

MAX-306HW2 Series

Models: MAX-306 ODU (2.5 GHz), MAX-316 ODU (3.5 GHz), MAX-306HW2 IDU

User's Guide

WiMAX MIMO Indoor/Outdoor
CPE (2.5GHz & 3.5GHz)



Default Login Details

IP Address: <http://192.168.100.1>

User Name: admin

Password: 1234

Firmware Version 3.6
Edition 2, 05/2009

www.zyxel.com

ZyXEL

Copyright © 2009
ZyXEL Communications Corporation

Company Confidential

About This User's Guide

Intended Audience

This manual is intended for people who want to configure this product using the web configurator. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

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.

- Web Configurator Online Help

Embedded web help for descriptions of individual screens and supplementary information.

- Command Reference Guide

The Command Reference Guide explains how to use the Command-Line Interface (CLI) and CLI commands to configure the WiMAX Device.

- Support Disc

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 WiMAX Device.

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











Syntax Conventions

- This product may be referred to as the "WiMAX Device", 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, **TOOLS > Logs > Log Settings** means you first click Tools in the navigation panel, then the Logs sub menu and finally the Log Settings 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 WiMAX Device icon is not an exact representation of your WiMAX Device.\

Table 1 Common Icons

| | | |
|--|---|--|
| Wireless Signal  | Internet Cloud  | Computer  |
| Notebook  | Server  | WiMAX Base Station  |
| Telephone  | Switch  | Router  |
| Network Cloud  | | |

Safety Warnings

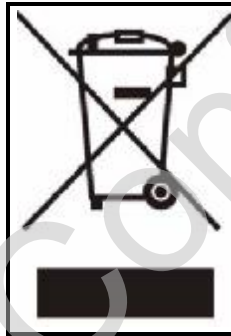
For your safety, be sure to read and follow all warning notices and instructions.

- 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.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- 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 it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- 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 device and the power source.
- 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).
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.

- The Power over Ethernet (PoE) device that supplies power must be indoors.
- Do not use the Indoor Unit's PoE feature to supply power to any other device other than the Outdoor Unit models specified in this User's Guide.
- Do not use any PoE device other than the Indoor Unit model specified in this User's Guide to supply power to the Outdoor Unit.
- You must maintain a minimum distance of 23 centimeters (9 inches) from the outdoor unit.

Your product is marked with this symbol, which is known as the WEEE mark.

WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.



Company Confidential

Contents Overview

| | |
|---|------------|
| Introduction and Wizards | 29 |
| Getting Started | 31 |
| Introducing the Web Configurator | 37 |
| Internet Connection Wizard | 47 |
| VoIP Connection Wizard | 59 |
| Basic Screens | 65 |
| The Setup Screens | 67 |
| Advanced Screens | 73 |
| The LAN Configuration Screens | 75 |
| The WAN Configuration Screens | 89 |
| The Wi-Fi Configuration Screens | 103 |
| The VPN Transport Screens | 113 |
| The NAT Configuration Screens | 125 |
| The System Configuration Screens | 135 |
| Voice Screens | 145 |
| The Service Configuration Screens | 147 |
| The Phone Screens | 165 |
| The Phone Book Screens | 175 |
| Tools & Status Screens | 181 |
| The Certificates Screens | 183 |
| The Firewall Screens | 203 |
| Content Filter | 213 |
| The Remote Management Screens | 217 |
| The Logs Screens | 227 |
| The UPnP Screen | 243 |
| The Status Screen | 253 |
| Troubleshooting and Specifications | 265 |
| Troubleshooting | 267 |
| Product Specifications | 275 |
| Appendices and Index | 277 |

Company Confidential

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 | 19 |
| List of Tables | 25 |
| | |
| Part I: Introduction and Wizards | 29 |
| | |
| Chapter 1 | |
| Getting Started | 31 |
| 1.1 Overview | 31 |
| 1.1.1 Wi-Fi Access Point | 32 |
| 1.1.2 WiMAX Internet Access | 32 |
| 1.1.3 Make Calls via Internet Telephony Service Provider | 33 |
| 1.2 WiMAX Device Hardware | 34 |
| 1.2.1 LEDs | 34 |
| 1.3 Good Habits for Managing the WiMAX Device | 35 |
| | |
| Chapter 2 | |
| Introducing the Web Configurator | 37 |
| 2.1 Overview | 37 |
| 2.1.1 Accessing the Web Configurator | 37 |
| 2.1.2 The Reset Button | 40 |
| 2.2 The Main Screen | 40 |
| | |
| Chapter 3 | |
| Internet Connection Wizard | 47 |
| 3.1 Overview | 47 |
| 3.1.1 Welcome to the ZyXEL Setup Wizard | 47 |
| 3.1.2 System Information | 48 |
| 3.1.3 Wireless LAN | 49 |

| | |
|---|-----------|
| 3.1.4 Authentication Settings | 54 |
| 3.1.5 IP Address | 56 |
| 3.1.6 Setup Complete | 58 |
| Chapter 4 | |
| VoIP Connection Wizard..... | 59 |
| 4.1 Overview | 59 |
| 4.2 Welcome to the ZyXEL Setup Wizard | 59 |
| 4.2.1 First Voice Account Settings | 60 |
| 4.2.2 Setup Complete | 63 |
| | |
| Part II: Basic Screens | 65 |
| | |
| Chapter 5 | |
| The Setup Screens..... | 67 |
| 5.1 Overview | 67 |
| 5.1.1 What You Can Do in This Chapter | 67 |
| 5.1.2 What You Need to Know | 67 |
| 5.1.3 Before You Begin | 68 |
| 5.2 Set IP Address | 68 |
| 5.3 DHCP Client | 69 |
| 5.4 Time Setting | 70 |
| 5.4.1 Pre-Defined NTP Time Servers List | 71 |
| 5.4.2 Resetting the Time | 72 |
| | |
| Part III: Advanced Screens..... | 73 |
| | |
| Chapter 6 | |
| The LAN Configuration Screens..... | 75 |
| 6.1 Overview | 75 |
| 6.1.1 What You Can Do in This Chapter | 75 |
| 6.1.2 What You Need to Know | 75 |
| 6.2 DHCP Setup | 76 |
| 6.3 Static DHCP | 78 |
| 6.4 IP Alias | 79 |
| 6.5 IP Static Route | 81 |
| 6.5.1 IP Static Route Setup | 82 |
| 6.6 Other Settings | 83 |
| 6.7 Technical Reference | 84 |
| 6.7.1 IP Address and Subnet Mask | 84 |

| | |
|--|------------|
| 6.7.2 DHCP Setup | 85 |
| 6.7.3 LAN TCP/IP | 85 |
| 6.7.4 DNS Server Address | 86 |
| 6.7.5 RIP Setup | 86 |
| 6.7.6 Multicast | 87 |
| Chapter 7 | |
| The WAN Configuration Screens..... | 89 |
| 7.1 Overview | 89 |
| 7.1.1 What You Can Do in This Chapter | 89 |
| 7.1.2 What You Need to Know | 89 |
| 7.2 Internet Connection | 93 |
| 7.3 WiMAX Configuration | 95 |
| 7.3.1 Frequency Ranges | 97 |
| 7.3.2 Configuring Frequency Settings | 97 |
| 7.3.3 Using the WiMAX Frequency Screen | 98 |
| 7.4 Traffic Redirect | 99 |
| 7.5 Advanced | 101 |
| Chapter 8 | |
| The Wi-Fi Configuration Screens | 103 |
| 8.1 Overview | 103 |
| 8.1.1 What You Can Do in This Chapter | 103 |
| 8.1.2 What You Need to Know | 103 |
| 8.2 General | 104 |
| 8.3 MAC Filter | 109 |
| 8.4 Advanced | 110 |
| Chapter 9 | |
| The VPN Transport Screens..... | 113 |
| 9.1 Overview | 113 |
| 9.1.1 What You Can Do in This Chapter | 114 |
| 9.1.2 What You Need to Know | 114 |
| 9.1.3 Before You Begin | 115 |
| 9.2 General | 116 |
| 9.3 Customer Interface | 116 |
| 9.3.1 Multi-Protocol Label Switching | 117 |
| 9.3.2 Generic Routing Encapsulation | 117 |
| 9.3.3 Customer Interface Options | 118 |
| 9.3.4 Customer Interface Setup | 120 |
| 9.4 Ethernet Pseudowire | 121 |
| 9.4.1 Ethernet Pseudowire Setup | 123 |
| 9.5 Statistics | 124 |

| | |
|--|------------|
| Chapter 10 | |
| The NAT Configuration Screens..... | 125 |
| 10.1 Overview | 125 |
| 10.1.1 What You Can Do in This Chapter | 125 |
| 10.2 General | 125 |
| 10.3 Port Forwarding | 126 |
| 10.3.1 Port Forwarding Options | 127 |
| 10.3.2 Port Forwarding Rule Setup | 129 |
| 10.4 Trigger Port | 130 |
| 10.4.1 Trigger Port Forwarding Example | 131 |
| 10.5 ALG | 132 |
| Chapter 11 | |
| The System Configuration Screens | 135 |
| 11.1 Overview | 135 |
| 11.1.1 What You Can Do in This Chapter | 135 |
| 11.1.2 What You Need to Know | 135 |
| 11.2 General | 137 |
| 11.3 Dynamic DNS | 138 |
| 11.4 Firmware | 140 |
| 11.4.1 The Firmware Upload Process | 141 |
| 11.5 Configuration | 142 |
| 11.5.1 The Restore Configuration Process | 143 |
| 11.6 Restart | 143 |
| 11.6.1 The Restart Process | 144 |
| Part IV: Voice Screens | 145 |
| Chapter 12 | |
| The Service Configuration Screens | 147 |
| 12.1 Overview | 147 |
| 12.1.1 What You Can Do in This Chapter | 147 |
| 12.1.2 What You Need to Know | 147 |
| 12.1.3 Before you Begin | 149 |
| 12.2 SIP Settings | 149 |
| 12.2.1 Advanced SIP Settings | 151 |
| 12.3 QoS | 158 |
| 12.4 Technical Reference | 159 |
| 12.4.1 SIP Call Progression | 159 |
| 12.4.2 SIP Client Server | 160 |
| 12.4.3 SIP User Agent | 160 |

| | |
|---|------------|
| 12.4.4 SIP Proxy Server | 160 |
| 12.4.5 SIP Redirect Server | 161 |
| 12.4.6 NAT and SIP | 162 |
| 12.4.7 DiffServ | 162 |
| 12.4.8 DSCP and Per-Hop Behavior | 163 |
| Chapter 13 | |
| The Phone Screens..... | 165 |
| 13.1 Overview | 165 |
| 13.1.1 What You Can Do in This Chapter | 165 |
| 13.1.2 What You Need to Know | 165 |
| 13.2 Analog Phone | 166 |
| 13.2.1 Advanced Analog Phone Setup | 168 |
| 13.3 Common | 169 |
| 13.4 Region | 170 |
| 13.5 Technical Reference | 170 |
| 13.5.1 The Flash Key | 170 |
| 13.5.2 Europe Type Supplementary Phone Services | 171 |
| 13.5.3 USA Type Supplementary Services | 173 |
| Chapter 14 | |
| The Phone Book Screens..... | 175 |
| 14.1 Overview | 175 |
| 14.1.1 What You Can Do in This Chapter | 175 |
| 14.1.2 What You Need to Know | 175 |
| 14.2 Incoming Call Policy | 176 |
| 14.3 Speed Dial | 178 |
| Part V: Tools & Status Screens..... | 181 |
| Chapter 15 | |
| The Certificates Screens..... | 183 |
| 15.1 Overview | 183 |
| 15.1.1 What You Can Do in This Chapter | 183 |
| 15.1.2 What You Need to Know | 183 |
| 15.2 My Certificates | 184 |
| 15.2.1 My Certificates Create | 186 |
| 15.2.2 My Certificate Edit | 189 |
| 15.2.3 My Certificate Import | 192 |
| 15.3 Trusted CAs | 193 |
| 15.3.1 Trusted CA Edit | 195 |

| | |
|---|------------|
| 15.3.2 Trusted CA Import | 197 |
| 15.4 Technical Reference | 198 |
| 15.4.1 Certificate Authorities | 198 |
| 15.4.2 Verifying a Certificate | 200 |
| Chapter 16 | |
| The Firewall Screens | 203 |
| 16.1 Overview | 203 |
| 16.1.1 What You Can Do in This Chapter | 203 |
| 16.1.2 What You Need to Know | 203 |
| 16.2 Firewall Setting | 204 |
| 16.2.1 Firewall Rule Directions | 204 |
| 16.2.2 Triangle Route | 205 |
| 16.2.3 Firewall Setting Options | 206 |
| 16.3 Service Setting | 207 |
| 16.4 Technical Reference | 208 |
| 16.4.1 Stateful Inspection Firewall. | 208 |
| 16.4.2 Guidelines For Enhancing Security With Your Firewall | 209 |
| 16.4.3 The “Triangle Route” Problem | 209 |
| Chapter 17 | |
| Content Filter..... | 213 |
| 17.1 Overview | 213 |
| 17.1.1 What You Can Do in This Chapter | 213 |
| 17.2 Filter | 214 |
| 17.3 Schedule | 216 |
| Chapter 18 | |
| The Remote Management Screens | 217 |
| 18.1 Overview | 217 |
| 18.1.1 What You Can Do in This Chapter | 217 |
| 18.1.2 What You Need to Know | 218 |
| 18.2 WWW | 219 |
| 18.3 Telnet | 220 |
| 18.4 FTP | 220 |
| 18.5 SNMP | 221 |
| 18.5.1 SNMP Traps | 222 |
| 18.5.2 SNMP Options | 223 |
| 18.6 DNS | 224 |
| 18.7 Security | 225 |
| Chapter 19 | |
| The Logs Screens | 227 |

| | |
|---|------------|
| 19.1 Overview | 227 |
| 19.1.1 What You Can Do in This Chapter | 227 |
| 19.1.2 What You Need to Know | 227 |
| 19.2 View Logs | 229 |
| 19.3 Log Settings | 231 |
| 19.4 Log Message Descriptions | 233 |
| Chapter 20 | |
| The UPnP Screen | 243 |
| 20.1 Overview | 243 |
| 20.1.1 What You Can Do in This Chapter | 243 |
| 20.1.2 What You Need to Know | 243 |
| 20.2 UPnP | 244 |
| 20.3 Technical Reference | 245 |
| 20.3.1 Installing UPnP in Windows XP | 245 |
| 20.3.2 Web Configurator Easy Access | 249 |
| Chapter 21 | |
| The Status Screen..... | 253 |
| 21.1 Overview | 253 |
| 21.2 Status Screen | 253 |
| 21.2.1 Packet Statistics | 258 |
| 21.2.2 WiMAX Site Information | 259 |
| 21.2.3 DHCP Table | 260 |
| 21.2.4 VoIP Statistics | 261 |
| 21.2.5 WiMAX Profile | 263 |
| Part VI: Troubleshooting and Specifications | 265 |
| Chapter 22 | |
| Troubleshooting..... | 267 |
| 22.1 Power, Hardware Connections, and LEDs | 267 |
| 22.2 WiMAX Device Access and Login | 268 |
| 22.3 Internet Access | 270 |
| 22.4 Phone Calls and VoIP | 272 |
| 22.5 Reset the WiMAX Device to Its Factory Defaults | 273 |
| 22.5.1 Pop-up Windows, JavaScripts and Java Permissions | 273 |
| Chapter 23 | |
| Product Specifications | 275 |

| | |
|---|------------|
| Part VII: Appendices and Index | 277 |
| Appendix A WiMAX Security | 279 |
| Appendix B Setting Up Your Computer's IP Address | 283 |
| Appendix C Wireless LANs | 311 |
| Appendix D Pop-up Windows, JavaScripts and Java Permissions | 327 |
| Appendix E IP Addresses and Subnetting | 337 |
| Appendix F Importing Certificates | 349 |
| Appendix G SIP Passthrough..... | 381 |
| Appendix H Common Services | 383 |
| Appendix I Legal Information..... | 387 |
| Appendix J Customer Support | 391 |
| Index..... | 399 |

List of Figures

| | |
|---|----|
| Figure 1 The IDU/ODU Setup | 31 |
| Figure 2 WiFi Access Point | 32 |
| Figure 3 WiMAX Device and Base Station | 32 |
| Figure 4 WiMAX Device's VoIP Features - Peer-to-Peer Calls | 33 |
| Figure 5 WiMAX Device's VoIP Features - Calls via VoIP Service Provider | 33 |
| Figure 6 The WiMAX Device's LEDs | 34 |
| Figure 7 Main Screen | 43 |
| Figure 8 Select a Mode | 47 |
| Figure 9 Internet Connection Wizard > System Information | 48 |
| Figure 10 Internet Connection Wizard > Wireless LAN Screen | 49 |
| Figure 11 Internet Connection Wizard > Basic (WEP) Screen | 51 |
| Figure 12 Internet Connection Wizard > Extended (WPA-PSK) Screen | 53 |
| Figure 13 Internet Connection Wizard > Authentication Settings Screen | 54 |
| Figure 14 Internet Connection Wizard > IP Address | 56 |
| Figure 15 Internet Connection Wizard > IP Address Assignment | 57 |
| Figure 16 Select a Mode | 59 |
| Figure 17 VoIP Connection > First Voice Account Settings | 60 |
| Figure 18 VoIP Connection > SIP Registration Test | 61 |
| Figure 19 VoIP Connection > SIP Registration Fail | 62 |
| Figure 20 VoIP Connection > Finish | 63 |
| Figure 21 SETUP > Set IP Address | 68 |
| Figure 22 SETUP > DHCP Client | 69 |
| Figure 23 SETUP > Time Setting | 70 |
| Figure 24 ADVANCED > LAN Configuration > DHCP Setup | 76 |
| Figure 25 ADVANCED > LAN Configuration > Static DHCP | 78 |
| Figure 26 ADVANCED > LAN Configuration > IP Alias | 79 |
| Figure 27 Advanced > LAN Configuration > IP Static Route | 81 |
| Figure 28 Advanced > LAN Configuration > IP Static Route Setup | 82 |
| Figure 29 ADVANCED > LAN Configuration > Advanced | 83 |
| Figure 30 WiMax: Mobile Station | 90 |
| Figure 31 WiMAX: Multiple Mobile Stations | 90 |
| Figure 32 Using an AAA Server | 91 |
| Figure 33 Traffic Redirect WAN Setup | 91 |
| Figure 34 Traffic Redirect LAN Setup | 92 |
| Figure 35 ADVANCED > WAN Configuration > Internet Connection | 93 |
| Figure 36 ADVANCED > WAN Configuration > WiMAX Configuration | 96 |
| Figure 37 Frequency Ranges | 97 |
| Figure 38 Completing the WiMAX Frequency Screen | 99 |

| | | |
|-----------|---|-----|
| Figure 39 | ADVANCED > WAN Configuration > Traffic Redirect | 99 |
| Figure 40 | ADVANCED > WAN Configuration > Advanced | 101 |
| Figure 41 | ADVANCED > Wi-Fi Configuration > General | 104 |
| Figure 42 | ADVANCED > Wi-Fi Configuration > WPA/WPA2 Options | 106 |
| Figure 43 | ADVANCED > Wi-Fi Configuration > WPA-PSK/WPA2-PSK Options | 107 |
| Figure 44 | ADVANCED > WAN Configuration > WiMAX Configuration | 109 |
| Figure 45 | ADVANCED > WAN Configuration > Traffic Redirect | 110 |
| Figure 46 | VPN Transport Example | 113 |
| Figure 47 | Identifying Users | 115 |
| Figure 48 | ADVANCED > VPN Transport > General | 116 |
| Figure 49 | Pseudowire Mapping | 117 |
| Figure 50 | VPLS Tunneling | 118 |
| Figure 51 | ADVANCED > VPN Transport > Customer Interface | 118 |
| Figure 52 | ADVANCED > VPN Transport > Customer Interface Setup | 120 |
| Figure 53 | Ethernet Pseudowire Settings Example | 121 |
| Figure 54 | Advance > VPN Transport > Ethernet Pseudowire | 121 |
| Figure 55 | ADVANCED > VPN Transport > Ethernet Pseudowire Setup | 123 |
| Figure 56 | ADVANCED > VPN Transport > Statistics | 124 |
| Figure 57 | ADVANCED > NAT Configuration > General | 125 |
| Figure 58 | Multiple Servers Behind NAT Example | 127 |
| Figure 59 | ADVANCED > NAT Configuration > Port Forwarding | 127 |
| Figure 60 | ADVANCED > NAT Configuration > Port Forwarding > Rule Setup | 129 |
| Figure 61 | ADVANCED > NAT Configuration > Trigger Port | 130 |
| Figure 62 | Trigger Port Forwarding Example | 131 |
| Figure 63 | ADVANCED > NAT Configuration > ALG | 133 |
| Figure 64 | ADVANCED > System Configuration > General | 137 |
| Figure 65 | ADVANCED > System Configuration > Dynamic DNS | 139 |
| Figure 66 | ADVANCED > System Configuration > Firmware | 140 |
| Figure 67 | ADVANCED > System Configuration > Configuration | 142 |
| Figure 68 | ADVANCED > System Configuration > Restart | 143 |
| Figure 69 | VOICE > Service Configuration > SIP Setting | 149 |
| Figure 70 | STUN | 151 |
| Figure 71 | VOICE > Service Configuration > SIP Settings > Advanced | 153 |
| Figure 72 | VOICE > Service Configuration > QoS | 158 |
| Figure 73 | SIP User Agent | 160 |
| Figure 74 | SIP Proxy Server | 161 |
| Figure 75 | SIP Redirect Server | 162 |
| Figure 76 | DiffServ: Differentiated Service Field | 163 |
| Figure 77 | VOICE > Phone > Analog Phone | 166 |
| Figure 78 | VOICE > Phone > Analog Phone > Advanced | 168 |
| Figure 79 | VOICE > Phone > Common | 169 |
| Figure 80 | VOICE > Phone > Region | 170 |
| Figure 81 | VOICE > Phone Book > Incoming Call Policy | 176 |

| | |
|--|-----|
| Figure 82 VOICE > Phone Book > Speed Dial | 178 |
| Figure 83 TOOLS > Certificates > My Certificates | 184 |
| Figure 84 TOOLS > Certificates > My Certificates > Create | 186 |
| Figure 85 TOOLS > Certificates > My Certificates > Edit | 189 |
| Figure 86 TOOLS > Certificates > My Certificates > Import | 192 |
| Figure 87 TOOLS > Certificates > Trusted CAs | 193 |
| Figure 88 TOOLS > Certificates > Trusted CAs > Edit | 195 |
| Figure 89 TOOLS > Certificates > Trusted CAs > Import | 198 |
| Figure 90 Remote Host Certificates | 201 |
| Figure 91 Certificate Details | 201 |
| Figure 92 Firewall Rule Directions | 204 |
| Figure 93 Ideal Firewall Setup | 205 |
| Figure 94 TOOLS > Firewall > Firewall Setting | 206 |
| Figure 95 TOOLS > Firewall > Service Setting | 207 |
| Figure 96 “Triangle Route” Problem | 210 |
| Figure 97 IP Alias | 211 |
| Figure 98 TOOLS > Content Filter > Filter | 214 |
| Figure 99 TOOLS > Content Filter > Schedule | 216 |
| Figure 100 TOOLS > Remote Management > WWW | 219 |
| Figure 101 TOOLS > Remote Management > Telnet | 220 |
| Figure 102 TOOLS > Remote Management > FTP | 220 |
| Figure 103 SNMP Management Model | 221 |
| Figure 104 TOOLS > Remote Management > SNMP | 223 |
| Figure 105 TOOLS > Remote Management > DNS | 224 |
| Figure 106 TOOLS > Remote Management > Security | 225 |
| Figure 107 TOOLS > Logs > View Logs | 229 |
| Figure 108 TOOLS > Logs > Log Settings | 231 |
| Figure 109 TOOLS > UPnP | 244 |
| Figure 110 Network Connections | 245 |
| Figure 111 Windows Optional Networking Components Wizard | 246 |
| Figure 112 Networking Services | 246 |
| Figure 113 Network Connections | 247 |
| Figure 114 Internet Connection Properties | 247 |
| Figure 115 Internet Connection Properties: Advanced Settings | 248 |
| Figure 116 Internet Connection Properties: Advanced Settings: Add | 248 |
| Figure 117 System Tray Icon | 248 |
| Figure 118 Internet Connection Status | 249 |
| Figure 119 Network Connections | 250 |
| Figure 120 Network Connections: My Network Places | 250 |
| Figure 121 Network Connections: My Network Places: Properties: Example | 251 |
| Figure 122 Status | 253 |
| Figure 123 Packet Statistics | 258 |
| Figure 124 WiMAX Site Information | 259 |

| | |
|---|-----|
| Figure 125 DHCP Table | 260 |
| Figure 126 VoIP Statistics | 261 |
| Figure 127 WiMAX Profile | 263 |
| Figure 128 Windows XP: Start Menu | 284 |
| Figure 129 Windows XP: Control Panel | 284 |
| Figure 130 Windows XP: Control Panel > Network Connections > Properties | 285 |
| Figure 131 Windows XP: Local Area Connection Properties | 285 |
| Figure 132 Windows XP: Internet Protocol (TCP/IP) Properties | 286 |
| Figure 133 Windows Vista: Start Menu | 287 |
| Figure 134 Windows Vista: Control Panel | 287 |
| Figure 135 Windows Vista: Network And Internet | 287 |
| Figure 136 Windows Vista: Network and Sharing Center | 288 |
| Figure 137 Windows Vista: Network and Sharing Center | 288 |
| Figure 138 Windows Vista: Local Area Connection Properties | 289 |
| Figure 139 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties | 290 |
| Figure 140 Mac OS X 10.4: Apple Menu | 291 |
| Figure 141 Mac OS X 10.4: System Preferences | 291 |
| Figure 142 Mac OS X 10.4: Network Preferences | 292 |
| Figure 143 Mac OS X 10.4: Network Preferences > TCP/IP Tab. | 292 |
| Figure 144 Mac OS X 10.4: Network Preferences > Ethernet | 293 |
| Figure 145 Mac OS X 10.4: Network Utility | 294 |
| Figure 146 Mac OS X 10.5: Apple Menu | 295 |
| Figure 147 Mac OS X 10.5: Systems Preferences | 295 |
| Figure 148 Mac OS X 10.5: Network Preferences > Ethernet | 296 |
| Figure 149 Mac OS X 10.5: Network Preferences > Ethernet | 297 |
| Figure 150 Mac OS X 10.5: Network Utility | 298 |
| Figure 151 Ubuntu 8: System > Administration Menu | 299 |
| Figure 152 Ubuntu 8: Network Settings > Connections | 299 |
| Figure 153 Ubuntu 8: Administrator Account Authentication | 300 |
| Figure 154 Ubuntu 8: Network Settings > Connections | 300 |
| Figure 155 Ubuntu 8: Network Settings > Properties | 301 |
| Figure 156 Ubuntu 8: Network Settings > DNS | 302 |
| Figure 157 Ubuntu 8: Network Tools | 303 |
| Figure 158 openSUSE 10.3: K Menu > Computer Menu | 304 |
| Figure 159 openSUSE 10.3: K Menu > Computer Menu | 305 |
| Figure 160 openSUSE 10.3: YaST Control Center | 305 |
| Figure 161 openSUSE 10.3: Network Settings | 306 |
| Figure 162 openSUSE 10.3: Network Card Setup | 307 |
| Figure 163 openSUSE 10.3: Network Settings | 308 |
| Figure 164 openSUSE 10.3: KNetwork Manager | 309 |
| Figure 165 openSUSE: Connection Status - KNetwork Manager | 309 |
| Figure 166 Peer-to-Peer Communication in an Ad-hoc Network | 311 |
| Figure 167 Basic Service Set | 312 |

| | |
|---|-----|
| Figure 168 Infrastructure WLAN | 313 |
| Figure 169 RTS/CTS | 314 |
| Figure 170 WPA(2) with RADIUS Application Example | 323 |
| Figure 171 WPA(2)-PSK Authentication | 324 |
| Figure 172 Pop-up Blocker | 327 |
| Figure 173 Internet Options: Privacy | 328 |
| Figure 174 Internet Options: Privacy | 329 |
| Figure 175 Pop-up Blocker Settings | 330 |
| Figure 176 Internet Options: Security | 331 |
| Figure 177 Security Settings - Java Scripting | 332 |
| Figure 178 Security Settings - Java | 333 |
| Figure 179 Java (Sun) | 334 |
| Figure 180 Mozilla Firefox: TOOLS > Options | 334 |
| Figure 181 Mozilla Firefox Content Security | 335 |
| Figure 182 Network Number and Host ID | 338 |
| Figure 183 Subnetting Example: Before Subnetting | 341 |
| Figure 184 Subnetting Example: After Subnetting | 342 |
| Figure 185 Conflicting Computer IP Addresses Example | 347 |
| Figure 186 Conflicting Computer IP Addresses Example | 347 |
| Figure 187 Conflicting Computer and Router IP Addresses Example | 348 |
| Figure 188 Internet Explorer 7: Certification Error | 350 |
| Figure 189 Internet Explorer 7: Certification Error | 350 |
| Figure 190 Internet Explorer 7: Certificate Error | 351 |
| Figure 191 Internet Explorer 7: Certificate | 351 |
| Figure 192 Internet Explorer 7: Certificate Import Wizard | 352 |
| Figure 193 Internet Explorer 7: Certificate Import Wizard | 352 |
| Figure 194 Internet Explorer 7: Certificate Import Wizard | 353 |
| Figure 195 Internet Explorer 7: Select Certificate Store | 353 |
| Figure 196 Internet Explorer 7: Certificate Import Wizard | 354 |
| Figure 197 Internet Explorer 7: Security Warning | 354 |
| Figure 198 Internet Explorer 7: Certificate Import Wizard | 355 |
| Figure 199 Internet Explorer 7: Website Identification | 355 |
| Figure 200 Internet Explorer 7: Public Key Certificate File | 356 |
| Figure 201 Internet Explorer 7: Open File - Security Warning | 356 |
| Figure 202 Internet Explorer 7: Tools Menu | 357 |
| Figure 203 Internet Explorer 7: Internet Options | 357 |
| Figure 204 Internet Explorer 7: Certificates | 358 |
| Figure 205 Internet Explorer 7: Certificates | 358 |
| Figure 206 Internet Explorer 7: Root Certificate Store | 358 |
| Figure 207 Firefox 2: Website Certified by an Unknown Authority | 360 |
| Figure 208 Firefox 2: Page Info | 361 |
| Figure 209 Firefox 2: Tools Menu | 362 |
| Figure 210 Firefox 2: Options | 362 |

| | |
|---|-----|
| Figure 211 Firefox 2: Certificate Manager | 363 |
| Figure 212 Firefox 2: Select File | 363 |
| Figure 213 Firefox 2: Tools Menu | 364 |
| Figure 214 Firefox 2: Options | 364 |
| Figure 215 Firefox 2: Certificate Manager | 365 |
| Figure 216 Firefox 2: Delete Web Site Certificates | 365 |
| Figure 217 Opera 9: Certificate signer not found | 366 |
| Figure 218 Opera 9: Security information | 367 |
| Figure 219 Opera 9: Tools Menu | 368 |
| Figure 220 Opera 9: Preferences | 369 |
| Figure 221 Opera 9: Certificate manager | 370 |
| Figure 222 Opera 9: Import certificate | 370 |
| Figure 223 Opera 9: Install authority certificate | 371 |
| Figure 224 Opera 9: Install authority certificate | 371 |
| Figure 225 Opera 9: Tools Menu | 372 |
| Figure 226 Opera 9: Preferences | 372 |
| Figure 227 Opera 9: Certificate manager | 373 |
| Figure 228 Konqueror 3.5: Server Authentication | 374 |
| Figure 229 Konqueror 3.5: Server Authentication | 374 |
| Figure 230 Konqueror 3.5: KDE SSL Information | 375 |
| Figure 231 Konqueror 3.5: Public Key Certificate File | 376 |
| Figure 232 Konqueror 3.5: Certificate Import Result | 376 |
| Figure 233 Konqueror 3.5: Kleopatra | 376 |
| Figure 234 Konqueror 3.5: Settings Menu | 378 |
| Figure 235 Konqueror 3.5: Configure | 378 |

