

MAX-206M1R Series

User's Guide

*WiMAX MIMO Indoor
Simple CPE*

Default Login Details

IP Address: http://192.168.1.1

User Name: admin

Password: 1234



Firmware Version 3.70
Edition 2, 07/2009

www.zyxel.com

ZyXEL

About This User's Guide

The following devices are covered in this book:

MODEL	FEATURES
MAX-206M1R	1 VoIP Port
MAX-216M1R	1 LAN Port
MAX-236M1R	
MAX-216M1R plus	2 External Antennas 1 VoIP Port 1 LAN Port
MAX-216MR	1 LAN Port

All graphics and Web Configurator screens shown in this book are based on the MAX-206M1R unless otherwise noted.

Intended Audience

This manual is intended for people who want to configure the ZyXEL WiMAX Modem 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 Modem.

Note: It is recommended you use the web configurator to configure the WiMAX Modem.

- 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 Modem.

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





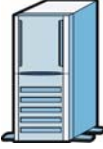






Syntax Conventions

- The product(s) described in this book may be referred to as the "WiMAX Modem", 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 Modem icon is not an exact representation of your WiMAX Modem.

Table 1 Common Icons

<p>WiMAX Access Point</p> 	<p>Computer</p> 	<p>Wireless Signal</p> 
<p>Notebook</p> 	<p>Server</p> 	<p>WiMAX Base Station</p> 
<p>Telephone</p> 	<p>Switch</p> 	<p>Router</p> 
<p>Internet Cloud</p> 	<p>Internet/WiMAX Cloud</p> 	

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.

- Make sure that the cable system is grounded so as to provide some protection against voltage surges.

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.



Contents Overview

Introduction and Wizards	29
Getting Started	31
Introducing the Web Configurator	37
Internet Connection Wizard	45
VoIP Connection Wizard	51
Basic Screens	55
The Setup Screens	57
Advanced Screens	63
The LAN Configuration Screens	65
The WAN Configuration Screens	77
The NAT Configuration Screens	89
The System Configuration Screens	99
Voice Screens	109
The Service Configuration Screens	111
The Phone Screens	129
The Phone Book Screens	139
Tools & Status Screens	145
The Certificates Screens	147
The Firewall Screens	169
Content Filter	179
The Remote Management Screens	183
QoS	195
The Logs Screens	199
The Status Screen	215
Troubleshooting and Specifications	227
Troubleshooting	229
Product Specifications	237
Appendices and Index	255

Table of Contents

About This User's Guide	3
Document Conventions.....	5
Safety Warnings.....	7
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 About Your WiMAX Modem	31
1.1.1 WiMAX Internet Access	32
1.1.2 Make Calls via Internet Telephony Service Provider	33
1.2 WiMAX Modem Hardware	34
1.2.1 LEDs	34
1.3 Good Habits for Managing the Device	36
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	41
Chapter 3	
Internet Connection Wizard	45
3.1 Overview	45
3.1.1 Welcome to the ZyXEL Setup Wizard	45
3.1.2 System Information	46
3.1.3 Authentication Settings	47
3.1.4 IP Address	49

3.1.5 Setup Complete	50
Chapter 4	
VoIP Connection Wizard.....	51
4.1 Overview	51
4.2 Welcome to the ZyXEL Setup Wizard	51
4.2.1 First Voice Account Settings	52
4.2.2 Setup Complete	54
Part II: Basic Screens	55
Chapter 5	
The Setup Screens.....	57
5.1 Overview	57
5.1.1 What You Can Do in This Chapter	57
5.1.2 What You Need to Know	57
5.1.3 Before You Begin	58
5.2 Set IP Address	58
5.3 DHCP Client	59
5.4 Time Setting	60
5.4.1 Pre-Defined NTP Time Servers List	61
5.4.2 Resetting the Time	62
Part III: Advanced Screens.....	63
Chapter 6	
The LAN Configuration Screens.....	65
6.1 Overview	65
6.1.1 What You Can Do in This Chapter	65
6.1.2 What You Need to Know	65
6.2 DHCP Setup	66
6.3 Static DHCP	68
6.4 IP Static Route	69
6.4.1 IP Static Route Setup	70
6.5 Other Settings	71
6.6 Technical Reference	72
6.6.1 IP Address and Subnet Mask	72
6.6.2 DHCP Setup	73
6.6.3 LAN TCP/IP	73
6.6.4 DNS Server Address	74

6.6.5 RIP Setup	74
6.6.6 Multicast	75
Chapter 7	
The WAN Configuration Screens.....	77
7.1 Overview	77
7.1.1 What You Can Do in This Chapter	77
7.1.2 What You Need to Know	77
7.2 Internet Connection	80
7.3 WiMAX Configuration	82
7.3.1 Frequency Ranges	84
7.3.2 Configuring Frequency Settings	84
7.3.3 Using the WiMAX Frequency Screen	85
7.4 Antenna Selection	86
7.5 Advanced	87
Chapter 8	
The NAT Configuration Screens.....	89
8.1 Overview	89
8.1.1 What You Can Do in This Chapter	89
8.2 General	89
8.3 Port Forwarding	90
8.3.1 Port Forwarding Options	91
8.3.2 Port Forwarding Rule Setup	93
8.4 Trigger Port	94
8.4.1 Trigger Port Forwarding Example	95
8.5 ALG	96
Chapter 9	
The System Configuration Screens	99
9.1 Overview	99
9.1.1 What You Can Do in This Chapter	99
9.1.2 What You Need to Know	99
9.2 General	101
9.3 Dynamic DNS	102
9.4 Firmware	104
9.4.1 The Firmware Upload Process	105
9.5 Configuration	106
9.5.1 The Restore Configuration Process	107
9.6 Restart	107
9.6.1 The Restart Process	108

Part IV: Voice Screens 109**Chapter 10****The Service Configuration Screens 111**

10.1 Overview	111
10.1.1 What You Can Do in This Chapter	111
10.1.2 What You Need to Know	111
10.1.3 Before you Begin	113
10.2 SIP Settings	113
10.2.1 Advanced SIP Settings	115
10.3 QoS	122
10.4 Technical Reference	123
10.4.1 SIP Call Progression	123
10.4.2 SIP Client Server	124
10.4.3 SIP User Agent	124
10.4.4 SIP Proxy Server	124
10.4.5 SIP Redirect Server	125
10.4.6 NAT and SIP	126
10.4.7 DiffServ	126
10.4.8 DSCP and Per-Hop Behavior	127

Chapter 11**The Phone Screens..... 129**

11.1 Overview	129
11.1.1 What You Can Do in This Chapter	129
11.1.2 What You Need to Know	129
11.2 Analog Phone	130
11.2.1 Advanced Analog Phone Setup	131
11.3 Common	132
11.4 Region	133
11.5 Technical Reference	134
11.5.1 The Flash Key	134
11.5.2 Europe Type Supplementary Phone Services	134
11.5.3 USA Type Supplementary Services	136

Chapter 12**The Phone Book Screens..... 139**

12.1 Overview	139
12.1.1 What You Can Do in This Chapter	139
12.1.2 What You Need to Know	139
12.2 Incoming Call Policy	140
12.3 Speed Dial	142

Part V: Tools & Status Screens	145
Chapter 13	
The Certificates Screens	147
13.1 Overview	147
13.1.1 What You Can Do in This Chapter	147
13.1.2 What You Need to Know	147
13.2 My Certificates	148
13.2.1 My Certificates Create	150
13.2.2 My Certificate Edit	154
13.2.3 My Certificate Import	157
13.3 Trusted CAs	158
13.3.1 Trusted CA Edit	160
13.3.2 Trusted CA Import	163
13.4 Technical Reference	163
13.4.1 Certificate Authorities	164
13.4.2 Verifying a Certificate	166
Chapter 14	
The Firewall Screens	169
14.1 Overview	169
14.1.1 What You Can Do in This Chapter	169
14.1.2 What You Need to Know	169
14.2 Firewall Setting	170
14.2.1 Firewall Rule Directions	170
14.2.2 Triangle Route	171
14.2.3 Firewall Setting Options	172
14.3 Services	173
14.4 Technical Reference	174
14.4.1 Stateful Inspection Firewall.	174
14.4.2 Guidelines For Enhancing Security With Your Firewall	175
14.4.3 The “Triangle Route” Problem	175
Chapter 15	
Content Filter	179
15.1 Overview	179
15.1.1 What You Can Do in This Chapter	179
15.2 Filter	180
15.3 Schedule	182
Chapter 16	
The Remote Management Screens	183
16.1 Overview	183

16.1.1 What You Can Do in This Chapter	183
16.1.2 What You Need to Know	184
16.2 WWW	185
16.3 Telnet	186
16.4 FTP	186
16.5 SNMP	187
16.5.1 SNMP Traps	188
16.5.2 SNMP Options	189
16.6 DNS	190
16.7 Security	191
16.8 TR0-69	192
Chapter 17	
QoS.....	195
17.1 Overview	195
17.2 General	195
17.3 Class Setup	196
17.3.1 Class Configuration	197
Chapter 18	
The Logs Screens.....	199
18.1 Overview	199
18.1.1 What You Can Do in This Chapter	199
18.1.2 What You Need to Know	199
18.2 View Logs	201
18.3 Log Settings	203
18.4 Log Message Descriptions	205
Chapter 19	
The Status Screen.....	215
19.1 Overview	215
19.2 Status Screen	215
19.2.1 Packet Statistics	219
19.2.2 WiMAX Site Information	221
19.2.3 DHCP Table	222
19.2.4 VoIP Statistics	223
19.2.5 WiMAX Profile	225
Part VI: Troubleshooting and Specifications	227
Chapter 20	
Troubleshooting.....	229

20.1 Power, Hardware Connections, and LEDs	229
20.2 WiMAX Modem Access and Login	230
20.3 Internet Access	232
20.4 Phone Calls and VoIP	234
20.5 Reset the WiMAX Modem to Its Factory Defaults	235
20.5.1 Pop-up Windows, JavaScripts and Java Permissions	235
Chapter 21	
Product Specifications	237
21.1 Wall-Mounting	251
21.1.1 The Wall-Mounting Kit	251
21.1.2 Instructions	251
Part VII: Appendices and Index	255
Appendix A WiMAX Security	257
Appendix B Setting Up Your Computer's IP Address	261
Appendix C Pop-up Windows, JavaScripts and Java Permissions	289
Appendix D IP Addresses and Subnetting	299
Appendix E Importing Certificates	311
Appendix F SIP Passthrough	343
Appendix G Common Services	345
Appendix H Legal Information	349
Appendix I Customer Support	353
Index.....	361

List of Figures

Figure 1 Mobile Station and Base Station	32
Figure 2 WiMAX Modem's VoIP Features - Peer-to-Peer Calls	33
Figure 3 WiMAX Modem's VoIP Features - Calls via VoIP Service Provider	33
Figure 4 The WiMAX Modem's LEDs	34
Figure 5 Main Screen	41
Figure 6 Select a Mode	45
Figure 7 Internet Connection Wizard > System Information	46
Figure 8 Internet Connection Wizard > Authentication Settings Screen	47
Figure 9 Internet Connection Wizard > IP Address	49
Figure 10 Internet Connection Wizard > Complete	50
Figure 11 Select a Mode	51
Figure 12 VoIP Connection > First Voice Account Settings	52
Figure 13 VoIP Connection > SIP Registration Test	53
Figure 14 VoIP Connection > SIP Registration Fail	54
Figure 15 VoIP Connection > Finish	54
Figure 16 SETUP > Set IP Address	58
Figure 17 SETUP > Set IP Address	59
Figure 18 SETUP > Time Setting	60
Figure 19 ADVANCED > LAN Configuration > DHCP Setup	66
Figure 20 ADVANCED > LAN Configuration > Static DHCP	68
Figure 21 Advanced> LAN Configuration > IP Static Route	69
Figure 22 Advanced> LAN Configuration > IP Static Route Setup	70
Figure 23 ADVANCED > LAN Configuration > Advanced	71
Figure 24 WiMax: Mobile Station	78
Figure 25 WiMAX: Multiple Mobile Stations	78
Figure 26 Using an AAA Server	79
Figure 27 ADVANCED > WAN Configuration > Internet Connection	80
Figure 28 ADVANCED > WAN Configuration >WiMAX Configuration	83
Figure 29 Frequency Ranges	84
Figure 30 Completing the WiMAX Frequency Screen	86
Figure 31 ADVANCED > WAN Configuration > Antenna Selection	86
Figure 32 ADVANCED > WAN Configuration > Advanced	87
Figure 33 ADVANCED > NAT Configuration > General	89
Figure 34 Multiple Servers Behind NAT Example	91
Figure 35 ADVANCED > NAT Configuration > Port Forwarding	91
Figure 36 ADVANCED > NAT Configuration > Port Forwarding > Rule Setup	93
Figure 37 ADVANCED > NAT Configuration > Trigger Port	94
Figure 38 Trigger Port Forwarding Example	95

Figure 39 ADVANCED > NAT Configuration > ALG	97
Figure 40 ADVANCED > System Configuration > General	101
Figure 41 ADVANCED > System Configuration > Dynamic DNS	103
Figure 42 ADVANCED > System Configuration > Firmware	104
Figure 43 ADVANCED > System Configuration > Configuration	106
Figure 44 ADVANCED > System Configuration > Restart	107
Figure 45 VOICE > Service Configuration > SIP Setting	113
Figure 46 STUN Example	115
Figure 47 VOICE > Service Configuration > SIP Settings > Advanced	117
Figure 48 VOICE > Service Configuration > QoS	122
Figure 49 SIP User Agent	124
Figure 50 SIP Proxy Server	125
Figure 51 SIP Redirect Server	126
Figure 52 DiffServ: Differentiated Service Field	127
Figure 53 VOICE > Phone > Analog Phone	130
Figure 54 VOICE > Phone > Analog Phone > Advanced	131
Figure 55 VOICE > Phone > Common	132
Figure 56 VOICE > Phone > Region	133
Figure 57 VOICE > Phone Book > Incoming Call Policy	140
Figure 58 VOICE > Phone Book > Speed Dial	142
Figure 59 TOOLS > Certificates > My Certificates	148
Figure 60 TOOLS > Certificates > My Certificates > Create	150
Figure 61 TOOLS > Certificates > My Certificates > Edit	154
Figure 62 TOOLS > Certificates > My Certificates > Import	157
Figure 63 TOOLS > Certificates > Trusted CAs	158
Figure 64 TOOLS > Certificates > Trusted CAs > Edit	160
Figure 65 TOOLS > Certificates > Trusted CAs > Import	163
Figure 66 Remote Host Certificates	166
Figure 67 Certificate Details	167
Figure 68 Firewall Rule Directions	170
Figure 69 Ideal Firewall Setup	171
Figure 70 TOOLS > Firewall > Firewall Setting	172
Figure 71 TOOLS > Firewall > Service Setting	173
Figure 72 "Triangle Route" Problem	176
Figure 73 IP Alias	177
Figure 74 TOOLS > Content Filter > Filter	180
Figure 75 TOOLS > Content Filter > Schedule	182
Figure 76 TOOLS > Remote Management > WWW	185
Figure 77 TOOLS > Remote Management > Telnet	186
Figure 78 TOOLS > Remote Management > FTP	186
Figure 79 SNMP Management Model	187
Figure 80 TOOLS > Remote Management > SNMP	189
Figure 81 TOOLS > Remote Management > DNS	190

Figure 82 TOOLS > Remote Management > Security	191
Figure 83 TR-069 Example	192
Figure 84 TOOLS > Remote Management > TR069	193
Figure 85 QoS > General	195
Figure 86 QoS > Class Setup	196
Figure 87 QoS > Class Setup > Class Configuration	197
Figure 88 TOOLS > Logs > View Logs	201
Figure 89 TOOLS > Logs > Log Settings	203
Figure 90 Status	215
Figure 91 Packet Statistics	219
Figure 92 WiMAX Site Information	221
Figure 93 DHCP Table	222
Figure 94 VoIP Statistics	223
Figure 95 WiMAX Profile	225
Figure 96 Windows XP: Start Menu	262
Figure 97 Windows XP: Control Panel	262
Figure 98 Windows XP: Control Panel > Network Connections > Properties	263
Figure 99 Windows XP: Local Area Connection Properties	263
Figure 100 Windows XP: Internet Protocol (TCP/IP) Properties	264
Figure 101 Windows Vista: Start Menu	265
Figure 102 Windows Vista: Control Panel	265
Figure 103 Windows Vista: Network And Internet	265
Figure 104 Windows Vista: Network and Sharing Center	266
Figure 105 Windows Vista: Network and Sharing Center	266
Figure 106 Windows Vista: Local Area Connection Properties	267
Figure 107 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties	268
Figure 108 Mac OS X 10.4: Apple Menu	269
Figure 109 Mac OS X 10.4: System Preferences	269
Figure 110 Mac OS X 10.4: Network Preferences	270
Figure 111 Mac OS X 10.4: Network Preferences > TCP/IP Tab.	270
Figure 112 Mac OS X 10.4: Network Preferences > Ethernet	271
Figure 113 Mac OS X 10.4: Network Utility	272
Figure 114 Mac OS X 10.5: Apple Menu	273
Figure 115 Mac OS X 10.5: Systems Preferences	273
Figure 116 Mac OS X 10.5: Network Preferences > Ethernet	274
Figure 117 Mac OS X 10.5: Network Preferences > Ethernet	275
Figure 118 Mac OS X 10.5: Network Utility	276
Figure 119 Ubuntu 8: System > Administration Menu	277
Figure 120 Ubuntu 8: Network Settings > Connections	277
Figure 121 Ubuntu 8: Administrator Account Authentication	278
Figure 122 Ubuntu 8: Network Settings > Connections	278
Figure 123 Ubuntu 8: Network Settings > Properties	279
Figure 124 Ubuntu 8: Network Settings > DNS	280

