

Vantage CNM 2.0

Centralized Network Management

User's Guide

Version 2.0.00.81.10

2.0.00.61.10

July 2004

ZyXEL
Unleash Networking Power

Copyright

Copyright © 2004 by ZyXEL Communications Corporation.

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

Published by ZyXEL Communications Corporation. All rights reserved.



Note: Refer also to the *“Open Software Announcements”* on page 316.

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 that (a) the Vantage CNM 2.0 software (henceforth called the SOFTWARE) will perform substantially in accordance with the accompanying written materials for a period of ninety (90) days from the date of receipt, and (b) any Support Services provided by ZyXEL shall be substantially as described in applicable written materials provided to you by ZyXEL, and ZyXEL support engineers will make commercially reasonable efforts to solve any problem issues. To the extent allowed by applicable law, implied warranties on the SOFTWARE, if any, are limited to ninety (90) days.

CUSTOMER REMEDIES.

ZyXEL's and its suppliers' entire liability and your exclusive remedy shall be, at ZyXEL's option, either (a) return of the price paid, if any, or (b) repair or replacement of the SOFTWARE that does not meet ZyXEL's Limited Warranty and which is returned to ZyXEL with a copy of your receipt. This Limited Warranty is void if failure of the SOFTWARE has resulted from accident, abuse, or misapplication. Any replacement SOFTWARE will be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer. Outside Taiwan, neither these remedies nor any product support services offered by ZyXEL are available without proof of purchase from an authorized international source.

NO OTHER WARRANTIES.

To the maximum extent permitted by applicable law, ZyXEL and its suppliers disclaim all other warranties and conditions, either express or implied, including, but not limited to, implied warranties of merchantability, fitness for a particular purpose, title, and non-infringement, with regard to the SOFTWARE, and the provision of or failure to provide Support Services. This limited warranty gives you specific legal rights. You may have others, which vary from state/jurisdiction to state/jurisdiction.

Please read the license screen in the installation wizard. You must accept the terms of the license in order to install Vantage CNM.

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 LOCATION	SUPPORT E-MAIL	TELEPHONE ^A	WEB SITE	REGULAR MAIL
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	
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	
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		
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		
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		
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		
NORWAY	support@zyxel.no	+47 22 80 61 80	www.zyxel.no	ZyXEL Communications A/S NielsHansensvei13 0667Oslo Norway
	sales@zyxel.no	+47 22 80 61 81		
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		
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		

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

Table of Contents

Copyright	2
ZyXEL Limited Warranty	3
Customer Support.....	4
List of Tables	24
Preface	28
Introducing Vantage Centralized Network Management (CNM) 2.0	28
Chapter 1	
Introducing Vantage.....	30
1.1 Key Features	30
1.1.1 Object Tree View	30
1.1.2 Flexible Friendly Device Registration	30
1.1.3 Building Blocks	30
1.1.4 Multiple Domain Administration	30
1.1.5 Complete Device Configuration	30
1.1.6 Configuration Synchronization	30
1.1.7 Firewall	31
1.1.8 One-Click VPN	31
1.1.9 Configuration File Management	31
1.1.10 Firmware Upgrade	31
1.1.11 Monitoring and Notifications	31
1.1.12 Logs	31
1.1.13 Data Maintenance	31
1.1.14 Vantage System Management	31
1.1.15 License Management	31
1.2 Vantage Requirements and Installation	32
Chapter 2	
GUI Introduction.....	34
2.1 Overview	34
2.1.1 Object Pane	34
2.2 Object Tree View Types	35
2.3 Searches	35

2.4 Folders	35
2.5 Devices	38
2.6 Content Pane	38
2.6.1 Object Path	38
2.6.2 Menu Path	38
2.7 Menu Overview	38
2.8 Procedure For Configuring A Device	39
2.9 Context-Sensitive Menus	40
2.10 Icon Key	40
Chapter 3	
Device Menus	44
3.1 Device Menus Overview	44
3.1.1 Device Main Screen	44
3.2 Device Status	46
3.3 Device Registration	46
3.3.1 Manual Option	48
3.3.1.1 Configuring ZyXEL Device using Commands	48
3.3.1.2 Configuring ZyXEL Device using Web Configurator	48
3.3.2 Import From an XML Registration File	49
3.3.2.1 Basic XML Syntax	50
3.3.2.2 Minimum Mandatory Device Settings	51
3.4 Device – Vantage Data Inconsistency: Synchronize	52
3.4.1 Vantage – Device Override Criteria	53
3.4.1.1 Vantage CNM Override Device	53
3.4.1.2 Device Override Vantage CNM	53
3.4.1.3 Synchronizing Device with Vantage	53
3.5 Firmware Management	53
3.5.1 Add Firmware Screen	54
3.5.2 Firmware Upgrade Select Product Line and Mode	55
3.5.3 Firmware Upgrade Process	56
3.5.4 Advisory Notes on Firmware Upgrade	56
3.5.5 Configuration File	56
3.5.6 Configuration File Management	57
3.5.7 Configuration File Backup	57
3.5.8 Configuration File Restore	58
Chapter 4	
Configuration > Select Device BB & General	60
4.1 Select Device BB	60
4.1.1 Procedure to Select and Apply a Device BB	62
4.2 Configuration General Screens	62
4.2.1 System	63

4.2.2 DDNS	64
4.2.3 Time Setting	66
4.2.4 Owner Info	67

Chapter 5

Configuration > LAN 70

5.1 LAN Overview	70
5.2 DHCP Setup	70
5.2.1 IP Pool Setup	70
5.2.2 DNS Servers	70
5.2.3 LAN TCP/IP	70
5.2.4 Factory LAN Defaults	70
5.2.5 IP Address and Subnet Mask	71
5.2.6 RIP Setup	71
5.2.7 Multicast	71
5.3 Configuring LAN IP – ZyWALL	72
5.4 Configuring LAN IP - Prestige	75
5.5 Configuring LAN Static DHCP – ZyWALL	77
5.6 Configuring LAN IP Alias – ZyWALL	78

Chapter 6

Configuration > WLAN 82

6.1 Wireless LAN Overview	82
6.1.1 Additional Installation Requirements for using 802.1x	82
6.2 Wireless LAN Basics	82
6.2.1 Channel	82
6.2.2 ESS ID	82
6.2.3 RTS/CTS	83
6.2.4 Fragmentation Threshold	84
6.2.5 WEP	84
6.3 Configuring Wireless LAN	84
6.3.1 WLAN Wireless	85
6.4 Configuring MAC Filter	86
6.5 802.1x Overview	87
6.5.1 Configuring 802.1x – ZyWALL	88
6.5.2 Configuring 802.1x – Prestige	88
6.6 Local User Database	90
6.6.1 Configuring Local User Database	90
6.6.2 RADIUS	91
6.6.2.1 Types of RADIUS Messages	92
6.6.3 EAP Authentication Overview	92
6.7 Configuring RADIUS	93

Chapter 7	
Configuration > DMZ	96
7.1 DMZ Overview	96
7.2 DMZ Addresses	96
7.3 Configuring DMZ	96
Chapter 8	
Configuration > WAN	100
8.1 General WAN – ZyWALL	100
8.1.1 TCP/IP Priority (Metric)	100
8.1.2 WAN ISP – ZyWALL	102
8.1.2.1 Ethernet Encapsulation	102
8.1.2.2 PPPoE Encapsulation	103
8.1.2.3 PPTP Encapsulation	105
8.2 WAN IP – ZyWALL	107
8.3 Dial Backup – ZyWALL	108
8.3.1 Traffic Redirect	109
8.3.2 Configuring Dial Backup - ZyWALL	109
8.3.3 Advanced Modem Setup – ZyWALL	112
8.3.3.1 AT Command Strings	112
8.3.4 Edit Dial Backup – ZyWALL	114
8.4 General WAN – Prestige	116
8.4.1 Traffic Shaping	117
8.4.2 Configuring Prestige WAN Setup	117
8.4.3 WAN Backup - Prestige	122
8.4.3.1 Traffic Redirect	122
8.4.4 Configuring WAN Backup - Prestige	122
8.4.5 Configuring Advanced WAN Backup – Prestige	125
8.4.6 Advanced Modem Setup – Prestige	128
Chapter 9	
Configuration > NAT	130
9.1 NAT Overview	130
9.1.1 NAT Definitions	130
9.1.2 What NAT Does	131
9.1.3 How NAT Works	131
9.1.4 NAT Mapping Types	131
9.1.5 SUA (Single User Account) Versus NAT	132
9.2 Configuring NAT	132
9.2.1 Disable NAT	133
9.3 SUA Servers	133
9.3.1 Port Forwarding: Services and Port Numbers	134
9.3.2 Configuring SUA Servers – ZyWALL	134

9.3.3 Configuring SUA Servers – Prestige	136
9.3.4 Full Feature Address Mapping	137
9.3.5 Edit Full Feature Address Mapping	138
9.4 Trigger Port Forwarding – ZyWALL	139
9.4.1 Configuring Trigger Port	140
9.4.2 Edit Trigger Port	142

Chapter 10

Configuration > Static Route..... 144

10.1 Static Route Overview	144
10.1.1 Static Route Summary	144
10.1.2 Edit Static Route	145

Chapter 11

Configuration > VPN 148

11.1 VPN Overview	148
11.1.1 IPSec	148
11.1.2 Security Association	148
11.1.3 Encryption	148
11.1.4 Data Confidentiality	148
11.1.5 Data Integrity	148
11.1.6 Data Origin Authentication	149
11.1.7 IPSec Algorithms	149
11.1.7.1 AH (Authentication Header) Protocol	149
11.1.7.2 ESP (Encapsulating Security Payload) Protocol	149
11.1.8 Key Management	150
11.1.9 Encapsulation	150
11.1.9.1 Transport Mode	150
11.1.9.2 Tunnel Mode	150
11.1.10 IPSec and NAT	151
11.1.11 Keep Alive	151
11.1.12 NAT Traversal	152
11.1.12.1 NAT Traversal Configuration	152
11.1.13 ID Type and Content	152
11.1.14 IKE Phases	153
11.1.15 Negotiation Mode	154
11.1.16 Diffie-Hellman (DH) Key Groups	154
11.1.17 Perfect Forward Secrecy (PFS)	155
11.1.18 Pre-Shared Key	155
11.2 VPN Tunnel Summary	155
11.2.1 Add a VPN Tunnel	156
11.2.2 Manual VPN Tunnel	161
11.3 VPN and NetBIOS	164

Chapter 12	
Configuration > Firewall	166
12.1 Firewall Overview	166
12.2 Types of Firewalls	166
12.2.1 Packet Filtering Firewalls	166
12.2.2 Application-level Firewalls	166
12.2.3 Stateful Inspection Firewalls	167
12.3 Introduction to ZyXEL's Firewall	167
12.3.1 Denial of Service	168
12.3.2 Basics	168
12.3.3 Types of DoS Attacks	168
12.4 Stateful Inspection	170
12.4.1 Stateful Inspection Process	171
12.4.2 Stateful Inspection and the ZyXEL device	172
12.4.3 TCP Security	172
12.4.4 UDP/ICMP Security	173
12.4.5 Upper Layer Protocols	173
12.4.6 Firewall Policies Overview	173
12.4.7 Rule Checklist	175
12.4.8 Security Ramifications	175
12.4.9 Key Fields For Configuring Rules	176
12.4.9.1 Action	176
12.4.9.2 Service	176
12.4.9.3 Source Address	176
12.4.9.4 Destination Address	176
12.4.10 Alerts	176
12.4.11 Services and Port Numbers	176
12.5 Firewall Configuration Screens	177
12.5.1 Firewall Summary Screen	177
12.5.1.1 Ordering Rules	177
12.5.2 DoS Settings	179
12.5.3 Add/Edit a Firewall Rule	181
12.5.4 Add/Edit Source/Destination IP Addresses	183
12.5.5 Custom Ports	184
Chapter 13	
Configuration > Device Log	186
13.1 Device Logs	186
13.2 Device Logging Options	187
13.3 Purge Logs	189

Chapter 14	
Configuration > ADSL Monitor	192
14.1 Introduction	192
14.2 Configuring ADSL Monitor	192
Chapter 15	
Configuration > Device Alarms	194
15.1 Device Alarms	194
15.1.1 Alarm Classifications	194
15.1.2 Alarm States	194
15.1.3 Current Alarms Screen	195
15.1.4 Historical Alarms Screen	196
Chapter 16	
Building Blocks (BBs)	198
16.1 Categories	198
16.2 BB Properties	198
16.3 Configuring Device BB Menus	198
16.3.1 Editing an Existing BB	199
16.3.2 Device BB Configuration Select	200
16.3.3 Adding a New BB	200
16.4 Configuration BBs	201
16.4.1 Adding a Configuration BB	202
16.4.2 Editing a Configuration BB	203
16.5 Component BBs	204
16.5.1 Adding a Component BB	205
16.5.1.1 Adding a Component BB: IP Type	205
16.5.1.2 Adding a Component BB: E-mail Type	206
16.5.2 Editing a Component BB	207
Chapter 17	
System > Administrators	208
17.1 Introduction to Administrators	208
17.1.1 Administrator Types	208
17.1.1.1 “Root” Administrator	208
17.1.1.2 “Super” Administrators	209
17.1.1.3 “Normal” Administrators	209
17.1.1.4 “Custom” Administrators	209
17.2 Configuring Administrators	209
17.3 Creating an Administrator Account	210
17.3.1 Administrator Details	210
17.3.2 Administrator Permissions	212

Chapter 18	
Other System Screens	214
18.1 Status	214
18.2 Vantage Upgrade	215
18.2.1 Upgrade Procedure	215
18.2.2 Version Format	217
18.3 License Management	218
18.3.1 License Upgrade	218
18.4 System >Preferences	219
18.4.1 General Vantage Preferences	219
18.4.2 User Access	220
18.4.3 Servers	221
18.4.3.1 Vantage Server Public IP Address	224
18.4.4 Notifications	225
18.4.5 Vantage Permissions: User Group	226
18.4.5.1 Add User Group	226
18.5 System Maintenance	228
18.5.1 System Maintenance Management	228
18.5.2 Back Up System Maintenance	228
18.5.3 Restore System Maintenance	229
18.6 Address Book	230
18.6.1 Address Book Add/Edit	231
18.7 Certificate Management Overview	232
18.7.1 Advantages of Certificates	233
18.7.2 Current Certification Information	233
18.7.3 Create a Certificate	235
18.7.4 Importing Certificates	235
18.8 Vantage Logs	236
18.8.1 CNM Server	236
18.8.2 Vantage Logging Options	237
18.9 About Vantage	238
Chapter 19	
Monitor > Alarms	240
19.1 Alarms	240
19.1.1 Alarm Types	240
19.1.2 Alarm Classifications	240
19.1.3 Alarm States	241
19.1.4 Current Alarms Screen	241
19.1.5 Historical Alarms	243

Chapter 20	
Other Monitor Screens	246
20.1 Firmware Upgrade Report	246
20.2 Status Monitor	246
20.3 VPN Editor	247
20.3.1 Graphical VPN Tunnel Creation	247
20.3.2 Graphical Tunnel Depictions	249
20.3.3 Map	250
Appendix A	
FTP Server (WFTPD) Setup Example	252
Installing WFTPD	252
Running WFTPD	255
WFTPD main screen.....	255
Appendix B	
Configuring the Kiwi Syslog Daemon	258
Installing the Kiwi Syslog Daemon	258
Importing the Syslog Configuration File	259
Starting the Telnet Service	261
Setting Up the Syslog Server in Vantage	262
Appendix C	
FTP and syslog Server Overview	264
Introduction	264
Appendix D	
Java Console Debug Messages.....	266
Introduction	266
Appendix E	
IP Subnetting.....	270
IP Addressing.....	270
IP Classes	270
Subnet Masks	271
Subnetting	271
Example: Two Subnets	272
Example: Four Subnets.....	274
Example Eight Subnets.....	275
Subnetting With Class A and Class B Networks.	276
Appendix F	

Setting up Your Computer's IP Address.....	278
Windows 95/98/Me.....	278
Installing Components.....	279
Configuring.....	280
Verifying Settings	281
Windows 2000/NT/XP	281
Verifying Settings	285
Macintosh OS 8/9.....	285
Verifying Settings	287
Macintosh OS X	287
Verifying Settings	288
Appendix G	
Virtual Circuit Topology	290
Introduction	290
Appendix H	
Wireless LAN and IEEE 802.11	292
Benefits of a Wireless LAN	292
IEEE 802.11	292
Ad-hoc Wireless LAN Configuration.....	293
Infrastructure Wireless LAN Configuration.....	293
Appendix I	
Wireless LAN With IEEE 802.1x	296
Security Flaws with IEEE 802.11	296
Deployment Issues with IEEE 802.11	296
IEEE 802.1x	296
Advantages of the IEEE 802.1x	296
RADIUS Server Authentication Sequence.....	297
Appendix J	
Types of EAP Authentication	298
Introduction	298
EAP-MD5 (Message-Digest Algorithm 5).....	298
EAP-TLS (Transport Layer Security).....	298
EAP-TTLS (Tunneled Transport Layer Service)	298
PEAP (Protected EAP).....	299
LEAP	299
Appendix K	
Log Descriptions	300

Introduction	300
Appendix L	
Open Software Announcements.....	316
Notice	316
Copyright (C) 1999-2001 Intalio, Inc. All Rights Reserved.....	316
Common Public License Version 1.0	317
Cryptix General License.....	321
TECHNOLOGY LICENSE FROM SUN MICROSYSTEMS, INC. TO DOUG LEA.....	322
JAVA Software Technologies.....	323
Apache License.....	325
Copyright (c) 2002, 2003 Gargoyle Software Inc. All rights reserved.	330
GNU LESSER GENERAL PUBLIC LICENSE	331
GNU GENERAL PUBLIC LICENSE.....	338
End-User License Agreement for Vantage CNM.....	343
Index.....	348

List of Figures

Figure 1	Main Screen	34
Figure 2	Object Tree View Types	35
Figure 3	Details Screen	35
Figure 4	Folder Right-Click Options	36
Figure 5	Add Devices	36
Figure 6	Associate Administrators	37
Figure 7	Associated Administrator Right-Click Options	37
Figure 8	Add New Folder Group Name	37
Figure 9	Account Folder Alarm Right-Click Options	38
Figure 10	Device Right-Click Options	38
Figure 11	Java Applet Window	40
Figure 12	Device > Status > Main Screen	45
Figure 13	Device > Status > Single Device	46
Figure 14	Device > Registration Wizard > Account Association	47
Figure 15	Device > Registration > Owner Selection	47
Figure 16	Device > Registration > Wizard Choices	48
Figure 17	Device > Registration > Manual Registration	49
Figure 18	Registration Wizard: Configuration File	52
Figure 19	.Registration: XML File Devices	52
Figure 20	Registration Wizard: Finish	52
Figure 21	Device > Synchronize	53
Figure 22	Device > Firmware Management	54
Figure 23	Device > Firmware Management > Add Firmware	55
Figure 24	Device Firmware Upgrade	55
Figure 25	TypeView	55
Figure 26	Firmware Upgrade > Select Product Line and Model	56
Figure 27	Device > Firmware Upgrade	56
Figure 28	Device > Configuration File > Management	57
Figure 29	Device > Configuration File > Back Up	58
Figure 30	Device > Configuration File > Restore	59
Figure 31	ZyWALL 10W Device BB	61
Figure 32	ZyWALL 70/35/5 Device BB	61
Figure 33	Configuration > General > System – ZyWALL	63
Figure 34	Configuration > General > DDNS	65
Figure 35	Configuration > General > Time Setting	66
Figure 36	Configuration > General > Owner Info	67

Figure 37	Configuration > LAN > IP – ZyWALL	73
Figure 38	Configuration > LAN > IP – Prestige	76
Figure 39	Configuration > LAN > Static DHCP – ZyWALL	78
Figure 40	Configuration > LAN > IP Alias	79
Figure 41	RTS Threshold	83
Figure 42	Configuration > WLAN > Wireless	85
Figure 43	Configuration > WLAN > MAC Filter	87
Figure 44	Configuration > WLAN > 802.1x – ZyWALL	88
Figure 45	Configuration > WLAN > 802.1x – Prestige	89
Figure 46	Configuration > WLAN > Local User	91
Figure 47	Configuration > WLAN > RADIUS	94
Figure 48	Configuration > DMZ	97
Figure 49	Configuration > WAN > General – ZyWALL	101
Figure 50	Configuration > WAN > ISP (Ethernet) – ZyWALL	102
Figure 51	Configuration > WAN > ISP (PPPoE) – ZyWALL	104
Figure 52	Configuration > WAN > ISP (PPTP) – ZyWALL	105
Figure 53	Configuration > WAN > IP – ZyWALL	107
Figure 54	Traffic Redirect WAN Setup	109
Figure 55	Traffic Redirect LAN Setup	109
Figure 56	Configuration > WAN > Dial Backup – ZyWALL	110
Figure 57	Configuration > WAN > Dial Backup > Advanced – ZyWALL	113
Figure 58	Configuration > WAN > Dial Backup > Edit – ZyWALL	115
Figure 59	Example of Traffic Shaping	117
Figure 60	Configuration > WAN > Setup – Prestige – Bridge Mode	118
Figure 61	Configuration > WAN > Setup – Prestige – Routing Mode	120
Figure 62	Configuration > WAN > Backup – Prestige	123
Figure 63	Advanced WAN Backup – Prestige	126
Figure 64	Configuration > NAT	133
Figure 65	Configuration > NAT > SUA Server – ZyWALL	135
Figure 66	Configuration > NAT > SUA Server – Prestige	136
Figure 67	Configuration > NAT > Full Feature > Address Mapping	137
Figure 68	Configuration > NAT > Full Feature > Edit Address Mapping	139
Figure 69	Configuration > NAT > Full Feature > Trigger Port	141
Figure 70	Configuration > NAT > Full Feature > Trigger Port > Edit	142
Figure 71	Configuration > Static Route	145
Figure 72	Configuration > Static Route > Edit	146
Figure 73	Configuration > VPN	155
Figure 74	Configuration > VPN > Tunnel IPsec Detail	157
Figure 75	Configuration > VPN > Manual Tunnel IPsec Detail	162
Figure 76	Configuration > VPN > NetBIOS	164
Figure 77	Configuration > Firewall	178
Figure 78	Configuration > Firewall > DoS Settings	180
Figure 79	Configuration > Firewall > Edit	182

Figure 80	Configuration >Firewall > IP Address	183
Figure 81	Firewall Custom Port	184
Figure 82	Configuration > Device Log > Device	186
Figure 83	Configuration > Device Logs > Log Settings	188
Figure 84	Purge Device Logs	190
Figure 85	Configuration > ADSL Monitor	193
Figure 86	Configuration > Device Alarms >Current	195
Figure 87	Configuration > Device Alarms > Historical	196
Figure 88	Building Block > Device BB	199
Figure 89	Building Block > Device BB > Edit	199
Figure 90	Building Block > Device BB > Edit > Configuration	200
Figure 91	Building Block > Device BB > Add	201
Figure 92	Building Block > Configuration	201
Figure 93	Building Block > Configuration BB > Add	202
Figure 94	Building Block > Configuration BB > Add > Next	203
Figure 95	Building Block > Configuration BB > Added	203
Figure 96	Building Block > Configuration BB > Edit	204
Figure 97	Building Block > Component BB	204
Figure 98	Building Block > Component BB > Add	205
Figure 99	Building Block > Component BB > Add > IP Address	206
Figure 100	Building Block > Component BB > Add > E-Mail Address	206
Figure 101	Component BBs Added	207
Figure 102	Building Block > Component BB > Edit	207
Figure 103	System > View Administrator List	210
Figure 104	System > Administrator Details	211
Figure 105	System > Administrator Permissions	212
Figure 106	System > Vantage Status	214
Figure 107	System > Upgrade > Online Administrators	216
Figure 108	System > Upgrade > Vantage Upgrade	216
Figure 109	System > Upgrade > Vantage Upgrade > Next	217
Figure 110	System > Upgrading	217
Figure 111	System > License > License Management	218
Figure 112	System > License > License Management > Upgrade	219
Figure 113	System > Preferences > General System	220
Figure 114	System > Preferences > User Access	221
Figure 115	System > Preferences > Server	223
Figure 116	Vantage Icon - Stop	224
Figure 117	Figure 2-5 Vantage Icon - Start	224
Figure 118	System > Preferences > Notifications	225
Figure 119	System > Preferences > User Group	226
Figure 120	System > Preferences > Permissions > Add	227
Figure 121	System > Maintenance > Management	228
Figure 122	System > Maintenance > Backup	229

Figure 123	System > Maintenance > Restore	230
Figure 124	System > Address Book	231
Figure 125	System > Address Book Add/Edit	232
Figure 126	System > Certificate Management > Information	234
Figure 127	System > Certificate Management > Create CSR	235
Figure 128	System > Certificate Management > Import Certificate	236
Figure 129	System > Logs > CNM Server	237
Figure 130	System > Logging Options	238
Figure 131	System > About Vantage	238
Figure 132	Monitor > Current Alarms	242
Figure 133	Monitor > Historical Alarms	244
Figure 134	Monitor > Firmware Upgrade Report	246
Figure 135	Monitor > Monitor Status	247
Figure 136	Monitor > VPN Editor > Tunnel IPsec Detail	248
Figure 137	Configuration > VPN - Example Tunnel Summary	249
Figure 138	Monitor > VPN Monitor – Graphical Tunnel	250
Figure 139	Monitor > VPN > Add MAP	250
Figure 140	Setup	252
Figure 141	Wizard 1	252
Figure 142	Information	253
Figure 143	Installation Type	253
Figure 144	Installation Directory	254
Figure 145	Create Directory	254
Figure 146	Begin Installation	254
Figure 147	Run WFTPD	255
Figure 148	WFTPD Main Screen	255
Figure 149	Windows Services	256
Figure 150	WFTPD Properties	256
Figure 151	WFTPD Pro Log On	257
Figure 152	Kiwi Syslog Daemon Installation: License Agreement	258
Figure 153	Kiwi Installation: Installation Options	259
Figure 154	Kiwi Installation: Installation Directory	259
Figure 155	Kiwi Syslog Daemon Setup	260
Figure 156	Kiwi Syslog Daemon Setup: Import Configuration File	260
Figure 157	Kiwi Syslog Daemon Setup: Import Configuration File: Confirm	261
Figure 158	Windows XP: My Computer	261
Figure 159	Windows XP: Computer Management	262
Figure 160	Vantage System Servers	263
Figure 161	Control Panel Java Plug-in Icon	266
Figure 162	Java Plug-in Control Panel	267
Figure 163	Java Plug-in Icon	267
Figure 164	Open Control Panel	267
Figure 165	Java Console	268

Figure 166	Windows 95/98/Me: Network: Configuration	279
Figure 167	Windows 95/98/Me: TCP/IP Properties: IP Address	280
Figure 168	Windows 95/98/Me: TCP/IP Properties: DNS Configuration	281
Figure 169	Windows XP: Start Menu	282
Figure 170	Windows XP: Control Panel	282
Figure 171	Windows XP: Control Panel: Network Connections: Properties	283
Figure 172	Windows XP: Local Area Connection Properties	283
Figure 173	Windows XP: Advanced TCP/IP Settings	284
Figure 174	Windows XP: Internet Protocol (TCP/IP) Properties	285
Figure 175	Macintosh OS 8/9: Apple Menu	286
Figure 176	Macintosh OS 8/9: TCP/IP	286
Figure 177	Macintosh OS X: Apple Menu	287
Figure 178	Macintosh OS X: Network	288
Figure 179	Virtual Circuit Topology	290
Figure 180	Peer-to-Peer Communication in an Ad-hoc Network	293
Figure 181	ESS Provides Campus-Wide Coverage	294
Figure 182	Sequences for EAP MD5–Challenge Authentication	297