List of Tables

| | |
|--|-----|
| Table 1 Common Icons | 5 |
| Table 2 The WiMAX Device | 34 |
| Table 3 Main > Icons | 40 |
| Table 4 Main | 42 |
| Table 5 Main > Icons | 43 |
| Table 6 Main | 44 |
| Table 7 Internet Connection Wizard > System Information | 48 |
| Table 8 Internet Connection Wizard > Wireless LAN Screen | 49 |
| Table 9 Internet Connection Wizard > Basic (WEP) Screen | 52 |
| Table 10 Internet Connection Wizard > Extended (WPA-PSK) Screen | 53 |
| Table 11 Internet Connection Wizard > Authentication Settings Screen | 54 |
| Table 12 Internet Connection Wizard > IP Address | 56 |
| Table 13 Internet Connection Wizard > IP Address | 58 |
| Table 14 VoIP Connection > First Voice Account Settings | 60 |
| Table 15 SETUP > Set IP Address | 69 |
| Table 16 SETUP > Set IP Address | 69 |
| Table 17 SETUP > DHCP Client | 70 |
| Table 18 Pre-defined NTP Time Servers | 71 |
| Table 19 ADVANCED > LAN Configuration > DHCP Setup | 77 |
| Table 20 ADVANCED > LAN Configuration > Static DHCP | 78 |
| Table 21 ADVANCED > LAN Configuration > IP Alias | 79 |
| Table 22 Advanced > LAN Configuration > IP Static Route | 81 |
| Table 23 Advanced > LAN Configuration > IP Static Route | 81 |
| Table 24 Management > Static Route > IP Static Route > Edit | 82 |
| Table 25 ADVANCED > LAN Configuration > Other Settings | 83 |
| Table 26 ADVANCED > WAN Configuration > Internet Connection > ISP Parameters for Internet Access 93 | |
| Table 27 Radio Frequency Conversion | 96 |
| Table 28 ADVANCED > WAN Configuration > WiMAX Configuration | 96 |
| Table 29 DL Frequency Example Settings | 98 |
| Table 30 ADVANCED > WAN Configuration > Traffic Redirect | 100 |
| Table 31 ADVANCED > WAN Configuration > Advanced | 101 |
| Table 32 ADVANCED > Wi-Fi Configuration > General | 104 |
| Table 33 ADVANCED > Wi-Fi Configuration > General | 107 |
| Table 34 ADVANCED > Wi-Fi Configuration > General | 108 |
| Table 35 ADVANCED > WAN Configuration > WiMAX Configuration | 109 |
| Table 36 ADVANCED > Wi-Fi Configuration > Advanced | 110 |
| Table 37 ADVANCED > VPN Transport > General | 116 |

| | | |
|----------|---|-----|
| Table 38 | Advanced> VPN Transport > Customer Interface | 119 |
| Table 39 | ADVANCED > VPN Transport > Customer Interface | 119 |
| Table 40 | ADVANCED > VPN Transport > Customer Interface Setup | 120 |
| Table 41 | Advanced> VPN Transport > Customer Interface | 122 |
| Table 42 | ADVANCED > VPN Transport > Ethernet Pseudowire | 122 |
| Table 43 | ADVANCED > VPN Transport > Ethernet Pseudowire Setup | 123 |
| Table 44 | ADVANCED > VPN Transport > Statistics | 124 |
| Table 45 | ADVANCED > NAT Configuration > General | 126 |
| Table 46 | Advanced> VPN Transport > Customer Interface | 128 |
| Table 47 | ADVANCED > NAT Configuration > Port Forwarding | 128 |
| Table 48 | ADVANCED > NAT Configuration > Port Forwarding > Rule Setup | 129 |
| Table 49 | ADVANCED > NAT Configuration > Trigger Port | 130 |
| Table 50 | ADVANCED > NAT Configuration > ALG | 133 |
| Table 51 | ADVANCED > System Configuration > General | 137 |
| Table 52 | ADVANCED > System Configuration > Dynamic DNS | 139 |
| Table 53 | ADVANCED > System Configuration > Firmware | 141 |
| Table 54 | ADVANCED > System Configuration > Configuration | 142 |
| Table 55 | ADVANCED > System Configuration > Firmware | 143 |
| Table 56 | VOICE > Service Configuration > SIP Setting | 150 |
| Table 57 | VOICE > Service Configuration > SIP Settings > Advanced | 153 |
| Table 58 | Custom Tones Details | 156 |
| Table 59 | VOICE > Service Configuration > QoS | 158 |
| Table 60 | SIP Call Progression | 159 |
| Table 61 | VOICE > Phone > Analog Phone | 167 |
| Table 62 | VOICE > Phone > Analog Phone > Advanced | 168 |
| Table 63 | VOICE > Phone > Common | 169 |
| Table 64 | VOICE > Phone > Region | 170 |
| Table 65 | European Type Flash Key Commands | 171 |
| Table 66 | USA Type Flash Key Commands | 173 |
| Table 67 | VOICE > Phone Book > Incoming Call Policy | 176 |
| Table 68 | Advanced> LAN Configuration > IP Static Route | 178 |
| Table 69 | VOICE > Phone Book > Speed Dial | 179 |
| Table 70 | TOOLS > Certificates > My Certificates | 184 |
| Table 71 | TOOLS > Certificates > My Certificates | 184 |
| Table 72 | TOOLS > Certificates > My Certificates > Create | 187 |
| Table 73 | TOOLS > Certificates > My Certificates > Edit | 190 |
| Table 74 | TOOLS > Certificates > My Certificates > Import | 192 |
| Table 75 | TOOLS > Certificates > Trusted CAs | 193 |
| Table 76 | TOOLS > Certificates > Trusted CAs | 193 |
| Table 77 | TOOLS > Certificates > Trusted CAs > Edit | 195 |
| Table 78 | TOOLS > Certificates > Trusted CAs Import | 198 |
| Table 79 | TOOLS > Firewall > Firewall Setting | 206 |
| Table 80 | TOOLS > Firewall > Service Setting | 207 |

| | |
|---|-----|
| Table 81 TOOLS > Content Filter > Filter | 215 |
| Table 82 TOOLS > Content Filter > Schedule | 216 |
| Table 83 Remote Management | 217 |
| Table 84 TOOLS > Remote Management > WWW | 219 |
| Table 85 TOOLS > Remote Management > Telnet | 220 |
| Table 86 TOOLS > Remote Management > FTP | 221 |
| Table 87 SNMP Traps | 222 |
| Table 88 TOOLS > Remote Management > SNMP | 223 |
| Table 89 TOOLS > Remote Management > DNS | 224 |
| Table 90 TOOLS > Remote Management > Security | 225 |
| Table 91 Syslog Logs | 228 |
| Table 92 RFC-2408 ISAKMP Payload Types | 228 |
| Table 93 TOOLS > Logs > View Logs | 229 |
| Table 94 TOOLS > Logs > Log Settings | 231 |
| Table 95 System Error Logs | 233 |
| Table 96 System Maintenance Logs | 233 |
| Table 97 Access Control Logs | 234 |
| Table 98 TCP Reset Logs | 234 |
| Table 99 Packet Filter Logs | 235 |
| Table 100 ICMP Logs | 235 |
| Table 101 PPP Logs | 236 |
| Table 102 UPnP Logs | 236 |
| Table 103 Content Filtering Logs | 236 |
| Table 104 Attack Logs | 237 |
| Table 105 Remote Management Logs | 238 |
| Table 106 ICMP Notes | 239 |
| Table 107 SIP Logs | 240 |
| Table 108 RTP Logs | 240 |
| Table 109 FSM Logs: Caller Side | 240 |
| Table 110 FSM Logs: Callee Side | 240 |
| Table 111 Lifeline Logs | 241 |
| Table 112 TOOLS > UPnP | 245 |
| Table 113 Status | 254 |
| Table 114 Packet Statistics | 258 |
| Table 115 WiMAX Site Information | 259 |
| Table 116 DHCP Table | 260 |
| Table 117 VoIP Statistics | 261 |
| Table 118 The WiMAX Profile Screen | 263 |
| Table 119 IDU Hardware Specifications | 275 |
| Table 120 Indoor Wireless LAN Specification | 275 |
| Table 121 ODU Hardware Specifications | 276 |
| Table 122 Outdoor Wireless LAN Specification | 276 |
| Table 123 IEEE 802.11g | 316 |

List of Tables

| | |
|---|-----|
| Table 124 Wireless Security Levels | 316 |
| Table 125 Comparison of EAP Authentication Types | 320 |
| Table 126 Wireless Security Relational Matrix | 324 |
| Table 127 IP Address Network Number and Host ID Example | 338 |
| Table 128 Subnet Masks | 339 |
| Table 129 Maximum Host Numbers | 339 |
| Table 130 Alternative Subnet Mask Notation | 340 |
| Table 131 Subnet 1 | 343 |
| Table 132 Subnet 2 | 343 |
| Table 133 Subnet 3 | 343 |
| Table 134 Subnet 4 | 343 |
| Table 135 Eight Subnets | 344 |
| Table 136 24-bit Network Number Subnet Planning | 344 |
| Table 137 16-bit Network Number Subnet Planning | 345 |
| Table 138 Commonly Used Services | 383 |

PART I

Introduction and Wizards

Getting Started (31)

Introducing the Web Configurator (37)

Internet Connection Wizard (47)

VoIP Connection Wizard (59)

Company Confidential

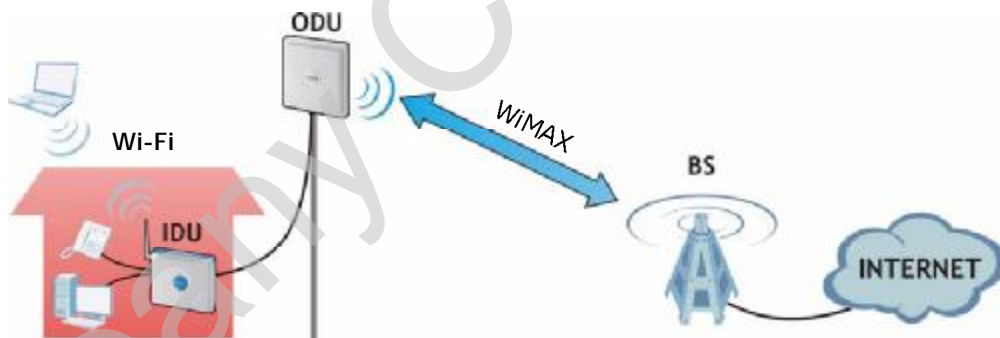
Getting Started

1.1 Overview

This product is a WiMAX subscriber station system comprised of an outdoor unit (ODU) and an indoor unit (IDU). The ODU connects to the WiMAX network while the IDU is the management point between the WiMAX network (via the ODU) and your computer/local area network. The IDU can also function as a Wi-Fi access point to the WiMAX network.

Note: This User's Guide is concerned strictly with the IDU, hereafter referred to as the "WiMAX Device". In the following figures both the IDU and ODU may be shown, but all configuration options are for the IDU alone.

Figure 1 The IDU/ODU Setup



With this product, you can:

- Connecting wirelessly to the Internet via WiMAX.
- Use a traditional analog telephone to make Internet calls using the WiMAX Device's Voice over IP (VoIP) communication capabilities.
- Set up an IEEE 802.11g wireless network (WLAN) using the WiMAX Device as an access point for the computers on your network.
- Configure firewall, content filtering and other features using the built-in browser-based Web Configurator.

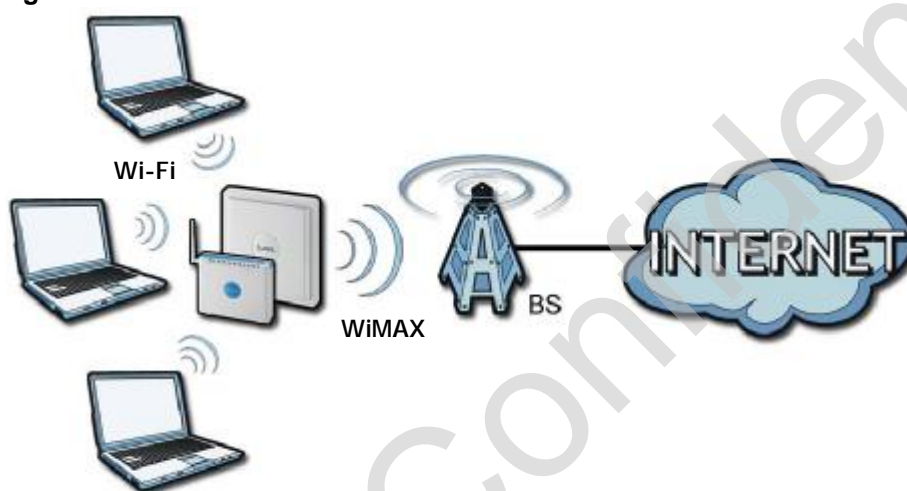
See [Chapter 23 on page 275](#) for a complete list of features for your model.

1.1.1 Wi-Fi Access Point

Activate the WiMAX Device's built-in IEEE 802.11g (also known as 'Wi-Fi' or 'WLAN') feature to allow it to function as a wireless Access Point (AP).

The illustration below shows a group of notebook computers connecting wirelessly to the WiMAX Device and then to the Internet through a WiMAX base station (BS).

Figure 2 WiFi Access Point



1.1.2 WiMAX Internet Access

Connect your computer or network directly to the WiMAX Device for WiMAX Internet access. In a wireless metropolitan area network (MAN), the WiMAX Device connects to a nearby WiMAX base station (BS) for Internet access.

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

Figure 3 WiMAX Device and Base Station



When the firewall is on, all incoming traffic from the Internet to your network is blocked unless it is initiated from your network.

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

1.1.3 Make Calls via Internet Telephony Service Provider

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

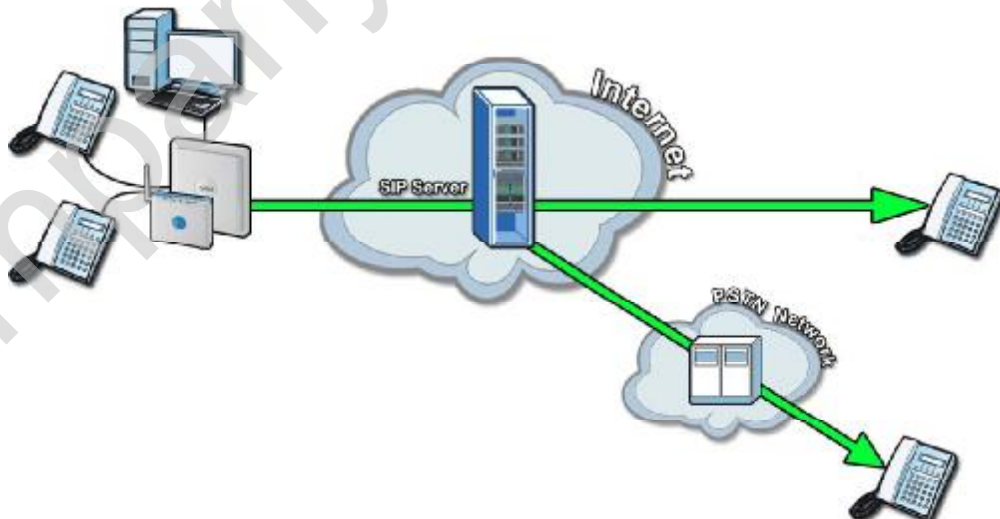
- Peer-to-Peer calls - Use the WiMAX Device to make a call directly to the recipient's IP address without using a SIP proxy server.

Figure 4 WiMAX Device's VoIP Features - Peer-to-Peer Calls



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

Figure 5 WiMAX Device's VoIP Features - Calls via VoIP Service Provider



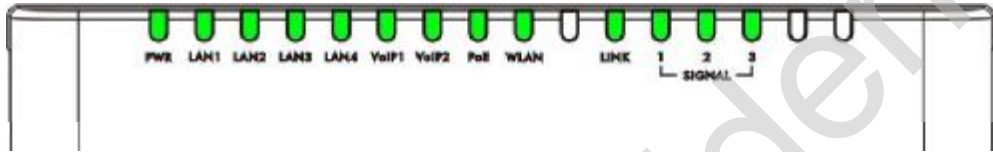
1.2 WiMAX Device Hardware

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 WiMAX Device.

Figure 6 The WiMAX Device's LEDs



The following table describes your WiMAX Device's LEDs (from right to left).

Table 2 The WiMAX Device

| LED | STATE | DESCRIPTION |
|----------|-----------------|---|
| PWR | Off | The WiMAX Device is not receiving power. |
| | Red | The WiMAX Device is receiving power but has been unable to start up correctly or is not receiving enough power. See the Troubleshooting section for more information. |
| | Solid Green | The WiMAX Device is receiving power and functioning correctly. |
| | Blinking Green | The WiMAX Device is performing a self-test. |
| LAN 1~4 | Off | The LAN is not connected. |
| | Green | The WiMAX Device has a successful Local Area Network (Ethernet) connection. |
| | Blinking Green | The WiMAX Device is the process of transmitting and receiving data. |
| VoIP 1~2 | Off | No SIP account is registered, or the WiMAX Device is not receiving power. |
| | Green | A SIP account is registered. |
| | Blinking Green | 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 on the SIP server. |
| | Blinking Orange | A SIP account is registered and has a voice message on the SIP server, and the phone attached to the LINE port is in use (off the hook). |

Table 2 The WiMAX Device

| LED | STATE | DESCRIPTION |
|------------|--|---|
| PoE | Off | The Power over Ethernet (PoE) link is not functioning. |
| | Green | The PoE link is functioning correctly |
| | Blinking Green | The WiMAX Device is transmitting and receiving data over the PoE link. |
| WLAN | Off | The Wi-Fi network is not operational. |
| | Green | The Wi-Fi network is operational. |
| | Blinking Green | The WiMAX Device is sending and receiving data across the Wi-Fi network. |
| LINK | Green | The WiMAX service set ID is registered and operational. |
| | Slow Blinking Green | The WiMAX Device is currently searching for a channel (approximate blink speed 1 second per). |
| | Fast Blinking Green | The WiMAX Device is currently the process of joining a WiMAX network (approximate blink speed is 0.5 second per). |
| SIGNAL 1~3 | The Signal LEDs display the Received Signal Strength Indication (RSSI) of the wireless (WiMAX) connection. | |
| | No Signal LEDS | There is no WiMAX connection. |
| | Signal 1 On | The signal strength is less than or equal to -90 dBm |
| | Signal 2 On | The signal strength is less than or equal to -80 dBm |
| | Signal 3 On | The signal strength is less than or equal to -70 dBm |

1.3 Good Habits for Managing the WiMAX Device

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

- Change your passwords regularly. Use passwords that are not easy to guess and that consist of different types of characters, such as numbers and letters.
- Write down your passwords but be sure to put them in a safe, secure place. Never store them in proximity to your computer or WiMAX Device.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the WiMAX Device becomes unstable or even crashes. If you forget your password, you will have to reset the WiMAX Device to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the WiMAX Device. You could simply restore your last configuration.

Company Confidential

Introducing the Web Configurator

2.1 Overview

The web configurator is an HTML-based management interface that allows easy device set up and management via any web browser that supports: HTML 4.0, CSS 2.0, and JavaScript 1.5, and higher. The recommended screen resolution for using the web configurator is 1024 by 768 pixels and 16-bit color, or higher.

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 many operating systems and web browsers.
- JavaScript (enabled by default in most web browsers).
- Java permissions (enabled by default in most web browsers).

See the [Appendix D on page 327](#) for more information on configuring your web browser.

2.1.1 Accessing the Web Configurator

- 1 Make sure your WiMAX Device hardware is properly connected (refer to the Quick Start Guide for more information).
- 2 Launch your web browser.
- 3 Enter "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**.



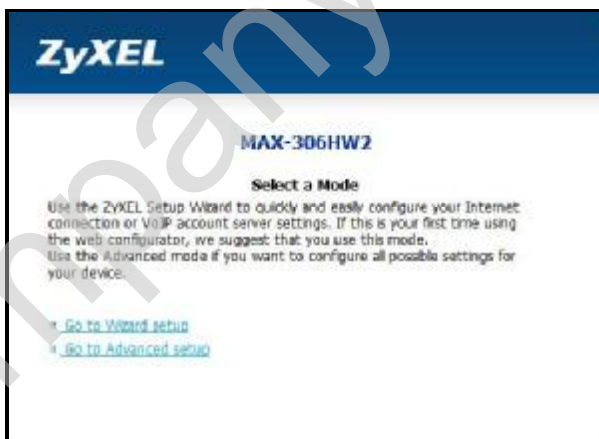
- 5 The following screen displays if you have not yet changed your password. It is highly recommended you change the default password. Enter a new password, retype it to confirm and click **Apply**; alternatively click **Ignore** to proceed to the main menu if you do not want to change the password now.



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



- 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 3 on page 47](#) 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 3 on page 40](#) for more information.
 - Click **Exit** if you want to log out.



Note: For security reasons, the WiMAX Device automatically logs you out if you do not use the web configurator for five minutes. If this happens, simply log in again.

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 WiMAX Device following the steps in your Quick Start Guide.

2.2 The Main Screen

When you first log into the web configurator, the Main screen appears. Here you can view a concise summary of your WiMAX Device connection status. This is also the default "home" page for the ZyXEL web configurator and it contains conveniently-placed shortcuts to all of the other screens.

Note: Some features in the web configurator may not be available depending on your firmware version and/or configuration.

Table 3 Main > Icons








| ICON | DESCRIPTION |
|---|---|
|  | <p>MAIN</p> <p>Click to return to the Main screen.</p> |
|  | <p>SETUP</p> <p>Click to go the Setup screen, where you can configure LAN, DHCP and WAN settings.</p> |
|  | <p>ADVANCED</p> <p>Click to go to the Advanced screen, where you can configure features like Port Forwarding and Triggering, SNTP and so on.</p> |

Table 3 Main > Icons (continued)

| ICON | DESCRIPTION |
|---|---|
|  | <p>VOICE</p> <p>Click to go to the Voice screen, where you can configure your voice service and phone settings.</p> |
|  | <p>TOOLS</p> <p>Click to go the Tools screen, where you can configure your firewall, QoS, and content filter, among other things.</p> |
|  | <p>STATUS</p> <p>Click to go to the Status screen, where you can view status and statistical information for all connections and interfaces.</p> |
|  | <p>Strength Indicator</p> <p>Displays a visual representation of the quality of your WiMAX connection.</p> <ul style="list-style-type: none"> • Disconnected - Zero bars • Poor reception - One bar • Good reception - Two bars • Excellent reception - Three bars |

The following table describes the labels in this screen.

Table 4 Main

| LABEL | DESCRIPTION |
|-------------------------|---|
| Help | Click to open the web configurator's online help. |
| Wizard | Click to run the Internet Connection and VoIP Connection Setup Wizard. All of the settings that you can configure in this wizard are also available in these web configurator screens. |
| Logout | Click to log out of the web configurator. Note: This does not log you off the WiMAX network, it simply logs you out of the WiMAX Device's browser-based configuration interface. |
| WiMAX Connection Status | This field indicates the current status of your WiMAX connection. Status messages are as follows: <ul style="list-style-type: none"> • Connected - Indicates that the WiMAX Device is connected to the WiMAX network. Use the Strength Indicator icon to determine the quality of your network connection. • Disconnected - Indicates that the WiMAX Device is not connected to the WiMAX network. • DL_SYN - Indicates a download synchronization is in progress. This means the firmware is checking with the server for any updates or settings alterations. |
| Software Version | This field indicates the version number of the WiMAX Device's firmware. The version number takes the form of: <i>Version(Build),release status (candidate) Version Release Date.</i> For example: V3.60(BCC.0)c4 07/08/2008 indicates that the firmware is 3.60, build BCC.0, candidate4, released on July 08, 2008. |
| Version Date | This field indicates the exact date and time the current firmware was compiled. |
| System Uptime | This field indicates how long the WiMAX Device has been on. This resets every time you shut the device down or restart it. |
| WiMAX Uptime | This field indicates how long the WiMAX Device has been connected to the WiMAX network. This resets every time you disconnect from the WiMAX network, shut the device down, or restart it. |
| Voice 1 | This field indicates the number and receiver status of the first voice account. |

Figure 7 Main Screen



The following table describes the icons in this screen.

Table 5 Main > Icons








| ICON | DESCRIPTION |
|---|--|
|  | MAIN Click to return to the Main screen. |
|  | SETUP Click to go the Setup screen, where you can configure LAN and DHCP settings. |
|  | ADVANCED Click to go to the Advanced screen, where you can configure features like Port Forwarding and Triggering, SNTP and so on. |
|  | VOICE Click to go to the Voice screen, where you can configure your voice service and phone settings. |
|  | TOOLS Click to go the Tools screen, where you can configure your firewall, QoS, and content filter, among other things. |

Table 5 Main > Icons (continued)

| ICON | DESCRIPTION |
|---|---|
|  | <p>STATUS</p> <p>Click to go to the Status screen, where you can view status and statistical information for all connections and interfaces.</p> |
|  | <p>Strength Indicator</p> <p>Displays a visual representation of the quality of your WiMAX connection.</p> <ul style="list-style-type: none"> • Disconnected - Zero bars • Poor reception - One bar • Good reception - Two bars • Excellent reception - Three bars |

The following table describes the labels in this screen.

Table 6 Main

| LABEL | DESCRIPTION |
|-------------------------|--|
| Help | Click to open the web configurator's online help. |
| Wizard | Click to run the Internet Connection and VoIP Connection Setup Wizard. All of the settings that you can configure in this wizard are also available in these web configurator screens. |
| Logout | <p>Click to log out of the web configurator.</p> <p>Note: This does not log you off the WiMAX network, it simply logs you out of the WiMAX Device's browser-based configuration interface.</p> |
| WiMAX Connection Status | <p>This field indicates the current status of your WiMAX connection.</p> <p>Status messages are as follows:</p> <ul style="list-style-type: none"> • Connected - Indicates that the WiMAX Device is connected to the WiMAX network. Use the Strength Indicator icon to determine the quality of your network connection. • Disconnected - Indicates that the WiMAX Device is not connected to the WiMAX network. • DL_SYN - Indicates a download synchronization is in progress. This means the firmware is checking with the server for any updates or settings alterations. |
| Software Version | <p>This field indicates the version number of the WiMAX Device's firmware. The version number takes the form of: <i>Version(Build), release status (candidate) Version Release Date</i>.</p> <p>For example: V3.60(BCC.0)c4 07/08/2009 indicates that the firmware is 3.60, build BCC.0, candidate 4, released on July 08, 2009.</p> |
| Version Date | This field indicates the exact date and time the current firmware was compiled. |
| System Uptime | This field indicates how long the WiMAX Device has been on. This resets every time you shut the device down or restart it. |

Table 6 Main (continued)

| LABEL | DESCRIPTION |
|--------------|--|
| WiMAX Uptime | This field indicates how long the WiMAX Device has been connected to the WiMAX network. This resets every time you disconnect from the WiMAX network, shut the device down, or restart it. |
| Voice 1 | This field indicates the number and receiver status of the first voice account. |
| Voice 2 | This field indicates the number and receiver status of the second voice account. |

Company Confidential

Internet Connection Wizard

3.1 Overview

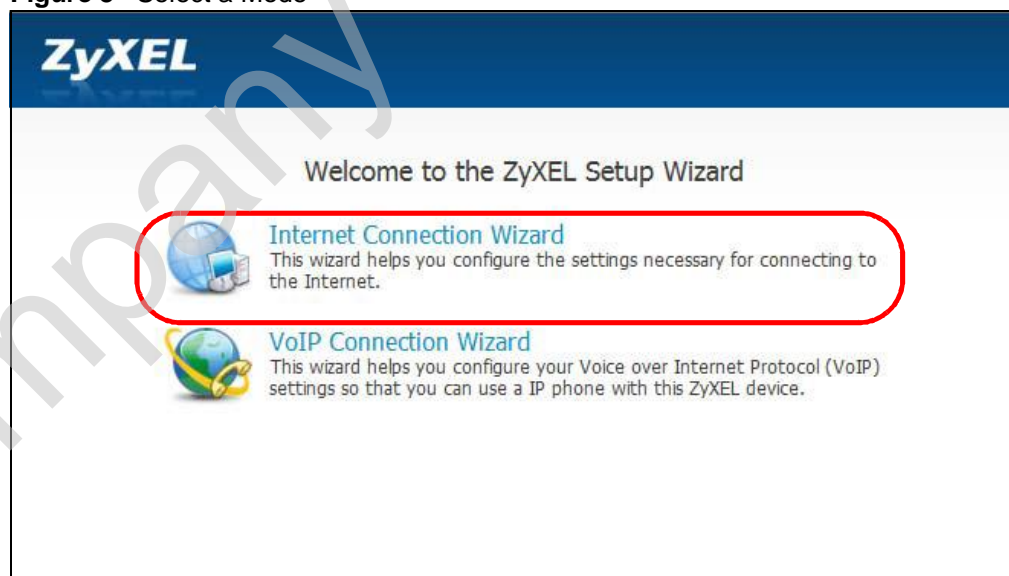
This chapter provides information on the Internet Connection Wizard screens. The wizard guides you through several steps in which you can configure your most basic (and essential) Internet settings.

Note: Screens are presented here in order of appearance as you work through the Internet Connection Wizard. To get to any particular screen, you must first navigate through the ones that came before it.

3.1.1 Welcome to the ZyXEL Setup Wizard

This is the welcome screen for the ZyXEL Setup Wizard. You can choose to either configure your Internet connection or your VoIP connection.

Figure 8 Select a Mode



Select Internet Connection Wizard to begin.

3.1.2 System Information

This Internet Connection Wizard screen allows you to configure your WiMAX Device's system information. The settings here correspond to the **ADVANCED > System Configuration > General** screen (Section 11.2 on page 137).

Figure 9 Internet Connection Wizard > System Information

The following table describes the labels in this screen.

Table 7 Internet Connection Wizard > System Information

| LABEL | DESCRIPTION |
|-------------|--|
| System Name | System Name is a unique name to identify the WiMAX 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 to display the previous screen. |
| Next | Click to proceed to the next screen. |
| Exit | Click to close the wizard without saving. |

3.1.3 Wireless LAN

This Internet Connection Wizard screen follows the **System Information** screen and allows you to configure your wireless network's security settings. The settings here correspond to the **Advanced > WiFi Configuration > General** screen, **Security** sub-section ([Section 8.2 on page 104](#)).

Note: The **Security** option you select here determines which screen comes next.

Figure 10 Internet Connection Wizard > Wireless LAN Screen

The following table describes the labels in this screen.

Table 8 Internet Connection Wizard > Wireless LAN Screen

| LABEL | DESCRIPTION |
|-------------------|---|
| Name (SSID) | This is the name you assign to your network and the name that appears in a wireless client's network selection options. Note: "SSID" means Service Set Identifier and is the technical term for a wireless network name. |
| Channel Selection | This is the radio channel on which the device broadcasts. If there are other networks in range, select a channel number than is not already in use in order to minimize possible cross-channel interference. |

Table 8 Internet Connection Wizard > Wireless LAN Screen (continued)

| LABEL | DESCRIPTION |
|----------|---|
| Security | <p>Select an encryption method for your network. This is to discourage people from accessing your network without authorization. Choose an encryption method compatible with all of your anticipated network clients.</p> <p>Security Options are:</p> <ul style="list-style-type: none"> • None - It is not recommended that you use this setting. With no security, anyone who has a wireless device can connect to your network. • Basic (WEP) - This is a basic form of encryption. It is not recommended that you use it as it can be by-passed quite easily. However, because it is one of the original wireless encryption methods, it is the most compatible with older wireless devices. Select this option if you require the widest range of compatibility. • Extend (WPA-PSK with customized key) - This provides both improved data encryption and user authentication. Using PSK, both the WiMAX Device and the connecting client share a common password in order to validate the connection. This type of encryption, while robust, is not as strong as WPA2-PSK. Use this type of security if you do not use a RADIUS server to authenticate user credentials. • Extend (WPA2-PSK with customize key) - This is a newer, more robust version of the WPA encryption standard. It offers slightly better security. Use this option if you do not have RADIUS server on your network to verify user credentials. <p>The option you select here changes the configuration options on this screen accordingly. For details on the specific security options, see subsequent tables.</p> |
| Back | Click to display the previous screen. |
| Next | Click to proceed to the next screen. |
| Exit | Click to close the wizard without saving. |

3.1.3.1 Wireless LAN - Basic (WEP)

This screen appears as a result of selecting **Basic WEP** as your **Security** option in the previous screen. It allows you to configure WEP encryption for your wireless network. The settings here correspond to the **Advanced > WiFi Configuration > General** screen, **Security** sub-section with the **Basic (WEP)** option selected ([Section 8.2 on page 104.](#))

Figure 11 Internet Connection Wizard > Basic (WEP) Screen

WIRELESS LAN

Passphrase
Use Passphrase to automatically generates a WEP key.

Passphrase

WEP Key
WEP Encryption

64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F").
128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").

ASCII Hex

The following table describes the labels in this screen.

Table 9 Internet Connection Wizard > Basic (WEP) Screen

| LABEL | DESCRIPTION |
|----------------|--|
| Passphrase | <p>Enter a password in this field if you want to have the WiMAX Device create a unique Hex-based key for you. After entering your password, click the Generate button. The Hex-based key appears in the field below.</p> <p>Note: If you Generate a passphrase, the length of the key created is determined by the option you select in the WEP encryption field.</p> |
| WEP Encryption | <p>Select the encryption strength for your WEP-enabled network.</p> <ul style="list-style-type: none"> • 64-Bit WEP - This is the older of the two available encryption algorithms. The key is smaller and requires less computational resources to cipher/decipher. For all intents and purposes, this is irrelevant for modern computers and wireless devices. Unfortunately, this level of security is rudimentary, at best, and easily broken. You should only use in circumstances where backwards compatibility with older devices is a significant issue. • 128-Bit WEP - This represents a higher standard of security for WEP encryption. Keys are larger, require slightly more computational resources, and are more difficult to crack. If backwards compatibility for older wireless devices is a non-issue, use this level of encryption for more robust security. <p>Note: Of all the encryption types available for wireless networks, WEP is the weakest and easiest to bypass. It is recommended that you use WPA or WPA2 whenever possible.</p> |
| ASCII / Hex | <p>If you choose not to have the WiMAX Device automatically create an encryption key, you can manually enter one here either in ASCII or in Hex.</p> <p>If you choose to allow the WiMAX Device to automatically create an encryption key for you using the Passphrase field and its corresponding Generate key, then the new key appears in this field.</p> <p>Remember to record the password and distribute it to your wireless clients accordingly (and securely).</p> <p>Note: For 64-bit encryption: Enter 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F").</p> <p>Note: For 128-bit encryption: Enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").</p> |
| Back | Click to display the previous screen. |
| Next | Click to proceed to the next screen. |
| Exit | Click to close the wizard without saving. |

3.1.3.2 Wireless LAN -Extended (WPA-PSK / WPA2-PSK)

This screen appears as a result of selecting either **WPA-PSK** or **WPA2-PSK** as your **Security** option in the previous screen. It allows you to configure WPA-PSK / WPA2-PSK encryption for your wireless network. The settings here correspond to the **Advanced > WiFi Configuration > General** screen, **Security** sub-section with the **Extend** option selected ([Section 8.2 on page 104.](#))

Note: Both WPA-PSK and WPA2-PSK configuration options use this screen, with only minimal variation.

Figure 12 Internet Connection Wizard > Extended (WPA-PSK) Screen

WIRELESS LAN

WPA Pre-Shared Key Setup

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

Pre-Shared Key

The following table describes the labels in this screen.

Table 10 Internet Connection Wizard > Extended (WPA-PSK) Screen

| LABEL | DESCRIPTION |
|----------------|--|
| Pre-shared Key | <p>This is a secret password that both the WiMAX Device and the wireless client must have in common in order for the wireless client to use the network.</p> <p>As the device administrator, you can generate this key how you see fit so long as it consists of a minimum of 8 alphanumeric letters and number. However, keep in mind that the more complex the key, the more difficult it is to break. The best keys consist of both letters and numbers.</p> <p>Note: This key is used by all wireless clients on your network to authenticate their connections, so be sure to distribute it accordingly (and securely).</p> |
| Back | Click to display the previous screen. |
| Next | Click to proceed to the next screen. |
| Exit | Click to close the wizard without saving. |

3.1.4 Authentication Settings

This Internet Connection Wizard screen follows the **Wireless LAN** security setup screens and allows you to configure your Internet access settings. The settings here correspond to the **ADVANCED > WAN Configuration > Internet Connection** screen (Section 7.2 on page 93).

Figure 13 Internet Connection Wizard > Authentication Settings Screen

Authentication Settings

Enter the required settings as issued by your ISP.

User Name: myuser@asb.com

Password:

Anonymous Identity: anonymous@asb.com

PKM: PKMV2

Authentication: TTLS

TTLS Inner EAP: CHAP

Certificate: auto_generated_self_signed_cert

<Back Next > Close

The following table describes the labels in this screen.

Table 11 Internet Connection Wizard > Authentication Settings Screen

| LABEL | DESCRIPTION |
|-----------------------|---|
| Authentication | |
| User | Enter the username associated with your Internet access account. You can enter up to 61 printable ASCII characters. |
| Password | 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 11 Internet Connection Wizard > Authentication Settings Screen (continued)

| LABEL | DESCRIPTION |
|----------------|--|
| PKM | This field displays the Privacy Key Management version number. PKM provides security between the WiMAX Device and the base station. At the time of writing, the WiMAX Device supports PKMv2 only. See the WiMAX security appendix for more information. |
| Authentication | <p>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).</p> <p>Check with your service provider if you are unsure of the correct setting for your account.</p> <p>Choose from the following user authentication methods:</p> <ul style="list-style-type: none"> • TTLS (Tunnelled Transport Layer Security) • TLS (Transport Layer Security) <p>Note: Not all WiMAX Devices support TLS authentication. Check with your service provider for details.</p> |
| TTLS Inner EAP | <p>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 WiMAX Device supports the following inner authentication types:</p> <ul style="list-style-type: none"> • CHAP (Challenge Handshake Authentication Protocol) • MSCHAP (Microsoft CHAP) • MSCHAPV2 (Microsoft CHAP version 2) • PAP (Password Authentication Protocol) |
| Certificate | This is the security certificate the WiMAX Device uses to authenticate the AAA server. Use the TOOLS > Certificates > Trusted CA screen to import certificates to the WiMAX Device. |
| Back | Click to display the previous screen. |
| Next | Click to proceed to the next screen. |
| Exit | Click to close the wizard without saving. |

3.1.5 IP Address

This Internet Connection Wizard screen follows the **Authentication Settings** screen and allows you to configure the method with which your WiMAX Device acquires its IP address. The settings here correspond to the **SETUP > Set IP Address** screen ([Section 5.2 on page 68](#)).

