	Nonce
`NOTFY`	Notification
`DEL`	Delete
`VID`	Vendor ID

APPENDIX J
Open Software Announcements

Notice

Information herein is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, except the express written permission of ZyXEL Communications Corporation.

This Product includes Castor

Copyright (C) 1999-2001 Intalio, Inc. All Rights Reserved.

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain copyright statements and notices. Redistributions must also contain a copy of this document.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name "ExoLab" must not be used to endorse or promote products derived from this Software without prior written permission of ExoLab Group. For written permission, please contact info@exolab.org.

4. Products derived from this Software may not be called "ExoLab" nor may "ExoLab" appear in their names without prior written permission of ExoLab Group. Exolab is a registered trademark of ExoLab Group.

5.Due credit should be given to the ExoLab Group (http://www.exolab.org).

THIS SOFTWARE IS PROVIDED BY INTALIO, INC. AND CONTRIBUTORS "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF ERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.

IN NO EVENT SHALL INTALIO, INC. OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This Product includes Junit under Common Public License Version 1.0

Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

"Contribution" means: a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and b) in the case of each subsequent Contributor: i) changes to the Program, and ii) additions to the Program; where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents " mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement: i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose; ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits; iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

This Product includes Cryptix

Cryptix General License

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE CRYPTIX FOUNDATION LIMITED AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE CRYPTIX FOUNDATION LIMITED OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This Product includes software of Java Software technologies.

TECHNOLOGY LICENSE FROM SUN MICROSYSTEMS, INC. TO DOUG LEA

Whereas Doug Lea desires to utlized certain Java Software technologies in the util.concurrent technology; and Whereas Sun Microsystems, Inc. (Sun) desires that Doug Lea utilize certain Java Software technologies in the util.concurrent technology; Therefore the parties agree as follows, effective May 31, 2002:

Java Software technologies means

classes/java/util/ArrayList.java, and

classes/java/util/HashMap.java.

DISTRIBUTING THE SOFTWARE OR ITS DERIVATIVES. IN NO EVENT WILL SUN MICROSYSTEMS, INC. OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR DIRECT, INDIRECT, SPECIAL, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF THE USE OF OR INABILITY TO USE SOFTWARE, EVEN IF SUN MICROSYSTEMS, INC. HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

You acknowledge that Software is not designed, licensed or intended for use in the design, construction, operation or maintenance of any nuclear facility.

signed [Doug Lea] dated

JAVA Software Technologies

JAVA(TM) 2 SOFTWARE DEVELOPMENT KIT (J2SDK), STANDARD EDITION, VERSION 1.4.1_X SUPPLEMENTAL LICENSE TERMS

These supplemental license terms ("Supplemental Terms") add to or modify the terms of the Binary Code License Agreement (collectively, the "Agreement"). Capitalized terms not defined in these Supplemental Terms shall have the same meanings ascribed to them in the Binary Code License Agreement. These Supplemental Terms shall supersede any inconsistent or conflicting terms in the Binary Code License Agreement, or in any license contained within the Software.

1. Software Internal Use and Development License Grant. Subject to the terms and conditions of this Agreement, including, but not limited to Section 4 (Java Technology Restrictions) of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce internally and use internally the binary form of the Software complete and unmodified for the sole purpose of designing, developing, testing, and running your Java applets and applications intended to run on Java-enabled general purpose desktop computers and servers ("Programs").

2. License to Distribute Software. Subject to the terms and conditions of this Agreement, including, but not limited to Section 4 (Java Technology Restrictions) of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce and distribute the Software, provided that (i) you distribute the Software complete and unmodified (unless otherwise specified in the applicable README file) and only bundled as part of, and for the sole purpose of running, your Programs, (ii) the Programs add significant and primary functionality to the Software, (iii) you do not distribute additional software intended to replace any omponent(s) of the Software (unless otherwise specified in

the applicable README file), (iv) you do not remove or alter any proprietary legends or notices contained in the Software, (v) you only distribute the Software subject to a license agreement that protects Sun's interests consistent with the terms contained in this Agreement, and (vi) you agree.