List of Tables

Table 1	Menus Overview	39
Table 2	Object Tree Icons	40
Table 3	Pop-up Menus Icons	41
Table 4	Content Pane Icons	41
Table 5	VPN Editor Icons	42
Table 6	Device > Status > Main Screen	45
Table 7	Device > Status > Single Device	46
Table 8	Device > Registration > Manual Registration	49
Table 9	Device > Firmware Management	54
Table 10	Device > Configuration File > Management	57
Table 11	Device > Configuration File > Back Up	58
Table 12	Device > Configuration File > Restore	59
Table 13	Configuration > General > System – ZyWALL	63
Table 14	Configuration > General > DDNS	65
Table 15	Configuration > General > Time Setting	66
Table 16	Configuration > General > Owner Info	67
Table 17	Configuration > LAN > IP – ZyWALL	73
Table 18	Configuration > LAN > IP – Prestige	76
Table 19	Configuration > LAN > Static DHCP – ZyWALL	78
Table 20	Configuration > LAN > IP Alias	79
Table 21	Configuration > WLAN > Wireless	85
Table 22	Configuration > WLAN > MAC Filter	87
Table 23	Configuration > WLAN > 802.1x – ZyWALL	88
Table 24	Configuration > WLAN > 802.1x – Prestige	89
Table 25	Configuration > WLAN > Local User	91
Table 26	Configuration > WLAN > RADIUS	94
Table 27	Configuration > DMZ	97
Table 28	Configuration > WAN > General – ZyWALL	101
Table 29	Configuration > WAN > ISP (Ethernet) – ZyWALL	102
Table 30	Configuration > WAN > ISP (PPPoE) – ZyWALL	104
Table 31	Configuration > WAN > ISP (PPTP) – ZyWALL	105
Table 32	Configuration > WAN > IP – ZyWALL	107
Table 33	Configuration > WAN > Dial Backup – ZyWALL	110
Table 34	Configuration > WAN > Dial Backup > Advanced – ZyWALL	113
Table 35	Configuration > WAN > Dial Backup > Edit – ZyWALL	115
Table 36	Configuration > WAN > Setup – Prestige – Bridge Mode	118
Table 37	Configuration > WAN > Setup – Prestige – Routing Mode	120
Table 38	WAN Backup – Prestige	123

Table 39	Advanced WAN Backup – Prestige	126
Table 40	NAT Definitions	130
Table 41	NAT Mapping Types	132
Table 42	Configuration > NAT	133
Table 43	Services and Port Numbers	134
Table 44	Configuration > NAT > SUA Server	135
Table 45	Configuration > NAT > SUA Server – Prestige	136
Table 46	Configuration > NAT > Full Feature > Address Mapping	137
Table 47	Configuration > NAT > Full Feature > Edit Address Mapping	139
Table 48	Configuration > NAT > Full Feature > Trigger Port	141
Table 49	Configuration > NAT > Full Feature > Trigger Port > Edit	142
Table 50	Configuration > Static Route	145
Table 51	Configuration > Static Route > Edit	146
Table 52	AH and ESP	149
Table 53	VPN and NAT	151
Table 54	Local ID Type and Content Fields	153
Table 55	Peer ID Type and Content Fields	153
Table 56	Configuration > VPN	155
Table 57	Configuration > VPN > Tunnel IPSec Detail	157
Table 58	Configuration > VPN > Manual Tunnel IPSec Detail	162
Table 59	Configuration > VPN > NetBIOS	164
Table 60	ICMP Commands That Trigger Alerts	169
Table 61	Legal NetBIOS Commands	170
Table 62	Legal SMTP Commands	170
Table 63	Services and Port Numbers	176
Table 64	Configuration > Firewall	178
Table 65	Configuration > Firewall > DoS Settings	180
Table 66	Configuration > Firewall > Edit	182
Table 67	Configuration > Firewall > IP Address	183
Table 68	Firewall Custom Port	184
Table 69	Device Log > Device	186
Table 70	Configuration > Device Logs > Log Settings	188
Table 71	Purge Device Logs	190
Table 72	ADSL Standards	192
Table 73	Configuration > ADSL Monitor	193
Table 74	Alarm Severity	194
Table 75	Alarm States	194
Table 76	Configuration > Device Alarms > Current	195
Table 77	Configuration > Device Alarms > Historical	196
Table 78	Building Block > Device BB	199
Table 79	Building Block > Device BB > Edit	199
Table 80	Building Block > Device BB > Add	201
Table 81	Building Block > Configuration	201

Table 82	Building Block > Configuration BB > Add	202
Table 83	Building Block > Configuration BB > Edit	204
Table 84	Building Block > Component BB	204
Table 85	Building Block > Component > Add	205
Table 86	Building Block > Component BB > Add > IP Address	206
Table 87	Building Block > Component BB > Add > E-Mail Address	206
Table 88	Building Block > Component BB > Edit	207
Table 89	System > View Administrator List	210
Table 90	System > Administrator Details	211
Table 91	System > Administrator Permissions	212
Table 92	System > Vantage Status	214
Table 93	Vantage Version Number	217
Table 94	System > License > License Management	218
Table 95	System > License > License Management > Upgrade	219
Table 96	System > Preferences > General System	220
Table 97	System > Preferences > User Access	221
Table 98	System > Preferences > Server	223
Table 99	System > Preferences > Notifications	225
Table 100	System > Preferences > Permissions	226
Table 101	System > Preferences > Permissions > Add	227
Table 102	System > Maintenance > Management	228
Table 103	System > Maintenance > Backup	229
Table 104	System > Maintenance > Restore	230
Table 105	System > Address Book	231
Table 106	System > Address Book Add/Edit	232
Table 107	System > Certificate Management > Information	234
Table 108	System > Certificate Management > Create CSR	235
Table 109	System > Certificate Management > Import Certificate	236
Table 110	System > Logs > CNM Server	237
Table 111	Types of Alarms	240
Table 112	Alarm Severity	240
Table 113	Alarm States	241
Table 114	Monitor > Current Alarms	243
Table 115	Monitor > Firmware Upgrade Report	246
Table 116	FTP and syslog Server Overview	264
Table 117	Classes of IP Addresses	270
Table 118	Allowed IP Address Range By Class	271
Table 119	“Natural” Masks	271
Table 120	Alternative Subnet Mask Notation	272
Table 121	Two Subnets Example	272
Table 122	Subnet 1	273
Table 123	Subnet 2	273
Table 124	Subnet 1	274

Table 125	Subnet 2	274
Table 126	Subnet 3	274
Table 127	Subnet 4	275
Table 128	Eight Subnets	275
Table 129	Class C Subnet Planning	275
Table 130	Class B Subnet Planning	276
Table 131	Comparison of EAP Authentication Types	299
Table 132	System Maintenance Logs	300
Table 133	System Error Logs	301
Table 134	Access Control Logs	301
Table 135	TCP Reset Logs	302
Table 136	Packet Filter Logs	302
Table 137	ICMP Logs	303
Table 138	CDR Logs	303
Table 139	PPP Logs	303
Table 140	UPnP Logs	304
Table 141	Content Filtering Logs	304
Table 142	Attack Logs	305
Table 143	IPSec Logs	306
Table 144	IKE Logs	306
Table 145	PKI Logs	309
Table 146	Certificate Path Verification Failure Reason Codes	310
Table 147	802.1X Logs	311
Table 148	ACL Setting Notes	312
Table 149	ICMP Notes	312
Table 150	Syslog Logs	313
Table 151	RFC-2408 ISAKMP Payload Types	313

Preface

Introducing Vantage Centralized Network Management (CNM) 2.0

Vantage Centralized Network Management 2.0 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 Vantage CNM 2.0 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 2.0 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 2.0.

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 One-Click VPN

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. 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.

1.1.15 License Management

Simply login into www.myZyXEL.com to acquire a new activation key when you purchase an expansion license letting you manage yet even more devices with Vantage CNM 2.0.

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 2.0 graphical user interface.

Figure 1 Main Screen



Main Menu Components

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

2.1.1 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 Object Tree View Types

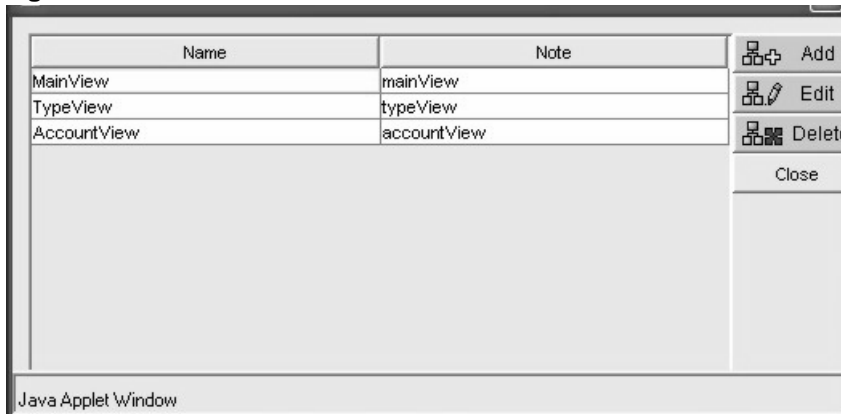
The **View** list box contains three default views called (device) **TypeView**, **AccountView** and **MainView**. You can also create custom views.

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



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 B-3* and then click **Edit** or **Delete**. Click **Close** to close the screen.

2.3 Searches

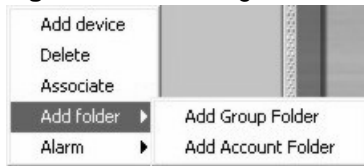
Select a folder first to define the scope of the search. Search for folders by folder name or devices by device name or MAC address within the selected folder in the Object tree. Results are displayed in the same split window.

2.4 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.

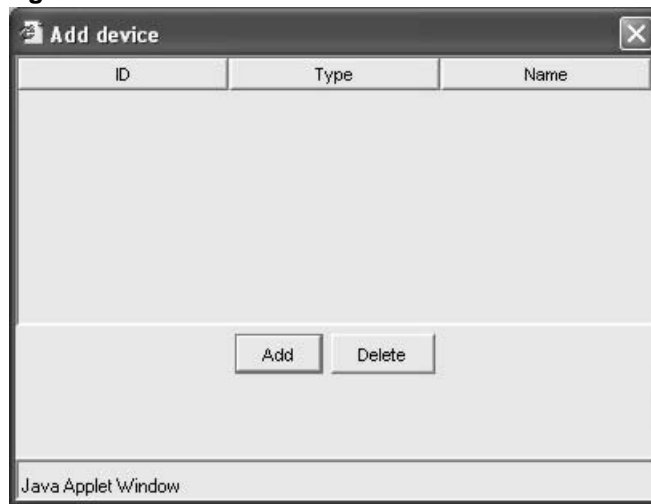
Folder right-click options are (in **MainView** only):

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



2 Delete.

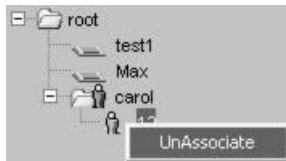
- This option displays a screen asking you if you want to delete the root folder and un-map the devices within the folder to the **Add devices** screen or
 - Delete the folder and un-map the devices within the folder. The device is still registered with Vantage but no longer associated with the folder. The latter action also disables Vantage within the device.
- 3 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 6 Associate Administrators



An administrator icon appears on the folder when you associate an administrator with a folder. To disassociate the administrator from this folder, right-click to select the icon and **UnAssociate**.

Figure 7 Associated Administrator Right-Click Options



4 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**).

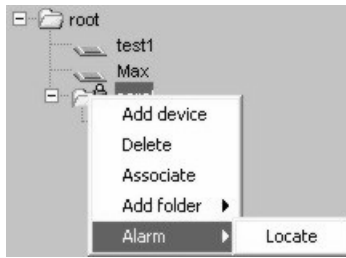
When you add a folder, you must enter a new folder group name.

Figure 8 Add New Folder Group Name



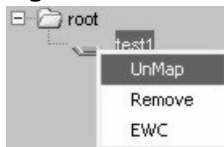
5 Alarm.

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

2.5 Devices

Right-click a device options are:

Figure 10 Device Right-Click Options

- **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.
- **Remove.** Delete the device registration from Vantage. Vantage disables CNM in the device.
- **EWC.** Click this to open the device's embedded web configurator. If you know the password you can log in directly and configure any item. You should synchronize with Vantage afterwards.

2.6 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).

2.6.1 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.

2.6.2 Menu Path

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

2.7 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 Menu Overview

DEVICE	CONFIGURATION	BUILDING BLOCK	SYSTEM	MONITOR	LOGOUT
Status	Select Device BB	Device BB	Administrators	Alarm	Logout
Registration	General	Configuration BB	Status	Firmware Report	
Synchronize	LAN	Component BB	Upgrade	Status Monitor	
Firmware Mgmt	WLAN		License	VPN Editor	
Firmware Upgrade	DMZ		Preferences		
Configuration File	WAN		Maintenance		
	NAT		Address Book		
	Static route		Certificate Mgmt		
	VPN		Logs		
	Firewall		About		
	Device Log				
	ADSL Monitor				
	Device Alarm				

2.8 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 or Monitor). 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.

2.9 Context-Sensitive Menus

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

Figure 11 Java Applet Window



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 2.0 installation directory\utilities (the default installation path is C:\Program Files\ZyXEL\Vantage CNM 2.0\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 2.0 functions normally whether the replacement is made or not.

2.10 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.

Table 2 Object Tree Icons (continued)

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

Table 4 Content Pane Icons

ICON	DESCRIPTION
	Click Apply the current configuration settings and apply to the server.
	Click Save the current configuration settings but not apply to the server. The configuration can be cancelled.
	Click Back to go to the previous page.
	Click Next to navigate to the next page.
	Click to Reset the current page.s
	Click OK to apply the configuration.
	Click Yes to confirm your configuration edit.
	Click No to cancel the configuration edit.
	Click Finish to complete the whole configuration.

Table 4 Content Pane Icons (continued)

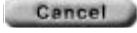
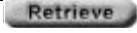




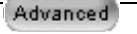
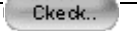








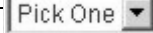
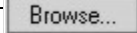





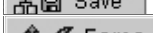
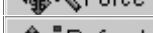
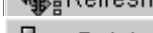



ICON	DESCRIPTION
	Click to Cancel the configuration and return to the previous page.
	Click Retrieve to get the logs from a device.
	Click this icon to choose from an existing BB.
	Click this icon to save a new BB.
	Click this icon to choose from an existing personal profile.
	Click this icon to save as a new personal profile.
	Click Advanced to show more details and configure.
	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.
	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.
	Type text in a text box.
	Choose from a list of pre-defined choices from a list box.
	This is a Browse icon allowing you to select a file external to Vantage.

Table 5 VPN Editor Icons

ICON	DESCRIPTION
	Description
	Add a new tunnel.
	Edit the selected tunnel.
	Delete the selected tunnel.
	Upload a map file to the VPN editor.
	Save the graphical tunnel depiction.
	Force deletes the selected tunnel even if the selected tunnel is active.
	Refresh the VPN monitor.
	Delete erases the selected tunnel if it is not active.
	The ZyXEL device is turned on.
	The ZyXEL device is turned off.

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 12 Device > Status > Main Screen

The screenshot shows a web interface window titled "Device >> Status". Below the title bar is a "Device Status" header. Underneath, there is a "By Status" dropdown menu set to "All" and a "Total devices: 3" indicator. The main content is a table with the following columns: Device Name, Type, MAC, IP, Status, Firmware Version, and Last Edit. Three rows of device data are visible.

Device Name	Type	MAC	IP	Status	Firmware Version	Last Edit
'rootzw35	ZyWALL35	00a0c5357000	0.0.0.0	Off		2004-6-17 16:05:01
'rootlisaIP662hw652hw	Prestige 652HW- 31	00a0c59989a8	172.21.3.203	Off	3.40(QR.1)_0608	2004-6-24 13:21:52
'rootlisaIP662hw652hw	Prestige 652HW	00a0c59989a8	172.21.3.203	Off	3.40(IU.3)	2004-6-24

The following table describes the fields in this screen.

Table 6 Device > Status > Main Screen

LABEL	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 13 Device > Status > Single Device



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

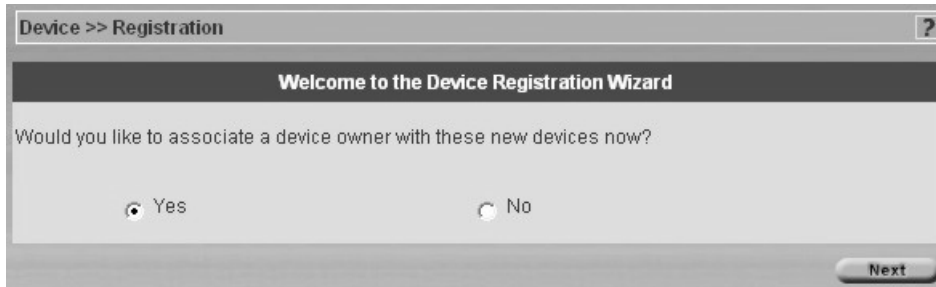
The following table describes the fields in this screen

Table 7 Device > Status > Single Device

LABEL	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 14 Device > Registration Wizard > Account Association

- 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 *Figure 1-5*. If you already selected an Account folder in the object tree, then the owner name is pre-selected here.

Figure 15 Device > Registration > Owner Selection

In the following screen select a radio button to either:

- **Manually add:** When you choose this option, you must enter the information shown in *Figure 1-6* 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 2.0\xml by default). Choose the 4-devices or 100-ZyWALL10W templates and modify accordingly.

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

Figure 16 Device > Registration > Wizard Choices

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 xxxxxxxx' where 'xxxxxxx' 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 17 Device > Registration > Manual Registration

The following table describes the fields in this screen

Table 8 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&fs=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 using 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.

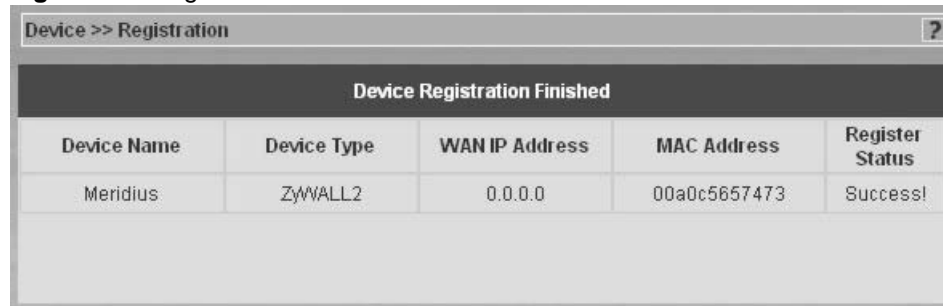


Note: For more detailed information on creating XML files for Vantage, please see the "Import Device Using XML Reference Manual" at the ZyXEL web site download library.

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

Figure 18 Registration Wizard: Configuration File

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 19 .Registration: XML File Devices**Figure 20** Registration Wizard: Finish

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 21 Device > Synchronize



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 22 Device > Firmware Management

The following table describes the fields in this screen

Table 9 Device > Firmware Management

TYPE	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 <ul style="list-style-type: none"> • 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 23 Device > Firmware Management > Add Firmware



Figure 24 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 25 TypeView



3.5.2 Firmware Upgrade Select Product Line and Mode

If you select a device in the object tree, Figure 27 on page 56 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 26 Firmware Upgrade > Select Product Line and Model

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 **Upgrade** to begin the device upgrade process

Figure 27 Device > Firmware Upgrade

See Figure 9 on page 54 for field descriptions. Click **Upgrade** to begin the device upgrade process.

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 (Configuration files).

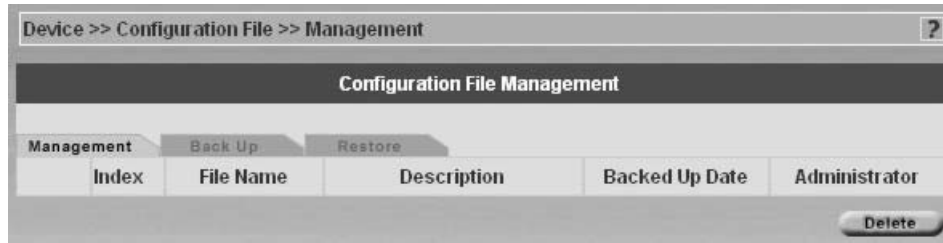
Select the device and then click **Device > Configuration File**.

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 28 Device > Configuration File > Management



The following table describes the fields in this screen

Table 10 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 29 Device > Configuration File > Back Up

The following table describes the fields in this screen

Table 11 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 device's 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 30 Device > Configuration File > Restore

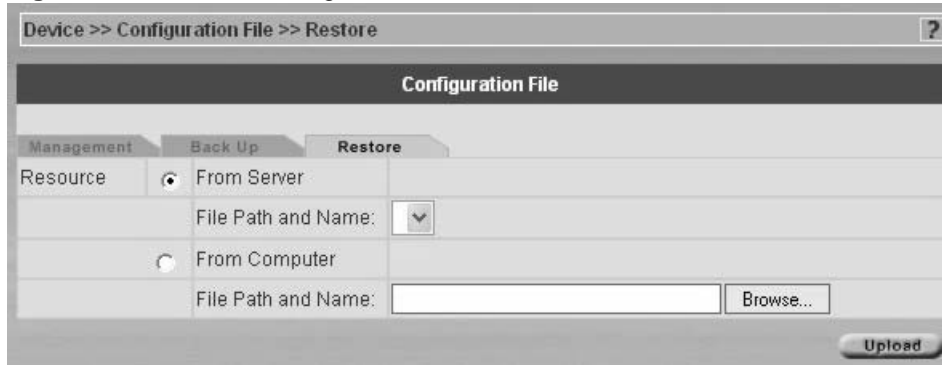


Table 12 Device > Configuration File > Restore

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.

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 show device BBs for the ZyWALL 10W and ZyWALL 70/35/5 (these three models have the same device BB). A check mark indicates that the device BB includes this configuration and an "X" denotes that it doesn't.

Figure 31 ZyWALL 10W Device BB



Configuration >> Select Device BB				
Configuration: Select Device BB				
Select Device BB 				
ZyWALL 10w				
General	LAN	WAN	WLAN	DMZ
System <input checked="" type="checkbox"/>	IP <input checked="" type="checkbox"/>	General <input checked="" type="checkbox"/>	Wireless <input checked="" type="checkbox"/>	All <input checked="" type="checkbox"/>
DDNS <input checked="" type="checkbox"/>	StaticDHCP <input checked="" type="checkbox"/>	ISP <input checked="" type="checkbox"/>	MacFilter <input checked="" type="checkbox"/>	
TimeSetting <input checked="" type="checkbox"/>	IP Alias <input checked="" type="checkbox"/>	IP <input checked="" type="checkbox"/>	802.1x <input checked="" type="checkbox"/>	
		DialBackup <input checked="" type="checkbox"/>	LocalUser <input checked="" type="checkbox"/>	
			Radius <input checked="" type="checkbox"/>	
NAT	Device Log	StaticRoute	Firewall	VPN
All <input checked="" type="checkbox"/>	Logs <input checked="" type="checkbox"/>	All <input checked="" type="checkbox"/>	All <input checked="" type="checkbox"/>	All <input checked="" type="checkbox"/>
	LogSetting <input checked="" type="checkbox"/>			
<p>Caution:</p> <p><input checked="" type="checkbox"/>: Device BB includes this feature.</p> <p><input checked="" type="checkbox"/>: Device BB does not include this feature.</p> <p>After you apply a Device BB, it overwrites existing Device BB-related configurations (only)!</p>				

Figure 32 ZyWALL 70/35/5 Device BB



Configuration >> Select Device BB				
Configuration: Select Device BB				
Select Device BB 				
ZyWALL 70/35/5				
General	LAN	WAN	WLAN	DMZ
System <input checked="" type="checkbox"/>	IP <input checked="" type="checkbox"/>	General <input checked="" type="checkbox"/>	Wireless <input checked="" type="checkbox"/>	All <input checked="" type="checkbox"/>
DDNS <input checked="" type="checkbox"/>	StaticDHCP <input checked="" type="checkbox"/>	ISP <input checked="" type="checkbox"/>	MacFilter <input checked="" type="checkbox"/>	
TimeSetting <input checked="" type="checkbox"/>	IP Alias <input checked="" type="checkbox"/>	IP <input checked="" type="checkbox"/>	802.1x <input checked="" type="checkbox"/>	
		DialBackup <input checked="" type="checkbox"/>	LocalUser <input checked="" type="checkbox"/>	
			Radius <input checked="" type="checkbox"/>	
NAT	Device Log	StaticRoute	Firewall	VPN
All <input checked="" type="checkbox"/>	Logs <input checked="" type="checkbox"/>	All <input checked="" type="checkbox"/>	All <input checked="" type="checkbox"/>	All <input checked="" type="checkbox"/>
	LogSetting <input checked="" type="checkbox"/>			
<p>Caution:</p> <p><input checked="" type="checkbox"/>: Device BB includes this feature.</p> <p><input checked="" type="checkbox"/>: Device BB does not include this feature.</p> <p>After you apply a Device BB, it overwrites existing Device BB-related configurations (only)!</p>				

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 33 Configuration > General > System – ZyWALL

The screenshot shows the 'Configuration >> General >> System' window. The title bar reads 'Configuration: General'. Below the title bar are four tabs: 'System', 'DDNS', 'Time Setting', and 'Owner Info'. The 'System' tab is active. The form contains the following fields:

- Password:** A text input field with asterisks (*****).
- MAC (Hex):** A text input field containing '00a0c5123456'.
- Device Type:** A text input field containing 'ZyWALL10W'.
- Encryption Mode:** A dropdown menu currently set to 'NONE'.
- Encryption Key:** An empty text input field.
- System Name:** An empty text input field.
- Domain Name:** An empty text input field.
- Administrator Inactivity Timer:** A text input field containing '5', with a note: *(Minutes, 0 means no timeout).
- First DNS Server:** A dropdown menu set to 'From ISP' and a text input field containing '0.0.0.0'.
- Second DNS Server:** A dropdown menu set to 'From ISP' and a text input field containing '0.0.0.0'.
- Third DNS Server:** A dropdown menu set to 'From ISP' and a text input field containing '0.0.0.0'.

At the bottom of the window, there are three buttons: 'Reset to Factory Default', 'Apply', and 'Reset'.

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.
Encryption Mode	<p>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.</p> <p>You do not need to add NAT or firewall rules when you encrypt this traffic.</p> <p>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</p>

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

FIELD	DESCRIPTION
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 <code>'CNM encrykey xxxxxxxxxx'</code> where <code>'xxxxxxxxxx'</code> 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 34 Configuration > General > DDNS

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 35 Configuration > General > Time Setting

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)
Time Zone	Choose the Time Zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).

Table 15 Configuration > General > Time Setting (continued)

LABEL	DESCRIPTION
Daylight Savings	Select this option if you use daylight savings time. 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.
Start Date	Enter the month and day that your daylight-savings time starts on if you selected Daylight Savings .
End Date	Enter the month and day that your daylight-savings time ends on if you selected Daylight Savings .
Calibrate (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 36 Configuration > General > Owner Info

The following table describes the fields in this screen.

Table 16 Configuration > General > Owner Info

TYPE	DESCRIPTION
Name	Type the full name of the owner of this device.
Description	Type some extra information about this customer.

Table 16 Configuration > General > Owner Info (continued)

TYPE	DESCRIPTION
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 Configuring LAN IP – ZyWALL

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

Figure 37 Configuration > LAN > IP – ZyWALL

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	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>
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 <i>sections 4 and 5 of RFC 2236</i> .
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.

5.4 Configuring LAN IP - Prestige

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

Figure 38 Configuration > LAN > IP – Prestige

The screenshot shows the 'Configuration >> LAN >> IP' window. The title bar reads 'Configuration : LAN'. Below the title bar, there are two tabs: 'IP' (selected) and 'DHCP'. The DHCP section includes the following fields:

- DHCP Mode: Server (dropdown)
- IP Pool Starting Address: 192.168.1.33 (text box with asterisk)
- Pool Size: 32 (text box with asterisk)
- First DNS Server IP: 0.0.0.0 (text box with refresh icon)
- Second DNS Server IP: 0.0.0.0 (text box with refresh icon)
- Remote DHCP Server: 0.0.0.0 (text box with asterisk and refresh icon)

 The TCP/IP section includes:

- IP Address: 192.168.1.1 (text box with asterisk and refresh icon)
- IP Subnet Mask: 255.255.255.0 (text box with asterisk)
- RIP Direction: Both (dropdown)
- RIP Version: RIP-1 (dropdown)
- Multicast: None (dropdown)

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

Table 18 Configuration > LAN > IP – Prestige

LABEL	DESCRIPTION
DHCP Mode	<p>DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (computers) to obtain TCP/IP configuration at startup from a server.</p> <p>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.</p> <p>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.</p> <p>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.</p>
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.
TCP/IP	

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

LABEL	DESCRIPTION
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 <i>sections 4 and 5 of RFC 2236</i> .
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 Static DHCP – ZyWALL

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 39 Configuration > LAN > Static DHCP – ZyWALL

Index	MAC Address	IP Address
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

The following table describes the fields in this screen

Table 19 Configuration > LAN > Static DHCP – ZyWALL

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.

