

DRAFT About This User's Guide

Congratulations on your purchase of the ZyXEL MAX-200HW2 Series WiMAX WiFi Router with Built-In Switch and VOIP. Your ZyXEL Device allows you to access WiMAX wireless networks, set up a WiFi network and make Voice over Internet (VoIP) phone calls.

Your ZyXEL Device is easy to install and configure.

Intended Audience

This manual is designed to guide you through the configuration of your ZyXEL Device for its various applications.

Related Documentation

- Quick Start Guide
The Quick Start Guide is designed to help you get up and running right away. It contains information on setting up your network and configuring for Internet access.
- Supporting Disk
Refer to the included CD for support documents.
- ZyXEL Web Site
Please refer to www.zyxel.com for additional support documentation and product certifications.

User's Guide Feedback

Help us help you. Send all User's Guide-related comments, questions or suggestions for improvement to the following address, or use e-mail instead. Thank you!

The Technical Writing Team,
ZyXEL Communications Corp.,
6 Innovation Road II,
Science-Based Industrial Park,
Hsinchu, 300, Taiwan.

E-mail: techwriters@zyxel.com.tw

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.



Warnings tell you about things that could harm you or your ZyXEL Device.



Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.









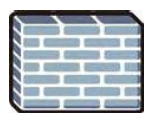
Syntax Conventions

- The ZyXEL MAX-200HW2 Series may be referred to as the “ZyXEL Device”, the “device”, the “system” or the “product” in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the “enter” or “return” key on your keyboard.
- “Enter” means for you to type one or more characters and then press the [ENTER] key. “Select” or “choose” means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the “metric” value or the “scientific” value. For example, “k” for kilo may denote “1000” or “1024”, “M” for mega may denote “1000000” or “1048576” and so on.
- “e.g.,” is a shorthand for “for instance”, and “i.e.,” means “that is” or “in other words”.

Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The ZyXEL Device icon is not an exact representation of your ZyXEL Device.

Table 1 Common Icons

<p>ZyXEL Device</p> 	<p>Computer</p> 	<p>Notebook</p> 
<p>Wireless Signal</p> 	<p>Wireless Base Station</p> 	<p>Internet Cloud</p> 
<p>Router</p> 	<p>Server</p> 	<p>Firewall</p> 

Safety Warnings



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

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

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- ONLY qualified service personnel should service or disassemble this device.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the power outlet.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).

This product is recyclable. Dispose of it properly.



Contents Overview

Introduction	31
Getting Started	33
Introducing the Web Configurator	39
Tutorials and Wizard	47
Tutorial	49
Internet Setup Wizard	61
VoIP Wizard	73
Web Configurator	77
Status Screens	79
Wireless LAN	91
WAN Setup	107
LAN	119
NAT	129
VPN Transport	137
SIP	149
Phone	165
Phone Book	173
Firewall	179
Certificates	187
Content Filter	205
Static Route	209
Remote MGMT	213
UPnP	221
System	233
Logs	241
Tools	255
Troubleshooting and Specifications	261
Troubleshooting	263
Product Specifications	269
Appendices and Index	273

Table of Contents

About This User's Guide	3
Document Conventions	4
Safety Warnings	6
Contents Overview	9
Table of Contents	11
List of Figures	21
List of Tables	27
Part I: Introduction	31
Chapter 1	
Getting Started	33
1.1 About Your ZyXEL Device	33
1.1.1 Wireless Internet Access	33
1.1.2 WiFi Network	34
1.1.3 Make Calls via Internet Telephony Service Provider	34
1.2 ZyXEL Device Hardware	35
1.2.1 LEDs	35
1.2.2 Antennas	36
1.3 Good Habits for Managing the ZyXEL Device	37
Chapter 2	
Introducing the Web Configurator	39
2.1 Web Configurator Overview	39
2.1.1 Accessing the Web Configurator	39
2.1.2 The RESET Button	41
2.2 Web Configurator Main Screen	42
2.2.1 Title Bar	42
2.2.2 Navigation Panel	43
2.2.3 Main Window	45
2.2.4 Status Bar	45

Part II: Tutorials and Wizard..... 47

**Chapter 3
Tutorial..... 49**

- 3.1 Connect to the Internet 49
 - 3.1.1 Configure Internet Access Settings 49
 - 3.1.2 Configure WiMAX Settings 52
- 3.2 Set Up a WiFi Network 53
 - 3.2.1 Configuring the AP (Your ZyXEL Device) 53
- 3.3 Connect to the WiFi Network 54
 - 3.3.1 Connecting to a Wireless LAN 55
- 3.4 Make a Telephone Call Over the Internet 57
 - 3.4.1 Configure Your SIP Account 57
 - 3.4.2 Configure a Phone 58
 - 3.4.3 Set Up Speed Dialing and Make a Call 59

**Chapter 4
Internet Setup Wizard..... 61**

- 4.1 Wizard Setup Overview 61
- 4.2 Internet Connection Wizard Setup 61
- 4.3 Step One: System Information 62
- 4.4 Step Two: Wireless LAN Wizard 63
 - 4.4.1 Wireless LAN Screen 63
 - 4.4.2 Basic (WEP) Security 64
 - 4.4.3 Extend (WPA-PSK or WPA2-PSK) Security 65
 - 4.4.4 The OTIST Screen 65
- 4.5 Step Three: Internet Configuration 66
 - 4.5.1 Connection Type Screen 66
 - 4.5.2 ISP Parameters for Internet Access Screen 67
 - 4.5.3 Antenna Selection Screen 68
 - 4.5.4 IP Address Screen 69
 - 4.5.5 WAN IP Address Assignment 70
 - 4.5.6 Wizard Complete 71

**Chapter 5
VoIP Wizard..... 73**

- 5.1 Introduction 73
- 5.2 VOIP Wizard Setup 73

Part III: Web Configurator 77

Chapter 6	
Status Screens	79
6.1 Status Screen	79
6.2 Site Information	83
6.3 Profile	84
6.4 Packet Statistics	85
6.5 DHCP Table Screen	86
6.6 VoIP Statistics Window	87
Chapter 7	
Wireless LAN.....	91
7.1 Wireless Network Overview	91
7.2 Wireless Security Overview	92
7.2.1 SSID	92
7.2.2 MAC Address Filter	92
7.2.3 User Authentication	92
7.2.4 Encryption	93
7.2.5 One-Touch Intelligent Security Technology (OTIST)	94
7.3 General Wireless LAN Screen	94
7.3.1 No Security	95
7.3.2 WEP Encryption	96
7.3.3 WPA-PSK/WPA2-PSK	97
7.3.4 WPA/WPA2	99
7.4 OTIST	101
7.4.1 Enabling OTIST	101
7.4.2 Starting OTIST	103
7.4.3 Notes on OTIST	103
7.5 MAC Filter	104
7.6 Wireless LAN Advanced Screen	105
Chapter 8	
WAN Setup.....	107
8.1 WAN Overview	107
8.2 WiMAX	107
8.2.1 Authentication	108
8.3 Internet Access Setup	108
8.4 Frequency Settings	111
8.4.1 Frequency Ranges	111
8.4.2 Configuring Frequency Settings	111
8.5 Configuring Advanced WAN Settings	114
8.6 Configuring Traffic Redirect Settings	115
8.6.1 Configuring The Antenna	117

Chapter 9	
LAN.....	119
9.1 LAN Overview	119
9.1.1 IP Address and Subnet Mask	119
9.1.2 DHCP Setup	120
9.1.3 LAN TCP/IP	120
9.1.4 DNS Server Address	120
9.1.5 RIP Setup	121
9.1.6 Multicast	121
9.2 LAN Screens	122
9.2.1 LAN IP Screen	122
9.2.2 LAN DHCP Setup Screen	122
9.2.3 LAN Static DHCP Screen	123
9.2.4 LAN Client List Screen	124
9.2.5 LAN IP Alias Screen	125
9.2.6 LAN Advanced Screen	126
Chapter 10	
NAT.....	129
10.1 NAT Overview	129
10.1.1 Port Forwarding: Services and Port Numbers	129
10.1.2 Trigger Port Forwarding	130
10.1.3 SIP ALG	131
10.2 NAT Screens	131
10.2.1 NAT General Screen	131
10.2.2 NAT Port Forwarding Screen	132
10.2.3 NAT Port Forwarding Edit Screen	133
10.2.4 NAT Trigger Port Screen	134
10.2.5 NAT ALG Screen	135
Chapter 11	
VPN Transport.....	137
11.1 Overview	137
11.1.1 What You Can Do in the VPN Transport Screens	138
11.1.2 What You Need to Know about VPN Transport	138
11.1.3 Before You Begin	140
11.2 The General Screen	140
11.3 The Customer Interface Screen	141
11.4 The Customer Interface Edit Screen	142
11.5 The Ethernet Pseudowire Screen	143
11.6 The Ethernet Pseudowire Edit Screen	144
11.7 The Statistics Screen	145
11.8 VPN Transport Technical Reference	146

11.8.1 Multi-Protocol Label Switching	146
11.8.2 Generic Routing Encapsulation	147
Chapter 12	
SIP	149
12.1 SIP Overview	149
12.1.1 Introduction to VoIP	149
12.1.2 Introduction to SIP	149
12.1.3 SIP Identities	149
12.1.4 SIP Call Progression	150
12.1.5 SIP Client Server	150
12.1.6 RTP	152
12.1.7 NAT and SIP	152
12.1.8 Voice Coding	153
12.1.9 PSTN Call Setup Signaling	154
12.1.10 MWI (Message Waiting Indication)	154
12.1.11 Custom Tones (IVR)	155
12.1.12 Quality of Service (QoS)	155
12.2 SIP Screens	157
12.2.1 SIP Settings Screen	157
12.2.2 Advanced SIP Setup Screen	158
12.2.3 SIP QoS Screen	162
Chapter 13	
Phone	165
13.1 Phone Overview	165
13.1.1 Voice Activity Detection/Silence Suppression/Comfort Noise	165
13.1.2 Echo Cancellation	165
13.1.3 Supplementary Phone Services Overview	165
13.2 Phone Screens	169
13.2.1 Analog Phone Screen	169
13.2.2 Advanced Analog Phone Setup Screen	170
13.2.3 Common Phone Settings Screen	171
13.2.4 Phone Region Screen	171
Chapter 14	
Phone Book	173
14.1 Phone Book Overview	173
14.2 Phone Book Screens	173
14.2.1 Incoming Call Policy Screen	173
14.2.2 Speed Dial Screen	175
Chapter 15	
Firewall	179

15.1 Firewall Overview	179
15.1.1 Stateful Inspection Firewall	179
15.1.2 About the ZyXEL Device Firewall	179
15.1.3 Guidelines For Enhancing Security With Your Firewall	180
15.1.4 The Firewall, NAT and Remote Management	180
15.2 Triangle Route	181
15.2.1 The “Triangle Route” Problem	181
15.2.2 Solving the “Triangle Route” Problem	182
15.3 Firewall Screens	183
15.3.1 General Firewall Screen	183
15.3.2 Firewall Services Screen	183
Chapter 16	
Certificates	187
16.1 Certificates Overview	187
16.1.1 Advantages of Certificates	188
16.2 Self-signed Certificates	188
16.3 Factory Default Certificate	188
16.3.1 Certificate File Formats	188
16.4 Certificate Configuration Screens Summary	189
16.5 Verifying a Certificate	189
16.5.1 Checking the Fingerprint of a Certificate on Your Computer	189
16.6 My Certificates Screen	190
16.6.1 My Certificates Create Screen	192
16.6.2 My Certificate Details Screen	195
16.6.3 My Certificate Import Screen	198
16.7 Trusted CAs	199
16.8 Trusted CA Details	201
16.9 Trusted CA Import	203
Chapter 17	
Content Filter.....	205
17.1 Content Filtering Overview	205
17.2 Content Filtering Screens	205
17.2.1 Content Filter Screen	205
17.2.2 Content Filter Schedule Screen	207
Chapter 18	
Static Route.....	209
18.1 Static Route Overview	209
18.2 Static Route Screens	209
18.2.1 IP Static Route Screen	209
18.2.2 IP Static Route Edit Screen	210

Chapter 19	
Remote MGMT	213
19.1 Remote Management Overview	213
19.1.1 Remote Management Limitations	213
19.1.2 Remote Management and NAT	213
19.1.3 System Timeout	214
19.2 Remote Management Screens	214
19.2.1 WWW Screen	214
19.2.2 Telnet Screen	214
19.2.3 FTP Screen	215
19.3 SNMP	216
19.3.1 Supported MIBs	217
19.3.2 SNMP Traps	217
19.3.3 Configuring SNMP	217
19.3.4 DNS Screen	218
19.3.5 Security Screen	219
Chapter 20	
UPnP	221
20.1 Introducing Universal Plug and Play	221
20.1.1 How do I know if I'm using UPnP?	221
20.1.2 NAT Traversal	221
20.1.3 Cautions with UPnP	221
20.1.4 UPnP and ZyXEL	222
20.2 UPnP Examples	222
20.2.1 Installing UPnP in Windows Example	222
20.2.2 Using UPnP in Windows XP Example	225
20.3 UPnP Screen	231
Chapter 21	
System	233
21.1 System Features Overview	233
21.1.1 System Name	233
21.1.2 Domain Name	233
21.1.3 DNS Server Address Assignment	233
21.1.4 Dynamic DNS	234
21.1.5 Pre-defined NTP Time Servers List	234
21.1.6 Resetting the Time	235
21.2 System Screens	235
21.2.1 General System Screen	235
21.2.2 Dynamic DNS Screen	236
21.2.3 Time Setting Screen	237

Chapter 22	
Logs	241
22.1 Logs Overview	241
22.1.1 Alerts	241
22.1.2 Syslog Logs	241
22.2 Logs Screens	243
22.2.1 Log Viewer Screen	243
22.2.2 Log Settings Screen	243
22.3 Log Message Descriptions	245
Chapter 23	
Tools.....	255
23.1 Tools Overview	255
23.1.1 Firmware	255
23.2 Tools Screens	255
23.2.1 Firmware Screen	255
23.2.2 Firmware Upload Screens	256
23.2.3 Configuration Screen	257
23.2.4 Restore Configuration Screens	258
23.2.5 Restart Screen	259
Part IV: Troubleshooting and Specifications.....	261
Chapter 24	
Troubleshooting.....	263
24.1 Power, Hardware Connections, and LEDs	263
24.2 ZyXEL Device Access and Login	264
24.3 Internet Access	265
24.4 Phone Calls and VoIP	267
24.5 Reset the ZyXEL Device to Its Factory Defaults	267
24.5.1 Pop-up Windows, JavaScripts and Java Permissions	268
24.6 Wireless LAN Troubleshooting	268
Chapter 25	
Product Specifications	269
Part V: Appendices and Index	273
Appendix A WiMAX Security	275
Appendix B Setting up Your Computer's IP Address.....	279

Appendix C Pop-up Windows, JavaScripts and Java Permissions 301

Appendix D IP Addresses and Subnetting 309

Appendix E Wireless LANs 319

Appendix F Common Services 333

Appendix G Legal Information 337

Appendix H Customer Support 341

Index..... 347

List of Figures

Figure 1 Mobile Station and Base Station	34
Figure 2 WLAN Application Example	34
Figure 3 ZyXEL Device's VoIP Features	35
Figure 4 The ZyXEL Device	35
Figure 5 Password Screen	40
Figure 6 Change Password Screen	40
Figure 7 Replace Certificate Screen	40
Figure 8 Wizard or Advanced Screen	41
Figure 9 Main Screen	42
Figure 10 Tutorial: Security	50
Figure 11 Tutorial: Trusted CAs Tab	50
Figure 12 Tutorial: Trusted CAs Screen	50
Figure 13 Tutorial: Network	51
Figure 14 Tutorial: Internet Access Settings	51
Figure 15 Tutorial: WiMAX Frequency Setup	52
Figure 16 Network > Wireless LAN > General	53
Figure 17 Network > Wireless LAN > Device Information	54
Figure 18 Network > Wireless LAN > Interface Status	54
Figure 19 ZyXEL Utility: Security Settings	56
Figure 20 ZyXEL Utility: Confirm Save	56
Figure 21 ZyXEL Utility: Link Info	56
Figure 22 Tutorial: SIP Account Setup	58
Figure 23 Tutorial: the Analog Phone Screen	59
Figure 24 Tutorial: the Speed Dial Screen	60
Figure 25 Tutorial: New Speed Dial Rule	60
Figure 26 Select a Mode	61
Figure 27 Connection Wizard: Introduction	62
Figure 28 Wizard > Step 1 > System Information	62
Figure 29 Wizard > Step 2 > Wireless LAN	63
Figure 30 Wizard > Step 2 > Basic (WEP) Security	64
Figure 31 Wizard > Step 2 > Extend (WPA-PSK or WPA2-PSK) Security	65
Figure 32 Wizard > Step 2 > OTIST	66
Figure 33 Wizard > Step 3 > Connection Type Screen	67
Figure 34 Wizard > Step 3 > ISP Parameters for Internet Access Screen	67
Figure 35 Wizard > Step 3 > Antenna Selection	69
Figure 36 Wizard > Step 3 > IP Address	70
Figure 37 Wizard > Step 3 > WAN IP Address Assignment	71
Figure 38 The Connection Wizard: Congratulations	72

Figure 39 Select a Mode	73
Figure 40 VOIP Wizard: Configuration	74
Figure 41 VoIP Wizard: SIP Registration Test	75
Figure 42 VoIP Wizard: Fail	75
Figure 43 VOIP Wizard: Finish	75
Figure 44 Status Screen	79
Figure 45 The Site Information Screen	83
Figure 46 The WiMAX Profile Screen	84
Figure 47 Packet Statistics	85
Figure 48 DHCP Table	86
Figure 49 VoIP Statistics	87
Figure 50 Example of a Wireless Network	91
Figure 51 Network > Wireless LAN > General	94
Figure 52 Network > Wireless LAN > General: No Security	95
Figure 53 Network > Wireless LAN > General: Static WEP	96
Figure 54 Network > Wireless LAN > General: WPA-PSK/WPA2-PSK	98
Figure 55 Network > Wireless LAN > General: WPA/WPA2	99
Figure 56 Network > Wireless LAN > OTIST	101
Figure 57 Example Wireless Client OTIST Screen	102
Figure 58 Security Key	103
Figure 59 OTIST in Progress (AP)	103
Figure 60 OTIST in Progress (Client)	103
Figure 61 No AP with OTIST Found	103
Figure 62 Start OTIST?	104
Figure 63 Network > Wireless LAN > MAC Filter	105
Figure 64 Network > Wireless LAN > Advanced	106
Figure 65 WiMax: Mobile Station	107
Figure 66 WiMAX: Multiple Mobile Stations	108
Figure 67 Using an AAA Server	108
Figure 68 Network > WAN > Internet Connection	109
Figure 69 Frequency Ranges	111
Figure 70 Network > WAN > WiMAX Frequency	113
Figure 71 Completing the WiMAX Frequency Screen	114
Figure 72 Network > WAN > Advanced	114
Figure 73 Network > WAN > Traffic Redirect	116
Figure 74 Network > WAN > Antenna Selection	117
Figure 75 Network > LAN > IP	122
Figure 76 Network > LAN > DHCP Setup	123
Figure 77 Network > LAN > Static DHCP	124
Figure 78 Network > LAN > Client List	125
Figure 79 Network > LAN > IP Alias	125
Figure 80 Network > LAN > Advanced	127
Figure 81 Multiple Servers Behind NAT Example	129

Figure 82 Trigger Port Forwarding Process: Example	130
Figure 83 Network > NAT > General	131
Figure 84 Network > NAT > Port Forwarding	132
Figure 85 Network > NAT > Port Forwarding > Edit	133
Figure 86 Network > NAT > Trigger Port	134
Figure 87 Network > NAT > ALG	135
Figure 88 VPN Transport example	137
Figure 89 Identifying Users	138
Figure 90 Ethernet Pseudowire Settings Example	139
Figure 91 Pseudowire Mapping	139
Figure 92 Network > VPN Transport > General	140
Figure 93 Network > VPN Transport > Customer Interface	141
Figure 94 Network > VPN Transport > Customer Interface Edit	142
Figure 95 Network > VPN Transport > Ethernet Pseudowire	144
Figure 96 Network > VPN Transport > Ethernet Pseudowire > Edit	145
Figure 97 Network > VPN Transport > Statistics	146
Figure 98 VPLS Tunneling	147
Figure 99 SIP User Agent	151
Figure 100 SIP Proxy Server	151
Figure 101 SIP Redirect Server	152
Figure 102 STUN	153
Figure 103 DiffServ: Differentiated Service Field	156
Figure 104 VoIP > SIP > SIP Settings	157
Figure 105 VoIP > SIP > SIP Settings > Advanced	159
Figure 106 VoIP > SIP > QoS	163
Figure 107 VoIP > Phone > Analog Phone	169
Figure 108 VoIP > Phone > Analog Phone > Advanced	170
Figure 109 VoIP > Phone > Common	171
Figure 110 VoIP > Phone > Region	171
Figure 111 VoIP > Phone Book > Incoming Call Policy	174
Figure 112 VoIP > Phone Book > Speed Dial	176
Figure 113 Firewall Rule Directions	180
Figure 114 Ideal Firewall Setup	181
Figure 115 "Triangle Route" Problem	182
Figure 116 IP Alias	182
Figure 117 Security > Firewall > General	183
Figure 118 Security > Firewall > Services	184
Figure 119 Remote Host Certificates	189
Figure 120 Certificate Details	190
Figure 121 Security > Certificates > My Certificates	191
Figure 122 Security > Certificates > My Certificates > Create	193
Figure 123 Security > Certificates > My Certificates > Details	196
Figure 124 Security > Certificates > My Certificates > Import	199

Figure 125 Security > Certificates > Trusted CAs	200
Figure 126 Security > Certificates > Trusted CAs > Details	201
Figure 127 Security > Certificates > Trusted CAs > Import	204
Figure 128 Security > Content Filter > Filter	206
Figure 129 Security > Content Filter > Schedule	207
Figure 130 Example of Static Routing Topology	209
Figure 131 Management > Static Route > IP Static Route	210
Figure 132 Management > Static Route > IP Static Route > Edit	211
Figure 133 Management > Remote MGMT > WWW	214
Figure 134 Management > Remote MGMT > Telnet	215
Figure 135 Management > Remote MGMT > FTP	215
Figure 136 SNMP Management Model	216
Figure 137 Management > Remote MGMT > SNMP	218
Figure 138 Management > Remote MGMT > DNS	219
Figure 139 Management > Remote MGMT > Security	219
Figure 140 Add/Remove Programs: Windows Setup: Communication	222
Figure 141 Add/Remove Programs: Windows Setup: Communication Components	223
Figure 142 Network Connections	223
Figure 143 Windows Optional Networking Components Wizard	224
Figure 144 Networking Services	224
Figure 145 Network Connections	225
Figure 146 Internet Connection Properties	226
Figure 147 Internet Connection Properties: Advanced Settings	227
Figure 148 Internet Connection Properties: Advanced Settings: Add	227
Figure 149 System Tray Icon	228
Figure 150 Internet Connection Status	228
Figure 151 Network Connections	229
Figure 152 Network Connections: My Network Places	230
Figure 153 Network Connections: My Network Places: Properties: Example	230
Figure 154 Management > UPnP	231
Figure 155 Maintenance > System > General	235
Figure 156 Maintenance > System > Dynamic DNS	236
Figure 157 Maintenance > System > Time Setting	238
Figure 158 Maintenance > Logs > View Log	243
Figure 159 Maintenance > Logs > Log Settings	244
Figure 160 Maintenance > Tools > Firmware	256
Figure 161 Firmware Upload In Process	256
Figure 162 Network Temporarily Disconnected	257
Figure 163 Firmware Upload Error	257
Figure 164 Maintenance > Tools > Configuration	257
Figure 165 Configuration Upload Successful	258
Figure 166 Network Temporarily Disconnected	259
Figure 167 Configuration Upload Error	259

Figure 168 Maintenance > Tools > Restart	259
Figure 169 Maintenance > Tools > Restart > In Progress	260
Figure 170 Windows 95/98/Me: Network: Configuration	280
Figure 171 Windows 95/98/Me: TCP/IP Properties: IP Address	281
Figure 172 Windows 95/98/Me: TCP/IP Properties: DNS Configuration	282
Figure 173 Windows XP: Start Menu	283
Figure 174 Windows XP: Control Panel	283
Figure 175 Windows XP: Control Panel: Network Connections: Properties	284
Figure 176 Windows XP: Local Area Connection Properties	284
Figure 177 Windows XP: Internet Protocol (TCP/IP) Properties	285
Figure 178 Windows XP: Advanced TCP/IP Properties	286
Figure 179 Windows XP: Internet Protocol (TCP/IP) Properties	287
Figure 180 Windows Vista: Start Menu	288
Figure 181 Windows Vista: Control Panel	288
Figure 182 Windows Vista: Network And Internet	288
Figure 183 Windows Vista: Network and Sharing Center	288
Figure 184 Windows Vista: Network and Sharing Center	289
Figure 185 Windows Vista: Local Area Connection Properties	289
Figure 186 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties	290
Figure 187 Windows Vista: Advanced TCP/IP Properties	291
Figure 188 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties	292
Figure 189 Macintosh OS 8/9: Apple Menu	293
Figure 190 Macintosh OS 8/9: TCP/IP	293
Figure 191 Macintosh OS X: Apple Menu	294
Figure 192 Macintosh OS X: Network	295
Figure 193 Red Hat 9.0: KDE: Network Configuration: Devices	296
Figure 194 Red Hat 9.0: KDE: Ethernet Device: General	296
Figure 195 Red Hat 9.0: KDE: Network Configuration: DNS	297
Figure 196 Red Hat 9.0: KDE: Network Configuration: Activate	297
Figure 197 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0	298
Figure 198 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0	298
Figure 199 Red Hat 9.0: DNS Settings in resolv.conf	298
Figure 200 Red Hat 9.0: Restart Ethernet Card	298
Figure 201 Red Hat 9.0: Checking TCP/IP Properties	299
Figure 202 Pop-up Blocker	301
Figure 203 Internet Options: Privacy	302
Figure 204 Internet Options: Privacy	303
Figure 205 Pop-up Blocker Settings	303
Figure 206 Internet Options: Security	304
Figure 207 Security Settings - Java Scripting	305
Figure 208 Security Settings - Java	305
Figure 209 Java (Sun)	306
Figure 210 Mozilla Firefox: Tools > Options	307

