# *MAX-206M2*

*WiMAX MIMO Indoor CPE (2.5 GHz)*

# *User's Guide*

Firmware Version 1.0
Edition 1, 08/2008

| DEFAULT LOGIN | |
|---|---|
| **IP Address** | **http://192.168.100.1** |
| **User Name** | **admin** |
| **Password** | **1234** |

ZyXEL

www.zyxel.com

# About This User's Guide

## 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.

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.

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

### Syntax Conventions

- The MAX-206M2 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

| | | |
|---|---|---|
| WiMAX Device  | WiMAX Access Point  | Computer  |
| Notebook  | Server  | WiMAX Base Station  |
| Telephone  | Switch  | Router  |
| Internet Cloud   | Internet/WiMAX Cloud  | Wireless Signal  |

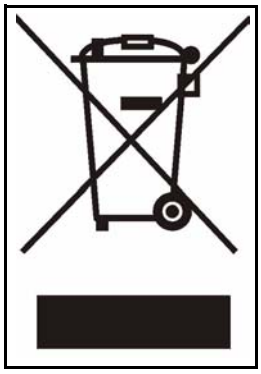
# Safety Warnings

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

# Table of Contents

# List of Figures

# List of Tables

# PART I
# Introduction and Wizards

# 1

# Getting Started

## 1.1 About Your WiMAX Modem

The WiMAX Modem has a built-in switch and two phone ports. 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 22 on page 223 for a complete list of features for your model.

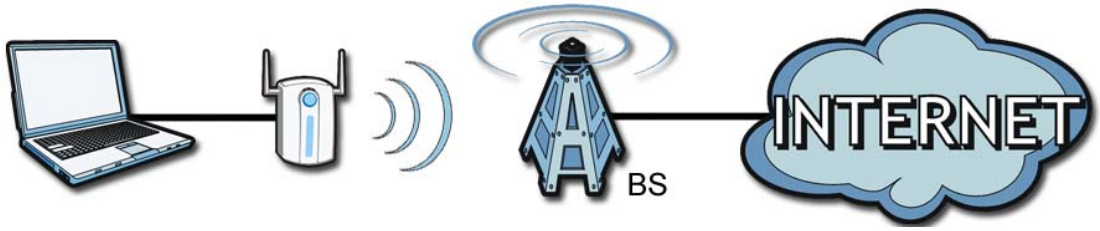
### 1.1.1 WiMAX Internet Access

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

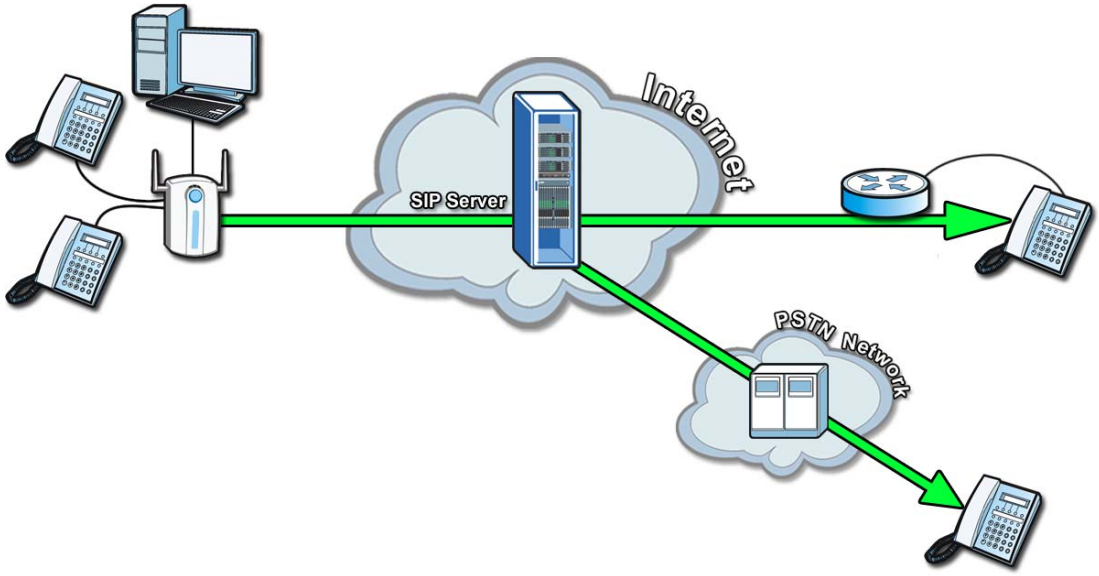
In a home or small office environment, you can use the WiMAX Modem to make and receive the following types of VoIP telephone calls:

- 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



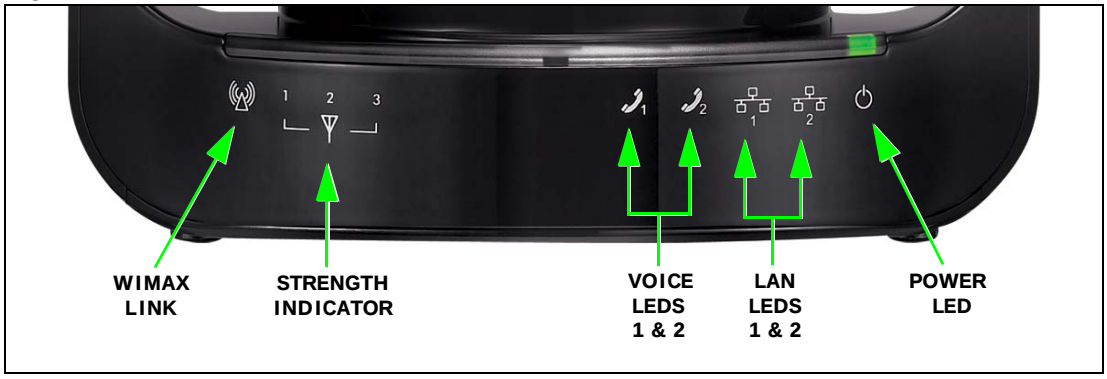
# 1.2 WiMAX Modem Hardware

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. |
| 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). |

**Table 2** The WiMAX Modem

| LED | STATE | DESCRIPTION |
|---|---|---|
| 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. | |
| | No Signal LEDS | There is no wireless connection. |
| | Signal 1 On | The signal strength is less than or equal to -70 dBm |
| | Signal 2 On | The signal strength is less than or equal to -50 dBm |
| | Signal 3 On | The signal strength is less than or equal to -30 dBm |

## 1.3 Good Habits for Managing the WiMAX Modem

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.

# 2

# 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 259 for more information on configuring your web browser.

### 2.1.1 Accessing the Web Configurator

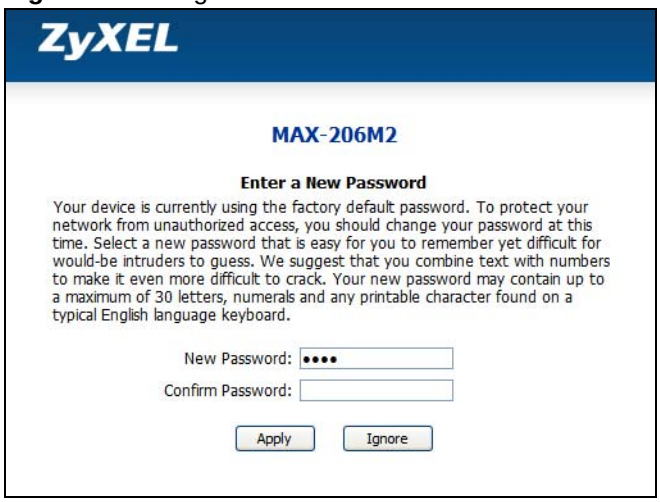
1. Make sure your WiMAX Modem hardware is properly connected (refer to the Quick Start Guide for more information).
2. Launch your web browser.
3. Enter "192.168.100.1" as the URL.

4 A password screen displays. The default password (“1234”) displays in non-readable characters. If you haven’t changed the password yet, you can just click **Login**. Click **Cancel** to revert to the default password in the password field. If you have changed the password, enter your password and click **Login**.

**Figure 5** Password Screen

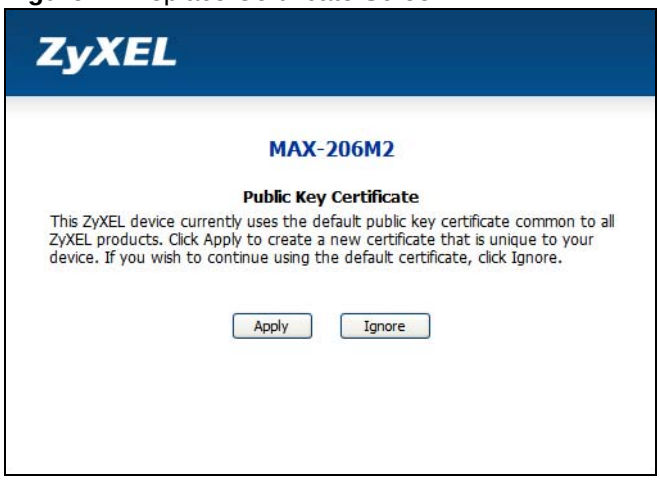

5 The following screen displays if you have not yet changed your password. It is highly recommended you change the default password. Enter a new password, retype it to confirm and click **Apply**; alternatively click **Ignore** to proceed to the main menu if you do not want to change the password now.

**Figure 6** Change Password Screen



6 Click **Apply** in the next screen to create a certificate using your 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.

**Figure 7** Replace Certificate Screen




7 A screen displays to let you choose whether to go to the wizard or the advanced screens.

- Click **Go to Wizard setup** if you are logging in for the first time or if you want to make basic changes. The wizard selection screen appears after you click **Apply**. See Chapter 3 on page 41 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 38 for more information.
- Click **Exit** if you want to log out.

**Figure 8** Wizard or Advanced Screen


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

### 2.1.2 The Reset Button

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

#### 2.1.2.1 Using The Reset Button

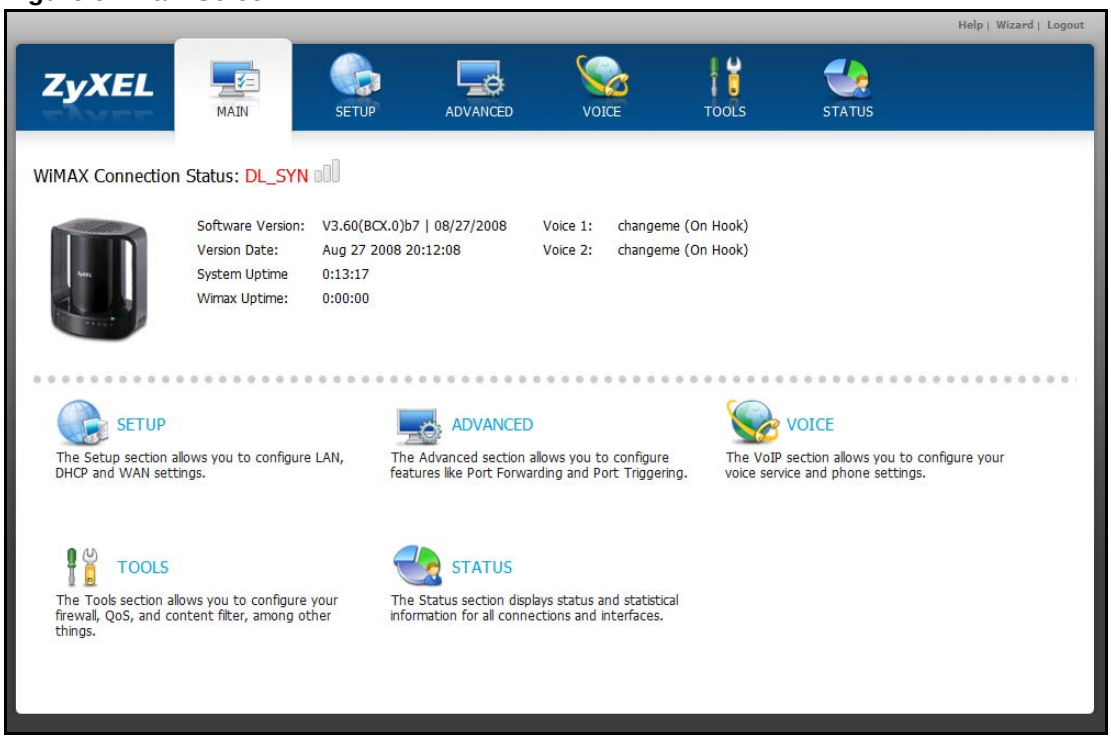
1. Make sure the **Power** light is on (not blinking).
2. To set the device back to the factory default settings, press the **Reset** button for ten seconds or until the **Power** light begins to blink and then release it. When the **Power** light begins to blink, the defaults have been restored and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

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

**Figure 9** Main Screen



The following table describes the icons in this screen.

**Table 3** Main > Icons

| ICON | DESCRIPTION |
|---|---|
|  | **MAIN**<br>Click to return to the Main screen. |
|  | **SETUP**<br>Click to go the Setup screen, where you can configure LAN, DHCP and WAN settings. |
|  | **ADVANCED**<br>Click to go to the Advanced screen, where you can configure features like Port Forwarding and Triggering, SNTP and so on. |
|  | **VOICE**<br>Click to go to the Voice screen, where you can configure your voice service and phone settings. |
|  | **TOOLS**<br>Click to go the Tools screen, where you can configure your firewall, QoS, and content filter, among other things. |
|  | **STATUS**<br>Click to go to the Status screen, where you can view status and statistical information for all connections and interfaces. |
|  | **Strength Indicator**<br>Displays a visual representation of the quality of your WiMAX connection.<br>• **Disconnected** - Zero bars<br>• **Poor** reception - One bar<br>• **Good** reception - Two bars<br>• **Excellent** reception - Three bars |

The following table describes the labels in this screen.

**Table 4** Main

| LABEL | DESCRIPTION |
|---|---|
| Help | Click to open the web configurator's online help. |
| Wizard | Click to run the Internet Connection and VoIP Connection Setup Wizard. All of the settings that you can configure in this wizard are also available in these web configurator screens. |
| Logout | Click to log out of the web configurator.<br><br>Note: This does not log you off the WiMAX network, it simply logs you out of the WiMAX Modem's browser-based configuration interface. |

**Table 4** Main (continued)

| LABEL | DESCRIPTION |
|---|---|
| WiMAX Connection Status | This field indicates the current status of your WiMAX connection.<br>Status messages are as follows:<br>• **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.<br>• **Disconnected** - Indicates that the WiMAX Modem is not connected to the WiMAX network.<br>• **DL_SYN** - Indicates a download synchronization is in progress. This means the firmware is checking with the server for any updates or settings alterations. |
| Software Version | This field indicates the version number of the WiMAX Modem's firmware. The version number takes the form of: *Version(Build),release status (candidate)* \| *Version Release Date*.<br>For example: V3.60(BCC.0)c4 \| 07/08/2008 indicates that the firmware is 3.60, build BCC.0, candidate4, released on July 08, 2008. |
| Version Date | This field indicates the exact date and time the current firmware was compiled. |
| System Uptime | This field indicates how long the WiMAX 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. |

# 3

# Internet Connection Wizard

## 3.1 Overview

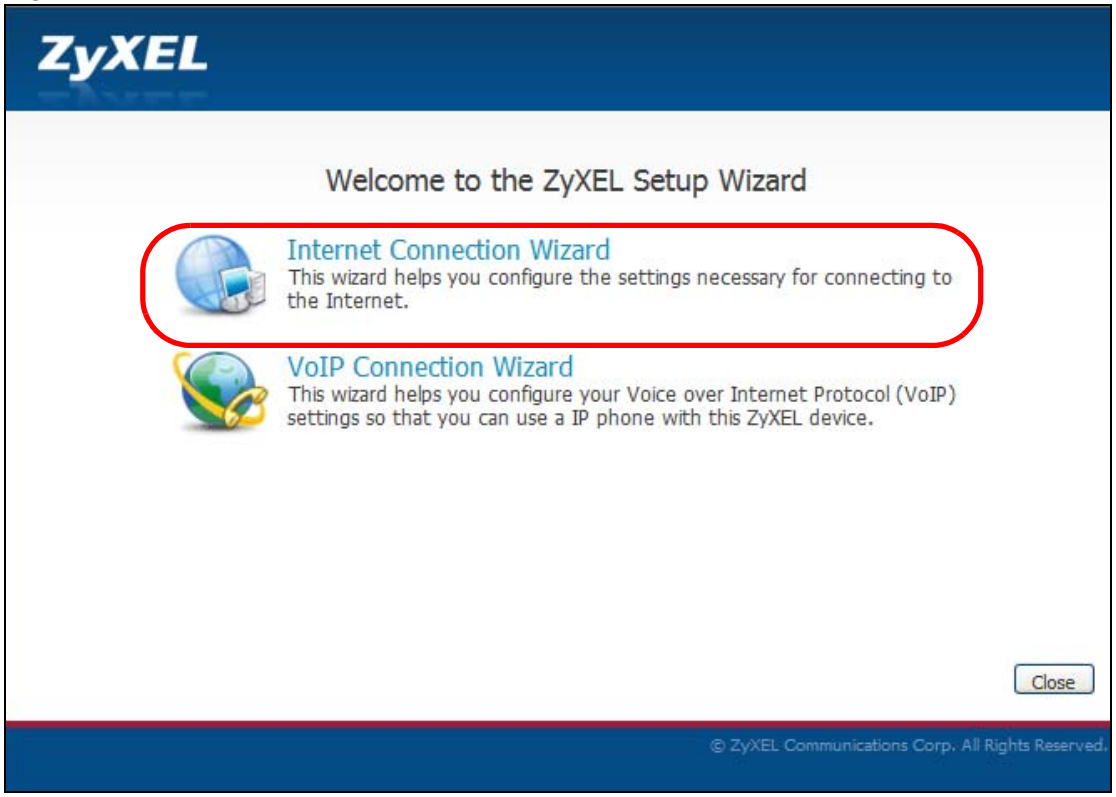
This chapter provides information on the ZyXEL Setup Wizard screens. The wizard guides you through several steps where you can configure your Internet and VoIP settings.

### 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.

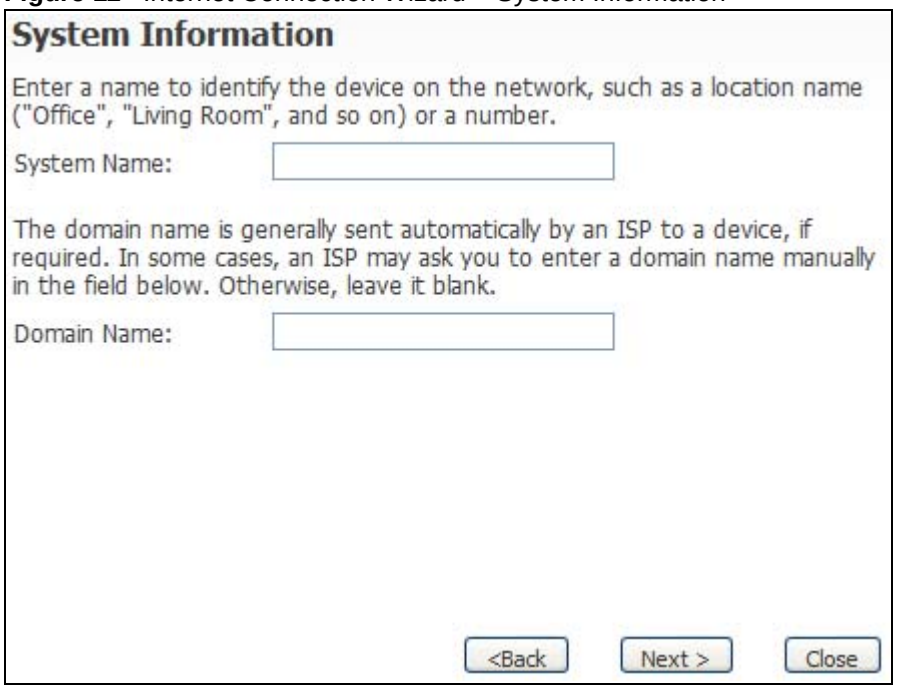
**Figure 10** Select a Mode



## 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 10.2 on page 102 for more).

**Figure 11** Internet Connection Wizard > System Information




The following table describes the labels in this screen.

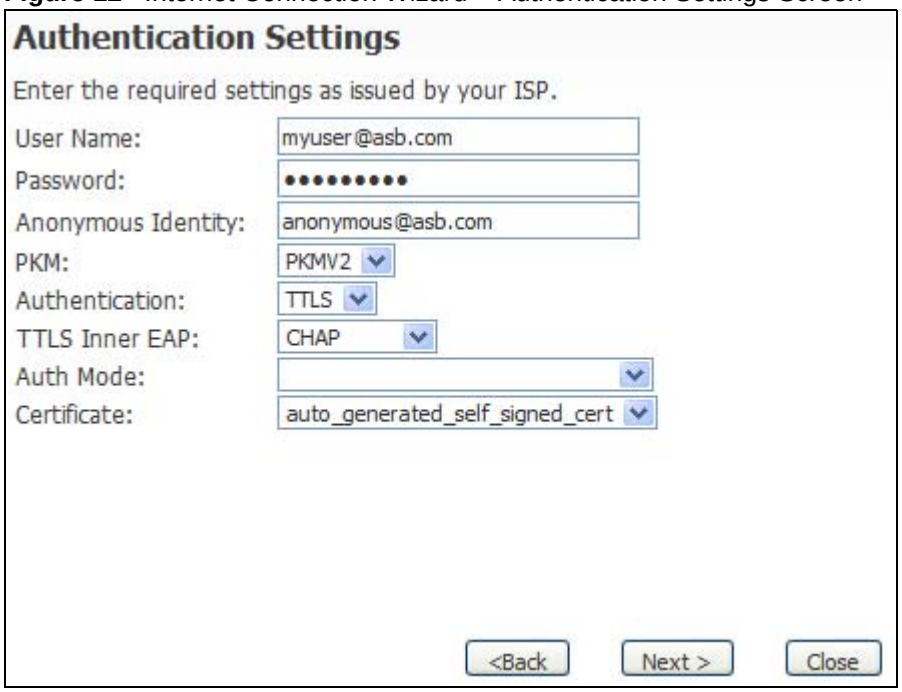
**Table 5** Internet Connection Wizard > System Information

| 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 74 for more).

**Figure 12** Internet Connection Wizard > Authentication Settings Screen




The following table describes the labels in this screen.

**Table 6** Internet Connection Wizard > Authentication Settings Screen

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

**Table 6** Internet Connection Wizard > Authentication Settings Screen (continued)

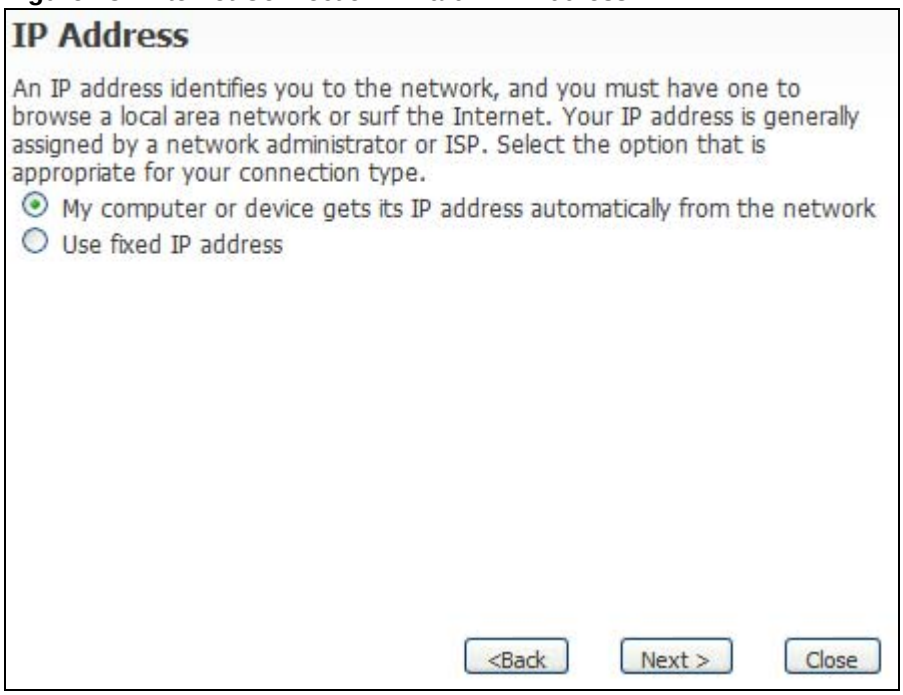
| LABEL | DESCRIPTION |
|---|---|
| Authentication | This field displays the user authentication method. Authentication is the process of confirming the identity of a mobile station (by means of a username and password, for example).<br>Check with your service provider if you are unsure of the correct setting for your account.<br>Choose from the following user authentication methods:<br>• **TTLS** (Tunnelled Transport Layer Security)<br>• **TLS** (Transport Layer Security)<br>Note: Not all WiMAX Modems support TLS authentication. Check with your service provider for details. |
| TTLS Inner EAP | This field displays the type of secondary authentication method. Once a secure EAP-TTLS connection is established, the inner EAP is the protocol used to exchange security information between the mobile station, the base station and the AAA server to authenticate the mobile station. See the WiMAX security appendix for more details. The WiMAX Modem supports the following inner authentication types:<br>• **CHAP** (Challenge Handshake Authentication Protocol)<br>• **MSCHAP** (Microsoft CHAP)<br>• **MSCHAPV2** (Microsoft CHAP version 2)<br>• **PAP** (Password Authentication Protocol) |
| Auth Mode | Select the authentication mode from the drop-down list box.<br>This field is not available in all WiMAX Modems. Check with your service provider for details.<br>The WiMAX Modem supports the following authentication modes:<br>• User Only<br>• Device Only with Cert<br>• Certs and User Authentication |
| 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 54).

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 13** Internet Connection Wizard > IP Address




The following table describes the labels in this screen.

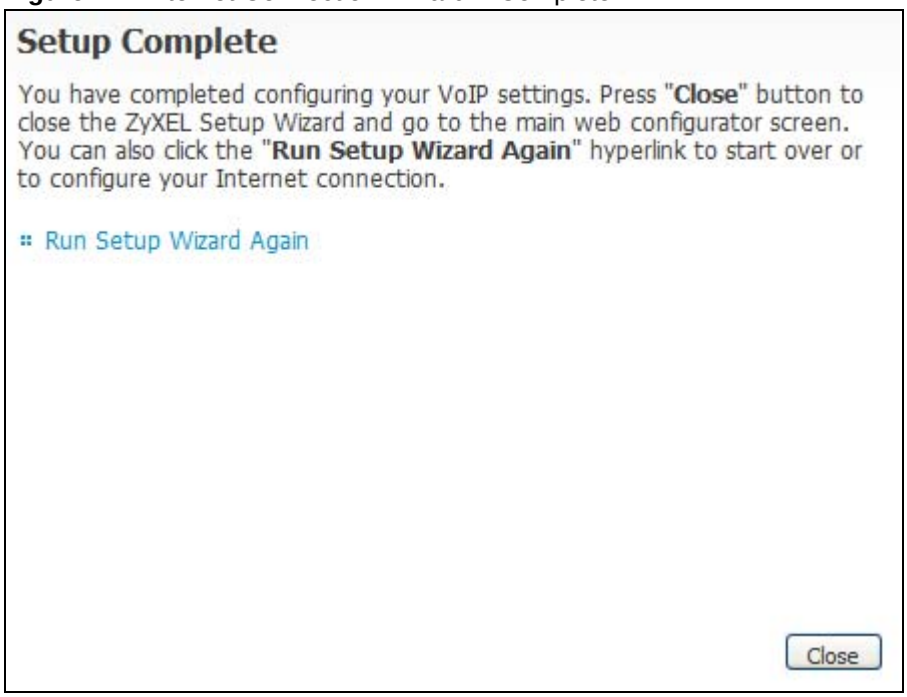
**Table 7** Internet Connection Wizard > IP Address

| LABEL | DESCRIPTION |
|---|---|
| IP Address | |
| My computer 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 14** Internet Connection Wizard > Complete




Launch your web browser and navigate to www.zyxel.com. If 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.

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.

# 4

# VoIP Connection Wizard

## 4.1 Overview

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

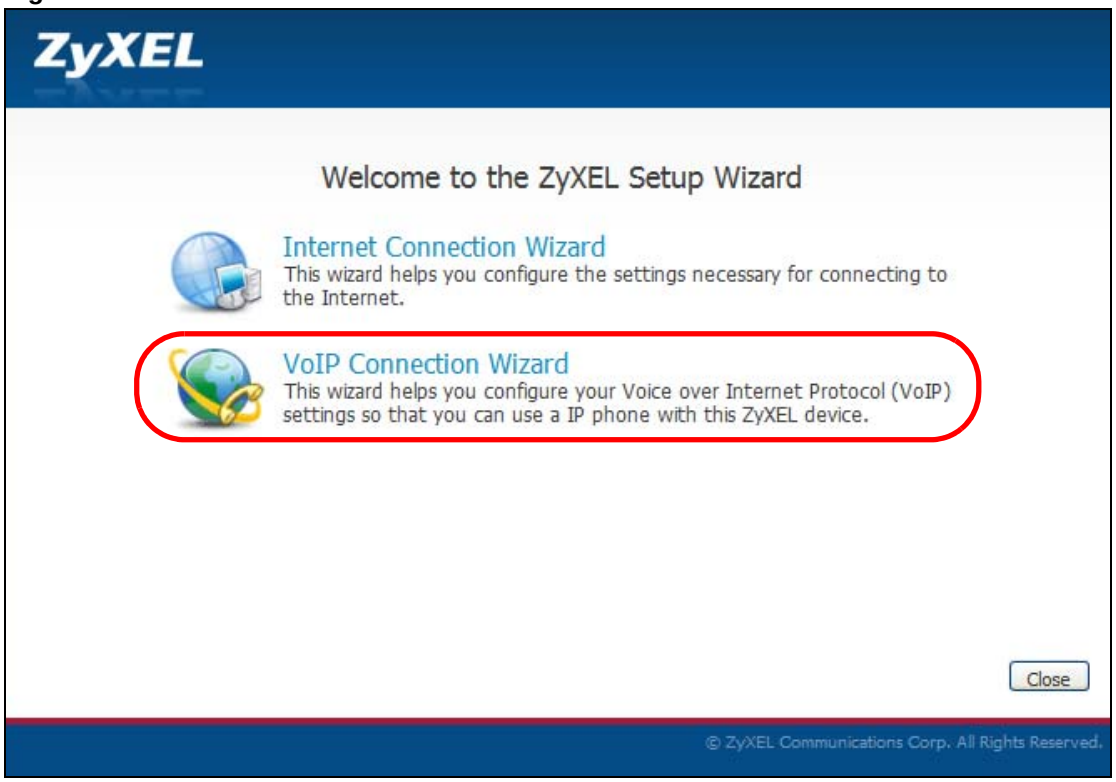
The WiMAX Modem has Voice over IP (VoIP) communication capabilities that allow you to use a traditional analog telephone to make Internet calls. You can configure the WiMAX Modem to use up to two SIP based VoIP accounts.

## 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 15** 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 11.2 on page 113 for more information).

**Figure 16** VoIP Connection > First Voice Account Settings

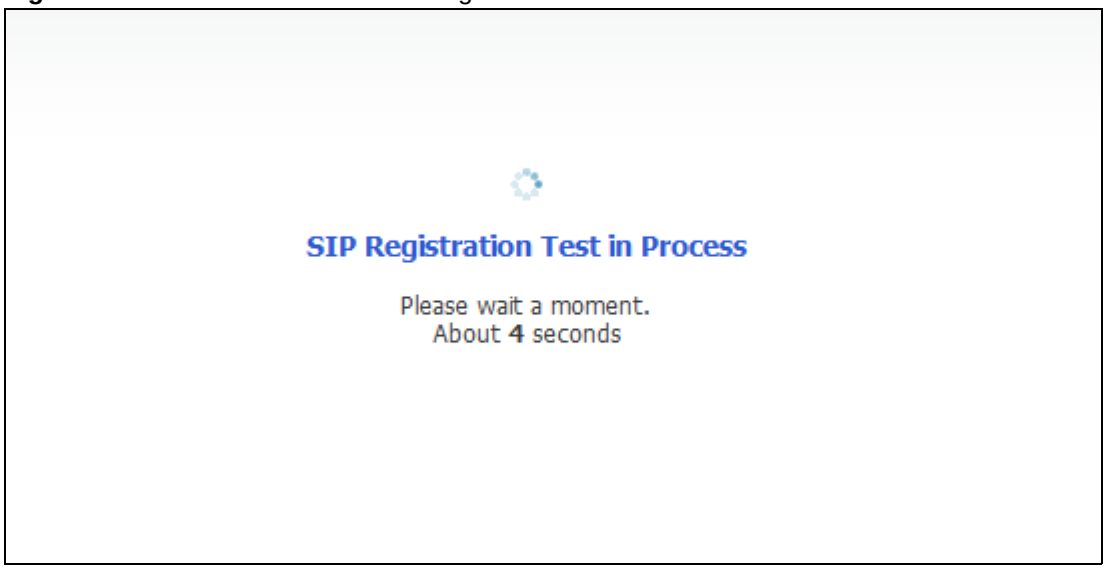

The following table describes the labels in this screen

**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. |
| 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. |

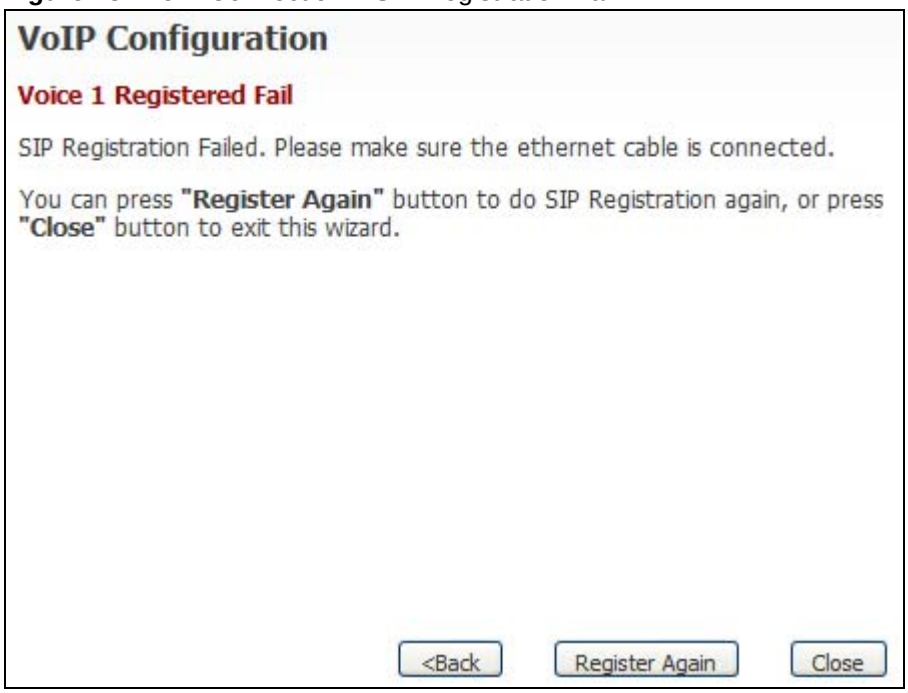
After you enter your voice account settings and click **Next**, the WiMAX Modem attempts to register your SIP account with the SIP server.

**Figure 17** 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.

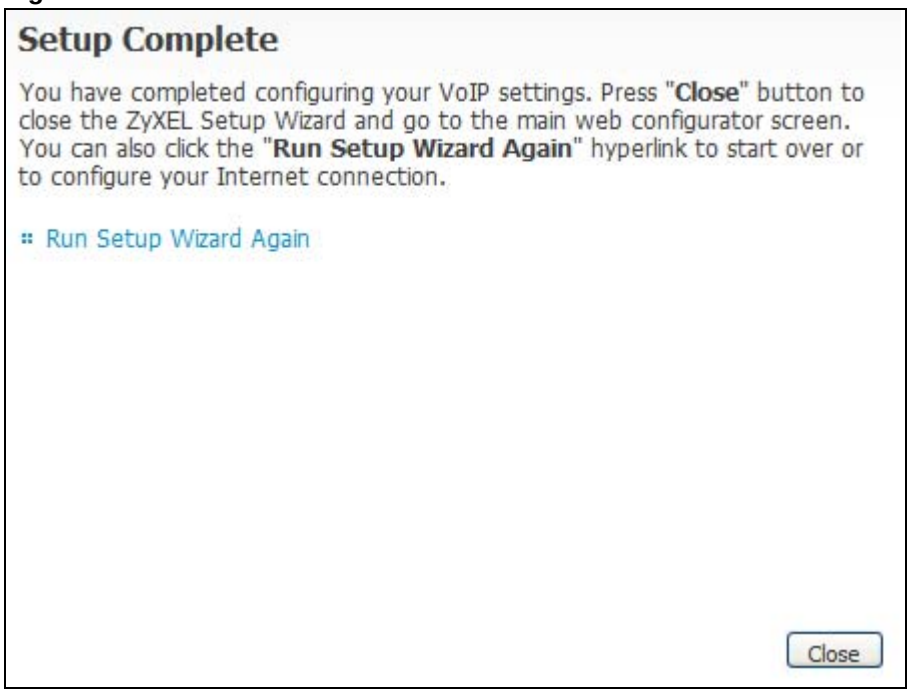
**Figure 18** VoIP Connection > SIP Registration Fail



### 4.2.2 Setup Complete

Click **Close** to complete and save the VoIP Connection settings or **Run Setup Wizard Again** to configure your Internet Connection settings.

**Figure 19** VoIP Connection > Finish




This screen displays if your SIP account registration was successful.

# PART II
# Basic Screens

# 5

# 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 54) lets you configure the WiMAX Modem's IP address and subnet mask.
- The **Time Setting** screen (Section 5.3 on page 55) 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.

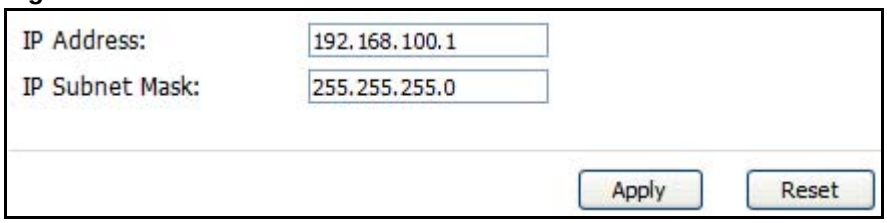
### 5.1.3 Before You Begin

- 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 20** SETUP > Set IP Address




The following table describes the labels in this screen.

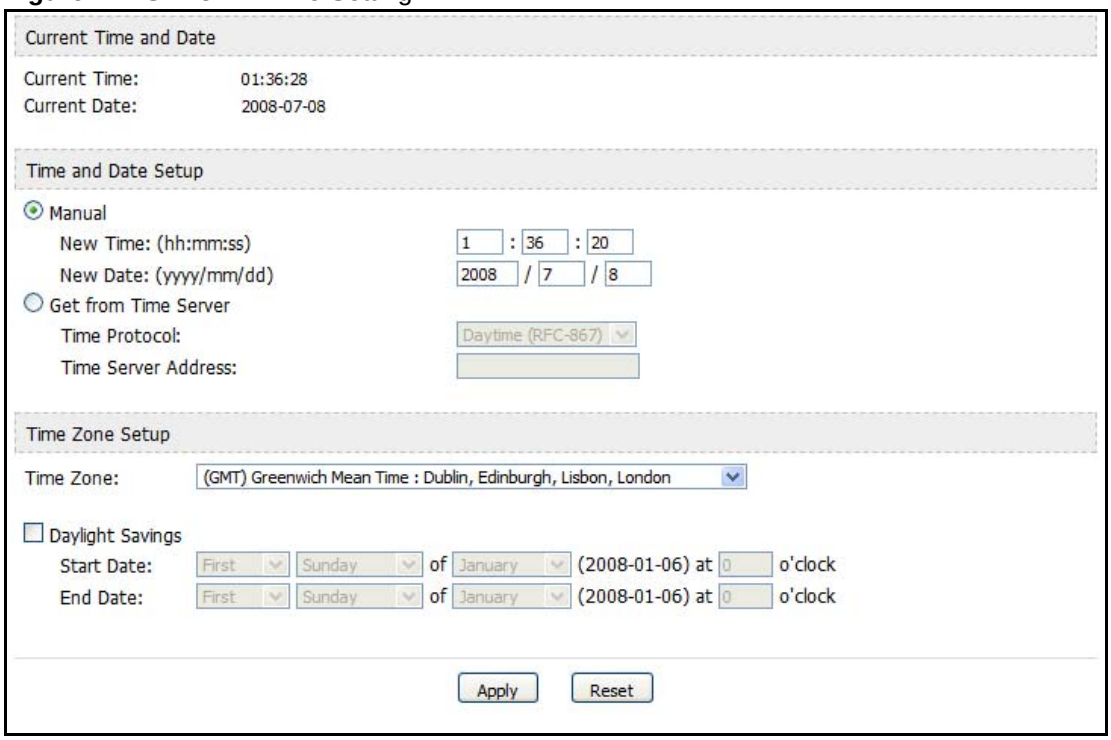
**Table 9** SETUP > Set IP Address

| LABEL | DESCRIPTION |
|---|---|
| IP Address | Enter the IP address of the WiMAX Modem on the LAN.<br><br>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 Time Setting

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

**Figure 21** SETUP > Time Setting




The following table describes the labels in this screen.

**Table 10** SETUP > DHCP Client

| LABEL | DESCRIPTION |
|---|---|
| Current Time and Date | |
| Current Time | Displays the current time according to the WiMAX Modem. |
| 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.<br>**Daytime (RFC 867)** - This format is day/month/year/time zone.<br>**Time (RFC 868)** - This format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0.<br>**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. |

**Table 10** SETUP > DHCP Client (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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. |

## 5.3.1 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 11** 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 |

## 5.3.2 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

# 6

# 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 60) lets you enable, disable, and configure the DHCP server in the WiMAX Modem.
- The **Static DHCP** screen (Section 6.3 on page 61) lets you assign specific IP addresses to specific computers on the LAN.
- The **IP Alias** screen (Section 6.4 on page 62) lets you add subnets on the LAN port. You can also control what routing information is sent and received by each subnet.
- The **IP Static Route** screen (Section 6.5 on page 64) lets you examine the static routes configured in the WiMAX Modem.
- The **Other Settings** screen (Section 6.6 on page 66) 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.