5.6 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 40 Configuration > LAN > IP Alias

The screenshot shows a web-based configuration interface for a ZyXEL device. The breadcrumb path is 'Configuration >> LAN >> IP Alias'. The main title is 'Configuration : LAN'. There are three tabs: 'IP', 'Static DHCP', and 'IP Alias', with 'IP Alias' being the active tab. The interface is divided into two sections for 'IP Alias1' and 'IP Alias2'. Each section has a checkbox to enable the alias. Below each checkbox are four fields: 'IP Address' and 'IP Subnet Mask' (both containing '0.0.0.0'), 'RIP Direction' (a dropdown menu set to 'None'), and 'RIP Version' (a dropdown menu set to 'RIP-1'). There are small icons to the right of the IP Address and Subnet Mask fields. At the bottom right, there are 'Apply' and 'Reset' buttons.

The following table describes the fields in this screen

Table 20 Configuration > LAN > IP Alias

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.
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 .

Table 20 Configuration > LAN > IP Alias (continued)

LABEL	DESCRIPTION
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 shows the wireless LAN screens.

6.1 Wireless LAN Overview

This section introduces the wireless LAN (WLAN) and some basic scenarios.

6.1.1 Additional Installation Requirements for using 802.1x

- A computer with an IEEE 802.11b wireless LAN card.
- A computer equipped with a web browser (with JavaScript enabled) and/or Telnet.
- A wireless client computer must be running IEEE 802.1x-compliant software. Currently, this is offered in Windows XP.
- An optional network RADIUS server for remote user authentication and accounting.

6.2 Wireless LAN Basics

This section provides background information on WLAN.

6.2.1 Channel

IEEE 802.11b wireless devices use radio frequencies called channels. Choose the radio channel depending on your geographical area. Adjacent Access Points (APs) should use different channels to reduce crosstalk. Crosstalk occurs when radio signals from access points overlap and cause interference that degrades performance.

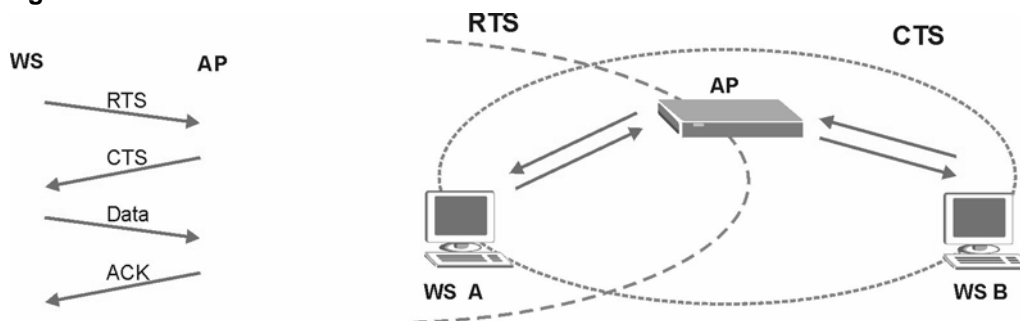
6.2.2 ESS ID

Extended Service Set (ESS) is defined as one or more APs acting as a bridge between a wired LAN and the associated wireless clients. The ESS ID is a unique ID given to the APs and the wireless clients that participate in the same wireless network. You can think of the ESS ID as being similar to a workgroup name in a Microsoft network.

6.2.3 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 41 RTS Threshold



Wireless stations (WS) A and B do not hear each other. They can hear the AP. When station A sends data to the ZyXEL device, 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.

6.2.4 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 ZyXEL device 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 Threshold** size.

6.2.5 WEP

WEP provides a mechanism for encrypting data using encryption keys. Both the AP and the wireless stations must use the same WEP key to encrypt and decrypt data. The ZyXEL device allows you to configure up to four 64-bit or 128-bit WEP keys, but only one key can be enabled at any one time.

6.3 Configuring Wireless LAN

If you are configuring the ZyXEL device from a computer connected to the wireless LAN and you change the ZyXEL device's ESSID or WEP settings, 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 ZyXEL device's new settings.

Select a device, and then click **Configuration > WLAN. Wireless** is the first screen.

6.3.1 WLAN Wireless

Figure 42 Configuration > WLAN > Wireless

The following table describes the fields in this screen

Table 21 Configuration > WLAN > Wireless

LABEL	DESCRIPTION
Enable Wireless LAN	The wireless LAN is turned off by default; before you enable the wireless LAN you should configure some security by setting MAC filters and/or 802.1x security; otherwise your wireless LAN will be vulnerable upon enabling it. Select the check box to enable the wireless LAN.
ESSID	(Extended Service Set IDentification) The ESSID identifies the Service Set the station is to connect to. Wireless clients associating to the Access Point must have the same ESSID. Enter a descriptive name (up to 32 characters) for the wireless LAN.
Hide ESSID	Select to hide the ESSID in the outgoing beacon frame so a station cannot obtain the ESSID through passive scanning.
Choose Channel ID	This allows you to set the operating frequency/channel depending on your particular region. Select a channel from the drop-down list box. CH01 2412 MHz / CH02 2417 MHz ~ CH11 2462 MHz (North America/FCC) CH01 2412 MHz / CH02 2417 MHz ~ CH13 2472 MHz (Europe CE/ ETSI) CH01 2412 MHz / CH02 2417 MHz ~ Ch14 2484 MHz (Japan) CH10 2457 MHz / CH11 2462 MHz (Spain)

Table 21 Configuration > WLAN > Wireless (continued)

LABEL	DESCRIPTION
RTS/CTS Threshold	(Request To Send) The threshold (number of bytes) for enabling RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be larger than the maximum MSDU (MAC service data unit) size turns off the RTS/CTS handshake. Setting this attribute to zero turns on the RTS/CTS handshake. Enter a value between 0 and 2432 .
Fragmentation Threshold	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter a value between 256 and 2432 .
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. 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.

6.4 Configuring MAC Filter

The MAC filter screen allows you to configure the ZyXEL device to give exclusive access to specific devices (**Allow Association**) or exclude specific devices from accessing the ZyXEL device (**Deny Association**). The Prestige can be configured to give exclusive access to up to 32 devices or exclude up to 32 devices from accessing the Prestige. The ZyWALL can be configured to give exclusive access to up to 12 devices or exclude up to 12 devices from accessing the ZyWALL. 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 address of the devices to configure this screen.

Select a device and then click **Configuration > WLAN > MAC Filter**. The screen appears as shown next.

Figure 43 Configuration > WLAN > MAC Filter

Table 22 Configuration > WLAN > MAC Filter

LABEL	DESCRIPTION
Activate MAC Filter	Enable MAC address filtering to have the router allow or deny access to wireless stations based on MAC addresses. Disable MAC address filtering to have the router not perform MAC filtering on the wireless stations.
Filter Action	Define the filter action for the list of MAC addresses in the MAC address filter table. Select Deny Association to block access to the router, MAC addresses not listed will be allowed to access the router. Select Allow Association to permit access to the router, MAC addresses not listed will be denied access to the router.
MAC Address	Enter the MAC addresses (in XXXXXXXXXXXX format) of the client computers that are allowed or denied access to the ZyXEL device 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.

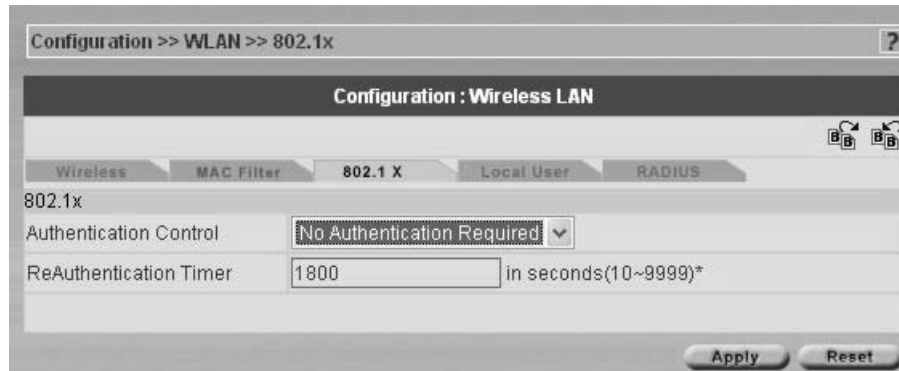
6.5 802.1x Overview

The IEEE 802.1x standard outlines enhanced security methods for both the authentication of wireless stations and encryption key management. Authentication can be done using the local user database internal to the ZyXEL device or an external RADIUS server for an unlimited number of users.

6.5.1 Configuring 802.1x – ZyWALL

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

Figure 44 Configuration > WLAN > 802.1x – ZyWALL



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.

6.5.2 Configuring 802.1x – Prestige

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

Figure 45 Configuration > WLAN > 802.1x – Prestige

The screenshot shows a web-based configuration interface for a Prestige device. The breadcrumb trail is Configuration >> WLAN >> 802.1x. The main title is Configuration : Wireless LAN. There are five tabs: Wireless, MAC Filter, 802.1 X (selected), Local User, and RADIUS. Below the tabs, the configuration for 802.1x is shown. The Authentication Control dropdown is set to 'No Authentication Required'. The ReAuthentication Timer is a text input field containing '1800' with the unit 'in Seconds(10~9999)*'. The Idle Timeout is a text input field containing '3600' with the unit 'in Seconds(10~9999)*'. The Authentication Databases dropdown is set to 'Radius Only'. At the bottom right, there are 'Apply' and 'Reset' buttons.

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	<p>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.</p> <p>Before you specify the priority, make sure you have set up the corresponding database correctly first.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>
Apply	Click Apply to save your changes back to the ZyXEL device.
Reset	Click Reset to begin configuring this screen afresh.

6.6 Local User Database

By storing user profiles locally on the ZyXEL device, the ZyXEL device is able to authenticate VPN extended authentication clients or wireless clients without interacting with a network RADIUS server. However, there is a limit on the number of users you may authenticate in this way.

6.6.1 Configuring Local User Database

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

Figure 46 Configuration > WLAN > Local User

Configuration >> WLAN >> Local User Database

Configuration : Wireless LAN

Wireless | MAC Filter | 802.1 X | **Local User** | RADIUS

Local User Database

Active	Index	User ID	Password
<input type="checkbox"/>	1	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	2	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	3	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	4	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	5	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	6	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	7	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	8	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	9	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	10	<input type="text"/>	<input type="text"/>

Next

Apply Reset

The following table describes the labels in this screen.

Table 25 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.

6.6.2 RADIUS

RADIUS is based on a client-server model that supports authentication and accounting, where access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks among others:

- Authentication
 - Determines the identity of the users.
- Accounting

Keeps track of the client's network activity.

RADIUS user is a simple package exchange in which the ZyXEL device acts as a message relay between the wireless client and the network RADIUS server.

6.6.2.1 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 the ZyXEL device 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 ZyXEL device 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 ZyXEL device 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.

6.6.3 EAP Authentication Overview

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, the access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server or the AP. The ZyXEL device supports EAP-TLS and EAP-TTLS with RADIUS.

The ZyXEL device supports EAP-MD5 (Message-Digest Algorithm 5) with the local user database.

The details below provide a general description of how IEEE 802.1x EAP authentication works. For an example list of EAP-MD5 authentication steps, see the IEEE 802.1x chapter in the *Appendices*.

- The wireless station sends a “start” message to the ZyXEL device.
- The ZyXEL device sends a “request identity” message to the wireless station for identity information.
- The wireless station replies with identity information, including username and password.
- The RADIUS server checks the user information against its user profile database and determines whether or not to authenticate the wireless station.

6.7 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 47 Configuration > WLAN > RADIUS

The screenshot shows a web-based configuration interface for RADIUS settings. At the top, there's a breadcrumb trail: Configuration >> WLAN >> RADIUS. Below that, a title bar reads 'Configuration : Wireless LAN'. A navigation menu includes 'Wireless', 'MAC Filter', '802.1 X', 'Local User', and 'RADIUS'. The main content area is titled 'RADIUS' and contains two sections. The first section, 'Activate Authentication', has a checkbox that is currently unchecked. Below it are three input fields: 'Server IP' (0.0.0.0), 'Port' (1812), and 'Key' (empty). The second section, 'Activate Accounting', also has an unchecked checkbox. Its fields are 'Server IP' (0.0.0.0), 'Port' (1813), and 'Key' (empty). At the bottom right, there are 'Apply' and 'Reset' buttons.

The following table describes the fields in this screen

Table 26 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.
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.

Table 26 Configuration > WLAN > RADIUS (continued)

LABEL	DESCRIPTION
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 48 Configuration > DMZ

The screenshot shows the 'Configuration: DMZ' window. It has a title bar 'Configuration >> DMZ' and a subtitle 'Configuration: DMZ'. The main area is divided into sections. The 'DMZ TCP/IP' section contains:

- IP Address: 0.0.0.0
- Subnet Mask: 0.0.0.0
- Multicast: None
- RIP Direction: Both
- RIP Version: RIP-1

 Below this is the 'Windows Networking (NetBIOS over TCP/IP)' section with two unchecked checkboxes:

- Allow from DMZ to LAN
- Allow from DMZ to WAN

 At the bottom right are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

Table 27 Configuration > DMZ

LABEL	DESCRIPTION
DMZ TCP/IP	
IP Address	Type the IP address of your ZyWALL 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 ZyWALL 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 ZyWALL 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 ZyWALL 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 ZyWALL 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 <i>sections 4 and 5 of RFC 2236</i> .

Table 27 Configuration > DMZ (continued)

LABEL	DESCRIPTION
Windows Networking (NetBIOS over TCP/IP)	
Allow from DMZ to LAN port	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 ZyWALL.
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 General WAN – ZyWALL

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

8.1.1 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".

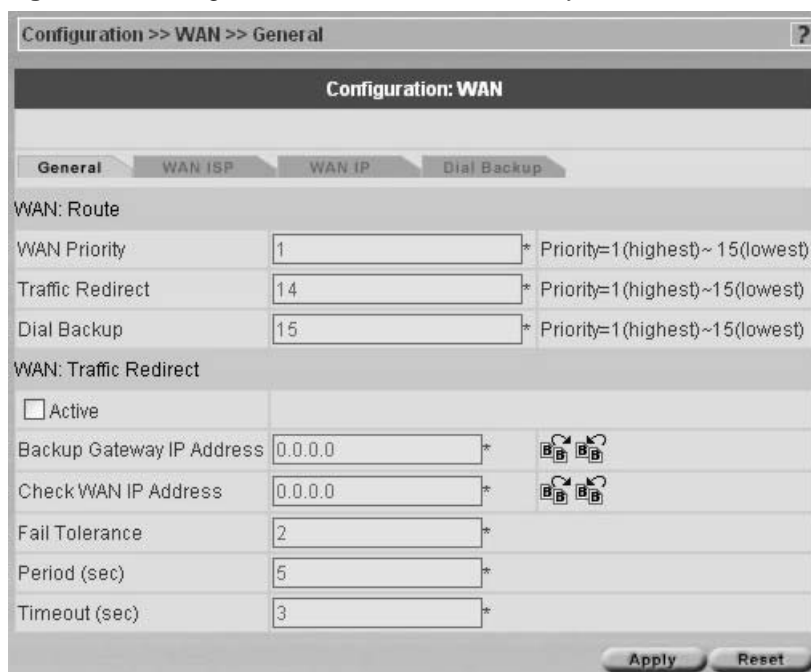
The metric sets the priority for the ZyXEL device's routes to the Internet. If any two of the default routes have the same metric, the ZyXEL device uses the following pre-defined priorities:

- Normal route: designated by the ISP.
- Traffic-redirect route. Traffic redirect forwards WAN traffic to a backup gateway when the ZyXEL device cannot connect to the Internet through its normal gateway. Connect the backup gateway on the WAN so that the ZyXEL device still provides firewall protection.
- Dial-backup route.

For example, if the normal route has a metric of "1" and the traffic-redirect route has a metric of "2" and dial-backup route has a metric of "3", then the normal route acts as the primary default route. If the normal route fails to connect to the Internet, the ZyXEL device tries the traffic-redirect route next. In the same manner, the ZyXEL device uses the dial-backup route if the traffic-redirect route also fails.

If you want the dial-backup route to take first priority over the traffic-redirect route or even the normal route, all you need to do is set the dial-backup route's metric to "1" and the others to "2" (or greater).

Figure 49 Configuration > WAN > General – ZyWALL



The following table describes the fields in this screen

Table 28 Configuration > WAN > General – ZyWALL

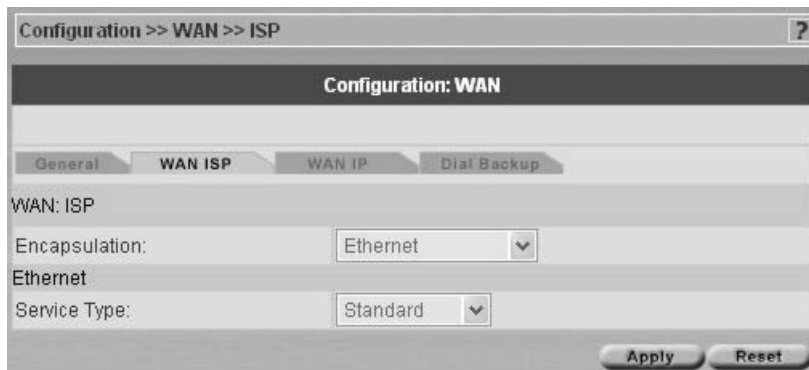
LABEL	DESCRIPTION
WAN Traffic Redirect Dial Backup	The default WAN connection is "1" as your broadband connection via the WAN port should always be your preferred method of accessing the WAN. The default priority of the routes is WAN , Traffic Redirect and then Dial Backup (dial backup does not apply 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.

Table 28 Configuration > WAN > General – ZyWALL (continued)

LABEL	DESCRIPTION
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.
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.

8.1.2 WAN ISP – ZyWALL

The screen differs by the encapsulation type chosen.

Figure 50 Configuration > WAN > ISP (Ethernet) – ZyWALL

8.1.2.1 Ethernet Encapsulation

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

Table 29 Configuration > WAN > ISP (Ethernet) – ZyWALL

LABEL	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.

8.1.2.2 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 51 Configuration > WAN > ISP (PPPoE) – ZyWALL

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

Table 30 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.

8.1.2.3 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 52 Configuration > WAN > ISP (PPTP) – ZyWALL

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

Table 31 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 31 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.

8.2 WAN IP – ZyWALL

Figure 53 Configuration > WAN > IP – ZyWALL

The following table describes the fields in this screen

Table 32 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 32 Configuration > WAN > IP – ZyWALL (continued)

LABEL	DESCRIPTION
RIP Direction	<p>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.</p> <p>Choose Both, None, In Only or Out Only.</p> <p>When set to Both or Out Only, the ZyXEL device will broadcast its routing table periodically.</p> <p>When set to Both or In Only, the ZyXEL device will incorporate RIP information that it receives.</p> <p>When set to None, the ZyXEL device will not send any RIP packets and will ignore any RIP packets received.</p> <p>By default, RIP Direction is set to Both.</p>
RIP Version	<p>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).</p> <p>Choose RIP-1, RIP-2B or RIP-2M.</p> <p>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.</p>
Multicast	<p>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.</p>
<p>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.</p>	
Allow from WAN to LAN	<p>Select this option to forward NetBIOS packets from the WAN port to the LAN port.</p>
Allow Trigger Dial	<p>Select this option to allow NetBIOS packets to initiate calls.</p>
Apply	<p>Click Apply to save your changes back to the ZyXEL device.</p>
Reset	<p>Click Reset to begin configuring this screen afresh.</p>

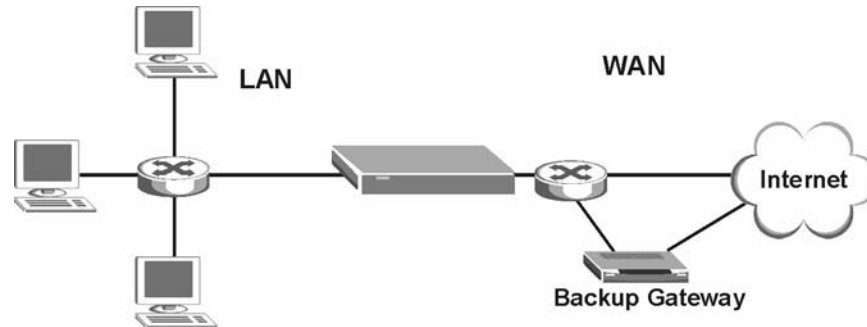
8.3 Dial Backup – ZyWALL

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

8.3.1 Traffic Redirect

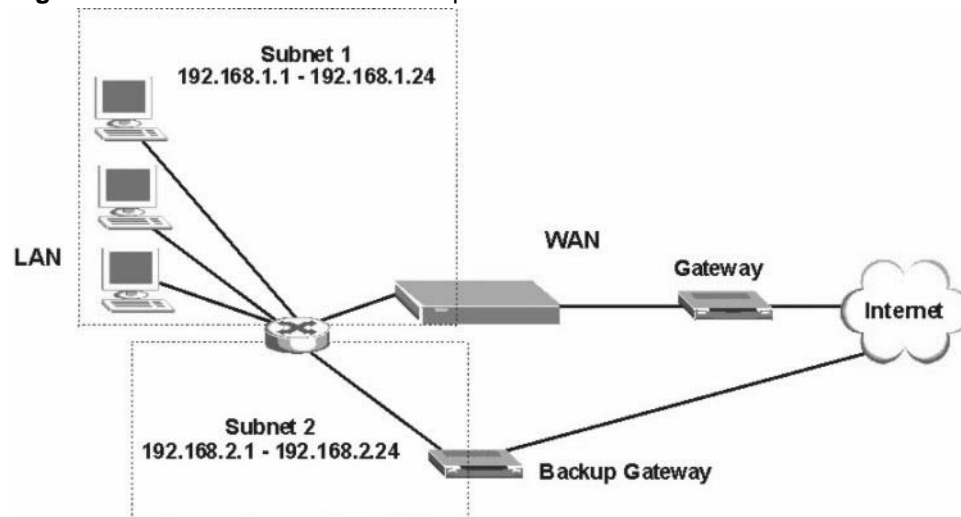
Traffic redirect forwards WAN traffic to a backup gateway when the ZyWALL cannot connect to the Internet through its normal gateway. Connect the backup gateway on the WAN so that the ZyWALL still provides firewall protection. This feature is not available on all models.

Figure 54 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 55 Traffic Redirect LAN Setup



8.3.2 Configuring Dial Backup - ZyWALL

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

Figure 56 Configuration > WAN > Dial Backup – ZyWALL

The following table describes the labels in this screen.

Table 33 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 33 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.

8.3.3 Advanced Modem Setup – ZyWALL

8.3.3.1 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.

8.3.3.1.1 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.

8.3.3.1.2 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 57 Configuration > WAN > Dial Backup > Advanced – ZyWALL

Configuration: WAN		
WAN: Dial Backup Advanced		
AT Command Strings	Dial	atdt
	Drop	~++++~ath
	Answer	ata
	<input checked="" type="checkbox"/> 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 34 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 34 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.	

8.3.4 Edit Dial Backup – ZyWALL

Click **Edit** in the **TCP/IP** field in the screen shown in Figure 56 on page 110 to display the next screen.

Figure 58 Configuration > WAN > Dial Backup > Edit – ZyWALL

The following table describes the fields in this screen

Table 35 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 35 Configuration > WAN > Dial Backup > Edit – ZyWALL (continued)

LABEL	DESCRIPTION
Enable SUA	<p>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.</p> <p>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).</p> <p>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.</p>
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 <i>sections 4 and 5 of RFC 2236</i> .
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.

8.4 General WAN – Prestige

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

8.4.1 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.

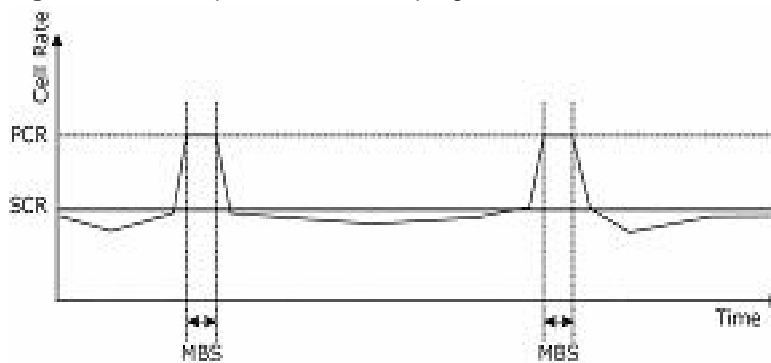
Maximum Burst Size (MBS) is the maximum number of cells that can be sent at the PCR. After MBS is reached, cell rates fall below SCR until cell rate averages to the SCR again. At this time, more cells (up to the MBS) can be sent at the PCR again.



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 59 Example of Traffic Shaping



8.4.2 Configuring Prestige WAN Setup

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

Figure 60 Configuration > WAN > Setup – Prestige – Bridge Mode

The following table describes the fields in this screen

Table 36 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 .

Table 36 Configuration > WAN > Setup – Prestige – Bridge Mode (continued)

LABEL	DESCRIPTION
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)
User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form <code>user@domain</code> 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 61 Configuration > WAN > Setup – Prestige – Routing Mode

The screenshot shows a configuration window titled "Configuration >> WAN" with a sub-header "Configuration: WAN". Below this, there are two tabs: "Setup" (selected) and "Backup". The main content area is titled "WAN: Prestige Setup" and contains the following fields:

- Name: MyISP
- Mode: Routing
- Encapsulation: PPPoA
- Multiplex: VC
- Virtual Circuit ID:
 - VPI: 8
 - VCI: 35
- 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: user@isp.ch
 - Password: (empty)
- IP Address:
 - Obtain an IP Address Automatically
 - Static IP Address

The following table describes the fields in this screen.

Table 37 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 .
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.

Table 37 Configuration > WAN > Setup – Prestige – Routing Mode (continued)

LABEL	DESCRIPTION
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 <u>user@domain</u> where domain identifies a service name, then enter both components exactly as given.
Password	Enter the password associated with the user name above.
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.

Table 37 Configuration > WAN > Setup – Prestige – Routing Mode (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.
Apply	Click Apply to save the changes.
Reset	Click Reset to begin configuring this screen afresh.

8.4.3 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.

8.4.3.1 Traffic Redirect

See page 109 for more information on traffic redirect.

8.4.4 Configuring WAN Backup - Prestige

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

Figure 62 Configuration > WAN > Backup – Prestige

The screenshot shows a web-based configuration interface for WAN Backup. The title bar reads 'Configuration >> WAN'. Below it, a sub-header says 'Configuration: WAN'. There are two tabs: 'Setup' and 'Backup', with 'Backup' selected. The main content area is titled 'WAN: Prestige Backup'. It contains several rows of configuration fields:

- Backup Type:** A dropdown menu set to 'DSL Link'.
- Check WAN IP Address1, 2, 3:** Three text input fields, each containing '0.0.0.0' and marked with an asterisk (*). To the right of each field are two circular refresh icons.
- Fail Tolerance:** A text input field containing '0' and marked with an asterisk (*).
- Recovery Interval:** A text input field containing '0' and marked with an asterisk (*).
- Timeout:** A text input field containing '0' and marked with an asterisk (*).
- Traffic Redirect:** A checkbox labeled 'active' which is currently unchecked.
- Metric:** A text input field containing '15' and marked with an asterisk (*).
- Backup Gateway:** A text input field containing '0.0.0.0' and marked with an asterisk (*).
- Dial Backup:** A checkbox labeled 'active' which is currently unchecked.
- Port Speed:** A dropdown menu set to '115200'.
- User Name, Password, Pri Phone:** Three empty text input fields.

At the bottom left, there is a section for 'Advanced Backup:' with a button labeled 'Advanced'. At the bottom right, there are two buttons: 'Apply' and 'Reset'.

The following table describes the fields in this screen.

Table 38 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 38 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 38 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.

8.4.5 Configuring Advanced WAN Backup – Prestige

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

Figure 63 Advanced WAN Backup – Prestige

Configuration >> WAN

Configuration: WAN

WAN: Prestige Backup Advanced

Basic:

Authentication Type: CHAP/PAP

Secondary Phone Number: (optional)

AT Command Initial String: at&fs0=0

Advanced Modem Setup: Edit

TCP/IP Options

Enable SUA

Enable RIP

RIP Direction: Both

RIP Version: RIP-1

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)

Back Apply Reset

The following table describes the fields in this screen.

