P-320W

802.11g Wireless Firewall Router

User's Guide

Version 1.00
11/2005
Edition 1

Copyright

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.

Federal Communications Commission (FCC) Interference Statement

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

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

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

If this equipment does cause harmful interference to radio/television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Caution

1. To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.
2. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Notice 1

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

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

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

Certifications

1 Go to www.zyxel.com

2 Select your product from the drop-down list box on the ZyXEL home page to go to that product's page.

3 Select the certification you wish to view from this page.

Safety Warnings

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

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

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind of character to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Customer Support

Please have the following information ready when you contact customer support.

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

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

METHOD	SUPPORT E-MAIL	TELEPHONE[A]	WEB SITE	REGULAR MAIL
LOCATION	SALES E-MAIL	FAX	FTP SITE	
POLAND	info@pl.zyxel.com	+48-22-5286603	www.pl.zyxel.com	ZyXEL Communications ul.Emilli Plater 53 00-113 Warszawa Poland
		+48-22-5206701		
RUSSIA	http://zyxel.ru/support	+7-095-542-89-29	www.zyxel.ru	ZyXEL Russia Ostrovityanova 37a Str. Moscow, 117279 Russia
	sales@zyxel.ru	+7-095-542-89-25		
SPAIN	support@zyxel.es	+34-902-195-420	www.zyxel.es	ZyXEL Communications Alejandro Villegas 33 1º, 28043 Madrid Spain
	sales@zyxel.es	+34-913-005-345		
SWEDEN	support@zyxel.se	+46-31-744-7700	www.zyxel.se	ZyXEL Communications A/S Sjöporten 4, 41764 Göteborg Sweden
	sales@zyxel.se	+46-31-744-7701		
UKRAINE	support@ua.zyxel.com	+380-44-247-69-78	www.ua.zyxel.com	ZyXEL Ukraine 13, Pimonenko Str. Kiev, 04050 Ukraine
	sales@ua.zyxel.com	+380-44-494-49-32		
UNITED KINGDOM	support@zyxel.co.uk	+44-1344 303044 08707 555779 (UK only)	www.zyxel.co.uk	ZyXEL Communications UK Ltd.,11 The Courtyard, Eastern Road, Bracknell, Berkshire, RG12 2XB, United Kingdom (UK)
	sales@zyxel.co.uk	+44-1344 303034	ftp.zyxel.co.uk	

[A] “+” is the (prefix) number you enter to make an international telephone call.

Table of Contents

Copyright 3

Federal Communications Commission (FCC) Interference Statement 4

Safety Warnings 6

ZyXEL Limited Warranty 7

Customer Support 8

Table of Contents 11

Preface 25

**Chapter 1
Getting to Know Your Prestige 27**

1.1 Prestige Overview 27
1.2 Prestige Features 27
1.2.1 Physical Features 27
1.2.2 Non-Physical Features 28
1.2.3 Wireless Features 30
1.3 Applications for the Prestige 31
1.3.1 Secure Broadband Internet Access via Cable or DSL Modem 31
1.3.2 Wireless LAN Application 32
1.3.3 Front Panel LEDs 32

**Chapter 2
Introducing the Web Configurator 35**

2.1 Web Configurator Overview 35
2.2 Accessing the Prestige Web Configurator 35
2.3 Resetting the Prestige 37
2.3.1 Procedure To Use The Reset Button 37
2.4 Navigating the Prestige Web Configurator 37
2.4.1 Navigation Panel 39
2.4.2 Summary: DHCP Table 41
2.4.3 Summary: Association List 42
2.4.4 Summary: Packet Statistics 42

**Chapter 3
Connection Wizard 45**

3.1 Wizard Setup 45

3.2 Connection Wizard: STEP 1: System Information 46
3.2.1 System Name 46
3.2.2 Domain Name 46
3.3 Connection Wizard: STEP 2: Wireless LAN 47
3.3.1 Basic(WEP) Security 49
3.3.2 Extend(WPA-PSK) Security..50
3.3.3 OTIST 51
3.4 Connection Wizard: STEP 3: Internet Configuration 52
3.4.1 Ethernet Connection Type 53
3.4.2 PPPoE Connection Type 53
3.4.3 PPTP Connection Type 55
3.4.4 Your IP Address..56
3.4.5 WAN MAC Address 57
3.4.6 Connection Wizard Complete..58

Chapter 4
Wireless LAN 61

4.1 Introduction 61
4.2 Wireless Security Overview 61
4.2.1 Encryption 61
4.2.2 Authentication 61
4.2.3 Restricted Access 62
4.2.4 Hide Prestige Identity 62
4.2.5 Using OTIST 62
4.3 Configuring Wireless LAN on the Prestige 62
4.4 General Wireless LAN Screen 63
4.4.1 No Security 64
4.4.2 WEP Encryption 65
4.4.3 Introduction to WPA 67
4.4.4 WPA-PSK Application Example 67
4.4.5 WPA-PSK Authentication Screen 68
4.4.6 WPA with RADIUS Application Example 69
4.4.7 Wireless Client WPA Supplicants 69
4.4.8 WPA Authentication Screen 69
4.4.9 IEEE 802.1x Overview 70
4.4.10 IEEE 802.1x and Dynamic WEP Key Exchange Screen 71
4.5 OTIST 72
4.5.1 Enabling OTIST 72
4.5.1.1 AP 72
4.5.1.2 Wireless Client 74
4.5.2 Starting OTIST 75
4.5.3 Notes on OTIST 75
4.6 MAC Filter 76

4.7 Wireless LAN Advanced Screen 78

Chapter 5
WAN 81

5.1 WAN IP Address Assignment 81
5.2 IP Address and Subnet Mask 81
5.3 DNS Server Address Assignment 82
5.4 TCP/IP Priority (Metric) 82
5.5 WAN MAC Address 83
5.6 Internet Connection 83
5.6.1 Ethernet Encapsulation 83
5.6.2 PPPoE Encapsulation 85
5.6.3 PPTP Encapsulation 87
5.7 Advanced WAN Screen 89
5.8 Traffic Redirect 90
5.9 Traffic Redirect Screen 90

Chapter 6
LAN 93

6.1 LAN Overview 93
6.1.1 IP Pool Setup 93
6.1.2 System DNS Servers 93
6.2 LAN TCP/IP 93
6.2.1 Factory LAN Defaults 93
6.2.2 IP Address and Subnet Mask 94
6.3 IP Screen 94

Chapter 7
DHCP Server 95

7.1 DHCP 95
7.2 DHCP Screen 95
7.3 Static DHCP Screen 96
7.4 Client List Screen 97

Chapter 8
Network Address Translation (NAT) 99

8.1 NAT Overview 99
8.1.1 NAT Definitions 99
8.1.2 What NAT Does 100
8.1.3 How NAT Works 100
8.1.4 NAT Application 101
8.1.5 Default Server IP Address 101
8.1.6 Port Forwarding: Services and Port Numbers 102

8.1.7 Configuring Servers Behind SUA (Example) 103
8.2 General NAT Screen 103
8.3 Port Forwarding Screen 104
8.3.1 Rule Setup Screen..105
8.4 Trigger Port Forwarding 106
8.4.1 Trigger Port Forwarding Example 106
8.4.2 Two Points To Remember About Trigger Ports 107
8.5 Trigger Port Forwarding Screen 107

Chapter 9
Firewall..109

9.1 Introduction to Firewall 109
9.1.1 What is a Firewall? 109
9.1.2 Stateful Inspection Firewall. 109
9.1.3 About the Prestige Firewall 109
9.1.4 Guidelines For Enhancing Security With Your Firewall 110
9.2 General Firewall Screen 110
9.3 Services Screen 111
9.3.1 Services 113

Chapter 10
Static Route Screens 115

10.1 Static Route Overview 115
10.2 IP Static Route Screen 115
10.2.1 Static Route Setup Screen..116

Chapter 11
Remote Management Screens..119

11.1 Remote Management Overview 119
11.1.1 Remote Management Limitations 119
11.1.2 Remote Management and NAT 119
11.1.3 System Timeout 120
11.2 WWW Screen 120
11.3 SNMP 121
11.3.1 Supported MIBs 122
11.3.2 SNMP Traps 122
11.4 SNMP Screen 122
11.5 Security Screen 123

Chapter 12
UPnP..125

12.1 Universal Plug and Play Overview 125
12.1.1 How Do I Know If I'm Using UPnP? 125

12.1.2 NAT Traversal 125
12.1.3 Cautions with UPnP 125
12.2 UPnP and ZyXEL 126
12.3 UPnP Screen 126
12.4 Installing UPnP in Windows Example 127
12.4.1 Installing UPnP in Windows Me 127
12.4.2 Installing UPnP in Windows XP 128
12.5 Using UPnP in Windows XP Example 129
12.5.1 Auto-discover Your UPnP-enabled Network Device 130
12.5.2 Web Configurator Easy Access 133

Chapter 13
System 135

13.1 System Overview 135
13.2 General Screen 135
13.3 Dynamic DNS 136
13.3.1 DynDNS Wildcard 136
13.4 Dynamic DNS Screen 137
13.5 Time Setting Screen 137

Chapter 14
Logs.......... 141

14.1 View Log 141
14.2 Log Settings 142

Chapter 15
Tools 145

15.1 Firmware Upload Screen 145
15.2 Configuration Screen 146
15.2.1 Backup Configuration 147
15.2.2 Restore Configuration 147
15.2.3 Back to Factory Defaults 148
15.3 Restart Screen 148

Chapter 16
Troubleshooting 151

16.1 Problems Starting Up the Prestige 151
16.2 Problems with the LAN 151
16.3 Problems with the WAN 152
16.4 Problems with the Password 152
16.5 Problems with Remote Management 153
16.6 Problems Accessing the Prestige 153
16.6.1 Pop-up Windows, JavaScripts and Java Permissions 154

16.6.1.1 Internet Explorer Pop-up Blockers 154
16.6.1.2 JavaScripts 157
16.6.1.3 Java Permissions 159
16.6.2 ActiveX Controls in Internet Explorer 161

Appendix A
Product Specifications 163

Appendix B
IP Subnetting 165

Appendix C
Setting up Your Computer's IP Address.. 173

Appendix D
PPPoE 189

Appendix E
PPTP... 191

Appendix F
Wireless LANs... 195

Appendix G
Antenna Selection and Positioning Recommendation..................................... 209

List of Figures

Figure 1 Secure Internet Access via Cable, DSL or Wireless Modem 31
Figure 2 Internet Access Application Example 32
Figure 3 Front Panel 32
Figure 4 Login 36
Figure 5 Language Selection 36
Figure 6 Change Password Screen 36
Figure 7 Select the Mode 37
Figure 8 Web Configurator Status Screen 38
Figure 9 Summary: DHCP Table 41
Figure 10 Summary: Association List 42
Figure 11 Summary: Packet Statistics 43
Figure 12 Select a Mode 45
Figure 13 Welcome to the Connection Wizard 46
Figure 14 Connection Wizard: STEP 1: System Information 47
Figure 15 Connection Wizard: STEP 2: Wireless LAN 48
Figure 16 Basic(WEP) Security 49
Figure 17 Extend(WPA-PSK) Security 50
Figure 18 OTIST 51
Figure 19 Connection Wizard: STEP 3: WAN Connection Type. 52
Figure 20 Ethernet Connection Type 53
Figure 21 PPPoE Connection Type 54
Figure 22 PPTP Connection Type 55
Figure 23 Your IP Address 56
Figure 24 WAN MAC Address 58
Figure 25 Connection Wizard Complete 59
Figure 26 Connection Wizard: Congratulation 59
Figure 27 Wireless: General 63
Figure 28 Wireless: No Security 65
Figure 29 Wireless: Static WEP Encryption 66
Figure 30 WPA-PSK Authentication 68
Figure 31 Wireless: WPA-PSK 68
Figure 32 WPA with RADIUS Application Example 69
Figure 33 Wireless: WPA 70
Figure 34 Wireless: 802.1x and Dynamic WEP 71
Figure 35 Wireless: OTIST 73
Figure 36 Example Wireless Client OTIST Screen 74

Figure 37 Security Key 75
Figure 38 OTIST in Progress (AP) 75
Figure 39 OTIST in Progress (Client) 75
Figure 40 No AP with OTIST Found 75
Figure 41 Start OTIST? 76
Figure 42 Wireless: MAC Address Filter 77
Figure 43 Wireless: Advanced 78
Figure 44 WAN: Ethernet Encapsulation 84
Figure 45 WAN: PPPoE Encapsulation 86
Figure 46 PPTP Encapsulation 88
Figure 47 Advanced 90
Figure 48 Traffic Redirect WAN Setup 90
Figure 49 WAN: Traffic Redirect 91
Figure 50 LAN IP 94
Figure 51 General 95
Figure 52 Static DHCP 97
Figure 53 Client List 98
Figure 54 How NAT Works 101
Figure 55 NAT Application With IP Alias 101
Figure 56 Multiple Servers Behind NAT Example 103
Figure 57 NAT: General 103
Figure 58 Port Forwarding 104
Figure 59 NAT: Port Forwarding: Rule Setup 105
Figure 60 Trigger Port Forwarding Process: Example 107
Figure 61 NAT: Trigger Port 108
Figure 62 Firewall: General 110
Figure 63 Firewall: Services 111
Figure 64 Example of Static Routing Topology 115
Figure 65 IP Static Route 116
Figure 66 Static Route Setup 117
Figure 67 WWW Remote Management 120
Figure 68 SNMP Management Model 121
Figure 69 SNMP Remote Management 123
Figure 70 Security Remote Management 124
Figure 71 Configuring UPnP 126
Figure 72 Add/Remove Programs: Windows Setup: Communication 127
Figure 73 Add/Remove Programs: Windows Setup: Communication: Components 128
Figure 74 Network Connections 128
Figure 75 Windows Optional Networking Components Wizard 129
Figure 76 Networking Services 129
Figure 77 Network Connections 130
Figure 78 Internet Connection Properties 131
Figure 79 Internet Connection Properties: Advanced Settings 131

Figure 80 Internet Connection Properties: Advanced Settings: Add 132
Figure 81 System Tray Icon 132
Figure 82 Internet Connection Status 132
Figure 83 Network Connections 133
Figure 84 Network Connections: My Network Places 134
Figure 85 Network Connections: My Network Places: Properties: Example 134
Figure 86 System General 135
Figure 87 Dynamic DNS 137
Figure 88 Time Setting 138
Figure 89 View Log 141
Figure 90 Log Settings 143
Figure 91 Maintenance Firmware Upload 145
Figure 92 Upload Warning 146
Figure 93 Network Temporarily Disconnected 146
Figure 94 Upload Error Message 146
Figure 95 Configuration 147
Figure 96 Configuration Restore Successful 148
Figure 97 Temporarily Disconnected 148
Figure 98 Configuration Restore Error 148
Figure 99 System Restart 149
Figure 100 Pop-up Blocker 154
Figure 101 Internet Options 155
Figure 102 Internet Options 156
Figure 103 Pop-up Blocker Settings 157
Figure 104 Internet Options 158
Figure 105 Security Settings - Java Scripting 159
Figure 106 Security Settings - Java 160
Figure 107 Java (Sun) 160
Figure 108 Internet Options Security 161
Figure 109 Security Setting ActiveX Controls 162
Figure 110 WIndows 95/98/Me: Network: Configuration 174
Figure 111 Windows 95/98/Me: TCP/IP Properties: IP Address 175
Figure 112 Windows 95/98/Me: TCP/IP Properties: DNS Configuration 176
Figure 113 Windows XP: Start Menu 177
Figure 114 Windows XP: Control Panel 177
Figure 115 Windows XP: Control Panel: Network Connections: Properties 178
Figure 116 Windows XP: Local Area Connection Properties 178
Figure 117 Windows XP: Internet Protocol (TCP/IP) Properties 179
Figure 118 Windows XP: Advanced TCP/IP Properties 180
Figure 119 Windows XP: Internet Protocol (TCP/IP) Properties 181
Figure 120 Macintosh OS 8/9: Apple Menu 182
Figure 121 Macintosh OS 8/9: TCP/IP 182
Figure 122 Macintosh OS X: Apple Menu 183

Figure 123 Macintosh OS X: Network 184
Figure 124 Red Hat 9.0: KDE: Network Configuration: Devices 185
Figure 125 Red Hat 9.0: KDE: Ethernet Device: General 185
Figure 126 Red Hat 9.0: KDE: Network Configuration: DNS 186
Figure 127 Red Hat 9.0: KDE: Network Configuration: Activate 186
Figure 128 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0 187
Figure 129 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0 187
Figure 130 Red Hat 9.0: DNS Settings in resolv.conf 187
Figure 131 Red Hat 9.0: Restart Ethernet Card 188
Figure 132 Red Hat 9.0: Checking TCP/IP Properties 188
Figure 133 Single-Computer per Router Hardware Configuration 190
Figure 134 ZyWALL as a PPPoE Client 190
Figure 135 Transport PPP frames over Ethernet 191
Figure 136 PPTP Protocol Overview 192
Figure 137 Example Message Exchange between Computer and an ANT 193
Figure 138 Peer-to-Peer Communication in an Ad-hoc Network 195
Figure 139 Basic Service Set 196
Figure 140 Infrastructure WLAN 197
Figure 141 RTS/CTS 198
Figure 142 EAP Authentication 201
Figure 143 WEP Authentication Steps 204
Figure 144 Roaming Example 207

List of Tables

Table 1 Front Panel LEDs 32
Table 2 Status Screen Icon Key 38
Table 3 Web Configurator Status Screen 38
Table 4 Screens Summary 39
Table 5 Summary: DHCP Table 41
Table 6 Summary: Wireless Association List 42
Table 7 Summary: Packet Statistics 43
Table 8 Connection Wizard: STEP 1: System Information 47
Table 9 Connection Wizard: STEP 2: Wireless LAN 48
Table 10 Basic(WEP) Security 49
Table 11 Extend(WPA-PSK) Security 51
Table 12 OTIST 52
Table 13 Connection Wizard: STEP 3: WAN Connection Type 53
Table 14 PPPoE Connection Type 54
Table 15 PPTP Connection Type 55
Table 16 Your IP Address 57
Table 17 Example of Network Properties for LAN Servers with Fixed IP Addresses 57
Table 18 WAN MAC Address 58
Table 19 ZyAIR Wireless Security Levels 63
Table 20 Wireless: General 64
Table 21 Wireless No Security 65
Table 22 Wireless: Static WEP Encryption 66
Table 23 Wireless: WPA-PSK 68
Table 24 Wireless: WPA 70
Table 25 Wireless: 802.1x and Dynamic WEP 71
Table 26 Wireless: OTIST 73
Table 27 MAC Address Filter 77
Table 28 Wireless: Advanced 78
Table 29 Private IP Address Ranges 81
Table 30 Example of Network Properties for LAN Servers with Fixed IP Addresses 83
Table 31 WAN: Ethernet Encapsulation 84
Table 32 WAN: PPPoE Encapsulation 86
Table 33 PPTP Encapsulation 88
Table 34 Advanced 90
Table 35 Traffic Redirect 91
Table 36 LAN IP 94

Table 37 General 96
Table 38 Static DHCP 97
Table 39 Client List 98
Table 40 NAT Definitions 100
Table 41 Services and Port Numbers 102
Table 42 NAT: General 103
Table 43 NAT: Port Forwarding 105
Table 44 NAT: Port Forwarding: Rule Setup 106
Table 45 NAT: Trigger Port 108
Table 46 Firewall: General 111
Table 47 Firewall: Services 112
Table 48 Commonly Used Services 113
Table 49 IP Static Route 116
Table 50 Static Route Setup 117
Table 51 WWW Remote Management 120
Table 52 SNMP Traps 122
Table 53 SNMP Remote Management 123
Table 54 Security Remote Management 124
Table 55 Configuring UPnP 126
Table 56 System General 136
Table 57 Dynamic DNS 137
Table 58 Time Setting 138
Table 59 View Log 142
Table 60 Log Settings 143
Table 61 Maintenance Firmware Upload 145
Table 62 Maintenance: Restore Configuration 147
Table 63 Troubleshooting Starting Up Your Prestige 151
Table 64 Troubleshooting the LAN 151
Table 65 Troubleshooting the WAN 152
Table 66 Troubleshooting the Password 152
Table 67 Troubleshooting Telnet 153
Table 68 Troubleshooting Accessing the Prestige 153
Table 69 Device 163
Table 70 Firmware 163
Table 71 Classes of IP Addresses 165
Table 72 Allowed IP Address Range By Class 166
Table 73 "Natural" Masks 166
Table 74 Alternative Subnet Mask Notation 167
Table 75 Two Subnets Example 167
Table 76 Subnet 1 168
Table 77 Subnet 2 168
Table 78 Subnet 1 169
Table 79 Subnet 2 169

Table 80 Subnet 3 169
Table 81 Subnet 4 170
Table 82 Eight Subnets 170
Table 83 Class C Subnet Planning 170
Table 84 Class B Subnet Planning 171
Table 85 IEEE802.11g 199
Table 86 Comparison of EAP Authentication Types 205
Table 87 Wireless Security Relational Matrix 206

Preface

Congratulations on your purchase of the P-320W, 802.11g Wireless Firewall Router. This manual is designed to guide you through the configuration of your Prestige for its various applications.

This manual may refer to the P-320W, 802.11g Wireless Firewall Router as the Prestige.

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 User’s Guide is designed to guide you through the configuration of your Prestige using the web configurator.

Related Documentation

- Supporting Disk

  Refer to the included CD for support documents.

- Quick Start Guide

  The Quick Start 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

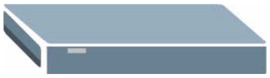
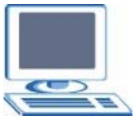
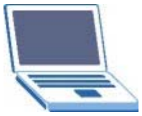
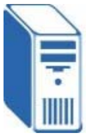
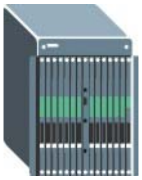
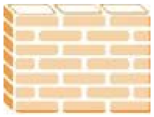
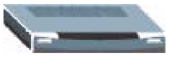
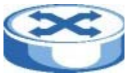
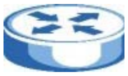
Help us help you! E-mail all User Guide-related comments, questions or suggestions for improvement to techwriters@zyxel.com.tw or send regular mail to The Technical Writing Team, ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 300, Taiwan. Thank you!

Syntax Conventions

- “Enter” means for you to type one or more characters. “Select” or “Choose” means for you to use one predefined choices.
- Mouse action sequences are denoted using a comma. For example, “In Windows, click **Start**, **Settings** and then **Control Panel**” means first click the **Start** button, then point your mouse pointer to **Settings** and then click **Control Panel**.

- “e.g.,” is a shorthand for “for instance”, and “i.e.,” means “that is” or “in other words”.

Graphics Icons Key

Prestige 	Computer 	Notebook computer 
Server 	DSLAM 	Firewall 
Modem 	Switch 	Router 

CHAPTER 1
Getting to Know Your Prestige

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

1.1 Prestige Overview

The Prestige is the ideal secure wireless firewall router for all data passing between the Internet and LAN’s.

The Prestige provides NAT, port forwarding, firewall, DHCP server and many other powerful features. The Prestige has an embedded mini-PCI module for 802.11g Wireless LAN connectivity.

The embedded web configurator is easy to operate.

Note: Only use firmware for your Prestige’s specific model.

1.2 Prestige Features

The following sections describe Prestige features.

1.2.1 Physical Features

10/100 Mbps Auto-negotiating Ethernet/Fast Ethernet Interface(s)

This auto-negotiation feature allows the Prestige to detect the speed of incoming transmissions and adjust appropriately without manual intervention. It allows data transfer of either 10 Mbps or 100 Mbps in either half-duplex or full-duplex mode depending on your Ethernet network.

Auto-negotiation allows data transfer of 100 Mbps in full-duplex mode

Auto-crossover 10/100 Mbps Ethernet Interface(s)

These interfaces automatically adjust to either a crossover or straight-through Ethernet cable.

4-Port Switch

A combination of switch and router makes your Prestige a cost-effective and viable network solution. You can add up to four computers to the Prestige without the cost of a hub. Add more than four computers to your LAN by using a hub.

Reset Button

The Prestige reset button is built into the rear panel. Use this button to restore the factory default password to 1234; IP address to 192.168.1.1, subnet mask to 255.255.255.0 and DHCP server enabled with a pool of 32 IP addresses starting at 192.168.1.33.

1.2.2 Non-Physical Features

Firewall

The Prestige is a stateful inspection firewall with DoS (Denial of Service) protection. By default, when the firewall is activated, all incoming traffic from the WAN to the LAN is blocked unless it is initiated from the LAN. The Prestige firewall supports TCP/UDP inspection, DoS detection and prevention, real time alerts, reports and logs.

Packet Filtering

The packet filtering mechanism blocks unwanted traffic from entering/leaving your network.

Time and Date

The Prestige allows you to get the current time and date from an external server when you turn on your Prestige. You can also set the time manually.

Universal Plug and Play (UPnP)

Using the standard TCP/IP protocol, the Prestige and other UPnP enabled devices can dynamically join a network, obtain an IP address and convey its capabilities to other devices on the network.

PPPoE

PPPoE facilitates the interaction of a host with an Internet modem to achieve access to high-speed data networks via a familiar "dial-up networking" user interface.

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 a TCP/IP-based network.

PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet. The Prestige supports one PPTP server connection at any given time.

Dynamic DNS Support

With Dynamic DNS (Domain Name System) support, you can have a static hostname alias for a dynamic IP address, allowing the host to be more easily accessible from various locations on the Internet. You must register for this service with a Dynamic DNS service provider.

IP Multicast

Deliver IP packets to a specific group of hosts using IP multicast. IGMP (Internet Group Management Protocol) is the protocol used to support multicast groups. The latest version is version 2 (see RFC 2236); the Prestige supports both versions 1 and 2.

SNMP

SNMP (Simple Network Management Protocol) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your Prestige supports SNMP agent functionality, which allows a manager station to manage and monitor the Prestige through the network. The Prestige supports SNMP version one (SNMPv1) and version two (SNMPv2).

Network Address Translation (NAT)

Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).

Traffic Redirect

Traffic Redirect forwards WAN traffic to a backup gateway on the LAN when the Prestige cannot connect to the Internet, thus acting as an auxiliary backup when your regular WAN connection fails.

Port Forwarding

Use this feature to forward incoming service requests to a server on your local network. 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.

DHCP (Dynamic Host Configuration Protocol)

DHCP (Dynamic Host Configuration Protocol) allows the individual client computers to obtain the TCP/IP configuration at start-up from a centralized DHCP server. The Prestige has built-in DHCP server capability, enabled by default, which means it can assign IP addresses, an IP default gateway and DNS servers to all systems that support the DHCP client.

Full Network Management

The embedded web configurator is an all-platform web-based utility that allows you to easily access the Prestige's management settings and configure the firewall. Most functions of the Prestige are also software configurable via the SMT (System Management Terminal) interface. The SMT is a menu-driven interface that you can access over a telnet connection.

RoadRunner Support

In addition to standard cable modem services, the Prestige supports Time Warner's RoadRunner Service.

Logging and Tracing

- Built-in message logging and packet tracing.
- Firewall logs.
- Content filtering logs.

Upgrade Prestige Firmware via LAN

The firmware of the Prestige can be upgraded via the LAN (refer to Maintenance- F/W Upload Screen).

Embedded FTP and TFTP Servers

The Prestige's embedded FTP and TFTP Servers enable fast firmware upgrades as well as configuration file backups and restoration.

1.2.3 Wireless Features

Wireless LAN

The Prestige supports the IEEE 802.11g standard, which is fully compatible with the IEEE 802.11b standard, meaning that you can have both IEEE 802.11b and IEEE 802.11g wireless clients in the same wireless network.

Note: The Prestige may be prone to RF (Radio Frequency) interference from other 2.4 GHz devices such as microwave ovens, wireless phones, Bluetooth enabled devices, and other wireless LANs.

Wi-Fi Protected Access

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i security specification standard. Key differences between WPA and WEP are user authentication and improved data encryption.

Antenna

The Prestige is equipped with a 2dBi fixed antenna to provide clear radio signal between the wireless stations and the access points.

Wireless LAN MAC Address Filtering

Your Prestige can check the MAC addresses of wireless stations against a list of allowed or denied MAC addresses.

WEP Encryption

WEP (Wired Equivalent Privacy) encrypts data frames before transmitting over the wireless network to help keep network communications private.

OTIST (One Touch Intelligent Security Technology)

OTIST allows your Prestige to assign its ESSID and security settings (WEP or WPA-PSK) to the ZyXEL wireless adapters that support OTIST and are within transmission range. The ZyXEL wireless adapters must also have OTIST enabled.

Association List

With the association list, you can see the list of the wireless stations that are currently using the Prestige to access your wired network.

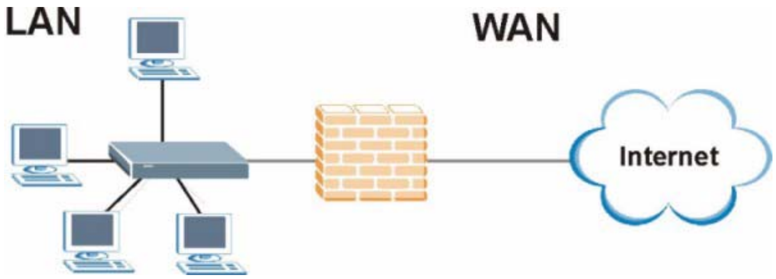
1.3 Applications for the Prestige

Here are some examples of what you can do with your Prestige.

1.3.1 Secure Broadband Internet Access via Cable or DSL Modem

You can connect a cable modem, DSL or wireless modem to the Prestige for broadband Internet access via an Ethernet or a wireless port on the modem. The Prestige guarantees not only high speed Internet access, but secure internal network protection and traffic management as well.

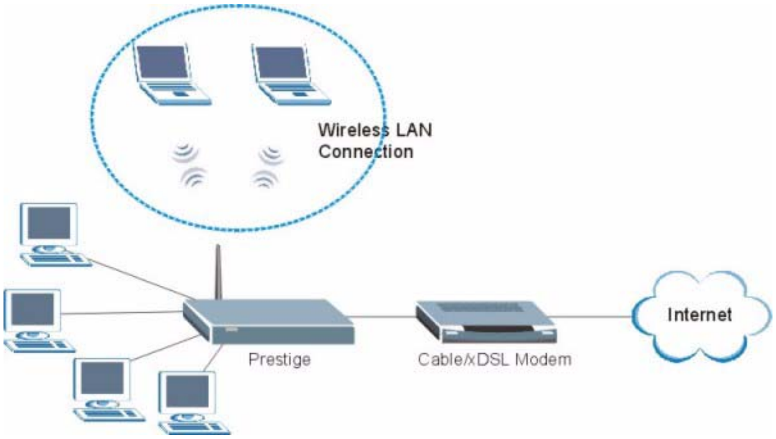
Figure 1 Secure Internet Access via Cable, DSL or Wireless Modem



1.3.2 Wireless LAN Application

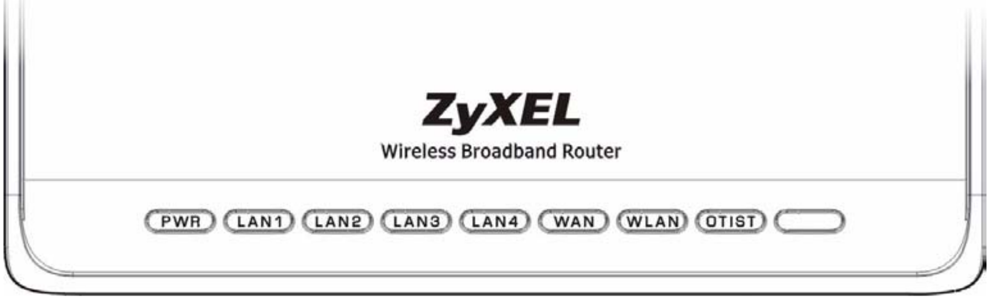
Add a wireless LAN to your existing network without expensive network cables. Wireless stations can move freely anywhere in the coverage area and use resources on the wired network.

Figure 2 Internet Access Application Example



1.3.3 Front Panel LEDs

Figure 3 Front Panel



The following table describes the LEDs.

Table 1 Front Panel LEDs

LED	COLOR	STATUS	DESCRIPTION
PWR	Green	On	The Prestige is receiving power and functioning properly.
		Blinking	The Prestige is performing testing.
	Red	On	Power to the Prestige is too low.
	None	Off	The Prestige is not receiving power.

Table 1 Front Panel LEDs (continued)

LED	COLOR	STATUS	DESCRIPTION
LAN 1-4	Green	On	The Prestige has a successful 10Mb Ethernet connection.
		Blinking	The Prestige is sending/receiving data.
	Amber	On	The Prestige has a successful 100Mb Ethernet connection.
		Blinking	The Prestige is sending/receiving data.
	None	Off	The LAN is not connected.
WAN	Green	On	The Prestige has a successful 10Mb WAN connection.
		Blinking	The Prestige is sending/receiving data.
	Amber	On	The Prestige has a successful 100Mb Ethernet connection.
		Blinking	The Prestige is sending/receiving data.
	None	Off	The WAN connection is not ready, or has failed.
WLAN	Green	On	The Prestige is ready, but is not sending/receiving data through the wireless LAN.
		Blinking	The Prestige is sending/receiving data through the wireless LAN.
	None	Off	The wireless LAN is not ready or has failed.
OTIST	Green	Blinking	OTIST is in progress
		On	OTIST is activated and the wireless security settings are given to a wireless client. The LED remains on unless the WLAN settings are changed.
	None	Off	OTIST is not activated or WLAN settings are manually configured after OTIST is successful.

CHAPTER 2 Introducing the Web Configurator

This chapter describes how to access the Prestige web configurator and provides an overview of its screens.

2.1 Web Configurator Overview

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

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

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

See the Troubleshooting chapter to see how to make sure these functions are allowed in Internet Explorer.

2.2 Accessing the Prestige Web Configurator

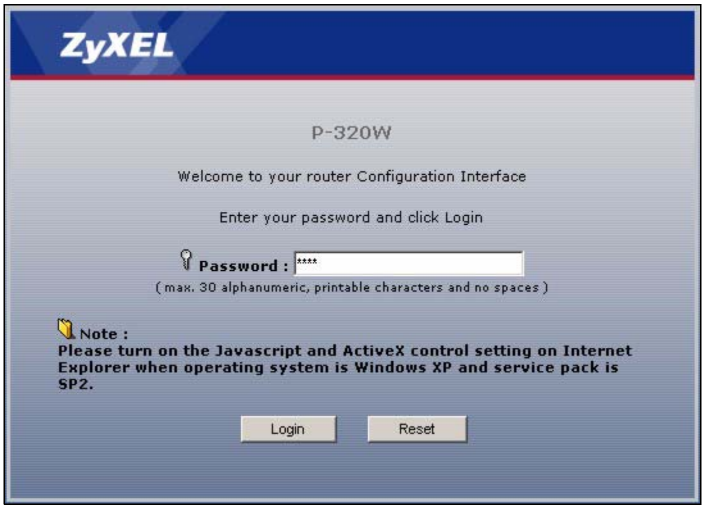
1 Make sure your Prestige hardware is properly connected and prepare your computer/ computer network to connect to the Prestige (refer to the Quick Start Guide).

2 Launch your web browser.

3 Type "192.168.1.1" as the URL.

4 Type "1234" (default) as the password and click **Login**. In some versions, the default password appears automatically - if this is the case, click **Login**.

Figure 4 Login



P-320W

Welcome to your router Configuration Interface

Enter your password and click Login

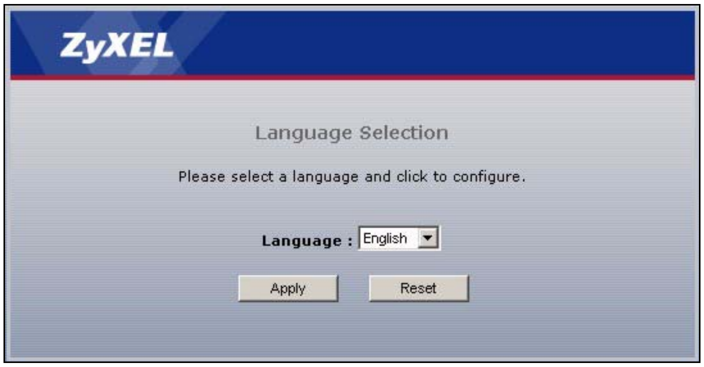
Password : ****

(max. 30 alphanumeric, printable characters and no spaces)

Note :
Please turn on the Javascript and ActiveX control setting on Internet Explorer when operating system is Windows XP and service pack is SP2.

5 Select your language. click **Apply**.

Figure 5 Language Selection



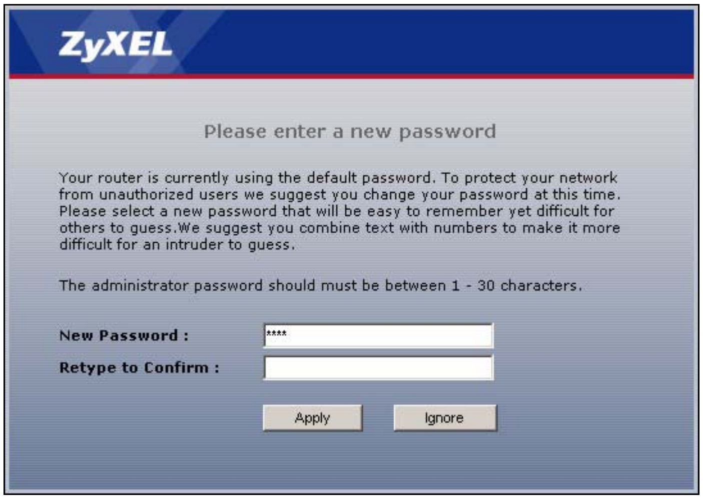
Language Selection

Please select a language and click to configure.

Language : English

6 You should see a screen asking you to change your password (highly recommended) as shown next. Type a new password (and retype it to confirm) and click **Apply** or click **Ignore**.

Figure 6 Change Password Screen



Please enter a new password

Your router is currently using the default password. To protect your network from unauthorized users we suggest you change your password at this time. Please select a new password that will be easy to remember yet difficult for others to guess.We suggest you combine text with numbers to make it more difficult for an intruder to guess.

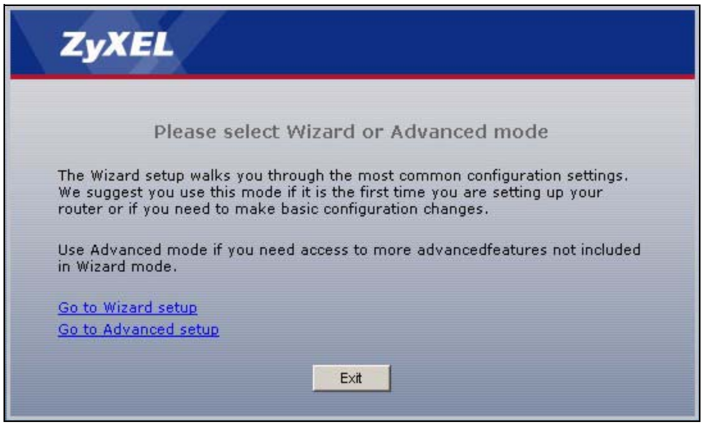
The administrator password should must be between 1 - 30 characters.

New Password : ****

Retype to Confirm :

7 Click **Go to Wizard setup** to do initial configuration withs the wizard, click **Go to Advanced setup** to configure advanced features, or click **Exit** to log out of the web configurator.

Figure 7 Select the Mode



Please select Wizard or Advanced mode

The Wizard setup walks you through the most common configuration settings. We suggest you use this mode if it is the first time you are setting up your router or if you need to make basic configuration changes.

Use Advanced mode if you need access to more advancedfeatures not included in Wizard mode.

Note: The management session automatically times out when the time period set in the **Administrator Inactivity Timer** field expires (default five minutes). Simply log back into the Prestige if this happens to you.

2.3 Resetting the Prestige

If you forget your password or cannot access the web configurator, you will need to use the **RESET** button at the back of the Prestige to reload the factory-default configuration file. This means that you will lose all configurations that you had previously and the password will be reset to "1234".

2.3.1 Procedure To Use The Reset Button

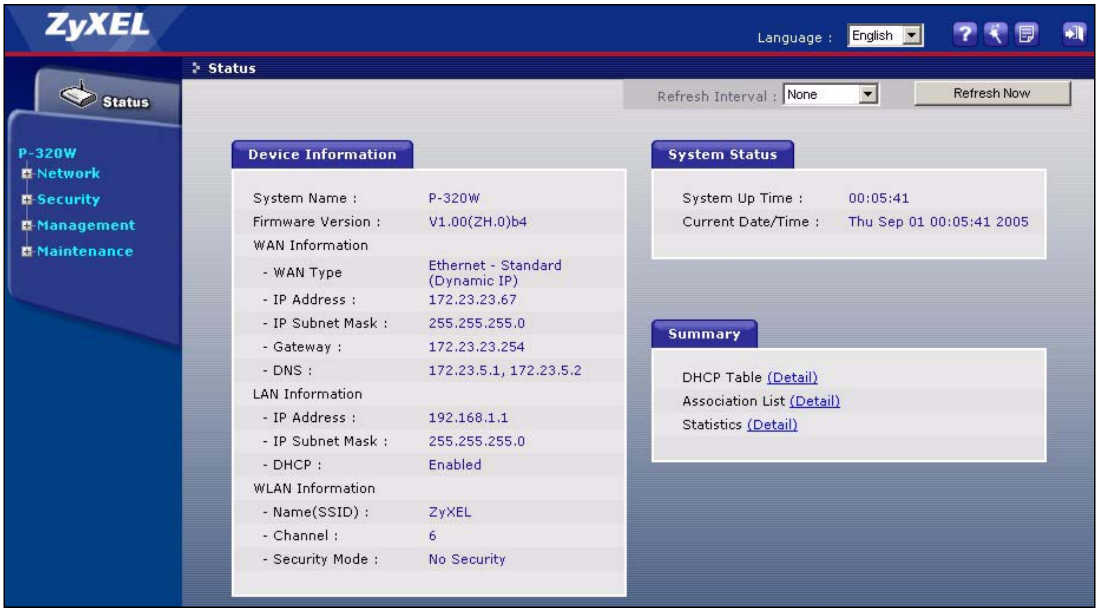
1 Make sure the **PWR** LED is on (not blinking).

2 Press the **RESET** button for ten seconds or until the **PWR** LED begins to blink and then release it. When the **PWR** LED begins to blink, the defaults have been restored and the Prestige restarts.

2.4 Navigating the Prestige Web Configurator

The following summarizes how to navigate the web configurator from the **Status** screen.

Figure 8 Web Configurator Status Screen



Device Information

System Name :	P-320W
Firmware Version :	V1.00(ZH.0)b4
WAN Information	
- WAN Type	Ethernet - Standard (Dynamic IP)
- IP Address :	172.23.23.67
- IP Subnet Mask :	255.255.255.0
- Gateway :	172.23.23.254
- DNS :	172.23.5.1, 172.23.5.2
LAN Information	
- IP Address :	192.168.1.1
- IP Subnet Mask :	255.255.255.0
- DHCP :	Enabled
WLAN Information	
- Name(SSID) :	ZyXEL
- Channel :	6
- Security Mode :	No Security

System Status

System Up Time :	00:05:41
Current Date/Time :	Thu Sep 01 00:05:41 2005

Summary

DHCP Table (Detail)
Association List (Detail)
Statistics (Detail)

The following table describes the icons shown in the **Status** screen.

Table 2 Status Screen Icon Key

ICON	DESCRIPTION
Language : English ▾ English German French Spanish Chinese Italian	Select a language from the drop-down list box to have the the web configurator display in that language.
?	Click this icon to open a web help page relevent to the screen you are currently configuring.
✦	Click this icon to open the setup wizard. The Prestige has a connection wizard and a bandwidth management wizard.
▤	Click this icon to view copyright and a link for related product information.
⇥	Click this icon at any time to exit the web configurator.
Refresh Interval: 20 seconds ▾	Select a number of seconds or **None** from the drop-down list box to refresh all screen statistics automatically at the end of every time interval or to not refresh the screen statistics.
Refresh Now	Click this button to refresh the status screen statistics.

The following table describes the labels shown in the **Status** screen.

Table 3 Web Configurator Status Screen

LABEL	DESCRIPTION
Device Information	
System Name	This is the **System Name** you enter in the **Maintenance**, **System**, **General** screen. It is for identification purposes.
Firmware Version	This is the firmware version and the date created.

Table 3 Web Configurator Status Screen

LABEL	DESCRIPTION
WAN Information	
- WAN Type	This shows the encapsulation method (and service type) the Prestige is using.
- IP Address	This shows the WAN port's IP address.
- IP Subnet Mask	This shows the WAN port's subnet mask.
- Gateway	This shows the gateway IP address.
- DNS	This shows the IP address(es) of the DNS server(s).
LAN Information	
- IP Address	This shows the LAN port's IP address.
- IP Subnet Mask	This shows the LAN port's subnet mask.
- DHCP	This shows whether the Prestige acts as a DHCP server (**Enabled**) or not (**Disabled**).
WLAN Information	
- Name(SSID)	This shows a descriptive name used to identify the Prestige in the wireless LAN.
- Channel	This shows the channel number which the Prestige uses over the wireless LAN.
- Security Mode	This shows the level of wireless security the Prestige is using.
System Status	
System Uptime	This is the total time the Prestige has been on.
Current Date/Time	This field displays your Prestige's present date and time along with the difference from the Greenwich Mean Time (GMT) zone. The difference from GMT is based on the time zone. It is also adjusted for Daylight Saving Time if you set the Prestige to use it.
Summary	
DHCP Table	Use this screen to view current DHCP client information.
Association List	Use this screen to view the wireless stations that are currently associated to the Prestige.
Statistics	Use this screen to view port status and packet specific statistics.

2.4.1 Navigation Panel

After you enter the password, use the sub-menus on the navigation panel to configure Prestige features. The navigation

The following table describes the sub-menus.