List of Figures

Figure 211 Mozilla Firefox Content Security	307
Figure 212 Network Number and Host ID	310
Figure 213 Subnetting Example: Before Subnetting	312
Figure 214 Subnetting Example: After Subnetting	313
Figure 215 Conflicting Computer IP Addresses Example	317
Figure 216 Conflicting Computer IP Addresses Example	317
Figure 217 Conflicting Computer and Router IP Addresses Example	318
Figure 218 Peer-to-Peer Communication in an Ad-hoc Network	319
Figure 219 Basic Service Set	320
Figure 220 Infrastructure WLAN	321
Figure 221 RTS/CTS	322
Figure 222 WPA(2) with RADIUS Application Example	329
Figure 223 WPA(2)-PSK Authentication	330

List of Tables

Table 1 Common Icons	5
Table 2 Models Covered	33
Table 3 The ZyXEL Device	35
Table 4 Web Configurator Icons in the Title Bar	43
Table 5 Navigation Panel Summary	43
Table 6 Example Internet Access Information	49
Table 7 Wizard > Step 1 > System Information	62
Table 8 Wizard > Step 2 > Wireless LAN	63
Table 9 Wizard > Step 2 > Basic (WEP) Security	64
Table 10 Wizard > Step 2 > Extend (WPA-PSK or WPA2-PSK) Security	65
Table 11 Wizard > Step 2 > OTIST	66
Table 12 Wizard > Step 3 > ISP Parameters for Internet Access Screen	67
Table 13 Wizard > Step 3 > Antenna Selection	69
Table 14 Wizard > Step 3 > IP Address	70
Table 15 Wizard > Step 3 > WAN IP Address Assignment	71
Table 16 VOIP Wizard Configuration	74
Table 17 Status Screen	80
Table 18 The Site Information Screen	84
Table 19 The WiMAX Profile Screen	84
Table 20 Packet Statistics	86
Table 21 DHCP Table	87
Table 22 VoIP Statistics	87
Table 23 Types of Encryption for Each Type of Authentication	93
Table 24 Network > Wireless LAN > General	95
Table 25 Wireless No Security	96
Table 26 Network > Wireless LAN > General: Static WEP	97
Table 27 Network > Wireless LAN > General: WPA-PSK/WPA2-PSK	98
Table 28 Network > Wireless LAN > General: WPA/WPA2	100
Table 29 Network > Wireless LAN > OTIST	102
Table 30 Network > Wireless LAN > MAC Filter	105
Table 31 Network > Wireless LAN > Advanced	106
Table 32 Network > WAN > Internet Connection	109
Table 33 Radio Frequency Conversion	111
Table 34 DL Frequency Example Settings	112
Table 35 Network > WAN > WiMAX Frequency	113
Table 36 Example Supported Frequencies (GHz)	113
Table 37 Network > WAN > Advanced	115
Table 38 Network > WAN > Traffic Redirect	116

Table 39 Network > WAN > Antenna Selection	117
Table 40 Network > LAN > IP	122
Table 41 Network > LAN > DHCP Setup	123
Table 42 Network > LAN > Static DHCP	124
Table 43 Network > LAN > Client List	125
Table 44 Network > LAN > IP Alias	126
Table 45 Network > LAN > Advanced	127
Table 46 Network > NAT > General	131
Table 47 Network > NAT > Port Forwarding	133
Table 48 Network > NAT > Port Forwarding > Edit	134
Table 49 Network > NAT > Trigger Port	135
Table 50 Network > NAT > ALG	135
Table 51 Network > VPN Transport > General	140
Table 52 Network > VPN Transport > Customer Interface	141
Table 53 Network > VPN Transport > Customer Interface Edit	142
Table 54 Network > VPN Transport > Ethernet Pseudowire	144
Table 55 Network > VPN Transport > Ethernet Pseudowire > Edit	145
Table 56 Network > VPN Transport > Statistics	146
Table 57 SIP Call Progression	150
Table 58 Custom Tones Details	155
Table 59 VoIP > SIP > SIP Settings	157
Table 60 VoIP > SIP > SIP Settings > Advanced	160
Table 61 VoIP > SIP > QoS	163
Table 62 European Type Flash Key Commands	166
Table 63 USA Type Flash Key Commands	168
Table 64 VoIP > Phone > Analog Phone	169
Table 65 VoIP > Phone > Analog Phone > Advanced	170
Table 66 VoIP > Phone > Common	171
Table 67 VoIP > Phone > Region	171
Table 68 VoIP > Phone Book > Incoming Call Policy	174
Table 69 VoIP > Phone Book > Speed Dial	176
Table 70 Security > Firewall > General	183
Table 71 Security > Firewall > Services	184
Table 72 Security > Certificates > My Certificates	191
Table 73 Security > Certificates > My Certificates > Create	193
Table 74 Security > Certificates > My Certificates > Details	196
Table 75 Security > Certificates > My Certificates > Import	199
Table 76 Security > Certificates > Trusted CAs	200
Table 77 Security > Certificates > Trusted CAs > Details	202
Table 78 Security > Certificates > Trusted CAs Import	204
Table 79 Security > Content Filter > Filter	206
Table 80 Security > Content Filter > Schedule	207
Table 81 Management > Static Route > IP Static Route	210

Table 82 Management > Static Route > IP Static Route > Edit	211
Table 83	213
Table 84 Management > Remote MGMT > WWW	214
Table 85 Management > Remote MGMT > Telnet	215
Table 86 Management > Remote MGMT > FTP	215
Table 87 SNMP Traps	217
Table 88 Remote Management: SNMP	218
Table 89 Management > Remote MGMT > DNS	219
Table 90 Management > Remote MGMT > Security	220
Table 91 Management > UPnP	231
Table 92 Pre-defined NTP Time Servers	234
Table 93 Maintenance > System > General	235
Table 94 Maintenance > System > Dynamic DNS	237
Table 95 Maintenance > System > Time Setting	238
Table 96 Syslog Logs	242
Table 97 RFC-2408 ISAKMP Payload Types	242
Table 98 Maintenance > Logs > View Log	243
Table 99 Maintenance > Logs > Log Settings	244
Table 100 System Error Logs	245
Table 101 System Maintenance Logs	246
Table 102 Access Control Logs	246
Table 103 TCP Reset Logs	247
Table 104 Packet Filter Logs	248
Table 105 ICMP Logs	248
Table 106 CDR Logs	248
Table 107 PPP Logs	248
Table 108 UPnP Logs	249
Table 109 Content Filtering Logs	249
Table 110 Attack Logs	249
Table 111 Remote Management Logs	250
Table 112 ICMP Notes	251
Table 113 SIP Logs	252
Table 114 RTP Logs	252
Table 115 FSM Logs: Caller Side	252
Table 116 FSM Logs: Callee Side	253
Table 117 Lifeline Logs	253
Table 118 Maintenance > Tools > Firmware	256
Table 119 Maintenance > Tools > Configuration	258
Table 120 Product Specifications	269
Table 121 Physical Features	270
Table 122 Non-Physical Features	270
Table 123 IP Address Network Number and Host ID Example	310
Table 124 Subnet Masks	311

List of Tables

Table 125 Maximum Host Numbers	311
Table 126 Alternative Subnet Mask Notation	311
Table 127 Subnet 1	313
Table 128 Subnet 2	314
Table 129 Subnet 3	314
Table 130 Subnet 4	314
Table 131 Eight Subnets	314
Table 132 24-bit Network Number Subnet Planning	315
Table 133 16-bit Network Number Subnet Planning	315
Table 134 IEEE 802.11g	323
Table 135 Wireless Security Levels	324
Table 136 Comparison of EAP Authentication Types	327
Table 137 Wireless Security Relational Matrix	330
Table 138 Commonly Used Services	333

PART I

Introduction

Getting Started (33)

Introducing the Web Configurator (39)

1

Getting Started

This chapter introduces the main features and applications of the ZyXEL Device.

1.1 About Your ZyXEL Device

The ZyXEL Device is a WiMAX WiFi router with built-in switch and VoIP. It allows you to access the Internet by connecting to a WiMAX wireless network.

You can create a WiFi network using the Wireless LAN feature.

You can use a traditional analog telephone to make Internet calls using the ZyXEL Device's Voice over IP (VoIP) communication capabilities.

You can configure firewall and content filtering for secure Internet access, as well as a host of other features.

The web browser-based Graphical User Interface (GUI), also known as the web configurator, provides easy management.

See [Chapter 25 on page 269](#) for a complete list of features for your model.

At the time of writing, this User's Guide covers the following models:

Table 2 Models Covered

MAX-200HW2	2.5Ghz
MAX-210HW2	3.5Ghz
MAX-230HW2	2.3Ghz

This User's Guide uses screens and example settings from the MAX-210HW2 model.

1.1.1 Wireless Internet Access

Connect your computer or network to the ZyXEL Device for wireless Internet access. See the Quick Start Guide for instructions on hardware connection.

In a wireless metropolitan area network (MAN), the ZyXEL Device connects to a base station (BS) for Internet access.

The following diagram shows a notebook computer equipped with the ZyXEL Device connecting to the Internet through a base station (marked **BS**).

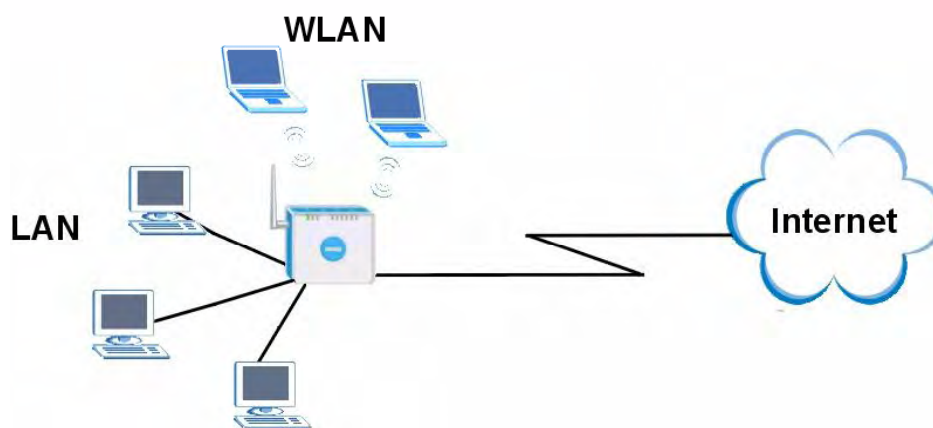
Figure 1 Mobile Station and Base Station

You can also configure firewall and content filtering on the ZyXEL Device for secure Internet access. When the firewall is on, all incoming traffic from the Internet to your network is blocked unless it is initiated from your network. This means that probes from the outside to your network are not allowed, but you can safely browse the Internet and download files.

Use content filtering to block access to web sites with URLs containing keywords that you specify. You can define time periods and days during which content filtering is enabled and include or exclude particular computers on your network from content filtering. For example, you could block access to certain web sites for the kids.

1.1.2 WiFi Network

The ZyXEL Device Wireless LAN feature allows IEEE 802.11b or IEEE 802.11g compatible wireless clients to access the Internet or the local network as well as to communicate with each other. Wireless stations can move freely anywhere in the coverage area and use resources on the wired network.

Figure 2 WLAN Application Example

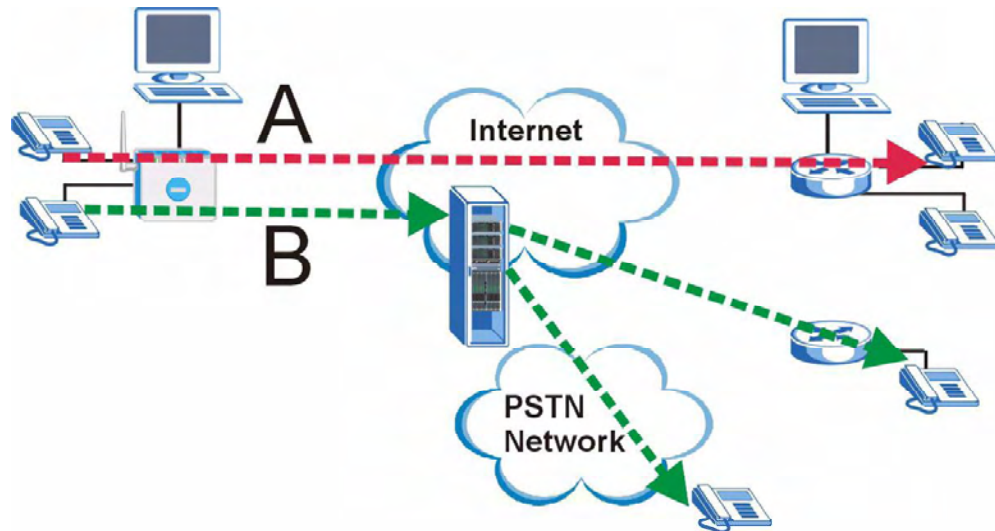
1.1.3 Make Calls via Internet Telephony Service Provider

In a home or small office environment, you can use the ZyXEL Device to make and receive the following types of VoIP telephone calls:

- Peer-to-Peer calls (A) - Use the ZyXEL Device to make a call to the recipient's IP address without using a SIP proxy server.

- Calls via a VoIP service provider (**B**) - The ZyXEL Device sends your call to a VoIP service provider's SIP server which forwards your calls to either VoIP or PSTN phones.

Figure 3 ZyXEL Device's VoIP Features



1.2 ZyXEL Device Hardware

Follow the instructions in the Quick Start Guide to make hardware connections.

1.2.1 LEDs

The following figure shows the LEDs (lights) on the ZyXEL Device.

Figure 4 The ZyXEL Device



The following table describes your ZyXEL Device's LEDs.

Table 3 The ZyXEL Device

LED	STATE	DESCRIPTION
PWR	OFF	The ZyXEL Device is not receiving power.
	RED	The ZyXEL Device is receiving power but has been unable to start up correctly. See the Troubleshooting section for more information.
	RED / ORANGE (BLINKING)	The ZyXEL Device is starting up.
	GREEN	The ZyXEL Device is receiving power and functioning correctly.
	GREEN (BLINKING)	The ZyXEL Device is performing a self-test.

Table 3 The ZyXEL Device

LED	STATE	DESCRIPTION
LAN 1 to 4	OFF	The LAN is not connected.
	GREEN	The ZyXEL Device has a successful Local Area Network (Ethernet) connection.
	GREEN (BLINKING)	Your device is sending/receiving data through the wireless LAN.
VoIP 1 to 2	OFF	No SIP account is registered, or the ZyXEL Device is not receiving power.
	GREEN	A SIP account is registered.
	GREEN (BLINKING)	A SIP account is registered, and the phone attached to the LINE port is in use (off the hook).
	ORANGE	A SIP account is registered and has a voice message.
	ORANGE (BLINKING)	A SIP account is registered and has a voice message, and the phone attached to the LINE port is in use (off the hook).
LINK	OFF	The ZyXEL Device is not connected to a wireless (WiMAX) network.
	GREEN	The ZyXEL Device is successfully connected to a wireless (WiMAX) network.
	GREEN (BLINKING SLOWLY)	The ZyXEL Device is searching for a wireless (WiMAX) network.
	GREEN (BLINKING QUICKLY)	The ZyXEL Device has found a wireless (WiMAX) network and is connecting.
WLAN	OFF	The wireless LAN is not ready or has failed.
	GREEN	The wireless LAN is active.
	GREEN (BLINKING)	The ZyXEL Device is sending/receiving data through the wireless LAN.
SIGNAL 1 ~ 5	The SIGNAL LEDs display the Received Signal Strength Indication (RSSI) of the wireless (WiMAX) connection.	
	NO SIGNAL LEDS ON	There is no wireless connection.
	SIGNAL 1 ON	The signal strength is less than -80 dBm
	SIGNAL 2 ON	The signal strength is between -79 and -70 dBm
	SIGNAL 3 ON	The signal strength is between -69 and -60 dBm
	SIGNAL 4 ON	The signal strength is between -59 and -50 dBm
	SIGNAL 5 ON	The signal strength is more than -50 dBm

1.2.2 Antennas

If you have a MAX-210HW2 you should have a 2dBi WiFi omni antenna and a 2dBi WiMAX omni antenna. Connect the WiFi antenna to the SMA connector port labelled WiFi. Connect the WiMAX antenna to the SMA connector port labelled WiMAX. Make sure you connect the correct antenna to the correct connector port.

If you have a MAX-200HW2 or MAX-210HW2 you should have a 2dBi Wifi omni antenna and a panel directional antenna. Connect the WiFi omni antenna to the connector port labelled WiFi. Connect the cable to the panel directional antenna and connector port labelled WiMAX. Make sure you position the panel directional antenna as far away from the device as possible to minimize interference. See the panel directional antenna documentation on how to set it up.

The MAX-210HW2 is also equipped with one internal 6dBi directional patch antenna for WiMAX. If your signal strength is poor (use the **SIGNAL** LEDs to gauge received signal strength) orient the front of the ZyXEL Device (the side with the LEDs) towards the base station. If you do not know the location of the base station, experiment with moving the ZyXEL Device while observing the **SIGNAL** LEDs.

1.3 Good Habits for Managing the ZyXEL Device

Do the following things regularly to make the ZyXEL Device more secure and to manage the ZyXEL Device more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the ZyXEL Device becomes unstable or even crashes. If you forget your password, you will have to reset the ZyXEL Device to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the ZyXEL Device. You could simply restore your last configuration.

2

Introducing the Web Configurator

This chapter describes how to access and navigate the web configurator.

2.1 Web Configurator Overview

The web configurator is an HTML-based management interface that allows easy device 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:

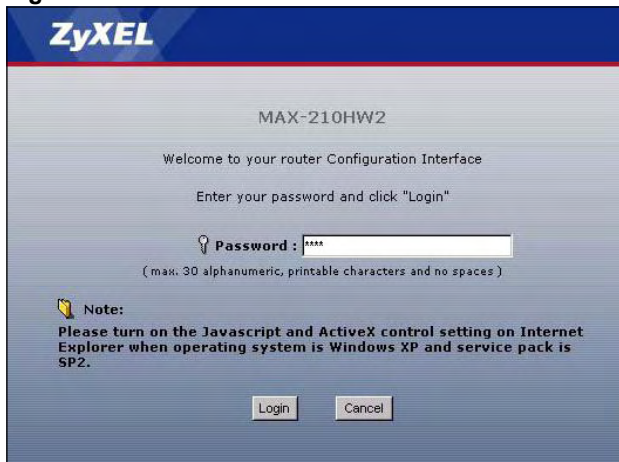
- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

See the Troubleshooting chapter if you need to make sure these functions are allowed in Internet Explorer.

2.1.1 Accessing the Web Configurator

- 1 Make sure your ZyXEL Device hardware is properly connected (refer to the Quick Start Guide).
- 2 Launch your web browser.
- 3 Type "192.168.1.1" as the URL.
- 4 A password screen displays. The default password ("1234") displays in non-readable characters. If you haven't changed the password yet, you can just click **Login**. Click **Cancel** to revert to the default password in the password field. If you have changed the password, enter your password and click **Login**.

Figure 5 Password Screen



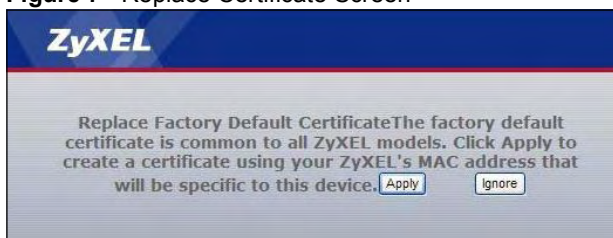
- 5 The following screen displays if you have not yet changed your password. It is highly recommended you change the default password. Enter a new password, retype it to confirm and click **Apply**; alternatively click **Ignore** to proceed to the main menu if you do not want to change the password now.

Figure 6 Change Password Screen



- 6 Click **Apply** in the next screen to create a certificate using your ZyXEL Device's MAC address that will be specific to this device. This certificate is used for authentication when using a secure HTTPS connection over the Internet.

Figure 7 Replace Certificate Screen

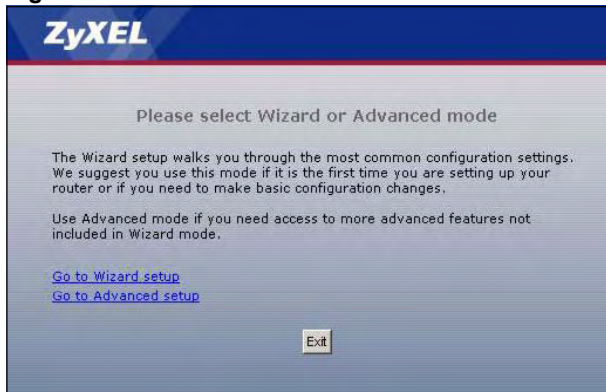


- 7 A screen displays to let you choose whether to go to the wizard or the advanced screens.
- Click **Go to Wizard setup** if you are logging in for the first time or if you want to make basic changes. The wizard selection screen appears after you click **Apply**. See [Chapter 4 on page 61](#) for more information.
 - Click **Go to Advanced setup** if you want to configure features that are not available in the wizards. The main screen appears after you click **Apply**. See [Section 2.2 on page 42](#) for more information.
 - Click **Exit** if you want to log out.



For security reasons, by default the ZyXEL Device automatically logs you out if you do not use the web configurator for five minutes. If this happens, log in again.

Figure 8 Wizard or Advanced Screen



2.1.2 The RESET Button

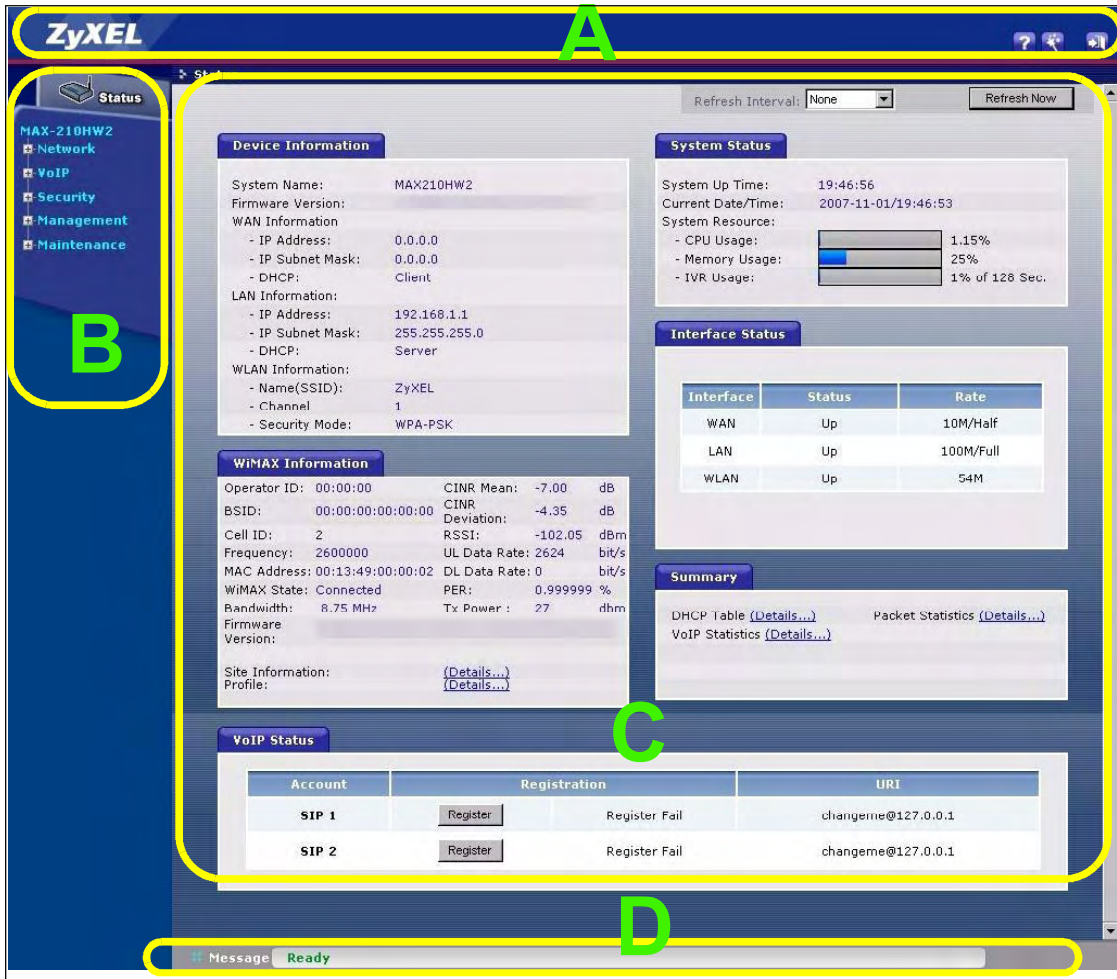
If you forget your password or cannot access the web configurator, you will need to use the **RESET** button to reload the factory-default configuration file. This means that you will lose all configurations that you had previously and the password will be reset to “1234”.

2.1.2.1 Using The Reset Button

- 1 Make sure the **POWER** light is on (not blinking).
- 2 To set the device back to the factory default settings, press the **RESET** button for ten seconds or until the **POWER** light begins to blink and then release it. When the **POWER** light begins to blink, the defaults have been restored and the device restarts.
- 3 Reconfigure the ZyXEL Device, following the steps in your Quick Start Guide.

2.2 Web Configurator Main Screen

Figure 9 Main Screen



As illustrated above, the main screen is divided into these parts:

- A - title bar
- B - navigation panel
- C - main window
- D - status bar



2.2.1 Title Bar

The title bar provides some icons in the upper right corner.



The icons have the following functions.

Table 4 Web Configurator Icons in the Title Bar

ICON	DESCRIPTION
	Wizards: Click this icon to go to the configuration wizards. See Chapter 4 on page 61 for more information.
	Logout: Click this icon to log out of the web configurator.

2.2.2 Navigation Panel

Use the menu items on the navigation panel to open screens to configure ZyXEL Device features. The following table describes the menu items.

Table 5 Navigation Panel Summary

LINK	TAB	FUNCTION
Status		This screen contains administrative and system-related information.
Network		
Wireless LAN	General	Use this screen to enable Wireless LAN and configure WiFi security.
	OTIST	Use this screen to enable OTIST.
	MAC Filter	Use this screen to configure the MAC address filtering options.
	Advanced	Use this screen to set the 802.11 mode.
WAN	Internet Connection	Use this screen to configure ISP parameters, WAN IP address assignment and other advanced properties.
	WiMAX Frequency	Use this screen to set the radio frequencies the ZyXEL Device searches for a WiMAX connection.
	Advanced	Use this screen to configure DNS servers, RIP & Multicast, and Windows networking settings.
	Traffic Redirect	Use this screen to configure your traffic redirect properties
	Antenna Selection	Use this screen to choose which antenna (external or internal) you want the ZyXEL Device to use.
LAN	IP	Use this screen to configure LAN TCP/IP settings.
	DHCP Setup	Use this screen to configure LAN DHCP and DNS settings.
	Static DHCP	Use this screen to always assign specific IP addresses to individual MAC addresses.
	Client List	Use this screen to view current DHCP client information.
	IP Alias	Use this screen to partition your LAN interface into subnets.
	Advanced	Use this screen to configure RIP and Multicast setup settings.
NAT	General	Use this screen to enable NAT.
	Port Forwarding	Use this screen to make your local servers visible to the outside world.
	Trigger Port	Use this screen to set port triggering rules.
	ALG	Use this screen to configure Application Level Gateway settings.