Table 39 Advanced WAN Backup – 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 39 Advanced WAN Backup – 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	<p>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.</p> <p>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.</p>
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	<p>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.</p> <p>Choose Both, In Only or Out Only.</p> <p>When set to Both or Out Only, the Prestige will broadcast its routing table periodically.</p> <p>When set to Both or In Only, the Prestige will incorporate RIP information that it receives.</p>
RIP Version	<p>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).</p> <p>Choose RIP-1, RIP-2B or RIP-2M.</p> <p>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.</p>
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 <i>sections 4 and 5 of RFC 2236</i> .
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 39 Advanced WAN Backup – 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.

8.4.6 Advanced Modem Setup – Prestige

Click **Edit** in the **Advanced Modem Setup** field. See the section on ZyWALL advanced modem setup on page 112 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 40 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 41 NAT Mapping Types

TYPE	IP MAPPING	SMT ABBREVIATION
One-to-One	ILA1 → 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

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**.

9.2.1 Disable NAT

Figure 64 Configuration > NAT



The following table describes the fields in this screen.

Table 42 Configuration > NAT

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

9.3 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.

9.3.1 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 43 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	

9.3.2 Configuring SUA Servers – ZyWALL

Select **SUA Only** in Figure 64 on page 133 and then click **Edit** to bring up the next screen.

Figure 65 Configuration > NAT > SUA Server – ZyWALL

Index	Active	Name	Start Port	End Port	Server IP Address
0	N/A	Default Server	All ports	All ports	0.0.0.0
1	<input type="checkbox"/>		0	0	0.0.0.0
2	<input type="checkbox"/>		0	0	0.0.0.0
3	<input type="checkbox"/>		0	0	0.0.0.0
4	<input type="checkbox"/>		0	0	0.0.0.0
5	<input type="checkbox"/>		0	0	0.0.0.0
6	<input type="checkbox"/>		0	0	0.0.0.0
7	<input type="checkbox"/>		0	0	0.0.0.0
8	<input type="checkbox"/>		0	0	0.0.0.0
9	<input type="checkbox"/>		0	0	0.0.0.0
10	<input type="checkbox"/>		0	0	0.0.0.0
11	<input type="checkbox"/>		0	0	0.0.0.0

The following table describes the labels in this screen.

Table 44 Configuration > NAT > SUA Server

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.
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.

9.3.3 Configuring SUA Servers – Prestige

Select **SUA Only** in Figure 64 on page 133 and then click **Edit** to bring up the next screen.

Figure 66 Configuration > NAT > SUA Server – Prestige

Index	Start Port	End Port	Server IP Address
0	All ports	All ports	0.0.0.0
1	0	0	0.0.0.0
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 45 Configuration > NAT > SUA Server – Prestige

LABEL	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.

9.3.4 Full Feature Address Mapping

Select **Full Feature** in Figure 64 on page 133 and then click **Edit** to bring up the next screen.

Figure 67 Configuration > NAT > Full Feature > Address Mapping

Configuration >> SUA/NAT						
Configuration : NAT						
Address Mapping						
	Index	Local Start IP	Local End IP	Global Start IP	Global End IP	Type
<input type="checkbox"/>	0	1-1
<input type="checkbox"/>	1	1-1
<input type="checkbox"/>	2	1-1
<input type="checkbox"/>	3	1-1
<input type="checkbox"/>	4	1-1
<input type="checkbox"/>	5	1-1
<input type="checkbox"/>	6	1-1
<input type="checkbox"/>	7	1-1
<input type="checkbox"/>	8	1-1
<input type="checkbox"/>	9	1-1

Buttons: Delete, Apply, Cancel

The following table describes the labels in this screen.

Table 46 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.

Table 46 Configuration > NAT > Full Feature > Address Mapping (continued)

LABEL	DESCRIPTION
Type	<ol style="list-style-type: none"> 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.
Apply	Click Apply to save your changes back to the ZyXEL device.
Cancel	Click Cancel to close this screen without applying any changes.

9.3.5 Edit Full Feature Address Mapping

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

Figure 68 Configuration > NAT > Full Feature > Edit Address Mapping

Table 47 Configuration > NAT > Full Feature > Edit Address Mapping

LABEL	DESCRIPTION
Type	<p>When you select Type you can choose a server mapping set. Choose the port mapping type from one of the following.</p> <ol style="list-style-type: none"> 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. 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. Many-to-Many Ov (Overload): Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses. Many One-to-One: Many One-to-one mode maps each local IP address to unique global IP addresses. 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	<p>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.</p> <p>This field is N/A for One-to-One and Server mapping types.</p>
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	<p>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.</p> <p>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.</p>
Save	Click Save to save your changes back to the ZyXEL device.
Cancel	Click Cancel to return to the previous screen.

9.4 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.

9.4.1 Configuring Trigger Port

Select **Full Feature** in, click **Edit** and then click the **Trigger Port** tab to bring up the next screen.

Figure 69 Configuration > NAT > Full Feature > Trigger Port

	Index	Name	Incoming		Trigger	
			Start Port	End Port	Start Port	End Port
<input type="checkbox"/>	0		0	0	0	0
<input type="checkbox"/>	1		0	0	0	0
<input type="checkbox"/>	2		0	0	0	0
<input type="checkbox"/>	3		0	0	0	0
<input type="checkbox"/>	4		0	0	0	0
<input type="checkbox"/>	5		0	0	0	0
<input type="checkbox"/>	6		0	0	0	0
<input type="checkbox"/>	7		0	0	0	0
<input type="checkbox"/>	8		0	0	0	0
<input type="checkbox"/>	9		0	0	0	0
<input type="checkbox"/>	10		0	0	0	0
<input type="checkbox"/>	11		0	0	0	0

The following table describes the labels in this screen.

Table 48 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 48 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.

9.4.2 Edit Trigger Port

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

Figure 70 Configuration > NAT > Full Feature > Trigger Port > Edit

The following table describes the labels in this screen.

Table 49 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 71 Configuration > Static Route

	Index	Name	Active	Destination	Gateway
<input type="radio"/>	1		false	0.0.0.0	0.0.0.0
<input type="radio"/>	2		false	0.0.0.0	0.0.0.0
<input type="radio"/>	3		false	0.0.0.0	0.0.0.0
<input type="radio"/>	4		false	0.0.0.0	0.0.0.0
<input type="radio"/>	5		false	0.0.0.0	0.0.0.0
<input type="radio"/>	6		false	0.0.0.0	0.0.0.0
<input type="radio"/>	7		false	0.0.0.0	0.0.0.0
<input type="radio"/>	8		false	0.0.0.0	0.0.0.0
<input type="radio"/>	9		false	0.0.0.0	0.0.0.0
<input type="radio"/>	10		false	0.0.0.0	0.0.0.0

1 2 3 4 5 Next

Edit Apply Reset

Table 50 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 72 Configuration > Static Route > Edit

Table 51 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.

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 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.

11.1.4 Data Confidentiality

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

11.1.5 Data Integrity

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

11.1.6 Data Origin Authentication

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

11.1.7 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.

11.1.7.1 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.

11.1.7.2 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 52 AH and ESP

ESP	AH
<p>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.</p>	<p>MD5 (default) MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.</p>
<p>3DES Triple DES (3DES) is a variant of DES, which iterates three times with three separate keys ($3 \times 56 = 168$ bits), effectively doubling the strength of DES.</p>	<p>SHA1 SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.</p>

Table 52 AH and ESP (continued)

ESP	AH
AES Advanced Encryption Standard data encryption 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 DES for minimal security and 3DES or AES for maximum. Select NULL to set up a tunnel without encryption.	Select MD5 for minimal security and SHA-1 for maximum security.

11.1.8 Key Management

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

11.1.9 Encapsulation

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

11.1.9.1 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.

11.1.9.2 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.

11.1.10 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 53 VPN and NAT

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

11.1.11 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 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.

11.1.12 NAT Traversal

NAT traversal allows you to set up a VPN connection when there are NAT routers between end IPSec VPN tunnel devices.

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.

11.1.12.1 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.

11.1.13 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 54 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 55 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 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.
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 Addr field below.	

11.1.14 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.

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.

11.1.15 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 known by the responder and both parties want to use pre-shared key authentication.

11.1.16 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.

11.1.17 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).

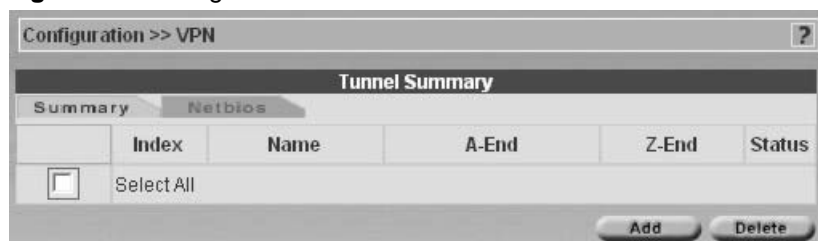
11.1.18 Pre-Shared Key

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.

11.2 VPN Tunnel Summary

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

Figure 73 Configuration > VPN



The following table describes the labels in this screen.

Table 56 Configuration > VPN

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

Table 56 Configuration > VPN (continued)

LABEL	DESCRIPTION
A-End/Z-End	<p>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.</p> <p>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.</p> <p>If you configure a Single-Side-VPN tunnel then a Non-ZyXEL-Device is supported at the Z-End.</p>
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 .

11.2.1 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 74 Configuration > VPN > Tunnel IPsec Detail

The following table describes the labels in this screen.

Table 57 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.
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.

Table 57 Configuration > VPN > Tunnel IPsec Detail (continued)

LABEL	DESCRIPTION
Active Protocol	<p>The ESP and AH protocols are necessary to create a Security Association (SA), the foundation of an IPsec VPN.</p> <p>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.</p> <p>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.</p>
Enable Replay Detection	
Keep Alive	<p>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.</p> <p>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</p>
A-End/Z-End	
NAT Traversal (Only Available in ZyWALL)	<p>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.</p> <p>The remote IPsec router must also have NAT traversal enabled.</p> <p>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.</p>
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	<p>Select IP to identify this ZyXEL device by its IP address.</p> <p>Select DNS to identify this ZyXEL device by a domain name.</p> <p>Select E-mail to identify this ZyXEL device by an e-mail address.</p> <p>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.</p>

Table 57 Configuration > VPN > Tunnel IPsec Detail (continued)

LABEL	DESCRIPTION
ID Content	<p>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.</p> <p>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.</p> <ul style="list-style-type: none"> ➤ 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	<p>This is the IP address(es) of computer(s) the A-end or Z-end of the VPN tunnel.</p> <p>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.</p> <p>The beginning and ending (static) IP addresses, in a range of computers are displayed when the Address Type is configured to Range.</p> <p>A (static) IP address and a subnet mask are displayed when the Address Type field is configured to Subnet.</p> <p>These addresses cannot be automatically generated by Vantage.</p>
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	<p>0 is the default and signifies any port.</p> <p>Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3</p> <p>Type a port number from 0 to 65535 for the starting port in a range.</p>
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 57 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 57 Configuration > VPN > Tunnel IPSec Detail (continued)

LABEL	DESCRIPTION
Encapsulation	<p>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.</p> <p>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</p>
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	<p>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.</p> <p>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.</p>
SA Life Time (Seconds)	<p>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).</p> <p>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.</p>
Perfect Forward Secrecy (PFS)	<p>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.</p> <p>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.</p> <p>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).</p>
Apply	Click Apply to apply your changes in this screen.
Cancel	Click Cancel to close this screen without applying any changes.

11.2.2 Manual VPN Tunnel

Select Manual from Figure 74 on page 157 to proceed to the next screen.

Figure 75 Configuration > VPN > Manual Tunnel IPsec Detail

The following table describes the labels in this screen.

Table 58 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 58 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	<p>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.</p> <p>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.</p>
Encapsulation	Select Tunnel mode or Transport mode from the drop-down list box.
Encryption Algorithm	<p>Select DES, 3DES or NULL from the drop-down list box.</p> <p>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.</p>
Authentication Algorithm	<p>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.</p>
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.

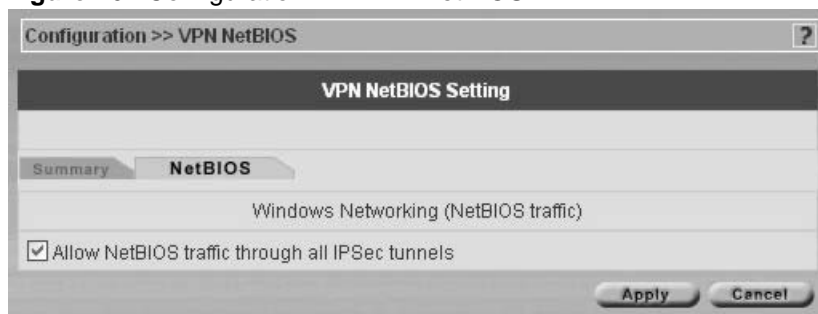
Table 58 Configuration > VPN > Manual Tunnel IPSec Detail (continued)

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

11.3 VPN and NetBIOS

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 76 Configuration > VPN > NetBIOS

The following table describes the labels in this screen.

Table 59 Configuration > VPN > NetBIOS

LABEL	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.

CHAPTER 12

Configuration > Firewall

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

12.1 Firewall Overview

Originally, the term *firewall* referred to a construction technique designed to prevent the spread of fire from one room to another. The networking term firewall is a system or group of systems that enforces an access-control policy between two networks. It may also be defined as a mechanism used to protect a trusted network from an untrusted network. Of course, firewalls cannot solve every security problem. A firewall is *one* of the mechanisms used to establish a network security perimeter in support of a network security policy. It should never be the *only* mechanism or method employed. For a firewall to guard effectively, you must design and deploy it appropriately. This requires integrating the firewall into a broad information-security policy. In addition, specific policies must be implemented within the firewall itself.

12.2 Types of Firewalls

There are three main types of firewalls:

- 1 Packet Filtering Firewalls
- 2 Application-level Firewalls
- 3 Stateful Inspection Firewalls

12.2.1 Packet Filtering Firewalls

Packet filtering firewalls restrict access based on the source/destination computer network address of a packet and the type of application.

12.2.2 Application-level Firewalls

Application-level firewalls restrict access by serving as proxies for external servers. Since they use programs written for specific Internet services, such as HTTP, FTP and telnet, they can evaluate network packets for valid application-specific data. Application-level gateways have a number of general advantages over the default mode of permitting application traffic directly to internal hosts:

- Information hiding prevents the names of internal systems from being made known via DNS to outside systems, since the application gateway is the only host whose name must be made known to outside systems.
- Robust authentication and logging pre-authenticates application traffic before it reaches internal hosts and causes it to be logged more effectively than if it were logged with standard host logging. Filtering rules at the packet filtering router can be less complex than they would be if the router needed to filter application traffic and direct it to a number of specific systems. The router need only allow application traffic destined for the application gateway and reject the rest.

12.2.3 Stateful Inspection Firewalls

Stateful inspection firewalls restrict access by screening data packets against defined access rules. They make access control decisions based on IP address and protocol. They also "inspect" the session data to assure the integrity of the connection and to adapt to dynamic protocols. These firewalls generally provide the best speed and transparency; however, they may lack the granular application level access control or caching that some proxies support.

Firewalls, of one type or another, have become an integral part of standard security solutions for enterprises.

12.3 Introduction to ZyXEL's Firewall

The ZyXEL device firewall is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated (in SMT menu 21.2 or in the web configurator). The ZyXEL device's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The ZyXEL device can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network. The ZyXEL device also has packet-filtering capabilities.

The ZyXEL device is installed between the LAN and a broadband modem connecting to the Internet. This allows it to act as a secure gateway for all data passing between the Internet and the LAN.

- The WAN (Wide Area Network) port attaches to the broadband modem (cable or ADSL) connecting to the Internet.
- The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers will have access to Internet services such as e-mail, FTP, and the World Wide Web. However, "inbound access" will not be allowed unless the remote host is authorized to use a specific service.

12.3.1 Denial of Service

Denials of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources. The ZyXEL device is pre-configured to automatically detect and thwart all known DoS attacks.

12.3.2 Basics

Computers share information over the Internet using a common language called TCP/IP. TCP/IP, in turn, is a set of application protocols that perform specific functions. An extension number, called the "TCP port" or "UDP port" identifies these protocols, such as HTTP (Web), FTP (File Transfer Protocol), POP3 (E-mail), etc. For example, Web traffic by default uses TCP port 80.

When computers communicate on the Internet, they are using the client/server model, where the server "listens" on a specific TCP/UDP port for information requests from remote client computers on the network. For example, a Web server typically listens on port 80. Please note that while a computer may be intended for use over a single port, such as Web on port 80, other ports are also active. If the person configuring or managing the computer is not careful, a hacker could attack it over an unprotected port.

Some of the most common IP ports are shown in Table 63 on page 176.

12.3.3 Types of DoS Attacks

There are four types of DoS attacks:

- 1 Those that exploit bugs in a TCP/IP implementation.

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

- 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.
- 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.

- 2 Those that exploit weaknesses in the TCP/IP specification.

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. 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.

- **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.
- 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.

3 Brute-force attacks that flood a network with useless data.

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.

- ICMP Vulnerability

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

Table 60 ICMP Commands That Trigger Alerts

13	TIMESTAMP_REQUEST
5	REDIRECT
14	TIMESTAMP_REPLY
17	ADDRESS_MASK_REQUEST
18	ADDRESS_MASK_REPLY

- Illegal Commands (NetBIOS and SMTP)

- NetBIOS

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

Table 61 Legal NetBIOS Commands

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

- SMTP

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

Table 62 Legal SMTP Commands

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

- 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.

4 IP Spoofing.

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 ZyXEL device blocks all IP Spoofing attempts.

12.4 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 ZyXEL device uses stateful packet inspection to protect the private LAN from hackers and vandals on the Internet. By default, the ZyXEL device'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.

12.4.1 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 packet is inspected by the firewall 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 **Firewall Summary** screen's **Action for packets that don't match firewall rules** field 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.

12.4.2 Stateful Inspection and the ZyXEL device

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 ZyXEL device itself (as with the "virtual connections" created for UDP and ICMP).

12.4.3 TCP Security

The ZyXEL device 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 ZyXEL device 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).

12.4.4 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 ZyXEL device 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.

12.4.5 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 ZyXEL device 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 Ports feature to do this.

12.4.6 Firewall Policies Overview

Firewall rules are grouped based on the direction of travel of packets to which they apply: The following example is for a ZyWALL 100 device.

- LAN to LAN/ZyWALL
- WAN to LAN
- DMZ to LAN

- LAN to WAN• WAN to WAN/ZyWALL• DMZ to WAN
- LAN to DMZ
- WAN to DMZDMZ to DMZ/ZyWALL



Note: DMZ is not available on all models. If a device has no DMZ port, the DMZ configuration menu will be grayed out.

By default, the ZyXEL device's stateful packet inspection allows packets traveling in the following directions:

- LAN to LAN/ZyWALL

This allows computers on the LAN to manage the ZyWALL and communicate between networks or subnets connected to the LAN interface.

- LAN to WAN
- LAN to DMZ
- WAN to DMZ
- DMZ to WAN

By default, the ZyXEL device's stateful packet inspection blocks packets traveling in the following directions:

- WAN to LAN
- WAN to WAN/ZyWALL

This prevents computers on the WAN from using the ZyXEL device as a gateway to communicate with other computers on the WAN and/or managing the ZyXEL device.

- DMZ to LAN
- DMZ to DMZ/ZyWALL

This prevents computers on the DMZ from communicating between networks or subnets connected to the DMZ interface and/or managing the ZyXEL device.

You may define additional rules and sets or modify existing ones but please exercise extreme caution in doing so.



Note: If you configure firewall rules without a good understanding of how they work, you might inadvertently introduce security risks to the firewall and to the protected network. Make sure you test your rules after you configure them.

For example, you may create rules to:

- Block certain types of traffic, such as IRC (Internet Relay Chat), from the LAN to the Internet.
- Allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN.
- Allow everyone except your competitors to access a Web server.
- Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

12.4.7 Rule Checklist

1. State the intent of the rule. For example, This restricts all IRC access from the LAN to the Internet. Or, This allows a remote Lotus Notes server to synchronize over the Internet to an inside Notes server.

- 1 Is the intent of the rule to forward or block traffic?
- 2 What direction of traffic does the rule apply to?
- 3 What IP services will be affected?
- 4 What computers on the LAN or DMZ are to be affected (if any)?
- 5 What computers on the Internet will be affected? The more specific, the better. For example, if traffic is being allowed from the Internet to the LAN, it is better to allow only certain machines on the Internet to access the LAN.

12.4.8 Security Ramifications

Once the logic of the rule has been defined, it is critical to consider the security ramifications created by the rule:

- 1 Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC is blocked, are there users that require this service?
- 2 Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?
- 3 Does a rule that allows Internet users access to resources on the LAN create a security vulnerability? For example, if FTP ports (TCP 20, 21) are allowed from the Internet to the LAN, Internet users may be able to connect to computers with running FTP servers.
- 4 Does this rule conflict with any existing rules?

Once these questions have been answered, adding rules is simply a matter of plugging the information into the correct fields in the web configurator screens.

12.4.9 Key Fields For Configuring Rules

12.4.9.1 Action

Should the action be to **Block** or **Forward**?



Note: Block means the firewall silently discards the packet.

12.4.9.2 Service

Select the service from the **Service** scrolling list box. If the service is not listed, it is necessary to first define it.

12.4.9.3 Source Address

What is the connection's source address; is it on the LAN, DMZ or WAN? Is it a single IP, a range of IPs or a subnet?

12.4.9.4 Destination Address

What is the connection's destination address; is it on the LAN, DMZ or WAN? Is it a single IP, a range of IPs or a subnet?

12.4.10 Alerts

Alerts are reports on events, such as attacks, that you may want to know about right away. You can choose to generate an alert when an attack is detected by selecting the **Generate alert when attack detected** checkbox.

Configure the **Log Settings** screen to have the ZyXEL device send an immediate e-mail message to you when an event generates an alert. Refer to the chapter on logs for details.

12.4.11 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.

Table 63 Services and Port Numbers

SERVICES	PORT NUMBER
ECHO	7
FTP (File Transfer Protocol)	21
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79

Table 63 Services and Port Numbers (continued)

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	

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 77 Configuration >Firewall

The following table describes the labels in this screen.

Table 64 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 <i>Appendices</i> for more on triangle route topology.
Attack Detected Alert	Select this checkbox to have the ZyXEL device generate an alert when it identifies an attack.
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 64 Configuration >Firewall (continued)

LABEL	DESCRIPTION
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.
Apply	Click Apply to save your changes back to the ZyXEL device.
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.

12.5.2 DoS Settings

Click the DoS settings link to configure global firewall Denial of Services settings.

Figure 78 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 *
<input type="checkbox"/> Blocking Time	0 (minutes)
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

The following table describes the labels in this screen.

Table 65 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 cause 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 65 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 80 on page 183, select an existing rule to edit it or click **Add** to create a new firewall rule.

Figure 79 Configuration >Firewall > Edit

The following table describes the labels in this screen.

Table 66 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 << .

Table 66 Configuration >Firewall > Edit (continued)

LABEL	DESCRIPTION
Custom Port	
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 80 Configuration >Firewall > IP Address

The following table describes the labels in this screen.

Table 67 Configuration >Firewall > IP Address

LABEL	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 81 Firewall Custom Port

The following table describes the labels in this screen.

Table 68 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 79 on page 182.
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 Logs

Select a device and then click **Configuration > Device Log**.

Figure 82 Configuration > Device Log > Device



The following table describes the labels in this screen.

Table 69 Device Log > Device

LABEL	DESCRIPTION
Select Time Period	Select the time period (Last Day, Last 2 Days...Last 7 Days) for which you wish to view logs.
Src	This field lists the source IP address and the port number of the incoming packet.
Dest	This field lists the destination IP address and the port number of the packet.
Time	This field displays the time the log was recorded. See the chapter on system maintenance and information to configure the ZyXEL device's time and date.
Content	This field states the reason for the log.
Note	This field displays a short description.
Retrieve	Click Retrieve to renew the logs displayed for the selected device.
Purge	Click Purge to erase the logs displayed for the selected device. Only an administrator with the correct permissions that can see the device can purge the logs.
Report	Click Report to generate a report on the logs for the time period selected and the current page displayed only.

13.2 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** and then click the **Log Settings** tab. The screen appears as shown next.

Figure 83 Configuration > Device Logs > Log Settings

Configuration >> Log >> Log Settings

Configuration: Log Settings

Device | **Log Setting**

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 Address (Server Name or IP Address)

Log Facility

Send Log

Log Schedule

Day for Sending Log

Time for Sending Log (Hour) (Minute)

Log Send Immediate Alert

System Maintenance

System Errors

Access Control

UPnP

Forward Web Sites

Blocked Web Sites

Attacks

IPSec

IKE

TCP Reset

Packet Filter

ICMP

Blocked Java etc.

PKI

802.1x

System Errors

Blocked Web Sites

Attacks

Blocked Java etc.

Access Control

IPSec

IKE

PKI

Apply Reset

The following table describes the labels in this screen.

Table 70 Configuration > Device Logs > 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.

Table 70 Configuration > Device Logs > Log Settings (continued)

LABEL	DESCRIPTION
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	<p>This drop-down menu is used to configure the frequency of log messages being sent as E-mail:</p> <ul style="list-style-type: none"> • Daily • Weekly • Hourly • When Log is Full • None. <p>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</p>
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.
Apply	Click Apply to save your customized settings and exit this screen.
Reset	Click Reset to begin configuring this screen afresh.

13.3 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 84 Purge Device Logs

The screenshot shows a configuration window titled "System>> Logs >> Vantage". Inside the window, the title "Purge Logs" is centered at the top. Below the title, there are two options, each with an unchecked checkbox: "Send e-mail Report to" followed by a text input field, and "Export Report". At the bottom right of the window, there are two buttons: "Apply" and "Cancel".

The following table describes the labels in this screen.

Table 71 Purge Device Logs

LABEL	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.

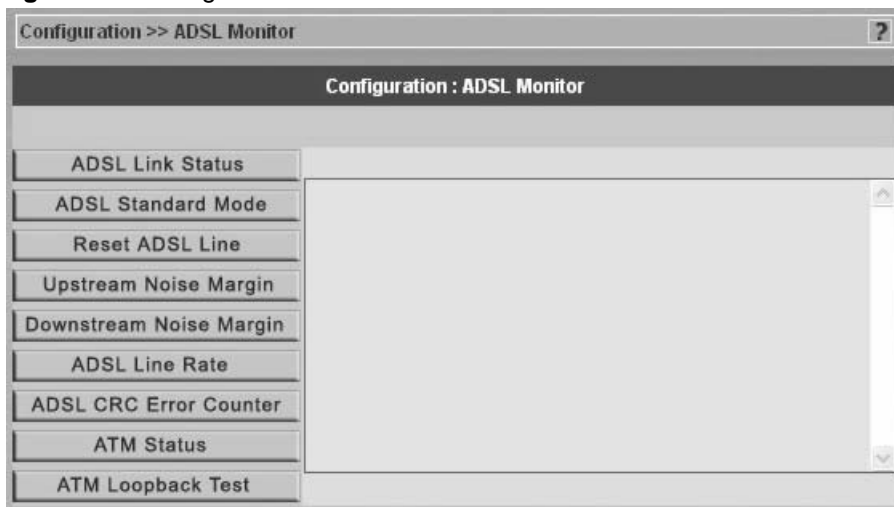
Table 72 ADSL Standards

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 85 Configuration > ADSL Monitor

The following table describes the labels in this screen.

Table 73 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 > Device Alarms

Use these screens to view and manage device alarms.

15.1 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.

15.1.1 Alarm Classifications

There are four alarm severity classifications.

Table 74 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.

15.1.2 Alarm States

When an alarm is received by Vantage, it can be in one of three states:

Table 75 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.

15.1.3 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 86 Configuration > Device Alarms >Current

The screenshot shows a web interface titled 'Config >> Alarms'. Below the title is a dark header 'Alarms' with two tabs: 'Current' (selected) and 'Historical'. There are three filter sections: 'Select Time Period' with a dropdown set to 'Last 24Hr', 'Select Severity of Alarm' with a dropdown set to 'All', and 'Select Responder' with a dropdown set to 'All'. Below these is a table with columns: Index, Type, Severity, Time, Status, Responder, Response Time, and Description. A 'Select All' checkbox is located below the table. At the bottom right are four buttons: 'Retrieve', 'Respond', 'Clear', and 'Report'.

The following table describes the labels in this screen.