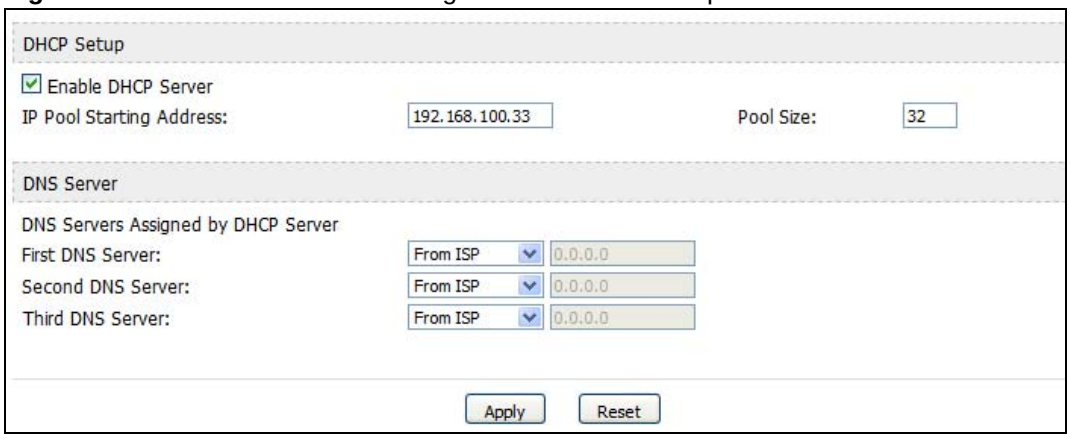
### DHCP

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 22** ADVANCED > LAN Configuration > DHCP Setup




The following table describes the labels in this screen.

**Table 12** 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 | |

**Table 12** ADVANCED > LAN Configuration > DHCP Setup (continued)

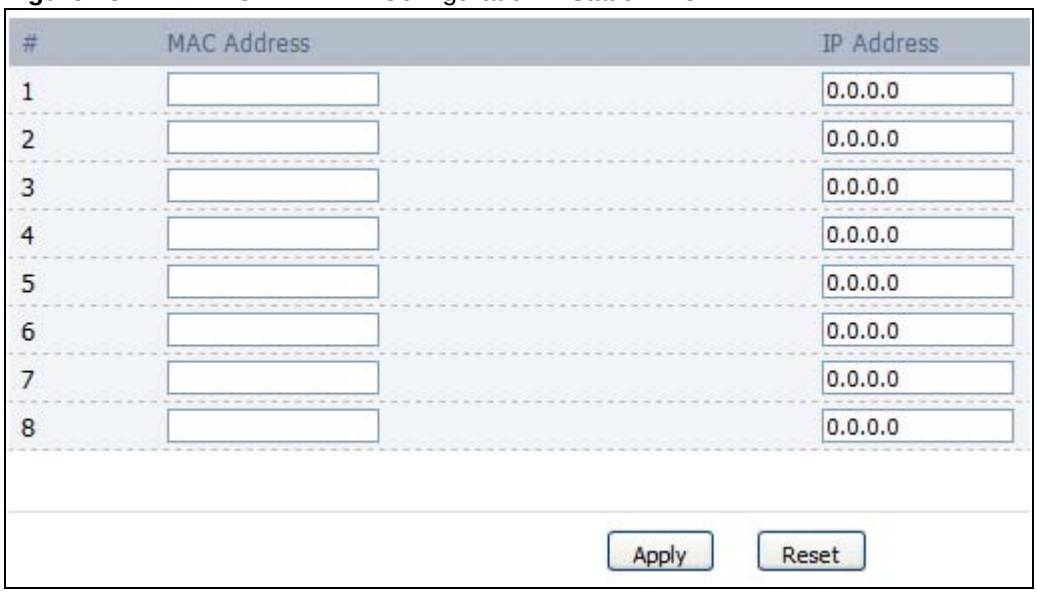
| LABEL | DESCRIPTION |
|---|---|
| First, Second and Third DNS Server | Specify the IP addresses of a maximum of three DNS servers that the network can use. The WiMAX Modem provides these IP addresses to DHCP clients. You can specify these IP addresses two ways.<br>**From ISP** - provide the DNS servers provided by the ISP on the WAN port.<br>**User Defined** - enter a static IP address.<br>**DNS Relay** - this setting will relay DNS information from the DNS server obtained by the WiMAX Modem.<br>**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.

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

**Figure 23** ADVANCED > LAN Configuration > Static DHCP



The following table describes the labels in this screen.

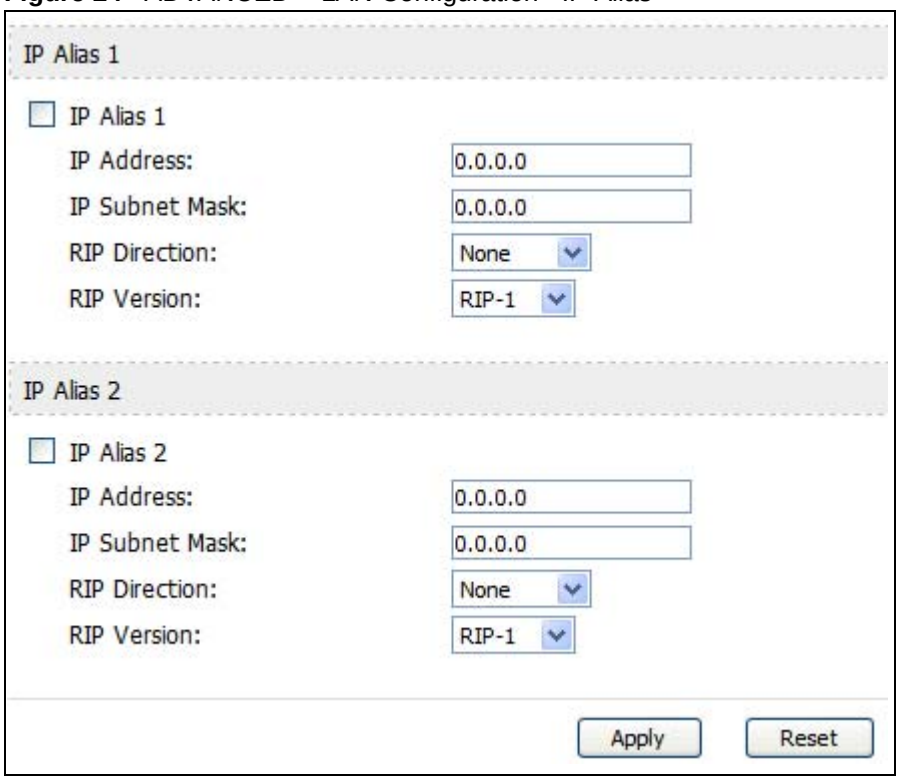
**Table 13** ADVANCED > LAN Configuration > Static DHCP

| 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 Alias

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

**Figure 24** ADVANCED > LAN Configuration> IP Alias




The following table describes the labels in this screen.

**Table 14** ADVANCED > LAN Configuration> IP Alias

| LABEL | DESCRIPTION |
|---|---|
| IP Alias 1 | Select this to add the specified subnet to the LAN port. |
| IP Address | Enter the IP address of the WiMAX Modem on the subnet. |
| IP Subnet Mask | Enter the subnet mask of the subnet. |

**Table 14** ADVANCED > LAN Configuration> IP Alias (continued)

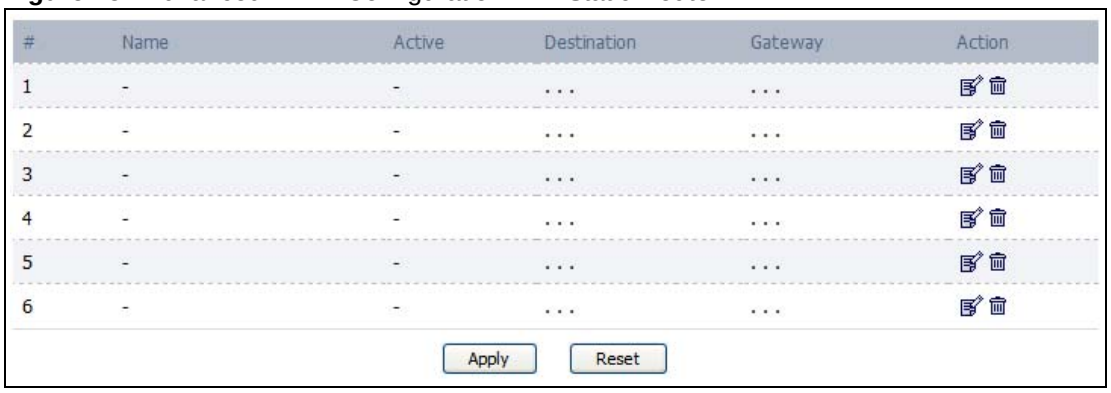
| LABEL | DESCRIPTION |
|---|---|
| RIP Direction | Use this field to control how much routing information the WiMAX Modem sends and receives on the subnet.<br>• **None** - The WiMAX Modem does not send or receive routing information on the subnet.<br>• **Both** - The WiMAX Modem sends and receives routing information on the subnet.<br>• **In Only** - The WiMAX Modem only receives routing information on the subnet.<br>• **Out Only** - The WiMAX Modem only sends routing information on the subnet. |
| RIP Version | Select which version of RIP the WiMAX Modem uses when it sends or receives information on the subnet.<br>• **RIP-1** - The WiMAX Modem uses RIPv1 to exchange routing information.<br>• **RIP-2B** - The WiMAX Modem broadcasts RIPv2 to exchange routing information.<br>• **RIP-2M** - The WiMAX Modem multicasts RIPv2 to exchange routing information. |
| IP Alias 2 | Select this to add the specified subnet to the LAN port. |
| IP Address | Enter the IP address of the WiMAX Modem on the subnet. |
| IP Subnet Mask | Enter the subnet mask of the subnet. |
| RIP Direction | Use this field to control how much routing information the WiMAX Modem sends and receives on the subnet.<br>• **None** - The WiMAX Modem does not send or receive routing information on the subnet.<br>• **Both** - The WiMAX Modem sends and receives routing information on the subnet.<br>• **In Only** - The WiMAX Modem only receives routing information on the subnet.<br>• **Out Only** - The WiMAX Modem only sends routing information on the subnet. |
| RIP Version | Select which version of RIP the WiMAX Modem uses when it sends or receives information on the subnet.<br>• **RIP-1** - The WiMAX Modem uses RIPv1 to exchange routing information.<br>• **RIP-2B** - The WiMAX Modem broadcasts RIPv2 to exchange routing information.<br>• **RIP-2M** - The WiMAX Modem multicasts RIPv2 to exchange routing information. |
| Apply | Click to save your changes. |
| Reset | Click to restore your previously saved settings. |

## 6.5 IP Static Route

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

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

**Figure 25** Advanced> LAN Configuration > IP Static Route




The following table describes the icons in this screen.

**Table 15** Advanced> LAN Configuration > IP Static Route

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

The following table describes the labels in this screen.

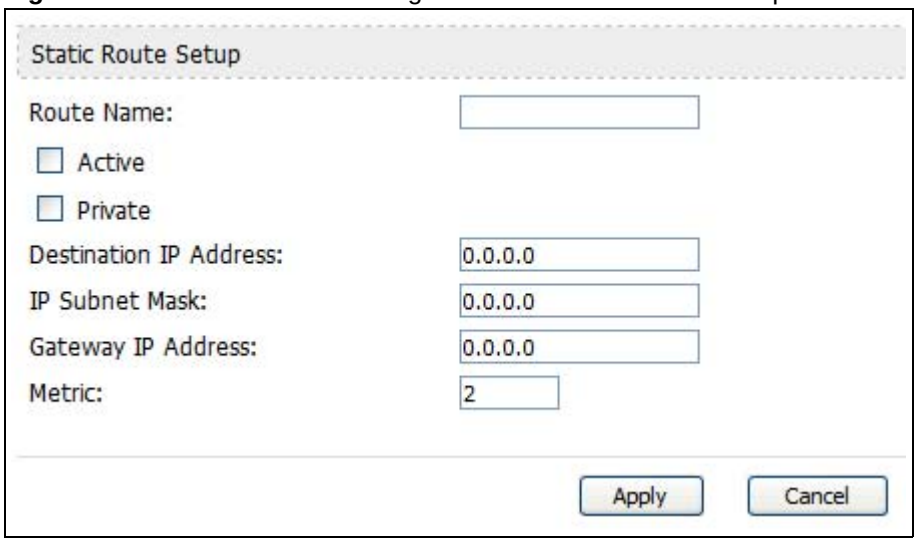
**Table 16** Advanced> LAN Configuration > IP Static Route

| 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. |

## 6.5.1 IP Static Route Setup

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

**Figure 26** Advanced> LAN Configuration > IP Static Route Setup




The following table describes the labels in this screen.

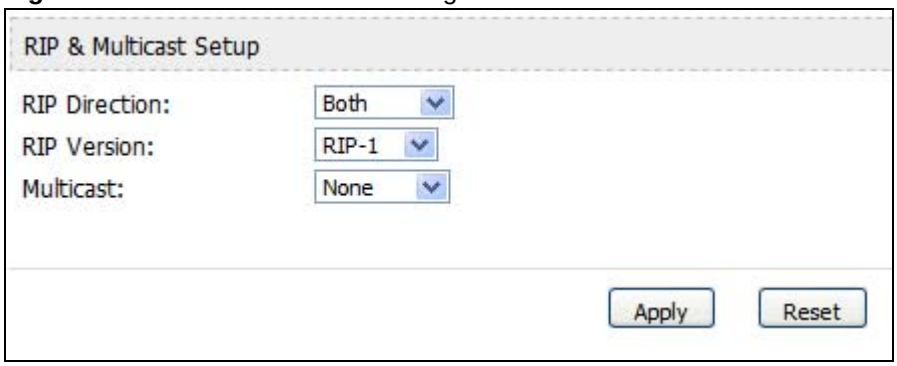
**Table 17** Management > Static Route > IP Static Route > Edit

| 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.<br>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. |
| Apply | Click to save your changes. |
| Cancel | Click to return to the previous screen without saving your changes. |

# 6.6 Other Settings

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

**Figure 27** 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 | Use this field to control how much routing information the WiMAX Modem sends and receives on the subnet.<br>• **None** - The WiMAX Modem does not send or receive routing information on the subnet.<br>• **Both** - The WiMAX Modem sends and receives routing information on the subnet.<br>• **In Only** - The WiMAX Modem only receives routing information on the subnet.<br>• **Out Only** - The WiMAX Modem only sends routing information on the subnet. |
| RIP Version | Select which version of RIP the WiMAX Modem uses when it sends or receives information on the subnet.<br>• **RIP-1** - The WiMAX Modem uses RIPv1 to exchange routing information.<br>• **RIP-2B** - The WiMAX Modem broadcasts RIPv2 to exchange routing information.<br>• **RIP-2M** - The WiMAX Modem multicasts RIPv2 to exchange routing information. |
| Multicast | You do not have to enable multicasting to use **RIP-2M**. (See **RIP Version**.)<br>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).<br>• **None** - The WiMAX Modem does not support multicasting.<br>• **IGMP-v1** - The WiMAX Modem supports IGMP version 1.<br>• **IGMP-v2** - The WiMAX Modem supports IGMP version 2.<br>Multicasting can improve overall network performance. However, it requires extra processing and generates more network traffic. In addition, other computers on the LAN have to support the same version of IGMP. |
| Apply | Click to save your changes. |
| Reset | Click to restore your previously saved settings. |

# 6.7 Technical Reference

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

## 6.7.1 IP Address and Subnet Mask

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

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

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the WiMAX 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 192.168.100.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.100.1, for your WiMAX 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.

## 6.7.2 DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the WiMAX 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 61.

### 6.7.3 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 192.168.100.1 with subnet mask of 255.255.255.0 (24 bits)
- DHCP server enabled with 32 client IP addresses starting from 192.168.1.33.

These parameters should work for the majority of installations. If your ISP gives you explicit DNS server address(es), see Section 6.3 on page 61.

### 6.7.4 DNS Server Address

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

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

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

### 6.7.5 RIP Setup

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

- **Both -** the WiMAX 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.

## 6.7.6 Multicast

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

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

The WiMAX 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.

# 7

# 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 74) lets you set up your WiMAX Modem's Internet settings.
- The **WiMAX Configuration** screen (Section 7.3 on page 76) lets set up the frequencies used by your WiMAX Modem.
- The **Traffic Redirect** screen (Section 7.4 on page 80) lets change your WiMAX Modem's traffic redirect settings.
- The **Other Settings** screen (Section 7.5 on page 81) 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 28** 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 29** 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.

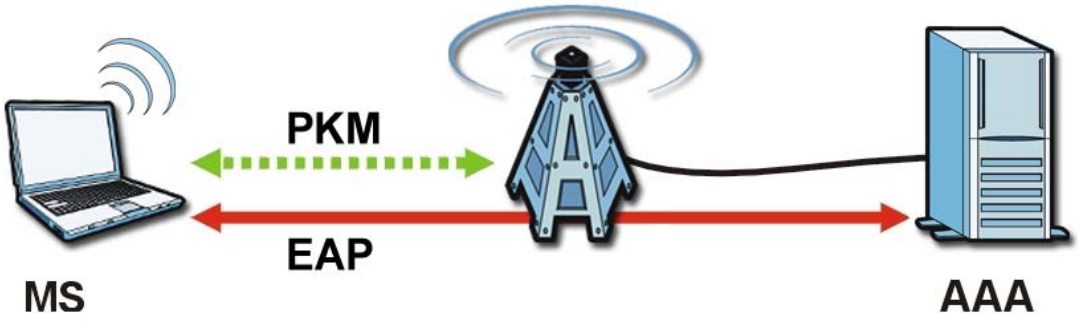
The radio frequency and bandwidth of the link between the WiMAX Modem and the base station are controlled by the base station. The WiMAX Modem follows the base station's configuration.

### 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 30** Using an AAA Server

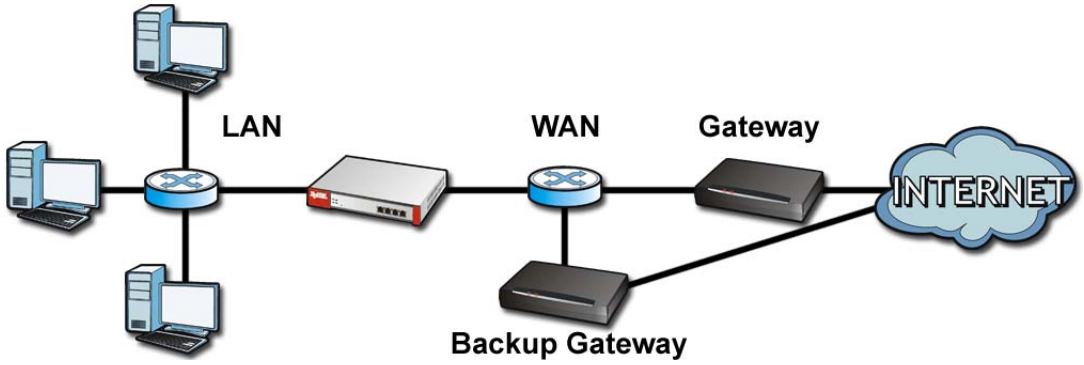


In this figure, the dashed arrow shows the PKM (Privacy Key Management) secured connection between the mobile station and the base station, and the solid arrow shows the EAP secured connection between the mobile station, the base station and the AAA server. See the WiMAX security appendix for more details.

### Traffic Redirect

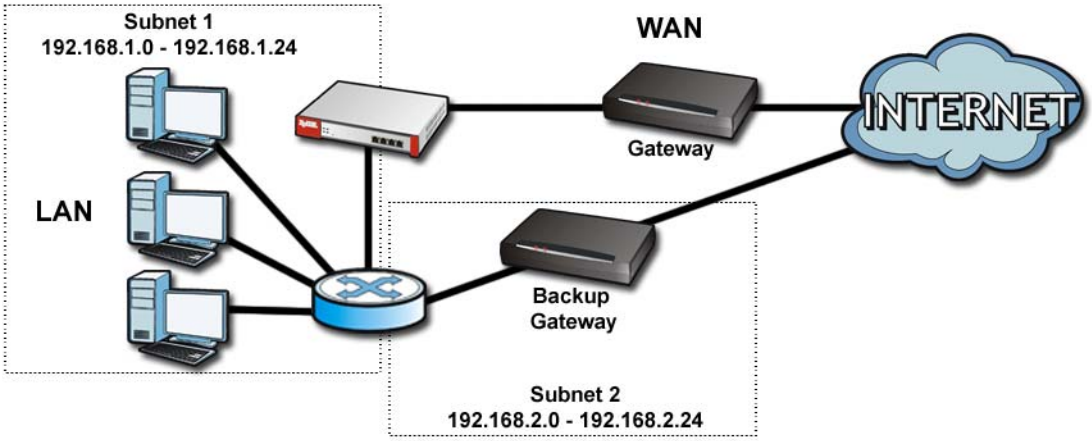
Traffic redirect forwards WAN traffic to a backup gateway when the WiMAX Modem cannot connect to the Internet through its normal gateway. Connect the backup gateway on the WAN so that the WiMAX Modem still provides firewall protection for the LAN.

**Figure 31** Traffic Redirect WAN Setup




IP alias allows you to avoid triangle route security issues when the backup gateway is connected to the LAN or DMZ. Use IP alias to configure the LAN into two or three logical networks with the WiMAX Modem itself as the gateway for each LAN network. Put the protected LAN in one subnet (Subnet 1 in the following figure) and the backup gateway in another subnet (Subnet 2). Configure a LAN to LAN/WiMAX Modem firewall rule that forwards packets from the protected LAN (Subnet 1) to the backup gateway (Subnet 2).

**Figure 32** Traffic Redirect LAN Setup

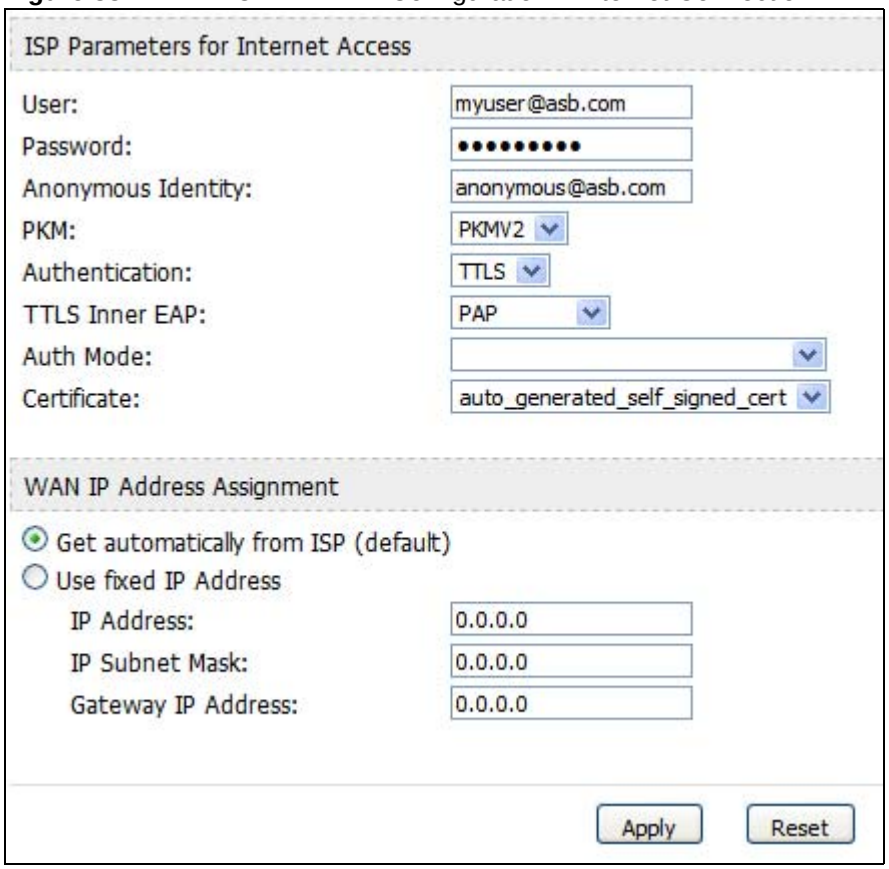


## 7.2 Internet Connection

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

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

**Figure 33** 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 | Use this field to enter the username associated with your Internet access account. You can enter up to 61 printable ASCII characters. |
| Password | Use this field to enter the password associated with your Internet access account. You can enter up to 47 printable ASCII characters. |

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

| LABEL | DESCRIPTION |
|---|---|
| Anonymous Identity | Enter the anonymous identity provided by your Internet Service Provider. Anonymous identity (also known as outer identity) is used with EAP-TTLS encryption. The anonymous identity is used to route your authentication request to the correct authentication server, and does not reveal your real user name. Your real user name and password are encrypted in the TLS tunnel, and only the anonymous identity can be seen.<br>Leave this field blank if your ISP did not give you an anonymous identity to use. |
| PKM | This field displays the Privacy Key Management version number. PKM provides security between the 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 | 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).<br>Check with your service provider if you are unsure of the correct setting for your account.<br>Choose from the following user authentication methods:<br>• **TTLS** (Tunnelled Transport Layer Security)<br>• **TLS** (Transport Layer Security)<br><br>Note: Not all WiMAX Modems support TLS authentication. Check with your service provider for details. |
| TTLS Inner EAP | This field displays the type of secondary authentication method. Once a secure EAP-TTLS connection is established, the inner EAP is the protocol used to exchange security information between the mobile station, the base station and the AAA server to authenticate the mobile station. See the WiMAX security appendix for more details.<br>This field is available only when **TTLS** is selected in the **Authentication** field.<br>The WiMAX Modem supports the following inner authentication types:<br>• **CHAP** (Challenge Handshake Authentication Protocol)<br>• **MSCHAP** (Microsoft CHAP)<br>• **MSCHAPV2** (Microsoft CHAP version 2)<br>• **PAP** (Password Authentication Protocol) |
| Auth Mode | Select the authentication mode from the drop-down list box.<br>This field is not available in all WiMAX Modems. Check with your service provider for details.<br>The WiMAX Modem supports the following authentication modes:<br>• User Only<br>• Device Only with Cert<br>• 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 | |
| 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. |

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

| LABEL | DESCRIPTION |
|---|---|
| IP Subnet Mask | Enter a subnet mask in dotted decimal notation.<br>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.

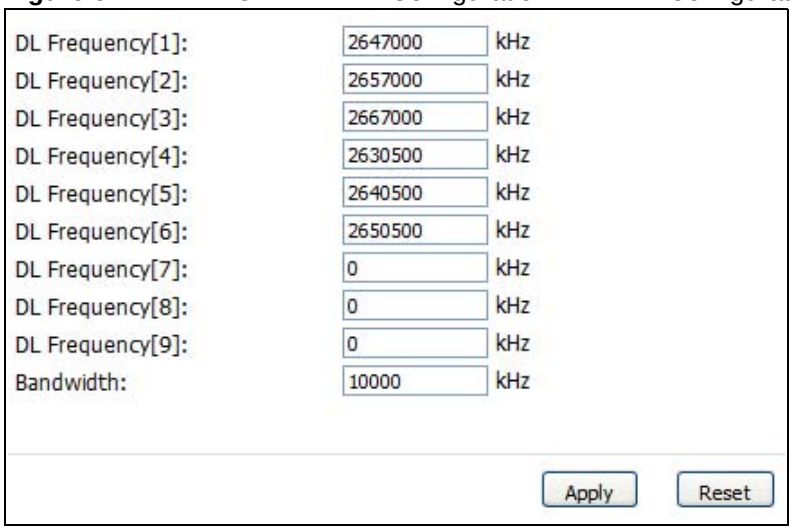
In a WiMAX network, a mobile or subscriber station must use a radio frequency supported by the base station to communicate. When the WiMAX Modem looks for a connection to a base station, it can search a range of frequencies.

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 34** ADVANCED > WAN Configuration >WiMAX Configuration



The following table describes the labels in this screen.

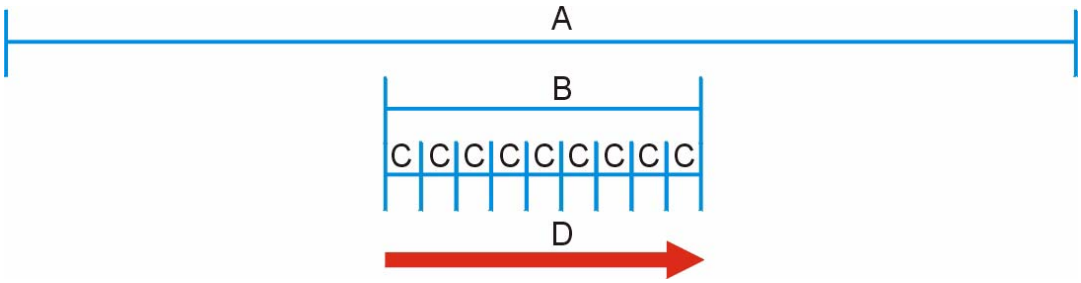
**Table 21** ADVANCED > WAN Configuration >WiMAX Configuration

| LABEL | DESCRIPTION |
|---|---|
| DL Frequency / Bandwidth | 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.<br><br>Note: The **Bandwidth** field is not user-configurable; when the WiMAX Modem finds a WiMAX connection, its frequency is displayed in this field.<br><br>Contact your service provider for details of supported frequencies. |
| 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 35** 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 79 for an example of using the **WiMAX Frequency** screen.

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]**.

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. | *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.* |

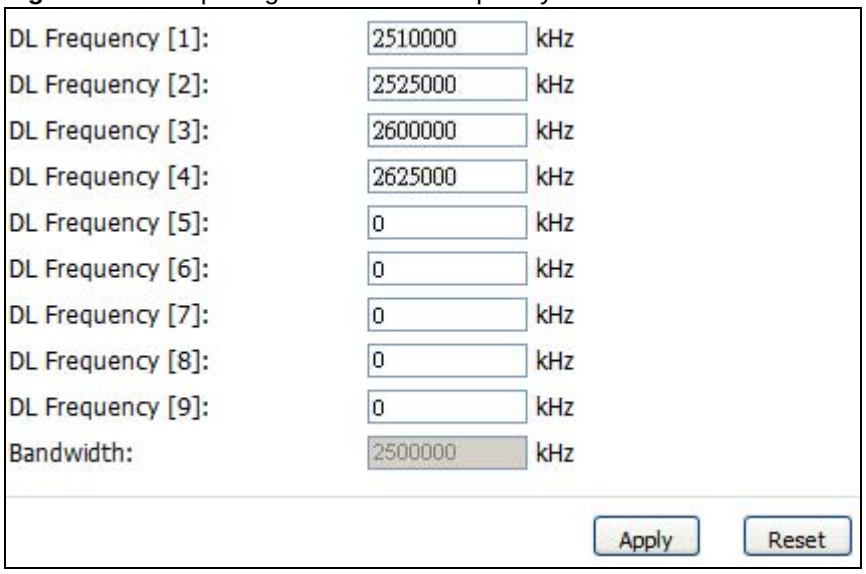
## 7.3.3 Using the WiMAX Frequency Screen

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 36** Completing the WiMAX Frequency Screen



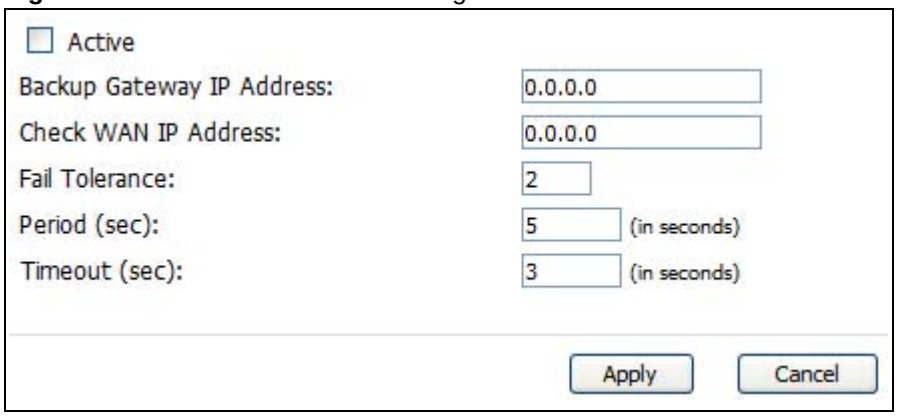

5. Click **Apply**. The WiMAX Modem stores your settings.

   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 Traffic Redirect

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

**Figure 37** ADVANCED > WAN Configuration > Traffic Redirect




The following table describes the labels in this screen.

**Table 23** ADVANCED > WAN Configuration > Traffic Redirect

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

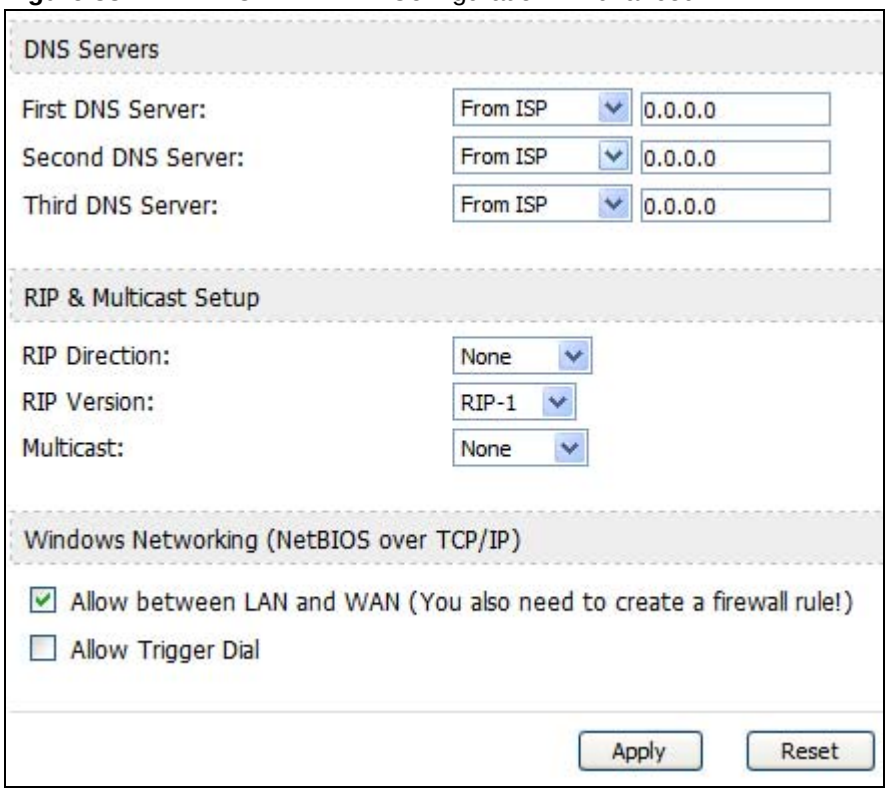
**Table 23** ADVANCED > WAN Configuration > Traffic Redirect (continued)

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

## 7.5 Other Settings

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

**Figure 38** ADVANCED > WAN Configuration > Advanced



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 | 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.<br>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**.<br>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. |
| 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 | 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.<br>Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN. |
| Allow Trigger Dial | Select this option to allow NetBIOS packets to initiate calls. |
| Apply | Click to save your changes. |
| Reset | Click to restore your previously saved settings. |

# 8

# The VPN Transport Screens

## 8.1 Overview

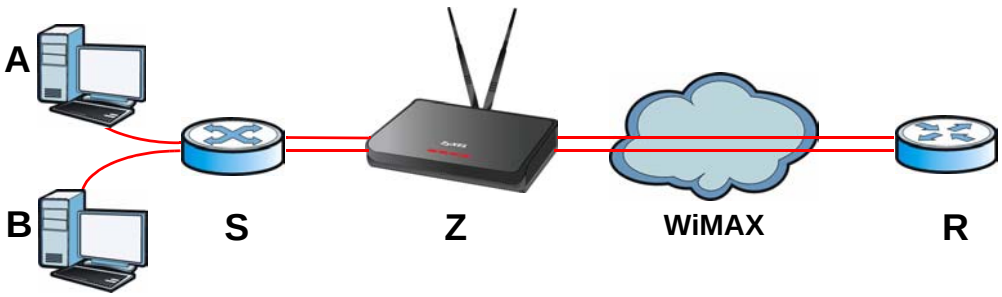
This chapter describes the **ADVANCED > VPN Transport** screens, where you can configure the WiMAX Modem to allow traffic from multiple users to pass through the WiMAX network to the service provider's router. Each user has his own personal connection to the service provider, even though there is only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

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

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

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

**Figure 39** VPN Transport Example




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

## 8.1.1 What You Can Do in This Chapter

- The **General** screen (Section 8.2 on page 85) lets you turn VPN transport on or off, and to set the VPN transport endpoint (your service provider's router).
- The **Customer Interface** screen (Section 8.3 on page 86) lets you specify which users can use which WiMAX network links.
- The **Ethernet Pseudowire** screen (Section 8.4 on page 90) lets you configure the links over the WiMAX network between the WiMAX Modem and the service provider's router.
- The **Statistics** screen (Section 8.5 on page 92) lets you view performance information about the VPN transport connections.

## 8.1.2 What You Need to Know

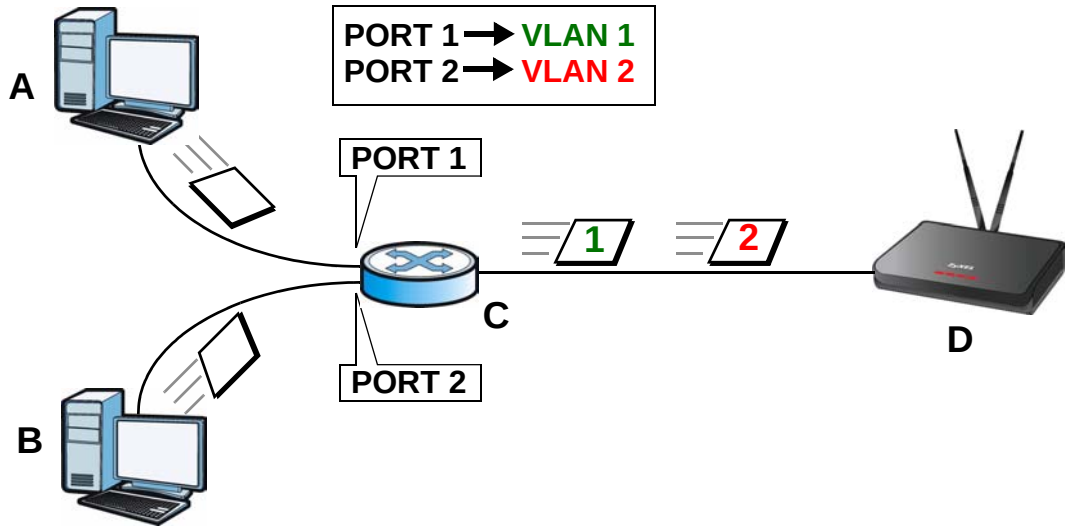
The following terms and concepts may help as you read through this chapter.

### Identifying Users

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

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

**Figure 40** Identifying Users



### 8.1.3 Before You Begin

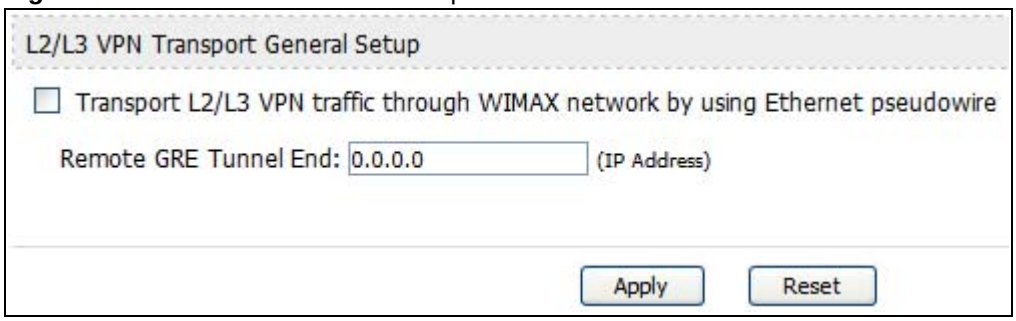
Before you start configuring your WiMAX Modem to use VPN transport, ensure that you have the following from the service provider:

- The IP address or domain name of the service provider's edge router.
- Virtual circuit (VC) labels for each Ethernet Pseudowire you want to create.
- Also make sure that you know the VLAN IDs (Virtual LAN IDentifiers) of the VLANs on your LAN.

## 8.2 General

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

**Figure 41** ADVANCED > VPN Transport > General




The following table describes the labels in this screen.

**Table 25** ADVANCED > VPN Transport > General

| LABEL | DESCRIPTION |
|---|---|
| L2/L3 VPN Transport General Setup | |
| Transport L2/L3 VPN... | Select this to turn the VPN transport feature on. Deselect it to turn the VPN transport feature off. |
| Remote GRE Tunnel End | Enter the domain name or IP address of your service provider's router. |
| Apply | Click to save your changes. |
| Reset | Click to restore your previously saved settings. |

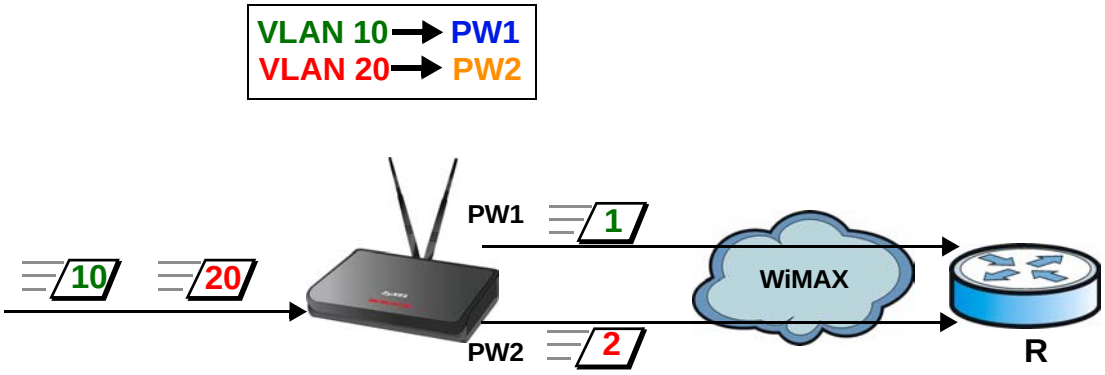
## 8.3 Customer Interface

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

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

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

**Figure 42** Pseudowire Mapping




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

### 8.3.1 Multi-Protocol Label Switching

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

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

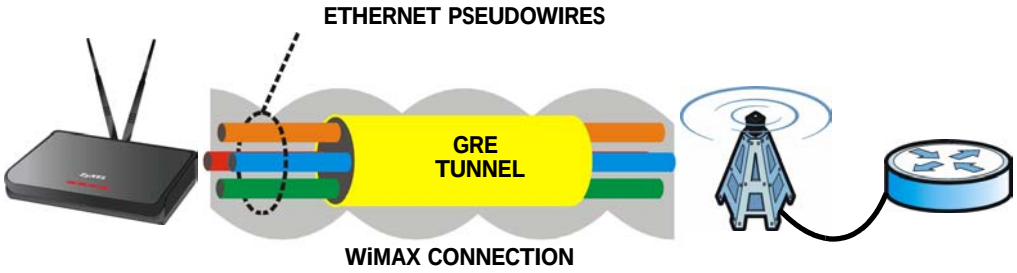
## 8.3.2 Generic Routing Encapsulation

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

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

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

**Figure 43** VPLS Tunneling




## 8.3.3 Customer Interface Options

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

**Figure 44** ADVANCED > VPN Transport > Customer Interface

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

The following table describes the icons in this screen.