Table 5 Navigation Panel Summary

LINK	TAB	FUNCTION
VPN Transport	General	Use the General screen to turn VPN transport on or off, and to set the VPN transport endpoint (your service provider's router).
	Customer Interface	Use this screen to configure the VPNs used by the ZyXEL Device.
	Ethernet Pseudowire	Use this screen to configure Ethernet pseudowires. Each Ethernet pseudowire mimics a regular wired Ethernet connection, transporting VPLS data over the WiMAX network.
	Statistics	Use this screen to view details and performance information of each active customer interface and its associated Ethernet pseudowire.
VoIP		
SIP	SIP Settings	Use this screen to configure your ZyXEL Device's Voice over IP settings.
	QoS	Use this screen to configure your ZyXEL Device's Quality of Service settings for VoIP.
Phone	Analog Phone	Use this screen to set which SIP account to use for outgoing or incoming calls.
	Common	Use this screen to configure general phone settings.
	Region	Use this screen to select your location and call service mode.
Phone Book	Incoming Call Policy	Use this screen to configure call-forwarding.
	Speed Dial	Use this screen to configure speed dial for SIP phone numbers that you call often.
Security		
Firewall	General	Use this screen to activate/deactivate the firewall and the default action to take on network traffic going in specific directions.
	Services	Use this screen to set the days and times for your device to perform service blocking.
Certificates	My Certificates	Use this screen to generate and export self-signed certificates or certification requests and import the ZyXEL Device's CA-signed certificates.
	Trusted CAs	Use this screen to save CA certificates and trusted remote host certificates to the ZyXEL Device.
Content Filter	Filter	Use this screen to block sites containing certain keywords in the URL, exclude a range of users on the LAN from content filtering on your ZyXEL Device and restrict certain web features.
	Schedule	Use this screen to set the days and times for your ZyXEL Device to perform content filtering.
Management		
Static Route	IP Static Route	Use this screen to configure IP static routes to tell your device about networks beyond the directly connected remote nodes.

Table 5 Navigation Panel Summary

LINK	TAB	FUNCTION
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 ZyXEL Device.
	Telnet	Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet to manage the ZyXEL Device.
	FTP	Use this screen to configure through which interface(s) and from which IP address(es) users can use FTP to access the ZyXEL Device.
	SNMP	Use this screen to configure your ZyXEL Device's settings for Simple Network Management Protocol management.
	DNS	Use this screen to configure through which interface(s) and from which IP address(es) users can send DNS queries to the ZyXEL Device.
	Security	Use this screen to set whether or not your device will respond to pings and probes for services that you have not made available.
UPnP	General	Use this screen to turn UPnP on or off.
Maintenance		
System	General	This screen contains administrative and system-related information and also allows you to change your password.
	Dynamic DNS	Use this screen to set up Dynamic DNS.
	Time Setting	Use this screen to change your ZyXEL Device's time and date.
Logs	View Log	Use this screen to display your device's logs.
	Log Settings	Use this screen to select which logs and/or immediate alerts your device is to record. You can also set it to e-mail the logs to you.
Tools	Firmware	Use this screen to upload firmware to your device.
	Configuration	Use this screen to backup and restore your device's configuration (settings) or reset the factory default settings.
	Restart	This screen allows you to reboot the ZyXEL Device without turning the power off.

2.2.3 Main Window

The main window displays information and configuration fields. It is discussed in the rest of this document.

Right after you log in, the **Status** screen is displayed. See [Chapter 6 on page 79](#) for more information about the **Status** screen.

2.2.4 Status Bar

Check the status bar when you click **Apply** or **OK** to verify that the configuration has been updated.

PART II

Tutorials and Wizard

Tutorial (49)

Internet Setup Wizard (61)

VoIP Wizard (73)

3

Tutorial

This chapter provides examples showing how to use the ZyXEL Device to access the Internet, set up a WiFi network, set up VoIP and make a telephone call over the Internet using the ZyXEL Device's speed dial feature.

3.1 Connect to the Internet

This section shows how to set up your Internet access details on the ZyXEL Device and configure your WiMAX frequency settings. See [Section 8.2 on page 107](#) for more information on how WiMAX works.

3.1.1 Configure Internet Access Settings

To access the Internet, you need information from your Internet Service Provider (ISP) about your account and the network. In this example, your ISP has given you the following information.

Table 6 Example Internet Access Information

Username	User1234
Password	4321
Certificate	Included on CD
Authentication Type	TTLS
TTLS Inner EAP mode	CHAP



The information provided by your ISP may be quite different from this example information. When you enter user information, always enter the information supplied by your service provider and leave other fields at their defaults.

Your ISP has also told you that you will be assigned a dynamic IP address each time you connect to the Internet. See [Section 8.3 on page 108](#) for more details about dynamic and static IP addresses.

Once you have connected the ZyXEL Device to your computer and accessed the Web Configurator (see the Quick Start Guide for details) follow the steps below to connect to a network.

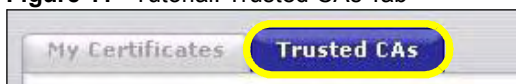
- 1 First, install your security certificate. In the Web Configurator, click **Security > Certificates**.

Figure 10 Tutorial: Security



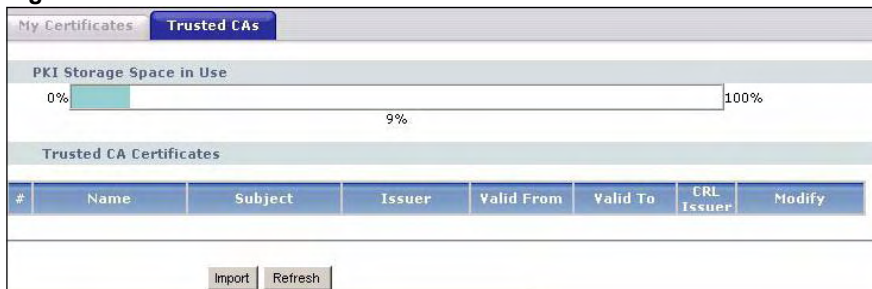
- 2 Click the **Trusted CAs** tab.

Figure 11 Tutorial: Trusted CAs Tab



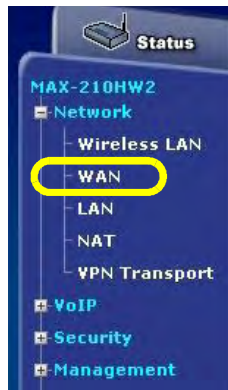
- 3 The following screen displays. This is where you can choose a security certificate for the ZyXEL Device to use.

Figure 12 Tutorial: Trusted CAs Screen



- 4 Click **Import**, then click **Browse** in the screen that appears. Browse to the location of your certificate (on the CD from your ISP in this example) and click **Open**.
- 5 The certificate's location displays in the **File Path** field. Click **Apply**. The **Trusted CAs** screen displays again, showing the certificate's details in the **Trusted CA Certificates** section. You have successfully uploaded your certificate!
- 6 Next, configure your Internet access settings. In the Web Configurator, click **Network > WAN** in the navigation panel.

Figure 13 Tutorial: Network



- 7 The following screen displays. This screen is where you enter your Internet access details.



Not all fields are available in all ZyXEL Devices.

Figure 14 Tutorial: Internet Access Settings

ISP Parameters for Internet Access	
User	<input type="text"/>
Password	<input type="password"/>
Anonymous Identity	<input type="text"/>
PKM	PKMV2
Authentication	TTLS
TTLS Inner EAP	CHAP
Auth Mode	6 - Certs and User Authentication
Certificate	<input type="text"/>
WAN IP Address Assignment	
<input checked="" type="radio"/> Get automatically from ISP (Default)	
<input type="radio"/> Use Fixed IP Address	
IP Address	<input type="text" value="0.0.0.0"/>
IP Subnet Mask	<input type="text" value="0.0.0.0"/>
Gateway IP Address	<input type="text" value="0.0.0.0"/>
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

In the **ISP Parameters for Internet Access** area, enter your username ('User1234') in the **User** field, and enter your password ('4321') in the **Password** field. Select **TTLS** from the **Authentication** list, and select **CHAP** from the **TTLS Inner EAP** list. Leave **PKM** at its default.

In the **WAN IP Address Assignment** area, make sure that **Get Automatically from ISP (Default)** is selected. Leave all other fields at their default values.

- 8 Click **Apply**. Your Internet access settings are saved to the ZyXEL Device, and are used automatically each time you connect to the Internet.

3.1.2 Configure WiMAX Settings

The **WiMAX Frequency** screen allows you to specify a set of frequencies to search for a connection to a base station. Before you start, you need information from your ISP about the supported frequencies.

In this example, your ISP has told you that the supported WiMAX frequencies are at 2.55 and 2.56 Gigahertz (GHz). See [Section 8.4 on page 111](#) for more information on radio frequencies.

Follow the steps below to configure your frequency settings.

- 1 Click **Network > WAN > WiMAX Frequency** to open the screen shown next.

Figure 15 Tutorial: WiMAX Frequency Setup

DL Frequency [0]	<input type="text" value="2600000"/>	kHz
DL Frequency [1]	<input type="text" value="2550000"/>	kHz
DL Frequency [2]	<input type="text" value="2560000"/>	kHz
DL Frequency [3]	<input type="text" value="0"/>	kHz
DL Frequency [4]	<input type="text" value="0"/>	kHz
DL Frequency [5]	<input type="text" value="0"/>	kHz
DL Frequency [6]	<input type="text" value="0"/>	kHz
DL Frequency [7]	<input type="text" value="0"/>	kHz
DL Frequency [8]	<input type="text" value="0"/>	kHz
DL Frequency [9]	<input type="text" value="0"/>	kHz

- 2 Enter the frequency settings your ISP gave you in the **DL Frequency** fields. Note that these fields are in kilohertz (**kHz**).
2.55 GHz is equal to 2550000 kHz, so enter **2550000** in the DL Frequency [1] field.
2.56 GHz is equal to 2560000 kHz, so enter **2560000** in the DL Frequency [2] field.
- 3 Click **Apply** to save your settings. The ZyXEL Device scans for an available wireless connection at the **DL Frequency [1]** setting (2.55 GHz) and, if it does not find an available connection, searches at the **DL Frequency [2]** setting (2.56 GHz). When it finds an available connection, the fields in this screen will be automatically set to use that frequency.
For an example of using the WiMAX Frequency screen to configure more frequencies, see [Section 8.4.2.1 on page 113](#).
- 4 Look at the LEDs on your ZyXEL Device. When the ZyXEL Device successfully connects to a base station, the **LINK** LED shines green steadily. The **SIGNAL 1 ~ 5** LEDs indicate the signal strength, with **SIGNAL 5** showing a very strong signal and **SIGNAL 1** showing a very weak signal.
- 5 Open your Internet browser and enter <http://www.zyxel.com> or the URL of any other web site in the address bar. If you are able to access the web site, your wireless

connection is successfully configured. If you cannot access the web site, check the Troubleshooting section of this User's Guide.

3.2 Set Up a WiFi Network

SSID	SSID_Example3
Channel	6
Security	WPA-PSK (Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey)
802.11 mode	IEEE 802.11b/g

An access point (AP) or wireless router is referred to as an “AP” and a computer with a wireless network card or USB/PCI adapter is referred to as a “wireless client” here.

We use the M-302 utility screens as an example for the wireless client. The screens may vary for different models.

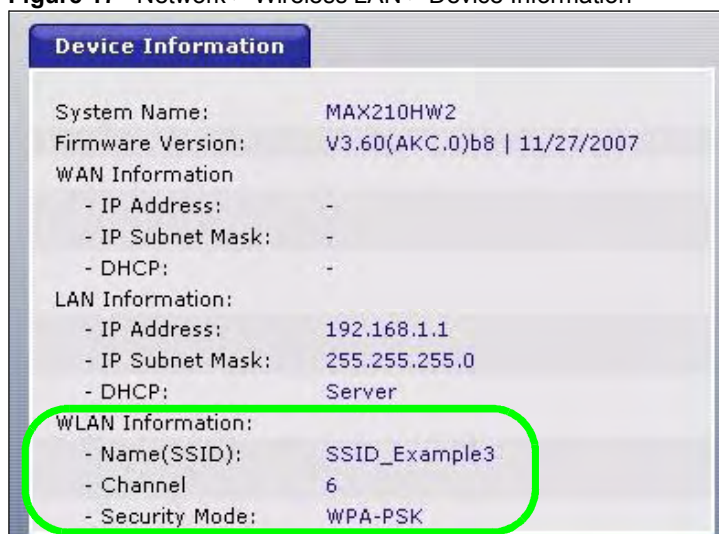
3.2.1 Configuring the AP (Your ZyXEL Device)

Follow the steps below to configure the wireless settings on your ZyXEL Device.

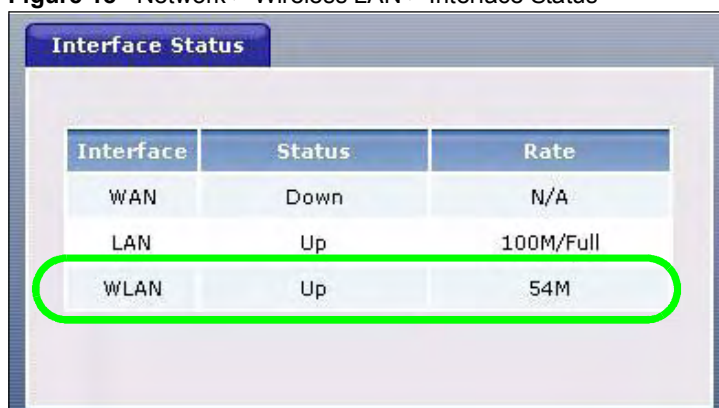
- 1 Open the **Wireless LAN > General** screen in the ZyXEL Device’s web configurator.

Figure 16 Network > Wireless LAN > General

- 2 Make sure the **Enable Wireless LAN** check box is selected.
- 3 Enter **SSID_Example3** as the SSID and select a channel.
- 4 Set security mode to **WPA-PSK** and enter **ThisismyWPA-PSKpre-sharedkey** in the **Pre-Shared Key** field. Click **Apply**.
- 5 Open the **Status** screen. Verify your wireless and wireless security settings under **Device Information**.

Figure 17 Network > Wireless LAN > Device Information

6 Check if the WLAN connection is up under **Interface Status**.

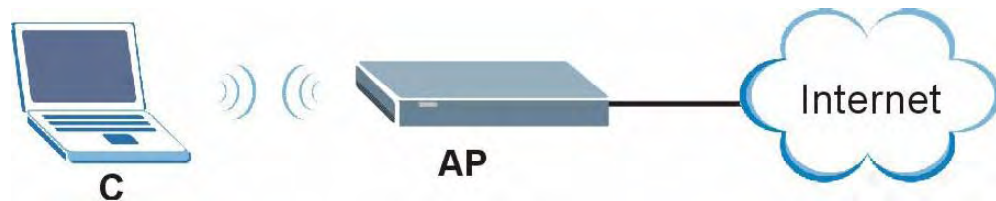
Figure 18 Network > Wireless LAN > Interface Status

3.3 Connect to the WiFi Network

This section describes how to connect the wireless client to your WiFi network.

3.3.1 Connecting to a Wireless LAN

The following sections show you how to join a wireless network using the ZyXEL utility, as in the following diagram. The wireless client is labelled **C** and the access point is labelled **AP**.



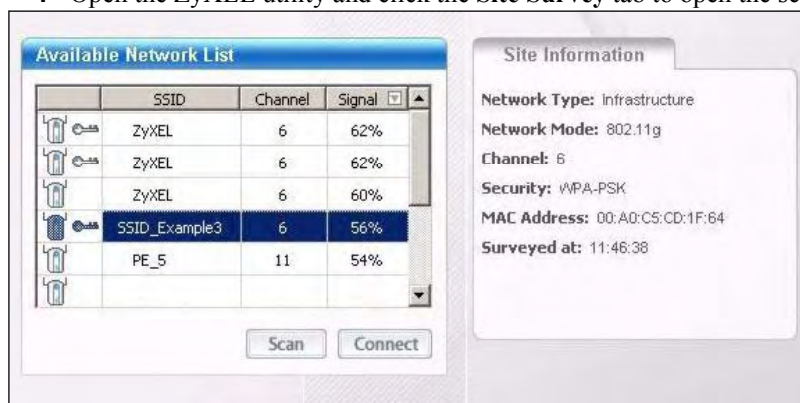
There are three ways to connect the client to an access point.

- Configure nothing and leave the wireless client to automatically scan for and connect to any available network that has no wireless security configured.
- Manually connect to a network.
- Configure a profile to have the wireless client automatically connect to a specific network or peer computer.

This example illustrates how to manually connect your wireless client to an access point (AP) which is configured for WPA-PSK security and connected to the Internet. Before you connect to the access point, you must know its Service Set IDentity (SSID) and WPA-PSK pre-shared key. In this example, the SSID is “SSID_Example3” and the pre-shared key is “ThisismyWPA-PSKpre-sharedkey”.

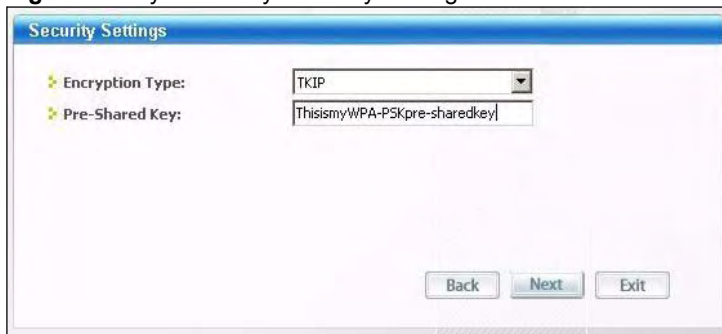
After you install the ZyXEL utility and then insert the wireless client, follow the steps below to connect to a network using the **Site Survey** screen.

- 1 Open the ZyXEL utility and click the **Site Survey** tab to open the screen shown next.

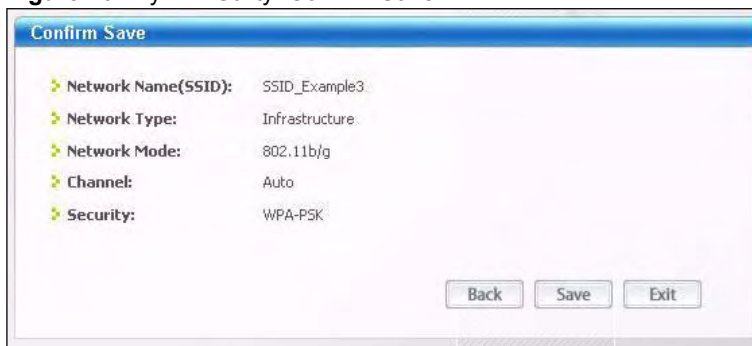


- 2 The wireless client automatically searches for available wireless networks. Click **Scan** if you want to search again. If no entry displays in the **Available Network List**, that means there is no wireless network available within range. Make sure the AP or peer computer is turned on or move the wireless client closer to the AP or peer computer.
- 3 When you try to connect to an AP with security configured, a window will pop up prompting you to specify the security settings. Enter the pre-shared key and leave the encryption type at the default setting.

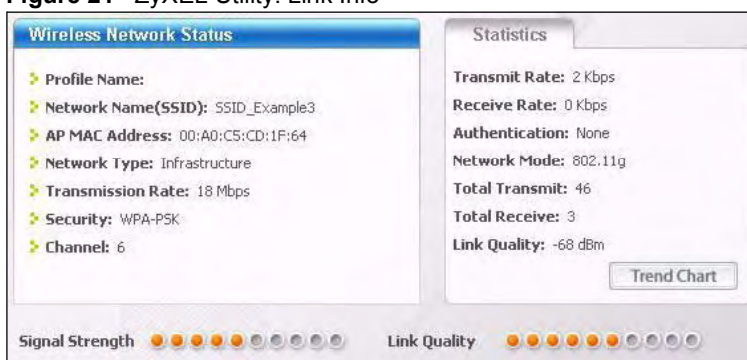
Use the **Next** button to move on to the next screen. You can use the **Back** button at any time to return to the previous screen, or the **Exit** button to return to the **Site Survey** screen.

Figure 19 ZyXEL Utility: Security Settings

4 The **Confirm Save** window appears. Check your settings and click **Save** to continue.

Figure 20 ZyXEL Utility: Confirm Save

5 The ZyXEL utility returns to the **Link Info** screen while it connects to the wireless network using your settings. When the wireless link is established, the ZyXEL utility icon in the system tray turns green and the **Link Info** screen displays details of the active connection. Check the network information in the **Link Info** screen to verify that you have successfully connected to the selected network. If the wireless client is not connected to a network, the fields in this screen remain blank.

Figure 21 ZyXEL Utility: Link Info

6 Open your Internet browser and enter <http://www.zyxel.com> or the URL of any other web site in the address bar. If you are able to access the web site, your wireless connection is successfully configured.

If you cannot access the web site, try changing the encryption type in the **Security Settings** screen, check the Troubleshooting section of this User's Guide or contact your network administrator.

3.4 Make a Telephone Call Over the Internet

To make a call over the Internet using the ZyXEL Device, first do the following things:

- Set up hardware connections from the ZyXEL Device to your computer, your telephone and the power supply (see the Quick Start Guide for more details on hardware connections).
- Set up your Internet access and WiMAX settings on the ZyXEL Device (see [Section 3.1.1 on page 49](#) and [Section 3.1.2 on page 52](#) for examples).
- Set up an account with a Voice over IP (VoIP) provider. This account (called a SIP account) allows you to make calls over the Internet. See [Chapter 12 on page 149](#) for more information on SIP accounts.

Use the sections below to set up your SIP account and speed dialing, and place a VoIP call.

3.4.1 Configure Your SIP Account

Your ZyXEL Device needs to be configured with the details of your SIP account before you can use it to make calls over the Internet. In this example, your SIP identity is “id123@abcvoip.com”, your user name is “id123” and your password is “zyx987”. Your VoIP provider has told you that the SIP server address is “sipserver-abcvoip.com”. See [Section 12.1.3 on page 149](#) for more information on SIP identities.

Once you have connected the ZyXEL Device to your computer and accessed the Web Configurator (see the Quick Start Guide for details) follow the steps below to configure your SIP settings.

- 1 In the Web Configurator, click **VoIP > SIP** in the navigation panel.
The following screen displays. This screen is where you enter your SIP account details.

Figure 22 Tutorial: SIP Account Setup

- 2 Select **SIP1** from the **SIP Account** list and make sure that the **Active SIP Account** box is selected.
- 3 Enter your SIP user name ('id123') in the **Number** field.
- 4 Enter your VoIP provider's SIP server name ('sipserver-abcvoip.com') in the **SIP Server Address** field. As your VoIP provider did not give you a different **REGISTER Server Address**, enter 'sipserver-abcvoip.com' again.
Enter your VoIP provider's domain name ('abcvoip.com') in the **SIP Service Domain** field.
- 5 In the Authentication area, enter 'id123' in the **User Name** field, and 'zyx987' in the **Password** field. Leave the **SIP Local Port**, **SIP Server Port** and **REGISTER Server Port** fields at their default values, as your VoIP provider did not supply port details.
Click **Apply**.
- 6 Click on the **Status** button in the navigation panel to check that your SIP account is correctly registered.
Look in the **VoIP Status** area towards the bottom of the **Status** screen. If the **SIP 1** account displays **Registered** in the **Registration** field, it is ready to use.
If the **Registration** field for the **SIP 1** account displays **Register Fail** or **Inactive**, click the **Register** button, check your settings in the **VoIP > SIP** screen or contact your VoIP provider to confirm that you have the correct settings and that your account is active.

3.4.2 Configure a Phone

Once you have set up your SIP account, click **VoIP > Phone > Analog Phone** in the navigation panel. The following screen displays.

Figure 23 Tutorial: the Analog Phone Screen

Phone Port Settings: Phone1

Outgoing Call Use

SIP1
 SIP2

Incoming Call apply to

SIP1
 SIP2

Apply Reset Advanced Setup

Use this screen to make sure that the phone connected to your ZyXEL Device uses the correct SIP account.

- 1 Select **Phone1** from the drop-down list box.
- 2 In the **Outgoing Call Use** area, select **SIP1**.
- 3 In the **Incoming Call apply to** area, select both **SIP1** and **SIP2**.
- 4 Click **Apply**. Your analog phone settings are saved.

3.4.3 Set Up Speed Dialing and Make a Call

In this example you want to set up speed dialling to make calls to a friend, Bob, whose SIP account number is 2345@xyzvoip.com. Your voIP provider, abcvoip.com, has told you that to call an xyzvoip.com number you must add '555' at its start.



Different VoIP providers implement calls to other networks in different ways. Check with your provider for details.

To configure speed dialling on the ZyXEL Device, click **VoIP > Phone Book > Speed Dial**. The following screen displays.

Figure 24 Tutorial: the Speed Dial Screen

Use the following steps to set up a speed dial entry.

- 1 You can have up to ten speed dial rules. Select the rule number (**1**, in this example) from the **Speed Dial** drop-down list box.
- 2 In the **Number** field, enter “5552345” and in the **Name** field enter “Bob”. Under **Type**, select **Use Proxy** and click **Add**.

The new speed dial rule is displayed in the **Speed Dial Phone book List**.

Figure 25 Tutorial: New Speed Dial Rule

Speed Dial	Number	Name:	Destination	Modify
#01	5552345	Bob		
#02				
#03				
#04				
#05				

Use the following steps to call a number from the speed dial list.

- 1 Ensure that your phone is correctly connected to the ZyXEL Device. See the Quick Start Guide for details of hardware connections.
- 2 Lift the phone’s receiver and type the speed dial number exactly as it appears in the **Speed Dial Phone Book** list. In this case, Bob’s phone number occupies rule #01, so dial “#01” on the phone’s keypad to make the call.

Internet Setup Wizard

This chapter provides information on the wizard setup screens for Internet access.

4.1 Wizard Setup Overview

The wizard will guide you through several steps. You will need to enter some information for identification purposes, then the wizard will guide you through configuring your Internet settings.