Table 76 Configuration > Device Alarms >Current

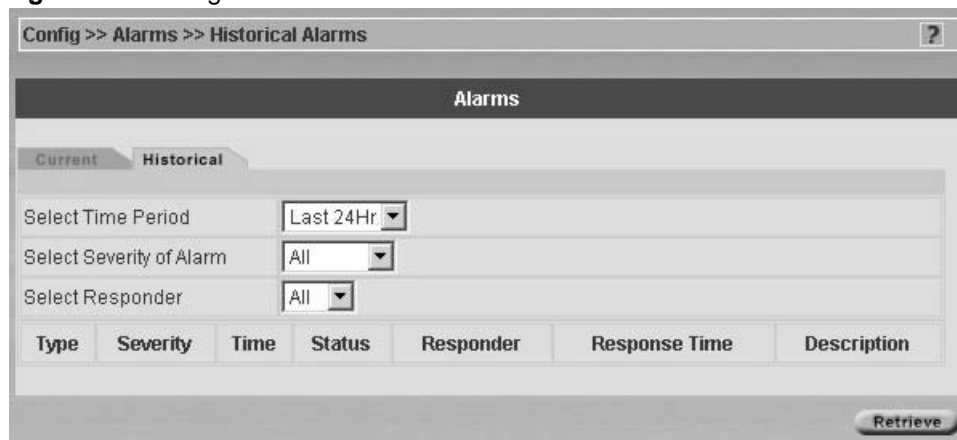
LABEL	DESCRIPTION
Select Time Period	Select the time period (24, 48 or 72 hours) for which you wish to view logs.
Select Severity of Alarm.	Select the severity of the alarm (see above) for which you wish to view logs
Select Responder	Select All or root to display all of the administrators or root administrators 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 76 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.

15.1.4 Historical Alarms Screen

This screen displays a history of device alarm logs.

Figure 87 Configuration > Device Alarms > Historical

The following table describes the labels in this screen.

Table 77 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 77 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 16

Building Blocks (BBs)

16.1 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.

16.2 BB Properties

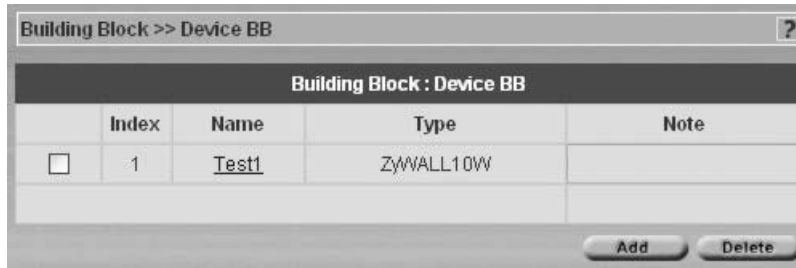
You can only view (and use) BBs in your own domain. You cannot view other administrator's BBs, including BBs created by the root administrator. When creating new BBs from old ones use the save as icon () to save as a new BB.

If you modify a BB, changes only affect new device configurations that use this BB and not previous ones.

16.3 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 88 Building Block > Device BB



The following table describes the fields in this screen

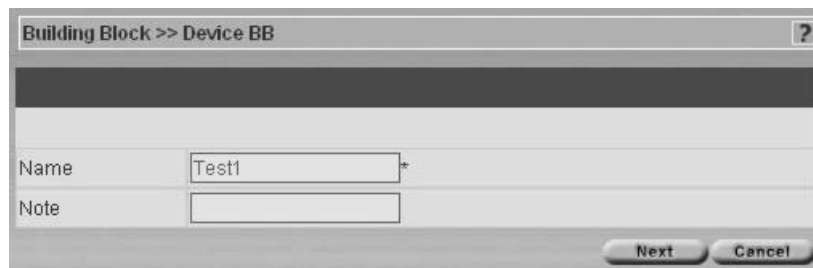
Table 78 Building Block > Device BB

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.

16.3.1 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 89 Building Block > Device BB > Edit



The following table describes the fields in this screen

Table 79 Building Block > Device BB > Edit

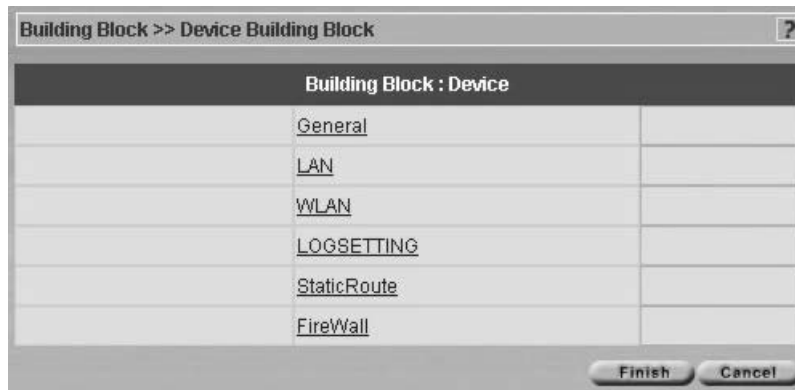
TYPE	DESCRIPTION
Name	Type a unique name for the building block.
Note	Type some extra description of the BB

Table 79 Building Block > Device BB > Edit (continued)

TYPE	DESCRIPTION
Next	Click to proceed to the following screen
Cancel	Click to return to the previous screen.

16.3.2 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 90 Building Block > Device BB > Edit > Configuration

16.3.3 Adding a New BB

Click **Add** from Figure 88 on page 199. 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 91 Building Block > Device BB > Add

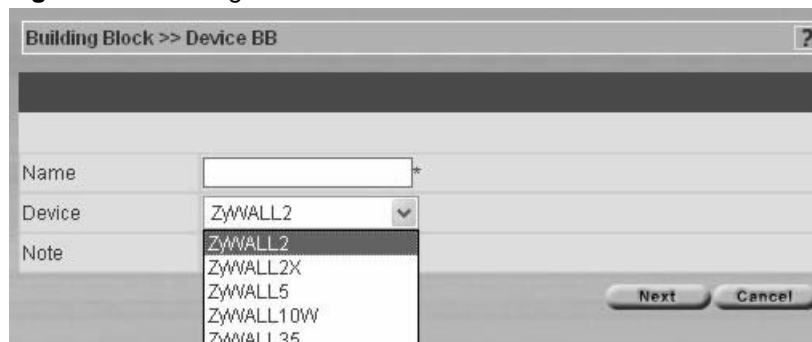


Table 80 Building Block > Device BB > Add

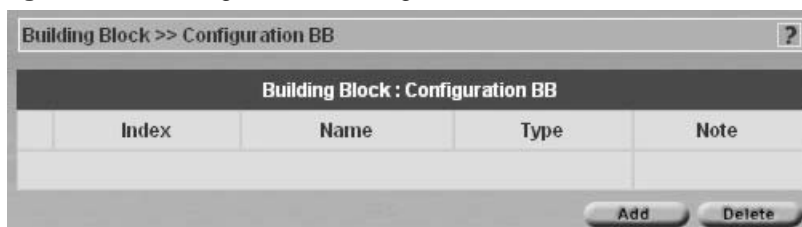
TYPE	DESCRIPTION
Name	Type a unique name for the building block.
Device	Select the device model.
Note	Type some extra description of the BB
Next	Click to proceed to the following screen
Cancel	Click to return to the previous screen.

16.4 Configuration BBs

Configuration building blocks depend on the device type.

Click **Building Block > Configuration BB**.

Figure 92 Building Block > Configuration



The following table describes the fields in this screen

Table 81 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.
Note	This field displays some extra description of the BB

Table 81 Building Block > Configuration (continued)

TYPE	DESCRIPTION
Add	Click to proceed to the next screen.
Delete	Click to delete a selected device BB.

16.4.1 Adding a Configuration BB

Click **Add** from Figure 92 on page 201. 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 93 Building Block > Configuration BB > Add

The following table describes the fields in this screen

Table 82 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 93 on page 202, the next screen that appears depends on the **Device** and **Type** fields you selected in Figure 93 on page 202. Figure 93 on page 202 and Figure 94 on page 203 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 94 Building Block > Configuration BB > Add > Next

Configuration >> General >> System

Configuration: General

System | DDNS | Time Setting

System Name *

Domain Name

Administrator Inactivity Timer *(Minutes, 0 means no timeout)

First DNS Server

Second DNS Server

Third DNS Server

The completed configuration BB is shown next. You may edit this BB by clicking the **Name** hyperlink.

Figure 95 Building Block > Configuration BB > Added

Building Block >> Configuration BB

Building Block : Configuration BB

	Index	Name	Type	Note
<input type="checkbox"/>	1	MyMy	ZyWALL2 : ZyWALL General	Marcom ZyWALL

16.4.2 Editing a Configuration BB

Click the **Name** hyperlink in the **Building Block > Configuration BB** screen (as shown in Figure 95 on page 203 for example) to edit an existing configuration. What you can edit in a configuration building block depends on the configuration type and device.

Figure 96 Building Block > Configuration BB > Edit

The following table describes the fields in this screen

Table 83 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 94 on page 203.
Cancel	Click Cancel to return to the previous screen.

16.5 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 97 Building Block > Component BB

The following table describes the fields in this screen

Table 84 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.
Type	This field displays the component type, for example, E-mail.
Note	This field displays some extra description of the BB

Table 84 Building Block > Component BB (continued)

TYPE	DESCRIPTION
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.

16.5.1 Adding a Component BB

Click **Add** in Figure 97 on page 204 to create a brand new component BB.

Figure 98 Building Block > Component BB > Add

The following table describes the fields in this screen

Table 85 Building Block > Component > Add

TYPE	DESCRIPTION
Name	Type a unique name for the building block.
Type	Select from IP or E-mail .
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.

16.5.1.1 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 99 Building Block > Component BB > Add > IP Address

The following table describes the fields in this screen

Table 86 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.

16.5.1.2 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 100 Building Block > Component BB > Add > E-Mail Address

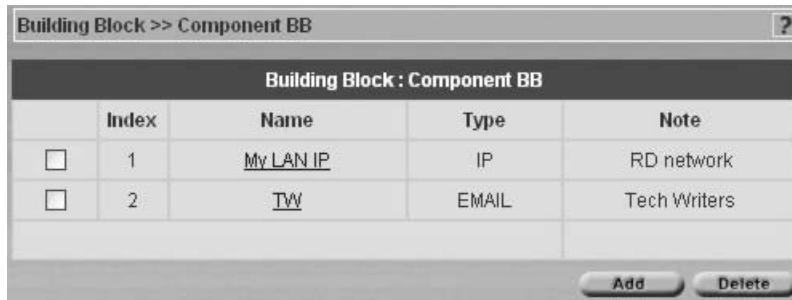
The following table describes the fields in this screen

Table 87 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.

The following screen then shows the component BBs you added. Click a **Name** hyperlink to edit the BB.

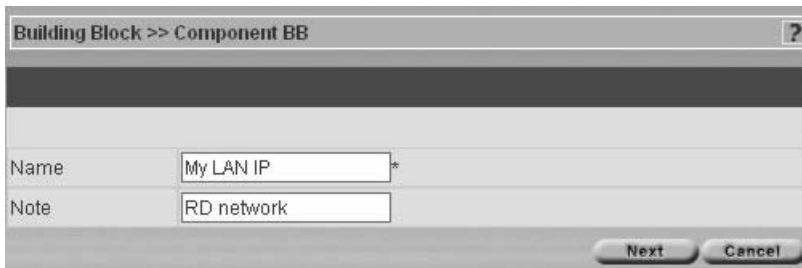
Figure 101 Component BBs Added



16.5.2 Editing a Component BB

Click the **Name** hyperlink in the component BB summary screen as shown in Figure 101 on page 207 to edit a component BB.

Figure 102 Building Block > Component BB > Edit



The following table describes the fields in this screen

Table 88 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 the next screen to edit the component BB details as shown in Figure 99 on page 206 or Figure 100 on page 206.
Cancel	Click Cancel to return to the previous screen.

CHAPTER 17

System > Administrators

Use these screens to manage Vantage administrators.

17.1 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".

17.1.1 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.

17.1.1.1 "Root" Administrator

The default system name (and password) when you first log in is "root". This is a default system Administrator account, which cannot be deleted by anyone from the system. 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.

17.1.1.2 “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.

17.1.1.3 “Normal” Administrators

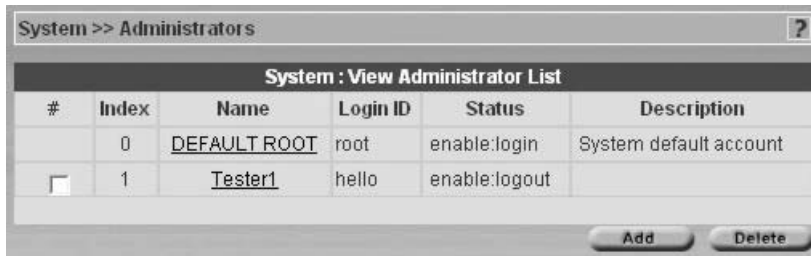
These administrators have default permissions enabled as shown on the screen. Some permissions are not allowed. The Administrator who creates the “Normal” Administrator determines which of the enabled permissions to disable. Normal Administrators cannot associate nor disassociate other Administrators.

17.1.1.4 “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.

17.2 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 103 System > View Administrator List

The following table describes the fields in this screen.

Table 89 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.
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.

17.3 Creating an Administrator Account

Click **Add** to create a new Administrator account or select an existing Administrator account to edit it.

17.3.1 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 104 System > Administrator Details

The following table describes the fields in this screen.

Table 90 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.
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.

17.3.2 Administrator Permissions

You may select which permissions (privileges) an administrator may have from the next screen.

Figure 105 System > Administrator Permissions

The following table describes the fields in this screen.

Table 91 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 <i>section 1.1</i> 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 91 System > Administrator Permissions (continued)

LABEL	DESCRIPTION
System Management	System Management is defined as follows: <ul style="list-style-type: none">➤ 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 18

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.

18.1 Status

Click **System > Status** to view the current Vantage system status. This is a read-only screen.

Figure 106 System > Vantage Status

System Status	
Vantage CNM Server public IP	172.21.3.18
FTP server	172.21.3.18 <input type="button" value="Check"/> Connection OK!
Mail Server	127.0.0.1 <input type="button" value="Check"/> Connection OK!
Syslog Server	172.21.3.18 <input type="button" value="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 92 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 92 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.

18.2 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.

18.2.1 Upgrade Procedure

- 1 Click **System > Upgrade** to start the upgrade procedure.

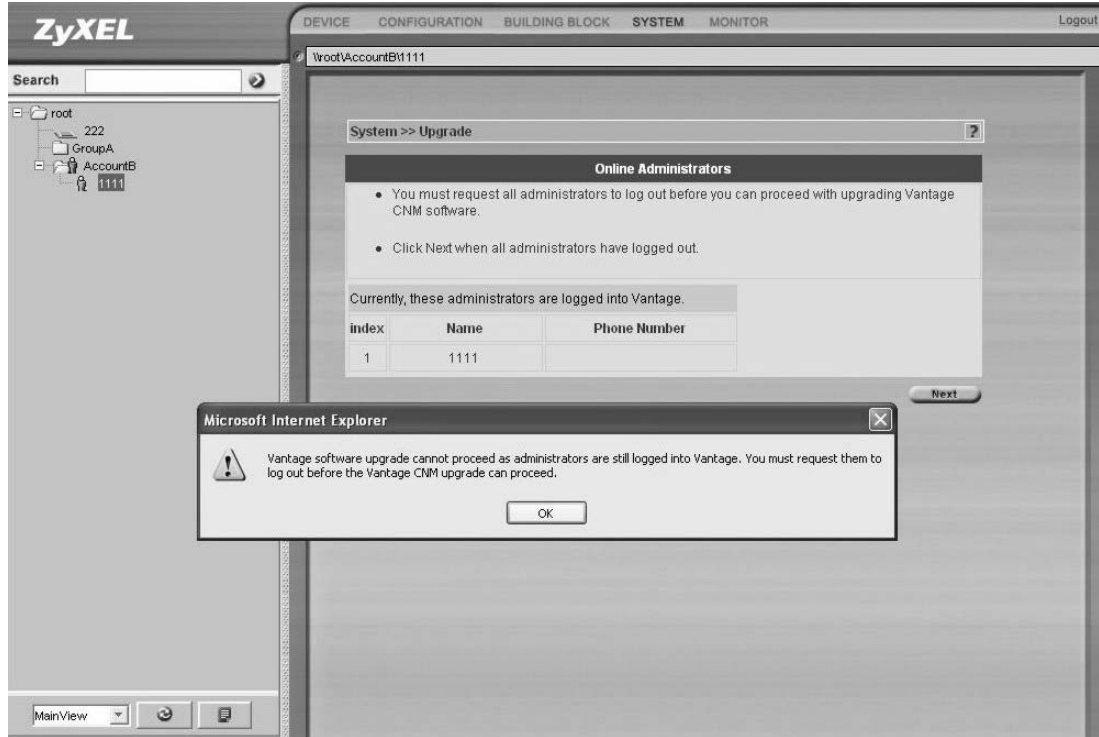
A warning screen appears if there are administrators logged into Vantage. Click **OK** to view the **Online Administrators** screen.



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.

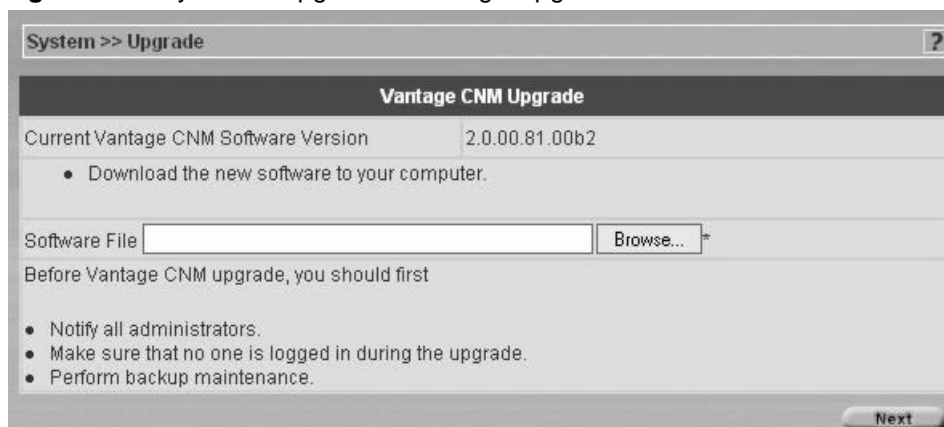
The administrator details include an administrator **Index** number, **Name** and **Phone** number (if configured).

Figure 107 System > Upgrade > Online Administrators

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 108 System > Upgrade > Vantage Upgrade

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 109 System > Upgrade > Vantage Upgrade > Next

You must wait while Vantage CNM is upgrading.

Figure 110 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.

18.2.2 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 93 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 the Vantage CNM 2.0 for Windows XP SP1 without a patch is **2.0.00.61.00**. The version code of the Vantage CNM 2.0 for RedHat Linux 9.0 without a patch is **2.0.00.81.00**.

18.3 License Management

You need a license key to generate an **Activation Key** and **Server Set Key** (at www.myZyZEL.com) 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 111 System > License > License Management

The following table describes the fields in this screen.

Table 94 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.

18.3.1 License Upgrade

Click **Upgrade** in Figure 111 on page 218 to display this screen.

Figure 112 System > License > License Management > Upgrade

The following table describes the fields in this screen.

Table 95 System > License > License Management > Upgrade

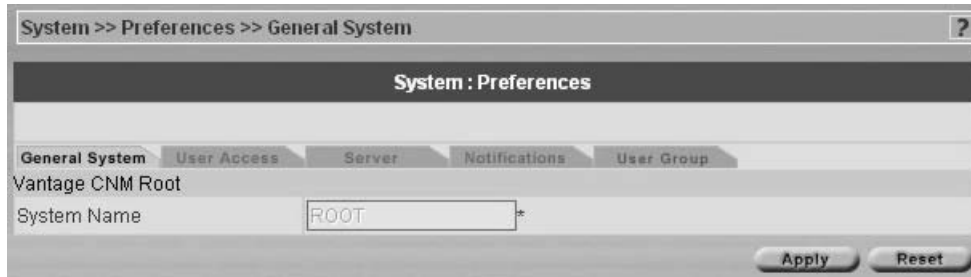
LABEL	DESCRIPTION
Activation Key	Copy and paste or type the Activation Key that is generated in the myZyXEL.com website.
Service Set Key	Copy and paste or type the Service Set Key that is generated in the myZyXEL.com website.
Apply	Click Apply to begin the license upgrade process. Vantage must have an Internet connection.
Cancel	Click Cancel to return to the previous screen.

18.4 System > Preferences

System preferences are global Vantage server settings.

18.4.1 General Vantage Preferences

This is a read only screen.

Figure 113 System > Preferences > General System

The following table describes the fields in this screen.

Table 96 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.

18.4.2 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 114 System > Preferences > User Access

The following table describes the fields in this screen.

Table 97 System > Preferences > User Access

LABEL	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.

18.4.3 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 *User's Guide appendices* for examples of setting up syslog and FTP servers. The syslog server must be either a Linux syslog server or Kiwi for Windows¹. Vantage communicates with a Linux syslog server using SSH, so you must enable the SSH daemon on the Linux syslog server. Vantage communicates with a Windows (Kiwi) syslog server using Telnet, so you must enable Telnet on the Windows (Kiwi) syslog server. See the *Quick Start Guide* for information on configuring the Linux syslog server to send logs to Vantage.

1. Only these syslog servers are supported at the time of writing.

Figure 115 System > Preferences > Server

The following table describes the fields in this screen.

Table 98 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.
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.

Table 98 System > Preferences > Server (continued)

LABEL	DESCRIPTION
Mail Server	The mail (SMTP) server is used to send Vantage notifications. Select the checkbox to activate the fields below.
IP Address	Type the IP address of the mail server here.
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.

18.4.3.1 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 116 Vantage Icon - Stop

Right-click the icon again and select **START**.

Figure 117 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.

18.4.4 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 118 System > Preferences > Notifications

The following table describes the fields in this screen.

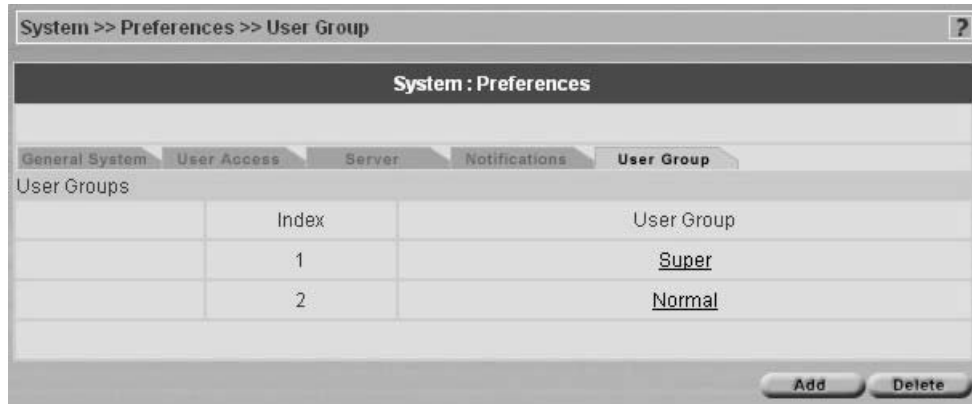
Table 99 System > Preferences > Notifications

LABEL	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.

18.4.5 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 119 System > Preferences > User Group



The following table describes the fields in this screen.

Table 100 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.

18.4.5.1 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 120 System > Preferences > Permissions > Add

System Preferences	
Add User Group	
User Group ID	<input type="text"/>
Device registration, deletion, mapping, unmapping	<input type="checkbox"/>
Administrator Management	<input type="checkbox"/>
Firmware Management, upgrade and configuration file Management	<input type="checkbox"/>
Monitor Management	<input type="checkbox"/>
Device Configuration	<input type="checkbox"/>
Device data synchronization	<input type="checkbox"/>
System Management	<input type="checkbox"/>

The following table describes the fields in this screen.

Table 101 System > Preferences > Permissions > Add

LABEL	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: <ul style="list-style-type: none"> ➤ 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.

18.5 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.

18.5.1 System Maintenance Management

Use this screen to delete previous (old) system backups.

Figure 121 System > Maintenance > Management



The following table describes the fields in this screen.

Table 102 System > Maintenance > Management

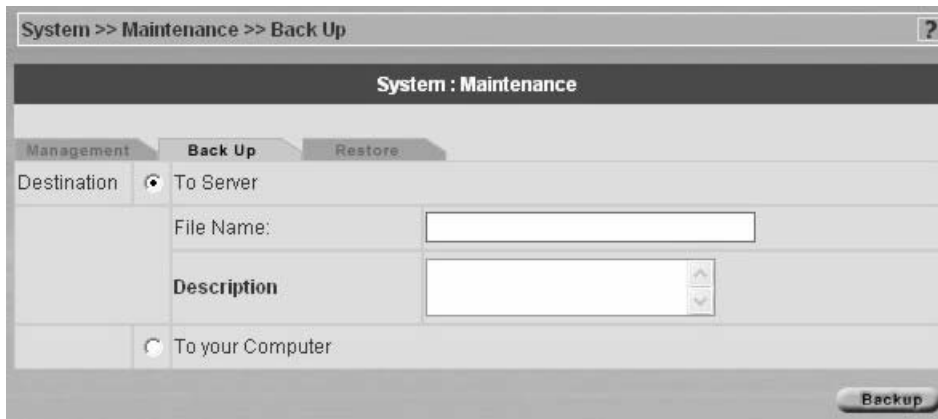
LABEL	DESCRIPTION
Index	This field displays the system backup file index number.
Name	This field displays the system backup file name.
Description	This field displays some extra description of the system backup file.
Backed Up Date	This field displays the date the system backup file was created.
Administrator	This field displays who created the system backup file.
Delete	Select a system backup file and then click Delete to remove it from Vantage.

18.5.2 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 122 System > Maintenance > Backup



The following table describes the fields in this screen.

Table 103 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.

18.5.3 Restore System Maintenance

Use this screen to restore a previously saved system backup (from your computer or Vantage) to Vantage.

Figure 123 System > Maintenance > Restore

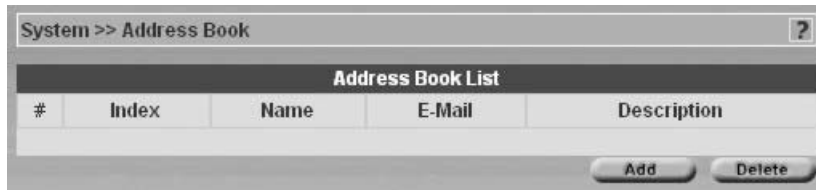
The following table describes the fields in this screen.

Table 104 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.

18.6 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 124 System > Address Book

The following table describes the labels in this screen.

Table 105 System > Address Book

LABEL	DESCRIPTION
#	This is a number defining an address book entry.
Index	This field displays the address book entry index number.
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.

18.6.1 Address Book Add/Edit

From Figure 124 on page 231, click **Add** to create a new entry or click an existing entry hyperlink to edit it.

Figure 125 System > Address Book Add/Edit

The screenshot shows a web-based form for adding or editing an address book entry. The form is titled 'System : address' and is part of the 'System >> Address Book' menu. It includes the following fields:

- Name: A text input field with an asterisk indicating it is required.
- Description: A text input field.
- Contact Address: A group of fields including Address line 1, Address line 2, City, State/Province, ZIP/Postal Code, and a Region dropdown menu.
- Telephone Number: A text input field.
- E-mail: A text input field.

At the bottom right of the form, there are two buttons: 'Apply' and 'Cancel'.

The following table describes the labels in this screen.

Table 106 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.

18.7 Certificate Management Overview

Some ZyXEL devices 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 the ZyXEL device 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.

The ZyXEL device 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).

18.7.1 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.

18.7.2 Current Certification Information

You can view your current certificate information in the following screen, including certificate name, type, origin and duration of validity.

Figure 126 System > Certificate Management > Information

The following table describes the labels in this screen.

Table 107 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. REQ represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the My Certificate Import screen to import the certificate and replace the request. SELF represents a self-signed certificate. *SELF represents the default self-signed certificate, which the ZyXEL device uses to sign imported trusted remote host certificates. CERT represents a certificate issued by a certification authority.
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). 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.

18.7.3 Create a Certificate

You can create certificates by entering the requested information into the fields below. Then click **Apply**.

Figure 127 System > Certificate Management > Create CSR

The following table describes the labels in this screen.

Table 108 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.

18.7.4 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 128 System > Certificate Management > Import Certificate

The following table describes the labels in this screen.