Figure 125 Ubuntu 8: Network Tools	281
Figure 126 openSUSE 10.3: K Menu > Computer Menu	282
Figure 127 openSUSE 10.3: K Menu > Computer Menu	283
Figure 128 openSUSE 10.3: YaST Control Center	283
Figure 129 openSUSE 10.3: Network Settings	284
Figure 130 openSUSE 10.3: Network Card Setup	285
Figure 131 openSUSE 10.3: Network Settings	286
Figure 132 openSUSE 10.3: KNetwork Manager	287
Figure 133 openSUSE: Connection Status - KNetwork Manager	287
Figure 134 Pop-up Blocker	289
Figure 135 Internet Options: Privacy	290
Figure 136 Internet Options: Privacy	291
Figure 137 Pop-up Blocker Settings	292
Figure 138 Internet Options: Security	293
Figure 139 Security Settings - Java Scripting	294
Figure 140 Security Settings - Java	295
Figure 141 Java (Sun)	296
Figure 142 Mozilla Firefox: TOOLS > Options	296
Figure 143 Mozilla Firefox Content Security	297
Figure 144 Network Number and Host ID	300
Figure 145 Subnetting Example: Before Subnetting	303
Figure 146 Subnetting Example: After Subnetting	304
Figure 147 Conflicting Computer IP Addresses Example	309
Figure 148 Conflicting Computer IP Addresses Example	309
Figure 149 Conflicting Computer and Router IP Addresses Example	310
Figure 150 Internet Explorer 7: Certification Error	312
Figure 151 Internet Explorer 7: Certification Error	312
Figure 152 Internet Explorer 7: Certificate Error	313
Figure 153 Internet Explorer 7: Certificate	313
Figure 154 Internet Explorer 7: Certificate Import Wizard	314
Figure 155 Internet Explorer 7: Certificate Import Wizard	314
Figure 156 Internet Explorer 7: Certificate Import Wizard	315
Figure 157 Internet Explorer 7: Select Certificate Store	315
Figure 158 Internet Explorer 7: Certificate Import Wizard	316
Figure 159 Internet Explorer 7: Security Warning	316
Figure 160 Internet Explorer 7: Certificate Import Wizard	317
Figure 161 Internet Explorer 7: Website Identification	317
Figure 162 Internet Explorer 7: Public Key Certificate File	318
Figure 163 Internet Explorer 7: Open File - Security Warning	318
Figure 164 Internet Explorer 7: Tools Menu	319
Figure 165 Internet Explorer 7: Internet Options	319
Figure 166 Internet Explorer 7: Certificates	320
Figure 167 Internet Explorer 7: Certificates	320

Figure 168 Internet Explorer 7: Root Certificate Store	320
Figure 169 Firefox 2: Website Certified by an Unknown Authority	322
Figure 170 Firefox 2: Page Info	323
Figure 171 Firefox 2: Tools Menu	324
Figure 172 Firefox 2: Options	324
Figure 173 Firefox 2: Certificate Manager	325
Figure 174 Firefox 2: Select File	325
Figure 175 Firefox 2: Tools Menu	326
Figure 176 Firefox 2: Options	326
Figure 177 Firefox 2: Certificate Manager	327
Figure 178 Firefox 2: Delete Web Site Certificates	327
Figure 179 Opera 9: Certificate signer not found	328
Figure 180 Opera 9: Security information	329
Figure 181 Opera 9: Tools Menu	330
Figure 182 Opera 9: Preferences	331
Figure 183 Opera 9: Certificate manager	332
Figure 184 Opera 9: Import certificate	332
Figure 185 Opera 9: Install authority certificate	333
Figure 186 Opera 9: Install authority certificate	333
Figure 187 Opera 9: Tools Menu	334
Figure 188 Opera 9: Preferences	334
Figure 189 Opera 9: Certificate manager	335
Figure 190 Konqueror 3.5: Server Authentication	336
Figure 191 Konqueror 3.5: Server Authentication	336
Figure 192 Konqueror 3.5: KDE SSL Information	337
Figure 193 Konqueror 3.5: Public Key Certificate File	338
Figure 194 Konqueror 3.5: Certificate Import Result	338
Figure 195 Konqueror 3.5: Kleopatra	338
Figure 196 Konqueror 3.5: Settings Menu	340
Figure 197 Konqueror 3.5: Configure	340

List of Tables

Table 1 Common Icons	6
Table 2 The WiMAX Modem	34
Table 3 Main > Icons	41
Table 4 Main	42
Table 5 Internet Connection Wizard > System Information	46
Table 6 Internet Connection Wizard > Authentication Settings Screen	47
Table 7 Internet Connection Wizard > IP Address	49
Table 8 VoIP Connection > First Voice Account Settings	52
Table 9 SETUP > Set IP Address	59
Table 10 SETUP > Set IP Address	59
Table 11 SETUP > Time Setting	60
Table 12 Pre-defined NTP Time Servers	62
Table 13 ADVANCED > LAN Configuration > DHCP Setup	67
Table 14 ADVANCED > LAN Configuration > Static DHCP	68
Table 15 Advanced> LAN Configuration > IP Static Route	69
Table 16 Advanced> LAN Configuration > IP Static Route	69
Table 17 Management > Static Route > IP Static Route > Edit	70
Table 18 ADVANCED > LAN Configuration > Other Settings	71
Table 19 ADVANCED > WAN Configuration > Internet Connection > ISP Parameters for Internet Access 80	
Table 20 Radio Frequency Conversion	83
Table 21 ADVANCED > WAN Configuration > WiMAX Configuration	83
Table 22 DL Frequency Example Settings	85
Table 23 ADVANCED > WAN Configuration > Advanced	86
Table 24 ADVANCED > WAN Configuration > Advanced	88
Table 25 ADVANCED > NAT Configuration > General	90
Table 26 Advanced> VPN Transport > Customer Interface	92
Table 27 ADVANCED > NAT Configuration > Port Forwarding	92
Table 28 ADVANCED > NAT Configuration > Port Forwarding > Rule Setup	93
Table 29 ADVANCED > NAT Configuration > Trigger Port	94
Table 30 ADVANCED > NAT Configuration > ALG	97
Table 31 ADVANCED > System Configuration > General	101
Table 32 ADVANCED > System Configuration > Dynamic DNS	103
Table 33 ADVANCED > System Configuration > Firmware	105
Table 34 ADVANCED > System Configuration > Configuration	106
Table 35 ADVANCED > System Configuration > Firmware	107
Table 36 VOICE > Service Configuration > SIP Setting	114
Table 37 VOICE > Service Configuration > SIP Settings > Advanced	117

Table 38 Custom Tones Details	120
Table 39 VOICE > Service Configuration > QoS	122
Table 40 SIP Call Progression	123
Table 41 VOICE > Phone > Analog Phone	131
Table 42 VOICE > Phone > Analog Phone > Advanced	132
Table 43 VOICE > Phone > Common	133
Table 44 VOICE > Phone > Region	133
Table 45 European Type Flash Key Commands	134
Table 46 USA Type Flash Key Commands	136
Table 47 VOICE > Phone Book > Incoming Call Policy	140
Table 48 Advanced> LAN Configuration > IP Static Route	142
Table 49 VOICE > Phone Book > Speed Dial	143
Table 50 TOOLS > Certificates > My Certificates	148
Table 51 TOOLS > Certificates > My Certificates	148
Table 52 TOOLS > Certificates > My Certificates > Create	151
Table 53 TOOLS > Certificates > My Certificates > Edit	154
Table 54 TOOLS > Certificates > My Certificates > Import	157
Table 55 TOOLS > Certificates > Trusted CAs	158
Table 56 TOOLS > Certificates > Trusted CAs	158
Table 57 TOOLS > Certificates > Trusted CAs > Edit	160
Table 58 TOOLS > Certificates > Trusted CAs Import	163
Table 59 TOOLS > Firewall > Firewall Setting	172
Table 60 TOOLS > Firewall > Service Setting	173
Table 61 TOOLS > Content Filter > Filter	181
Table 62 TOOLS > Content Filter > Schedule	182
Table 63 Remote Management	183
Table 64 TOOLS > Remote Management > WWW	185
Table 65 TOOLS > Remote Management > Telnet	186
Table 66 TOOLS > Remote Management > FTP	187
Table 67 SNMP Traps	188
Table 68 TOOLS > Remote Management > SNMP	189
Table 69 TOOLS > Remote Management > DNS	190
Table 70 TOOLS > Remote Management > Security	191
Table 71 TOOLS > Remote Management > TR069	193
Table 72 TOOLS > Remote Management > Security	195
Table 73 QoS Class Setup	196
Table 74 QoS Class Setup	197
Table 75 Syslog Logs	200
Table 76 RFC-2408 ISAKMP Payload Types	200
Table 77 TOOLS > Logs > View Logs	201
Table 78 TOOLS > Logs > Log Settings	204
Table 79 System Error Logs	205
Table 80 System Maintenance Logs	205

Table 81 Access Control Logs	206
Table 82 TCP Reset Logs	207
Table 83 Packet Filter Logs	207
Table 84 ICMP Logs	208
Table 85 PPP Logs	208
Table 86 UPnP Logs	208
Table 87 Content Filtering Logs	209
Table 88 Attack Logs	209
Table 89 Remote Management Logs	210
Table 90 ICMP Notes	211
Table 91 SIP Logs	212
Table 92 RTP Logs	212
Table 93 FSM Logs: Caller Side	213
Table 94 FSM Logs: Callee Side	213
Table 95 Lifeline Logs	213
Table 96 Status	216
Table 97 Packet Statistics	220
Table 98 WiMAX Site Information	221
Table 99 DHCP Table	222
Table 100 VoIP Statistics	223
Table 101 The WiMAX Profile Screen	225
Table 102 Environmental and Hardware Specifications	237
Table 103 Radio Specifications	238
Table 104 Firmware Specifications	238
Table 105 Standards Supported	240
Table 106 Voice Features	241
Table 107 Star (*) and Pound (#) Code Support	243
Table 108 Environmental and Hardware Specifications	243
Table 109 Radio Specifications	244
Table 110 Firmware Specifications	245
Table 111 Standards Supported	246
Table 112 Voice Features	248
Table 113 Star (*) and Pound (#) Code Support	249
Table 114 IP Address Network Number and Host ID Example	300
Table 115 Subnet Masks	301
Table 116 Maximum Host Numbers	301
Table 117 Alternative Subnet Mask Notation	302
Table 118 Subnet 1	305
Table 119 Subnet 2	305
Table 120 Subnet 3	305
Table 121 Subnet 4	305
Table 122 Eight Subnets	306
Table 123 24-bit Network Number Subnet Planning	306

Table 124 16-bit Network Number Subnet Planning 307
Table 125 Commonly Used Services 345

PART I

Introduction and Wizards

Getting Started (31)

Introducing the Web Configurator (37)

Internet Connection Wizard (45)

VoIP Connection Wizard (51)

Getting Started

The following devices are covered in this book:

MODEL	FEATURES
MAX-206M1R	1 VoIP Port
MAX-216M1R	1 LAN Port
MAX-236M1R	
MAX-216M1R plus	2 External Antennas 1 VoIP Port 1 LAN Port
MAX-216MR	1 LAN Port

All graphics and Web Configurator screens shown in this book are based on the MAX-206M1R unless otherwise noted.

1.1 About Your WiMAX Modem

The WiMAX Modem has a built-in switch and one phone port. It allows you to access the Internet by connecting to a WiMAX wireless network.

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

You can configure firewall and content filtering as well as a host of other features.

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

See [Chapter 21 on page 237](#) for a complete list of features for your model.

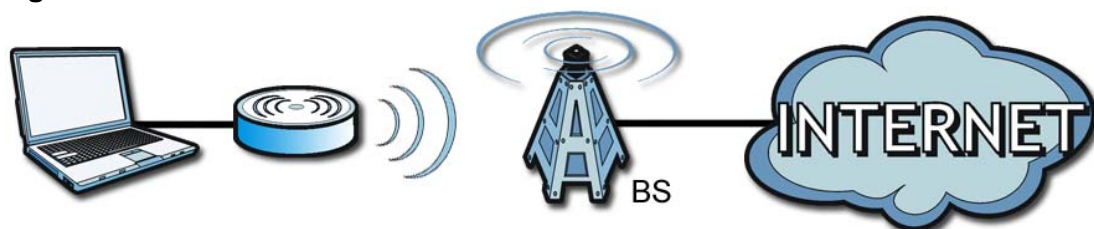
1.1.1 WiMAX Internet Access

Connect your computer or network to the WiMAX Modem for WiMAX Internet access. See the Quick Start Guide for instructions on hardware connection.

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

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

Figure 1 Mobile Station 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. For example, you could block access to certain web sites for the kids.

1.1.2 Make Calls via Internet Telephony Service Provider

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

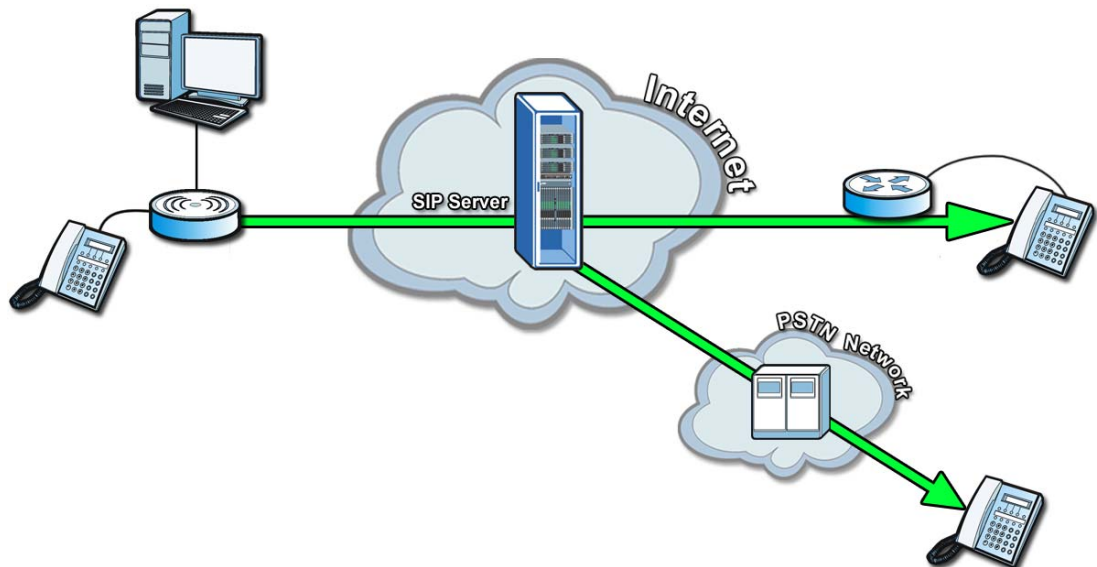
- Peer-to-Peer calls - Use the WiMAX Modem to make a call directly to the recipient's IP address without using a SIP proxy server.

Figure 2 WiMAX Modem's VoIP Features - Peer-to-Peer Calls



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

Figure 3 WiMAX Modem's VoIP Features - Calls via VoIP Service Provider



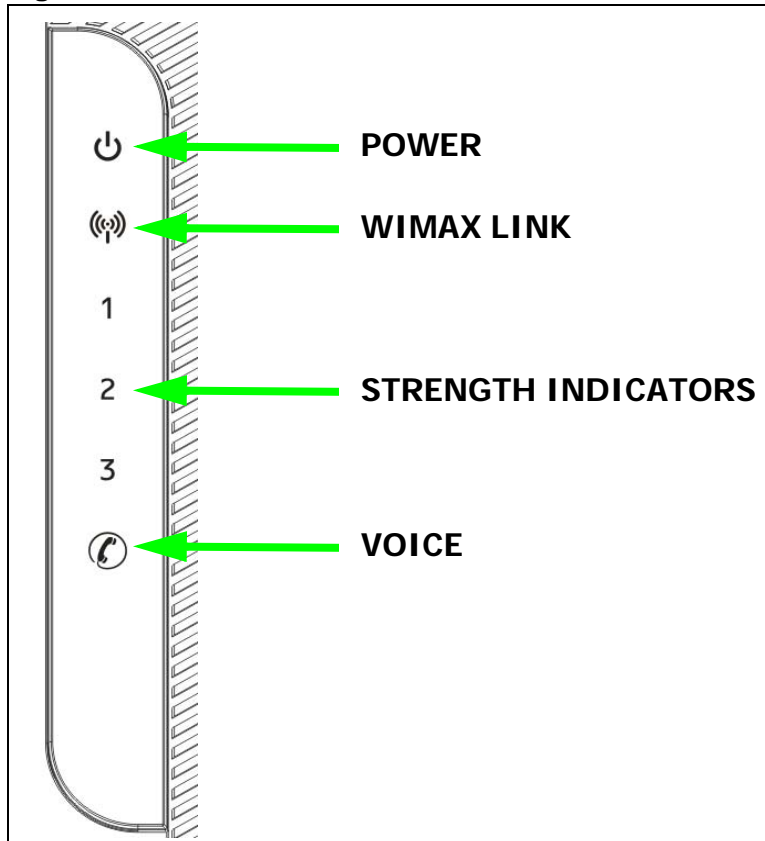
1.2 WiMAX Modem Hardware

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 Modem.