A fixed (static) IP address is one that your ISP gives you. Your WiMAX Device uses that IP address every time you connect to the Internet. On the other hand, an automatic (dynamic) IP address is variable in that the ISP assigns you a different one each time you connect to the Internet.

Figure 14 Internet Connection Wizard > IP Address

IP Address

An IP address identifies you to the network, and you must have one to browse a local area network or surf the Internet. Your IP address is generally assigned by a network administrator or ISP. Select the option that is appropriate for your connection type.

My computer or device gets its IP address automatically from the network
 Use fixed IP address

<Back Next > Close

The following table describes the labels in this screen.

Table 12 Internet Connection Wizard > IP Address

| LABEL | DESCRIPTION |
|--|---|
| IP Address | |
| My computer or device gets its IP address automatically from the network (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. Note: Selecting this option takes you to the Setup Complete screen. |

Table 12 Internet Connection Wizard > IP Address (continued)

| LABEL | DESCRIPTION |
|----------------------|---|
| Use Fixed IP Address | Select this option to enter static IP address or a fixed IP that your ISP gives you. Note: Selecting this option takes you to the IP Address Assignment screen. |
| Back | Click to display the previous screen. |
| Next | Click to proceed to the next screen. |
| Exit | Click to close the wizard screen without saving. |

3.1.5.1 IP Address Assignment

This screen appears as a result of selecting the **Used Fixed IP Address** option in the previous screen. It allows you to configure your static WAN and DNS IP Addresses. Use the information given to you by your Internet Service Provider.

The settings for **WAN IP Address Assignment** correspond to the **Advanced > WAN Configuration > Internet Connection** screen ([Section 7.2 on page 93](#)).

The settings for **DNS Server Address Assignment** correspond to the **Advanced > LAN Configuration > DHCP Setup** screen, **DNS Server** sub-section.

Figure 15 Internet Connection Wizard > IP Address Assignment

The screenshot shows a window titled 'WAN IP Address Assignment' and 'DNS Server Address Assignment'. Under 'WAN IP Address Assignment', there are three input fields: 'My WAN IP Address', 'My WAN IP Subnet Mask', and 'Gateway IP Address', all containing '0.0.0.0'. Under 'DNS Server Address Assignment', there are three input fields: 'First DNS Server', 'Second DNS Server', and 'Third DNS Server', all containing '0.0.0.0'. At the bottom right, there are three buttons: '<Back', 'Next >', and 'Close'.

The following table describes the labels in this screen.

Table 13 Internet Connection Wizard > IP Address

| LABEL | DESCRIPTION |
|------------------------------------|--|
| WAN IP Address Assignment | |
| My WAN IP Address | Enter your ISP-assigned IP Address here. |
| 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 | Specify the IP addresses of a maximum of three DNS servers that the network can use. The WiMAX Device provides these IP addresses to DHCP clients. If you enter nothing in these fields, no DNS service will be provided by the WiMAX Device. |
| Back | Click to display the previous screen. |
| Next | Click to proceed to the next screen. |
| Exit | Click to close the wizard screen without saving. |

3.1.6 Setup Complete

Click Close to complete and save the Internet Connection Wizard settings.

Launch your web browser and navigate to www.zyxel.com. If everything was configured properly, the web page should display. You can now surf the Internet!

Refer to the rest of this guide for more detailed information on the complete range of WiMAX Device features available in the more advanced web configurator.

Note: 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 Connection Wizard

4.1 Overview

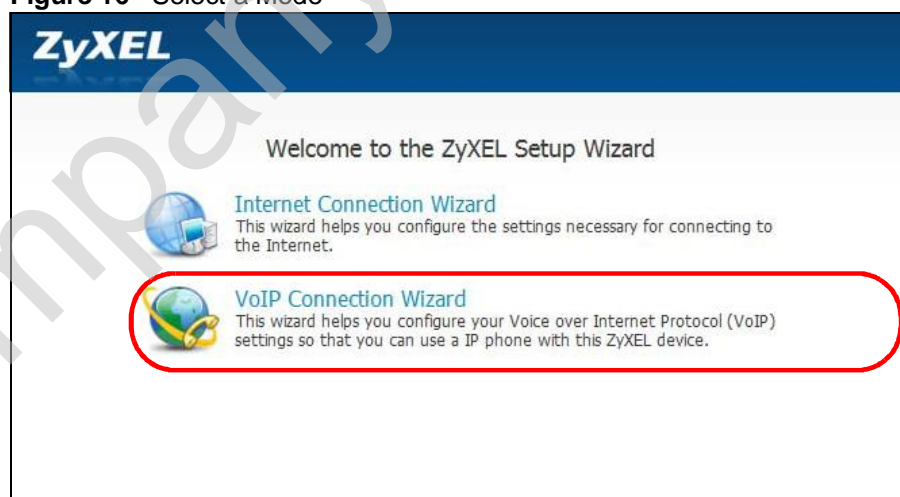
This chapter provides information on the VoIP Connection Wizard screens. The wizard guides you through several steps in which you can configure the minimum required settings for placing phone calls over the Internet. You can configure the WiMAX Device to use up to two SIP-based VoIP accounts.

Note: Screens are presented here in order of appearance as you work through either the VoIP Connection Wizard. To get to any particular screen, you must first navigate through the ones that came before it.

4.2 Welcome to the ZyXEL Setup Wizard

This is the welcome screen for the ZyXEL Setup Wizard. You can choose to either configure your Internet connection or your VoIP connection.

Figure 16 Select a Mode



Select VoIP Connection Wizard to begin.

4.2.1 First Voice Account Settings

This VoIP Connection Wizard screen allows you to configure your voice account. The settings here correspond to the **VOICE > Service Configuration > SIP Setting** screen (see [Section 12.2 on page 149](#) for more information).

Figure 17 VoIP Connection > First Voice Account Settings

The following table describes the labels in this screen

Table 14 VoIP Connection > First Voice Account Settings

| 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. |

Table 14 VoIP Connection > First Voice Account Settings (continued)

| LABEL | DESCRIPTION |
|------------------------------------|---|
| Configure the second voice account | Select this check box if you have a second SIP account that you want to use. You will need to configure the same fields as displayed on this screen for the second SIP account. |
| Back | Click to return to the previous screen. |
| Apply | Click to complete the wizard setup and save your configuration. |
| Exit | Click to close the wizard without saving your settings. |

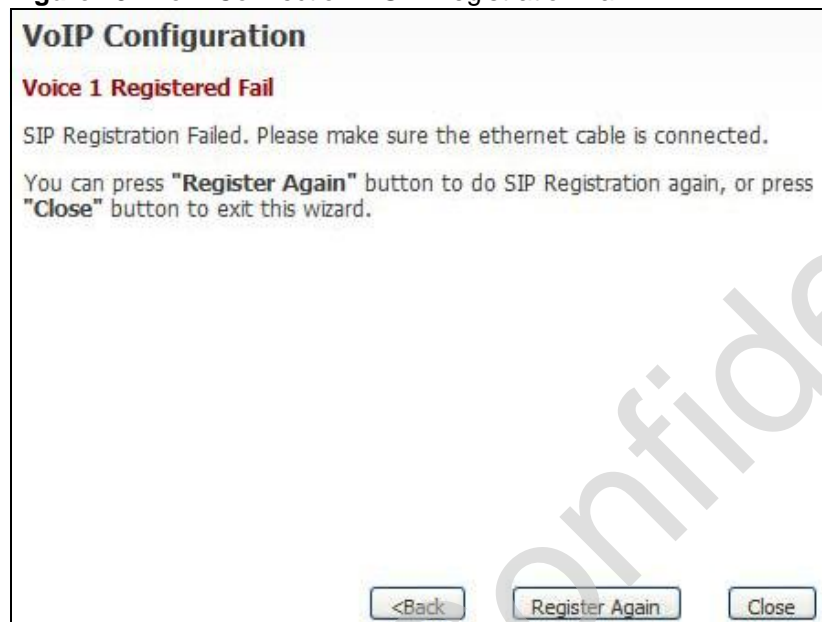
After you enter your voice account settings and click **Next**, the WiMAX Device attempts to register your SIP account with the SIP server.

Figure 18 VoIP Connection > SIP Registration Test

This screen displays if SIP account registration fails. Check your WiMAX connection using the **WiMAX Link and Strength Indicator LEDs** on the front of the WiMAX 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 19 VoIP Connection > SIP Registration Fail



4.2.2 Setup Complete

Click **Close** to complete and save the VoIP Connection settings.

Figure 20 VoIP Connection > Finish



This screen displays if your SIP account registration was successful.

Company Confidential

PART II

Basic Screens

The Main Screen (40)

The Setup Screens (67)

Company Confidential

The Setup Screens

5.1 Overview

Use these screens to configure or view LAN, DHCP Client and WAN settings.

5.1.1 What You Can Do in This Chapter

- The **Set IP Address** screen ([Section 5.2 on page 68](#)) lets you configure the WiMAX Device's IP address and subnet mask.
- The **DHCP Client** screen ([Section 5.3 on page 69](#)) lets you view a list of all connected DHCP clients.
- The **Time Setting** screen ([Section 5.4 on page 70](#)) lets you configure your WiMAX Device's time and date keeping settings.

5.1.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

LAN

A Local Area Network, or a shared communication system to which many computers are attached. A LAN, as its name implies, is limited to a local area such as a home or office environment. LANs have different topologies, the most common being the linear bus and the star configuration.

IP Address

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet Mask

The subnet mask specifies the network number portion of an IP address. Your device will compute the subnet mask automatically based on the IP Address that

you entered. You do not need to change the computer subnet mask unless you are instructed to do so.

Daytime

A network protocol used by devices for debugging and time measurement. A computer can use this protocol to set its internal clock but only if it knows in which order the year, month, and day are returned by the server. Not all servers use the same format.

Time

A network protocol for retrieving the current time from a server. The computer issuing the command compares the time on its clock to the information returned by the server, adjusts itself automatically for time zone differences, then calculates the difference and corrects itself if there has been any temporal drift.

NTP

NTP stands for Network Time Protocol. It is employed by devices connected to the Internet in order to obtain a precise time setting from an official time server. These time servers are accurate to within 200 microseconds.

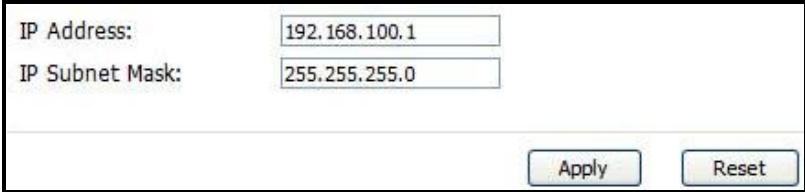
5.1.3 Before You Begin

- Make sure that you have made all the appropriate hardware connections to the WiMAX Device, as described in the Quick Start Guide.
- Make sure that you have logged in to the web configurator at least one time and changed your password from the default, as described in the Quick Start Guide.

5.2 Set IP Address

Click the **SETUP** icon in the navigation bar to set up the WiMAX Device's IP address and subnet mask. This screen displays this screen by default. If you are in any other sub-screen you can simply choose **Set IP Address** from the navigation menu on the left to open it again.

Figure 21 SETUP > Set IP Address



| | |
|---|--|
| IP Address: | <input type="text" value="192.168.100.1"/> |
| IP Subnet Mask: | <input type="text" value="255.255.255.0"/> |
| <input type="button" value="Apply"/> <input type="button" value="Reset"/> | |

The following table describes the labels in this screen.

Table 15 SETUP > Set IP Address

| LABEL | DESCRIPTION |
|----------------|---|
| IP Address | Enter the IP address of the WiMAX Device on the LAN. Note: This field is the IP address you use to access the WiMAX Device on the LAN. If the web configurator is running on a computer on the LAN, you lose access to it 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 to save your changes. |
| Reset | Click to restore your previously saved settings. |

5.3 DHCP Client

Click **SETUP > DHCP Client** to view a list of all connected DHCP clients. DHCP clients are those devices connected to the WiMAX Device, either directly with Ethernet cables or over a Wi-Fi network, and which have an IP address assigned to them by an associated DHCP server.

Figure 22 SETUP > DHCP Client

| # | IP Address | Host Name | MAC Address | Reserve |
|---|----------------|--------------|-------------------|--------------------------|
| 1 | 192.168.100.33 | TWPC13435-XP | 00:02:e3:56:16:9d | <input type="checkbox"/> |

The following table describes the labels in this screen.

Table 16 SETUP > Set IP Address

| LABEL | DESCRIPTION |
|-------------|--|
| # | This is the number of the item in this list. |
| IP Address | This indicates the IP address of the connected DHCP client device. |
| Host Name | This indicates the name of the connected DHCP client device. |
| MAC Address | Indicates the MAC address of the connected DHCP client. |
| Reserve | Indicates whether the IP address of the connected client is reserved for that client or not. |
| Apply | Click to save your changes. |
| Reset | Click to restore your previously saved settings. |

5.4 Time Setting

Click **SETUP > Time Setting** to set the date, time, and time zone for the WiMAX Device.

Figure 23 SETUP > Time Setting

The following table describes the labels in this screen.

Table 17 SETUP > DHCP Client

| LABEL | DESCRIPTION |
|-----------------------|---|
| Current Time and Date | |
| Current Time | Displays the current time according to the WiMAX Device. |
| Current Date | Displays the current time according to the WiMAX Device. |
| Time and Date Setup | |
| Manual | Select this if you want to specify the current date and time in the fields below. |
| New Time | Enter the new time in this field, and click Apply . |
| New Date | Enter the new date in this field, and click Apply . |
| Get from Time Server | Select this if you want to use a time server to update the current date and time in the WiMAX Device. |

Table 17 SETUP > DHCP Client (continued)

| LABEL | DESCRIPTION |
|---------------------|---|
| Time Protocol | Select the time service protocol that your time server uses. Check with your ISP or network administrator, or use trial-and-error to find a protocol that works. Daytime (RFC 867) - This format is day/month/year/time zone. Time (RFC 868) - This format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. NTP (RFC 1305) - This format is similar to Time (RFC 868). |
| Time Server Address | Enter the IP address or URL of your time server. Check with your ISP or network administrator if you are unsure of this information. |
| Time Zone Setup | |
| Time Zone | Select the time zone at your location. |
| Daylight Savings | Select this if your location uses daylight savings time. Daylight savings is a period from late spring to early fall when many places set their clocks ahead of normal local time by one hour to give more daytime light in the evening. |
| Start Date | Enter which hour on which day of which week of which month daylight-savings time starts. |
| End Date | Enter which hour on the which day of which week of which month daylight-savings time ends. |
| Apply | Click to save your changes. |
| Reset | Click to restore your previously saved settings. |

5.4.1 Pre-Defined NTP Time Servers List

The WiMAX Device uses a pre-defined list of NTP time servers if you do not specify a time server or it cannot synchronize with the time server you specified. It can use this list regardless of the time protocol you select.

When the WiMAX Device uses the list, it randomly selects one server and tries to synchronize with it. If the synchronization fails, then it goes through the rest of the list in order until either it is successful or all the pre-defined NTP time servers have been tried.

Table 18 Pre-defined NTP Time Servers

| |
|---------------------|
| ntp1.cs.wisc.edu |
| ntp1.gbg.netnod.se |
| ntp2.cs.wisc.edu |
| tock.usno.navy.mil |
| ntp3.cs.wisc.edu |
| ntp.cs.strath.ac.uk |
| ntp1.sp.se |

Table 18 Pre-defined NTP Time Servers (continued)

| |
|---------------------|
| time1.stupi.se |
| tick.stdtime.gov.tw |
| tock.stdtime.gov.tw |
| time.stdtime.gov.tw |

5.4.2 Resetting the Time

The WiMAX Device automatically resets the time in the following circumstances:

- When the device starts up, such as when you press the **Power** button.
- When you click **Apply** in the **SETUP > Time Setting** screen.
- Once every 24-hours after starting up.

PART III

Advanced Screens

The LAN Configuration Screens (75)

The WAN Configuration Screens (89)

The VPN Transport Screens (113)

The NAT Configuration Screens (125)

The System Configuration Screens (135)

Company Confidential

The LAN Configuration Screens

6.1 Overview

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

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.

6.1.1 What You Can Do in This Chapter

- The **DHCP Setup** screen ([Section 6.2 on page 76](#)) lets you enable, disable, and configure the DHCP server in the WiMAX Device.
- The **Static DHCP** screen ([Section 6.3 on page 78](#)) lets you assign specific IP addresses to specific computers on the LAN.
- The **IP Alias** screen ([Section 6.4 on page 79](#)) lets you add subnets on the LAN port. You can also control what routing information is sent and received by each subnet.
- The **IP Static Route** screen ([Section 6.5 on page 81](#)) lets you examine the static routes configured in the WiMAX Device.
- The **Other Settings** screen ([Section 6.6 on page 83](#)) lets you control the routing information that is sent and received by each subnet assign specific IP addresses to specific computers on the LAN.

6.1.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

IP Address

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to

communicate across the network. These networking devices are also known as hosts.

Subnet Masks

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

DNS

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 networking device before you can access it.

DHCP

A DHCP (Dynamic Host Configuration Protocol) server can assign a device an IP address, subnet mask, DNS and other routing information when it's turned on.

6.2 DHCP Setup

Click **ADVANCED > LAN Configuration > DHCP Setup** to enable, disable, and configure the DHCP server in the WiMAX Device.

Figure 24 ADVANCED > LAN Configuration > DHCP Setup

| | |
|--|------------------|
| DHCP Setup | |
| <input checked="" type="checkbox"/> Enable DHCP Server | |
| IP Pool Starting Address: | 192.168.100.33 |
| Pool Size: | 32 |
| DNS Server | |
| DNS Servers Assigned by DHCP Server | |
| First DNS Server: | From ISP 0.0.0.0 |
| Second DNS Server: | From ISP 0.0.0.0 |
| Third DNS Server: | From ISP 0.0.0.0 |
| Apply Reset | |

The following table describes the labels in this screen.

Table 19 ADVANCED > LAN Configuration > DHCP Setup

| LABEL | DESCRIPTION |
|------------------------------------|---|
| DHCP Setup | |
| Enable DHCP Server | Select this if you want the WiMAX Device to be the DHCP server on the LAN. As a DHCP server, the WiMAX 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 WiMAX Device begins allocating IP addresses, if you have not specified an IP address for the computers on your network in ADVANCED > LAN Configuration > 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 WiMAX Device is in). For example, if the IP Pool Start Address is 10.10.10.10, the WiMAX Device can allocate up to 10.10.10.254, or 245 IP addresses. |
| DNS Server | |
| First, Second and Third DNS Server | Specify the IP addresses of a maximum of three DNS servers that the network can use. The WiMAX 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 WiMAX Device. None - no DNS service will be provided by the WiMAX Device. |
| Apply | Click to save your changes. |
| Reset | Click to restore your previously saved settings. |

6.3 Static DHCP

Click **ADVANCED > LAN Configuration > Static DHCP** to assign specific IP addresses to specific computers on the LAN.

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

Figure 25 ADVANCED > LAN Configuration > Static DHCP

| # | 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"/> |

The following table describes the labels in this screen.

Table 20 ADVANCED > LAN Configuration > Static DHCP

| LABEL | DESCRIPTION |
|-------------|---|
| # | The number of the item in this list. |
| MAC Address | Enter the MAC address of the computer to which you want the WiMAX Device to assign the same IP address. |
| IP Address | Enter the IP address you want the WiMAX Device to assign to the computer. |
| Apply | Click to save your changes. |
| Reset | Click to restore your previously saved settings. |

6.4 IP Alias

Click **ADVANCED > LAN Configuration > IP Alias** to add subnets on the LAN port. You can also control what routing information is sent and received by each subnet.

Figure 26 ADVANCED > LAN Configuration > IP Alias

The screenshot shows the 'IP Alias' configuration screen. It contains two sections, 'IP Alias 1' and 'IP Alias 2'. Each section has a checkbox to enable the alias, followed by four fields: 'IP Address', 'IP Subnet Mask', 'RIP Direction', and 'RIP Version'. In both sections, the IP Address and IP Subnet Mask are set to '0.0.0.0', 'RIP Direction' is set to 'None', and 'RIP Version' is set to 'RIP-1'. At the bottom of the screen are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

Table 21 ADVANCED > LAN Configuration > IP Alias

| LABEL | DESCRIPTION |
|----------------|--|
| IP Alias 1 | Select this to add the specified subnet to the LAN port. |
| IP Address | Enter the IP address of the WiMAX 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 WiMAX Device sends and receives on the subnet. <ul style="list-style-type: none"> • None - The WiMAX Device does not send or receive routing information on the subnet. • Both - The WiMAX Device sends and receives routing information on the subnet. • In Only - The WiMAX Device only receives routing information on the subnet. • Out Only - The WiMAX Device only sends routing information on the subnet. |

Table 21 ADVANCED > LAN Configuration > IP Alias (continued)

| LABEL | DESCRIPTION |
|----------------|--|
| RIP Version | Select which version of RIP the WiMAX Device uses when it sends or receives information on the subnet. <ul style="list-style-type: none"> • RIP-1 - The WiMAX Device uses RIPv1 to exchange routing information. • RIP-2B - The WiMAX Device broadcasts RIPv2 to exchange routing information. • RIP-2M - The WiMAX Device multicasts RIPv2 to exchange routing information. |
| IP Alias 2 | Select this to add the specified subnet to the LAN port. |
| IP Address | Enter the IP address of the WiMAX 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 WiMAX Device sends and receives on the subnet. <ul style="list-style-type: none"> • None - The WiMAX Device does not send or receive routing information on the subnet. • Both - The WiMAX Device sends and receives routing information on the subnet. • In Only - The WiMAX Device only receives routing information on the subnet. • Out Only - The WiMAX Device only sends routing information on the subnet. |
| RIP Version | Select which version of RIP the WiMAX Device uses when it sends or receives information on the subnet. <ul style="list-style-type: none"> • RIP-1 - The WiMAX Device uses RIPv1 to exchange routing information. • RIP-2B - The WiMAX Device broadcasts RIPv2 to exchange routing information. • RIP-2M - The WiMAX Device multicasts RIPv2 to exchange routing information. |
| Apply | Click to save your changes. |
| Reset | Click to restore your previously saved settings. |

6.5 IP Static Route

Click **ADVANCED > LAN Configuration > IP Static Route** to look at the static routes configured in the WiMAX Device.



Note: The first static route is the default route and cannot be modified or deleted.

Figure 27 Advanced> LAN Configuration > IP Static Route

| # | Name | Active | Destination | Gateway | Action |
|---|------|--------|-------------|---------|---|
| 1 | - | - | ... | ... |   |
| 2 | - | - | ... | ... |   |
| 3 | - | - | ... | ... |   |
| 4 | - | - | ... | ... |   |
| 5 | - | - | ... | ... |   |
| 6 | - | - | ... | ... |   |

The following table describes the icons in this screen.

Table 22 Advanced> LAN Configuration > IP Static Route

| ICON | DESCRIPTION |
|---|--------------------------------------|
|  | Edit Click to edit this item. |
|  | Delete Click to delete this item. |

The following table describes the labels in this screen.

Table 23 Advanced> LAN Configuration > IP Static Route

| LABEL | DESCRIPTION |
|-------------|--|
| # | The number of the item in this list. |
| Name | This field displays the name that describes the static route. |
| Active | This field shows whether this static route is active (Yes) or not (No). |
| Destination | This field displays the destination IP address(es) that this static route affects. |
| Gateway | This field displays the IP address of the gateway to which the WiMAX Device should send packets for the specified Destination . The gateway is a router or a switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations. |
| Apply | Click to save your changes. |
| Reset | Click to restore your previously saved settings. |

6.5.1 IP Static Route Setup

Click an **Edit** icon in **ADVANCED > LAN Configuration > IP Static Route** to edit a static route in the WiMAX Device.

Figure 28 Advanced > LAN Configuration > IP Static Route Setup

The following table describes the labels in this screen.

Table 24 Management > Static Route > IP Static Route > Edit

| LABEL | DESCRIPTION |
|------------------------|--|
| Route Name | Enter the name of the static route. |
| Active | Select this if you want the static route to be used. Clear this if you do not want the static route to be used. |
| Private | Select this if you do not want the WiMAX Device to tell other routers about this static route. For example, you might select this if the static route is in your LAN. Clear this if you want the WiMAX Device to tell other routers about this static route. |
| Destination IP Address | Enter one of the destination IP addresses that this static route affects. |
| IP Subnet Mask | Enter the subnet mask that defines the range of destination IP addresses that this static route affects. If this static route affects only one IP address, enter 255.255.255.255. |
| Gateway IP Address | Enter the IP address of the gateway to which the WiMAX Device should send packets for the specified Destination . The gateway is a router or a switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations. |
| Metric | Usually, you should keep the default value. This field is related to RIP. The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". The smaller the metric, the lower the "cost". RIP uses hop count as the measurement of cost, where 1 is for a directly-connected network. The metric must be 1-15; if you use a value higher than 15, the routers assume the link is down. |

Table 24 Management > Static Route > IP Static Route > Edit (continued)

| LABEL | DESCRIPTION |
|--------|---|
| Apply | Click to save your changes. |
| Cancel | Click to return to the previous screen without saving your changes. |

6.6 Other Settings

Click **ADVANCED > LAN Configuration > Other Settings** to set the RIP and Multicast options.

Figure 29 ADVANCED > LAN Configuration > Advanced

RIP & Multicast Setup

RIP Direction: Both

RIP Version: RIP-1

Multicast: None

Apply Reset

The following table describes the labels in this screen.

Table 25 ADVANCED > LAN Configuration > Other Settings

| LABEL | DESCRIPTION |
|-----------------------|---|
| RIP & Multicast Setup | |
| RIP Direction | <p>Use this field to control how much routing information the WiMAX Device sends and receives on the subnet.</p> <ul style="list-style-type: none"> • None - The WiMAX Device does not send or receive routing information on the subnet. • Both - The WiMAX Device sends and receives routing information on the subnet. • In Only - The WiMAX Device only receives routing information on the subnet. • Out Only - The WiMAX Device only sends routing information on the subnet. |
| RIP Version | <p>Select which version of RIP the WiMAX Device uses when it sends or receives information on the subnet.</p> <ul style="list-style-type: none"> • RIP-1 - The WiMAX Device uses RIPv1 to exchange routing information. • RIP-2B - The WiMAX Device broadcasts RIPv2 to exchange routing information. • RIP-2M - The WiMAX Device multicasts RIPv2 to exchange routing information. |

Table 25 ADVANCED > LAN Configuration > Other Settings (continued)

| LABEL | DESCRIPTION |
|-----------|--|
| Multicast | <p>You do not have to enable multicasting to use RIP-2M. (See RIP Version.)</p> <p>Select which version of IGMP the WiMAX 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).</p> <ul style="list-style-type: none"> • None - The WiMAX Device does not support multicasting. • IGMP-v1 - The WiMAX Device supports IGMP version 1. • IGMP-v2 - The WiMAX Device supports IGMP version 2. <p>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.</p> |
| Apply | Click to save your changes. |
| Reset | Click to restore your previously saved settings. |

6.7 Technical Reference

The following section contains additional technical information about the WiMAX Device features described in this chapter.

6.7.1 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 WiMAX 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 192.168.100.1 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, 192.168.100.1, for your WiMAX 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 WiMAX 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 WiMAX Device unless you are instructed to do otherwise.

6.7.2 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 WiMAX Device as a DHCP server or disable it. When configured as a server, the WiMAX 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 WiMAX 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 6.3 on page 78](#).

6.7.3 LAN TCP/IP

The WiMAX 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 WiMAX Device are preset in the factory with the following values:

- IP address of 192.168.100.1 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 6.3 on page 78](#).

6.7.4 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 WiMAX 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 WiMAX Device tells the DHCP clients that it itself is the DNS server. When a computer sends a DNS query to the WiMAX Device, the WiMAX 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 WiMAX Device can pass the DNS servers to the computers and the computers can query the DNS server directly without the WiMAX Device's intervention.

6.7.5 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 WiMAX Device will broadcast its routing table periodically and incorporate the RIP information that it receives.
- **In Only** - the WiMAX Device will not send any RIP packets but will accept all RIP packets received.
- **Out Only** - the WiMAX Device will send out RIP packets but will not accept any RIP packets received.

- **None** - the WiMAX 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 WiMAX 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.

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

Company Confidential

The WAN Configuration Screens

7.1 Overview

Use the **ADVANCED > WAN Configuration** screens to set up your WiMAX Device's Wide Area Network (WAN) or Internet features.

A Wide Area Network (or WAN) links geographically dispersed locations to other networks or the Internet. A WAN configuration can include switched and permanent telephone circuits, terrestrial radio systems and satellite systems.

7.1.1 What You Can Do in This Chapter

- The **Internet Connection** screen ([Section 7.2 on page 93](#)) lets you set up your WiMAX Device's Internet settings.
- The **WiMAX Configuration** screen ([Section 7.3 on page 95](#)) lets set up the frequencies used by your WiMAX Device.
- The **Traffic Redirect** screen ([Section 7.4 on page 99](#)) lets change your WiMAX Device's traffic redirect settings.
- The **Advanced** screen ([Section 7.5 on page 101](#)) lets configure your DNS server, RIP, Multicast and Windows Networking settings.

7.1.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

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 30 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 31 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.

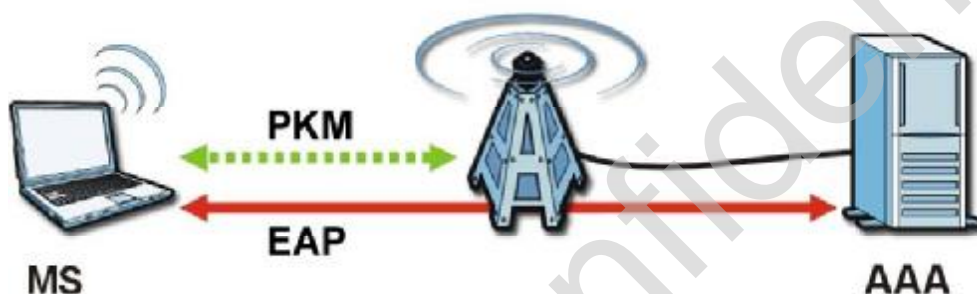
The radio frequency and bandwidth of the link between the WiMAX Device and the base station are controlled by the base station. The WiMAX Device follows the base station's configuration.

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 32 Using an AAA Server

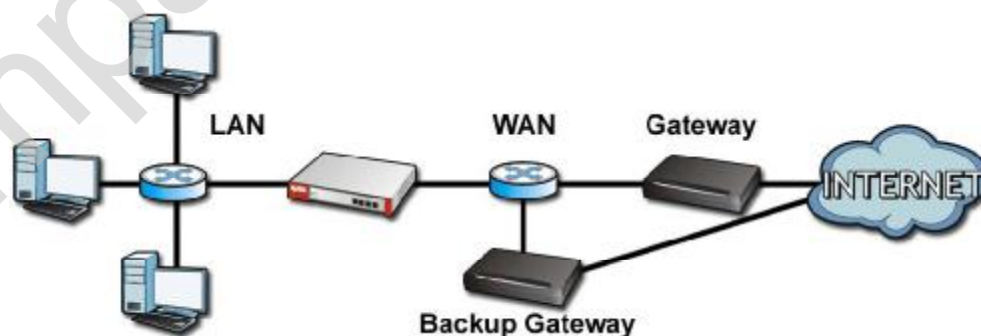


In this figure, the dashed arrow shows the PKM (Privacy Key Management) secured connection between the mobile station and the base station, and the solid arrow shows the EAP secured connection between the mobile station, the base station and the AAA server. See the WiMAX security appendix for more details.

Traffic Redirect

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

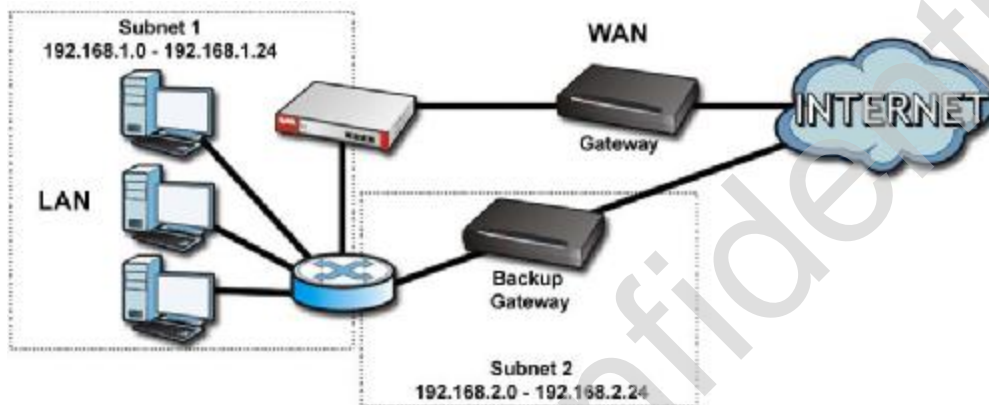
Figure 33 Traffic Redirect WAN Setup



IP alias allows you to avoid triangle route security issues when the backup gateway is connected to the LAN or DMZ. Use IP alias to configure the LAN into

two or three logical networks with the WiMAX Device itself as the gateway for each LAN network. Put the protected LAN in one subnet (Subnet 1 in the following figure) and the backup gateway in another subnet (Subnet 2). Configure a LAN to LAN/WiMAX Device firewall rule that forwards packets from the protected LAN (Subnet 1) to the backup gateway (Subnet 2).

Figure 34 Traffic Redirect LAN Setup



7.2 Internet Connection

Click **ADVANCED > WAN Configuration** to set up your WiMAX Device's Internet settings.

Note: Not all WiMAX Device models have all the fields shown here.

Figure 35 ADVANCED > WAN Configuration > Internet Connection

The following table describes the labels in this screen.

Table 26 ADVANCED > WAN Configuration > Internet Connection > ISP Parameters for Internet Access

| 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 26 ADVANCED > WAN Configuration > Internet Connection > ISP Parameters for Internet Access (continued)

| LABEL | DESCRIPTION |
|--------------------|---|
| Anonymous Identity | <p>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.</p> <p>Leave this field blank if your ISP did not give you an anonymous identity to use.</p> |
| PKM | <p>This field displays the Privacy Key Management version number. PKM provides security between the WiMAX Device and the base station. At the time of writing, the WiMAX Device supports PKMv2 only. See the WiMAX security appendix for more information.</p> |
| Authentication | <p>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).</p> <p>Check with your service provider if you are unsure of the correct setting for your account.</p> <p>Choose from the following user authentication methods:</p> <ul style="list-style-type: none"> • TTLS (Tunnelled Transport Layer Security) • TLS (Transport Layer Security) <p>Note: Not all WiMAX Devices support TLS authentication. Check with your service provider for details.</p> |
| TTLS Inner EAP | <p>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.</p> <p>This field is available only when TTLS is selected in the Authentication field.</p> <p>The WiMAX Device supports the following inner authentication types:</p> <ul style="list-style-type: none"> • CHAP (Challenge Handshake Authentication Protocol) • MSCHAP (Microsoft CHAP) • MSCHAPV2 (Microsoft CHAP version 2) • PAP (Password Authentication Protocol) |

Table 26 ADVANCED > WAN Configuration > Internet Connection > ISP Parameters for Internet Access (continued)

| LABEL | DESCRIPTION |
|--------------------------------------|---|
| Auth Mode | Select the authentication mode from the drop-down list box. This field is not available in all WiMAX Devices. Check with your service provider for details. The WiMAX 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 WiMAX Device uses to authenticate the AAA server. Use the TOOLS > > Trusted CAs screen to import certificates to the WiMAX 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. |
| IP Address | Enter your ISP-assigned IP Address here. |
| 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 to save your changes. |
| Reset | Click to restore your previously saved settings. |

7.3 WiMAX Configuration

Click **ADVANCED > WAN Configuration > WiMAX Configuration** to set up the frequencies used by your WiMAX Device.