4.2 Internet Connection Wizard Setup


- 1 After you enter the password to access the web configurator, select **Go to Wizard setup**. Otherwise, click the wizard icon () in the top right corner of the web configurator to go to the wizards.

Figure 26 Select a Mode

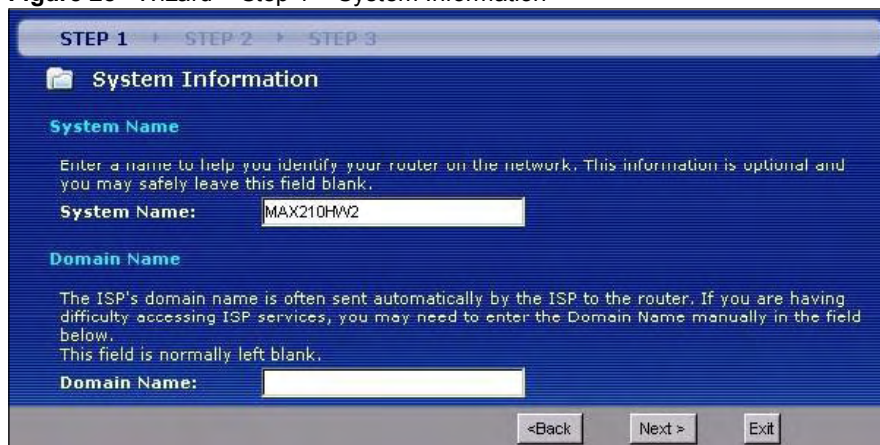


- 2 Click **CONNECTION WIZARD** to configure the system for Internet access.
- 3 The following screen displays. Click **Next** to continue. Click **Back** at any time to return to the previous screen, or **Exit** to leave the wizard setup.

Figure 27 Connection Wizard: Introduction

4.3 Step One: System Information

In the next screen you can give your ZyXEL Device a name (optional) in the **System Name** field. Enter up to thirty letters (this field is case-sensitive) or numbers. The ‘at’ symbol (@), dash (-), underscore (_) and period (.) are also permitted. Enter your ISP’s IP address in the **Domain Name** field if your ISP has instructed you to do so, or if you are having trouble accessing the Internet. Otherwise, leave this field blank. Click **Next**.

Figure 28 Wizard > Step 1 > System Information

The following table describes the labels in this screen.

Table 7 Wizard > Step 1 > System Information

LABEL	DESCRIPTION
System Name	System Name is a unique name to identify the ZyXEL Device 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.

4.4 Step Two: Wireless LAN Wizard

Set up your wireless LAN using the following screens.

4.4.1 Wireless LAN Screen

Figure 29 Wizard > Step 2 > Wireless LAN

The following table describes the labels in this screen.

Table 8 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 ZyXEL Device, make sure all wireless stations use the same SSID in order to access the network.
Security	Select a Security level from the drop-down list box. Choose Auto to have the ZyXEL Device generate a pre-shared key automatically. If you choose this option go directly to Section 4.4.4 on page 65 . Choose None to have no wireless LAN security configured. If you do not enable any wireless security on your ZyXEL Device, your network is accessible to any wireless networking device that is within range. If you choose this option, skip directly to Section 4.4.4 on page 65 . Choose Basic (WEP) security if you want to configure WEP Encryption parameters. If you choose this option, go directly to Section 4.4.2 on page 64 . Choose Extend (WPA-PSK or WPA2-PSK) 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 4.4.3 on page 65 .
Channel Selection	The range of radio frequencies used by IEEE 802.11b/g wireless devices is called a channel. Click the Scan button to have the ZyXEL Device automatically select a channel.
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.



The ZyXEL Device and other wireless devices must use the same SSID, channel ID and WEP encryption key (if WEP is enabled), WPA-PSK (if WPA-PSK is enabled) or WPA2-PSK (if WPA2-PSK is enabled) for wireless communication.

4.4.2 Basic (WEP) Security

Choose **Basic (WEP)** to set up WEP Encryption parameters.

Figure 30 Wizard > Step 2 > Basic (WEP) Security

STEP 1 | **STEP 2** | STEP 3

WIRELESS LAN

Passphrase
Use Passphrase to automatically generates a WEP key.
Passphrase

WEP Key
The higher the WEP Encryption, the higher the security but the slower the throughput.
Select 64-bit WEP, 128-bit WEP or 256-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: 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).
256-bit WEP: Enter 29 ASCII characters or 58 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

The following table describes the labels in this screen.

Table 9 Wizard > Step 2 > Basic (WEP) Security

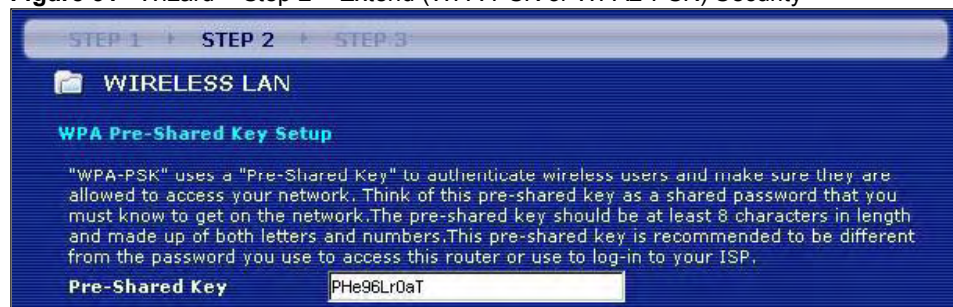
LABEL	DESCRIPTION
Passphrase	Type a Passphrase (up to 32 printable characters) and click Generate . The ZyXEL Device automatically generates a WEP key.
WEP Encryption	Select 64-bit WEP or 128-bit WEP to allow data encryption.
ASCII	Select this option in order to enter ASCII characters as the WEP keys. ASCII characters include the characters available on a standard English language keyboard.
HEX	Select this option to enter hexadecimal characters as the WEP keys. The preceding "0x" is entered automatically.

Table 9 Wizard > Step 2 > Basic (WEP) Security

LABEL	DESCRIPTION
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the ZyXEL Device 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. Proceed to Section 4.4.4 on page 65 .
Exit	Click Exit to close the wizard screen without saving.

4.4.3 Extend (WPA-PSK or WPA2-PSK) Security

Choose **Extend (WPA-PSK)** or **Extend (WPA2-PSK)** security in the Wireless LAN setup screen to set up a **Pre-Shared Key**.

Figure 31 Wizard > Step 2 > Extend (WPA-PSK or WPA2-PSK) Security

The following table describes the labels in this screen.

Table 10 Wizard > Step 2 > Extend (WPA-PSK or WPA2-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. Proceed to
Exit	Click Exit to close the wizard screen without saving.

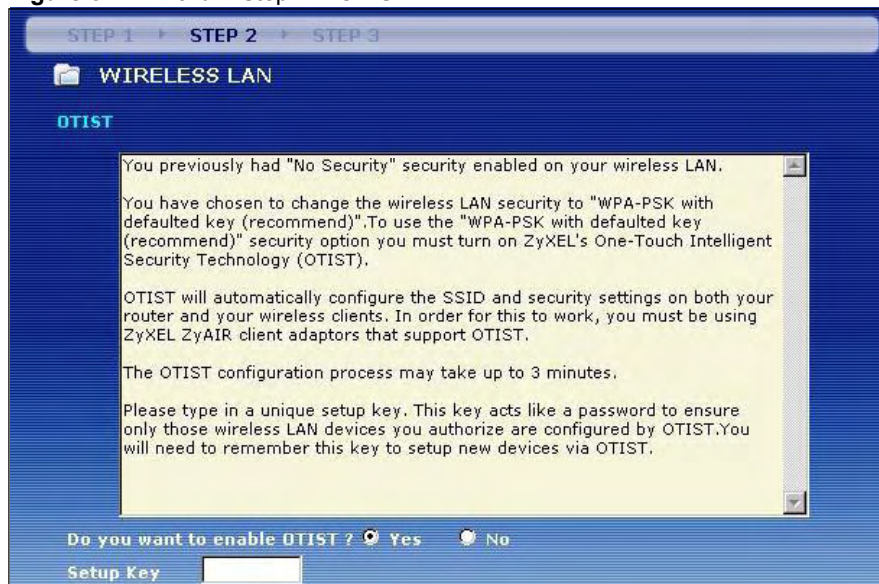
4.4.4 The OTIST Screen

After configuring your security settings or choosing **Auto** or **None** the OTIST screen will display.

You must enable OTIST if you have selected **Auto**. For the other security types you may click **No** if you do not plan to use OTIST. OTIST is only compatible with certain wireless devices, please check your other device's documentation to see if it supports OTIST. For more information on OTIST see [Section 7.4 on page 101](#).

Note: The text in the screen below may be different depending on your chosen security settings.

Figure 32 Wizard > Step 2 > OTIST



The following table describes the labels in this screen.

Table 11 Wizard > Step 2 > OTIST

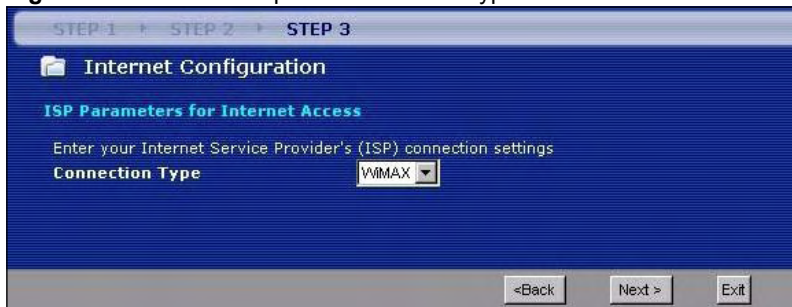
LABEL	DESCRIPTION
Enable OTIST	Select Yes to enable OTIST. Select No to not use OTIST.
Setup Key	If you select Yes then type an OTIST Setup Key of exactly eight ASCII characters in length.
Back	Click Back to display the previous screen.
Next	Click Next to proceed to the next screen. Proceed to Section 4.5 on page 66
Exit	Click Exit to close the wizard screen without saving.

4.5 Step Three: Internet Configuration

Set up your Internet access using the following screens.

4.5.1 Connection Type Screen

Leave the **Connection Type** at the default setting **WIMAX** and click **Next**.

Figure 33 Wizard > Step 3 > Connection Type Screen

4.5.2 ISP Parameters for Internet Access Screen

Enter your Internet account information (username and password) exactly as provided by your ISP. Leave the fields for which you were not given information at their default settings. Click **Next** to continue.

Figure 34 Wizard > Step 3 > ISP Parameters for Internet Access Screen

The following table describes the labels in this screen.

Table 12 Wizard > Step 3 > ISP Parameters for Internet Access Screen

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
User	Use this field to enter the username associated with your Internet access account. You can enter up to 61 printable ASCII characters.
Password	Use this field to enter the password associated with your Internet access account. You can enter up to 47 printable ASCII characters.

Table 12 Wizard > Step 3 > ISP Parameters for Internet Access Screen

LABEL	DESCRIPTION
Anonymous Identity	Enter the anonymous identity provided by your Internet Service Provider. Anonymous identity (also known as outer identity) is used with EAP-TTLS encryption. The anonymous identity is used to route your authentication request to the correct authentication server, and does not reveal your real user name. Your real user name and password are encrypted in the TLS tunnel, and only the anonymous identity can be seen. Leave this field blank if your ISP did not give you an anonymous identity to use.
PKM	This field displays the Privacy Key Management version number. PKM provides security between the ZyXEL Device and the base station. At the time of writing, the ZyXEL Device supports PKMv2 only. See the WiMAX security appendix for more information.
Authentication	This field displays the user authentication method. Authentication is the process of confirming the identity of a mobile station (by means of a username and password, for example). Check with your service provider if you are unsure of the correct setting for your account. Choose from the following user authentication methods: <ul style="list-style-type: none"> • TTLS (Tunnelled Transport Layer Security) • TLS (Transport Layer Security) <p>Note: Not all ZyXEL Devices support TLS authentication. Check with your service provider for details.</p>
TTLS Inner EAP	This field displays the type of secondary authentication method. Once a secure EAP-TTLS connection is established, the inner EAP is the protocol used to exchange security information between the mobile station, the base station and the AAA server to authenticate the mobile station. See the WiMAX security appendix for more details. The ZyXEL Device supports the following inner authentication types: <ul style="list-style-type: none"> • CHAP (Challenge Handshake Authentication Protocol) • MSCHAP (Microsoft CHAP) • MSCHAPV2 (Microsoft CHAP version 2) • PAP (Password Authentication Protocol)
Auth Mode	Select the authentication mode from the drop-down list box. This field is not available in all ZyXEL Devices. Check with your service provider for details. The ZyXEL Device supports the following authentication modes: <ul style="list-style-type: none"> • User Only • Device Only with Cert • Certs and User Authentication
Certificate	This is the security certificate the ZyXEL Device uses to authenticate the AAA server. Use the Security > Certificates > Trusted CA screen to import certificates to the ZyXEL Device.
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.

4.5.3 Antenna Selection Screen

If you have the MAX-210HW2 you can choose to use the internal antenna or external antenna for WiMAX. The internal antenna is fixed, and the external antenna is removable.

In the screen that appears, you can select which antenna to use. Select **Automatic Selection** to have the ZyXEL Device use whichever antenna has the best reception (recommended). Alternatively, if you do not want to use the external antenna, select **Use Internal Antenna**, and if you do not want to use the internal antenna, select **Use External Antenna**. Click **Next**.



The MAX-200HW2 and MAX-230HW2 do not have an internal antenna.

Figure 35 Wizard > Step 3 > Antenna Selection



The following table describes the labels in this screen.

Table 13 Wizard > Step 3 > Antenna Selection

LABEL	DESCRIPTION
Automatic Selection	Select Automatic Selection to have the ZyXEL Device choose which antenna to use. This setting is recommend as it will choose the antenna with the best signal to the base station.
Use Internal Antenna	Select Use Internal Antenna to have the ZyXEL Device use it's internal antenna. This option is not applicable for the MAX-200HW2 and MAX-230HW2.
Use External Antenna	Select Use External Antenna to have the ZyXEL Device use it's external antenna.
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.

4.5.4 IP Address Screen

A fixed IP address is a static IP that your ISP gives you. An automatic (dynamic) IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet.

In the following screen, select **Use fixed IP address provided by your ISP** if your ISP gave you an IP address to use. Otherwise, select **Get automatically from your ISP**.

Figure 36 Wizard > Step 3 > IP Address

The following table describes the labels in this screen.

Table 14 Wizard > Step 3 > IP Address

LABEL	DESCRIPTION
Your IP Address	
Get automatically from ISP (Default)	Select this if you have a dynamic IP address. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet.
Use Fixed IP Address provided by your ISP	A static IP address is a fixed IP that your ISP gives you.
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.

4.5.5 WAN IP Address Assignment

If you selected **Get automatically from your ISP** in the previous screen, skip this step. If you selected **Use fixed IP address provided by your ISP**, the following screen appears.

Enter your IP address, subnet mask, gateway address and DNS details exactly as they were given to you by your ISP.

Figure 37 Wizard > Step 3 > WAN IP Address Assignment

The screenshot shows a wizard window with a blue background. At the top, it says 'STEP 1', 'STEP 2', and 'STEP 3'. Below that is a folder icon and the text 'Internet Configuration'. Underneath is the title 'WAN IP Address Assignment' in blue. There are three rows of labels and input fields: 'My WAN IP Address', 'My WAN IP Subnet Mask', and 'Gateway IP Address'. Each input field contains '0.0.0.0'. Below this is another section titled 'DNS Server Address Assignment' in blue. It has three rows of labels and input fields: 'First DNS Server', 'Second DNS Server', and 'Third DNS Server'. Each input field contains '0.0.0.0'. At the bottom of the window, there are three buttons: '<Back', 'Next >', and 'Exit'.

The following table describes the labels in this screen.

Table 15 Wizard > Step 3 > WAN IP Address Assignment

LABEL	DESCRIPTION
WAN IP Address Assignment	
My WAN IP Address	Type your ISP assigned IP address in this field.
My WAN IP Subnet Mask	Enter a subnet mask in dotted decimal notation. Refer to the appendices to calculate a subnet mask if you are implementing subnetting.
Gateway IP Address	Specify a gateway IP address (supplied by your ISP).
DNS Server Address Assignment	
First, Second and Third DNS Server	Enter the DNS server's IP address in the field(s). Leave the IP address set to 0.0.0.0 to ignore the field.
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.

4.5.6 Wizard Complete

Click **Finish** to complete and save the Connection Wizard settings.

Figure 38 The Connection Wizard: Congratulations



Launch your web browser and navigate to www.zyxel.com. Internet access is just the beginning. Refer to the rest of this guide for more detailed information on the complete range of ZyXEL Device features. If you cannot access the Internet, open the web configurator again to confirm that the Internet settings you configured in the wizard setup are correct.

VoIP Wizard

This chapter shows you how to use the wizard to set up your SIP account(s).

5.1 Introduction

The ZyXEL Device has Voice over IP (VoIP) communication capabilities that allow you to use a traditional analog telephone to make Internet calls. You can configure the ZyXEL Device to use up to two SIP based VoIP accounts.

5.2 VOIP Wizard Setup


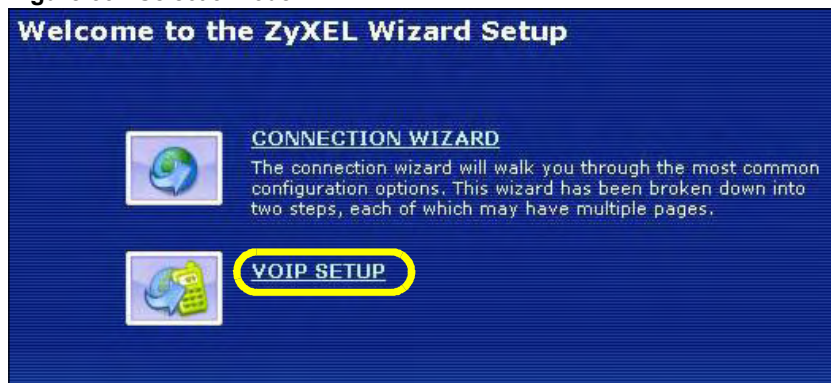
- 1 After you enter the password to access the web configurator, select **Go to Wizard setup**. Otherwise, click the wizard icon () in the top right corner of the web configurator to display the wizard main screen. Click **VOIP SETUP** to configure the system for Voice Over Internet connection.

Figure 39 Select a Mode



- 2 The following screen displays. This wizard screen allows you to configure your voice settings for SIP account 1. Fill in the fields with information from your VoIP service provider. Leave the default settings in fields for which no information was provided (except if otherwise specified). See [Chapter 12 on page 149](#) for background information on these fields.

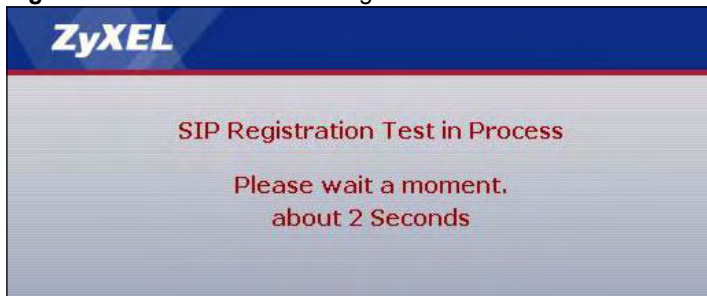
Figure 40 VoIP Wizard: Configuration

The following table describes the labels in this screen

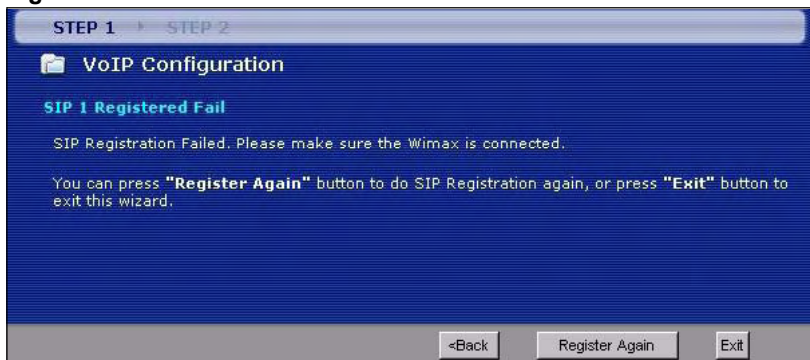
Table 16 VoIP Wizard Configuration

LABEL	DESCRIPTION
SIP Number	Enter your SIP number in this field (use the number or text that comes before the @ symbol in a SIP account like 1234@VoIP-provider.com). You can use up to 127 ASCII characters.
SIP Server Address	Type the IP address or domain name of the SIP server in this field. It doesn't matter whether the SIP server is a proxy, redirect or register server. You can use up to 95 ASCII characters.
SIP Service Domain	Enter the SIP service domain name in this field (the domain name that comes after the @ symbol in a SIP account like 1234@VoIP-provider.com). You can use up to 127 ASCII Extended set characters.
User Name	This is the user name for registering this SIP account with the SIP register server. Type the user name exactly as it was given to you. You can use up to 95 ASCII characters.
Password	Type the password associated with the user name above. You can use up to 95 ASCII Extended set characters.
Check here to set up SIP2 settings.	This screen configures SIP account 1. Select the check box if you have a second SIP account that you want to use. You will need to configure the same fields for the second SIP account.
Back	Click Back to return to the previous screen.
Apply	Click Apply to complete the wizard setup and save your configuration.
Exit	Click Exit to close the wizard without saving your settings.

- 3 The ZyXEL Device attempts to register your SIP account with the SIP server.

Figure 41 VoIP Wizard: SIP Registration Test

- 4 This screen displays if SIP account registration fails. Check your WiMAX connection using the **LINK** and **SIGNAL** LEDs on the front of the ZyXEL Device. Then wait a few seconds and click **Register Again**. If your Internet connection was already working, you can click **Back** and try re-entering your SIP account settings.

Figure 42 VoIP Wizard: Fail

- 5 This screen displays if your SIP account registration was successful. Click **Return to Wizard Main Page** if you want to use another configuration wizard. Click **Go to Advanced Setup page** or **Finish** to close the wizard and go to the main web configurator screens.

Figure 43 VOIP Wizard: Finish

PART III

Web Configurator

Status Screens (79)

Network

Wireless LAN (91)

WAN Setup (107)

LAN (119)

NAT (129)

VPN Transport (137)

VoIP

SIP (149)

Phone (165)

Phone Book (173)

Security

Firewall (179)

Certificates (187)

Content Filter (205)

Management

Static Route (209)

Remote MGMT (213)

UPnP (221)

Maintenance

System (233)

Logs (241)

Tools (255)

6

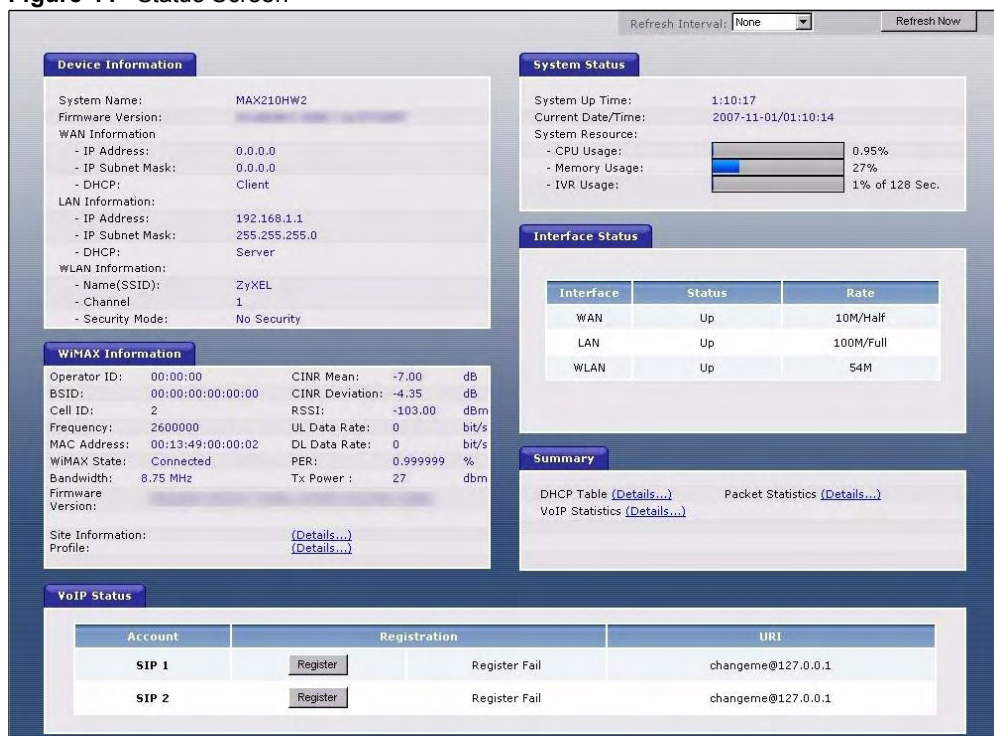
Status Screens

Use the **Status** screens to look at the current status of the device, system resources, interfaces (LAN, WAN and WLAN), and SIP accounts. You can also register and unregister SIP accounts. The **Status** screen also provides detailed information from DHCP and statistics from WiMAX, VoIP, bandwidth management, and traffic.

6.1 Status Screen

Click **Status** to open this screen.

Figure 44 Status Screen



Each field is described in the following table.

Table 17 Status Screen

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the ZyXEL Device to update this screen.
Refresh Now	Click this to update this screen immediately.
Device Information	
System Name	This field displays the ZyXEL Device system name. It is used for identification. You can change this in the Maintenance > System > General screen's System Name field.
Firmware Version	This field displays the current version of the firmware inside the device. It also shows the date the firmware version was created. You can change the firmware version by uploading new firmware in Maintenance > Tools > Firmware .
WAN Information	
IP Address	This field displays the current IP address of the ZyXEL Device in the WAN.
IP Subnet Mask	This field displays the current subnet mask on the WAN.
DHCP	This field displays what DHCP services the ZyXEL Device is using in the WAN. Choices are: Client - The ZyXEL Device is a DHCP client in the WAN. Its IP address comes from a DHCP server on the WAN. None - The ZyXEL Device is not using any DHCP services in the WAN. It has a static IP address. If you are not using Roadrunner on Ethernet, you can change this in Network > WAN . If you are using Roadrunner on Ethernet, this is controlled by Roadrunner.
LAN Information	
IP Address	This field displays the current IP address of the ZyXEL Device in the LAN.
IP Subnet Mask	This field displays the current subnet mask in the LAN.
DHCP	This field displays what DHCP services the ZyXEL Device is providing to the LAN. Choices are: Server - The ZyXEL Device is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN. Relay - The ZyXEL Device is routing DHCP requests to one or more DHCP servers. The DHCP server(s) may be on another network. None - The ZyXEL Device is not providing any DHCP services to the LAN. You can change this in Network > LAN > DHCP Setup .
WLAN Information	
Name (SSID)	This is the descriptive name used to identify the ZyXEL Device in the wireless LAN.
Channel	This is the channel number used by the ZyXEL Device.
Security Mode	This is the WiFi security mode used by the ZyXEL Device.
WiMAX Information	
Operator ID	Every WiMAX service provider has a unique Operator ID number, which is broadcast by each base station it owns. You can only connect to the Internet through base stations belonging to your service provider's network.