Figure 4 The WiMAX Modem's LEDs



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

Table 2 The WiMAX Modem

LED	STATE	DESCRIPTION
Power	Off	The WiMAX Modem is not receiving power.
	Red	The WiMAX Modem is receiving power but has been unable to start up correctly or is not receiving enough power. See the Troubleshooting section for more information.
	Green	The WiMAX Modem is receiving power and functioning correctly.

Table 2 The WiMAX Modem

LED	STATE	DESCRIPTION
LAN	Off	The LAN is not connected.
	Green	The WiMAX Modem has a successful Local Area Network (Ethernet) connection and is active during modem activity.
Voice	Off	No SIP account is registered, or the WiMAX Modem is not receiving power.
	Green	A SIP account is registered.
	Green (Blinking)	A SIP account is registered, and the phone attached to the LINE port is in use (off the hook).
	Yellow	A SIP account is registered and has a voice message on the SIP server.
	Yellow (Blinking)	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).
WiMAN Link	Off	The WiMAX Modem is not connected to a wireless (WiMAX) network.
	Green	The WiMAX Modem is successfully connected to a wireless (WiMAX) network.
	Green (Blinking Slowly)	The WiMAX Modem is searching for a wireless (WiMAX) network.
	Green (Blinking Quickly)	The WiMAX Modem has found a wireless (WiMAX) network and is connecting.
Strength Indicator	The Strength Indicator LEDs display the Received Signal Strength Indication (RSSI) of the wireless (WiMAX) connection.	
	3 Signal LEDs	The signal strength is greater than or equal to -70 dBm
	2 Signal LEDs	The signal strength is between -70 and -80 dBm
	1 Signal LED	The signal strength is between -80 and -90 dBm
	0 Signal LEDs	The signal strength is less than -90 dBm.

1.3 Good Habits for Managing the Device

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

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

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:

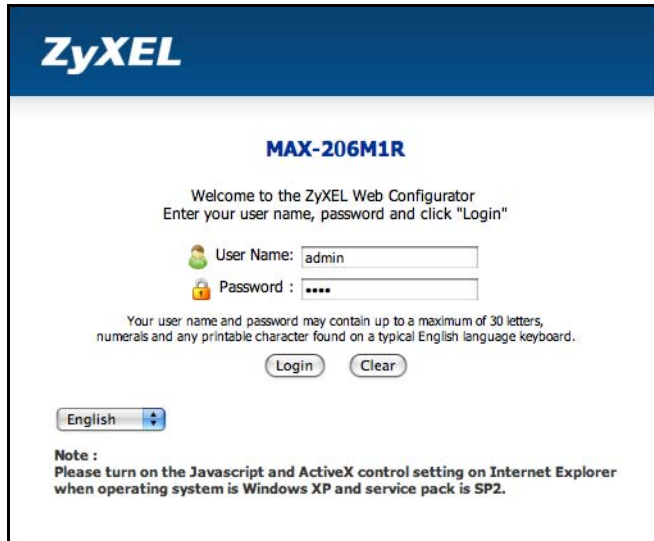
- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in many operating systems and web browsers.
- JavaScript (enabled by default in most web browsers).
- Java permissions (enabled by default in most web browsers).

See the [Appendix C on page 289](#) for more information on configuring your web browser.

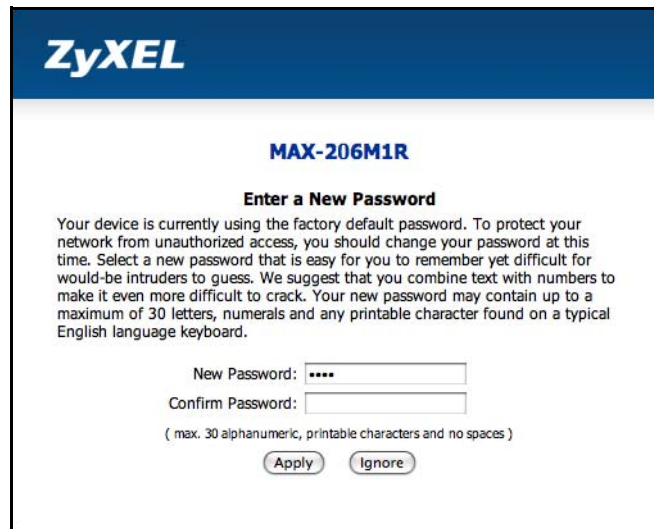
2.1.1 Accessing the Web Configurator

- 1 Make sure your WiMAX Modem 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**.



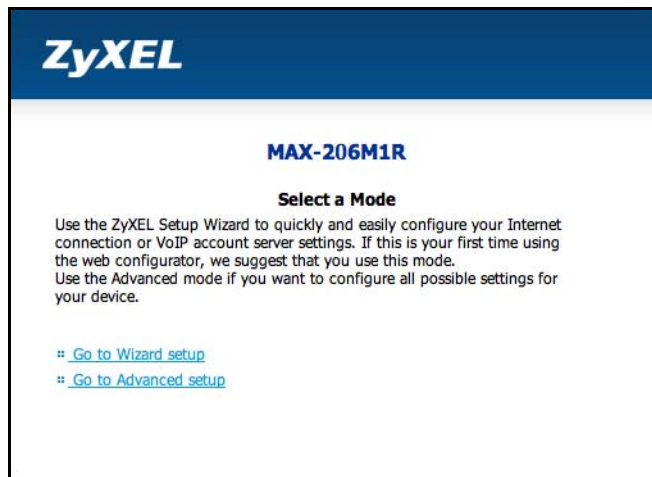
- 5 The following screen displays if you have not yet changed your password. It is highly recommended you change the default password. Enter a new password, retype it to confirm and click **Apply**; alternatively click **Ignore** to proceed to the main menu if you do not want to change the password now.



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



- 7 A screen displays to let you choose 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 45](#) 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 Modem automatically logs you out if you do not use the Web Configurator for five minutes. If this happens, 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

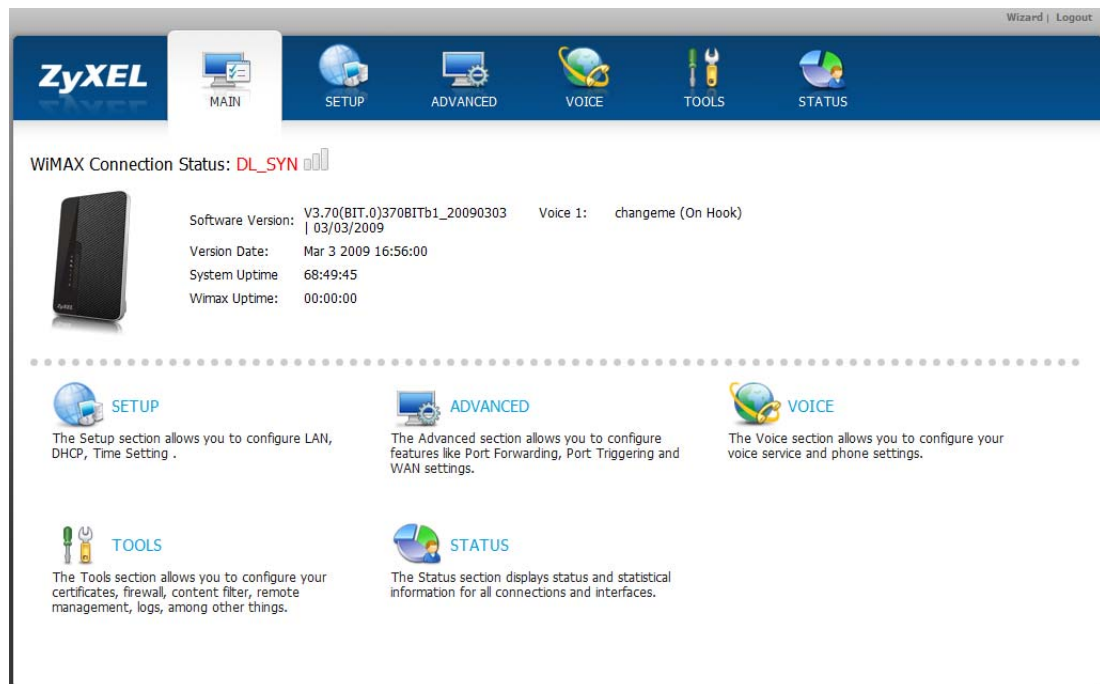
- 1 Make sure the **Power** light is on (not blinking).
- 2 To set the device back to the factory default settings, press the **Reset** button for ten seconds or until the **Power** light begins to blink and then release it. When the **Power** light begins to blink, the defaults have been restored and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

2.2 The Main Screen

When you first log into the web configurator and by-pass the wizard, the Main screen appears. Here you can view a summary of your WiMAX Modem 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.

Figure 5 Main Screen



The following table describes the icons in this screen.

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	<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 Modem'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 Modem is connected to the WiMAX network. Use the Strength Indicator icon to determine the quality of your network connection. • Disconnected - Indicates that the WiMAX Modem 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.

Table 4 Main (continued)

LABEL	DESCRIPTION
Software Version	<p>This field indicates the version number of the WiMAX Modem'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 07/08/2008 indicates that the firmware is 3.60, build BCC.0, candidate4, released on July 08, 2008.</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 Modem has been on. This resets every time you shut the device down or restart it.
WiMAX Uptime	This field indicates how long the WiMAX Modem 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.

Internet Connection Wizard

3.1 Overview

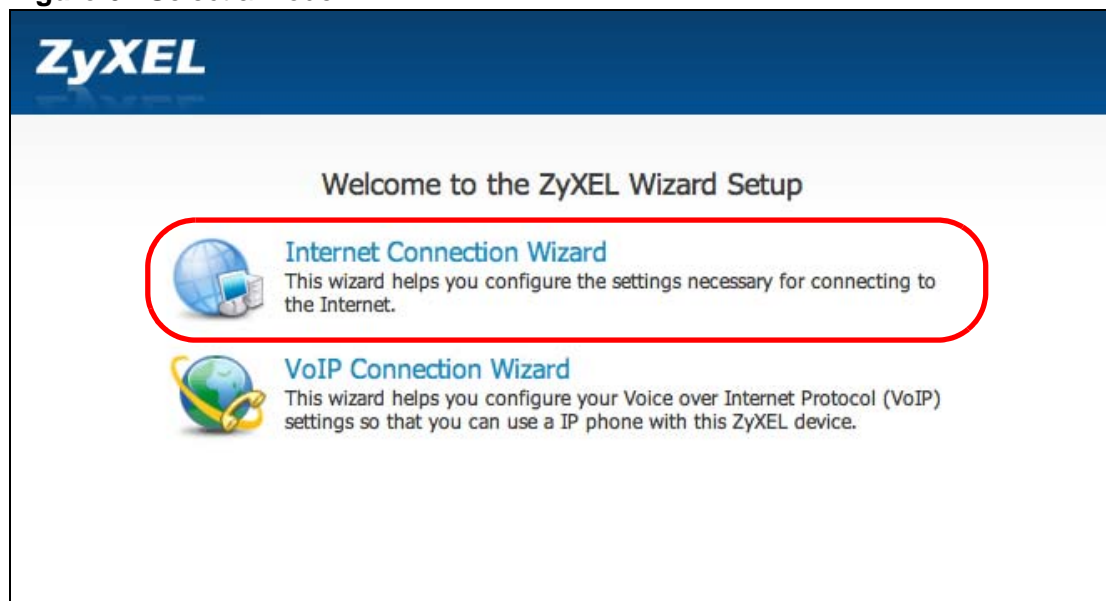
This chapter provides information on the ZyXEL Setup Wizard screens. The wizard guides you through several steps where you can configure your Internet and VoIP settings.

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.

The Internet Connection Wizard screens are described in detail in the following sections.

Figure 6 Select a Mode



3.1.2 System Information

This Internet Connection Wizard screen allows you to configure your WiMAX Modem's system information. The settings here correspond to the **ADVANCED > System Configuration > General** screen (see [Section 9.2 on page 101](#) for more).

Figure 7 Internet Connection Wizard > System Information

System Information

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

System Name:

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

Domain Name:

<Back Next > Close

The following table describes the labels in this screen.

Table 5 Internet Connection Wizard > System Information

LABEL	DESCRIPTION
System Name	System Name is a unique name to identify the WiMAX Modem 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 Authentication Settings

This Internet Connection Wizard screen allows you to configure your Internet access settings. The settings here correspond to the **ADVANCED > WAN Configuration > Internet Connection** screen (see [Section 7.2 on page 80](#) for more information).

Figure 8 Internet Connection Wizard > Authentication Settings Screen

Authentication Settings

Enter the required settings as issued by your ISP.

User Name:

Password:

Anonymous Identity:

PKM:

Authentication:

TTLS Inner EAP:

Certificate:

<Back Next > Close

The following table describes the labels in this screen.

Table 6 Internet Connection Wizard > Authentication Settings Screen

LABEL	DESCRIPTION
Authentication	
User Name	Use this field to enter the username associated with your Internet access account. You can enter up to 61 printable ASCII characters.
Password	Use this field to enter the password associated with your Internet access account. You can enter up to 47 printable ASCII characters.
Anonymous Identity	<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>

Table 6 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 Modem and the base station. At the time of writing, the WiMAX Modem 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 Modems 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 Modem 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 Modem uses to authenticate the AAA server. Use the TOOLS > Certificates > Trusted CA screen to import certificates to the WiMAX Modem.
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 IP Address

This Internet Connection Wizard screen allows you to configure your IP address. The settings here correspond to the **SETUP > Set IP Address** screen (see [Section 5.2 on page 58](#)).

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

Figure 9 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.

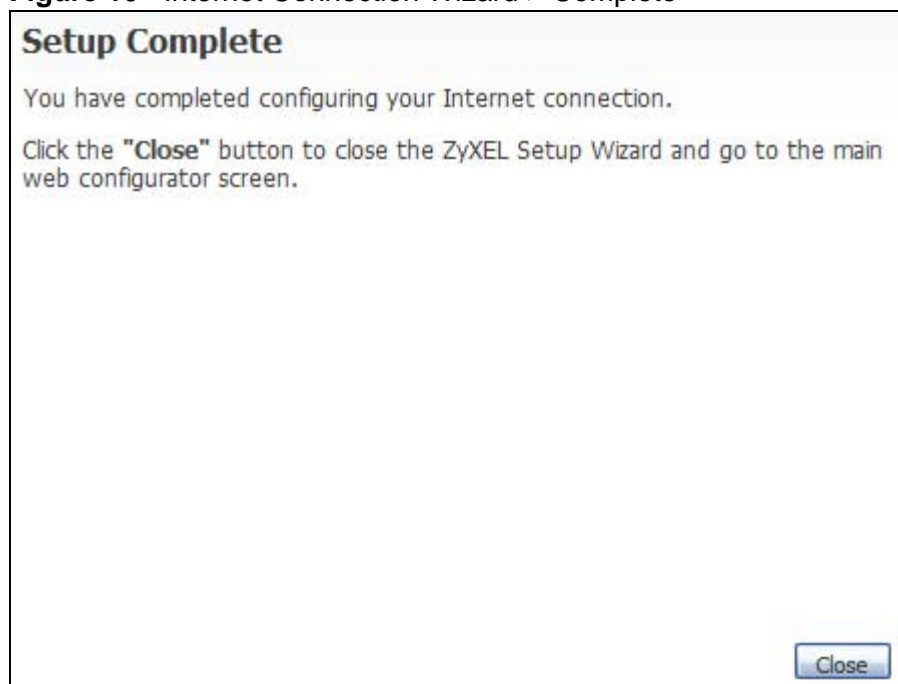
Table 7 Internet Connection Wizard > IP Address

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.
Use Fixed IP Address	A static IP address is a fixed IP that your ISP gives you.
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 Setup Complete

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

Figure 10 Internet Connection Wizard > Complete



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 Modem 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 shows you how to use the wizard to set up your voice account(s).