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

Radio frequency is measured in Hertz (Hz).

Table 27 Radio Frequency Conversion

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

Figure 36 ADVANCED > WAN Configuration >WiMAX Configuration

The screenshot shows a configuration window with the following fields:

- DL Frequency [1]: 2647000 kHz
- DL Frequency [2]: 2657000 kHz
- DL Frequency [3]: 2667000 kHz
- DL Frequency [4]: 2630500 kHz
- DL Frequency [5]: 2640500 kHz
- DL Frequency [6]: 2650500 kHz
- DL Frequency [7]: 0 kHz
- DL Frequency [8]: 0 kHz
- DL Frequency [9]: 0 kHz
- DL Frequency [10]: 0 kHz
- DL Frequency [11]: 0 kHz
- DL Frequency [12]: 0 kHz
- DL Frequency [13]: 0 kHz
- DL Frequency [14]: 0 kHz
- DL Frequency [15]: 0 kHz
- DL Frequency [16]: 0 kHz
- DL Frequency [17]: 0 kHz
- DL Frequency [18]: 0 kHz
- DL Frequency [19]: 0 kHz
- Bandwidth: 10000 kHz

Buttons: Apply, Reset

The following table describes the labels in this screen.

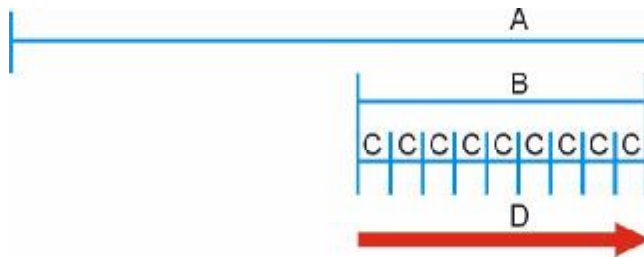
Table 28 ADVANCED > WAN Configuration >WiMAX Configuration

| LABEL | DESCRIPTION |
|-----------------------------------|---|
| DL Frequency / Bandwidth [1 ~ 19] | <p>These fields show the downlink frequency settings in kilohertz (kHz). Enter values in these fields to have the WiMAX Device scan these frequencies for available channels in ascending numerical order.</p> <p>Note: The Bandwidth field is not user-configurable; when the WiMAX Device finds a WiMAX connection, its frequency is displayed in this field.</p> <p>Contact your service provider for details of supported frequencies.</p> |
| Apply | Click to save your changes. |
| Reset | Click to restore your previously saved settings. |

7.3.1 Frequency Ranges

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

Figure 37 Frequency Ranges



In this figure, **A** is the WiMAX frequency range. "WiMAX frequency range" refers to the entire range of frequencies the WiMAX 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 WiMAX Device searching for a connection.

Have the WiMAX 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 WiMAX 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.

7.3.2 Configuring Frequency Settings

You need to set the WiMAX 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 7.3.3 on page 98](#) for an example of using the **WiMAX Frequency** screen.

Note: It may take several minutes for the WiMAX Device to find a connection.

- The WiMAX Device searches the **DL Frequency** settings in ascending numerical order, from [1] to [19].

Note: The **Bandwidth** field is not user-configurable; when the WiMAX Device finds a WiMAX connection, its frequency is displayed in this field.

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

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

Table 29 DL Frequency Example Settings

| | EXAMPLE 1 | EXAMPLE 2 |
|-------------------|--|--|
| Bandwidth: | 2500000 | 2500000 |
| DL Frequency [1]: | 2550000 | 2550000 |
| DL Frequency [2]: | 0 | 2600000 |
| DL Frequency [3]: | 0 | 0 |
| DL Frequency [4]: | 0 | 0 |
| | The WiMAX Device searches at 2500000 kHz, and then searches at 2550000 kHz if it has not found a connection. | The WiMAX 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. |

7.3.3 Using the WiMAX Frequency Screen

In this example, your Internet service provider has given you a list of supported frequencies: 2.51, 2.525, 2.6, and 2.625.

- 1 In the **DL Frequency [1]** field, enter 2510000 (2510000 kilohertz (kHz) is equal to 2.51 gigahertz).
- 2 In the **DL Frequency [2]** field, enter 2525000.
- 3 In the **DL Frequency [3]** field, enter 2600000.

- 4 In the **DL Frequency [4]** field, enter **2625000**.

Leave the rest of the **DL Frequency** fields at zero. The screen appears as follows.

Figure 38 Completing the WiMAX Frequency Screen

| | | |
|-------------------|--------------------------------------|-----|
| DL Frequency [1]: | <input type="text" value="2510000"/> | kHz |
| DL Frequency [2]: | <input type="text" value="2525000"/> | kHz |
| DL Frequency [3]: | <input type="text" value="2600000"/> | kHz |
| DL Frequency [4]: | <input type="text" value="2625000"/> | 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 |
| Bandwidth: | <input type="text" value="2500000"/> | kHz |

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

When the WiMAX Device searches for available frequencies, it scans all frequencies from **DL Frequency [1]** to **DL Frequency [4]**. When it finds an available connection, the fields in this screen will be automatically set to use that frequency.

7.4 Traffic Redirect

Click **ADVANCED > WAN Configuration > Traffic Redirect** to change your WiMAX Device's traffic redirect settings.

Figure 39 ADVANCED > WAN Configuration > Traffic Redirect

| | |
|---------------------------------|---|
| <input type="checkbox"/> Active | |
| Backup Gateway IP Address: | <input type="text" value="0.0.0.0"/> |
| Check WAN IP Address: | <input type="text" value="0.0.0.0"/> |
| Fail Tolerance: | <input type="text" value="2"/> |
| Period (sec): | <input type="text" value="5"/> (in seconds) |
| Timeout (sec): | <input type="text" value="3"/> (in seconds) |

The following table describes the labels in this screen.

Table 30 ADVANCED > WAN Configuration > Traffic Redirect

| LABEL | DESCRIPTION |
|---------------------------|---|
| Active | <p>Select this check box to have the WiMAX Device use traffic redirect if the normal WAN connection goes down.</p> <p>Note: If you activate traffic redirect, you must configure the Check WAN IP Address field.</p> |
| Backup Gateway IP Address | <p>Type the IP address of your backup gateway in dotted decimal notation. The WiMAX Device automatically forwards traffic to this IP address if the WiMAX Device's Internet connection terminates.</p> |
| Check WAN IP Address | <p>Configure this field to test your WiMAX Device's WAN accessibility. Type the IP address of a reliable nearby computer (for example, your ISP's DNS server address).</p> <p>Note: If you activate either traffic redirect or dial backup, you must configure an IP address here.</p> <p>When using a WAN backup connection, the WiMAX Device periodically pings the addresses configured here and uses the other WAN backup connection (if configured) if there is no response.</p> |
| Fail Tolerance | <p>Type the number of times (2 recommended) that your WiMAX 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).</p> |
| Period (sec) | <p>The WiMAX 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.</p> <p>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.</p> |
| Timeout (sec) | <p>Type the number of seconds (1 to 10) for your WiMAX 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.</p> |
| Apply | <p>Click to save your changes.</p> |
| Reset | <p>Click to restore your previously saved settings.</p> |

7.5 Advanced

Click **ADVANCED > WAN Configuration > Advanced** to configure your DNS server, RIP, Multicast and Windows Networking settings.

Figure 40 ADVANCED > WAN Configuration > Advanced

The screenshot shows the 'ADVANCED > WAN Configuration > Advanced' configuration screen. It is divided into three main sections:

- DNS Servers:** Contains three rows for 'First DNS Server:', 'Second DNS Server:', and 'Third DNS Server:'. Each row has a dropdown menu set to 'From ISP' and a text input field containing '0.0.0.0'.
- RIP & Multicast Setup:** Contains three rows: 'RIP Direction:' with a dropdown set to 'None', 'RIP Version:' with a dropdown set to 'RIP-1', and 'Multicast:' with a dropdown set to 'None'.
- Windows Networking (NetBIOS over TCP/IP):** Contains two checkboxes: 'Allow between LAN and WAN (You also need to create a firewall rule!)' which is checked, and 'Allow Trigger Dial' which is unchecked.

At the bottom right of the form are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

Table 31 ADVANCED > WAN Configuration > 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 WiMAX 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> |

Table 31 ADVANCED > WAN Configuration > Advanced (continued)

| LABEL | DESCRIPTION |
|--|--|
| 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 WiMAX Device supports both IGMP version 1 (IGMP-v1) and IGMP-v2. Select None to disable it. |
| Windows Networking (NetBIOS over TCP/IP) | |
| Allow between LAN and WAN | 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. Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN. |
| Allow Trigger Dial | Select this option to allow NetBIOS packets to initiate calls. |
| Apply | Click to save your changes. |
| Reset | Click to restore your previously saved settings. |

The Wi-Fi Configuration Screens

8.1 Overview

Use the **ADVANCED > Wi-Fi Configuration** screens to set up your WiMAX Device's Wi-Fi network features.

8.1.1 What You Can Do in This Chapter

- The **General** screen ([Section 8.2 on page 104](#)) allows you to set up your WiMAX Device's basic Wi-Fi settings and security.
- The **MAC Filter** screen ([Section 8.3 on page 109](#)) allows you to create a list of computer MAC addresses that you can allow or deny on your network.
- The **Advanced** screen ([Section 8.4 on page 110](#)) allows you to adjust your advanced Wi-Fi network settings.

8.1.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

MAC Address

On a local area network (LAN) or other network, the MAC address is a computer's unique hardware number. (On an Ethernet LAN, it's the same as your Ethernet address). The MAC layer frames data for transmission over the network, then passes the frame to the physical layer interface where it is transmitted as a stream of bits.

MAC Filtering

Media Access Control filtering filters incoming frames based on MAC (Media Access Control) address(es) that you specify.

RTS/CTS

Request to Send / Clear to Send is a mechanism for reducing interference (or collisions) on a network by delaying other data in the pipeline. The network device

using RTS/CTS initiates the delay as soon as a data frame over a specified size enters the network. The length of the delay is specified in the RTS/CTS configuration parameters.

Fragmentation

On a wireless network, fragmentation refers to the mechanism used to ensure data integrity during transmission. If a network experiences an inordinate amount of interference (or collisions), then artificially fragmenting the data moving across it can reduce this risk.

8.2 General

Click **ADVANCED > Wi-Fi Configuration**. This screen allows you to set up your WiMAX Device's basic wireless settings and security.

Note: The security options in this screen change according to the **Security Mode** option that you select.

Figure 41 ADVANCED > Wi-Fi Configuration > General

The screenshot shows the 'Wi-Fi Configuration' screen with two main sections: 'Wireless Setup' and 'Security'. In the 'Wireless Setup' section, 'Enable Wireless LAN' is checked, the SSID is 'Coffee Bean', 'Hide SSID' is unchecked, and the channel is 'Channel-06 2437MHz'. In the 'Security' section, 'Security Mode' is set to 'WPA2-PSK' (highlighted with a red circle), 'WPA Compatible' is unchecked, the Pre-Shared Key is '12345678', and the ReAuthentication Timer, Idle Timeout, and Group Key Update Timer are all set to 1800 seconds.

The following table describes the labels in this screen.

Table 32 ADVANCED > Wi-Fi Configuration > General

| LABEL | DESCRIPTION |
|---------------------|---|
| Wireless Setup | |
| Enable Wireless LAN | Select this turn to have the WiMAX Device broadcast an IEEE 802.11b/g Wi-Fi signal. |

Table 32 ADVANCED > Wi-Fi Configuration > General (continued)

| LABEL | DESCRIPTION |
|-------------------|--|
| Name (SSID) | Enter the SSID name that the wireless network signal will be listed as on compatible Wi-Fi clients. |
| Hide SSID | Select this option to mask your Wi-Fi network signal. While this may "hide" it from casual scanning programs and devices, it cannot truly hide it from dedicated signal sniffers. If you know the SSID, however, you can still connect to it when prompted to enter an SSID either by your operating system's connection mechanism or the Wi-Fi software you use. |
| Channel Selection | Select a channel on which to broadcast your Wi-Fi network signal. Ideally, you should choose a channel that is currently not in use by other devices within range of this one. |
| Security | |
| Security Mode | Select a security encryption protocol to protect your Wi-Fi network from unwanted visitors. The options are: Security Options are: <ul style="list-style-type: none"> • No Security - It is not recommended that you use this setting. With no security, anyone who has a Wi-Fi device can connect to your network. • Static WEP - This is a basic form of encryption. It is not recommended that you use it as it can be by-passed quite easily. However, because it is one of the original Wi-Fi encryption methods, it is the most compatible with older devices. Select this option if you require maximum compatibility. • WPA-PSK - This provides both improved data encryption and user authentication. Using PSK, both the WiMAX Device and the connecting client share a common password in order to validate the connection. This type of encryption, while robust, is not as strong as WPA, WPA2 or even WPA2-PSK. Use this type of security if you do not use a RADIUS server to authenticate user credentials. • WPA - This is a security subset of WPA2. It requires the presence of a RADIUS server on your network in order to validate user credentials. This encryption standard is slightly older than WPA2 and therefore is more compatible with older devices. • WPA2-PSK - This is a newer, more robust version of the WPA encryption standard. It offers slightly better security, although the use of PSK makes it less robust than it could be. Use this option if you do not have RADIUS server on your network to verify user credentials. • WPA2 - This is currently the most robust form of encryption for wireless networks. It requires a RADIUS server to authenticate user credentials and is a full implementation the security protocol. Use this security option for maximum protection of your network. However, it is the least backwards compatible with older devices. <p>The option you select here changes the configuration options on this screen accordingly. For details on the specific security options, see subsequent tables.</p> |
| Apply | Click to save your changes. |
| Reset | Click to restore your previously saved settings. |

The subsequent screens describe the individual Security Mode options.

Figure 42 ADVANCED > Wi-Fi Configuration > WPA/WPA2 Options

The screenshot shows a configuration window titled "Security". The "Security Mode" is set to "WPA2" via a dropdown menu. Below this, there is a checkbox for "WPA Compatible" which is currently unchecked. Three timer settings are listed: "ReAuthentication Timer" (1800 seconds), "Idle Timeout" (3600 seconds), and "Group Key Update Timer" (1800 seconds). Under the "Authentication Server" section, there are input fields for "IP Address" (0.0.0.0), "Port Number" (0), and "Shared Secret". The "Accounting Server" section includes an unchecked "Active" checkbox and input fields for "IP Address" (0.0.0.0), "Port Number" (0), and "Shared Secret".

| Field | Value |
|------------------------|--------------------------|
| Security Mode | WPA2 |
| WPA Compatible | <input type="checkbox"/> |
| 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 | 0 |
| Shared Secret | |
| Accounting Server | |
| Active | <input type="checkbox"/> |
| IP Address | 0.0.0.0 |
| Port Number | 0 |
| Shared Secret | |

The following table describes the **Security Mode** options for both WPA and WPA2.

Table 33 ADVANCED > Wi-Fi Configuration > General

| LABEL | DESCRIPTION |
|------------------------|---|
| Security Mode | Select WPA or WPA2 to display the following Wi-Fi network security options. |
| WPA Compatible | Select this option to ensure backwards compatibility with the WPA encryption protocol while in WPA2 mode, thus allowing both WPA and WPA2 clients to connect simultaneously. Note: This option does not appear in WPA mode. It only appears in WPA2 mode. |
| ReAuthentication Time | Set the time (in seconds) that the WiMAX Device waits before requiring a connected client to reauthenticate their session. |
| Idle Timeout | Set the time (in seconds) the WiMAX Device waits before disconnecting an idle client. If a client becomes active before the idle count is up, the count resets. |
| Group Key Update Timer | Set the time (in seconds) that WiMAX Device updates the encryption key used for all connected clients on the Wi-Fi network. |
| Authentication Server | This is a server used to securely check one's login credentials, such as a RADIUS server. |
| IP Address | Enter the IP address of the authentication server. |
| Port Number | Enter the port number of the authentication server. |
| Shared Secret | Enter the password for the authentication server. |
| Accounting Server | This is a server that measures the duration of all active connections, usually for accounting purposes, such as an ISP that charges users per minute online rather than a flat fee per month. |
| Active | Select this option to have the WiMAX Device use an accounting server in tandem with the authentication server. |
| IP Address | Enter the IP address of the accounting server. |
| Port Number | Enter the port number of the accounting server. |
| Shared Secret | Enter the password for the accounting server. |

Figure 43 ADVANCED > Wi-Fi Configuration > WPA-PSK/WPA2-PSK Options

| Security | |
|---|--|
| Security Mode | WPA2-PSK <input type="button" value="v"/> |
| <input type="checkbox"/> WPA Compatible | |
| Pre-Shared Key | <input type="text" value="12345678"/> |
| ReAuthentication Timer | <input type="text" value="1800"/> (In Seconds) |
| Idle Timeout | <input type="text" value="3600"/> (In Seconds) |
| Group Key Update Timer | <input type="text" value="1800"/> (In Seconds) |

The following table describes the **Security Mode** options for both WPA-PSK and WPA2-PSK.

Table 34 ADVANCED > Wi-Fi Configuration > General

| LABEL | DESCRIPTION |
|------------------------|---|
| Security Mode | Select WPA-PSK or WPA2-PSK to display the following Wi-Fi network security options. |
| WPA Compatible | Select this option to ensure backwards compatibility with the WPA-PSK encryption protocol while in WPA2-PSK mode, thus allowing both WPA and WPA2 clients to connect simultaneously. Note: This option does not appear in WPA-PSK mode. It only appears in WPA2-PSK mode. |
| Pre-Shared Key | Enter the password that wireless clients will have to match in order to make a secure Wi-Fi network connection with this device. |
| ReAuthentication Time | Set the time (in seconds) that the WiMAX Device waits before requiring a connected client to reauthenticate their session. |
| Idle Timeout | Set the time (in seconds) the WiMAX Device waits before disconnecting an idle client. If a client becomes active before the idle count is up, the count resets. |
| Group Key Update Timer | Set the time (in seconds) that WiMAX Device updates the encryption key used for all connected clients on the wireless network. |

8.3 MAC Filter

Click **ADVANCED > Wi-Fi Configuration > MAC Filter**. This screen allows you to create a list of MAC addresses that you will allow or deny on your network.

Note: If you do not want to enable this feature, enter 00:00:00:00:00:00 in the MAC address fields. (This is the default setting.)

Figure 44 ADVANCED > WAN Configuration > WiMAX Configuration

| 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 |

The following table describes the labels in this screen.

Table 35 ADVANCED > WAN Configuration > WiMAX Configuration

| LABEL | DESCRIPTION |
|---------------|--|
| Active | Select this option to enable MAC address filtering on your WiMAX Device. When active, only clients whose MAC addresses match those you enter on this list are filtered. |
| Filter Action | Select the the type of filter you want to employ: <ul style="list-style-type: none"> Allow - Select this option to allow connections only to the MAC addresses on the list. Deny - Select this option to disallow connection only to the MAC addresses on this list. |
| Set | The number of the item in the list. |
| MAC Address | Enter the MAC address to filter. MAC addresses are always written as 8 hexadecimal pairs separated by colons. |
| Apply | Click to save your changes. |
| Reset | Click to restore your previously saved settings. |

8.4 Advanced

Click **ADVANCED > Wi-Fi Configuration > Advanced**. This screen allows to adjust your advanced Wi-Fi network settings.

Note: For more information on RTS/CTS and Fragmentation Thresholds, see Appendix C on page 313.

Figure 45 ADVANCED > WAN Configuration > Traffic Redirect

The screenshot shows a configuration screen titled "Wireless Advanced Setup". It contains three settings:

- RTS/CTS Threshold:** A text input field containing "2346" and a range indicator "(256 ~ 2346)".
- Fragmentation Threshold:** A text input field containing "2346" and a range indicator "(256 ~ 2346)".
- 802.11 Mode:** A dropdown menu currently showing "802.11b/g".

The following table describes the labels in this screen.

Table 36 ADVANCED > Wi-Fi Configuration > Advanced

| LABEL | DESCRIPTION |
|-------------------------|---|
| RTS/CTS Threshold | <p>Enter a value between 256 and 2346 if you want to use the RTS (Request to Send) / CTS (Clear to Send) mechanism to reduce potential packet collisions.</p> <p>If you notice that your Wi-Fi clients are suffering from data loss or slow data packet transmission/reception, use this feature.</p> <p>Note: Setting the value to 2346 effectively turns this off.</p> |
| Fragmentation Threshold | <p>Enter a value between 256 and 2346 if you want to use the Fragmentation Threshold mechanism. This reduces packet loss resulting from signal interference (such as from other nearby wireless transmitters) by pre-emptively and logically fragmenting data packets and reassembling them at their destination.</p> <p>As with the RTS/CTS Threshold mechanism, using this feature can improve network performance if you are detecting an abnormal number of packet collisions.</p> <p>Note: Setting the value to 2346 effectively turns this off.</p> |

Table 36 ADVANCED > Wi-Fi Configuration > Advanced (continued)

| LABEL | DESCRIPTION |
|-------------|---|
| 802.11 Mode | <p>Select the Wi-Fi protocol to use while broadcasting.</p> <ul style="list-style-type: none"> • 802.11b - This protocol is one of the older ones and is not nearly as robust as later versions (b, g, n). In many countries, it shares the same frequency range (2.4 GHz) as other devices, like cordless phones, Bluetooth devices, and microwave ovens, and so may be prone to interference from them. This protocol has an approximate maximum data throughput of: 11 Mbit/s (average is about 4.5 Mbit/s in a typical networking environment). Select this mode if all your clients are using 'b' and if you have moderate to low bandwidth requirements. • 802.11g - This protocol is newer and marginally more robust than its predecessor. Like the 'b' protocol, it, too, tends to overlap frequencies with other kinds of devices (2.4 GHz) and is similarly prone to interference from them. However, differences in how it operates give it much higher bandwidth capabilities and output power. This protocol has an approximate maximum data throughput of: 54 Mbit/s (average is about 19 Mbit/s in a typical networking environment.) Select this mode if your clients are using 'g' or a mix of 'g' and 'b' and if you have moderate to high bandwidth requirements. • 802.11b/g - This is a hybrid protocol that incorporates all the advantages of the individual protocols with few, if any, of their drawbacks. More importantly, it does not suffer from interference from other devices in its frequency range. Select this method if you have clients who are using either 'b', 'g', or both. |
| Apply | Click to save your changes. |
| Reset | Click to restore your previously saved settings. |

Company Confidential

The VPN Transport Screens

9.1 Overview

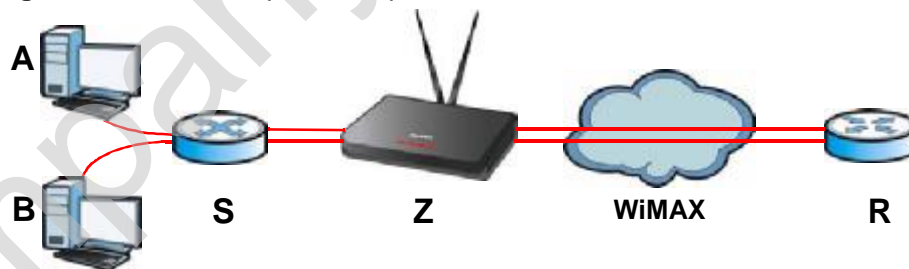
This chapter describes the **ADVANCED > VPN Transport** screens, where you can configure the WiMAX Device to allow traffic from multiple users to pass through the WiMAX network to the service provider's router. Each user has his own personal connection to the service provider, even though there is only a single WiMAX connection. This allows the service provider to identify which user traffic comes from.

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

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

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

Figure 46 VPN Transport Example



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

9.1.1 What You Can Do in This Chapter

- The **General** screen ([Section 9.2 on page 116](#)) lets you turn VPN transport on or off, and to set the VPN transport endpoint (your service provider's router).
- The **Customer Interface** screen ([Section 9.3 on page 116](#)) lets you specify which users can use which WiMAX network links.
- The **Ethernet Pseudowire** screen ([Section 9.4 on page 121](#)) lets you configure the links over the WiMAX network between the WiMAX Device and the service provider's router.
- The **Statistics** screen ([Section 9.5 on page 124](#)) lets you view performance information about the VPN transport connections.

9.1.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

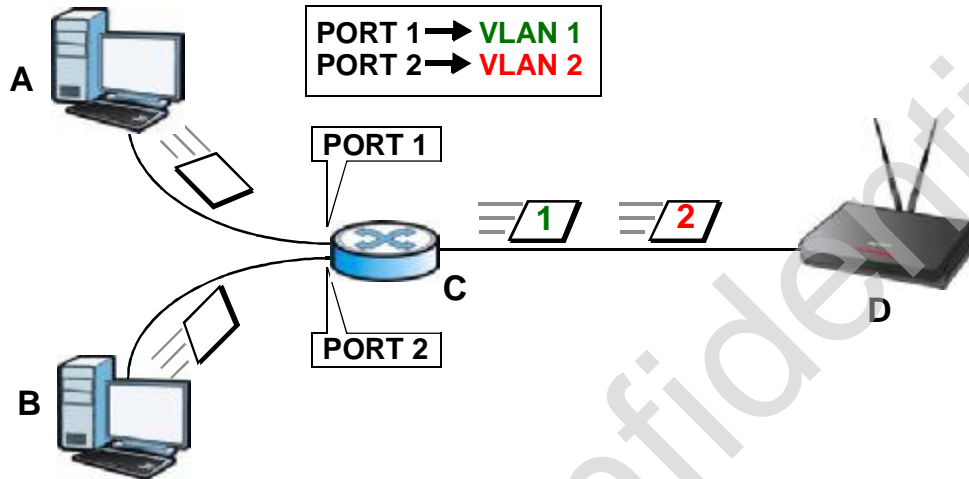
Identifying Users

For the WiMAX 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 WiMAX Device (D), their source is identified by examining their VLAN tags.

Figure 47 Identifying Users



9.1.3 Before You Begin

Before you start configuring your WiMAX 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 make sure that you know the VLAN IDs (Virtual LAN IDentifiers) of the VLANs on your LAN.

9.2 General

Click **ADVANCED > VPN Transport** to turn VPN transport on or off and to set the VPN transport endpoint (your service provider's router).

Figure 48 ADVANCED > VPN Transport > General

L2/L3 VPN Transport General Setup

Transport L2/L3 VPN traffic through WIMAX network by using Ethernet pseudowire

Remote GRE Tunnel End: (IP Address)

Apply Reset

The following table describes the labels in this screen.

Table 37 ADVANCED > VPN Transport > General

| LABEL | DESCRIPTION |
|-----------------------------------|--|
| L2/L3 VPN Transport General Setup | |
| Transport L2/L3 VPN... | 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 to save your changes. |
| Reset | Click to restore your previously saved settings. |

9.3 Customer Interface

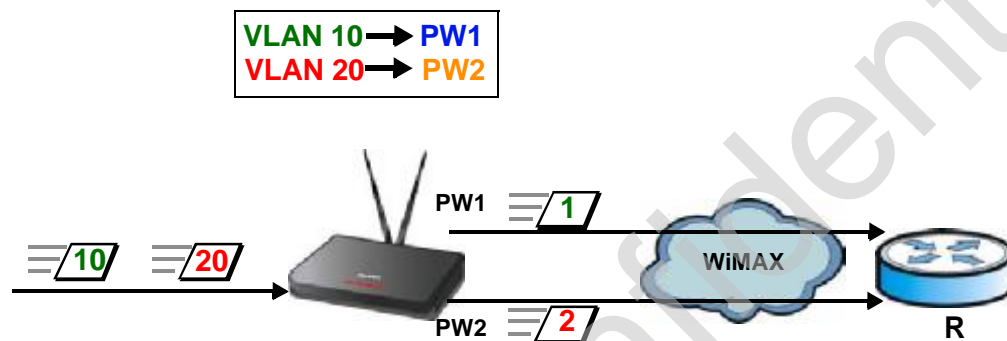
Customer interfaces connect data coming from your computers to Ethernet pseudowires, according to the data's VLAN (Virtual Local Area Network) information. One customer interface is for traffic that has no tag; this is the default interface (rule 0) which cannot be deleted in the GUI. All other customer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

Once the WiMAX 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 this example, the WiMAX 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 49 Pseudowire Mapping



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

9.3.1 Multi-Protocol Label Switching

The WiMAX 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.

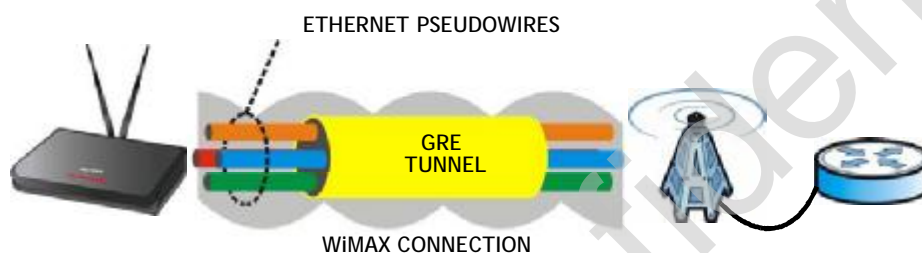
9.3.2 Generic Routing Encapsulation

In order to transport the VPLS traffic over the WiMAX network, the WiMAX 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 WiMAX 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 WiMAX Device (A) and your service provider's router (B), consisting of GRE-encapsulated Ethernet pseudowire traffic.

Figure 50 VPLS Tunneling



9.3.3 Customer Interface Options

Click **ADVANCED > VPN Transport > Customer Interface** to configure the VPNs used by the WiMAX Device.



Note: You cannot delete the **Untagged** entry. It is required for the WiMAX Device to function properly.

Figure 51 ADVANCED > VPN Transport > Customer Interface

| # | Active | Interface | | Mode | Associated Ethernet Pseudowire (Ingress, Egress) | DSCP | Interface Description | Action |
|---|--------|-----------|---------|---------|--|------|-----------------------|--------|
| | | Type | VLAN ID | | | | | |
| 1 | | Untagged | -1 | Routing | - | - | for Routing/NAT | |
| 2 | | | | | | | | |
| 3 | | | | | | | | |
| 4 | | | | | | | | |
| 5 | | | | | | | | |
| 6 | | | | | | | | |
| 7 | | | | | | | | |
| 8 | | | | | | | | |

The following table describes the icons in this screen.

Table 38 Advanced > VPN Transport > Customer Interface

| ICON | DESCRIPTION |
|---|--------------------------------------|
|  | Edit Click to edit this item. |
|  | Delete Click to delete this item. |

The following table describes the labels in this screen.

Table 39 ADVANCED > VPN Transport > Customer Interface

| LABEL | DESCRIPTION |
|--|---|
| # | The number of the item in this list. |
| 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. |
| VLAN ID | For a tagged interface, this displays the IEEE 802.1Q VLAN ID number. For the untagged interface, -1 displays. |
| Mode | This displays either B (bridging) or R (routing). Only the default interface, interface 0, can be a routing interface. |
| Associated Ethernet Pseudowire (Ingress, Egress) | 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. 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". |
| Action | 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. |

9.3.4 Customer Interface Setup

Click the **Edit** icon in the **ADVANCED > VPN Transport > Customer Interface** screen to open the **Customer Interface Setup**.

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.

Figure 52 ADVANCED > VPN Transport > Customer Interface Setup

The following table describes the labels in this screen.

Table 40 ADVANCED > VPN Transport > Customer Interface Setup

| LABEL | DESCRIPTION |
|--------------------------------|---|
| Active | Select to make this customer interface active. Deselect it to make the customer interface inactive. |
| 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. |
| 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 ADVANCED > VPN Transport > Ethernet Pseudowire screen) before you select it. |

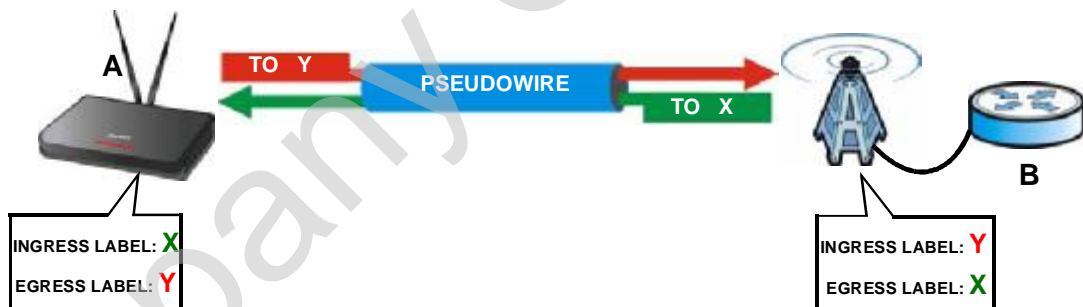
Table 40 ADVANCED > VPN Transport > Customer Interface Setup (continued)

| LABEL | DESCRIPTION |
|-----------------------|---|
| 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 WiMAX Device's WiMAX link. |
| Interface Description | Enter a brief (up to 31 characters) name or description for this interface. |
| Apply | Click to save your changes. |
| Cancel | Click to return to the previous screen without saving your changes. |

9.4 Ethernet Pseudowire

Because VPLS mimics a simple wired Ethernet connection to your service provider's router, the connection between the WiMAX 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 WiMAX Device and B is your service provider's router.

Figure 53 Ethernet Pseudowire Settings Example



Click **ADVANCED > VPN Transport > Ethernet Pseudowire** to configure the WiMAX Device's Ethernet pseudowires.

Figure 54 Advance > VPN Transport > Ethernet Pseudowire

| # | Active | MPLS VC Label | | Pseudowire Description | Action |
|---|--------|---------------|--------|------------------------|--------|
| | | Ingress | Egress | | |
| 1 | | | | | |
| 2 | | | | | |
| 3 | | | | | |

The following table describes the icons in this screen.

Table 41 Advanced > VPN Transport > Customer Interface

| ICON | DESCRIPTION |
|---|--------------------------------------|
|  | Edit Click to edit this item. |
|  | Delete Click to delete this item. |

The following table describes the labels in this screen.

Table 42 ADVANCED > VPN Transport > Ethernet Pseudowire

| LABEL | DESCRIPTION |
|------------------------|---|
| # | The number of the item in this list. |
| 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. |
| MPLS VC Label | |
| 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. |
| Action | Click the Edit icon to set up an Ethernet pseudowire or alter the configuration of an existing Ethernet pseudowire. Click the Delete icon to remove an existing Ethernet pseudowire. |

9.4.1 Ethernet Pseudowire Setup

Click a pseudowire entry's **Edit** icon in the **ADVANCED > VPN Transport > Ethernet Pseudowire** screen to set up or modify an Ethernet pseudowire's configuration.

Figure 55 ADVANCED > VPN Transport > Ethernet Pseudowire Setup

The following table describes the labels in this screen.


Table 43 ADVANCED > VPN Transport > Ethernet Pseudowire Setup

| LABEL | DESCRIPTION |
|------------------------|--|
| Active | Select this to enable the pseudowire. Deselect it to disable the pseudowire. |
| MPLS VC Label | |
| 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 WiMAX 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 WiMAX Device. |
| Pseudowire Description | Enter a brief (up to 31 characters) description for this pseudowire. |
| Apply | Click to save your changes. |
| Cancel | Click to return to the previous screen without saving your changes. |

9.5 Statistics

Click **ADVANCED > VPN Transport > Statistics** to view details and performance information of each active customer interface and its associated Ethernet pseudowire.

Figure 56 ADVANCED > 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 | | | | | | |

The following table describes the labels in this screen.