Table 4 Screens Summary

LINK	TAB	FUNCTION
Status		This screen shows the Prestige's general device and system status information. Use this screen to access the wizard, and summary statistics tables.
Network		

Table 4 Screens Summary

LINK	TAB	FUNCTION
Wireless LAN	General	Use this screen to configure wireless LAN.
	OTIST	This screen allows you to assign wireless clients the Prestige’s wireless security settings.
	MAC Filter	Use the MAC filter screen to configure the Prestige to block access to devices or block the devices from accessing the Prestige.
	Advanced	This screen allows you to configure other advanced WLAN properties.
WAN	Internet Connection	This screen allows you to configure ISP parameters, WAN IP address assignment and the WAN MAC address.
	Advanced	Use this screen to configure DNS servers.
	Traffic Redirect	Use this screen to configure your traffic redirect properties and parameters.
LAN	IP	Use this screen to configure LAN settings.
DHCP Server	General	Use this screen to enable the Prestige’s DHCP server and to have DNS servers assigned by the DHCP server.
	Static DHCP	Use this screen to assign IP addresses on the LAN to specific individual computers based on their MAC addresses.
	Client List	Use this screen to view current DHCP client information and to always assign an IP address to a MAC address (and host name).
NAT	General	Use this screen to enable NAT.
	Port Forwarding	Use this screen to configure servers behind the Prestige.
	Trigger Port	Use this screen to change your Prestige’s port triggering settings.
Security		
Firewall	General	Use this screen to activate/deactivate the firewall.
	Services	This screen shows a summary of the firewall rules, and allows you to edit/ add a firewall rule.
Management		
Static Route	Static Route Rules	Use this screen to configure IP static routes.
Remote MGMT	WWW	Use this screen to configure through which interface(s) and from which IP address(es) users can use HTTP to manage the Prestige.
	SNMP	Use this screen to configure your Prestige’s settings for Simple Network Management Protocol management.
	Security	Use this screen to change your anti-probing settings.
UPnP	General	Use this screen to enable UPnP on the Prestige.
Maintenance		
System	General	This screen contains administrative.
	Dynamic DNS	Use this screen to set up dynamic DNS.
	Time Setting	Use this screen to change your Prestige’s time and date.
Logs	View Log	Use this screen to view the logs for the categories that you selected.
	Log Settings	Use this screen to change your Prestige’s log settings.

Table 4 Screens Summary

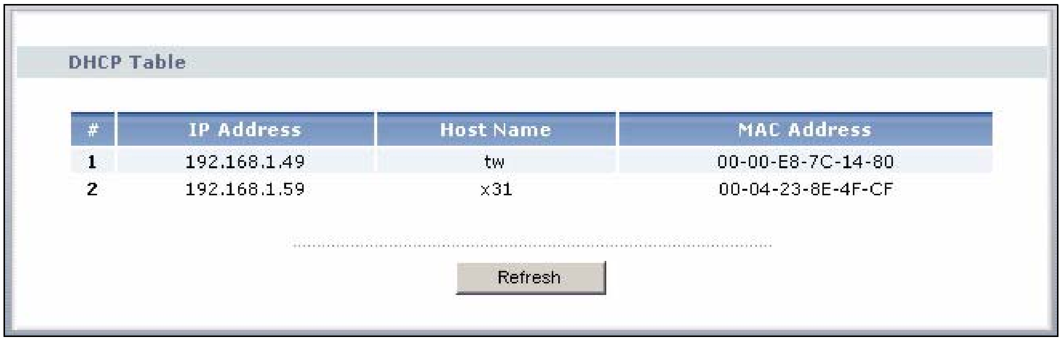
LINK	TAB	FUNCTION
Tools	Firmware	Use this screen to upload firmware to your Prestige.
	Configuration	Use this screen to backup and restore the configuration or reset the factory defaults to your Prestige.
	Restart	This screen allows you to reboot the Prestige without turning the power off.

2.4.2 Summary: DHCP Table

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

Click the **DHCP Table (Detail)** hyperlink in the **Status** screen. Read-only information here relates to your DHCP status. The DHCP table shows current DHCP client information (including **IP Address**, **Host Name** and **MAC Address**) of all network clients using the Prestige's DHCP server.

Figure 9 Summary: DHCP Table



DHCP Table

#	IP Address	Host Name	MAC Address
1	192.168.1.49	tw	00-00-E8-7C-14-80
2	192.168.1.59	x31	00-04-23-8E-4F-CF

The following table describes the labels in this screen.

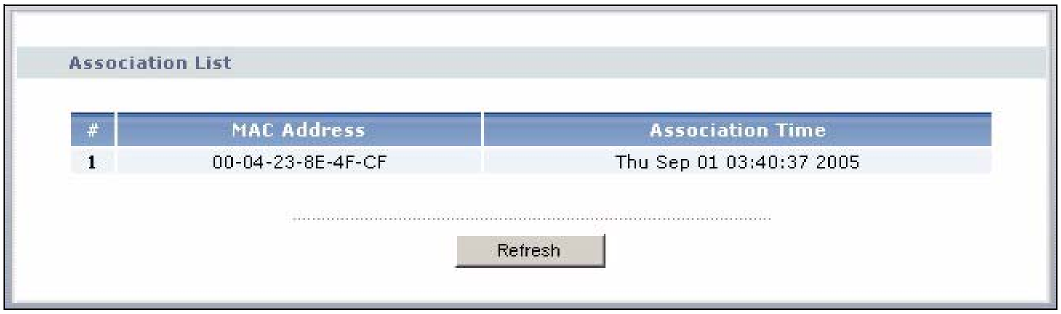
Table 5 Summary: DHCP Table

	DESCRIPTION
#	This is the index number of the host computer.
IP Address	This field displays the IP address relative to the # field listed above.
Host Name	This field displays the computer host name.
MAC Address	This field shows the MAC address of the computer with the name in the **Host Name** field. 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.
Refresh	Click **Refresh** to renew the screen.

2.4.3 Summary: Association List

Click the **Association List (Detail)** hyperlink in the **Status** screen. View the wireless stations that are currently associated to the Prestige in the **Association List** screen.

Figure 10 Summary: Association List



Association List

#	MAC Address	Association Time
1	00-04-23-8E-4F-CF	Thu Sep 01 03:40:37 2005

The following table describes the labels in this screen.

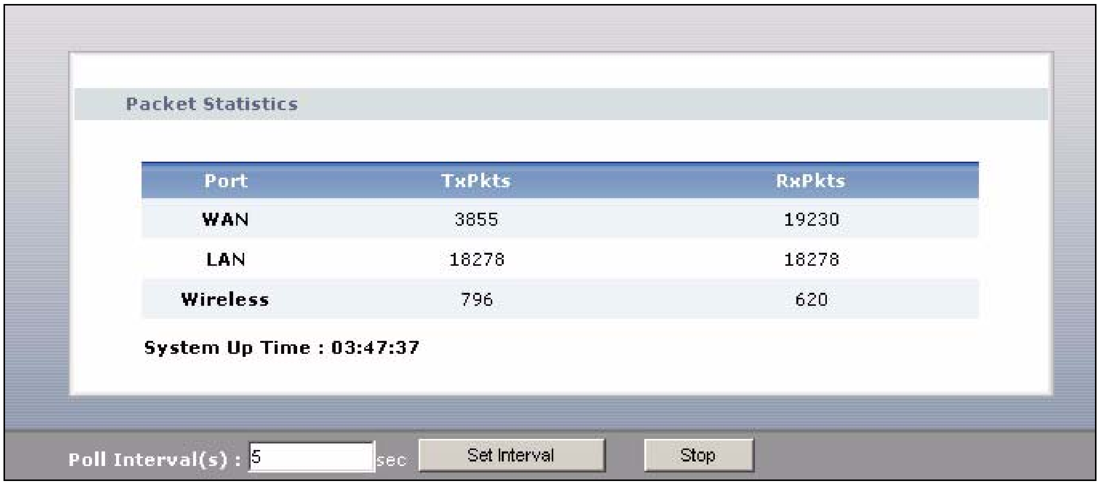
Table 6 Summary: Wireless Association List

LABEL	DESCRIPTION
#	This is the index number of an associated wireless station.
MAC Address	This field displays the MAC address of an associated wireless station.
Association Time	This field displays the time a wireless station first associated with the Prestige.
Refresh	Click **Refresh** to redisplay the current screen.

2.4.4 Summary: Packet Statistics

Click the **Statistics (Detail)** hyperlink in the **Status** screen. Read-only information here includes packet specific statistics. Also provided are "system up time" and "poll interval(s)". The **Poll Interval(s)** field is configurable.

Figure 11 Summary: Packet Statistics



Packet Statistics

Port	TxPkts	RxPkts
WAN	3855	19230
LAN	18278	18278
Wireless	796	620

System Up Time : 03:47:37

Poll Interval(s) : 5 sec

The following table describes the labels in this screen.

Table 7 Summary: Packet Statistics

LABEL	DESCRIPTION
Port	This is the WAN, LAN or WLAN port.
TxPkts	This is the number of transmitted packets on this port.
RxPkts	This is the number of received packets on this port.
System Up Time	This is the total time the Prestige has been on.
Poll Interval(s)	Enter the time interval for refreshing statistics in this field.
Set Interval	Click this button to apply the new poll interval you entered in the **Poll Interval(s)** field.
Stop	Click **Stop** to stop refreshing statistics, click **Stop**.

CHAPTER 3
Connection Wizard

This chapter provides information on the Wizard setup screens in the web configurator.

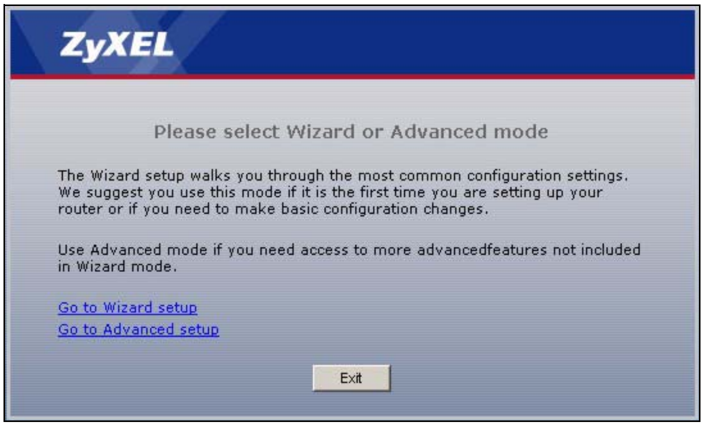
3.1 Wizard Setup

The web configurator’s Wizard setup helps you configure your device to access the Internet. Refer to your ISP (Internet Service Provider) checklist in the Quick Start Guide to know what to enter in each field. Leave a field blank if you don’t have that information.

1 After you access the Prestige web configurator, click the **Go to Wizard setup** hyperlink.

You can click the **Go to Advanced setup** hyperlink to skip this wizard setup and configure advanced features.

Figure 12 Select a Mode



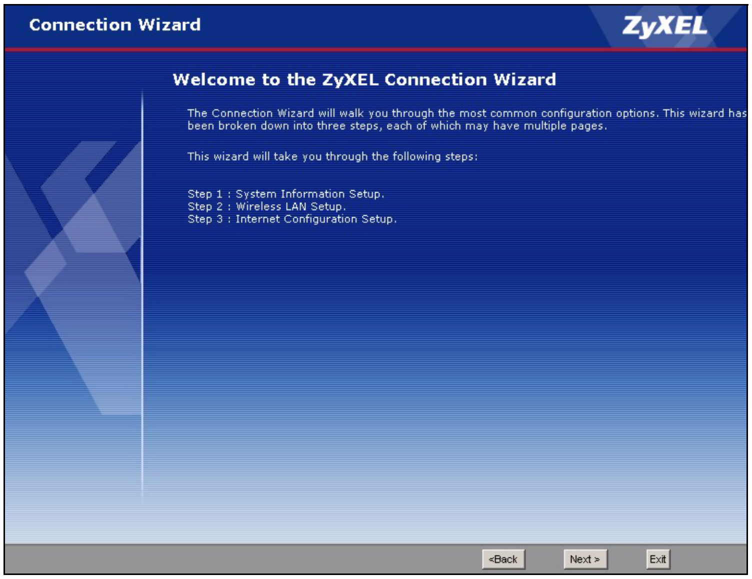
Please select Wizard or Advanced mode

The Wizard setup walks you through the most common configuration settings. We suggest you use this mode if it is the first time you are setting up your router or if you need to make basic configuration changes.

Use Advanced mode if you need access to more advancedfeatures not included in Wizard mode.

2 Read the on-screen information and click **Next**.

Figure 13 Welcome to the Connection Wizard



Welcome to the ZyXEL Connection Wizard

The Connection Wizard will walk you through the most common configuration options. This wizard has been broken down into three steps, each of which may have multiple pages.

This wizard will take you through the following steps:

Step 1 : System Information Setup.
Step 2 : Wireless LAN Setup.
Step 3 : Internet Configuration Setup.

3.2 Connection Wizard: STEP 1: System Information

System Information contains administrative and system-related information.

3.2.1 System Name

System Name is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name".

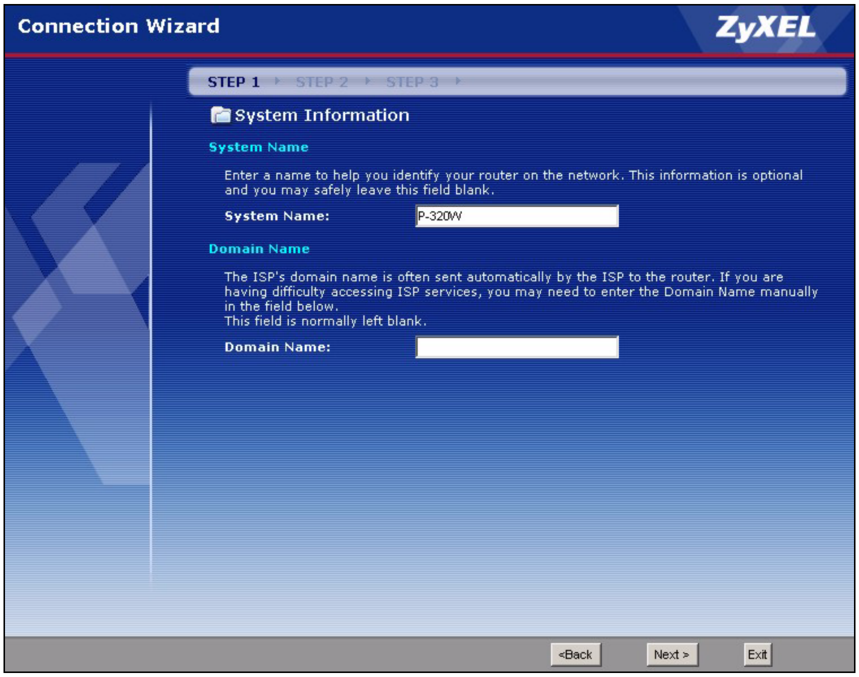
- In Windows 95/98 click **Start**, **Settings**, **Control Panel**, **Network**. Click the Identification tab, note the entry for the **Computer Name** field and enter it as the **System Name**.
- In Windows 2000, click **Start**, **Settings** and **Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the **System Name**.
- In Windows XP, click **Start**, **My Computer**, **View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the Prestige **System Name**.

3.2.2 Domain Name

The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. If you leave this blank, the domain name obtained by DHCP from the ISP is used. While you must enter the host name (System Name) on each individual computer, the domain name can be assigned from the Prestige via DHCP.

Click **Next** to configure the Prestige for Internet access.

Figure 14 Connection Wizard: STEP 1: System Information



System Information

System Name

Enter a name to help you identify your router on the network. This information is optional and you may safely leave this field blank.

System Name: P-320W

Domain Name

The ISP's domain name is often sent automatically by the ISP to the router. If you are having difficulty accessing ISP services, you may need to enter the Domain Name manually in the field below.
This field is normally left blank.

Domain Name:

The following table describes the labels in this screen.

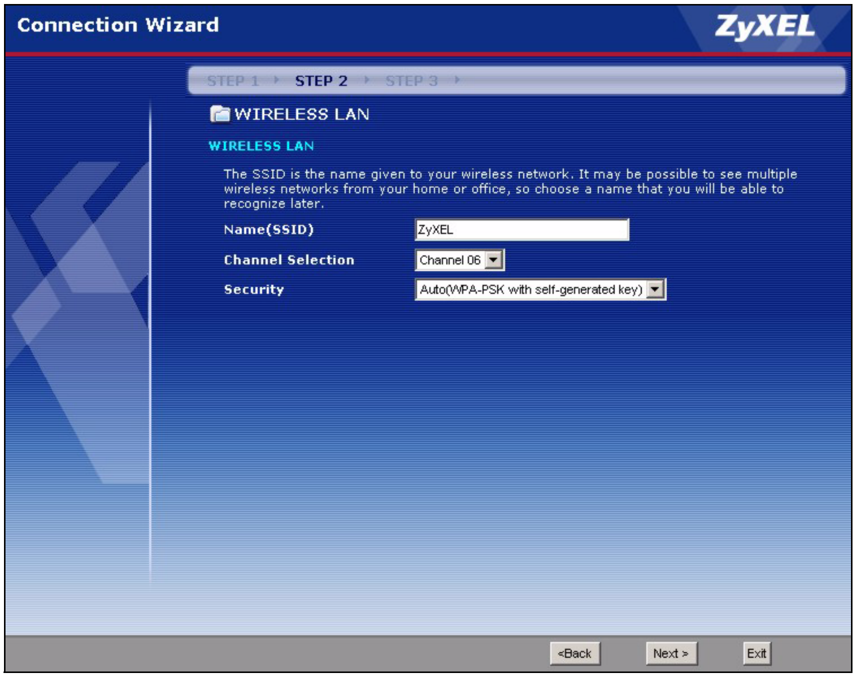
Table 8 Connection Wizard: STEP 1: System Information

LABEL	DESCRIPTION
System Name	System Name is a unique name to identify the Prestige in an Ethernet network. Enter a descriptive name. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	Type the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. The domain name entered by you is given priority over the ISP assigned domain name.
Back	Click **Back** to display the previous screen.
Next	Click **Next** to proceed to the next screen.
Exit	Click **Exit** to close the wizard screen without saving.

3.3 Connection Wizard: STEP 2: Wireless LAN

Set up your wireless LAN using the following screen.

Figure 15 Connection Wizard: STEP 2: Wireless LAN



Connection Wizard

WIRELESS LAN

WIRELESS LAN

The SSID is the name given to your wireless network. It may be possible to see multiple wireless networks from your home or office, so choose a name that you will be able to recognize later.

Name(SSID): ZyXEL

Channel Selection: Channel 06

Security: Auto(WPA-PSK with self-generated key)

The following table describes the labels in this screen.

Table 9 Connection Wizard: STEP 2: Wireless LAN

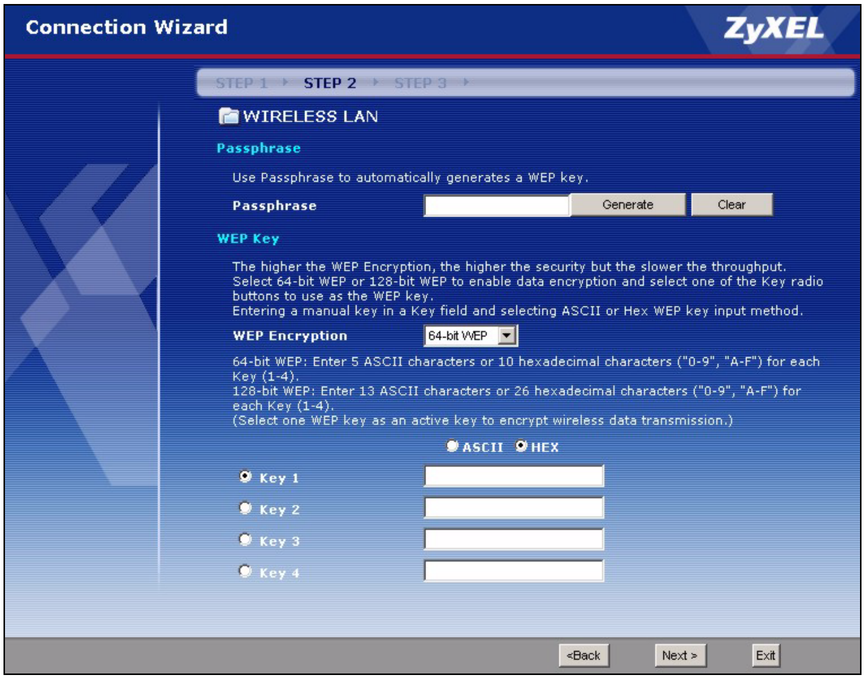
LABEL	DESCRIPTION
Name(SSID)	Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. If you change this field on the Prestige, make sure all wireless stations use the same SSID in order to access the network.
Channel Selection	The range of radio frequencies used by IEEE 802.11b/g wireless devices is called a channel. Select a channel ID that is not already in use by a neighboring device.
Security	Select a **Security** level from the drop-down list box. Choose **Auto (WPA-PSK with self-generated key)** to use WPA-PSK security with a default Pre-Shared Key and only if your wireless clients support WPA-PSK. If you choose this option, skip directly to Section 3.3.3 on page 51. Choose **None** to have no wireless LAN security configured. If you do not enable any wireless security on your Prestige, your network is accessible to any wireless networking device that is within range. If you choose this option, skip directly to section 3.3.3. Choose **Basic (WEP)** security if you want to configure WEP Encryption parameters. If you choose this option, go directly to Section 3.3.1 on page 49. Choose **Extend (WPA-PSK with customized key)** security to configure a Pre-Shared Key. Choose this option only if your wireless clients support WPA-PSK or WPA2-PSK respectively. If you choose this option, skip directly to Section 3.3.2 on page 50.
Back	Click **Back** to display the previous screen.
Next	Click **Next** to proceed to the next screen.
Exit	Click **Exit** to close the wizard screen without saving.

Note: The wireless stations and Prestige must use the same SSID, channel ID and WEP encryption key (if WEP is enabled), WPA-PSK (if WPA-PSK is enabled) for wireless communication.

3.3.1 Basic(WEP) Security

Choose **Basic(WEP)** to setup WEP Encryption parameters.

Figure 16 Basic(WEP) Security



Connection Wizard

ZyXEL

STEP 1 ▸ STEP 2 ▸ STEP 3 ▸

WIRELESS LAN

Passphrase

Use Passphrase to automatically generates a WEP key.

Passphrase [ ] Generate Clear

WEP Key

The higher the WEP Encryption, the higher the security but the slower the throughput.
Select 64-bit WEP or 128-bit WEP to enable data encryption and select one of the Key radio buttons to use as the WEP key.
Entering a manual key in a Key field and selecting ASCII or Hex WEP key input method.

WEP Encryption: 64-bit WEP

64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F") for each Key (1-4).
128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F") for each Key (1-4).
(Select one WEP key as an active key to encrypt wireless data transmission.)

○ ASCII ● HEX

● Key 1 [ ]
○ Key 2 [ ]
○ Key 3 [ ]
○ Key 4 [ ]

<Back Next > Exit

The following table describes the labels in this screen.

Table 10 Basic(WEP) Security

LABEL	DESCRIPTION
Passphrase	Type a Passphrase (up to 32 printable characters) and click **Generate**. The Prestige automatically generates four different WEP keys.
Generate	After you enter the passphrase, click **Generate** to have the Prestige generates four different WEP keys automatically.
Clear	Click **Clear** to discard the passphrase you configured in the **Passphrase** field and the WEP key(s) generated automatically or maually configured.
WEP Encryption	Select **64-bit WEP** or **128-bit WEP** to allow data encryption.
ASCII	Select this option in order to enter ASCII characters as the WEP keys.
HEX	Select this option to enter hexadecimal characters as the WEP keys. The preceding "0x" is entered automatically.

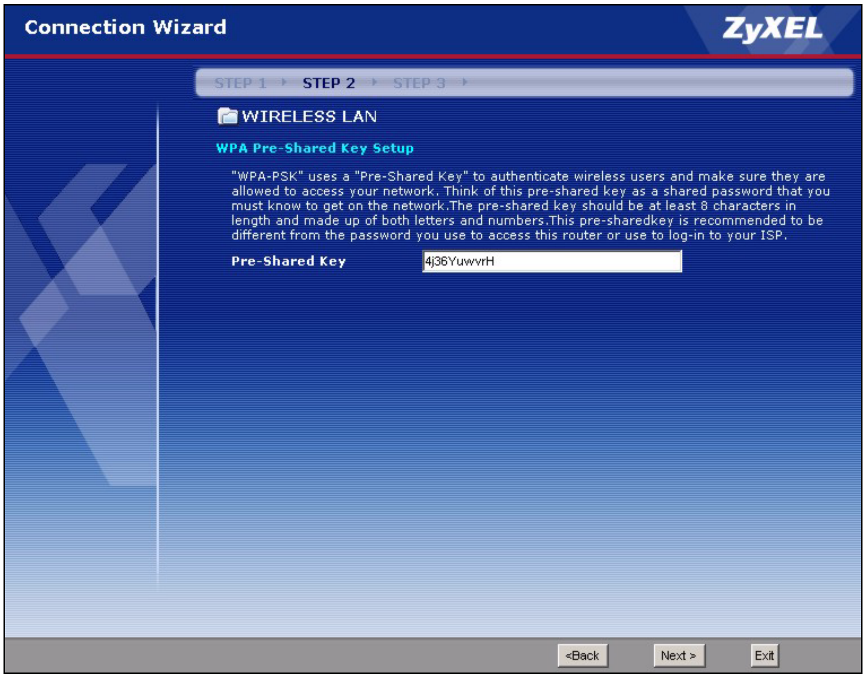
Table 10 Basic(WEP) Security

LABEL	DESCRIPTION
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the Prestige and the wireless stations must use the same WEP key for data transmission. If you chose **64-bit WEP**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit WEP**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). You must configure at least one key, only one key can be activated at any one time. The default key is key 1.
Back	Click **Back** to display the previous screen.
Next	Click **Next** to proceed to the next screen.
Exit	Click **Exit** to close the wizard screen without saving.

3.3.2 Extend(WPA-PSK) Security

Choose **Extend(WPA-PSK)** security in the Wireless LAN setup screen to set up a **Pre-Shared Key**.

Figure 17 Extend(WPA-PSK) Security



WPA Pre-Shared Key Setup

"WPA-PSK" uses a "Pre-Shared Key" to authenticate wireless users and make sure they are allowed to access your network. Think of this pre-shared key as a shared password that you must know to get on the network.The pre-shared key should be at least 8 characters in length and made up of both letters and numbers.This pre-sharedkey is recommended to be different from the password you use to access this router or use to log-in to your ISP.

Pre-Shared Key: 4j36YuwvrH

The following table describes the labels in this screen.

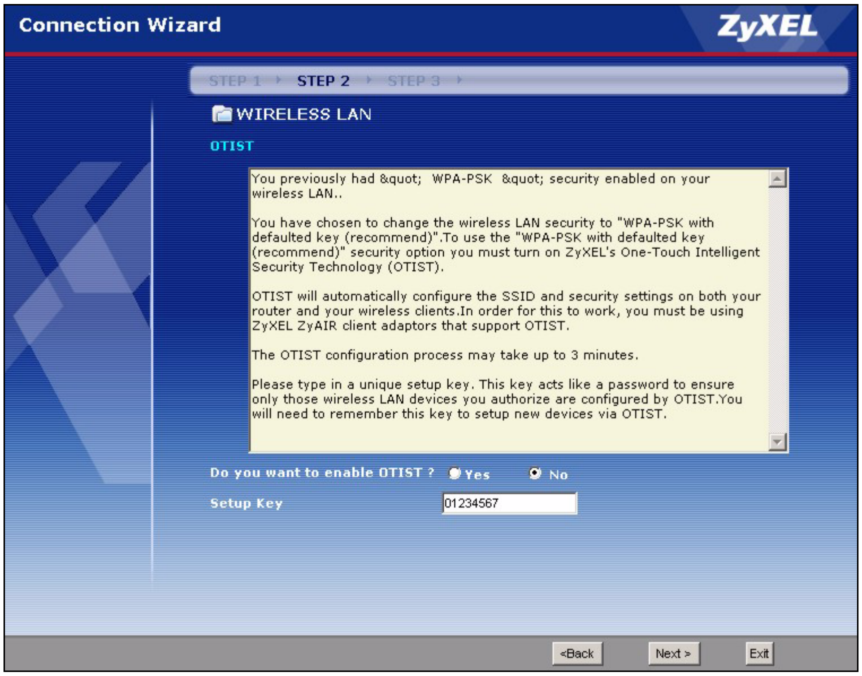
Table 11 Extend(WPA-PSK) Security

LABEL	DESCRIPTION
Pre-Shared Key	Type from 8 to 63 case-sensitive ASCII characters. You can set up the most secure wireless connection by configuring WPA in the wireless LAN screens. You need to configure an authentication server to do this.
Back	Click **Back** to display the previous screen.
Next	Click **Next** to proceed to the next screen.
Exit	Click **Exit** to close the wizard screen without saving.

3.3.3 OTIST

The following screen allows you to enable Prestige One-Touch Intelligent Security Technology (OTIST). One-Touch Intelligent Security Technology (OTIST) allows your Prestige to assign wireless clients the Prestige’s SSID and static WEP or WPA-PSK encryption settings. The wireless client must also support OTIST and have OTIST enabled. See Section 4.5 on page 72 for more information.

Figure 18 OTIST



You previously had &quot; WPA-PSK &quot; security enabled on your wireless LAN..

You have chosen to change the wireless LAN security to "WPA-PSK with defaulted key (recommend)".To use the "WPA-PSK with defaulted key (recommend)" security option you must turn on ZyXEL's One-Touch Intelligent Security Technology (OTIST).

OTIST will automatically configure the SSID and security settings on both your router and your wireless clients.In order for this to work, you must be using ZyXEL ZyAIR client adaptors that support OTIST.

The OTIST configuration process may take up to 3 minutes.

Please type in a unique setup key. This key acts like a password to ensure only those wireless LAN devices you authorize are configured by OTIST.You will need to remember this key to setup new devices via OTIST.

Do you want to enable OTIST ? ○ Yes ● No

Setup Key: 01234567

The following table describes the labels in this screen.

Table 12 OTIST

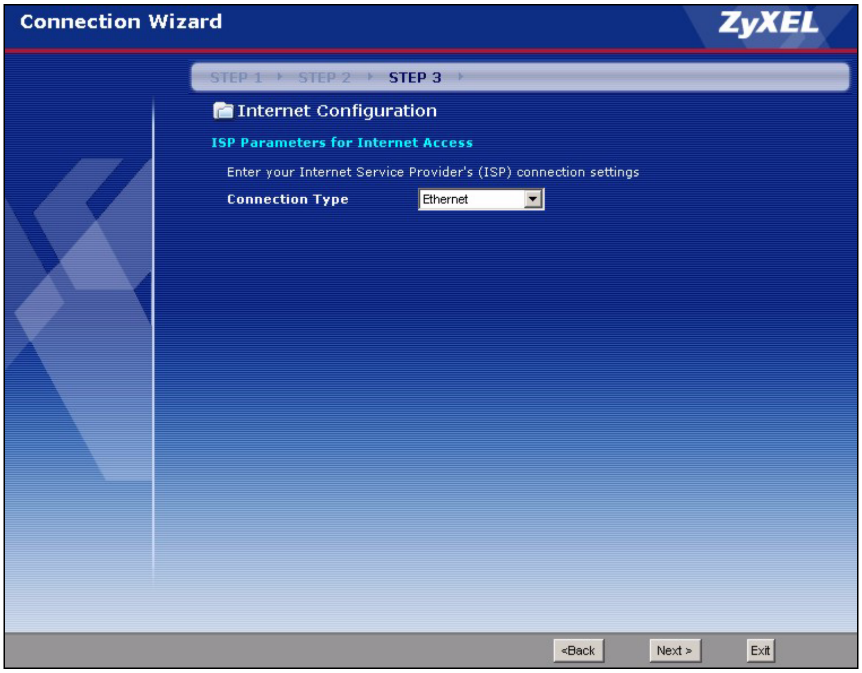
LABEL	DESCRIPTION
Do you want to enable OTIST?	Select the **Yes** radio button and click **Next** to proceed with the setup wizard and enable OTIST only when you click **Finish** in the final wizard screen. Click **No** and then **Next** to proceed to the following screen.
Setup Key	The default OTIST **Setup Key** is "01234567". This key can be changed in the web configurator. Be sure to use the same OTIST **Setup Key** on the Prestige and wireless clients.
Back	Click **Back** to display the previous screen.
Next	Click **Next** to proceed to the next screen.
Exit	Click **Exit** to close the wizard screen without saving.

Refer to the chapter on wireless LAN for more information.

3.4 Connection Wizard: STEP 3: Internet Configuration

The Prestige offers three Internet connection types. They are **Ethernet**, **PPP over Ethernet** or **PPTP**. The wizard attempts to detect which WAN connection type you are using. If the wizard does not detect a connection type, you must select one from the drop-down list box. Check with your ISP to make sure you use the correct type.

Figure 19 Connection Wizard: STEP 3: WAN Connection Type.



Connection Wizard

Internet Configuration

ISP Parameters for Internet Access

Enter your Internet Service Provider's (ISP) connection settings

Connection Type: Ethernet

The following table describes the labels in this screen,

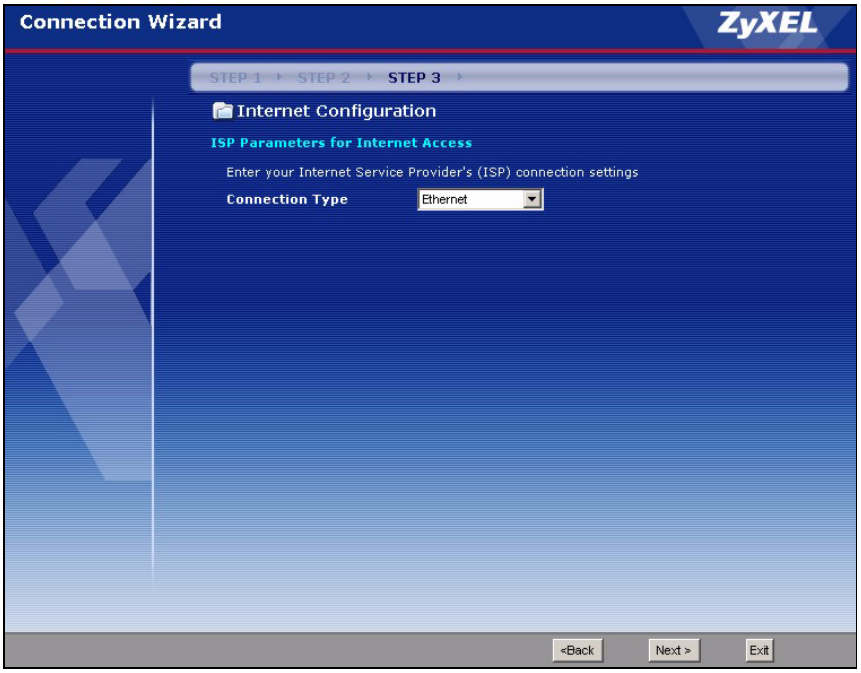
Table 13 Connection Wizard: STEP 3: WAN Connection Type

CONNECTION TYPE	DESCRIPTION
Ethernet	Select the **Ethernet** option when the WAN port is used as a regular Ethernet.
PPPoE	Select the **PPP over Ethernet** option for a dial-up connection. If your ISP gave you a an IP address and/or subnet mask, then select **PPTP**.
PPTP	Select the **PPTP** option for a dial-up connection.

3.4.1 Ethernet Connection Type

Choose **Ethernet** when the WAN port is used as a regular Ethernet.

Figure 20 Ethernet Connection Type



Enter your Internet Service Provider's (ISP) connection settings

Connection Type: Ethernet

3.4.2 PPPoE Connection Type

Point-to-Point Protocol over Ethernet (PPPoE) functions as a dial-up connection. PPPoE is an IETF (Internet Engineering Task Force) standard specifying how a host personal computer interacts with a broadband modem (for example DSL, cable, wireless, etc.) to achieve access to high-speed data networks.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for instance, RADIUS).

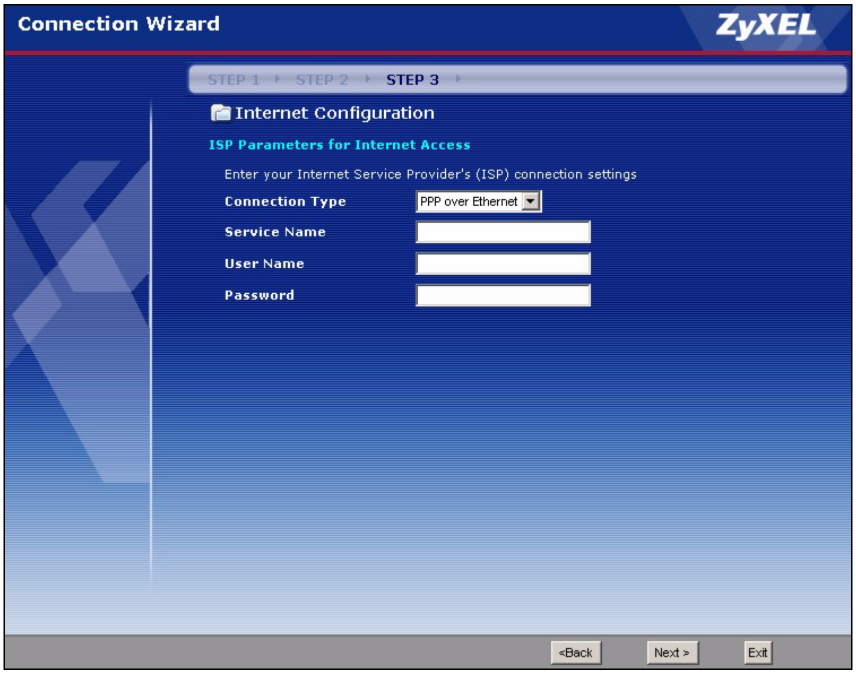
One of the benefits of PPPoE is the ability to let end users access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for specific users.

Operationally, PPPoE saves significant effort for both the subscriber and the ISP/carrier, as it requires no specific configuration of the broadband modem at the subscriber’s site.

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

Refer to the appendix for more information on PPPoE.

Figure 21 PPPoE Connection Type



Enter your Internet Service Provider's (ISP) connection settings

Connection Type: PPP over Ethernet

The following table describes the labels in this screen.

Table 14 PPPoE Connection Type

LABEL	DESCRIPTION
ISP Parameter for Internet Access	
Service Name	Type the name of your service provider.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Next	Click **Next** to continue.
Back	Click **Back** to return to the previous screen.
Exit	Click **Exit** to close the wizard screen without saving.

3.4.3 PPTP Connection Type

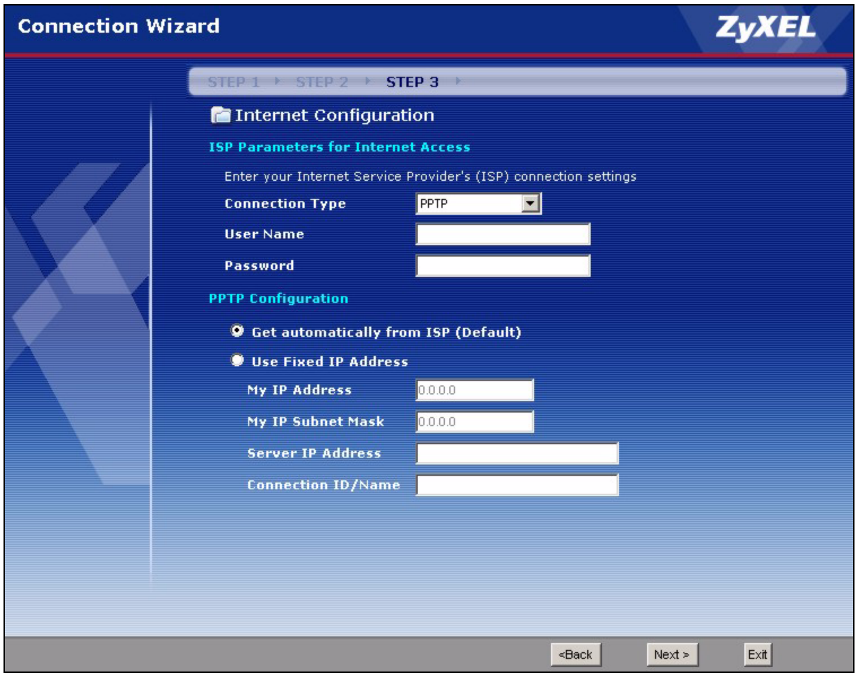
Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables transfers of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.

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

Refer to the appendix for more information on PPTP.

Note: The Prestige supports one PPTP server connection at any given time.

Figure 22 PPTP Connection Type



Connection Wizard

STEP 1 ▸ STEP 2 ▸ STEP 3 ▸

Internet Configuration

ISP Parameters for Internet Access

Enter your Internet Service Provider's (ISP) connection settings

Connection Type: PPTP

User Name:

Password:

PPTP Configuration

● Get automatically from ISP (Default)

○ Use Fixed IP Address

My IP Address: 0.0.0.0

My IP Subnet Mask: 0.0.0.0

Server IP Address:

Connection ID/Name:

The following table describes the fields in this screen

Table 15 PPTP Connection Type

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.
PPTP Configuration	
Get automatically from ISP	Select this radio button if your ISP did not assign you a fixed IP address.
Use fixed IP address	Select this radio button, provided by your ISP to give the Prestige a fixed, unique IP address.
My IP Address	Type the (static) IP address assigned to you by your ISP.

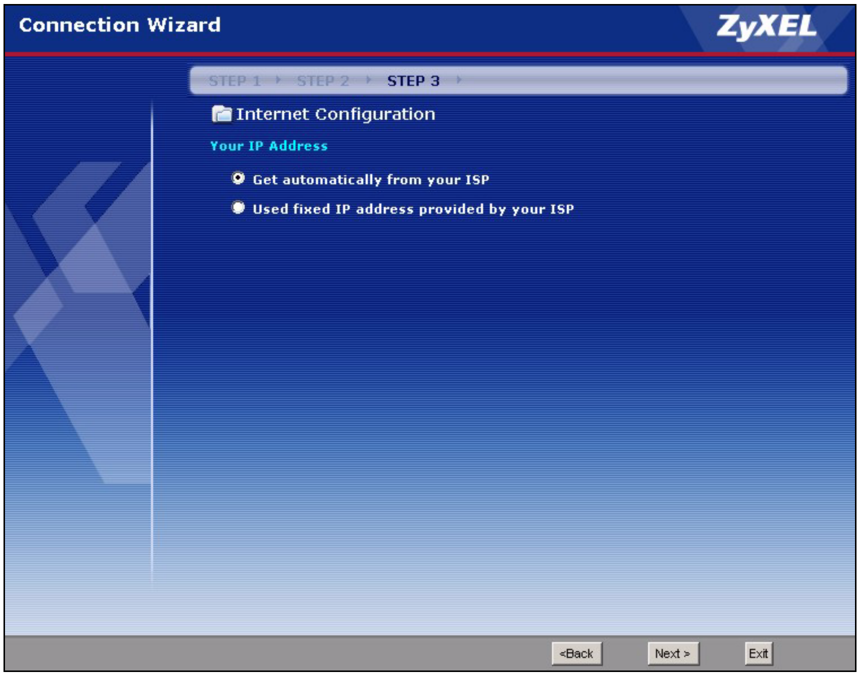
Table 15 PPTP Connection Type

LABEL	DESCRIPTION
My IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).
Server IP Address	Type the IP address of the PPTP server.
Connection ID/ Name	Enter the connection ID or connection name in this field. It must follow the "c:id" and "n:name" format. For example, C:12 or N:My ISP. This field is optional and depends on the requirements of your ISP.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.
Exit	Click **Exit** to close the wizard screen without saving.

3.4.4 Your IP Address

The following wizard screen allows you to assign a fixed IP address or give the Prestige an automatically assigned IP address depending on your ISP.

Figure 23 Your IP Address



Connection Wizard

Internet Configuration

Your IP Address

● Get automatically from your ISP

○ Used fixed IP address provided by your ISP

The following table describes the labels in this screen

Table 16 Your IP Address

LABEL	DESCRIPTION
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 provided by your ISP	Select this option If the ISP assigned a fixed IP address. The fixed IP address should be in the same subnet as your broadband modem or router.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.
Exit	Click **Exit** to close the wizard screen without saving.

3.4.5 WAN MAC Address

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.

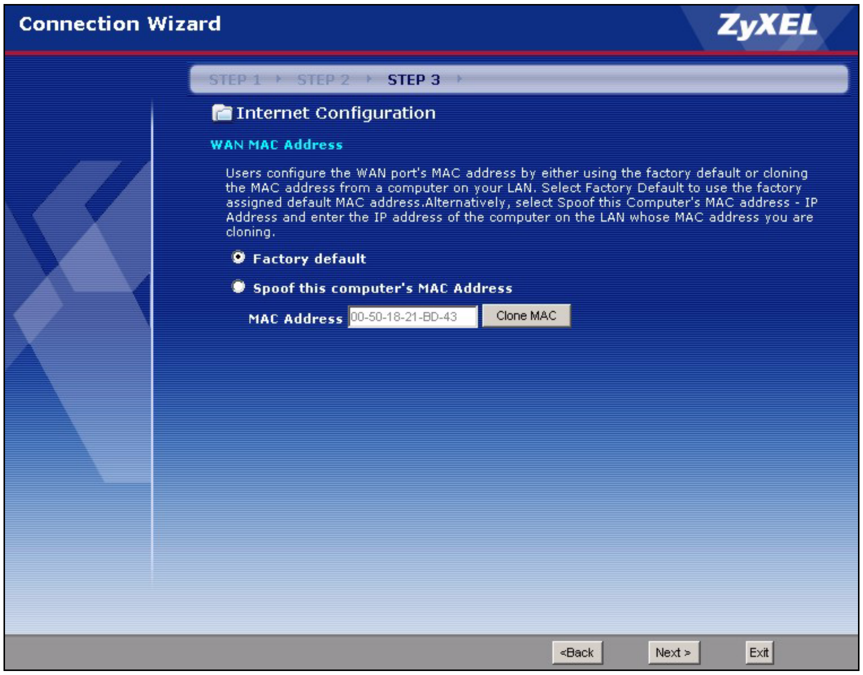
You can configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Once it is successfully configured, the address will be copied to the "rom" file (ZyNOS configuration file). It will not change unless you change the setting or upload a different "rom" file.

Table 17 Example of Network Properties for LAN Servers with Fixed IP Addresses

Choose an IP address	192.168.1.2-192.168.1.32; 192.168.1.65-192.168.1.254.
Subnet mask	255.255.255.0
Gateway (or default route)	192.168.1.1(Prestige LAN IP)

This screen allows users to configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN.

Figure 24 WAN MAC Address



WAN MAC Address

Users configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Select Factory Default to use the factory assigned default MAC address.Alternatively, select Spoof this Computer's MAC address - IP Address and enter the IP address of the computer on the LAN whose MAC address you are cloning.

● Factory default

○ Spoof this computer's MAC Address

MAC Address 00-50-18-21-BD-43

The following table describes the fields in this screen.