**Table 26** Advanced> VPN Transport > Customer Interface

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

The following table describes the labels in this screen.

**Table 27** ADVANCED > VPN Transport > Customer Interface

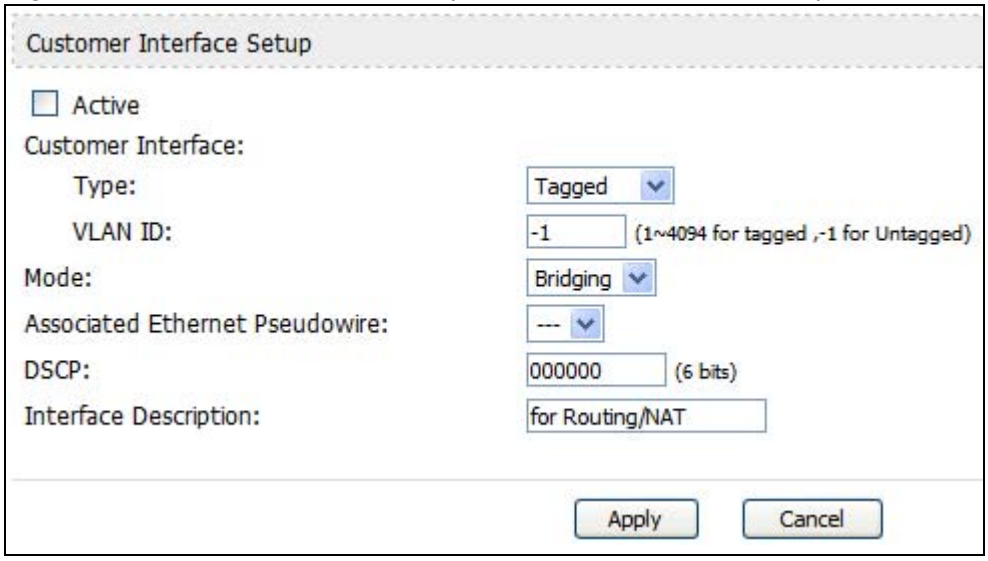
| LABEL | DESCRIPTION |
|---|---|
| # | The number of the item in this list. |
| Active | This icon is green if the associated interface is enabled. The icon is grey if the associated interface is disabled. Enable or disable an interface by clicking its **Edit** icon and selecting or deselecting **Active** and clicking **Apply** in the screen that displays. |
| Interface | |
| Type | This displays either **Tagged** or **Untagged**. A tagged interface controls traffic with a specific IEEE 802.1Q VLAN tag, whereas an untagged interface controls traffic that does not have a VLAN tag. There can be only one untagged interface. |
| VLAN ID | For a tagged interface, this displays the IEEE 802.1Q VLAN ID number. For the untagged interface, **-1** displays. |
| Mode | This displays either **B** (bridging) or **R** (routing). Only the default interface, interface 0, can be a routing interface. |
| Associated Ethernet Pseudowire (Ingress, Egress) | This displays the number of the Ethernet pseudowire that this interface uses, as well as the ingress and egress MPLS (Multi-Protocol Label Switching) VC (Virtual Circuit) label numbers. |
| DSCP | This displays the DiffServ Control Point value you previously entered in binary. This determines the pseudowire's priority on the network. The DSCP value is displayed in binary notation and has six bits. |
| Interface Description | This displays the information you previously entered describing the interface. For the default interface, interface 0, the description reads "for routing / NAT". |
| Action | Click the **Edit** icon to set up a new interface or alter the configuration of an existing interface.<br>Click the **Delete** icon to remove an existing interface. |

## 8.3.4 Customer Interface Setup

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

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

**Figure 45** ADVANCED > VPN Transport > Customer Interface Setup




The following table describes the labels in this screen.

**Table 28** ADVANCED > VPN Transport > Customer Interface Setup

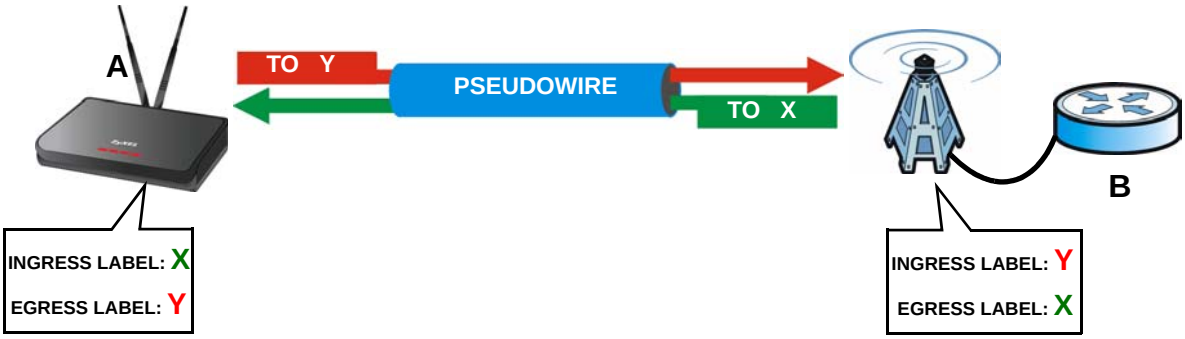
| LABEL | DESCRIPTION |
|---|---|
| Active | Select to make this customer interface active. Deselect it to make the customer interface inactive. |
| Customer Interface | |
| Type | A customer interface can be tagged (controlling traffic that has a specific VLAN ID) or untagged (controlling traffic without a specific VLAN ID). There can be only one untagged interface. |
| VLAN ID | Enter the Virtual Local Area Network Identifier number (1 ~ 4094) for this interface. This VLAN ID must not be used by any other customer interface.<br>For the untagged interface, **-1** displays. |
| Mode | This displays **Bridging** or **Routing**. A tagged interface can operate in bridging mode only. |
| Associated Ethernet Pseudowire | Select the Ethernet pseudowire this interface should use for communications over the WiMAX network. You should configure the pseudowire (in the **ADVANCED > VPN Transport** > **Ethernet Pseudowire** screen) before you select it. |
| DSCP | If you wish to prioritize an interface, enter a DiffServ Code Point value of six bits in binary notation. The higher the value, the higher the interface's priority on the WiMAX Modem's WiMAX link. |
| Interface Description | Enter a brief (up to 31 characters) name or description for this interface. |
| Apply | Click to save your changes. |
| Cancel | Click to return to the previous screen without saving your changes. |

## 8.4 Ethernet Pseudowire

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

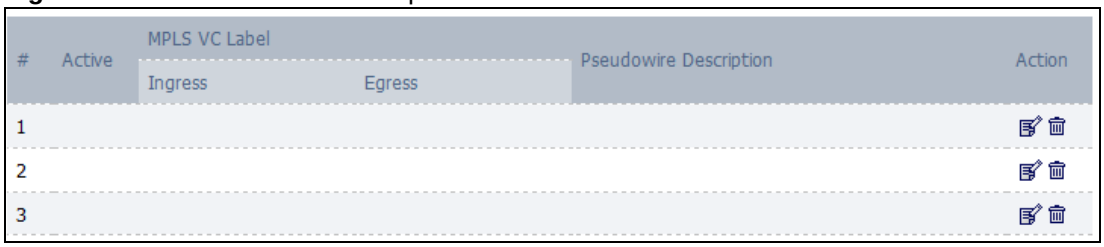
The Ethernet pseudowires use MPLS (MultiProtocol Label Switching) virtual circuit labels to define the connection. In any such pseudowire, the ingress label on one device must be the same as the egress label on the peer device, as shown in the following figure. **A** is your WiMAX Modem and **B** is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

**Figure 46** Ethernet Pseudowire Settings Example




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

**Figure 47** Advance > VPN Transport > Ethernet Pseudowire




The following table describes the icons in this screen.

**Table 29** Advanced> VPN Transport > Customer Interface

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

The following table describes the labels in this screen.

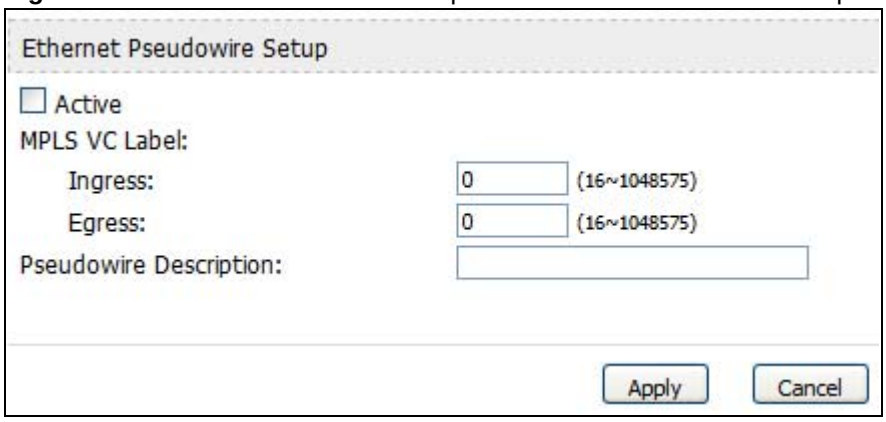
**Table 30** ADVANCED > VPN Transport > Ethernet Pseudowire

| LABEL | DESCRIPTION |
|---|---|
| # | The number of the item in this list. |
| Active | This icon is green if the associated pseudowire is enabled. The icon is grey if the associated pseudowire is disabled. Enable or disable a pseudowire by clicking its **Edit** icon. |
| MPLS VC Label | |
| Ingress | This is the MPLS virtual circuit label number for traffic coming from the peer device. |
| Egress | This is the MPLS virtual circuit label number for traffic going to the peer device. |
| Pseudowire Description | This displays the information you previously entered describing the pseudowire. |
| Action | Click the **Edit** icon to set up an Ethernet pseudowire or alter the configuration of an existing Ethernet pseudowire.<br>Click the **Delete** icon to remove an existing Ethernet pseudowire. |

## 8.4.1 Ethernet Pseudowire Setup

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

**Figure 48** ADVANCED > VPN Transport > Ethernet Pseudowire Setup




The following table describes the labels in this screen.

**Table 31** ADVANCED > VPN Transport > Ethernet Pseudowire Setup

| LABEL | DESCRIPTION |
|---|---|
| Active | Select this to enable the pseudowire. Deselect it to disable the pseudowire. |
| MPLS VC Label | |
| Ingress | Enter the VC ingress label number for this pseudowire. This must be the egress label number of the peer device. This should not be the ingress label number of any other Ethernet pseudowire configured on the WiMAX Modem. |

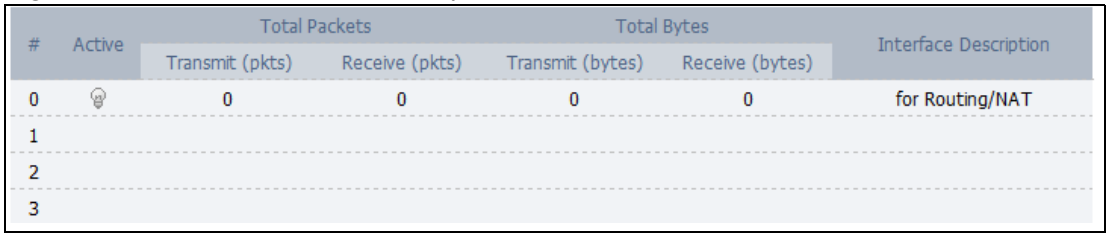
**Table 31** ADVANCED > VPN Transport > Ethernet Pseudowire Setup (continued)

| LABEL | DESCRIPTION |
|---|---|
| Egress | Enter the egress label number for this pseudowire. This must be the ingress label of the peer device. This should not be the egress label number of any other Ethernet pseudowire configured on the WiMAX Modem. |
| Pseudowire Description | Enter a brief (up to 31 characters) description for this pseudowire. |
| Apply | Click to save your changes. |
| Cancel | Click to return to the previous screen without saving your changes. |

# 8.5 Statistics

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

**Figure 49** ADVANCED > VPN Transport > Statistics




The following table describes the labels in this screen.

**Table 32** ADVANCED > VPN Transport > Statistics

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

# 9

# The NAT Configuration Screens

## 9.1 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.

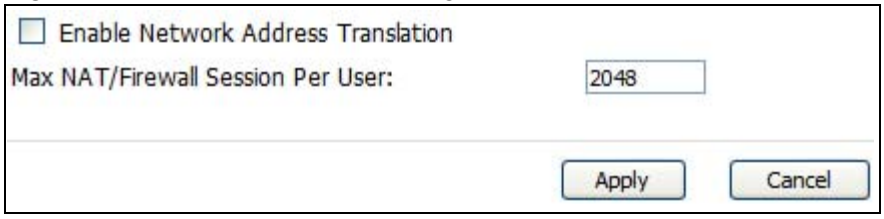
### 9.1.1 What You Can Do in This Chapter

- The **General** screen (Section 9.2 on page 93) lets you enable or disable NAT and to allocate memory for NAT and firewall rules.
- The **Port Forwarding** screen (Section 9.3 on page 94) 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 9.4 on page 97) lets you maintain trigger port forwarding rules for the WiMAX Modem.
- The **ALG** screen (Section 9.5 on page 99) lets you enable and disable SIP (VoIP), FTP (file transfer), and H.323 (audio-visual) ALG in the WiMAX Modem.

## 9.2 General

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

**Figure 50** ADVANCED > NAT Configuration > General



The following table describes the labels in this screen.

**Table 33** 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 | 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.<br>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.<br>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. |
| Apply | Click to save your changes. |
| Cancel | Click to return to the previous screen without saving your changes. |

## 9.3 Port Forwarding

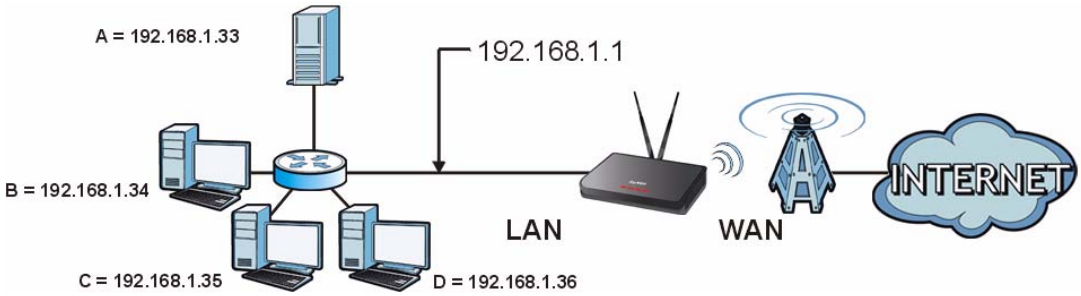
A NAT server set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make accessible to the outside world even though NAT makes your whole inside network appear as a single machine to the outside world.

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.

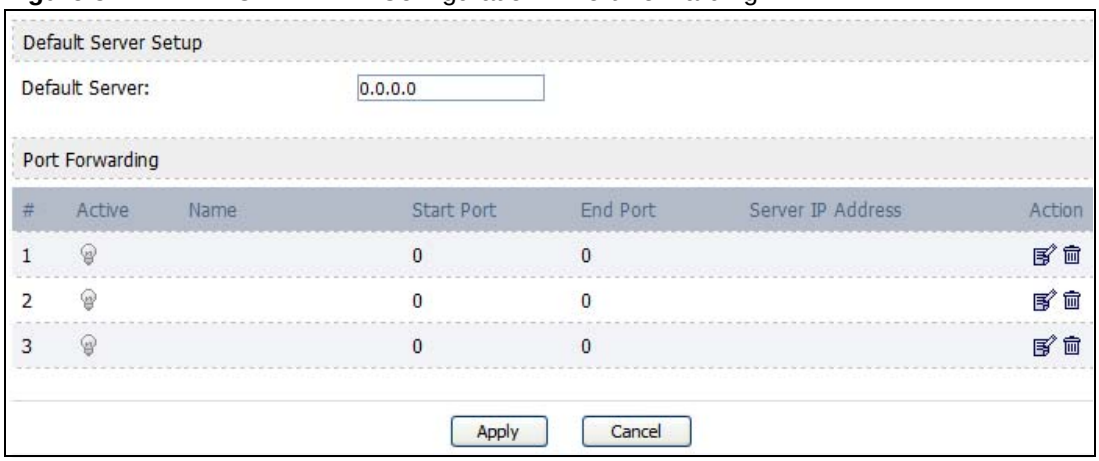
**Figure 51** Multiple Servers Behind NAT Example




## 9.3.1 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 52** ADVANCED > NAT Configuration > Port Forwarding




The following table describes the icons in this screen.

**Table 34** Advanced> VPN Transport > Customer Interface

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

The following table describes the labels in this screen.

**Table 35** 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. |

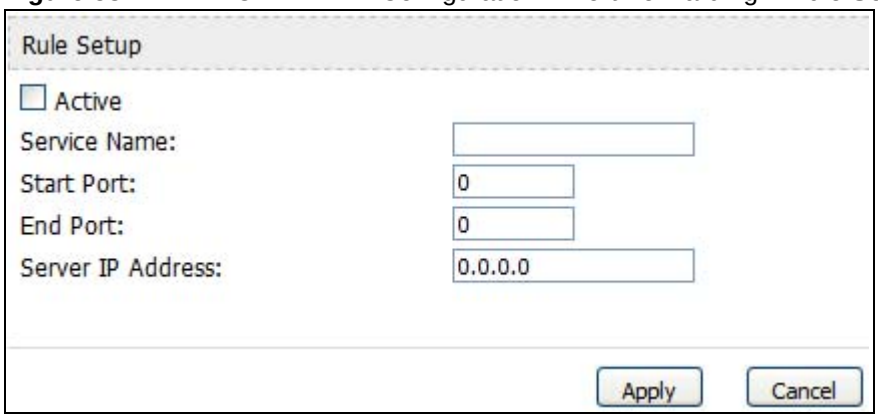
**Table 35** ADVANCED > NAT Configuration > Port Forwarding (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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.<br>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. |

## 9.3.2 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 53** ADVANCED > NAT Configuration > Port Forwarding > Rule Setup




The following table describes the labels in this screen.

**Table 36** 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. |

**Table 36** ADVANCED > NAT Configuration > Port Forwarding > Rule Setup (continued)

| LABEL | DESCRIPTION |
|---|---|
| Start Port<br>End Port | Enter the port number or range of port numbers you want to forward to the specified server.<br>To forward one port number, enter the port number in the **Start Port** and **End Port** fields.<br>To forward a range of ports,<br>• enter the port number at the beginning of the range in the **Start Port** field<br>• 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. |

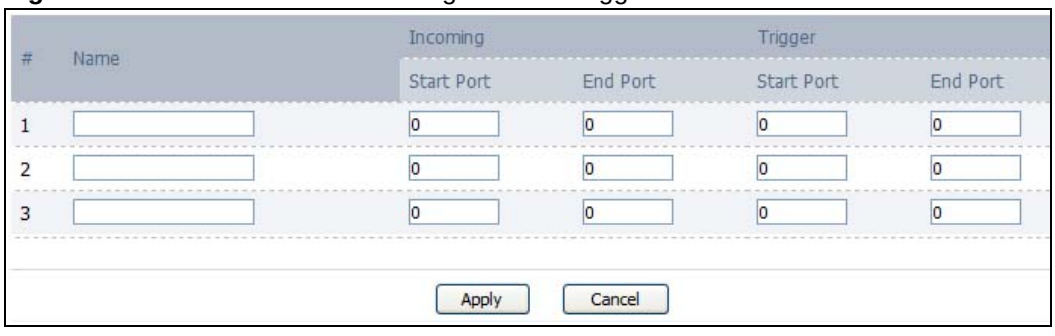
## 9.4 Trigger Port

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 54** ADVANCED > NAT Configuration > Trigger Port



The following table describes the labels in this screen.

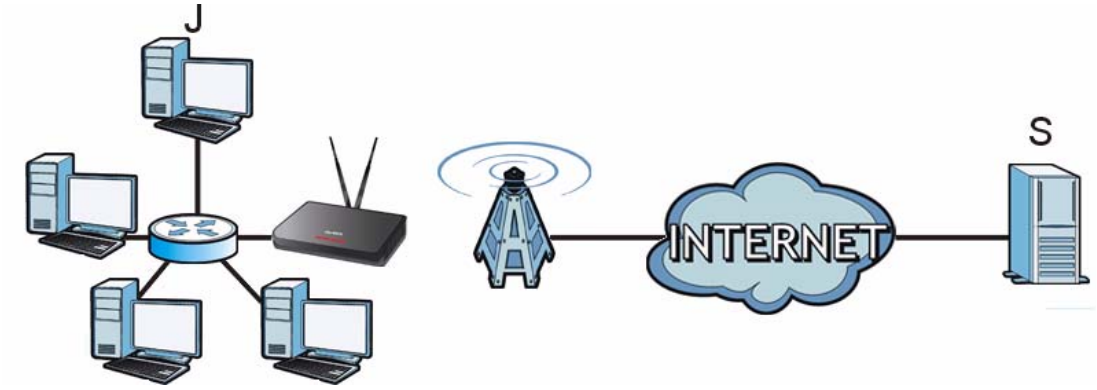
**Table 37** ADVANCED > NAT Configuration > Trigger Port

| 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 | |
| Start Port<br>End Port | Enter the incoming port number or range of port numbers you want to forward to the IP address the WiMAX Modem records.<br>To forward one port number, enter the port number in the **Start Port** and **End Port** fields.<br>To forward a range of ports,<br>• enter the port number at the beginning of the range in the **Start Port** field<br>• enter the port number at the end of the range in the **End Port** field.<br>If you want to delete this rule, enter zero in the **Start Port** and **End Port** fields. |
| Trigger | |
| Start Port<br>End Port | 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).<br>To select one port number, enter the port number in the **Start Port** and **End Port** fields.<br>To select a range of ports,<br>• enter the port number at the beginning of the range in the **Start Port** field<br>• enter the port number at the end of the range in the **End Port** field.<br>If you want to delete this rule, enter zero in the **Start Port** and **End Port** fields. |
| Apply | Click to save your changes. |
| Cancel | Click to return to the previous screen without saving your changes. |

## 9.4.1 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 55** 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.

## 9.5 ALG

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

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

A SIP ALG allows SIP calls to pass through NAT by examining and translating IP addresses embedded in the data stream.

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 56** ADVANCED > NAT Configuration > ALG


The following table describes the labels in this screen.

**Table 38** 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. |

# 10

# The System Configuration Screens

## 10.1 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.

### 10.1.1 What You Can Do in This Chapter

- The **General** screen (Section 10.2 on page 102) 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 10.3 on page 103) lets you set up the WiMAX Modem as a dynamic DNS client.
- The **Firmware** screen (Section 10.4 on page 105) lets you upload new firmware to the WiMAX Modem.
- The **Configuration** screen (Section 10.5 on page 106) lets you back up or restore the configuration of the WiMAX Modem.
- The **Restart** screen (Section 10.6 on page 108) lets you restart your WiMAX Modem from within the web configurator.

### 10.1.2 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.

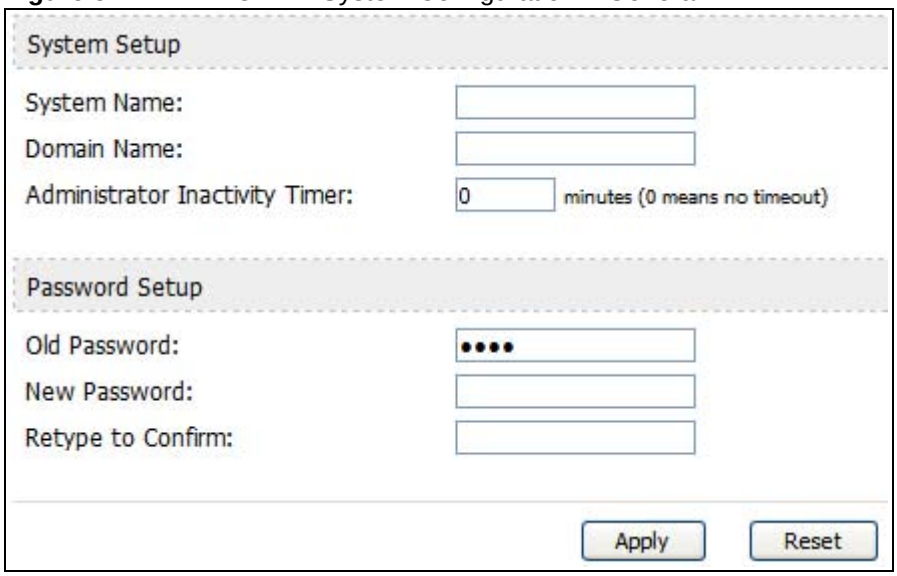
The WiMAX Modem can get the DNS server addresses in the following ways:

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.

## 10.2 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 57** ADVANCED > System Configuration > General



The following table describes the labels in this screen.

**Table 39** 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. |
| Retype to Confirm | Enter the new password again. |
| Apply | Click to save your changes. |
| Reset | Click to restore your previously saved settings. |

## 10.3 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.

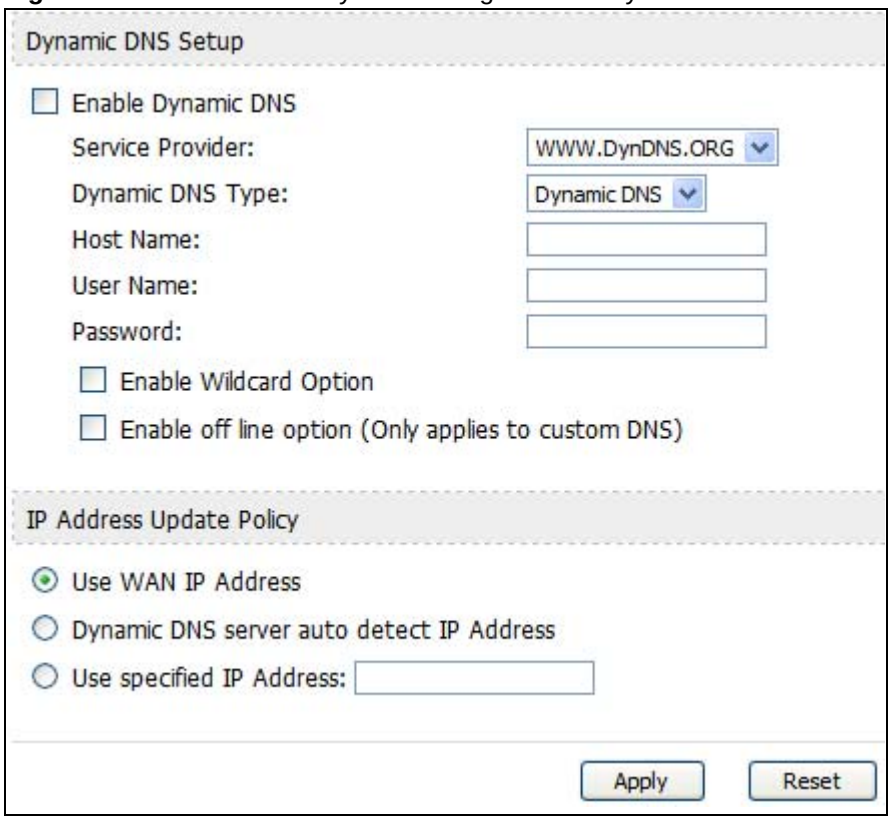
First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

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.

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 58** ADVANCED > System Configuration > Dynamic DNS




The following table describes the labels in this screen.

**Table 40** 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. |
| 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. |

**Table 40** ADVANCED > System Configuration > Dynamic DNS (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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.<br><br>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. |

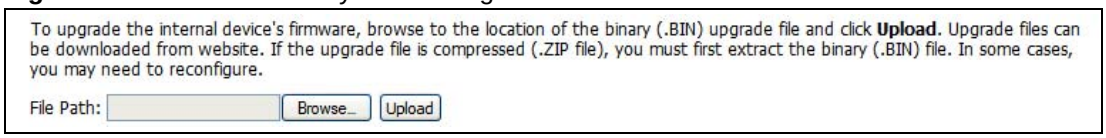
## 10.4 Firmware

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.

Only use firmware for your WiMAX Modem's specific model.

**Figure 59** ADVANCED > System Configuration > Firmware




The following table describes the labels in this screen.

**Table 41** 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.<br><br>Note: Do not turn off the device while firmware upload is in progress! |

### 10.4.1 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.

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.

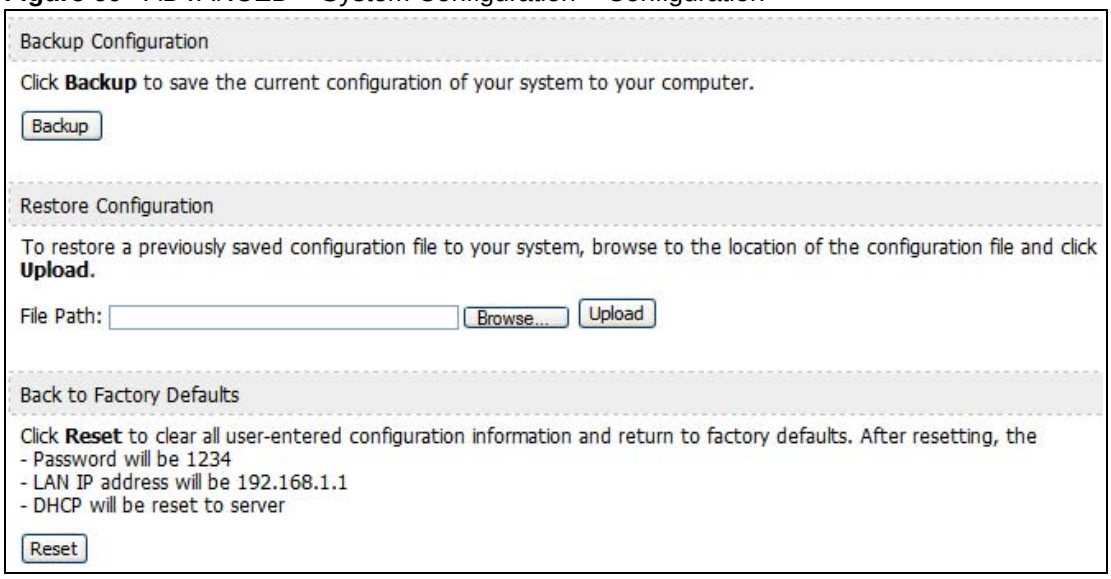
If the upload is not successful, you will be notified by error message.

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

## 10.5 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 60** ADVANCED > System Configuration > Configuration



The following table describes the labels in this screen.

**Table 42** 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.<br>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. |

## 10.5.1 The Restore Configuration Process

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

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:

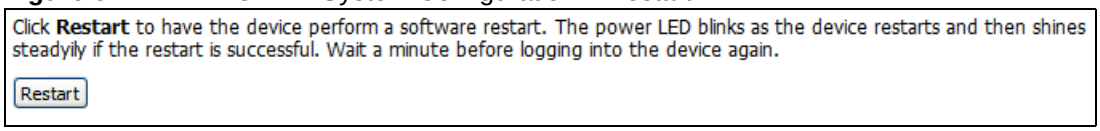
Click **Return** to go back to the **Configuration** screen.

# 10.6 Restart

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

Restarting the WiMAX Modem does not affect its configuration.

**Figure 61** ADVANCED > System Configuration > Restart




The following table describes the labels in this screen.

**Table 43** ADVANCED > System Configuration > Firmware

| LABEL | DESCRIPTION |
|---|---|
| Restart | 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.<br><br>Note: Wait one minute before logging back into the WiMAX Modem after a restart. |

## 10.6.1 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

# 11

# The Service Configuration Screens

## 11.1 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 it's 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.

### 11.1.1 What You Can Do in This Chapter

- The **SIP Settings** screen (Section 11.2 on page 113) lets you setup and maintain your SIP account(s) in the WiMAX Modem.
- The **Advanced SIP Settings** screen (Section 11.2.1 on page 114) lets you set up and maintain advanced settings for each SIP account
- The **QoS** screen (Section 11.3 on page 120) lets you set up and maintain ToS and VLAN settings for the WiMAX Modem.

### 11.1.2 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.

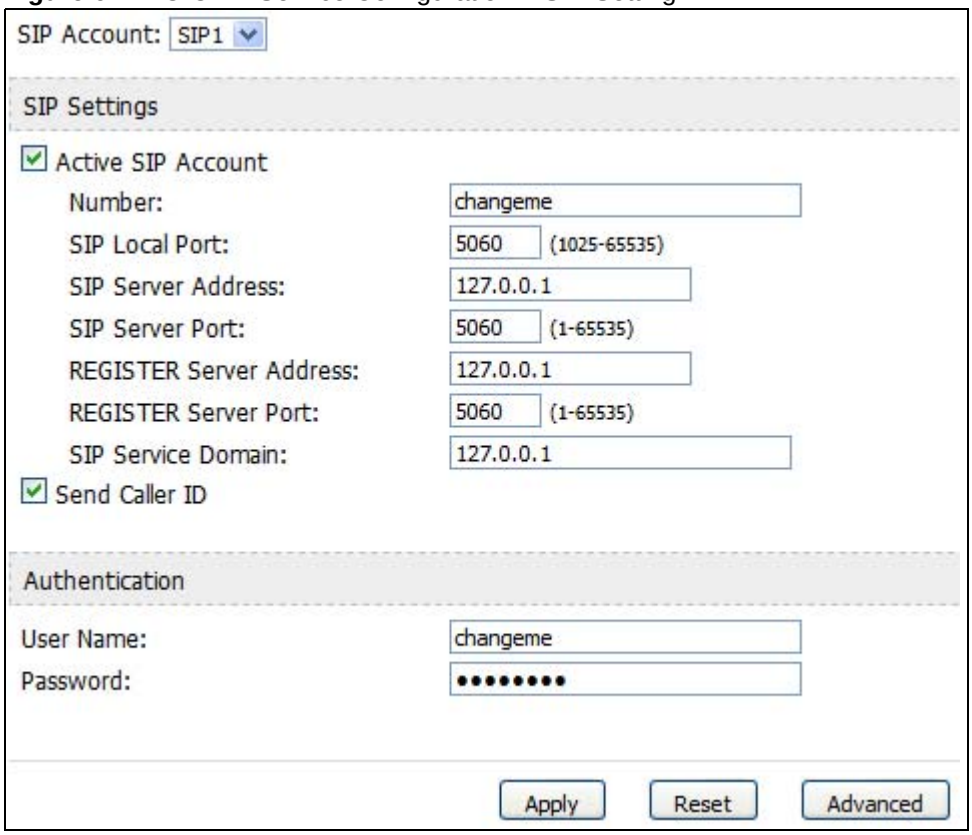
### 11.1.3 Before you Begin

- 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.

## 11.2 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 62** VOICE > Service Configuration > SIP Setting




The following table describes the labels in this screen.

**Table 44** 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. |

**Table 44** VOICE > Service Configuration > SIP Setting (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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. |

## 11.2.1 Advanced SIP Settings

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

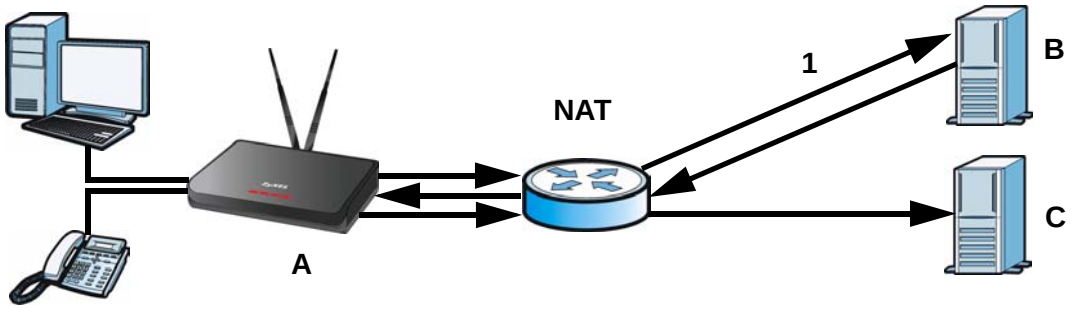
### 11.2.1.1 STUN

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 63** STUN




### 11.2.1.2 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).

### 11.2.1.3 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.

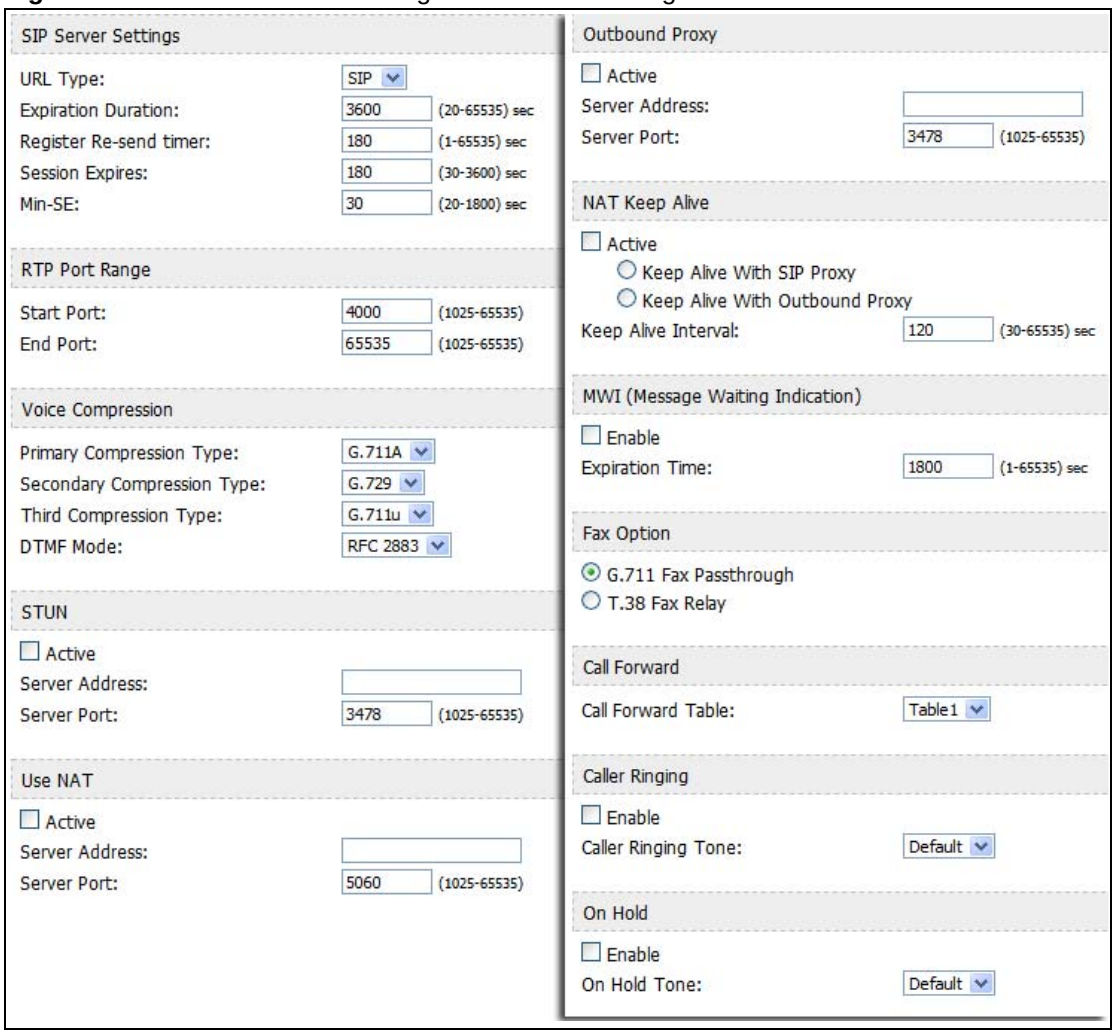
### 11.2.1.4 MWI (Message Waiting Indication)

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.

### 11.2.1.5 Advanced SIP Settings Options

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

**Figure 64** VOICE > Service Configuration > SIP Settings > Advanced




The following table describes the labels in this screen.

**Table 45** 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.<br>• **SIP** - include the SIP service domain name<br>• **TEL** - do not include the SIP service domain name |

**Table 45** 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<br>End Port | Enter the listening port number(s) for RTP traffic, if your VoIP service provider gave you this information. Otherwise, keep the default values.<br>To enter one port number, enter the port number in the **Start Port** and **End Port** fields.<br>To enter a range of ports:<br>• Type the port number at the beginning of the range in the **Start Port** field<br>• Type the port number at the end of the range in the **End Port** field. |
| Voice Compression | |
| Primary, Secondary, and Third Compression | Select the type of voice coder/decoder (codec) that you want the WiMAX Modem to use.<br>G.711 provides high voice quality but requires more bandwidth (64 kbps).<br>• **G.711A** is typically used in Europe.<br>• **G.711u** is typically used in North America and Japan.<br>• **G.723** provides good voice quality, and requires 20 or 40 kbps.<br>• **G.729** requires only 8 kbps.<br>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.<br>For more on voice compression, see Voice Coding on page 115 |
| DTMF Mode | 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.<br>• **RFC 2833** - send the DTMF tones in RTP packets<br>• **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.<br>• **SIP INFO** - send the DTMF tones in SIP messages |
| STUN | |
| Active | Select this if all of the following conditions are satisfied.<br>• There is a NAT router between the WiMAX Modem and the SIP server.<br>• The NAT router is not a SIP ALG.<br>• Your VoIP service provider gave you an IP address or domain name for a STUN server.<br>• 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 | |

**Table 45** VOICE > Service Configuration > SIP Settings > Advanced (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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. |
| 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. |

**Table 45** VOICE > Service Configuration > SIP Settings > Advanced (continued)

| LABEL | DESCRIPTION |
|---|---|
| Caller Ringing Tone | Select the tone you want people to hear when they call you. See Custom Tones (IVR) on page 119 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 119 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. |

### 11.2.1.6 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 46** Custom Tones Details

| LABEL | DESCRIPTION |
|---|---|
| Total Time for All Tones | 128 seconds for all custom tones combined |
| Maximum Time per Individual Tone | 20 seconds |
| Total Number of Tones Recordable | 8<br>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.

## 11.3 QoS

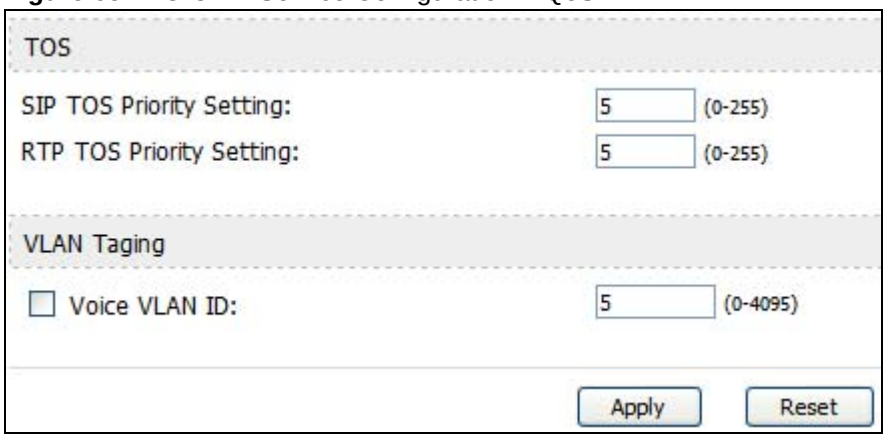
Network traffic can be classified by setting the ToS (Type Of Service) values at the data source (for example, at the WiMAX Modem) so a server can decide the best method of delivery, that is the least cost, fastest route and so on.