Table 44 ADVANCED > VPN Transport > Statistics

| LABEL | DESCRIPTION |
|-----------------------|---|
| # | The number of the item in this list. |
| 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 configured in the ADVANCED > VPN Transport > Customer Interface Setup screen. |

The NAT Configuration Screens

10.1 Overview

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

Network Address Translation (NAT) maps a host's IP address within one network to a different IP address in another network. For example, you can use a NAT router to map one IP address from your ISP to multiple private IP addresses for the devices in your home network.

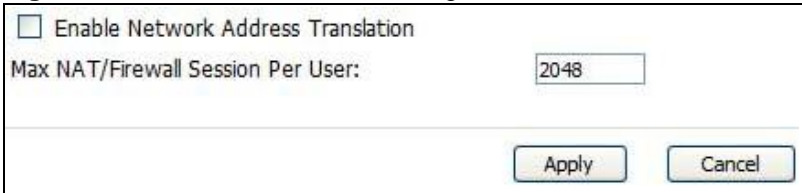
10.1.1 What You Can Do in This Chapter

- The **General** screen ([Section 10.2 on page 125](#)) lets you enable or disable NAT and to allocate memory for NAT and firewall rules.
- The **Port Forwarding** screen ([Section 10.3 on page 126](#)) lets you look at the current port-forwarding rules in the WiMAX Device, and to enable, disable, activate, and deactivate each one.
- The **Trigger Port** screen ([Section 10.4 on page 130](#)) lets you maintain trigger port forwarding rules for the WiMAX Device.
- The **ALG** screen ([Section 10.5 on page 132](#)) lets you enable and disable SIP (VoIP), FTP (file transfer), and H.323 (audio-visual) ALG in the WiMAX Device.

10.2 General

Click **ADVANCED > NAT Configuration > General** to enable or disable NAT and to allocate memory for NAT and firewall rules.

Figure 57 ADVANCED > NAT Configuration > General



| |
|--|
| <input type="checkbox"/> Enable Network Address Translation |
| Max NAT/Firewall Session Per User: <input type="text" value="2048"/> |
| <input type="button" value="Apply"/> <input type="button" value="Cancel"/> |

The following table describes the labels in this screen.

Table 45 ADVANCED > NAT Configuration > General

| LABEL | DESCRIPTION |
|------------------------------------|--|
| Enable Network Address Translation | Select this if you want to use port forwarding, trigger ports, or any of the ALG. |
| 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 WiMAX 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 to save your changes. |
| Cancel | Click to return to the previous screen without saving your changes. |

10.3 Port Forwarding

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 **ADVANCED > NAT Configuration > 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.

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 58 Multiple Servers Behind NAT Example



10.3.1 Port Forwarding Options



Click **ADVANCED > NAT Configuration > Port Forwarding** to look at the current port-forwarding rules in the WiMAX 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.

Figure 59 ADVANCED > NAT Configuration > Port Forwarding

| Default Server Setup | | | | | | |
|----------------------|--------------------------|--|------------|----------|-------------------|--------|
| Default Server: | | <input type="text" value="0.0.0.0"/> | | | | |
| Port Forwarding | | | | | | |
| # | Active | Name | Start Port | End Port | Server IP Address | Action |
| 1 | <input type="checkbox"/> | | 0 | 0 | | |
| 2 | <input type="checkbox"/> | | 0 | 0 | | |
| 3 | <input type="checkbox"/> | | 0 | 0 | | |
| | | <input type="button" value="Apply"/> <input type="button" value="Cancel"/> | | | | |

The following table describes the icons in this screen.

Table 46 Advanced > VPN Transport > Customer Interface

| ICON | DESCRIPTION |
|---|--------------------------------------|
|  | Edit Click to edit this item. |
|  | Delete Click to delete this item. |

The following table describes the labels in this screen.

Table 47 ADVANCED > NAT Configuration > Port Forwarding

| LABEL | DESCRIPTION |
|----------------------|--|
| Default Server Setup | |
| Default Server | Enter the IP address of the server to which the WiMAX Device should forward packets for ports that are not specified in the Port Forwarding section below or in the TOOLS > Remote MGMT screens. Enter 0.0.0.0 if you want the WiMAX Device to discard these packets instead. |
| Port Forwarding | |
| # | The number of the item in this list. |
| 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. |
| Action | Click the Edit icon to set up a port forwarding rule or alter the configuration of an existing port forwarding rule. Click the Delete icon to remove an existing port forwarding rule. |
| Apply | Click to save your changes. |
| Reset | Click to restore your previously saved settings. |

10.3.2 Port Forwarding Rule Setup

Click a port forwarding rule's **Edit** icon in the **ADVANCED > NAT Configuration > Port Forwarding** screen to activate, deactivate, or edit it.

Figure 60 ADVANCED > NAT Configuration > Port Forwarding > Rule Setup

The screenshot shows a dialog box titled "Rule Setup". It has the following fields and controls:

- Active
- Service Name: [text input field]
- Start Port: [0] [input field]
- End Port: [0] [input field]
- Server IP Address: [0.0.0.0] [input field]
- [Apply] [Cancel] buttons

The following table describes the labels in this screen.

Table 48 ADVANCED > NAT Configuration > Port Forwarding > Rule Setup

| 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 to save your changes. |
| Cancel | Click to return to the previous screen without saving your changes. |

10.4 Trigger Port

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 WiMAX 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 WiMAX Device's WAN port receives a response with a specific port number and protocol ("incoming" port), the WiMAX 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.

Click **ADVANCED > NAT Configuration > Trigger Port** to maintain trigger port forwarding rules for the WiMAX Device.

Figure 61 ADVANCED > NAT Configuration > Trigger Port

| # | 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"/> |

The following table describes the labels in this screen.

Table 49 ADVANCED > NAT Configuration > Trigger Port

| LABEL | DESCRIPTION |
|----------|---|
| # | The number of the item in this list. |
| 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 | |

Table 49 ADVANCED > NAT Configuration > Trigger Port (continued)

| LABEL | DESCRIPTION |
|------------------------|--|
| Start Port End Port | <p>Enter the incoming port number or range of port numbers you want to forward to the IP address the WiMAX Device records.</p> <p>To forward one port number, enter the port number in the Start Port and End Port fields.</p> <p>To forward a range of ports,</p> <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. <p>If you want to delete this rule, enter zero in the Start Port and End Port fields.</p> |
| Trigger | |
| Start Port End Port | <p>Enter the outgoing port number or range of port numbers that makes the WiMAX Device record the source IP address and assign it to the selected incoming port number(s).</p> <p>To select one port number, enter the port number in the Start Port and End Port fields.</p> <p>To select a range of ports,</p> <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. <p>If you want to delete this rule, enter zero in the Start Port and End Port fields.</p> |
| Apply | Click to save your changes. |
| Cancel | Click to return to the previous screen without saving your changes. |

10.4.1 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 62 Trigger Port Forwarding Example

- 1 Jane requests a file from the Real Audio server (port 7070).
- 2 Port 7070 is a "trigger" port and causes the WiMAX Device to record Jane's computer IP address. The WiMAX 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 WiMAX 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 WiMAX Device times out in three minutes with UDP (User Datagram Protocol), or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

Two points to remember about trigger ports:

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

10.5 ALG

Some applications, such as SIP, cannot operate through NAT (are NAT unfriendly) 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.

Click **ADVANCED > NAT Configuration > ALG** to enable and disable SIP (VoIP), FTP (file transfer), and H.323 (audio-visual) ALG in the WiMAX Device.

Figure 63 ADVANCED > NAT Configuration > ALG

The screenshot shows a configuration window with three checked checkboxes:

- Enable SIP ALG
- Enable FTP ALG
- Enable H.323 ALG

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

The following table describes the labels in this screen.

Table 50 ADVANCED > NAT Configuration > 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. |
| 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 to save your changes. |
| Cancel | Click to return to the previous screen without saving your changes. |

Company Confidential

The System Configuration Screens

11.1 Overview

Click **ADVANCED > System Configuration** to set up general system settings, change the system mode, change the password, configure the DDNS server settings, and set the current date and time.

11.1.1 What You Can Do in This Chapter

- The **General** screen ([Section 11.2 on page 137](#)) lets you change the WiMAX Device's mode, set up its system name, domain name, idle timeout, and administrator password.
- The **Dynamic DNS** screen ([Section 11.3 on page 138](#)) lets you set up the WiMAX Device as a dynamic DNS client.
- The **Firmware** screen ([Section 11.4 on page 140](#)) lets you upload new firmware to the WiMAX Device.
- The **Configuration** screen ([Section 11.5 on page 142](#)) lets you back up or restore the configuration of the WiMAX Device.
- The **Restart** screen ([Section 11.6 on page 143](#)) lets you restart your WiMAX Device from within the web configurator.

11.1.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

System Name

The **System Name** is often used for identification purposes. Because some ISPs check this name you should enter your computer's "Computer Name".

- In Windows 2000: Click **Start > Settings > Control Panel** and then double-click the **System** icon. Select the **Network Identification** tab and then click the **Properties** button. Note the entry for the **Computer Name** field and enter it as the **System Name**.

- In Windows XP: Click **Start > My Computer > View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the **WiMAX Device System Name**.

Domain Name

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

DNS Server Address Assignment

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

The WiMAX Device can get the DNS server addresses in the following ways:

- 1 The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the **DNS Server** fields in the **SYSTEM General** screen.
- 2 If the ISP did not give you DNS server information, leave the **DNS Server** fields in the **SYSTEM General** screen set to 0.0.0.0 for the ISP to dynamically assign the DNS server IP addresses.

11.2 General

Click **ADVANCED > System Configuration > General** to change the WiMAX Device's mode, set up its system name, domain name, idle timeout, and administrator password.

Figure 64 ADVANCED > System Configuration > General

The screenshot shows a web-based configuration interface. At the top, there's a header 'System Setup' with a dashed border. Below it are three input fields: 'System Name:', 'Domain Name:', and 'Administrator Inactivity Timer:'. The 'Administrator Inactivity Timer' field has the value '0' and a label 'minutes (0 means no timeout)'. Below this is another section header 'Password Setup' with a dashed border. It contains three input fields: 'Old Password:', 'New Password:', and 'Retype to Confirm:'. The 'Old Password' field shows four asterisks. At the bottom right, there are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

Table 51 ADVANCED > System Configuration > General

| LABEL | DESCRIPTION |
|--------------------------------|--|
| System Setup | |
| System Name | Enter your computer's "Computer Name". This is for identification purposes, but some ISPs also check this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted. |
| Domain Name | Enter the domain name entry that is propagated to DHCP clients on the LAN. If you leave this blank, the domain name obtained from the ISP is used. Use up to 38 alphanumeric characters. Spaces are not allowed, but dashes "-" and periods "." are accepted. |
| Administrator Inactivity Timer | Enter the number of minutes a management session can be left idle before the session times out. After it times out, you have to log in again. A value of "0" means a management session never times out, no matter how long it has been left idle. This is not recommended. Long idle timeouts may have security risks. The default is five minutes. |
| Password Setup | |
| Old Password | Enter the current password you use to access the WiMAX Device. |
| New Password | Enter the new password for the WiMAX Device. You can use up to 30 characters. As you type the password, the screen displays an asterisk (*) for each character you type. |

Table 51 ADVANCED > System Configuration > General (continued)

| LABEL | DESCRIPTION |
|-------------------|--|
| Retype to Confirm | Enter the new password again. |
| Apply | Click to save your changes. |
| Reset | Click to restore your previously saved settings. |

11.3 Dynamic DNS

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

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

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

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

Click **ADVANCED > System Configuration > Dynamic DNS** to set up the WiMAX Device as a dynamic DNS client.

Figure 65 ADVANCED > System Configuration > Dynamic DNS

The following table describes the labels in this screen.

Table 52 ADVANCED > System Configuration > Dynamic DNS

| LABEL | DESCRIPTION |
|------------------------|--|
| Dynamic DNS Setup | |
| Enable Dynamic DNS | Select this to use dynamic DNS. |
| Service Provider | Select the name of your Dynamic DNS service provider. |
| Dynamic DNS Type | Select the type of service that you are registered for from your Dynamic DNS service provider. |
| Host Name | Enter the host name. You can specify up to two host names, separated by a comma (","). |
| User Name | Enter your user name. |
| Password | Enter the password assigned to you. |
| Enable Wildcard Option | Select this to enable the DynDNS Wildcard feature. |

Table 52 ADVANCED > System Configuration > Dynamic DNS (continued)

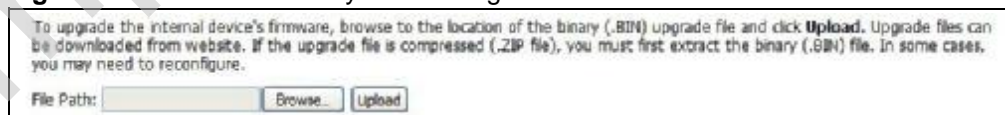
| LABEL | DESCRIPTION |
|---|---|
| Enable offline option | This field is available when CustomDNS is selected in the DDNS Type field. Select this if your Dynamic DNS service provider redirects traffic to a URL that you can specify while you are off line. Check with your Dynamic DNS service provider. |
| IP Address Update Policy | |
| Use WAN IP Address | Select this if you want the WiMAX Device to update the domain name with the WAN port's IP address. |
| Dynamic DNS server auto detect IP address | Select this if you want the DDNS server to update the IP address of the host name(s) automatically. Select this option when there are one or more NAT routers between the WiMAX Device and the DDNS server. Note: The DDNS server may not be able to detect the proper IP address if there is an HTTP proxy server between the WiMAX Device and the DDNS server. |
| Use specified IP address | Select this if you want to use the specified IP address with the host name(s). Then, specify the IP address. Use this option if you have a static IP address. |
| Apply | Click to save your changes. |
| Reset | Click to restore your previously saved settings. |

11.4 Firmware

Click **ADVANCED > System Configuration > Firmware** to upload new firmware to the WiMAX Device. Firmware files usually use the system model name with a ".bin" extension, such as "WiMAX Device.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Contact your service provider for information on available firmware upgrades.

Note: Only use firmware for your WiMAX Device's specific model.

Figure 66 ADVANCED > System Configuration > Firmware

The following table describes the labels in this screen.

Table 53 ADVANCED > System Configuration > Firmware

| LABEL | DESCRIPTION |
|-----------|--|
| File Path | Enter the location of the *.bin file you want to upload, or click Browse... to find it. You must decompress compressed (.zip) files before you can upload them. |
| Browse... | Click this to find the *.bin file you want to upload. |
| Upload | Click this to begin uploading the selected file. This may take up to two minutes. Note: Do not turn off the device while firmware upload is in progress! |

11.4.1 The Firmware Upload Process

When the WiMAX Device uploads new firmware, the process usually takes about two minutes. The device also automatically restarts in this time. This causes a temporary network disconnect.

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

After two minutes, log in again, and check your new firmware version in the **Status** screen. You might have to open a new browser window to log in.

If the upload is not successful, you will be notified by error message.

Click **Return** to go back to the **Firmware** screen.

11.5 Configuration

Click **ADVANCED > System Configuration > Configuration** to back up or restore the configuration of the WiMAX Device. You can also use this screen to reset the WiMAX Device to the factory default settings.

Figure 67 ADVANCED > System Configuration > Configuration

The screenshot shows a web interface with three main sections separated by dashed lines:

- Backup Configuration:** Contains the instruction "Click **Backup** to save the current configuration of your system to your computer." and a "Backup" button.
- Restore Configuration:** Contains the instruction "To restore a previously saved configuration file to your system, browse to the location of the configuration file and click **Upload**." Below this is a "File Path:" label, an empty text input field, a "Browse..." button, and an "Upload" button.
- Back to Factory Defaults:** Contains the instruction "Click **Reset** to clear all user entered configuration information and return to factory defaults. After resetting, the" followed by a list:
 - Password will be 1234
 - LAN IP address will be 192.168.1.1
 - DHCP will be reset to server
 and a "Reset" button.

The following table describes the labels in this screen.

Table 54 ADVANCED > System Configuration > Configuration

| LABEL | DESCRIPTION |
|---------------------------------|--|
| Backup Configuration | |
| Backup | Click this to save the WiMAX Device's current configuration to a file on your computer. Once your device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file is useful if you need to return to your previous settings. |
| Restore Configuration | |
| File Path | Enter the location of the file you want to upload, or click Browse... to find it. |
| Browse | Click this to find the file you want to upload. |
| Upload | Click this to restore the selected configuration file. Note: Do not turn off the device while configuration file upload is in progress. |
| Back to Factory Defaults | |
| Reset | Click this to clear all user-entered configuration information and return the WiMAX Device to its factory defaults. There is no warning screen. |

11.5.1 The Restore Configuration Process

When the WiMAX Device restores a configuration file, the device automatically restarts. This causes a temporary network disconnect.

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

If the WiMAX Device's IP address is different in the configuration file you selected, you may need to change the IP address of your computer to be in the same subnet as that of the default management IP address (192.168.5.1). See the Quick Start Guide or the appendices for details on how to set up your computer's IP address.

You might have to open a new browser to log in again.

If the upload was not successful, you are notified by **Configuration Upload Error** message:

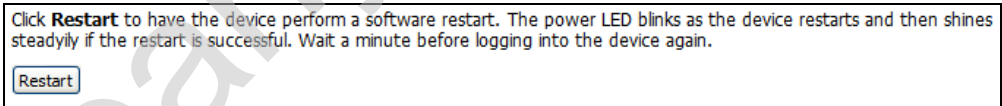
Click **Return** to go back to the **Configuration** screen.

11.6 Restart

Click **ADVANCED > System Configuration > Restart** to reboot the WiMAX Device without turning the power off.

Note: Restarting the WiMAX Device does not affect its configuration.

Figure 68 ADVANCED > System Configuration > Restart



The following table describes the labels in this screen.

Table 55 ADVANCED > System Configuration > Firmware

| LABEL | DESCRIPTION |
|---------|---|
| Restart | <p>Click this button to have the device perform a software restart. The Power LED blinks as it restarts and the shines steadily if the restart is successful.</p> <p>Note: Wait one minute before logging back into the WiMAX Device after a restart.</p> |

11.6.1 The Restart Process

When you click **Restart**, the the process usually takes about two minutes. Once the restart is complete you can log in again.

Company Confidential

PART IV

Voice Screens

The Service Configuration Screens (147)

The Phone Screens (165)

The Phone Book Screens (175)

Company Confidential

The Service Configuration Screens

12.1 Overview

The **VOICE > Service Configuration** screens allow you to set up your voice accounts and configure your QoS settings.

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.

12.1.1 What You Can Do in This Chapter

- The **SIP Settings** screen ([Section 12.2 on page 149](#)) lets you setup and maintain your SIP account(s) in the WiMAX Device.
- The **Advanced SIP Settings** screen ([Section 12.2.1 on page 151](#)) lets you set up and maintain advanced settings for each SIP account
- The **QoS** screen ([Section 12.3 on page 158](#)) lets you set up and maintain ToS and VLAN settings for the WiMAX Device.

12.1.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

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.

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.

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 for example) or numbers like a telephone number ([1122334455@VoIP-provider.com](tel:1122334455@VoIP-provider.com) for example).

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](tel:1122334455@VoIP-provider.com), then "VoIP-provider.com" is the SIP service domain.

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.

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.

Use NAT

If you know the NAT router's public IP address and SIP port number, you can use the Use NAT feature to manually configure the WiMAX Device to use a them in the SIP messages. This eliminates the need for STUN or a SIP ALG. You must also configure the NAT router to forward traffic with this port number to the WiMAX Device.

12.1.3 Before you Begin

- Ensure that you have all of your voice account information on hand. If not, contact your voice account service provider to find out which settings in this chapter you should configure in order to use your telephone with the WiMAX Device.
- Connect your WiMAX Device to the Internet, as described in the Quick Start Guide. If you have not already done so, then you will not be able to test your VoIP settings.

12.2 SIP Settings

Click **VOICE > Service Configuration > SIP Setting** to setup and maintain your SIP account(s) in the WiMAX Device. Your VoIP or Internet service provider should provide you with your account information. You can also enable and disable each SIP account.

Figure 69 VOICE > Service Configuration > SIP Setting

SIP Account: SIP1

SIP Settings

Active SIP Account

Number: changeme

SIP Local Port: 5060 (1025-65535)

SIP Server Address: 127.0.0.1

SIP Server Port: 5060 (1-65535)

REGISTER Server Address: 127.0.0.1

REGISTER Server Port: 5060 (1-65535)

SIP Service Domain: 127.0.0.1

Send Caller ID

Authentication

User Name: changeme

Password: ●●●●●●

Apply Reset Advanced

The following table describes the labels in this screen.

Table 56 VOICE > Service Configuration > SIP Setting

| LABEL | DESCRIPTION |
|-------------------------|---|
| SIP Account | Select the SIP account you want to see in this screen. If you change this field, the screen automatically refreshes. |
| SIP Settings | |
| Active SIP Account | Select this if you want the WiMAX Device to use this account. Clear it if you do not want the WiMAX Device to use this account. |
| Number | Enter your SIP number. In the full SIP URI, this is the part before the @ symbol. You can use up to 127 printable ASCII characters. |
| SIP Local Port | Enter the WiMAX Device's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value. |
| SIP Server Address | Enter the IP address or domain name of the SIP server provided by your VoIP service provider. You can use up to 95 printable ASCII characters. It does not matter whether the SIP server is a proxy, redirect or register server. |
| SIP Server Port | Enter the SIP server's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value. |
| REGISTER Server Address | Enter the IP address or domain name of the SIP register server, if your VoIP service provider gave you one. Otherwise, enter the same address you entered in the SIP Server Address field. You can use up to 95 printable ASCII characters. |
| REGISTER Server Port | Enter the SIP register server's listening port number, if your VoIP service provider gave you one. Otherwise, enter the same port number you entered in the SIP Server Port field. |
| SIP Service Domain | Enter the SIP service domain name. In the full SIP URI, this is the part after the @ symbol. You can use up to 127 printable ASCII Extended set characters. |
| Send Caller ID | Select this if you want to send identification when you make VoIP phone calls. Clear this if you do not want to send identification. |
| Authentication | |
| User Name | Enter the user name for registering this SIP account, exactly as it was given to you. You can use up to 95 printable ASCII characters. |
| Password | Enter the user name for registering this SIP account, exactly as it was given to you. You can use up to 95 printable ASCII Extended set characters. |
| Apply | Click to save your changes. |
| Reset | Click to restore your previously saved settings. |
| Advanced | Click this to edit the advanced settings for this SIP account. The Advanced SIP Settings screen appears. |

12.2.1 Advanced SIP Settings

This section describes the features of the Advanced SIP settings screen.

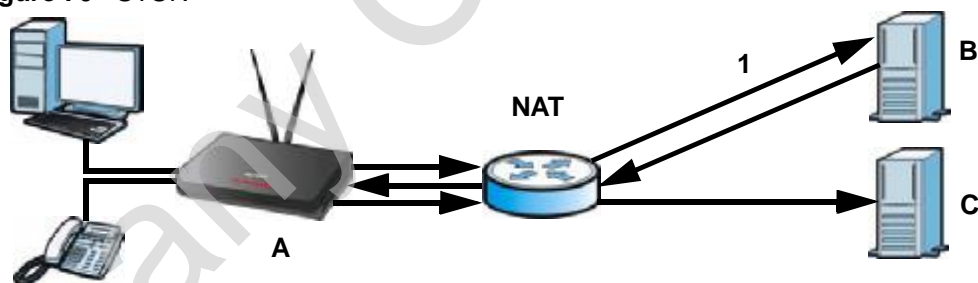
12.2.1.1 STUN

STUN (Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators) allows the WiMAX Device to find the presence and types of NAT routers and/or firewalls between it and the public Internet. STUN also allows the WiMAX Device to find the public IP address that NAT assigned, so the WiMAX Device can embed it in the SIP data stream. STUN does not work with symmetric NAT routers or firewalls. See RFC 3489 for details on STUN.

The following figure shows how STUN works.

- 1 The WiMAX Device (A) sends SIP packets to the STUN server (B).
- 2 The STUN server (B) finds the public IP address and port number that the NAT router used on the WiMAX Device's SIP packets and sends them to the WiMAX Device.
- 3 The WiMAX Device uses the public IP address and port number in the SIP packets that it sends to the SIP server (C).

Figure 70 STUN



12.2.1.2 Outbound Proxy

Your VoIP service provider may host a SIP outbound proxy server to handle all of the WiMAX Device's VoIP traffic. This allows the WiMAX Device to work with any type of NAT router and eliminates the need for STUN or a SIP ALG. Turn off a SIP ALG on a NAT router in front of the WiMAX Device to keep it from re-translating the IP address (since this is already handled by the outbound proxy server).

12.2.1.3 Voice Coding

A codec (coder/decoder) codes analog voice signals into digital signals and decodes the digital signals back into voice signals. The WiMAX Device supports the following codecs.

- **G.711** is a Pulse Code Modulation (PCM) waveform codec. PCM measures analog signal amplitudes at regular time intervals (sampling) and converts them into digital bits (quantization). Quantization “reads” the analog signal and then “writes” it to the nearest digital value. For this reason, a digital sample is usually slightly different from its analog original (this difference is known as “quantization noise”). G.711 provides excellent sound quality but requires 64kbps of bandwidth.
- **G.723** is an Adaptive Differential Pulse Code Modulation (ADPCM) waveform codec. Differential (or Delta) PCM is similar to PCM, but encodes the audio signal based on the difference between one sample and a prediction based on previous samples, rather than encoding the sample’s actual quantized value. Many thousands of samples are taken each second, and the differences between consecutive samples are usually quite small, so this saves space and reduces the bandwidth necessary.

However, DPCM produces a high quality signal (high signal-to-noise ratio or SNR) for high difference signals (where the actual signal is very different from what was predicted) but a poor quality signal (low SNR) for low difference signals (where the actual signal is very similar to what was predicted). This is because the level of quantization noise is the same at all signal levels. Adaptive DPCM solves this problem by adapting the difference signal’s level of quantization according to the audio signal’s strength. A low difference signal is given a higher quantization level, increasing its signal-to-noise ratio. This provides a similar sound quality at all signal levels. G.723 provides high quality sound and requires 20 or 40 kbps.

- **G.729** is an Analysis-by-Synthesis (AbS) hybrid waveform codec. It uses a filter based on information about how the human vocal tract produces sounds. The codec analyzes the incoming voice signal and attempts to synthesize it using its list of voice elements. It tests the synthesized signal against the original and, if it is acceptable, transmits details of the voice elements it used to make the synthesis. Because the codec at the receiving end has the same list, it can exactly recreate the synthesized audio signal. G.729 provides good sound quality and reduces the required bandwidth to 8kbps.

12.2.1.4 MWI (Message Waiting Indication)

Enable Message Waiting Indication (MWI) enables your phone to give you a message-waiting (beeping) dial tone when you have one or more voice messages. Your VoIP service provider must have a messaging system that sends message-waiting-status SIP packets as defined in RFC 3842.

12.2.1.5 Advanced SIP Settings Options

Click **Advanced** in **VOICE > Service Configuration > SIP Settings** to set up and maintain advanced settings for each SIP account.

Figure 71 VOICE > Service Configuration > SIP Settings > Advanced

The screenshot shows the 'Advanced' settings for a SIP account. The settings are organized into several sections:

- SIP Server Settings:** URL Type (SIP), Expiration Duration (3600 sec), Register Re-send timer (180 sec), Session Expires (180 sec), Min-SE (30 sec).
- RTP Port Range:** Start Port (4000), End Port (65535).
- Voice Compression:** Primary (G.711A), Secondary (G.729), Third (G.711u), DTMF Mode (RFC 2883).
- STUN:** Active checkbox, Server Address, Server Port (3478).
- Use NAT:** Active checkbox, Server Address, Server Port (5060).
- Outbound Proxy:** Active checkbox, Server Address, Server Port (3478).
- NAT Keep Alive:** Active checkbox, Keep Alive With SIP Proxy/Outbound Proxy radio buttons, Keep Alive Interval (120 sec).
- MWI (Message Waiting Indication):** Enable checkbox, Expiration Time (1800 sec).
- Fax Option:** G.711 Fax Passthrough (selected), T.38 Fax Relay.
- Call Forward:** Call Forward Table (Table1).
- Caller Ringing:** Enable checkbox, Caller Ringing Tone (Default).
- On Hold:** Enable checkbox, On Hold Tone (Default).

The following table describes the labels in this screen.

Table 57 VOICE > Service Configuration > SIP Settings > Advanced

| LABEL | DESCRIPTION |
|---------------------|--|
| SIP Server Settings | |
| URL Type | Select whether or not to include the SIP service domain name when the WiMAX Device sends the SIP number. <ul style="list-style-type: none"> SIP - include the SIP service domain name TEL - do not include the SIP service domain name |

Table 57 VOICE > Service Configuration > SIP Settings > Advanced (continued)

| LABEL | DESCRIPTION |
|---|---|
| Expiration Duration | Enter the number of seconds your SIP account is registered with the SIP register server before it is deleted. The WiMAX Device automatically tries to re-register your SIP account when one-half of this time has passed. (The SIP register server might have a different expiration.) |
| Register Re-send timer | Enter the number of seconds the WiMAX Device waits before it tries again to register the SIP account, if the first try failed or if there is no response. |
| Session Expires | Enter the number of seconds the conversation can last before the call is automatically disconnected. Usually, when one-half of this time has passed, the WiMAX Device or the other party updates this timer to prevent this from happening. |
| Min-SE | Enter the minimum number of seconds the WiMAX Device accepts for a session expiration time when it receives a request to start a SIP session. If the request has a shorter time, the WiMAX Device rejects it. |
| RTP Port Range | |
| Start Port End Port | <p>Enter the listening port number(s) for RTP traffic, if your VoIP service provider gave you this information. Otherwise, keep the default values.</p> <p>To enter one port number, enter the port number in the Start Port and End Port fields.</p> <p>To enter a range of ports:</p> <ul style="list-style-type: none"> Type the port number at the beginning of the range in the Start Port field Type the port number at the end of the range in the End Port field. |
| Voice Compression | |
| Primary, Secondary, and Third Compression | <p>Select the type of voice coder/decoder (codec) that you want the WiMAX Device to use.</p> <p>G.711 provides high voice quality but requires more bandwidth (64 kbps).</p> <ul style="list-style-type: none"> G.711A is typically used in Europe. G.711u is typically used in North America and Japan. G.723 provides good voice quality, and requires 20 or 40 kbps. G.729 requires only 8 kbps. <p>The WiMAX Device must use the same codec as the peer. When two SIP devices start a SIP session, they must agree on a codec.</p> <p>For more on voice compression, see Voice Coding on page 152</p> |
| DTMF Mode | <p>Control how the WiMAX Device handles the tones that your telephone makes when you push its buttons. You should use the same mode your VoIP service provider uses.</p> <ul style="list-style-type: none"> RFC 2833 - send the DTMF tones in RTP packets PCM - send the DTMF tones in the voice data stream. This method works best when you are using a codec that does not use compression (like G.711). Codecs that use compression (like G.729) can distort the tones. SIP INFO - send the DTMF tones in SIP messages |
| STUN | |

Table 57 VOICE > Service Configuration > SIP Settings > Advanced (continued)

| LABEL | DESCRIPTION |
|----------------------------------|--|
| Active | Select this if all of the following conditions are satisfied. <ul style="list-style-type: none"> • There is a NAT router between the WiMAX Device and the SIP server. • The NAT router is not a SIP ALG. • Your VoIP service provider gave you an IP address or domain name for a STUN server. • Otherwise, clear this field. |
| Server Address | Enter the IP address or domain name of the STUN server provided by your VoIP service provider. |
| Server Port | Enter the STUN server's listening port, if your VoIP service provider gave you one. Otherwise, keep the default value. |
| Use NAT | |
| Active | Select this if you want the WiMAX Device to send SIP traffic to a specific NAT router. You must also configure the NAT router to forward traffic with the specified port to the WiMAX Device. This eliminates the need for STUN or a SIP ALG. |
| Server Address | Enter the public IP address or domain name of the NAT router. |
| Server Port | Enter the port number that your SIP sessions use with the public IP address of the NAT router. |
| Outbound Proxy | |
| Active | Select this if your VoIP service provider has a SIP outbound server to handle voice calls. This allows the WiMAX Device to work with any type of NAT router and eliminates the need for STUN or a SIP ALG. Turn off any SIP ALG on a NAT router in front of the WiMAX Device to keep it from re-translating the IP address (since this is already handled by the outbound proxy server). |
| Server Address | Enter the IP address or domain name of the SIP outbound proxy server. |
| Server Port | Enter the SIP outbound proxy server's listening port, if your VoIP service provider gave you one. Otherwise, keep the default value. |
| NAT Keep Alive | |
| Active | Select this to stop NAT routers between the WiMAX Device and SIP server (a SIP proxy server or outbound proxy server) from dropping the SIP session. The WiMAX Device does this by sending SIP notify messages to the SIP server based on the specified interval. |
| Keep Alive with SIP Proxy | Select this if the SIP server is a SIP proxy server. |
| Keep Alive with Outbound Proxy | Select this if the SIP server is an outbound proxy server. You must enable Outbound Proxy to use this. |
| Keep Alive Interval | Enter how often (in seconds) the WiMAX Device should send SIP notify messages to the SIP server. |
| MWI (Message Waiting Indication) | |
| Enable | Select this if you want to hear a waiting (beeping) dial tone on your phone when you have at least one voice message. Your VoIP service provider must support this feature. |

Table 57 VOICE > Service Configuration > SIP Settings > Advanced (continued)

| LABEL | DESCRIPTION |
|-----------------------|---|
| Expiration Time | Keep the default value, unless your VoIP service provider tells you to change it. Enter the number of seconds the SIP server should provide the message waiting service each time the WiMAX Device subscribes to the service. Before this time passes, the WiMAX Device automatically subscribes again. |
| Fax Option | |
| G.711 Fax Passthrough | Select this if the WiMAX Device should use G.711 to send fax messages. The peer devices must also use G.711. |
| T.38 Fax Relay | Select this if the WiMAX Device should send fax messages as UDP or TCP/IP packets through IP networks. This provides better quality, but it may have inter-operability problems. The peer devices must also use T.38. |
| Call Forward | |
| Call Forward Table | Select which call forwarding table you want the WiMAX Device to use for incoming calls. You set up these tables in VOICE > Phone Book > Incoming Call Policy . |
| Caller Ringing | |
| Enable | Check this box if you want people to hear a customized recording when they call you. |
| Caller Ringing Tone | Select the tone you want people to hear when they call you. See Custom Tones (IVR) on page 156 for information on how to record these tones. |
| On Hold | |
| Enable | Check this box if you want people to hear a customized recording when you put them on hold. |
| On Hold Tone | Select the tone you want people to hear when you put them on hold. See Custom Tones (IVR) on page 156 for information on how to record these tones. |
| Back | Click this to return to the SIP Settings screen without saving your changes. |
| Apply | Click to save your changes. |
| Reset | Click to restore your previously saved settings. |

12.2.1.6 Custom Tones (IVR)

IVR (Interactive Voice Response) is a feature that allows you to use your telephone to interact with the WiMAX Device. The WiMAX Device allows you to record custom tones for the **Caller Ringing Tone** and **On Hold Tone** functions. The same recordings apply to both the caller ringing and on hold tones.