Table 109 System > Certificate Management > Import Certificate

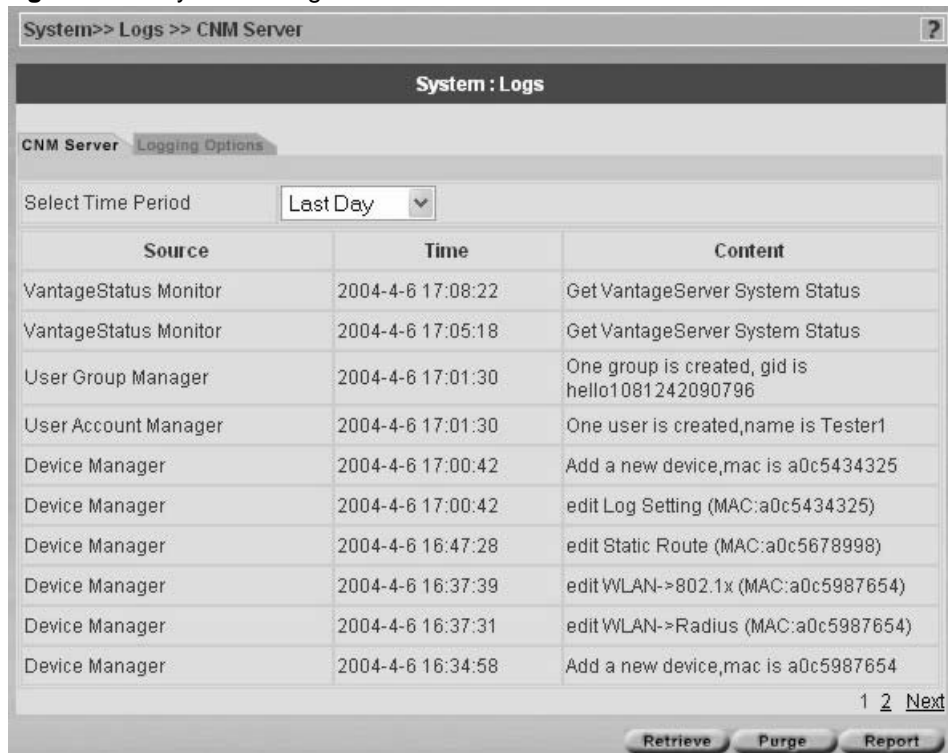
LABEL	DESCRIPTION
Input Certificate	
Input Your Certificate Path	Type in the location of the certificate you want to upload in this field or click Browse ... to find it.
Apply	Click Apply to save these changes.
Back	Click Back to return to the previous screen.

18.8 Vantage Logs

Use these screens to view and configure Vantage system log preferences.

18.8.1 CNM Server

You can view system logs for previous day, the last two days or up to one week here.

Figure 129 System > Logs > CNM Server

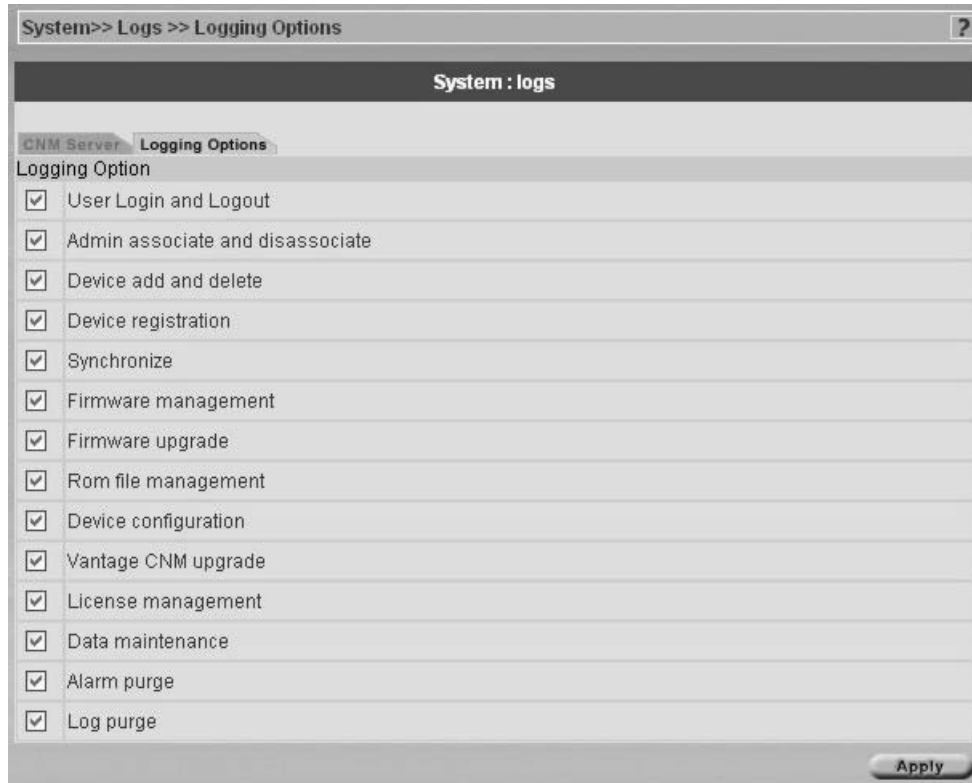
The following table describes the labels in this screen.

Table 110 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.

18.8.2 Vantage Logging Options

Select what type of system logs you wish to log as shown in the following screen.

Figure 130 System > Logging Options

18.9 About Vantage

The **About** screen provides some basic information about Vantage as shown in the following screen.

Figure 131 System > About Vantage

System >> About	
System : About	
Version	2.0.00.81.00b2
Date	2004-05-31
Copyright	Copyright ZyXEL Communications Corporation 1995-2004.

CHAPTER 19

Monitor > Alarms

This chapter describes the monitor alarms.

19.1 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.

19.1.1 Alarm Types

There are three types of alarms.

Table 111 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.

19.1.2 Alarm Classifications

There are four alarm severity classifications.

Table 112 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.

19.1.3 Alarm States

When an alarm is received by Vantage, it can be in one of three states:

Table 113 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.

19.1.4 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 132 Monitor > Current Alarms

Monitor >> Alarms

Alarms

Current Historical

Select Time Period: Last 24Hr

Select Type of Alarm: All

Select Severity of Alarm: All

Select Responder: All

<input type="checkbox"/>	Index	Type	Source	Severity	Time	Status	Responder	Response Time	Description
<input type="checkbox"/>	0	CNM	System Manager	!	2004-3-24-15:51:49	Active		0	Found syslog server doesn't work,when receive log. Please configure right Syslog Server!
<input type="checkbox"/>	1	CNM	System Manager	!	2004-3-24-15:41:36	Active		0	Found syslog server doesn't work,when receive log. Please configure right Syslog Server!
<input type="checkbox"/>	2	CNM	System Manager	!	2004-3-24-15:31:23	Active		0	Found syslog server doesn't work,when receive log. Please configure right Syslog Server!
<input type="checkbox"/>	3	CNM	System Manager	!	2004-3-24-15:21:10	Active		0	Found syslog server doesn't work,when receive log. Please configure right Syslog Server!
<input type="checkbox"/>	4	CNM	System Manager	!	2004-3-24-15:10:57	Active		0	Found syslog server doesn't work,when receive log. Please configure right Syslog Server!
<input type="checkbox"/>	5	CNM	System Manager	!	2004-3-24-15:0:44	Active		0	Found syslog server doesn't work,when receive log. Please configure right Syslog Server!
<input type="checkbox"/>	6	CNM	System Manager	!	2004-3-24-14:50:31	Active		0	Found syslog server doesn't work,when receive log. Please configure right Syslog Server!
<input type="checkbox"/>	7	CNM	System Manager	!	2004-3-24-14:40:18	Active		0	Found syslog server doesn't work,when receive log. Please configure right Syslog Server!
<input type="checkbox"/>	8	CNM	System Manager	!	2004-3-24-14:30:5	Active		0	Found syslog server doesn't work,when receive log. Please configure right Syslog Server!
<input type="checkbox"/>	9	CNM	System Manager	!	2004-3-24-14:19:52	Active		0	Found syslog server doesn't work,when receive log. Please configure right Syslog Server!
<input type="checkbox"/>	10	CNM	System Manager	!	2004-3-24-14:9:39	Active		0	Found syslog server doesn't work,when receive log. Please configure right Syslog Server!
<input type="checkbox"/>	11	CNM	ADSL Monitor	!	2004-3-24-14:1:38	Active		0	This Device test2 has not Registered to CNM all along!
<input type="checkbox"/>	12	CNM	ADSL Monitor	!	2004-3-24-14:1:36	Active		0	This Device test2 has not Registered to CNM all along!
<input type="checkbox"/>	13	CNM	System Manager	!	2004-3-24-13:59:26	Active		0	Found syslog server doesn't work,when receive log. Please configure right Syslog Server!
<input type="checkbox"/>	14	CNM	System Manager	!	2004-3-24-13:49:13	Active		0	Found syslog server doesn't work,when receive log. Please configure right Syslog Server!

Select All

1 2 3 [Next](#)

Table 114 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.
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.

19.1.5 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 133 Monitor > Historical Alarms

Monitor >> Alarms >> Historical Alarms

Alarms

Current Historical

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
------	--------	----------	------	--------	-----------	---------------	-------------

Retrieve

4See Table 114 on page 243 for more information on fields in this table.

CHAPTER 20

Other Monitor Screens

Firmware Upgrade means that Vantage signals the device to request a firmware FTP upload from Vantage.

20.1 Firmware Upgrade Report

Details of firmware uploaded to Vantage are shown as in the next screen.

Figure 134 Monitor > Firmware Upgrade Report



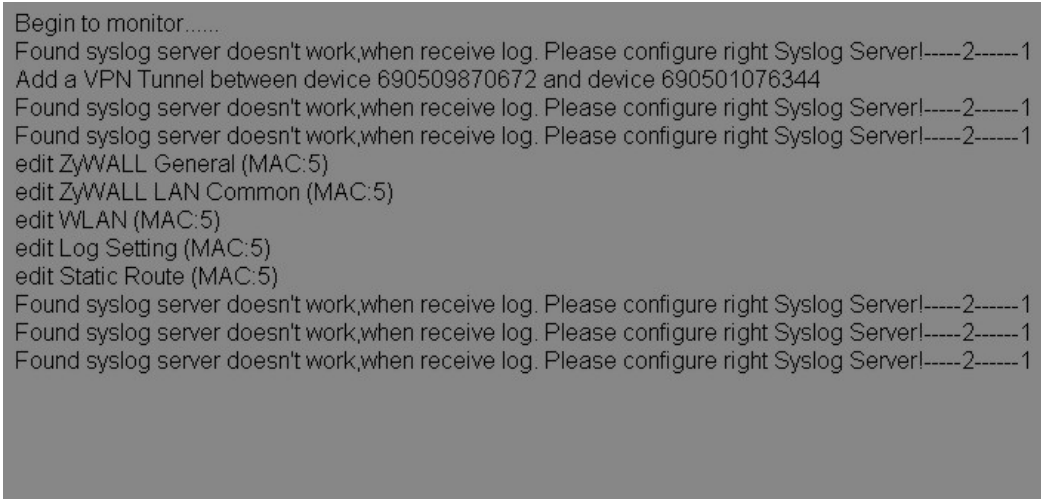
The following table describes the labels in this screen.

Table 115 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 data maintenance prior to uploading.
Purge	Select Purge to delete selected reports from the Vantage server.

20.2 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 135 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
```

20.3 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.

20.3.1 Graphical VPN Tunnel Creation

Configure IPSec tunnels graphically as follows

- 1 Drag the ZyXEL device icons around the screen as you please. Drag them apart to view each device more clearly. Save this view by clicking **Save**.
- 2 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.
- 3 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 Table 57 on page 157 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 136 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	<input type="text"/> \root\Easter	Z-End Device	<input type="text"/> \root\Taiwan\Meridius
My IP	<input type="text"/> 0.0.0.0*	My IP	<input type="text"/> 0.0.0.0*
Peer IP	<input type="text"/> 0.0.0.0*	Peer IP	<input type="text"/> 0.0.0.0*
ID Type	<input type="text"/> IP	ID Type	<input type="text"/> IP
ID Content	<input type="text"/>	ID Content	<input type="text"/>
Address Type	<input type="text"/> Single	Address Type	<input type="text"/> Single
Address Start	<input type="text"/> *	Address Start	<input type="text"/> *
Address End	<input type="text"/>	Address End	<input type="text"/>
Port Start	<input type="text"/> 0*	Port Start	<input type="text"/> 0*
Port End	<input type="text"/> 0	Port End	<input type="text"/> 0

Phase 1		Phase 2	
Negotiation Mode	<input type="text"/> Main	Active Protocol	<input type="text"/> ESP
Pre-Shared Key	<input type="text"/> *	Encapsulation	<input type="text"/> Tunnel
Encryption Algorithm	<input type="text"/> DES	Encryption Algorithm	<input type="text"/> DES
Authentication Algorithm	<input type="text"/> MD5	Authentication Algorithm	<input type="text"/> MD5
SA Life Time (Seconds)	<input type="text"/> 28800*	SA Life Time (Seconds)	<input type="text"/> 28800*
Key Group	<input type="text"/> DH1	Perfect Forward Secrecy (PFS)	<input type="text"/> None

Back Apply Cancel

- 4 See Table 57 on page 157 for more information on the fields in this screen. 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 137 Configuration > VPN - Example Tunnel Summary

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](#)

If you are not redirected, click the **Try here** hyperlink to go to the next screen.

The **Tunnel Summary** details are added to the top of the **IPSec Summary**, see *Figure 4-5* in the order they are configured (last tunnel appears last in the list).

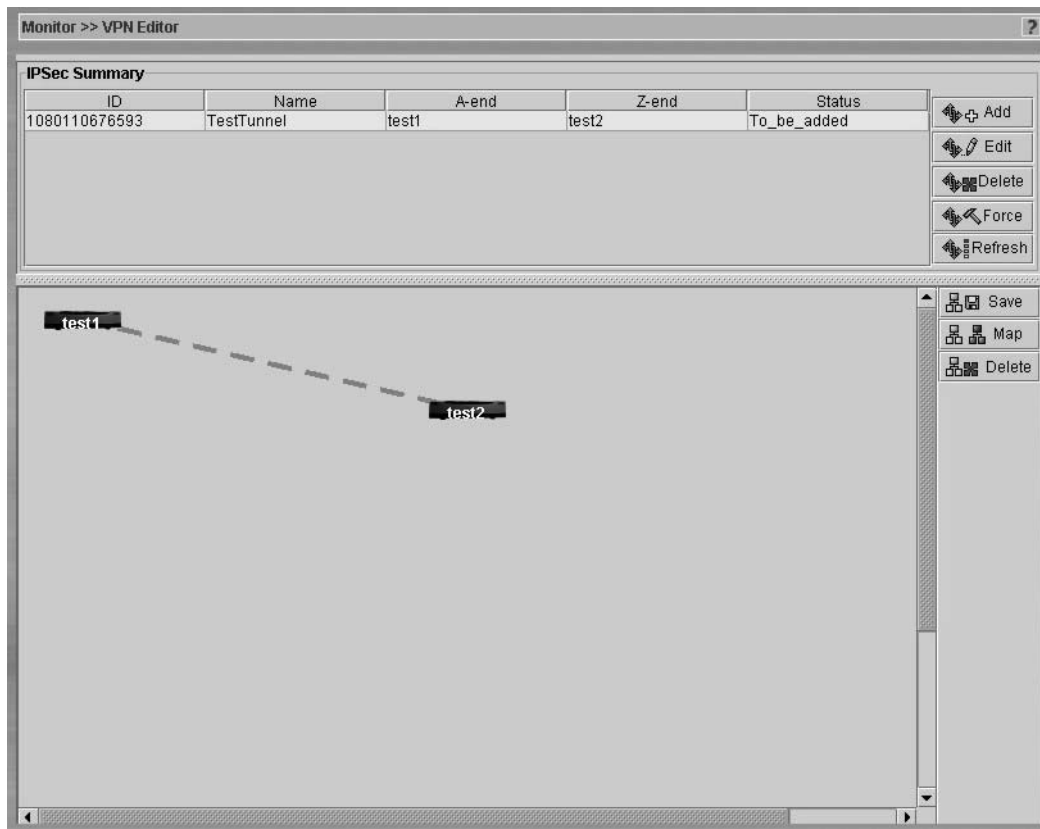
20.3.2 Graphical Tunnel Depictions

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).

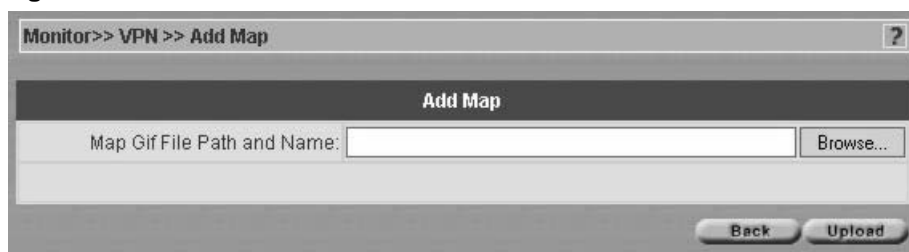
A green solid line means an active tunnel (with traffic) between the ZyXEL devices.

The icons are dragged apart and dashed lines indicating VPN Tunnels are created after configuring the **Tunnel IPSec Detail** screen.

Figure 138 Monitor > VPN Monitor – Graphical Tunnel

20.3.3 Map

Click the **Map** button to upload a background image such as a map. Click the **Map** button in the IPsec **Summary** to upload a background gif (only) image. Type a file and path name or browse for your required file. Click **Upload**.

Figure 139 Monitor > VPN > Add MAP

Appendix A

FTP Server (WFTPD) Setup Example

Installing WFTPD

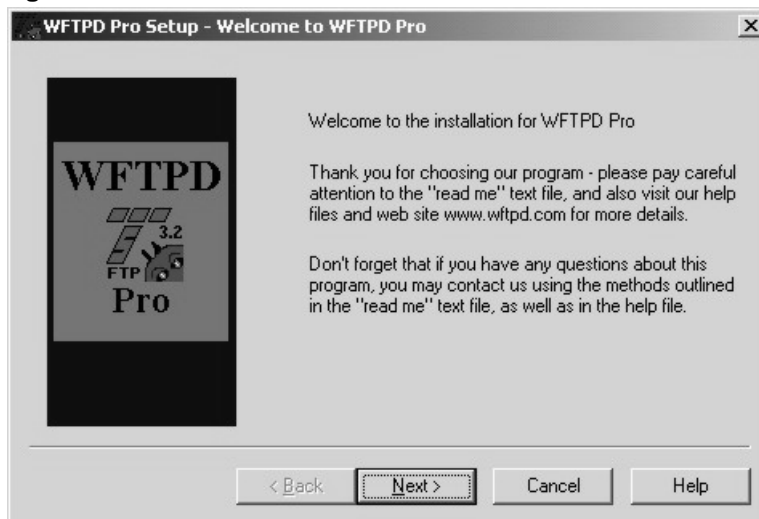
- 1 Download the WFTPD software from www.wftpd.com to where you want to install it.
- 2 Double-click setup.exe to begin the wizard.

Figure 140 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

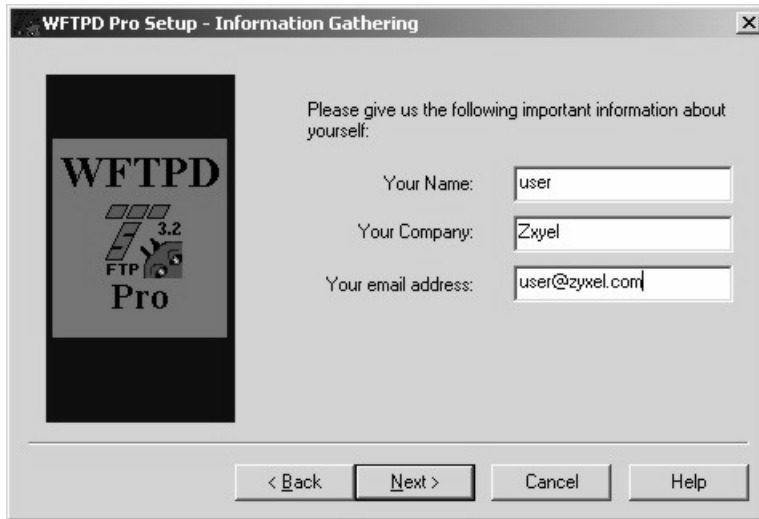
- 3 Click **Next** to begin and then follow the wizard prompts.

Figure 141 Wizard 1



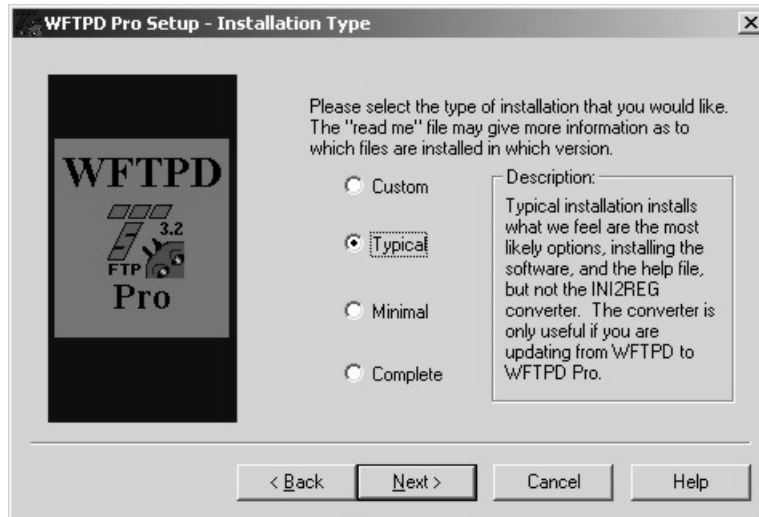
- 4 Enter your details here as shown and click **Next**.

Figure 142 Information

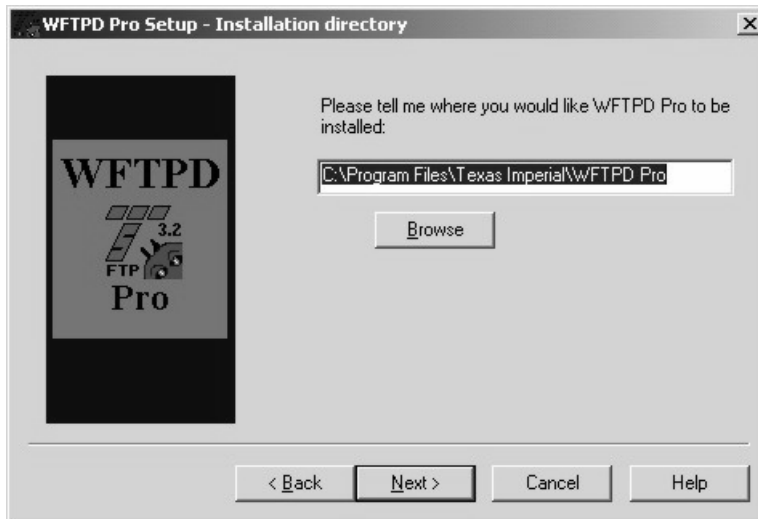


5 Select the installation type and click **Next**.

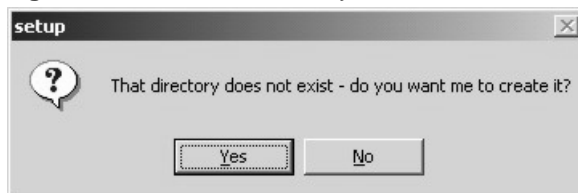
Figure 143 Installation Type



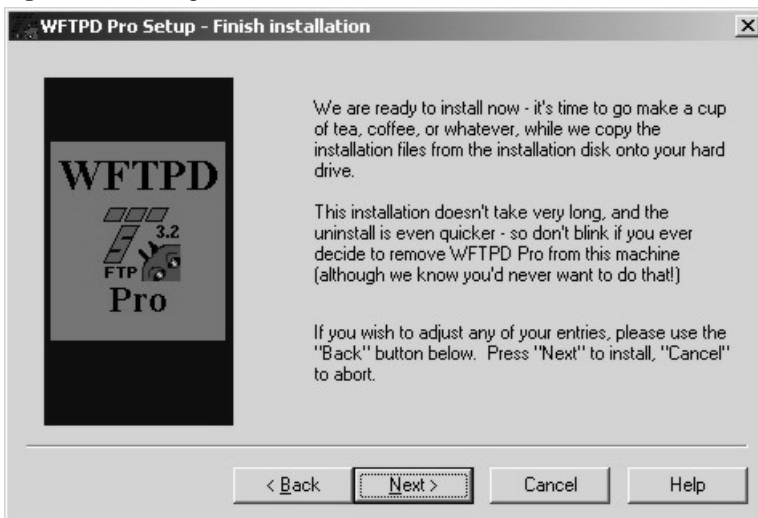
6 Select where to install WFTPD Pro and click **Next**.

Figure 144 Installation Directory

- 7 You are prompted to create the directory if it doesn't already exist. Click **Yes** to create a new directory.

Figure 145 Create Directory

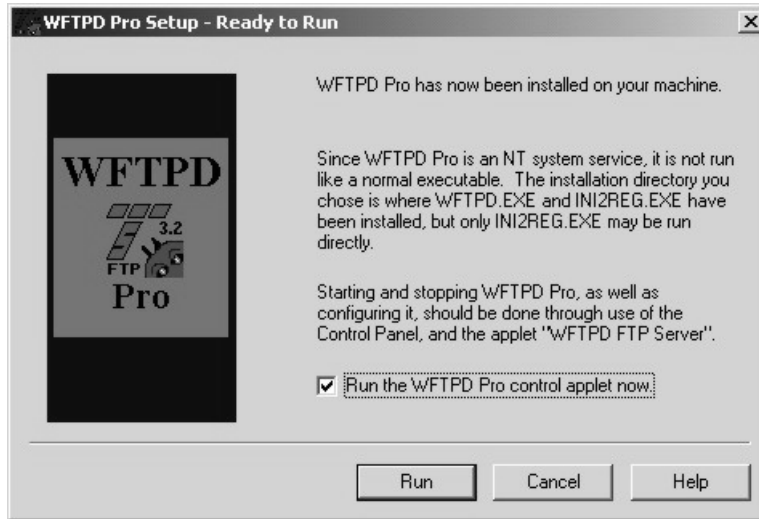
- 8 Click **Next** to begin the installation.

Figure 146 Begin Installation

- 9 WFTPD has been installed. Click **Run** to start it. Make sure the check box is selected.

Running WFTPD

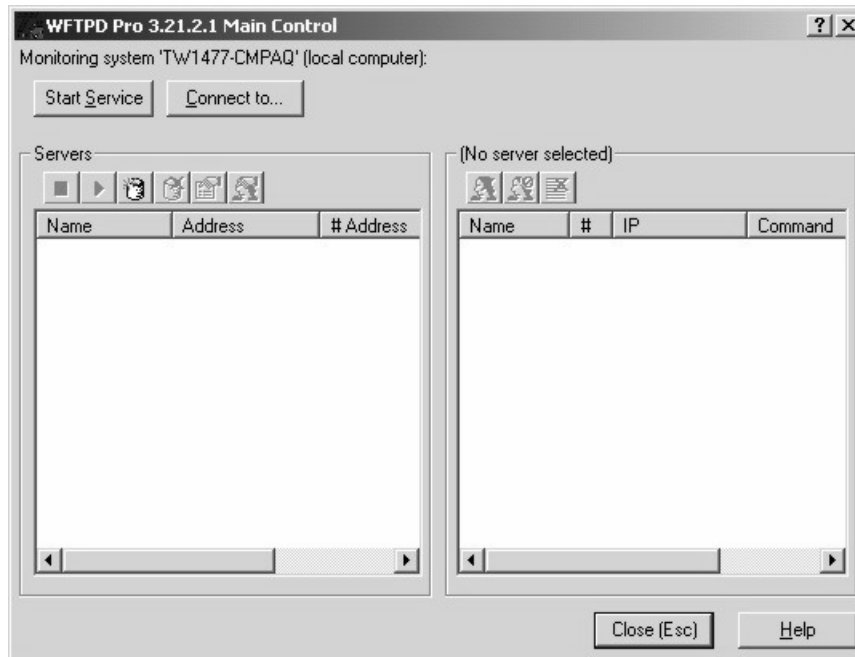
Figure 147 Run WFTPD



10 Click **Start Service** form the WFTPD main screen.

WFTPD main screen.

Figure 148 WFTPD Main Screen



11 Open **Administrative Tools** in the Windows **Control Panel** and then select **Services** to see the WFTPD Pro service.

Figure 149 Windows Services

Service Name	Description	Status	Startup Type	Log On As
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 150 WFTPD Properties

WFTPD Pro Properties (Local Computer)

General | Log On | Recovery | Dependencies

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\WFTPD~1\WFTPD.EXE

Startup type: Automatic

Service status: Started

Start Stop Pause Resume

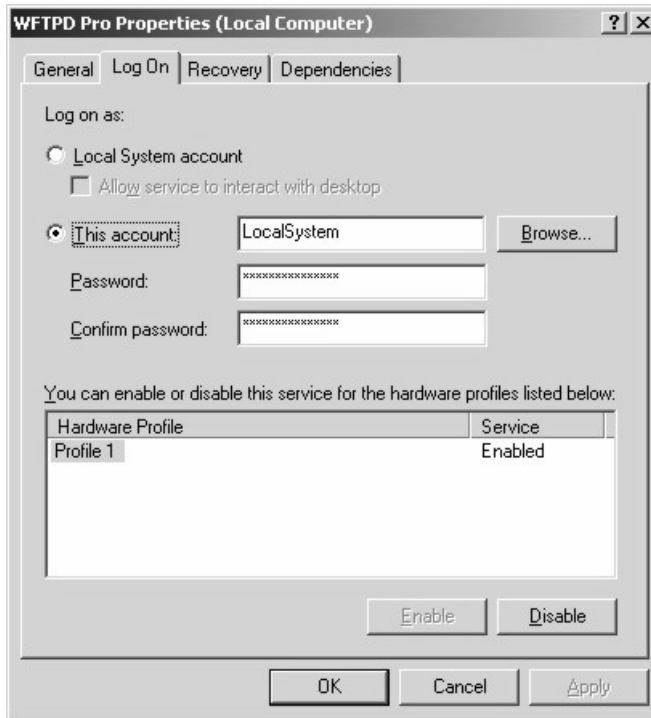
You can specify the start parameters that apply when you start the service from here.

Start parameters:

OK Cancel Apply

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 151 WFTPD Pro Log On



Appendix B

Configuring the Kiwi Syslog Daemon

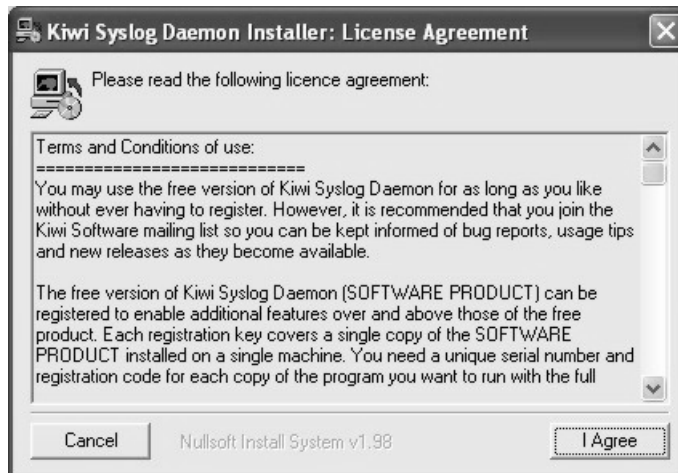
This section shows you how to install and configure the KiWi Syslog Daemon for use with Vantage CNM 2.0.

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 152 Kiwi Syslog Daemon Installation: License Agreement



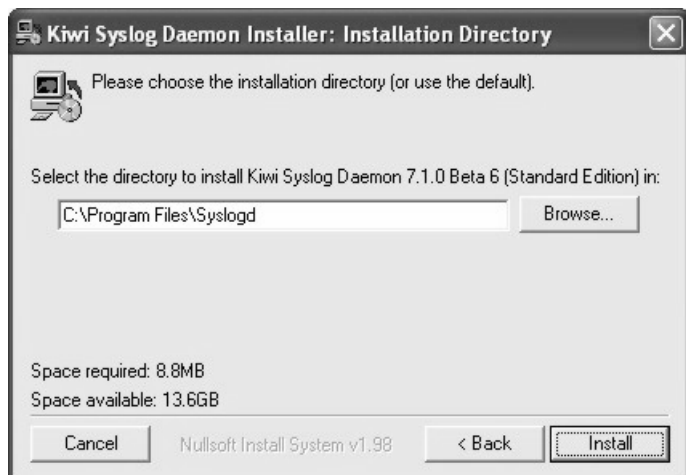
- 3 Select the installation type (the default is **Normal**) and click **Next**.

Figure 153 Kiwi Installation: Installation Options

4 Click **Install** to install Kiwi to the default directory.



Note: You must install Kiwi in the C:\Program Files\Syslog directory for the Vantage CNM 2.0 syslog function to work.

Figure 154 Kiwi Installation: Installation Directory

Wait before the installation process completes.

Importing the Syslog Configuration File

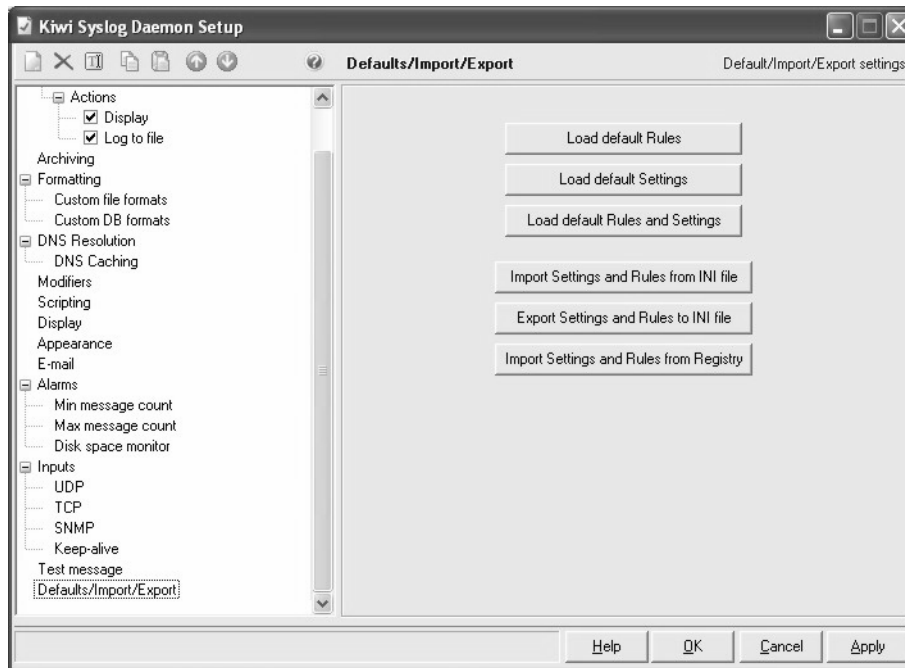
After installing the Kiwi Syslog Daemon, follow the steps below to import the configuration file.

- 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**.

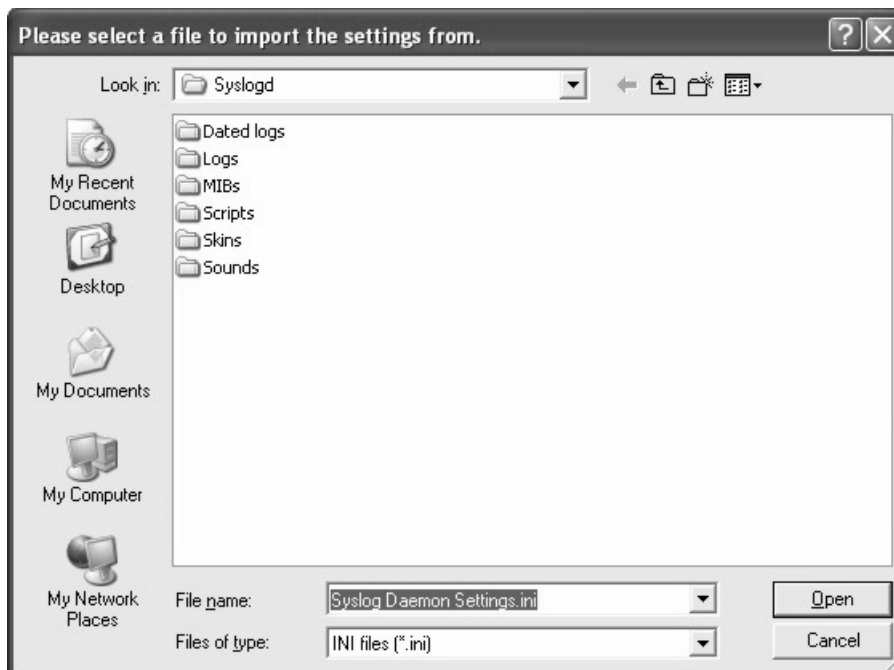
4 Click **Import Settings and Rules from INI file**.

Figure 155 Kiwi Syslog Daemon Setup



5 Locate the “.ini” syslog configuration file you saved to your computer in step 1 and click **Open**.

Figure 156 Kiwi Syslog Daemon Setup: Import Configuration File



6 Click **Yes** to confirm the configuration file import.

Figure 157 Kiwi Syslog Daemon Setup: Import Configuration File: Confirm

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**.

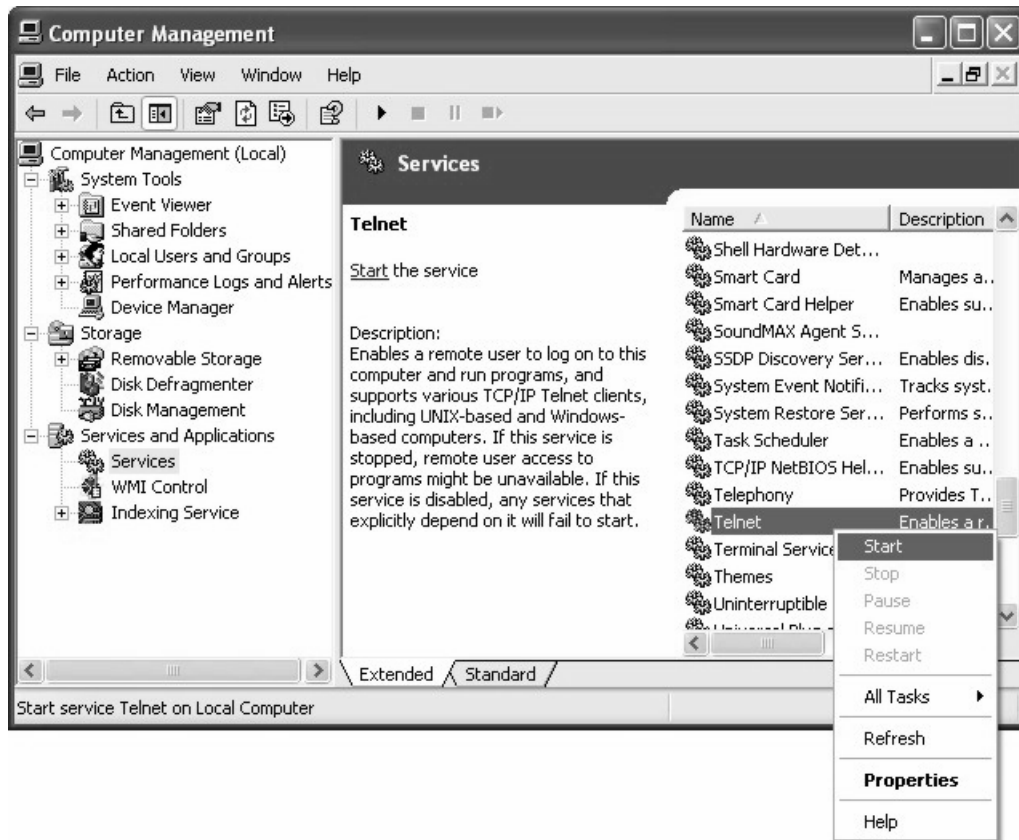
Figure 158 Windows XP: My Computer



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 159 Windows XP: Computer Management



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 2.0. 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 160 Vantage System Servers

The screenshot shows the 'System Preferences' window with the 'Server' tab selected. The window title is 'System >> Preferences >> Server'. The 'Server' tab is active, showing configuration options for four server types: Com Server, FTP Server, Syslog Server, and Mail Server. Each server type has a checkbox and several input fields. The 'Syslog Server' section is highlighted, indicating it is the current focus. The 'Syslog Server OS' dropdown is set to 'Linux'. At the bottom right, there are 'Apply' and 'Reset' buttons.

Server Type	IP Address	User Name	Password	Other Fields
<input type="checkbox"/> Com Server	1.1.1.1			
<input type="checkbox"/> FTP Server	172.31.3.80	user	••••	
<input type="checkbox"/> Syslog Server	172.31.3.80	user	••••	Syslog Server OS: Linux
<input type="checkbox"/> Mail Server	172.31.3.80	user	••••	

- 3 Select **Syslog Server**, then 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

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..

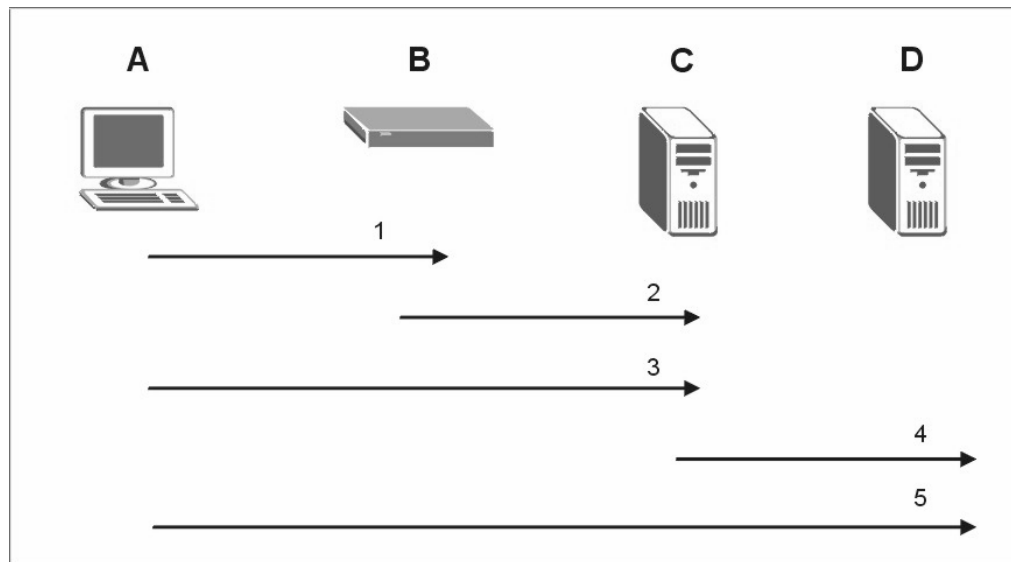


Table 116 FTP and syslog Server Overview

LABEL	DESCRIPTION
A	This is the Vantage CNM 2.0 server.
B	This is any ZyXEL device.
C	This is a syslog server
D	This is an FTP server
1	Vantage sends syslog server and FTP server information to the device when you register the device with Vantage.
2	The syslog server must receive the log at local facility 2 ^a and then writes the log file to <code>/var/log/vantage.log</code> .
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 116 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 footnote a}

Appendix D

Java Console Debug Messages

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 161 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 162 Java Plug-in Control Panel



- 3 Open Internet Explorer and log into Vantage CNM 2.0. 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 163 Java Plug-in Icon

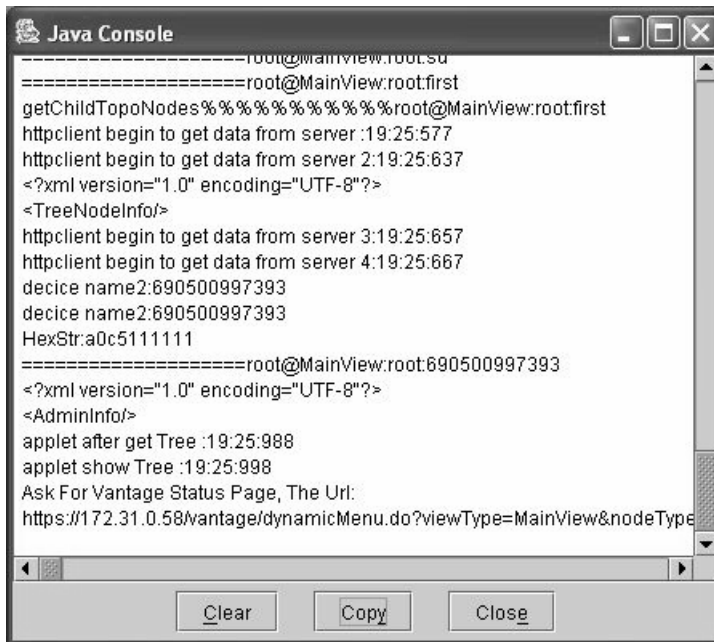


- 4 Right-click on the Java plug-in icon and select **Open Control Panel**, to view the Java Console screen.

Figure 164 Open Control Panel



- 5 In the Java Console window, click **Copy**.

Figure 165 Java ConsoleA screenshot of a Java Console window. The window title is "Java Console". The text inside the console shows a sequence of log messages. It starts with "root@MainView.root:sd", followed by "====root@MainView.root:sd", "getChildTopoNodes%%%%%%%%root@MainView:root:sd", "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 :19:25:988", "Ask For Vantage Status Page, The Url:", "https://172.31.0.58/vantage/dynamicMenu.do?viewType=MainView&nodeType". At the bottom of the window, there are three buttons: "Clear", "Copy", and "Close".