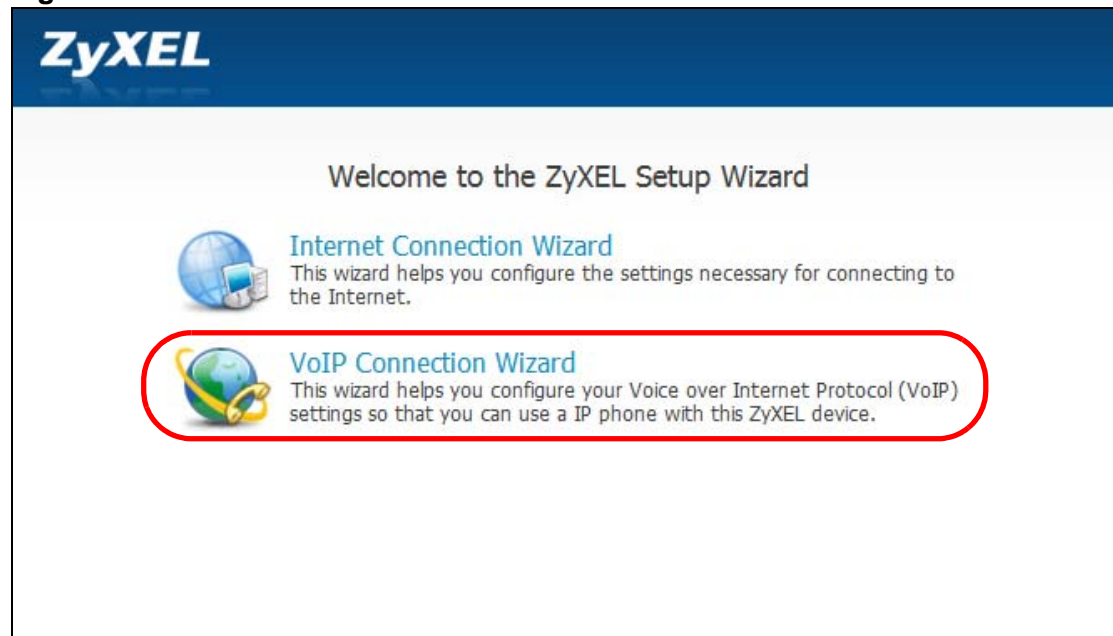
The WiMAX Modem has Voice over IP (VoIP) communication capabilities that allow you to use a traditional analog telephone to make Internet calls. You can configure the WiMAX Modem to use up to two SIP based VoIP accounts.

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.

The VoIP Connection Wizard screens are described in detail in the following sections.

Figure 11 Select a Mode



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 10.2 on page 113](#) for more information).

Figure 12 VoIP Connection > First Voice Account Settings

The following table describes the labels in this screen

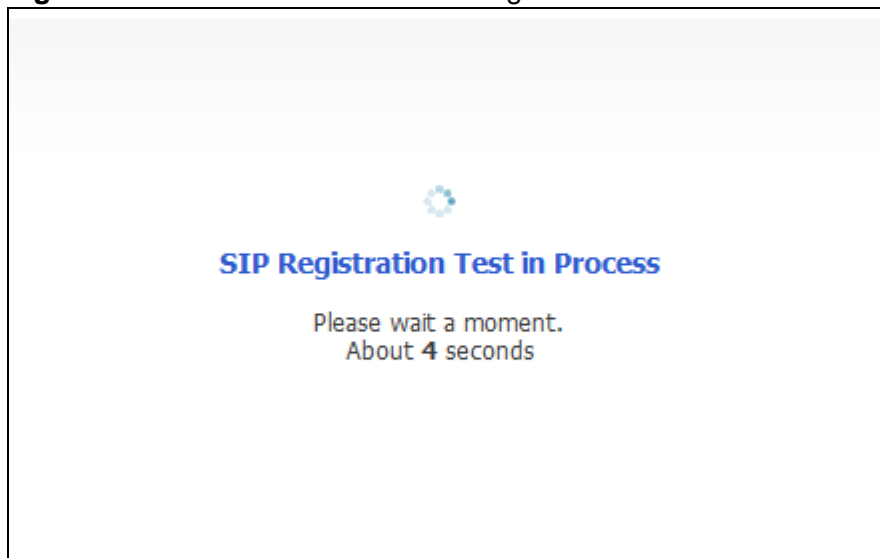
Table 8 VoIP Connection > First Voice Account Settings

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 8 VoIP Connection > First Voice Account Settings (continued)

LABEL	DESCRIPTION
Check here to set up SIP2 settings.	This screen configures SIP account 1. Select the check box if you have a second SIP account that you want to use. You will need to configure the same fields for the second SIP account.
Back	Click 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.

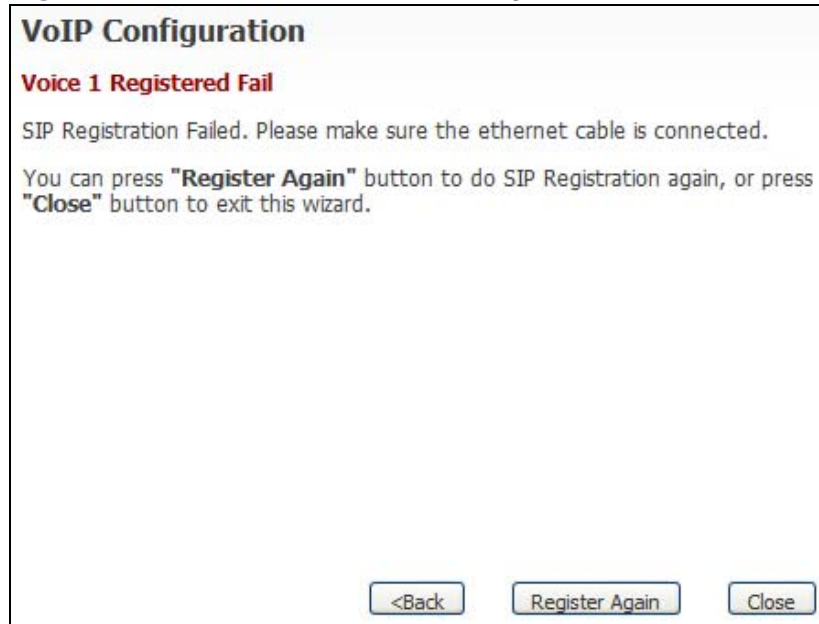
After you enter your voice account settings and click **Next**, the WiMAX Modem attempts to register your SIP account with the SIP server.

Figure 13 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 Modem, 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.

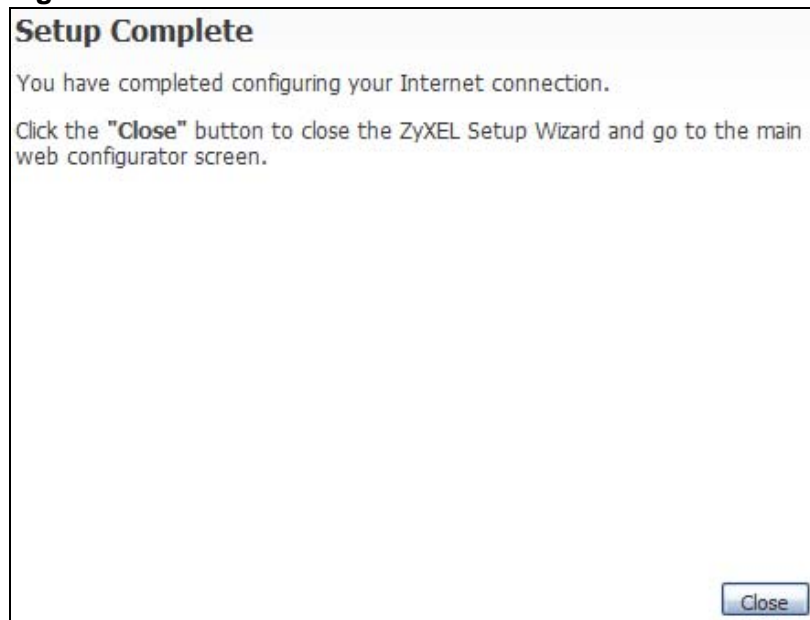
Figure 14 VoIP Connection > SIP Registration Fail



4.2.2 Setup Complete

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

Figure 15 VoIP Connection > Finish



This screen displays if your SIP account registration was successful.

PART II

Basic Screens

The Main Screen (41)

The Setup Screens (57)

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 58](#)) lets you configure the WiMAX Modem's IP address and subnet mask.
- The **DHCP Client** screen ([Section 5.3 on page 59](#)) to view connection information for clients configured by the WiMAX Modem's internal DHCP server.
- The **Time Setting** screen ([Section 5.4 on page 60](#)) lets you configure your WiMAX Modem'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.

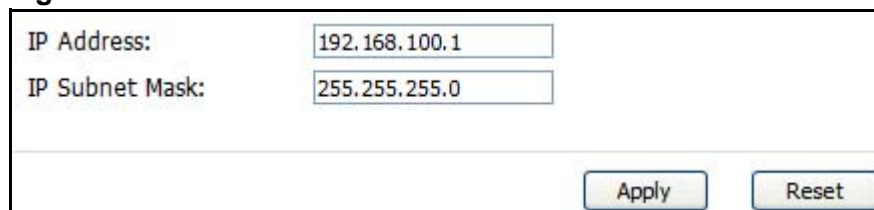
5.1.3 Before You Begin

- Make sure that you have made all the appropriate hardware connections to the WiMAX Modem, 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 Modem'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 16 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 9 SETUP > Set IP Address

LABEL	DESCRIPTION
IP Address	Enter the IP address of the WiMAX Modem on the LAN. Note: This field is the IP address you use to access the WiMAX Modem 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 the **SETUP > DHCP Client** to view connection information for all clients that have been configured by the WiMAX Modem's internal DHCP server.

Figure 17 SETUP > Set IP Address

DHCP Client				
#	IP Address	Host Name	MAC Address	Reserve
1	192.168.1.33	Coffee-Bean	00:1f:5b:ed:6c:7a	<input type="checkbox"/>
2	192.168.1.34	twpc13435	00:21:85:0c:44:1a	<input type="checkbox"/>

The following table describes the labels in this screen.

Table 10 SETUP > Set IP Address

LABEL	DESCRIPTION
#	This indicates the number of the item in this list.
IP Address	This indicates the IP address of a connected client device.
Host Name	This indicates the host name of a connected client device. If the device is computer, then the host name is the computer name.
MAC Address	This indicates the MAC address of a connected client device.

Table 10 SETUP > Set IP Address (continued)

LABEL	DESCRIPTION
Reserve	This indicates whether the IP address for the connected client device is reserved. When the DHCP server issues IP addresses, reserved IPs are assigned to specific client devices. If the IP address is reserved, the client device identified by its MAC address will always receive this IP address from the DHCP server.
Apply	Click to save your changes.
Refresh	Click to refresh the information in the screen.

5.4 Time Setting

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

Figure 18 SETUP > Time Setting

The following table describes the labels in this screen.

Table 11 SETUP > Time Setting

LABEL	DESCRIPTION
Current Time and Date	
Current Time	Displays the current time according to the WiMAX Modem.

Table 11 SETUP > Time Setting (continued)

LABEL	DESCRIPTION
Current Date	Displays the current time according to the WiMAX Modem.
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 Modem.
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 Modem 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 Modem 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 12 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
time1.stupi.se
tick.stdtime.gov.tw
tock.stdtime.gov.tw
time.stdtime.gov.tw

5.4.2 Resetting the Time

The WiMAX Modem 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 (65)

The WAN Configuration Screens (77)

The NAT Configuration Screens (89)

The System Configuration Screens (99)

The LAN Configuration Screens

6.1 Overview

Use the **ADVANCED > LAN Configuration** screens to set up the WiMAX Modem on the LAN. You can configure its IP address and subnet mask, DHCP services, and other subnets. You can also control how the WiMAX Modem 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 66](#)) lets you enable, disable, and configure the DHCP server in the WiMAX Modem.
- The **Static DHCP** screen ([Section 6.3 on page 68](#)) lets you assign specific IP addresses to specific computers on the LAN.
- The **IP Static Route** screen ([Section 6.4 on page 69](#)) lets you examine the static routes configured in the WiMAX Modem.
- The **Other Settings** screen ([Section 6.5 on page 71](#)) 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 your WiMAX Modem 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 Modem.

Figure 19 ADVANCED > LAN Configuration > DHCP Setup

DHCP Setup

Enable DHCP Server

IP Pool Starting Address: Pool Size:

DNS Server

DNS Servers Assigned by DHCP Server

First DNS Server:

Second DNS Server:

Third DNS Server:

The following table describes the labels in this screen.

Table 13 ADVANCED > LAN Configuration > DHCP Setup

LABEL	DESCRIPTION
DHCP Setup	
Enable DHCP Server	Select this if you want the WiMAX Modem to be the DHCP server on the LAN. As a DHCP server, the WiMAX Modem 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 Modem begins allocating IP addresses, if you have not specified an IP address for this computer 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 Modem is in). For example, if the IP Pool Start Address is 10.10.10.10, the WiMAX Modem 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 Modem 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 Modem. None - no DNS service will be provided by the WiMAX Modem.
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 20 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 14 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 Modem to assign the same IP address.
IP Address	Enter the IP address you want the WiMAX Modem to assign to the computer.
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

6.4 IP Static Route

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



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

Figure 21 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 15 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 16 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 Modem 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.

6.4.1 IP Static Route Setup

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

Figure 22 Advanced> LAN Configuration > IP Static Route Setup

The screenshot shows a configuration window titled "Static Route Setup". It contains the following fields and controls:

- Route Name:** An empty text input field.
- Active:** An unchecked checkbox.
- Private:** An unchecked checkbox.
- Destination IP Address:** A text input field containing "0.0.0.0".
- IP Subnet Mask:** A text input field containing "0.0.0.0".
- Gateway IP Address:** A text input field containing "0.0.0.0".
- Metric:** A text input field containing "2".
- Buttons:** "Apply" and "Cancel" buttons at the bottom right.

The following table describes the labels in this screen.

Table 17 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 Modem 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 Modem 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 Modem 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 17 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.

6.5 Other Settings

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

Figure 23 ADVANCED > LAN Configuration > Advanced

The following table describes the labels in this screen.

Table 18 ADVANCED > LAN Configuration > Other Settings

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

Table 18 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 Modem 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 Modem does not support multicasting. • IGMP-v1 - The WiMAX Modem supports IGMP version 1. • IGMP-v2 - The WiMAX Modem 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.

6.6 Technical Reference

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

6.6.1 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 Modem. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your WiMAX Modem, 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 Modem 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 Modem unless you are instructed to do otherwise.

6.6.2 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 Modem as a DHCP server or disable it. When configured as a server, the WiMAX Modem 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 Modem 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 68](#).

6.6.3 LAN TCP/IP

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

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

These parameters should work for the majority of installations. If your ISP gives you explicit DNS server address(es), see [Section 6.3 on page 68](#).

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

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

- **None** - the WiMAX Modem 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 Modem 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.

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

The WAN Configuration Screens

7.1 Overview

Use the **ADVANCED > WAN Configuration** screens to set up your WiMAX Modem'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 80](#)) lets you set up your WiMAX Modem's Internet settings.
- The **WiMAX Configuration** screen ([Section 7.3 on page 82](#)) lets set up the frequencies used by your WiMAX Modem.
- The **Antenna Selection** screen ([Section 7.4 on page 86](#)) to switch between the WiMAX Modem's internal antenna and the external antennas (MAX-216M1R plus only; other models do not support this option.)
- The **Advanced** screen ([Section 7.5 on page 87](#)) 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 24 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 25 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.

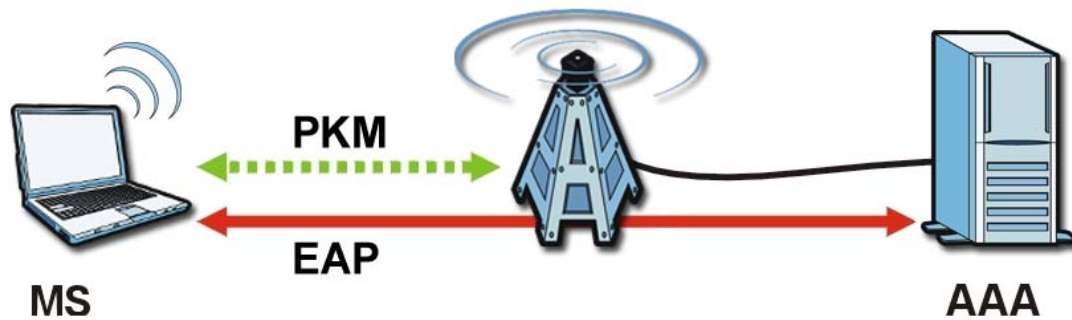
The radio frequency and bandwidth of the link between the WiMAX Modem and the base station are controlled by the base station. The WiMAX Modem follows the base station's configuration.

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 26 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.

7.2 Internet Connection

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

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

Figure 27 ADVANCED > WAN Configuration > Internet Connection

The following table describes the labels in this screen.

Table 19 ADVANCED > WAN Configuration > Internet Connection > ISP Parameters for Internet Access

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

Table 19 ADVANCED > WAN Configuration > Internet Connection > ISP
Parameters for Internet Access (continued)

LABEL	DESCRIPTION
PKM	This field displays the Privacy Key Management version number. PKM provides security between the WiMAX Modem and the base station. At the time of writing, the WiMAX Modem 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 Modems 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 Modem 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)
Auth Mode	<p>Select the authentication mode from the drop-down list box.</p> <p>This field is not available in all WiMAX Modems. Check with your service provider for details.</p> <p>The WiMAX Modem supports the following authentication modes:</p> <ul style="list-style-type: none"> • User Only • Device Only with Cert • Certs and User Authentication
Certificate	This is the security certificate the WiMAX Modem uses to authenticate the AAA server. Use the TOOLS > > Trusted CAs screen to import certificates to the WiMAX Modem.
WAN IP Address Assignment	

Table 19 ADVANCED > WAN Configuration > Internet Connection > ISP Parameters for Internet Access (continued)

LABEL	DESCRIPTION
Get automatically from ISP (Default)	Select this if you have a dynamic IP address. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet.
Use Fixed IP Address	A static IP address is a fixed IP that your ISP gives you. Type your ISP assigned IP address in the IP Address field below.
IP Subnet Mask	Enter a subnet mask in dotted decimal notation. Refer to the appendices to calculate a subnet mask If you are implementing subnetting.
Gateway IP Address	Specify a gateway IP address (supplied by your ISP).
Apply	Click 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 Modem.