Table 58 Custom Tones Details

| LABEL | DESCRIPTION |
|--------------------------|---|
| Total Time for All Tones | 128 seconds for all custom tones combined |

Table 58 Custom Tones Details

| LABEL | DESCRIPTION |
|----------------------------------|--|
| Maximum Time per Individual Tone | 20 seconds |
| Total Number of Tones Recordable | 8 You can record up to eight different custom tones but the total time must be 128 seconds or less. |

Use the following steps if you would like to create new tones or change your tones:

- 1 Pick up the phone and press **** on your phone's keypad and wait for the message that says you are in the configuration menu.
- 2 Press a number from 1101~1108 on your phone followed by the # key.
- 3 Play your desired music or voice recording into the receiver's mouthpiece. Press the # key.
- 4 You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

Do the following to listen to a custom tone:

- 1 Pick up the phone and press **** on your phone's keypad and wait for the message that says you are in the configuration menu.
- 2 Press a number from 1201~1208 followed by the # key to listen to the tone.
- 3 You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

Do the following to delete a custom tone:

- 1 Pick up the phone and press **** on your phone's keypad and wait for the message that says you are in the configuration menu.
- 2 Press a number from 1301~1308 followed by the # key to delete the tone of your choice. Press 14 followed by the # key if you wish to clear all your custom tones.
- 3 You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

12.3 QoS

Network traffic can be classified by setting the ToS (Type Of Service) values at the data source (for example, at the WiMAX Device) so a server can decide the best method of delivery, that is the least cost, fastest route and so on.

Virtual Local Area Network (VLAN) allows a physical network to be partitioned into multiple logical networks. Only stations within the same group can communicate with each other.

Your WiMAX Device can add IEEE 802.1Q VLAN ID tags to voice frames that it sends to the network. This allows the WiMAX Device to communicate with a SIP server that is a member of the same VLAN group. Some ISPs use the VLAN tag to identify voice traffic and give it priority over other traffic.

Click **VOICE > Service Configuration > QoS** to set up and maintain ToS and VLAN settings for the WiMAX Device. QoS (Quality of Service) refers to both a network's ability to deliver data with minimum delay and the networking methods used to provide bandwidth for real-time multimedia applications.

Figure 72 VOICE > Service Configuration > QoS

The screenshot shows a configuration interface for QoS. It has a title bar 'TOS' and a dashed line separator. Below the separator, there are two rows of settings: 'SIP TOS Priority Setting:' with a text input field containing '5' and '(0-255)' to its right, and 'RTP TOS Priority Setting:' with a text input field containing '5' and '(0-255)' to its right. Another dashed line separator follows. Below it is the 'VLAN Taging' section, which includes a checkbox labeled 'Voice VLAN ID:' followed by a text input field containing '5' and '(0-4095)' to its right. At the bottom right of the form are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

Table 59 VOICE > Service Configuration > QoS

| LABEL | DESCRIPTION |
|--------------------------|---|
| TDS | |
| SIP TOS Priority Setting | Enter the priority for SIP voice transmissions. The WiMAX Device creates Type of Service priority tags with this priority to voice traffic that it transmits. |
| RTP TOS Priority Setting | Enter the priority for RTP voice transmissions. The WiMAX Device creates Type of Service priority tags with this priority to RTP traffic that it transmits. |
| VLAN Taging | |

Table 59 VOICE > Service Configuration > QoS

| LABEL | DESCRIPTION |
|---------------|---|
| Voice VLAN ID | Select this if the WiMAX Device has to be a member of a VLAN to communicate with the SIP server. Ask your network administrator, if you are not sure. Enter the VLAN ID provided by your network administrator in the field on the right. Your LAN and gateway must be configured to use VLAN tags. Otherwise, clear this field. |
| Apply | Click to save your changes. |
| Reset | Click to restore your previously saved settings. |

12.4 Technical Reference

The following section contains additional technical information about the WiMAX Device features described in this chapter.

12.4.1 SIP Call Progression

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

Table 60 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.

12.4.2 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.

12.4.3 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 73 SIP User Agent



12.4.4 SIP Proxy Server

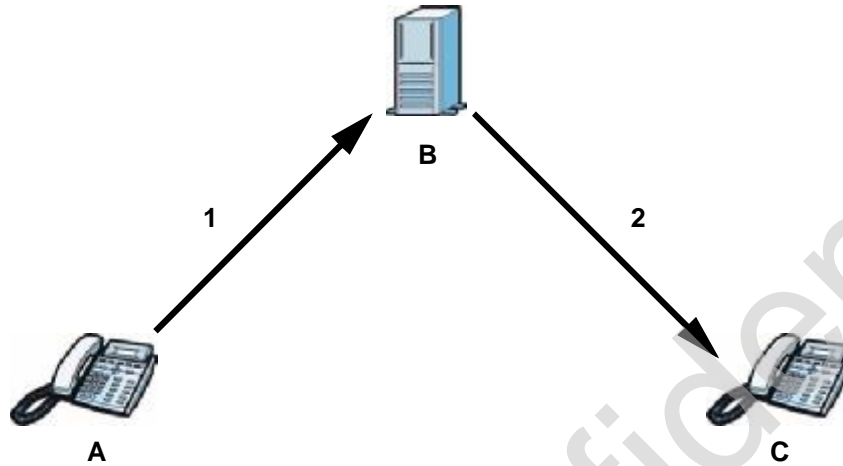
A SIP proxy server receives requests from clients and forwards them to another server.

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 74 SIP Proxy Server



12.4.5 SIP Redirect Server

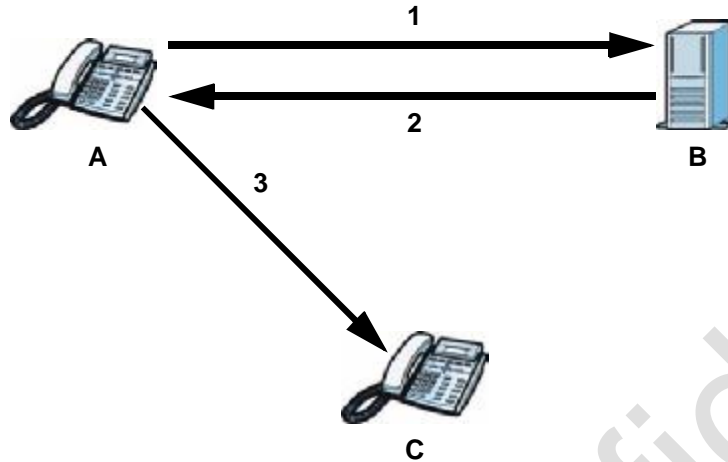
A SIP redirect server accepts SIP requests, translates the destination address to an IP address and sends the translated IP address back to the device that sent the request. Then the client device that originally sent the request can send requests to the IP address that it received back from the redirect 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 75 SIP Redirect Server



12.4.6 NAT and SIP

The WiMAX Device must register its public IP address with a SIP register server. If there is a NAT router between the WiMAX Device and the SIP register server, the WiMAX Device probably has a private IP address. The WiMAX 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 WiMAX Device's IP address from inside the SIP message and maps it to your SIP identity. If the WiMAX Device has a private IP address listed in the SIP message, the SIP server cannot map it to your SIP identity. See [Chapter 10 The NAT Configuration Screens](#) for more information.

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

12.4.7 DiffServ

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

12.4.8 DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

Figure 76 DiffServ: Differentiated Service Field

| | |
|-----------------|-------------------|
| DSCP (6-bit) | Unused (2-bit) |
|-----------------|-------------------|

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

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

Company Confidential

The Phone Screens

13.1 Overview

Use the **VOICE > Phone** screens to configure the volume, echo cancellation, VAD settings and custom tones for the phone port on the WiMAX Device. You can also select which SIP account to use for making outgoing calls.

13.1.1 What You Can Do in This Chapter

- The **Analog Phone** screen ([Section 13.2 on page 166](#)) lets you control which SIP accounts each phone uses.
- The **Common** screen ([Section 13.3 on page 169](#)) lets you activate and deactivate immediate dialing.
- The **Region** screen ([Section 13.4 on page 170](#)) lets you maintain settings that often depend on the region of the world in which the WiMAX Device is located.

13.1.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

Voice Activity Detection/Silence Suppression/Comfort Noise

Voice Activity Detection (VAD) detects whether or not speech is present. This lets the WiMAX Device reduce the bandwidth that a call uses by not transmitting "silent packets" when you are not speaking.

When using VAD, the WiMAX Device generates comfort noise when the other party is not speaking. The comfort noise lets you know that the line is still connected as total silence could easily be mistaken for a lost connection.

Echo Cancellation

G.168 is an ITU-T standard for eliminating the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.

Supplementary Phone Services Overview

Supplementary services such as call hold, call waiting, call transfer, etc. are generally available from your VoIP service provider. The WiMAX Device supports the following services:

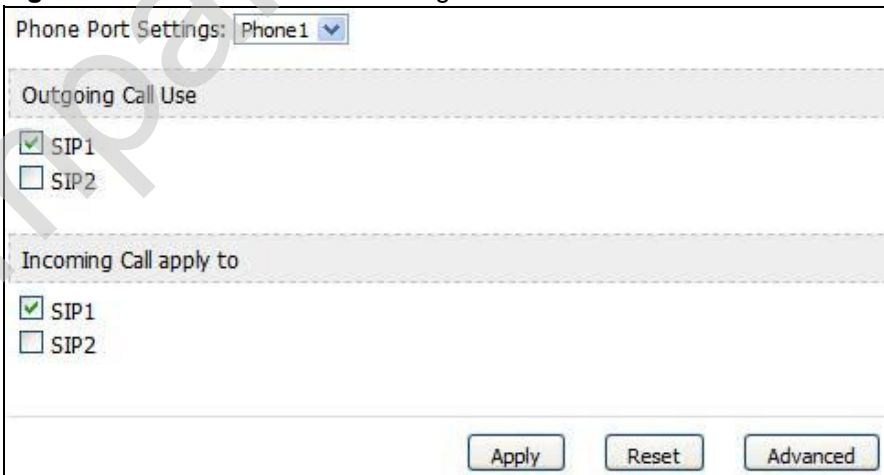
- Call Hold
- Call Waiting
- Making a Second Call
- Call Transfer
- Call Forwarding
- Three-Way Conference
- Internal Calls
- Caller ID
- CLIP (Calling Line Identification Presentation)
- CLIR (Calling Line Identification Restriction)

Note: To take full advantage of the supplementary phone services available through the WiMAX Device's phone port, you may need to subscribe to the services from your VoIP service provider.

13.2 Analog Phone

Click **VOICE > Phone > Analog Phone** to control which SIP accounts each phone uses.

Figure 77 VOICE > Phone > Analog Phone



Phone Port Settings: Phone1

Outgoing Call Use

SIP1
 SIP2

Incoming Call apply to

SIP1
 SIP2

Apply Reset Advanced

The following table describes the labels in this screen.

Table 61 VOICE > Phone > Analog Phone

| LABEL | DESCRIPTION |
|------------------------|--|
| Phone Port Settings | Select the phone port you want to see in this screen. If you change this field, the screen automatically refreshes. |
| Outgoing Call Use | |
| SIP1 | Select this if you want this phone port to use the SIP1 account when it makes calls. If you select both SIP accounts, the WiMAX Device tries to use SIP2 first. |
| SIP2 | Select this if you want this phone port to use the SIP2 account when it makes calls. If you select both SIP accounts, the WiMAX Device tries to use SIP2 first. |
| Incoming Call apply to | |
| SIP1 | Select this if you want to receive phone calls for the SIP1 account on this phone port. If you select more than one source for incoming calls, there is no way to distinguish between them when you receive phone calls. |
| SIP2 | Select this if you want to receive phone calls for the SIP2 account on this phone port. If you select more than one source for incoming calls, there is no way to distinguish between them when you receive phone calls. |
| Apply | Click to save your changes. |
| Reset | Click to restore your previously saved settings. |
| Advanced Setup | Click this to edit the advanced settings for this phone port. The Advanced Analog Phone Setup screen appears. |

13.2.1 Advanced Analog Phone Setup

Click the **Advanced** button in **VOICE > Phone > Analog Phone** to edit advanced settings for each phone port.

Figure 78 VOICE > Phone > Analog Phone > Advanced

The following table describes the labels in this screen.

Table 62 VOICE > Phone > Analog Phone > Advanced

| LABEL | DESCRIPTION |
|-------------------------|--|
| Voice Volume Control | |
| Speaking Volume | Enter the loudness that the WiMAX Device uses for speech that it sends to the peer device. -1 is the quietest, and 1 is the loudest. |
| Listening Volume | Enter the loudness that the WiMAX Device uses for speech that it receives from the peer device. -1 is the quietest, and 1 is the loudest. |
| Echo Cancellation | |
| G.168 Active | Select this if you want to eliminate the echo caused by the sound of your voice reverberating in the telephone receiver while you talk. |
| Dialing Interval Select | |
| Dialing Interval Select | Enter the number of seconds the WiMAX Device should wait after you stop dialing numbers before it makes the phone call. The value depends on how quickly you dial phone numbers. If you select Active Immediate Dial in VOICE > Phone > Common , you can press the pound key (#) to tell the WiMAX Device to make the phone call immediately, regardless of this setting. |
| VAD Support | Select this if the WiMAX Device should stop transmitting when you are not speaking. This reduces the bandwidth the WiMAX Device uses. Note: The G.711 codec does not support this feature. |

Table 62 VOICE > Phone > Analog Phone > Advanced

| LABEL | DESCRIPTION |
|-------|---|
| Back | Click this to return to the Analog Phone screen without saving your changes. |
| Apply | Click to save your changes. |
| Reset | Click to restore your previously saved settings. |

13.3 Common

Click **VOICE > Phone > Common** to activate and deactivate immediate dialing.

Figure 79 VOICE > Phone > Common

The following table describes the labels in this screen.

Table 63 VOICE > Phone > Common

| LABEL | DESCRIPTION |
|-----------------------|--|
| Active Immediate Dial | Select this if you want to use the pound key (#) to tell the WiMAX Device to make the phone call immediately, instead of waiting the number of seconds you selected in the Dialing Interval Select in VOICE > Phone > Analog Phone . If you select this, dial the phone number, and then press the pound key if you do not want to wait. The WiMAX Device makes the call immediately. |
| Apply | Click to save your changes. |
| Reset | Click to restore your previously saved settings. |

13.4 Region

Click **VOICE > Phone > Region** to maintain settings that often depend on the region of the world in which the WiMAX Device is located.

Figure 80 VOICE > Phone > Region

The screenshot shows a settings screen with two dropdown menus. The first is labeled 'Region Settings' and is set to 'United States'. The second is labeled 'Call Service Mode' and is set to 'USA Type'. At the bottom right, there are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

Table 64 VOICE > Phone > Region

| LABEL | DESCRIPTION |
|-------------------|--|
| Region Settings | Select the place in which the WiMAX Device is located. Do not select Default. |
| Call Service Mode | Select the mode for supplementary phone services (call hold, call waiting, call transfer and three-way conference calls) that your VoIP service provider supports. <ul style="list-style-type: none"> • Europe Type - use supplementary phone services in European mode • USA Type - use supplementary phone services American mode You might have to subscribe to these services to use them. Contact your VoIP service provider. |
| Apply | Click to save your changes. |
| Reset | Click to restore your previously saved settings. |

13.5 Technical Reference

The following section contains additional technical information about the WiMAX Device features described in this chapter.

13.5.1 The Flash Key

Flashing means to press the hook for a short period of time (a few hundred milliseconds) before releasing it. On newer telephones, there should be a "flash" key (button) that generates the signal electronically. If the flash key is not available, you can tap (press and immediately release) the hook by hand to achieve the same effect. However, using the flash key is preferred since the timing is much more precise. The WiMAX Device may interpret manual tapping as hanging up if the duration is too long

You can invoke all the supplementary services by using the flash key.

13.5.2 Europe Type Supplementary Phone Services

This section describes how to use supplementary phone services with the **Europe Type Call Service Mode**. Commands for supplementary services are listed in the table below.

After pressing the flash key, if you do not issue the sub-command before the default sub-command timeout (2 seconds) expires or issue an invalid sub-command, the current operation will be aborted.

Table 65 European Type Flash Key Commands

| COMMAND | SUB-COMMAND | DESCRIPTION |
|---------|-------------|---|
| Flash | | Put a current call on hold to place a second call. Switch back to the call (if there is no second call). |
| Flash | 0 | Drop the call presently on hold or reject an incoming call which is waiting for answer. |
| Flash | 1 | Disconnect the current phone connection and answer the incoming call or resume with caller presently on hold. |
| Flash | 2 | 1. Switch back and forth between two calls. 2. Put a current call on hold to answer an incoming call. 3. Separate the current three-way conference call into two individual calls (one is on-line, the other is on hold). |
| Flash | 3 | Create three-way conference connection. |
| Flash | *98# | Transfer the call to another phone. |

European Call Hold allows you to put a call (A) on hold by pressing the flash key.

If you have another call, press the flash key and then "2" to switch back and forth between caller A and B by putting either one on hold.

Press the flash key and then "0" to disconnect the call presently on hold and keep the current call on line.

Press the flash key and then "1" to disconnect the current call and resume the call on hold.

If you hang up the phone but a caller is still on hold, there will be a remind ring.

European Call Waiting allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.

If there is a second call to a telephone number, you will hear a call waiting tone. Take one of the following actions.

- Reject the second call.
Press the flash key and then press "0".
- Disconnect the first call and answer the second call.
Either press the flash key and press "1", or just hang up the phone and then answer the phone after it rings.
- Put the first call on hold and answer the second call.
Press the flash key and then "2".

European Call Transfer allows you to transfer an incoming call (that you have answered) to another phone. To do so:

- 1 Press the flash key to put the caller on hold.
- 2 When you hear the dial tone, dial "*98#" followed by the number to which you want to transfer the call. to operate the Intercom.
- 3 After you hear the ring signal or the second party answers it, hang up the phone.

European Three-Way Conference allows you to make three-way conference calls. To do so:

- 1 When you are on the phone talking to someone, place the flash key to put the caller on hold and get a dial tone.
- 2 Dial a phone number directly to make another call.
- 3 When the second call is answered, press the flash key and press "3" to create a three-way conversation.
- 4 Hang up the phone to drop the connection.
- 5 If you want to separate the activated three-way conference into two individual connections (one is on-line, the other is on hold), press the flash key and press "2".

13.5.3 USA Type Supplementary Services

This section describes how to use supplementary phone services with the **USA Type Call Service Mode**. Commands for supplementary services are listed in the table below.

After pressing the flash key, if you do not issue the sub-command before the default sub-command timeout (2 seconds) expires or issue an invalid sub-command, the current operation will be aborted.

Table 66 USA Type Flash Key Commands

| COMMAND | SUB-COMMAND | DESCRIPTION |
|---------|-------------|--|
| Flash | | Put a current call on hold to place a second call. After the second call is successful, press the flash key again to have a three-way conference call. Put a current call on hold to answer an incoming call. |
| Flash | *98# | Transfer the call to another phone. |

USA Call Hold allows you to put a call (A) on hold by pressing the flash key.

If you have another call, press the flash key to switch back and forth between caller A and B by putting either one on hold.

If you hang up the phone but a caller is still on hold, there will be a remind ring.

USA Call Waiting allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.

If there is a second call to your telephone number, you will hear a call waiting tone.

Press the flash key to put the first call on hold and answer the second call.

USA Call Transfer allows you to transfer an incoming call (that you have answered) to another phone. To do so:

- 1 Press the flash key to put the caller on hold.
- 2 When you hear the dial tone, dial "*98#" followed by the number to which you want to transfer the call. to operate the Intercom.
- 3 After you hear the ring signal or the second party answers it, hang up the phone.

USA Three-Way Conference allows you to make three-way conference calls. To do so:

- 1 When you are making a call, press the flash key to put the call on hold and get a dial tone.
- 2 Dial a phone number to make a second call.
- 3 When the second call is answered, press the flash key to create a three-way conversation.
- 4 If you want to separate the three-way conference into two individual calls (one call is online, the other is on hold), press the flash key. The first call is online and the second call is on hold. Pressing the flash key again will recreate the three-way conversation. The next time you press the flash key, the second call is online and the first call is on hold.
- 5 Hang up the phone to drop the connection.

The Phone Book Screens

14.1 Overview

The VOICE > Phone Book screens allow you to configure the WiMAX Device's phone book for making VoIP calls.

14.1.1 What You Can Do in This Chapter

- The Incoming Call Policy screen ([Section 14.2 on page 176](#)) lets you maintain rules for handling incoming calls. You can block, redirect, or accept them.
- The Speed Dial screen ([Section 14.3 on page 178](#)) lets you add, edit, or remove speed-dial entries.

14.1.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

Speed Dial and Peer-to-Peer Calling

Speed dial provides shortcuts for dialing frequently used (VoIP) phone numbers. It is also required if you want to make peer-to-peer calls.

In peer-to-peer calls, you call another VoIP device directly without going through a SIP server. In the WiMAX Device, you must set up a speed dial entry in the phone book in order to do this. Select **Non-Proxy (Use IP or URL)** in the **Type** column and enter the callee's IP address or domain name. The WiMAX Device sends SIP INVITE requests to the peer VoIP device when you use the speed dial entry.

You do not need to configure a SIP account in order to make a peer-to-peer VoIP call.

14.2 Incoming Call Policy

Click **VOICE > Phone Book > Incoming Call Policy** to maintain rules for handling incoming calls. You can block, redirect, or accept them.

Figure 81 VOICE > Phone Book > Incoming Call Policy

The following table describes the labels in this screen.

Table 67 VOICE > Phone Book > Incoming Call Policy

| LABEL | DESCRIPTION |
|---------------------------------|--|
| Table Number | Select the call-forwarding table you want to see in this screen. If you change this field, the screen automatically refreshes. |
| Forward to Number Setup | |
| Unconditional Forward to Number | Select this if you want the WiMAX Device to forward all incoming calls to the specified phone number, regardless of other rules in the Forward to Number section. Specify the phone number in the field on the right. |
| Busy Forward to Number | Select this if you want the WiMAX Device to forward incoming calls to the specified phone number if the phone port is busy. Specify the phone number in the field on the right. If you have call waiting, the incoming call is forwarded to the specified phone number if you reject or ignore the second incoming call. |

Table 67 VOICE > Phone Book > Incoming Call Policy

| LABEL | DESCRIPTION |
|-----------------------------|--|
| No Answer Forward to Number | Select this if you want the WiMAX Device to forward incoming calls to the specified phone number if the call is unanswered. (See No Answer Waiting Time .) Specify the phone number in the field on the right. |
| No Answer Waiting Time | This field is used by the No Answer Forward to Number feature and No Answer conditions below. Enter the number of seconds the WiMAX Device should wait for you to answer an incoming call before it considers the call is unanswered. |
| Advanced Setup | |
| # | The number of the item in this list. |
| Activate | Select this to enable this rule. Clear this to disable this rule. |
| Incoming Call Number | Enter the phone number to which this rule applies. |
| Forward to Number | Enter the phone number to which you want to forward incoming calls from the Incoming Call Number . You may leave this field blank, depending on the Condition . |
| Condition | Select the situations in which you want to forward incoming calls from the Incoming Call Number , or select an alternative action. <ul style="list-style-type: none"> • Unconditional - The WiMAX Device immediately forwards any calls from the Incoming Call Number to the Forward to Number. • Busy - The WiMAX Device forwards any calls from the Incoming Call Number to the Forward to Number when your SIP account already has a call connected. • No Answer - The WiMAX Device forwards any calls from the Incoming Call Number to the Forward to Number when the call is unanswered. (See No Answer Waiting Time.) • Block - The WiMAX Device rejects calls from the Incoming Call Number. • Accept - The WiMAX Device allows calls from the Incoming Call Number. You might create a rule with this condition if you do not want incoming calls from someone to be forwarded by rules in the Forward to Number section. |
| Apply | Click to save your changes. |
| Reset | Click to restore your previously saved settings. |

Note: The WiMAX Device checks the Advanced rules first before checking the Forward to Number rules. All rules are checked in order from top to bottom.

14.3 Speed Dial

Click **VOICE > Phone Book > Speed Dial** to add, edit, or remove speed-dial entries.


You must create speed-dial entries if you want to make peer-to-peer calls or call SIP numbers that use letters. You can also create speed-dial entries for frequently-used SIP phone numbers.

Figure 82 VOICE > Phone Book > Speed Dial

The screenshot shows the 'Speed Dial Setup' and 'Speed Dial Phone Book' sections. The 'Speed Dial Setup' section has the following fields: 'Speed Dial' (dropdown menu with '#01' selected), 'Number' (text input), 'Name' (text input), and 'Type' (radio buttons for 'Use Proxy' and 'Non-Proxy (Use IP or URL)'). There is an 'Add' button to the right of the 'Type' section. The 'Speed Dial Phone Book' section is a table with the following columns: '#', 'Number', 'Name', 'Destination', and 'Action'. The 'Action' column contains a delete icon for each row. At the bottom of the page, there are 'Clear' and 'Reset' buttons.

The following table describes the icons in this screen.

Table 68 Advanced > LAN Configuration > IP Static Route

| ICON | DESCRIPTION |
|---|--------------------------------------|
|  | Delete Click to delete this item. |

The following table describes the labels in this screen.

Table 69 VOICE > Phone Book > Speed Dial

| LABEL | DESCRIPTION |
|-------------|--|
| Speed Dial | Select the speed-dial number you want to use for this phone number. |
| Number | Enter the SIP number you want the WiMAX Device to call when you dial the speed-dial number. |
| Name | Enter a name to identify the party you call when you dial the speed-dial number. You can use up to 127 printable ASCII characters. |
| Type | Select Use Proxy if you want to use one of your SIP accounts to call this phone number. Select Non-Proxy (Use IP or URL) if you want to use a different SIP server or if you want to make a peer-to-peer call. In this case, enter the IP address or domain name of the SIP server or the other party in the field below. |
| Add | Click to add the new number to the list below. |
| # | This is a list of speed dial numbers. |
| Number | This is the SIP number the WiMAX Device calls when you use this speed dial number. |
| Name | This is the name of the party associated with this speed-dial number. |
| Type | This indicates whether this speed dial number uses a proxy or not when placing a call to the phone number associated with it. |
| Destination | This indicates if the speed-dial entry uses one of your SIP accounts or uses the IP address or domain name of the SIP server. |
| Action | Click the Delete icon to erase this speed-dial entry. |
| Apply | Click to save your changes. |
| Clear | Click to clear all fields on the screen and begin anew. |

Company Confidential

PART V

Tools & Status Screens

The Certificates Screens (183)

The Firewall Screens (203)

Content Filter (213)

The Remote Management Screens (217)

The Logs Screens (227)

The UPnP Screen (243)

The Status Screen (253)

Company Confidential

The Certificates Screens

15.1 Overview

Use the **TOOLS > Certificates** screens to manage public key certificates on the WiMAX Device.

The WiMAX Device can use public key certificates (also sometimes called “digital IDs”) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner’s identity and public key. Certificates provide a way to exchange public keys for use in authentication.

Public key certificates are used by web browsers to ensure that a secure web site is legitimate. When a certificate authority such as VeriSign, Comodo, or Network Solutions (to name a few) receives a certificate request from a website operator, they confirm that the web domain and contact information in the request match those on public record with a domain name registrar. If they match, then the certificate is issued to the website operator, who then places it on his site to be issued to all visiting web browsers to let them know that the site is legitimate.

15.1.1 What You Can Do in This Chapter

- The **My Certificates** screen ([Section 15.2 on page 184](#)) lets you generate and export self-signed certificates or certification requests and import the WiMAX Device’s CA-signed certificates.
- The **Trusted CAs** screen ([Section 15.3 on page 193](#)) lets you display a summary list of certificates of the certification authorities that you have set the WiMAX Device to accept as trusted.

15.1.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

Certificate Authorities

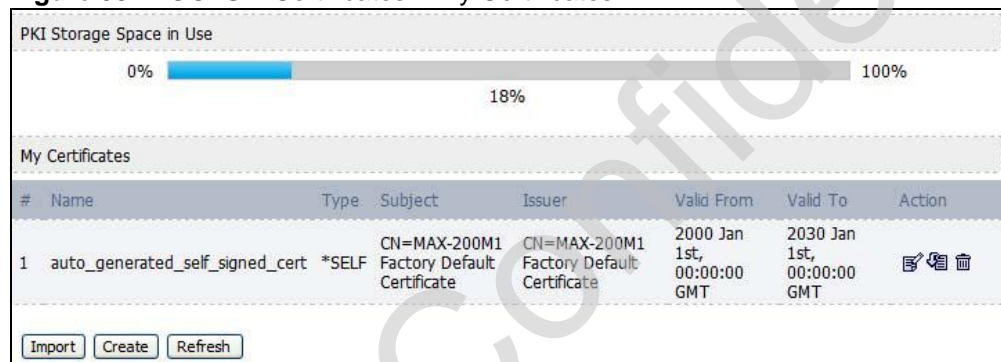
A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. You can use the

WiMAX Device to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

15.2 My Certificates

Click **TOOLS > Certificates > My Certificates** to generate and export self-signed certificates or certification requests and import the WiMAX Device's CA-signed certificates.

Figure 83 TOOLS > Certificates > My Certificates



The following table describes the icons in this screen.

Table 70 TOOLS > Certificates > My Certificates

| ICON | DESCRIPTION |
|------|--------------------------------------|
| | Edit Click to edit this item. |
| | Import Click to import an item. |
| | Delete Click to delete this item. |

The following table describes the labels in this screen.

Table 71 TOOLS > Certificates > My Certificates

| LABEL | DESCRIPTION |
|--------------------------|---|
| PKI Storage Space in Use | This bar displays the percentage of the WiMAX Device's PKI storage space that is currently in use. When the storage space is almost full, you should consider deleting expired or unnecessary certificates before adding more certificates. |
| # | The number of the item in this list. |

Table 71 TOOLS > Certificates > My Certificates (continued)

| LABEL | DESCRIPTION |
|------------|--|
| Name | This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name. |
| Type | <p>This field displays what kind of certificate this is.</p> <p>REQ represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the My Certificate Import screen to import the certificate and replace the request.</p> <p>SELF represents a self-signed certificate.</p> <p>*SELF represents the default self-signed certificate which signs the imported remote host certificates.</p> <p>CERT represents a certificate issued by a certification authority.</p> |
| Subject | This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information. |
| Issuer | This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the Subject field. |
| Valid From | This field displays the date that the certificate becomes applicable. |
| Valid To | This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired. |
| Action | <p>Click the Edit icon to open a screen with an in-depth list of information about the certificate.</p> <p>Click the Export icon to save a copy of the certificate without its private key. Browse to the location you want to use and click Save.</p> <p>Click the Delete icon to remove a certificate. A window displays asking you to confirm that you want to delete the certificate. Subsequent certificates move up by one when you take this action.</p> <p>The WiMAX Device keeps all of your certificates unless you specifically delete them. Uploading new firmware or default configuration file does not delete your certificates.</p> <p>You cannot delete certificates that any of the WiMAX Device's features are configured to use.</p> |
| Import | Click to a certificate into the WiMAX Device. |
| Create | Click to go to the screen where you can have the WiMAX Device generate a certificate or a certification request. |
| Refresh | Click to display the current validity status of the certificates. |

15.2.1 My Certificates Create

Click **TOOLS > Certificates > My Certificates** and then the **Create** icon to open the **My Certificates Create** screen. Use this screen to have the WiMAX Device create a self-signed certificate, enroll a certificate with a certification authority or generate a certification request.

Figure 84 TOOLS > Certificates > My Certificates > Create

Certificate Name:

Subject Information

Common Name:

Host IP Address: . . .

Host Domain Name:

E-Mail:

Organizational Unit:

Organization:

Country:

Key Length: 1024

Enrollment Options

Create a self-signed certificate

Create a certification request and save it locally for later manual enrollment

Create a certification request and enroll for a certificate immediately online

Enrollment Protocol: Simple Certificate Enrollment Protocol (SCEP)

CA Server Address:

CA Certificate: (See [Trusted CAs](#))

Request Authentication

Key:

The following table describes the labels in this screen.

Table 72 TOOLS > Certificates > My Certificates > Create

| LABEL | DESCRIPTION |
|--|---|
| Certificate Name | Type a name to identify this certificate. You can use up to 31 alphanumeric and ;`~!@#\$\$%^&()_+[]{}',.- characters. |
| Subject Information | Use these fields to record information that identifies the owner of the certificate. You do not have to fill in every field, although the Common Name is mandatory. The certification authority may add fields (such as a serial number) to the subject information when it issues a certificate. It is recommended that each certificate have unique subject information. |
| Common Name | <p>Select a radio button to identify the certificate's owner by IP address, domain name or e-mail address. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address is for identification purposes only and can be any string.</p> <p>A domain name can be up to 255 characters. You can use alphanumeric characters, the hyphen and periods.</p> <p>An e-mail address can be up to 63 characters. You can use alphanumeric characters, the hyphen, the @ symbol, periods and the underscore.</p> |
| Organizational Unit | Identify the organizational unit or department to which the certificate owner belongs. You can use up to 63 characters. You can use alphanumeric characters, the hyphen and the underscore. |
| Organization | Identify the company or group to which the certificate owner belongs. You can use up to 63 characters. You can use alphanumeric characters, the hyphen and the underscore. |
| Country | Identify the state in which the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore. |
| Key Length | Select a number from the drop-down list box to determine how many bits the key should use (512 to 2048). The longer the key, the more secure it is. A longer key also uses more PKI storage space. |
| Enrollment Options | These radio buttons deal with how and when the certificate is to be generated. |
| Create a self-signed certificate | Select Create a self-signed certificate to have the WiMAX Device generate the certificate and act as the Certification Authority (CA) itself. This way you do not need to apply to a certification authority for certificates. |
| Create a certification request and save it locally for later manual enrollment | <p>Select Create a certification request and save it locally for later manual enrollment to have the WiMAX Device generate and store a request for a certificate. Use the My Certificate Details screen to view the certification request and copy it to send to the certification authority.</p> <p>Copy the certification request from the My Certificate Details screen and then send it to the certification authority.</p> |

Table 72 TOOLS > Certificates > My Certificates > Create

| LABEL | DESCRIPTION |
|--|---|
| Create a certification request and enroll for a certificate immediately online | <p>Select Create a certification request and enroll for a certificate immediately online to have the WiMAX Device generate a request for a certificate and apply to a certification authority for a certificate.</p> <p>You must have the certification authority's certificate already imported in the Trusted CAs screen.</p> <p>When you select this option, you must select the certification authority's enrollment protocol and the certification authority's certificate from the drop-down list boxes and enter the certification authority's server address. You also need to fill in the Reference Number and Key if the certification authority requires them.</p> |
| Enrollment Protocol | <p>This field applies when you select Create a certification request and enroll for a certificate immediately online. Select the certification authority's enrollment protocol from the drop-down list box.</p> <p>Simple Certificate Enrollment Protocol (SCEP) is a TCP-based enrollment protocol that was developed by VeriSign and Cisco.</p> <p>Certificate Management Protocol (CMP) is a TCP-based enrollment protocol that was developed by the Public Key Infrastructure X.509 working group of the Internet Engineering Task Force (IETF) and is specified in RFC 2510.</p> |
| CA Server Address | <p>This field applies when you select Create a certification request and enroll for a certificate immediately online. Enter the IP address (or URL) of the certification authority server.</p> <p>For a URL, you can use up to 511 of the following characters. a-zA-Z0-9'()+,/:.=?;!*#@\$_%&-</p> |
| CA Certificate | <p>This field applies when you select Create a certification request and enroll for a certificate immediately online. Select the certification authority's certificate from the CA Certificate drop-down list box.</p> <p>You must have the certification authority's certificate already imported in the Trusted CAs screen. Click Trusted CAs to go to the Trusted CAs screen where you can view (and manage) the WiMAX Device's list of certificates of trusted certification authorities.</p> |
| Request Authentication | <p>When you select Create a certification request and enroll for a certificate immediately online, the certification authority may want you to include a reference number and key to identify you when you send a certification request.</p> <p>Fill in both the Reference Number and the Key fields if your certification authority uses CMP enrollment protocol. Just the Key field displays if your certification authority uses the SCEP enrollment protocol.</p> <p>For the reference number, use 0 to 999999999.</p> <p>For the key, use up to 31 of the following characters. a-zA-Z0-9; `~!@#%&^*()_+\\{}':./<>=-</p> |

The following table describes the labels in this screen.