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 65** VOICE > Service Configuration > QoS




The following table describes the labels in this screen.

**Table 47** 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 47** 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.<br>Otherwise, clear this field. |
| Apply | Click to save your changes. |
| Reset | Click to restore your previously saved settings. |

# 11.4 Technical Reference

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

## 11.4.1 SIP Call Progression

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

**Table 48** 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.

## 11.4.2 SIP Client Server

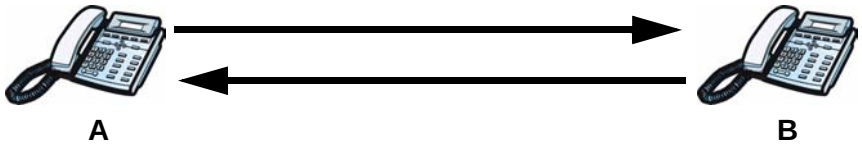
SIP is a client-server protocol. A SIP client is an application program or device that sends SIP requests. A SIP server responds to the SIP requests.

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.

## 11.4.3 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 66** SIP User Agent



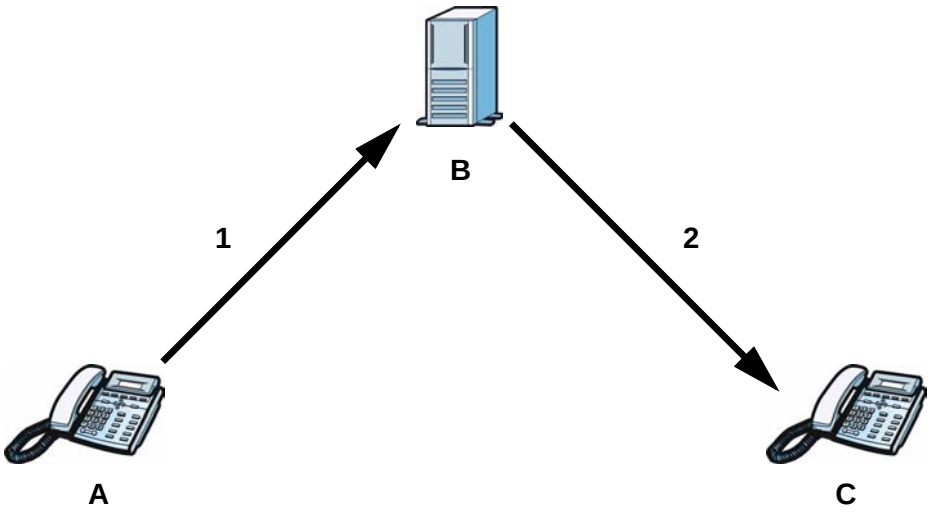

## 11.4.4 SIP Proxy Server

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 67** SIP Proxy Server



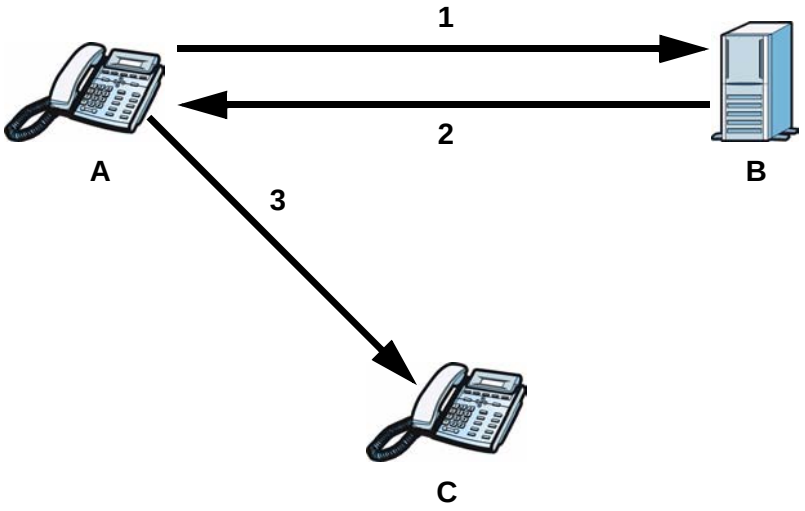
## 11.4.5 SIP Redirect Server

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

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

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

**Figure 68** SIP Redirect Server




## 11.4.6 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 9 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.

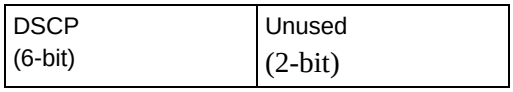
## 11.4.7 DiffServ

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.

## 11.4.8 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 69** DiffServ: Differentiated Service Field




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.

# 12

# The Phone Screens

## 12.1 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.

### 12.1.1 What You Can Do in This Chapter

- The **Analog Phone** screen (Section 12.2 on page 126) lets you control which SIP accounts each phone uses.
- The **Common** screen (Section 12.3 on page 128) lets you activate and deactivate immediate dialing.
- The **Region** screen (Section 12.4 on page 129) lets you maintain settings that often depend on the region of the world in which the WiMAX Modem is located.

### 12.1.2 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

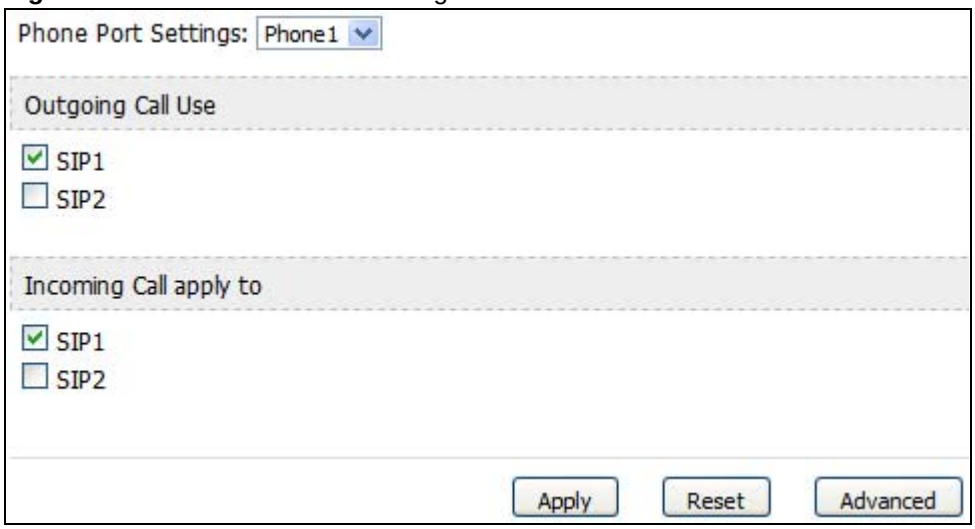
- Making a Second Call
- Call Transfer
- Call Forwarding
- Three-Way Conference
- Internal Calls
- Caller ID
- CLIP (Calling Line Identification Presentation)
- CLIR (Calling Line Identification Restriction)

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

## 12.2 Analog Phone

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

**Figure 70** VOICE > Phone > Analog Phone




The following table describes the labels in this screen.

**Table 49** VOICE > Phone > Analog Phone

| LABEL | DESCRIPTION |
|---|---|
| Phone Port Settings | Select the phone port you want to see in this screen. If you change this field, the screen automatically refreshes. |
| Outgoing Call Use | |
| SIP1 | Select this if you want this phone port to use the SIP1 account when it makes calls. If you select both SIP accounts, the WiMAX Modem tries to use SIP2 first. |
| SIP2 | Select this if you want this phone port to use the SIP2 account when it makes calls. If you select both SIP accounts, the WiMAX Modem tries to use SIP2 first. |

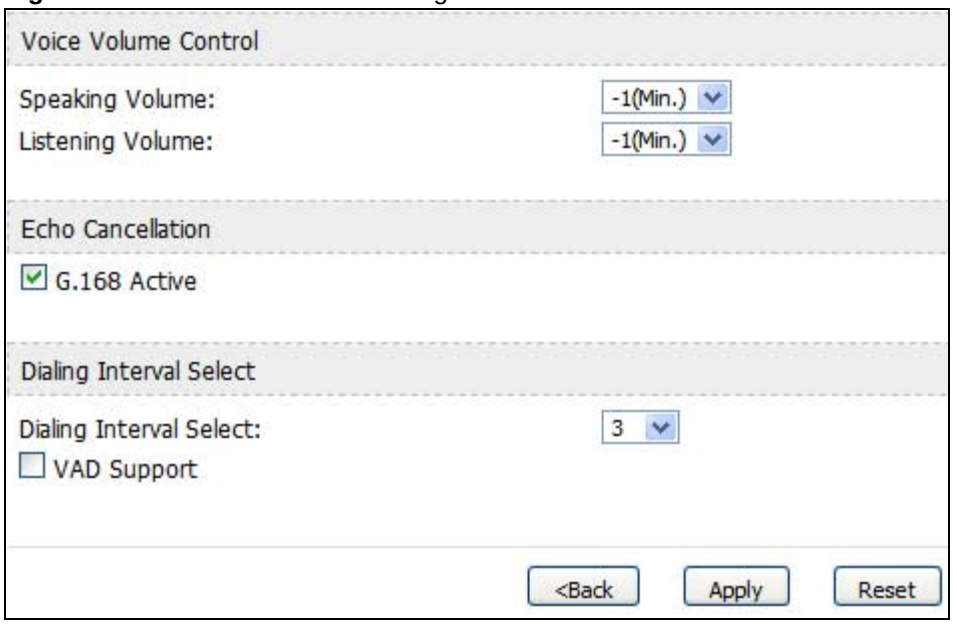
**Table 49** VOICE > Phone > Analog Phone

| LABEL | DESCRIPTION |
|---|---|
| Incoming Call apply to | |
| SIP1 | Select this if you want to receive phone calls for the SIP1 account on this phone port. If you select more than one source for incoming calls, there is no way to distinguish between them when you receive phone calls. |
| SIP2 | Select this if you want to receive phone calls for the SIP2 account on this phone port. If you select more than one source for incoming calls, there is no way to distinguish between them when you receive phone calls. |
| Apply | Click to save your changes. |
| Reset | Click to restore your previously saved settings. |
| Advanced Setup | Click this to edit the advanced settings for this phone port. The **Advanced Analog Phone Setup** screen appears. |

## 12.2.1 Advanced Analog Phone Setup

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

**Figure 71** VOICE > Phone > Analog Phone > Advanced




The following table describes the labels in this screen.

**Table 50** 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. -1 is the quietest, and 1 is the loudest. |
| Listening Volume | Enter the loudness that the WiMAX Modem uses for speech that it receives from the peer device. -1 is the quietest, and 1 is the loudest. |
| Echo Cancellation | |

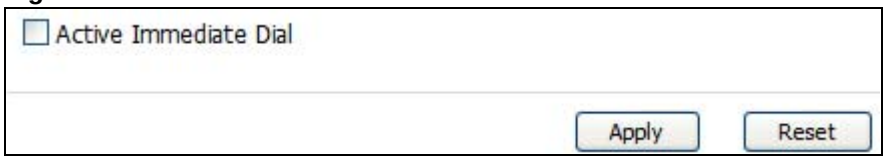
**Table 50** VOICE > Phone > Analog Phone > Advanced

| LABEL | DESCRIPTION |
|---|---|
| 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.<br>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. |

## 12.3 Common

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

**Figure 72** VOICE > Phone > Common




The following table describes the labels in this screen.

**Table 51** 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**.<br>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. |

## 12.4 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 73** VOICE > Phone > Region


The following table describes the labels in this screen.

**Table 52** 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.<br>• **Europe Type** - use supplementary phone services in European mode<br>• **USA Type** - use supplementary phone services American mode<br>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. |

## 12.5 Technical Reference

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

### 12.5.1 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.

## 12.5.2 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 53** European Type Flash Key Commands

| COMMAND | SUB-COMMAND | DESCRIPTION |
|---|---|---|
| Flash | | Put a current call on hold to place a second call.<br>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.<br>2. Put a current call on hold to answer an incoming call.<br>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”.

### 12.5.3 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 54** 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.<br>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.

# 13

# The Phone Book Screens

## 13.1 Overview

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

### 13.1.1 What You Can Do in This Chapter

- The **Incoming Call Policy** screen (Section 13.2 on page 134) lets you maintain rules for handling incoming calls. You can block, redirect, or accept them.
- The **Speed Dial** screen (Section 13.3 on page 136) lets you add, edit, or remove speed-dial entries.

### 13.1.2 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.

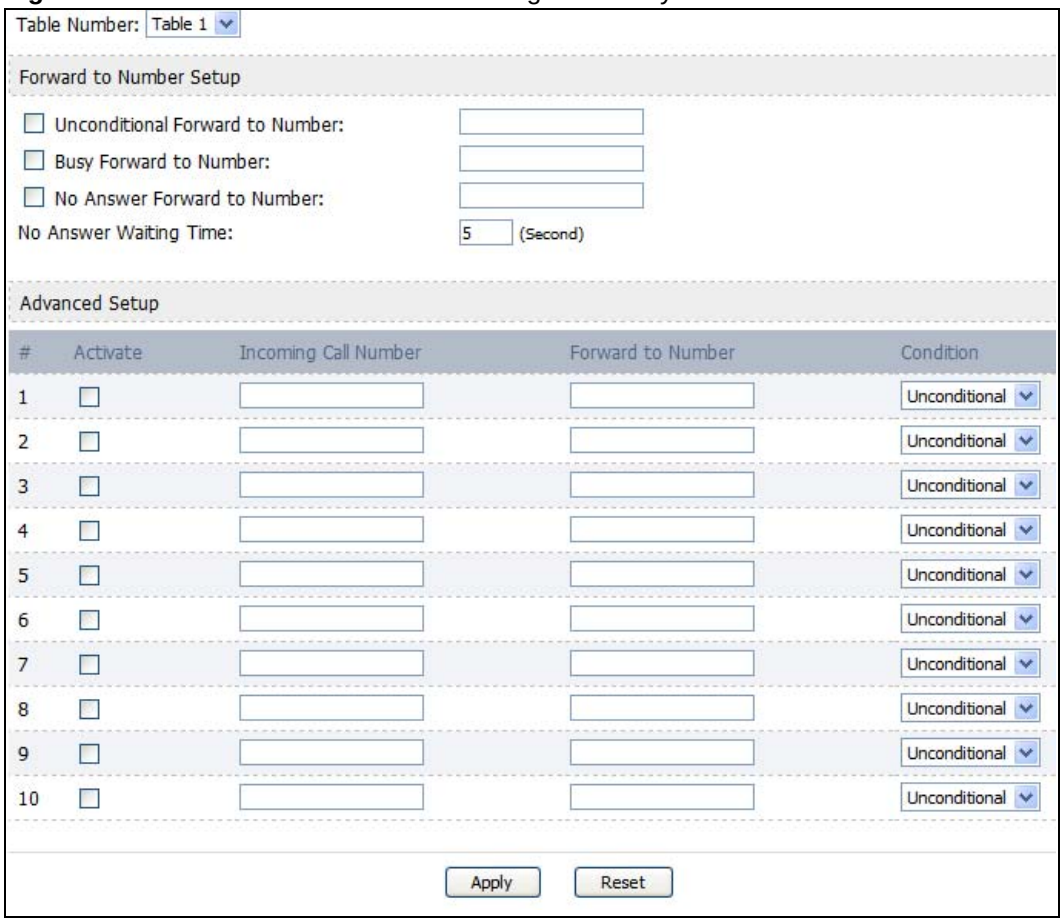
In peer-to-peer calls, you call another VoIP device directly without going through a SIP server. In the WiMAX Modem, you must set up a speed dial entry in the phone book in order to do this. Select **Non-Proxy (Use IP or URL)** in the **Type** column and enter the callee's IP address or domain name.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

## 13.2 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 74** VOICE > Phone Book > Incoming Call Policy




The following table describes the labels in this screen.

**Table 55** 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. |
| 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. |

**Table 55** VOICE > Phone Book > Incoming Call Policy

| LABEL | DESCRIPTION |
|---|---|
| No Answer Waiting Time | This field is used by the **No Answer Forward to Number** feature and **No Answer** conditions below.<br>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.<br>• **Unconditional** - The WiMAX Modem immediately forwards any calls from the **Incoming Call Number** to the **Forward to Number**.<br>• **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.<br>• **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**.)<br>• **Block -** The WiMAX Modem rejects calls from the **Incoming Call Number**.<br>• **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. |

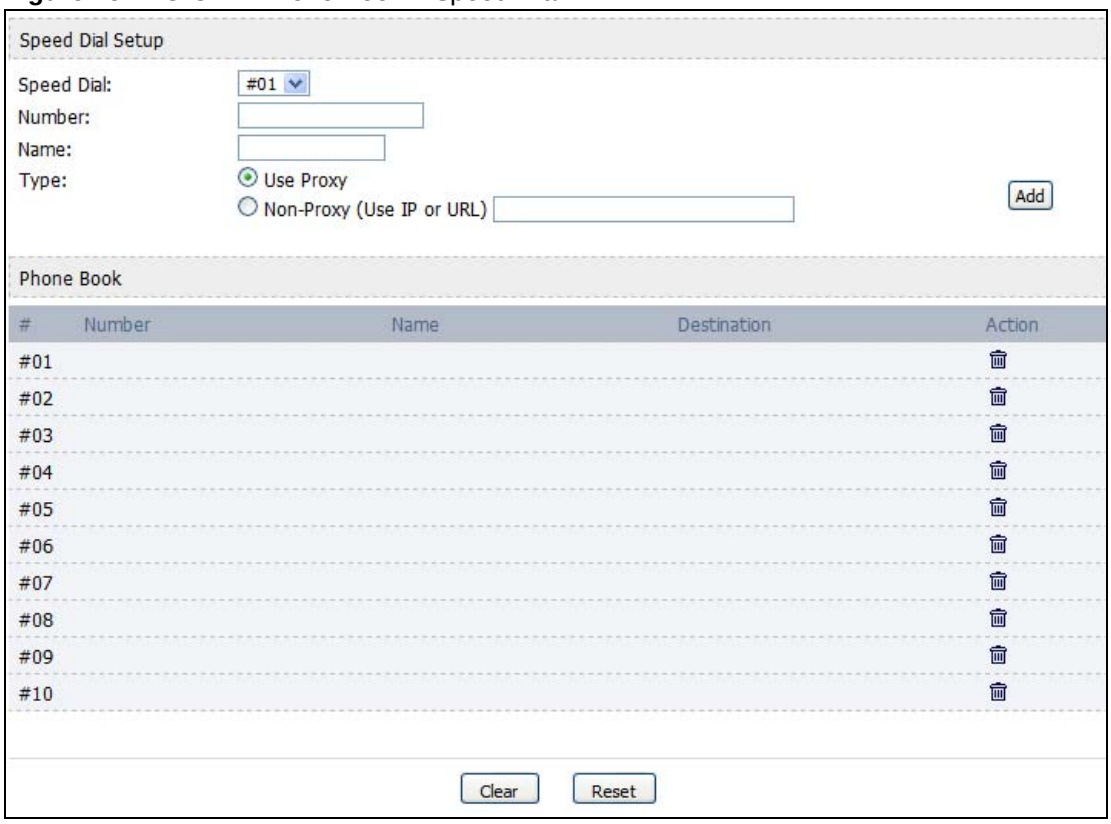
The WiMAX Modem checks the Advanced rules first before checking the Forward to Number rules. All rules are checked in order from top to bottom.

# 13.3 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 75** VOICE > Phone Book > Speed Dial




The following table describes the icons in this screen.

**Table 56** Advanced> LAN Configuration > IP Static Route

| ICON | DESCRIPTION |
|---|---|
| | Delete<br>Click to delete this item. |

The following table describes the labels in this screen.

**Table 57** 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. |

**Table 57** VOICE > Phone Book > Speed Dial

| LABEL | DESCRIPTION |
|---|---|
| Type | Select **Use Proxy** if you want to use one of your SIP accounts to call this phone number.<br>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

# 14

# The Certificates Screens

## 14.1 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.

### 14.1.1 What You Can Do in This Chapter

- The **My Certificates** screen (Section 14.2 on page 142) 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 14.3 on page 150) lets you display a summary list of certificates of the certification authorities that you have set the WiMAX Modem to accept as trusted.

### 14.1.2 What You Need to Know

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

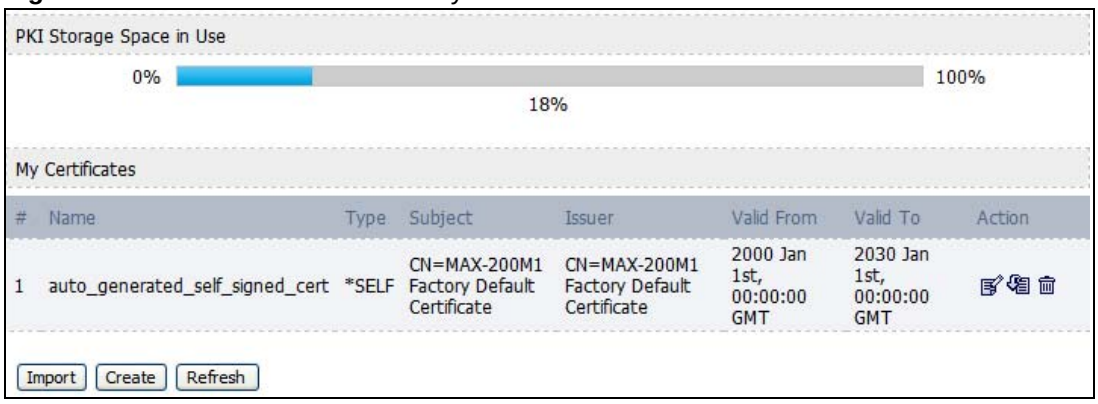
#### Certificate Authorities

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.

## 14.2 My Certificates

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

**Figure 76** TOOLS > Certificates > My Certificates




The following table describes the icons in this screen.

**Table 58** TOOLS > Certificates > My Certificates

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

The following table describes the labels in this screen.

**Table 59** 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. |
| Name | This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name. |
| Type | This field displays what kind of certificate this is.<br>**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.<br>**SELF** represents a self-signed certificate.<br>***SELF** represents the default self-signed certificate which signs the imported remote host certificates.<br>**CERT** represents a certificate issued by a certification authority. |

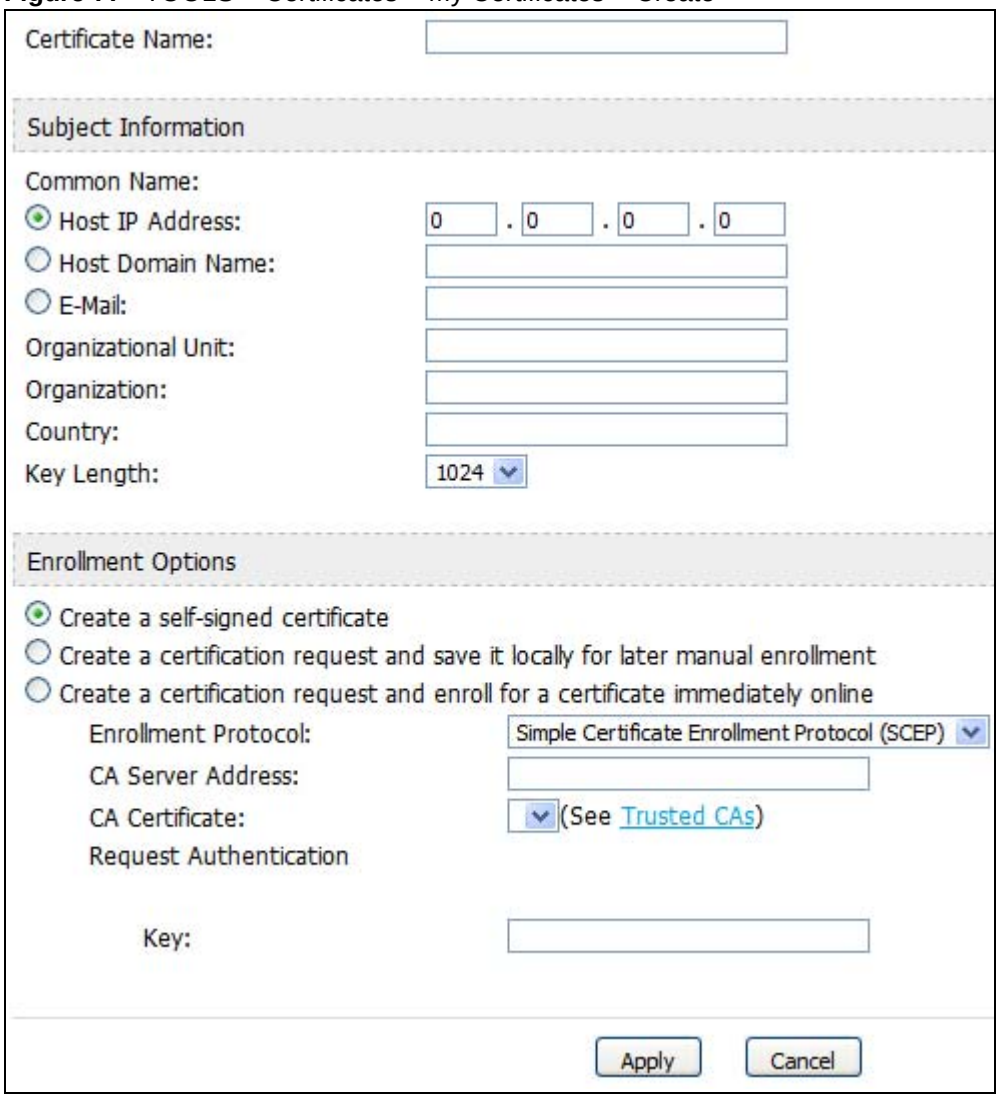
**Table 59** TOOLS > Certificates > My Certificates (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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 | Click the **Edit** icon to open a screen with an in-depth list of information about the certificate.<br>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**.<br>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.<br>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.<br>You cannot delete certificates that any of the WiMAX Modem's features are configured to use. |
| 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. |

### 14.2.1 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 77** TOOLS > Certificates > My Certificates > Create




The following table describes the labels in this screen.

**Table 60** 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. |

**Table 60** TOOLS > Certificates > My Certificates > Create

| LABEL | DESCRIPTION |
|---|---|
| Common Name | 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.<br>A domain name can be up to 255 characters. You can use alphanumeric characters, the hyphen and periods.<br>An e-mail address can be up to 63 characters. You can use alphanumeric characters, the hyphen, the @ symbol, periods and the underscore. |
| 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 | 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.<br>Copy the certification request from the **My Certificate Details** screen and then send it to the certification authority. |
| Create a certification request and enroll for a certificate immediately online | 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.<br>You must have the certification authority's certificate already imported in the **Trusted CAs** screen.<br>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. |
| Enrollment Protocol | 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.<br>**Simple Certificate Enrollment Protocol (SCEP)** is a TCP-based enrollment protocol that was developed by VeriSign and Cisco.<br>**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. |

**Table 60** TOOLS > Certificates > My Certificates > Create

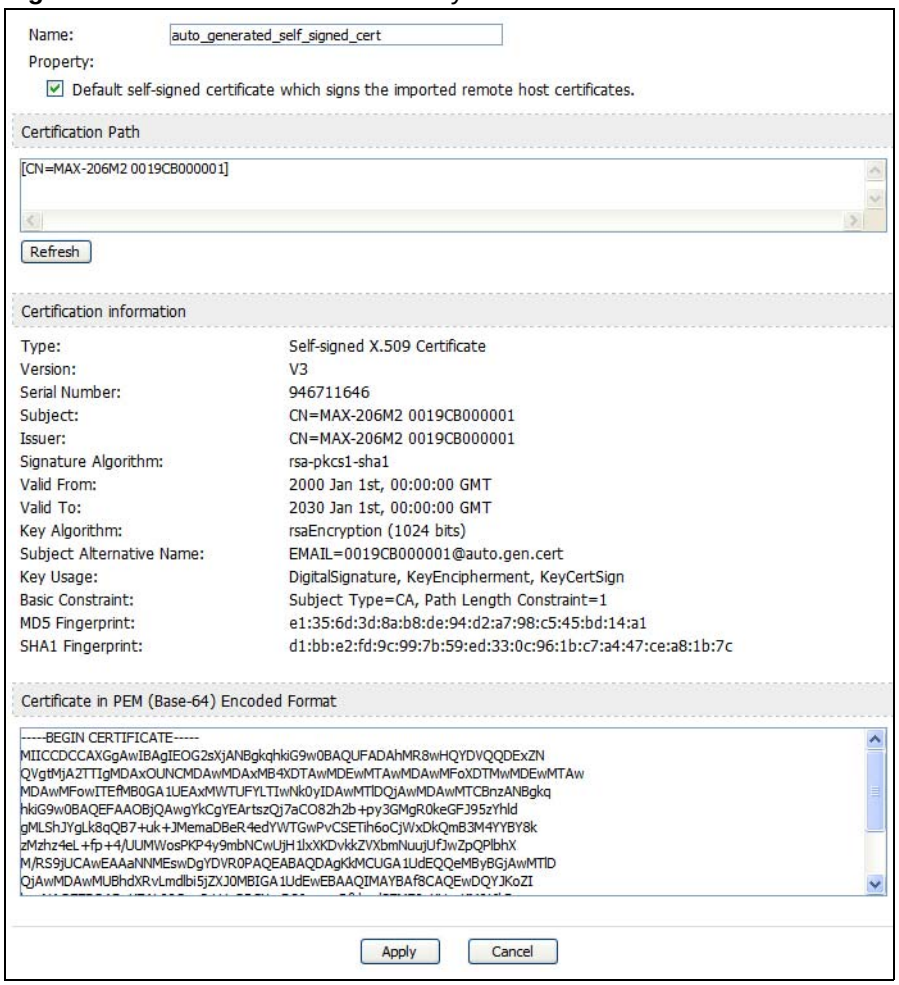
| LABEL | DESCRIPTION |
|---|---|
| CA Server Address | This field applies when you select **Create a certification request and enroll for a certificate immediately online**. Enter the IP address (or URL) of the certification authority server.<br>For a URL, you can use up to 511 of the following characters. a-zA-Z0-9'()+,/ :.=?;!*#@$_%- |
| CA Certificate | This field applies when you select **Create a certification request and enroll for a certificate immediately online**. Select the certification authority's certificate from the **CA Certificate** drop-down list box.<br>You must have the certification authority's certificate already imported in the **Trusted CAs** screen. Click **Trusted CAs** to go to the **Trusted CAs** screen where you can view (and manage) the WiMAX Modem's list of certificates of trusted certification authorities. |
| Request Authentication | When you select **Create a certification request and enroll for a certificate immediately online**, the certification authority may want you to include a reference number and key to identify you when you send a certification request.<br>Fill in both the **Reference Number** and the **Key** fields if your certification authority uses CMP enrollment protocol. Just the **Key** field displays if your certification authority uses the SCEP enrollment protocol.<br>For the reference number, use 0 to 99999999.<br>For the key, use up to 31 of the following characters. a-zA-Z0-9;\|`~!@#$%^&*()_+\{}':,./<>=- |
| 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.

## 14.2.2 My Certificate Edit

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

**Figure 78** TOOLS > Certificates > My Certificates > Edit




The following table describes the labels in this screen.

**Table 61** 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 61** TOOLS > Certificates > My Certificates > Edit

| LABEL | DESCRIPTION |
|---|---|
| Certification Path | This field displays for a certificate, not a certification request.<br>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).<br>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. |
| 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 | This field displays identifying information about the certificate’s issuing certification authority, such as Common Name, Organizational Unit, Organization and Country.<br>With self-signed certificates, this is the same as the **Subject Name** field.<br>“none” displays for a certification request. |
| 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). |
| 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. |

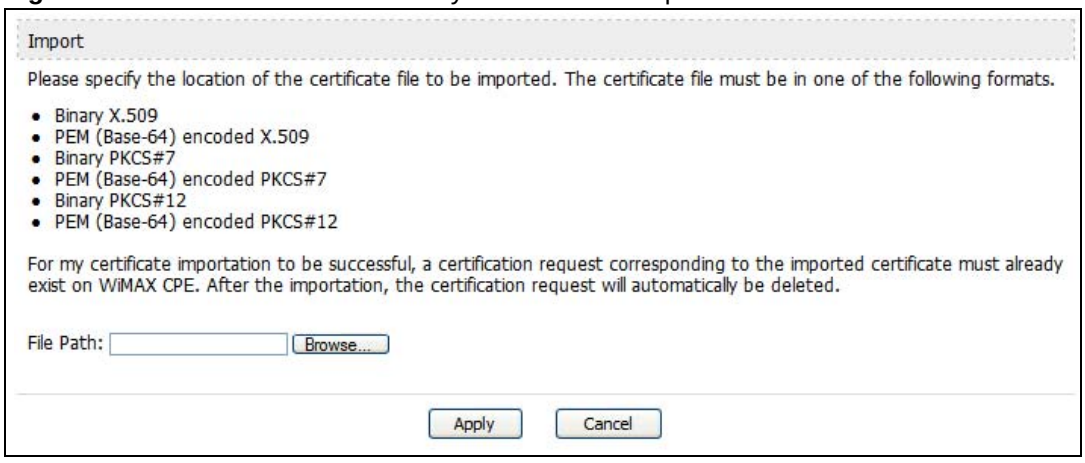
**Table 61** TOOLS > Certificates > My Certificates > Edit

| LABEL | DESCRIPTION |
|---|---|
| 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 | 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.<br>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.<br>You can copy and paste a certificate into an e-mail to send to friends or colleagues or you can copy and paste a certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example). |
| Apply | Click to save your changes. |
| Cancel | Click to return to the previous screen without saving your changes. |

## 14.2.3 My Certificate Import

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

**Figure 79** TOOLS > Certificates > My Certificates > Import




The following table describes the labels in this screen.

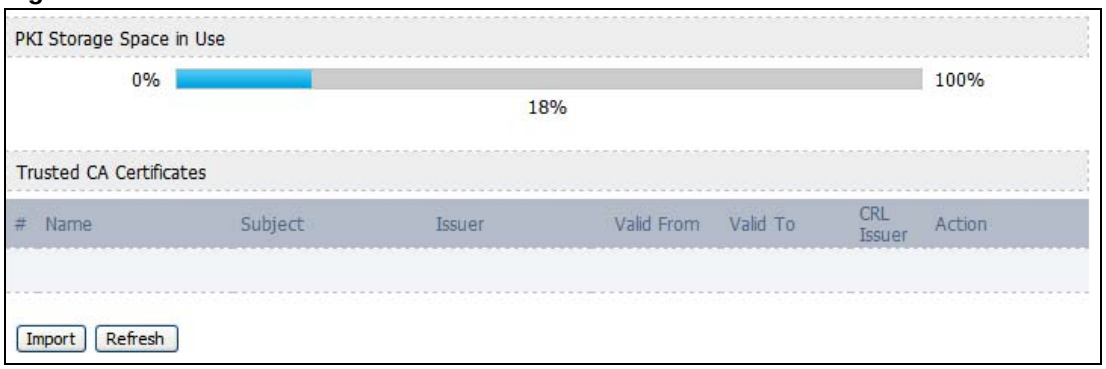
**Table 62** TOOLS > Certificates > My Certificates > Import

| LABEL | DESCRIPTION |
|---|---|
| File Path | Type in the location of the file you want to upload in this field or click **Browse** to find it.<br>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. |

## 14.3 Trusted CAs

Click **TOOLS** > **Certificates** > **Trusted CAs** to display a summary list of certificates of the certification authorities that you have set the WiMAX 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 80** TOOLS > Certificates > Trusted CAs




The following table describes the icons in this screen.

**Table 63** TOOLS > Certificates > Trusted CAs

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

The following table describes the labels in this screen.

**Table 64** 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. |
| 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. |

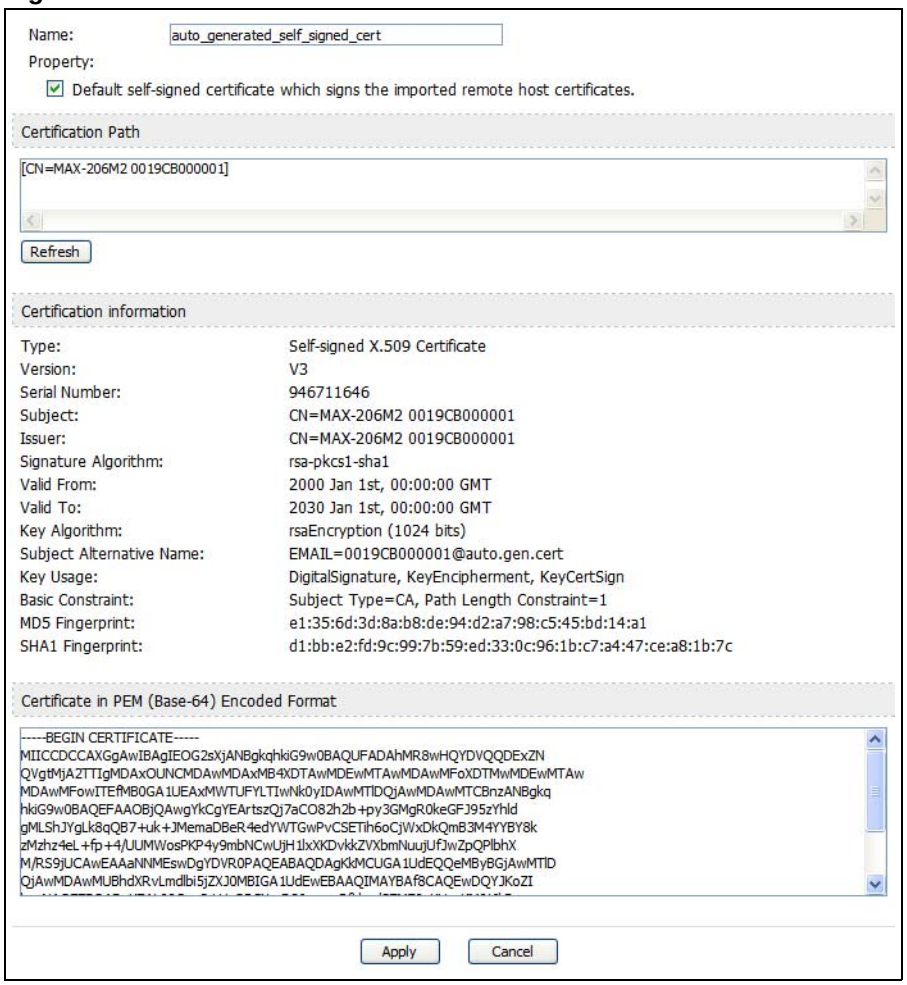
**Table 64** TOOLS > Certificates > Trusted CAs (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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 | Click the **Edit** icon to open a screen with an in-depth list of information about the certificate.<br>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**.<br>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. |
| 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. |

## 14.3.1 Trusted CA Edit

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

**Figure 81** TOOLS > Certificates > Trusted CAs > Edit




The following table describes the labels in this screen.

**Table 65** 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 65** TOOLS > Certificates > Trusted CAs > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Certification Path | This field displays for a certificate, not a certification request.<br>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).<br>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. |
| 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 | This field displays identifying information about the certificate’s issuing certification authority, such as Common Name, Organizational Unit, Organization and Country.<br>With self-signed certificates, this is the same as the **Subject Name** field.<br>“none” displays for a certification request. |
| 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). |
| 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. |

**Table 65** TOOLS > Certificates > Trusted CAs > Edit (continued)

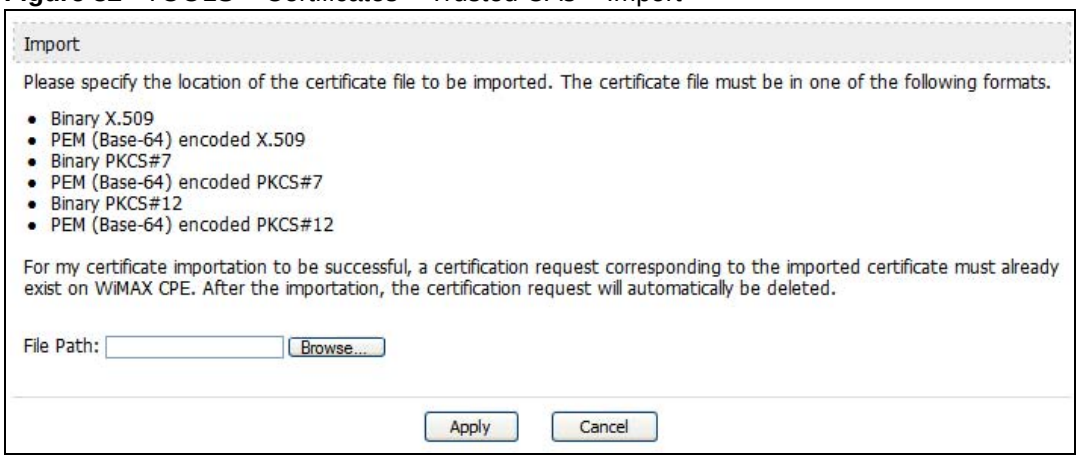
| LABEL | DESCRIPTION |
|---|---|
| MD5 Fingerprint | This is the certificate's message digest that the WiMAX Modem calculated using the MD5 algorithm. |
| SHA1 Fingerprint | This is the certificate's message digest that the WiMAX Modem calculated using the SHA1 algorithm. |
| Certificate in PEM (Base-64) Encoded Format | 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.<br>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.<br>You can copy and paste a certificate into an e-mail to send to friends or colleagues or you can copy and paste a certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example). |
| Apply | Click to save your changes. |
| Cancel | Click to return to the previous screen without saving your changes. |

## 14.3.2 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.

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

**Figure 82** TOOLS > Certificates > Trusted CAs > Import



The following table describes the labels in this screen.

**Table 66** 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. |

## 14.4 Technical Reference

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

### 14.4.1 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).

#### 14.4.1.1 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.

#### 14.4.1.2 Self-signed Certificates

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

#### 14.4.1.3 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.

#### 14.4.1.4 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.

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.

## 14.4.2 Verifying a Certificate

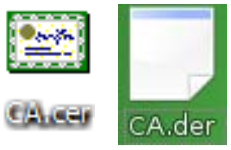
Before you import a certificate into the WiMAX Modem, you should verify that you have the correct certificate. This is especially true of trusted certificates since the WiMAX Modem also trusts any valid certificate signed by any of the imported trusted certificates.