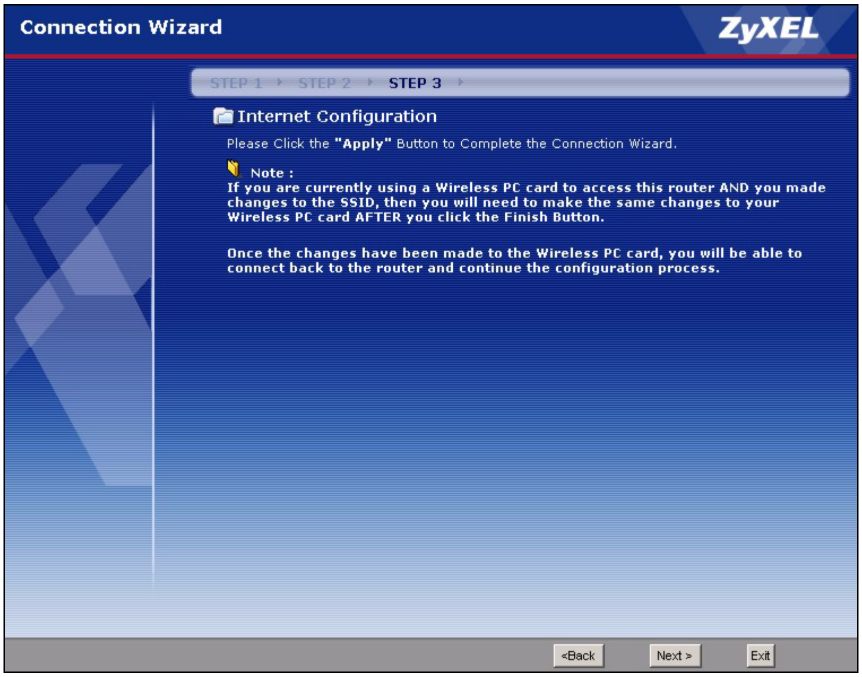
Table 18 WAN MAC Address

LABEL	DESCRIPTION
Factory Default	Select **Factory Default** to use the factory assigned default MAC address.
Spoof this computer's MAC address	Select this option and click **Clone MAC** to clone the MAC address in the **MAC Address** field. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file. It is advisable to clone the MAC address from a computer on your LAN even if your ISP does not presently require MAC address authentication.
MAC Address	Enter the MAC address of the computer on the LAN whose MAC address you want to clone.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.
Exit	Click **Exit** to close the wizard screen without saving.

3.4.6 Connection Wizard Complete

Follow the on-screen instructions and click **Next**.

Figure 25 Connection Wizard Complete



Internet Configuration

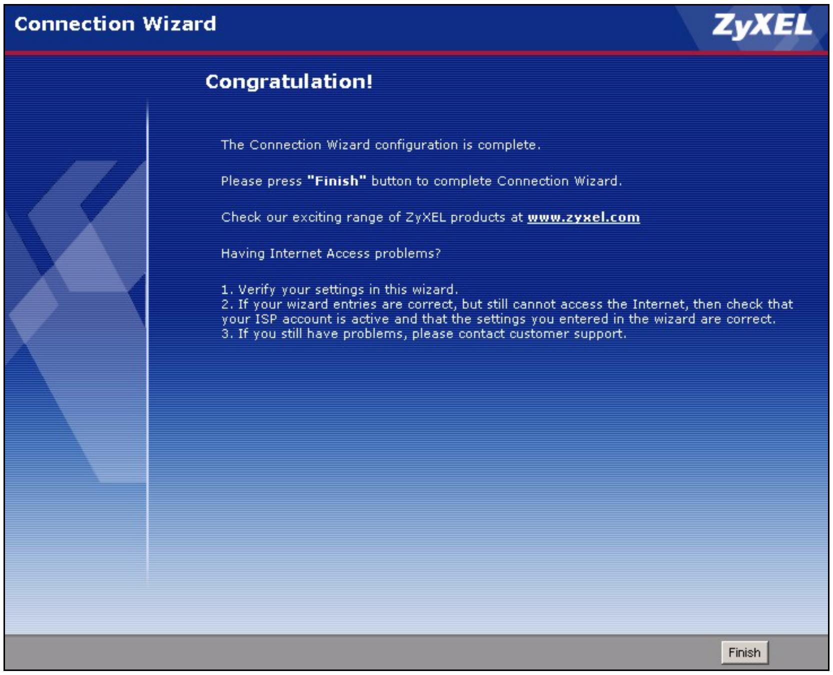
Please Click the **"Apply"** Button to Complete the Connection Wizard.

Note :
If you are currently using a Wireless PC card to access this router AND you made changes to the SSID, then you will need to make the same changes to your Wireless PC card AFTER you click the Finish Button.

Once the changes have been made to the Wireless PC card, you will be able to connect back to the router and continue the configuration process.

Click **Finish** to complete the wizard setup and save your configuration.

Figure 26 Connection Wizard: Congratulation



Congratulation!

The Connection Wizard configuration is complete.

Please press **"Finish"** button to complete Connection Wizard.

Check our exciting range of ZyXEL products at www.zyxel.com

Having Internet Access problems?

1. Verify your settings in this wizard.
2. If your wizard entries are correct, but still cannot access the Internet, then check that your ISP account is active and that the settings you entered in the wizard are correct.
3. If you still have problems, please contact customer support.

Well done! You have successfully set up your Prestige to operate on your network and access the Internet.

CHAPTER 4 Wireless LAN

This chapter discusses how to configure Wireless LAN.

4.1 Introduction

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

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

4.2 Wireless Security Overview

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

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

4.2.1 Encryption

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

4.2.2 Authentication

WPA has user authentication and you can also configure IEEE 802.1x to use a RADIUS server to authenticate wireless clients before joining your network.

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

4.2.3 Restricted Access

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

4.2.4 Hide Prestige Identity

If you hide the ESSID, then the Prestige cannot be seen when a wireless client scans for local APs. The trade-off for the extra security of "hiding" the Prestige may be inconvenient for some valid WLAN clients.

4.2.5 Using OTIST

In a wireless network, the wireless clients must have the same SSID and security settings as the access point (AP) or wireless router (we will refer to both as "AP" here) in order to associate with it. Traditionally this meant that you had to configure the settings on the AP and then manually configure the exact same settings on each wireless client.

OTIST (One-Touch Intelligent Security Technology) allows you to transfer your AP's SSID and WEP or WPA-PSK security settings to wireless clients that support OTIST and are within transmission range. You can also choose to have OTIST generate a WPA-PSK key for you if you didn't configure one manually.

Note: OTIST replaces the pre-configured wireless settings on the wireless clients.

4.3 Configuring Wireless LAN on the Prestige

1. Configure the **SSID** and **Security Mode** in the **Wireless** screen. If you configure **WEP**, you can't configure **WPA** or **WPA-PSK**.
2. Use the **MAC Filter** screen to restrict access to your wireless network by MAC address.
3. If you have OTIST-enabled clients, configure **OTIST** in the **OTIST** screen. **OTIST** transfers device SSID and WEP or WPA-PSK key settings (if enabled) to wireless clients.

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

Table 19 ZyAIR Wireless Security Levels

Security Level	Security Type
Least Secure	Unique SSID (Default)
	Unique SSID with Hide SSID Enabled
	MAC Address Filtering
	WEP Encryption
	IEEE802.1x EAP with RADIUS Server Authentication
Most Secure	Wi-Fi Protected Access (WPA)

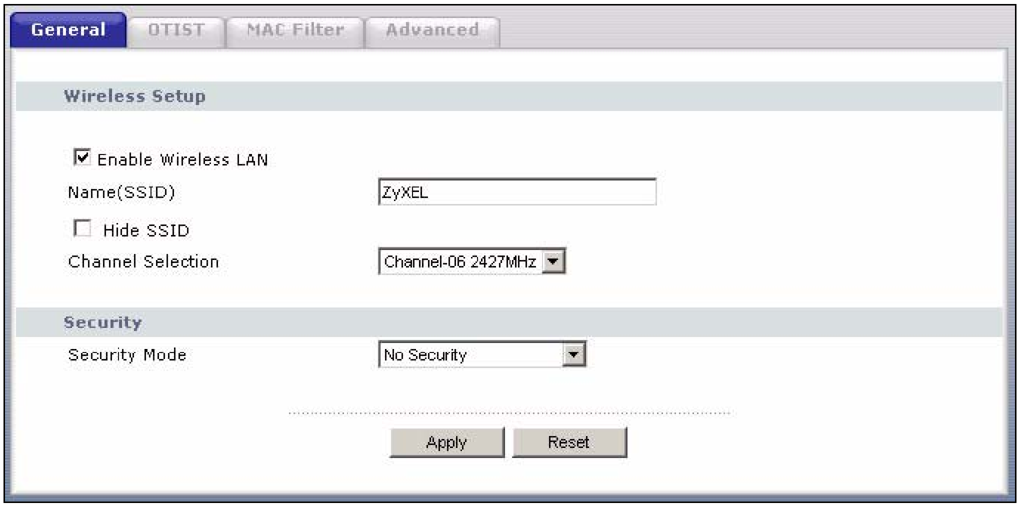
Note: You must enable the same wireless security settings on the Prestige and on all wireless clients that you want to associate with it.

4.4 General Wireless LAN Screen

Note: If you are configuring the Prestige from a computer connected to the wireless LAN and you change the Prestige’s SSID 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 Prestige’s new settings.

Click the **Wireless LAN** link under **Network** to open the **General** screen.

Figure 27 Wireless: General



Wireless Setup

☑ Enable Wireless LAN

Name(SSID): ZyXEL

□ Hide SSID

Channel Selection: Channel-06 2427MHz

Security

Security Mode: No Security

The following table describes the general wireless LAN labels in this screen.

Table 20 Wireless: General

LABEL	DESCRIPTION
Enable Wireless LAN	Click the check box to activate wireless LAN.
Name(SSID)	(Service Set IDentity) The SSID identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. **Note:** If you are configuring the Prestige from a computer connected to the wireless LAN and you change the Prestige's SSID 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 Prestige's new settings.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through passive scanning using a site survey tool.
Channel Selection	Set the operating frequency/channel depending on your particular region. Select a channel from the drop-down list box. Refer to the Connection Wizard chapter for more information on channels.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to reload the previous configuration for this screen.

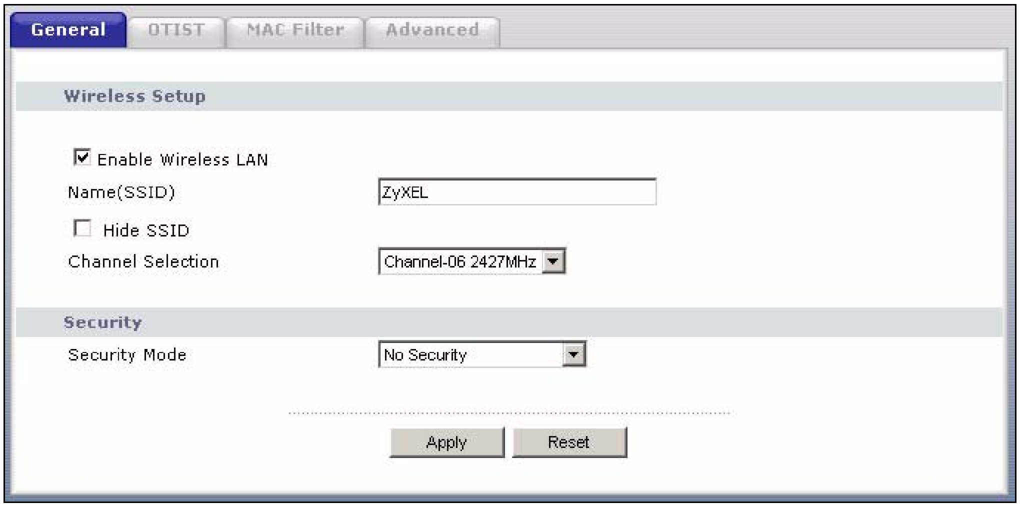
See the rest of this chapter for information on the other labels in this screen.

4.4.1 No Security

Select **No Security** to allow wireless stations to communicate with the access points without any data encryption.

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

Figure 28   Wireless: No Security



Wireless Setup

☑ Enable Wireless LAN

Name(SSID) ZyXEL

☐ Hide SSID

Channel Selection Channel-06 2427MHz

Security

Security Mode No Security

The following table describes the labels in this screen.

Table 21   Wireless No Security

LABEL	DESCRIPTION
Security Mode	Choose **No Security** from the drop-down list box.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to reload the previous configuration for this screen.

4.4.2 WEP Encryption

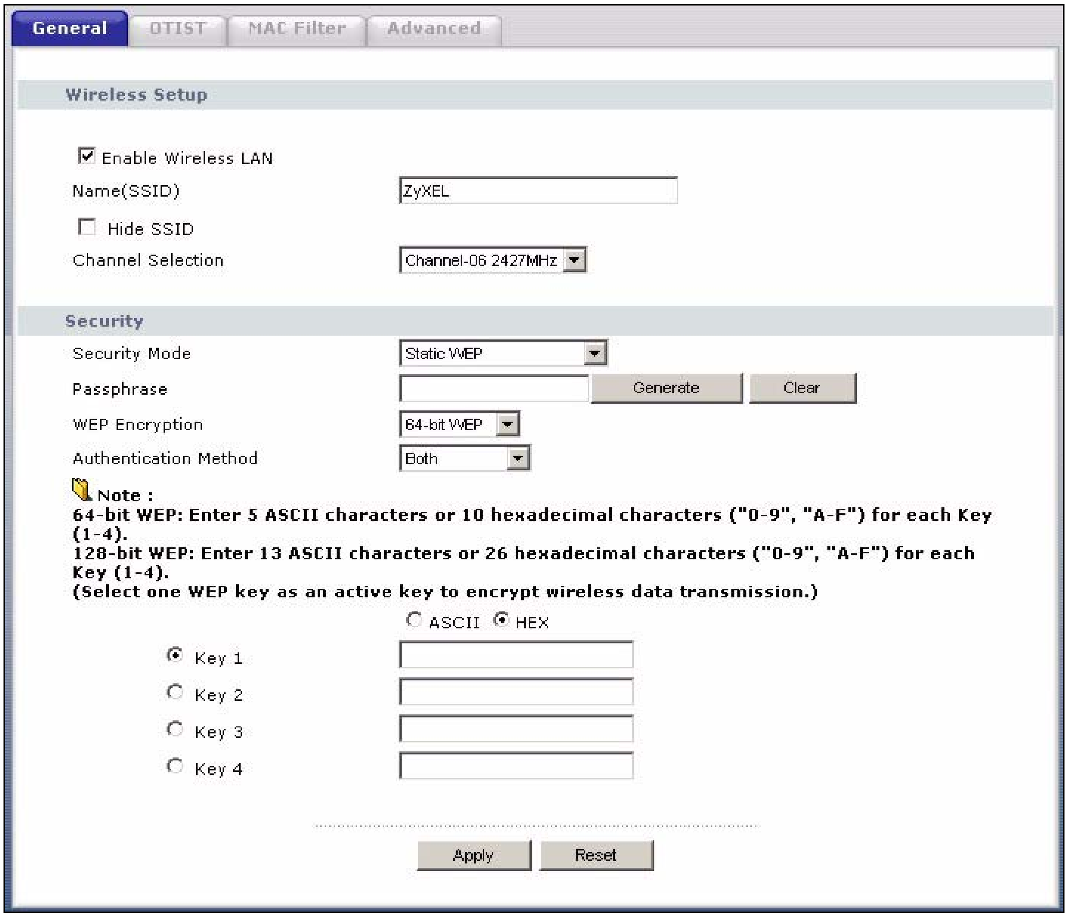
WEP encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private. It encrypts unicast and multicast communications in a network. Both the wireless stations and the access points must use the same WEP key.

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

In order to configure and enable WEP encryption; click **Wireless LAN** and **Wireless** to display the **General** screen.

Select **Static WEP** from the **Security Mode** list.

Figure 29 Wireless: Static WEP Encryption



Wireless Setup

☑ Enable Wireless LAN

Name(SSID): ZyXEL

□ Hide SSID

Channel Selection: Channel-06 2427MHz

Security

Security Mode: Static WEP

Passphrase: [ ] Generate Clear

WEP Encryption: 64-bit WEP

Authentication Method: Both

Note :
64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F") for each Key (1-4).
128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F") for each Key (1-4).
(Select one WEP key as an active key to encrypt wireless data transmission.)

○ ASCII ● HEX

● Key 1

○ Key 2

○ Key 3

○ Key 4

Apply Reset

The following table describes the wireless LAN security labels in this screen.

Table 22 Wireless: Static WEP Encryption

LABEL	DESCRIPTION
Passphrase	Enter a Passphrase (up to 32 printable characters) and clicking **Generate**. The Prestige automatically generates four different WEP keys.
Generate	After you enter the passphrase, click **Generate** to have the Prestige generates four different WEP keys automatically.
Clear	Click **Clear** to discard the passphrase you configured in the **Passphrase** field and the WEP key(s) generated automatically or maually configured.
WEP Encryption	Select **64-bit WEP** or **128-bit WEP** to enable data encryption.
Authentication Method	Select **Auto**, **Open System** or **Shared Key** from the drop-down list box.
ASCII	Select this option in order to enter ASCII characters as the WEP key.
Hex	Select this option in order to enter hexadecimal characters as a WEP key. The preceding "0x", that identifies a hexadecimal key, is entered automatically.

Table 22 Wireless: Static WEP Encryption

LABEL	DESCRIPTION
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the Prestige and the wireless stations must use the same WEP key for data transmission. If you chose **64-bit WEP**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit WEP**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). You must configure at least one key, only one key can be activated at any one time. The default key is key 1.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to reload the previous configuration for this screen.

4.4.3 Introduction to WPA

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

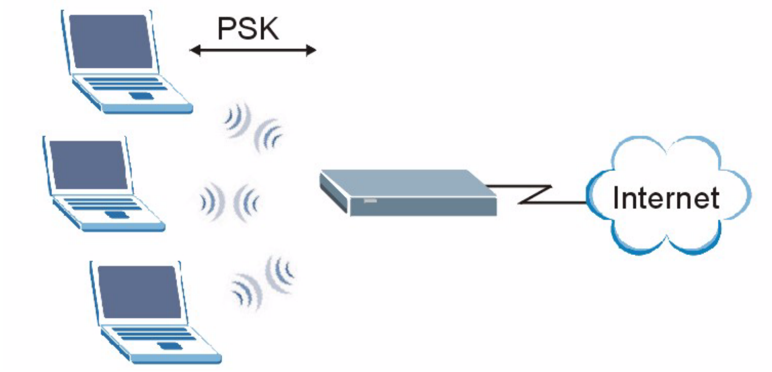
If both an AP and the wireless clients support WPA and you have an external RADIUS server, use WPA for stronger data encryption. If you don't have an external RADIUS server, you should use WPA-PSK (WPA-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

4.4.4 WPA-PSK Application Example

A WPA-PSK application looks as follows.

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

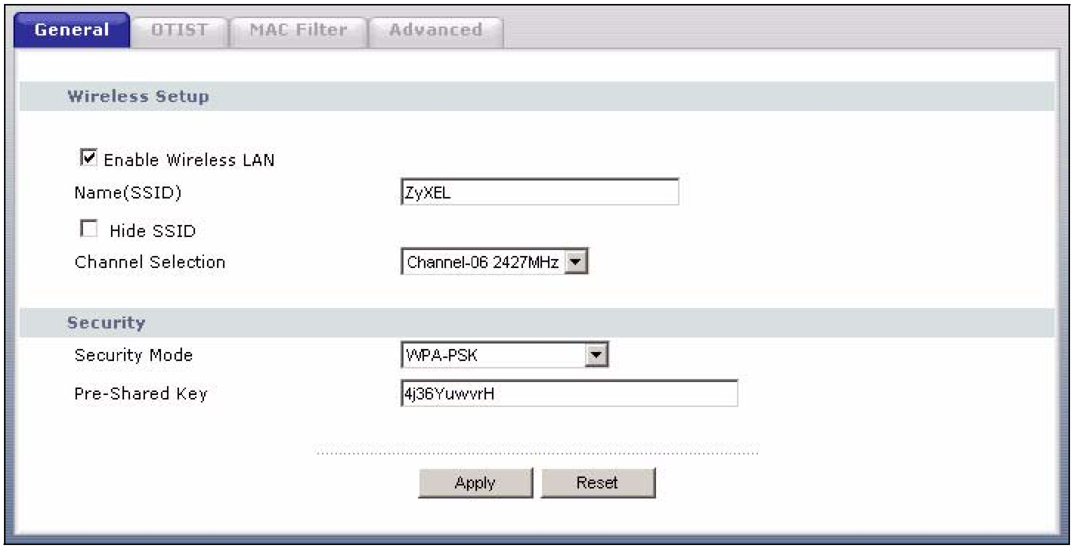
Figure 30 WPA-PSK Authentication



4.4.5 WPA-PSK Authentication Screen

In order to configure and enable WPA-PSK Authentication; click the **Wireless LAN** link under **Network** to display the **General** screen. Select **WPA-PSK** from the **Security Mode** list.

Figure 31 Wireless: WPA-PSK



Wireless Setup

☑ Enable Wireless LAN

Name(SSID): ZyXEL

□ Hide SSID

Channel Selection: Channel-06 2427MHz

Security

Security Mode: WPA-PSK

Pre-Shared Key: 4j36YuwvrH

The following table describes the labels in this screen.

Table 23 Wireless: WPA-PSK

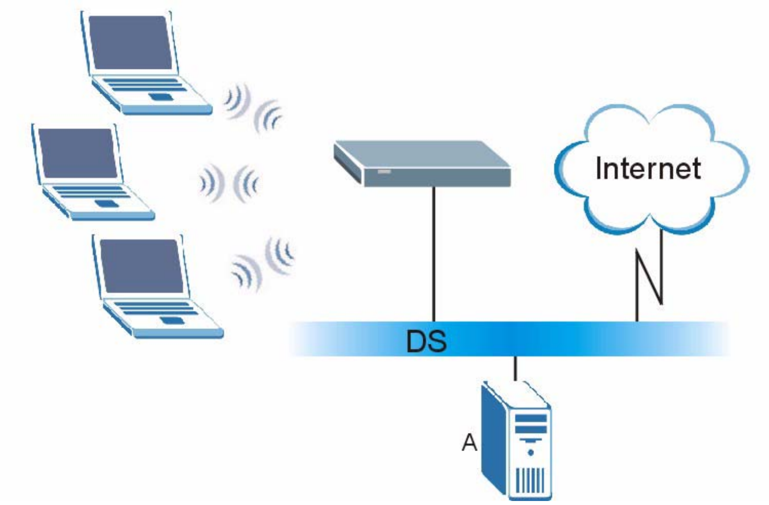
LABEL	DESCRIPTION
Pre-Shared Key	The encryption mechanisms used for **WPA** and **WPA-PSK** are the same. The only difference between the two is that **WPA-PSK** uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to reload the previous configuration for this screen.

4.4.6 WPA with RADIUS Application Example

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

1. The AP passes the wireless client's authentication request to the RADIUS server.
2. The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
3. The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Figure 32 WPA with RADIUS Application Example



4.4.7 Wireless Client WPA Supplicants

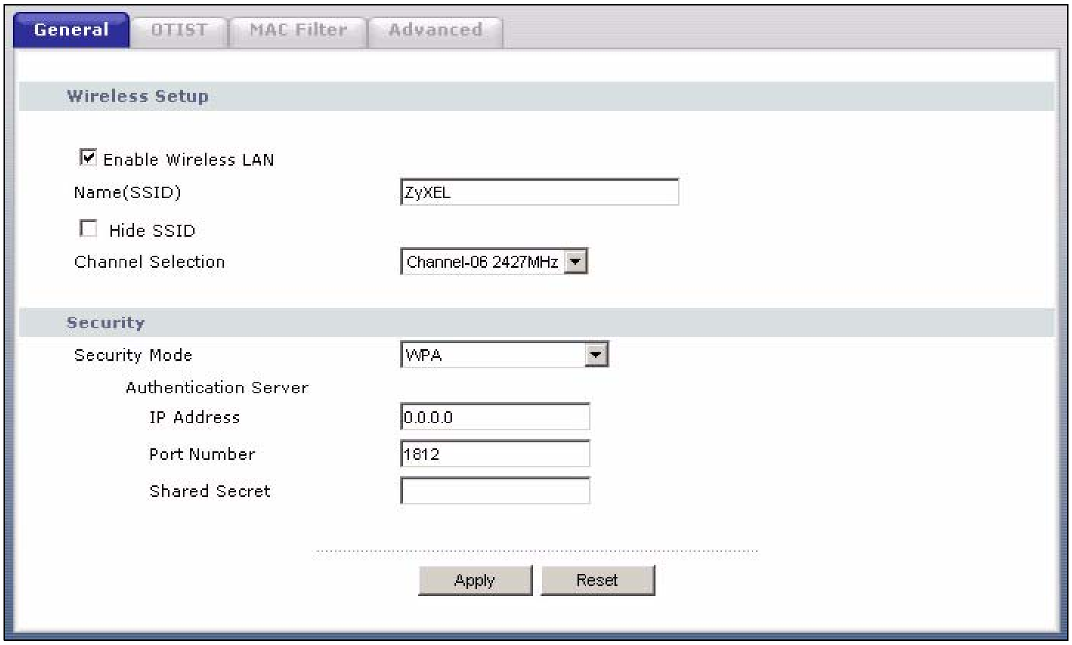
A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client.

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

4.4.8 WPA Authentication Screen

In order to configure and enable WPA Authentication; click the **Wireless LAN** link under **Network** to display the **General** screen. Select **WPA** from the **Security Mode** list.

Figure 33 Wireless: WPA



Wireless Setup

☑ Enable Wireless LAN

Name(SSID): ZyXEL

□ Hide SSID

Channel Selection: Channel-06 2427MHz

Security

Security Mode: WPA

Authentication Server

IP Address: 0.0.0.0

Port Number: 1812

Shared Secret:

The following table describes the labels in this screen.

Table 24 Wireless: WPA

LABEL	DESCRIPTION
Authentication Server	
IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. The default port number is **1812**. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the Prestige. The key must be the same on the external authentication server and your Prestige. The key is not sent over the network.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to reload the previous configuration for this screen.

4.4.9 IEEE 802.1x Overview

You need the following for IEEE 802.1x authentication.

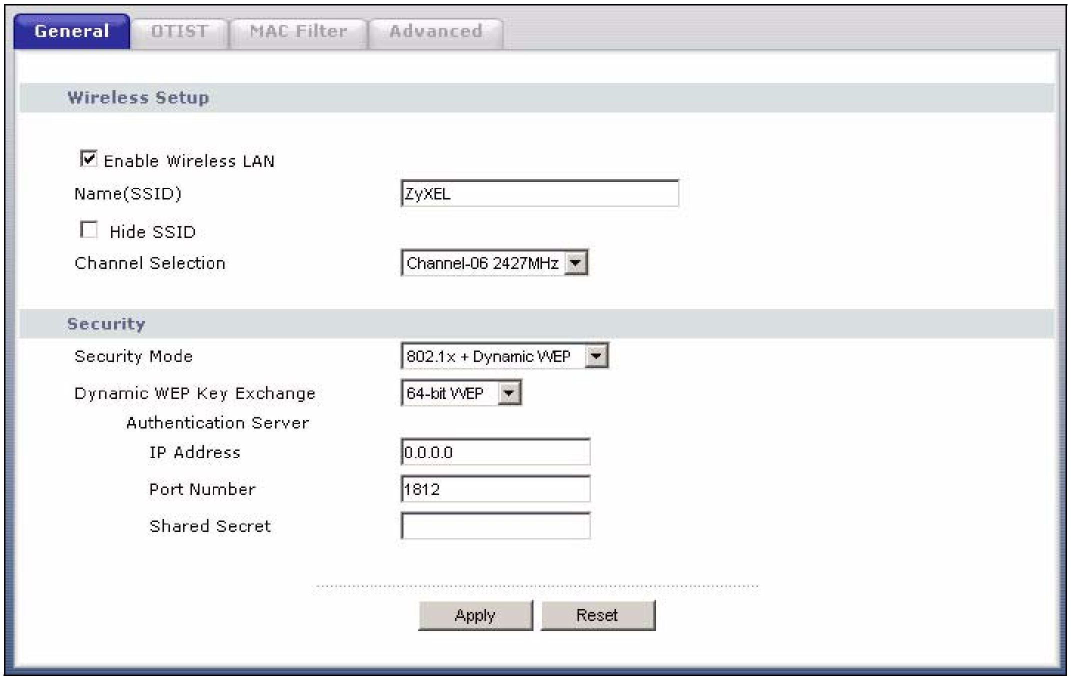
- A computer with an IEEE 802.11 a/b/g wireless LAN adapter and equipped with a web browser (with JavaScript enabled) and/or Telnet.

- A wireless station computer must be running IEEE 802.1x-compliant software. Not all Windows operating systems support IEEE 802.1x (see the Microsoft web site for details). For other operating systems, see their documentation. If your operating system does not support IEEE 802.1x, then you may need to install IEEE 802.1x client software.
- An optional network RADIUS server for remote user authentication and accounting.

4.4.10 IEEE 802.1x and Dynamic WEP Key Exchange Screen

In order to configure and enable 802.1x and dynamic WEP key exchange; click the **Wireless LAN** link under **Network** to display the **General** screen. Select **802.1x + Dynamic WEP** from the **Security Mode** list.

Figure 34 Wireless: 802.1x and Dynamic WEP



☑ Enable Wireless LAN

Name(SSID): ZyXEL

□ Hide SSID

Channel Selection: Channel-06 2427MHz

Security Mode: 802.1x + Dynamic WEP

Dynamic WEP Key Exchange: 64-bit WEP

Authentication Server

IP Address: 0.0.0.0

Port Number: 1812

Shared Secret:

The following table describes the labels in this screen.

Table 25 Wireless: 802.1x and Dynamic WEP

LABEL	DESCRIPTION
Dynamic WEP Key Exchange	Select **64-bit WEP** or **128-bit WEP** to enable data encryption. Up to 32 stations can access the Prestige when you configure dynamic WEP key exchange.
Authentication Server	
IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. The default port number is **1812**. You need not change this value unless your network administrator instructs you to do so with additional information.

Table 25 Wireless: 802.1x and Dynamic WEP

LABEL	DESCRIPTION
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the Prestige. The key must be the same on the external authentication server and your Prestige. The key is not sent over the network.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to reload the previous configuration for this screen.

4.5 OTIST

OTIST (One-Touch Intelligent Security Technology) allows your Prestige to set the wireless client to use the same wireless settings as the Prestige.

Note: The wireless client must support OTIST and have OTIST enabled.

The following are the wireless settings that the Prestige assigns to the wireless client if OTIST is enabled on both devices and the OTIST setup keys are the same.

- SSID
- Security (WEP or WPA-PSK)

Note: This will replace the pre-configured wireless settings on the wireless clients.

4.5.1 Enabling OTIST

You must enable OTIST on both the AP and wireless client before you start transferring settings.

Note: The AP and wireless client(s) MUST use the same **Setup key**.

4.5.1.1 AP

You can enable OTIST using the Reset button or the web configurator.

4.5.1.1.1 Reset button

If you use the **Reset** button, the default (01234567) or previous saved (through the web configurator) **Setup key** is used to encrypt the settings that you want to transfer.

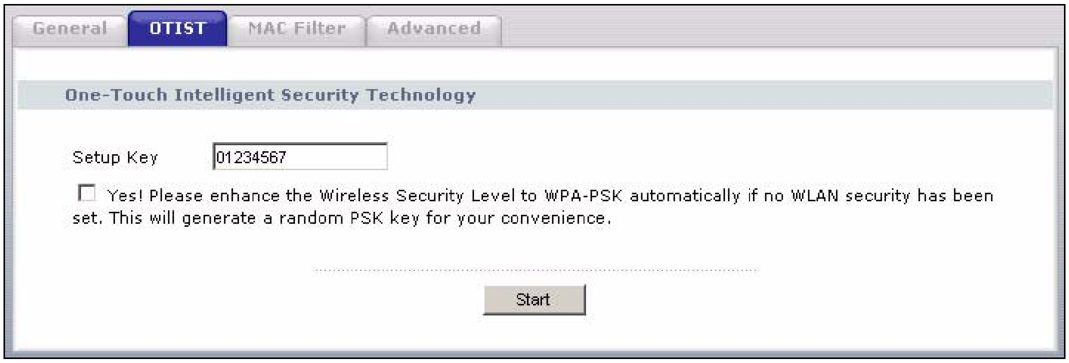
Hold in the **Reset** button for one or two seconds.

Note: If you hold in the **Reset** button too long, the device will reset to the factory defaults!

4.5.1.1.2 Web Configurator

Click the **Wireless LAN** link under **Network** and then the **OTIST** tab. The following screen displays.

Figure 35 Wireless: OTIST



One-Touch Intelligent Security Technology

Setup Key 01234567

□ Yes! Please enhance the Wireless Security Level to WPA-PSK automatically if no WLAN security has been set. This will generate a random PSK key for your convenience.

The following table describes the labels in this screen.

Table 26 Wireless: OTIST

LABEL	DESCRIPTION
Setup Key	Type an OTIST **Setup Key** of exactly eight ASCII characters in length. The default OTIST setup key is "01234567". **Note:** If you change the OTIST setup key here, you must also make the same change on the wireless client(s).

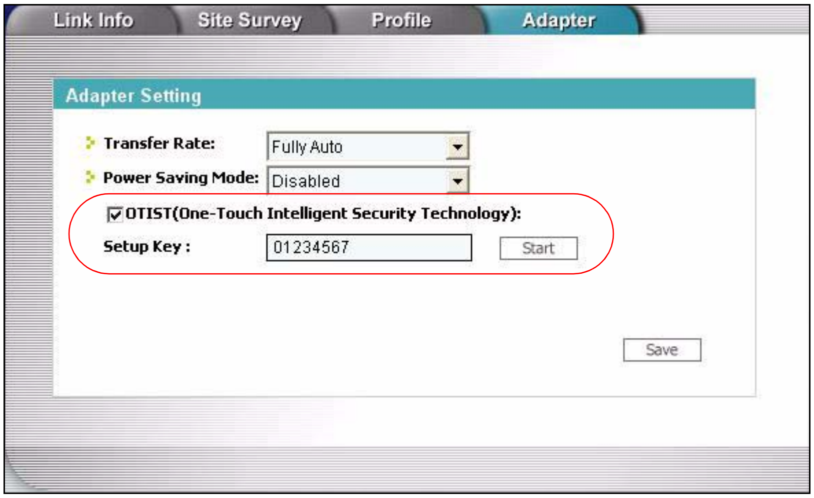
Table 26 Wireless: OTIST

LABEL	DESCRIPTION
Yes!	To have OTIST automatically generate a WPA-PSK key, select this check box. If you manually configured a WEP key or a WPA-PSK key and you also select this check box, then the key you manually configured is used. If you want to configure your own WPA-PSK and have OTIST use that WPA-PSK, you must: • Configure a WPA-PSK in the **Wireless General** screen. • Clear the **Yes!** checkbox in the **OTIST** screen and click **Apply**. **Note:** If you already have a WPA-PSK configured in the **Wireless General** screen, and you run OTIST with **Yes!** selected, OTIST will not replace the WPA-PSK. Clear the checkbox in the OTIST screen. If you want OTIST to automatically generate a WPA-PSK, you must: • Change your security to **No Security** in the **Wireless General** screen. • Select the the **Yes!** checkbox in the **OTIST** screen and click **Apply**. • The **Wireless General** screen displays an auto generated WPA-PSK and is now in WPA-PSK security mode. The WPA-PSK security settings are assigned to the wireless client when you start OTIST.
Start	Click **Start** to encrypt the wireless security data using the setup key and have the Prestige set the wireless station to use the same wireless settings as the Prestige. You must also activate and start OTIST on the wireless station at the same time. The process takes three minutes to complete.

4.5.1.2 Wireless Client

Start the ZyXEL utility and click the **Adapter** tab. Select the **OTIST** check box, enter the same **Setup Key** as your AP's and click **Save**.

Figure 36 Example Wireless Client OTIST Screen



Transfer Rate: Fully Auto

Power Saving Mode: Disabled

☑ OTIST(One-Touch Intelligent Security Technology):

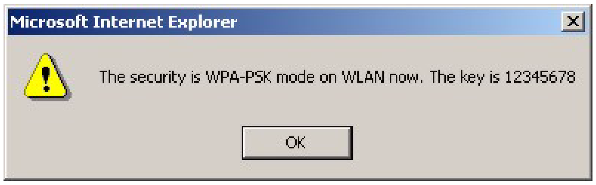
Setup Key : 01234567

4.5.2 Starting OTIST

Note: You must click **Start** in the AP **OTIST** web configurator screen and in the wireless client(s) **Adapter** screen all within three minutes (at the time of writing). You can start OTIST in the wireless clients and AP in any order but they must all be within range and have OTIST enabled.

1 In the AP, a web configurator screen pops up showing you the security settings to transfer. After reviewing the settings, click **OK**.

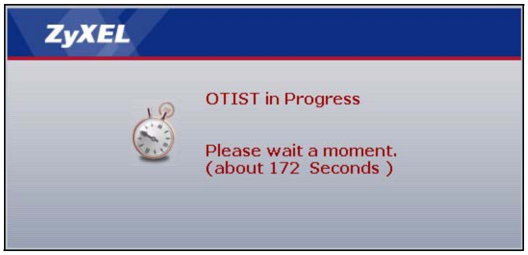
Figure 37 Security Key


Microsoft Internet Explorer

The security is WPA-PSK mode on WLAN now. The key is 12345678

2 This screen appears while OTIST settings are being transferred. It closes when the transfer is complete.

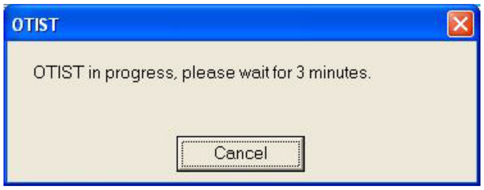
Figure 38 OTIST in Progress (AP)



OTIST in Progress

Please wait a moment.
(about 172 Seconds)

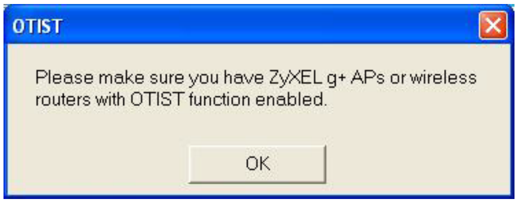
Figure 39 OTIST in Progress (Client)


OTIST

OTIST in progress, please wait for 3 minutes.

- In the wireless client, you see this screen if it can't find an OTIST-enabled AP (with the same **Setup key**). Click **OK** to go back to the ZyXEL utility main screen.

Figure 40 No AP with OTIST Found


OTIST

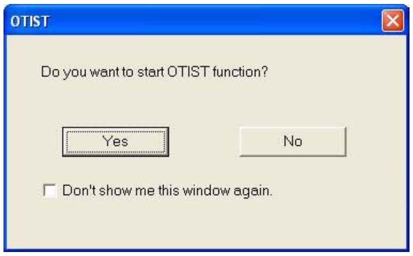
Please make sure you have ZyXEL g+ APs or wireless routers with OTIST function enabled.

- If there is more than one OTIST-enabled AP within range, you see a screen asking you to select one AP to get settings from.

4.5.3 Notes on OTIST

1 If you enabled OTIST in the wireless client, you see this screen each time you start the utility. Click **Yes** for it to search for an OTIST-enabled AP.

Figure 41 Start OTIST?



OTIST

Do you want to start OTIST function?

□ Don't show me this window again.

2 If an OTIST-enabled wireless client loses its wireless connection for more than ten seconds, it will search for an OTIST-enabled AP for up to one minute. (If you manually have the wireless client search for an OTIST-enabled AP, there is no timeout; click **Cancel** in the OTIST progress screen to stop the search.)

3 When the wireless client finds an OTIST-enabled AP, you must still click **Start** in the AP **OTIST** web configurator screen or hold in the **Reset** button (for one or two seconds) for the AP to transfer settings.

4 If you change the SSID or the keys on the AP after using OTIST, you need to run OTIST again or enter them manually in the wireless client(s).

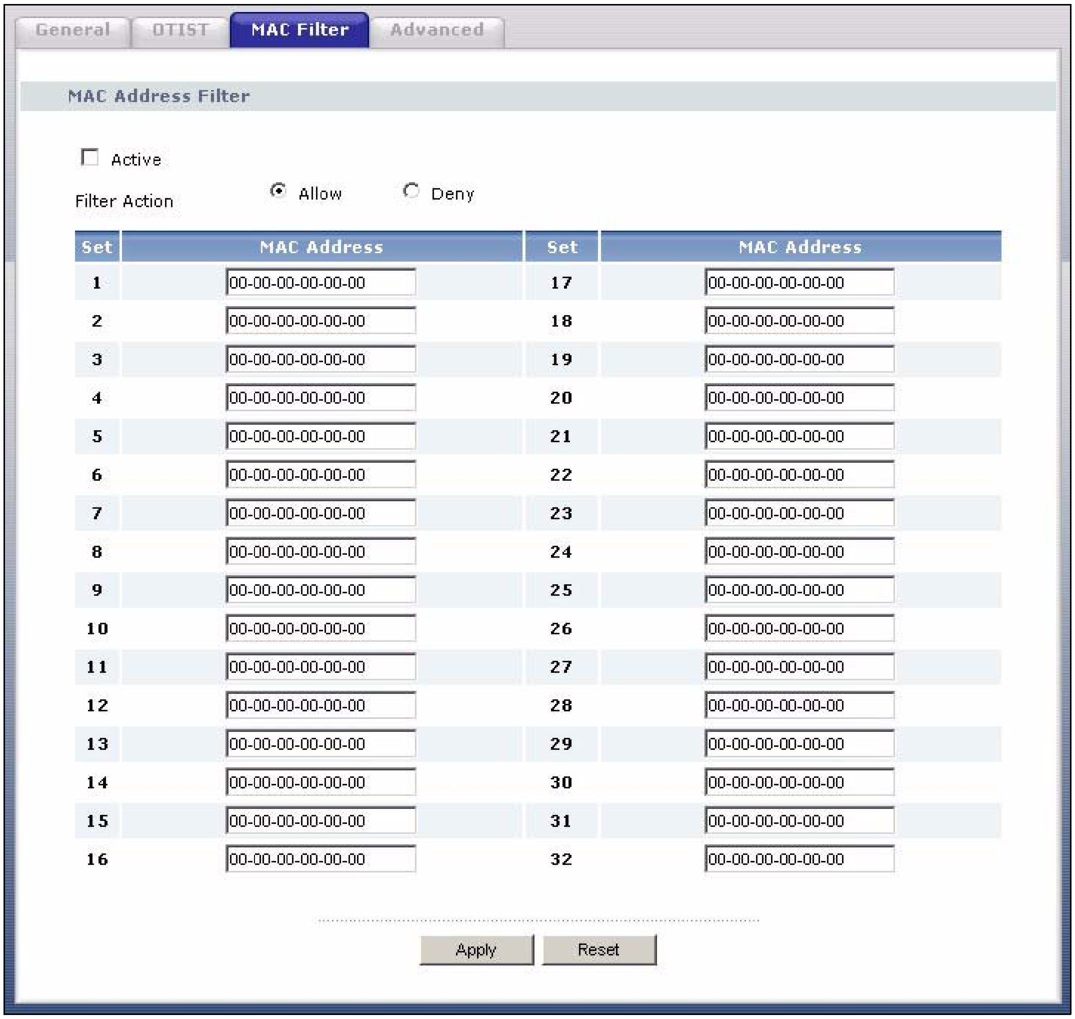
5 If you configure OTIST to generate a WPA-PSK key, this key changes each time you run OTIST. Therefore, if a new wireless client joins your wireless network, you need to run OTIST on the AP and ALL wireless clients again.

4.6 MAC Filter

The MAC filter screen allows you to configure the Prestige to give exclusive access to up to 32 devices (**Allow**) or exclude up to 32 devices from accessing the Prestige (**Deny**). 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.

To change your Prestige's MAC filter settings, click the **Wireless LAN** link under **Network** and then the **MAC Filter** tab. The screen appears as shown.

Figure 42 Wireless: MAC Address Filter



MAC Address Filter

□ Active

Filter Action ● Allow ○ Deny

Set	MAC Address	Set	MAC Address
1	00-00-00-00-00-00	17	00-00-00-00-00-00
2	00-00-00-00-00-00	18	00-00-00-00-00-00
3	00-00-00-00-00-00	19	00-00-00-00-00-00
4	00-00-00-00-00-00	20	00-00-00-00-00-00
5	00-00-00-00-00-00	21	00-00-00-00-00-00
6	00-00-00-00-00-00	22	00-00-00-00-00-00
7	00-00-00-00-00-00	23	00-00-00-00-00-00
8	00-00-00-00-00-00	24	00-00-00-00-00-00
9	00-00-00-00-00-00	25	00-00-00-00-00-00
10	00-00-00-00-00-00	26	00-00-00-00-00-00
11	00-00-00-00-00-00	27	00-00-00-00-00-00
12	00-00-00-00-00-00	28	00-00-00-00-00-00
13	00-00-00-00-00-00	29	00-00-00-00-00-00
14	00-00-00-00-00-00	30	00-00-00-00-00-00
15	00-00-00-00-00-00	31	00-00-00-00-00-00
16	00-00-00-00-00-00	32	00-00-00-00-00-00

The following table describes the labels in this menu.

Table 27 MAC Address Filter

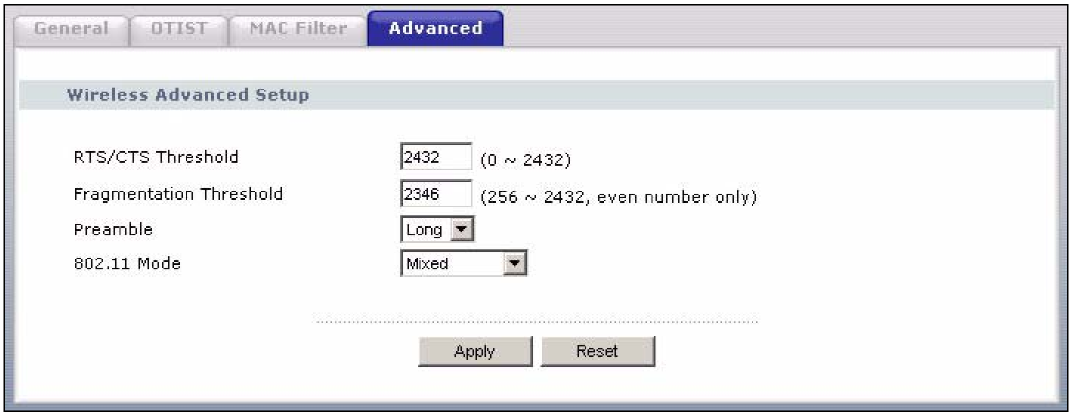
LABEL	DESCRIPTION
Active	Select **Yes** from the drop down list box to enable MAC address filtering.
Filter Action	Define the filter action for the list of MAC addresses in the **MAC Address** table. Select **Deny** to block access to the Prestige, MAC addresses not listed will be allowed to access the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

4.7 Wireless LAN Advanced Screen

See the appendix for background information on roaming.

To enable roaming on your Prestige, click the **Wireless LAN** link under **Network** and then the **Advanced** tab. The screen appears as shown.