Table 17 Status Screen

LABEL	DESCRIPTION
BSID	This field displays the identification number of the wireless base station to which the ZyXEL Device is connected. Every base station transmits a unique BSID, which identifies it across the network.
Cell ID	A base station's coverage area can be divided into multiple cells. This field shows the identification number of the cell in which the ZyXEL Device is connected.
Frequency	This field displays the radio frequency of the ZyXEL Device's wireless connection to a base station.
MAC address	This field displays the Media Access Control address of the ZyXEL Device. Every network device has a unique MAC address which identifies it across the network.
WiMAX State	This field displays the status of the ZyXEL Device's current connection. <ul style="list-style-type: none"> • NA: the ZyXEL Device is starting up. • Fail: The ZyXEL Device is unable to connect to a base station. • Initial Synchronization: the ZyXEL Device is attempting to locate a base station. • Initial DCD (Downlink Channel Descriptor): the ZyXEL Device has located a base station and is receiving information about a possible downlink connection. • Initial UCD (Uplink Channel Descriptor): the ZyXEL Device is receiving information from the base station about a possible uplink connection. • Initial Ranging and Calibration: the ZyXEL Device and the base station are transmitting and receiving information about the distance between them. Ranging allows the ZyXEL Device to use a lower transmission power level when communicating with a nearby base station, and a higher transmission power level when communicating with a distant base station. • Initial Negotiation: the ZyXEL Device and the base station are exchanging information about their capabilities. • Initial PKM (Privacy Key Management): the ZyXEL Device and the base station are exchanging security information. • Initial Registration: the ZyXEL Device is registering with a RADIUS server. • Running: the ZyXEL Device has successfully registered with the base station. Traffic can now flow between the ZyXEL Device and the base station. • Sleep: the ZyXEL Device is in power saving mode, but periodically checks whether a base station has traffic waiting. • Idle: the ZyXEL Device is in power saving mode, but can connect when a base station alerts it that there is traffic waiting. • Handover: the ZyXEL Device is moving from one coverage area to another, and is connecting to the new base station.
Bandwidth	This field shows the size of the bandwidth step the ZyXEL Device uses to connect to a base station in megahertz (MHz).
CINR mean	This field shows the average Carrier to Interference plus Noise Ratio of the current connection. This value is an indication of overall radio signal quality. A higher value indicates a higher signal quality, and a lower value indicates a lower signal quality.
CINR deviation	This field shows the amount of change in the CINR level. This value is an indication of radio signal stability. A lower number indicates a more stable signal, and a higher number indicates a less stable signal.
RSSI	This field shows the Received Signal Strength Indication. This value is a measurement of overall radio signal strength. A higher RSSI level indicates a stronger signal, and a lower RSSI level indicates a weaker signal. A strong signal does not necessarily indicate a good signal: a strong signal may have a low signal-to-noise ratio (SNR).
UL Data Rate	This field shows the number of data packets uploaded from the ZyXEL Device to the base station each second.
DL Data Rate	This field shows the number of data packets downloaded to the ZyXEL Device from the base station each second.

Table 17 Status Screen

LABEL	DESCRIPTION
PER	This field shows the Packet Error Rate. The PER is the percentage of data packets transmitted across the network but not successfully received.
Tx Power	This field shows the output transmission (Tx) level of the ZyXEL Device.
Firmware Version	This shows the WiMAX chipset firmware version.
Site Information	Click the Details... link to view details of the radio frequencies used by the ZyXEL Device to connect to a base station.
Profile	Click the Details... link to view details of the current wireless security settings.
System Status	
System Up Time	This field displays how long the ZyXEL Device has been running since it last started up. The ZyXEL Device starts up when you plug it in, when you restart it (Maintenance > Tools > Restart), or when you reset it (see Section 2.1.2 on page 41).
Current Date/Time	This field displays the current date and time in the ZyXEL Device. You can change this in Maintenance > System > Time Setting .
CPU Usage	This field displays what percentage of the ZyXEL Device's processing ability is currently being used. The higher the CPU usage, the more likely the ZyXEL Device is to slow down. You can reduce this by disabling some services, such as DHCP, NAT, or content filtering.
Memory Usage	This field displays what percentage of the ZyXEL Device's memory is currently used. The higher the memory usage, the more likely the ZyXEL Device is to slow down. Some memory is required just to start the ZyXEL Device and to run the web configurator. You can reduce the memory usage by disabling some services (see CPU Usage); by reducing the amount of memory allocated to NAT and firewall rules (you may have to reduce the number of NAT rules or firewall rules to do so); or by deleting rules in functions such as incoming call policies, speed dial entries, and static routes.
IVR Usage	This field displays what percentage of the ZyXEL Device's IVR memory is currently used. IVR (Interactive Voice Response) refers to the customizable ring tone and on-hold music you set. See Section 12.1.11 on page 155 for more information.
Interface Status	
Interface	This column displays each interface of the ZyXEL Device.
Status	This field indicates whether or not the ZyXEL Device is using the interface. For the WAN interface, this field displays Up when the ZyXEL Device is connected to a WiMAX network, and Down when the ZyXEL Device is not connected to a WiMAX network. For the LAN interface, this field displays Up when the ZyXEL Device is using the interface and Down when the ZyXEL Device is not using the interface. For the WLAN port, it displays Up when WLAN is enabled or Down when WLAN is disabled.
Rate	For the LAN ports this displays the port speed and duplex setting. For the WAN interface, it displays the downstream and upstream transmission rate or N/A if the ZyXEL Device is not connected to a base station. For the WLAN port, it displays the transmission rate when WLAN is enabled or N/A when WLAN is disabled.
Summary	
Packet Statistics	Click this link to view port status and packet specific statistics.

Table 17 Status Screen

LABEL	DESCRIPTION
DHCP Table	Click this link to see details of computers to which the ZyXEL Device has given an IP address.
VoIP Statistics	Click this link to view statistics about your VoIP usage.
VoIP Status	
Account	This column displays each SIP account in the ZyXEL Device.
Registration	<p>This field displays the current registration status of the SIP account. You have to register SIP accounts with a SIP server to use VoIP.</p> <p>If the SIP account is already registered with the SIP server, Click Unregister to delete the SIP account's registration in the SIP server. This does not cancel your SIP account, but it deletes the mapping between your SIP identity and your IP address or domain name.</p> <p>The second field displays Registered.</p> <p>If the SIP account is not registered with the SIP server, Click Register to have the ZyXEL Device attempt to register the SIP account with the SIP server.</p> <p>The second field displays the reason the account is not registered.</p> <p>Inactive - The SIP account is not active. You can activate it in VoIP > SIP > SIP Settings.</p> <p>Register Fail - The last time the ZyXEL Device tried to register the SIP account with the SIP server, the attempt failed. The ZyXEL Device automatically tries to register the SIP account when you turn on the ZyXEL Device or when you activate it.</p>
URI	This field displays the account number and service domain of the SIP account. You can change these in VoIP > SIP > SIP Settings .

6.2 Site Information

Click **Status > Site Information** to view this screen. This read-only screen shows information about the ZyXEL Device's connection with a WiMAX base station. To configure these settings, go to the **Network > WAN > WiMAX Frequency** screen.

Figure 45 The Site Information Screen

Site Information	
DL Frequency [0] :	<input type="text" value="2545000"/> kHz
DL Frequency [1] :	<input type="text" value="2546000"/> kHz
DL Frequency [2] :	<input type="text" value="2547000"/> kHz
DL Frequency [3] :	<input type="text" value="0"/> kHz
DL Frequency [4] :	<input type="text" value="0"/> kHz
DL Frequency [5] :	<input type="text" value="0"/> kHz
DL Frequency [6] :	<input type="text" value="0"/> kHz
DL Frequency [7] :	<input type="text" value="0"/> kHz
DL Frequency [8] :	<input type="text" value="0"/> kHz
DL Frequency [9] :	<input type="text" value="0"/> kHz

The following table describes the labels in this screen.

Table 18 The Site Information Screen

LABEL	DESCRIPTION
Site Information	
DL Frequency [0] ~ [9]	These fields show the downlink frequency settings in kilohertz (kHz). These settings determine how the ZyXEL Device searches for an available wireless connection. See Section 8.4 on page 111 for more information.

6.3 Profile

Click **Status > Profile** to view this screen. This read-only screen displays information about the security settings you are using. To configure these settings, go to the **Network > WAN > Internet Connection** screen.



Not all ZyXEL Device models have all the fields shown here.

Figure 46 The WiMAX Profile Screen

The screenshot shows the 'Profile' screen with the following fields and values:

User	wimax@zyxel.com.tw
Password	****
Anonymous Identity	anonymous@zyxel.com.tw
PKM	PKMV2
Authentication	TTLS
TTLS Inner EAP	CHAP
Auth Mode	6 - Certs and User Authentication
Certificate	

The following table describes the labels in this screen.

Table 19 The WiMAX Profile Screen

LABEL	DESCRIPTION
Profile	
User	This is the username for your Internet access account.
Password	This is the password for your Internet access account. The password displays as a row of asterisks.
Anonymous Identity	This is the anonymous identity provided by your Internet Service Provider. Anonymous identity (also known as outer identity) is used with EAP-TTLS encryption.
PKM	This field displays the Privacy Key Management version number. PKM provides security between the ZyXEL Device and the base station. See the WiMAX security appendix for more information.

Table 19 The WiMAX Profile Screen

LABEL	DESCRIPTION
Authentication	This field displays the user authentication method. Authentication is the process of confirming the identity of a user (by means of a username and password, for example). EAP-TTLS allows an MS/SS and a base station to establish a secure link (or 'tunnel') with an AAA (Authentication, Authorization and Accounting) server in order to exchange authentication information. See the WiMAX security appendix for more details.
TTLS Inner EAP	This field displays the type of secondary authentication method. Once a secure EAP-TTLS connection is established, the inner EAP is the protocol used to exchange security information between the mobile station, the base station and the AAA server to authenticate the mobile station. See the WiMAX security appendix for more details. The ZyXEL Device supports the following inner authentication types: <ul style="list-style-type: none"> • CHAP (Challenge Handshake Authentication Protocol) • MSCHAP (Microsoft CHAP) • MSCHAPV2 (Microsoft CHAP version 2) • PAP (Password Authentication Protocol)
Auth Mode	This is the authentication mode. The ZyXEL Device supports the following authentication modes: <ul style="list-style-type: none"> • User Only • Device Only with Cert • Certs and User Authentication
Certificate	This is the security certificate the ZyXEL Device uses to authenticate the AAA server.

6.4 Packet Statistics

To access this screen, open the **Status** screen (see [Section 6.1 on page 79](#)), and click **(Details...)** next to **Packet Statistics**. Read-only information here includes port status and packet specific statistics. Also provided are "system up time" and "poll interval(s)". The **Poll Interval(s)** field is configurable.

Figure 47 Packet Statistics

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	Down	14068	110	0	0	0	00:00:00
LAN	100M/Full	13344	14383	0	0	0	0:58:14
WLAN	54M	6133	0	0	0	0	46:27:04

System Up Time : 46:27:10

Poll Interval : 5 sec Set Interval Stop

The following table describes the fields in this screen.


Table 20 Packet Statistics

LABEL	DESCRIPTION
Packet Statistics	
Port	This column displays each interface of the ZyXEL Device.
Status	This field indicates whether or not the ZyXEL Device is using the interface. For the WAN interface, this field displays Up when the ZyXEL Device is connected to a WiMAX network, and Down when the ZyXEL Device is not connected to a WiMAX network. For the LAN interface, this field displays Up when the ZyXEL Device is using the interface and Down when the ZyXEL Device is not using the interface. For the WLAN port, it displays Up when WLAN is enabled or Down when WLAN is disabled.
TxPkts	This field displays the number of packets transmitted on this interface.
RxPkts	This field displays the number of packets received on this interface.
Collisions	This field displays the number of collisions on this port.
Tx B/s	This field displays the number of bytes transmitted in the last second.
Rx B/s	This field displays the number of bytes received in the last second.
Up Time	This field displays the elapsed time this interface has been connected.
System up Time	This is the elapsed time the system has been on.
Poll Interval(s)	Type the time interval for the browser to refresh system statistics.
Set Interval	Click this button to apply the new poll interval you entered in the Poll Interval field above.
Stop	Click this button to halt the refreshing of the system statistics.

6.5 DHCP Table Screen

This screen displays information about computers that received an IP address from the ZyXEL Device. To access this screen, open the **Status** screen (see [Section 6.1 on page 79](#)), and click **(Details...)** next to **DHCP Table**.

Figure 48 DHCP Table



DHCP Table			
#	IP Address	Host Name	MAC Address
1	192.168.1.33	TWPC12731	00:50:8d:48:59:1f

Refresh

Each field is described in the following table.

Table 21 DHCP Table

LABEL	DESCRIPTION
DHCP Table	
#	This field is a sequential value. It is not associated with a specific entry.
IP Address	This field displays the IP address the ZyXEL Device assigned to a computer in the network.
Host Name	This field displays the system name of the computer to which the ZyXEL Device assigned the IP address.
MAC Address	This field displays the MAC address of the computer to which the ZyXEL Device assigned the IP address.
Refresh	Click this to update this screen.

6.6 VoIP Statistics Window

This screen displays SIP registration information, status of calls and VoIP traffic statistics. To access this screen, open the **Status** screen (see [Section 6.1 on page 79](#)), and click **(Details...)** next to **VoIP Statistics**.

Figure 49 VoIP Statistics

The screenshot shows the VoIP Statistics window with two main sections: SIP Status and Call Statistics. At the bottom, there is a 'Poll Interval' control set to 5 seconds with 'Set Interval' and 'Stop' buttons.

SIP Status:							
Account	Registration	Last Registration	URI	Protocol	Message Waiting	Last Incoming Number	Last Outgoing Number
SIP1	Register Fail	N/A	changeme@127.0.0.1	UDP	No	N/A	N/A
SIP2	Inactive	N/A	changeme@127.0.0.1	UDP	No	N/A	N/A

Call Statistics:									
Phone	Hook	Status	Codec	Peer Number	Duration	TxPkts	RxPkts	Tx B/s	Rx B/s
Phone1	On	N/A	N/A	N/A	0:00:00	0	0	0	0

Each field is described in the following table.

Table 22 VoIP Statistics

LABEL	DESCRIPTION
SIP Status	
Account	This column displays each SIP account in the ZyXEL Device.

Table 22 VoIP Statistics

LABEL	DESCRIPTION
Registration	This field displays the current registration status of the SIP account. You can change this in the Status screen. Registered - The SIP account is registered with a SIP server. Register Fail - The last time the ZyXEL Device tried to register the SIP account with the SIP server, the attempt failed. The ZyXEL Device automatically tries to register the SIP account when you turn on the ZyXEL Device or when you activate it. Inactive - The SIP account is not active. You can activate it in VoIP > SIP > SIP Settings .
Last Registration	This field displays the last time you successfully registered the SIP account. It displays N/A if you never successfully registered this account.
URI	This field displays the account number and service domain of the SIP account. You can change these in VoIP > SIP > SIP Settings .
Protocol	This field displays the transport protocol the SIP account uses. SIP accounts always use UDP.
Message Waiting	This field indicates whether or not there are any messages waiting for the SIP account.
Last Incoming Number	This field displays the last number that called the SIP account. It displays N/A if no number has ever dialed the SIP account.
Last Outgoing Number	This field displays the last number the SIP account called. It displays N/A if the SIP account has never dialed a number.
Call Statistics	
Phone	This field displays the ZyXEL Device's phone port number.
Hook	This field indicates whether the phone is on the hook or off the hook. On - The phone is hanging up or already hung up. Off - The phone is dialing, calling, or connected.
Status	This field displays the current state of the phone call. N/A - There are no current VoIP calls, incoming calls or outgoing calls being made. DIAL - The callee's phone is ringing. RING - The phone is ringing for an incoming VoIP call. Process - There is a VoIP call in progress. DISC - The callee's line is busy, the callee hung up or your phone was left off the hook.
Codec	This field displays what voice codec is being used for a current VoIP call through a phone port.
Peer Number	This field displays the SIP number of the party that is currently engaged in a VoIP call through a phone port.
Duration	This field displays how long the current call has lasted.
Tx Pkts	This field displays the number of packets the ZyXEL Device has transmitted in the current call.
Rx Pkts	This field displays the number of packets the ZyXEL Device has received in the current call.
Tx B/s	This field displays how quickly the ZyXEL Device has transmitted packets in the current call. The rate is the average number of bytes transmitted per second.
Rx B/s	This field displays how quickly the ZyXEL Device has received packets in the current call. The rate is the average number of bytes transmitted per second.

Table 22 VoIP Statistics

LABEL	DESCRIPTION
Poll Interval(s)	Enter how often you want the ZyXEL Device to update this screen, and click Set Interval .
Set Interval	Click this to make the ZyXEL Device update the screen based on the amount of time you specified in Poll Interval .
Stop	Click this to make the ZyXEL Device stop updating the screen.

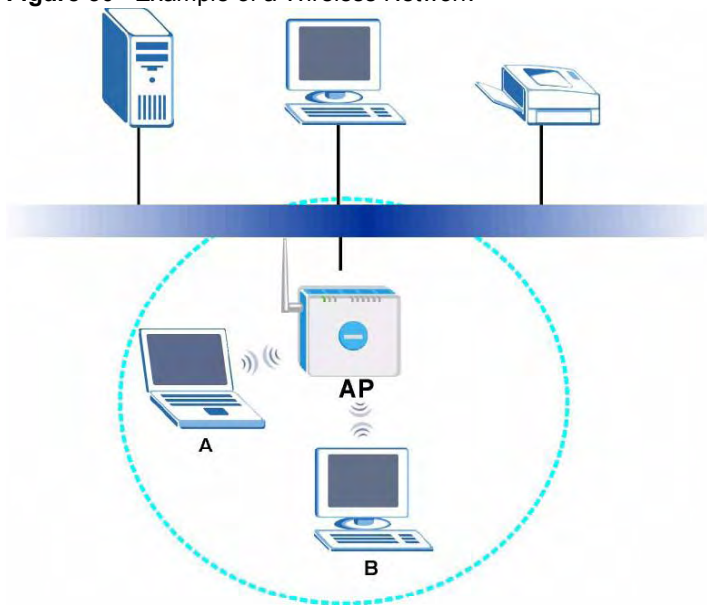
Wireless LAN

This chapter discusses how to configure the wireless network settings in your ZyXEL Device. See the appendices for more detailed information about wireless networks.

7.1 Wireless Network Overview

The following figure provides an example of a wireless network.

Figure 50 Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices A and B are called wireless clients. The wireless clients use the access point (AP) to interact with other devices (such as the printer) or with the Internet. Your ZyXEL Device is the AP.

Every wireless network must follow these basic guidelines.

- Every wireless client in the same wireless network must use the same SSID. The SSID is the name of the wireless network. It stands for Service Set Identity.
- If two wireless networks overlap, they should use different channels. Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.

- Every wireless client in the same wireless network must use security compatible with the AP.

Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

7.2 Wireless Security Overview

The following sections introduce different types of wireless security you can set up in the wireless network.

7.2.1 SSID

Normally, the AP acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the AP does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized devices to get the SSID. In addition, unauthorized devices can still see the information that is sent in the wireless network.

7.2.2 MAC Address Filter

Every wireless client has a unique identification number, called a MAC address.¹ A MAC address is usually written using twelve hexadecimal characters²; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each wireless client, see the appropriate User's Guide or other documentation.

You can use the MAC address filter to tell the AP which wireless clients are allowed or not allowed to use the wireless network. If a wireless client is allowed to use the wireless network, it still has to have the correct settings (SSID, channel, and security). If a wireless client is not allowed to use the wireless network, it does not matter if it has the correct settings.

This type of security does not protect the information that is sent in the wireless network. Furthermore, there are ways for unauthorized devices to get the MAC address of an authorized wireless client. Then, they can use that MAC address to use the wireless network.

7.2.3 User Authentication

You can make every user log in to the wireless network before they can use it. This is called user authentication. However, every wireless client in the wireless network has to support IEEE 802.1x to do this.

For wireless networks, there are two typical places to store the user names and passwords for each user.

- In the AP: this feature is called a local user database or a local database.
- In a RADIUS server: this is a server used in businesses more than in homes.

1. Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.

2. Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

If your AP does not provide a local user database and if you do not have a RADIUS server, you cannot set up user names and passwords for your users.

Unauthorized devices can still see the information that is sent in the wireless network, even if they cannot use the wireless network. Furthermore, there are ways for unauthorized wireless users to get a valid user name and password. Then, they can use that user name and password to use the wireless network.


Local user databases also have an additional limitation that is explained in the next section.

7.2.4 Encryption

Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message.

The types of encryption you can choose depend on the type of user authentication. (See [Section 7.2.3 on page 92](#) for information about this.)

Table 23 Types of Encryption for Each Type of Authentication

	NO AUTHENTICATION	RADIUS SERVER
Weakest  Strongest	No Security	WPA
	Static WEP	
	WPA-PSK	
	WPA2-PSK	WPA2

For example, if the wireless network has a RADIUS server, you can choose **WPA** or **WPA2**. If users do not log in to the wireless network, you can choose no encryption, **Static WEP**, **WPA-PSK**, or **WPA2-PSK**.

Usually, you should set up the strongest encryption that every wireless client in the wireless network supports. For example, suppose the AP does not have a local user database, and you do not have a RADIUS server. Therefore, there is no user authentication. Suppose the wireless network has two wireless clients. Device A only supports WEP, and device B supports WEP and WPA. Therefore, you should set up **Static WEP** in the wireless network.



It is recommended that wireless networks use **WPA-PSK**, **WPA**, or stronger encryption. IEEE 802.1x and WEP encryption are better than none at all, but it is still possible for unauthorized devices to figure out the original information pretty quickly.



It is not possible to use **WPA-PSK**, **WPA** or stronger encryption with a local user database. In this case, it is better to set up stronger encryption with no authentication than to set up weaker encryption with the local user database.

When you select **WPA2** or **WPA2-PSK** in your ZyXEL Device, you can also select an option (**WPA Compatible**) to support WPA as well. In this case, if some wireless clients support WPA and some support WPA2, you should set up **WPA2-PSK** or **WPA2** (depending on the type of wireless network login) and select the **WPA Compatible** option in the ZyXEL Device.

Many types of encryption use a key to protect the information in the wireless network. The longer the key, the stronger the encryption. Every wireless client in the wireless network must have the same key.

7.2.5 One-Touch Intelligent Security Technology (OTIST)

With ZyXEL's OTIST, you set up the SSID and WPA-PSK on the ZyXEL Device. Then, the ZyXEL Device transfers them to the devices in the wireless networks. As a result, you do not have to set up the SSID and encryption on every device in the wireless network.

The devices in the wireless network have to support OTIST, and they have to be in range of the ZyXEL Device when you activate it. See [Section 7.4 on page 101](#) for more details.

7.3 General Wireless LAN Screen



If you are configuring the ZyXEL Device from a computer connected to the wireless LAN and you change the ZyXEL Device's SSID, channel or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the ZyXEL Device's new settings.

Click **Network > Wireless LAN** to open the **General** screen.

Figure 51 Network > Wireless LAN > General

General		OTIST	MAC Filter	Advanced
Wireless Setup				
<input checked="" type="checkbox"/>	Enable Wireless LAN			
	Name(SSID)	ZyXEL		
<input type="checkbox"/>	Hide SSID			
	Channel Selection	Channel-01 2412MHz		
Security				
	Security Mode	No Security		
		Apply	Reset	

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

Table 24 Network > Wireless LAN > 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.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through 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. The options vary depending on whether you are using A or B/G frequency band and the country you are in. Refer to the Connection Wizard chapter for more information on channels.
Apply	Click Apply to save your changes back to the ZyXEL Device.
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.

7.3.1 No Security

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



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

Figure 52 Network > Wireless LAN > General: No Security

The screenshot shows the 'General' tab of the Wireless LAN configuration page. Under 'Wireless Setup', the 'Enable Wireless LAN' checkbox is checked. The 'Name(SSID)' field contains 'ZyXEL'. The 'Hide SSID' checkbox is unchecked. The 'Channel Selection' dropdown menu is set to 'Channel-01 2412MHz'. Under the 'Security' section, the 'Security Mode' dropdown menu is set to 'No Security'. At the bottom of the page, there are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

Table 25 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 ZyXEL Device.
Reset	Click Reset to reload the previous configuration for this screen.

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

In order to configure and enable WEP encryption, click **Network > Wireless LAN** to display the **General** screen. Select **Static WEP** from the **Security Mode** list.

Figure 53 Network > Wireless LAN > General: Static WEP

The screenshot shows the 'General' tab of the Wireless LAN configuration page. Under 'Wireless Setup', 'Enable Wireless LAN' is checked, SSID is 'ZyXEL', and Channel Selection is 'Channel-06 2437MHz'. Under 'Security', 'Security Mode' is set to 'Static WEP', 'WEP Encryption' is '64-bit WEP', and 'Authentication Method' is 'Auto'. A 'Generate' button is next to the Passphrase field. A note explains key requirements for 64-bit, 128-bit, and 256-bit WEP. Below the note are radio buttons for 'ASCII' (selected) and 'Hex', and four key input fields labeled 'Key 1' through 'Key 4'. 'Apply' and 'Reset' buttons are at the bottom.

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

Table 26 Network > Wireless LAN > General: Static WEP

LABEL	DESCRIPTION
Passphrase	Enter a passphrase (password phrase) of up to 32 printable characters and click Generate . The ZyXEL Device automatically generates four different WEP keys and displays them in the Key fields below.
WEP Encryption	Select 64-bit WEP or 128-bit WEP to enable data encryption.
Authentication Method	This field is activated when you select 64-bit WEP or 128-bit WEP in the WEP Encryption field. Select Auto , Open System or Shared Key from the drop-down list box.
ASCII	Select this option in order to enter ASCII characters as 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.
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the ZyXEL Device 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 ZyXEL Device.
Reset	Click Reset to reload the previous configuration for this screen.

7.3.3 WPA-PSK/WPA2-PSK

Click **Network > Wireless LAN** to display the **General** screen. Select **WPA-PSK** or **WPA2-PSK** from the **Security Mode** list.