Table 73 TOOLS > Certificates > My Certificates > Edit

| LABEL | DESCRIPTION |
|----------------------------------|---|
| Name | This field displays the identifying name of this certificate. You can use up to 31 alphanumeric and ;`~!@#%&^&()_+[]{}',.- characters. |
| Property | Select Default self-signed certificate which signs the imported remote host certificates to use this certificate to sign the remote host certificates you upload in the TOOLS > Certificates > Trusted CAs screen. |
| Certification Path | This field displays for a certificate, not a certification request. Click the Refresh button to have this read-only text box display the hierarchy of certification authorities that validate the certificate (and the certificate itself). If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the certificate itself). If the certificate is a self-signed certificate, the certificate itself is the only one in the list. The WiMAX Device does not trust the certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked. |
| Refresh | Click to display the certification path. |
| Certification Information | |
| Type | This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). "X.509" means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates. |
| Version | This field displays the X.509 version number. " |
| Serial Number | This field displays the certificate's identification number given by the certification authority or generated by the WiMAX Device. |
| Subject | This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C). |
| Issuer | This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same as the Subject Name field. "none" displays for a certification request. |
| Signature Algorithm | This field displays the type of algorithm that was used to sign the certificate. The WiMAX Device uses rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Some certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm). |
| Valid From | This field displays the date that the certificate becomes applicable. "none" displays for a certification request. |

Table 73 TOOLS > Certificates > My Certificates > Edit

| LABEL | DESCRIPTION |
|---|--|
| Valid To | This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired. "none" displays for a certification request. |
| Key Algorithm | This field displays the type of algorithm that was used to generate the certificate's key pair (the WiMAX Device uses RSA encryption) and the length of the key set in bits (1024 bits for example). |
| Subject Alternative Name | This field displays the certificate owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL). |
| Key Usage | This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text. |
| Basic Constraint | This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path. This field does not display for a certification request. |
| MD5 Fingerprint | This is the certificate's message digest that the WiMAX Device calculated using the MD5 algorithm. |
| SHA1 Fingerprint | This is the certificate's message digest that the WiMAX Device calculated using the SHA1 algorithm. |
| Certificate in PEM (Base-64) Encoded Format | <p>This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses lowercase letters, uppercase letters and numerals to convert the binary certificate into a printable form.</p> <p>You can copy and paste a certification request into a certification authority's web page, an e-mail that you send to the certification authority or a text editor and save the file on a management computer for later manual enrollment.</p> <p>You can copy and paste a certificate into an e-mail to send to friends or colleagues or you can copy and paste a certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).</p> |
| Apply | Click to save your changes. |
| Cancel | Click to return to the previous screen without saving your changes. |

15.2.3 My Certificate Import

Click **TOOLS > Certificates > My Certificates > Import** to import a certificate that matches a corresponding certification request that was generated by the WiMAX Device. You must remove any spaces from the certificate's filename before you can import it.

Figure 86 TOOLS > Certificates > My Certificates > Import

The following table describes the labels in this screen.

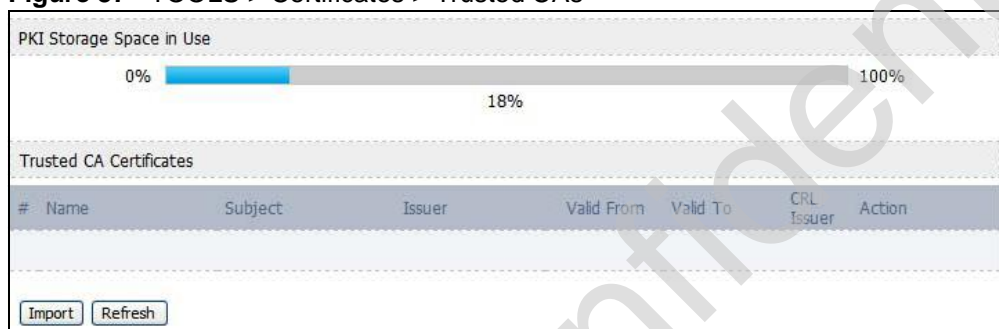
Table 74 TOOLS > Certificates > My Certificates > Import

| LABEL | DESCRIPTION |
|-----------|--|
| File Path | Type in the location of the file you want to upload in this field or click Browse to find it. You cannot import a certificate with the same name as a certificate that is already in the WiMAX Device. |
| Browse | Click to find the certificate file you want to upload. |
| Apply | Click to save your changes. |
| Cancel | Click to return to the previous screen without saving your changes. |

15.3 Trusted CAs




Click **TOOLS > Certificates > Trusted CAs** to display a summary list of certificates of the certification authorities that you have set the WiMAX Device to accept as trusted. The WiMAX Device accepts any valid certificate signed by a certification authority on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certification authorities.

Figure 87 TOOLS > Certificates > Trusted CAs



The following table describes the icons in this screen.

Table 75 TOOLS > Certificates > Trusted CAs

| ICON | DESCRIPTION |
|---|--------------------------------------|
|  | Edit Click to edit this item. |
|  | Export Click to export an item. |
|  | Delete Click to delete this item. |

The following table describes the labels in this screen.

Table 76 TOOLS > Certificates > Trusted CAs

| LABEL | DESCRIPTION |
|--------------------------|--|
| PKI Storage Space in Use | This bar displays the percentage of the WiMAX Device's PKI storage space that is currently in use. When the storage space is almost full, you should consider deleting expired or unnecessary certificates before adding more certificates. |
| # | The number of the item in this list. |
| Name | This field displays the name used to identify this certificate. |
| Subject | This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information. |

Table 76 TOOLS > Certificates > Trusted CAs (continued)

| LABEL | DESCRIPTION |
|------------|---|
| Issuer | This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the Subject field. |
| Valid From | This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable. |
| Valid To | This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired. |
| CRL Issuer | This field displays Yes if the certification authority issues CRL (Certificate Revocation Lists) for the certificates that it has issued and you have selected the Check incoming certificates issued by this CA against a CRL check box in the certificate's details screen to have the WiMAX Device check the CRL before trusting any certificates issued by the certification authority. Otherwise the field displays No. |
| Action | <p>Click the Edit icon to open a screen with an in-depth list of information about the certificate.</p> <p>Use the Export icon to save the certificate to a computer. Click the icon and then Save in the File Download screen. The Save As screen opens, browse to the location that you want to use and click Save.</p> <p>Click the Delete icon to remove the certificate. A window displays asking you to confirm that you want to delete the certificate. Note that subsequent certificates move up by one when you take this action.</p> |
| Import | Click Import to open a screen where you can save the certificate of a certification authority that you trust, from your computer to the WiMAX Device. |
| Refresh | Click this button to display the current validity status of the certificates. |

15.3.1 Trusted CA Edit

Click **TOOLS > Certificates > Trusted CAs** and then click the **Edit** icon to open the **Trusted CAs** screen to view in-depth certificate information and change the certificate's name.

Figure 88 TOOLS > Certificates > Trusted CAs > Edit

The following table describes the labels in this screen.

Table 77 TOOLS > Certificates > Trusted CAs > Edit

| LABEL | DESCRIPTION |
|----------|--|
| Name | This field displays the identifying name of this certificate. You can use up to 31 alphanumeric and ;`~!@#\$\$%^&()_+[]{}',.- characters. |
| Property | Select Default self-signed certificate which signs the imported remote host certificates to use this certificate to sign the remote host certificates you upload in the TOOLS > Certificates > Trusted CAs screen. |

Table 77 TOOLS > Certificates > Trusted CAs > Edit (continued)

| LABEL | DESCRIPTION |
|---------------------------|--|
| Certification Path | <p>This field displays for a certificate, not a certification request.</p> <p>Click the Refresh button to have this read-only text box display the hierarchy of certification authorities that validate the certificate (and the certificate itself).</p> <p>If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the certificate itself). If the certificate is a self-signed certificate, the certificate itself is the only one in the list. The WiMAX Device does not trust the certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.</p> |
| Refresh | Click Refresh to display the certification path. |
| Certification Information | |
| Type | This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). "X.509" means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates. |
| Version | This field displays the X.509 version number. " |
| Serial Number | This field displays the certificate's identification number given by the certification authority or generated by the WiMAX Device. |
| Subject | This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C). |
| Issuer | <p>This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country.</p> <p>With self-signed certificates, this is the same as the Subject Name field.</p> <p>"none" displays for a certification request.</p> |
| Signature Algorithm | This field displays the type of algorithm that was used to sign the certificate. The WiMAX Device uses rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Some certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm). |
| Valid From | This field displays the date that the certificate becomes applicable. "none" displays for a certification request. |
| Valid To | This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired. "none" displays for a certification request. |
| Key Algorithm | This field displays the type of algorithm that was used to generate the certificate's key pair (the WiMAX Device uses RSA encryption) and the length of the key set in bits (1024 bits for example). |
| Subject Alternative Name | This field displays the certificate owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL). |

Table 77 TOOLS > Certificates > Trusted CAs > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Key Usage | This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text. |
| Basic Constraint | This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path. This field does not display for a certification request. |
| MD5 Fingerprint | This is the certificate's message digest that the WiMAX Device calculated using the MD5 algorithm. |
| SHA1 Fingerprint | This is the certificate's message digest that the WiMAX Device calculated using the SHA1 algorithm. |
| Certificate in PEM (Base-64) Encoded Format | This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses lowercase letters, uppercase letters and numerals to convert the binary certificate into a printable form. You can copy and paste a certification request into a certification authority's web page, an e-mail that you send to the certification authority or a text editor and save the file on a management computer for later manual enrollment. You can copy and paste a certificate into an e-mail to send to friends or colleagues or you can copy and paste a certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example). |
| Apply | Click to save your changes. |
| Cancel | Click to return to the previous screen without saving your changes. |

15.3.2 Trusted CA Import

Click **TOOLS > Certificates > Trusted CAs** and then click **Import** to open the **Trusted CA Import** screen. Follow the instructions in this screen to save a trusted certification authority's certificate from a computer to the WiMAX Device. The WiMAX Device trusts any valid certificate signed by any of the imported trusted CA certificates.

Note: You must remove any spaces from the certificate's filename before you can import the certificate.

Figure 89 TOOLS > Certificates > Trusted CAs > Import

The following table describes the labels in this screen.

Table 78 TOOLS > Certificates > Trusted CAs Import

| LABEL | DESCRIPTION |
|-----------|--|
| File Path | Type in the location of the file you want to upload in this field or click Browse to find it. |
| Choose... | Click to find the certificate file you want to upload. |
| Apply | Click to save your changes. |
| Cancel | Click to return to the previous screen without saving your changes. |

15.4 Technical Reference

The following section contains additional technical information about the WiMAX Device features described in this chapter.

15.4.1 Certificate Authorities

When using public-key cryptology for authentication, each host has two keys. One key is public and can be made openly available. The other key is private and must be kept secure.

These keys work like a handwritten signature (in fact, certificates are often referred to as "digital signatures"). Only you can write your signature exactly as it ought to look. When people know what your signature ought to look like, they can verify whether something was signed by you, or by someone else. In the same way, your private key "writes" your digital signature and your public key allows

people to verify whether data was signed by you, or by someone else. This process works as follows.

- 1 Tim wants to send a message to Jenny. He needs her to be sure that it comes from him, and that the message content has not been altered by anyone else along the way. Tim generates a public key pair (one public key and one private key).
- 2 Tim keeps the private key and makes the public key openly available. This means that anyone who receives a message seeming to come from Tim can read it and verify whether it is really from him or not.
- 3 Tim uses his private key to sign the message and sends it to Jenny.
- 4 Jenny receives the message and uses Tim's public key to verify it. Jenny knows that the message is from Tim, and she knows that although other people may have been able to read the message, no-one can have altered it (because they cannot re-sign the message with Tim's private key).
- 5 Additionally, Jenny uses her own private key to sign a message and Tim uses Jenny's public key to verify the message.

The WiMAX Device uses certificates based on public-key cryptology to authenticate users attempting to establish a connection, not to encrypt the data that you send after establishing a connection. The method used to secure the data that you send through an established connection depends on the type of connection. For example, a VPN tunnel might use the triple DES encryption algorithm.

The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates.

A certification path is the hierarchy of certification authority certificates that validate a certificate. The WiMAX Device does not trust a certificate if any certificate on its path has expired or been revoked.

Certification authorities maintain directory servers with databases of valid and revoked certificates. A directory of certificates that have been revoked before the scheduled expiration is called a CRL (Certificate Revocation List). The WiMAX Device can check a peer's certificate against a directory server's list of revoked certificates. The framework of servers, software, procedures and policies that handles keys is called PKI (public-key infrastructure).

15.4.1.1 Advantages of Certificates

Certificates offer the following benefits.

- The WiMAX Device only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.
- Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

15.4.1.2 Self-signed Certificates

You can have the WiMAX Device act as a certification authority and sign its own certificates.

15.4.1.3 Factory Default Certificate

The WiMAX Device generates its own unique self-signed certificate when you first turn it on. This certificate is referred to in the GUI as the factory default certificate.

15.4.1.4 Certificate File Formats

Any certificate that you want to import has to be in one of these file formats:

- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
- PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses lowercase letters, uppercase letters and numerals to convert a binary X.509 certificate into a printable form.
- Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. A PKCS #7 file is used to transfer a public key certificate. The private key is not included. The WiMAX Device currently allows the importation of a PKS#7 file that contains a single certificate.
- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses lowercase letters, uppercase letters and numerals to convert a binary PKCS#7 certificate into a printable form.

Note: Be careful to not convert a binary file to text during the transfer process. It is easy for this to occur since many programs use text files by default.

15.4.2 Verifying a Certificate

Before you import a certificate into the WiMAX Device, you should verify that you have the correct certificate. This is especially true of trusted certificates since the WiMAX Device also trusts any valid certificate signed by any of the imported trusted certificates.

15.4.2.1 Checking the Fingerprint of a Certificate on Your Computer

A certificate's fingerprints are message digests calculated using the MD5 or SHA1 algorithms. The following procedure describes how to check a certificate's fingerprint to verify that you have the actual certificate.

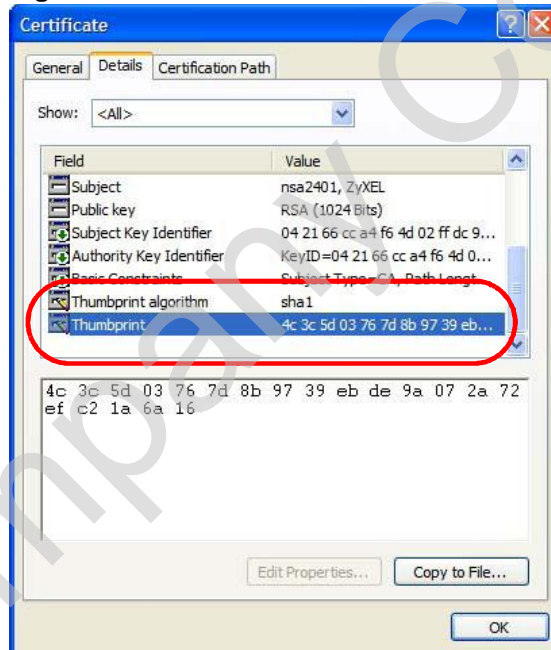
- 1 Browse to where you have the certificate saved on your computer.
- 2 Make sure that the certificate has a ".cer" or ".crt" file name extension. (On some Linux distributions, the file extension may be ".der".)

Figure 90 Remote Host Certificates



- 3 Double-click the certificate's icon to open the Certificate window. Click the Details tab and scroll down to the Thumbprint Algorithm and Thumbprint fields.

Figure 91 Certificate Details



- 4 Use a secure method to verify that the certificate owner has the same information in the Thumbprint Algorithm and Thumbprint fields. The secure method may vary based on your situation. Possible examples would be over the telephone or through an HTTPS connection.

Company Confidential

The Firewall Screens

16.1 Overview

Use the **TOOLS > Firewall** screens to manage WiMAX Device's firewall security measures.

Originally, the term *firewall* referred to a construction technique designed to prevent the spread of fire from one room to another. The networking term "firewall" is a system or group of systems that enforces an access-control policy between two networks. It may also be defined as a mechanism used to protect a trusted network from an untrusted network. Of course, firewalls cannot solve every security problem.

A firewall is one of the mechanisms used to establish a network security perimeter in support of a network security policy. It should never be the only mechanism or method employed. For a firewall to guard effectively, you must design and deploy it appropriately. This requires integrating the firewall into a broad information-security policy. In addition, specific policies must be implemented within the firewall itself.

16.1.1 What You Can Do in This Chapter

- The **Firewall Setting** screen ([Section 16.2 on page 204](#)) lets you configure the basic settings for your firewall.
- The **Service Setting** screen ([Section 16.3 on page 207](#)) lets you enable service blocking, set up the date and time service blocking is effective, and to maintain the list of services you want to block.

16.1.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

About the WiMAX Device Firewall

The WiMAX Device firewall is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated. The WiMAX Device's purpose is to allow a private Local Area Network (LAN) to be securely connected to

the Internet. The WiMAX Device can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network.

The WiMAX Device is installed between the LAN and a WiMAX base station connecting to the Internet. This allows it to act as a secure gateway for all data passing between the Internet and the LAN.

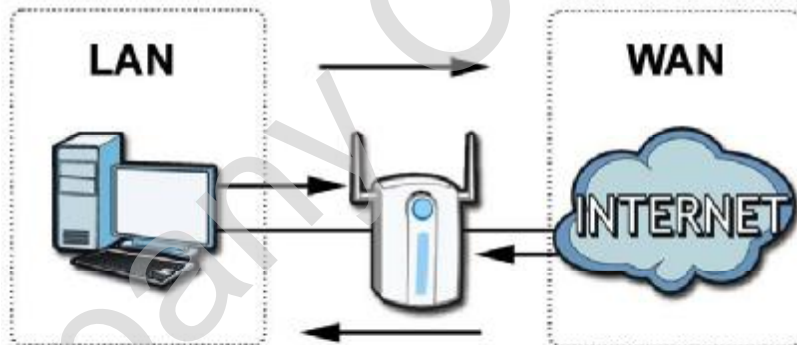
The WiMAX Device has one Ethernet (LAN) port. The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers will have access to Internet services such as e-mail, FTP and the World Wide Web. However, "inbound access" is not allowed (by default) unless the remote host is authorized to use a specific service.

16.2 Firewall Setting

This section describes firewalls and the built-in WiMAX Device's firewall features.

16.2.1 Firewall Rule Directions

Figure 92 Firewall Rule Directions



LAN-to-WAN rules are local network to Internet firewall rules. The default is to forward all traffic from your local network to the Internet.

You can block certain LAN-to-WAN traffic in the **Services** screen (click the **Services** tab). All services displayed in the **Blocked Services** list box are LAN-to-WAN firewall rules that block those services originating from the LAN.

Blocked LAN-to-WAN packets are considered alerts. Alerts are "higher priority logs" that include system errors, attacks and attempted access to blocked web sites. Alerts appear in red in the **View Log** screen. You may choose to have alerts e-mailed immediately in the **Log Settings** screen.

LAN-to-LAN/WiMAX Device means the LAN to the WiMAX Device LAN interface. This is always allowed, as this is how you manage the WiMAX Device from your local computer.

WAN-to-LAN rules are Internet to your local network firewall rules. The default is to block all traffic from the Internet to your local network.

How can you forward certain WAN to LAN traffic? You may allow traffic originating from the WAN to be forwarded to the LAN by:

- Configuring NAT port forwarding rules.
- Configuring WAN or LAN & WAN access for services in the Remote MGMT screens or SMT menus. When you allow remote management from the WAN, you are actually configuring WAN-to-WAN/WiMAX Device firewall rules. WAN-to-WAN/WiMAX Device firewall rules are Internet to the WiMAX Device WAN interface firewall rules. The default is to block all such traffic. When you decide what WAN-to-LAN packets to log, you are in fact deciding what WAN-to-LAN and WAN-to-WAN/WiMAX Device packets to log.

Forwarded WAN-to-LAN packets are not considered alerts.

16.2.2 Triangle Route

When the firewall is on, your WiMAX Device acts as a secure gateway between your LAN and the Internet. In an ideal network topology, all incoming and outgoing network traffic passes through the WiMAX Device to protect your LAN against attacks.

Figure 93 Ideal Firewall Setup



16.2.3 Firewall Setting Options

Click **TOOLS > Firewall > Firewall Setting** to configure the basic settings for your firewall.

Figure 94 TOOLS > Firewall > Firewall Setting

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

Max NAT/Firewall Session Per User:

| Packet Direction | Log |
|------------------|--------|
| LAN to WAN | No Log |
| WAN to LAN | No Log |

The following table describes the labels in this screen.

Table 79 TOOLS > Firewall > Firewall Setting

| LABEL | DESCRIPTION |
|--|--|
| Enable Firewall | Select this to activate the firewall. The WiMAX Device controls access and protects against Denial of Service (DoS) attacks when the firewall is activated. |
| Bypass Triangle Route | Select this if you want to let some traffic from the WAN go directly to a computer in the LAN without passing through the WiMAX Device. |
| Max NAT/ Firewall Session Per User | Select the maximum number of NAT rules and firewall rules the WiMAX Device enforces at one time. The WiMAX Device automatically allocates memory for the maximum number of rules, regardless of whether or not there is a rule to enforce. This is the same number you enter in Network > NAT > General . |
| Packet Direction | |
| Log | Select the situations in which you want to create log entries for firewall events. <ul style="list-style-type: none"> No Log - do not create any log entries Log Blocked - (LAN to WAN only) create log entries when packets are blocked Log Forwarded - (WAN to LAN only) create log entries when packets are forwarded Log All - create log entries for every packet |
| Apply | Click to save your changes. |
| Reset | Click to restore your previously saved settings. |

16.3 Service Setting

Click **TOOLS > Firewall > Service Setting** to enable service blocking, set up the date and time service blocking is effective, and to maintain the list of services you want to block.

Figure 95 TOOLS > Firewall > Service Setting

The following table describes the labels in this screen.

Table 80 TOOLS > Firewall > Service Setting

| LABEL | DESCRIPTION |
|--------------------------|---|
| Service Setup | |
| Enable Services Blocking | Select this to activate service blocking. The Schedule to Block section controls what days and what times service blocking is actually effective, however. |
| Available Services | This is a list of pre-defined services (destination ports) you may prohibit your LAN computers from using. Select the port you want to block, and click Add to add the port to the Blocked Services field. A custom port is a service that is not available in the pre-defined Available Services list. You must define it using the Type and Port Number fields. |

Table 80 TOOLS > Firewall > Service Setting (continued)

| LABEL | DESCRIPTION |
|----------------------|---|
| Blocked Services | This is a list of services (ports) that are inaccessible to computers on your LAN when service blocking is effective. To remove a service from this list, select the service, and click Delete . |
| Type | Select TCP or UDP , based on which one the custom port uses. |
| Port Number | Enter the range of port numbers that defines the service. For example, suppose you want to define the Gnutella service. Select TCP type and enter a port range of 6345-6349 . |
| Add | Click this to add the selected service in Available Services to the Blocked Services list. |
| Delete | Select a service in the Blocked Services , and click this to remove the service from the list. |
| Clear All | Click this to remove all the services in the Blocked Services list. |
| Schedule to Block | |
| Day to Block | Select which days of the week you want the service blocking to be effective. |
| Time of Day to Block | Select what time each day you want service blocking to be effective. Enter times in 24-hour format; for example, 3:00pm should be entered as 15:00. |
| Apply | Click to save your changes. |
| Reset | Click to restore your previously saved settings. |

16.4 Technical Reference

The following section contains additional technical information about the WiMAX Device features described in this chapter.

16.4.1 Stateful Inspection Firewall.

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

16.4.2 Guidelines For Enhancing Security With Your Firewall

- 1 Change the default password via web configurator.
- 2 Think about access control before you connect to the network in any way.
- 3 Limit who can access your router.
- 4 Don't enable any local service (such as telnet or FTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.
- 5 For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.
- 6 Protect against IP spoofing by making sure the firewall is active.
- 7 Keep the firewall in a secured (locked) room.

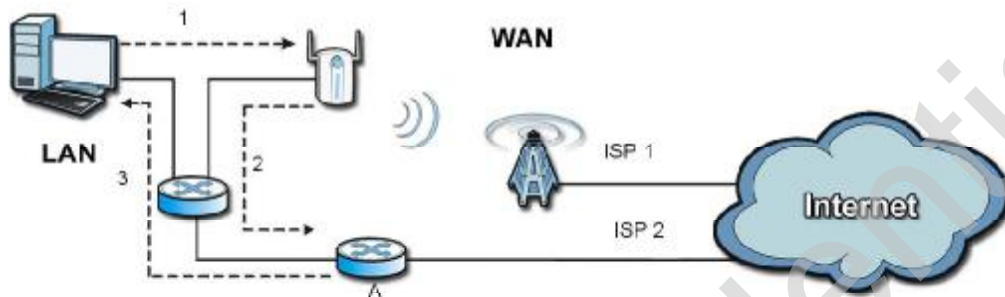
16.4.3 The “Triangle Route” Problem

A traffic route is a path for sending or receiving data packets between two Ethernet devices. You may have more than one connection to the Internet (through one or more ISPs). If an alternate gateway is on the LAN (and its IP address is in the same subnet as the WiMAX Device's LAN IP address), the “triangle route” (also called asymmetrical route) problem may occur. The steps below describe the “triangle route” problem.

- 1 A computer on the LAN initiates a connection by sending out a SYN packet to a receiving server on the WAN.
- 2 The WiMAX Device reroutes the SYN packet through Gateway A on the LAN to the WAN.
- 3 The reply from the WAN goes directly to the computer on the LAN without going through the WiMAX Device.

As a result, the WiMAX Device resets the connection, as the connection has not been acknowledged.

Figure 96 “Triangle Route” Problem



16.4.3.1 Solving the “Triangle Route” Problem

If you have the WiMAX Device allow triangle route sessions, traffic from the WAN can go directly to a LAN computer without passing through the WiMAX Device and its firewall protection.

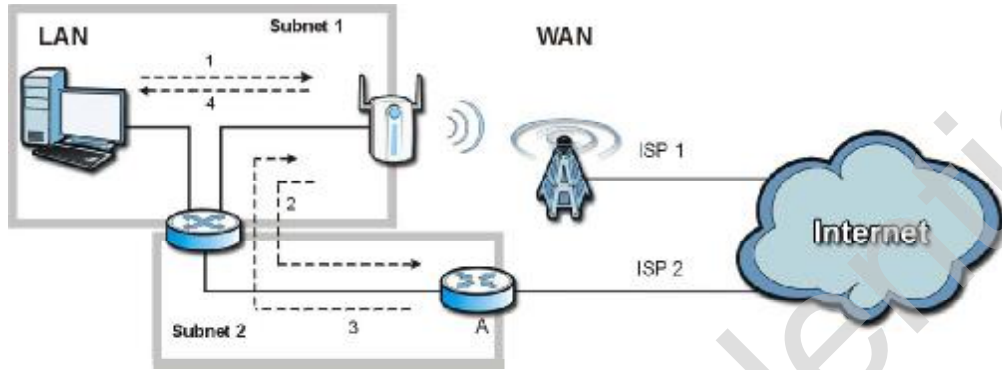
Another solution is to use IP alias. IP alias allows you to partition your network into logical sections over the same Ethernet interface. Your WiMAX Device supports up to three logical LAN interfaces with the WiMAX Device being the gateway for each logical network.

It's like having multiple LAN networks that actually use the same physical cables and ports. By putting your LAN and Gateway A in different subnets, all returning network traffic must pass through the WiMAX Device to your LAN. The following steps describe such a scenario.

- 1 A computer on the LAN initiates a connection by sending a SYN packet to a receiving server on the WAN.
- 2 The WiMAX Device reroutes the packet to Gateway A, which is in Subnet 2.
- 3 The reply from the WAN goes to the WiMAX Device.

- The WiMAX Device then sends it to the computer on the LAN in Subnet 1.

Figure 97 IP Alias



Company Confidential

Content Filter

17.1 Overview

Use the **TOOLS > Content Filter** screens to create and enforce policies that restrict access to the Internet based on content

Internet content filtering allows you to create and enforce Internet access policies tailored to their needs. Content filtering is the ability to block certain web features or specific URL keywords. The WiMAX Device can block web features such as ActiveX controls, Java applets, cookies and disable web proxies. The WiMAX Device also allows you to define time periods and days during which the WiMAX Device performs content filtering.

17.1.1 What You Can Do in This Chapter

- The Filter screen ([Section 17.2 on page 214](#)) lets you set up a trusted IP address, which web features are restricted, and which keywords are blocked when content filtering is effective.
- The Schedule screen ([Section 17.3 on page 216](#)) lets you schedule content filtering.

17.2 Filter

Click **TOOLS > Content Filter > Filter** to set up a trusted IP address, which web features are restricted, and which keywords are blocked when content filtering is effective.

Figure 98 TOOLS > Content Filter > Filter

The screenshot shows a configuration window titled "Filter" with the following sections:

- Trusted IP Setup:** A text box for "Trusted Computer IP Address" containing "0.0.0.0".
- Restrict Web Features:** Four unchecked checkboxes for "ActiveX", "Java", "Cookies", and "Web Proxy".
- Keyword Blocking:** A checked checkbox for "Enable URL Keyword Blocking". Below it is a "Keyword:" text box with an "Add" button.
- Keyword List:** A list box containing "spam" and "wankle%20rotary%20engine". Below the list are "Delete" and "Clear All" buttons.
- Message to display when a site is blocked:** A text box for "Denied Access Message:".
- Buttons:** "Apply" and "Reset" buttons at the bottom.

The following table describes the labels in this screen.

Table 81 TOOLS > Content Filter > Filter

| LABEL | DESCRIPTION |
|-----------------------------|--|
| Trusted IP Setup | |
| Trusted Computer IP Address | You can allow a specific computer to access all Internet resources without the restrictions you set in these screens. Enter the IP address of the trusted computer. |
| Restrict Web Features | Select the web features you want to disable. If a user downloads a page with a restricted feature, that part of the web page appears blank or grayed out. ActiveX - This is a tool for building dynamic and active Web pages and distributed object applications. When you visit an ActiveX Web site, ActiveX controls are downloaded to your browser, where they remain in case you visit the site again. Java - This is used to build downloadable Web components or Internet and intranet business applications of all kinds. Cookies - This is used by Web servers to track usage and to provide service based on ID. Web Proxy - This is a server that acts as an intermediary between a user and the Internet to provide security, administrative control, and caching service. When a proxy server is located on the WAN, it is possible for LAN users to avoid content filtering restrictions. |
| Keyword Blocking | |
| Enable URL Keyword Blocking | Select this if you want the WiMAX Device to block Web sites based on words in the web site address. For example, if you block the keyword bad , http://www.website.com/bad.html is blocked. |
| Keyword | Type a keyword you want to block in this field. You can use up to 64 printable ASCII characters. There is no wildcard character, however. |
| Add | Click this to add the specified Keyword to the Keyword List . You can enter up to 64 keywords. |
| Keyword List | This field displays the keywords that are blocked when Enable URL Keyword Blocking is selected. To delete a keyword, select it, click Delete , and click Apply . |
| Delete | Click Delete to remove the selected keyword in the Keyword List . The keyword disappears after you click Apply . |
| Clear All | Click this button to remove all of the keywords in the Keyword List . |
| Denied Access Message | Enter the message that is displayed when the WiMAX Device's content filter feature blocks access to a web site. |
| Apply | Click to save your changes. |
| Reset | Click to restore your previously saved settings. |

17.3 Schedule

Click **TOOLS > Content Filter > Schedule** to schedule content filtering.

Figure 99 TOOLS > Content Filter > Schedule

Day to Block:

Everyday

Sun Mon Tue Wed Thu Fri Sat

Time of Day to Block: (24-Hour Format)

All day

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

The following table describes the labels in this screen.

Table 82 TOOLS > Content Filter > Schedule

| LABEL | DESCRIPTION |
|----------------------|--|
| Day to Block | Select which days of the week you want content filtering to be effective. |
| Time of Day to Block | Select what time each day you want content filtering to be effective. Enter times in 24-hour format; for example, 3:00pm should be entered as 15:00. |
| Apply | Click to save your changes. |
| Reset | Click to restore your previously saved settings. |

The Remote Management Screens

18.1 Overview

Use the **TOOLS > Remote Management** screens to control which computers can use which services to access the WiMAX Device on each interface.

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

You may manage your WiMAX Device from a remote location via:

Table 83 Remote Management

- Internet (WAN only)
- ALL (LAN and WAN)
- LAN only
- Neither (Disable).

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

You may only have one remote management session running at a time. The WiMAX Device automatically disconnects a remote management session of lower priority when another remote management session of higher priority starts. The priorities for the different types of remote management sessions are as follows: Telnet or HTTP.

18.1.1 What You Can Do in This Chapter

- The **WWW** screen ([Section 18.2 on page 219](#)) lets you control HTTP access to your WiMAX Device.
- The **Telnet** screen ([Section 18.3 on page 220](#)) lets you control Telnet access to your WiMAX Device.
- The **FTP** screen ([Section 18.4 on page 220](#)) lets you control FTP access to your WiMAX Device.
- The **SNMP** screen ([Section 18.5 on page 221](#)) lets you control SNMP access to your WiMAX Device.

- The **DNS** screen ([Section 18.6 on page 224](#)) lets you control DNS access to your WiMAX Device.
- The **Security** screen ([Section 18.7 on page 225](#)) lets you control how your WiMAX Device responds to other types of requests.
- The **Security** screen ([Section 18.7 on page 225](#)) lets you control how your WiMAX Device responds to other types of requests.

18.1.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

Remote Management Limitations

Remote management over LAN or WAN will not work when:

- 1 A filter in SMT menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
- 2 You have disabled that service in one of the remote management screens.
- 3 The IP address in the **Secured Client IP** field does not match the client IP address. If it does not match, the WiMAX Device will disconnect the session immediately.
- 4 There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.

Remote Management and NAT

When NAT is enabled:

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

System Timeout

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

SNMP

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

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

18.2 WWW

Click **TOOLS > Remote Management > WWW** to control HTTP access to your WiMAX Device.

Figure 100 TOOLS > Remote Management > WWW

Server Port:

Server Access:

Secured Client IP Address: All Selected

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

The following table describes the labels in this screen.

Table 84 TOOLS > Remote Management > WWW

| LABEL | DESCRIPTION |
|---------------------------|---|
| Server Port | Enter the port number this service can use to access the WiMAX Device. The computer must use the same port number. |
| Server Access | Select the interface(s) through which a computer may access the WiMAX Device using this service. |
| Secured Client IP Address | Select All to allow any computer to access the WiMAX Device using this service. Select Selected to only allow the computer with the IP address that you specify to access the WiMAX Device using this service. |
| Apply | Click to save your changes. |
| Reset | Click to restore your previously saved settings. |

18.3 Telnet

Click **TOOLS > Remote Management > Telnet** to control Telnet access to your WiMAX Device.

Figure 101 TOOLS > Remote Management > Telnet

The following table describes the labels in this screen.