Figure 43 Wireless: Advanced



Wireless Advanced Setup

RTS/CTS Threshold 2432 (0 ~ 2432)

Fragmentation Threshold 2346 (256 ~ 2432, even number only)

Preamble Long

802.11 Mode Mixed

The following table describes the labels in this screen.

Table 28 Wireless: Advanced

LABEL	DESCRIPTION
Wireless Advanced Setup	
RTS/CTS Threshold	Enter a value between 0 and 2432.
Fragmentation Threshold	It is the maximum data fragment size that can be sent. Enter a value between 256 and 2432.
Preamble	Preamble is used to signal that data is coming to the receiver. Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11b compliant wireless adapters support long preamble, but not all support short preamble. Select **Long** preamble if you are unsure what preamble mode the wireless adapters support, and to provide more reliable communications in busy wireless networks. Select **Short** preamble if you are sure the wireless adapters support it, and to provide more efficient communications. **Note:** The Prestige and the wireless stations MUST use the same preamble mode in order to communicate.
802.11 Mode	Select **802.11b Only** to allow only IEEE 802.11b compliant WLAN devices to associate with the Prestige. Select **802.11g Only** to allow only IEEE 802.11g compliant WLAN devices to associate with the Prestige. Select **Mixed** to allow either IEEE802.11b or IEEE802.11g compliant WLAN devices to associate with the Prestige. The transmission rate of your Prestige might be reduced.

Table 28 Wireless: Advanced

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to reload the previous configuration for this screen.

CHAPTER 5
WAN

This chapter describes how to configure WAN settings.

5.1 WAN IP Address Assignment

Every computer on the Internet must have a unique IP address. If your networks are isolated from the Internet, for instance, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks.

Table 29 Private IP Address Ranges

10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255

You can obtain your IP address from the IANA, from an ISP or have it assigned by a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Note: Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, Address Allocation for Private Internets and RFC 1466, Guidelines for Management of IP Address Space.

5.2 IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your Prestige, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your Prestige will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the Prestige unless you are instructed to do otherwise.

5.3 DNS Server Address Assignment

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of www.zyxel.com is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

The Prestige can get the DNS server addresses in the following way.

1 The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the DNS Server fields in DHCP Setup.

If the ISP did not give you DNS server information, leave the DNS Server fields in DHCP Setup set to 0.0.0.0 for the ISP to dynamically assign the DNS server IP addresses.

5.4 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 Prestige's routes to the Internet. If the routes have the same metric, the Prestige uses the following pre-defined priorities:

1 **WAN**: designated by the ISP or a static route (see Chapter 10 on page 115)

2 **Traffic Redirect** (see Section 5.9 on page 90)

For example, if **WAN** has a metric of "1" and **Traffic Redirect** has a metric of "2", the **WAN** connection acts as the primary default route. If the **WAN** route fails to connect to the Internet, the Prestige tries **Traffic Redirect** next.

5.5 WAN MAC Address

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 can configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Once it is successfully configured, the address will be copied to the "rom" file (ZyNOS configuration file). It will not change unless you change the setting or upload a different "rom" file.

Table 30 Example of Network Properties for LAN Servers with Fixed IP Addresses

Choose an IP address	192.168.1.2-192.168.1.32; 192.168.1.65-192.168.1.254.
Subnet mask	255.255.255.0
Gateway (or default route)	192.168.1.1(Prestige LAN IP)

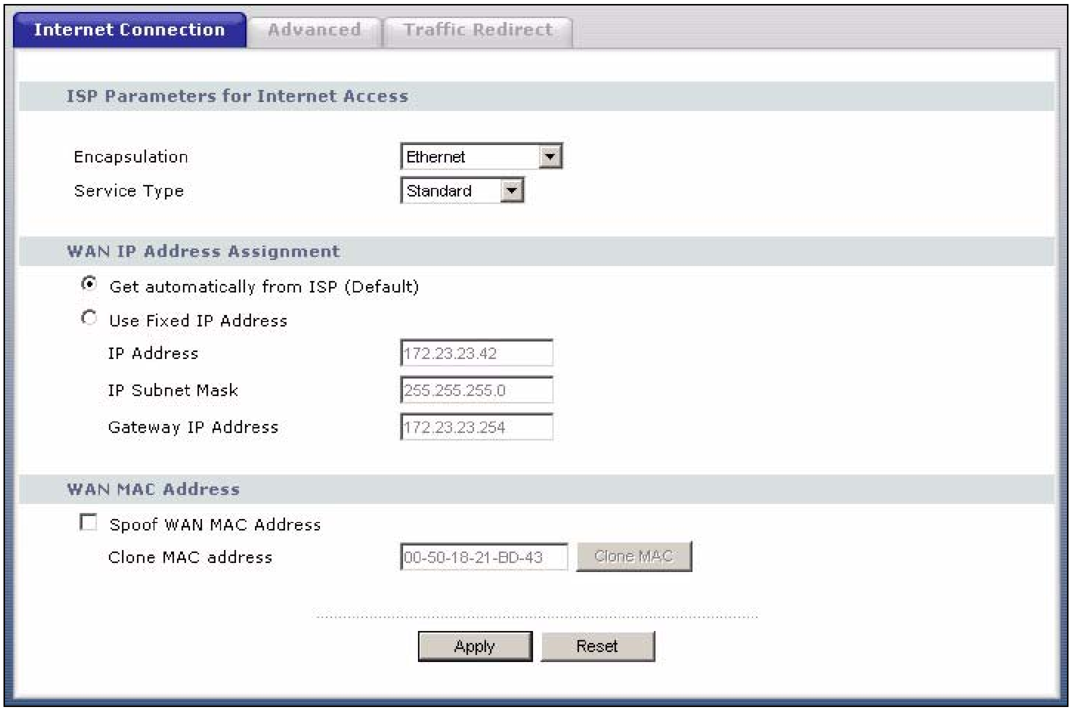
5.6 Internet Connection

To change your Prestige’s WAN ISP, IP and MAC settings, click **WAN** under **Network**. The screen differs by the encapsulation.

5.6.1 Ethernet Encapsulation

The screen shown next is for **Ethernet** encapsulation.

Figure 44   WAN: Ethernet Encapsulation



ISP Parameters for Internet Access

Encapsulation: Ethernet

Service Type: Standard

WAN IP Address Assignment

● Get automatically from ISP (Default)

○ Use Fixed IP Address

IP Address: 172.23.23.42

IP Subnet Mask: 255.255.255.0

Gateway IP Address: 172.23.23.254

WAN MAC Address

□ Spoof WAN MAC Address

Clone MAC address: 00-50-18-21-BD-43

The following table describes the labels in this screen.

Table 31   WAN: Ethernet Encapsulation

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.
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.
IP Address	Enter your WAN IP address in this field if you selected **Use Fixed IP Address.**
Remote IP Subnet Mask	Enter the **Remote IP Subnet Mask** (if your ISP gave you one) in this field.
Backup Gateway IP Address	Enter a **Backup Gateway IP Address** (if your ISP gave you one) in this field.
WAN MAC Address	

Table 31 WAN: Ethernet Encapsulation

LABEL	DESCRIPTION
Spoof WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Clear the check box to use the factory assigned default MAC Address. Select this option and and click **Clone MAC** to clone the MAC address in the **MAC Address** field.
Clone MAC address	Enter the MAC address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

5.6.2 PPPoE Encapsulation

The Prestige supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The **PPP over Ethernet** 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).

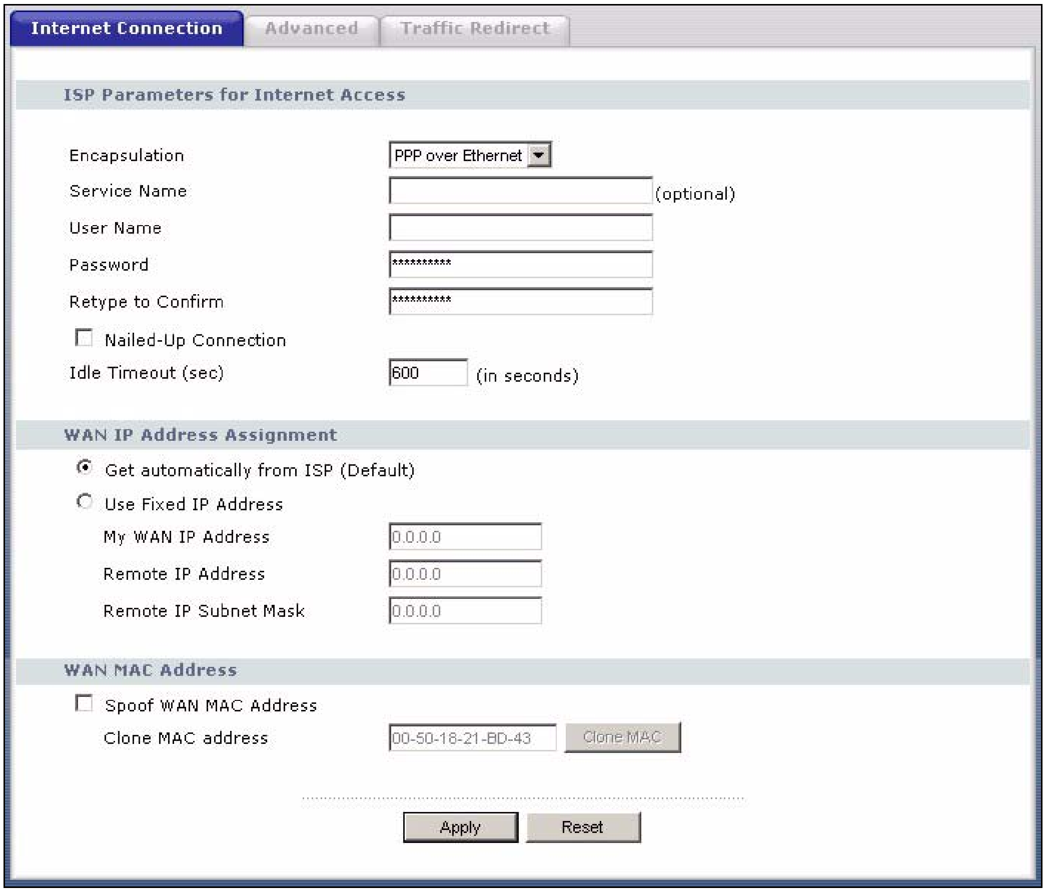
One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

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 Prestige (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the Prestige does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

The screen shown next is for **PPPoE** encapsulation.

Figure 45 WAN: PPPoE Encapsulation



ISP Parameters for Internet Access

Encapsulation: PPP over Ethernet
Service Name: (optional)
User Name:
Password: **********
Retype to Confirm: **********
□ Nailed-Up Connection
Idle Timeout (sec): 600 (in seconds)

WAN IP Address Assignment

● Get automatically from ISP (Default)
○ Use Fixed IP Address
My WAN IP Address: 0.0.0.0
Remote IP Address: 0.0.0.0
Remote IP Subnet Mask: 0.0.0.0

WAN MAC Address

□ Spoof WAN MAC Address
Clone MAC address: 00-50-18-21-BD-43

The following table describes the labels in this screen.

Table 32 WAN: PPPoE Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	The **PPP over Ethernet** choice is for a dial-up connection using PPPoE. The Prestige supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF 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 is correctly.
Nailed-Up Connection	Select **Nailed-Up Connection** if you do not want the connection to time out.

Table 32 WAN: PPPoE Encapsulation

LABEL	DESCRIPTION
Idle Timeout	This value specifies the time in seconds that elapses before the router automatically disconnects from the PPPoE server.
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**.
Remote IP Address	Enter the Remote IP Address (if your ISP gave you one) in this field.
Remote IP Subnet Mask	Enter the Rmote IP subnet Mask in this field.
WAN MAC Address	
Spoof WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Clear the check box to use the factory assigned default MAC Address. Select this option and and click **Clone MAC** to clone the MAC address in the **MAC Address** field.
Clone MAC address	Enter the MAC address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

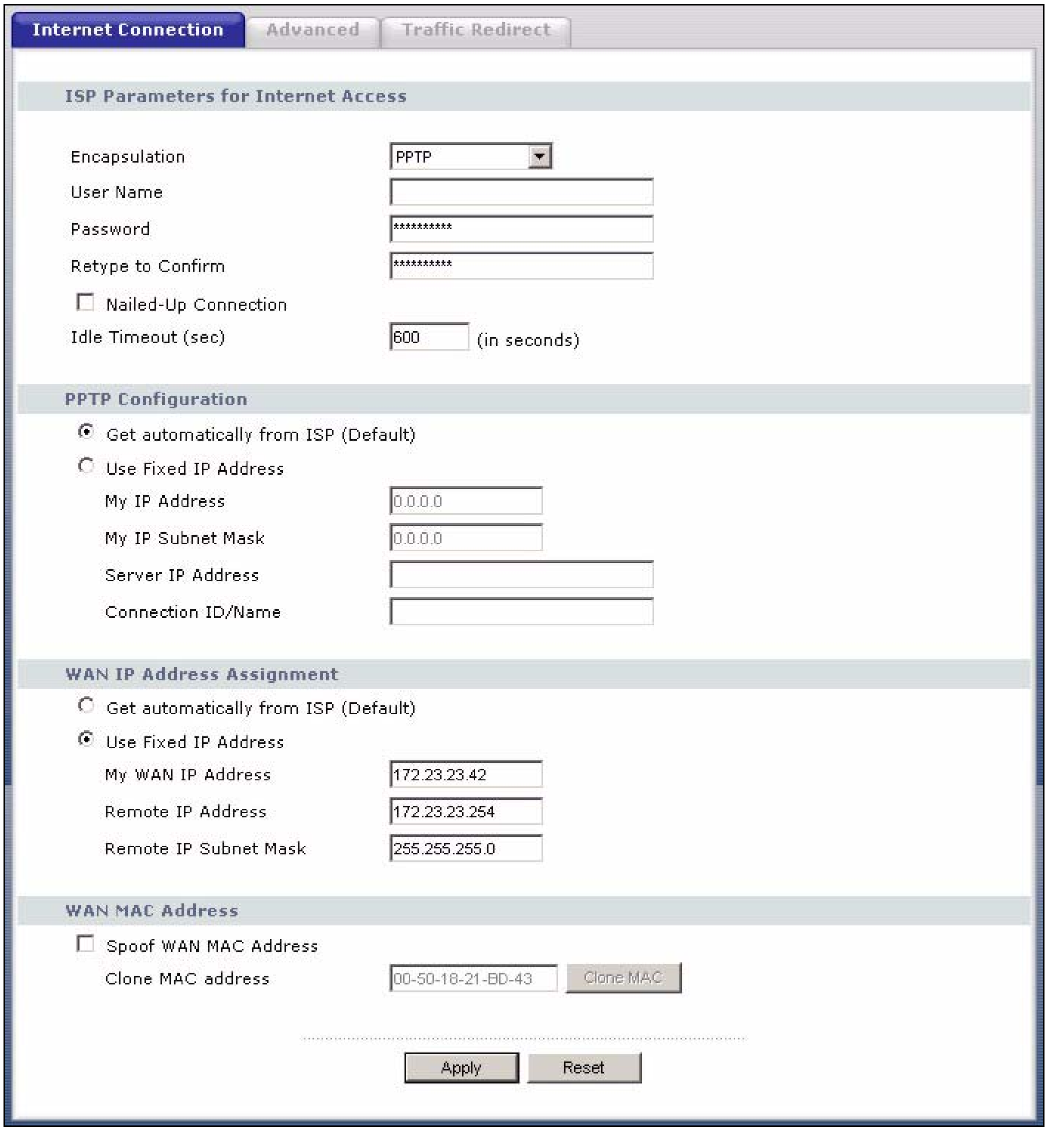
5.6.3 PPTP Encapsulation

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.

The screen shown next is for **PPTP** encapsulation.

Figure 46 PPTP Encapsulation



ISP Parameters for Internet Access

Encapsulation: PPTP

User Name:

Password: **********

Retype to Confirm: **********

□ Nailed-Up Connection

Idle Timeout (sec): 600 (in seconds)

PPTP Configuration

● Get automatically from ISP (Default)

○ Use Fixed IP Address

My IP Address: 0.0.0.0

My IP Subnet Mask: 0.0.0.0

Server IP Address:

Connection ID/Name:

WAN IP Address Assignment

○ Get automatically from ISP (Default)

● Use Fixed IP Address

My WAN IP Address: 172.23.23.42

Remote IP Address: 172.23.23.254

Remote IP Subnet Mask: 255.255.255.0

WAN MAC Address

□ Spoof WAN MAC Address

Clone MAC address: 00-50-18-21-BD-43 Clone MAC

Apply Reset

The following table describes the labels in this screen.

Table 33 PPTP Encapsulation

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 Prestige 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.
User Name	Type the user name given to you by your ISP.

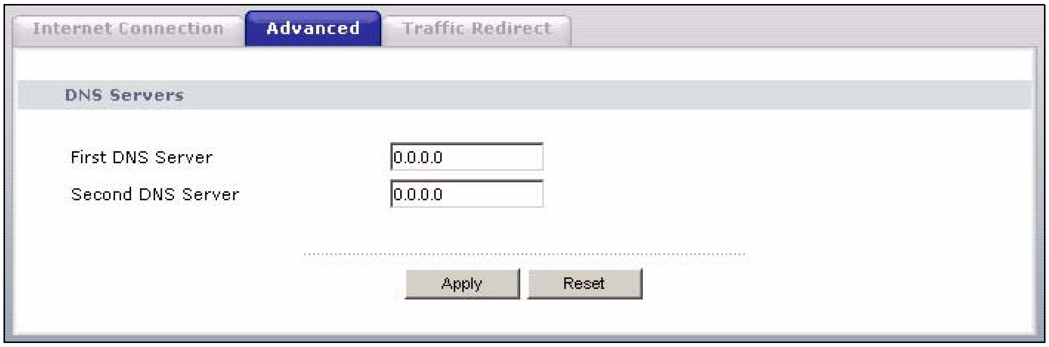
Table 33 PPTP Encapsulation

LABEL	DESCRIPTION
Password	Type the password associated with the User Name above.
Retype to Confirm	Type your password again to make sure that you have entered is 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 Prestige automatically disconnects from the PPTP server.
PPTP Configuration	
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 IP Address	Type the (static) IP address assigned to you by your ISP.
My IP Subnet Mask	Your Prestige 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 Prestige.
Server IP Address	Type the IP address of the PPTP server.
Connection ID/ Name	Type your identification name for the PPTP server.
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**.
Remote IP Address	Enter the Remote IP Address (if your ISP gave you one) in this field.
Remote IP Subnet Mask	Enter the Rmote IP subnet Mask in this field.
WAN MAC Address	
Spoof WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Clear the check box to use the factory assigned default MAC Address. Select this option and and click **Clone MAC** to clone the MAC address in the **MAC Address** field.
Clone MAC address	Enter the MAC address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

5.7 Advanced WAN Screen

To change your Prestige’s advanced WAN settings, click the **WAN** link under Network, and the **Advanced** tab. The screen appears as shown.

Figure 47 Advanced



DNS Servers

First DNS Server 0.0.0.0

Second DNS Server 0.0.0.0

The following table describes the labels in this screen.

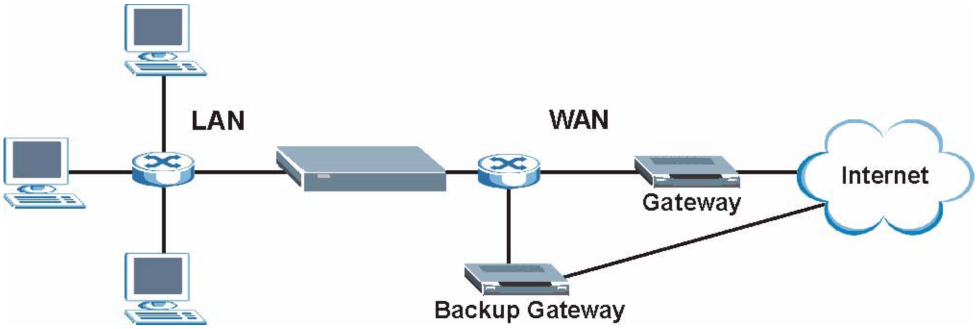
Table 34 Advanced

LABEL	DESCRIPTION
DNS Servers	
First DNS Server Second DNS Server	Enter the IP address(es) of the DNS server(s). If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

5.8 Traffic Redirect

Traffic redirect forwards WAN traffic to a backup gateway when the Prestige cannot connect to the Internet through its normal gateway. Connect the backup gateway on the WAN so that the Prestige still provides firewall protection.

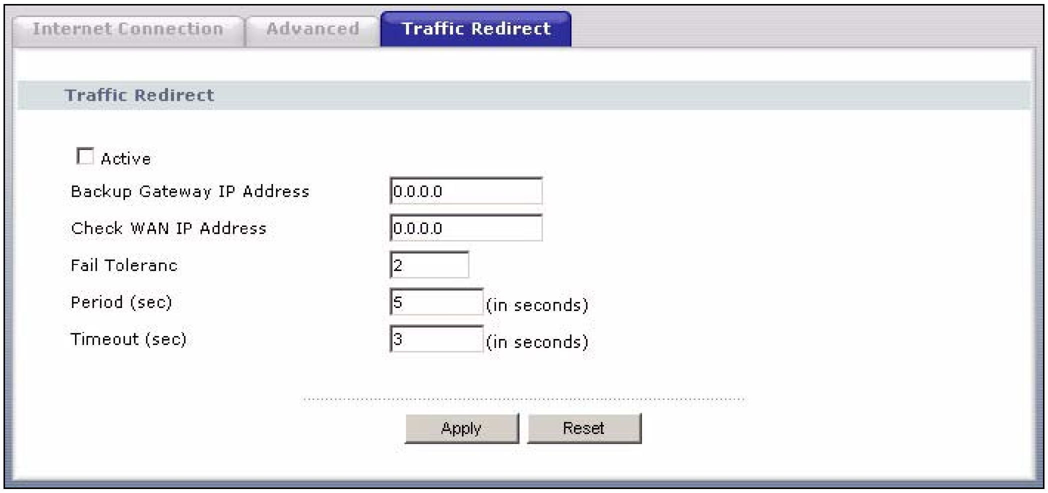
Figure 48 Traffic Redirect WAN Setup



5.9 Traffic Redirect Screen

To change your Prestige's Traffic Redirect settings, click the **WAN** link under **Network** and the **Traffic Redirect** tab. The screen appears as shown.

Figure 49 WAN: Traffic Redirect



□ Active

Backup Gateway IP Address	0.0.0.0	
Check WAN IP Address	0.0.0.0	
Fail Toleranc	2	
Period (sec)	5	(in seconds)
Timeout (sec)	3	(in seconds)

The following table describes the labels in this screen.

Table 35 Traffic Redirect

LABEL	DESCRIPTION
Active	Select this check box to have the Prestige 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 Prestige automatically forwards traffic to this IP address if the Prestige's Internet connection terminates.
Check WAN IP Address	Configuration of this field is optional. If you do not enter an IP address here, the Prestige will use the default gateway IP address. 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 are using PPTP or PPPoE Encapsulation, type "**0.0.0.0**" to configure the Prestige to check the PVC (Permanent Virtual Circuit) or PPTP tunnel.
Fail Tolerance	Type the number of times your Prestige may attempt and fail to connect to the Internet before traffic is forwarded to the backup gateway.
Period (seconds)	Type the number of seconds for the Prestige 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 (seconds)	Type the number of seconds for your Prestige 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 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.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

CHAPTER 6
LAN

This chapter describes how to configure LAN settings.

6.1 LAN Overview

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

6.1.1 IP Pool Setup

The Prestige 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 Prestige itself) in the lower range for other server computers, for instance, servers for mail, FTP, TFTP, web, etc., that you may have.

6.1.2 System DNS Servers

Refer to the *IP Address and Subnet Mask* section in the **Wizard Connection** chapter.

6.2 LAN TCP/IP

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

6.2.1 Factory LAN Defaults

The LAN parameters of the Prestige 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.

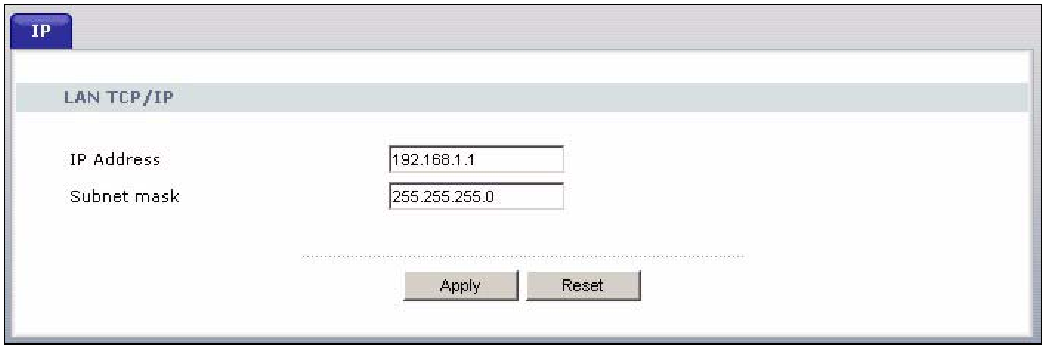
6.2.2 IP Address and Subnet Mask

Refer to the section about IP address and subnet mask in the **Wizard Setup** chapter for this information.

6.3 IP Screen

Click the **LAN** link under **Network** to open the **IP** screen.

Figure 50 LAN IP



IP Address 192.168.1.1

Subnet mask 255.255.255.0

The following table describes the labels in this screen.

Table 36 LAN IP

LABEL	DESCRIPTION
LAN TCP/IP	
IP Address	Type the IP address of your Prestige in dotted decimal notation 192.168.1.1 (factory default).
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your Prestige 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 Prestige 255.255.255.0.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

CHAPTER 7 DHCP Server

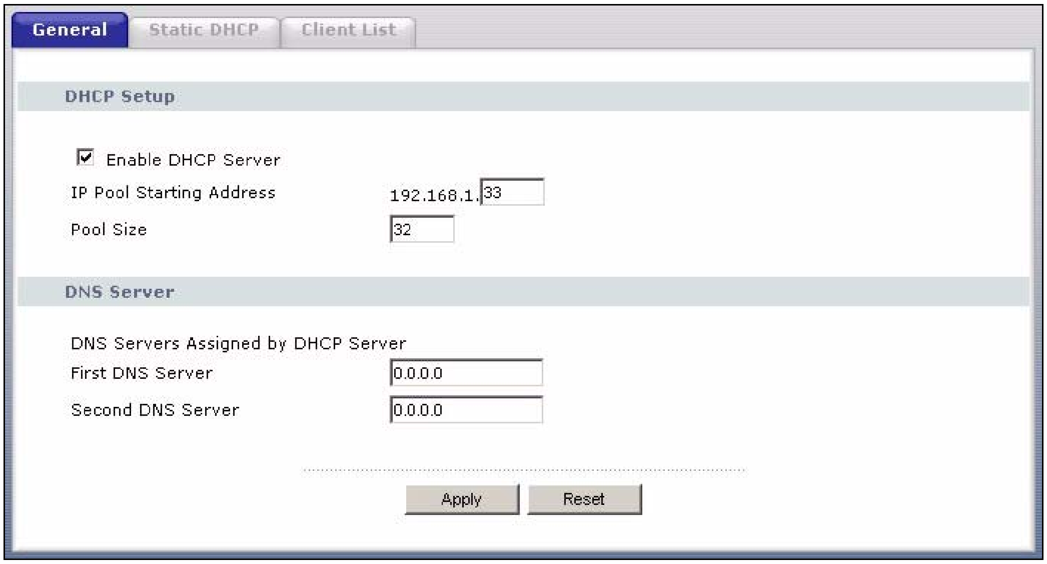
7.1 DHCP

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

7.2 DHCP Screen

Click the **DHCP Server** link under **Network** and the **General** tab. The following screen displays.

Figure 51 General



DHCP Setup

☑ Enable DHCP Server

IP Pool Starting Address 192.168.1. 33

Pool Size 32

DNS Server

DNS Servers Assigned by DHCP Server

First DNS Server 0.0.0.0

Second DNS Server 0.0.0.0

The following table describes the labels in this screen.

Table 37 General

LABEL	DESCRIPTION
Enable DHCP Server	DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (computers) to obtain TCP/IP configuration at startup from a server. Leave the **Enable DHCP Server** check box selected unless your ISP instructs you to do otherwise. Clear it to disable the Prestige acting as a DHCP server. When configured as a server, the Prestige 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 computers must be manually configured. When set as a server, fill in the following four 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.
DNS Servers Assigned by DHCP Server The Prestige passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP clients. The Prestige only passes this information to the LAN DHCP clients when you select the **Enable DHCP Server** check box. When you clear the **Enable DHCP Server** check box, 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.	
First DNS Server Second DNS Server	Enter the IP address(es) of the DNS server(s). If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

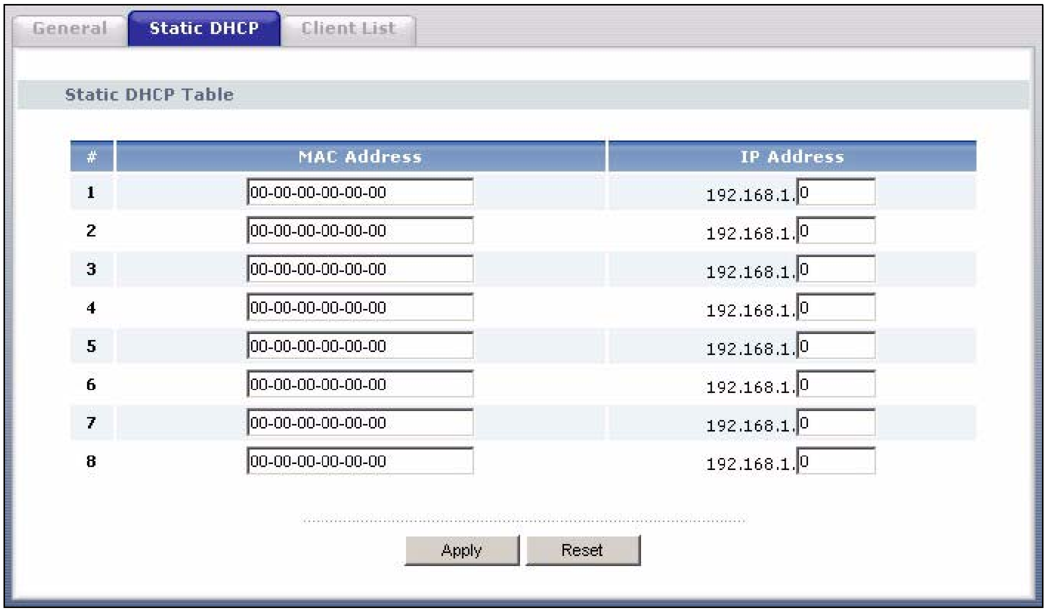
7.3 Static DHCP Screen

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.

To change your Prestige’s Static DHCP settings, click the **DHCP Server** link under **Network** and the **Static DHCP** tab. The following screen displays.

Figure 52 Static DHCP



Static DHCP Table

#	MAC Address	IP Address
1	00-00-00-00-00-00	192.168.1. 0
2	00-00-00-00-00-00	192.168.1. 0
3	00-00-00-00-00-00	192.168.1. 0
4	00-00-00-00-00-00	192.168.1. 0
5	00-00-00-00-00-00	192.168.1. 0
6	00-00-00-00-00-00	192.168.1. 0
7	00-00-00-00-00-00	192.168.1. 0
8	00-00-00-00-00-00	192.168.1. 0

The following table describes the labels in this screen.

Table 38 Static DHCP

LABEL	DESCRIPTION
#	This is the index number of the Static IP table entry (row).
MAC Address	Type the MAC address (with colons) of a computer on your LAN.
IP Address	Type the LAN IP address of a computer on your LAN.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

7.4 Client List Screen

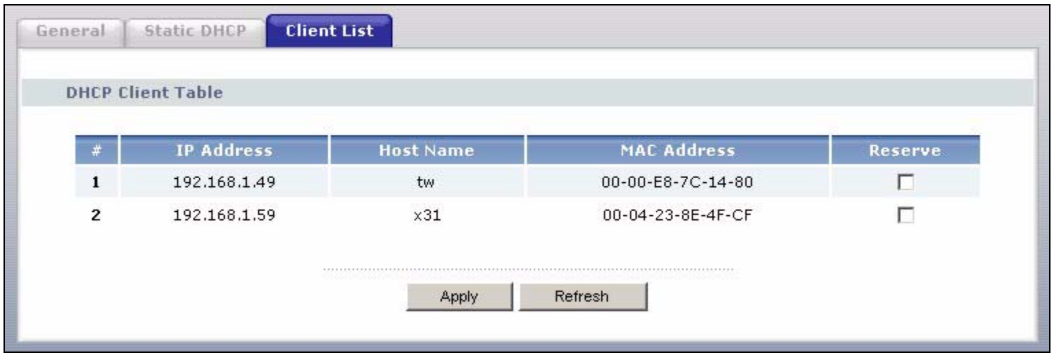
The DHCP table shows current DHCP client information (including **IP Address**, **Host Name** and **MAC Address**) of all network clients using the Prestige’s DHCP server.

Configure this screen to always assign an IP address to a MAC address (and host name). Click the **DHCP Server** link under **Network** and the **Client List** tab.

Note: You can also view a read-only client list by clicking the **DHCP Table (Detail)** hyperlink in the **Status** screen.

The following screen displays.

Figure 53 Client List



#	IP Address	Host Name	MAC Address	Reserve
1	192.168.1.49	tw	00-00-E8-7C-14-80	□
2	192.168.1.59	x31	00-04-23-8E-4F-CF	□

The following table describes the labels in this screen.

Table 39 Client List

LABEL	DESCRIPTION
#	This is the index number of the host computer.
IP Address	This field displays the IP address relative to the # field listed above.
Host Name	This field displays the computer host name.
MAC Address	The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation). A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address.
Reserve	Select this check box to have the Prestige always assign this IP address to this MAC address (and host name). You can select up to 8 entries in this table. After you click **Apply**, the MAC address and IP address also display in the **Static DHCP** screen (where you can edit them).
Apply	Click **Apply** to save your changes back to the Prestige.
Refresh	Click **Refresh** to reload the DHCP table.

CHAPTER 8 Network Address Translation (NAT)

This chapter discusses how to configure NAT on the Prestige.

8.1 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.

8.1.1 NAT Definitions

Inside/outside denotes where a host is located relative to the Prestige. 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.

8.1.2 What NAT Does

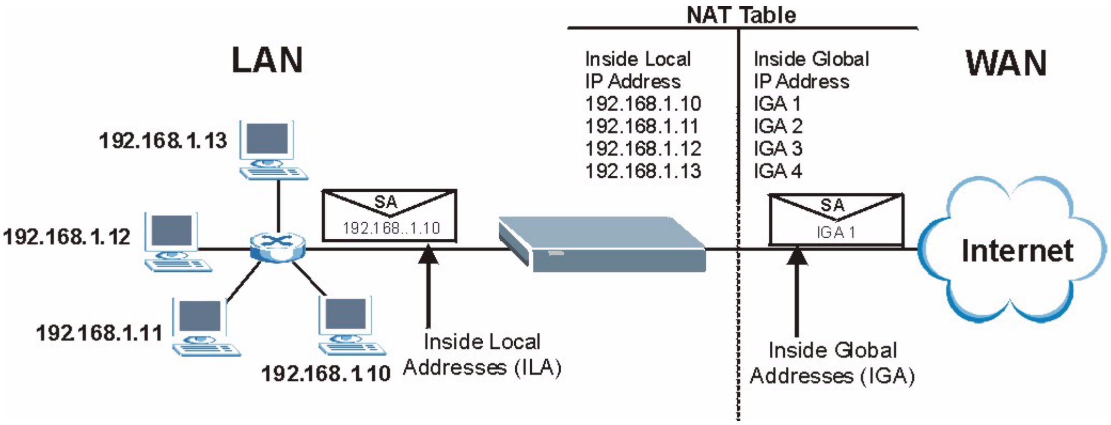
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) 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. 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, your Prestige 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)*.

8.1.3 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 Prestige keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

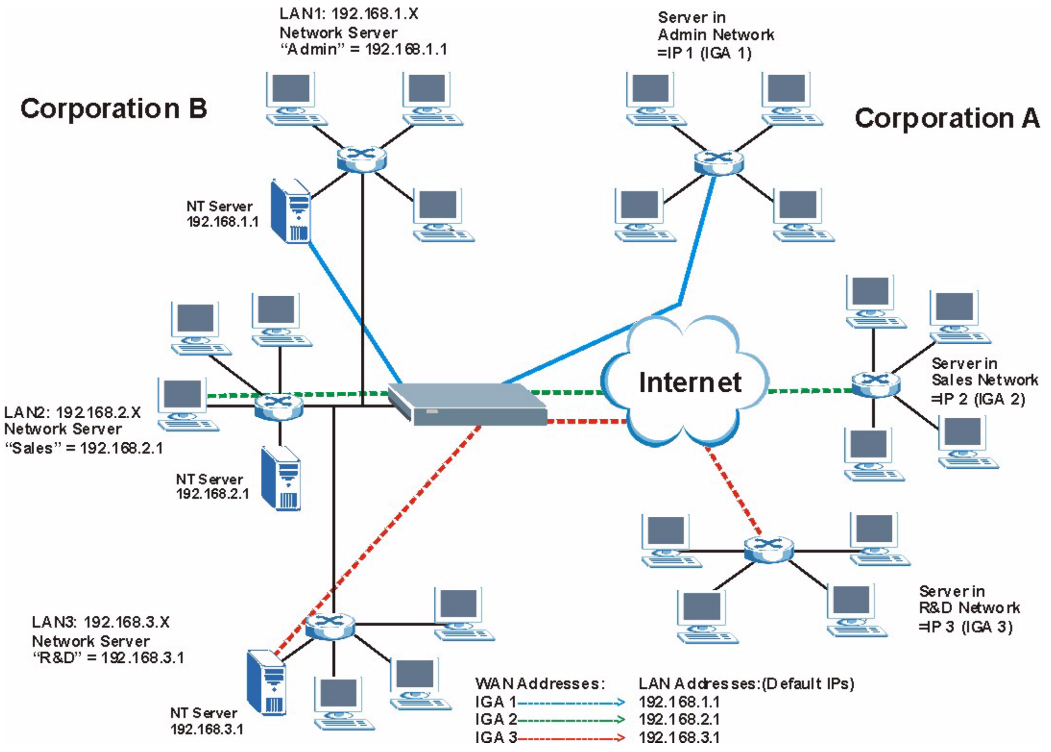
Figure 54 How NAT Works



8.1.4 NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP Alias) behind the Prestige can communicate with three distinct WAN networks. More examples follow at the end of this chapter.

Figure 55 NAT Application With IP Alias



8.1.5 Default Server IP Address

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 Prestige discards all packets received for ports that are not specified in this screen or remote management.

8.1.6 Port Forwarding: Services and Port Numbers

A SUA server set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make accessible to the outside world even though NAT makes your whole inside network appear as a single machine to the outside world.

Use the **Port Forwarding** page to forward incoming service requests to the server(s) on your local network. 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.

In addition to the servers for specified services, NAT supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default is not defined, the service request is simply discarded.

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.

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.

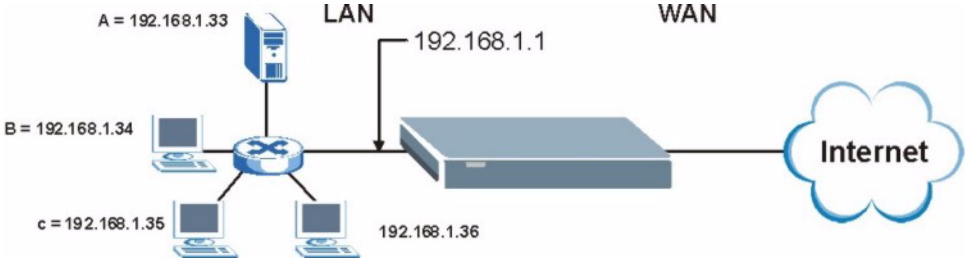
Table 41 Services and Port Numbers

SERVICE	PORT NUMBER
ECHO	7
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

8.1.7 Configuring Servers Behind SUA (Example)

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (A in the example), port 80 to another (B in the example) and assign a default server IP address of 192.168.1.35 to a third (C in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet

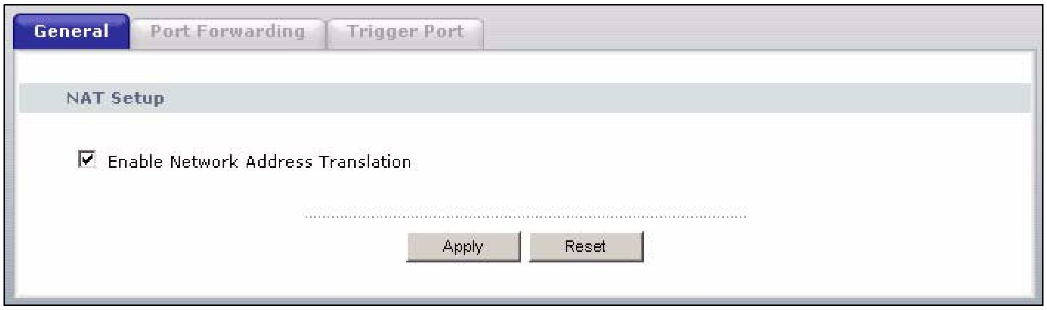
Figure 56 Multiple Servers Behind NAT Example



8.2 General NAT Screen

Click the **NAT** link under **Network** to open the **General** screen.

Figure 57 NAT: General



☑ Enable Network Address Translation

The following table describes the labels in this screen.

Table 42 NAT: General

LABEL	DESCRIPTION
Enable Network Address Translation	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). Select the check box to enable NAT.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

8.3 Port Forwarding Screen

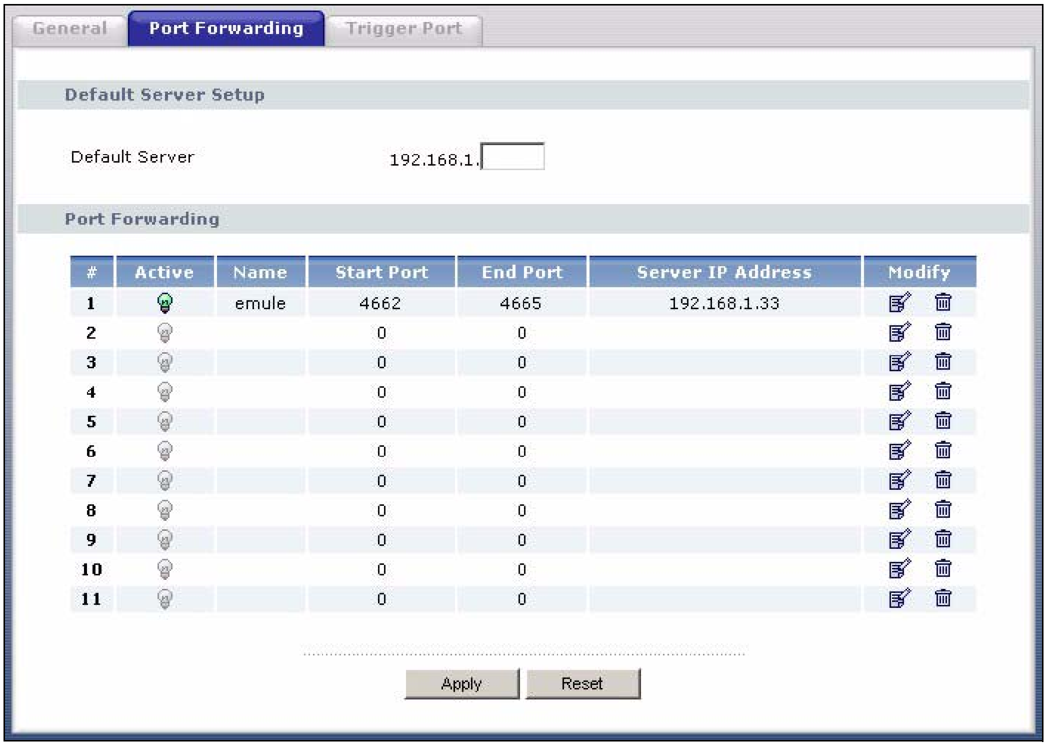
Ordering your rules is important because the Prestige applies the rules in the order that you specify. When a rule matches the current packet, the Prestige takes the corresponding action and the remaining rules are ignored. If there are any empty rules before your new configured rule, your configured rule will be pushed up by that number of empty rules. For example, if you have already configured rules 1 to 6 in your current set and now you configure rule number 9. In the set summary screen, the new rule will be rule 7, not 9. Now if you delete rule 4, rules 5 to 7 will be pushed up by 1 rule, so old rules 5, 6 and 7 become new rules 4, 5 and 6.

Refer to Table 41 on page 102 for port numbers commonly used for particular services.

Note: If you do not assign a **Default Server** IP Address, the Prestige discards all packets received for ports that are not specified in this screen or remote management.

To change your Prestige’s port forwarding settings, click the **NAT** link under **Network** and the **Port Forwarding** tab. The screen appears as shown.

Figure 58 Port Forwarding



Default Server Setup

Default Server 192.168.1.

Port Forwarding

#	Active	Name	Start Port	End Port	Server IP Address	Modify
1	●	emule	4662	4665	192.168.1.33	✎ 🗑
2	○		0	0		✎ 🗑
3	○		0	0		✎ 🗑
4	○		0	0		✎ 🗑
5	○		0	0		✎ 🗑
6	○		0	0		✎ 🗑
7	○		0	0		✎ 🗑
8	○		0	0		✎ 🗑
9	○		0	0		✎ 🗑
10	○		0	0		✎ 🗑
11	○		0	0		✎ 🗑

The following table describes the labels in this screen.