3. License to Distribute Redistributables. Subject to the terms and conditions of this Agreement, including but not limited to Section 4 (Java Technology Restrictions) of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce and distribute those files specifically identified as redistributable in the Software "README" file ("Redistributables") provided that: (i) you distribute the Redistributables complete and unmodified (unless otherwise specified in the applicable README file), and only bundled as part of Programs, (ii) you do not distribute additional software intended to supersede any component(s) of the Redistributables (unless otherwise specified in the applicable README file), (iii) you do not remove or alter any proprietary legends or notices contained in or on the Redistributables, (iv) you only distribute the Redistributables pursuant to a license agreement that protects Sun's interests consistent with the terms contained in the Agreement.

4. Java Technology Restrictions. You may not modify the Java Platform Interface ("JPI", identified as classes contained within the "java" package or any subpackages of he "java" package), by creating additional classes within the JPI or otherwise causing the addition to or modification of the classes in the JPI. In the event that you create an additional class and associated API(s) which (i) extends the functionality of the Java platform, and (ii) is exposed to third party software developers for the purpose of developing additional software which invokes such additional API, you must promptly publish broadly an accurate specification for such API for free use by all developers. You may not create, or authorize your licensees to create, additional classes, interfaces, or subpackages that are in any way identified as "java", "javax", "sun" or similar convention as specified by Sun in any naming convention designation.

5. Notice of Automatic Software Updates from Sun. You acknowledge that the Software may automatically download, install, and execute applets, applications, software extensions, and updated versions of the Software from Sun ("Software Updates"), which may require you to accept updated terms and conditions for installation. If additional terms and conditions are not presented on installation, the Software Updates will be considered part of the Software and subject to the terms and conditions of the Agreement.

6. Notice of Automatic Downloads. You acknowledge that, by your use of the Software and/or by requesting services that require use of the Software, the Software may automatically download, install, and execute software applications from sources other than Sun ("Other Software"). Sun makes no representations of a relationship of any kind to licensors of Other Software. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL SUN OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE OTHER SOFTWARE, EVEN IF SUN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. Distribution by Publishers. This section pertains to your distribution of the Software with your printed book or magazine (as those terms are commonly used in the industry) relating to Java technology ("Publication"). Subject to and conditioned upon your compliance with the restrictions and obligations contained in the Agreement, in addition to the license granted in Paragraph 1 above, Sun hereby grants to you a non-exclusive, nontransferable limited right to reproduce complete and unmodified copies of the Software on electronic media (the "Media") for the sole purpose of inclusion and distribution with your Publication(s), subject to the following terms: (i) You may not distribute the Software on a stand-alone basis; it must be distributed with your Publication(s); (ii) You are responsible for downloading the Software from the applicable Sun web site; (iii) You must refer to the Software as JavaTM 2 Software Development Kit, Standard Edition, Version 1.4.1; (iv) The Software must be reproduced in its ent

8. Trademarks and Logos. You acknowledge and agree as between you and Sun that Sun owns the SUN, SOLARIS, JAVA, JINI, FORTE, and iPLANET trademarks and all SUN, SOLARIS, JAVA, JINI, FORTE, and iPLANET-related trademarks, service marks, logos and other brand designations ("Sun Marks"), and you agree to comply with the Sun Trademark and Logo Usage Requirements currently located at http://www.sun.com/policies/trademarks. Any use you make of the Sun Marks inures to Sun's benefit.

9. Source Code. Software may contain source code that is provided solely for reference purposes pursuant to the terms of this Agreement. Source code may not be redistributed unless expressly provided for in this Agreement.

10. Termination for Infringement. Either party may terminate this Agreement immediately should any Software become, or in either party's opinion be likely to become,the subject of a claim of infringement of any intellectual property right.

For inquiries please contact: Sun Microsystems, Inc., 4150Network Circle, Santa Clara, California 95054, U.S.A (LFI#134402/Form ID#011801)

This Product includes software of Apache Software Foundation.

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition,

"control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works hereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

Version 1.1

Copyright (c) 1999-2003 The Apache Software Foundation. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are

permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

The end-user documentation included with the redistribution, if any, must include the following acknowledgment: This product includes software developed by the Apache Software Foundation (http://www.apache.org/). Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.

The names Apache and Apache Software Foundation must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.

Products derived from this software may not be called Apache, nor may Apache appear in their name, without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. For more information on the Apache Software Foundation, please see <http://www.apache.org/>.