Figure 54 Network > Wireless LAN > General: WPA-PSK/WPA2-PSK

The following table describes the labels in this screen.

Table 27 Network > Wireless LAN > General: WPA-PSK/WPA2-PSK

LABEL	DESCRIPTION
WPA Compatible	This check box is available only when you select WPA2-PSK or WPA2 in the Security Mode field. Select the check box to have both WPA2 and WPA wireless clients be able to communicate with the ZyXEL Device even when the ZyXEL Device is using WPA2-PSK or WPA2.
Pre-Shared Key	The encryption mechanisms used for WPA/WPA2 and WPA-PSK/WPA2-PSK are the same. The only difference between the two is that WPA-PSK/WPA2-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).
ReAuthentication Timer (in seconds)	Specify how often wireless stations have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes). Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The ZyXEL Device automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. The default time interval is 3600 seconds (or 1 hour).
Group Key Update Timer	The Group Key Update Timer is the rate at which the AP (if using WPA-PSK/WPA2-PSK key management) or RADIUS server (if using WPA/WPA2 key management) sends a new group key out to all clients. The re-keying process is the WPA/WPA2 equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the Group Key Update Timer is also supported in WPA-PSK/WPA2-PSK mode. The default is 1800 seconds (30 minutes).

Table 27 Network > Wireless LAN > General: WPA-PSK/WPA2-PSK

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

7.3.4 WPA/WPA2

Click **Network > Wireless LAN** to display the **General** screen. Select **WPA** or **WPA2** from the **Security Mode** list.

Figure 55 Network > Wireless LAN > General: WPA/WPA2

The screenshot shows the 'General' configuration page for Wireless LAN. It is divided into two main sections: 'Wireless Setup' and 'Security'.

Wireless Setup:

- Enable Wireless LAN
- Name(SSID): ZyXEL
- Hide SSID
- Channel Selection: Channel-06 2437MHz

Security:

- Security Mode: WPA2
- WPA Compatible
- ReAuthentication Timer: 1800 (In Seconds)
- Idle Timeout: 3600 (In Seconds)
- Group Key Update Timer: 1800 (In Seconds)
- Authentication Server:
 - IP Address: 0.0.0.0
 - Port Number: 1812
 - Shared Secret: [Empty]
- Accounting Server:
 - Active
 - IP Address: 0.0.0.0
 - Port Number: 1813
 - Shared Secret: [Empty]

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

The following table describes the labels in this screen.

Table 28 Network > Wireless LAN > General: WPA/WPA2

LABEL	DESCRIPTION
WPA Compatible	This check box is available only when you select WPA2-PSK or WPA2 in the Security Mode field. Select the check box to have both WPA2 and WPA wireless clients be able to communicate with the ZyXEL Device even when the ZyXEL Device is using WPA2-PSK or WPA2.
ReAuthentication Timer (in seconds)	Specify how often wireless stations have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes). Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The ZyXEL Device automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. The default time interval is 3600 seconds (or 1 hour).
Group Key Update Timer	The Group Key Update Timer is the rate at which the AP (if using WPA-PSK/WPA2-PSK key management) or RADIUS server (if using WPA/WPA2 key management) sends a new group key out to all clients. The re-keying process is the WPA/WPA2 equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the Group Key Update Timer is also supported in WPA-PSK/WPA2-PSK mode. The ZyXEL Device default is 1800 seconds (30 minutes).
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 ZyXEL Device. The key must be the same on the external authentication server and your ZyXEL Device. The key is not sent over the network.
Accounting Server	
Active	Select the checkbox to enable user accounting through an external authentication server.
IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Port Number	Enter the port number of the external accounting server. The default port number is 1813 . 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 accounting server and the ZyXEL Device. The key must be the same on the external accounting server and your ZyXEL Device. The key is not sent over the network.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Reset	Click Reset to reload the previous configuration for this screen.

7.4 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 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.



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

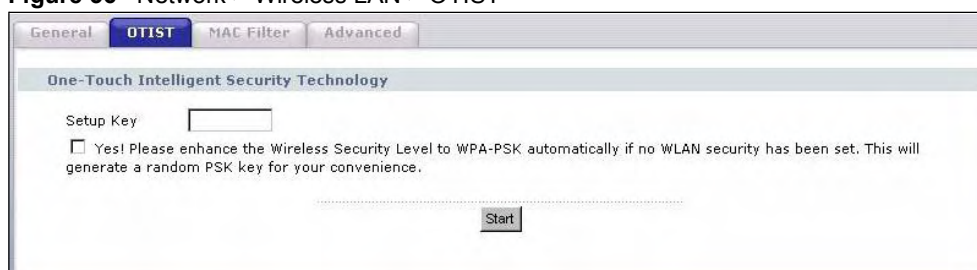
7.4.1 Enabling OTIST

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

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

Click the **Network > Wireless LAN > OTIST**. The following screen displays.

Figure 56 Network > Wireless LAN > OTIST



The following table describes the labels in this screen.

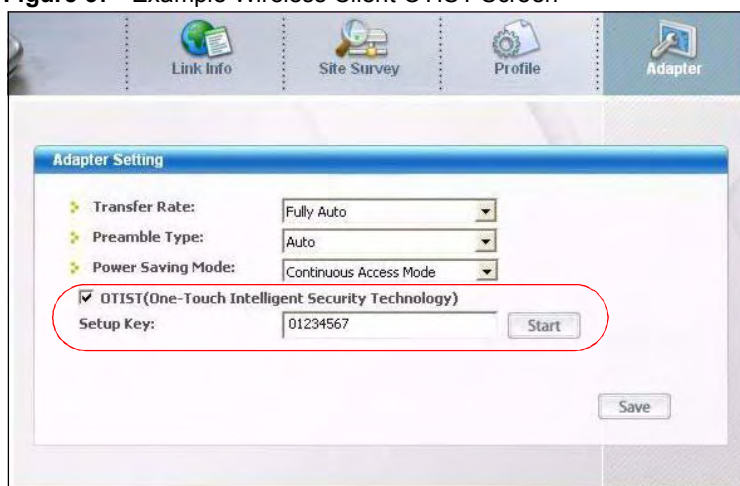
Table 29 Network > Wireless LAN > OTIST

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).
Yes!	If you want OTIST to automatically generate a WPA-PSK, you must: <ul style="list-style-type: none"> • Change your security to any security other than WPA-PSK in the Wireless LAN > General screen. • Select the Yes! checkbox in the OTIST screen and click Start. • The wireless 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. Note: If you already have a WPA-PSK configured in the Wireless LAN > General screen, and you run OTIST with Yes! selected, OTIST will use the existing WPA-PSK.
Start	Click Start to encrypt the wireless security data using the setup key and have the ZyXEL Device set the wireless client to use the same wireless settings as the ZyXEL Device. You must also activate and start OTIST on the wireless client all within three minutes.

7.4.1.1 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 57 Example Wireless Client OTIST Screen

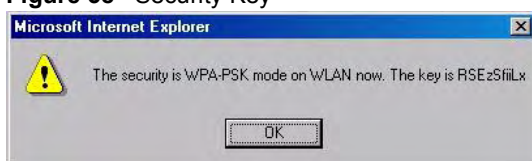


7.4.2 Starting OTIST

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. You can use the key in this screen to set up WPA-PSK encryption manually for non-OTIST devices in the wireless network. After reviewing the settings, click **OK**.

Figure 58 Security Key



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

Figure 59 OTIST in Progress (AP)

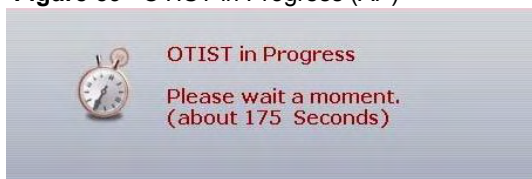
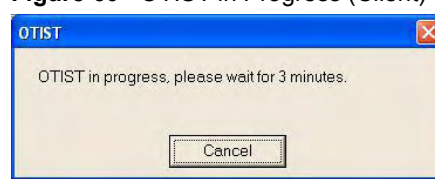


Figure 60 OTIST in Progress (Client)



- 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.

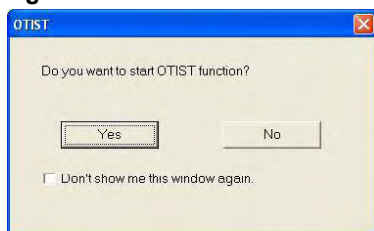
Figure 61 No AP with OTIST Found



- 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.

7.4.3 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 62 Start OTIST?

- 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 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.

7.5 MAC Filter

The MAC filter screen allows you to configure the ZyXEL Device to give exclusive access to up to 32 devices (Allow) or exclude up to 32 devices from accessing the ZyXEL Device (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 ZyXEL Device's MAC filter settings, click **Network > Wireless LAN > MAC Filter**. The screen appears as shown.

Figure 63 Network > Wireless LAN > MAC 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

Apply Reset

The following table describes the labels in this menu.

Table 30 Network > Wireless LAN > MAC 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 ZyXEL Device, MAC addresses not listed will be allowed to access the ZyXEL Device. Select Allow to permit access to the ZyXEL Device, MAC addresses not listed will be denied access to the ZyXEL Device.
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 ZyXEL Device 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 ZyXEL Device.
Reset	Click Reset to reload the previous configuration for this screen.

7.6 Wireless LAN Advanced Screen

Click **Network > Wireless LAN > Advanced**. The screen appears as shown.

Figure 64 Network > Wireless LAN > Advanced

The following table describes the labels in this screen.

Table 31 Network > Wireless LAN > Advanced

LABEL	DESCRIPTION
Wireless Advanced Setup	
RTS/CTS Threshold	Data with its frame size larger than this value will perform the RTS (Request To Send)/CTS (Clear To Send) handshake. If the RTS/CTS value is greater than the Fragmentation Threshold value, then the RTS/CTS handshake will never occur as data frames will be fragmented before they reach RTS/CTS size. 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.
802.11 Mode	Select 802.11b to allow only IEEE 802.11b compliant WLAN devices to associate with the ZyXEL Device. Select 802.11g to allow only IEEE 802.11g compliant WLAN devices to associate with the ZyXEL Device. Select 802.11b/g to allow either IEEE802.11b or IEEE802.11g compliant WLAN devices to associate with the ZyXEL Device. The transmission rate of your ZyXEL Device might be reduced.
Apply	Click Apply to save your changes back to the ZyXEL Device.
Reset	Click Reset to reload the previous configuration for this screen.

WAN Setup

This chapter describes how to configure WAN settings.

8.1 WAN Overview

A WAN (Wide Area Network) is an outside connection to another network or the Internet. Your ZyXEL Device uses the IEEE 802.16e WiMAX standard to connect wirelessly to a WiMAX base station (see [Section 1.1 on page 33](#)).

8.2 WiMAX

WiMAX (Worldwide Interoperability for Microwave Access) is the IEEE 802.16 wireless networking standard, which provides high-bandwidth, wide-range wireless service across wireless Metropolitan Area Networks (MANs). ZyXEL is a member of the WiMAX Forum, the industry group dedicated to promoting and certifying interoperability of wireless broadband products.

In a wireless MAN, a wireless-equipped computer is known either as a mobile station (MS) or a subscriber station (SS). Mobile stations use the IEEE 802.16e standard and are able to maintain connectivity while switching their connection from one base station to another base station (handover) while subscriber stations use other standards that do not have this capability (IEEE 802.16-2004, for example). The following figure shows an MS-equipped notebook computer **MS1** moving from base station **BS1**'s coverage area and connecting to **BS2**.

Figure 65 WiMax: Mobile Station



WiMAX technology uses radio signals (around 2 to 10 GHz) to connect subscriber stations and mobile stations to local base stations. Numerous subscriber stations and mobile stations connect to the network through a single base station (BS), as in the following figure.

Figure 66 WiMAX: Multiple Mobile Stations

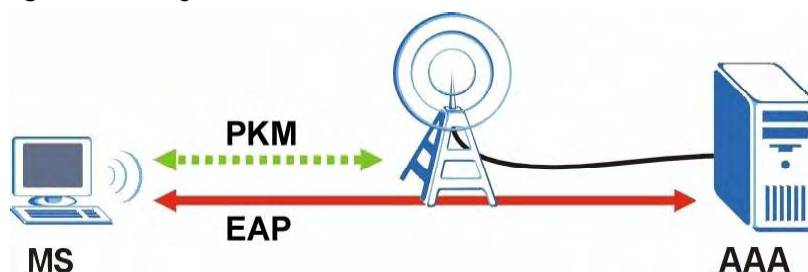
A base station's coverage area can extend over many hundreds of meters, even under poor conditions. A base station provides network access to subscriber stations and mobile stations, and communicates with other base stations.

The radio frequency and bandwidth of the link between the ZyXEL Device and the base station are controlled by the base station. The ZyXEL Device follows the base station's configuration.

8.2.1 Authentication

When authenticating a user, the base station uses a third-party RADIUS or Diameter server known as an AAA (Authentication, Authorization and Accounting) server to authenticate the mobile or subscriber stations.

The following figure shows a base station using an AAA server to authenticate mobile station MS, allowing it to access the Internet.

Figure 67 Using an AAA Server

In this figure, the dashed arrow shows the PKM (Privacy Key Management) secured connection between the mobile station and the base station, and the solid arrow shows the EAP secured connection between the mobile station, the base station and the AAA server. See the WiMAX security appendix for more details.

8.3 Internet Access Setup

To change your ZyXEL Device's Internet access settings, click **Network > WAN**. The **Internet Connection** screen displays.



Not all ZyXEL Device models have all the fields shown here.

Figure 68 Network > WAN > Internet Connection

ISP Parameters for Internet Access

User	<input style="width: 90%;" type="text"/>
Password	<input style="width: 90%;" type="password"/>
Anonymous Identity	<input style="width: 90%;" type="text"/>
PKM	<input style="width: 40%;" type="text" value="PKMV2"/>
Authentication	<input style="width: 40%;" type="text" value="TTLS"/>
TTLS Inner EAP	<input style="width: 40%;" type="text" value="CHAP"/>
Auth Mode	<input style="width: 40%;" type="text" value="6 - Certs and User Authentication"/>
Certificate	<input style="width: 40%;" type="text"/>

WAN IP Address Assignment

Get automatically from ISP (Default)

Use Fixed IP Address

IP Address	<input style="width: 60%;" type="text" value="0.0.0.0"/>
IP Subnet Mask	<input style="width: 60%;" type="text" value="0.0.0.0"/>
Gateway IP Address	<input style="width: 60%;" type="text" value="0.0.0.0"/>

The following table describes the labels in this screen.

Table 32 Network > WAN > Internet Connection

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
User	Use this field to enter the username associated with your Internet access account. You can enter up to 61 printable ASCII characters.
Password	Use this field to enter the password associated with your Internet access account. You can enter up to 47 printable ASCII characters.
Anonymous Identity	Enter the anonymous identity provided by your Internet Service Provider. Anonymous identity (also known as outer identity) is used with EAP-TTLS encryption. The anonymous identity is used to route your authentication request to the correct authentication server, and does not reveal your real user name. Your real user name and password are encrypted in the TLS tunnel, and only the anonymous identity can be seen. Leave this field blank if your ISP did not give you an anonymous identity to use.

Table 32 Network > WAN > Internet Connection

LABEL	DESCRIPTION
PKM	This field displays the Privacy Key Management version number. PKM provides security between the ZyXEL Device and the base station. At the time of writing, the ZyXEL Device supports PKMv2 only. See the WiMAX security appendix for more information.
Authentication	This field displays the user authentication method. Authentication is the process of confirming the identity of a mobile station (by means of a username and password, for example). Check with your service provider if you are unsure of the correct setting for your account. Choose from the following user authentication methods: <ul style="list-style-type: none"> • TTLS (Tunnelled Transport Layer Security) • TLS (Transport Layer Security) <p>Note: Not all ZyXEL Devices support TLS authentication. Check with your service provider for details.</p>
TTLS Inner EAP	This field displays the type of secondary authentication method. Once a secure EAP-TTLS connection is established, the inner EAP is the protocol used to exchange security information between the mobile station, the base station and the AAA server to authenticate the mobile station. See the WiMAX security appendix for more details. This field is available only when TTLS is selected in the Authentication field. The ZyXEL Device supports the following inner authentication types: <ul style="list-style-type: none"> • CHAP (Challenge Handshake Authentication Protocol) • MSCHAP (Microsoft CHAP) • MSCHAPV2 (Microsoft CHAP version 2) • PAP (Password Authentication Protocol)
Auth Mode	Select the authentication mode from the drop-down list box. This field is not available in all ZyXEL Devices. Check with your service provider for details. The ZyXEL Device supports the following authentication modes: <ul style="list-style-type: none"> • User Only • Device Only with Cert • Certs and User Authentication
Certificate	This is the security certificate the ZyXEL Device uses to authenticate the AAA server. Use the Security > Certificates > Trusted CA screen to import certificates to the ZyXEL Device.
WAN IP Address Assignment	
Get automatically from ISP (Default)	Select this if you have a dynamic IP address. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet.
Use Fixed IP Address	A static IP address is a fixed IP that your ISP gives you. Type your ISP assigned IP address in the IP Address field below.
IP Subnet Mask	Enter a subnet mask in dotted decimal notation. Refer to the appendices to calculate a subnet mask if you are implementing subnetting.
Gateway IP Address	Specify a gateway IP address (supplied by your ISP).
Apply	Click this button to save your settings.
Reset	Click this button to return all the fields in this screen to their default values.

8.4 Frequency Settings

In a WiMAX network, a mobile or subscriber station must use a radio frequency supported by the base station to communicate. When the ZyXEL Device looks for a connection to a base station, it can search a range of frequencies.

Radio frequency is measured in Hertz (Hz).

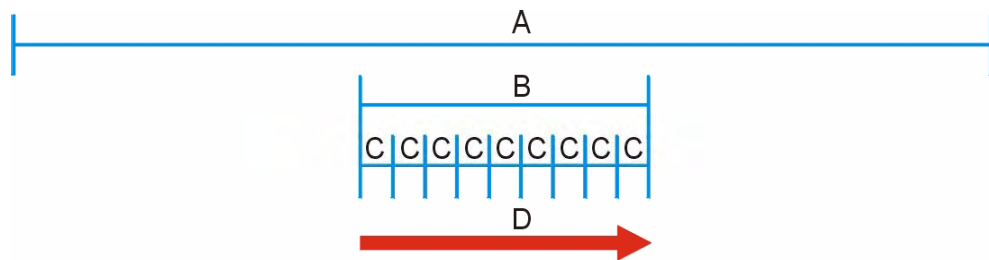
Table 33 Radio Frequency Conversion

1 kHz = 1000 Hz
1 MHz = 1000 kHz (1000000 Hz)
1 GHz = 1000 MHz (1000000 kHz)

8.4.1 Frequency Ranges

The following figure shows the ZyXEL Device searching a range of frequencies to find a connection to a base station.

Figure 69 Frequency Ranges



In this figure, **A** is the WiMAX frequency range. “WiMAX frequency range” refers to the entire range of frequencies the ZyXEL Device is capable of using to transmit and receive (see the Product Specifications appendix for details).

In the figure, **B** shows the operator frequency range. This is the range of frequencies within the WiMAX frequency range supported by your operator (service provider).

The operator range is subdivided into bandwidth steps. In the figure, each **C** is a bandwidth step.

The arrow **D** shows the ZyXEL Device searching for a connection.

Have the ZyXEL Device search only certain frequencies by configuring the downlink frequencies. Your operator can give you information on the supported frequencies.

The downlink frequencies are points of the frequency range your ZyXEL Device searches for an available connection. Use the **Site Survey** screen to set these bands. You can set the downlink frequencies anywhere within the WiMAX frequency range. In this example, the downlink frequencies have been set to search all of the operator range for a connection.

8.4.2 Configuring Frequency Settings

You need to set the ZyXEL Device to scan one or more specific radio frequencies to find an available connection to a WiMAX base station.

Use the **WiMAX Frequency** screen to define the radio frequencies to be searched for available wireless connections. See [Section 8.4.2.1 on page 113](#) for an example of using the **WiMAX Frequency** screen.



It may take several minutes for the ZyXEL Device to find a connection.

- The ZyXEL Device searches the **DL Frequency** settings in ascending numerical order, from [0] to [9].
- If you enter a 0 in a **DL Frequency** field, the ZyXEL Device immediately moves on to the next **DL Frequency** field.
- When the ZyXEL Device connects to a base station, the values in this screen are automatically set to the base station's frequency. The next time the ZyXEL Device searches for a connection, it searches only this frequency. If you want the ZyXEL Device to search other frequencies, enter them in the **DL Frequency** fields.

The following table describes some examples of **DL Frequency** settings.

Table 34 DL Frequency Example Settings

	EXAMPLE 1	EXAMPLE 2
DL Frequency [0]:	2500000	2500000
DL Frequency [1]:	2550000	2550000
DL Frequency [2]:	0	2600000
DL Frequency [3]:	0	0
DL Frequency [4]:	0	0
	The ZyXEL Device searches at 2500000 kHz, and then searches at 2550000 kHz if it has not found a connection.	<i>The ZyXEL Device searches at 2500000 kHz and then at 2550000 kHz if it has not found an available connection. If it still does not find an available connection, it searches at 2600000 kHz.</i>

Click **Network > WAN > WiMAX Frequency** to display the screen shown next.

Figure 70 Network > WAN > WiMAX Frequency

DL Frequency [0]	2545000	kHz
DL Frequency [1]	2546000	kHz
DL Frequency [2]	0	kHz
DL Frequency [3]	0	kHz
DL Frequency [4]	0	kHz
DL Frequency [5]	0	kHz
DL Frequency [6]	0	kHz
DL Frequency [7]	0	kHz
DL Frequency [8]	0	kHz
DL Frequency [9]	0	kHz

Apply Reset

The following table describes the labels in this screen.

Table 35 Network > WAN > WiMAX Frequency

LABEL	DESCRIPTION
DL Frequency [0] ~ [9]	These fields show the downlink frequency settings in kilohertz (kHz). Enter values in these fields to have the ZyXEL Device scan these frequencies for available channels in ascending numerical order. Contact your service provider for details of supported frequencies.
Apply	Click this button to save your settings.
Reset	Click this button to return all the fields in this screen to their default values.

8.4.2.1 Using the WiMAX Frequency Screen: Example

In this example, your Internet service provider has given you a list of supported frequencies, as follows.

Table 36 Example Supported Frequencies (GHz)

2.5
2.525
2.6
2.625

Use the **WiMAX Frequency** screen to enter the frequencies you want the ZyXEL Device to scan for a connection to a base station.

- 1** In the **DL Frequency [0]** field, enter **2500000** (2500000 kilohertz (kHz) is equal to 2.5 gigahertz).
 - 2** In the **DL Frequency [1]** field, enter **2525000**.
 - 3** In the **DL Frequency [2]** field, enter **2600000**.
 - 4** In the **DL Frequency [3]** field, enter **2625000**.
- Leave the rest of the **DL Frequency** fields at zero. The screen appears as follows.

Figure 71 Completing the WiMAX Frequency Screen

DL Frequency [0]	<input type="text" value="2500000"/>	kHz
DL Frequency [1]	<input type="text" value="2525000"/>	kHz
DL Frequency [2]	<input type="text" value="2600000"/>	kHz
DL Frequency [3]	<input type="text" value="2625000"/>	kHz
DL Frequency [4]	<input type="text" value="0"/>	kHz
DL Frequency [5]	<input type="text" value="0"/>	kHz
DL Frequency [6]	<input type="text" value="0"/>	kHz
DL Frequency [7]	<input type="text" value="0"/>	kHz
DL Frequency [8]	<input type="text" value="0"/>	kHz
DL Frequency [9]	<input type="text" value="0"/>	kHz

- 5 Click **Apply**. The ZyXEL Device stores your settings.

When the ZyXEL Device searches for available frequencies, it scans all frequencies from **DL Frequency [0]** to **DL Frequency [3]**. When it finds an available connection, the fields in this screen will be automatically set to use that frequency.

8.5 Configuring Advanced WAN Settings

Click **Network > WAN > Advanced** to display the following screen.

Figure 72 Network > WAN > Advanced

DNS Servers	
First DNS Server	<input type="text" value="From ISP"/> <input type="text" value="0.0.0.0"/>
Second DNS Server	<input type="text" value="From ISP"/> <input type="text" value="0.0.0.0"/>
Third DNS Server	<input type="text" value="From ISP"/> <input type="text" value="0.0.0.0"/>
RIP & Multicast Setup	
RIP Direction	<input type="text" value="None"/>
RIP Version	<input type="text" value="RIP-1"/>
Multicast	<input type="text" value="None"/>
Windows Networking (NetBIOS over TCP/IP)	
<input checked="" type="checkbox"/>	Allow between LAN and WAN (You also need to create a firewall rule!)
<input type="checkbox"/>	Allow Trigger Dial

The following table describes the labels in this screen.

Table 37 Network > WAN > Advanced

LABEL	DESCRIPTION
DNS Servers	
First, Second and Third DNS Server	<p>Select Obtained from ISP if your ISP dynamically assigns DNS server information (and the ZyXEL Device's WAN IP address). Use the drop-down list box to select a DNS server IP address that the ISP assigns in the field to the right.</p> <p>Select UserDefined if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose UserDefined, but leave the IP address set to 0.0.0.0, UserDefined changes to None after you click Apply. If you set a second choice to UserDefined, and enter the same IP address, the second UserDefined changes to None after you click Apply.</p> <p>Select None if you do not want to configure DNS servers. You must have another DHCP server on your LAN, or else the computers must have their DNS server addresses manually configured. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.</p>
RIP & Multicast Setup	
RIP Direction	Select the RIP direction from None , Both , In Only and Out Only .
RIP Version	Select the RIP version from RIP-1 , RIP-2B and RIP-2M .
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group. The ZyXEL Device supports both IGMP version 1 (IGMP-v1) and IGMP-v2 . Select None to disable it.
Windows Networking (NetBIOS over TCP/IP)	NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls. However it may sometimes be necessary to allow NetBIOS packets to pass through to the WAN in order to find a computer on the WAN.
Allow between LAN and WAN	<p>Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you also need to enable the default WAN to LAN firewall rule that forwards NetBIOS traffic.</p> <p>Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN.</p>
Allow Trigger Dial	Select this option to allow NetBIOS packets to initiate calls.
Apply	Click this button to save your settings.
Reset	Click this button to return all the fields in this screen to their default values.

8.6 Configuring Traffic Redirect Settings

To change your ZyXEL Device's traffic redirect settings, click **Network > WAN > Traffic Redirect**. The screen appears as shown.