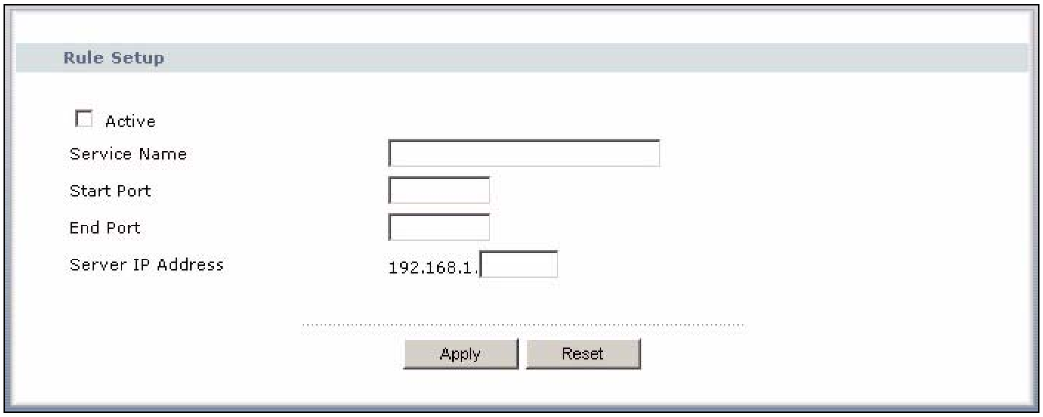
Table 43 NAT: Port Forwarding

LABEL	DESCRIPTION
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, the Prestige discards all packets received for ports that are not specified in this screen or remote management.
#	Number of an individual SUA server entry.
Active	This icon is turned on when the port forwarding entry is enabled. Click the edit icon under **Modify** and select the **Active** checkbox in the **Rule Setup** screen to enable the port forwarding entry. Clear the checkbox to disable forwarding of these ports to an inside server without having to delete the entry.
Name	This field displays a name to identify this port-forwarding rule.
Start Port	This field displays a start port number.
End Port	This field displays an end port number. If the same port number as the **Start Port** is displayed then a single port is forwarded. If a different number to the **Start Port** number is displayed then a range of ports are forwarded.
Server IP Address	This field displays the inside IP address of the server.
Modify	Click the edit icon to open the address mapping rule screen. Modify an existing rule or create a new rule in the **Rule Setup** screen. Click the delete icon to remove an address mapping rule.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

8.3.1 Rule Setup Screen

To edit a port forwarding rule, click the edit icon under **Modify**. The following screen displays.

Figure 59 NAT: Port Forwarding: Rule Setup



Rule Setup

☐ Active

Service Name	
Start Port	
End Port	
Server IP Address	192.168.1.

The following table describes the labels in this screen.

Table 44 NAT: Port Forwarding: Rule Setup

LABEL	DESCRIPTION
Active	Select the check box to enable this port forwarding entry. Clear the checkbox to disallow forwarding of these ports to an inside server without having to delete the entry.
Service Name	Type a **Service Name** to identify this port-forwarding rule.
Start Port	Type a start port number. To forward only one port, enter it again in the **End Port** field. To specify a range of ports, enter the last port to be forwarded in the **End Port** field.
End Port	Type an end port number.
Server IP Address	Type the inside IP address of the server.
Apply	Click **Apply** to save your changes back to the Prestige.
Cancel	Click **Cancel** to return to the previous screen and not save your changes.

8.4 Trigger Port Forwarding

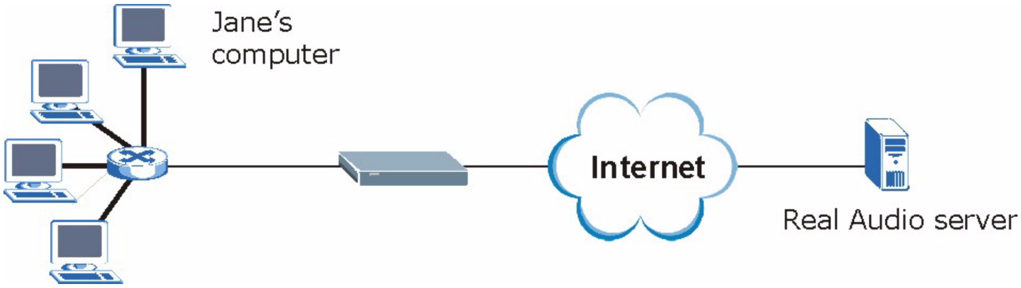
Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem 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 Prestige 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 Prestige's WAN port receives a response with a specific port number and protocol ("incoming" port), the Prestige 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.

8.4.1 Trigger Port Forwarding Example

The following is an example of trigger port forwarding.

Figure 60 Trigger Port Forwarding Process: Example



1. Jane requests a file from the Real Audio server (port 7070).
2. Port 7070 is a "trigger" port and causes the Prestige to record Jane's computer IP address. The Prestige associates Jane's computer IP address with the "incoming" port range of 6970-7170.
3. The Real Audio server responds using a port number ranging between 6970-7170.
4. The Prestige forwards the traffic to Jane's computer IP address.
5. Only Jane can connect to the Real Audio server until the connection is closed or times out. The Prestige times out in three minutes with UDP (User Datagram Protocol), or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

8.4.2 Two Points To Remember About Trigger Ports

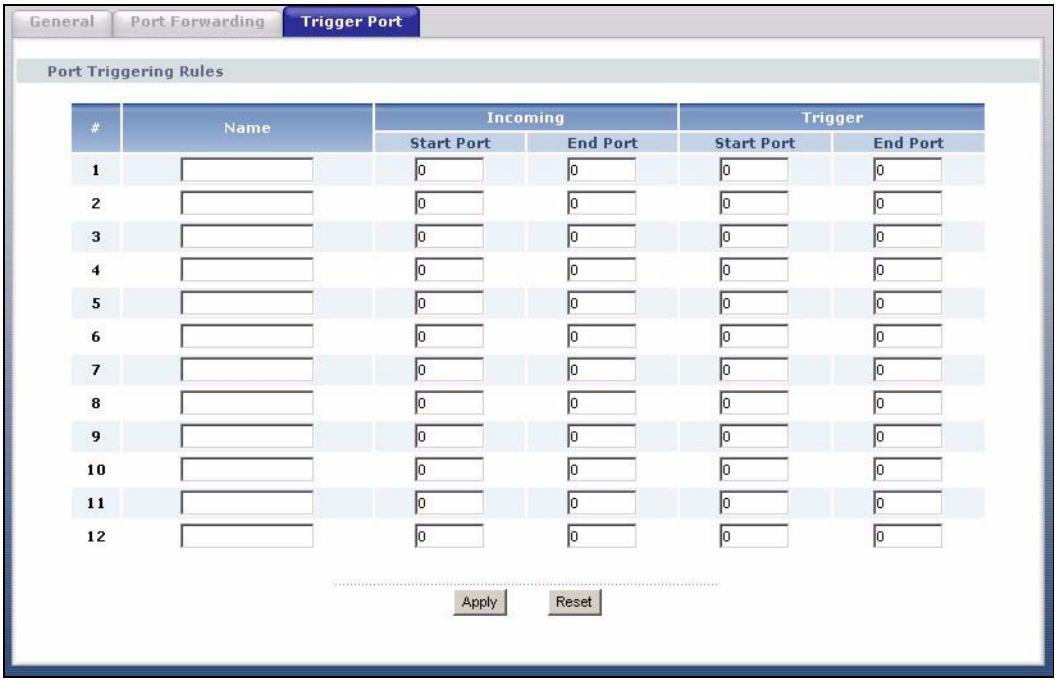
1. Trigger events only happen on data that is going coming from inside the Prestige and going to the outside.
2. If an application needs a continuous data stream, that port (range) will be tied up so that another computer on the LAN can't trigger it.

8.5 Trigger Port Forwarding Screen

To change your Prestige's trigger port settings, click the **NAT** link under **Network** and the **Trigger Port** tab. The screen appears as shown.

Note: Only one LAN computer can use a trigger port (range) at a time.

Figure 61 NAT: Trigger Port



Port Triggering Rules

#	Name	Incoming		Trigger	
		Start Port	End Port	Start Port	End Port
1		0	0	0	0
2		0	0	0	0
3		0	0	0	0
4		0	0	0	0
5		0	0	0	0
6		0	0	0	0
7		0	0	0	0
8		0	0	0	0
9		0	0	0	0
10		0	0	0	0
11		0	0	0	0
12		0	0	0	0

The following table describes the labels in this screen.

Table 45 NAT: Trigger Port

LABEL	DESCRIPTION
#	This is the rule index number (read-only).
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 Prestige 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 Prestige 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.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

CHAPTER 9 Firewall

This chapter gives some background information on firewalls and explains how to get started with the Prestige firewall.

9.1 Introduction to Firewall

9.1.1 What is a Firewall?

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.

9.1.2 Stateful Inspection Firewall.

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.

9.1.3 About the Prestige Firewall

The Prestige firewall is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated (click the **General** tab under **Firewall** and then click the **Enable Firewall** check box). The Prestige's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The Prestige 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 Prestige 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 Prestige has one Ethernet WAN port and four Ethernet LAN ports, which are used to physically separate the network into two areas.The WAN (Wide Area Network) port attaches to the broadband (cable or DSL) modem 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" is not allowed (by default) unless the remote host is authorized to use a specific service.

9.1.4 Guidelines For Enhancing Security With Your Firewall

1 Change the default password via web configurator.

2 Think about access control before you connect to the network in any way, including attaching a modem to the port.

3 Limit who can access your router.

4 Don't enable any local service (such as SNMP or NTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.

5 For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.

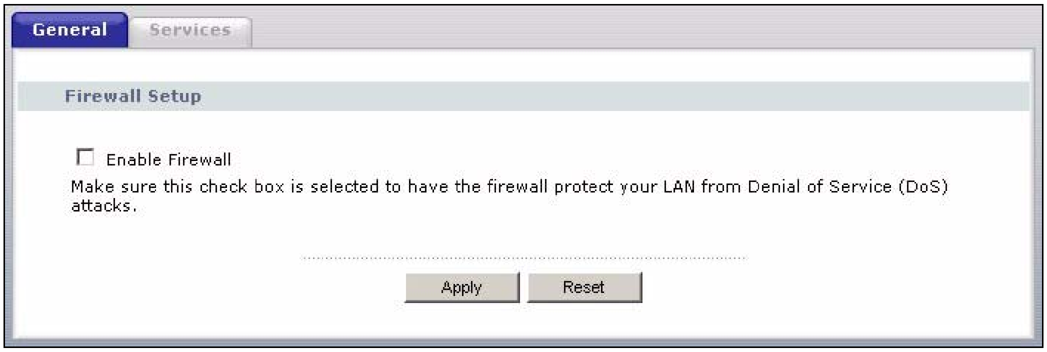
6 Protect against IP spoofing by making sure the firewall is active.

7 Keep the firewall in a secured (locked) room.

9.2 General Firewall Screen

Click the **Firewall** link under **Security** to open the **General** screen.

Figure 62 Firewall: General



□ Enable Firewall

Make sure this check box is selected to have the firewall protect your LAN from Denial of Service (DoS) attacks.

The following table describes the labels in this screen.

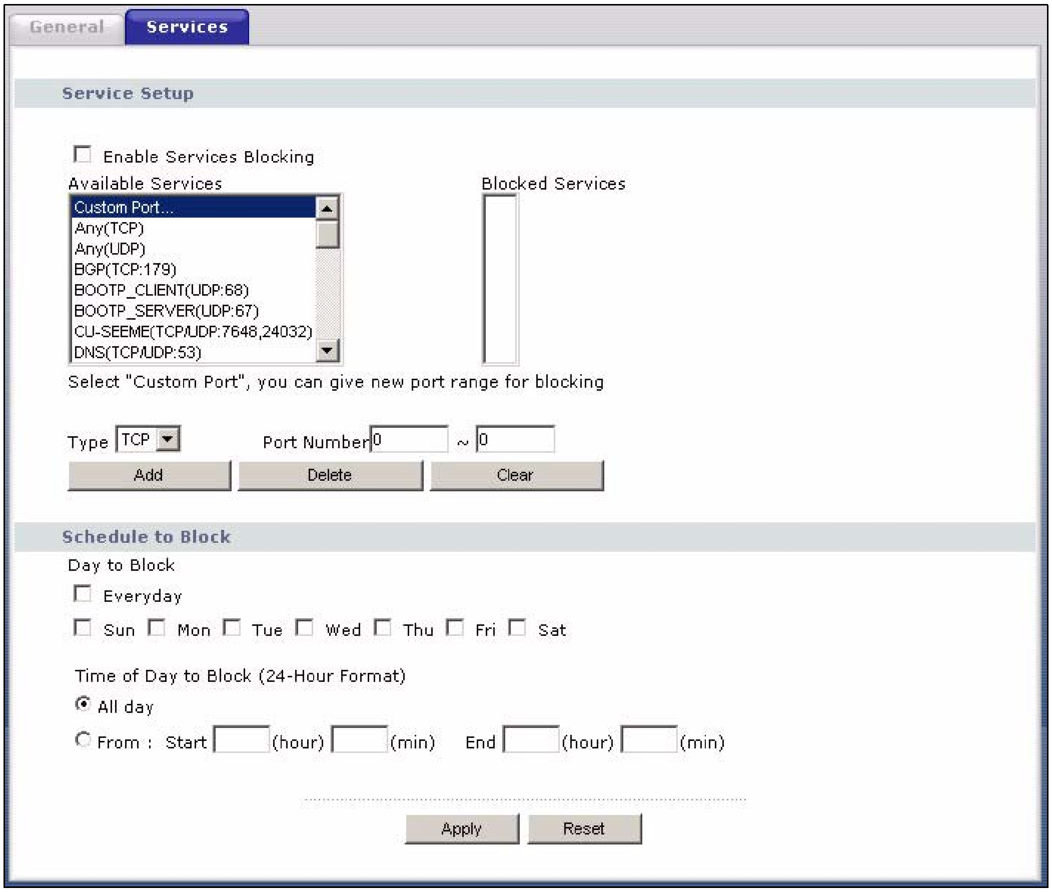
Table 46 Firewall: General

LABEL	DESCRIPTION
Enable Firewall	Select this check box to activate the firewall. The Prestige performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Apply	Click **Apply** to save the settings.
Reset	Click **Reset** to start configuring this screen again.

9.3 Services Screen

Click the **Firewall** link under **Security** and the **Services** tab. The screen appears as shown next. Use this screen to enable service blocking, enter/delete/modify the services you want to block and the date/time you want to block them.

Figure 63 Firewall: Services



General | Services

Service Setup

□ Enable Services Blocking

Available Services: Custom Port..., Any(TCP), Any(UDP), BGP(TCP:179), BOOTP_CLIENT(UDP:68), BOOTP_SERVER(UDP:67), CU-SEEME(TCP/UDP:7648,24032), DNS(TCP/UDP:53)

Blocked Services

Select "Custom Port", you can give new port range for blocking

Type: TCP   Port Number: 0 ~ 0

Add | Delete | Clear

Schedule to Block

Day to Block

□ Everyday

□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

Time of Day to Block (24-Hour Format)

● All day

○ From : Start ____ (hour) ____ (min) End ____ (hour) ____ (min)

Apply | Reset

The following table describes the labels in this screen.

Table 47 Firewall: Services

LABEL	DESCRIPTION
Enable Services Blocking	Select this check box to enable this feature.
Available Services	This is a list of pre-defined services (ports) you may prohibit your LAN computers from using. Please see Section 9.3.1 on page 113 for more information on services available. Select the port you want to block using the drop-down list and click **Add** to add the port to the **Blocked Services** field.
Blocked Services	This is a list of services (ports) that will be inaccessible to computers on your LAN once you enable service blocking. Choose the IP port (**TCP**, **UDP** or **TCP**/**UDP**) that defines your customized port from the drop down list box.
Custom Port	A custom port is a service that is not available in the pre-defined **Available Services** list and you must define using the next two fields.
Type	Services are either **TCP** and/or **UDP**. Select from either **TCP** or **UDP**.
Port Number	Enter the port number range that defines the service. For example, suppose you want to define the Gnutella service. Select TCP type and enter a port range from 6345-6349.
Add	Select a service from the **Available Services** drop-down list and then click **Add** to add a service to the **Blocked Services**.
Delete	Select a service from the **Blocked Services** list and then click **Delete** to remove this service from the list.
Clear	Click **Clear** to empty the **Blocked Services**.
Day to Block:	Select a check box to configure which days of the week (or everyday) you want the content filtering to be active.
Time of Day to Block (24-Hour Format)	Select the time of day you want service blocking to take effect. Configure blocking to take effect all day by selecting the **All Day** check box. You can also configure specific times that by entering the start time in the **Start (hr)** and **Start (min)** fields and the end time in the **End (hr)** and **End (min)** fields. Enter times in 24-hour format, for example, "3:00pm" should be entered as "15:00".
Apply	Click **Apply** to save the settings.
Reset	Click **Reset** to start configuring this screen again.

9.3.1 Services

The commonly used services and port numbers are shown in the following table. Please refer to RFC 1700 for further information about port numbers. Next to the name of the service, two fields appear in brackets. The first field indicates the IP protocol type (TCP, UDP, or ICMP). The second field indicates the IP port number that defines the service. (Note that there may be more than one IP protocol type. For example, look at the DNS service. (UDP/TCP:53) means UDP port 53 and TCP port 53.

Table 48 Commonly Used Services

SERVICE	DESCRIPTION
AIM/New-ICQ(TCP:5190)	AOL's Internet Messenger service, used as a listening port by ICQ.
AUTH(TCP:113)	Authentication protocol used by some servers.
BGP(TCP:179)	Border Gateway Protocol.
BOOTP_CLIENT(UDP:68)	DHCP Client.
BOOTP_SERVER(UDP:67)	DHCP Server.
CU-SEEME(TCP/UDP:7648, 24032)	A popular videoconferencing solution from White Pines Software.
DNS(UDP/TCP:53)	Domain Name Server, a service that matches web names (e.g. www.zyxel.com) to IP numbers.
FINGER(TCP:79)	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP(TCP:20.21)	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323(TCP:1720)	NetMeeting uses this protocol.
HTTP(TCP:80)	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS(TCP:443)	HTTPS is a secured http session often used in e-commerce.
ICQ(UDP:4000)	This is a popular Internet chat program.
IKE(UDP:500)	The Internet Key Exchange algorithm is used for key distribution and management.
IPSEC_TUNNEL(AH:0)	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
IPSEC_TUNNEL(ESP:0)	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
IRC(TCP/UDP:6667)	This is another popular Internet chat program.
MSN Messenger(TCP:1863)	Microsoft Networks' messenger service uses this protocol.
MULTICAST(IGMP:0)	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
NEW-ICQ(TCP:5190)	An Internet chat program.
NEWS(TCP:144)	A protocol for news groups.
NFS(UDP:2049)	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP(TCP:119)	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.

Table 48 Commonly Used Services

SERVICE	DESCRIPTION
PING(ICMP:0)	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3(TCP:110)	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP(TCP:1723)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL(GRE:0)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the data channel.
RCMD(TCP:512)	Remote Command Service.
REAL_AUDIO(TCP:7070)	A streaming audio service that enables real time sound over the web.
REXEC(TCP:514)	Remote Execution Daemon.
RLOGIN(TCP:513)	Remote Login.
RTELNET(TCP:107)	Remote Telnet.
RTSP(TCP/UDP:554)	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP(TCP:115)	Simple File Transfer Protocol.
SMTP(TCP:25)	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP(TCP/UDP:161)	Simple Network Management Program.
SNMP-TRAPS(TCP/UDP:162)	Traps for use with the SNMP (RFC:1215).
SQL-NET(TCP:1521)	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH(TCP/UDP:22)	Secure Shell Remote Login Program.
STRM WORKS(UDP:1558)	Stream Works Protocol.
SYSLOG(UDP:514)	Syslog allows you to send system logs to a UNIX server.
TACACS(UDP:49)	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET(TCP:23)	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP(UDP:69)	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE(TCP:7000)	Another videoconferencing solution.

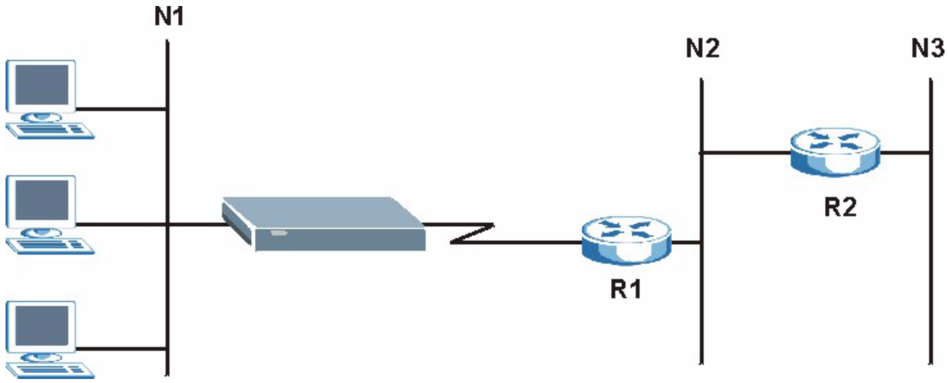
CHAPTER 10 Static Route Screens

This chapter shows you how to configure static routes for your Prestige.

10.1 Static Route Overview

Each remote node specifies only the network to which the gateway is directly connected, and the Prestige has no knowledge of the networks beyond. For instance, the Prestige knows about network N2 in the following figure through remote node router R1. However, the Prestige is unable to route a packet to network N3 because it doesn't know that there is a route through the same remote node router R1 (via gateway router R2). The static routes are for you to tell the Prestige about the networks beyond the remote nodes.

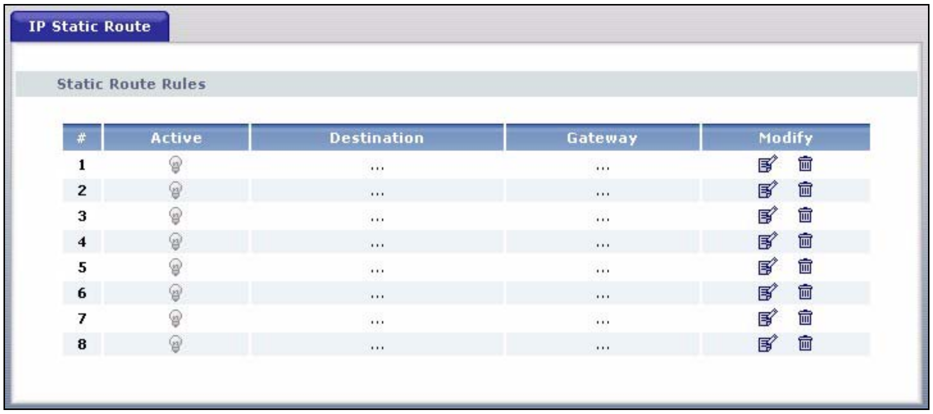
Figure 64 Example of Static Routing Topology



10.2 IP Static Route Screen

Click the **IP Static Route** link under **Management** to open the **IP Static Route** screen. The following screen displays.

Figure 65   IP Static Route



IP Static Route

Static Route Rules

#	Active	Destination	Gateway	Modify
1	💡	...	...	✎ 🗑
2	💡	...	...	✎ 🗑
3	💡	...	...	✎ 🗑
4	💡	...	...	✎ 🗑
5	💡	...	...	✎ 🗑
6	💡	...	...	✎ 🗑
7	💡	...	...	✎ 🗑
8	💡	...	...	✎ 🗑

The following table describes the labels in this screen.

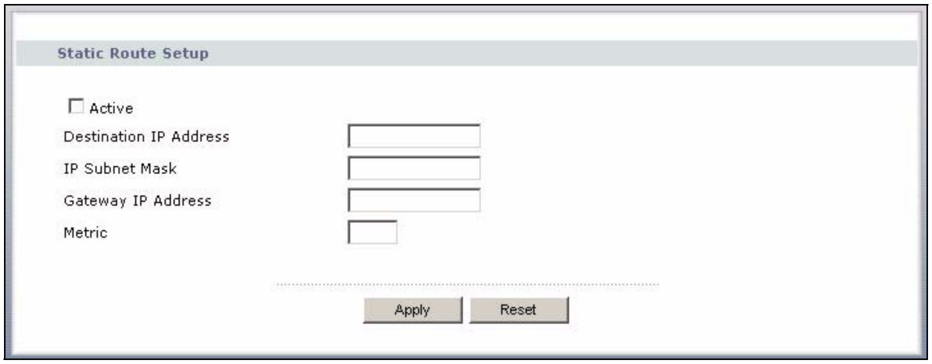
Table 49   IP Static Route

LABEL	DESCRIPTION
#	Number of an individual static route.
Active	This icon is turned on when this static route is active. Click the edit icon under **Modify** and select the **Active** checkbox in the **Static Route Setup** screen to enable the static route. Clear the checkbox to disable this static route without having to delete the entry.
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 your Prestige that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your Prestige; over the WAN, the gateway must be the IP address of one of the remote nodes.
Modify	Click the edit icon to open the static route setup screen. Modify a static route or create a new static route in the **Static Route Setup** screen. Click the delete icon to remove a static route.

10.2.1 Static Route Setup Screen

To edit a static route, click the edit icon under **Modify**. The following screen displays. Fill in the required information for each static route.

Figure 66 Static Route Setup



Static Route Setup

□ Active

Destination IP Address

IP Subnet Mask

Gateway IP Address

Metric

The following table describes the labels in this screen.

Table 50 Static Route Setup

LABEL	DESCRIPTION
Active	This field 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 your Prestige that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your Prestige; 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.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to start configuring this screen again.

CHAPTER 11 Remote Management Screens

This chapter provides information on the Remote Management screens.

11.1 Remote Management Overview

Remote management allows you to determine which services/protocols can access which Prestige interface (if any) from which computers.

Note: When you configure remote management to allow management from the WAN, you still need to configure a firewall rule to allow access. See the firewall chapters for details on configuring firewall rules.

You may manage your Prestige from a remote location via:

- LAN only
- ALL (LAN and WAN)

To disable remote management of a service, select **LAN** in the corresponding **Server Access** field.

11.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

1. You have disabled that service in one of the remote management screens.
2. The IP address in the **Secured Client IP** field does not match the client IP address. If it does not match, the Prestige will disconnect the session immediately.
3. There is a firewall rule that blocks it.

11.1.2 Remote Management and NAT

When NAT is enabled:

- Use the Prestige's WAN IP address when configuring from the WAN.
- Use the Prestige's LAN IP address when configuring from the LAN.

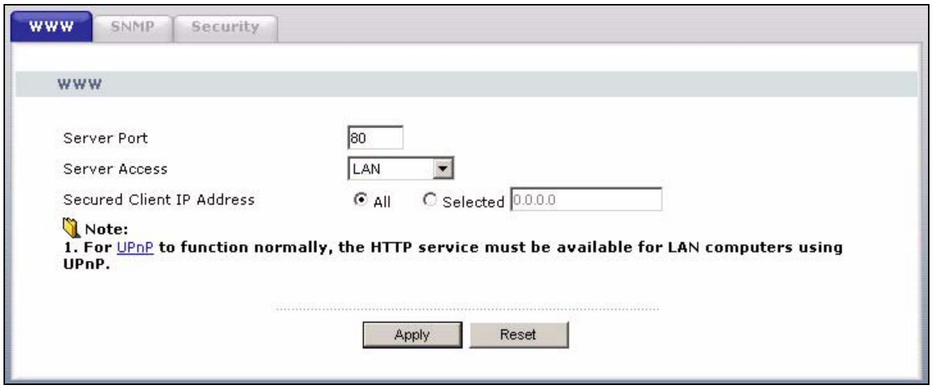
11.1.3 System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). The Prestige automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling. You can change the timeout period in the **System** screen

11.2 WWW Screen

To change your Prestige's World Wide Web settings, click the **Remote MGMT** link under **Management** to display the **WWW** screen.

Figure 67 WWW Remote Management



Server Port: 80
Server Access: LAN
Secured Client IP Address: ● All ○ Selected 0.0.0.0

Note:
1. For UPnP to function normally, the HTTP service must be available for LAN computers using UPnP.

The following table describes the labels in this screen.

Table 51 WWW Remote Management

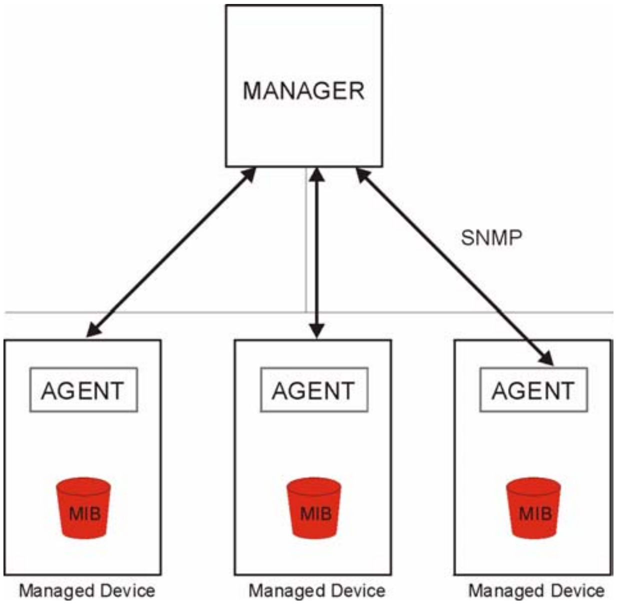
LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the Prestige using this service.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to communicate with the Prestige using this service. Select **All** to allow any computer to access the Prestige using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the Prestige using this service.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

11.3 SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your Prestige supports SNMP agent functionality, which allows a manager station to manage and monitor the Prestige through the network. The Prestige supports SNMP version one (SNMPv1) and version two (SNMPv2). The next figure illustrates an SNMP management operation.

Note: SNMP is only available if TCP/IP is configured.

Figure 68 SNMP Management Model



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

An agent is a management software module that resides in a managed device (the Prestige). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

11.3.1 Supported MIBs

The Prestige supports MIB II that is defined in RFC-1213 and RFC-1215. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance.

11.3.2 SNMP Traps

The Prestige will send traps to the SNMP manager when any one of the following events occurs:

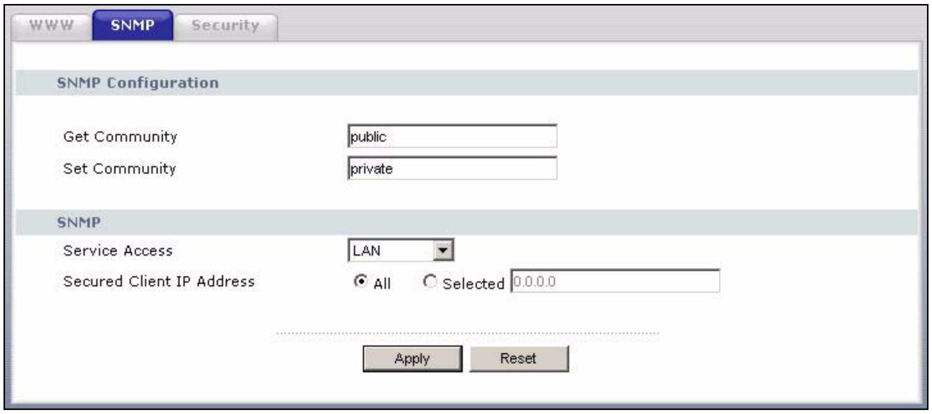
Table 52 SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
0	coldStart (defined in *RFC-1215*)	A trap is sent after booting (power on).
1	warmStart (defined in *RFC-1215*)	A trap is sent after booting (software reboot).
4	authenticationFailure (defined in *RFC-1215*)	A trap is sent to the manager when receiving any SNMP get or set requirements with the wrong community (password).
6	whyReboot (defined in ZYXEL-MIB)	A trap is sent with the reason of restart before rebooting when the system is going to restart (warm start).
6a	For intentional reboot :	A trap is sent with the message "System reboot by user!" if reboot is done intentionally, (for example, download new files, CI command "sys reboot", etc.).
6b	For fatal error :	A trap is sent with the message of the fatal code if the system reboots because of fatal errors.

11.4 SNMP Screen

To change your Prestige’s SNMP settings, click the **Remote MGMT** link under **Management**, and the **SNMP** tab. The screen appears as shown.

Figure 69 SNMP Remote Management



SNMP Configuration

Get Community: public

Set Community: private

SNMP

Service Access: LAN

Secured Client IP Address: ● All ○ Selected 0.0.0.0

The following table describes the labels in this screen.

Table 53 SNMP Remote Management

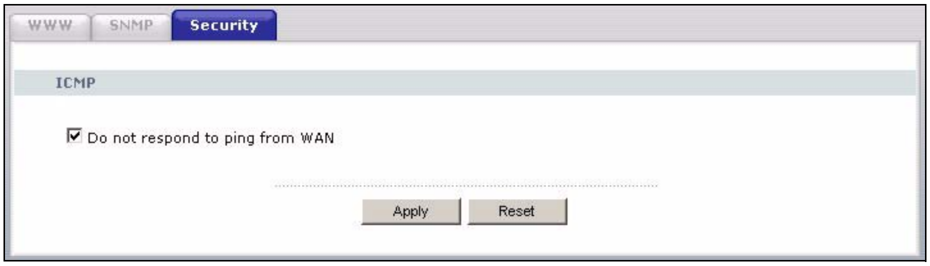
LABEL	DESCRIPTION
SNMP Configuration	
Get Community	Enter the **Get Community**, which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the **Set community**, which is the password for incoming Set requests from the management station. The default is public and allows all requests.
SNMP	
Service Access	Select the interface(s) through which a computer may access the Prestige using this service.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to communicate with the Prestige using this service. Select **All** to allow any computer to access the Prestige using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the Prestige using this service.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

11.5 Security Screen

To change your Prestige’s security settings, click the **Remote MGMT** link under **Management** and the **Security** tab. The screen appears as shown.

If an outside user attempts to probe an unsupported port on your Prestige, an ICMP response packet is automatically returned. This allows the outside user to know the Prestige exists. Your Prestige supports anti-probing, which prevents the ICMP response packet from being sent. This keeps outsiders from discovering your Prestige when unsupported ports are probed.

Figure 70 Security Remote Management



☑ Do not respond to ping from WAN

The following table describes the labels in this screen.

Table 54 Security Remote Management

LABEL	DESCRIPTION
ICMP	Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.
Do not respond to ping from WAN	The Prestige will not respond to any incoming WAN Ping requests when the check box is selected.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

CHAPTER 12 UPNP

This chapter introduces the Universal Plug and Play feature.

12.1 Universal Plug and Play Overview

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

12.1.1 How Do I Know If I'm Using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

12.1.2 NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

1. Dynamic port mapping
2. Learning public IP addresses
3. Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

See the SUA/NAT chapter for further information about NAT.

12.1.3 Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

12.2 UPnP and ZyXEL

ZyXEL has achieved UPnP certification from the Universal Plug and Play Forum Creates UPnP™ Implementers Corp. (UIC). ZyXEL's UPnP implementation supports IGD 1.0 (Internet Gateway Device). At the time of writing ZyXEL's UPnP implementation supports Windows Messenger 4.6 and 4.7 while Windows Messenger 5.0 and Xbox are still being tested.

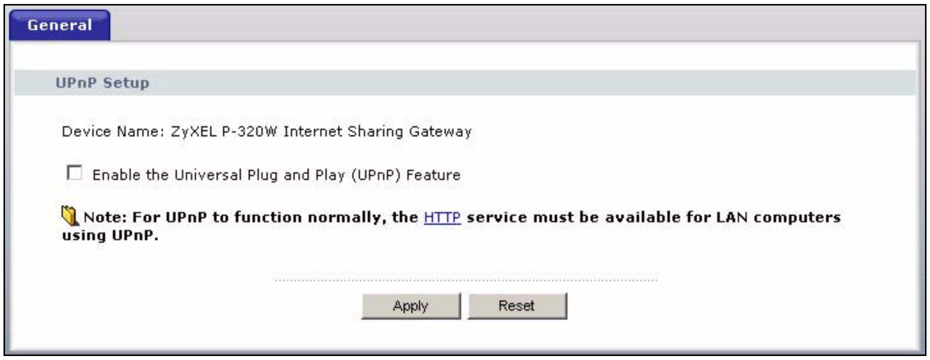
UPnP broadcasts are only allowed on the LAN.

Please see later in this User's Guide for examples of installing UPnP in Windows XP and Windows Me as well as an example of using UPnP in Windows.

12.3 UPnP Screen

Click the **UPnP** link under **Management** to display the UPnP screen.

Figure 71 Configuring UPnP



Device Name: ZyXEL P-320W Internet Sharing Gateway

□ Enable the Universal Plug and Play (UPnP) Feature

Note: For UPnP to function normally, the HTTP service must be available for LAN computers using UPnP.

The following table describes the labels in this screen.

Table 55 Configuring UPnP

LABEL	DESCRIPTION
Enable the Universal Plug and Play (UPnP) feature	Select this checkbox to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the Prestige's IP address (although you must still enter the password to access the web configurator).
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

12.4 Installing UPnP in Windows Example

This section shows how to install UPnP in Windows Me and Windows XP.

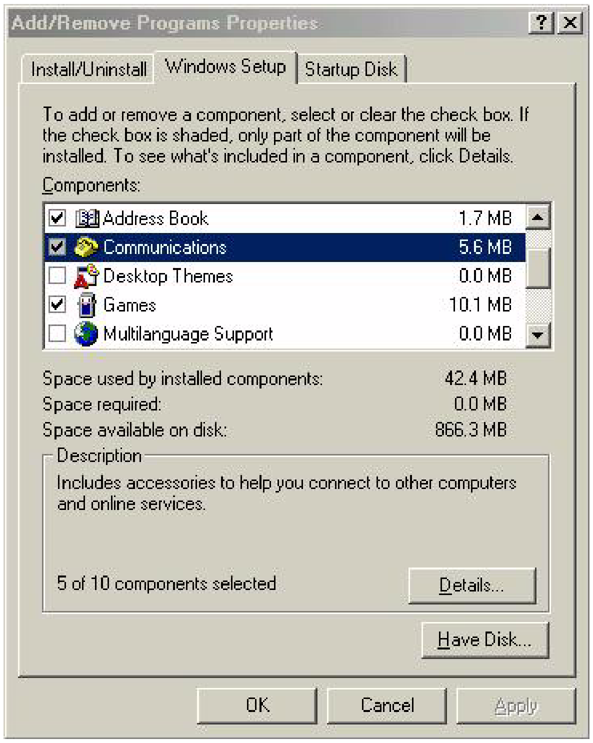
12.4.1 Installing UPnP in Windows Me

Follow the steps below to install UPnP in Windows Me.

1 Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.

2 Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.

Figure 72 Add/Remove Programs: Windows Setup: Communication



Add/Remove Programs Properties

Install/Uninstall | Windows Setup | Startup Disk

To add or remove a component, select or clear the check box. If the check box is shaded, only part of the component will be installed. To see what's included in a component, click Details.

Components:

☑	Address Book	1.7 MB
☑	Communications	5.6 MB
□	Desktop Themes	0.0 MB
☑	Games	10.1 MB
□	Multilanguage Support	0.0 MB

Space used by installed components:	42.4 MB
Space required:	0.0 MB
Space available on disk:	866.3 MB

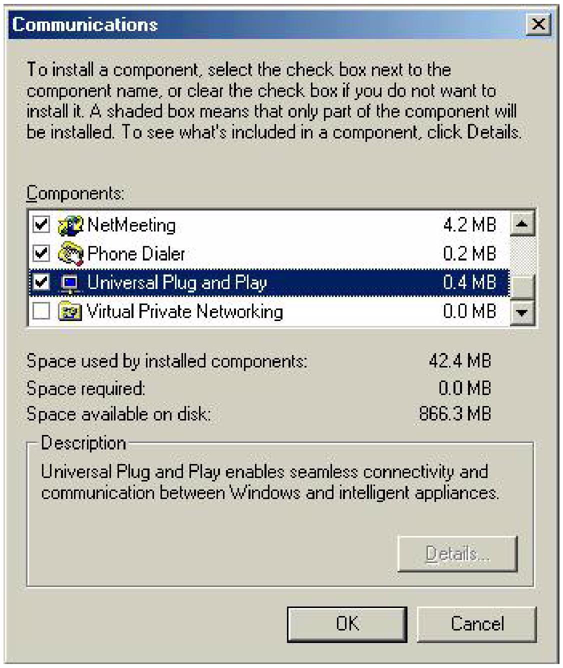
Description

Includes accessories to help you connect to other computers and online services.

5 of 10 components selected

3 In the **Communications** window, select the **Universal Plug and Play** check box in the **Components** selection box.

Figure 73 Add/Remove Programs: Windows Setup: Communication: Components



Communications

To install a component, select the check box next to the component name, or clear the check box if you do not want to install it. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

☑	NetMeeting	4.2 MB
☑	Phone Dialer	0.2 MB
☑	Universal Plug and Play	0.4 MB
□	Virtual Private Networking	0.0 MB

Space used by installed components:	42.4 MB
Space required:	0.0 MB
Space available on disk:	866.3 MB

Description

Universal Plug and Play enables seamless connectivity and communication between Windows and intelligent appliances.

4 Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.

5 Restart the computer when prompted.

12.4.2 Installing UPnP in Windows XP

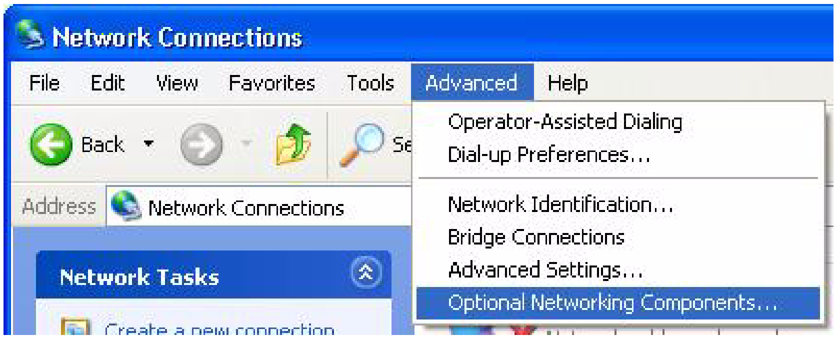
Follow the steps below to install the UPnP in Windows XP.

1 Click **Start** and **Control Panel**.

2 Double-click **Network Connections**.

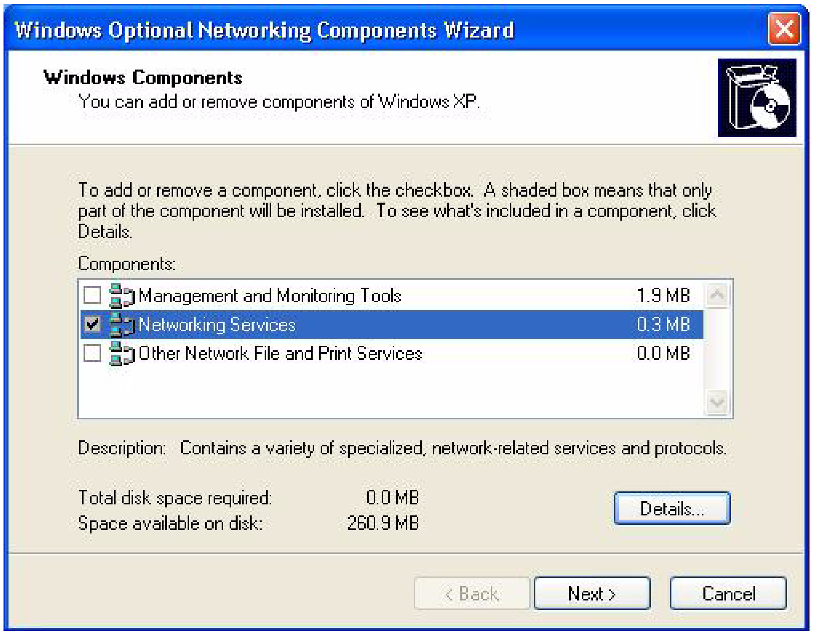
3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ….**

Figure 74 Network Connections



4 The **Windows Optional Networking Components Wizard** window displays. Select **Networking Service** in the **Components** selection box and click **Details**.

Figure 75 Windows Optional Networking Components Wizard



Windows Optional Networking Components Wizard

Windows Components
You can add or remove components of Windows XP.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

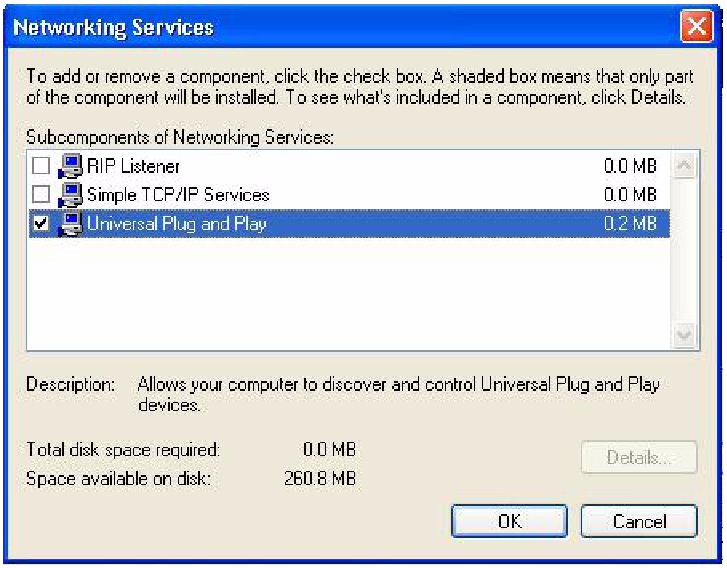
□	Management and Monitoring Tools	1.9 MB
☑	Networking Services	0.3 MB
□	Other Network File and Print Services	0.0 MB

Description: Contains a variety of specialized, network-related services and protocols.

Total disk space required: 0.0 MB
Space available on disk: 260.9 MB

5 In the **Networking Services** window, select the **Universal Plug and Play** check box.

Figure 76 Networking Services



Networking Services

To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Networking Services:

□	RIP Listener	0.0 MB
□	Simple TCP/IP Services	0.0 MB
☑	Universal Plug and Play	0.2 MB

Description: Allows your computer to discover and control Universal Plug and Play devices.

Total disk space required: 0.0 MB
Space available on disk: 260.8 MB

Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.

12.5 Using UPnP in Windows XP Example

This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the ZyXEL device.

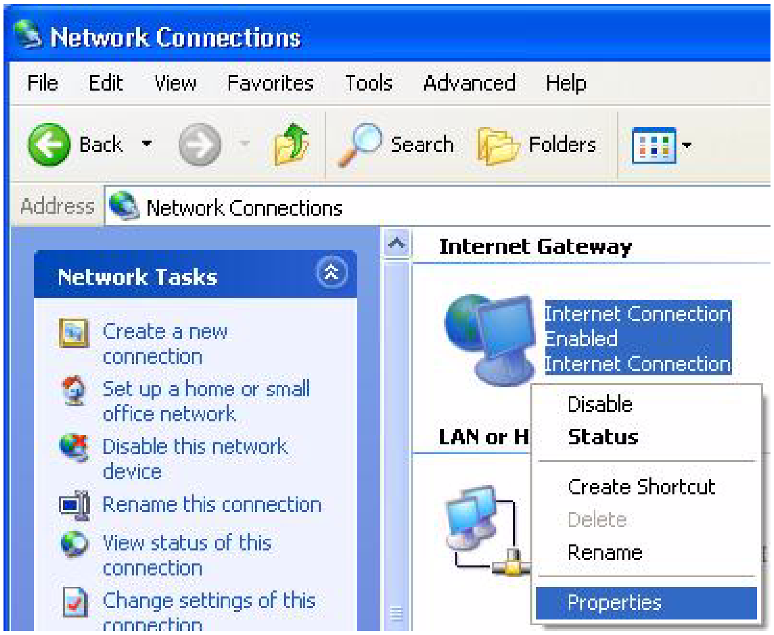
Make sure the computer is connected to a LAN port of the ZyXEL device. Turn on your computer and the ZyXEL device.