Portions of this software are based upon public domain software originally written at the National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign.

NOTE: Some components of the Vantage CNM software incorporate source code covered under the **Apache License**. To obtain the source code covered under the **Apache License**, please contact ZyXEL customer support.

Copyright (c) 2002, 2003 Gargoyle Software Inc. All rights reserved.

This Product includes software-Jboss,yGuard under LGPL

This Product includes J3SSH under LGPL. Copyright (C) 2002 Lee David Painter. All right reserved.

GNU LESSER GENERAL PUBLIC LICENSE

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get

it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License. In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License").

Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables. The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library. Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions: a) The modified work must itself be a software library. b) You must cause the files modified to carry prominent

notices stating that you changed the files and the date of any change. c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License. d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful. (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.) These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote

it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library. In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices. Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy. This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange. If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not

compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables. When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law. If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.) Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications. You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things: a) Accompany the work with the complete corresponding

machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.) b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a

copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with. c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution. d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place. e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy. For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things: a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above. b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to

refrain entirely from distribution of the Library. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing

and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCHDAMAGES.

END OF TERMS AND CONDITIONS

This Product includes MySQl database under GPL.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it. For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software. Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you". Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program. In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.) The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE; THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

All other trademarks or trade names mentioned herein, if any, are the property of their respective owners.

End-User License Agreement for Vantage CNM

WARNING: ZyXEL Communications Corp. IS WILLING TO LICENSE THE ENCLOSED SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AS INSTALLING THE SOFTWARE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN ZyXEL, INC. IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE UNINSTALLED SOFTWARE AND PACKAGING TO THE PLACE FROM WHICH IT WAS ACQUIRED, AND YOUR MONEY WILL BE REFUNDED.

1.Grant of License for Personal Use

ZyXEL Communications Corp. ("ZyXEL") grants you a non-exclusive, non-sublicense, non-transferable license to use the program with which this license is distributed (the "Software"), including any documentation files accompanying the Software ("Documentation"), for internal business use only, for up to the number of users specified in sales order and invoice. You have the right to make one backup copy of the Software and Documentation solely for archival, back-up or disaster recovery purposes. You shall not exceed the scope of the license granted hereunder. Any rights not expressly granted by ZyXEL to you are reserved by ZyXEL, and all implied licenses are disclaimed.

2.Ownership

You have no ownership rights in the Software. Rather, you have a license to use the Software as long as this License Agreement remains in full force and effect. Ownership of the Software, Documentation and all intellectual property rights therein shall remain at all times with ZyXEL. Any other use of the Software by any other entity is strictly forbidden and is a violation of this License Agreement.

3.Copyright

The Software and Documentation contain material that is protected by United States Copyright Law and trade secret law, and by international treaty provisions. All rights not granted to you herein are expressly reserved by ZyXEL. You may not remove any proprietary notice of ZyXEL or any of its licensors from any copy of the Software or Documentation.

4.Restrictions

You may not publish, display, disclose, sell, rent, lease, modify, store, loan, distribute, or create derivative works of the Software, or any part thereof. You may not assign, sublicense, convey or otherwise transfer, pledge as security or otherwise encumber the rights and licenses granted hereunder with respect to the Software. You may not copy, reverse engineer, decompile, reverse compile, translate, adapt, or disassemble the Software, or any part thereof, nor shall you attempt to create the source code from the object code for the Software. You may not market, co-brand, private label or otherwise permit third parties to link to the Software, or any part thereof. You may not use the Software, or any part thereof, in the operation of a service bureau or for the benefit of any other person or entity. You may not cause, assist or permit any third party to do any of the foregoing.

5.Confidentiality

You acknowledge that the Software contains proprietary trade secrets of ZyXEL and you hereby agree to maintain the confidentiality of the Software using at least as great a degree of care as you use to maintain the confidentiality of your own most confidential information. You agree to reasonably communicate the terms and conditions of this License Agreement to those persons employed by you who come into contact with the Software, and to use reasonable best efforts to ensure their compliance with such terms and conditions, including, without limitation, not knowingly permitting such persons to use any portion of the Software for the purpose of deriving the source code of the Software.