### 14.4.2.1 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.

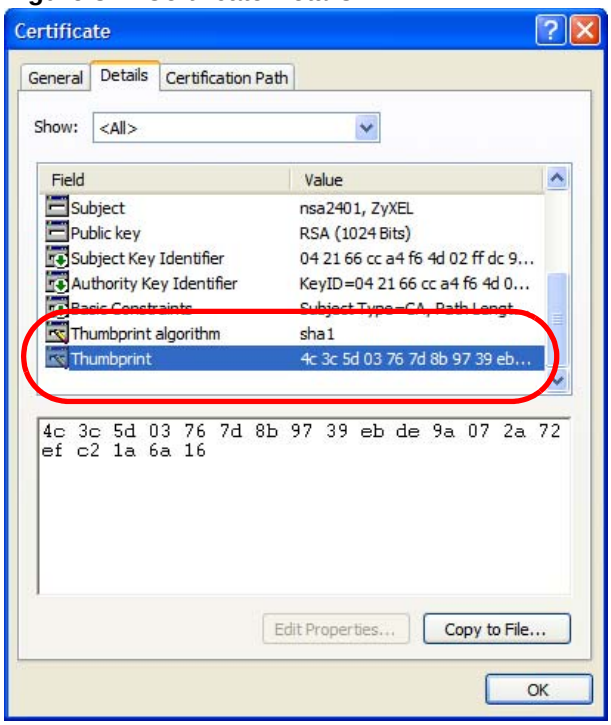
1. Browse to where you have the certificate saved on your computer.
2. Make sure that the certificate has a ".cer" or ".crt" file name extension. (On some Linux distributions, the file extension may be ".der".)

**Figure 83** 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 84** 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 very based on your situation. Possible examples would be over the telephone or through an HTTPS connection.

# 15

# The Firewall Screens

## 15.1 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.

### 15.1.1 What You Can Do in This Chapter

- The **Firewall Setting** screen (Section 15.2 on page 160) lets you configure the basic settings for your firewall.
- The **Service Setting** screen (Section 15.3 on page 163) 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.

### 15.1.2 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.

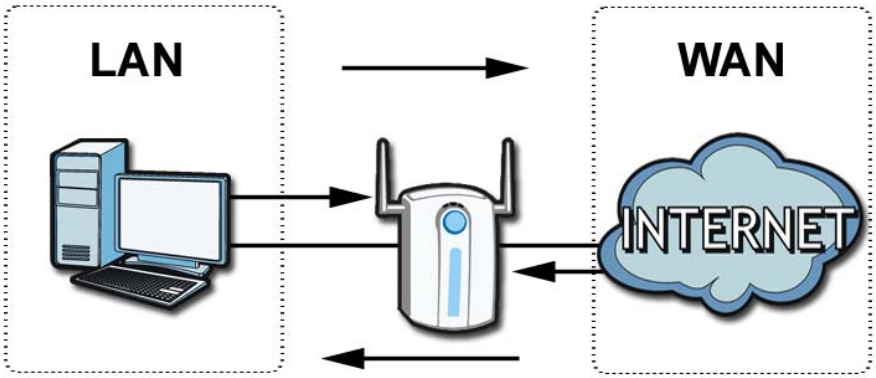
The WiMAX Modem has one Ethernet (LAN) port. The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers will have access to Internet services such as e-mail, FTP and the World Wide Web. However, “inbound access” is not allowed (by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

## 15.2 Firewall Setting

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

### 15.2.1 Firewall Rule Directions

**Figure 85** 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.

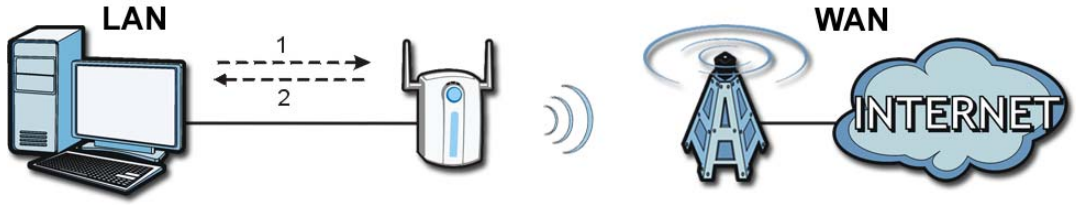
- Configuring **WAN** or **LAN & WAN** access for services in the **Remote MGMT** screens or SMT menus. When you allow remote management from the WAN, you are actually configuring WAN-to-WAN/WiMAX Modem firewall rules. WAN-to-WAN/WiMAX Modem firewall rules are Internet to the WiMAX Modem WAN interface 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.

## 15.2.2 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.

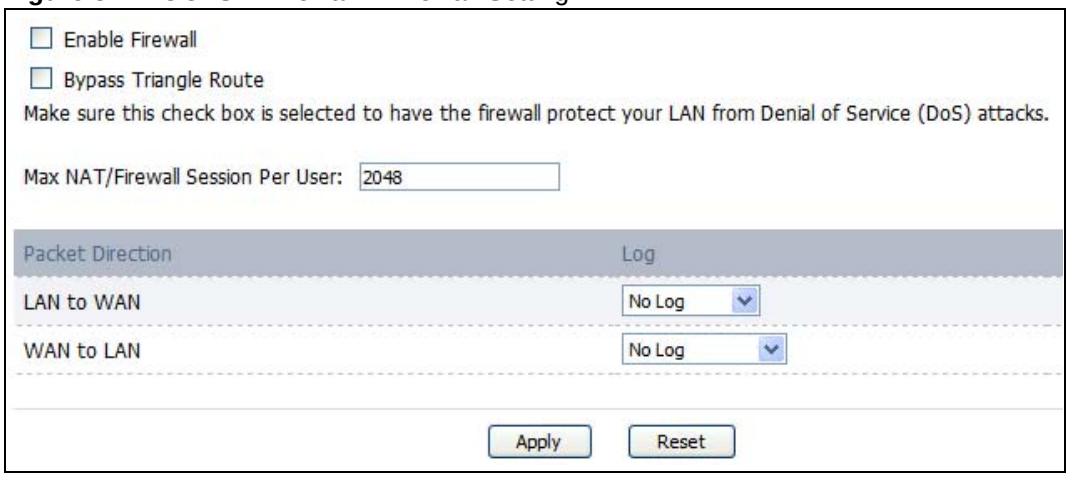
**Figure 86** Ideal Firewall Setup




## 15.2.3 Firewall Setting Options

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

**Figure 87** TOOLS > Firewall > Firewall Setting



The following table describes the labels in this screen.

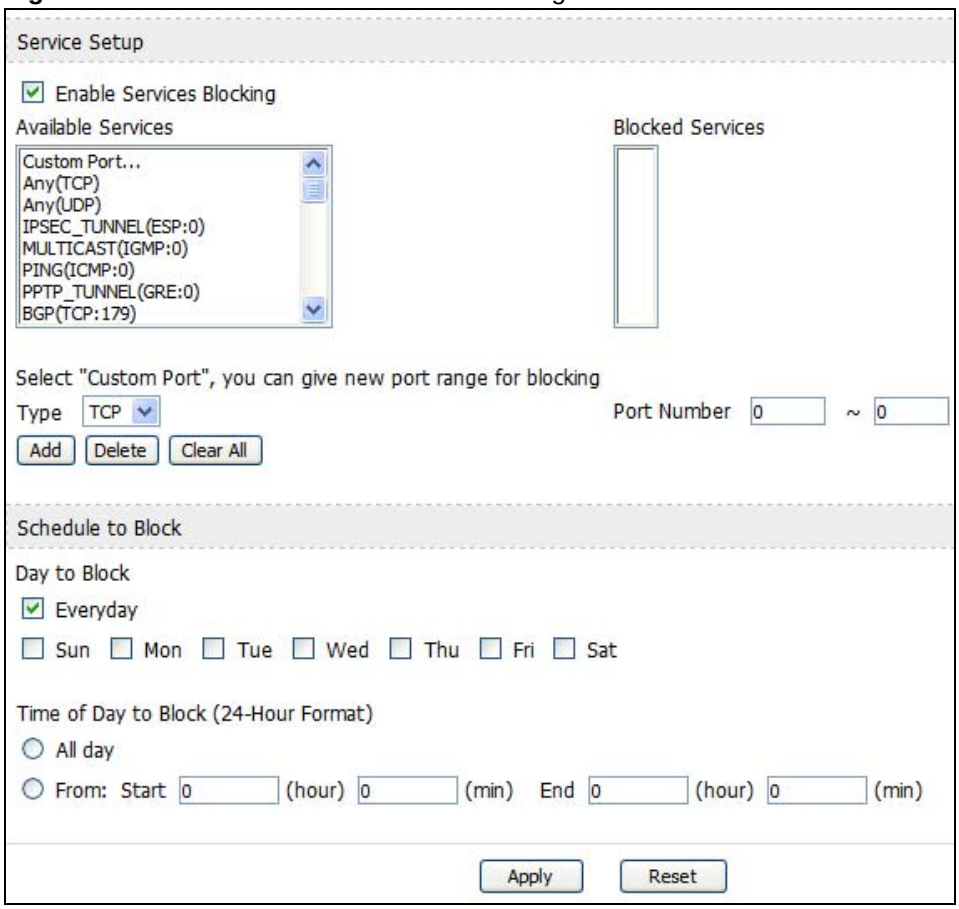
**Table 67** TOOLS > Firewall > Firewall Setting

| 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 **Network > NAT > General**. |
| Packet Direction | |
| Log | Select the situations in which you want to create log entries for firewall events.<br>**No Log** - do not create any log entries<br>**Log Blocked** - (**LAN to WAN** only) create log entries when packets are blocked<br>**Log Forwarded -** (**WAN to LAN** only) create log entries when packets are forwarded<br>**Log All** - create log entries for every packet |
| Apply | Click to save your changes. |
| Reset | Click to restore your previously saved settings. |

## 15.3 Service Setting

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

**Figure 88** TOOLS > Firewall > Service Setting




The following table describes the labels in this screen.

**Table 68** 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.<br>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. |
| 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. |

**Table 68** TOOLS > Firewall > Service Setting (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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. |

## 15.4 Technical Reference

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

### 15.4.1 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.

### 15.4.2 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.

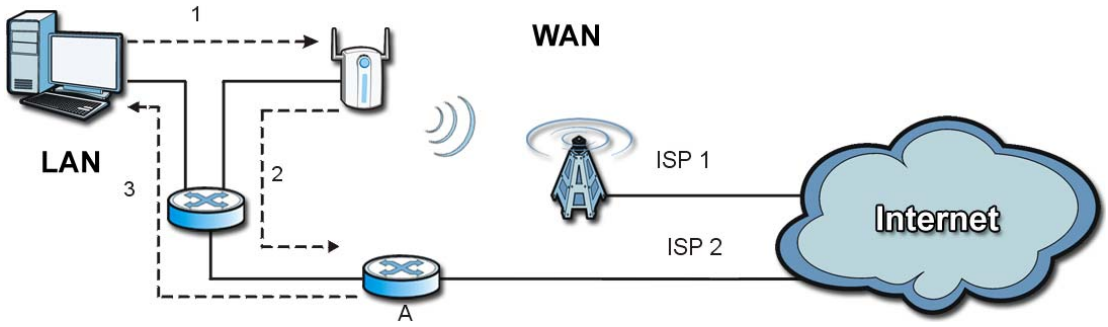
## 15.4.3 The “Triangle Route” Problem

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 89** “Triangle Route” Problem




### 15.4.3.1 Solving the “Triangle Route” Problem

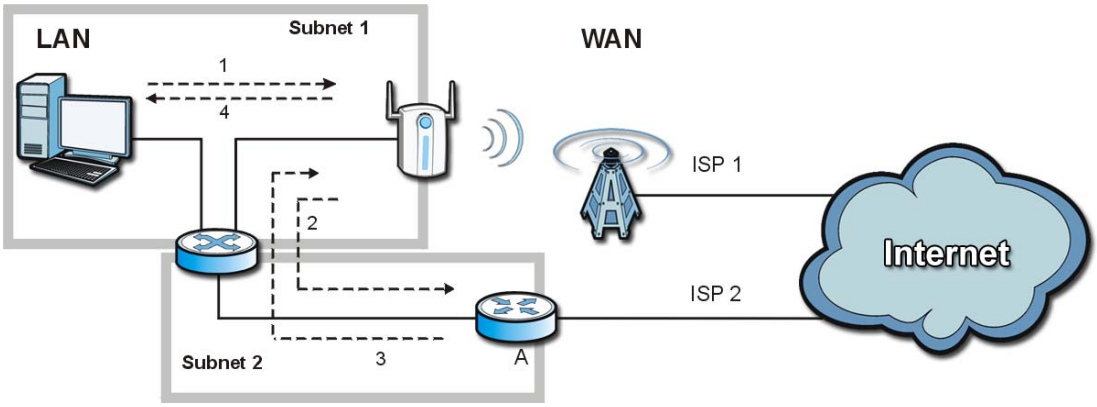
If you have the WiMAX Modem allow triangle route sessions, traffic from the WAN can go directly to a LAN computer without passing through the WiMAX Modem and its firewall protection.

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 90** IP Alias



# 16

# Content Filter

## 16.1 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.

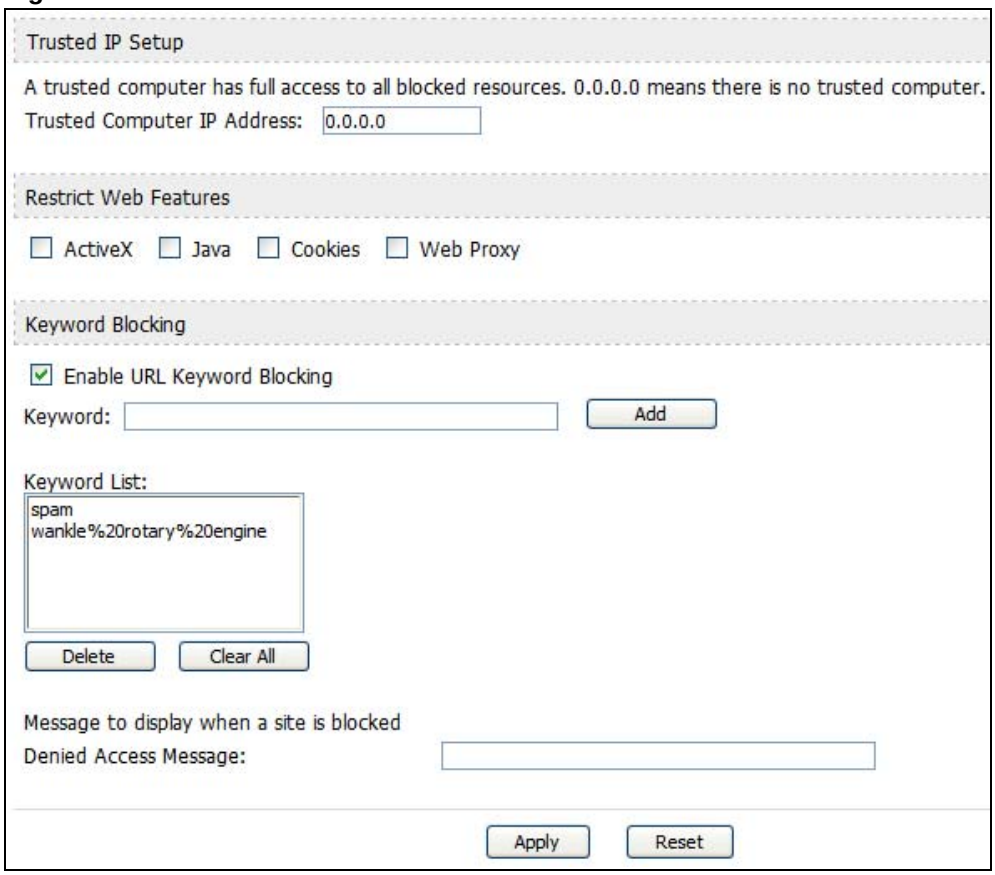
### 16.1.1 What You Can Do in This Chapter

- The **Filter** screen (Section 16.2 on page 168) 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 16.3 on page 170) lets you schedule content filtering.

## 16.2 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 91** TOOLS > Content Filter > Filter



The following table describes the labels in this screen.

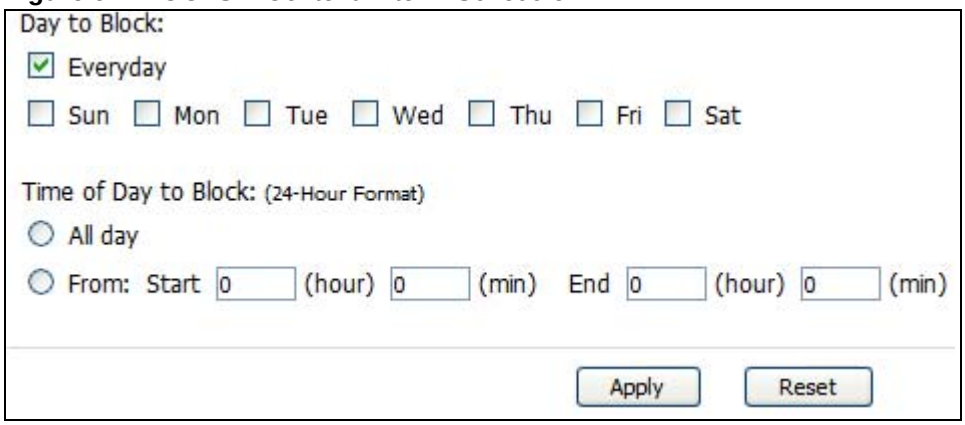
**Table 69** TOOLS > Content Filter > Filter

| 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.<br>**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.<br>**Java** - This is used to build downloadable Web components or Internet and intranet business applications of all kinds.<br>**Cookies** - This is used by Web servers to track usage and to provide service based on ID.<br>**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 64 printable ASCII characters. There is no wildcard character, however. |
| Add | Click this to add the specified **Keyword** to the **Keyword List**. You can enter up to 64 keywords. |
| Keyword List | This field displays the keywords that are blocked when **Enable URL Keyword Blocking** is selected. To delete a keyword, select it, click **Delete**, and click **Apply**. |
| Delete | Click **Delete** to remove the selected keyword in the **Keyword List**. The keyword disappears after you click **Apply**. |
| Clear All | Click this button to remove all of the keywords in the **Keyword List**. |
| Denied Access Message | Enter the message that is displayed when the WiMAX 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. |

## 16.3 Schedule

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

**Figure 92** TOOLS > Content Filter > Schedule




The following table describes the labels in this screen.

**Table 70** 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. |

# 17

# The Remote Management Screens

## 17.1 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 71** Remote Management

- Internet (WAN only)
- LAN only
- ALL (LAN and WAN)
- 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

### 17.1.1 What You Can Do in This Chapter

- The **WWW** screen (Section 17.2 on page 173) lets you control HTTP access to your WiMAX Modem.
- The **Telnet** screen (Section 17.3 on page 173) lets you control Telnet access to your WiMAX Modem.
- The **FTP** screen (Section 17.4 on page 174) lets you control FTP access to your WiMAX Modem.
- The **SNMP** screen (Section 17.5 on page 175) lets you control SNMP access to your WiMAX Modem.
- The **DNS** screen (Section 17.6 on page 177) lets you control DNS access to your WiMAX Modem.
- The **Security** screen (Section 17.7 on page 178) lets you control how your WiMAX Modem responds to other types of requests.

## 17.1.2 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.

SNMP is only available if TCP/IP is configured.

## 17.2 WWW

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

**Figure 93** TOOLS > Remote Management > WWW


The following table describes the labels in this screen.

**Table 72** 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.<br>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. |

## 17.3 Telnet

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

**Figure 94** TOOLS > Remote Management > Telnet

The following table describes the labels in this screen.

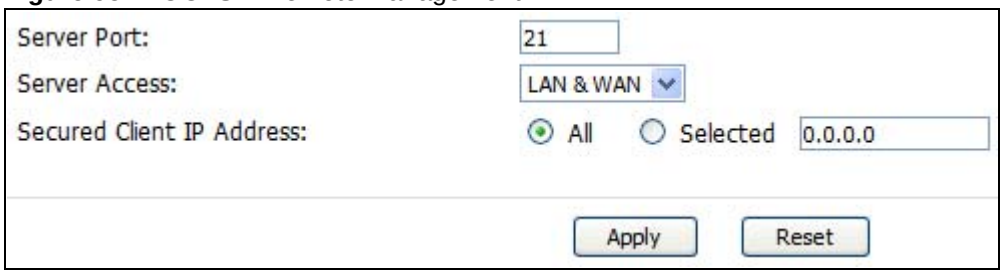
**Table 73** TOOLS > Remote Management > Telnet

| 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.<br>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. |

## 17.4 FTP

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

**Figure 95** TOOLS > Remote Management > FTP




The following table describes the labels in this screen.

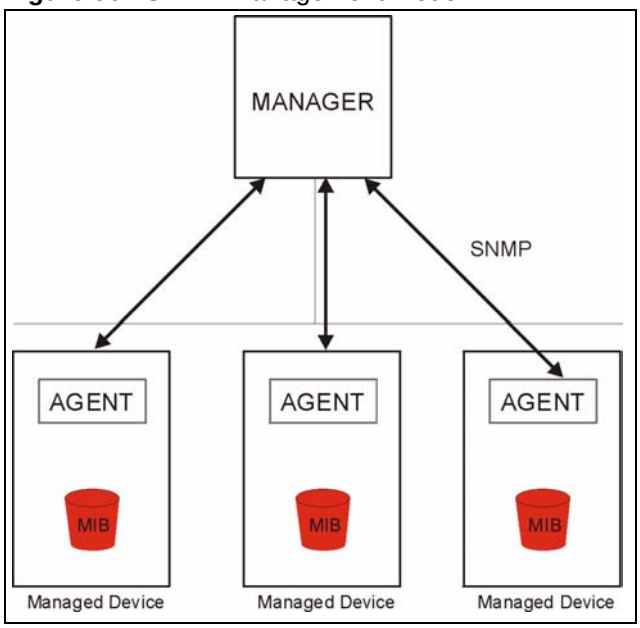
**Table 74** TOOLS > Remote Management > FTP

| 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.<br>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. |

## 17.5 SNMP

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

**Figure 96** 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.

## 17.5.1 SNMP Traps

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

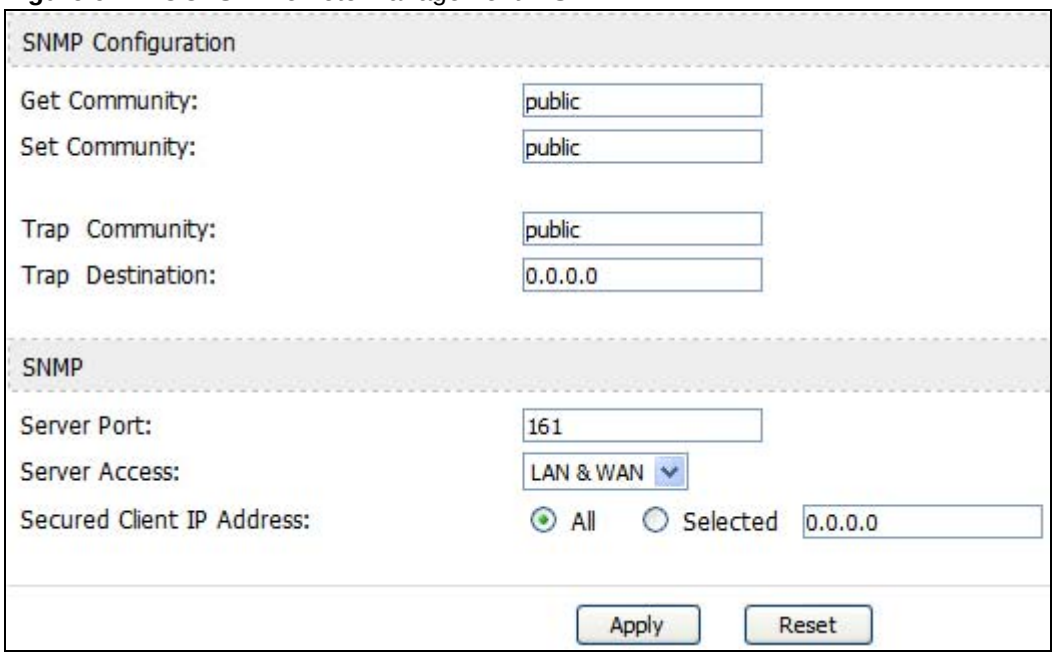
**Table 75** SNMP Traps

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

## 17.5.2 SNMP Options

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

**Figure 97** TOOLS > Remote Management > SNMP



The following table describes the labels in this screen.

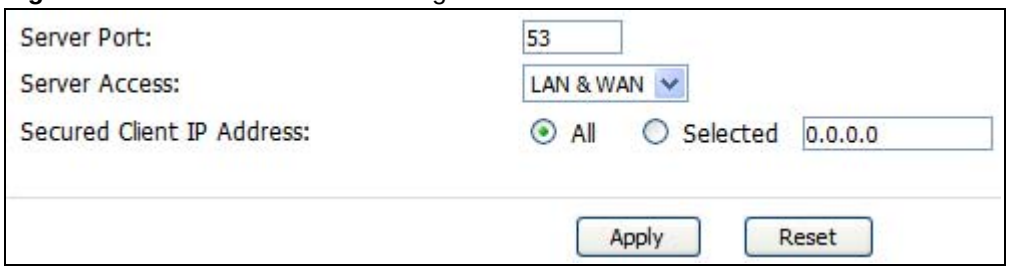
**Table 76** TOOLS > Remote Management > SNMP

| 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. |
| Secured Client IP | A secured client is a “trusted” computer that is allowed to communicate with the WiMAX Modem using this service.<br>Select **All** to allow any computer to access the WiMAX Modem using this service.<br>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. |

## 17.6 DNS

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

**Figure 98** TOOLS > Remote Management > DNS



The following table describes the labels in this screen.

**Table 77** 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.<br>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. |

## 17.7 Security

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

**Figure 99** TOOLS > Remote Management > Security


The following table describes the labels in this screen.

**Table 78** TOOLS > Remote Management > Security

| LABEL | DESCRIPTION |
|---|---|
| Respond to Ping on | Select the interface(s) on which the WiMAX Modem should respond to incoming ping requests.<br>• **Disable** - the WiMAX Modem does not respond to any ping requests.<br>• **LAN** - the WiMAX Modem only responds to ping requests received from the LAN.<br>• **WAN** - the WiMAX Modem only responds to ping requests received from the WAN.<br>• **LAN & WAN** - the WiMAX Modem responds to ping requests received from the LAN or the WAN. |
| Do not respond to requests for unauthorized services | 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.<br>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. |
| Apply | Click to save your changes. |
| Reset | Click to restore your previously saved settings. |

# 18

# 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 187.

### 18.1.1 What You Can Do in This Chapter

- The **View Logs** screen (Section 18.2 on page 183) lets you look at log entries and alerts.
- The **Log Settings** screen (Section 18.3 on page 185) 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 79** 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.

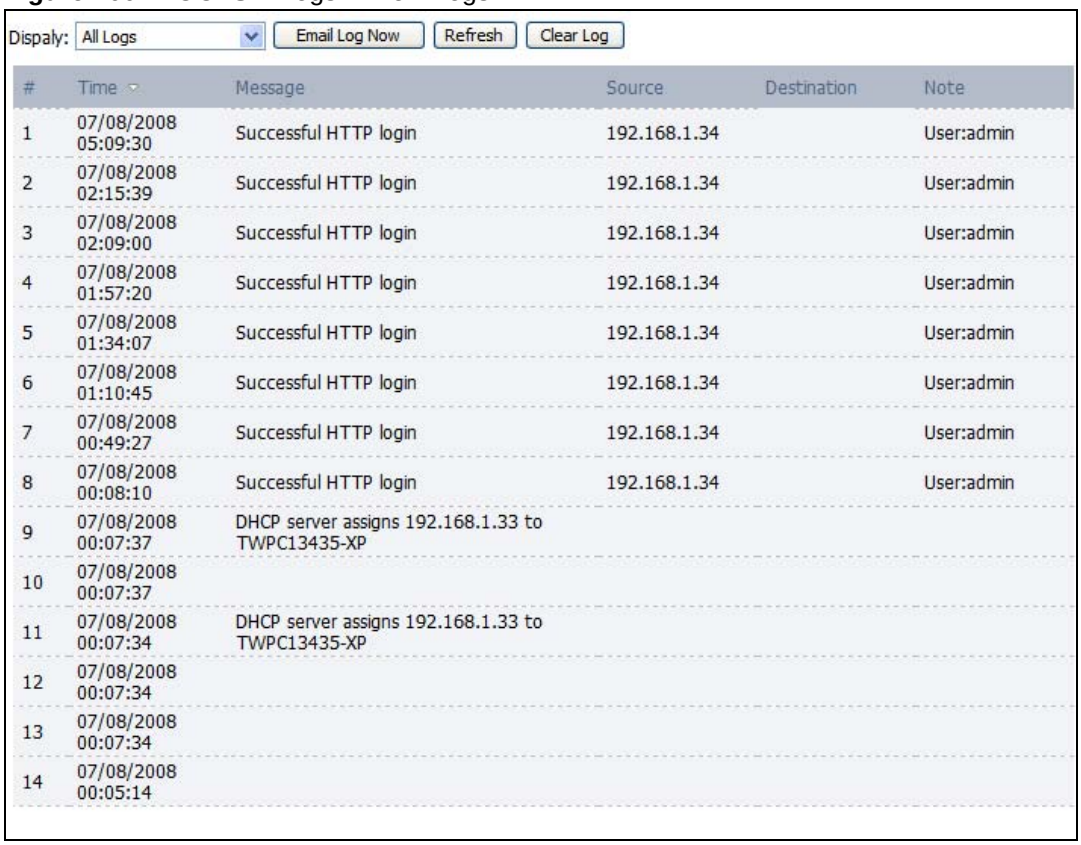
**Table 80** RFC-2408 ISAKMP Payload Types

| 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 |

## 18.2 View Logs

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

**Figure 100** TOOLS > Logs > View Logs




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

The following table describes the labels in this screen.

**Table 81** TOOLS > Logs > View Logs

| LABEL | DESCRIPTION |
|---|---|
| Display | Select a category whose log entries you want to view. To view all logs, select **All Logs**. The list of categories depends on what log categories are selected in the **Log Settings** page. |
| Email Log Now | Click this to send the log screen to the e-mail address specified in the **Log Settings** page. |
| Refresh | Click to renew the log screen. |
| Clear Log | Click to clear all the log entries, regardless of what is shown on the log screen. |
| # | The number of the item in this list. |
| Time | This field displays the time the log entry was recorded. |
| Message | This field displays the reason for the log entry. See Section 18.4 on page 187. |
| Source | This field displays the source IP address and the port number of the incoming packet. In many cases, some or all of this information may not be available. |

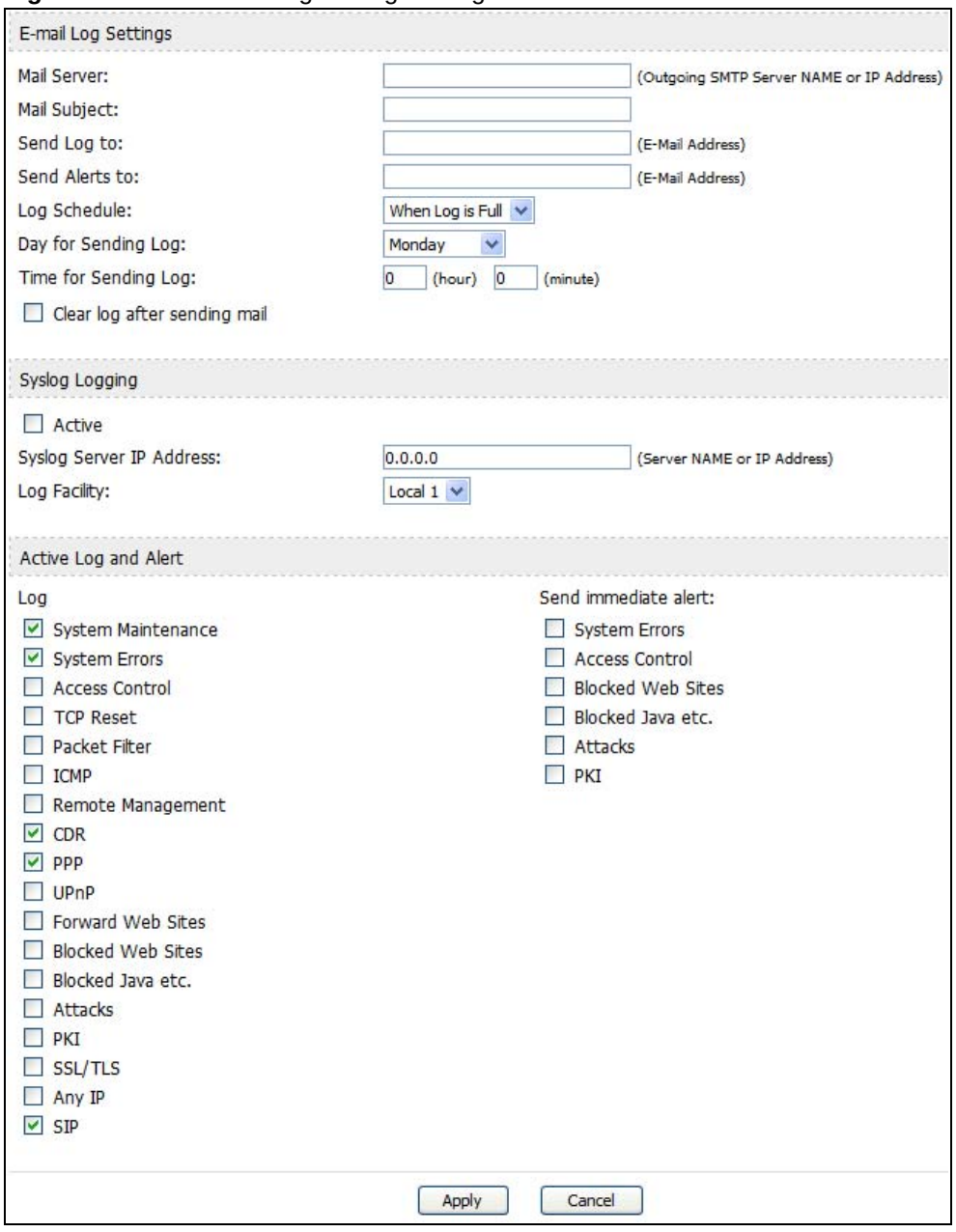
**Table 81** TOOLS > Logs > View Logs (continued)

| LABEL | DESCRIPTION |
|---|---|
| Destination | This field lists the destination IP address and the port number of the incoming packet. In many cases, some or all of this information may not be available. |
| Note | This field displays additional information about the log entry. |

# 18.3 Log Settings

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

**Figure 101** TOOLS > Logs > Log Settings



The following table describes the labels in this screen.

**Table 82** TOOLS > Logs > Log Settings

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

## 18.4 Log Message Descriptions

The following tables provide descriptions of example log messages.

**Table 83** System Error Logs

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

**Table 84** System Maintenance Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Time calibration is successful | The device has adjusted its time based on information from the time server. |
| Time calibration failed | The device failed to get information from the time server. |
| WAN interface gets IP: %s | The WAN interface got a new IP address from the DHCP or PPPoE server. |
| DHCP client gets %s | A DHCP client got a new IP address from the DHCP server. |
| DHCP client IP expired | A DHCP client's IP address has expired. |
| DHCP server assigns %s | The DHCP server assigned an IP address to a client. |
| Successful WEB login | Someone has logged on to the device's web configurator interface. |
| WEB login failed | Someone has failed to log on to the device's web configurator interface. |
| TELNET Login Successfully | Someone has logged on to the router via telnet. |
| TELNET Login Fail | Someone has failed to log on to the router via telnet. |
| Successful FTP login | Someone has logged on to the device via ftp. |
| FTP login failed | Someone has failed to log on to the device via ftp. |
| NAT Session Table is Full! | The maximum number of NAT session table entries has been exceeded and the table is full. |
| Time initialized by Daytime Server | The device got the time and date from the Daytime server. |
| Time initialized by Time server | The device got the time and date from the time server. |
| Time initialized by NTP server | The device got the time and date from the NTP server. |
| Connect to Daytime server fail | The device was not able to connect to the Daytime server. |
| Connect to Time server fail | The device was not able to connect to the Time server. |
| Connect to NTP server fail | The device was not able to connect to the NTP server. |
| Too large ICMP packet has been dropped | The device dropped an ICMP packet that was too large. |
| Configuration Change: PC = 0x%x, Task ID = 0x%x | The device is saving configuration changes. |

**Table 85** Access Control Logs

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

**Table 86** TCP Reset Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| `Under SYN flood attack, sent TCP RST` | The router sent a TCP reset packet when a host was under a SYN flood attack (the TCP incomplete count is per destination host.) |
| `Exceed TCP MAX incomplete, sent TCP RST` | The router sent a TCP reset packet when the number of TCP incomplete connections exceeded the user configured threshold. (the TCP incomplete count is per destination host.) |
| `Peer TCP state out of order, sent TCP RST` | The router sent a TCP reset packet when a TCP connection state was out of order.Note: The firewall refers to RFC793 Figure 6 to check the TCP state. |
| `Firewall session time out, sent TCP RST` | The router sent a TCP reset packet when a dynamic firewall session timed out.<br>The default timeout values are as follows:<br>ICMP idle timeout: 3 minutes<br>UDP idle timeout: 3 minutes<br>TCP connection (three way handshaking) timeout: 270 seconds<br>TCP FIN-wait timeout: 2 MSL (Maximum Segment Lifetime set in the TCP header).<br>TCP idle (established) timeout (s): 150 minutes<br>TCP reset timeout: 10 seconds |

**Table 86** TCP Reset Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| `Exceed MAX incomplete, sent TCP RST` | The router sent a TCP reset packet when the number of incomplete connections (TCP and UDP) exceeded the user-configured threshold. (Incomplete count is for all TCP and UDP connections through the firewall.)Note: When the number of incomplete connections (TCP + UDP) > “Maximum Incomplete High”, the router sends TCP RST packets for TCP connections and destroys TOS (firewall dynamic sessions) until incomplete connections < “Maximum Incomplete Low”. |
| `Access block, sent TCP RST` | The router sends a TCP RST packet and generates this log if you turn on the firewall TCP reset mechanism (via CI command: `sys firewall tcprst`). |

**Table 87** Packet Filter Logs

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

For type and code details, see Table 94 on page 192.

**Table 88** ICMP Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| `Firewall default policy: ICMP <Packet Direction>, <type:%d>, <code:%d>` | ICMP access matched the default policy and was blocked or forwarded according to the user's setting. |
| `Firewall rule [NOT] match: ICMP <Packet Direction>, <rule:%d>, <type:%d>, <code:%d>` | ICMP access matched (or didn’t match) a firewall rule (denoted by its number) and was blocked or forwarded according to the rule. |
| `Triangle route packet forwarded: ICMP` | The firewall allowed a triangle route session to pass through. |
| `Packet without a NAT table entry blocked: ICMP` | The router blocked a packet that didn’t have a corresponding NAT table entry. |
| `Unsupported/out-of-order ICMP: ICMP` | The firewall does not support this kind of ICMP packets or the ICMP packets are out of order. |
| `Router reply ICMP packet: ICMP` | The router sent an ICMP reply packet to the sender. |

**Table 89** PPP Logs

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

**Table 89** PPP Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| ppp:LCP Closing | The PPP connection's Link Control Protocol stage is closing. |
| ppp:IPCP Closing | The PPP connection's Internet Protocol Control Protocol stage is closing. |

**Table 90** UPnP Logs

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

**Table 91** Content Filtering Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| %s: Keyword blocking | The content of a requested web page matched a user defined keyword. |
| %s: Not in trusted web list | The web site is not in a trusted domain, and the router blocks all traffic except trusted domain sites. |
| %s: Forbidden Web site | The web site is in the forbidden web site list. |
| %s: Contains ActiveX | The web site contains ActiveX. |
| %s: Contains Java applet | The web site contains a Java applet. |
| %s: Contains cookie | The web site contains a cookie. |
| %s: Proxy mode detected | The router detected proxy mode in the packet. |
| %s: Trusted Web site | The web site is in a trusted domain. |
| %s | When the content filter is not on according to the time schedule: |
| Waiting content filter server timeout | The external content filtering server did not respond within the timeout period. |
| DNS resolving failed | The WiMAX Modem cannot get the IP address of the external content filtering via DNS query. |
| Creating socket failed | The WiMAX Modem cannot issue a query because TCP/UDP socket creation failed, port:port number. |
| Connecting to content filter server fail | The connection to the external content filtering server failed. |
| License key is invalid | The external content filtering license key is invalid. |

For type and code details, see Table 94 on page 192.

**Table 92** Attack Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| attack [ TCP \| UDP \| IGMP \| ESP \| GRE \| OSPF ] | The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF attack. |
| attack ICMP (type:%d, code:%d) | The firewall detected an ICMP attack. |

**Table 92** Attack Logs (continued)

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

**Table 93** Remote Management Logs

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

**Table 94** ICMP Notes

| TYPE | CODE | DESCRIPTION |
|---|---|---|
| 0 | | Echo Reply |
| | 0 | Echo reply message |
| 3 | | Destination Unreachable |
| | 0 | Net unreachable |
| | 1 | Host unreachable |
| | 2 | Protocol unreachable |
| | 3 | Port unreachable |
| | 4 | A packet that needed fragmentation was dropped because it was set to Don't Fragment (DF) |
| | 5 | Source route failed |
| 4 | | Source Quench |
| | 0 | A gateway may discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network. |
| 5 | | Redirect |
| | 0 | Redirect datagrams for the Network |
| | 1 | Redirect datagrams for the Host |
| | 2 | Redirect datagrams for the Type of Service and Network |
| | 3 | Redirect datagrams for the Type of Service and Host |
| 8 | | Echo |
| | 0 | Echo message |
| 11 | | Time Exceeded |

**Table 94** ICMP Notes (continued)

| TYPE | CODE | DESCRIPTION |
|---|---|---|
| | 0 | Time to live exceeded in transit |
| | 1 | Fragment reassembly time exceeded |
| 12 | | Parameter Problem |
| | 0 | Pointer indicates the error |
| 13 | | Timestamp |
| | 0 | Timestamp request message |
| 14 | | Timestamp Reply |
| | 0 | Timestamp reply message |
| 15 | | Information Request |
| | 0 | Information request message |
| 16 | | Information Reply |
| | 0 | Information reply message |

**Table 95** SIP Logs

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

**Table 96** RTP Logs

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

**Table 97** FSM Logs: Caller Side

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

**Table 98** FSM Logs: Callee Side

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

**Table 99** Lifeline Logs

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

# 19

# The UPnP Screen

## 19.1 Overview

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

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

### 19.1.1 What You Can Do in This Chapter

The **UPnP** screen (Section 19.2 on page 196) lets you enable the UPnP feature in your WiMAX Modem.

### 19.1.2 What You Need to Know

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

#### How do I know if I'm using UPnP?

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

#### NAT Traversal

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

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

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

See Chapter 9 on page 93 for further information about NAT.

### Cautions with UPnP

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

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

### UPnP and ZyXEL

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

The WiMAX Modem only sends UPnP multicasts to the LAN.

## 19.2 UPnP

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

**Figure 102** TOOLS > UPnP


The following table describes the labels in this screen.