12.5.1 Auto-discover Your UPnP-enabled Network Device

1 Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.

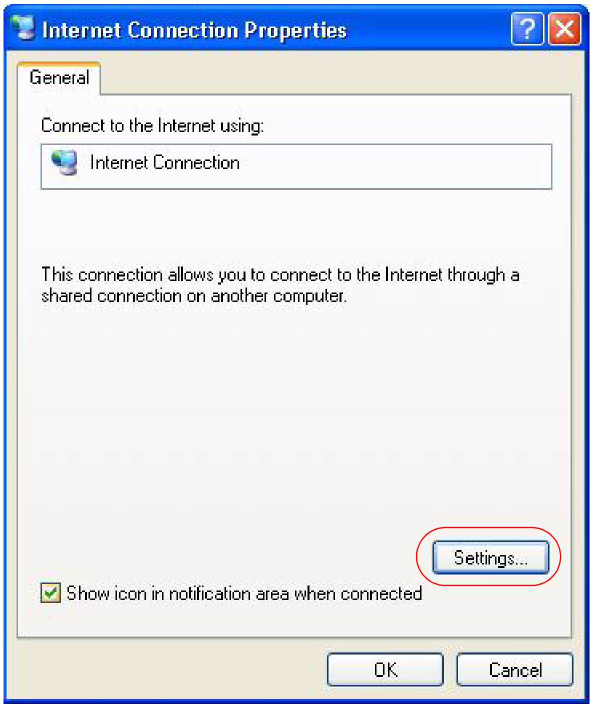
2 Right-click the icon and select **Properties**.

Figure 77 Network Connections



3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings there were automatically created.

Figure 78   Internet Connection Properties



Internet Connection Properties

General

Connect to the Internet using:

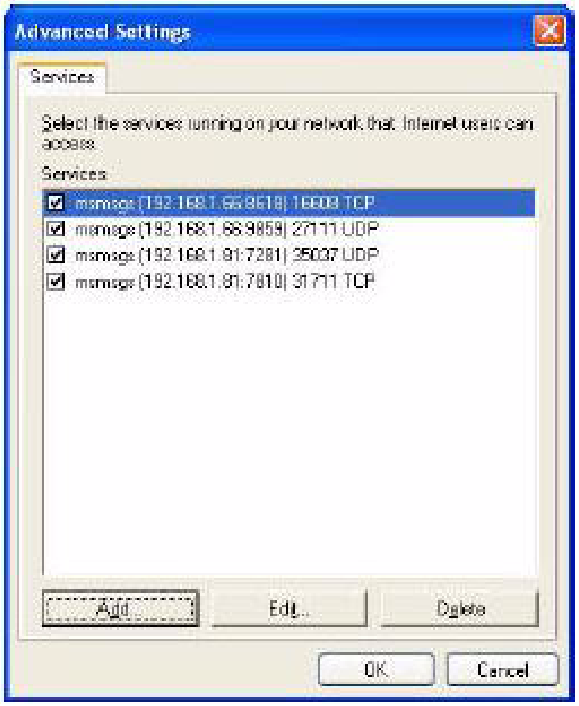
Internet Connection

This connection allows you to connect to the Internet through a shared connection on another computer.

☑ Show icon in notification area when connected

4 You may edit or delete the port mappings or click **Add** to manually add port mappings.

Figure 79   Internet Connection Properties: Advanced Settings



Advanced Settings

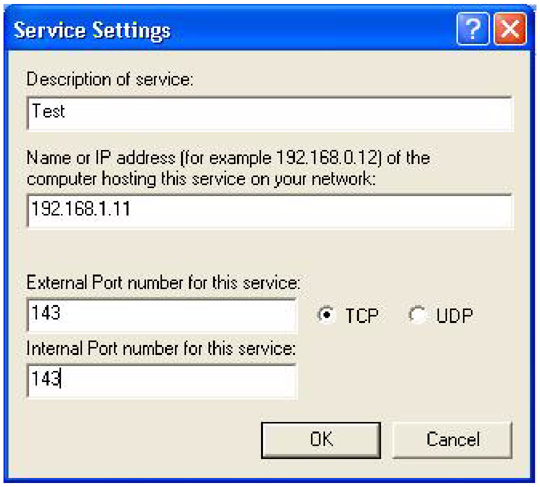
Services

Select the services running on your network that Internet users can access.

Services

☑ msmsgs (192.168.1.66:8618) 16609 TCP
☑ msmsgs (192.168.1.66:9859) 27111 UDP
☑ msmsgs (192.168.1.81:7281) 35037 UDP
☑ msmsgs (192.168.1.81:7810) 31711 TCP

Figure 80 Internet Connection Properties: Advanced Settings: Add



Service Settings

Description of service:
Test

Name or IP address (for example 192.168.0.12) of the computer hosting this service on your network:
192.168.1.11

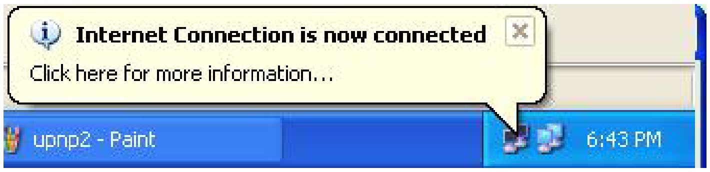
External Port number for this service:
143
● TCP ○ UDP

Internal Port number for this service:
143

5 When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

6 Select **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray.

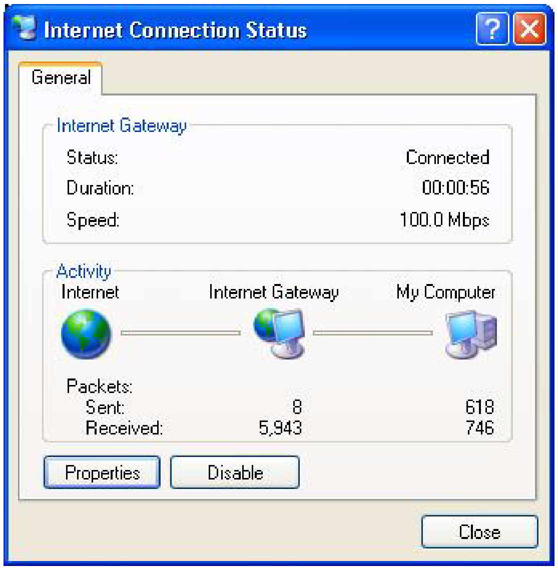
Figure 81 System Tray Icon



Internet Connection is now connected
Click here for more information...

7 Double-click on the icon to display your current Internet connection status.

Figure 82 Internet Connection Status



Internet Connection Status

Internet Gateway

Status:	Connected
Duration:	00:00:56
Speed:	100.0 Mbps

Activity

	Internet	Internet Gateway	My Computer
Packets:			
Sent:		8	618
Received:		5,943	746

12.5.2 Web Configurator Easy Access

With UPnP, you can access the web-based configurator on the ZyXEL device without finding out the IP address of the ZyXEL device first. This is helpful if you do not know the IP address of the ZyXEL device.

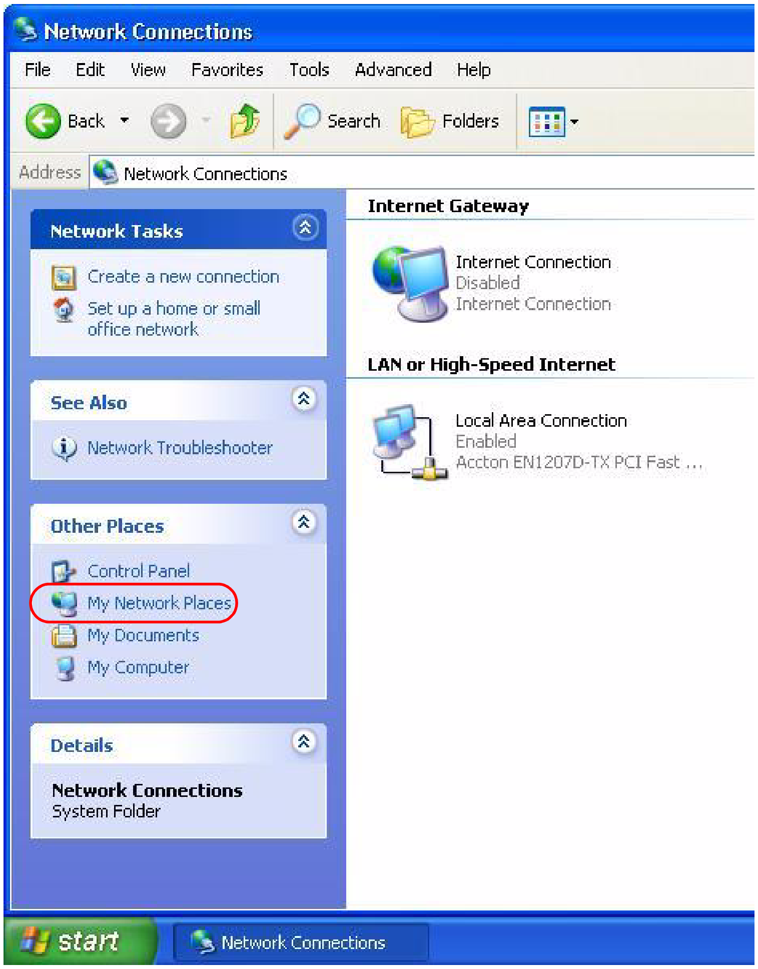
Follow the steps below to access the web configurator.

1 Click **Start** and then **Control Panel**.

2 Double-click **Network Connections**.

3 Select **My Network Places** under **Other Places**.

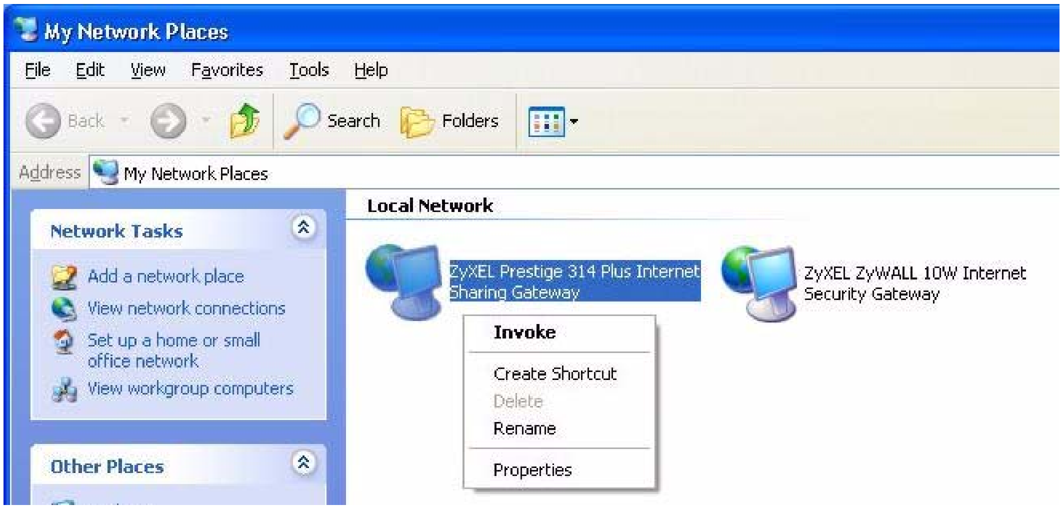
Figure 83 Network Connections



4 An icon with the description for each UPnP-enabled device displays under **Local Network**.

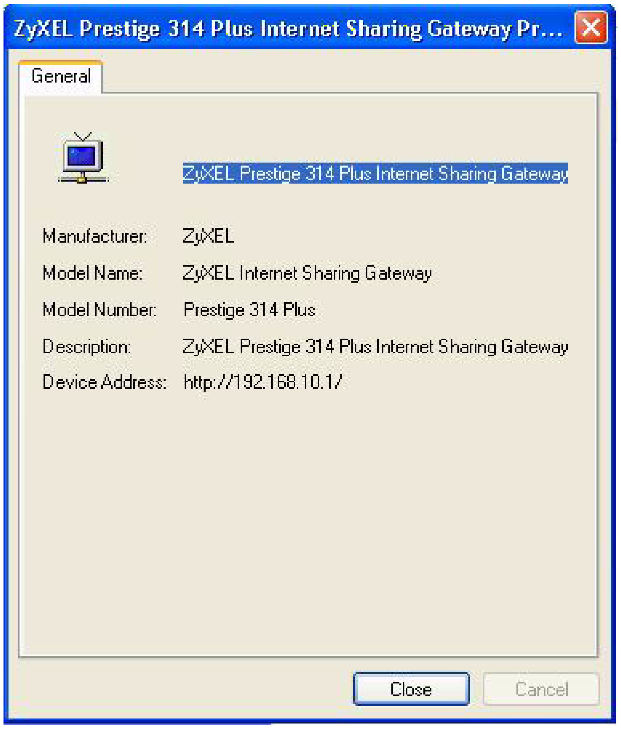
5 Right-click on the icon for your Prestige and select **Invoke**. The web configurator login screen displays.

Figure 84   Network Connections: My Network Places



6 Right-click on the icon for your Prestige and select **Properties**. A properties window displays with basic information about the Prestige.

Figure 85   Network Connections: My Network Places: Properties: Example



ZyXEL Prestige 314 Plus Internet Sharing Gateway

Manufacturer: ZyXEL

Model Name: ZyXEL Internet Sharing Gateway

Model Number: Prestige 314 Plus

Description: ZyXEL Prestige 314 Plus Internet Sharing Gateway

Device Address: http://192.168.10.1/

CHAPTER 13 System

This chapter provides information on the System screens.

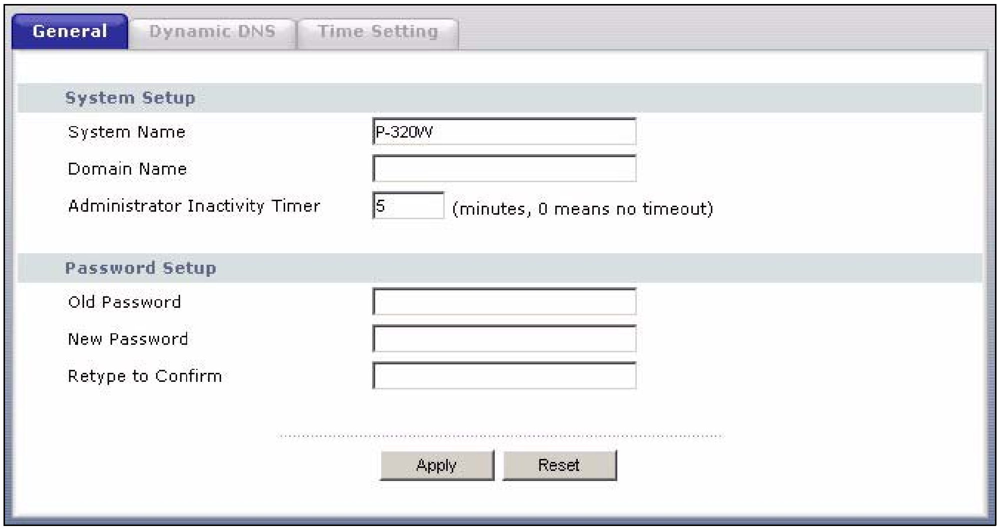
13.1 System Overview

See the Wizard Setup chapter for more information on the next few screens.

13.2 General Screen

Click the **System** link under **Maintenance** and the **General** tab. The following screen displays.

Figure 86 System General



System Setup

System Name: P-320W

Domain Name:

Administrator Inactivity Timer: 5 (minutes, 0 means no timeout)

Password Setup

Old Password:

New Password:

Retype to Confirm:

The following table describes the labels in this screen.

Table 56 System General

LABEL	DESCRIPTION
System Name	System Name is a unique name to identify the Prestige in an Ethernet network.. It is recommended you enter your computer's "Computer name" in this field (see the Wizard Setup chapter for how to find your computer's name). This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. The domain name entered by you is given priority over the ISP assigned domain name.
Administrator Inactivity Timer	Type how many minutes a management session (either via the web configurator or SMT) can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Password Setup	Change your Prestige's password (recommended) using the fields as shown.
Old Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type your new system password (up to 30 characters). Note that as you type a password, the screen displays an asterisk (*) for each character you type.
Retype to Confirm	Type the new password again in this field.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

13.3 Dynamic DNS

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

13.3.1 DynDNS Wildcard

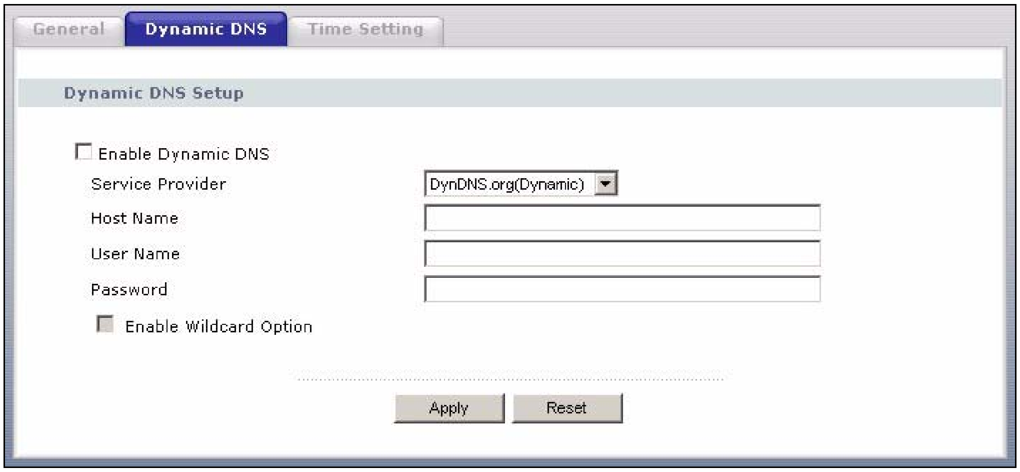
Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

Note: If you have a private WAN IP address, then you cannot use Dynamic DNS.

13.4 Dynamic DNS Screen

To change your Prestige's DDNS, click the **System** link under **Maintenance** and the **Dynamic DNS** tab. The screen appears as shown.

Figure 87 Dynamic DNS



□ Enable Dynamic DNS

Service Provider: DynDNS.org(Dynamic)

Host Name:

User Name:

Password:

□ Enable Wildcard Option

The following table describes the labels in this screen.

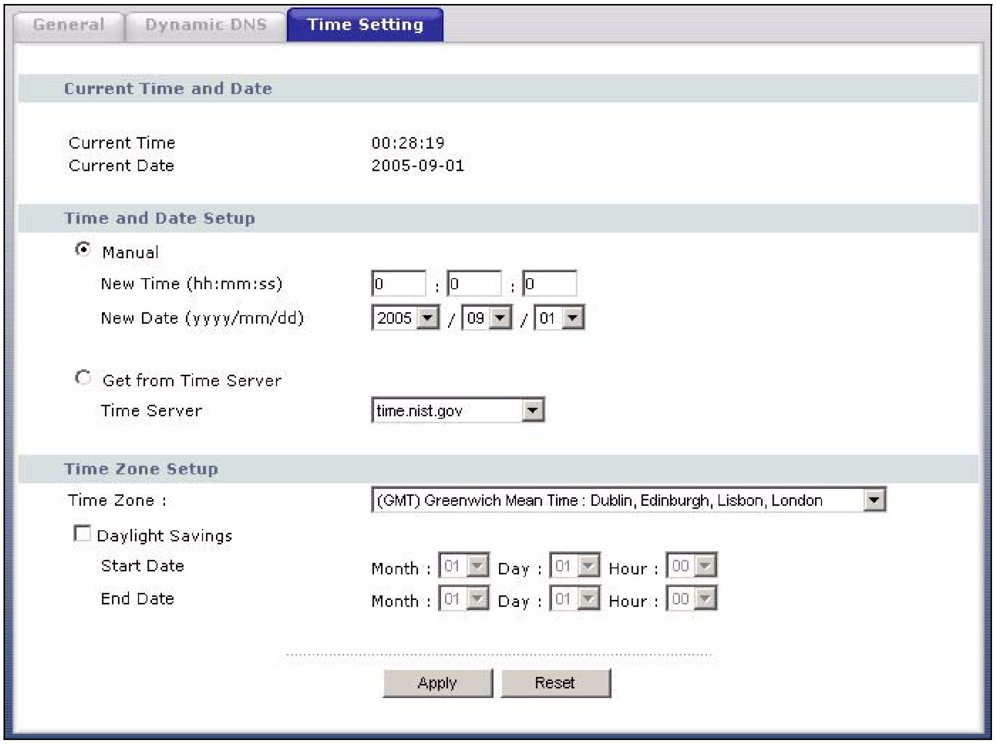
Table 57 Dynamic DNS

LABEL	DESCRIPTION
Enable Dynamic DNS	Select this check box to use dynamic DNS.
Service Provider	Select the name of your Dynamic DNS service provider.
Host Name	Enter a host namesin the feld provided. You can specify up to two host names in the field separated by a comma (",").
User Name	Enter your user name.
Password	Enter the password assigned to you.
Enable Wildcard Option	Select the check box to enable DynDNS Wildcard.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

13.5 Time Setting Screen

To change your Prestige's time and date, click the **System** link under **Maintenance** and the **Time Setting** tab. The screen appears as shown. Use this screen to configure the Prestige's time based on your local time zone.

Figure 88 Time Setting



Current Time and Date

Current Time 00:28:19
Current Date 2005-09-01

Time and Date Setup

● Manual
New Time (hh:mm:ss) 0 : 0 : 0
New Date (yyyy/mm/dd) 2005 / 09 / 01

○ Get from Time Server
Time Server time.nist.gov

Time Zone Setup

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

□ Daylight Savings
Start Date Month : 01 Day : 01 Hour : 00
End Date Month : 01 Day : 01 Hour : 00

The following table describes the labels in this screen.

Table 58 Time Setting

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the time of your Prestige. Each time you reload this page, the Prestige synchronizes the time with the time server.
Current Date	This field displays the date of your Prestige. Each time you reload this page, the Prestige synchronizes the date with the time server.
Time and Date Setup	
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, Time Zone and Daylight Saving at the same time, the new time and date you entered has priority and the Time Zone and Daylight Saving settings do not affect it.
New Time (hh:mm:ss)	This field displays the last updated time from the time server or the last time configured manually. When you set **Time and Date Setup** to **Manual**, enter the new time in this field and then click **Apply**.
New Date (yyyy-mm-dd)	This field displays the last updated date from the time server or the last date configured manually. When you set **Time and Date Setup** to **Manual**, enter the new date in this field and then click **Apply**.

Table 58 Time Setting

LABEL	DESCRIPTION
Get from Time Server	Select this radio button to have the Prestige get the time and date from the time server you specified below.
Time Server	Select the URL of your time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected **Daylight Savings**. The **Hour** field uses the 24 hour format.
End Date	Configure the day and time when Daylight Saving Time ends if you selected **Daylight Savings**. The **Hour** field uses the 24 hour format.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

CHAPTER 14
Logs

This chapter contains information about configuring general log settings and viewing the Prestige’s logs. Refer to the appendices for example log message explanations.

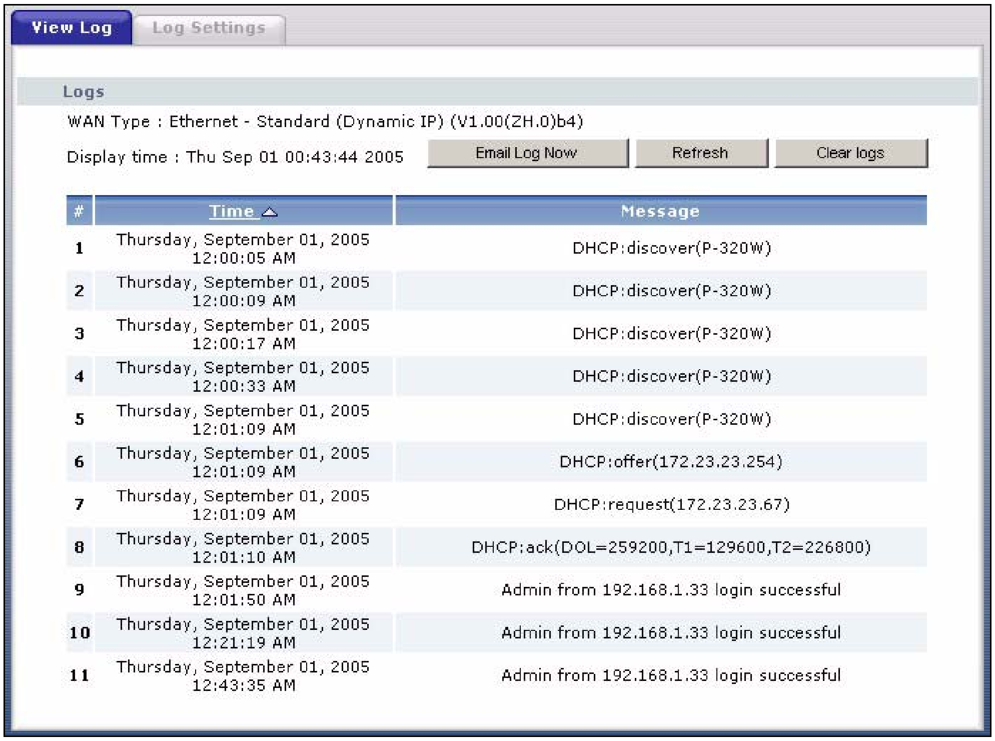
14.1 View Log

The web configurator allows you to look at all of the Prestige’s logs in one location.

Click the **Logs** link under **Maintenance** to open the **View Log** screen.

Log entries in red indicate system error logs. The log wraps around and deletes the old entries after it fills. Click a column heading to sort the entries. A triangle indicates ascending or descending sort order.

Figure 89 View Log



Logs

WAN Type : Ethernet - Standard (Dynamic IP) (V1.00(ZH.0)b4)

Display time : Thu Sep 01 00:43:44 2005

#	Time △	Message
1	Thursday, September 01, 2005 12:00:05 AM	DHCP:discover(P-320W)
2	Thursday, September 01, 2005 12:00:09 AM	DHCP:discover(P-320W)
3	Thursday, September 01, 2005 12:00:17 AM	DHCP:discover(P-320W)
4	Thursday, September 01, 2005 12:00:33 AM	DHCP:discover(P-320W)
5	Thursday, September 01, 2005 12:01:09 AM	DHCP:discover(P-320W)
6	Thursday, September 01, 2005 12:01:09 AM	DHCP:offer(172.23.23.254)
7	Thursday, September 01, 2005 12:01:09 AM	DHCP:request(172.23.23.67)
8	Thursday, September 01, 2005 12:01:10 AM	DHCP:ack(DOL=259200,T1=129600,T2=226800)
9	Thursday, September 01, 2005 12:01:50 AM	Admin from 192.168.1.33 login successful
10	Thursday, September 01, 2005 12:21:19 AM	Admin from 192.168.1.33 login successful
11	Thursday, September 01, 2005 12:43:35 AM	Admin from 192.168.1.33 login successful

The following table describes the labels in this screen.

Table 59 View Log

LABEL	DESCRIPTION
WAN Type	This shows the encapsulation method (and service type) the Prestige is using and the firmware version.
Display Time	This displays the time this screen was refreshed.
Email Log Now	Click **Email Log Now** to send the log screen to the e-mail address specified in the **Log Settings** page (make sure that you have first filled in the **E-mail Log Settings** fields in **Log Settings**).
Refresh	Click **Refresh** to renew the log screen.
Clear Logs	Click **Clear Logs** to delete all the logs.
Time	This field displays the time the log was recorded. See the chapter on time setting to configure the Prestige's time and date.
Message	This field states the reason for the log.

14.2 Log Settings

You can configure the Prestige's general log settings in one location.

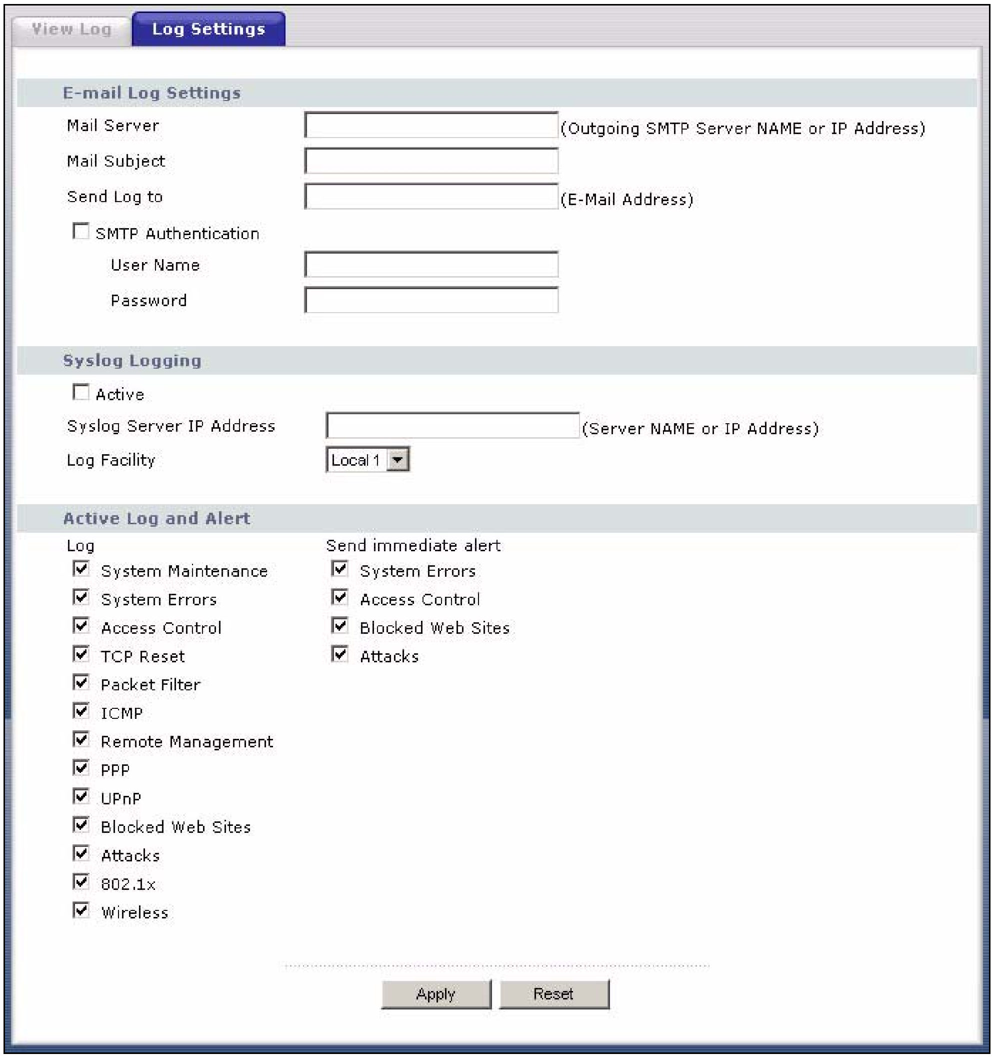
Click the **Logs** link under **Maintenance** in the navigation panel and the **Log Settings** tab to open the **Log Settings** screen.

Use the **Log Settings** screen to configure to where the Prestige is to send logs; the schedule for when the Prestige is to send the logs and which logs and/or immediate alerts the Prestige 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 **View Log** 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. Selecting many alert and/or log categories (especially **Access Control**) may result in many e-mails being sent

Figure 90 Log Settings



E-mail Log Settings

Mail Server (Outgoing SMTP Server NAME or IP Address)

Mail Subject

Send Log to (E-Mail Address)

□ SMTP Authentication

User Name

Password

Syslog Logging

□ Active

Syslog Server IP Address (Server NAME or IP Address)

Log Facility: Local 1

Active Log and Alert

Log	Send immediate alert
☑ System Maintenance	☑ System Errors
☑ System Errors	☑ Access Control
☑ Access Control	☑ Blocked Web Sites
☑ TCP Reset	☑ Attacks
☑ Packet Filter	
☑ ICMP	
☑ Remote Management	
☑ PPP	
☑ UPnP	
☑ Blocked Web Sites	
☑ Attacks	
☑ 802.1x	
☑ Wireless	

The following table describes the labels in this screen.

Table 60 Log Settings

LABEL	DESCRIPTION
E-mail Log Settings	
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 Prestige sends. Not all Prestige models have this field.
Send Log To	The Prestige sends logs to the e-mail address specified in this field. If this field is left blank, the Prestige does not send logs via e-mail.
SMTP Authentication	SMTP (Simple Mail Transfer Protocol) is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another. Select the check box to activate SMTP authentication. If mail server authentication is needed but this feature is disabled, you will not receive the e-mail logs.

Table 60 Log Settings (continued)

LABEL	DESCRIPTION
User Name	Enter the user name (up to 31 characters) (usually the user name of a mail account).
Password	Enter the password associated with the user name above.
Syslog Logging	The Prestige sends a log to an external syslog server.
Active	Click **Active** to enable syslog logging.
Syslog Server IP Address	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
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 syslog server manual for more information.
Active Log and Alert	
Log	Select the categories of logs that you want to record.
Send Immediate Alert	Select log categories for which you want the Prestige to send E-mail alerts immediately.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

CHAPTER 15
Tools

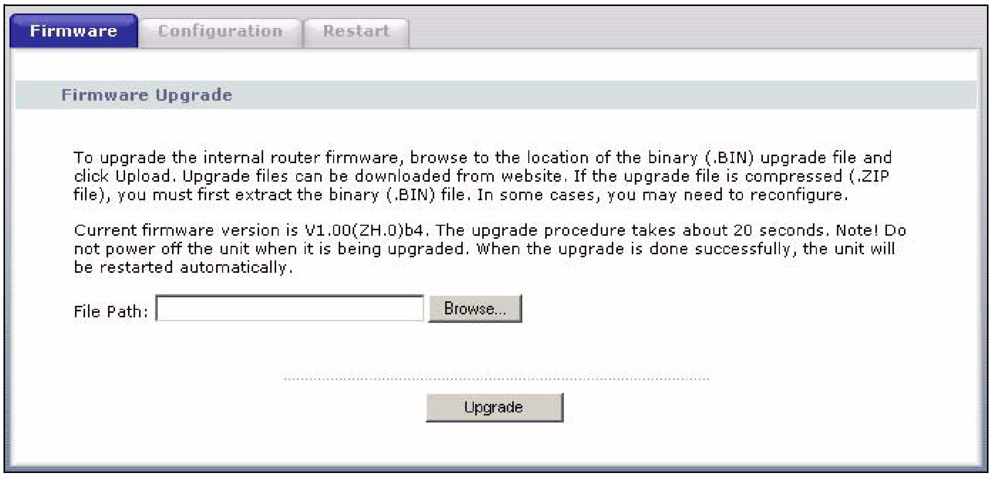
This chapter shows you how to upload a new firmware, upload or save backup configuration files and restart the Prestige.

15.1 Firmware Upload Screen

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a .bin extension, for example, "Prestige.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Click the **Tools** link under **Maintenance** in the navigation panel. Follow the instructions in this screen to upload firmware to your Prestige.

Figure 91 Maintenance Firmware Upload



To upgrade the internal router firmware, browse to the location of the binary (.BIN) upgrade file and click Upload. Upgrade files can be downloaded from website. If the upgrade file is compressed (.ZIP file), you must first extract the binary (.BIN) file. In some cases, you may need to reconfigure.

Current firmware version is V1.00(ZH.0)b4. The upgrade procedure takes about 20 seconds. Note! Do not power off the unit when it is being upgraded. When the upgrade is done successfully, the unit will be restarted automatically.

File Path:

The following table describes the labels in this screen.

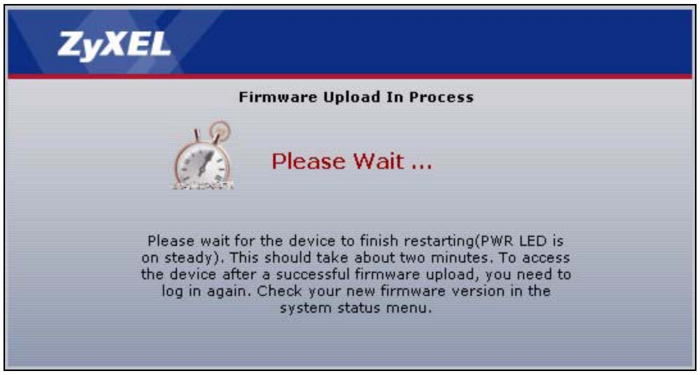
Table 61 Maintenance Firmware Upload

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upgrade	Click **Upgrade** to begin the upload process. This process may take up to two minutes.

Note: Do not turn off the Prestige while firmware upload is in progress!

After you see the **Firmware Upload In Process** screen, wait two minutes before logging into the Prestige again.

Figure 92 Upload Warning



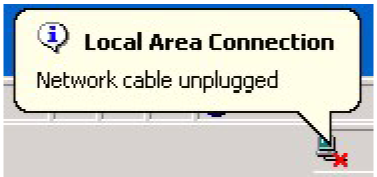
Firmware Upload In Process

Please Wait ...

Please wait for the device to finish restarting(PWR LED is on steady). This should take about two minutes. To access the device after a successful firmware upload, you need to log in again. Check your new firmware version in the system status menu.

The Prestige automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 93 Network Temporarily Disconnected



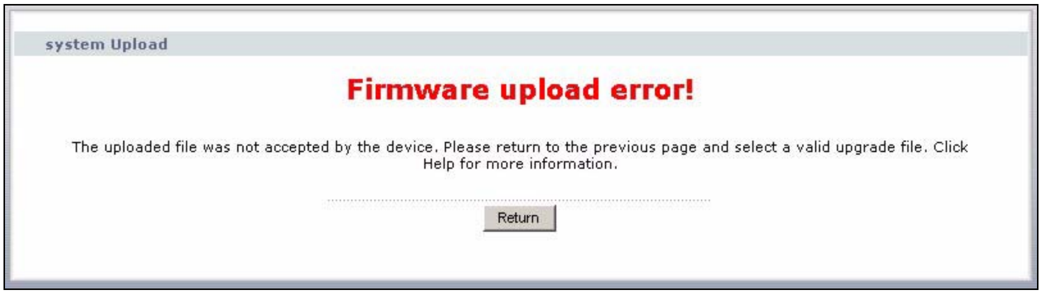
Local Area Connection

Network cable unplugged

After two minutes, log in again and check your new firmware version in the **Status** screen.

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **Firmware** screen.

Figure 94 Upload Error Message



system Upload

Firmware upload error!

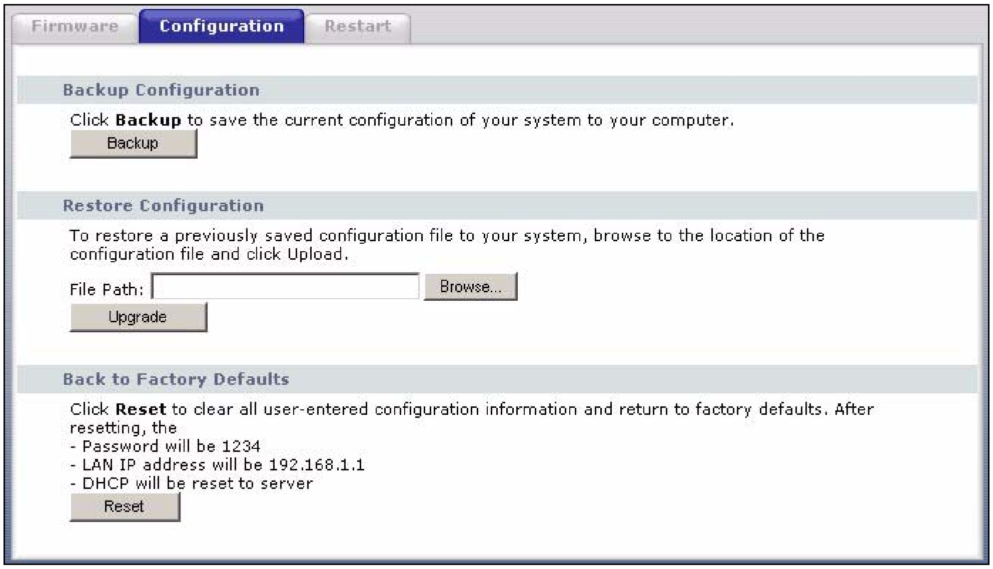
The uploaded file was not accepted by the device. Please return to the previous page and select a valid upgrade file. Click Help for more information.

15.2 Configuration Screen

See the Firmware and Configuration File Maintenance chapter for transferring configuration files using FTP/TFTP commands.

Click the **Tools** link under **Maintenance**, and the **Configuration** tab. Information related to factory defaults, backup configuration, and restoring configuration appears as shown next.

Figure 95 Configuration



Backup Configuration

Click **Backup** to save the current configuration of your system to your computer.

Restore Configuration

To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.

File Path:

Back to Factory Defaults

Click **Reset** to clear all user-entered configuration information and return to factory defaults. After resetting, the
- Password will be 1234
- LAN IP address will be 192.168.1.1
- DHCP will be reset to server

15.2.1 Backup Configuration

Backup configuration allows you to back up (save) the Prestige's current configuration to a file on your computer. Once your Prestige 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.

Click **Backup** to save the Prestige's current configuration to your computer

15.2.2 Restore Configuration

Restore configuration allows you to upload a new or previously saved configuration file from your computer to your Prestige.

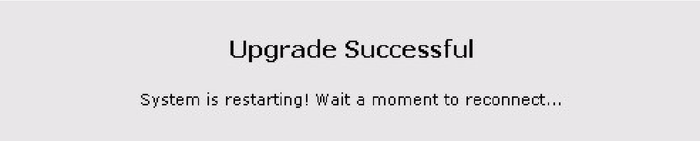
Table 62 Maintenance: Restore Configuration

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upgrade	Click **Upgrade** to begin the upload process.

Note: Do not turn off the Prestige while configuration file upload is in progress

After you see a "Upgrade Successful" screen, you must then wait one minute before logging into the Prestige again.

Figure 96 Configuration Restore Successful

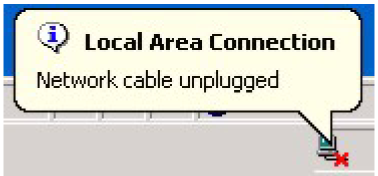


Upgrade Successful

System is restarting! Wait a moment to reconnect...

The Prestige automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 97 Temporarily Disconnected



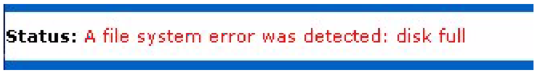
Local Area Connection

Network cable unplugged

If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default Prestige IP address (192.168.1.1). See the appendix for details on how to set up your computer's IP address.

If the upload was not successful, the following screen will appear.

Figure 98 Configuration Restore Error



Status: A file system error was detected: disk full

15.2.3 Back to Factory Defaults

Pressing the **Restart** button in this section clears all user-entered configuration information and returns the Prestige to its factory defaults.

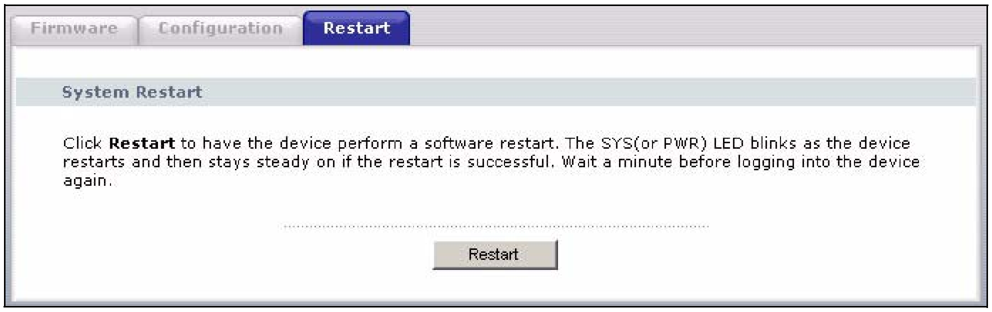
You can also press the **RESET** button on the rear panel to reset the factory defaults of your Prestige. Refer to Chapter 2 on page 35 for more information on the **RESET** button.

15.3 Restart Screen

System restart allows you to reboot the Prestige without turning the power off.

Click the Tools link under **Maintenance**, and the **Restart** tab. Click **Restart** to have the Prestige reboot. This does not affect the Prestige's configuration.

Figure 99 System Restart



System Restart

Click **Restart** to have the device perform a software restart. The SYS(or PWR) LED blinks as the device restarts and then stays steady on if the restart is successful. Wait a minute before logging into the device again.

CHAPTER 16
Troubleshooting

This chapter covers potential problems and the corresponding remedies.

16.1 Problems Starting Up the Prestige

Table 63 Troubleshooting Starting Up Your Prestige

PROBLEM	CORRECTIVE ACTION
None of the LEDs turn on when I turn on the Prestige.	Make sure that the Prestige's power adaptor is connected to the Prestige and plugged in to an appropriate power source. Make sure that the Prestige and the power source are both turned on. Turn the Prestige off and on. If the error persists, you may have a hardware problem. In this case, you should contact your vendor.

16.2 Problems with the LAN

Table 64 Troubleshooting the LAN

PROBLEM	CORRECTIVE ACTION
The LAN LEDs do not turn on.	Check your Ethernet cable connections (refer to the Quick Start Guide for details). Check for faulty Ethernet cables.
	Make sure your computer's Ethernet Card is working properly.
I cannot access the Prestige from the LAN.	If **Any IP** is disabled, make sure that the IP address and the subnet mask of the Prestige and your computer(s) are on the same subnet.

16.3 Problems with the WAN

Table 65 Troubleshooting the WAN

PROBLEM	CORRECTIVE ACTION
The WAN LED is off.	Check the connections between the Prestige WAN port and the cable/DSL modem or ethernet jack.
	Check whether your cable/DSL device requires a crossover or straight-through cable.
I cannot get a WAN IP address from the ISP.	Click WAN to verify your settings. The username and password apply to PPPoE and PPPoA encapsulation only. Make sure that you have entered the correct **Service Type**, **User Name** and **Password** (be sure to use the correct casing). Refer to the WAN Setup chapter.
I cannot access the Internet.	Make sure the Prestige is turned on and connected to the network. Verify your WAN settings. Refer to the chapter on WAN setup. Make sure you entered the correct user name and password. If you use PPPoE pass through, make sure that bridge mode is turned on.
The Internet connection disconnects.	If you use PPPoE encapsulation, check the idle time-out setting. Refer to the Chapter 5 on page 81.

16.4 Problems with the Password

Table 66 Troubleshooting the Password

PROBLEM	CORRECTIVE ACTION
Cannot access the Prestige.	The password field is case sensitive. Make sure that you enter the correct password using the proper casing.
	Use the **RESET** button to restore the factory default configuration file. This will restore all of the factory defaults including the password; see Section 2.3 on page 37 for details.