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

Radio frequency is measured in Hertz (Hz).

Table 20 Radio Frequency Conversion

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

Figure 28 ADVANCED > WAN Configuration > WiMAX Configuration

DL Frequency [1]	<input type="text" value="0"/>	kHz
DL Frequency [2]	<input type="text" value="0"/>	kHz
DL Frequency [3]	<input type="text" value="0"/>	kHz
DL Frequency [4]	<input type="text" value="0"/>	kHz
DL Frequency [5]	<input type="text" value="0"/>	kHz
DL Frequency [6]	<input type="text" value="0"/>	kHz
DL Frequency [7]	<input type="text" value="0"/>	kHz
DL Frequency [8]	<input type="text" value="0"/>	kHz
DL Frequency [9]	<input type="text" value="0"/>	kHz
DL Frequency [10]	<input type="text" value="0"/>	kHz
DL Frequency [11]	<input type="text" value="0"/>	kHz
DL Frequency [12]	<input type="text" value="0"/>	kHz
DL Frequency [13]	<input type="text" value="0"/>	kHz
DL Frequency [14]	<input type="text" value="0"/>	kHz
DL Frequency [15]	<input type="text" value="0"/>	kHz
DL Frequency [16]	<input type="text" value="0"/>	kHz
DL Frequency [17]	<input type="text" value="0"/>	kHz
DL Frequency [18]	<input type="text" value="0"/>	kHz
DL Frequency [19]	<input type="text" value="0"/>	kHz
Bandwidth	<input type="text" value="10000"/>	KHz

The following table describes the labels in this screen.

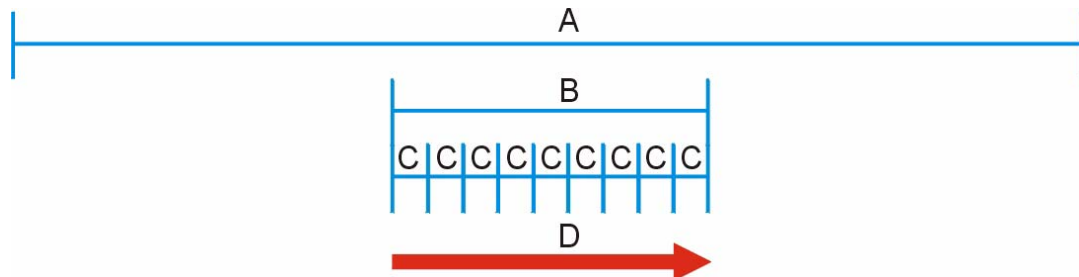
Table 21 ADVANCED > WAN Configuration > WiMAX Configuration

LABEL	DESCRIPTION
DL Frequency / Bandwidth	<p>These fields show the downlink frequency settings in kilohertz (kHz). Enter values in these fields to have the WiMAX Modem scan these frequencies for available channels in ascending numerical order.</p> <p>Note: The Bandwidth field is not user-configurable; when the WiMAX Modem 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 Modem searching a range of frequencies to find a connection to a base station.

Figure 29 Frequency Ranges



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

Have the WiMAX Modem 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 Modem 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 Modem 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 85](#) for an example of using the **WiMAX Frequency** screen.

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

- The WiMAX Modem searches the **DL Frequency** settings in ascending numerical order, from **[1]** to **[9]**.

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

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

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

Table 22 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 Modem searches at 2500000 kHz, and then searches at 2550000 kHz if it has not found a connection.	<i>The WiMAX Modem searches at 2500000 kHz and then at 2550000 kHz if it has not found an available connection. If it still does not find an available connection, it searches at 2600000 kHz.</i>

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 30 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

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

When the WiMAX Modem 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 Antenna Selection

Click **ADVANCED > WAN Configuration > Antenna Selection** to switch between the WiMAX Modem's internal antenna and the (optional) external antennas, if they are installed.

Note: This screen only pertains to the MAX-216M1R plus. Other devices in this series do not support external antennas.

Figure 31 ADVANCED > WAN Configuration > Antenna Selection

Select the Antenna Switch Mode

Use Internal Antenna

Use External Antenna

The following table describes the labels in this screen.

Table 23 ADVANCED > WAN Configuration > Advanced

LABEL	DESCRIPTION
Select the Antenna Switch Mode	
Use Internal Antenna	Select this to use the device's internal antenna.
Use External Antenna	Select this to use the device's external antenna. If you select this option but do not have external antennas attached, you may experience poor reception. External antennas are optional and not required.

Table 23 ADVANCED > WAN Configuration > Advanced (continued)

LABEL	DESCRIPTION
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

7.5 Advanced

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

Figure 32 ADVANCED > WAN Configuration > Advanced

The screenshot displays the 'Advanced' configuration page for WAN settings, organized into three 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 24 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 Modem's WAN IP address). Use the drop-down list box to select a DNS server IP address that the ISP assigns in the field to the right.</p> <p>Select UserDefined if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose UserDefined, but leave the IP address set to 0.0.0.0, UserDefined changes to None after you click Apply. If you set a second choice to UserDefined, and enter the same IP address, the second UserDefined changes to None after you click Apply.</p> <p>Select None if you do not want to configure DNS servers. You must have another DHCP server on your LAN, or else the computers must have their DNS server addresses manually configured. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.</p>
RIP & Multicast Setup	
RIP Direction	Select the RIP direction from None , Both , In Only and Out Only .
RIP Version	Select the RIP version from RIP-1 , RIP-2B and RIP-2M .
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group. The WiMAX Modem 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	<p>Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you also need to enable the default WAN to LAN firewall rule that forwards NetBIOS traffic.</p> <p>Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN.</p>
Allow Trigger Dial	Select this option to allow NetBIOS packets to initiate calls.
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

The NAT Configuration Screens

8.1 Overview

Use these screens to configure port forwarding and trigger ports for the WiMAX Modem. 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.

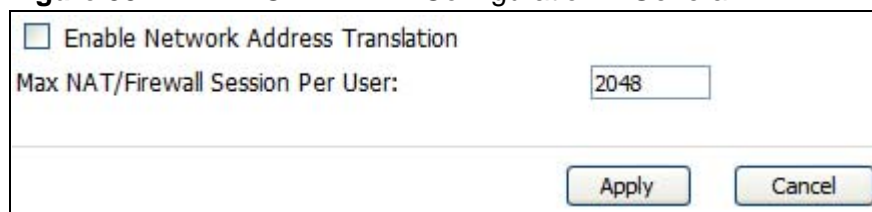
8.1.1 What You Can Do in This Chapter

- The **General** screen ([Section 8.2 on page 89](#)) lets you enable or disable NAT and to allocate memory for NAT and firewall rules.
- The **Port Forwarding** screen ([Section 8.3 on page 90](#)) lets you look at the current port-forwarding rules in the WiMAX Modem, and to enable, disable, activate, and deactivate each one.
- The **Trigger Port** screen ([Section 8.4 on page 94](#)) lets you maintain trigger port forwarding rules for the WiMAX Modem.
- The **ALG** screen ([Section 8.5 on page 96](#)) lets you enable and disable SIP (VoIP), FTP (file transfer), and H.323 (audio-visual) ALG in the WiMAX Modem.

8.2 General

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

Figure 33 ADVANCED > NAT Configuration > General



Enable Network Address Translation

Max NAT/Firewall Session Per User:

The following table describes the labels in this screen.

Table 25 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 Modem.</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.

8.3 Port Forwarding

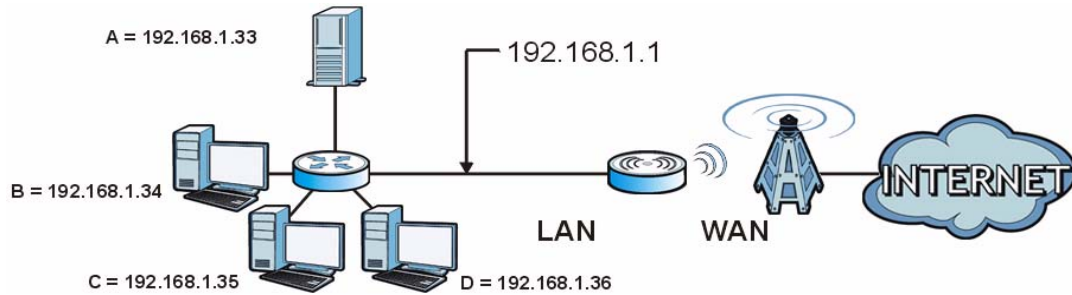
A NAT server set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make accessible to the outside world even though NAT makes your whole inside network appear as a single machine to the outside world.

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 34 Multiple Servers Behind NAT Example



8.3.1 Port Forwarding Options



Click **ADVANCED > NAT Configuration > Port Forwarding** to look at the current port-forwarding rules in the WiMAX Modem, 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 35 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 26 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 27 ADVANCED > NAT Configuration > Port Forwarding

LABEL	DESCRIPTION
Default Server Setup	
Default Server	Enter the IP address of the server to which the WiMAX Modem 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 Modem 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.

8.3.2 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 36 ADVANCED > NAT Configuration > Port Forwarding > Rule Setup

The screenshot shows a window titled "Rule Setup" with the following elements:

- Active
- Service Name: []
- Start Port: [0]
- End Port: [0]
- Server IP Address: [0.0.0.0]
- Buttons: Apply, Cancel

The following table describes the labels in this screen.

Table 28 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	<p>Enter the port number or range of port numbers you want to forward to the specified server.</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.
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.

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

Figure 37 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 29 ADVANCED > NAT Configuration > Trigger Port

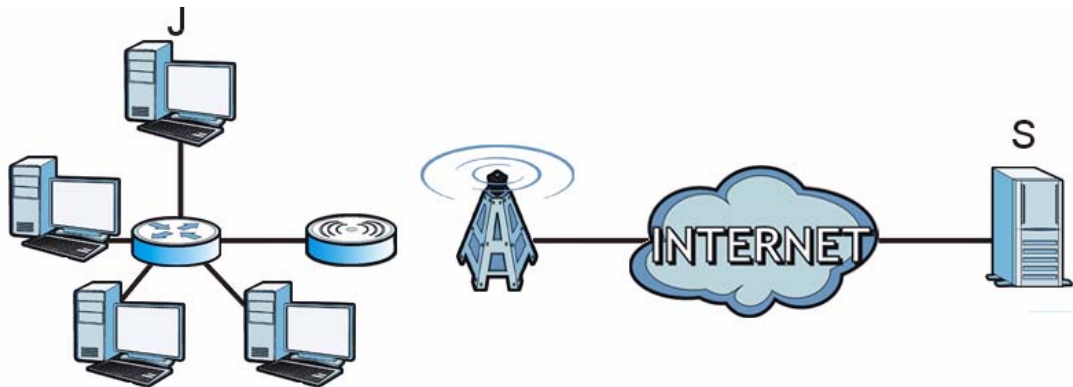
LABEL	DESCRIPTION
#	The number of the item in this list.
Name	Enter a name to identify this rule. You can use 1 - 15 printable ASCII characters, or you can leave this field blank. It does not have to be a unique name.
Incoming	

Table 29 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 Modem 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 Modem 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.

8.4.1 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 38 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 Modem to record Jane's computer IP address. The WiMAX Modem 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 Modem 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 Modem 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 Modem and going to the outside.
- 2 If an application needs a continuous data stream, that port (range) will be tied up so that another computer on the LAN can't trigger it.

8.5 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 Modem.

Figure 39 ADVANCED > NAT Configuration > ALG

The screenshot shows a configuration window with a white background and a thin black border. At the top left, there are three lines of text, each preceded by a green checkmark in a small square box: 'Enable SIP ALG', 'Enable FTP ALG', and 'Enable H.323 ALG'. Below these options is a horizontal separator line. At the bottom right of the window, there are two rectangular buttons with rounded corners: 'Apply' and 'Cancel', both with a light blue gradient and a thin black border.

The following table describes the labels in this screen.

Table 30 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.

The System Configuration Screens

9.1 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.

9.1.1 What You Can Do in This Chapter

- The **General** screen ([Section 9.2 on page 101](#)) lets you change the WiMAX Modem's mode, set up its system name, domain name, idle timeout, and administrator password.
- The **Dynamic DNS** screen ([Section 9.3 on page 102](#)) lets you set up the WiMAX Modem as a dynamic DNS client.
- The **Firmware** screen ([Section 9.4 on page 104](#)) lets you upload new firmware to the WiMAX Modem.
- The **Configuration** screen ([Section 9.5 on page 106](#)) lets you back up or restore the configuration of the WiMAX Modem.
- The **Restart** screen ([Section 9.6 on page 107](#)) lets you restart your WiMAX Modem from within the web configurator.

9.1.2 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 Modem **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 Modem 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 Modem 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.

9.2 General

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

Figure 40 ADVANCED > System Configuration > General

The screenshot shows a web-based configuration interface. It has a title bar 'System Setup' and a subtitle 'Password Setup'. Under 'System Setup', there are three input fields: 'System Name', 'Domain Name', and 'Administrator Inactivity Timer' (with a value of '0' and the text 'minutes (0 means no timeout)'). Under 'Password Setup', there are three input fields: 'Old Password' (masked with '••••'), 'New Password', and 'Retype to Confirm'. At the bottom right, there are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

Table 31 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 Modem.
New Password	Enter the new password for the WiMAX Modem. You can use up to 30 characters. As you type the password, the screen displays an asterisk (*) for each character you type.

Table 31 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.

9.3 Dynamic DNS

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

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

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 Modem as a dynamic DNS client.

Figure 41 ADVANCED > System Configuration > Dynamic DNS

The following table describes the labels in this screen.

Table 32 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 32 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 Modem 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 Modem 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 Modem 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.

9.4 Firmware

Click **ADVANCED > System Configuration > Firmware** to upload new firmware to the WiMAX Modem. Firmware files usually use the system model name with a "*.bin" extension, such as "WiMAX Modem.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 Modem's specific model.

Figure 42 ADVANCED > System Configuration > Firmware

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

File Path:

The following table describes the labels in this screen.

Table 33 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!

9.4.1 The Firmware Upload Process

When the WiMAX Modem 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.

9.5 Configuration

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

Figure 43 ADVANCED > System Configuration > Configuration

The screenshot shows a web interface with three main sections: Backup Configuration, Restore Configuration, and Back to Factory Defaults. Each section has a title bar and a description. The Backup section has a 'Backup' button. The Restore section has a 'File Path' input field, a 'Browse...' button, and an 'Upload' button. The Back to Factory Defaults section has a 'Reset' button and a list of default settings.

The following table describes the labels in this screen.

Table 34 ADVANCED > System Configuration > Configuration

LABEL	DESCRIPTION
Backup Configuration	
Backup	Click this to save the WiMAX Modem'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 Modem to its factory defaults. There is no warning screen.

9.5.1 The Restore Configuration Process

When the WiMAX Modem 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 Modem'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.

9.6 Restart

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

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

Figure 44 ADVANCED > System Configuration > Restart

Click **Restart** to have the device perform a software restart. The power LED blinks as the device restarts and then shines steadily if the restart is successful. Wait a minute before logging into the device again.

Restart

The following table describes the labels in this screen.

Table 35 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 Modem after a restart.</p>

9.6.1 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.

PART IV

Voice Screens

The Service Configuration Screens (111)

The Phone Screens (129)

The Phone Book Screens (139)

The Service Configuration Screens

10.1 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.

10.1.1 What You Can Do in This Chapter

- The **SIP Settings** screen ([Section 10.2 on page 113](#)) lets you setup and maintain your SIP account(s) in the WiMAX Modem.
- The **Advanced SIP Settings** screen ([Section 10.2.1 on page 115](#)) lets you set up and maintain advanced settings for each SIP account
- The **QoS** screen ([Section 10.3 on page 122](#)) lets you set up and maintain ToS and VLAN settings for the WiMAX Modem.

10.1.2 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 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, 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 Modem 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 Modem.

10.1.3 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 Modem.
- Connect your WiMAX Modem 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.

10.2 SIP Settings

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

Figure 45 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 36 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 Modem to use this account. Clear it if you do not want the WiMAX Modem 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 Modem'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.

10.2.1 Advanced SIP Settings

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

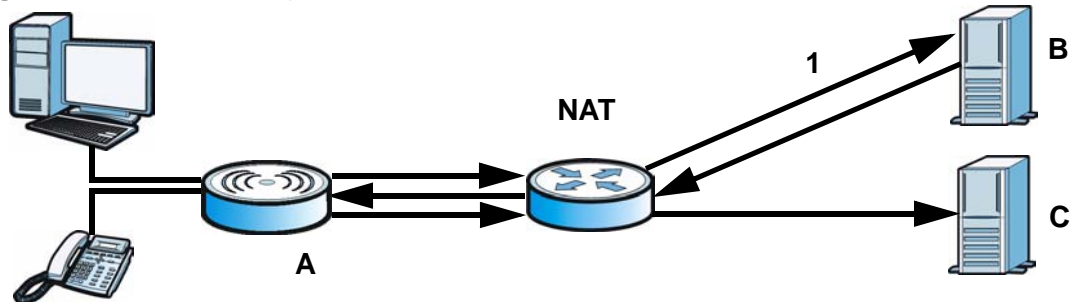
10.2.1.1 STUN

STUN (Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators) allows the WiMAX Modem to find the presence and types of NAT routers and/or firewalls between it and the public Internet. STUN also allows the WiMAX Modem to find the public IP address that NAT assigned, so the WiMAX Modem 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 Modem (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 Modem's SIP packets and sends them to the WiMAX Modem.
- 3 The WiMAX Modem uses the public IP address and port number in the SIP packets that it sends to the SIP server (C).