```
====root@MainView.root:sd
====root@MainView.root:sd
getChildTopoNodes%%%%%%%%root@MainView:root:sd
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 :19:25:988
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 E

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 117 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 118 Allowed IP Address Range By Class

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

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). A subnet mask has 32 bits. If a bit in the subnet mask is a “1” then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is “0” then the corresponding bit in the IP address is part of the host ID.

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 119 “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 120 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 121 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 122 Subnet 1

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

Table 123 Subnet 2

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

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

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

Example: Four Subnets

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

Table 124 Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 125 Subnet 2

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	01000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 126 Subnet 3

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	10000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 127 Subnet 4

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	11000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example Eight Subnets

Similarly use a 27-bit mask to create 8 subnets (001, 010, 011, 100, 101, 110).

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

Table 128 Eight Subnets

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

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

Table 129 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 117) available for subnetting.

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

Table 130 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 F

Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

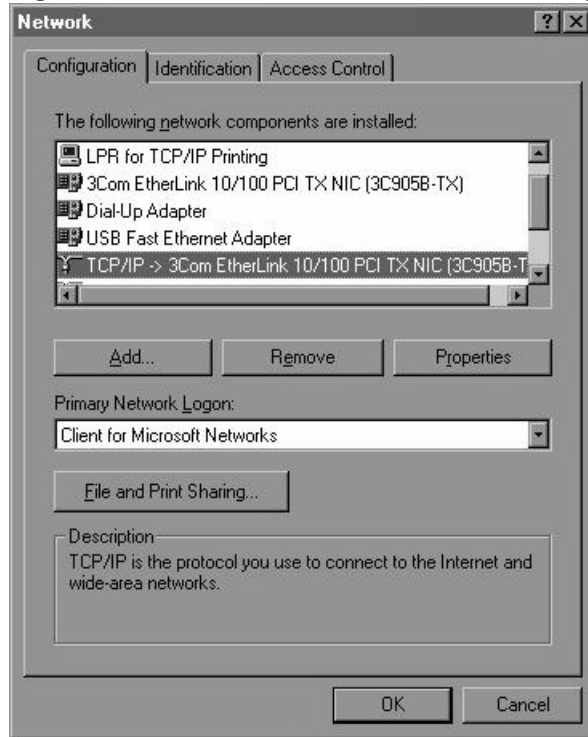
TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the Prestige's LAN port.

Windows 95/98/Me

Click **Start, Settings, Control Panel** and double-click the **Network** icon to open the **Network** window

Figure 166 Windows 95/98/Me: Network: Configuration

Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

- 1 In the **Network** window, click **Add**.
- 2 Select **Adapter** and then click **Add**.
- 3 Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

- 1 In the **Network** window, click **Add**.
- 2 Select **Protocol** and then click **Add**.
- 3 Select **Microsoft** from the list of **manufacturers**.
- 4 Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

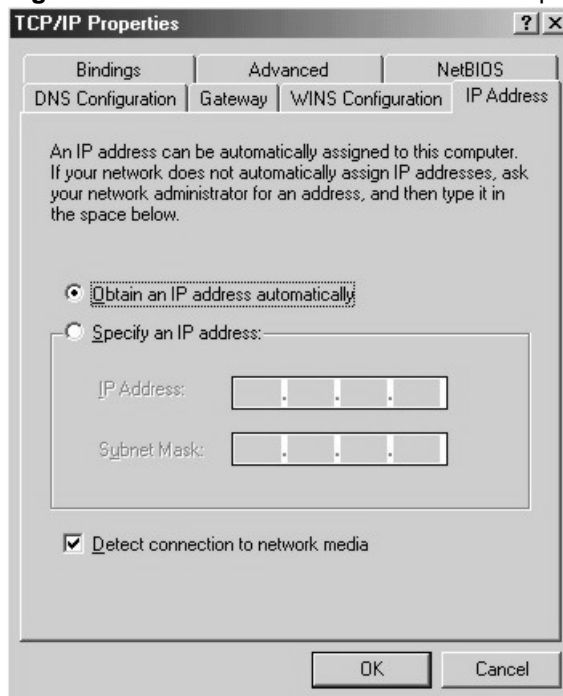
- 1 Click **Add**.
- 2 Select **Client** and then click **Add**.

- 3 Select **Microsoft** from the list of manufacturers.
- 4 Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.
- 5 Restart your computer so the changes you made take effect.

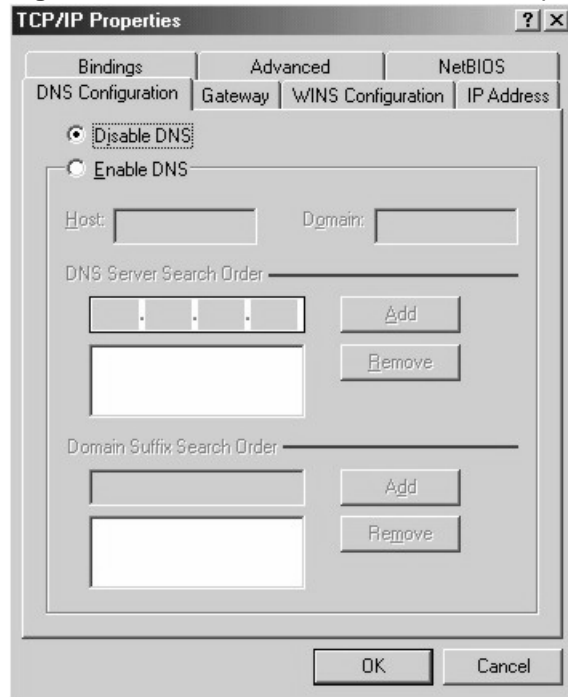
Configuring

- 1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**
- 2 Click the **IP Address** tab.
 - If your IP address is dynamic, select **Obtain an IP address automatically**.
 - If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

Figure 167 Windows 95/98/Me: TCP/IP Properties: IP Address



- 3 Click the **DNS Configuration** tab.
 - If you do not know your DNS information, select **Disable DNS**.
 - If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

Figure 168 Windows 95/98/Me: TCP/IP Properties: DNS Configuration**4** Click the **Gateway** tab.

- If you do not know your gateway's IP address, remove previously installed gateways.
- If you have a gateway IP address, type it in the **New gateway field** and click **Add**.

5 Click **OK** to save and close the **TCP/IP Properties** window.**6** Click **OK** to close the **Network** window. Insert the Windows CD if prompted.**7** Turn on your Prestige and restart your computer when prompted.

Verifying Settings

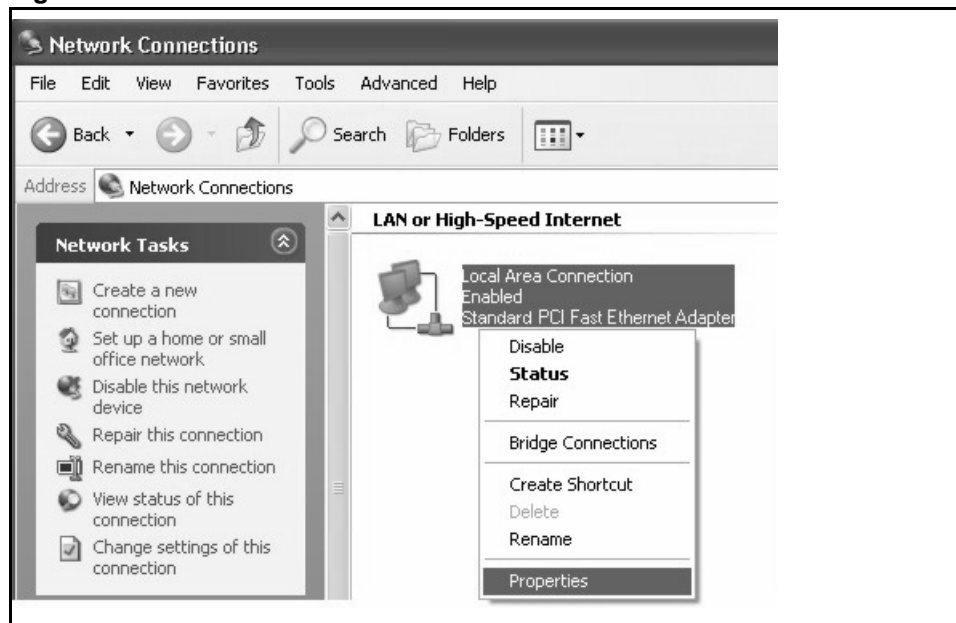
1 Click **Start** and then **Run**.**2** In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.**3** Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

1 For Windows XP, click **start, Control Panel**. In Windows 2000/NT, click **Start, Settings, Control Panel**.

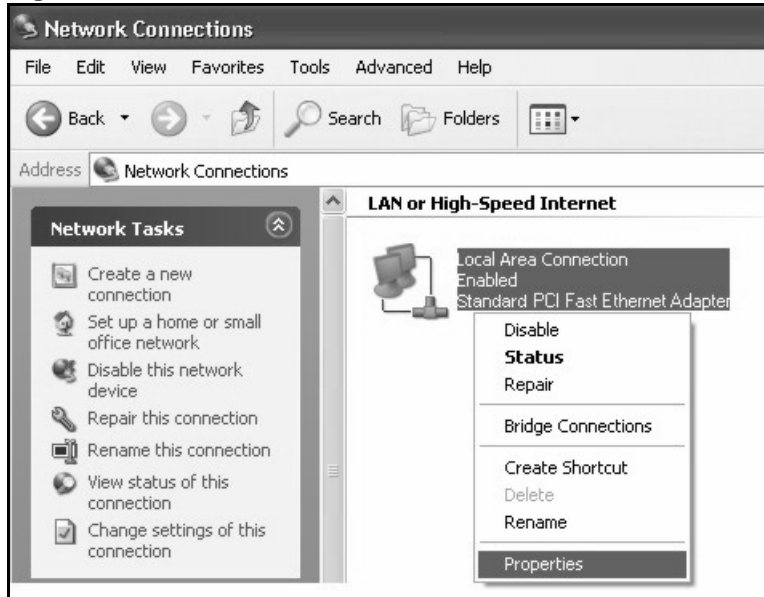
Figure 169 Windows XP: Start Menu

- 2 For Windows XP, click **Network Connections**. For Windows 2000/NT, click **Network and Dial-up Connections**.

Figure 170 Windows XP: Control Panel

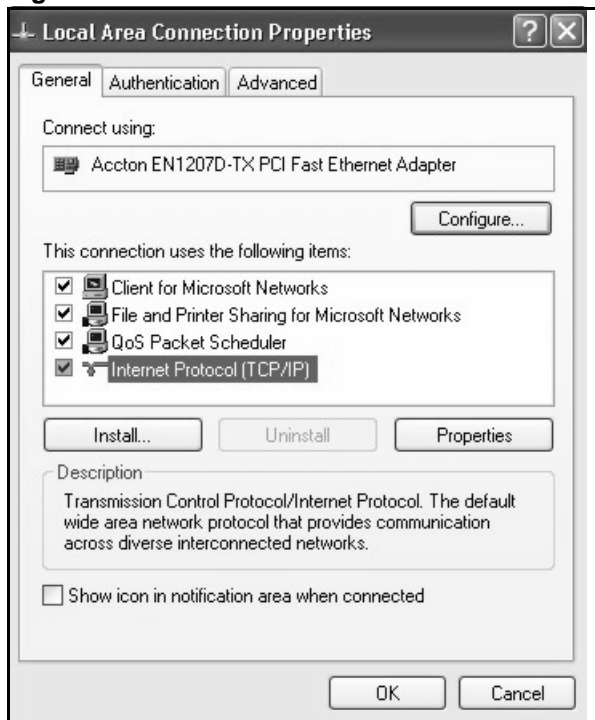
- 3 Right-click **Local Area Connection** and then click **Properties**.