16.5 Problems with Remote Management

Table 67 Troubleshooting Telnet

PROBLEM	CORRECTIVE ACTION
Cannot access the Prestige from the LAN or WAN.	Refer to Section 11.1.1 on page 119 for scenarios when remote management may not be possible.
	When NAT is enabled: • Use the Prestige's WAN IP address when configuring from the WAN. • Use the Prestige's LAN IP address when configuring from the LAN.

16.6 Problems Accessing the Prestige

Table 68 Troubleshooting Accessing the Prestige

PROBLEM	CORRECTIVE ACTION
I cannot access the Prestige.	The username is "admin". The default password is "1234". The **Password** and **Username** fields are case-sensitive. Make sure that you enter the correct password and username using the proper casing. If you have changed the password and have now forgotten it, you will need to upload the default configuration file. This restores all of the factory defaults including the password.
I cannot access the web configurator.	Use the Prestige's WAN IP address when configuring from the WAN. Refer to the instructions on checking your WAN connection. Use the Prestige's LAN IP address when configuring from the LAN. Refer to for instructions on checking your LAN connection. Check that you have enabled web service access. If you have configured a secured client IP address, your computer's IP address must match it. Refer to the chapter on remote management for details. Your computer's and the Prestige's IP addresses must be on the same subnet for LAN access. If you changed the Prestige's LAN IP address, then enter the new one as the URL. See the following section to check that pop-up windows, JavaScripts and Java permissions are allowed.
	You may also need to clear your Internet browser's cache. In Internet Explorer, click **Tools** and then **Internet Options** to open the **Internet Option**s screen. In the **General** tab, click **Delete Files**. In the pop-up window, select the **Delete all offline content** check box and click **OK**. Click **OK** in the **Internet Options** screen to close it.
	If you disconnect your computer from one device and connect it to another device that has the same IP address, your computer's ARP (Address Resolution Protocol) table may contain an entry that maps the management IP address to the previous device's MAC address). In Windows, use **arp -d** at the command prompt to delete all entries in your computer's ARP table.

16.6.1 Pop-up Windows, JavaScripts and Java Permissions

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

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

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

16.6.1.1 Internet Explorer Pop-up Blockers

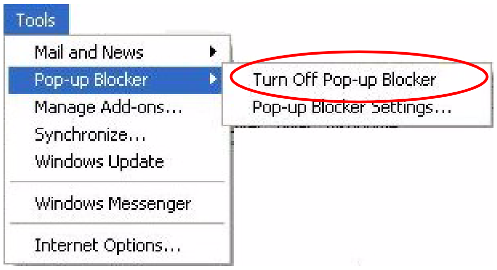
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

16.6.1.1.1 Disable pop-up Blockers

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

Figure 100 Pop-up Blocker

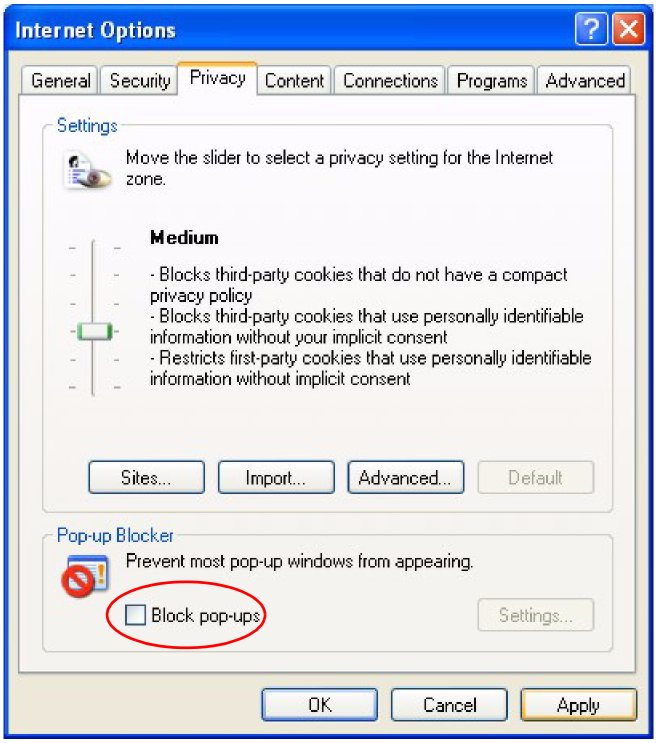


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 101 Internet Options



Move the slider to select a privacy setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

Prevent most pop-up windows from appearing.

□ Block pop-ups

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

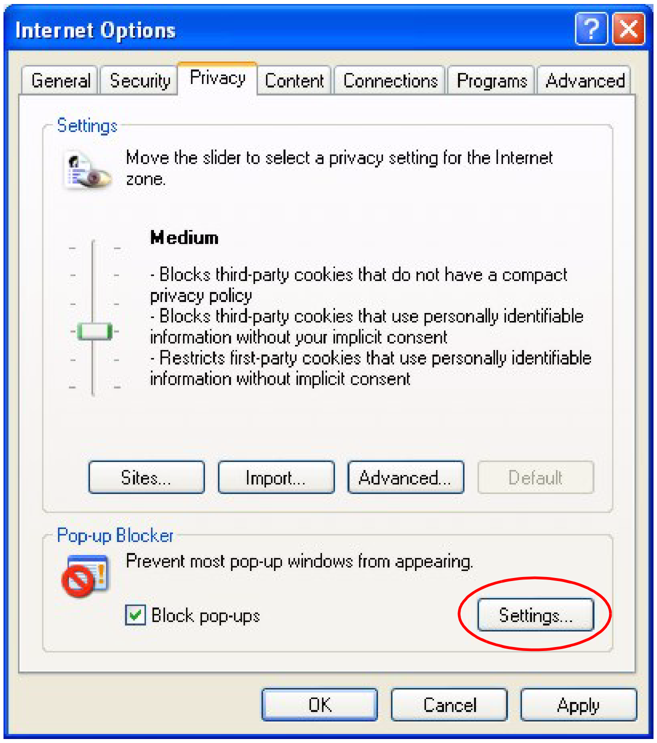
16.6.1.1.2 Enable pop-up Blockers with Exceptions

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

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings…**to open the **Pop-up Blocker Settings** screen.

Figure 102 Internet Options



Move the slider to select a privacy setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

Prevent most pop-up windows from appearing.

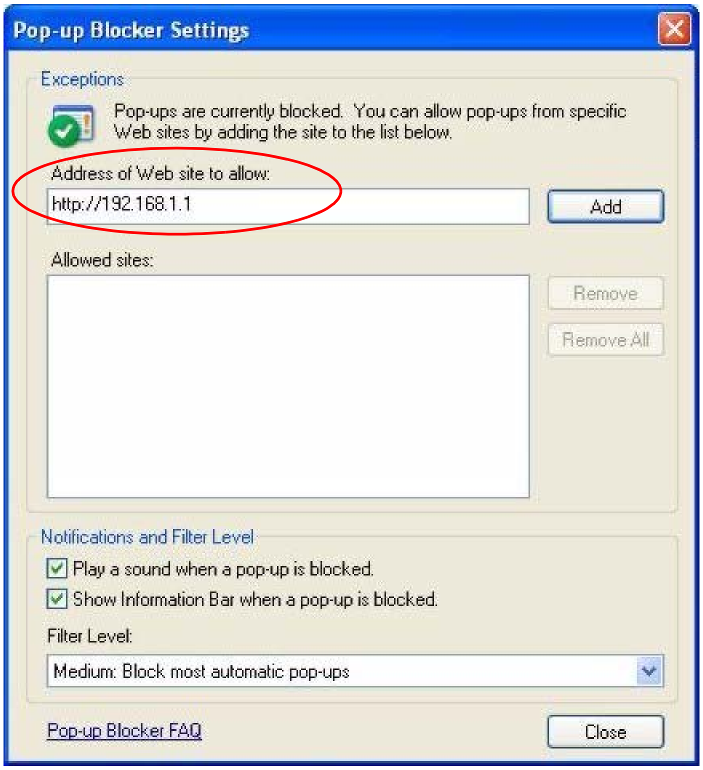
☑ Block pop-ups

3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix “http://”. For example, http://192.168.1.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

Note: If you change the IP address of your device, make sure that the new address matches the address you type in the **Pop-up Blocker Settings** screen.

Figure 103 Pop-up Blocker Settings



Pop-up Blocker Settings

Exceptions

Pop-ups are currently blocked. You can allow pop-ups from specific Web sites by adding the site to the list below.

Address of Web site to allow: http://192.168.1.1

Allowed sites:

Notifications and Filter Level

☑ Play a sound when a pop-up is blocked.

☑ Show Information Bar when a pop-up is blocked.

Filter Level: Medium: Block most automatic pop-ups

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

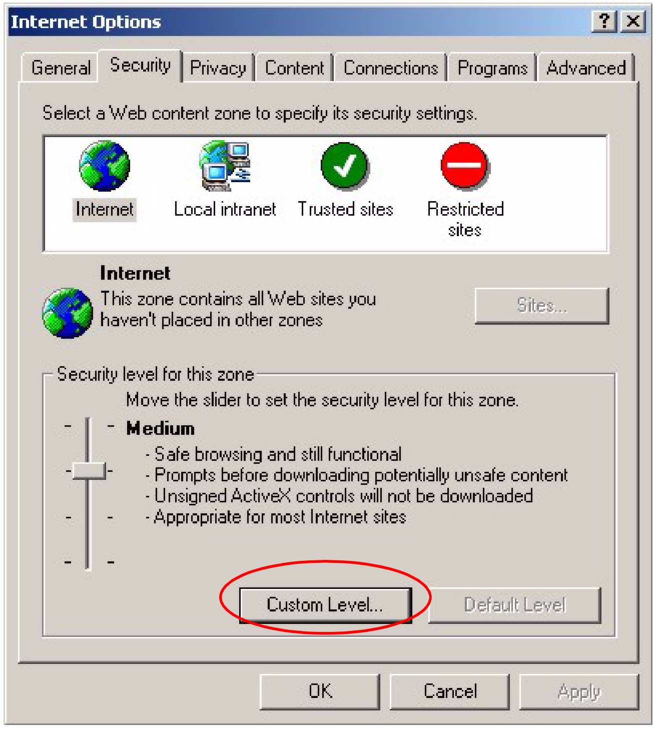
6 Click **Apply** to save this setting.

16.6.1.2 JavaScripts

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

Figure 104 Internet Options



Select a Web content zone to specify its security settings.

Internet

This zone contains all Web sites you haven't placed in other zones

Security level for this zone

Move the slider to set the security level for this zone.

Medium

- Safe browsing and still functional
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded
- Appropriate for most Internet sites

2 Click the **Custom Level...** button.

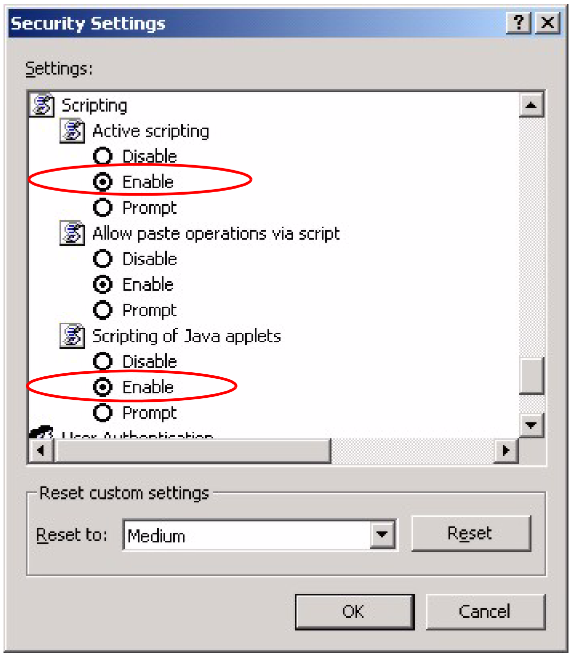
3 Scroll down to **Scripting**.

4 Under **Active scripting** make sure that **Enable** is selected (the default).

5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

6 Click **OK** to close the window.

Figure 105 Security Settings - Java Scripting



Security Settings

Settings:

Scripting

Active scripting

○ Disable

● Enable

○ Prompt

Allow paste operations via script

○ Disable

● Enable

○ Prompt

Scripting of Java applets

○ Disable

● Enable

○ Prompt

User Authentication

Reset custom settings

Reset to: Medium

16.6.1.3 Java Permissions

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

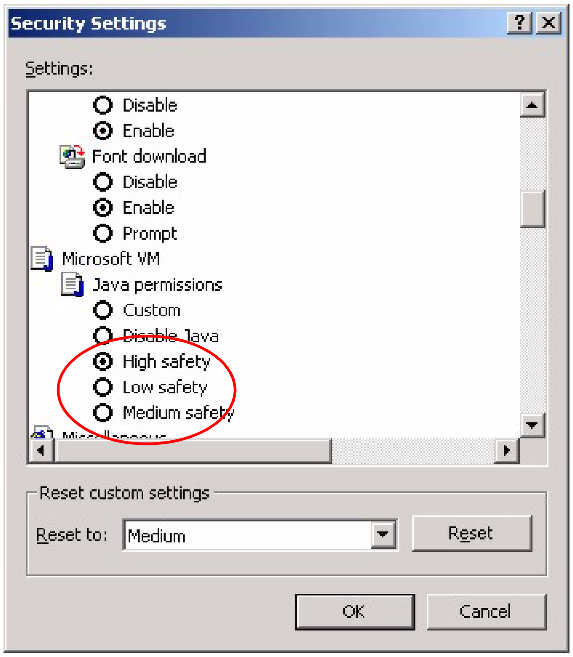
2 Click the **Custom Level...** button.

3 Scroll down to **Microsoft VM**.

4 Under **Java permissions** make sure that a safety level is selected.

5 Click **OK** to close the window.

Figure 106 Security Settings - Java



Settings:

- ○ Disable
- ● Enable
- Font download
  - ○ Disable
  - ● Enable
  - ○ Prompt
- Microsoft VM
  - Java permissions
    - ○ Custom
    - ○ Disable Java
    - ● High safety
    - ○ Low safety
    - ○ Medium safety
- Miscellaneous

Reset to: Medium

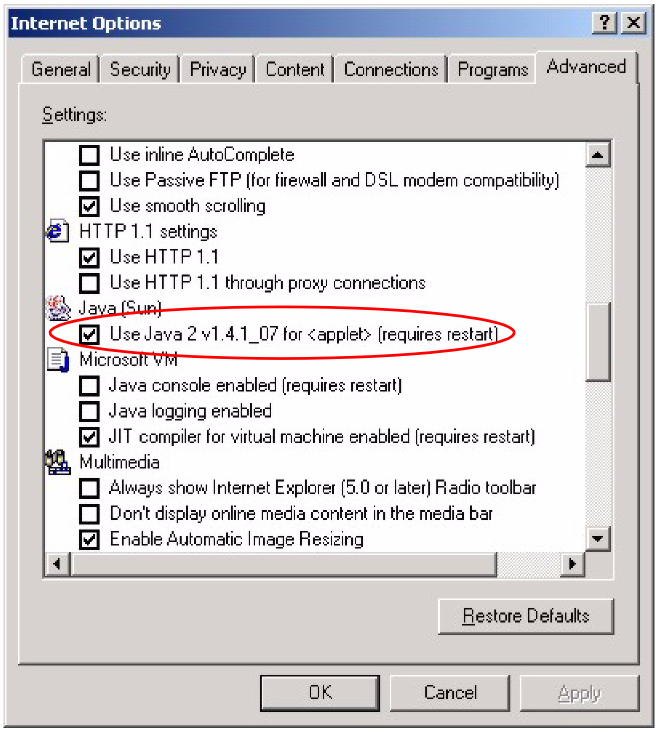
16.6.1.3.1 JAVA (Sun)

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.

2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

3 Click **OK** to close the window.

Figure 107 Java (Sun)



Settings:

- □ Use inline AutoComplete
- □ Use Passive FTP (for firewall and DSL modem compatibility)
- ☑ Use smooth scrolling
- HTTP 1.1 settings
  - ☑ Use HTTP 1.1
  - □ Use HTTP 1.1 through proxy connections
- Java (Sun)
  - ☑ Use Java 2 v1.4.1_07 for <applet> (requires restart)
- Microsoft VM
  - □ Java console enabled (requires restart)
  - □ Java logging enabled
  - ☑ JIT compiler for virtual machine enabled (requires restart)
- Multimedia
  - □ Always show Internet Explorer (5.0 or later) Radio toolbar
  - □ Don't display online media content in the media bar
  - ☑ Enable Automatic Image Resizing

16.6.2 ActiveX Controls in Internet Explorer

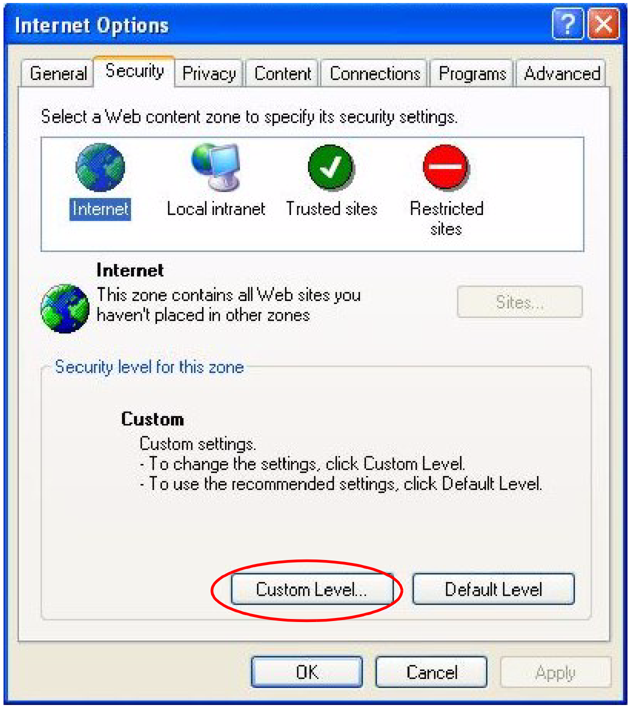
If ActiveX is disabled, you will not be able to download ActiveX controls or to use Trend Micro Security Serivces. Make sure that ActiveX controls are allowed in Internet Explorer.

Screen shots for Internet Explorer 6 are shown. Steps may vary depending on your version of Internet Explorer.

1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

2 In the **Internet Options** window, click **Custom Level**.

Figure 108 Internet Options Security



Select a Web content zone to specify its security settings.

Internet
This zone contains all Web sites you haven't placed in other zones

Custom
Custom settings.
- To change the settings, click Custom Level.
- To use the recommended settings, click Default Level.

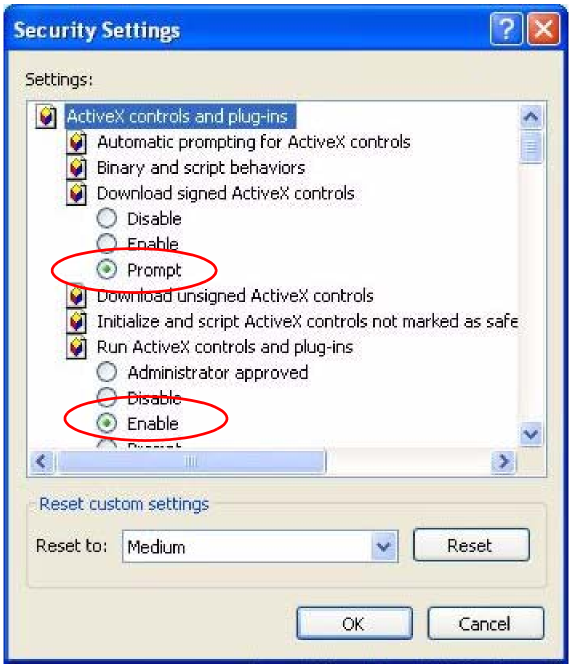
3 Scroll down to **ActiveX controls and plug-ins**.

4 Under **Download signed ActiveX controls** select the **Prompt** radio button.

5 Under **Run ActiveX controls and plug-ins** make sure the **Enable** radio button is selected.

6 Then click the **OK** button.

Figure 109   Security Setting ActiveX Controls



Security Settings

Settings:

- ActiveX controls and plug-ins
  - Automatic prompting for ActiveX controls
  - Binary and script behaviors
  - Download signed ActiveX controls
    - ○ Disable
    - ○ Enable
    - ● Prompt
  - Download unsigned ActiveX controls
  - Initialize and script ActiveX controls not marked as safe
  - Run ActiveX controls and plug-ins
    - ○ Administrator approved
    - ○ Disable
    - ● Enable

Reset custom settings

Reset to: Medium

APPENDIX A
Product Specifications

See also the Introduction chapter for a general overview of the key features.

Specification Tables

Table 69 Device

Default IP Address	192.168.1.1
Default Subnet Mask	255.255.255.0 (24 bits)
Default Password	1234
DHCP Pool	192.168.1.32 to 192.168.1.64
Dimensions	(181 W) x (128 D) x (36 H) mm
Weight	424g
Power Specification	12VAC
Built-in Switch	Four auto-negotiating, auto MDI/MDI-X 10/100/1000 Mbps RJ-45 Ethernet ports
Operation Temperature	0º C ~ 65º C
Storage Temperature	-20º ~ 60º C
Operation Humidity	15% ~ 90% RH
Storage Humidity	10% ~ 90% RH

Table 70 Firmware

Standards	IEEE 802.3 Ethernet IEEE 802.3u Fast Ethernet IEEE 802.3ab Gigabit Ethernet TCP, UDP, ICMP, ARP, RIP - 1/RIP - 2 IP Routing (RFC 791) PPP over Ethernet (RFC 2516) MAC encapsulated routing (ENET encapsulation)
Other Protocol Support	PPP (Point-to-Point Protocol) link layer protocol. DHCP Server (RFC 2131, 2132) RIP I/RIP II ICMP SNMP v1 and v2c with MIB II support (RFC 1213) UPnP
Management	Embedded Web Configurator Remote Management via Web SNMP manageable Configuration backup and restoration. Built-in Diagnostic Tools for FLASH memory, RAM and LAN port Syslog

Table 70 Firmware (continued)

Wireless	IEEE 802.11g Compliance Frequency Range: 2.4 GHz Advanced Orthogonal Frequency Division Multiplexing (OFDM) Data Rates: 54Mbps and Auto Fallback Wired Equivalent Privacy (WEP) Data Encryption 64/128/256 bit. WLAN bridge to LAN Up to 32 MAC Address filters WPA, WPA-PSK OTIST (One Touch Intelligent Security Technology) IEEE 802.1x External Radius server using EAP-MD5, TLS, TTLS
Firewall	Stateful Packet Inspection. Prevent Denial of Service attacks such as Fraggle, SYN Flood, Land attack, Smurf etc. Real time E-mail alerts Reports and logs
NAT/SUA	Port Forwarding 4096 NAT sessions Multimedia application PPTP under NAT/SUA IPSec passthrough SIP ALG passthrough Cone NAT (Port-restricted NAT)
Static Routes	8 IP
Other Features	Traffic Redirect Dynamic DNS SMTP Authentication

APPENDIX B
IP Subnetting

IP Addressing

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

IP Classes

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

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

Table 71 Classes of IP Addresses

			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 72 Allowed IP Address Range By Class

	ALLOWED RANGE OF FIRST OCTET (BINARY)	ALLOWED RANGE OF FIRST OCTET (DECIMAL)
Class A	**0**0000000 to **0**1111111	0 to 127
Class B	**10**000000 to **10**111111	128 to 191
Class C	**110**00000 to **110**11111	192 to 223
Class D	**1110**0000 to **1110**1111	224 to 239

Subnet Masks

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

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

Table 73 "Natural" Masks

	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 74 Alternative Subnet Mask Notation

	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 75 Two Subnets Example

		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 76 Subnet 1

		LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**0**0000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	**1**0000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 77 Subnet 2

		LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**1**0000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	**1**0000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

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

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

Example: Four Subnets

The above example illustrated using a 25-bit subnet mask to divide a class "C" address space into two subnets. Similarly to divide a class "C" address into four subnets, you need to "borrow" two host ID bits to give four possible combinations of 00, 01, 10 and 11. The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192. Each subnet contains 6 host ID bits, giving 2^6-2 or 62 hosts for each subnet (all 0's is the subnet itself, all 1's is the broadcast address on the subnet).

Table 78 Subnet 1

		LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 79 Subnet 2

		LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 80 Subnet 3

		LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 81 Subnet 4

		LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example Eight Subnets

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

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

Table 82 Eight Subnets

	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

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

Table 83 Class C Subnet Planning

	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 71 on page 165) available for subnetting.

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

Table 84 Class B Subnet Planning

	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 C
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.

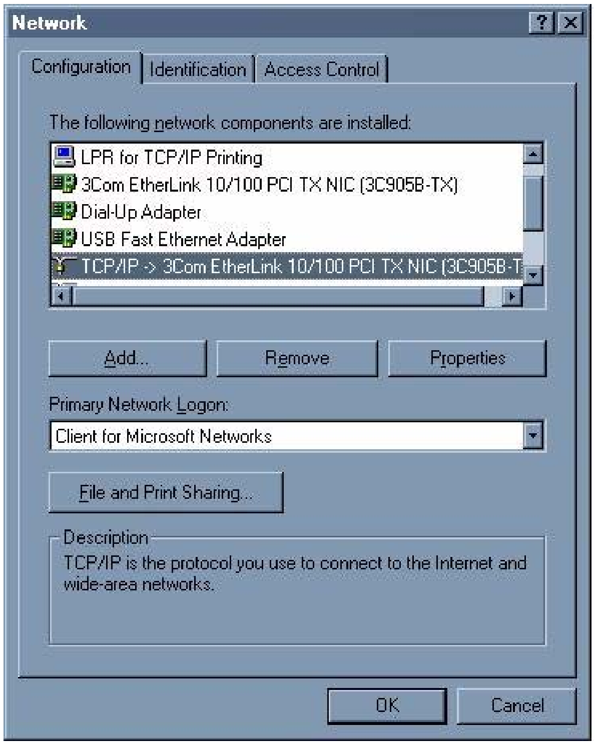
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

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 110 WIndows 95/98/Me: Network: Configuration



Network

Configuration | Identification | Access Control

The following network components are installed:

- LPR for TCP/IP Printing
- 3Com EtherLink 10/100 PCI TX NIC (3C905B-TX)
- Dial-Up Adapter
- USB Fast Ethernet Adapter
- TCP/IP -> 3Com EtherLink 10/100 PCI TX NIC (3C905B-T

Primary Network Logon:

Client for Microsoft Networks

Description

TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

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.

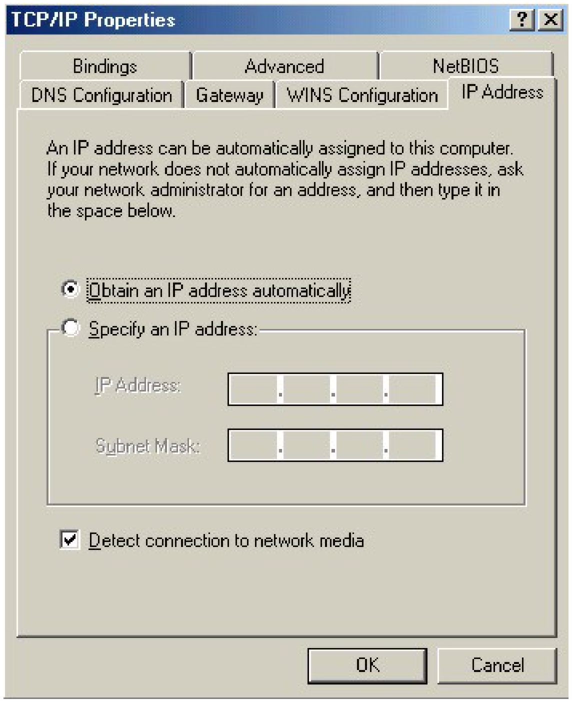
Configuring

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 111 Windows 95/98/Me: TCP/IP Properties: IP Address



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

○ Specify an IP address:

IP Address: . . .

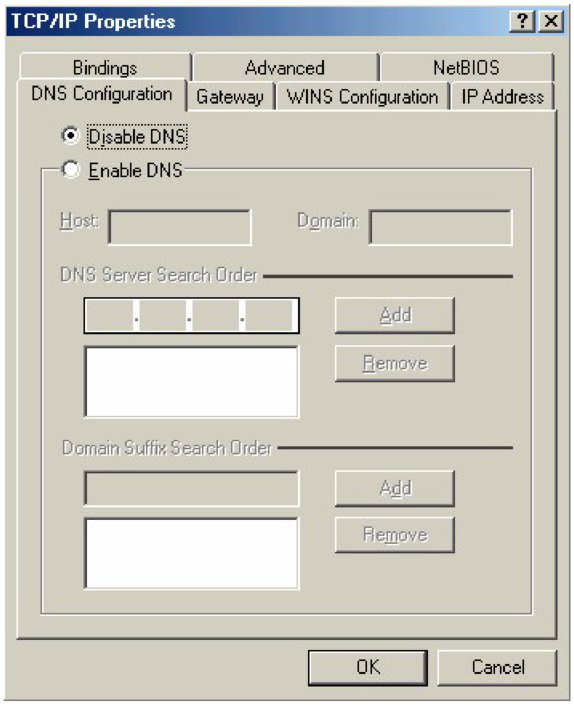
Subnet Mask: . . .

☑ Detect connection to network media

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 112 Windows 95/98/Me: TCP/IP Properties: DNS Configuration



● Disable DNS

○ Enable DNS

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.

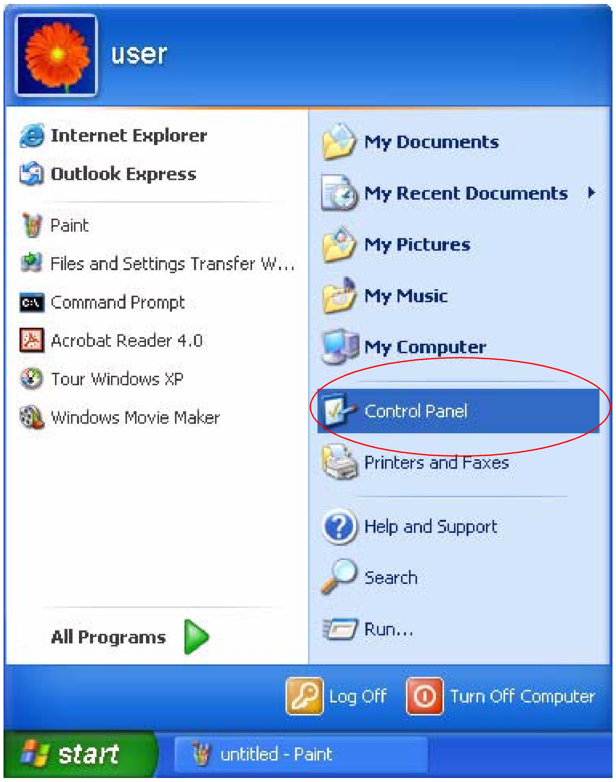
3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

The following example figures use the default Windows XP GUI theme.

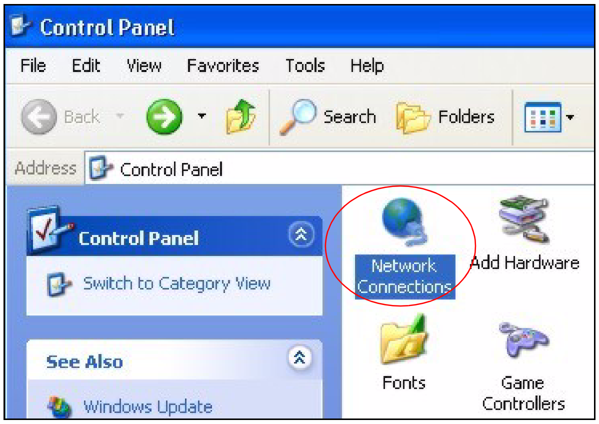
1 Click **start** (**Start** in Windows 2000/NT), **Settings**, **Control Panel**.

Figure 113 Windows XP: Start Menu



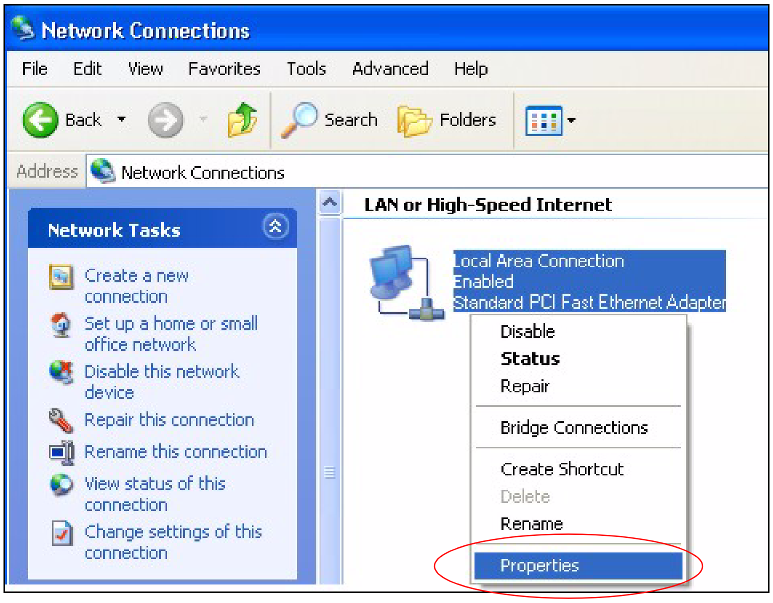
2 In the **Control Panel**, double-click **Network Connections** (**Network and Dial-up Connections** in Windows 2000/NT).

Figure 114 Windows XP: Control Panel



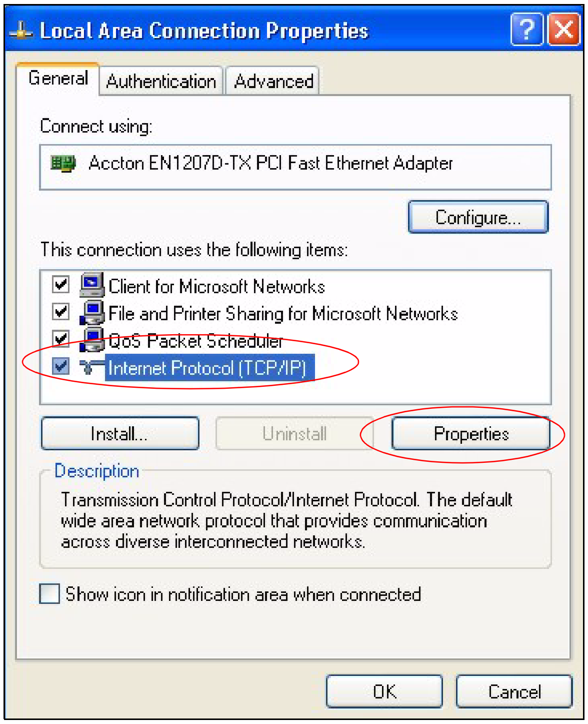
3 Right-click **Local Area Connection** and then click **Properties**.

Figure 115   Windows XP: Control Panel: Network Connections: Properties



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

Figure 116   Windows XP: Local Area Connection Properties

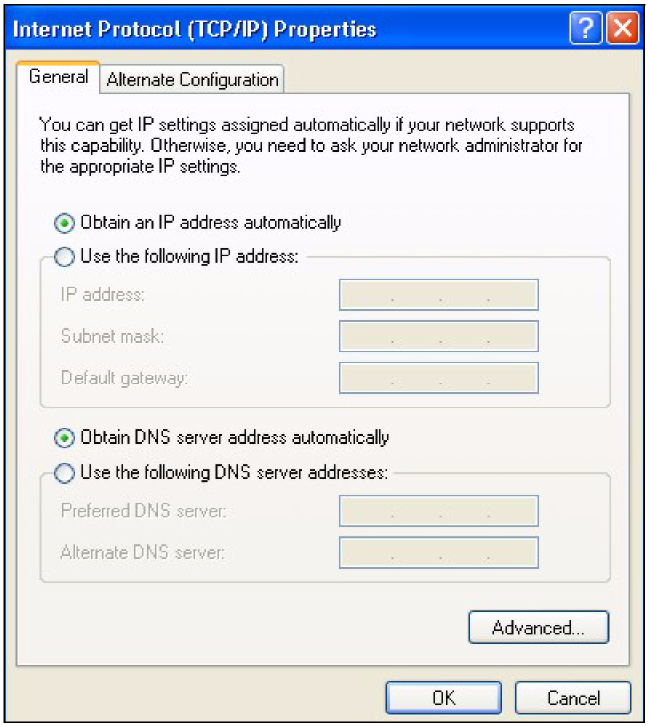

Local Area Connection Properties
General
Authentication
Advanced
Connect using:
Accton EN1207D-TX PCI Fast Ethernet Adapter
Configure...
This connection uses the following items:
☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)
Install...
Uninstall
Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
☐ Show icon in notification area when connected
OK
Cancel

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 117 Windows XP: Internet Protocol (TCP/IP) Properties



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:
IP address: . . .
Subnet mask: . . .
Default gateway: . . .

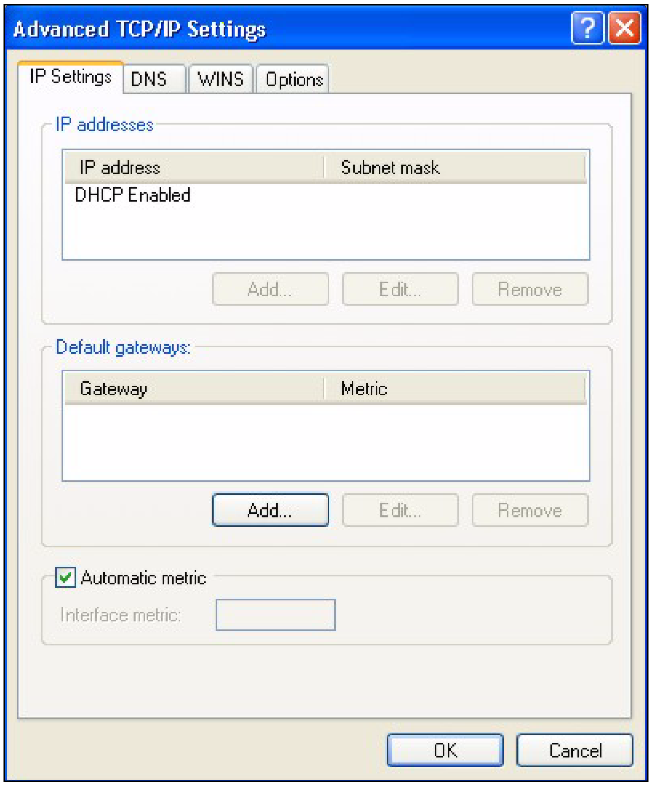
● Obtain DNS server address automatically
○ Use the following DNS server addresses:
Preferred DNS server: . . .
Alternate DNS server: . . .

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.

Figure 118 Windows XP: Advanced TCP/IP Properties



IP addresses

IP address	Subnet mask
DHCP Enabled	

Default gateways:

Gateway	Metric

☑ Automatic metric

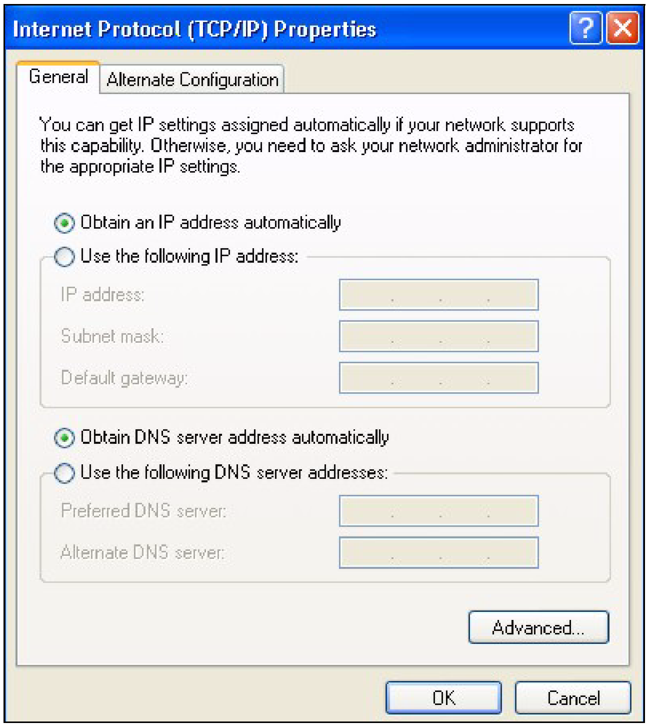
Interface metric:

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 119 Windows XP: Internet Protocol (TCP/IP) Properties



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

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

9 Click **Close** (**OK** in Windows 2000/NT) to close the **Local Area Connection Properties** window.

10 Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).

11Turn on your Prestige and restart your computer (if prompted).

Verifying Settings

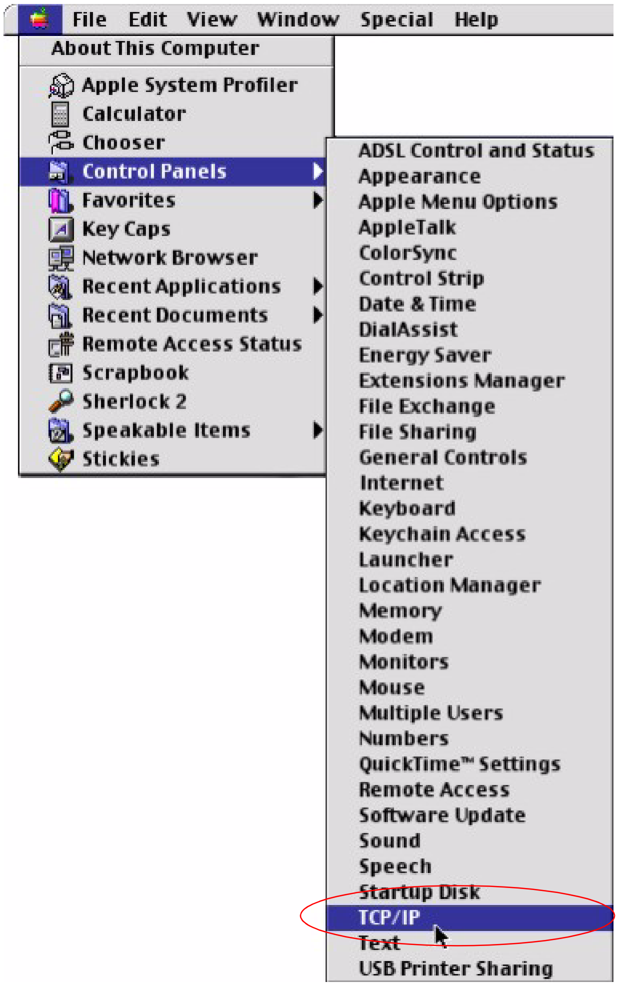
1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

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

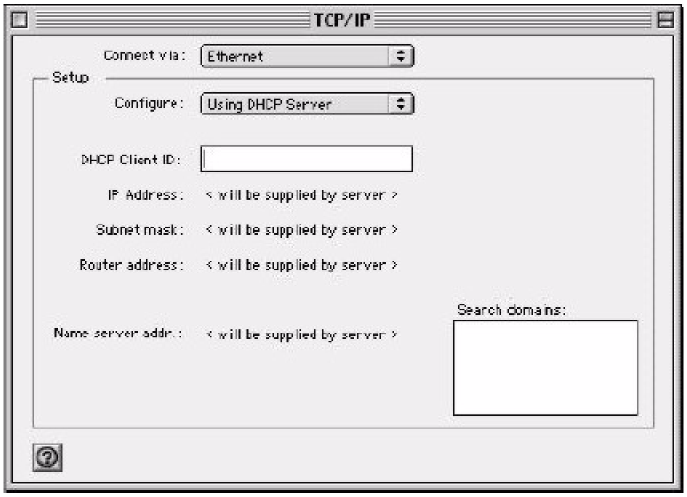
1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 120 Macintosh OS 8/9: Apple Menu



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

Figure 121 Macintosh OS 8/9: TCP/IP



Connect via: Ethernet

Configure: Using DHCP Server

DHCP Client ID:

IP Address: < will be supplied by server >

Subnet mask: < will be supplied by server >

Router address: < will be supplied by server >

Name server addr.: < will be supplied by server >

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).

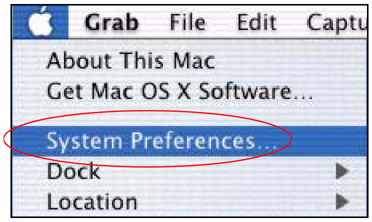
Verifying Settings

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 122 Macintosh OS X: Apple Menu

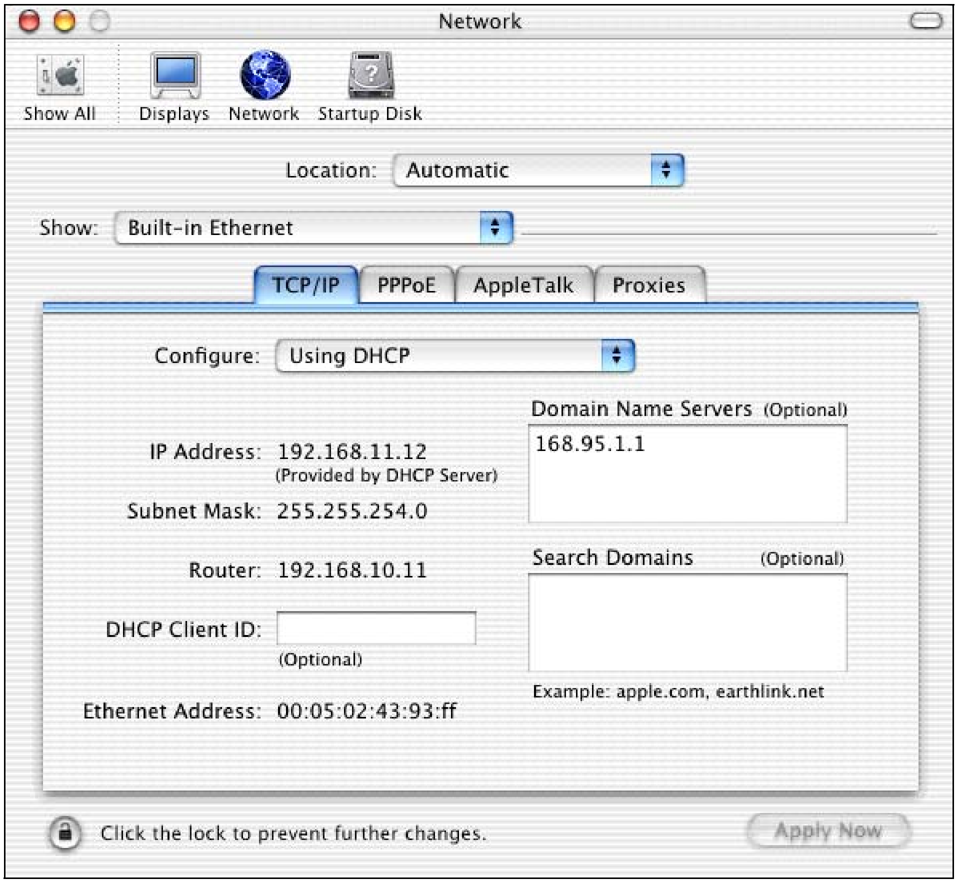


2 Click **Network** in the icon bar.

- 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 123 Macintosh OS X: Network



Location: Automatic

Show: Built-in Ethernet

Configure: Using DHCP

IP Address: 192.168.11.12
(Provided by DHCP Server)

Subnet Mask: 255.255.254.0

Router: 192.168.10.11

DHCP Client ID:
(Optional)

Ethernet Address: 00:05:02:43:93:ff

Domain Name Servers (Optional)
168.95.1.1

Search Domains (Optional)

Example: apple.com, earthlink.net

Click the lock to prevent further changes.