Figure 46 STUN Example



10.2.1.2 Outbound Proxy

Your VoIP service provider may host a SIP outbound proxy server to handle all of the WiMAX Modem's VoIP traffic. This allows the WiMAX Modem 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 Modem to keep it from re-translating the IP address (since this is already handled by the outbound proxy server).

10.2.1.3 Voice Coding

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

10.2.1.4 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.

10.2.1.5 Advanced SIP Settings Options

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

Figure 47 VOICE > Service Configuration > SIP Settings > Advanced

SIP Server Settings URL Type: <input type="text" value="SIP"/> (dropdown) Expiration Duration: <input type="text" value="3600"/> (20-65535) sec Register Re-send timer: <input type="text" value="180"/> (1-65535) sec Session Expires: <input type="text" value="180"/> (30-3600) sec Min-SE: <input type="text" value="30"/> (20-1800) sec		Outbound Proxy <input type="checkbox"/> Active Server Address: <input type="text"/> Server Port: <input type="text" value="3478"/> (1025-65535)	
RTP Port Range Start Port: <input type="text" value="4000"/> (1025-65535) End Port: <input type="text" value="65535"/> (1025-65535)		NAT Keep Alive <input type="checkbox"/> Active <input type="radio"/> Keep Alive With SIP Proxy <input type="radio"/> Keep Alive With Outbound Proxy Keep Alive Interval: <input type="text" value="120"/> (30-65535) sec	
Voice Compression Primary Compression Type: <input type="text" value="G.711A"/> (dropdown) Secondary Compression Type: <input type="text" value="G.729"/> (dropdown) Third Compression Type: <input type="text" value="G.711u"/> (dropdown) DTMF Mode: <input type="text" value="RFC 2883"/> (dropdown)		MWI (Message Waiting Indication) <input type="checkbox"/> Enable Expiration Time: <input type="text" value="1800"/> (1-65535) sec	
STUN <input type="checkbox"/> Active Server Address: <input type="text"/> Server Port: <input type="text" value="3478"/> (1025-65535)		Fax Option <input checked="" type="radio"/> G.711 Fax Passthrough <input type="radio"/> T.38 Fax Relay	
Use NAT <input type="checkbox"/> Active Server Address: <input type="text"/> Server Port: <input type="text" value="5060"/> (1025-65535)		Call Forward Call Forward Table: <input type="text" value="Table1"/> (dropdown)	
		Caller Ringing <input type="checkbox"/> Enable Caller Ringing Tone: <input type="text" value="Default"/> (dropdown)	
		On Hold <input type="checkbox"/> Enable On Hold Tone: <input type="text" value="Default"/> (dropdown)	

The following table describes the labels in this screen.

Table 37 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 Modem 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 37 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 Modem 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 Modem 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 Modem or the other party updates this timer to prevent this from happening.
Min-SE	Enter the minimum number of seconds the WiMAX Modem 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 Modem 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 Modem 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 Modem 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 115</p>
DTMF Mode	<p>Control how the WiMAX Modem 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

Table 37 VOICE > Service Configuration > SIP Settings > Advanced (continued)

LABEL	DESCRIPTION
STUN	
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 Modem 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 Modem 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 Modem. 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 Modem 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 Modem 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 Modem and SIP server (a SIP proxy server or outbound proxy server) from dropping the SIP session. The WiMAX Modem 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 Modem 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 37 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 Modem subscribes to the service. Before this time passes, the WiMAX Modem automatically subscribes again.
Fax Option	
G.711 Fax Passthrough	Select this if the WiMAX Modem 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 Modem 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 Modem 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 120 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 120 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.

10.2.1.6 Custom Tones (IVR)

IVR (Interactive Voice Response) is a feature that allows you to use your telephone to interact with the WiMAX Modem. The WiMAX Modem 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 38 Custom Tones Details

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

Table 38 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.

10.3 QoS

Network traffic can be classified by setting the ToS (Type Of Service) values at the data source (for example, at the WiMAX Modem) 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 Modem can add IEEE 802.1Q VLAN ID tags to voice frames that it sends to the network. This allows the WiMAX Modem 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 Modem. 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 48 VOICE > Service Configuration > QoS

The screenshot shows a configuration interface for QoS. It has a title bar 'TOS'. Below it are two rows: 'SIP TOS Priority Setting:' with a text box containing '5' and '(0-255)' to its right, and 'RTP TOS Priority Setting:' with a text box containing '5' and '(0-255)' to its right. A dashed line separates this from the 'VLAN Tagging' section. Under 'VLAN Tagging', there is a checkbox labeled 'Voice VLAN ID:' which is unchecked, followed by a text box 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 39 VOICE > Service Configuration > QoS

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

Table 39 VOICE > Service Configuration > QoS

LABEL	DESCRIPTION
Voice VLAN ID	Select this if the WiMAX Modem 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.

10.4 Technical Reference

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

10.4.1 SIP Call Progression

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

Table 40 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.

10.4.2 SIP Client Server

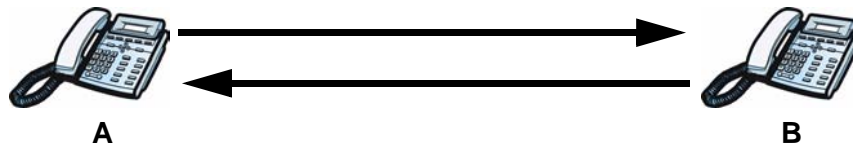
SIP is a client-server protocol. A SIP client is an application program or device that sends SIP requests. A SIP server responds to the SIP requests.

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.

10.4.3 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 49 SIP User Agent



10.4.4 SIP Proxy Server

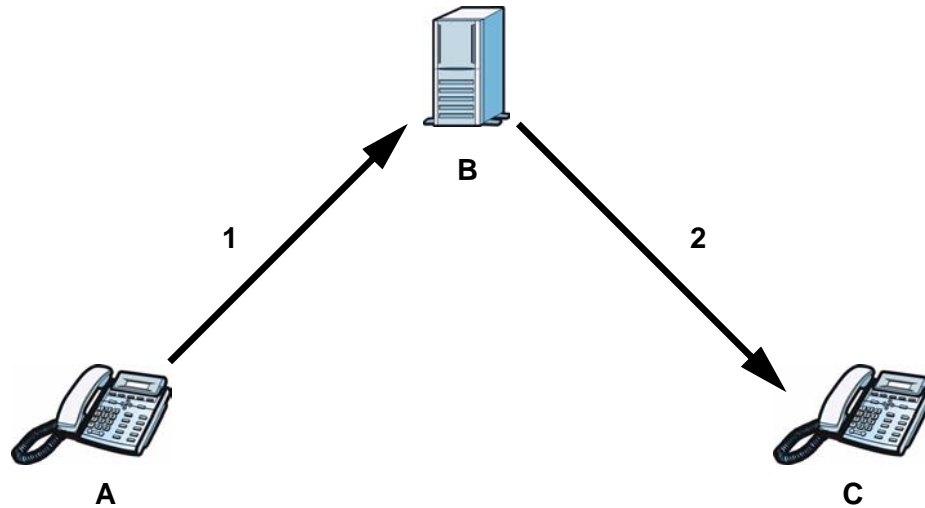
A SIP proxy server receives requests from clients and forwards them to another server.

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 50 SIP Proxy Server



10.4.5 SIP Redirect Server

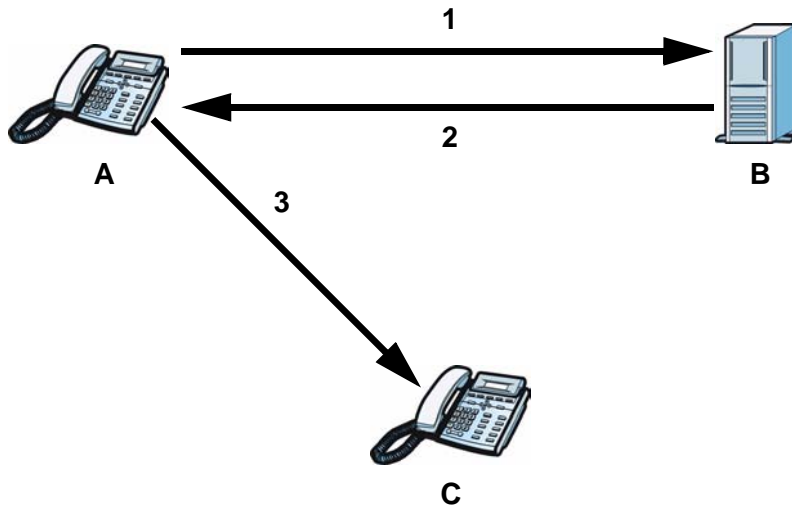
A SIP redirect server accepts SIP requests, translates the destination address to an IP address and sends the translated IP address back to the device that sent the request. Then the client device that originally sent the request can send requests to the IP address that it received back from the redirect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

- Client device A then sends the call invitation to client device C.

Figure 51 SIP Redirect Server



10.4.6 NAT and SIP

The WiMAX Modem must register its public IP address with a SIP register server. If there is a NAT router between the WiMAX Modem and the SIP register server, the WiMAX Modem probably has a private IP address. The WiMAX Modem 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 Modem's IP address from inside the SIP message and maps it to your SIP identity. If the WiMAX Modem has a private IP address listed in the SIP message, the SIP server cannot map it to your SIP identity. See [Chapter 8 The NAT Configuration Screens](#) for more information.

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

10.4.7 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.

10.4.8 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 52 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.

The Phone Screens

11.1 Overview

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

11.1.1 What You Can Do in This Chapter

- The **Analog Phone** screen ([Section 11.2 on page 130](#)) lets you control which SIP accounts each phone uses.
- The **Common** screen ([Section 11.3 on page 132](#)) lets you activate and deactivate immediate dialing.
- The **Region** screen ([Section 11.4 on page 133](#)) lets you maintain settings that often depend on the region of the world in which the WiMAX Modem is located.

11.1.2 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 Modem reduce the bandwidth that a call uses by not transmitting “silent packets” when you are not speaking.

When using VAD, the WiMAX Modem 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 Modem 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 Modem's phone port, you may need to subscribe to the services from your VoIP service provider.

11.2 Analog Phone

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

Figure 53 VOICE > Phone > Analog Phone



Phone Port Settings: Phone1

Outgoing Call Use

SIP1

Incoming Call apply to

SIP1

Apply Reset Advanced

The following table describes the labels in this screen.

Table 41 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.
Phone Port Settings	Displays the phone port number.
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 Modem 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.
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.

11.2.1 Advanced Analog Phone Setup

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

Figure 54 VOICE > Phone > Analog Phone > Advanced

Voice Volume Control

Speaking Volume: -1 (Min.)

Listening Volume: -1 (Min.)

Echo Cancellation

G.168 Active

Dialing Interval Select

Dialing Interval Select: 3

VAD Support

<Back Apply Reset

The following table describes the labels in this screen.

Table 42 VOICE > Phone > Analog Phone > Advanced

LABEL	DESCRIPTION
Voice Volume Control	
Speaking Volume	Enter the loudness that the WiMAX Modem uses for speech that it sends to the peer device. -14 is the quietest, and 14 is the loudest.
Listening Volume	Enter the loudness that the WiMAX Modem uses for speech that it receives from the peer device. -14 is the quietest, and 14 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 Modem 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 Modem to make the phone call immediately, regardless of this setting.
VAD Support	Select this if the WiMAX Modem should stop transmitting when you are not speaking. This reduces the bandwidth the WiMAX Modem uses.
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.

11.3 Common

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

Figure 55 VOICE > Phone > Common

The screenshot shows a user interface for the 'VOICE > Phone > Common' settings. At the top, there is a checkbox labeled 'Active Immediate Dial' which is currently unchecked. Below the checkbox, there are two buttons: 'Apply' and 'Reset', both of which are highlighted with a light blue border.

The following table describes the labels in this screen.

Table 43 VOICE > Phone > Common

LABEL	DESCRIPTION
Active Immediate Dial	Select this if you want to use the pound key (#) to tell the WiMAX Modem 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 Modem makes the call immediately.
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

11.4 Region

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

Figure 56 VOICE > Phone > Region

The screenshot shows a settings window for 'Region'. It contains two dropdown menus. The first is labeled 'Region Settings:' and is currently set to 'United States'. The second is labeled 'Call Service Mode:' and is currently set to 'USA Type'. Below these menus are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

Table 44 VOICE > Phone > Region

LABEL	DESCRIPTION
Region Settings	Select the place in which the WiMAX Modem 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.

11.5 Technical Reference

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

11.5.1 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 Modem 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.

11.5.2 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 45 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".

11.5.3 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 46 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

12.1 Overview

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

12.1.1 What You Can Do in This Chapter

- The **Incoming Call Policy** screen ([Section 12.2 on page 140](#)) lets you maintain rules for handling incoming calls. You can block, redirect, or accept them.
- The **Speed Dial** screen ([Section 12.3 on page 142](#)) lets you add, edit, or remove speed-dial entries.

12.1.2 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 Modem, 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 Modem 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.

12.2 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 57 VOICE > Phone Book > Incoming Call Policy

Table Number: <input type="text" value="Table 1"/>				
Forward to Number Setup				
<input type="checkbox"/>	Unconditional Forward to Number:	<input type="text"/>		
<input type="checkbox"/>	Busy Forward to Number:	<input type="text"/>		
<input type="checkbox"/>	No Answer Forward to Number:	<input type="text"/>		
	No Answer Waiting Time:	<input type="text" value="5"/> (Second)		
Advanced Setup				
#	Activate	Incoming Call Number	Forward to Number	Condition
1	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	Unconditional <input type="button" value="v"/>
2	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	Unconditional <input type="button" value="v"/>
3	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	Unconditional <input type="button" value="v"/>
4	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	Unconditional <input type="button" value="v"/>
5	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	Unconditional <input type="button" value="v"/>
6	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	Unconditional <input type="button" value="v"/>
7	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	Unconditional <input type="button" value="v"/>
8	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	Unconditional <input type="button" value="v"/>
9	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	Unconditional <input type="button" value="v"/>
10	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	Unconditional <input type="button" value="v"/>
<input type="button" value="Apply"/> <input type="button" value="Reset"/>				

The following table describes the labels in this screen.

Table 47 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 Modem 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 Modem 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 47 VOICE > Phone Book > Incoming Call Policy

LABEL	DESCRIPTION
No Answer Forward to Number	Select this if you want the WiMAX Modem 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 Modem 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 Modem immediately forwards any calls from the Incoming Call Number to the Forward to Number. • Busy - The WiMAX Modem 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 Modem 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 Modem rejects calls from the Incoming Call Number. • Accept - The WiMAX Modem 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 Modem checks the Advanced rules first before checking the Forward to Number rules. All rules are checked in order from top to bottom.

12.3 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 58 VOICE > Phone Book > Speed Dial

Speed Dial Setup

Speed Dial: #01

Number:

Name:

Type: Use Proxy Non-Proxy (Use IP or URL)

Phone Book

#	Number	Name	Destination	Action
#01				
#02				
#03				
#04				
#05				
#06				
#07				
#08				
#09				
#10				

The following table describes the icons in this screen.

Table 48 Advanced > LAN Configuration > IP Static Route

ICON	DESCRIPTION
	Delete Click to delete this item.

The following table describes the labels in this screen.

Table 49 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 Modem 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 Modem 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.

PART V

Tools & Status Screens

The Certificates Screens (147)

The Firewall Screens (169)

Content Filter (179)

The Remote Management Screens (183)

OoS (195)

The Logs Screens (199)

The Status Screen (215)

The Certificates Screens

13.1 Overview

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

The WiMAX Modem 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.

13.1.1 What You Can Do in This Chapter

- The **My Certificates** screen ([Section 13.2 on page 148](#)) lets you generate and export self-signed certificates or certification requests and import the WiMAX Modem’s CA-signed certificates.
- The **Trusted CAs** screen ([Section 13.3 on page 158](#)) lets you display a summary list of certificates of the certification authorities that you have set the WiMAX Modem to accept as trusted.