**Table 100** TOOLS > UPnP

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

## 19.3 Technical Reference

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

### 19.3.1 Installing UPnP in Windows XP

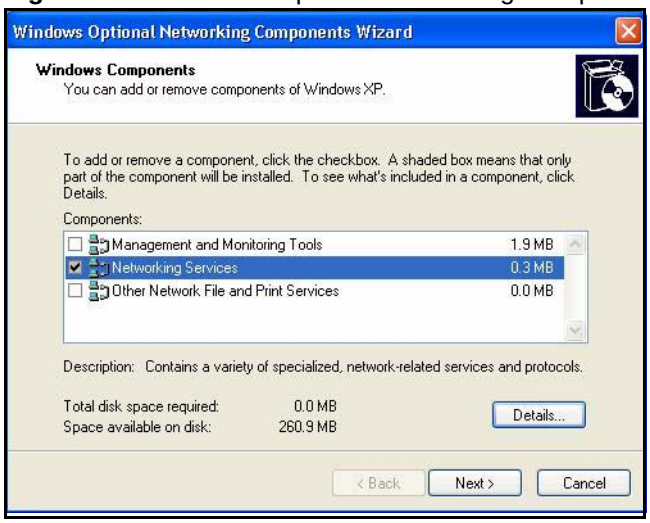
Follow the steps below to install the UPnP in Windows XP.

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

**Figure 103** Network Connections

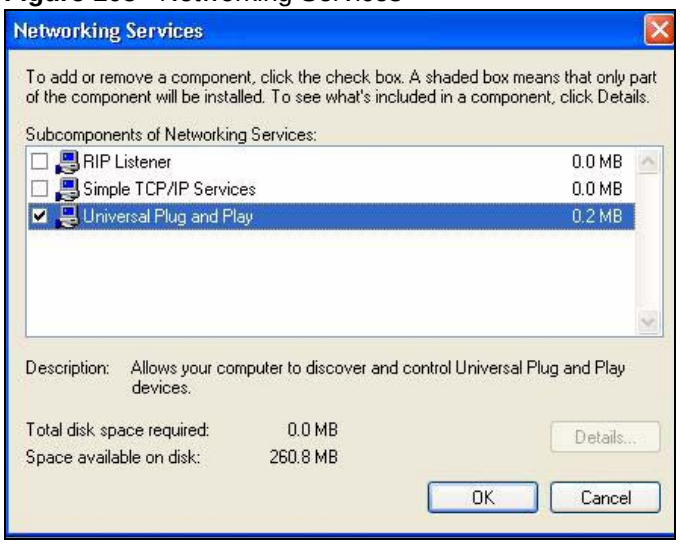

4. The **Windows Optional Networking Components Wizard** window displays. Select **Networking Service** in the **Components** selection box and click **Details**.

**Figure 104** Windows Optional Networking Components Wizard




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

**Figure 105** Networking Services




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

### 19.3.1.1 Auto-discover Your UPnP-enabled Network Device in Windows XP

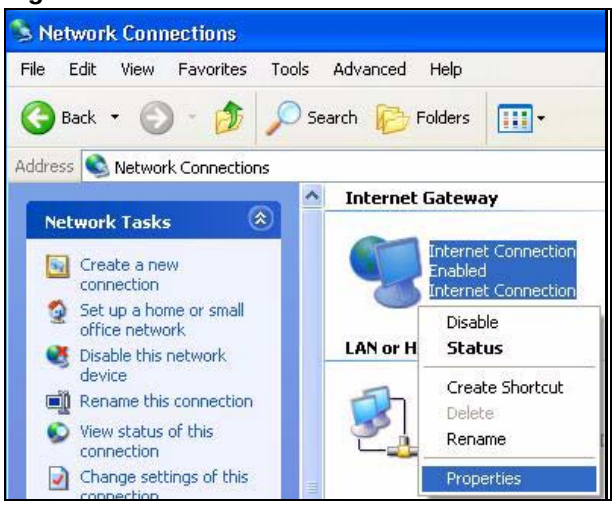
This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the WiMAX Modem.

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

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

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

**Figure 106** Network Connections



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

**Figure 107** Internet Connection Properties


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

**Figure 108** Internet Connection Properties: Advanced Settings

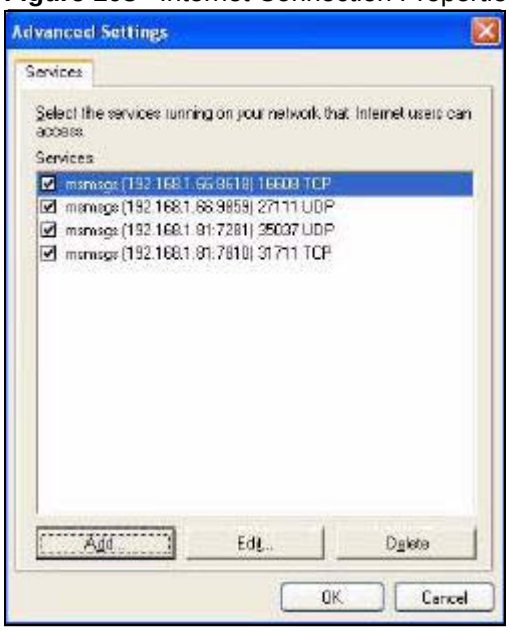
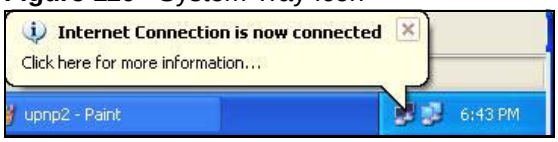


**Figure 109** Internet Connection Properties: Advanced Settings: Add


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

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

**Figure 110** System Tray Icon




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

**Figure 111** Internet Connection Status

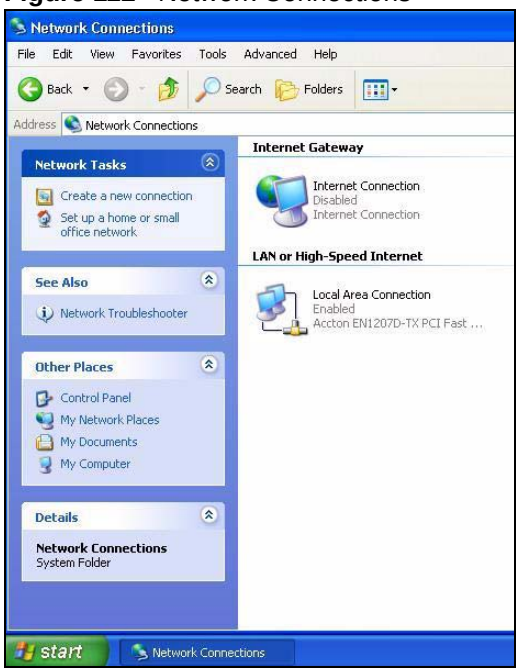
## 19.3.2 Web Configurator Easy Access

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

Follow the steps below to access the web configurator:

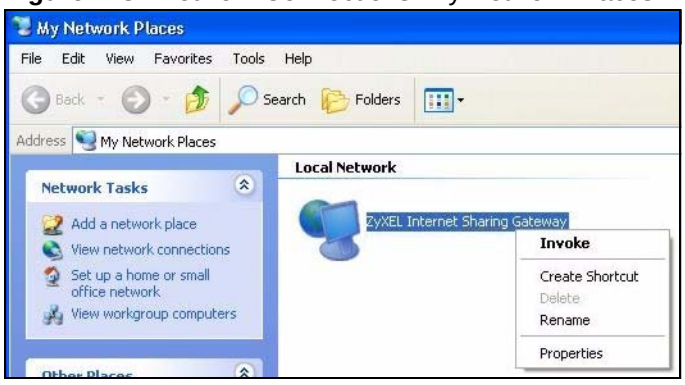
1. Click **Start** and then **Control Panel**.
2. Double-click **Network Connections**.
3. Select **My Network Places** under **Other Places**.

**Figure 112** Network Connections




4. An icon with the description for each UPnP-enabled device displays under **Local Network**.
5. Right-click on the icon for your WiMAX Modem and select **Invoke**. The web configurator login screen displays.

**Figure 113** Network Connections: My Network Places



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

**Figure 114** Network Connections: My Network Places: Properties: Example

# 20

# The Status Screen

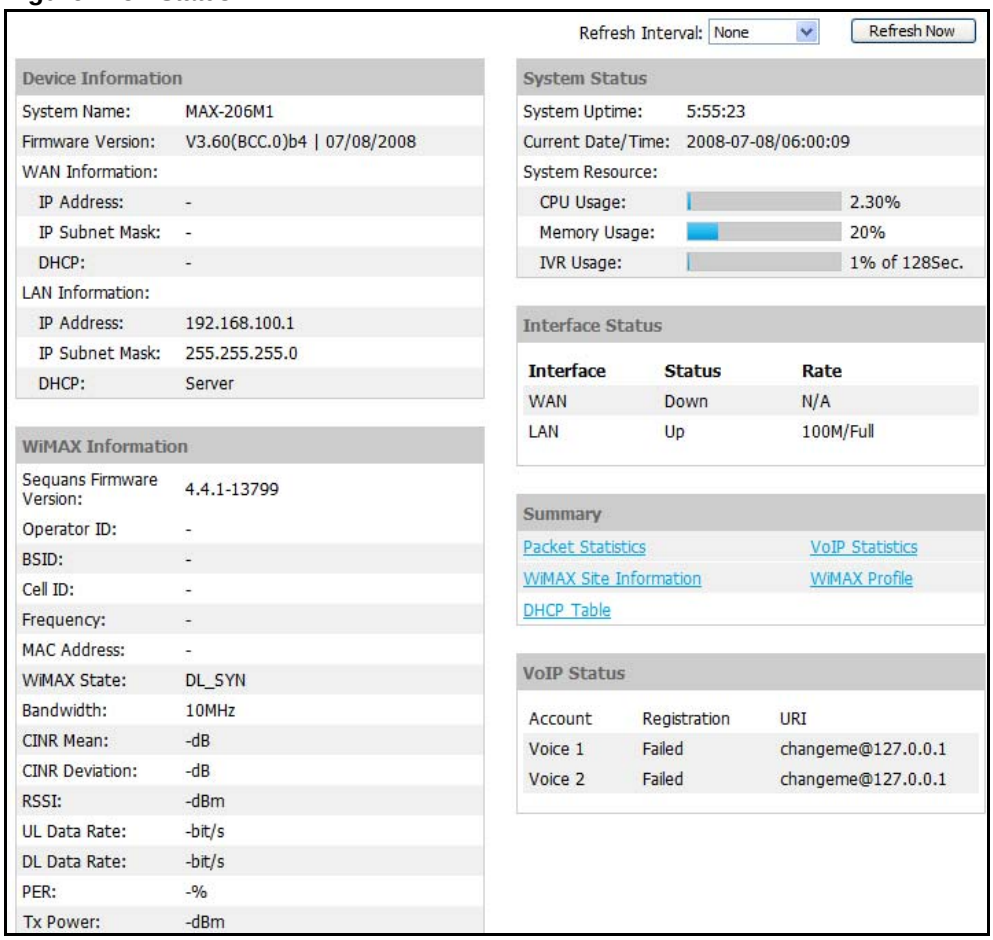
## 20.1 Overview

Use this screen to view a complete summary of your WiMAX Modem connection status.

## 20.2 Status Screen

Click the **STATUS** icon in the navigation bar to go to this screen, where you can view the current status of the device, system resources, interfaces (LAN and WAN), and SIP accounts. You can also register and un-register SIP accounts as well as view detailed information from DHCP and statistics from WiMAX, VoIP, bandwidth management, and traffic.

**Figure 115** Status



The following tables describe the labels in this screen.

**Table 101** Status

| LABEL | DESCRIPTION |
|---|---|
| Refresh Interval | Select how often you want the WiMAX Modem to update this screen. |
| Refresh Now | Click this to update this screen immediately. |
| Device Information | |
| System Name | This field displays the WiMAX Modem system name. It is used for identification.<br>You can change this in the **ADVANCED > System Configuration > General** screen's **System Name** field. |
| Firmware Version | This field displays the current version of the firmware inside the device. It also shows the date the firmware version was created.<br>You can change the firmware version by uploading new firmware in **ADVANCED > System Configuration > Firmware**. |
| WAN Information | |
| IP Address | This field displays the current IP address of the WiMAX Modem in the WAN. |
| IP Subnet Mask | This field displays the current subnet mask on the WAN. |
| DHCP | This field displays what DHCP services the WiMAX Modem is using in the WAN. Choices are:<br>**Client** - The WiMAX Modem is a DHCP client in the WAN. Its IP address comes from a DHCP server on the WAN.<br>**None** - The WiMAX Modem is not using any DHCP services in the WAN. It has a static IP address. |
| LAN Information | |
| IP Address | This field displays the current IP address of the WiMAX Modem in the LAN. |
| IP Subnet Mask | This field displays the current subnet mask in the LAN. |
| DHCP | This field displays what DHCP services the WiMAX Modem is providing to the LAN. Choices are:<br>**Server** - The WiMAX Modem is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN.<br>**Relay** - The WiMAX Modem is routing DHCP requests to one or more DHCP servers. The DHCP server(s) may be on another network.<br>**None** - The WiMAX Modem is not providing any DHCP services to the LAN.<br>You can change this in **ADVANCED > LAN Configuration > DHCP Setup**. |
| WiMAX Information | |
| Operator ID | Every WiMAX service provider has a unique Operator ID number, which is broadcast by each base station it owns. You can only connect to the Internet through base stations belonging to your service provider's network. |
| BSID | This field displays the identification number of the wireless base station to which the WiMAX Modem is connected. Every base station transmits a unique BSID, which identifies it across the network. |
| Cell ID | A base station's coverage area can be divided into multiple cells. This field shows the identification number of the cell in which the WiMAX Modem is connected. |
| Frequency | This field displays the radio frequency of the WiMAX Modem's wireless connection to a base station. |
| MAC address | This field displays the Media Access Control address of the WiMAX Modem. Every network device has a unique MAC address which identifies it across the network. |

**Table 101** Status (continued)

| LABEL | DESCRIPTION |
|---|---|
| WiMAX State | This field displays the status of the WiMAX Modem's current connection.<br>• **INIT**: the WiMAX Modem is starting up.<br>• **DL_SYN**: The WiMAX Modem is unable to connect to a base station.<br>• **RANGING**: the WiMAX Modem and the base station are transmitting and receiving information about the distance between them. Ranging allows the WiMAX Modem to use a lower transmission power level when communicating with a nearby base station, and a higher transmission power level when communicating with a distant base station.<br>• **CAP_NEGO**: the WiMAX Modem and the base station are exchanging information about their capabilities.<br>• **AUTH**: the WiMAX Modem and the base station are exchanging security information.<br>• **REGIST**: the WiMAX Modem is registering with a RADIUS server.<br>• **OPERATIONAL**: the WiMAX Modem has successfully registered with the base station. Traffic can now flow between the WiMAX Modem and the base station.<br>• **IDLE**: the WiMAX Modem is in power saving mode, but can connect when a base station alerts it that there is traffic waiting. |
| Bandwidth | This field shows the size of the bandwidth step the WiMAX Modem uses to connect to a base station in megahertz (MHz). |
| CINR mean | This field shows the average Carrier to Interference plus Noise Ratio of the current connection. This value is an indication of overall radio signal quality. A higher value indicates a higher signal quality, and a lower value indicates a lower signal quality. |
| CINR deviation | This field shows the amount of change in the CINR level. This value is an indication of radio signal stability. A lower number indicates a more stable signal, and a higher number indicates a less stable signal. |
| RSSI | This field shows the Received Signal Strength Indication. This value is a measurement of overall radio signal strength. A higher RSSI level indicates a stronger signal, and a lower RSSI level indicates a weaker signal.<br>A strong signal does not necessarily indicate a good signal: a strong signal may have a low signal-to-noise ratio (SNR). |
| UL Data Rate | This field shows the number of data packets uploaded from the WiMAX Modem to the base station each second. |
| DL Data Rate | This field shows the number of data packets downloaded to the WiMAX Modem from the base station each second. |
| PER | This field shows the Packet Error Rate. The PER is the percentage of data packets transmitted across the network but not successfully received. |
| Tx Power | This field shows the output transmission (Tx) level of the WiMAX Modem. |
| System Status | |
| System Uptime | This field displays how long the WiMAX Modem has been running since it last started up. The WiMAX Modem starts up when you plug it in, when you restart it (**ADVANCED > System Configuration > Restart**), or when you reset it. |
| Current Date/ Time | This field displays the current date and time in the WiMAX Modem. You can change this in **SETUP > Time Setting**. |
| CPU Usage | This field displays what percentage of the WiMAX Modem's processing ability is currently being used. The higher the CPU usage, the more likely the WiMAX Modem is to slow down. You can reduce this by disabling some services, such as DHCP, NAT, or content filtering. |

**Table 101** Status (continued)

| LABEL | DESCRIPTION |
|---|---|
| Memory Usage | This field displays what percentage of the WiMAX Modem's memory is currently used. The higher the memory usage, the more likely the WiMAX Modem is to slow down. Some memory is required just to start the WiMAX Modem and to run the web configurator. You can reduce the memory usage by disabling some services (see **CPU Usage**); by reducing the amount of memory allocated to NAT and firewall rules (you may have to reduce the number of NAT rules or firewall rules to do so); or by deleting rules in functions such as incoming call policies, speed dial entries, and static routes. |
| IVR Usage | This field displays what percentage of the WiMAX Modem's IVR memory is currently used. IVR (Interactive Voice Response) refers to the customizable ring tone and on-hold music you set. |
| Interface Status | |
| Interface | This column displays each interface of the WiMAX Modem. |
| Status | This field indicates whether or not the WiMAX Modem is using the interface.<br>For the WAN interface, this field displays **Up** when the WiMAX Modem is connected to a WiMAX network, and **Down** when the WiMAX Modem is not connected to a WiMAX network.<br>For the LAN interface, this field displays **Up** when the WiMAX Modem is using the interface and **Down** when the WiMAX Modem is not using the interface. |
| Rate | For the LAN ports this displays the port speed and duplex setting.<br>For the WAN interface, it displays the downstream and upstream transmission rate or **N/A** if the WiMAX Modem is not connected to a base station.<br>For the WLAN interface, it displays the transmission rate when WLAN is enabled or **N/A** when WLAN is disabled. |
| Summary | |
| Packet Statistics | Click this link to view port status and packet specific statistics. |
| WiMAX Site Information | Click this link to view details of the radio frequencies used by the WiMAX Modem to connect to a base station. |
| DHCP Table | Click this link to see details of computers to which the WiMAX Modem has given an IP address. |
| VoIP Statistics | Click this link to view statistics about your VoIP usage. |
| WiMAX Profile | Click this link to view details of the current wireless security settings. |
| VoIP Status | |
| Account | This column displays each SIP account in the WiMAX Modem. |

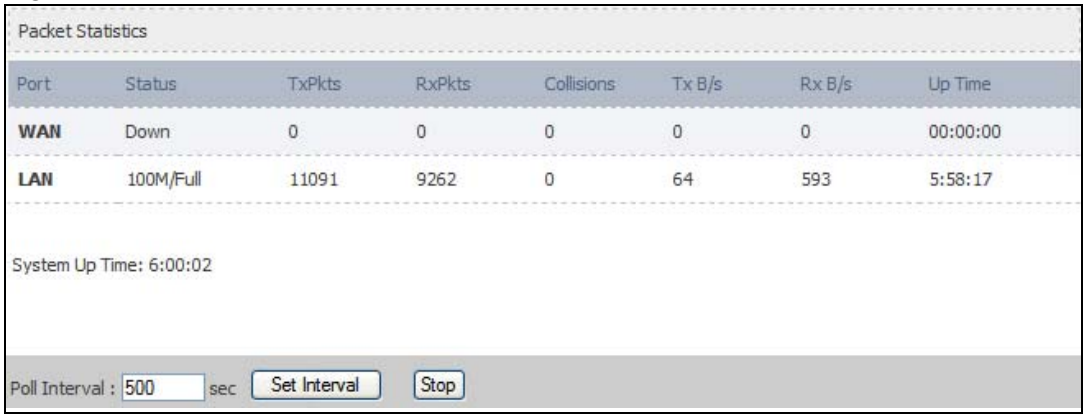
**Table 101** Status (continued)

| LABEL | DESCRIPTION |
|---|---|
| Registration | This field displays the current registration status of the SIP account. You have to register SIP accounts with a SIP server to use VoIP.<br>If the SIP account is already registered with the SIP server,<br>Click **Unregister** to delete the SIP account's registration in the SIP server. This does not cancel your SIP account, but it deletes the mapping between your SIP identity and your IP address or domain name.<br>The second field displays **Registered**.<br>If the SIP account is not registered with the SIP server,<br>Click **Register** to have the WiMAX Modem attempt to register the SIP account with the SIP server.<br>The second field displays the reason the account is not registered.<br>**Inactive** - The SIP account is not active. You can activate it in **VOICE > SIP > SIP Settings**.<br>**Register Fail** - The last time the WiMAX Modem tried to register the SIP account with the SIP server, the attempt failed. The WiMAX Modem automatically tries to register the SIP account when you turn on the WiMAX Modem or when you activate it. |
| URI | This field displays the account number and service domain of the SIP account. You can change these in **VOICE > SIP > SIP Settings**. |

## 20.2.1 Packet Statistics

Click **Status** > **Packet Statistics** to open this screen. This read-only screen displays information about the data transmission through the WiMAX Modem. To configure these settings, go to the corresponding area in the **Advanced** screens.

**Figure 116** Packet Statistics



The following table describes the fields in this screen.

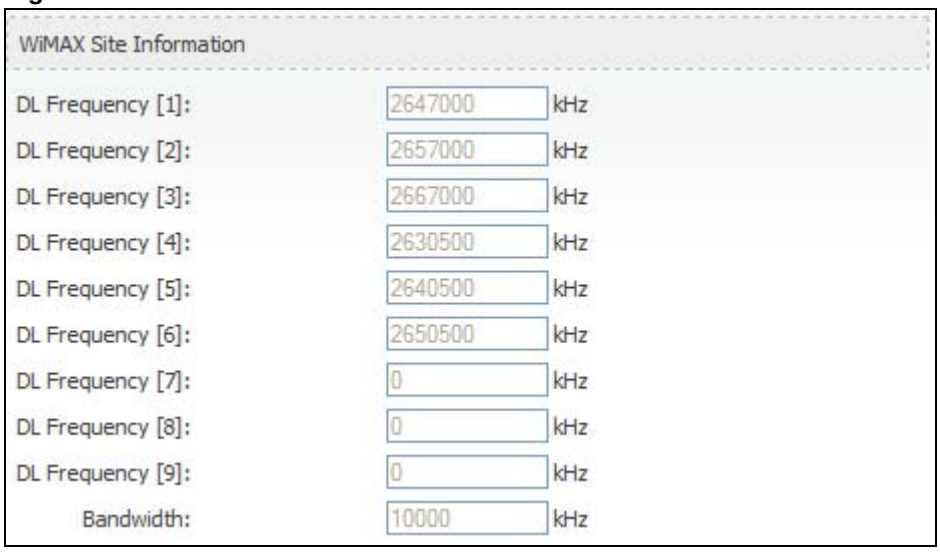
**Table 102** Packet Statistics

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

## 20.2.2 WiMAX Site Information

Click **Status** > **WiMAX Site Information** to open this screen. This read-only screen shows WiMAX frequency information for the WiMAX Modem. These settings can be configured in the **ADVANCED** > **WAN Configuration** > **WiMAX Configuration** screen.

**Figure 117** WiMAX Site Information



The following table describes the labels in this screen.

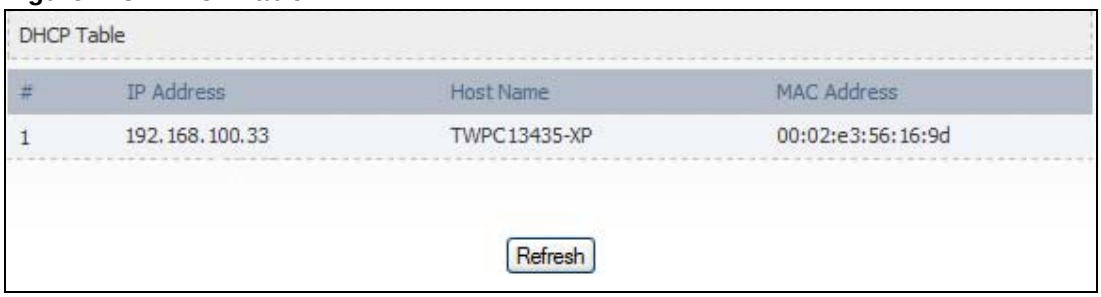
**Table 103** WiMAX Site Information

| LABEL | DESCRIPTION |
|---|---|
| DL Frequency<br>[0] ~ [9] | These fields show the downlink frequency settings in kilohertz (kHz). These settings determine how the WiMAX Modem searches for an available wireless connection. |

## 20.2.3 DHCP Table

Click **Status** > **DHCP Table** to open this screen. This read-only screen shows the IP addresses, Host Names and MAC addresses of the devices currently connected to the WiMAX Modem. These settings can be configured in the **ADVANCED** > **LAN Configuration** > **DHCP Setup** screen.

**Figure 118** DHCP Table




Each field is described in the following table.

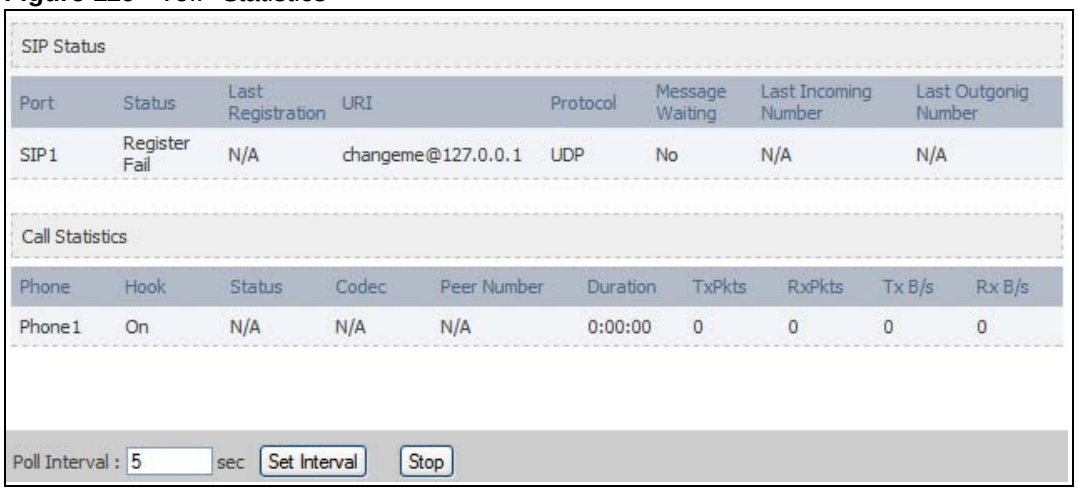
**Table 104** DHCP Table

| LABEL | DESCRIPTION |
|---|---|
| # | The number of the item in this list. |
| IP Address | This field displays the IP address the WiMAX Modem assigned to a computer in the network. |
| Host Name | This field displays the system name of the computer to which the WiMAX Modem assigned the IP address. |
| MAC Address | This field displays the MAC address of the computer to which the WiMAX Modem assigned the IP address. |
| Refresh | Click this button to update the table data. |

## 20.2.4 VoIP Statistics

Click **Status** > **DHCP Table** to open this screen. This read-only screen shows SIP registration information, status of calls and VoIP traffic statistics. These settings can be configured in the **VOICE** > **Service Configuration** > **SIP Setting** screen.

**Figure 119** VoIP Statistics




Each field is described in the following table.

**Table 105** VoIP Statistics

| LABEL | DESCRIPTION |
|---|---|
| SIP Status | |
| Port | This column displays each SIP account in the WiMAX Modem. |
| Status | This field displays the current registration status of the SIP account. You can change this in the **Status** screen.<br>**Registered** - The SIP account is registered with a SIP server.<br>**Register Fail** - The last time the WiMAX Modem tried to register the SIP account with the SIP server, the attempt failed. The WiMAX Modem automatically tries to register the SIP account when you turn on the WiMAX Modem or when you activate it.<br>**Inactive** - The SIP account is not active. You can activate it in **VOICE > SIP > SIP Settings**. |
| Last Registration | This field displays the last time you successfully registered the SIP account. It displays **N/A** if you never successfully registered this account. |
| URI | This field displays the account number and service domain of the SIP account. You can change these in **VOICE > SIP > SIP Settings**. |
| Protocol | This field displays the transport protocol the SIP account uses. SIP accounts always use UDP. |
| Message Waiting | This field indicates whether or not there are any messages waiting for the SIP account. |
| Last Incoming Number | This field displays the last number that called the SIP account. It displays **N/A** if no number has ever dialed the SIP account. |
| Last Outgoing Number | This field displays the last number the SIP account called. It displays **N/A** if the SIP account has never dialed a number. |
| Call Statistics | |
| Phone | This field displays the WiMAX Modem's phone port number. |

**Table 105** VoIP Statistics

| LABEL | DESCRIPTION |
|---|---|
| Hook | This field indicates whether the phone is on the hook or off the hook.<br>**On** - The phone is hanging up or already hung up.<br>**Off** - The phone is dialing, calling, or connected. |
| Status | This field displays the current state of the phone call.<br>**N/A** - There are no current VoIP calls, incoming calls or outgoing calls being made.<br>**DIAL** - The callee's phone is ringing.<br>**RING** - The phone is ringing for an incoming VoIP call.<br>**Process** - There is a VoIP call in progress.<br>**DISC** - The callee's line is busy, the callee hung up or your phone was left off the hook. |
| Codec | This field displays what voice codec is being used for a current VoIP call through a phone port. |
| Peer Number | This field displays the SIP number of the party that is currently engaged in a VoIP call through a phone port. |
| Duration | This field displays how long the current call has lasted. |
| Tx Pkts | This field displays the number of packets the WiMAX Modem has transmitted in the current call. |
| Rx Pkts | This field displays the number of packets the WiMAX Modem has received in the current call. |
| Tx B/s | This field displays how quickly the WiMAX Modem has transmitted packets in the current call. The rate is the average number of bytes transmitted per second. |
| Rx B/s | This field displays how quickly the WiMAX Modem has received packets in the current call. The rate is the average number of bytes transmitted per second. |
| Poll Interval(s) | Enter how often you want the WiMAX Modem to update this screen, and click **Set Interval**. |
| Set Interval | Click this to make the WiMAX Modem update the screen based on the amount of time you specified in **Poll Interval**. |
| Stop | Click this to make the WiMAX Modem stop updating the screen. |

## 20.2.5 WiMAX Profile

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

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

**Figure 120** WiMAX Profile


The following table describes the labels in this screen.

**Table 106** The WiMAX Profile Screen

| LABEL | DESCRIPTION |
|---|---|
| User | This is the username for your Internet access account. |
| Password | This is the password for your Internet access account. The password displays as a row of asterisks for security purposes. |
| Anonymous Identity | This is the anonymous identity provided by your Internet Service Provider. Anonymous identity (also known as outer identity) is used with EAP-TTLS encryption. |
| PKM | This field displays the Privacy Key Management version number. PKM provides security between the WiMAX Modem and the base station. See the WiMAX security appendix for more information. |
| Authentication | This field displays the user authentication method. Authentication is the process of confirming the identity of a user (by means of a username and password, for example).<br>EAP-TTLS allows an MS/SS and a base station to establish a secure link (or 'tunnel') with an AAA (Authentication, Authorization and Accounting) server in order to exchange authentication information. See the WiMAX security appendix for more details. |

**Table 106** The WiMAX Profile Screen (continued)

| LABEL | DESCRIPTION |
|---|---|
| TTLS Inner EAP | This field displays the type of secondary authentication method. Once a secure EAP-TTLS connection is established, the inner EAP is the protocol used to exchange security information between the mobile station, the base station and the AAA server to authenticate the mobile station. See the WiMAX security appendix for more details.<br>The WiMAX Modem supports the following inner authentication types:<br>• **CHAP** (Challenge Handshake Authentication Protocol)<br>• **MSCHAP** (Microsoft CHAP)<br>• **MSCHAPV2** (Microsoft CHAP version 2)<br>• **PAP** (Password Authentication Protocol) |
| Auth Mode | This is the authentication mode. The WiMAX Modem supports the following authentication modes:<br>• User Only<br>• Device Only with Cert<br>• Certs and User Authentication |
| Certificate | This is the security certificate the WiMAX Modem uses to authenticate the AAA server, if one is available. |

# PART VI
# Troubleshooting and Specifications

# 21

# Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories:

- Power, Hardware Connections, and LEDs
- WiMAX Modem Access and Login
- Internet Access
- Phone Calls and VoIP
- Reset the WiMAX Modem to Its Factory Defaults

## 21.1 Power, Hardware Connections, and LEDs

### The WiMAX Modem does not turn on. None of the LEDs turn on.

1. Make sure you are using the power adapter or cord included with the WiMAX Modem.
2. Make sure the power adapter or cord is connected to the WiMAX Modem and plugged in to an appropriate power source. Make sure the power source is turned on.
3. Disconnect and re-connect the power adapter or cord to the WiMAX Modem.
4. If the problem continues, contact the vendor.

### One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 1.2.1 on page 33 for more information.
2. Check the hardware connections. See the Quick Start Guide.
3. Inspect your cables for damage. Contact the vendor to replace any damaged cables.
4. Disconnect and re-connect the power adapter to the WiMAX Modem.
5. If the problem continues, contact the vendor.

## 21.2 WiMAX Modem Access and Login

### I forgot the IP address for the WiMAX Modem.

1. The default IP address is http://192.168.100.1.
2. If you changed the IP address and have forgotten it, you might get the IP address of the WiMAX Modem by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start** > **Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the WiMAX Modem (it depends on the network), so enter this IP address in your Internet browser.
3. If this does not work, you have to reset the WiMAX Modem to its factory defaults. See Section 21.1 on page 217.

### I forgot the password.

1. The default password is **1234**.
2. If this does not work, you have to reset the WiMAX Modem to its factory defaults. See Section 10.5 on page 106.

### I cannot see or access the **Login** screen in the web configurator.

1. Make sure you are using the correct IP address.
   - The default IP address is http://192.168.100.1.
   - If you changed the IP address (Section 5.2 on page 54), use the new IP address.
   - If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the WiMAX Modem.
2. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.2.1 on page 33.
3. Make sure your Internet browser does not block pop-up windows and has JavaScript and Java enabled. See Appendix C on page 259.
4. If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. Your WiMAX Modem is a DHCP server by default.

   If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the WiMAX Modem. See Appendix D on page 267.
5. Reset the WiMAX Modem to its factory defaults, and try to access the WiMAX Modem with the default IP address. See Section 10.6 on page 108.
6. If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

**Advanced Suggestions**

- Try to access the WiMAX Modem using another service, such as Telnet. If you can access the WiMAX Modem, check the remote management settings and firewall rules to find out why the WiMAX Modem does not respond to HTTP.
- If your computer is connected wirelessly, use a computer that is connected to a **LAN/ ETHERNET** port.

### I can see the **Login** screen, but I cannot log in to the WiMAX Modem.

1. Make sure you have entered the user name and password correctly. The default user name is **admin**, and the default password is **1234**. These fields are case-sensitive, so make sure [Caps Lock] is not on.
2. You cannot log in to the web configurator while someone is using Telnet to access the WiMAX Modem. Log out of the WiMAX Modem in the other session, or ask the person who is logged in to log out.
3. Disconnect and re-connect the power adapter or cord to the WiMAX Modem.
4. If this does not work, you have to reset the WiMAX Modem to its factory defaults. See Section 10.5 on page 106.

### I cannot Telnet to the WiMAX Modem.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

## 21.3 Internet Access

### I cannot access the Internet.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.2.1 on page 33.
2. Make sure you entered your ISP account information correctly in the wizard. These fields are case-sensitive, so make sure [Caps Lock] is not on.
3. Check your security settings. In the web configurator, go to the **Status** screen. Click the **WiMAX Profile** link in the **Summary** box and make sure that you are using the correct security settings for your Internet account.
4. Check your WiMAX settings. The WiMAX Modem may have been set to search the wrong frequencies for a wireless connection. In the web configurator, go to the **Status** screen. Click the **WiMAX Site Information** link in the **Summary** box and ensure that

the values are correct. If the values are incorrect, enter the correct frequency settings in the **ADVANCED > WAN Configuration > WiMAX Configuration** screen. If you are unsure of the correct values, contact your service provider.

5 If you are trying to access the Internet wirelessly, make sure the wireless settings in the wireless client are the same as the settings in the AP.

6 Disconnect all the cables from your WiMAX Modem, and follow the directions in the Quick Start Guide again.

7 If the problem continues, contact your ISP.

## I cannot access the Internet any more. I had access to the Internet (with the WiMAX Modem), but my Internet connection is not available any more.

1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.2.1 on page 33.

2 Disconnect and re-connect the power adapter to the WiMAX Modem.

3 If the problem continues, contact your ISP.

## The Internet connection is slow or intermittent.

1 The quality of the WiMAX Modem's wireless connection to the base station may be poor. Poor signal reception may be improved by moving the WiMAX Modem away from thick walls and other obstructions, or to a higher floor in your building.

2 There may be radio interference caused by nearby electrical devices such as microwave ovens and radio transmitters. Move the WiMAX Modem away or switch the other devices off. Weather conditions may also affect signal quality.

3 As well as having an external antenna connector, the MAX-210HW2 is equipped with an internal directional antenna. If you know the location of the base station, orient the front of the WiMAX Modem (the side with the LEDs) towards the base station. If you do not know the location of the base station, experiment by moving the WiMAX Modem while observing the **Strength Indicator** LEDs for an increase in received signal strength. The MAX-200HW2 and MAX-230HW2 do not have internal antennas.

4 There might be a lot of traffic on the network. Look at the LEDs, and check Section 1.2.1 on page 33. If the WiMAX Modem is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.

5 Disconnect and re-connect the power adapter to the WiMAX Modem.

6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

### The Internet connection disconnects.

1. Check your WiMAX link and signal strength using the **WiMAX Link** and **Strength Indicator** LEDs on the device.
2. Contact your ISP if the problem persists.

## 21.4 Phone Calls and VoIP

### The telephone port won't work or the telephone lacks a dial tone.

1. Check the telephone connections and telephone wire.
2. Make sure you have the **VOICE > Service Configuration > SIP Settings** screen properly configured (Chapter 11 on page 111).

### I can access the Internet, but cannot make VoIP calls.

1. Make sure you have the **VOICE > Service Configuration > SIP Settings** screen properly configured (Chapter 11 on page 111).
2. The **VoIP** LED should come on. Make sure that your telephone is connected to the **VoIP** port (see the Quick Start Guide for information on connecting telephone cables to the these ports).
3. You can also check the VoIP status in the **Status** screen.
4. If the VoIP settings are correct, use speed dial to make peer-to-peer calls. If you cannot make a call using speed dial, there may be something wrong with the SIP server. Contact your VoIP service provider.

### Problems With Multiple SIP Accounts

You can set up two SIP accounts on your WiMAX Modem. By default your WiMAX Modem uses SIP account 1 for outgoing calls, and it uses SIP accounts 1 and 2 for incoming calls. With this setting, you always use SIP account 1 for your outgoing calls and you cannot distinguish which SIP account the calls are coming in through. If you want to control the use of different dialing plans for accounting purposes or other reasons, you need to configure your phone port in order to control which SIP account you are using when placing or receiving calls.

## 21.5 Reset the WiMAX Modem to Its Factory Defaults

If you reset the WiMAX Modem, you lose all of the changes you have made. The WiMAX Modem re-loads its default settings, and the password resets to **1234**. You have to make all of your changes again.

You will lose all of your changes when you push the **Reset** button.

To reset the WiMAX Modem,

1. Make sure the **Power LED** is on and not blinking.
2. Press and hold the **Reset** button for five to ten seconds. Release the **Reset** button when the **Power** LED begins to blink. The default settings have been restored.

If the WiMAX Modem restarts automatically, wait for the WiMAX Modem to finish restarting, and log in to the web configurator. The password is “1234”.

If the WiMAX Modem does not restart automatically, disconnect and reconnect the WiMAX Modem’s power. Then, follow the directions above again.

### 21.5.1 Pop-up Windows, JavaScripts and Java Permissions

Please see Appendix C on page 259.

# 22

# Product Specifications

This chapter gives details about your WiMAX Modem's hardware and firmware features.