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.

Linux

This section shows you how to configure your computer’s TCP/IP settings in Red Hat Linux 9.0. Procedure, screens and file location may vary depending on your Linux distribution and release version.

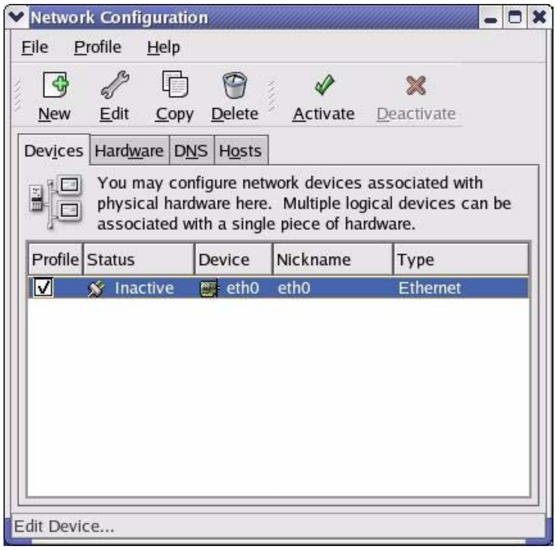
Note: Make sure you are logged in as the root administrator.

Using the K Desktop Environment (KDE)

Follow the steps below to configure your computer IP address using the KDE.

1 Click the Red Hat button (located on the bottom left corner), select **System Setting** and click **Network**.

Figure 124 Red Hat 9.0: KDE: Network Configuration: Devices

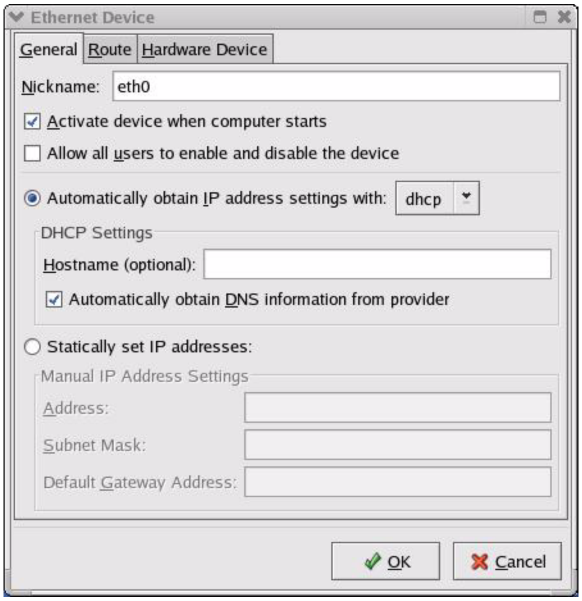


You may configure network devices associated with physical hardware here. Multiple logical devices can be associated with a single piece of hardware.

Profile	Status	Device	Nickname	Type
☑	Inactive	eth0	eth0	Ethernet

2 Double-click on the profile of the network card you wish to configure. The **Ethernet Device General** screen displays as shown.

Figure 125 Red Hat 9.0: KDE: Ethernet Device: General



Nickname: eth0

☑ Activate device when computer starts

□ Allow all users to enable and disable the device

● Automatically obtain IP address settings with: dhcp

DHCP Settings

Hostname (optional):

☑ Automatically obtain DNS information from provider

○ Statically set IP addresses:

Manual IP Address Settings

Address:

Subnet Mask:

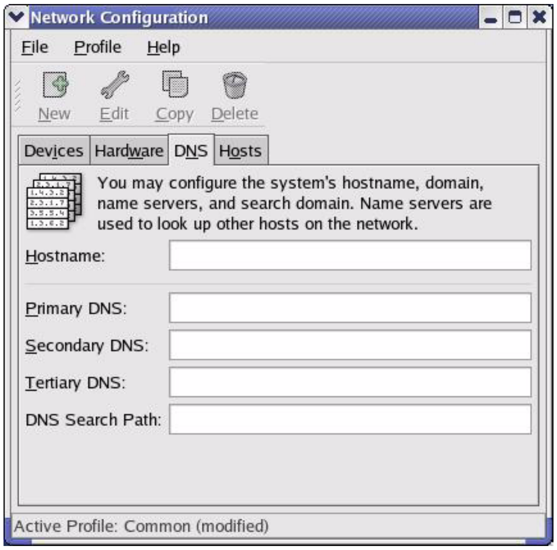
Default Gateway Address:

- If you have a dynamic IP address, click **Automatically obtain IP address settings with** and select **dhcp** from the drop down list.
- If you have a static IP address, click **Statically set IP Addresses** and fill in the **Address**, **Subnet mask**, and **Default Gateway Address** fields.

3 Click **OK** to save the changes and close the **Ethernet Device General** screen.

4 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Configuration** screen. Enter the DNS server information in the fields provided.

Figure 126 Red Hat 9.0: KDE: Network Configuration: DNS



You may configure the system's hostname, domain, name servers, and search domain. Name servers are used to look up other hosts on the network.

Hostname:

Primary DNS:

Secondary DNS:

Tertiary DNS:

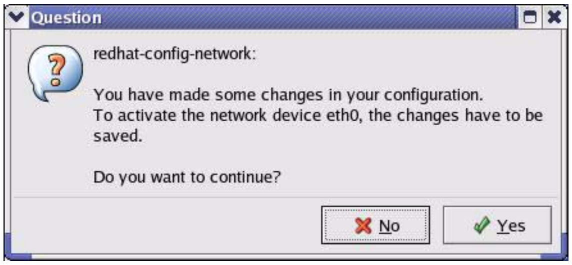
DNS Search Path:

Active Profile: Common (modified)

5 Click the **Devices** tab.

6 Click the **Activate** button to apply the changes. The following screen displays. Click **Yes** to save the changes in all screens.

Figure 127 Red Hat 9.0: KDE: Network Configuration: Activate



redhat-config-network:

You have made some changes in your configuration.
To activate the network device eth0, the changes have to be saved.

Do you want to continue?

7 After the network card restart process is complete, make sure the **Status** is **Active** in the **Network Configuration** screen.

Using Configuration Files

Follow the steps below to edit the network configuration files and set your computer IP address.

1 Assuming that you have only one network card on the computer, locate the `ifconfig-eth0` configuration file (where `eth0` is the name of the Ethernet card). Open the configuration file with any plain text editor.

- If you have a dynamic IP address, enter **`dhcp`** in the `BOOTPROTO=` field. The following figure shows an example.

Figure 128 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- If you have a static IP address, enter **`static`** in the `BOOTPROTO=` field. Type `IPADDR=` followed by the IP address (in dotted decimal notation) and type `NETMASK=` followed by the subnet mask. The following example shows an example where the static IP address is 192.168.1.10 and the subnet mask is 255.255.255.0.

Figure 129 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.10
NETMASK=255.255.255.0
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

2 If you know your DNS server IP address(es), enter the DNS server information in the `resolv.conf` file in the `/etc` directory. The following figure shows an example where two DNS server IP addresses are specified.

Figure 130 Red Hat 9.0: DNS Settings in resolv.conf

```
nameserver 172.23.5.1
nameserver 172.23.5.2
```

3 After you edit and save the configuration files, you must restart the network card. Enter `./network restart` in the `/etc/rc.d/init.d` directory. The following figure shows an example.

Figure 131 Red Hat 9.0: Restart Ethernet Card

```
[root@localhost init.d]# network restart

Shutting down interface eth0:                  [OK]
Shutting down loopback interface:              [OK]
Setting network parameters:                    [OK]
Bringing up loopback interface:                [OK]
Bringing up interface eth0:                    [OK]
```

Verifying Settings

Enter `ifconfig` in a terminal screen to check your TCP/IP properties.

Figure 132 Red Hat 9.0: Checking TCP/IP Properties

```
[root@localhost]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:BA:72:5B:44
          inet addr:172.23.19.129  Bcast:172.23.19.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:717 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:730412 (713.2 Kb)  TX bytes:1570 (1.5 Kb)
          Interrupt:10 Base address:0x1000
[root@localhost]#
```

Appendix D
PPPoE

PPPoE in Action

An ADSL modem bridges a PPP session over Ethernet (PPP over Ethernet, RFC 2516) from your computer to an ATM PVC (Permanent Virtual Circuit) which connects to a DSL Access Concentrator where the PPP session terminates (see Figure 133 on page 190). One PVC can support any number of PPP sessions from your LAN. PPPoE provides access control and billing functionality in a manner similar to dial-up services using PPP.

Benefits of PPPoE

PPPoE offers the following benefits:

It provides you with a familiar dial-up networking (DUN) user interface.

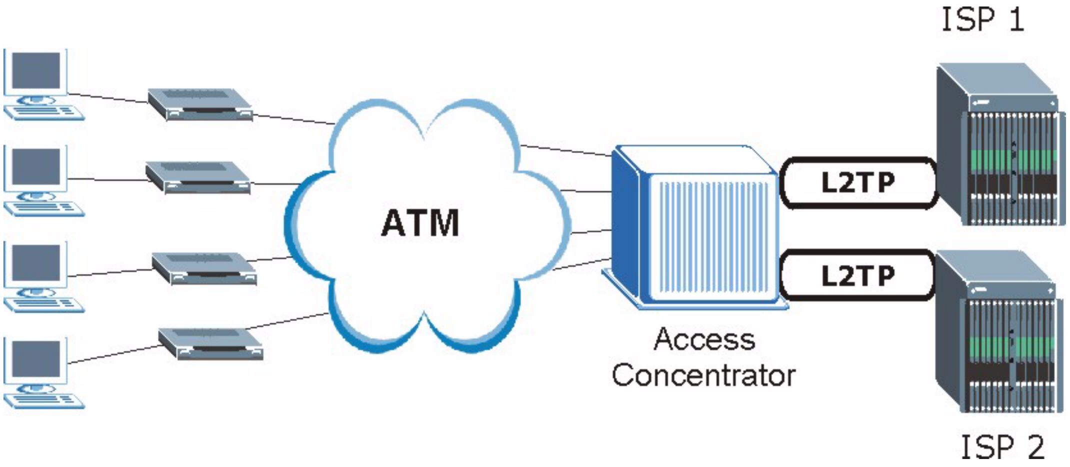
It lessens the burden on the carriers of provisioning virtual circuits all the way to the ISP on multiple switches for thousands of users. For GSTN (PSTN and ISDN), the switching fabric is already in place.

It allows the ISP to use the existing dial-up model to authenticate and (optionally) to provide differentiated services.

Traditional Dial-up Scenario

The following diagram depicts a typical hardware configuration where the computers use traditional dial-up networking.

Figure 133 Single-Computer per Router Hardware Configuration



How PPPoE Works

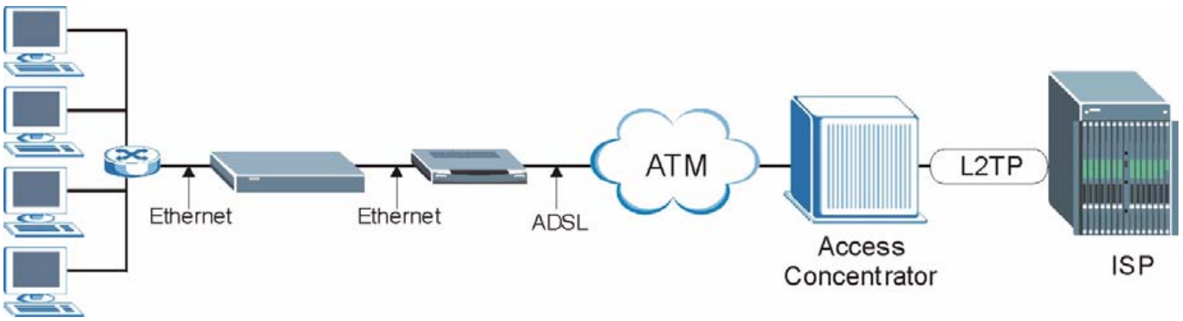
The PPPoE driver makes the Ethernet appear as a serial link to the computer and the computer runs PPP over it, while the modem bridges the Ethernet frames to the Access Concentrator (AC). Between the AC and an ISP, the AC is acting as a L2TP (Layer 2 Tunneling Protocol) LAC (L2TP Access Concentrator) and tunnels the PPP frames to the ISP. The L2TP tunnel is capable of carrying multiple PPP sessions.

With PPPoE, the VC (Virtual Circuit) is equivalent to the dial-up connection and is between the modem and the AC, as opposed to all the way to the ISP. However, the PPP negotiation is between the computer and the ISP.

ZyWALL as a PPPoE Client

When using the ZyWALL as a PPPoE client, the computers on the LAN see only Ethernet and are not aware of PPPoE. This alleviates the administrator from having to manage the PPPoE clients on the individual computers.

Figure 134 ZyWALL as a PPPoE Client



APPENDIX E
PPTP

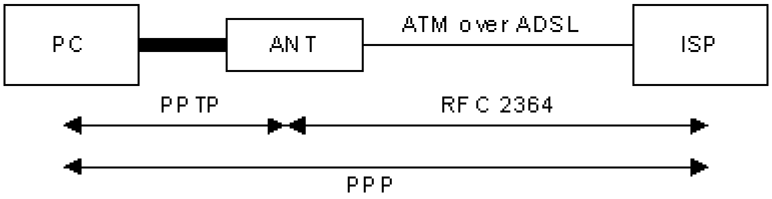
What is PPTP?

PPTP (Point-to-Point Tunneling Protocol) is a Microsoft proprietary protocol (RFC 2637 for PPTP is informational only) to tunnel PPP frames.

How can we transport PPP frames from a computer to a broadband modem over Ethernet?

A solution is to build PPTP into the ANT (ADSL Network Termination) where PPTP is used only over the short haul between the computer and the modem over Ethernet. For the rest of the connection, the PPP frames are transported with PPP over AAL5 (RFC 2364) The PPP connection, however, is still between the computer and the ISP. The various connections in this setup are depicted in the following diagram. The drawback of this solution is that it requires one separate ATM VC per destination.

Figure 135 Transport PPP frames over Ethernet



PPTP and the ZyWALL

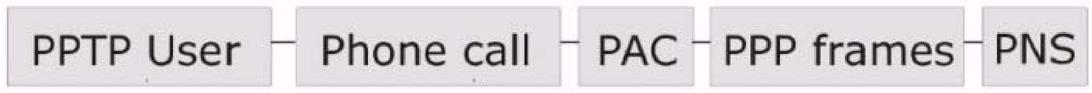
When the ZyWALL is deployed in such a setup, it appears as a computer to the ANT.

In Windows VPN or PPTP Pass-Through feature, the PPTP tunneling is created from Windows 95, 98 and NT clients to an NT server in a remote location. The pass-through feature allows users on the network to access a different remote server using the ZyWALL's Internet connection. In SUA/NAT mode, the ZyWALL is able to pass the PPTP packets to the internal PPTP server (i.e. NT server) behind the NAT. You need to configure port forwarding for port 1723 to have the ZyWALL forward PPTP packets to the server. In the case above as the remote PPTP Client initializes the PPTP connection, the user must configure the PPTP clients. The ZyWALL initializes the PPTP connection hence; there is no need to configure the remote PPTP clients.

PPTP Protocol Overview

PPTP is very similar to L2TP, since L2TP is based on both PPTP and L2F (Cisco’s Layer 2 Forwarding). Conceptually, there are three parties in PPTP, namely the PNS (PPTP Network Server), the PAC (PPTP Access Concentrator) and the PPTP user. The PNS is the box that hosts both the PPP and the PPTP stacks and forms one end of the PPTP tunnel. The PAC is the box that dials/answers the phone calls and relays the PPP frames to the PNS. The PPTP user is not necessarily a PPP client (can be a PPP server too). Both the PNS and the PAC must have IP connectivity; however, the PAC must in addition have dial-up capability. The phone call is between the user and the PAC and the PAC tunnels the PPP frames to the PNS. The PPTP user is unaware of the tunnel between the PAC and the PNS.

Figure 136 PPTP Protocol Overview



Microsoft includes PPTP as a part of the Windows OS. In Microsoft’s implementation, the computer, and hence the ZyWALL, is the PNS that requests the PAC (the ANT) to place an outgoing call over AAL5 to an RFC 2364 server.

Control & PPP Connections

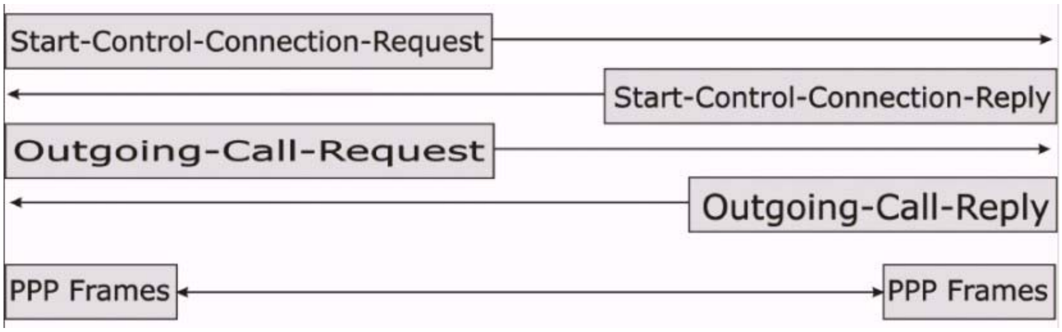
Each PPTP session has distinct control connection and PPP data connection.

Call Connection

The control connection runs over TCP. Similar to L2TP, a tunnel control connection is first established before call control messages can be exchanged. Please note that a tunnel control connection supports multiple call sessions.

The following diagram depicts the message exchange of a successful call setup between a computer and an ANT.

Figure 137 Example Message Exchange between Computer and an ANT


Start-Control-Connection-Request
Start-Control-Connection-Reply
Outgoing-Call-Request
Outgoing-Call-Reply
PPP Frames
PPP Frames

PPP Data Connection

The PPP frames are tunneled between the PNS and PAC over GRE (General Routing Encapsulation, RFC 1701, 1702). The individual calls within a tunnel are distinguished using the Call ID field in the GRE header.

Appendix F
Wireless LANs

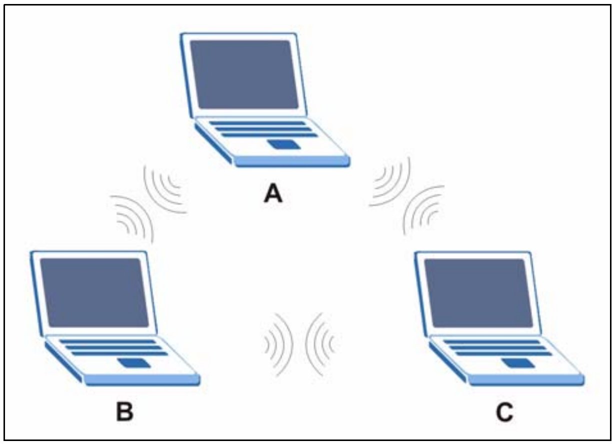
Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless stations (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an Ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an Ad-hoc wireless LAN.

Figure 138 Peer-to-Peer Communication in an Ad-hoc Network

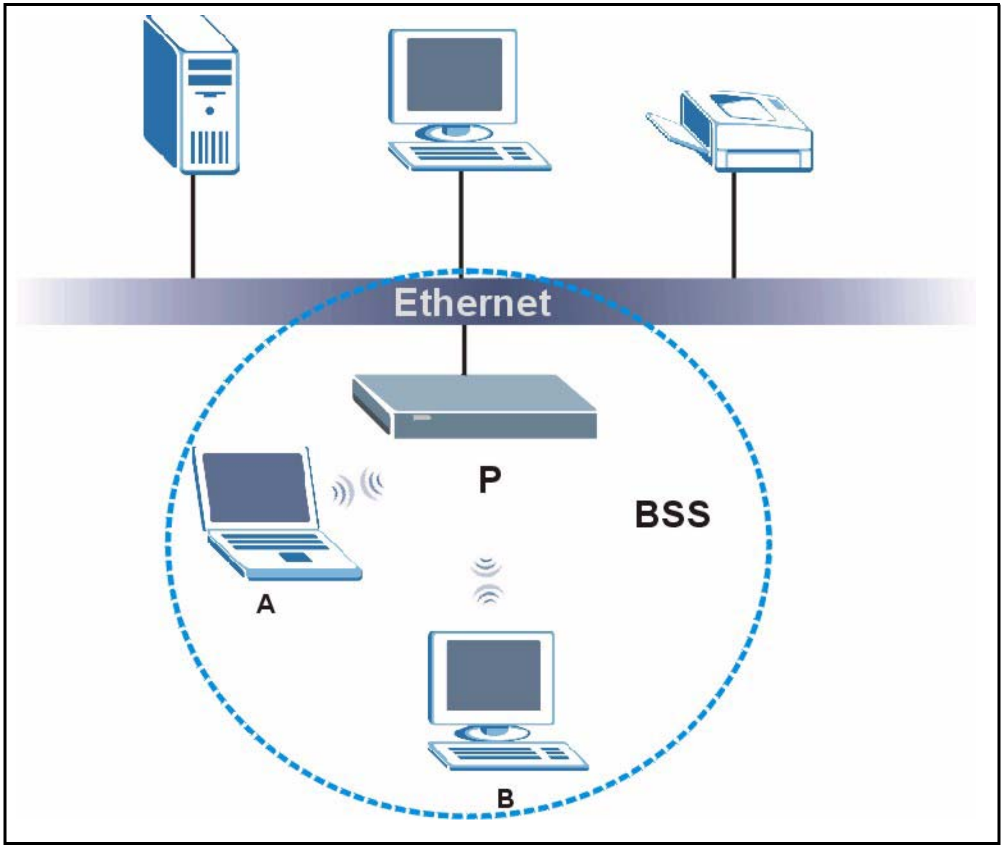


BSS

A Basic Service Set (BSS) exists when all communications between wireless stations or between a wireless station and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless stations in the BSS. When Intra-BSS is enabled, wireless station A and B can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless station A and B can still access the wired network but cannot communicate with each other.

Figure 139 Basic Service Set



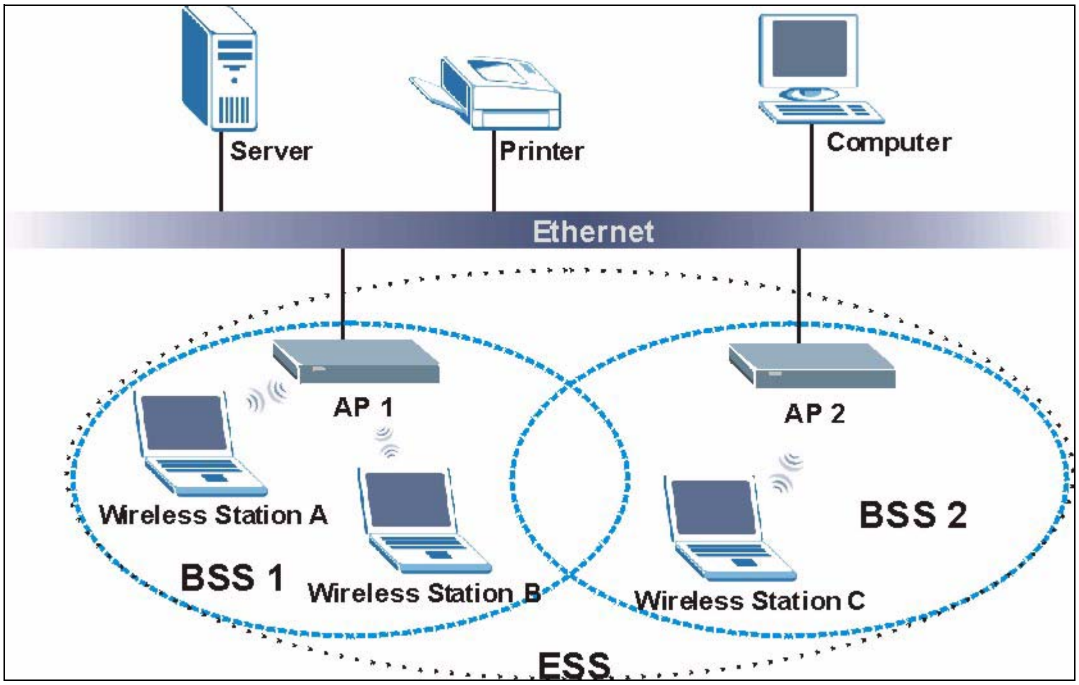
ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless stations within the same ESS must have the same ESSID in order to communicate.

Figure 140 Infrastructure WLAN



Channel

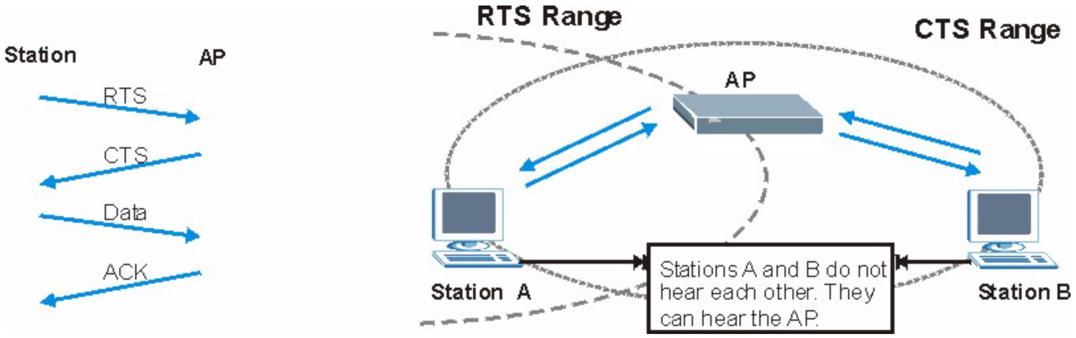
A channel is the radio frequency(ies) used by IEEE 802.11a/b/g wireless devices. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a different channel than an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

Figure 141 RTS/CTS


Station
AP
RTS
CTS
Data
ACK
RTS Range
CTS Range
AP
Station A
Station B
Stations A and B do not hear each other. They can hear the AP.

When station A sends data to the AP, it might not know that the station B is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS/CTS is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Note: Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Preamble Type

A preamble is used to synchronize the transmission timing in your wireless network. There are two preamble modes: **Long** and **Short**.

Short preamble takes less time to process and minimizes overhead, so it should be used in a good wireless network environment when all wireless stations support it.

Select **Long** if you have a 'noisy' network or are unsure of what preamble mode your wireless stations support as all IEEE 802.11b compliant wireless adapters must support long preamble. However, not all wireless adapters support short preamble. Use long preamble if you are unsure what preamble mode the wireless adapters support, to ensure interpretability between the AP and the wireless stations and to provide more reliable communication in 'noisy' networks.

Select **Dynamic** to have the AP automatically use short preamble when all wireless stations support it, otherwise the AP uses long preamble.

Note: The AP and the wireless stations MUST use the same preamble mode in order to communicate.

IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

Table 85 IEEE802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless stations.

RADIUS

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

- Authentication

  Determines the identity of the users.
- Authorization

  Determines the network services available to authenticated users once they are connected to the network.
- Accounting

  Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless station and the network RADIUS server.

Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request

  Sent by an access point requesting authentication.
- Access-Reject

  Sent by a RADIUS server rejecting access.
- Access-Accept

  Sent by a RADIUS server allowing access.

- Access-Challenge

  Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request

  Sent by the access point requesting accounting.

- Accounting-Response

  Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

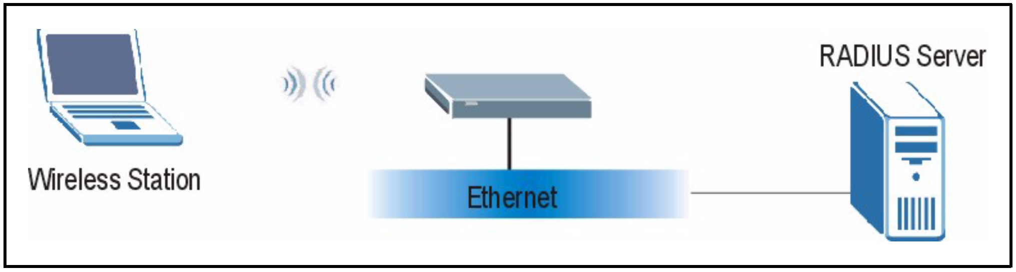
EAP Authentication

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 following figure shows an overview of authentication when you specify a RADIUS server on your access point.

Figure 142 EAP Authentication



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 appendix.

1. The wireless station sends a “start” message to the device.
2. The device sends a “request identity” message to the wireless station for identity information.

3 The wireless station replies with identity information, including username and password.

4 The RADIUS server checks the user information against its user profile database and determines whether or not to authenticate the wireless station.

Types of Authentication

This section discusses some popular authentication types: **EAP-MD5**, **EAP-TLS**, **EAP-TTLS**, **PEAP** and **LEAP**.

The type of authentication you use depends on the RADIUS server or the AP. Consult your network administrator for more information.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless station. The wireless station 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless stations for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

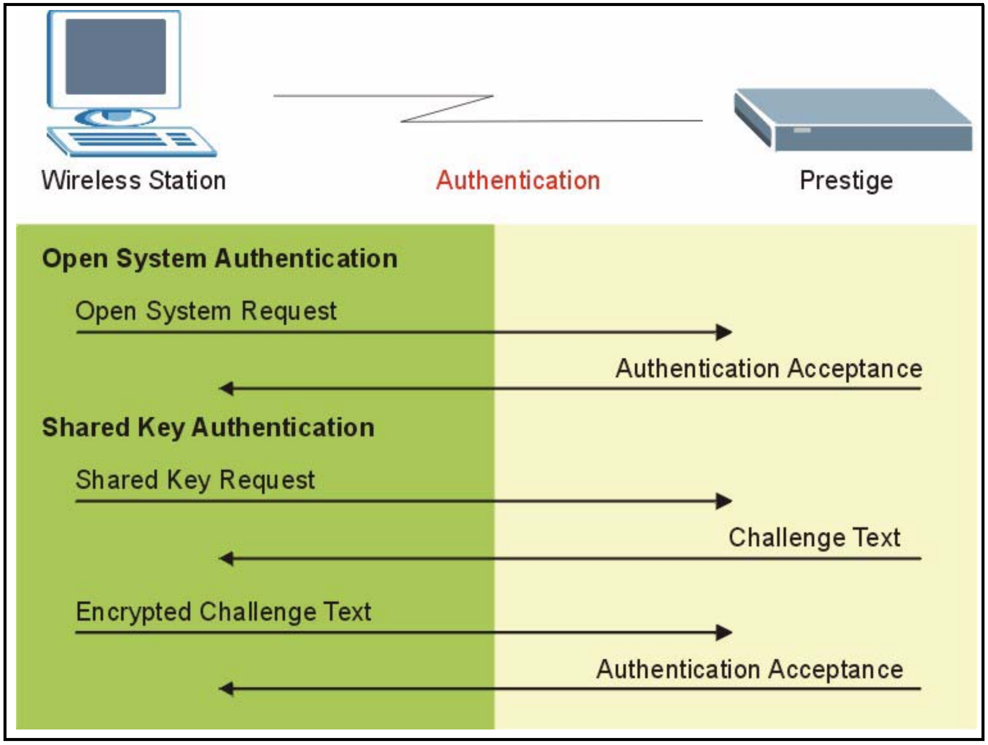
WEP Encryption

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

WEP Authentication Steps

Three different methods can be used to authenticate wireless stations to the network: **Open System**, **Shared Key**, and **Auto**. The following figure illustrates the steps involved.

Figure 143 WEP Authentication Steps



Open system authentication involves an unencrypted two-message procedure. A wireless station sends an open system authentication request to the AP, which will then automatically accept and connect the wireless station to the network. In effect, open system is not authentication at all as any station can gain access to the network.

Shared key authentication involves a four-message procedure. A wireless station sends a shared key authentication request to the AP, which will then reply with a challenge text message. The wireless station must then use the AP's default WEP key to encrypt the challenge text and return it to the AP, which attempts to decrypt the message using the AP's default WEP key. If the decrypted message matches the challenge text, the wireless station is authenticated.

When your device authentication method is set to open system, it will only accept open system authentication requests. The same is true for shared key authentication. However, when it is set to auto authentication, the device will accept either type of authentication request and the device will fall back to use open authentication if the shared key does not match.

Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the Wireless screen. You may still configure and store keys here, but they will not be used while Dynamic WEP is enabled.

Note: EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

Table 86 Comparison of EAP Authentication Types

		EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

WPA

User Authentication

WPA applies IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless stations using an external RADIUS database.

Encryption

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP) or Advanced Encryption Standard (AES), Message Integrity Check (MIC) and IEEE 802.1x.

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. It includes a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

TKIP regularly changes and rotates the encryption keys so that the same encryption key is never used twice.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless stations. This all happens in the background automatically.

AES (Advanced Encryption Standard) also uses a secret key. This implementation of AES applies a 128-bit key to 128-bit blocks of data.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), TKIP makes it much more difficult to decrypt data on a Wi-Fi network than WEP, making it difficult for an intruder to break into the network.

The encryption mechanisms used for WPA and WPA-PSK are the same. The only difference between the two is that WPA-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs an easier-to-use, consistent, single, alphanumeric password.

Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each Authentication Method/ key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 87 Wireless Security Relational Matrix

	ENCRYPTION METHOD	ENTER MANUAL KEY	ENABLE IEEE 802.1X
Open	None	No	No
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	WEP	No	Yes
WPA	TKIP	No	Yes
WPA-PSK	WEP	Yes	Yes
WPA-PSK	TKIP	Yes	Yes

Roaming

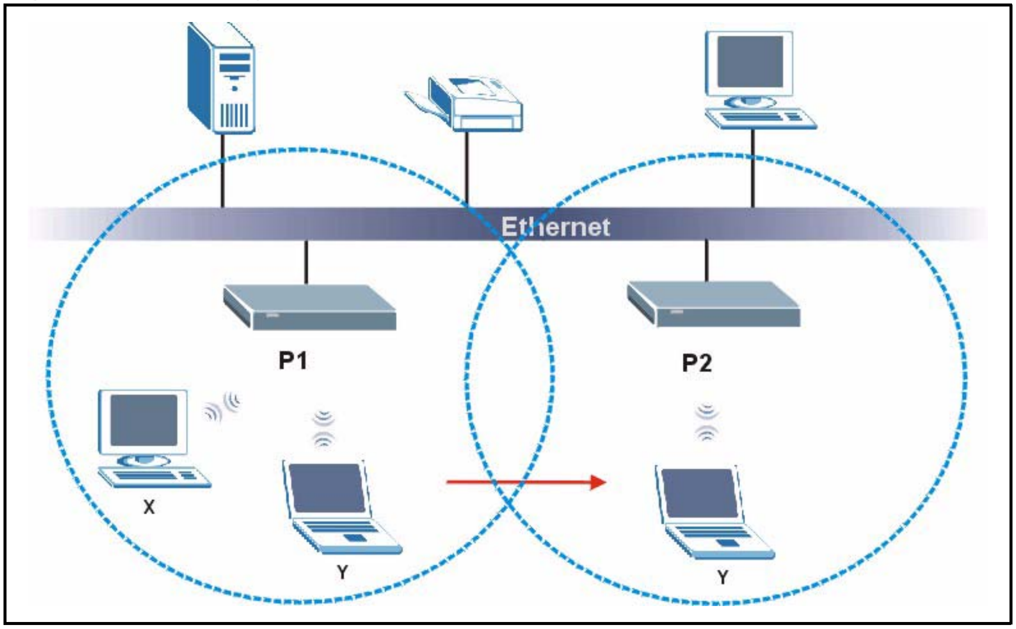
A wireless station is a device with an IEEE 802.11 mode compliant wireless adapter. An access point (AP) acts as a bridge between the wireless and wired networks. An AP creates its own wireless coverage area. A wireless station can associate with a particular access point only if it is within the access point's coverage area.

In a network environment with multiple access points, wireless stations are able to switch from one access point to another as they move between the coverage areas. This is roaming. As the wireless station moves from place to place, it is responsible for choosing the most appropriate access point depending on the signal strength, network utilization or other factors.

The roaming feature on the access points allows the access points to relay information about the wireless stations to each other. When a wireless station moves from a coverage area to another, it scans and uses the channel of a new access point, which then informs the access points on the LAN about the change. The new information is then propagated to the other access points on the LAN. An example is shown in Figure 144.

If the roaming feature is not enabled on the access points, information is not communicated between the access points when a wireless station moves between coverage areas. The wireless station may not be able to communicate with other wireless stations on the network and vice versa.

Figure 144 Roaming Example



The steps below describe the roaming process.

1 As wireless station **Y** moves from the coverage area of access point **P1** to that of access point

2 **P2**, it scans and uses the signal of access point **P2**.

3 Access point **P2** acknowledges the presence of wireless station **Y** and relays this information to access point **P1** through the wired LAN.

4 Access point **P1** updates the new position of wireless station.

5 Wireless station **Y** sends a request to access point **P2** for re-authentication.

Requirements for Roaming

The following requirements must be met in order for wireless stations to roam between the coverage areas.

1 All the access points must be on the same subnet and configured with the same ESSID.

2 If IEEE 802.1x user authentication is enabled and to be done locally on the access point, the new access point must have the user profile for the wireless station.

3 The adjacent access points should use different radio channels when their coverage areas overlap.

4 All access points must use the same port number to relay roaming information.

5 The access points must be connected to the Ethernet and be able to get IP addresses from a DHCP server if using dynamic IP address assignment.

APPENDIX G
Antenna Selection and Positioning Recommendation

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Choosing the right antennas and positioning them properly increases the range and coverage area of a wireless LAN.

Antenna Characteristics

Frequency

An antenna in the frequency of 2.4GHz (IEEE 802.11b) or 5GHz (IEEE 802.11a) is needed to communicate efficiently in a wireless LAN.

Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna’s coverage area.

Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

Types of Antennas For WLAN

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight. The angle of the beam width determines the direction of the coverage pattern; typically ranges from 20 degrees (less directional) to 90 degrees (very directional). The directional antennas are ideal for hallways and outdoor point-to-point applications.

Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to –point application, position both transmitting and receiving antenna at the same height and in a direct line of sight to each other to attend the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

Index

Numerics

110V AC 6
230V AC 6
802.1x 70

A

Abnormal Working Conditions 7
AC 6
Accessories 6
Acts of God 7
Airflow 6
Alternative Subnet Mask Notation 167
American Wire Gauge 6
Antenna
    Directional 210
    Omni-directional 210
Antenna gain 209
AP (access point) 197
Authentication 203
Authority 4
AWG 6

B

Backup 147
Basement 6
Basic wireless security 49
BSS 195

C

CA 202
Cables, Connecting 6
Certificate Authority 202
Certifications 5
Changes or Modifications 4
Channel 197
    Interference 197
Channel ID 64
Charge 7
Circuit 4
Class B 4
Communications 4
Compliance, FCC 4
Components 7
Condition 7
Configuration 41, 95
Connecting Cables 6
Consequential Damages 7
Contact Information 8
Contacting Customer Support 8
Copyright 3
Correcting Interference 4
Corrosive Liquids 6
Covers 6
CTS (Clear to Send) 198
Customer Support 8

D

Damage 6
Dampness 6
Danger 6
Dealer 4
Default 148
Defective 7
Denmark, Contact Information 8
DHCP 41, 93, 95, 96, 136
DHCP Table Summary 41
DHCP_client list 97
Disclaimer 3
Discretion 7
Domain Name 102
Dust 6

Dynamic DNS 136
Dynamic WEP Key Exchange 204
DYNDNS Wildcard 136

E

EAP 61
EAP Authentication 201, 202
ECHO 102
Electric Shock 6
Electrical Pipes 6
Electrocution 6
Encryption 205
Equal Value 7
ESS 196
Ethernet 163
Ethernet Encapsulation 102
Europe 6
Exposure 6
Extended Service Set 196
Extended Service Set IDentification 64
Extended wireless security 50

F

Factory LAN Defaults 93
Failure 7
FCC 4
  Compliance 4
  Rules, Part 15 4
FCC Rules 4
Federal Communications Commission 4
Finger 102
Finland, Contact Information 8
Firewall 109, 110
Firmware File
  Maintenance 146
Fitness 7
Fragmentation Threshold 198
Fragmentation threshold 198
France, Contact Information 8
FTP 93, 102, 119, 136
FTP Restrictions 119
Functionally Equivalent 7

G

Gas Pipes 6
General Setup 135
General wireless LAN screen 63
Germany, Contact Information 8
Global 100
God, act of 7

H

Harmful Interference 4
Hidden node 197
High Voltage Points 6
Host 136
Host IDs 165
HTTP 102

I

IBSS 195
IEEE 802.11g 30, 199
IEEE 802.11i 30
Independent Basic Service Set 195
Indirect Damages 7
initialization vector (IV) 205
Inside 100
Inside Global Address 99
Inside Local Address 99
Install UPnP
  Windows XP 128
Insurance 7
Interference 4
Interference Correction Measures 4
Interference Statement 4
Internet Access Setup 152
IP Address 41, 94, 97, 101, 102, 104, 105
IP Addressing 165
IP Classes 165
IP Pool 96
IP Pool Setup 93

L

Labor 7
LAN Setup 81, 93
LAN TCP/IP 93
Legal Rights 7
Liability 3
License 3
Lightning 6
Liquids, Corrosive 6
Local 100

M

MAC Address Filter Action 77
MAC Address Filtering 76
MAC Filter 76
MAC filter 62
Management Information Base (MIB) 121
Materials 7
Merchantability 7
Message Integrity Check (MIC) 205
Metric 82, 117
Modifications 4

N

NAT 101, 102
- Definitions 99
- How NAT Works 100
- Server Sets 102
- What NAT does 100

Navigation Panel 39
Network Management 102
New 7
NNTP 102
North America 6
North America Contact Information 8
Norway, Contact Information 8

O

Opening 6
Operating Condition 7
OTIST 72
OTIST Wizard 51
Out-dated Warranty 7
Outlet 4
Outside 100

P

Packet statistics 42
Pairwise Master Key (PMK) 205
Parts 7
Patent 3
Permission 3
Photocopying 3
Pipes 6
Point-to-Point Tunneling Protocol 87, 102
Pool 6
POP3 102
Port Numbers 102
Postage Prepaid. 7
Power Adaptor 6
Power Cord 6
Power Outlet 6
Power Supply 6
Power Supply, repair 6
PPPoE 189
PPTP 102
Preamble Mode 199
Product Model 8
Product Page 5
Product Serial Number 8
Products 7
Proof of Purchase 7
Proper Operating Condition 7
Purchase, Proof of 7
Purchaser 7

Q

Qualified Service Personnel 6

R

Radio Communications 4

Radio Frequency Energy 4
Radio Interference 4
Radio Reception 4
Radio Technician 4
RADIUS 200
  Shared Secret Key 201
RADIUS Message Types 200
RADIUS Messages 200
Receiving Antenna 4
Registered 3
Registered Trademark 3
Regular Mail 8
Related Documentation 25
Relocate 4
Re-manufactured 7
Remote Management and NAT 119
Remote Management Limitations 119
Removing 6
Reorient 4
Repair 6, 7
Replace 7
Replacement 7
Reproduction 3
Restore 7, 147
Return Material Authorization (RMA) Number 7
Returned Products 7
Returns 7
RF (Radio Frequency) 30
Rights 3
Rights, Legal 7
Risk 6
Risks 6
RMA 7
Roaming 78, 206
  Example 207
  Requirements 208
RTS (Request To Send) 198
RTS Threshold 197, 198

S

Safety Warnings 6
Security Parameters 206
Separation Between Equipment and Receiver 4
Serial Number 8
Service 6, 7
Service Personnel 6
Service Set 64
Service Type 152
Services 102, 111
Shipping 7
Shock, Electric 6
SMTP 102
SNMP 102, 110, 121
  Manager 121
  MIBs 122
Spain, Contact Information 9
Stateful Inspection 109
Static DHCP 96
Static Route 115
SUA 102, 103
Subnet Mask 94
Subnet Masks 166
Subnetting 166
Supply Voltage 6
Support E-mail 8
Sweden, Contact Information 9
Swimming Pool 6
Syntax Conventions 25
System information 46
System Timeout 120

T

Tampering 7
TCP/IP 94
Telecommunication Line Cord. 6
Telephone 8
Television Interference 4
Television Reception 4
Temporal Key Integrity Protocol (TKIP) 205
TFTP Restrictions 119
Thunderstorm 6
Time Zone 137
Trademark 3
Trademark Owners 3
Trademarks 3
Traffic Redirect 90
Translation 3
Trigger Port Forwarding
  Process 106
TV Technician 4

U

Undesired Operations **4**
Universal Plug and Play (UPnP) **125**
User Authentication **205**
User Name **137**

V

Value **7**
Vendor **6**
Ventilation Slots **6**
Viewing Certifications **5**
Voltage Supply **6**
Voltage, High **6**
VPN **87**

W

Wall Mount **6**
WAN advanced **89**
WAN MAC address **57**
WAN Wizard **52**
Warnings **6**
Warranty **7**
Warranty Information **8**
Warranty Period **7**
Water **6**
Water Pipes **6**
Web **120**
Web Configurator **35**, **37**
Web Site **8**
WEP (Wired Equivalent Privacy) **31**
WEP Encryption **66**, **68**
WEP encryption **65**, **203**
Wet Basement **6**
Wi-Fi Protected Access **67**
Wi-Fi Protected Access (WPA) **30**
Wireless association list summary **42**
Wireless Client WPA Supplicants **69**
Wireless LAN MAC Address Filtering **31**
Wireless LAN Wizard **47**
Wireless security **61**
WLAN
  Interference **197**
  Security parameters **206**
Workmanship **7**
Worldwide Contact Information **8**
WPA **67**
Written Permission **3**

Z

ZyNOS **3**
ZyXEL Communications Corporation **3**
ZyXEL Home Page **5**
ZyXEL Limited Warranty
  Note **7**
ZyXEL Network Operating System **3**