13.1.2 What You Need to Know

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

Certificate Authorities

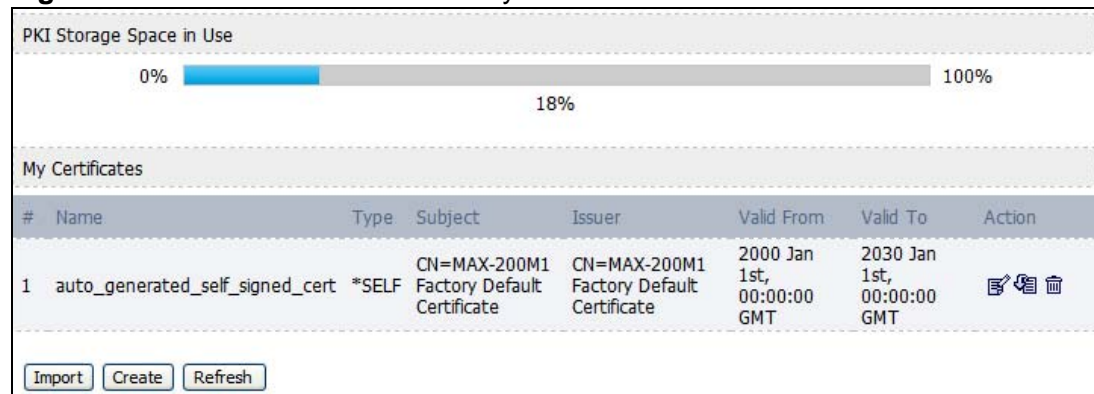
A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. You can use the

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

13.2 My Certificates

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

Figure 59 TOOLS > Certificates > My Certificates



The following table describes the icons in this screen.

Table 50 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 51 TOOLS > Certificates > My Certificates

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the WiMAX Modem'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 51 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 Modem 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 Modem's features are configured to use.</p>
Import	Click to a certificate into the WiMAX Modem.
Create	Click to go to the screen where you can have the WiMAX Modem generate a certificate or a certification request.
Refresh	Click to display the current validity status of the certificates.

13.2.1 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 Modem create a self-signed certificate, enroll a certificate with a certification authority or generate a certification request.

Figure 60 TOOLS > Certificates > My Certificates > Create

The screenshot shows a web-based form for creating certificates. It is divided into three main sections: Certificate Name, Subject Information, and Enrollment Options.

- Certificate Name:** A single text input field.
- Subject Information:** A section with a dashed border containing:
 - Common Name:** A radio button selection for 'Host IP Address' (selected), 'Host Domain Name', or 'E-Mail'. The 'Host IP Address' option has four input fields for IP octets, each containing '0'.
 - Organizational Unit:** A text input field.
 - Organization:** A text input field.
 - Country:** A text input field.
 - Key Length:** A dropdown menu set to '1024'.
- Enrollment Options:** A section with a dashed border containing:
 - Three radio button options: 'Create a self-signed certificate' (selected), 'Create a certification request and save it locally for later manual enrollment', and 'Create a certification request and enroll for a certificate immediately online'.
 - Enrollment Protocol:** A dropdown menu set to 'Simple Certificate Enrollment Protocol (SCEP)'.
 - CA Server Address:** A text input field.
 - CA Certificate:** A dropdown menu with '(See [Trusted CAs](#))' next to it.
 - Request Authentication:** A text input field.
 - Key:** A text input field.

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

The following table describes the labels in this screen.

Table 52 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 Modem 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 Modem 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 52 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 Modem 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 Modem'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 99999999.</p> <p>For the key, use up to 31 of the following characters. a-zA-Z0-9; `~!@#\$\$%^&*()_+{\}'<./>=-</p>

Table 52 TOOLS > Certificates > My Certificates > Create

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

If you configured the **My Certificate Create** screen to have the WiMAX Modem enroll a certificate and the certificate enrollment is not successful, you see a screen with a **Return** button that takes you back to the **My Certificate Create** screen. Click **Return** and check your information in the **My Certificate Create** screen. Make sure that the certification authority information is correct and that your Internet connection is working properly if you want the WiMAX Modem to enroll a certificate online.

13.2.2 My Certificate Edit

Click **TOOLS > Certificates > My Certificates** then the **Edit** icon to access this screen. Use this screen to view in-depth certificate information and change the certificate's name.

Figure 61 TOOLS > Certificates > My Certificates > Edit

The following table describes the labels in this screen.

Table 53 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.

Table 53 TOOLS > Certificates > My Certificates > Edit

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 Modem 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 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 Modem.
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 Modem 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 Modem 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 53 TOOLS > Certificates > My Certificates > Edit

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 Modem calculated using the MD5 algorithm.
SHA1 Fingerprint	This is the certificate's message digest that the WiMAX Modem 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.

13.2.3 My Certificate Import

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

Figure 62 TOOLS > Certificates > My Certificates > Import

Import

Please specify the location of the certificate file to be imported. The certificate file must be in one of the following formats.

- Binary X.509
- PEM (Base-64) encoded X.509
- Binary PKCS#7
- PEM (Base-64) encoded PKCS#7
- Binary PKCS#12
- PEM (Base-64) encoded PKCS#12

For my certificate importation to be successful, a certification request corresponding to the imported certificate must already exist on WiMAX CPE. After the importation, the certification request will automatically be deleted.

File Path:

The following table describes the labels in this screen.

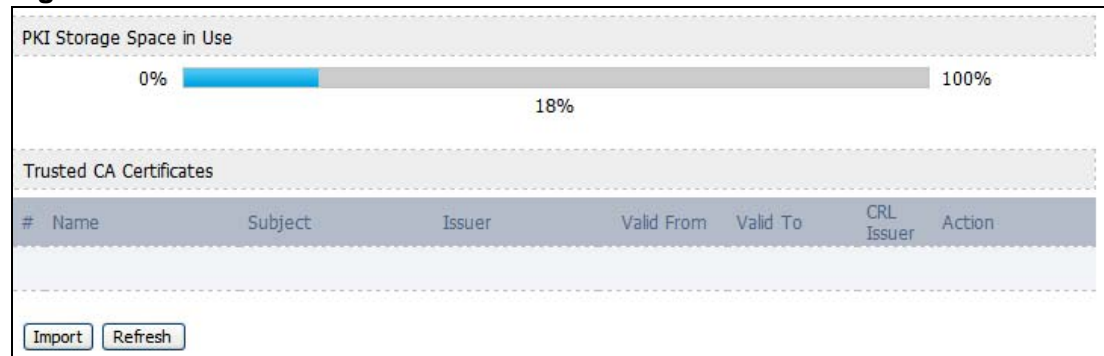
Table 54 TOOLS > Certificates > My Certificates > Import

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 Modem.
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.

13.3 Trusted CAs




Click **TOOLS > Certificates > Trusted CAs** access this screen. Use this screen to display a summary list of certificates of the certification authorities that you have set the WiMAX Modem to accept as trusted. The WiMAX Modem 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 63 TOOLS > Certificates > Trusted CAs



The following table describes the icons in this screen.

Table 55 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 56 TOOLS > Certificates > Trusted CAs

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the WiMAX Modem'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 56 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 Modem 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 Modem.
Refresh	Click this button to display the current validity status of the certificates.

13.3.1 Trusted CA Edit

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

Figure 64 TOOLS > Certificates > Trusted CAs > Edit

The following table describes the labels in this screen.

Table 57 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 57 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 Modem 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 Modem.
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 Modem 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 Modem 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 57 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 Modem calculated using the MD5 algorithm.
SHA1 Fingerprint	This is the certificate's message digest that the WiMAX Modem 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.

13.3.2 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 Modem. The WiMAX Modem 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 65 TOOLS > Certificates > Trusted CAs > Import

The following table describes the labels in this screen.

Table 58 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.

13.4 Technical Reference

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

13.4.1 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 Modem 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 Modem 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 Modem 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).

13.4.1.1 Advantages of Certificates

Certificates offer the following benefits.

- The WiMAX Modem 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.

13.4.1.2 Self-signed Certificates

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

13.4.1.3 Factory Default Certificate

The WiMAX Modem 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.

13.4.1.4 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 Modem 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.

13.4.2 Verifying a Certificate

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

13.4.2.1 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.

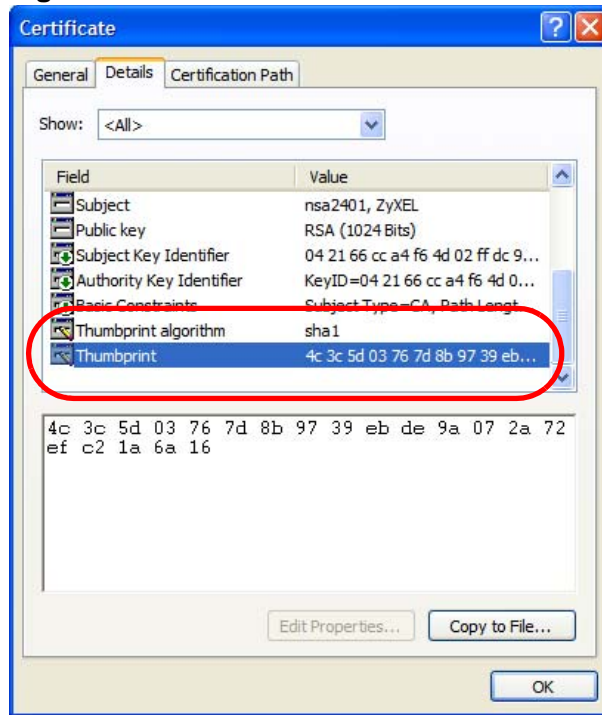
- 1 Browse to where you have the certificate saved on your computer.
- 2 Make sure that the certificate has a ".cer" or ".crt" file name extension. (On some Linux distributions, the file extension may be ".der".)

Figure 66 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 67 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.

The Firewall Screens

14.1 Overview

Use the **TOOLS > Firewall** screens to manage WiMAX Modem'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.

14.1.1 What You Can Do in This Chapter

- The **Firewall Setting** screen ([Section 14.2 on page 170](#)) lets you configure the basic settings for your firewall.
- The **Service Setting** screen ([Section 14.3 on page 173](#)) 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.

14.1.2 What You Need to Know

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

About the WiMAX Modem Firewall

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

the Internet. The WiMAX Modem 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 Modem 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.

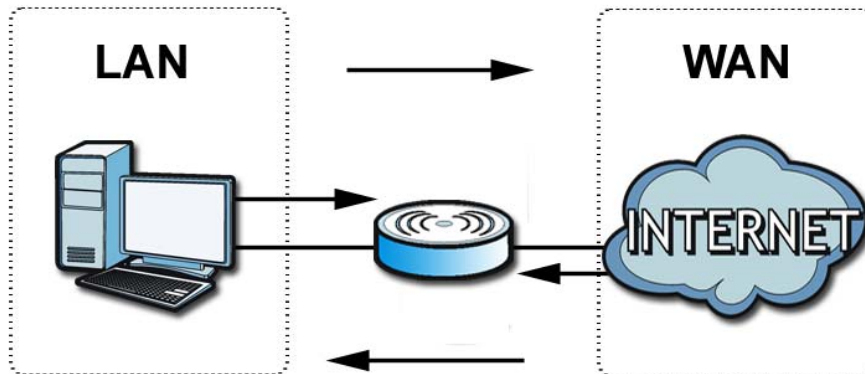
The WiMAX Modem has one Ethernet (LAN) port. The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers will have access to Internet services such as e-mail, FTP and the World Wide Web. However, “inbound access” is not allowed (by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

14.2 Firewall Setting

This section describes firewalls and the built-in WiMAX Modem’s firewall features.

14.2.1 Firewall Rule Directions

Figure 68 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 Modem means the LAN to the WiMAX Modem LAN interface. This is always allowed, as this is how you manage the WiMAX Modem 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 Modem firewall rules. WAN-to-WAN/WiMAX Modem firewall rules are Internet to the WiMAX Modem 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 Modem packets to log.

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

14.2.2 Triangle Route

When the firewall is on, your WiMAX Modem 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 Modem to protect your LAN against attacks.

Figure 69 Ideal Firewall Setup



14.2.3 Firewall Setting Options

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

Figure 70 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 59 TOOLS > Firewall > Firewall Setting

LABEL	DESCRIPTION
Enable Firewall	Select this to activate the firewall. The WiMAX Modem 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 Modem.
Max NAT/ Firewall Session Per User	Select the maximum number of NAT rules and firewall rules the WiMAX Modem enforces at one time. The WiMAX Modem 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 ADVANCED > NAT Configuration > General .
Packet Direction	
Log	Select the situations in which you want to create log entries for firewall events. 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.

14.3 Services

Click **TOOLS > Firewall > Services** 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 71 TOOLS > Firewall > Service Setting

The following table describes the labels in this screen.

Table 60 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 60 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.

14.4 Technical Reference

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

14.4.1 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.

14.4.2 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.

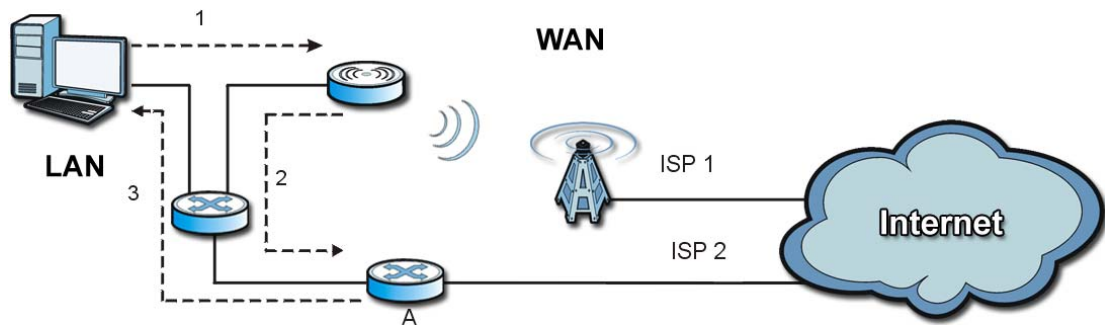
14.4.3 The “Triangle Route” Problem

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 Modem'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 Modem 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 Modem.

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

Figure 72 “Triangle Route” Problem



14.4.3.1 Solving the “Triangle Route” Problem

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

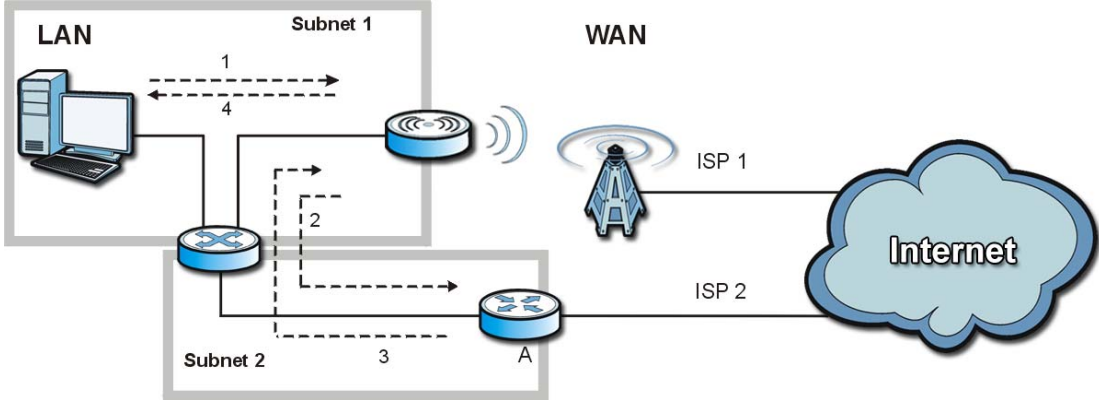
Another solution is to use IP alias. IP alias allows you to partition your network into logical sections over the same Ethernet interface. Your WiMAX Modem supports up to three logical LAN interfaces with the WiMAX Modem being the gateway for each logical network.

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 Modem 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 Modem reroutes the packet to Gateway A, which is in Subnet 2.
- 3 The reply from the WAN goes to the WiMAX Modem.

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

Figure 73 IP Alias



Content Filter

15.1 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 Modem can block web features such as ActiveX controls, Java applets, cookies and disable web proxies. The WiMAX Modem also allows you to define time periods and days during which the WiMAX Modem performs content filtering.

15.1.1 What You Can Do in This Chapter

- The **Filter** screen ([Section 15.2 on page 180](#)) 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 15.3 on page 182](#)) lets you schedule content filtering.

15.2 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 74 TOOLS > Content Filter > Filter

Trusted IP Setup

A trusted computer has full access to all blocked resources. 0.0.0.0 means there is no trusted computer.

Trusted Computer IP Address:

Restrict Web Features

ActiveX Java Cookies Web Proxy

Keyword Blocking

Enable URL Keyword Blocking

Keyword:

Keyword List:

spam
wankle%20rotary%20engine

Message to display when a site is blocked

Denied Access Message:

The following table describes the labels in this screen.

Table 61 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 Modem 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 128 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 128 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 Modem's content filter feature blocks access to a web site.
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

15.3 Schedule

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

Figure 75 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)

Apply Reset

The following table describes the labels in this screen.

Table 62 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

16.1 Overview

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

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

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

Table 63 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 Modem 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.

- 1 Telnet
- 2 HTTP

16.1.1 What You Can Do in This Chapter

- The **WWW** screen ([Section 16.2 on page 185](#)) lets you control HTTP access to your WiMAX Modem.
- The **Telnet** screen ([Section 16.3 on page 186](#)) lets you control Telnet access to your WiMAX Modem.
- The **FTP** screen ([Section 16.4 on page 186](#)) lets you control FTP access to your WiMAX Modem.

- The **SNMP** screen (Section 16.5 on page 187) lets you control SNMP access to your WiMAX Modem.
- The **DNS** screen (Section 16.6 on page 190) lets you control DNS access to your WiMAX Modem.
- The **Security** screen (Section 16.7 on page 191) lets you control how your WiMAX Modem responds to other types of requests.
- The **TR069** screen (Section 16.8 on page 192) lets you configure the WiMAX Modem's auto-configuration and dynamic service configuration options.