Figure 73 Network > WAN > Traffic Redirect

The following table describes the labels in this screen.

Table 38 Network > WAN > Traffic Redirect

LABEL	DESCRIPTION
Traffic Redirect	
Active	Select this check box to have the ZyXEL Device use traffic redirect if the normal WAN connection goes down. Note: If you activate traffic redirect, you must configure the Check WAN IP Address field.
Backup Gateway IP Address	Type the IP address of your backup gateway in dotted decimal notation. The ZyXEL Device automatically forwards traffic to this IP address if the ZyXEL Device's Internet connection terminates.
Check WAN IP Address	Configure this field to test your ZyXEL Device's WAN accessibility. Type the IP address of a reliable nearby computer (for example, your ISP's DNS server address). Note: If you activate either traffic redirect or dial backup, you must configure an IP address here. When using a WAN backup connection, the ZyXEL Device periodically pings the addresses configured here and uses the other WAN backup connection (if configured) if there is no response.
Fail Tolerance	Type the number of times (2 recommended) that your ZyXEL Device may ping the IP addresses configured in the Check WAN IP Address field without getting a response before switching to a WAN backup connection (or a different WAN backup connection).
Period (sec)	The ZyXEL Device tests a WAN connection by periodically sending a ping to either the default gateway or the address in the Check WAN IP Address field. Type a number of seconds (5 to 300) to set the time interval between checks. Allow more time if your destination IP address handles lots of traffic.
Timeout (sec)	Type the number of seconds (1 to 10) for your ZyXEL Device to wait for a response to the ping before considering the check to have failed. This setting must be less than the Period . Use a higher value in this field if your network is busy or congested.
Apply	Click this button to save your settings.
Reset	Click this button to return all the fields in this screen to their default values.

8.6.1 Configuring The Antenna

In this screen you can select whether to use the internal or external antenna for WiMAX. Select **Automatic Selection** to have the ZyXEL Device use whichever antenna has the best signal reception (recommended). Alternatively, if you do not want to use the external antenna, select **Use Internal Antenna**, and if you do not want to use the internal antenna, select **Use External Antenna**.



The MAX-200HW2 and MAX-230HW2 does not have an internal antenna.

To choose which antenna to use, click **Network > WAN > Antenna Selection**. The screen appears as shown.

Figure 74 Network > WAN > Antenna Selection

The following table describes the labels in this screen.

Table 39 Network > WAN > Antenna Selection

LABEL	DESCRIPTION
Automatic Selection	Select Automatic Selection to have the ZyXEL Device choose which antenna to use. This setting is recommend as it will choose the antenna with the stronger signal reception.
Use Internal Antenna	Select Use Internal Antenna to have the ZyXEL Device use it's internal antenna. This option is not applicable for the MAX-200HW2 and MAX-230HW2.
Use External Antenna	Select Use External Antenna to have the ZyXEL Device use it's external antenna.
Apply	Click this button to save your settings.
Reset	Click this button to return the fields in this screen to their default settings.

9

LAN

Use these screens to set up the ZyXEL Device on the LAN. You can configure its IP address and subnet mask, DHCP services, and other subnets. You can also control how the ZyXEL Device sends routing information using RIP.

9.1 LAN Overview

A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is usually a computer network limited to the immediate area, such as the same building or floor of a building.

9.1.1 IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, 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. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the ZyXEL Device. 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 ZyXEL Device, 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 ZyXEL Device 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 ZyXEL Device unless you are instructed to do otherwise.

9.1.2 DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the ZyXEL Device as a DHCP server or disable it. When configured as a server, the ZyXEL Device provides the TCP/IP configuration for the clients. If DHCP service is disabled, you must have another DHCP server on your LAN, or else each computer must be manually configured.

The ZyXEL Device is pre-configured with a pool of IP addresses for the DHCP clients (DHCP Pool). See the product specifications in the appendices. Do not assign static IP addresses from the DHCP pool to your LAN computers.

These parameters should work for the majority of installations. If your ISP gives you explicit DNS server address(es), see [Section 9.2.2 on page 122](#).

9.1.3 LAN TCP/IP

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

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

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

These parameters should work for the majority of installations. If your ISP gives you explicit DNS server address(es), see [Section 9.2.2 on page 122](#).

9.1.4 DNS Server Address

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it. The DNS server addresses that you enter in the DHCP setup are passed to the client machines along with the assigned IP address and subnet mask.

There are two ways that an ISP disseminates the DNS server addresses. The first is for an ISP to tell a customer the DNS server addresses, usually in the form of an information sheet, when s/he signs up. If your ISP gives you the DNS server addresses, enter them in the **DNS Server** fields in **DHCP Setup**, otherwise, leave them blank.

Some ISPs choose to pass the DNS servers using the DNS server extensions of PPP IPCP (IP Control Protocol) after the connection is up. If your ISP did not give you explicit DNS servers, chances are the DNS servers are conveyed through IPCP negotiation. The ZyXEL Device supports the IPCP DNS server extensions through the DNS proxy feature.

If the **Primary** and **Secondary DNS Server** fields in the **LAN Setup** screen are not specified, for instance, left as 0.0.0.0, the ZyXEL Device tells the DHCP clients that it itself is the DNS server. When a computer sends a DNS query to the ZyXEL Device, the ZyXEL Device forwards the query to the real DNS server learned through IPCP and relays the response back to the computer.

Please note that DNS proxy works only when the ISP uses the IPCP DNS server extensions. It does not mean you can leave the DNS servers out of the DHCP setup under all circumstances. If your ISP gives you explicit DNS servers, make sure that you enter their IP addresses in the **LAN Setup** screen. This way, the ZyXEL Device can pass the DNS servers to the computers and the computers can query the DNS server directly without the ZyXEL Device's intervention.

9.1.5 RIP Setup

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

- **Both** - the ZyXEL Device will broadcast its routing table periodically and incorporate the RIP information that it receives.
- **In Only** - the ZyXEL Device will not send any RIP packets but will accept all RIP packets received.
- **Out Only** - the ZyXEL Device will send out RIP packets but will not accept any RIP packets received.
- **None** - the ZyXEL Device will not send any RIP packets and will ignore any RIP packets received.

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

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

9.1.6 Multicast

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

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

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

9.2 LAN Screens

9.2.1 LAN IP Screen

Use this screen to set up the ZyXEL Device's IP address and subnet mask. To access this screen, click **Network > LAN > IP**.

Figure 75 Network > LAN > IP

Each field is described in the following table.

Table 40 Network > LAN > IP

LABEL	DESCRIPTION
IP Address	Enter the IP address of the ZyXEL Device on the LAN. Note: This field is the IP address you use to access the ZyXEL Device on the LAN. If the web configurator is running on a computer on the LAN, you lose access to the web configurator as soon as you change this field and click Apply . You can access the web configurator again by typing the new IP address in the browser.
IP Subnet Mask	Enter the subnet mask of the LAN.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its default value.

9.2.2 LAN DHCP Setup Screen

Use this screen to enable, disable, and configure the DHCP server in the ZyXEL Device. To access this screen, click **Network > LAN > DHCP Setup**.

Figure 76 Network > LAN > DHCP Setup

Each field is described in the following table.

Table 41 Network > LAN > DHCP Setup

LABEL	DESCRIPTION
DHCP Setup	
Enable DHCP Server	Select this if you want the ZyXEL Device to be the DHCP server on the LAN. As a DHCP server, the ZyXEL Device assigns IP addresses to DHCP clients on the LAN and provides the subnet mask and DNS server information.
IP Pool Starting Address	Enter the IP address from which the ZyXEL Device begins allocating IP addresses, if you have not specified an IP address for this computer in Network > LAN > Static DHCP .
Pool Size	Enter the number of IP addresses to allocate. This number must be at least one and is limited by a subnet mask of 255.255.255.0 (regardless of the subnet the ZyXEL Device is in). For example, if the IP Pool Start Address is 10.10.10.10, the ZyXEL Device can allocate up to 10.10.10.254, or 245 IP addresses.
DNS Server	
First DNS Server Second DNS Server Third DNS Server	Specify the IP addresses of a maximum of three DNS servers that the network can use. The ZyXEL Device provides these IP addresses to DHCP clients. You can specify these IP addresses two ways. From ISP - provide the DNS servers provided by the ISP on the WAN port. User Defined - enter a static IP address. DNS Relay - this setting will relay DNS information from the DNS server obtained by the ZyXEL Device. None - no DNS service will be provided by the ZyXEL Device.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its default value.

9.2.3 LAN Static DHCP Screen



This screen has no effect if the DHCP server is not enabled. You can enable it in **Network > LAN > DHCP Setup**.

Use this screen to make the ZyXEL Device assign a specific IP address to a specific computer on the LAN. To access this screen, click **Network > LAN > Static DHCP**.

Figure 77 Network > LAN > Static DHCP

Static DHCP Table		
#	MAC Address	IP Address
1	<input type="text"/>	<input type="text" value="0.0.0.0"/>
2	<input type="text"/>	<input type="text" value="0.0.0.0"/>
3	<input type="text"/>	<input type="text" value="0.0.0.0"/>
4	<input type="text"/>	<input type="text" value="0.0.0.0"/>
5	<input type="text"/>	<input type="text" value="0.0.0.0"/>
6	<input type="text"/>	<input type="text" value="0.0.0.0"/>
7	<input type="text"/>	<input type="text" value="0.0.0.0"/>
8	<input type="text"/>	<input type="text" value="0.0.0.0"/>

Each field is described in the following table.

Table 42 Network > LAN > Static DHCP

LABEL	DESCRIPTION
#	This field is a sequential value. It is not associated with a specific entry.
MAC Address	Enter the MAC address of the computer to which you want the ZyXEL Device to assign the same IP address.
IP Address	Enter the IP address you want the ZyXEL Device to assign to the computer.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its default value.

9.2.4 LAN Client List Screen



This screen is empty if the DHCP server is not enabled. You can enable it in **Network > LAN > DHCP Setup**.

Use this screen to look at the IP addresses the ZyXEL Device has assigned to DHCP clients on the LAN. To access this screen, click **Network > LAN > Client List**.

Figure 78 Network > LAN > Client List

DHCP Client Table				
#	IP Address	Host Name	MAC Address	Reserve
1	192.168.1.33	WPC131	00:50:1f:48:59:00	<input type="checkbox"/>

Each field is described in the following table.

Table 43 Network > LAN > Client List

LABEL	DESCRIPTION
#	This field is a sequential value. It is not associated with a specific entry.
IP Address	This field displays the IP address the ZyXEL Device assigned to the computer.
Host Name	This field displays the system name of the computer to which the ZyXEL Device assigned the IP address.
MAC Address	This field displays the MAC address of the computer to which the ZyXEL Device assigned the IP address.
Reserve	Select this if you want to always assign this IP address to this MAC address. Then, click Apply . The ZyXEL Device creates an entry in the LAN Static DHCP screen. See Section 9.2.2 on page 122 .
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Reset	Click this to set every field in this screen to its default value.

9.2.5 LAN IP Alias Screen

Use this screen to add subnets on the LAN port. You can also control what routing information is sent and received by each subnet. To access this screen, click **Network > LAN > IP Alias**.

Figure 79 Network > LAN > IP Alias

IP Alias 1	
<input type="checkbox"/> IP Alias 1	
IP Address	<input type="text" value="0.0.0.0"/>
IP Subnet Mask	<input type="text" value="0.0.0.0"/>
RIP Direction	<input type="text" value="None"/>
RIP Version	<input type="text" value="RIP-1"/>
IP Alias 2	
<input type="checkbox"/> IP Alias 2	
IP Address	<input type="text" value="0.0.0.0"/>
IP Subnet Mask	<input type="text" value="0.0.0.0"/>
RIP Direction	<input type="text" value="None"/>
RIP Version	<input type="text" value="RIP-1"/>

Each field is described in the following table.

Table 44 Network > LAN > IP Alias

LABEL	DESCRIPTION
IP Alias 1	
IP Alias 1	Select this to add the specified subnet to the LAN port.
IP Address	Enter the IP address of the ZyXEL Device on the subnet.
IP Subnet Mask	Enter the subnet mask of the subnet.
RIP Direction	Use this field to control how much routing information the ZyXEL Device sends and receives on the subnet. None - The ZyXEL Device does not send or receive routing information on the subnet. Both - The ZyXEL Device sends and receives routing information on the subnet. In Only - The ZyXEL Device only receives routing information on the subnet. Out Only - The ZyXEL Device only sends routing information on the subnet.
RIP Version	Select which version of RIP the ZyXEL Device uses when it sends or receives information on the subnet. RIP-1 - The ZyXEL Device uses RIPv1 to exchange routing information. RIP-2B - The ZyXEL Device broadcasts RIPv2 to exchange routing information. RIP-2M - The ZyXEL Device multicasts RIPv2 to exchange routing information.
IP Alias 2	
IP Alias 2	Select this to add the specified subnet to the LAN port.
IP Address	Enter the IP address of the ZyXEL Device on the subnet.
IP Subnet Mask	Enter the subnet mask of the subnet.
RIP Direction	Use this field to control how much routing information the ZyXEL Device sends and receives on the subnet. None - The ZyXEL Device does not send or receive routing information on the subnet. Both - The ZyXEL Device sends and receives routing information on the subnet. In Only - The ZyXEL Device only receives routing information on the subnet. Out Only - The ZyXEL Device only sends routing information on the subnet.
RIP Version	Select which version of RIP the ZyXEL Device uses when it sends or receives information on the subnet. RIP-1 - The ZyXEL Device uses RIPv1 to exchange routing information. RIP-2B - The ZyXEL Device broadcasts RIPv2 to exchange routing information. RIP-2M - The ZyXEL Device multicasts RIPv2 to exchange routing information.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its default value.

9.2.6 LAN Advanced Screen

Use this screen to control what routing information is sent and received by each subnet. To access this screen, click **Network > LAN > Advanced**.

Figure 80 Network > LAN > Advanced

The screenshot shows the 'RIP & Multicast Setup' configuration page. At the top, there are tabs for 'IP', 'DHCP Setup', 'Static DHCP', 'Client List', 'IP Alias', and 'Advanced'. The 'Advanced' tab is selected. Below the tabs, the 'RIP & Multicast Setup' section contains three dropdown menus: 'RIP Direction' (set to 'Both'), 'RIP Version' (set to 'RIP-1'), and 'Multicast' (set to 'None'). At the bottom of the section are 'Apply' and 'Reset' buttons.

Each field is described in the following table.

Table 45 Network > LAN > Advanced

LABEL	DESCRIPTION
RIP & Multicast Setup	
RIP Direction	Use this field to control how much routing information the ZyXEL Device sends and receives on the subnet. None - The ZyXEL Device does not send or receive routing information on the subnet. Both - The ZyXEL Device sends and receives routing information on the subnet. In Only - The ZyXEL Device only receives routing information on the subnet. Out Only - The ZyXEL Device only sends routing information on the subnet.
RIP Version	Select which version of RIP the ZyXEL Device uses when it sends or receives information on the subnet. RIP-1 - The ZyXEL Device uses RIPv1 to exchange routing information. RIP-2B - The ZyXEL Device broadcasts RIPv2 to exchange routing information. RIP-2M - The ZyXEL Device multicasts RIPv2 to exchange routing information.
Multicast	You do not have to enable multicasting to use RIP-2M . (See RIP Version .) Select which version of IGMP the ZyXEL Device uses to support multicasting on the LAN. Multicasting sends packets to some computers on the LAN and is an alternative to unicasting (sending packets to one computer) and broadcasting (sending packets to every computer). None - The ZyXEL Device does not support multicasting. IGMP-v1 - The ZyXEL Device supports IGMP version 1. IGMP-v2 - The ZyXEL Device supports IGMP version 2. Multicasting can improve overall network performance. However, it requires extra processing and generates more network traffic. In addition, other computers on the LAN have to support the same version of IGMP.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Reset	Click this to set every field in this screen to its default value.

10

NAT

Use these screens to configure port forwarding and trigger ports for the ZyXEL Device. You can also enable and disable SIP, FTP, and H.323 ALG.

10.1 NAT Overview

10.1.1 Port Forwarding: Services and Port Numbers

A NAT 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.

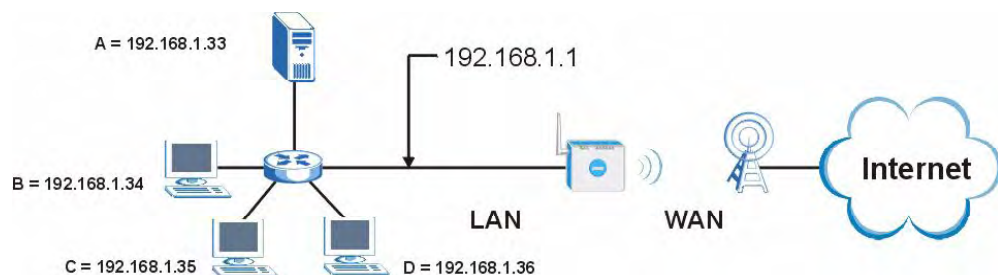
Use the [NAT Port Forwarding Screen](#) to forward incoming service requests to the server(s) on your local network. You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service 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.

See [Appendix F on page 333](#) for some examples of services.

For 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 81 Multiple Servers Behind NAT Example



10.1.2 Trigger Port Forwarding

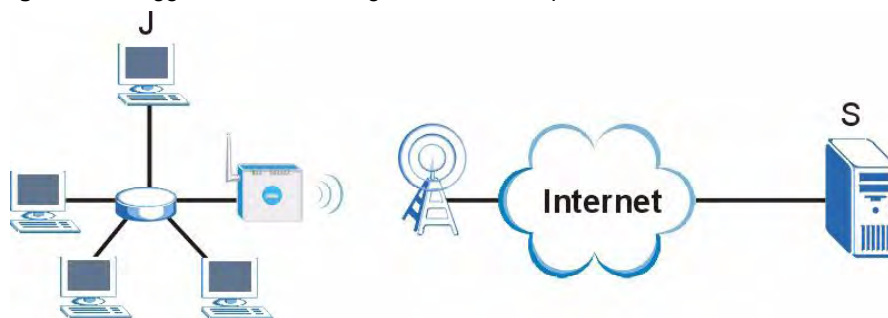
Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem 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 ZyXEL Device records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the ZyXEL Device's WAN port receives a response with a specific port number and protocol ("incoming" port), the ZyXEL Device forwards the traffic to the LAN IP address of the computer that sent the request. After that computer's connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

10.1.2.1 Trigger Port Forwarding Example

The following is an example of trigger port forwarding. In this example, **J** is Jane's computer and **S** is the Real Audio server.

Figure 82 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 ZyXEL Device to record Jane's computer IP address. The ZyXEL Device 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 ZyXEL Device 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 ZyXEL Device times out in three minutes with UDP (User Datagram Protocol), or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

10.1.2.2 Two Points To Remember About Trigger Ports

- 1 Trigger events only happen on data that is coming from inside the ZyXEL Device 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.

10.1.3 SIP ALG

Some applications, such as SIP, cannot operate through NAT (are NAT un-friendly) because they embed IP addresses and port numbers in their packets' data payload.

Some NAT routers may include a SIP Application Layer Gateway (ALG). An Application Layer Gateway (ALG) manages a specific protocol (such as SIP, H.323 or FTP) at the application layer.

A SIP ALG allows SIP calls to pass through NAT by examining and translating IP addresses embedded in the data stream. See [Section 10.2.5 on page 135](#) for information on configuring the ZyXEL Device's ALG.

10.2 NAT Screens

10.2.1 NAT General Screen

Use this screen to enable and disable NAT and to allocate memory for NAT and firewall rules. To access this screen, click **Network > NAT > General**.

Figure 83 Network > NAT > General

Each field is described in the following table.

Table 46 Network > NAT > General

LABEL	DESCRIPTION
NAT Setup	
Enable Network Address Translation	Select this if you want to use port forwarding, trigger ports, or any of the ALG.

Table 46 Network > NAT > General

LABEL	DESCRIPTION
Max NAT/Firewall Session Per User	<p>When computers use peer to peer applications, such as file sharing applications, they may use a large number of NAT sessions. If you do not limit the number of NAT sessions a single client can establish, this can result in all of the available NAT sessions being used. In this case, no additional NAT sessions can be established, and users may not be able to access the Internet.</p> <p>Each NAT session establishes a corresponding firewall session. Use this field to limit the number of NAT/firewall sessions each client computer can establish through the ZyXEL Device.</p> <p>If your network has a small number of clients using peer to peer applications, you can raise this number to ensure that their performance is not degraded by the number of NAT sessions they can establish. If your network has a large number of users using peer to peer applications, you can lower this number to ensure no single client is using all of the available NAT sessions.</p>
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its last-saved value.

10.2.2 NAT Port Forwarding Screen

Use this screen to look at the current port-forwarding rules in the ZyXEL Device, and to enable, disable, activate, and deactivate each one. You can also set up a default server to handle ports not covered by rules. To access this screen, click **Network > NAT > Port Forwarding**.

Figure 84 Network > NAT > Port Forwarding

Default Server Setup

Default Server:

Port Forwarding

#	Active	Name	Start Port	End Port	Server IP Address	Modify
1	<input type="checkbox"/>		0	0		
2	<input type="checkbox"/>		0	0		
3	<input type="checkbox"/>		0	0		
4	<input type="checkbox"/>		0	0		
5	<input type="checkbox"/>		0	0		
6	<input type="checkbox"/>		0	0		
7	<input type="checkbox"/>		0	0		
8	<input type="checkbox"/>		0	0		
9	<input type="checkbox"/>		0	0		
10	<input type="checkbox"/>		0	0		
11	<input type="checkbox"/>		0	0		

Apply Cancel

Each field is described in the following table.

Table 47 Network > NAT > Port Forwarding

LABEL	DESCRIPTION
Default Server Setup	
Default Server	Enter the IP address of the server to which the ZyXEL Device should forward packets for ports that are not specified in the Port Forwarding section below or in the Management > Remote MGMT screens. Enter 0.0.0.0 if you want the ZyXEL Device to discard these packets instead.
Port Forwarding	
#	This field is a sequential value, and it is not associated with a specific rule. The sequence is important, however. The ZyXEL Device checks each rule in order, and it only follows the first one that applies.
Active	Select this to enable this rule. Clear this to disable this rule.
Name	This field displays the name of the rule. It does not have to be unique.
Start Port	This field displays the beginning of the range of port numbers forwarded by this rule.
End Port	This field displays the end of the range of port numbers forwarded by this rule. If it is the same as the Start Port , only one port number is forwarded.
Server IP Address	This field displays the IP address of the server to which packet for the selected port(s) are forwarded.
Modify	This column provides icons to edit and delete rules. To edit a rule, click the Edit icon next to the rule. The NAT Port Forwarding Edit screen appears. To delete a rule, click the Remove icon next to the rule. All the information in the rule returns to the default settings.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Reset	Click this to set every field in this screen to its last-saved value.

10.2.3 NAT Port Forwarding Edit Screen

Use this screen to activate, deactivate, and edit each port-forwarding rule in the ZyXEL Device. To access this screen, click an **Edit** icon in **Network > NAT > Port Forwarding**.

Figure 85 Network > NAT > Port Forwarding > Edit

The screenshot shows a web-based configuration interface for editing a NAT rule. The title bar reads "Rule Setup". Below the title, there are several configuration options:

- Active
- Service Name:
- Start Port:
- End Port:
- Server IP Address:

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

Each field is described in the following table.

Table 48 Network > NAT > Port Forwarding > Edit

LABEL	DESCRIPTION
Active	Select this to enable this rule. Clear this to disable this rule.
Service Name	Enter a name to identify this rule. You can use 1 - 31 printable ASCII characters, or you can leave this field blank. It does not have to be a unique name.
Start Port End Port	Enter the port number or range of port numbers you want to forward to the specified server. To forward one port number, enter the port number in the Start Port and End Port fields. To forward a range of ports, <ul style="list-style-type: none"> • enter the port number at the beginning of the range in the Start Port field • enter the port number at the end of the range in the End Port field.
Server IP Address	Enter the IP address of the server to which to forward packets for the selected port number(s). This server is usually on the LAN.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its last-saved value.

10.2.4 NAT Trigger Port Screen

Use this screen to maintain port-triggering rules in the ZyXEL Device. To access this screen, click **Network > NAT > Trigger Port**.

Figure 86 Network > NAT > Trigger Port

Port Triggering Rules					
#	Name	Incoming		Trigger	
		Start Port	End Port	Start Port	End Port
1	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
2	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
3	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
4	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
5	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
6	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
7	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
8	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
9	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
10	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
11	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
12	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

Each field is described in the following table.

Table 49 Network > NAT > Trigger Port

LABEL	DESCRIPTION
Name	Enter a name to identify this rule. You can use 1 - 15 printable ASCII characters, or you can leave this field blank. It does not have to be a unique name.
Incoming	
Start Port End Port	Enter the incoming port number or range of port numbers you want to forward to the IP address the ZyXEL Device records. To forward one port number, enter the port number in the Start Port and End Port fields. To forward a range of ports, <ul style="list-style-type: none"> enter the port number at the beginning of the range in the Start Port field enter the port number at the end of the range in the End Port field. If you want to delete this rule, enter zero in the Start Port and End Port fields.
Trigger	
Start Port End Port	Enter the outgoing port number or range of port numbers that makes the ZyXEL Device record the source IP address and assign it to the selected incoming port number(s). To select one port number, enter the port number in the Start Port and End Port fields. To select a range of ports, <ul style="list-style-type: none"> enter the port number at the beginning of the range in the Start Port field enter the port number at the end of the range in the End Port field. If you want to delete this rule, enter zero in the Start Port and End Port fields.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to discard your changes.

10.2.5 NAT ALG Screen

Use this screen to enable and disable SIP (VoIP), FTP (file transfer), and H.323 (audio-visual) ALG in the ZyXEL Device. To access this screen, click **Network > NAT > ALG**.

Figure 87 Network > NAT > ALG

The screenshot shows a window titled "ALG Setup". Inside the window, there are three checked checkboxes: "Enable SIP ALG", "Enable FTP ALG", and "Enable H.323 ALG". At the bottom right of the window, there are two buttons: "Apply" and "Cancel".

Each field is described in the following table.

Table 50 Network > NAT > ALG

LABEL	DESCRIPTION
Enable SIP ALG	Select this to make sure SIP (VoIP) works correctly with port-forwarding and port-triggering rules.
Enable FTP ALG	Select this to make sure FTP (file transfer) works correctly with port-forwarding and port-triggering rules.

Table 50 Network > NAT > ALG

LABEL	DESCRIPTION
Enable H.323 ALG	Select this to make sure H.323 (audio-visual programs, such as NetMeeting) works correctly with port-forwarding and port-triggering rules.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to discard your most recent changes.