Table 85 TOOLS > Remote Management > Telnet

| LABEL | DESCRIPTION |
|---------------------------|---|
| Server Port | Enter the port number this service can use to access the WiMAX Device. The computer must use the same port number. |
| Server Access | Select the interface(s) through which a computer may access the WiMAX Device using this service. |
| Secured Client IP Address | Select All to allow any computer to access the WiMAX Device using this service. Select Selected to only allow the computer with the IP address that you specify to access the WiMAX Device using this service. |
| Apply | Click to save your changes. |
| Reset | Click to restore your previously saved settings. |

18.4 FTP

Click **TOOLS > Remote Management > FTP** to control FTP access to your WiMAX Device.

Figure 102 TOOLS > Remote Management > FTP

The following table describes the labels in this screen.

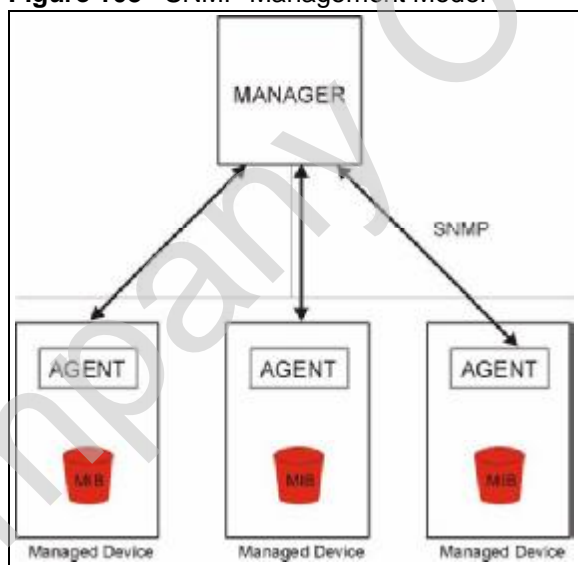
Table 86 TOOLS > Remote Management > FTP

| LABEL | DESCRIPTION |
|---------------------------|---|
| Server Port | Enter the port number this service can use to access the WiMAX Device. The computer must use the same port number. |
| Server Access | Select the interface(s) through which a computer may access the WiMAX Device using this service. |
| Secured Client IP Address | Select All to allow any computer to access the WiMAX Device using this service. Select Selected to only allow the computer with the IP address that you specify to access the WiMAX Device using this service. |
| Apply | Click to save your changes. |
| Reset | Click to restore your previously saved settings. |

18.5 SNMP

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

Figure 103 SNMP Management Model



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

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects. The WiMAX Device supports MIB II that is defined in RFC-1213 and RFC-1215. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance.

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

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

18.5.1 SNMP Traps

The WiMAX Device sends traps to the SNMP manager when any of the following events occurs:

Table 87 SNMP Traps

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

18.5.2 SNMP Options

Click **TOOLS > Remote Management > SNMP** to control SNMP access to your WiMAX Device.

Figure 104 TOOLS > Remote Management > SNMP

The following table describes the labels in this screen.

Table 88 TOOLS > Remote Management > SNMP

| LABEL | DESCRIPTION |
|--------------------|--|
| SNMP Configuration | |
| Get Community | Enter the Get Community , which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests. |
| Set Community | Enter the Set community , which is the password for incoming Set requests from the management station. The default is public and allows all requests. |
| Trap Community | Enter the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests. |
| Trap Destination | Enter the IP address of the station to send your SNMP traps to. |
| SNMP | |
| Port | You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management. |
| Access Status | Select the interface(s) through which a computer may access the WiMAX Device using this service. |

Table 88 TOOLS > Remote Management > SNMP (continued)

| LABEL | DESCRIPTION |
|-------------------|--|
| Secured Client IP | A secured client is a "trusted" computer that is allowed to communicate with the WiMAX Device using this service. Select All to allow any computer to access the WiMAX Device using this service. Choose Selected to just allow the computer with the IP address that you specify to access the WiMAX Device using this service. |
| Apply | Click to save your changes. |
| Reset | Click to restore your previously saved settings. |

18.6 DNS

Click **TOOLS > Remote Management > DNS** to control DNS access to your WiMAX Device.

Figure 105 TOOLS > Remote Management > DNS

The following table describes the labels in this screen.

Table 89 TOOLS > Remote Management > DNS

| LABEL | DESCRIPTION |
|---------------------------|---|
| Server Port | This field is read-only. This field displays the port number this service uses to access the WiMAX Device. The computer must use the same port number. |
| Server Access | Select the interface(s) through which a computer may access the WiMAX Device using this service. |
| Secured Client IP Address | Select All to allow any computer to access the WiMAX Device using this service. Select Selected to only allow the computer with the IP address that you specify to access the WiMAX Device using this service. |
| Apply | Click to save your changes. |
| Reset | Click to restore your previously saved settings. |

18.7 Security

Click **TOOLS > Remote Management > Security** to control how your WiMAX Device responds to other types of requests.

Figure 106 TOOLS > Remote Management > Security

The following table describes the labels in this screen.

Table 90 TOOLS > Remote Management > Security

| LABEL | DESCRIPTION |
|--|--|
| Respond to Ping on | <p>Select the interface(s) on which the WiMAX Device should respond to incoming ping requests.</p> <ul style="list-style-type: none"> • Disable - the WiMAX Device does not respond to any ping requests. • LAN - the WiMAX Device only responds to ping requests received from the LAN. • WAN - the WiMAX Device only responds to ping requests received from the WAN. • LAN & WAN - the WiMAX Device responds to ping requests received from the LAN or the WAN. |
| Do not respond to requests for unauthorized services | <p>Select this to prevent outsiders from discovering your WiMAX Device by sending requests to unsupported port numbers. If an outside user attempts to probe an unsupported port on your WiMAX Device, an ICMP response packet is automatically returned. This allows the outside user to know the WiMAX Device exists. Your WiMAX Device supports anti-probing, which prevents the ICMP response packet from being sent. This keeps outsiders from discovering your WiMAX Device when unsupported ports are probed.</p> <p>If you clear this, your WiMAX Device replies with an ICMP Port Unreachable packet for a port probe on unused UDP ports and with a TCP Reset packet for a port probe on unused TCP ports.</p> |
| Apply | Click to save your changes. |
| Reset | Click to restore your previously saved settings. |

Company Confidential

The Logs Screens

19.1 Overview

Use the **TOOLS > Logs** screens to look at log entries and alerts and to configure the WiMAX Device's log and alert settings.

For a list of log messages, see [Section 19.4 on page 233](#).

19.1.1 What You Can Do in This Chapter

- The **View Logs** screen ([Section 19.2 on page 229](#)) lets you look at log entries and alerts.
- The **Log Settings** screen ([Section 19.3 on page 231](#)) lets you configure where the WiMAX Device sends logs and alerts, the schedule for sending logs, and which logs and alerts are sent or recorded.

19.1.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

Alerts

An alert is a type of log that warrants more serious attention. Some categories such as **System Errors** consist of both logs and alerts.

Syslog Logs

There are two types of syslog: event logs and traffic logs.

The device generates an event log when a system event occurs, for example, when a user logs in or the device is under attack. The device generates a traffic log when a "session" is terminated.

A traffic log summarizes the session's type, when it started and stopped the amount of traffic that was sent and received and so on. An external log analyzer

can reconstruct and analyze the traffic flowing through the device after collecting the traffic logs.

Table 91 Syslog Logs

| LOG MESSAGE | DESCRIPTION |
|--|---|
| Event Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="<msg>" note="<note>" devID="<mac address>" cat="<category>" | This message is sent by the system ("RAS" displays as the system name if you haven't configured one) when the router generates a syslog. The facility is defined in the Log Settings screen. The severity is the log's syslog class. The definition of messages and notes are defined in the various log charts throughout this appendix. The "devID" is the MAC address of the router's LAN port. The "cat" is the same as the category in the router's logs. |
| Traffic Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="Traffic Log" note="Traffic Log" devID="<mac address>" cat="Traffic Log" duration=seconds sent=sentBytes rcvd=receiveBytes dir="<from:to>" protoID=IPProtocolID proto="serviceName" trans="IPSec/Normal" | This message is sent by the device when the connection (session) is closed. The facility is defined in the Log Settings screen. The severity is the traffic log type. The message and note always display "Traffic Log". The "proto" field lists the service name. The "dir" field lists the incoming and outgoing interfaces ("LAN:LAN", "LAN:WAN", "LAN:DEV" for example). |

The following table shows RFC-2408 ISAKMP payload types that the log displays. Please refer to the RFC for detailed information on each type.

Table 92 RFC-2408 ISAKMP Payload Types

| LOG DISPLAY | PAYLOAD TYPE |
|-------------|----------------------|
| SA | Security Association |
| PROP | Proposal |
| TRANS | Transform |
| KE | Key Exchange |
| ID | Identification |
| CER | Certificate |
| CER_REQ | Certificate Request |
| HASH | Hash |
| SIG | Signature |
| NONCE | Nonce |
| NOTFY | Notification |
| DEL | Delete |
| VID | Vendor ID |

19.2 View Logs

Click **TOOLS > Logs > View Log** to look at log entries and alerts. Alerts are written in red.

Figure 107 TOOLS > Logs > View Logs

| # | Time | Message | Source | Destination | Note |
|----|------------------------|--|--------------|-------------|------------|
| 1 | 07/08/2008 05:09:30 | Successful HTTP login | 192.168.1.34 | | User:admin |
| 2 | 07/08/2008 02:15:39 | Successful HTTP login | 192.168.1.34 | | User:admin |
| 3 | 07/08/2008 02:09:00 | Successful HTTP login | 192.168.1.34 | | User:admin |
| 4 | 07/08/2008 01:57:20 | Successful HTTP login | 192.168.1.34 | | User:admin |
| 5 | 07/08/2008 01:34:07 | Successful HTTP login | 192.168.1.34 | | User:admin |
| 6 | 07/08/2008 01:10:45 | Successful HTTP login | 192.168.1.34 | | User:admin |
| 7 | 07/08/2008 00:49:27 | Successful HTTP login | 192.168.1.34 | | User:admin |
| 8 | 07/08/2008 00:08:10 | Successful HTTP login | 192.168.1.34 | | User:admin |
| 9 | 07/08/2008 00:07:37 | DHCP server assigns 192.168.1.33 to TWPC13435-XP | | | |
| 10 | 07/08/2008 00:07:37 | | | | |
| 11 | 07/08/2008 00:07:34 | DHCP server assigns 192.168.1.33 to TWPC13435-XP | | | |
| 12 | 07/08/2008 00:07:34 | | | | |
| 13 | 07/08/2008 00:07:34 | | | | |
| 14 | 07/08/2008 00:05:14 | | | | |

Click a column header to sort log entries in descending (later-to-earlier) order. Click again to sort in ascending order. The small triangle next to a column header indicates how the table is currently sorted (pointing downward is descending; pointing upward is ascending).

The following table describes the labels in this screen.

Table 93 TOOLS > Logs > View Logs

| LABEL | DESCRIPTION |
|---------------|--|
| Display | Select a category whose log entries you want to view. To view all logs, select All Logs . The list of categories depends on what log categories are selected in the Log Settings page. |
| Email Log Now | Click this to send the log screen to the e-mail address specified in the Log Settings page. |
| Refresh | Click to renew the log screen. |
| Clear Log | Click to clear all the log entries, regardless of what is shown on the log screen. |

Table 93 TOOLS > Logs > View Logs (continued)

| LABEL | DESCRIPTION |
|-------------|--|
| # | The number of the item in this list. |
| Time | This field displays the time the log entry was recorded. |
| Message | This field displays the reason for the log entry. See Section 19.4 on page 233 . |
| Source | This field displays the source IP address and the port number of the incoming packet. In many cases, some or all of this information may not be available. |
| Destination | This field lists the destination IP address and the port number of the incoming packet. In many cases, some or all of this information may not be available. |
| Note | This field displays additional information about the log entry. |

19.3 Log Settings

Click **TOOLS > Logs > Log Settings** to configure where the WiMAX Device sends logs and alerts, the schedule for sending logs, and which logs and alerts are sent or recorded.

Figure 108 TOOLS > Logs > Log Settings

The following table describes the labels in this screen.

Table 94 TOOLS > Logs > Log Settings

| LABEL | DESCRIPTION |
|---------------------|---|
| E-mail Log Settings | |
| Mail Server | Enter the server name or the IP address of the mail server the WiMAX Device should use to e-mail logs and alerts. Leave this field blank if you do not want to send logs or alerts by e-mail. |
| Mail Subject | Enter the subject line used in e-mail messages the WiMAX Device sends. |

Table 94 TOOLS > Logs > Log Settings

| LABEL | DESCRIPTION |
|------------------------------|--|
| Send Log to | Enter the e-mail address to which log entries are sent by e-mail. Leave this field blank if you do not want to send logs by e-mail. |
| Send Alerts to | Enter the e-mail address to which alerts are sent by e-mail. Leave this field blank if you do not want to send alerts by e-mail. |
| Log Schedule | <p>Select the frequency with which the WiMAX Device should send log messages by e-mail.</p> <ul style="list-style-type: none"> • Daily • Weekly • Hourly • When Log is Full • None. <p>If the Weekly or the Daily option is selected, specify a time of day when the E-mail should be sent. If the Weekly option is selected, then also specify which day of the week the E-mail should be sent. If the When Log is Full option is selected, an alert is sent when the log fills up. If you select None, no log messages are sent.</p> |
| Day for Sending Log | <p>This field is only available when you select Weekly in the Log Schedule field.</p> <p>Select which day of the week to send the logs.</p> |
| Time for Sending Log | <p>This field is only available when you select Daily or Weekly in the Log Schedule field.</p> <p>Enter the time of day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.</p> |
| Clear log after sending mail | Select this to clear all logs and alert messages after logs are sent by e-mail. |
| Syslog Logging | |
| Active | Select this to enable syslog logging. |
| Syslog Server IP Address | Enter the server name or IP address of the syslog server that logs the selected categories of logs. |
| Log Facility | Select a location. The log facility allows you to log the messages in different files in the syslog server. See the documentation of your syslog for more details. |
| Active Log and Alert | |
| Log | Select the categories of logs that you want to record. |
| Send immediate alert | Select the categories of alerts that you want the WiMAX Device to send immediately. |
| Apply | Click to save your changes. |
| Cancel | Click to return to the previous screen without saving your changes. |

19.4 Log Message Descriptions

The following tables provide descriptions of example log messages.

Table 95 System Error Logs

| LOG MESSAGE | DESCRIPTION |
|---|--|
| WAN connection is down. | The WAN connection is down. You cannot access the network through this interface. |
| %s exceeds the max. number of session per host! | This attempt to create a NAT session exceeds the maximum number of NAT session table entries allowed to be created per host. |

Table 96 System Maintenance Logs

| LOG MESSAGE | DESCRIPTION |
|------------------------------------|--|
| Time calibration is successful | The device has adjusted its time based on information from the time server. |
| Time calibration failed | The device failed to get information from the time server. |
| WAN interface gets IP: %s | The WAN interface got a new IP address from the DHCP or PPPoE server. |
| DHCP client gets %s | A DHCP client got a new IP address from the DHCP server. |
| DHCP client IP expired | A DHCP client's IP address has expired. |
| DHCP server assigns %s | The DHCP server assigned an IP address to a client. |
| Successful WEB login | Someone has logged on to the device's web configurator interface. |
| WEB login failed | Someone has failed to log on to the device's web configurator interface. |
| TELNET Login Successfully | Someone has logged on to the router via telnet. |
| TELNET Login Fail | Someone has failed to log on to the router via telnet. |
| Successful FTP login | Someone has logged on to the device via ftp. |
| FTP login failed | Someone has failed to log on to the device via ftp. |
| NAT Session Table is Full! | The maximum number of NAT session table entries has been exceeded and the table is full. |
| Time initialized by Daytime Server | The device got the time and date from the Daytime server. |
| Time initialized by Time server | The device got the time and date from the time server. |
| Time initialized by NTP server | The device got the time and date from the NTP server. |
| Connect to Daytime server fail | The device was not able to connect to the Daytime server. |
| Connect to Time server fail | The device was not able to connect to the Time server. |

Table 96 System Maintenance Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Connect to NTP server fail | The device was not able to connect to the NTP server. |
| Too large ICMP packet has been dropped | The device dropped an ICMP packet that was too large. |
| Configuration Change: PC = 0x%x, Task ID = 0x%x | The device is saving configuration changes. |

Table 97 Access Control Logs

| LOG MESSAGE | DESCRIPTION |
|---|--|
| Firewall default policy: [TCP UDP IGMP ESP GRE OSPF] <Packet Direction> | Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched the default policy and was blocked or forwarded according to the default policy's setting. |
| Firewall rule [NOT] match:[TCP UDP IGMP ESP GRE OSPF] <Packet Direction>, <rule:%d> | Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched (or did not match) a configured firewall rule (denoted by its number) and was blocked or forwarded according to the rule. |
| Triangle route packet forwarded: [TCP UDP IGMP ESP GRE OSPF] | The firewall allowed a triangle route session to pass through. |
| Packet without a NAT table entry blocked: [TCP UDP IGMP ESP GRE OSPF] | The router blocked a packet that didn't have a corresponding NAT table entry. |
| Router sent blocked web site message: TCP | The router sent a message to notify a user that the router blocked access to a web site that the user requested. |
| Exceed maximum sessions per host (%d). | The device blocked a session because the host's connections exceeded the maximum sessions per host. |
| Firewall allowed a packet that matched a NAT session: [TCP UDP] | A packet from the WAN (TCP or UDP) matched a cone NAT session and the device forwarded it to the LAN. |

Table 98 TCP Reset Logs

| LOG MESSAGE | DESCRIPTION |
|---|--|
| Under SYN flood attack, sent TCP RST | The router sent a TCP reset packet when a host was under a SYN flood attack (the TCP incomplete count is per destination host.) |
| Exceed TCP MAX incomplete, sent TCP RST | The router sent a TCP reset packet when the number of TCP incomplete connections exceeded the user configured threshold. (the TCP incomplete count is per destination host.) |
| Peer TCP state out of order, sent TCP RST | The router sent a TCP reset packet when a TCP connection state was out of order. Note: The firewall refers to RFC793 Figure 6 to check the TCP state. |

Table 98 TCP Reset Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Firewall session time out, sent TCP RST | The router sent a TCP reset packet when a dynamic firewall session timed out. The default timeout values are as follows: ICMP idle timeout: 3 minutes UDP idle timeout: 3 minutes TCP connection (three way handshaking) timeout: 270 seconds TCP FIN-wait timeout: 2 MSL (Maximum Segment Lifetime set in the TCP header). TCP idle (established) timeout (s): 150 minutes TCP reset timeout: 10 seconds |
| Exceed MAX incomplete, sent TCP RST | The router sent a TCP reset packet when the number of incomplete connections (TCP and UDP) exceeded the user-configured threshold. (Incomplete count is for all TCP and UDP connections through the firewall.)Note: When the number of incomplete connections (TCP + UDP) > "Maximum Incomplete High", the router sends TCP RST packets for TCP connections and destroys TOS (firewall dynamic sessions) until incomplete connections < "Maximum Incomplete Low". |
| Access block, sent TCP RST | The router sends a TCP RST packet and generates this log if you turn on the firewall TCP reset mechanism (via CLI command: <code>sys firewall tcprst</code>). |

Table 99 Packet Filter Logs

| LOG MESSAGE | DESCRIPTION |
|---|--|
| [TCP UDP ICMP IGMP Generic] packet filter matched (set: %d, rule: %d) | Attempted access matched a configured filter rule (denoted by its set and rule number) and was blocked or forwarded according to the rule. |

For type and code details, see [Table 106 on page 239](#).

Table 100 ICMP Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Firewall default policy: ICMP <Packet Direction>, <type:%d>, <code:%d> | ICMP access matched the default policy and was blocked or forwarded according to the user's setting. |
| Firewall rule [NOT] match: ICMP <Packet Direction>, <rule:%d>, <type:%d>, <code:%d> | ICMP access matched (or didn't match) a firewall rule (denoted by its number) and was blocked or forwarded according to the rule. |
| Triangle route packet forwarded: ICMP | The firewall allowed a triangle route session to pass through. |

Table 100 ICMP Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|--|---|
| Packet without a NAT table entry blocked: ICMP | The router blocked a packet that didn't have a corresponding NAT table entry. |
| Unsupported/out-of-order ICMP: ICMP | The firewall does not support this kind of ICMP packets or the ICMP packets are out of order. |
| Router reply ICMP packet: ICMP | The router sent an ICMP reply packet to the sender. |

Table 101 PPP Logs

| LOG MESSAGE | DESCRIPTION |
|-------------------|--|
| ppp:LCP Starting | The PPP connection's Link Control Protocol stage has started. |
| ppp:LCP Opening | The PPP connection's Link Control Protocol stage is opening. |
| ppp:CHAP Opening | The PPP connection's Challenge Handshake Authentication Protocol stage is opening. |
| ppp:IPCP Starting | The PPP connection's Internet Protocol Control Protocol stage is starting. |
| ppp:IPCP Opening | The PPP connection's Internet Protocol Control Protocol stage is opening. |
| ppp:LCP Closing | The PPP connection's Link Control Protocol stage is closing. |
| ppp:IPCP Closing | The PPP connection's Internet Protocol Control Protocol stage is closing. |

Table 102 UPnP Logs

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

Table 103 Content Filtering Logs

| LOG MESSAGE | DESCRIPTION |
|-----------------------------|---|
| %s: Keyword blocking | The content of a requested web page matched a user defined keyword. |
| %s: Not in trusted web list | The web site is not in a trusted domain, and the router blocks all traffic except trusted domain sites. |
| %s: Forbidden Web site | The web site is in the forbidden web site list. |
| %s: Contains ActiveX | The web site contains ActiveX. |
| %s: Contains Java applet | The web site contains a Java applet. |
| %s: Contains cookie | The web site contains a cookie. |
| %s: Proxy mode detected | The router detected proxy mode in the packet. |

Table 103 Content Filtering Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|--|---|
| %s: Trusted Web site | The web site is in a trusted domain. |
| %s | When the content filter is not on according to the time schedule: |
| Waiting content filter server timeout | The external content filtering server did not respond within the timeout period. |
| DNS resolving failed | The WiMAX Device cannot get the IP address of the external content filtering via DNS query. |
| Creating socket failed | The WiMAX Device cannot issue a query because TCP/UDP socket creation failed, port:port number. |
| Connecting to content filter server fail | The connection to the external content filtering server failed. |
| License key is invalid | The external content filtering license key is invalid. |

For type and code details, see [Table 106 on page 239](#).

Table 104 Attack Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| attack [TCP UDP IGMP ESP GRE OSPF] | The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF attack. |
| attack ICMP (type:%d, code:%d) | The firewall detected an ICMP attack. |
| land [TCP UDP IGMP ESP GRE OSPF] | The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF land attack. |
| land ICMP (type:%d, code:%d) | The firewall detected an ICMP land attack. |
| ip spoofing - WAN [TCP UDP IGMP ESP GRE OSPF] | The firewall detected an IP spoofing attack on the WAN port. |
| ip spoofing - WAN ICMP (type:%d, code:%d) | The firewall detected an ICMP IP spoofing attack on the WAN port. |
| icmp echo : ICMP (type:%d, code:%d) | The firewall detected an ICMP echo attack. |
| syn flood TCP | The firewall detected a TCP syn flood attack. |
| ports scan TCP | The firewall detected a TCP port scan attack. |
| teardrop TCP | The firewall detected a TCP teardrop attack. |
| teardrop UDP | The firewall detected an UDP teardrop attack. |
| teardrop ICMP (type:%d, code:%d) | The firewall detected an ICMP teardrop attack. |
| illegal command TCP | The firewall detected a TCP illegal command attack. |
| NetBIOS TCP | The firewall detected a TCP NetBIOS attack. |

Table 104 Attack Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|--|---|
| ip spoofing - no routing entry [TCP UDP IGMP ESP GRE OSPF] | The firewall classified a packet with no source routing entry as an IP spoofing attack. |
| ip spoofing - no routing entry (type:%d, code:%d) | The firewall classified an ICMP packet with no source routing entry as an IP spoofing attack. |
| vulnerability ICMP (type:%d, code:%d) | The firewall detected an ICMP vulnerability attack. |
| traceroute ICMP (type:%d, code:%d) | The firewall detected an ICMP traceroute attack. |
| ports scan UDP | The firewall detected a UDP port scan attack. |
| Firewall sent TCP packet in response to DoS attack TCP | The firewall sent TCP packet in response to a DoS attack |
| ICMP Source Quench ICMP | The firewall detected an ICMP Source Quench attack. |
| ICMP Time Exceed ICMP | The firewall detected an ICMP Time Exceed attack. |
| ICMP Destination Unreachable ICMP | The firewall detected an ICMP Destination Unreachable attack. |
| ping of death. ICMP | The firewall detected an ICMP ping of death attack. |
| smurf ICMP | The firewall detected an ICMP smurf attack. |

Table 105 Remote Management Logs

| LOG MESSAGE | DESCRIPTION |
|--|--|
| Remote Management: FTP denied | Attempted use of FTP service was blocked according to remote management settings. |
| Remote Management: TELNET denied | Attempted use of TELNET service was blocked according to remote management settings. |
| Remote Management: HTTP or UPnP denied | Attempted use of HTTP or UPnP service was blocked according to remote management settings. |
| Remote Management: WWW denied | Attempted use of WWW service was blocked according to remote management settings. |
| Remote Management: HTTPS denied | Attempted use of HTTPS service was blocked according to remote management settings. |
| Remote Management: SSH denied | Attempted use of SSH service was blocked according to remote management settings. |
| Remote Management: ICMP Ping response denied | Attempted use of ICMP service was blocked according to remote management settings. |
| Remote Management: DNS denied | Attempted use of DNS service was blocked according to remote management settings. |

Table 106 ICMP Notes

| TYPE | CODE | DESCRIPTION |
|------|------|---|
| 0 | | Echo Reply |
| | 0 | Echo reply message |
| 3 | | Destination Unreachable |
| | 0 | Net unreachable |
| | 1 | Host unreachable |
| | 2 | Protocol unreachable |
| | 3 | Port unreachable |
| | 4 | A packet that needed fragmentation was dropped because it was set to Don't Fragment (DF) |
| | 5 | Source route failed |
| 4 | | Source Quench |
| | 0 | A gateway may discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network. |
| 5 | | Redirect |
| | 0 | Redirect datagrams for the Network |
| | 1 | Redirect datagrams for the Host |
| | 2 | Redirect datagrams for the Type of Service and Network |
| | 3 | Redirect datagrams for the Type of Service and Host |
| 8 | | Echo |
| | 0 | Echo message |
| 11 | | Time Exceeded |
| | 0 | Time to live exceeded in transit |
| | 1 | Fragment reassembly time exceeded |
| 12 | | Parameter Problem |
| | 0 | Pointer indicates the error |
| 13 | | Timestamp |
| | 0 | Timestamp request message |
| 14 | | Timestamp Reply |
| | 0 | Timestamp reply message |
| 15 | | Information Request |
| | 0 | Information request message |
| 16 | | Information Reply |
| | 0 | Information reply message |

Table 107 SIP Logs

| LOG MESSAGE | DESCRIPTION |
|--|---|
| SIP Registration Success by SIP:SIP Phone Number | The listed SIP account was successfully registered with a SIP register server. |
| SIP Registration Fail by SIP:SIP Phone Number | An attempt to register the listed SIP account with a SIP register server was not successful. |
| SIP UnRegistration Success by SIP:SIP Phone Number | The listed SIP account's registration was deleted from the SIP register server. |
| SIP UnRegistration Fail by SIP:SIP Phone Number | An attempt to delete the listed SIP account's registration from the SIP register server failed. |

Table 108 RTP Logs

| LOG MESSAGE | DESCRIPTION |
|------------------------------------|--|
| Error, RTP init fail | The initialization of an RTP session failed. |
| Error, Call fail: RTP connect fail | A VoIP phone call failed because the RTP session could not be established. |
| Error, RTP connection cannot close | The termination of an RTP session failed. |

Table 109 FSM Logs: Caller Side

| LOG MESSAGE | DESCRIPTION |
|---|--|
| VoIP Call Start Ph[Phone Port Number] <- Outgoing Call Number | Someone used a phone connected to the listed phone port to initiate a VoIP call to the listed destination. |
| VoIP Call Established Ph[Phone Port] -> Outgoing Call Number | Someone used a phone connected to the listed phone port to make a VoIP call to the listed destination. |
| VoIP Call End Phone[Phone Port] | A VoIP phone call made from a phone connected to the listed phone port has terminated. |

Table 110 FSM Logs: Callee Side

| LOG MESSAGE | DESCRIPTION |
|---|--|
| VoIP Call Start from SIP[SIP Port Number] | A VoIP phone call came to the WiMAX Device from the listed SIP number. |

Table 110 FSM Logs: Callee Side (continued)

| LOG MESSAGE | DESCRIPTION |
|--|--|
| VoIP Call Established Ph[Phone Port] <- Outgoing Call Number | A VoIP phone call was set up from the listed SIP number to the WiMAX Device. |
| VoIP Call End Phone[Phone Port] | A VoIP phone call that came into the WiMAX Device has terminated. |

Table 111 Lifeline Logs

| LOG MESSAGE | DESCRIPTION |
|-----------------------|---------------------------------|
| PSTN Call Start | A PSTN call has been initiated. |
| PSTN Call End | A PSTN call has terminated. |
| PSTN Call Established | A PSTN call has been set up. |

Company Confidential

The UPnP Screen

20.1 Overview

Use the TOOLS > UPnP screen to enable the WiMAX Device's UPnP feature.

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

20.1.1 What You Can Do in This Chapter

The UPnP screen ([Section 20.2 on page 244](#)) lets you enable the UPnP feature in your WiMAX Device.

20.1.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

How do I know if I'm using UPnP?

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

NAT Traversal

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

- Dynamic port mapping

- Learning public IP addresses
- Assigning lease times to mappings

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

See [Chapter 10 on page 125](#) for further information about NAT.

Cautions with UPnP

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

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

UPnP and ZyXEL

ZyXEL has received UPnP certification from the official UPnP Forum (<http://www.upnp.org>). ZyXEL's UPnP implementation supports IGD 1.0 (Internet Gateway Device).

The WiMAX Device only sends UPnP multicasts to the LAN.

20.2 UPnP

Click **TOOLS > UPnP** to enable UPnP in your WiMAX Device.

Figure 109 TOOLS > UPnP

Enable the Universal Plug and Play (UPnP) Feature

Allow users to make configuration changes through UPnP

Allow UPnP to pass through Firewall

NOTE:
For UPnP to function normally, the [HTTP](#) service must be available for LAN computers using UPnP.

Apply Reset

The following table describes the labels in this screen.

Table 112 TOOLS > UPnP

| LABEL | DESCRIPTION |
|--|--|
| Device Name | This field identifies your device in UPnP applications. |
| Enable the Universal Plug and Play (UPnP) Feature | Select this to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the WiMAX Device's IP address. You still have to enter the password, however. |
| Allow users to make configuration changes through UPnP | Select this to allow UPnP-enabled applications to automatically configure the WiMAX Device so that they can communicate through the WiMAX Device. For example, using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application. |
| Allow UPnP to pass through Firewall | Select this to allow traffic from UPnP-enabled applications to bypass the firewall. Clear this if you want the firewall to check UPnP application packets (for example, MSN packets). |
| Apply | Click to save your changes. |
| Reset | Click to restore your previously saved settings. |

20.3 Technical Reference

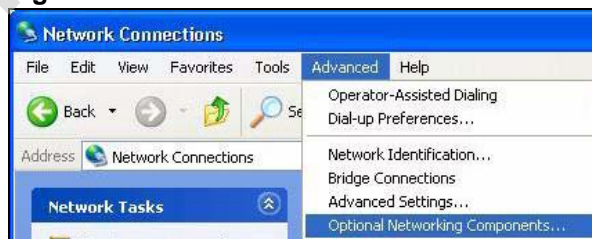
The following section contains additional technical information about the WiMAX Device features described in this chapter.

20.3.1 Installing UPnP in Windows XP

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

- 1 Click **Start > Control Panel**.
- 2 Double-click **Network Connections**.
- 3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ...**.

Figure 110 Network Connections



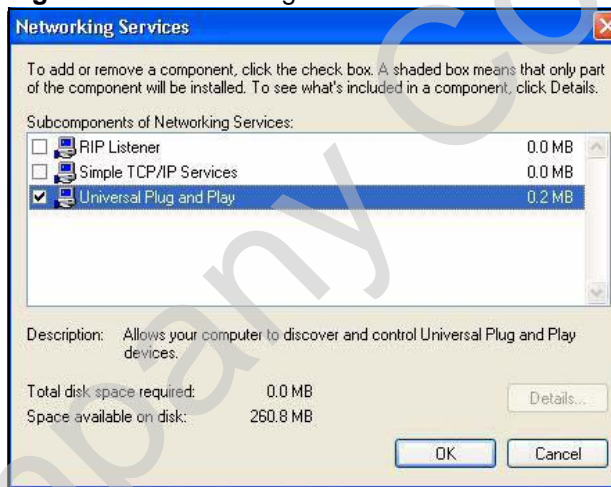
- 4 The **Windows Optional Networking Components Wizard** window displays. Select **Networking Service** in the **Components** selection box and click **Details**.

Figure 111 Windows Optional Networking Components Wizard



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

Figure 112 Networking Services



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

20.3.1.1 Auto-discover Your UPnP-enabled Network Device in Windows XP

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

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

- 1 Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under **Internet Gateway**.
- 2 Right-click the icon and select **Properties**.

Figure 113 Network Connections



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

Figure 114 Internet Connection Properties



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

Figure 115 Internet Connection Properties: Advanced Settings

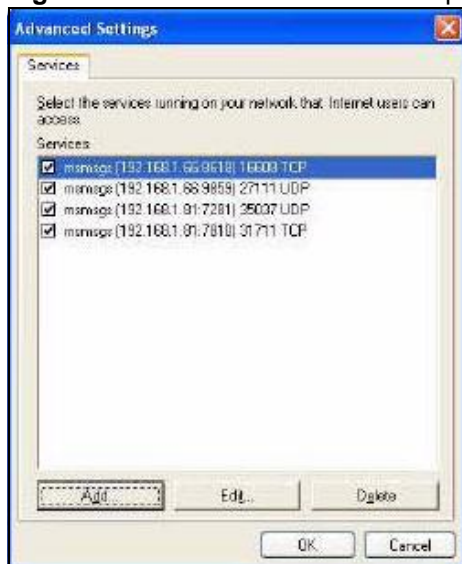
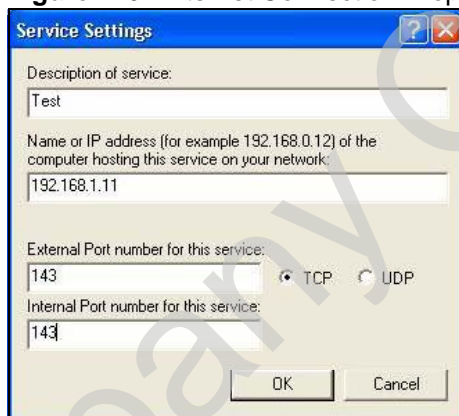


Figure 116 Internet Connection Properties: Advanced Settings: Add



- 5 When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.
- 6 Select **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray.

Figure 117 System Tray Icon



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

Figure 118 Internet Connection Status



20.3.2 Web Configurator Easy Access

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

Follow the steps below to access the web configurator:

- 1 Click **Start** and then **Control Panel**.
- 2 Double-click **Network Connections**.

3 Select My Network Places under Other Places.

Figure 119 Network Connections



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

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

Figure 120 Network Connections: My Network Places