16.1.2 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 Modem 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 Modem's WAN IP address when configuring from the WAN.
- Use the WiMAX Modem'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 Modem 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 Modem supports SNMP agent functionality, which allows a manager station to manage and monitor the WiMAX Modem through the network. The WiMAX Modem 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.

16.2 WWW

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

Figure 76 TOOLS > Remote Management > WWW

The screenshot shows a configuration window for WWW access. It contains three main sections: 'Server Port' with a text box containing '80'; 'Server Access' with a dropdown menu showing 'LAN & WAN'; and 'Secured Client IP Address' with two radio buttons, 'All' (which is selected) and 'Selected', followed by a text box containing '0.0.0.0'. At the bottom of the window are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

Table 64 TOOLS > Remote Management > WWW

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

16.3 Telnet

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

Figure 77 TOOLS > Remote Management > Telnet

The screenshot shows a configuration form for Telnet access. It includes three main sections: 'Server Port' with a text input containing '23'; 'Server Access' with a dropdown menu set to 'LAN & WAN'; and 'Secured Client IP Address' with two radio buttons, 'All' (which is selected) and 'Selected', followed by a text input containing '0.0.0.0'. At the bottom right, there are two buttons labeled 'Apply' and 'Reset'.

The following table describes the labels in this screen.

Table 65 TOOLS > Remote Management > Telnet

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

16.4 FTP

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

Figure 78 TOOLS > Remote Management > FTP

The screenshot shows a configuration form for FTP access. It includes three main sections: 'Server Port' with a text input containing '21'; 'Server Access' with a dropdown menu set to 'LAN & WAN'; and 'Secured Client IP Address' with two radio buttons, 'All' (which is selected) and 'Selected', followed by a text input containing '0.0.0.0'. At the bottom right, there are two buttons labeled 'Apply' and 'Reset'.

The following table describes the labels in this screen.

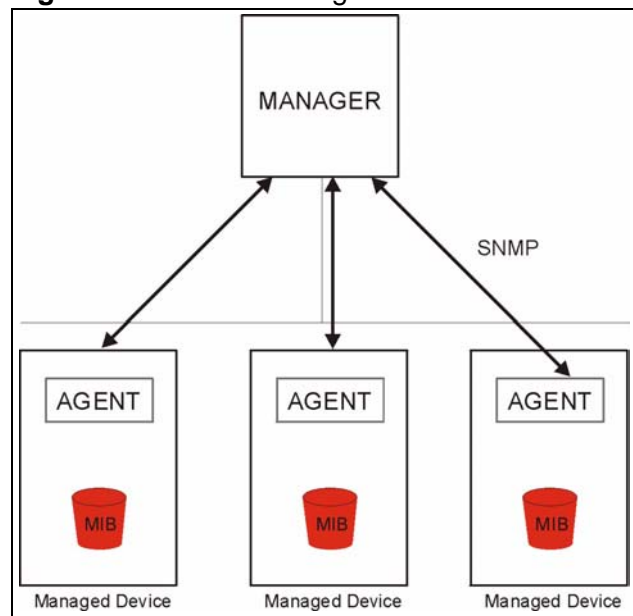
Table 66 TOOLS > Remote Management > FTP

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

16.5 SNMP

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

Figure 79 SNMP Management Model



An agent is a management software module that resides in a managed device (the WiMAX Modem). 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 Modem 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.

16.5.1 SNMP Traps

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

Table 67 SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
0	coldStart (defined in <i>RFC-1215</i>)	A trap is sent after booting (power on).
1	warmStart (defined in <i>RFC-1215</i>)	A trap is sent after booting (software reboot).
4	authenticationFailure (defined in <i>RFC-1215</i>)	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, C1 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.

16.5.2 SNMP Options

Click **TOOLS > Remote Management > SNMP** to access this screen. Use SNMP options to control SNMP access to your WiMAX Modem.

Figure 80 TOOLS > Remote Management > SNMP

SNMP Configuration	
Get Community:	<input type="text" value="public"/>
Set Community:	<input type="text" value="public"/>
Trap Community:	<input type="text" value="public"/>
Trap Destination:	<input type="text" value="0.0.0.0"/>
SNMP	
Server Port:	<input type="text" value="161"/>
Server Access:	<input type="button" value="LAN & WAN"/>
Secured Client IP Address:	<input checked="" type="radio"/> All <input type="radio"/> Selected <input type="text" value="0.0.0.0"/>
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

The following table describes the labels in this screen.

Table 68 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 Modem using this service.

Table 68 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 Modem using this service. Select All to allow any computer to access the WiMAX Modem using this service. Choose Selected to just allow the computer with the IP address that you specify to access the WiMAX Modem using this service.
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

16.6 DNS

Click **TOOLS > Remote Management > DNS** to access this screen. Use this screen to control DNS access to your WiMAX Modem.

Figure 81 TOOLS > Remote Management > DNS

The following table describes the labels in this screen.

Table 69 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 Modem. The computer must use the same port number.
Server Access	Select the interface(s) through which a computer may access the WiMAX Modem using this service.
Secured Client IP Address	Select All to allow any computer to access the WiMAX Modem using this service. Select Selected to only allow the computer with the IP address that you specify to access the WiMAX Modem using this service.
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

16.7 Security

Click **TOOLS > Remote Management > Security** to access this screen. Use this screen to control how your WiMAX Modem responds to other types of requests.

Figure 82 TOOLS > Remote Management > Security

Respond to Ping on: LAN & WAN

Do not respond to requests for unauthorized services

Apply Reset

The following table describes the labels in this screen.

Table 70 TOOLS > Remote Management > Security

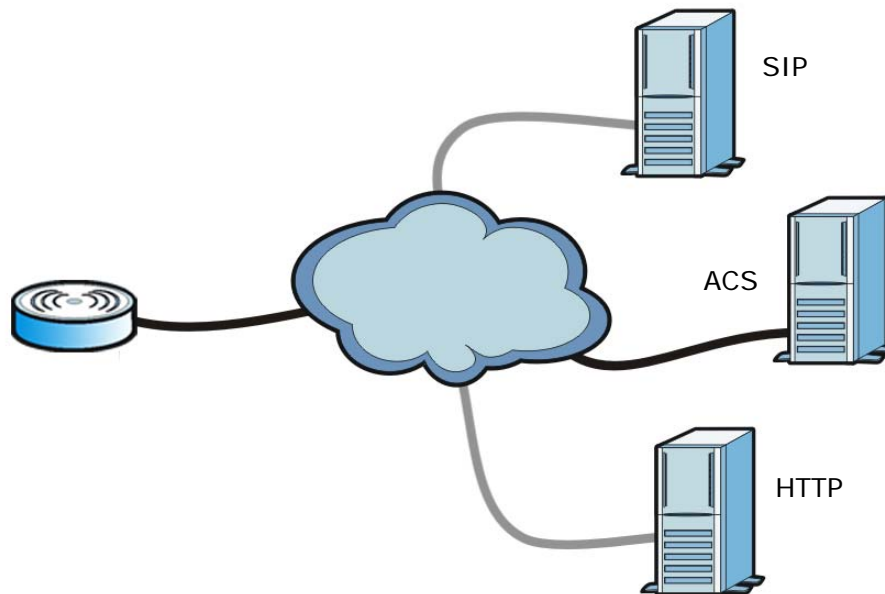
LABEL	DESCRIPTION
Respond to Ping on	<p>Select the interface(s) on which the WiMAX Modem should respond to incoming ping requests.</p> <ul style="list-style-type: none"> • Disable - the WiMAX Modem does not respond to any ping requests. • LAN - the WiMAX Modem only responds to ping requests received from the LAN. • WAN - the WiMAX Modem only responds to ping requests received from the WAN. • LAN & WAN - the WiMAX Modem 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 Modem by sending requests to unsupported port numbers. If an outside user attempts to probe an unsupported port on your WiMAX Modem, an ICMP response packet is automatically returned. This allows the outside user to know the WiMAX Modem exists. Your WiMAX Modem supports anti-probing, which prevents the ICMP response packet from being sent. This keeps outsiders from discovering your WiMAX Modem when unsupported ports are probed.</p> <p>If you clear this, your WiMAX Modem 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.

16.8 TR0-69

TR-069 is an abbreviation of “Technical Reference 069”, a protocol designed to facilitate the remote management of Customer Premise Equipment (CPE), such as the WiMAX Modem. It can be managed over a WAN by means of an Auto Configuration Server (ACS). TR-069 is based on sending Remote Procedure Calls (RPCs) between the ACS and the client device. RPCs are sent in Extensible Markup Language (XML) format over HTTP or HTTPS.

An administrator can use an ACS to remotely set up the WiMAX Modem, modify its settings, perform firmware upgrades, and monitor and diagnose it. In order to do so, you must enable the TR-069 feature on your WiMAX Modem and then configure it appropriately. (The ACS server which it will use must also be configured by its administrator.)

Figure 83 TR-069 Example



In this example, the WiMAX Modem receives data from at least 3 sources: A SIP server for handling voice calls, an HTTP server for handling web services, and an ACS, for configuring the WiMAX Modem remotely. All three servers are owned and operated by the client’s Internet Service Provider. However, without the configuration settings from the ACS, the WiMAX Modem cannot access the other two servers. Once the WiMAX Modem receives its configuration settings and implements them, it can connect to the other servers. If the settings change, it will once again be unable to connect until it receives its updates from the ACS.

The WiMAX Modem can be configured to periodically check for updates from the auto-configuration server so that the end user need not be worried about it.

Click **TOOLS > Remote Management > TR069** to access this screen. Use this screen to open WiMAX Modem's auto-configuration and dynamic service configuration options.

Figure 84 TOOLS > Remote Management > TR069

<input type="checkbox"/> Active	
ACS URL:	<input type="text" value="http://172.89.76.1"/>
User Name:	<input type="text" value="alcsprn1045"/>
Password:	<input type="text" value="180945767fa102395601"/>
Connection Request User Name:	<input type="text" value="uio14601"/>
Connection Request Password:	<input type="text" value="ZxER87qqM0arUNubZ"/>
<input type="checkbox"/> Periodic Inform Enable	
Periodic Inform Interval:	<input type="text" value="86400"/> sec (Range: 30 ~ 2147483647)
Periodic Inform Time(yyyy-mm-ddThh:mm:ss):	<input type="text" value="2012-01-01T03:30:00"/>
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

The following table describes the labels in this screen.

Table 71 TOOLS > Remote Management > TR069

LABEL	DESCRIPTION
Active	Select this option to turn on the WiMAX Modem's TR-069 feature. Note: If this feature is not enabled then the WiMAX Modem cannot be managed remotely.
ACS URL	Enter the URL or IP address of the auto-configuration server.
User Name	Enter the user name sent when the WiMAX Modem connects to the ACS and which is used for authentication. You can enter up to 31 alphanumeric characters (a-z, A-Z, 0-9) and underscores but spaces are not allowed.
Password	Enter the password sent when the WiMAX Modem connects to an ACS and which is used for authentication. You can enter up to 31 alphanumeric characters (a-z, A-Z, 0-9) and underscores but spaces are not allowed.
Connection Request User Name	Enter the connection request user name that the ACS must send to the WiMAX Modem when it requests a connection. You can enter up to 31 alphanumeric characters (a-z, A-Z, 0-9) and underscores but spaces are not allowed. Note: This must be provided by the ACS administrator.
Connection Request Password	Enter the connection request password that the ACS must send to the WiMAX Modem when it requests a connection. You can enter up to 31 alphanumeric characters (a-z, A-Z, 0-9) and underscores but spaces are not allowed. Note: This must be provided by the ACS administrator.

Table 71 TOOLS > Remote Management > TR069

LABEL	DESCRIPTION
Periodic Inform Enable	<p>Select this to allow the WiMAX Modem to periodically connect to the ACS and check for configuration updates.</p> <p>If you do not enable this feature then the WiMAX Modem can only be updated automatically when the ACS initiates contact with it and if you selected the Active checkbox on this screen.</p>
Periodic Inform Interval	<p>Enter the time interval (in seconds) at which the WiMAX Modem connects to the auto-configuration server.</p>
Periodic Inform Time	<p>Enter a time interval that the WiMAX Modem will trigger a periodic inform interval. This works in tandem with the Periodic Inform Interval and is not mutually exclusive of it.</p> <p>The Periodic Inform Time must be in the following format: yyyy-mm-ddThh:mm:ss where yyyy is a four digit year ("2009"), mm is a two digit month (01~12), dd is a two digit day (01~28), hh is a two-digit hour in 24-hour format (01~24), mm is a two digit minutes value (01-60) and ss is a two digit seconds value (01-60).</p> <p>Note: You must separate the day information from the hour information with a "T".</p> <p>This feature gives the WiMAX Modem a baseline from which to begin calculating when each periodic inform happens.</p> <p>If the inform time is set for some point in the past, the WiMAX Modem interpolates the inform interval forward to the current time and begins its periodic inform at the appropriate time based on this interpolation.</p> <p>If the inform time is set for some point in the future, then the WiMAX Modem interpolates backwards to the current time and actually begins at the appropriate time based on this interpolation.</p>
Apply	<p>Click to save your changes.</p>
Reset	<p>Click to restore your previously saved settings.</p>

17.1 Overview

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical application such as video-on-demand.

17.2 General

Click **TOOLS > QoS** to open the screen as shown next. Use this screen to enable or disable QoS.

Figure 85 QoS > General

The following table describes the labels in this screen.

Table 72 TOOLS > Remote Management > Security

LABEL	DESCRIPTION
Active QoS	Select this to enable QoS for the WiMAX Modem. Selecting this may improve network performance, especially if you are using VoIP applications or are playing online video games.
Apply	Click to save your changes.
Reset	Click to restore your previously saved settings.

17.3 Class Setup

Use this screen to add, edit or delete QoS classifiers. A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming interface. For example, you can configure a classifier to select traffic from the same protocol port (such as Telnet) to form a flow.

You can give different priorities to traffic that the WiMAX Modem forwards out through the WAN interface. Give high priority to voice and video to make them run more smoothly. Similarly, give low priority to many large file downloads so that they do not reduce the quality of other applications.

Click **TOOLS > QoS > Class Setup** to open the following screen.

Figure 86 QoS > Class Setup

Create New Class						
#	Active	Name	Interface	DSCP	Class Index	Action
1		Default Class	From LAN	0	99	
2		Default Class	From WAN	0	99	

The following table describes the labels in this screen.

Table 73 QoS Class Setup

LABEL	DESCRIPTION
Create New Class	Click this button to create a new class.
#	This field displays the index number of the class.
Active	This field indicates whether the QoS class is enabled or not.
Name	This field indicates the name of the class.
Interface	This field indicates the Ethernet port on which traffic is being monitored and prioritized.
DSCP	This field indicates the Differentiated Services Code Point (DSCP) value for the associated class.
Class Index	This field indicates the index for this QoS class. Classes are implemented based on index number, from lowest to highest.
Action	Click the Edit icon to go to the screen where you can edit the rule. Click the Delete icon to delete an existing rule. Note that subsequent rules move up by one when you take this action.
Apply	Click this button to save your changes back to the WiMAX Modem.
Cancel	Click this button to begin configuring this screen afresh.

17.3.1 Class Configuration

Click the **Create New Class** button or the edit icon in the **Class Setup** screen to configure a classifier.

Figure 87 QoS > Class Setup > Class Configuration

The following table describes the labels in this screen.

Table 74 QoS Class Setup

LABEL	DESCRIPTION
Class Configuration	
Active	Select this to make a class active.
Index	Enter an index number for the class. Similar classes are processed in order of index number, from lowest to highest.
Name	Enter a descriptive name of up to 20 printable English keyboard characters, including spaces.
Interface	Select an interface to which the class will apply: <ul style="list-style-type: none"> From WAN - The class is applied to all packets incoming from the WAN (Wide Area Network). From LAN - The class is applied to all packets outgoing from the LAN (Local Area Network).
DSCP	Enter a DSCP value with which the WiMAX Modem replaces the DSCP field in the packets.
Filter Configuration	

Table 74 QoS Class Setup (continued)

LABEL	DESCRIPTION
Source / Destination	
Address	Enter the source IP address in dotted decimal notation.
Subnet Mask	Enter the source subnet mask.
Port Range	Enter the beginning and ending port numbers. You can use the same number in both fields to indicate a single port, or you can enter 0 in both fields to indicate all ports.
Exclude	Select this to use the class to exclude packets based on these settings.
Others	
Service	Select a pre-configured service for this class. Options are: SIP, FTP and H.323 . This loads pre-configured values specifically for these service types.
Protocol	Select a protocol. Options are: TCP, UDP and User Defined .
Exclude	Select this to use the class to exclude packets based on these settings.
Apply	Click this button to save your changes back to the WiMAX Modem.
Cancel	Click this button to begin configuring this screen afresh.

The Logs Screens

18.1 Overview

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

For a list of log messages, see [Section 18.4 on page 205](#).

18.1.1 What You Can Do in This Chapter

- The **View Logs** screen ([Section 18.2 on page 201](#)) lets you look at log entries and alerts.
- The **Log Settings** screen ([Section 18.3 on page 203](#)) lets you configure where the WiMAX Modem sends logs and alerts, the schedule for sending logs, and which logs and alerts are sent or recorded.

18.1.2 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 75 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 76 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