6.No Warranty

THE SOFTWARE IS PROVIDED "AS IS." TO THE MAXIMUM EXTENT PERMITTED BY LAW, ZyXEL DISCLAIMS ALL WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. ZyXEL DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET ANY REQUIREMENTS OR NEEDS YOU MAY HAVE, OR THAT THE SOFTWARE WILL OPERATE ERROR FREE, OR IN AN UNINTERUPTED FASHION, OR THAT ANY DEFECTS OR ERRORS IN THE SOFTWARE WILL BE CORRECTED, OR THAT THE SOFTWARE IS COMPATIBLE WITH ANY PARTICULAR PLATFORM. SOME JURISDICTIONS DO NOT ALLOW THE WAIVER OR EXCLUSION OF IMPLIED WARRANTIES SO THEY MAY NOT APPLY TO YOU. IF THIS EXCLUSION IS HELD TO BE UNENFORCEABLE BY A COURT OF COMPETENT JURISDICTION, THEN ALL EXPRESS AND IMPLIED WARRANTIES SHALL BE LIMITED IN DURATION TO A PERIOD OF THIRTY (30) DAYS FROM THE DATE OF PURCHASE OF THE SOFTWARE, AND NO WARRANTIES SHALL APPLY AFTER THAT PERIOD.

7.LIMITATION OF LIABILITY. To the maximum extent permitted by applicable law, in no event shall ZyXEL or its suppliers be liable for any special, incidental, indirect, or consequential damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising out of the use of or inability to use the SOFTWARE or the provision of or failure to provide Support Services, even if ZyXEL has been advised of the possibility of such damages. In any case, ZyXEL's entire liability under any provision of this EULA shall be limited to the greater of the amount actually paid by you for the SOFTWARE; provided, however, if you have entered into a ZyXEL Support Services Agreement, ZyXEL's entire liability regarding Support Services shall be governed by the terms of that agreement.

8.Export Restrictions

THIS LICENSE AGREEMENT IS EXPRESSLY MADE SUBJECT TO ANY APPLICABLE LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS ON THE EXPORT OF THE SOFTWARE OR INFORMATION ABOUT SUCH SOFTWARE WHICH MAY BE IMPOSED FROM TIME TO TIME. YOU SHALL NOT EXPORT THE SOFTWARE, DOCUMENTATION OR INFORMATION ABOUT THE SOFTWARE AND DOCUMENTATION WITHOUT COMPLYING WITH SUCH LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS. YOU AGREE TO INDEMNIFY ZyXEL AGAINST ALL CLAIMS, LOSSES, DAMAGES, LIABILITIES, COSTS AND EXPENSES, INCLUDING REASONABLE ATTORNEYS' FEES, TO THE EXTENT SUCH CLAIMS ARISE OUT OF ANY BREACH OF THIS SECTION 8.

9.Audit Rights

ZyXEL SHALL HAVE THE RIGHT, AT ITS OWN EXPENSE, UPON REASONABLE PRIOR NOTICE, TO PERIODICALLY INSPECT AND AUDIT YOUR RECORDS TO ENSURE YOUR COMPLIANCE WITH THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT.

10.Termination

This License Agreement is effective until it is terminated. You may terminate this License Agreement at any time by destroying or returning to ZyXEL all copies of the Software and Documentation in your possession or under your control. ZyXEL may terminate this License Agreement for any reason, including, but not limited to, if ZyXEL finds that you have violated any of the terms of this License Agreement. Upon notification of termination, you agree to destroy or return to ZyXEL all copies of the Software and Documentation and to certify in writing that all known copies, including backup copies, have been destroyed. All provisions relating to confidentiality, proprietary rights, and non-disclosure shall survive the termination of this Software License Agreement.

12.General

This License Agreement shall be construed, interpreted and governed by the laws of Republic of China without regard to conflicts of laws provisions thereof. The exclusive forum for any disputes arising out of or relating to this License Agreement shall be an appropriate court or Commercial Arbitration Association sitting in ROC, Taiwan. This License Agreement shall constitute the entire Agreement between the parties hereto. This License Agreement, the rights granted hereunder, the Software and Documentation shall not be assigned by you without the prior written consent of ZyXEL. Any waiver or modification of this License Agreement shall only be effective if it is in writing and signed by both parties hereto. If any part of this License Agreement is found invalid or unenforceable by a court of competent jurisdiction, the remainder of this License Agreement shall be interpreted so as to reasonably effect the intention of the parties.