**Table 107** Environmental and Hardware Specifications

| FEATURE | DESCRIPTION |
|---|---|
| Operating Temperature | 0°C to 45°C |
| Storage Temperature | -25°C to 55°C |
| Operating Humidity | 20% ~ 90% (non-condensing) |
| Storage Humidity | 10% to 95% (non-condensing) |
| Power Supply | 12V DC, 2 A |
| Power consumption | 18W |
| Ethernet Interface | Two auto-negotiating, auto-MDI/MDI-X NWay 10/100 Mbps RJ-45 Ethernet ports |
| Telephony Interface | Two analog ATA interfaces for standard telephones through RJ-11 FXS (Foreign Exchange Subscriber) analog connector |
| Antennas | Two internal 5dBi WiMAX antennas |
| Weight | 480g |
| Dimensions | 160mm (W) x 118mm (D) x 167mm (H) |
| Safety Approvals | UL 60950-1<br>CAN/CSA C22.2 No. 60950-1-03<br>EN 60950-1<br>IEC 60950-1 |
| EMI Approvals | EN 301489-1 v1.6.1<br>EN 61000-3-2<br>EN 61000-3-3 |
| EMS Approvals | EN 301489-4 v1.3.1 |
| RF Approvals | EN 302326 |

**Table 108** Radio Specifications

| FEATURE | DESCRIPTION |
|---|---|
| Media Access Protocol | IEEE 802.16e |
| WiMAX Bandwidth | 2.5 GHz |

**Table 108** Radio Specifications (continued)

| | |
|---|---|
| Data Rate | Download:<br>Maximum 20 Mbps<br>Average 6 Mbps<br>Upload:<br>Maximum 4 Mbps<br>Average 3 Mbps |
| Modulation | QPSK (uplink and downlink)<br>16-QAM (uplink and downlink)<br>64-QAM (downlink only) |
| Output Power | 27dBm with external antennas attached |
| Duplex mode | Time Division Duplex (TDD) |
| Security | PKMv2<br>EAP<br>CCMP, 128-bit AES |

**Table 109** Firmware Specifications

| FEATURE | DESCRIPTION |
|---|---|
| Web-based Configuration and Management Tool | Also known as “the web configurator”, this is a firmware-based management solution for the WiMAX Modem. You must connect using a compatible web browser in order to use it. |
| High Speed Wireless Internet Access | The WiMAX Modem is ideal for high-speed wireless Internet browsing.<br>WiMAX (Worldwide Interoperability for Microwave Access) is a wireless networking standard providing high-bandwidth, wide-range secured wireless service. The WiMAX Modem is a WiMAX mobile station (MS) compatible with the IEEE 802.16e standard. |
| Firewall | The WiMAX Modem is a stateful inspection firewall with DoS (Denial of Service) protection. By default, when the firewall is activated, all incoming traffic from the WAN to the LAN is blocked unless it is initiated from the LAN. The WiMAX Modem’s firewall supports TCP/UDP inspection, DoS detection and prevention, real time alerts, reports and logs. |
| Content Filtering | The WiMAX Modem can block access to web sites containing specified keywords. You can define time periods and days during which content filtering is enabled and include or exclude a range of users on the LAN from content filtering. |
| Network Address Translation (NAT) | Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). |
| Universal Plug and Play (UPnP) | Your device and other UPnP enabled devices can use the standard TCP/IP protocol to dynamically join a network, obtain an IP address and convey their capabilities to each other. |
| Dynamic DNS Support | With Dynamic DNS support, you can have a static hostname alias for a dynamic IP address, allowing the host to be more easily accessible from various locations on the Internet. You must register for this service with a Dynamic DNS service provider. |

**Table 109** Firmware Specifications (continued)

| FEATURE | DESCRIPTION |
|---|---|
| DHCP | DHCP (Dynamic Host Configuration Protocol) allows the individual clients (computers) to obtain the TCP/IP configuration at start-up from a centralized DHCP server. Your device has built-in DHCP server capability enabled by default. It can assign IP addresses, an IP default gateway and DNS servers to DHCP clients. Your device can also act as a surrogate DHCP server (DHCP Relay) where it relays IP address assignment from the actual real DHCP server to the clients. |
| IP Alias | IP alias allows you to partition a physical network into logical networks over the same Ethernet interface. Your device supports three logical LAN interfaces via its single physical Ethernet interface with the your device itself as the gateway for each LAN network. |
| Multiple SIP Accounts | You can configure multiple voice (SIP) accounts. |
| SIP ALG | Your device is a SIP Application Layer Gateway (ALG). It allows VoIP calls to pass through NAT for devices behind it (such as a SIP-based VoIP software application on a computer). |
| Dynamic Jitter Buffer | The built-in adaptive buffer helps to smooth out the variations in delay (jitter) for voice traffic (up to 60 ms). This helps ensure good voice quality for your conversations. |
| Voice Activity Detection/ Silence Suppression | Voice Activity Detection (VAD) reduces the bandwidth that a call uses by not transmitting when you are not speaking. |
| Comfort Noise Generation | Your device generates background noise to fill moments of silence when the other device in a call stops transmitting because the other party is not speaking (as total silence could easily be mistaken for a lost connection). |
| Echo Cancellation | You device supports G.168 of at least 24 ms.<br>This an ITU-T standard for eliminating the echo caused by the sound of your voice reverberating in the telephone receiver while you talk. |
| Time and Date | Get the current time and date from an external server when you turn on your WiMAX Modem. You can also set the time manually. |
| Logging | Use the WiMAX Modem's logging feature to view connection history, surveillance logs, and error messages. |
| Codecs | Enhanced Variable Rate Codec (EVRC), G.711 (PCM μ-law and a-law), G.729a, and G.723.1 |
| Fax Support | T.38 FAX relay (FAX over UDP).<br>G.711 fax relay for fax calls and be able to renegotiate codec to G.711 if a fax call is detected. |
| Ring Tones | Supports different distinctive ring tones on each line. |
| Call Prioritization | Prioritize VoIP traffic originating from the RJ-11 ports over any other traffic. |

**Table 110** Standards Supported

| STANDARD | DESCRIPTION |
|---|---|
| RFC 768 | User Datagram Protocol |
| RFC 791 | Internet Protocol v4 |
| RFC 792 | Internet Control Message Protocol |
| RFC 792 | Transmission Control Protocol |
| RFC 826 | Address Resolution Protocol |
| RFC 854 | Telnet Protocol |

**Table 110** Standards Supported (continued)

| STANDARD | DESCRIPTION |
|---|---|
| RFC 1349 | Type of Service Protocol |
| RFC 1706 | DNS NSAP Resource Records |
| RFC 1889 | Real-time Transport Protocol (RTP) |
| RFC 1890 | Real-time Transport Control Protocol (RTCP) |
| RFC 2030 | Simple Network Time Protocol |
| RFC 2104 | HMAC: Keyed-Hashing for Message Authentication |
| RFC 2131 | Dynamic Host Configuration Protocol |
| RFC 2401 | Security Architecture for the Internet Protocol |
| RFC 2409 | Internet Key Exchange |
| RFC 2475 | Architecture for Differentiated Services (Diffserv) |
| RFC 2617 | Hypertext Transfer Protocol (HTTP) Authentication: Basic and Digest Access Authentication |
| RFC 2782 | A DNS RR for specifying the location of services (DNS SRV) |
| RFC 2833 | Real-time Transport Protocol Payload for DTMF Digits, Telephony Tones and Telephony Signals |
| RFC 2976 | The SIP INFO Method |
| RFC 3261 | Session Initiation Protocol (SIP version 2) |
| RFC 3262 | Reliability of Provisional Responses in the Session Initiation Protocol (SIP). |
| RFC 3263 | Session Initiation Protocol (SIP): Locating SIP Servers |
| RFC 3264 | An Offer/Answer Model with the Session Description Protocol (SDP) |
| RFC 3265 | Session Initiation Protocol (SIP)-Specific Event Notification |
| RFC 3323 | A Privacy Mechanism for SIP |
| RFC 3325 | Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks |
| RFC 3550 | RTP - A Real Time Protocol for Real-Time Applications |
| RFC 3581 | An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing |
| RFC 3611 | RTP Control Protocol Extended Reports (RTCP XR)-XR |
| RFC 3715 | IP Sec/NAT Compatibility |
| RFC 3842 | A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP) |
| IEEE 802.3 | 10BASE5 10 Mbit/s (1.25 MB/s) |
| IEEE 802.3u | 100BASE-TX, 100BASE-T4, 100BASE-FX Fast Ethernet at 100 Mbit/s (12.5 MB/s) with auto-negotiation |

**Table 111** Voice Features

| | |
|---|---|
| Call Park and Pickup | Call park and pickup lets you put a call on hold (park) and then continue the call (pickup). The caller must still pay while the call is parked.<br>When you park the call, you enter a number of your choice (up to eight digits), which you must enter again when you pick up the call. If you do not enter the correct number, you cannot pickup the call. This means that only someone who knows the number you have chosen can pick up the call.<br>You can have more than one call on hold at the same time, but you must give each call a different number. |
| Call Return | With call return, you can place a call to the last number that called you (either answered or missed). The last incoming call can be through either SIP or PSTN. |
| Country Code | Phone standards and settings differ from one country to another, so the settings on your WiMAX Modem must be configured to match those of the country you are in. The country code feature allows you to do this by selecting the country from a list rather than changing each setting manually. Configure the country code feature when you move the WiMAX Modem from one country to another. |
| Do not Disturb (DnD) | This feature allows you to set your phone not to ring when someone calls you. You can set each phone independently using its keypad, or configure global settings for all phones using the command line interpreter. |
| Auto Dial | You can set the WiMAX Modem to automatically dial a specified number immediately whenever you lift a phone off the hook. Use the Web Configurator to set the specified number. Use the command line interpreter to have the WiMAX Modem wait a specified length of time before dialing the number. |
| Phone config | The phone config table allows you to customize the phone keypad combinations you use to access certain features on the WiMAX Modem, such as call waiting, call return, call forward, etc. The phone config table is configurable in command interpreter mode. |
| Firmware update enable / disable | If your service provider uses this feature, you hear a recorded message when you pick up the phone when new firmware is available for your WiMAX Modem. Enter *99# in your phone's keypad to have the WiMAX Modem upgrade the firmware, or enter #99# to not upgrade. If your service provider gave you different numbers to use, enter them instead. If you enter the code to not upgrade, you can make a call as normal. You will hear the recording again each time you pick up the phone, until you upgrade. |
| Call waiting | This feature allows you to hear an alert when you are already using the phone and another person calls you. You can then either reject the new incoming call, put your current call on hold and receive the new incoming call, or end the current call and receive the new incoming call. |
| Call forwarding | With this feature, you can set the WiMAX Modem to forward calls to a specified number, either unconditionally (always), when your number is busy, or when you do not answer. You can also forward incoming calls from one specified number to another. |
| Caller ID | The WiMAX Modem supports caller ID, which allows you to see the originating number of an incoming call (on a phone with a suitable display). |
| REN | A Ringer Equivalence Number (REN) is used to determine the number of devices (like telephones or fax machines) that may be connected to the telephone line. Your device has a REN of three, so it can support three devices per telephone port. |
| QoS (Quality of Service) | Quality of Service (QoS) mechanisms help to provide better service on a per-flow basis. Your device supports Type of Service (ToS) tagging and Differentiated Services (DiffServ) tagging. This allows the device to tag voice frames so they can be prioritized over the network. |

**Table 111** Voice Features

| | |
|---|---|
| SIP ALG | Your device is a SIP Application Layer Gateway (ALG). It allows VoIP calls to pass through NAT for devices behind it (such as a SIP-based VoIP software application on a computer). |
| Other Voice Features | SIP version 2 (Session Initiating Protocol RFC 3261)<br>SDP (Session Description Protocol RFC 2327)<br>RTP (RFC 1889)<br>RTCP (RFC 1890)<br>Voice codecs (coder/decoders) G.711, G.726, G.729<br>Fax and data modem discrimination<br>DTMF Detection and Generation<br>DTMF: In-band and Out-band traffic (RFC 2833),(PCM), (SIP INFO)<br>Point-to-point call establishment between two IADs<br>Quick dialing through predefined phone book, which maps the phone dialing number and destination URL.<br>Flexible Dial Plan (RFC3525 section 7.1.14) |

**Table 112** Star (*) and Pound (#) Code Support

| | |
|---|---|
| *0 | Wireless Operator Services |
| *2 | Customer Care Access |
| *66 | Repeat Dialing |
| *67 | Plus the 10 digit phone number to block Caller ID on a single call basis |
| *69 | Return last call received |
| *70 | Followed by the 10 digit phone number to cancel Call Waiting on a single call basis |
| *72 | Activate Call Forwarding (*72 followed by the 10 digit phone number that is requesting call forwarding service) |
| *720 | Activate Call Forwarding (*720 followed by the 10 digit phone number that is requesting deactivation of call forwarding service) |
| *73 | Plus the forward to phone number to activate Call Forwarding No Answer (no VM service plan) |
| *730 | Deactivate Call Forwarding No Answer |
| *740 | Plus the forward to phone number to activate Call Forwarding Busy (no VM service plan) |
| *911/911 | Emergency phone number (same as dialing 911) |
| *411/411 | Wireless Information Services |

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 voice account service provider.

Not all features are supported by all service providers. Consult your service provider for more information.

# PART VII
# Appendices and Index

# A

# WiMAX Security

Wireless security is vital to protect your wireless communications. Without it, information transmitted over the wireless network would be accessible to any networking device within range.

## User Authentication and Data Encryption

The WiMAX (IEEE 802.16) standard employs user authentication and encryption to ensure secured communication at all times.

User authentication is the process of confirming a user's identity and level of authorization. Data encryption is the process of encoding information so that it cannot be read by anyone who does not know the code.

WiMAX uses PKMv2 (Privacy Key Management version 2) for authentication, and CCMP (Counter Mode with Cipher Block Chaining Message Authentication Protocol) for data encryption.

WiMAX supports EAP (Extensible Authentication Protocol, RFC 2486) which allows additional authentication methods to be deployed with no changes to the base station or the mobile or subscriber stations.

### PKMv2

PKMv2 is a procedure that allows authentication of a mobile or subscriber station and negotiation of a public key to encrypt traffic between the MS/SS and the base station. PKMv2 uses standard EAP methods such as Transport Layer Security (EAP-TLS) or Tunneled TLS (EAP-TTLS) for secure communication.

In cryptography, a 'key' is a piece of information, typically a string of random numbers and letters, that can be used to 'lock' (encrypt) or 'unlock' (decrypt) a message. Public key encryption uses key pairs, which consist of a public (freely available) key and a private (secret) key. The public key is used for encryption and the private key is used for decryption. You can decrypt a message only if you have the private key. Public key certificates (or 'digital IDs') allow users to verify each other's identity.

## RADIUS

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

- Authentication

  Determines the identity of the users.
- Authorization

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

  Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your base station acts as a message relay between the MS/SS and the network RADIUS server.

### Types of RADIUS Messages

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

- Access-Request

  Sent by an base station requesting authentication.
- Access-Reject

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

  Sent by a RADIUS server allowing access.
- Access-Challenge

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

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

- Accounting-Request

  Sent by the base station requesting accounting.
- Accounting-Response

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

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

### Diameter

Diameter (RFC 3588) is a type of AAA server that provides several improvements over RADIUS in efficiency, security, and support for roaming.

# Security Association

The set of information about user authentication and data encryption between two computers is known as a security association (SA). In a WiMAX network, the process of security association has three stages.

- Authorization request and reply

  The MS/SS presents its public certificate to the base station. The base station verifies the certificate and sends an authentication key (AK) to the MS/SS.
- Key request and reply

  The MS/SS requests a transport encryption key (TEK) which the base station generates and encrypts using the authentication key.
- Encrypted traffic

  The MS/SS decrypts the TEK (using the authentication key). Both stations can now securely encrypt and decrypt the data flow.

## CCMP

All traffic in a WiMAX network is encrypted using CCMP (Counter Mode with Cipher Block Chaining Message Authentication Protocol). CCMP is based on the 128-bit Advanced Encryption Standard (AES) algorithm.

'Counter mode' refers to the encryption of each block of plain text with an arbitrary number, known as the counter. This number changes each time a block of plain text is encrypted. Counter mode avoids the security weakness of repeated identical blocks of encrypted text that makes encrypted data vulnerable to pattern-spotting.

'Cipher Block Chaining Message Authentication' (also known as CBC-MAC) ensures message integrity by encrypting each block of plain text in such a way that its encryption is dependent on the block before it. This series of 'chained' blocks creates a message authentication code (MAC or CMAC) that ensures the encrypted data has not been tampered with.

# Authentication

The WiMAX Modem supports EAP-TTLS authentication.

## EAP-TTLS (Tunneled Transport Layer Service)

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

# B

# Setting Up Your Computer's IP Address

Your specific ZyXEL device may not support all of the operating systems described in this appendix. See the product specifications for more information about which operating systems are supported.

This appendix shows you how to configure the IP settings on your computer in order for it to be able to communicate with the other devices on your network. Windows Vista/XP/2000, Mac OS 9/OS X, and all versions of UNIX/LINUX include the software components you need to use TCP/IP on your computer.

If you manually assign IP information instead of using a dynamic IP, make sure that your network's computers have IP addresses that place them in the same subnet.

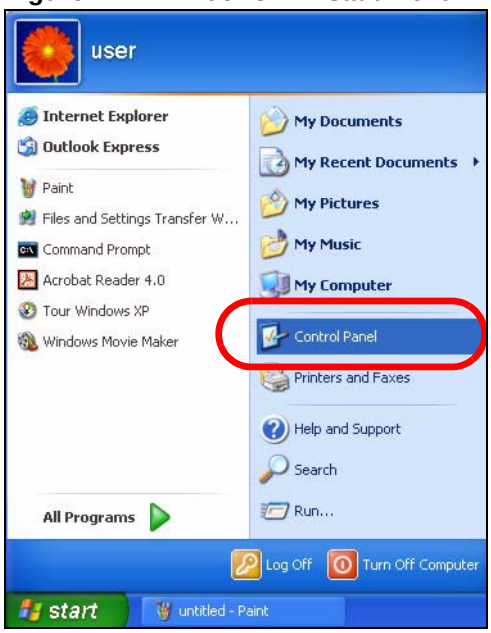
In this appendix, you can set up an IP address for:

# Windows XP/NT/2000

The following example uses the default Windows XP display theme but can also apply to Windows 2000 and Windows NT.

1 Click **Start** > **Control Panel**.

**Figure 121** Windows XP: Start Menu

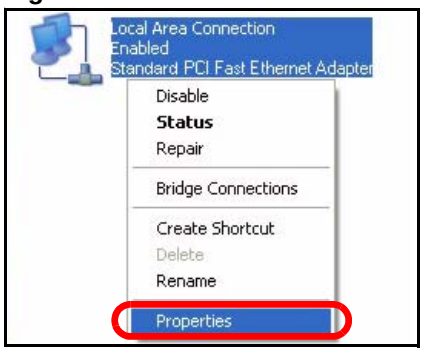



2 In the **Control Panel**, click the **Network Connections** icon.

**Figure 122** Windows XP: Control Panel

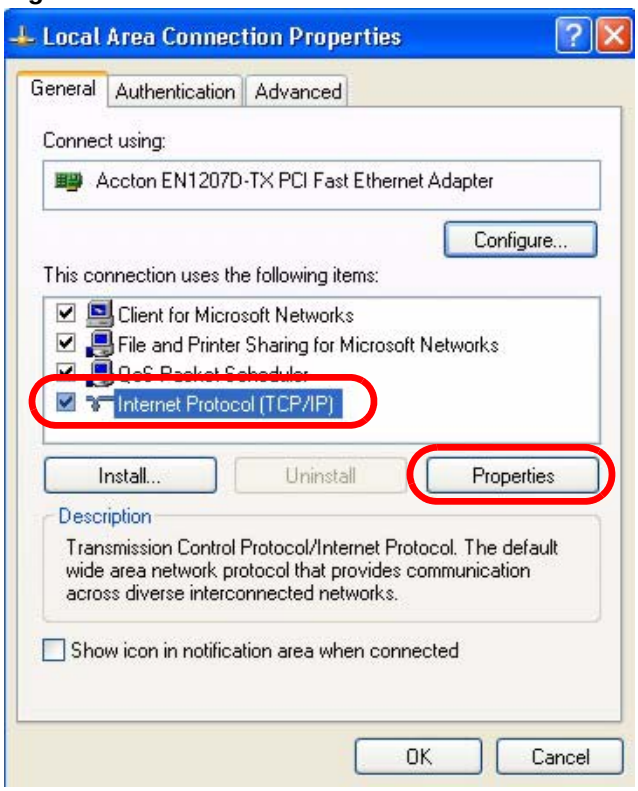

3 Right-click **Local Area Connection** and then select **Properties**.

**Figure 123** Windows XP: Control Panel > Network Connections > Properties



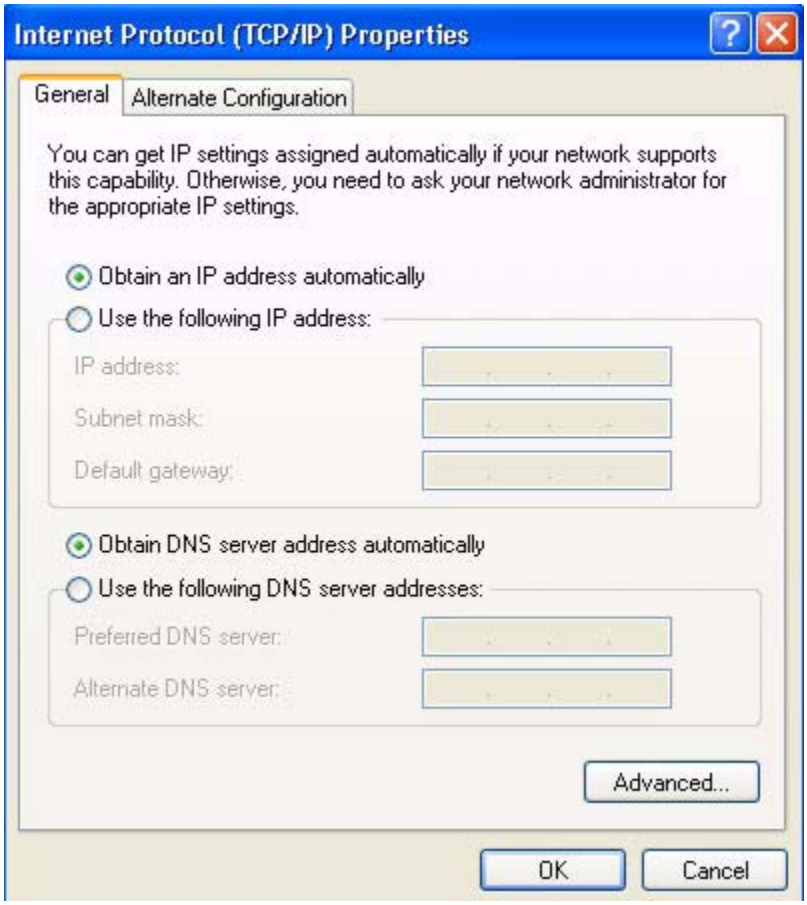

4 On the **General** tab, select **Internet Protocol (TCP/IP)** and then click **Properties**.

**Figure 124** Windows XP: Local Area Connection Properties



5 The **Internet Protocol TCP/IP Properties** window opens.

**Figure 125** Windows XP: Internet Protocol (TCP/IP) Properties




6 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided.

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

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

## Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

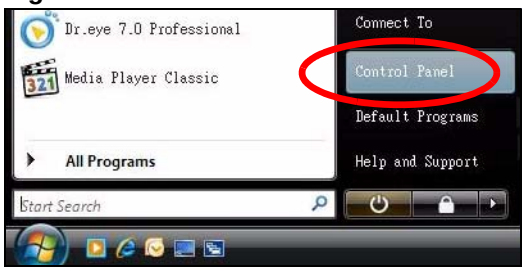
You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

# Windows Vista

This section shows screens from Windows Vista Professional.

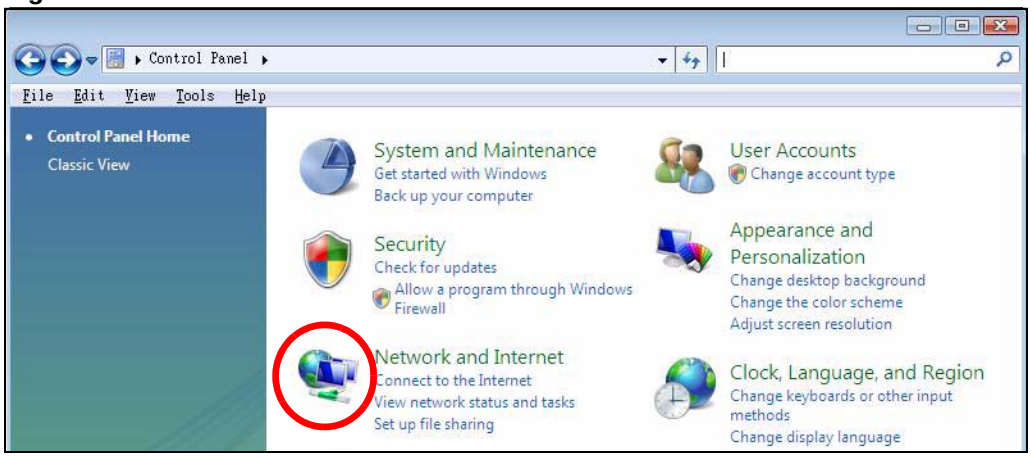
1 Click **Start** > **Control Panel**.

**Figure 126** Windows Vista: Start Menu



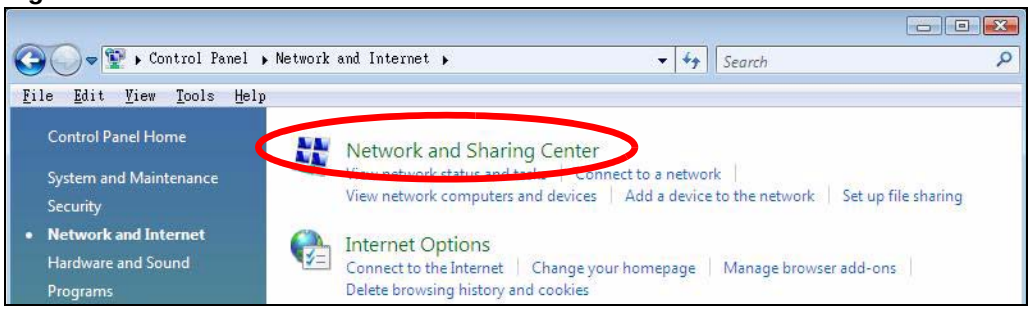

2 In the **Control Panel**, click the **Network and Internet** icon.

**Figure 127** Windows Vista: Control Panel



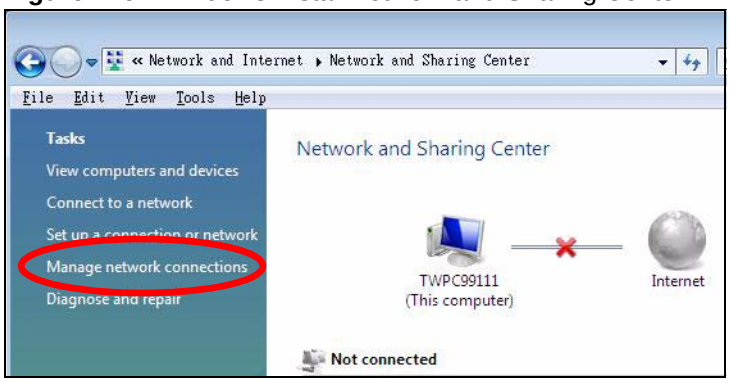

3 Click the **Network and Sharing Center** icon.

**Figure 128** Windows Vista: Network And Internet



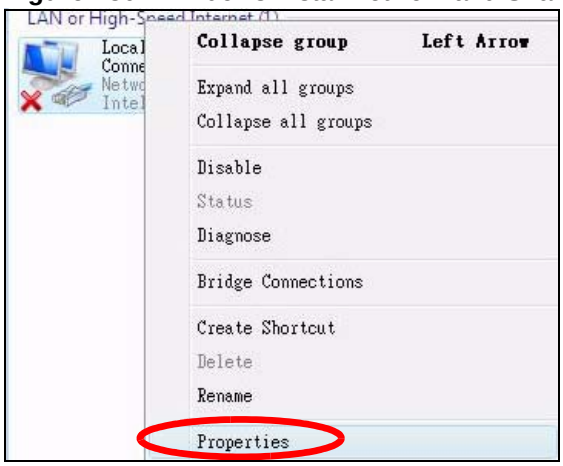
4 Click **Manage network connections**.

**Figure 129** Windows Vista: Network and Sharing Center




5 Right-click **Local Area Connection** and then select **Properties**.

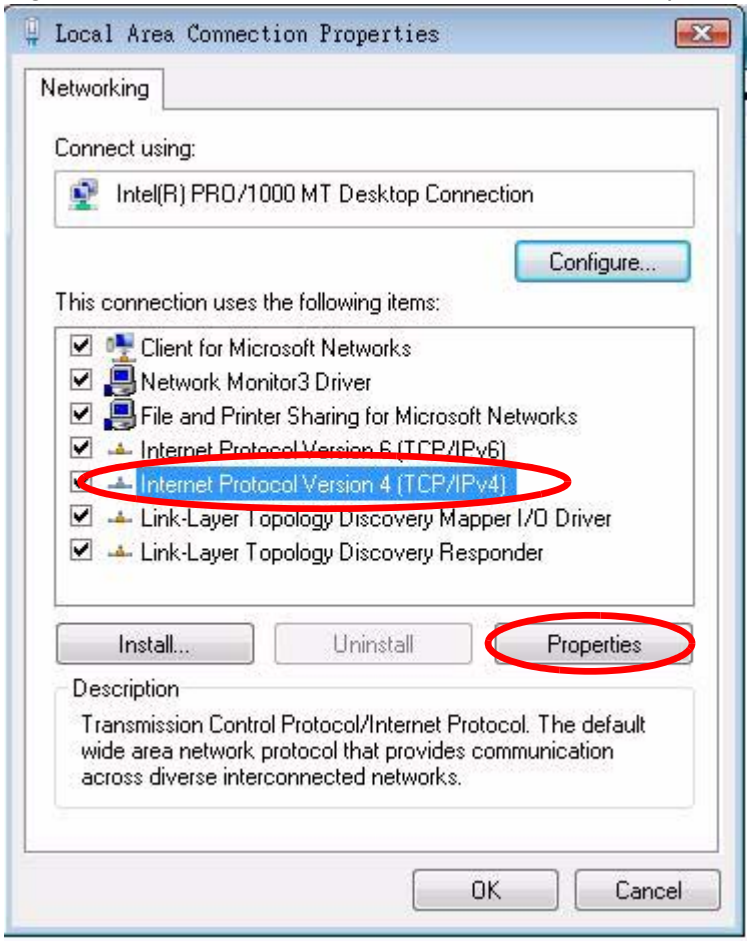
**Figure 130** Windows Vista: Network and Sharing Center




During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

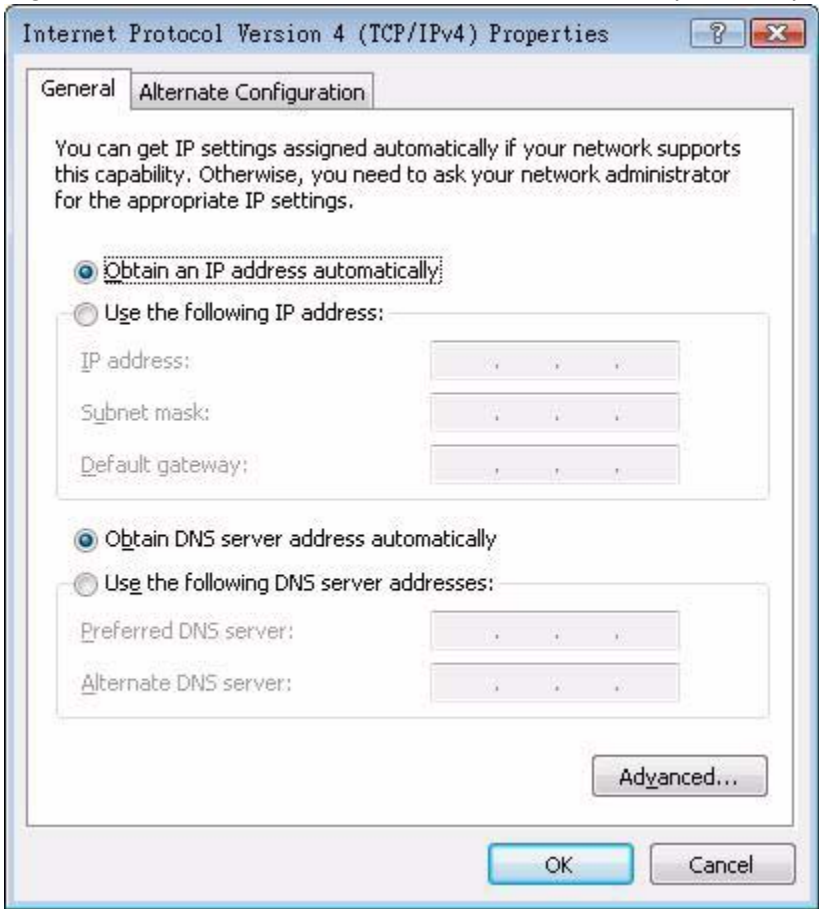
6 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.

**Figure 131** Windows Vista: Local Area Connection Properties



7 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens.

**Figure 132** Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties




8 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided.Click **Advanced**.

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

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

## Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

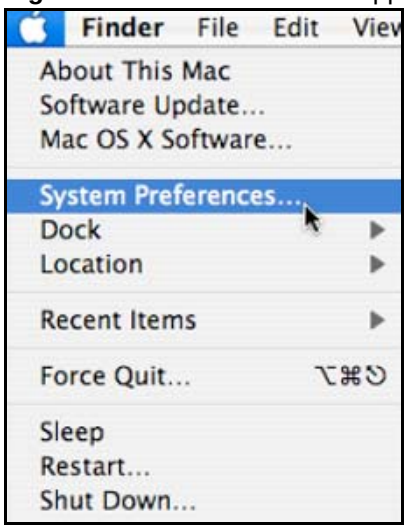
You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

# Mac OS X: 10.3 and 10.4

The screens in this section are from Mac OS X 10.4 but can also apply to 10.3.

1 Click **Apple** > **System Preferences**.

**Figure 133** Mac OS X 10.4: Apple Menu

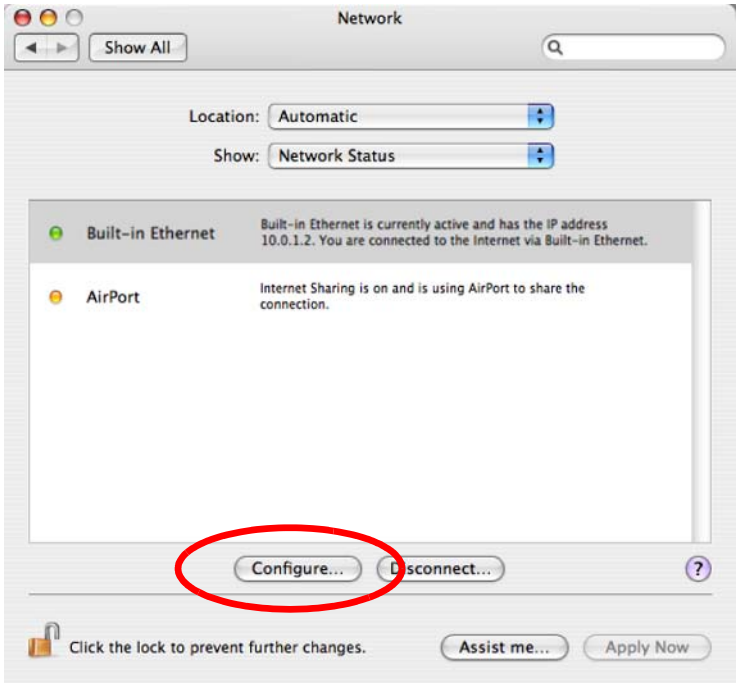



2 In the **System Preferences** window, click the **Network** icon.

**Figure 134** Mac OS X 10.4: System Preferences

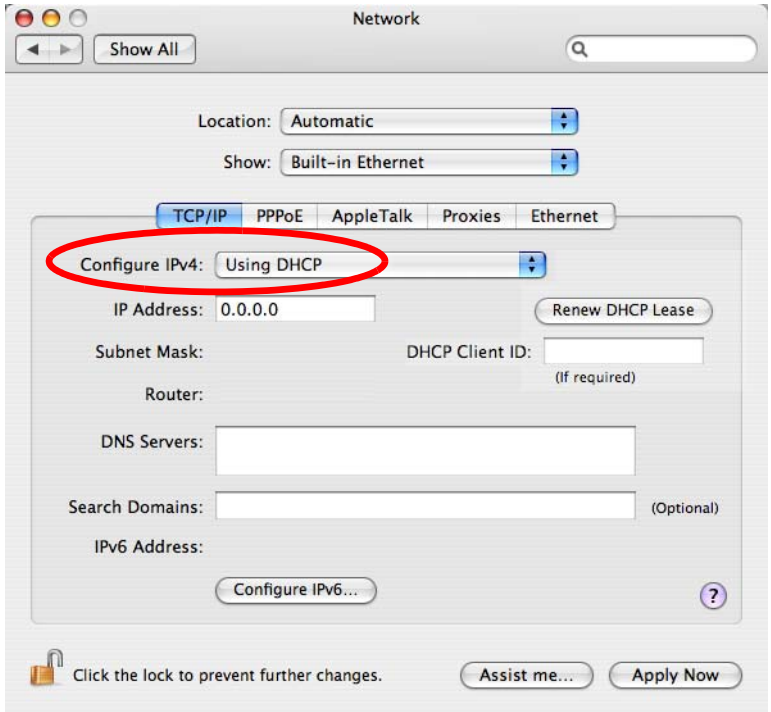
3 When the **Network** preferences pane opens, select **Built-in Ethernet** from the network connection type list, and then click **Configure.**

**Figure 135** Mac OS X 10.4: Network Preferences



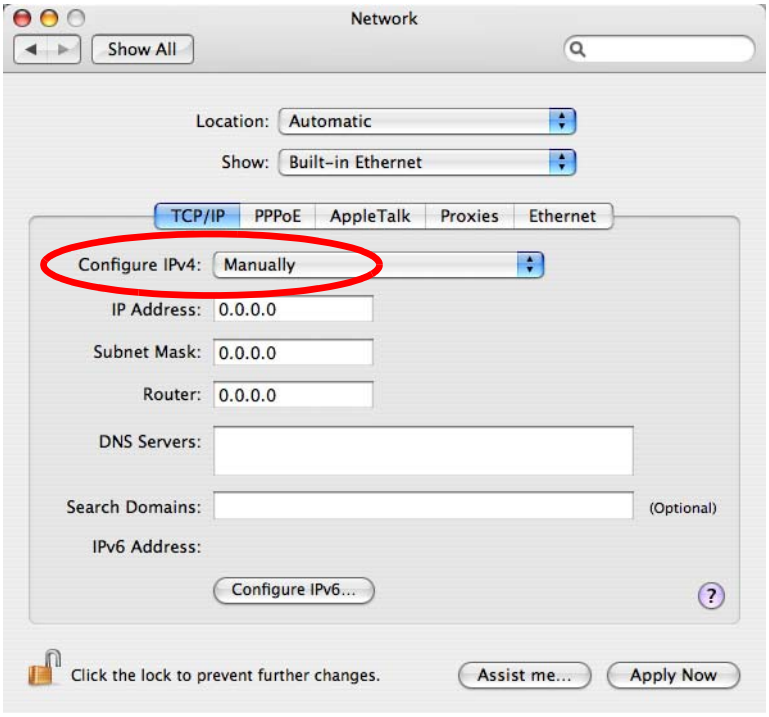

4 For dynamically assigned settings, select **Using DHCP** from the **Configure IPv4** list in the **TCP/IP** tab.

**Figure 136** Mac OS X 10.4: Network Preferences > TCP/IP Tab.



5 For statically assigned settings, do the following:
- From the **Configure IPv4** list, select **Manually**.
- In the **IP Address** field, type your IP address.
- In the **Subnet Mask** field, type your subnet mask.
- In the **Router** field, type the IP address of your device.

**Figure 137** Mac OS X 10.4: Network Preferences > Ethernet

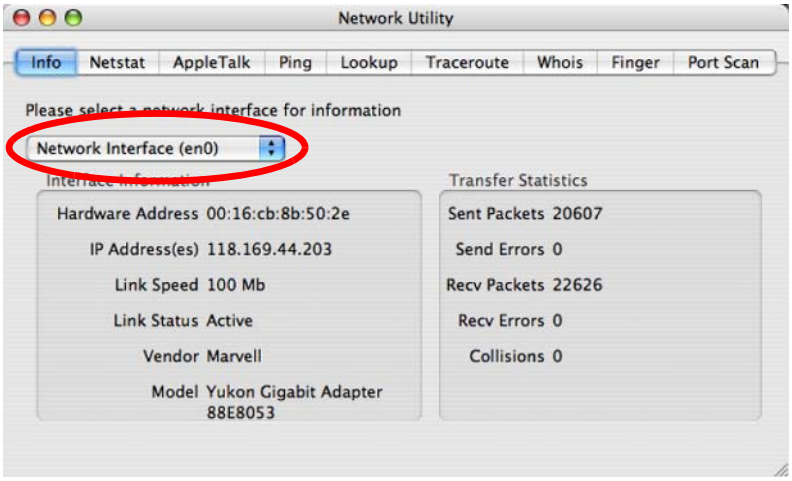



Click **Apply Now** and close the window.

## Verifying Settings

Check your TCP/IP properties by clicking **Applications** > **Utilities** > **Network Utilities**, and then selecting the appropriate **Network Interface** from the **Info** tab.

**Figure 138** Mac OS X 10.4: Network Utility

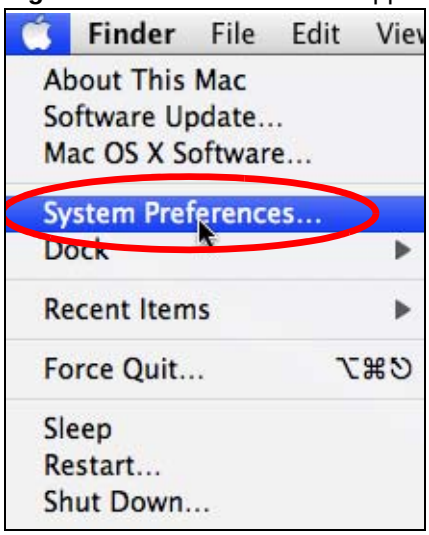


# Mac OS X: 10.5

The screens in this section are from Mac OS X 10.5.

1 Click **Apple** > **System Preferences**.

**Figure 139** Mac OS X 10.5: Apple Menu

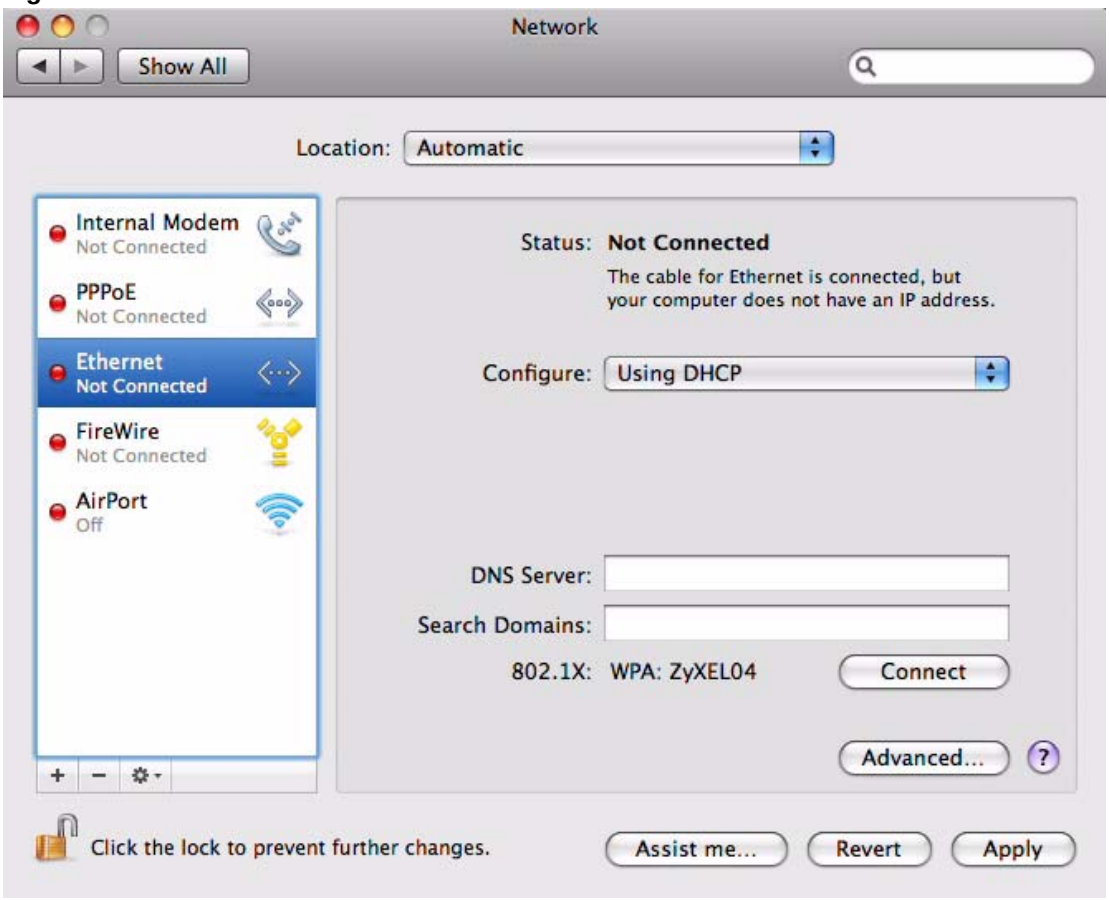



2 In **System Preferences**, click the **Network** icon.

**Figure 140** Mac OS X 10.5: Systems Preferences

3 When the **Network** preferences pane opens, select **Ethernet** from the list of available connection types.

**Figure 141** Mac OS X 10.5: Network Preferences > Ethernet

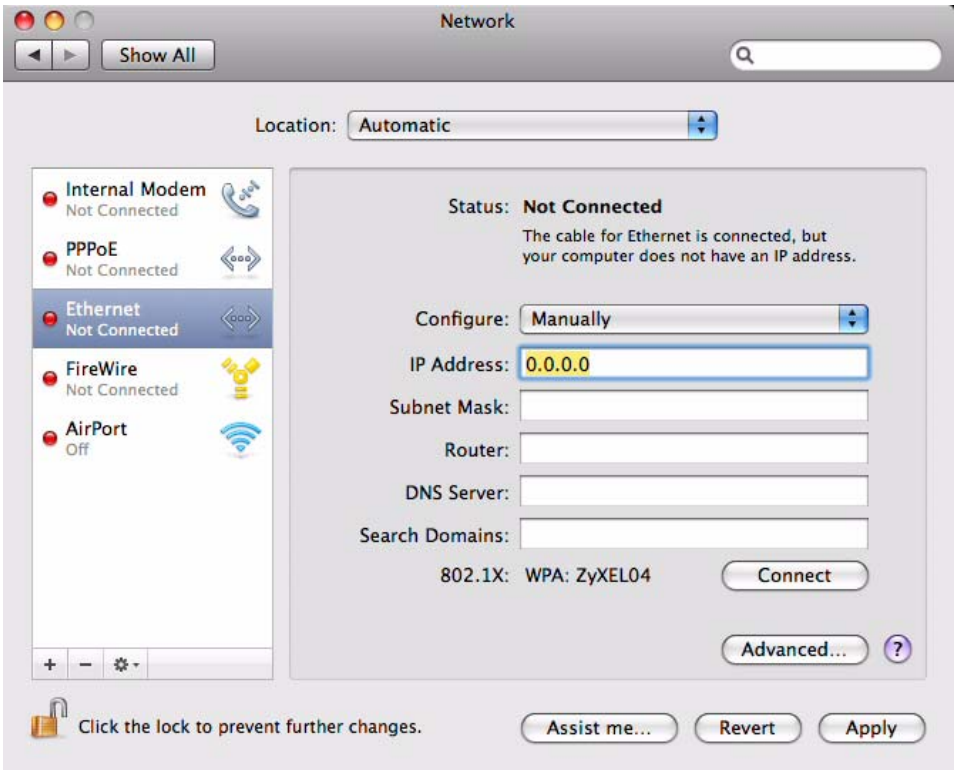



4 From the **Configure** list, select **Using DHCP** for dynamically assigned settings.

5 For statically assigned settings, do the following:

- From the **Configure** list, select **Manually**.
- In the **IP Address** field, enter your IP address.
- In the **Subnet Mask** field, enter your subnet mask.
- In the **Router** field, enter the IP address of your WiMAX Modem.