Figure 171 Windows XP: Control Panel: Network Connections: Properties



4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and click **Properties**.

Figure 172 Windows XP: Local Area Connection Properties

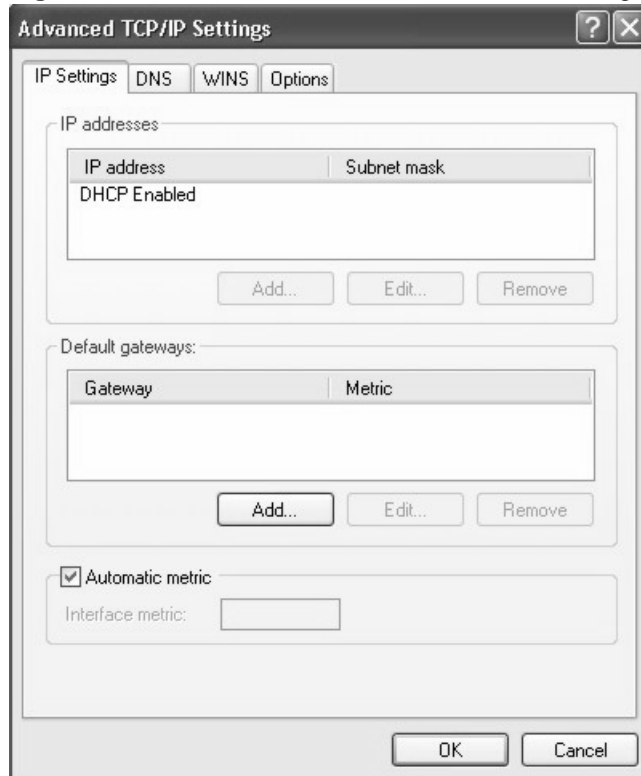


5 The **Internet Protocol TCP/IP Properties** window opens (the **General** tab in Windows XP).

- If you have a dynamic IP address click **Obtain an IP address automatically**.

- If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields. Click **Advanced**.

Figure 173 Windows XP: Advanced TCP/IP Settings



- 6** If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

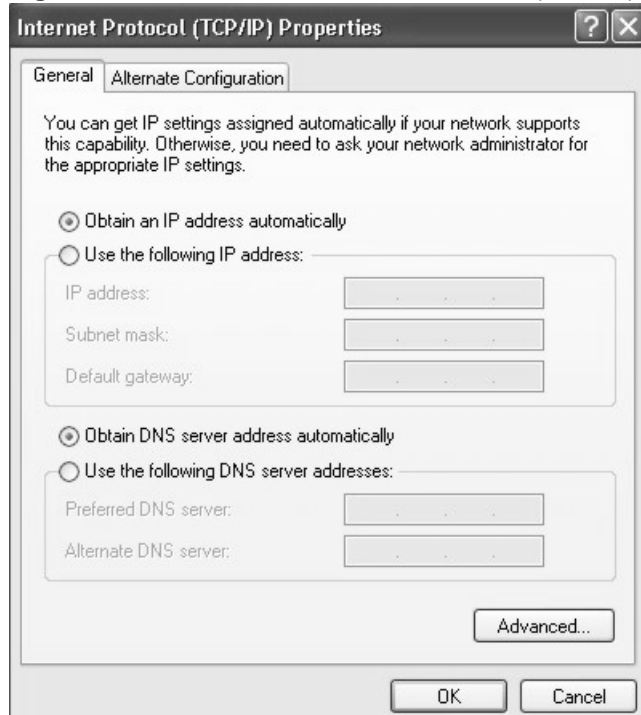
- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.
- Click **OK** when finished.

- 7** In the **Internet Protocol TCP/IP Properties** window (the **General tab** in Windows XP):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

Figure 174 Windows XP: Internet Protocol (TCP/IP) Properties



8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9 Click **OK** to close the **Local Area Connection Properties** window.

10 Turn on your Prestige and restart your computer (if prompted).

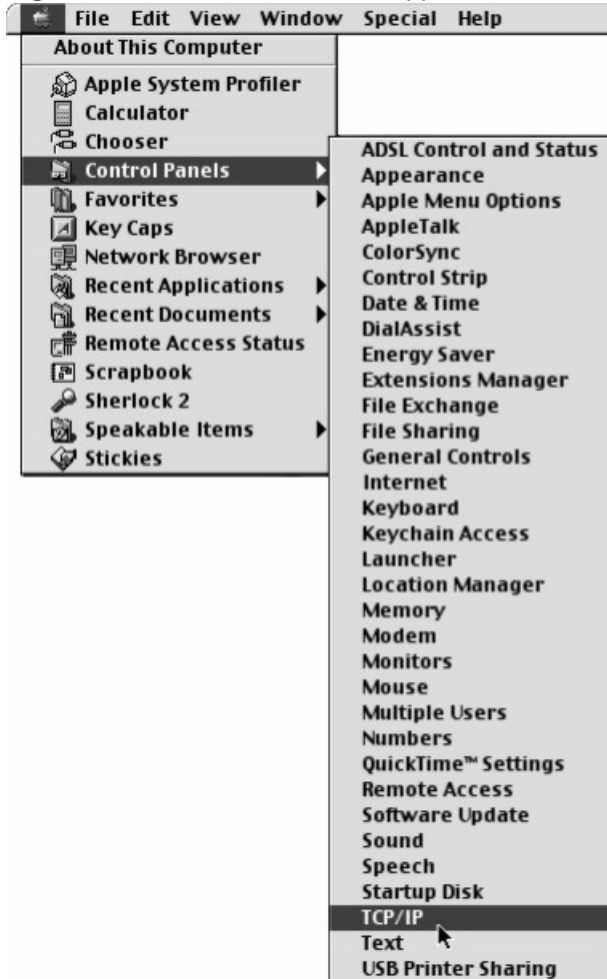
Verifying Settings

- 1** Click **Start, All Programs, Accessories** and then **Command Prompt**.
- 2** In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Macintosh OS 8/9

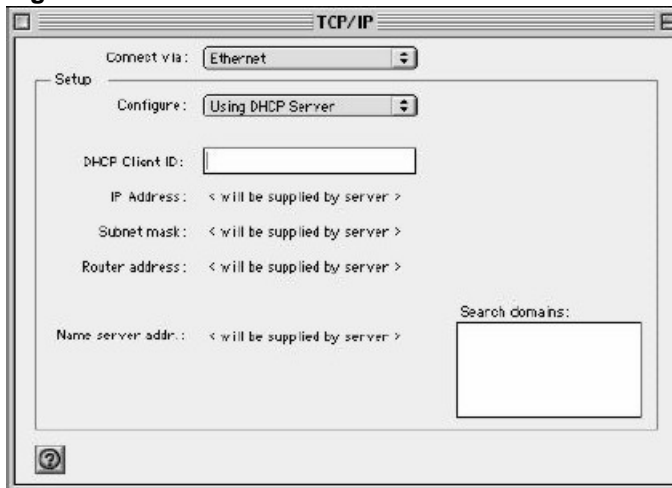
- 1** Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 175 Macintosh OS 8/9: Apple Menu



2 Select **Ethernet built-in** from the **Connect via** list.

Figure 176 Macintosh OS 8/9: TCP/IP



3 For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.

- 4 For statically assigned settings, do the following:
 - From the **Configure** box, select **Manually**.
 - Type your IP address in the **IP Address** box.
 - Type your subnet mask in the **Subnet mask** box.
 - Type the IP address of your Prestige in the **Router address** box.
- 5 Close the **TCP/IP Control Panel**.
- 6 Click **Save** if prompted, to save changes to your configuration.
- 7 Turn on your Prestige and restart your computer (if prompted).

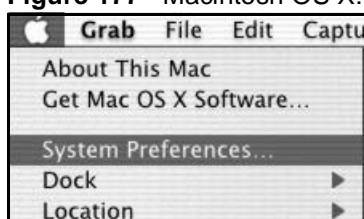
Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

Macintosh OS X

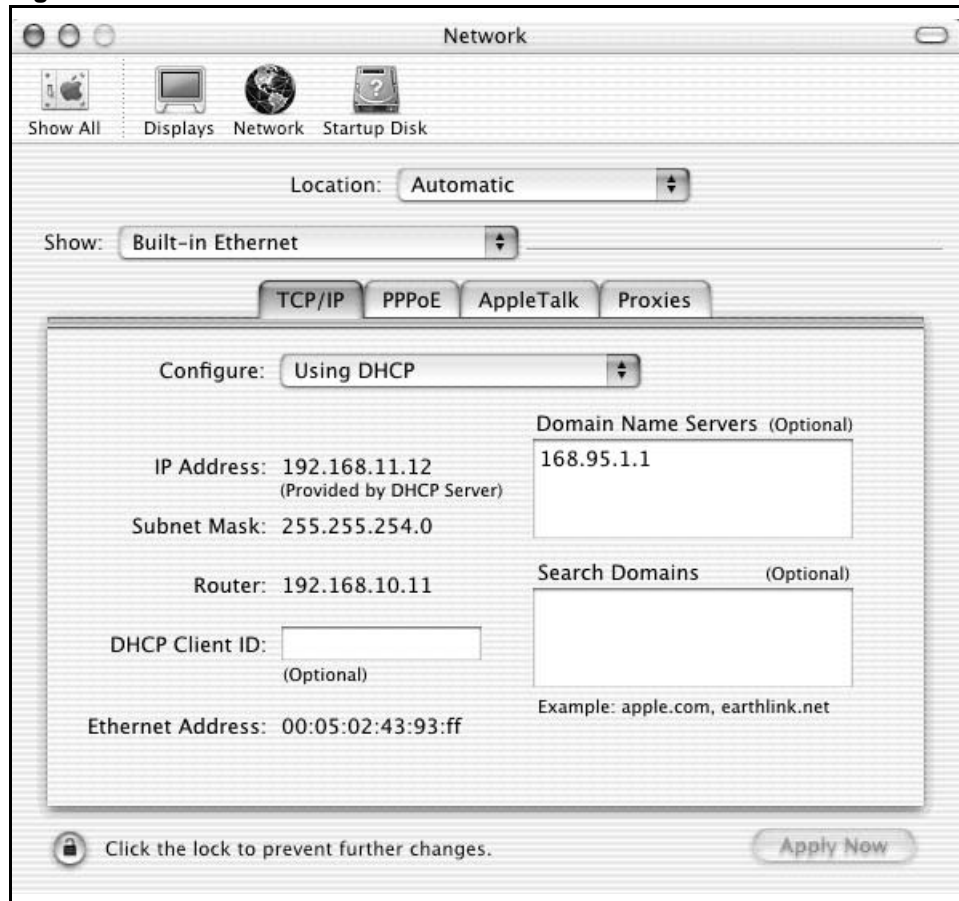
- 1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

Figure 177 Macintosh OS X: Apple Menu



- 2 Click **Network** in the icon bar.
 - Select **Automatic** from the **Location** list.
 - Select **Built-in Ethernet** from the **Show** list.
 - Click the **TCP/IP** tab.
- 3 For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

Figure 178 Macintosh OS X: Network



4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your Prestige in the **Router address** box.

5 Click **Apply Now** and close the window.

6 Turn on your Prestige and restart your computer (if prompted).

Verifying Settings

Check your TCP/IP properties in the **Network** window.

Appendix G

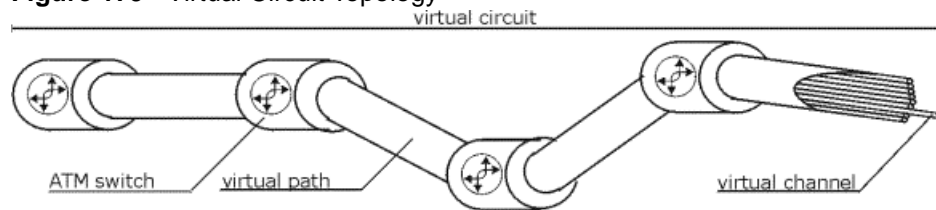
Virtual Circuit Topology

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 179 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 LAN and IEEE 802.11

A wireless LAN (WLAN) provides a flexible data communications system that you can use to access various services (navigating the Internet, E-mail, printer services, etc.) without the use of a cabled connection. In effect a wireless LAN environment provides you the freedom to stay connected to the network while roaming around in the coverage area.

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

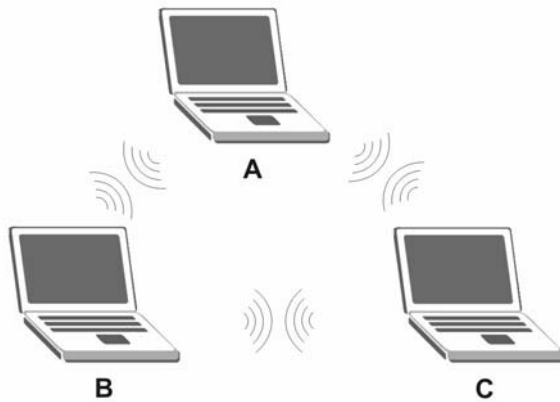
The 1997 completion of the IEEE 802.11 standard for wireless LANs (WLANs) was a first important step in the evolutionary development of wireless networking technologies. The standard was developed to maximize inter operability between differing brands of wireless LANs as well as to introduce a variety 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 180 Peer-to-Peer Communication in an Ad-hoc Network

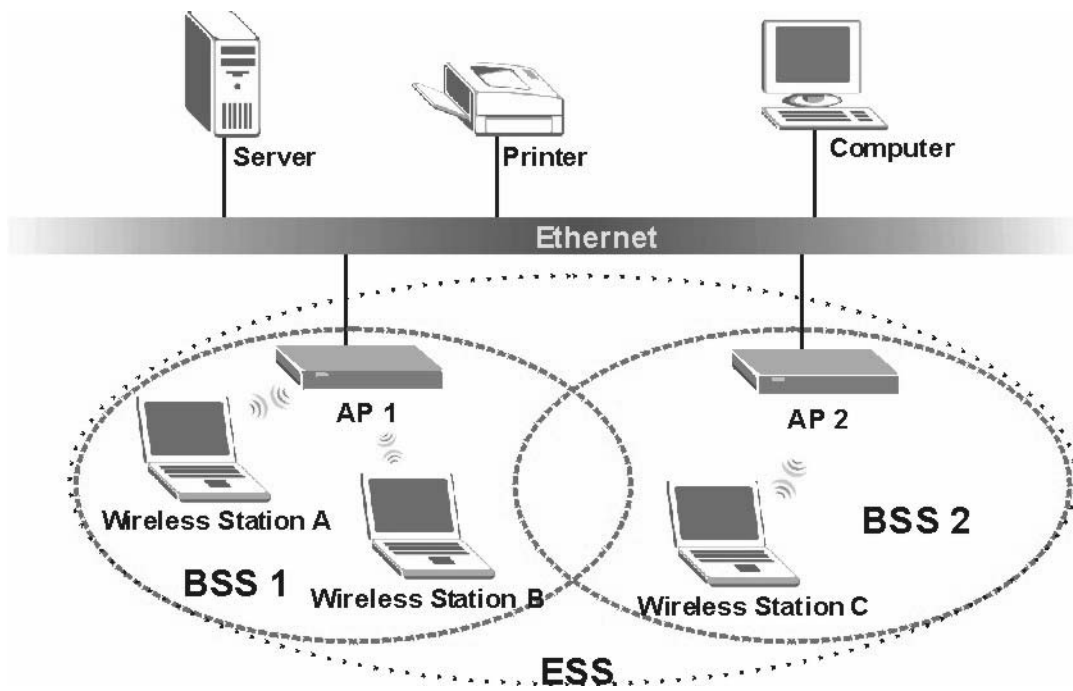


Infrastructure Wireless LAN Configuration

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 181 ESS Provides Campus-Wide Coverage



Appendix I

Wireless LAN With IEEE 802.1x

As wireless networks become popular for both portable computing and corporate networks, security is now a priority.

Security Flaws with IEEE 802.11

Wireless networks based on the original IEEE 802.11 have a poor reputation for safety. The IEEE 802.11b wireless access standard, first published in 1999, was based on the MAC address. As the MAC address is sent across the wireless link in clear text, it is easy to spoof and fake. Even the WEP (Wire Equivalent Privacy) data encryption is unreliable as it can be easily decrypted with current computer speed

Deployment Issues with IEEE 802.11

User account management has become a network administrator's nightmare in a corporate environment, as the IEEE 802.11b standard does not provide any central user account management. User access control is done through manual modification of the MAC address table on the access point. Although WEP data encryption offers a form of data security, you have to reset the WEP key on the clients each time you change your WEP key on the access point.

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.

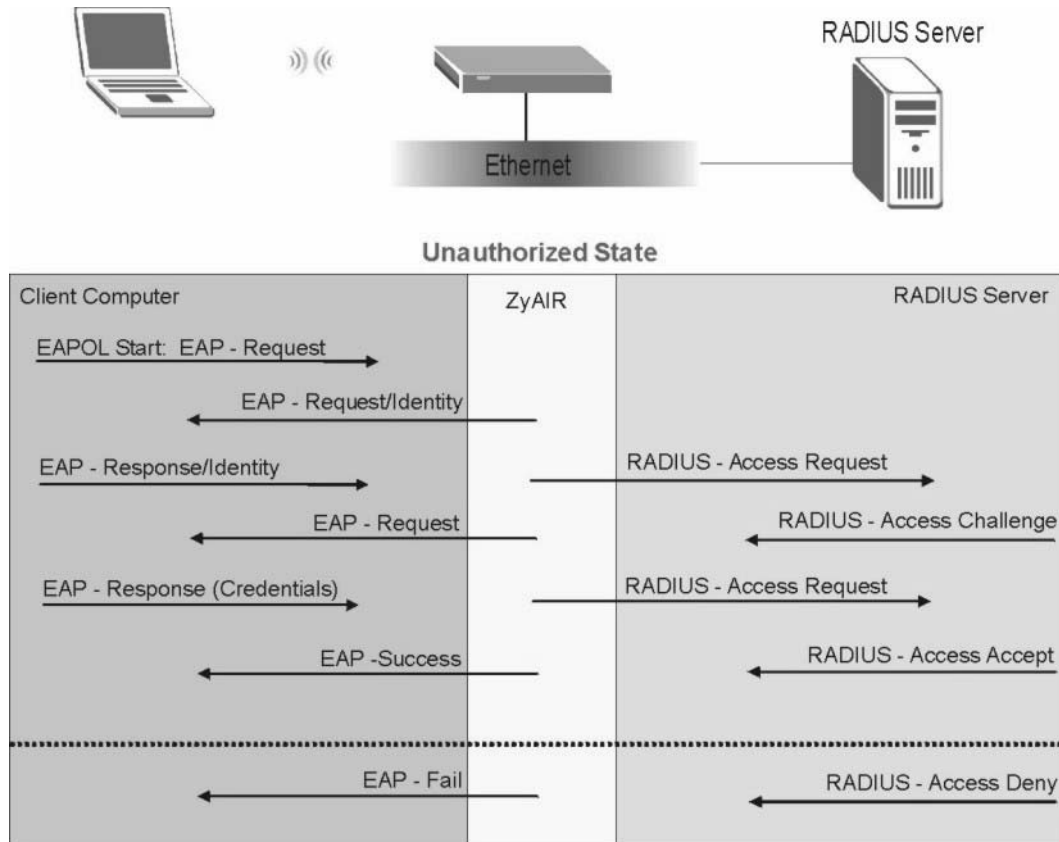
Advantages of the IEEE 802.1x

- 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 clients.

RADIUS Server Authentication Sequence

The following figure depicts a typical wireless network with a remote RADIUS server for user authentication using EAPOL (EAP Over LAN).

Figure 182 Sequences for EAP MD5–Challenge Authentication



Appendix J

Types of EAP Authentication

Introduction

This appendix discusses three popular EAP authentication types: **EAP-MD5**, **EAP-TLS** and **EAP-TTLS**. 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 IEEE802.1x.

Table 131 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

Appendix K

Log Descriptions

Introduction

This appendix provides descriptions of example device log messages.

Table 132 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.
Too large ICMP packet has been dropped	The router dropped an ICMP packet that was too large.

Table 132 System Maintenance Logs (continued)

LOG MESSAGE	DESCRIPTION
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 133 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 134 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 134 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 135 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): 60 UDP idle timeout (s): 60 TCP connection (three way handshaking) timeout (s): 30 TCP FIN-wait timeout (s): 60 TCP 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 CLI command: "sys firewall tcprst").

Table 136 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 137 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 149.
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 149.
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 138 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 139 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 139 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 140 UPnP Logs

LOG MESSAGE	DESCRIPTION
UPnP pass through Firewall	UPnP packets can pass through the firewall.

Table 141 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 141 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 142 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 149.
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 149.
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 149.
icmp echo : ICMP (type:%d, code:%d)	The firewall detected an ICMP echo attack. For type and code details, see Table 149.
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 149.
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 149.
traceroute ICMP (type:%d, code:%d)	The firewall detected an ICMP traceroute attack. For type and code details, see Table 149.

Table 143 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" CLI 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 144 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 144 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 144 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 1 verification 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 144 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 145 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 145 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 146 for the corresponding descriptions of the codes.

Table 146 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 146 Certificate Path Verification Failure Reason Codes (continued)

CODE	DESCRIPTION
26	Database method failed.
27	Path was not verified.
28	Maximum path length reached.

Table 147 802.1X 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 method.	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 148 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 149 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 149 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 150 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 151 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 151 RFC-2408 ISAKMP Payload Types (continued)

LOG DISPLAY	PAYLOAD TYPE
SIG	Signature
NONCE	Nonce
NOTFY	Notification
DEL	Delete
VID	Vendor ID

Appendix L

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 MERCHANTABILITY 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

Copyright (c) 1995, 1996, 1997, 1998, 1999, 2000 The Cryptix Foundation Limited. All rights reserved.

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 utilize 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.

The Java Software technologies are Copyright (c) 1994-2000 Sun Microsystems, Inc. All rights reserved.

Sun hereby grants Doug Lea a non-exclusive, worldwide, non-transferrable license to use, reproduce, create derivative works of, and distribute the Java Software and derivative works thereof in source and binary forms as part of a larger work, and to sublicense the right to use, reproduce and distribute the Java Software and Doug Lea's derivative works as the part of larger works through multiple tiers of sublicensees provided that the following conditions are met:

-Neither the name of or trademarks of Sun may be used to endorse or promote products including or derived from the Java Software technology without specific prior written permission; and

-Redistributions of source or binary code must contain the above copyright notice, this notice and the following disclaimers:

THIS SOFTWARE IS PROVIDED "AS IS," WITHOUT A WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE HEREBY EXCLUDED. SUN MICROSYSTEMS, INC. AND ITS LICENSORS SHALL NOT BE LIABLE FOR ANY DAMAGES SUFFERED BY LICENSEE AS A RESULT OF USING, MODIFYING OR

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

Copyright 1994-2000 Sun Microsystems, Inc. All right reserved

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 component(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 the "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 Java™ 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., 4150 Network 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.

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 above 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.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment: "This product includes software developed by Gargoyle Software Inc. (<http://www.GargoyleSoftware.com/>)"

Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.

4. The name "Gargoyle Software" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact info@GargoyleSoftware.com.
5. Products derived from this software may not be called "HtmlUnit", nor may "HtmlUnit" appear in their name, without prior written permission of Gargoyle Software Inc.

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 GARGOYLE SOFTWARE 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 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

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. [This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

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 SUCH DAMAGES.

END OF TERMS AND CONDITIONS

This Product includes MySQL database under GPL.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

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 UNINTERRUPTED 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.

Index

A

Access Point **85**
Aggressive **159**
Alarms **240**
Alternative Subnet Mask Notation **272**
Application-level Firewalls **166**
Attack Types **169**
Authentication Algorithm **160, 161**

B

Basic Service Set **293**
Blocking Time **181**
Brute-force Attack, **169**
BSS **293**
Bypass Triangle Route **178**

C

CA **298**
Cable Modem **167**
Certificate Authority **298**
Channel ID **85**
Configuration **70**
Copyright **2**
Cryptography Model **63**
Custom Ports
 Creating/Editing **184**
Customer Support **4**

D

Default Policy Log **178**
DeMilitarized Zone **96**
Denial of Service **167, 168**
Destination Address **176, 182**
DHCP **64, 70, 71, 73, 76**
Diffie-Hellman (DH) **160**
Direct Sequence Spread Spectrum **292**
Distribution System **293**
DMZ **96**
 And the Firewall **96**
Domain Name **64**
DoS
 Basics **168**
 Types **168**
DS **293**
DSSS **292**
DTR **112**

E

EAP Authentication **298**
Enable Wireless LAN **85**
Encapsulation **161**
 encrymode **63**
Encryption Algorithm **160, 161**
EnterSee Syntax Conventions **29**
ESS **293**
ESS ID **82**
Extended Service Set **293**
Extended Service Set IDentification **85**

F

Factory LAN Defaults **70**
FHSS **292**
Firewall
 Address Type **183**
 Alerts **176**
 Introduction **167**
 Policies **173**
 Types **166**
Fragmentation Threshold **84**
Frequency-Hopping Spread Spectrum **292**
FTP **70, 133**

H

Host IDs **270**
HTTP **166, 168**

I

IBSS **293**
ICMP echo **169**
IGMP **71, 72**
Independent Basic Service Set **293**
Inside Local Address **130**
Internet Control Message Protocol (ICMP) **169**
IP Address **71, 74, 77, 134**
IP Pool **73, 76**
IP Pool Setup **70**
IP Spoofing **170**
IPSec Management
 1-Click VPN **247**

K

Key Fields For Configuring Rules **176**
Key Group **160**

L

LAN TCP/IP **70**
LAND **169**

M

MAC (Hex **63**)
MAC Address Filter Action **87**
MAC Address Filtering **86**
MAC service data unit **86**
Main **159**
Many to Many No OverloadSee NAT **131**
Many to Many OverloadSee NAT **131**
Many to OneSee NAT **131**
Map **250**
Maximum Burst Size **117**
Maximum Incomplete High **180**
Maximum Incomplete Low **180**
Max-incomplete Low **180**
MD5 **160, 161**
Metric **100, 146**
MSDU **86**
Multicast **71, 75, 77**

N

Name **157**
NAT **133, 134**
 Definitions **130**
 How NAT Works **131**
 Mapping Types **131**
 What NAT does **131**
NetBIOS commands **170**
Network Management **177**

O

One Minute High **180**
One Minute Low **180**
One to OneSee NAT **131**
One-Click VPN **247**

P

Packet Filtering Firewalls **166**
Peak Cell Rate **117**
Perfect Forward Secrecy (PFS **161**)
Ping of Death **168**
Point-to-Point Tunneling Protocol **177**
Point-to-Point Tunneling ProtocolSee PPTP **105**
POP3 **168**
Port Configuration **184**
Port Number **176**
Port Numbers **176**
Public Servers **96**

R

RADIUS **91**
 Shared Secret Key **92**
RADIUS Message Types **92**
Read Me First **28**
Related Documentation **28**
RF signals **292**
RIP **71**
RTS Threshold **83**
RTS/CTS handshake **86**
Rules
 Checklist **175**
 Key Fields **176**

S

SA Life Time **160, 161**
Saving the State **170**
Secret Key **64**
Security Ramifications **175**
SelectSee Syntax Conventions **29**
Server **66, 132**
Service **176**
Service Set **85**
Service Type **184**
Services **134, 176**
SHA-1 (Secure Hash Algorithm) **160, 161**
Smurf **169**
Source Address **176, 182**
Stateful Inspection **166, 167, 170**
SUA **133**
Subnet Mask **71, 74, 77, 183**
Subnet Masks **271**
Supporting Disk **28**
Sustained Cell Rate **117**
SYN Flood **169**
SYN-ACK **169**
Syntax Conventions **29**

T

TCP Maximum Incomplete **181**
TCP Security **172**
TCP/IP **74, 76, 168, 169**
Teardrop **168**
Traceroute **170**
Traffic Redirect **109, 122**
Traffic Shapping **117**
Transport mode **161**
Tunnel Graphical Depictions **249**
Tunnel mode **161**

U

UDP/ICMP Security **173**

Upper Layer Protocols **172, 173**

User Name **65**

User Profiles **90**

V

VPN **105**

W

WAN Backup **122**

Web Configurator **167, 173, 175**

WEP Encryption **86**

Wireless LAN **292**

WLAN **292**

Z

ZyXEL's Firewall

Introduction **167**