A

Abnormal Working Conditions **2**
Acts of God **2**
Address Assignment **242**
Address Resolution Protocol (ARP) **83**
Advanced Encryption Standard (AES) **168**
AES **168**
Aggressive **183, 270**
AH **168**
Alarms **304**
Alternative Subnet Mask Notation **410**
AP (access point) **420**
Attack Types **214**
Authentication Algorithm **184, 185, 270, 271**
Authentication databases **104**
Authentication Header (AH) **168**

B

bandwidth reports **312**
Basic Service Set **428**
Blocking Time **224**
Brute-force Attack, **214**
BSS **418, 428**
Bypass Triangle Route **221**

C

CA **425**
certificate **193**
Certificate Authority **425**
Channel **420**
  Interference **420**
Charge **2**
Components **2**
Condition **2**
Configuration **80**
Consequential Damages **3**
Contact Information **3**
Contacting Customer Support **3**
Copyright **2**
Cryptography Model **75**
CTS (Clear to Send) **421**
Custom Ports
  Creating/Editing **227**
Customer Support **3**

D

Data Encryption Standard (DES) **168**
Default Policy Log **221**
Defective **2**
DeMilitarized Zone **110**
Denmark, Contact Information **3**
DES **168**
Destination Address **225**
DHCP **75, 80, 81, 84, 87, 250**
Diffie-Hellman (DH) **184, 271**
Direct Sequence Spread Spectrum **428**
Disclaimer **2**
Discretion **2**
Distribution System **429**
Distribution System (DS) **98**
DMZ **110**
  And the Firewall **110**
DNS Server
  For VPN Host **243**
Domain Name **75**
DoS
  Types **212**
DS **429**
DSSS **428**
DTR **127**
Dynamic DNS **250**
Dynamic WEP Key Exchange **425**
Dynamic WEP key exchange **104**
DYNDNS Wildcard **243, 250**

E

EAP **92**
EAP Authentication **424**
Encapsulating Security Payload (ESP) **168**
Encapsulation **185, 271**
encrymode **75**
Encryption **426**
Encryption Algorithm **184, 185, 270, 271**
EnterSee Syntax Conventions **35**
Equal Value **2**
ESP **168**
ESS **419, 429**
ESSID (Extended Service Set Identification) **95**
Extended Service Set **419, 429**

F

Factory LAN Defaults **80**
Failure **2**
FHSS **428**
Finland, Contact Information **3**
Firewall
  Address Type **226**
  Firewall Vs Filters **219**
  Guidelines For Enhancing Security **219**
  When To Use **220**
Fitness **3**
Fragmentation Threshold **421**
Fragmentation threshold **421**
France, Contact Information **4**

Frequency-Hopping Spread Spectrum **428**
FTP **80, 149, 250**
Functionally Equivalent **2**

G

Germany, Contact Information **4**
God, act of **2**

H

Hidden node **420**
Host IDs **408**

I

IBSS **418, 428**
ICMP echo **214**
IEEE 802.11g **422**
IGMP **81, 82**
Independent Basic Service Set **418, 428**
Indirect Damages **3**
initialization vector (IV) **426**
Inside Local Address **144**
Insurance **3**
Internet Control Message Protocol (ICMP) **214**
IP Address **81, 85, 88**
IP Pool **84, 87**
IP Pool Setup **80**
IP Spoofing **212, 215**
IPSec algorithms **168**
IPSec and NAT **169**
IPSec architecture **167**

K

Key Group **184, 271**

L

Labor **2**
LAN TCP/IP **80**
LAND **212, 213**
Legal Rights **3**
Liability **2**
License **2**
Local user database **107**

M

MAC (Hex **74**
MAC (Media Access Control) address. **96**
MAC Address Filter Action **97**
MAC Address Filtering **96**
MAC filter **93**
Main **183, 270**
Many to Many No OverloadSee NAT **145**
Many to Many OverloadSee NAT **145**
Many to OneSee NAT **145**
Materials **2**
Maximum Burst Size **132**
Maximum Incomplete High **223**
Maximum Incomplete Low **223**
Max-incomplete Low **223**
MD5 **184, 185, 270, 271**
Merchantability **3**
Message Integrity Check (MIC) **426**
Metric **115, 164**
Multicast **81, 86, 88**