VPN Transport

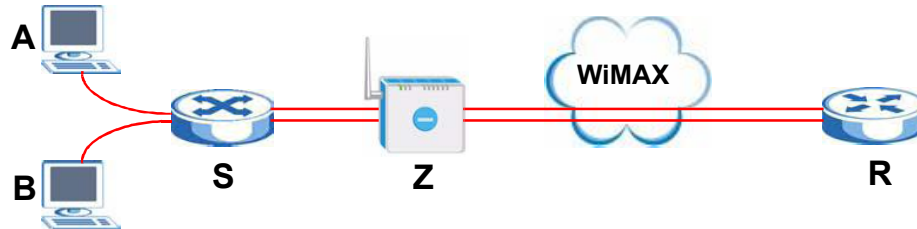
11.1 Overview

This chapter describes the **Network > VPN Transport** screens.

The ZyXEL Device's VPN Transport feature allows traffic from multiple users to pass through the WiMAX network, to the service provider's router. Each user has his own personal connection to the service provider, even though there is only a single WiMAX connection. This allows the service provider to identify which user traffic comes from.

The following figure shows two users (**A** and **B**), connecting to the ZyXEL Device (**Z**) through a switch (**S**). Each user has his own connection over the WiMAX network to the service provider's router (**R**).

Figure 88 VPN Transport example



The services available may vary, depending upon the service provider.

VPN stands for “Virtual Private Network”. There are many types of VPN; the type used by the ZyXEL Device is known as Virtual Private LAN Service, or VPLS.



Unlike some other types of VPN (such as IPSec VPNs) VPLS VPNs do not use authentication or encryption to secure the data they carry.

11.1.1 What You Can Do in the VPN Transport Screens

- Use the **Network > VPN Transport > General** screen (see [Section 11.2 on page 140](#)) to turn VPN transport on or off, and to set the VPN transport endpoint (your service provider's router).
- Use the **Network > VPN Transport > Customer Interface** screen (see [Section 11.3 on page 141](#)) to specify which users can use which WiMAX network links.
- Use the **Network > VPN Transport > Ethernet Pseudowire** screen (see [Section 11.5 on page 143](#)) to configure the links over the WiMAX network between the ZyXEL Device and the service provider's router.
- Use the **Network > VPN Transport > Statistics** screen (see [Section 11.7 on page 145](#)) to view performance information about the VPN transport connections.

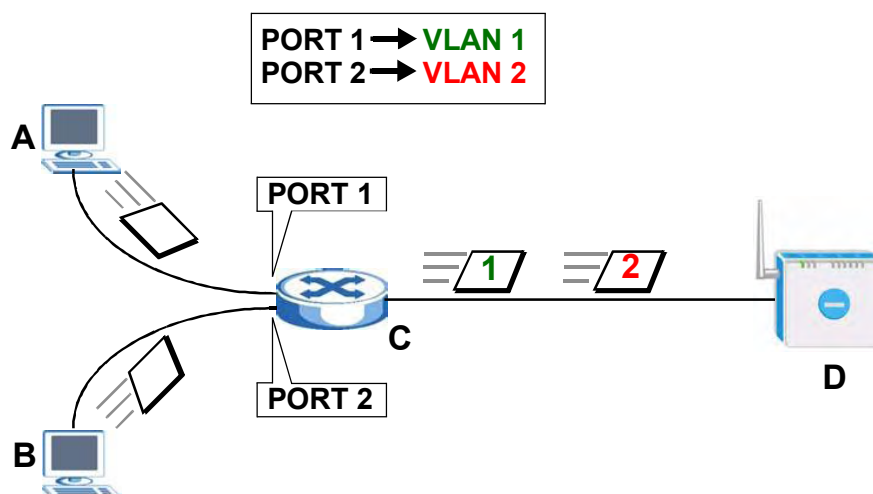
11.1.2 What You Need to Know about VPN Transport

Identifying Users

For the ZyXEL Device's VPN Transport feature to work, it must be able to identify users on the LAN. It does this by examining VLAN (Virtual Local Area Network) tags.

These tags must be added to the data packets by a switch on the LAN. In the following example, two users (**A** and **B**) are connected to a switch (**C**). **A** and **B** are connected to different ports on the switch (port 1 and port 2). **A** and **B** send untagged packets to the switch. The switch adds tags to packets depending on the physical port on which they arrive. Packets arriving on port 1 are given a VLAN ID (VLAN Identifier) of 1, and packets arriving on port 2 are given a VLAN ID of 2. When the packets reach the ZyXEL Device (**D**), their source is identified by examining their VLAN tags.

Figure 89 Identifying Users



Ethernet Pseudowires

Because VPLS mimics a simple wired Ethernet connection to your service provider's router, the connection between the ZyXEL Device and the peer device is known as an "Ethernet pseudowire" or "PW".

The Ethernet pseudowires use MPLS (MultiProtocol Label Switching) virtual circuit labels to define the connection. In any such pseudowire, the ingress label on one device must be the same as the egress label on the peer device, as shown in the following figure. **A** is your ZyXEL Device and **B** is your service provider's router.

Figure 90 Ethernet Pseudowire Settings Example

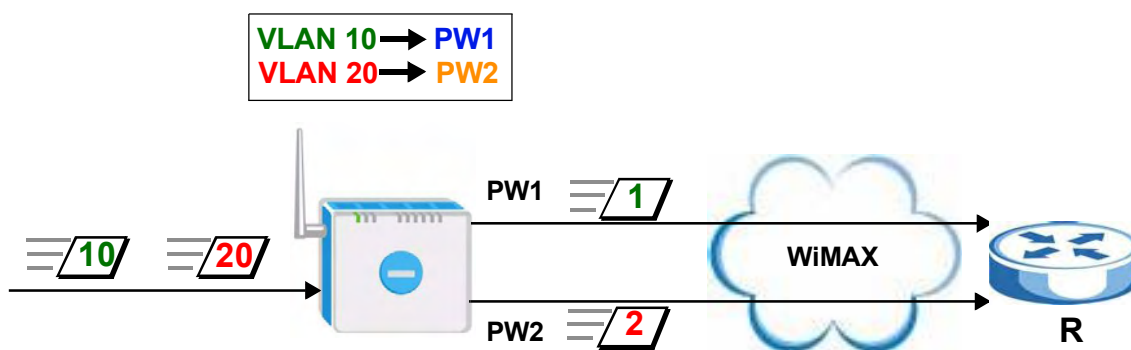


Customer Interface Mapping

Once the ZyXEL Device has examined a frame's VLAN tag, it is able to assign the frame to a specified path. This is done using a customer interface. The customer interface is simply a set of information that takes frames from a VLAN and put them on an Ethernet pseudowire, and vice versa.

In the following example, the ZyXEL Device takes frames tagged with two different VLAN IDs (**10** and **20**) and using the customer interfaces, assigns them to specific pseudowires (**PW1** and **PW2**).

Figure 91 Pseudowire Mapping



The ZyXEL Device has a default customer interface configured for frames that arrive at the ZyXEL Device without VLAN tags.

11.1.3 Before You Begin

Before you start configuring your ZyXEL Device to use VPN transport, ensure that you have the following from the service provider.

- The IP address or domain name of the service provider's edge router.
- Virtual circuit (VC) labels for each Ethernet Pseudowire you want to create.

Also, ensure you know the VLAN IDs (Virtual LAN IDentifiers) of the VLANs on your LAN.

11.2 The General Screen

Use this screen to turn VPN transport on or off, and to set the VPN transport endpoint (your service provider's router). Click **Network > VPN Transport > General**. The following screen displays.

Figure 92 Network > VPN Transport > General

The following table describes the labels in this screen.

Table 51 Network > VPN Transport > General

LABEL	DESCRIPTION
L2/L3 VPN Transport General Setup	
Transport L2/L3 VPN traffic through WiMAX network by using Ethernet pseudowire	Select this to turn the VPN transport feature on. Deselect it to turn the VPN transport feature off.
Remote GRE Tunnel End	Enter the domain name or IP address of your service provider's router.
Apply	Click this to save your settings.
Reset	Click this to return the fields in this screen to their defaults.

11.3 The Customer Interface Screen

Use this screen to configure the VPNs used by the ZyXEL Device. The customer interfaces connect data coming from your computers to Ethernet pseudowires, according to the data's VLAN (Virtual Local Area Network) information. One customer interface is for traffic that has no tag; this is the default interface (rule 0) which cannot be deleted in the GUI. All other customer interfaces are identified by their VLAN ID.

Click **Network > VPN Transport > Customer Interface**. The following screen displays.

Figure 93 Network > VPN Transport > Customer Interface

#	Active	Interface		Mode	Associated Ethernet Pseudowire (Ingress, Egress)	DSCP	Interface Description	Modify
		Type	VLAN ID					
0		Untagged	-1	Routing	-	-	for Routing/NAT	
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								

The following table describes the labels in this screen.

Table 52 Network > VPN Transport > Customer Interface

LABEL	DESCRIPTION
#	This displays the interface index number. Interface 0 is the default rule for routing, and cannot be deleted.
Active	This icon is green if the associated interface is enabled. The icon is grey if the associated interface is disabled. Enable or disable an interface by clicking its Edit icon and selecting or deselecting Active and clicking Apply in the screen that displays.
Interface	
Type	This displays either Tagged or Untagged . A tagged interface controls traffic with a specific IEEE 802.1Q VLAN tag, whereas an untagged interface controls traffic that does not have a VLAN tag. There can be only one untagged interface.

Table 52 Network > VPN Transport > Customer Interface

LABEL	DESCRIPTION
VLAN ID	For a tagged interface, this displays the IEEE 802.1Q VLAN ID number. For the untagged interface, -1 displays.
Mode (B, R)	This displays either B (bridging) or R (routing). Only the default interface, interface 0, can be a routing interface.
Associated Ethernet Pseudowire	This displays the number of the Ethernet pseudowire that this interface uses, as well as the ingress and egress MPLS (Multi-Protocol Label Switching) VC (Virtual Circuit) label numbers.
dscp	This displays the DiffServ Control Point value you previously entered in binary (see Section 12.1.12 on page 155 for more information on DSCP). This determines the pseudowire's priority on the network. The DSCP value is displayed in binary notation and has six bits.
Interface Description	This displays the information you previously entered describing the interface. For the default interface, interface 0, the description reads "for routing / NAT".
Modify	Click the Edit icon to set up a new interface or alter the configuration of an existing interface. Click the Delete icon to remove an existing interface.

11.4 The Customer Interface Edit Screen

Customer interfaces map traffic onto specific Ethernet pseudowires for transport over the WiMAX network. There is also a default customer interface for routing traffic that does not possess a VLAN tag.

Use this screen to configure the customer interface settings. Click the **Edit** icon in the **Network > VPN Transport > Customer Interface** screen. The following screen displays.

Figure 94 Network > VPN Transport > Customer Interface Edit

Customer Interface Setup

Active

Customer Interface

Type: Untagged

VLAN ID: -1 (1~4094 for tagged, -1 for Untagged)

Mode: Routing

Associated Ethernet Pseudowire: #0(0,0)

DSCP: 000000 (6 bits)

Interface Description: for Routing/NAT

Apply Cancel

The following table describes the labels in this screen.

Table 53 Network > VPN Transport > Customer Interface Edit

LABEL	DESCRIPTION
Customer Interface	
Type	A customer interface can be tagged (controlling traffic that has a specific VLAN ID) or untagged (controlling traffic without a specific VLAN ID). There can be only one untagged interface.

Table 53 Network > VPN Transport > Customer Interface Edit

LABEL	DESCRIPTION
VLAN ID	Enter the Virtual Local Area Network Identifier number (1 ~ 4094) for this interface. This VLAN ID must not be used by any other customer interface. For the untagged interface, -1 displays.
Mode	This displays Bridging or Routing . A tagged interface can operate in bridging mode only.
Associated Ethernet Pseudowire	Select the Ethernet pseudowire this interface should use for communications over the WiMAX network. You should configure the pseudowire (in the Network > VPN Transport > Ethernet Pseudowire screen) before you select it.
DSCP	If you wish to prioritize an interface, enter a DiffServ Code Point value of six bits in binary notation. The higher the value, the higher the interface's priority on the ZyXEL Device's WiMAX link. See Section 12.1.12 on page 155 for more information on DSCP.
Interface Description	Enter a brief (up to 31 characters) name or description for this interface.
Apply	Click this to save your changes and return to the previous screen.
Cancel	Click this to return to the previous screen without saving your changes.

11.5 The Ethernet Pseudowire Screen

Use this screen to configure Ethernet pseudowires. Each Ethernet pseudowire mimics a regular wired Ethernet connection, transporting VPLS data over the WiMAX network between the ZyXEL Device and the peer device (the endpoint you specify in the **Network > VPN Transport > General** screen).

Click **Network > VPN Transport > Ethernet Pseudowire**. The following screen displays.

Figure 95 Network > VPN Transport > Ethernet Pseudowire

#	Active	MPLS VC Label		Pseudowire Description	Modify
		Ingress	Egress		
0		0	0		
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					

The following table describes the labels in this screen.

Table 54 Network > VPN Transport > Ethernet Pseudowire

LABEL	DESCRIPTION
#	This displays the pseudowire index number.
Active	This icon is green if the associated pseudowire is enabled. The icon is grey if the associated pseudowire is disabled. Enable or disable a pseudowire by clicking its Edit icon.
Ingress	This is the MPLS virtual circuit label number for traffic coming from the peer device.
Egress	This is the MPLS virtual circuit label number for traffic going to the peer device.
Pseudowire Description	This displays the information you previously entered describing the pseudowire.
Modify	Click the Edit icon to set up a new interface or alter the configuration of an existing pseudowire. Click the Delete icon to remove an existing pseudowire.

11.6 The Ethernet Pseudowire Edit Screen

Use this screen to set up or modify an Ethernet pseudowire's configuration. Click a pseudowire entry's **Edit** icon in the **Network > VPN Transport > Ethernet Pseudowire** screen. The following screen displays.

Figure 96 Network > VPN Transport > Ethernet Pseudowire > Edit

The following table describes the labels in this screen.

Table 55 Network > VPN Transport > Ethernet Pseudowire > Edit

LABEL	DESCRIPTION
Active	Select this to enable the pseudowire. Deselect it to disable the pseudowire.
Ingress	Enter the VC ingress label number for this pseudowire. This must be the egress label number of the peer device. This should not be the ingress label number of any other Ethernet pseudowire configured on the ZyXEL Device.
Egress	Enter the egress label number for this pseudowire. This must be the ingress label of the peer device. This should not be the egress label number of any other Ethernet pseudowire configured on the ZyXEL Device.
Pseudowire Description	Enter a brief (up to 31 characters) description for this pseudowire.
Apply	Click this to save your settings and return to the previous screen.
Reset	Click this to reset the fields in this screen to their last-saved values.

11.7 The Statistics Screen

Use this screen to view details and performance information of each active customer interface and its associated Ethernet pseudowire. Click **Network > VPN Transport > Statistics**. The following screen displays.

Figure 97 Network > VPN Transport > Statistics

#	Active	Total Packets		Total Bytes		Interface Description
		Transmit (pkts)	Receive (pkts)	Transmit (bytes)	Receive (bytes)	
0		0	0	0	0	for Routing/NAT
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						

The following table describes the labels in this screen.

Table 56 Network > VPN Transport > Statistics

LABEL	DESCRIPTION
#	This is the index number of the customer interface.
Active	This icon is green if the associated interface is enabled. The icon is grey if the associated interface is disabled. Enable or disable an interface by clicking its Edit icon.
Total Packets	This displays the number of packets received (Receive) and sent (Transmit) on the customer interface since the interface was activated, or the Clear button pressed.
Total Bytes	This displays the number of bytes received (Receive) and sent (Transmit) on the customer interface since the interface was activated, or the Clear button pressed.
Interface Description	This is the brief name or description of the customer interface you configured in the Network > VPN Transport > Customer Interface > Edit screen.

11.8 VPN Transport Technical Reference

This section includes background information about VPN Transport.

11.8.1 Multi-Protocol Label Switching

The ZyXEL Device uses MPLS VPNs to create virtual private LANs. MPLS stands for Multi-Protocol Label Switching, and is a packet-switching technology that allows packets with different VLAN tags to be transported on different paths (known as LSPs, or Label Switched Paths). Each packet is identified by its VLAN tag and sent to a specific LSP for transport over the WiMAX network.

Each LSP has a defined start-point and end-point. Since MPLS creates mono-directional paths (traffic flows in only one direction), each Ethernet pseudowire uses two LSPs so that traffic can flow both ways. One LSP carries upstream traffic, and the other carries downstream traffic.

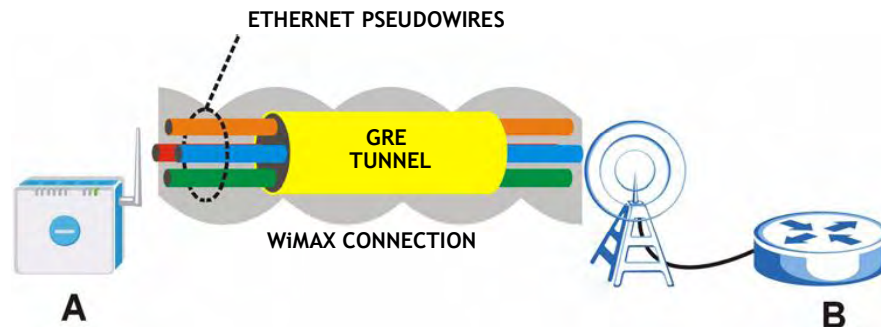
11.8.2 Generic Routing Encapsulation

In order to transport the VPLS traffic over the WiMAX network, the ZyXEL Device uses the Generic Routing Encapsulation (GRE) protocol. Like MPLS, GRE is a tunneling protocol that has specified endpoints. The GRE tunnel is bi-directional, and transports both LSPs. The GRE tunnel runs across the WiMAX network between the ZyXEL Device and your service provider's router.

It is necessary to encapsulate the Ethernet pseudowire since the WiMAX connection is IP-only. MPLS information is carried in a packet's Ethernet header and, without encapsulation, would be stripped from the packet prior to the packet's transmission over the WiMAX link.

The following figure shows the VPLS connection between your ZyXEL Device (A) and your service provider's router (B), consisting of GRE-encapsulated Ethernet pseudowire traffic.

Figure 98 VPLS Tunneling



Use these screens to set up your SIP accounts and to configure QoS settings.

12.1 SIP Overview

12.1.1 Introduction to VoIP

VoIP (Voice over IP) is the sending of voice signals over the Internet Protocol. This allows you to make phone calls and send faxes over the Internet at a fraction of the cost of using the traditional circuit-switched telephone network. You can also use servers to run telephone service applications like PBX services and voice mail. Internet Telephony Service Provider (ITSP) companies provide VoIP service. A company could alternatively set up an IP-PBX and provide its own VoIP service.

Circuit-switched telephone networks require 64 kilobits per second (kbps) in each direction to handle a telephone call. VoIP can use advanced voice coding techniques with compression to reduce the required bandwidth.

12.1.2 Introduction to SIP

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet.

SIP signaling is separate from the media for which it handles sessions. The media that is exchanged during the session can use a different path from that of the signaling. SIP handles telephone calls and can interface with traditional circuit-switched telephone networks.

12.1.3 SIP Identities

A SIP account uses an identity (sometimes referred to as a SIP address). A complete SIP identity is called a SIP URI (Uniform Resource Identifier). A SIP account's URI identifies the SIP account in a way similar to the way an e-mail address identifies an e-mail account. The format of a SIP identity is SIP-Number@SIP-Service-Domain.

12.1.3.1 SIP Number

The SIP number is the part of the SIP URI that comes before the “@” symbol. A SIP number can use letters like in an e-mail address ([johndoe@your-ITSP.com](mailto: johndoe@your-ITSP.com) for example) or numbers like a telephone number ([1122334455@VoIP-provider.com](tel: 1122334455@VoIP-provider.com) for example).

12.1.3.2 SIP Service Domain

The SIP service domain of the VoIP service provider (the company that lets you make phone calls over the Internet) is the domain name in a SIP URI. For example, if the SIP address is 1122334455@VoIP-provider.com, then “VoIP-provider.com” is the SIP service domain.

12.1.4 SIP Call Progression

The following figure displays the basic steps in the setup and tear down of a SIP call. A calls B.

Table 57 SIP Call Progression

A		B
1. INVITE		
		2. Ringing
		3. OK
4. ACK		
	5. Dialogue (voice traffic)	
6. BYE		
		7. OK

- 1 A sends a SIP INVITE request to B. This message is an invitation for B to participate in a SIP telephone call.
- 2 B sends a response indicating that the telephone is ringing.
- 3 B sends an OK response after the call is answered.
- 4 A then sends an ACK message to acknowledge that B has answered the call.
- 5 Now A and B exchange voice media (talk).
- 6 After talking, A hangs up and sends a BYE request.
- 7 B replies with an OK response confirming receipt of the BYE request and the call is terminated.

12.1.5 SIP Client Server

SIP is a client-server protocol. A SIP client is an application program or device that sends SIP requests. A SIP server responds to the SIP requests.

When you use SIP to make a VoIP call, it originates at a client and terminates at a server. A SIP client could be a computer or a SIP phone. One device can act as both a SIP client and a SIP server.

12.1.5.1 SIP User Agent

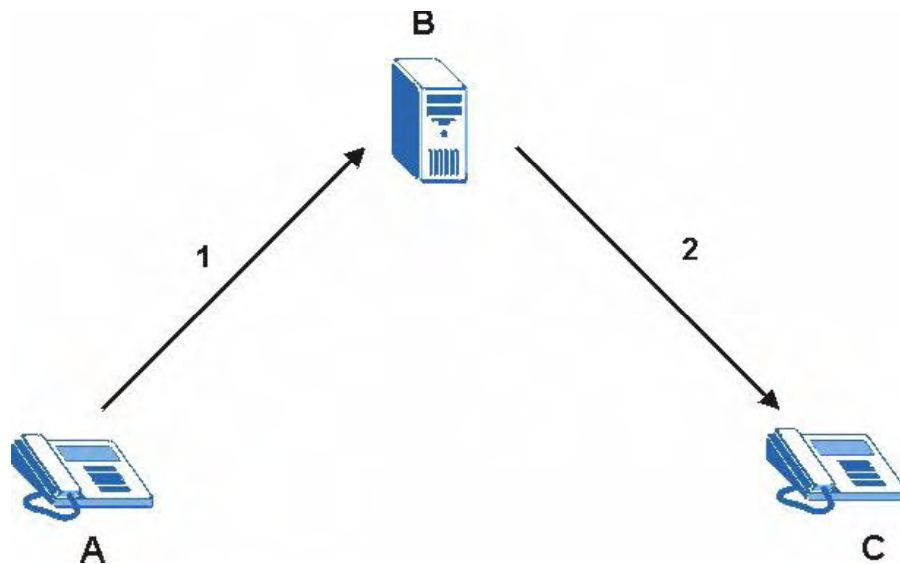
A SIP user agent can make and receive VoIP telephone calls. This means that SIP can be used for peer-to-peer communications even though it is a client-server protocol. In the following figure, either A or B can act as a SIP user agent client to initiate a call. A and B can also both act as a SIP user agent to receive the call.

Figure 99 SIP User Agent**12.1.5.2 SIP Proxy Server**

A SIP proxy server receives requests from clients and forwards them to another server.

In the following example, you want to use client device A to call someone who is using client device C.

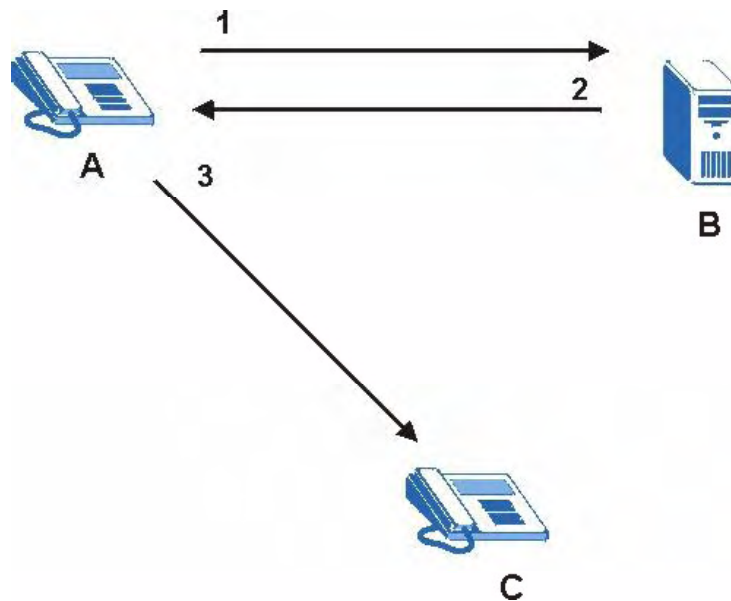
- 1 The client device (A in the figure) sends a call invitation to the SIP proxy server (B).
- 2 The SIP proxy server forwards the call invitation to C.

Figure 100 SIP Proxy Server**12.1.5.3 SIP Redirect Server**

A SIP redirect server accepts SIP requests, translates the destination address to an IP address and sends the translated IP address back to the device that sent the request. Then the client device that originally sent the request can send requests to the IP address that it received back from the redirect server. Redirect servers do not initiate SIP requests.

In the following example, you want to use client device A to call someone who is using client device C.

- 1 Client device A sends a call invitation for C to the SIP redirect server (B).
- 2 The SIP redirect server sends the invitation back to A with C's IP address (or domain name).
- 3 Client device A then sends the call invitation to client device C.

Figure 101 SIP Redirect Server

12.1.5.4 SIP Register Server

A SIP register server maintains a database of SIP identity-to-IP address (or domain name) mapping. The register server checks your user name and password when you register.

12.1.6 RTP

When you make a VoIP call using SIP, the RTP (Real time Transport Protocol) is used to handle voice data transfer. See RFC 1889 for details on RTP.

12.1.7 NAT and SIP

The ZyXEL Device must register its public IP address with a SIP register server. If there is a NAT router between the ZyXEL Device and the SIP register server, the ZyXEL Device probably has a private IP address. The ZyXEL Device lists its IP address in the SIP message that it sends to the SIP register server. NAT does not translate this IP address in the SIP message. The SIP register server gets the ZyXEL Device's IP address from inside the SIP message and maps it to your SIP identity. If the ZyXEL Device has a private IP address listed in the SIP message, the SIP server cannot map it to your SIP identity. See [Chapter 10 on page 129](#) for more information about NAT.

Use a SIP ALG (Application Layer Gateway), Use NAT, STUN, or outbound proxy to allow the ZyXEL Device to list its public IP address in the SIP messages.

12.1.7.1 SIP ALG

See [Section 10.1.3 on page 131](#).