N

Name **181**
NAT **149**
    Definitions **144**
    How NAT Works **145**
    Mapping Types **145**
    What NAT does **145**
NAT traversal **174**
NetBIOS commands **215**
New **2**
North America Contact Information **4**
Norway, Contact Information **4**

O

One Minute High **223**
One Minute Low **223**
One to OneSee NAT **145**
Operating Condition **2**
Out-dated Warranty **3**

P

Packet Filtering **219**
Pairwise Master Key (PMK) **426**
Parts **2**
Patent **2**
Peak Cell Rate **132**
Perfect Forward Secrecy (PFS **185, 272**
Permission **2**
Photocopying **2**
Ping of Death **212**
Point-to-Point Tunneling ProtocolSee PPTP **120**
Port Configuration **227**
Postage Prepaid. **3**
Preamble Mode **422**
Pre-Shared Key **193, 266**
    Format **98**
Product Model **3**
Product Serial Number **3**

Products 2
Proof of Purchase 2, 3
Proper Operating Condition 2
Public Servers 110
Purchase, Proof of 2
Purchaser 3

R

Radio frequency 95
RADIUS 423
  Shared Secret Key 424
RADIUS Message Types 423
RADIUS Messages 423
Read Me First 34
Registered 2
Registered Trademark 2
Regular Mail 3
Related Documentation 34
Re-manufactured 2
Repair 2, 3
Replace 2
Replacement 2, 3
Reproduction 2
Restore 2
Return Material Authorization (RMA) Number 3
Returned Products 3
Returns 3
RF signals 428
Rights 2
Rights, Legal 3
RIP 81
RMA 3
RTS (Request To Send) 421
RTS (Request To Send) threshold 96
RTS Threshold 420, 421

S

SA Life Time 184, 185, 270, 271
Saving the State 215
Secret Key 75
Security Parameters 427
SelectSee Syntax Conventions 35
Serial Number 3
Server 77, 145, 146
Service 3
service reports 312
Service Type 227
Services 150
SHA-1 (Secure Hash Algorithm) 184, 185, 270, 271
Shipping 3
Smurf 214
Source Address 225
Spain, Contact Information 4
Stateful Inspection 215, 216
  Process 216
  ZyWALL 217
SUA 149
Subnet Mask 81, 85, 88, 226
Subnet Masks 409
Support E-mail 3
Supporting Disk 34
Sustained Cell Rate 132
Sweden, Contact Information 4
SYN Flood 212, 213
SYN-ACK 213
Syntax Conventions 34

T

Tampering 2
TCP Maximum Incomplete 224
TCP Security 217
TCP/IP 85, 88, 212
Teardrop 212
Telephone 3
Temporal Key Integrity Protocol (TKIP) 426
Three-Way Handshake 213
Traceroute 215
Trademark 2
Trademark Owners 2
Trademarks 2
Traffic Redirect 124, 137
Traffic Shapping 132
Translation 2
Transport mode 169, 185, 271
Tunnel mode 169, 185, 271

U

UDP/ICMP Security 218
Upper Layer Protocols 217, 218
User Authentication 426
User Name 76
User Profiles 107

V

Value 2
VPN 120
  encapsulation 168
  key management 168
  secure gateway 173
VPN Editor 309

W

WAN Backup 137
Warranty 2
Warranty Information 3

Warranty Period 2
Web Configurator 219
Web Site 3
WEP encryption 94
Wi-Fi Protected Access 97
Wireless Client WPA Supplicants 99
Wireless LAN
  Configuring 94
Wireless security 92
WLAN
  Interference 420
  Security parameters 427
Workmanship 2
Worldwide Contact Information 3
WPA 97
  Supplicants 99
  with RADIUS Application Example 98
WPA -Pre-Shared Key 98
WPA with RADIUS Application 98
WPA-PSK 98
WPA-PSK Application 98
Written Permission 2

Z

ZyNOS 2
ZyXEL Limited Warranty
  Note 3
ZyXEL Network Operating System 2