**Figure 142** Mac OS X 10.5: Network Preferences > Ethernet

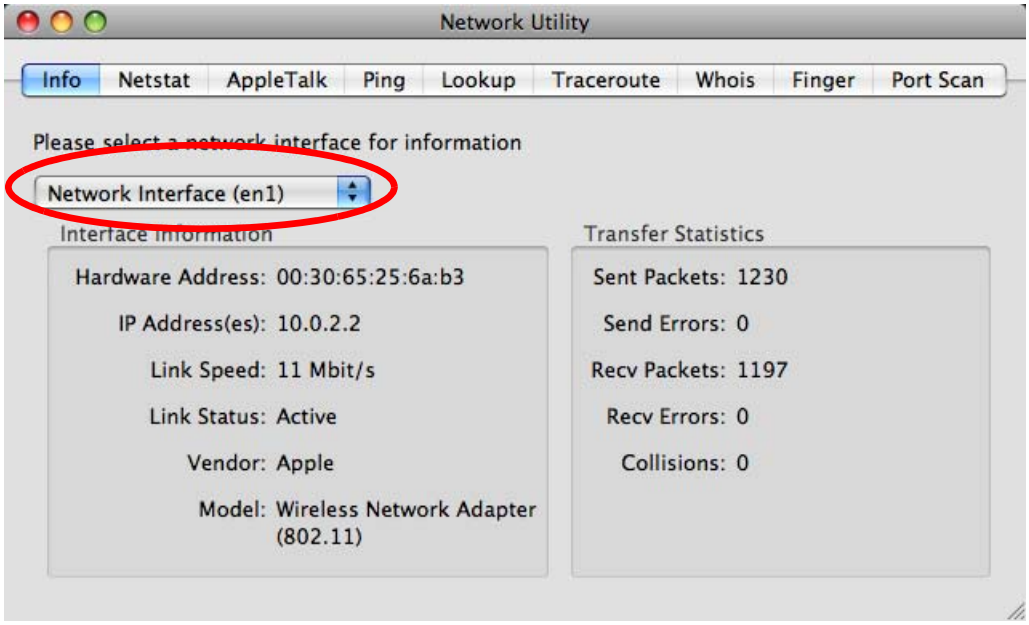



6 Click **Apply** and close the window.

## Verifying Settings

Check your TCP/IP properties by clicking **Applications** > **Utilities** > **Network Utilities**, and then selecting the appropriate **Network interface** from the **Info** tab.

**Figure 143** Mac OS X 10.5: Network Utility



# Linux: Ubuntu 8 (GNOME)

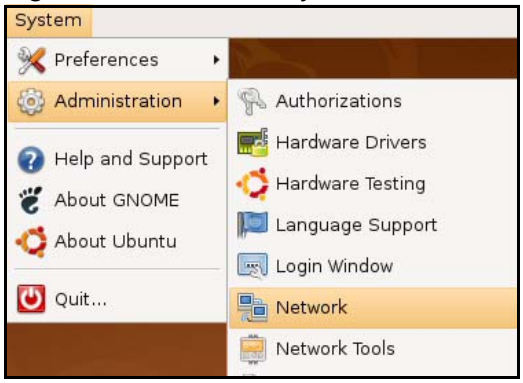
This section shows you how to configure your computer's TCP/IP settings in the GNU Object Model Environment (GNOME) using the Ubuntu 8 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default Ubuntu 8 installation.

Make sure you are logged in as the root administrator.

Follow the steps below to configure your computer IP address in GNOME:

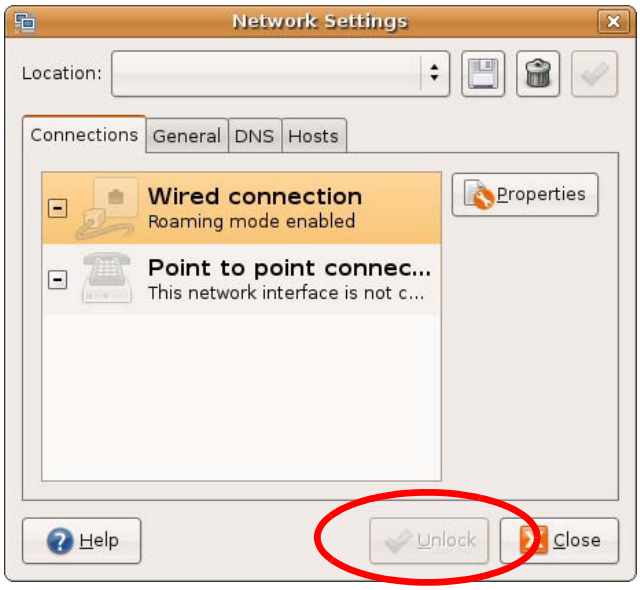
1 Click **System** > **Administration** > **Network**.

**Figure 144** Ubuntu 8: System > Administration Menu




2 When the **Network Settings** window opens, click **Unlock** to open the **Authenticate** window. (By default, the **Unlock** button is greyed out until clicked.) You cannot make changes to your configuration unless you first enter your admin password.

**Figure 145** Ubuntu 8: Network Settings > Connections



3 In the **Authenticate** window, enter your admin account name and password then click the **Authenticate** button.

**Figure 146** Ubuntu 8: Administrator Account Authentication


4 In the **Network Settings** window, select the connection that you want to configure, then click **Properties**.

**Figure 147** Ubuntu 8: Network Settings > Connections


5 The **Properties** dialog box opens.

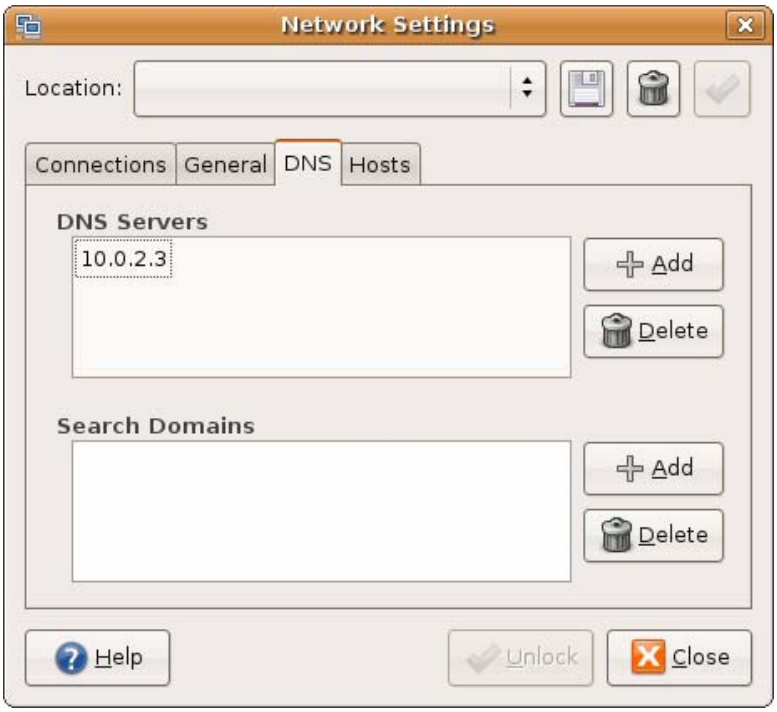
**Figure 148** Ubuntu 8: Network Settings > Properties


- In the **Configuration** list, select **Automatic Configuration (DHCP)** if you have a dynamic IP address.
- In the **Configuration** list, select **Static IP address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Gateway address** fields.

6 Click **OK** to save the changes and close the **Properties** dialog box and return to the **Network Settings** screen.

7 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Settings** window and then enter the DNS server information in the fields provided.

**Figure 149** Ubuntu 8: Network Settings > DNS

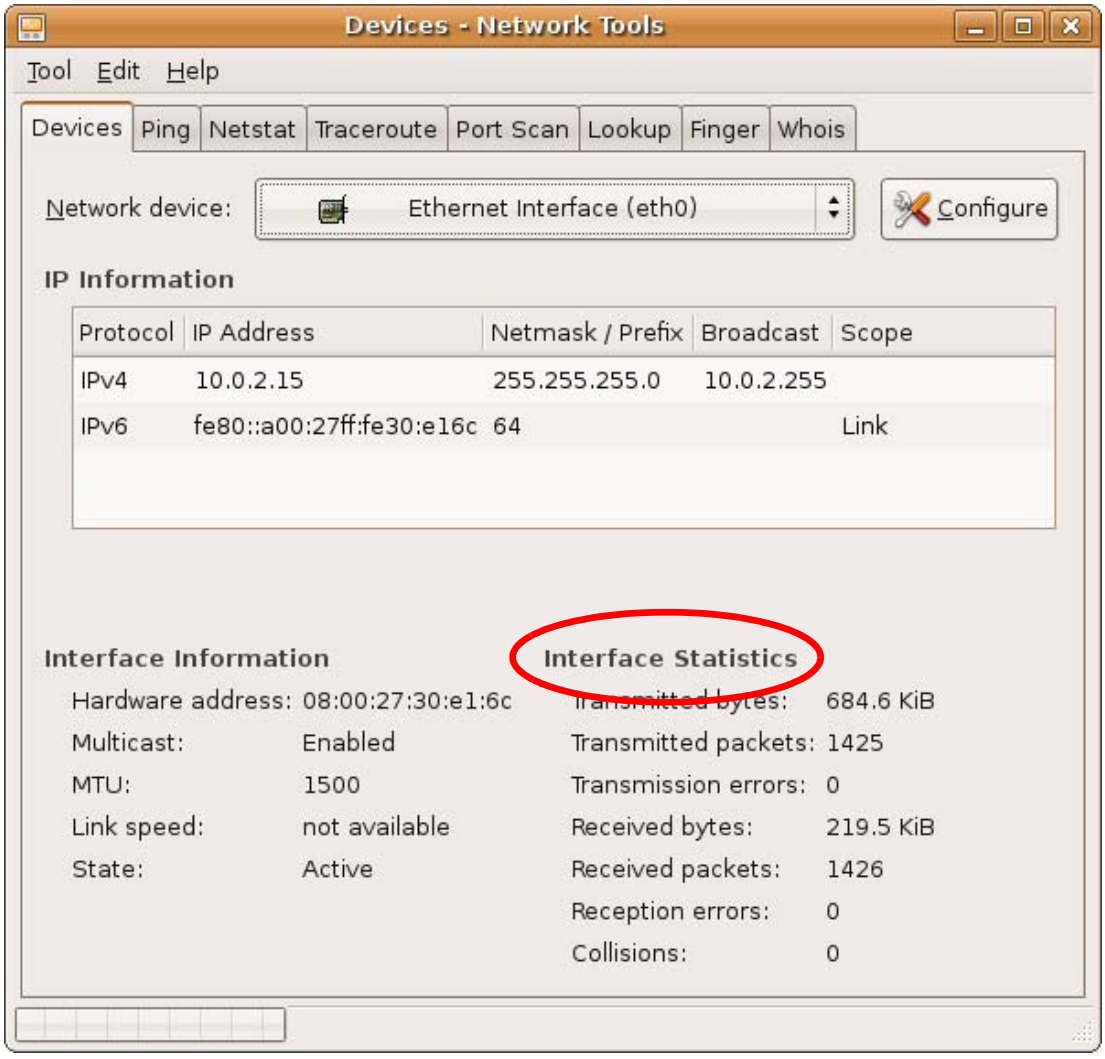



8 Click the **Close** button to apply the changes.

## Verifying Settings

Check your TCP/IP properties by clicking **System > Administration > Network Tools**, and then selecting the appropriate **Network device** from the **Devices** tab. The **Interface Statistics** column shows data if your connection is working properly.

**Figure 150** Ubuntu 8: Network Tools



# Linux: openSUSE 10.3 (KDE)

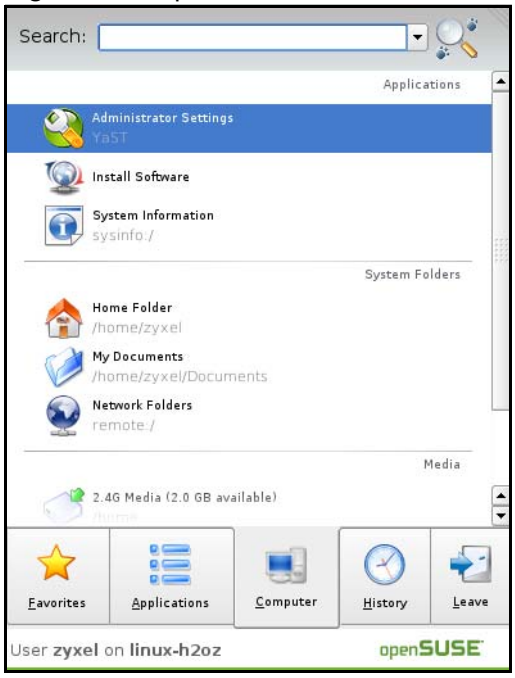
This section shows you how to configure your computer's TCP/IP settings in the K Desktop Environment (KDE) using the openSUSE 10.3 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default openSUSE 10.3 installation.

Make sure you are logged in as the root administrator.

Follow the steps below to configure your computer IP address in the KDE:

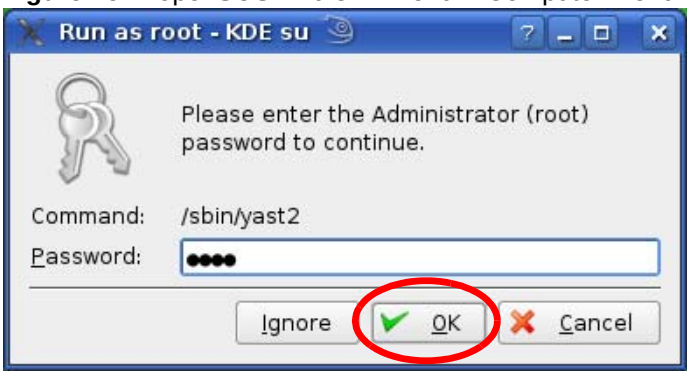
1 Click **K Menu** > **Computer** > **Administrator Settings (YaST)**.

**Figure 151** openSUSE 10.3: K Menu > Computer Menu



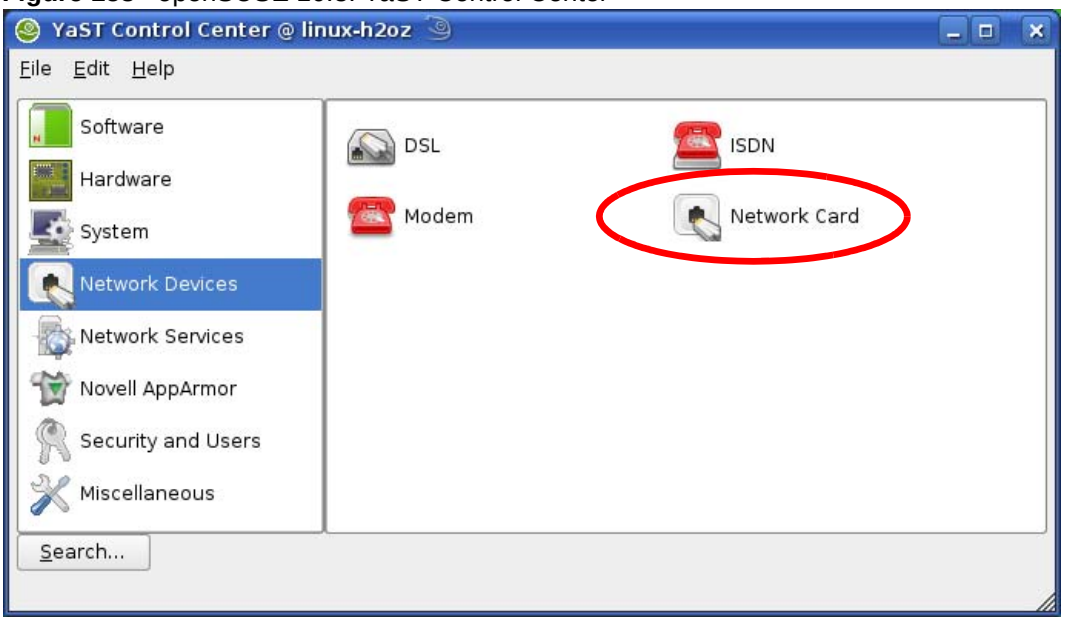

2 When the **Run as Root - KDE su** dialog opens, enter the admin password and click **OK**.

**Figure 152** openSUSE 10.3: K Menu > Computer Menu



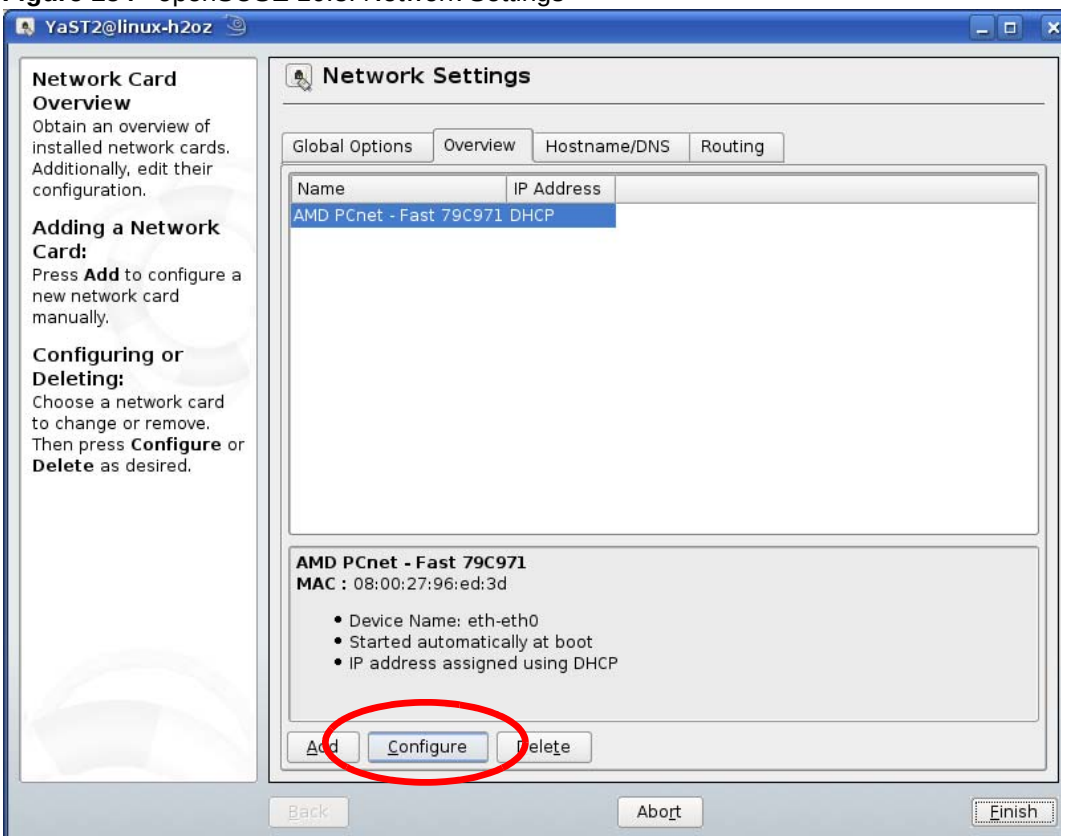
3 When the **YaST Control Center** window opens, select **Network Devices** and then click the **Network Card** icon.

**Figure 153** openSUSE 10.3: YaST Control Center



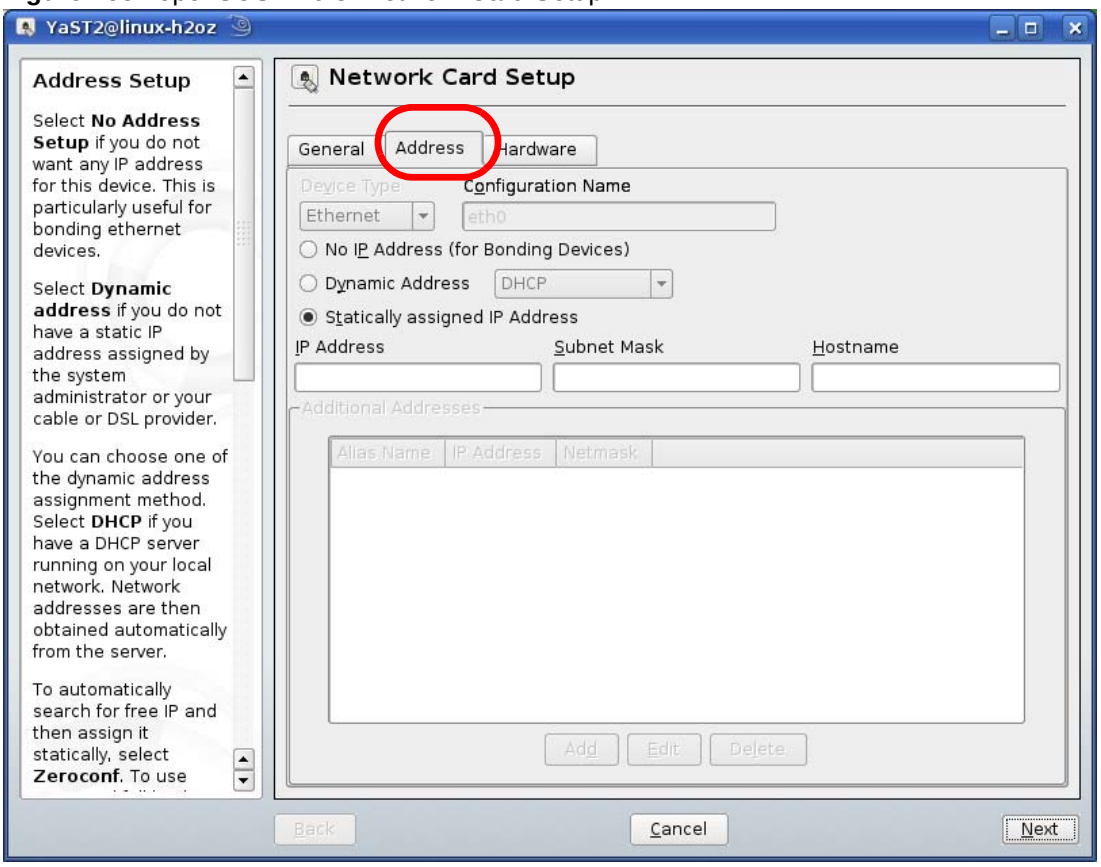

4 When the **Network Settings** window opens, click the **Overview** tab, select the appropriate connection **Name** from the list, and then click the **Configure** button.

**Figure 154** openSUSE 10.3: Network Settings



5 When the **Network Card Setup** window opens, click the **Address** tab

**Figure 155** openSUSE 10.3: Network Card Setup

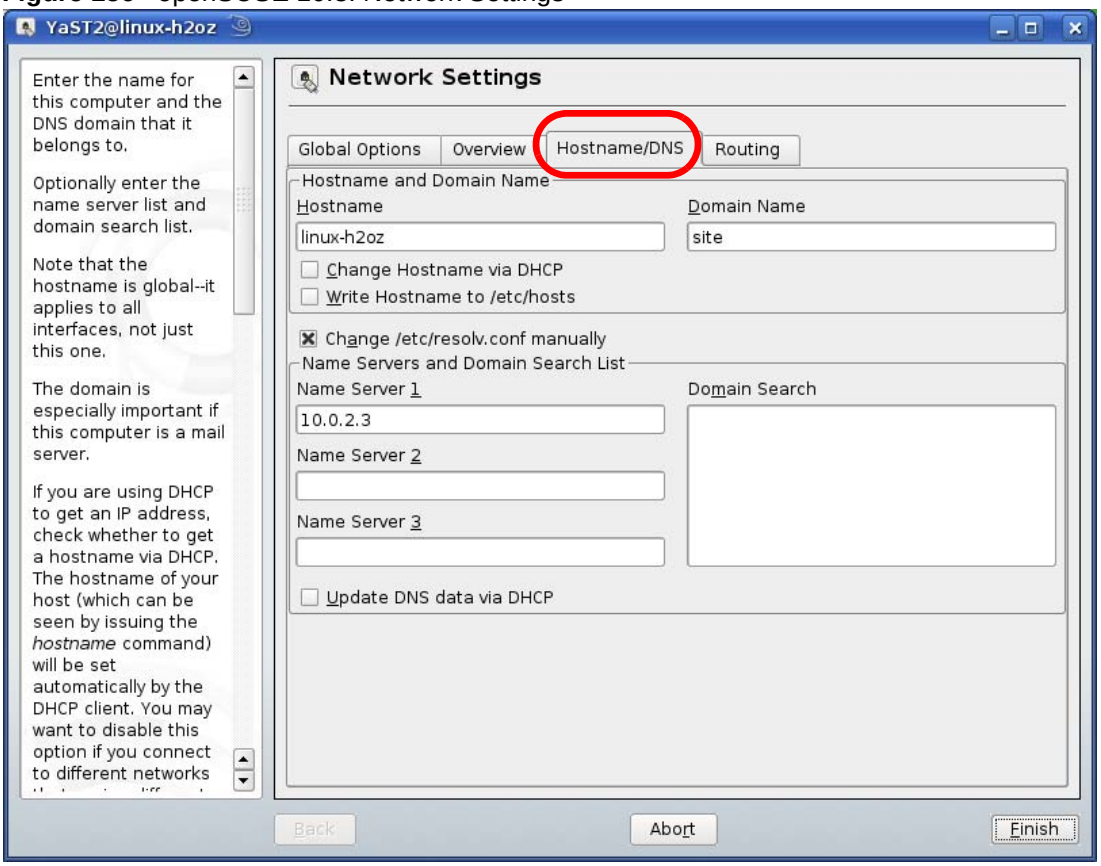



6 Select **Dynamic Address (DHCP)** if you have a dynamic IP address.
Select **Statically assigned IP Address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Hostname** fields.

7 Click **Next** to save the changes and close the **Network Card Setup** window.

8 If you know your DNS server IP address(es), click the **Hostname/DNS** tab in **Network Settings** and then enter the DNS server information in the fields provided.

**Figure 156** openSUSE 10.3: Network Settings

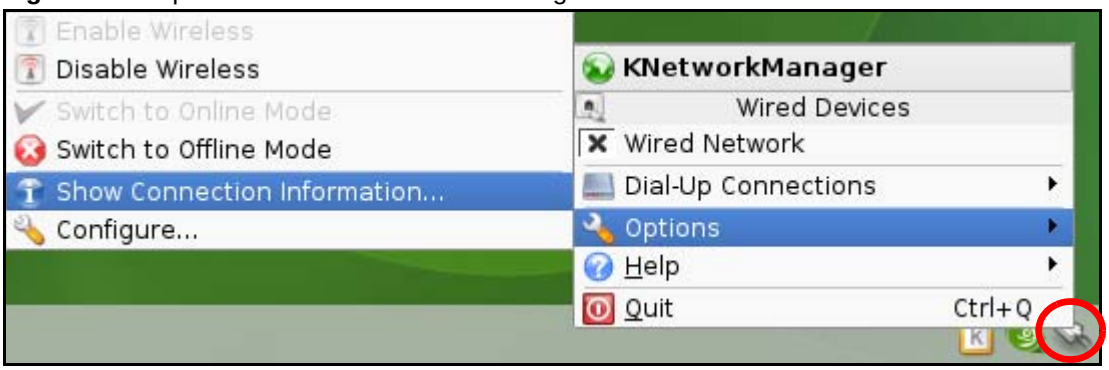



9 Click **Finish** to save your settings and close the window.

## Verifying Settings

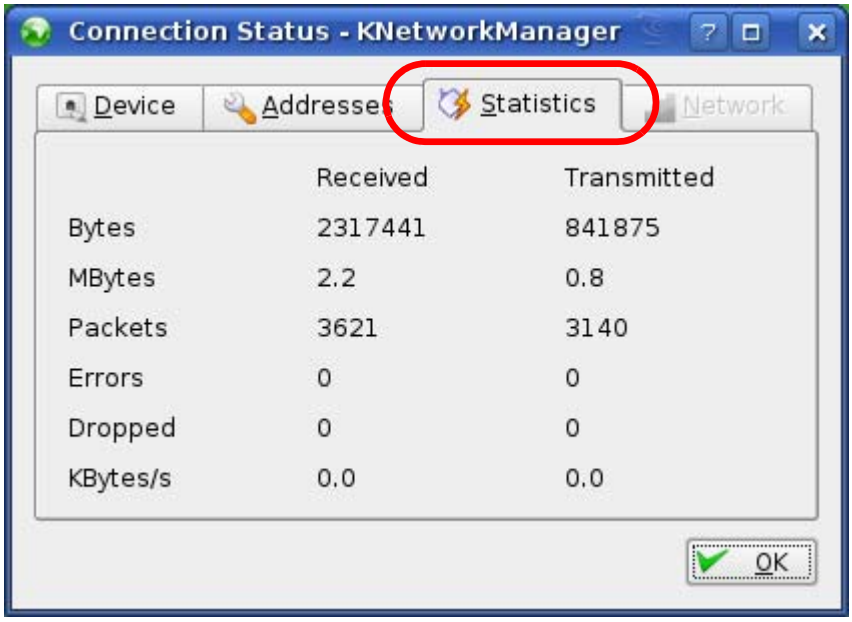
Click the **KNetwork Manager** icon on the **Task bar** to check your TCP/IP properties. From the **Options** sub-menu, select **Show Connection Information**.

**Figure 157** openSUSE 10.3: KNetwork Manager




When the **Connection Status - KNetwork Manager** window opens, click the **Statistics tab** to see if your connection is working properly.

**Figure 158** openSUSE: Connection Status - KNetwork Manager



C

# Pop-up Windows, JavaScripts and Java Permissions

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

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

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

## Internet Explorer Pop-up Blockers

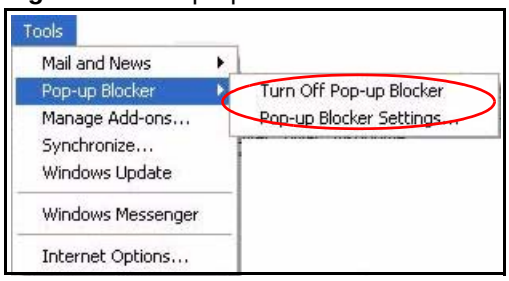
You may have to disable pop-up blocking to log into your device.

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

### Disable Pop-up Blockers

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

**Figure 159** Pop-up Blocker




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

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

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

**Figure 160** Internet Options: Privacy


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

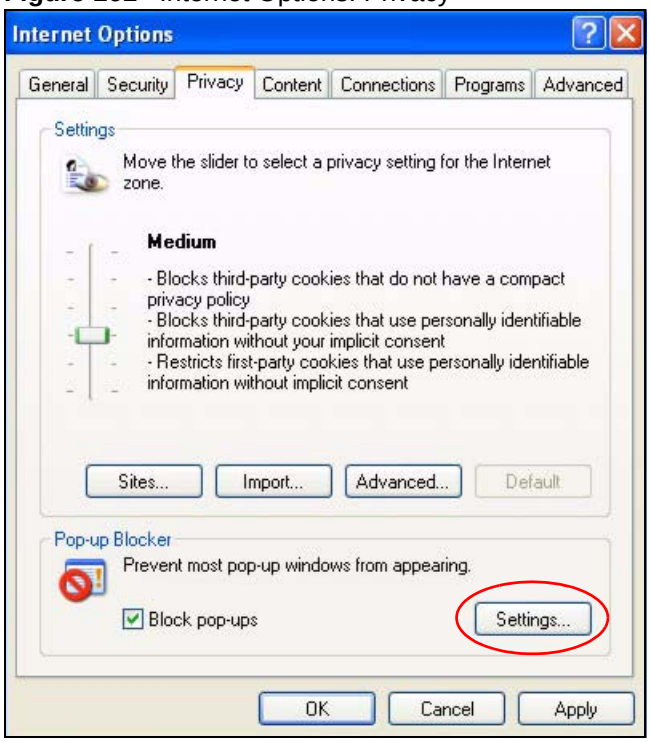
## Enable Pop-up Blockers with Exceptions

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

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

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

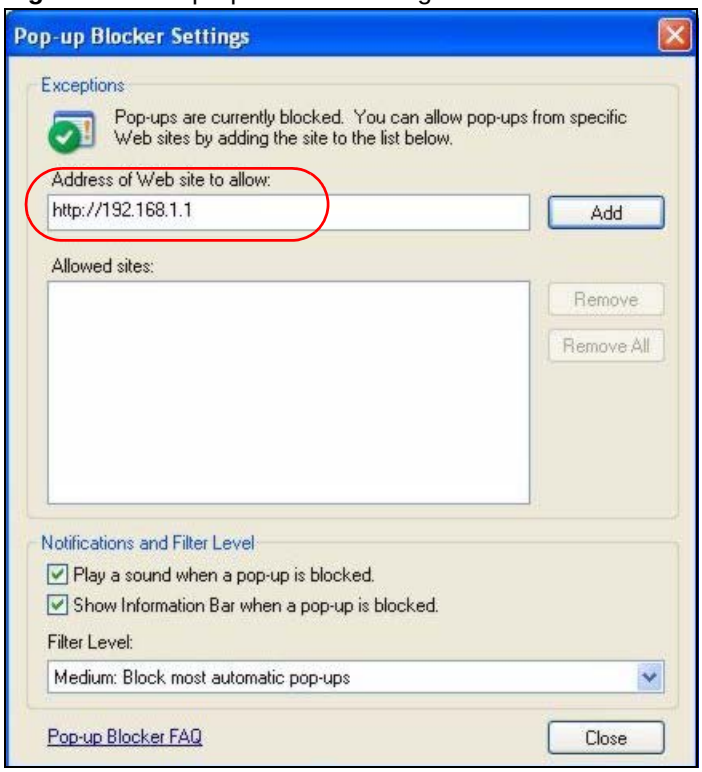
**Figure 161** Internet Options: Privacy




3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.167.1.

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

**Figure 162** Pop-up Blocker Settings



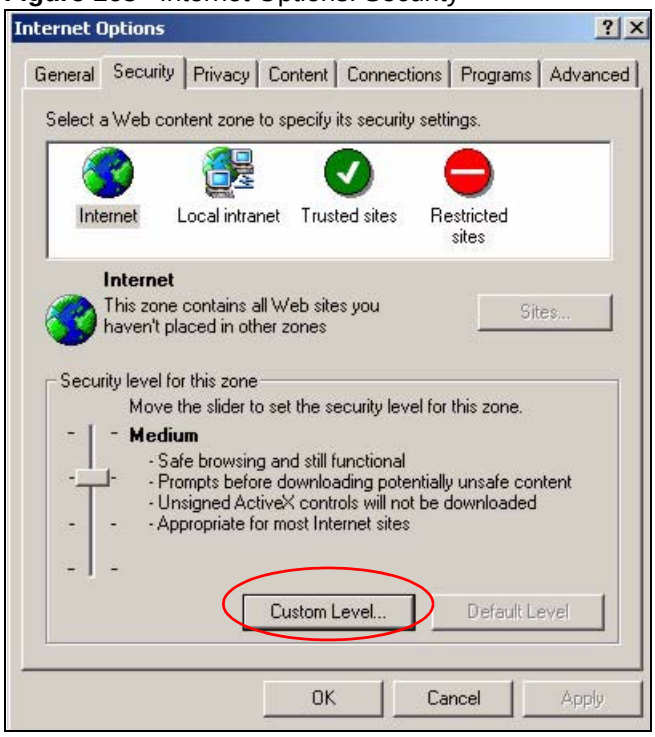
5 Click **Close** to return to the **Privacy** screen.
6 Click **Apply** to save this setting.

# JavaScripts

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

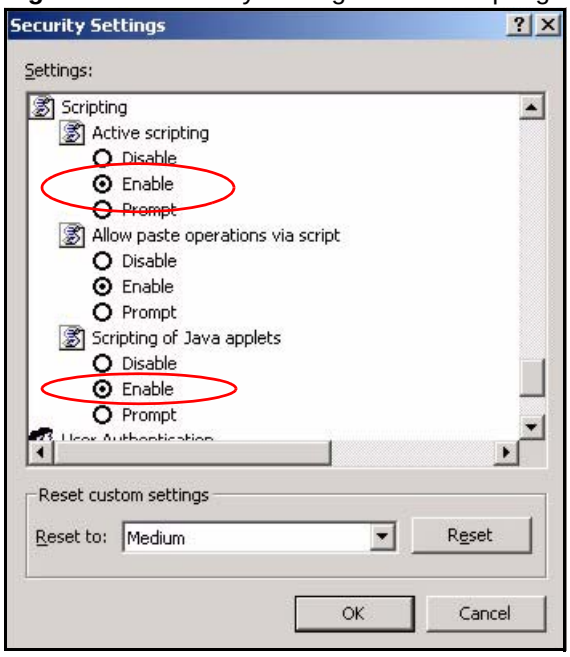
1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

**Figure 163** Internet Options: Security




2 Click the **Custom Level...** button.
3 Scroll down to **Scripting**.
4 Under **Active scripting** make sure that **Enable** is selected (the default).
5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).
6 Click **OK** to close the window.

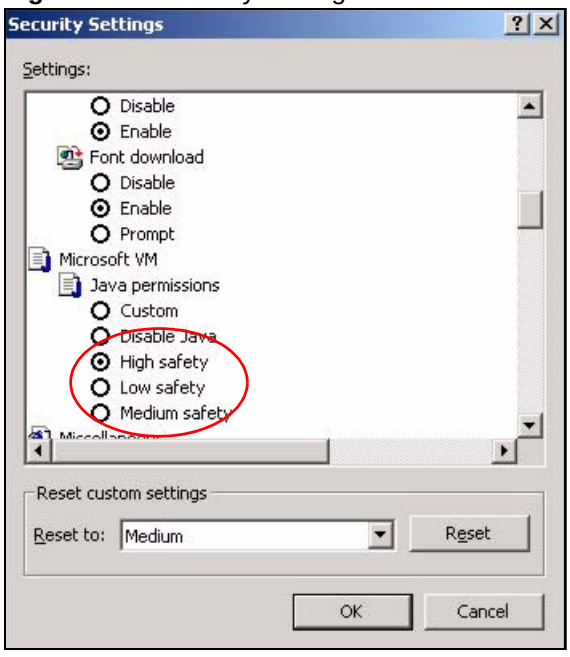
**Figure 164** Security Settings - Java Scripting




## Java Permissions

1. From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.
2. Click the **Custom Level...** button.
3. Scroll down to **Microsoft VM**.
4. Under **Java permissions** make sure that a safety level is selected.
5. Click **OK** to close the window.

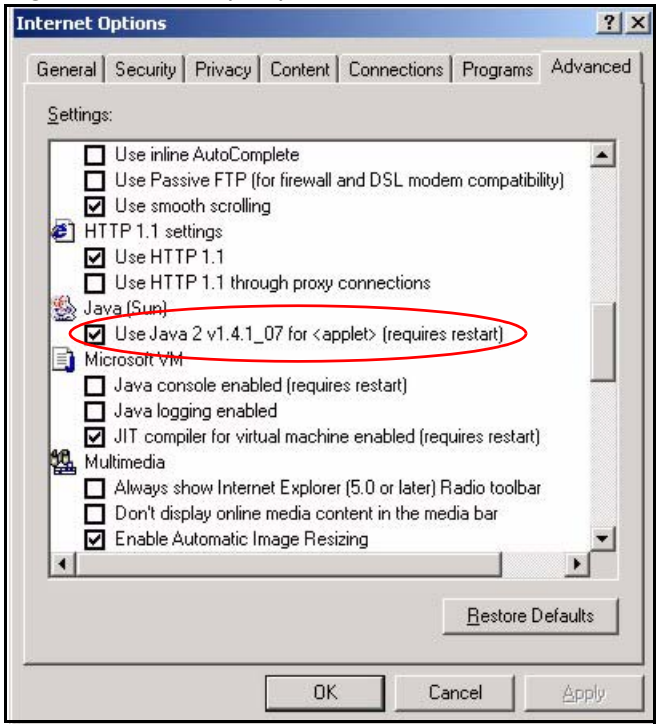
**Figure 165** Security Settings - Java



## JAVA (Sun)

1. From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.
2. Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.
3. Click **OK** to close the window.

**Figure 166** Java (Sun)



# Mozilla Firefox

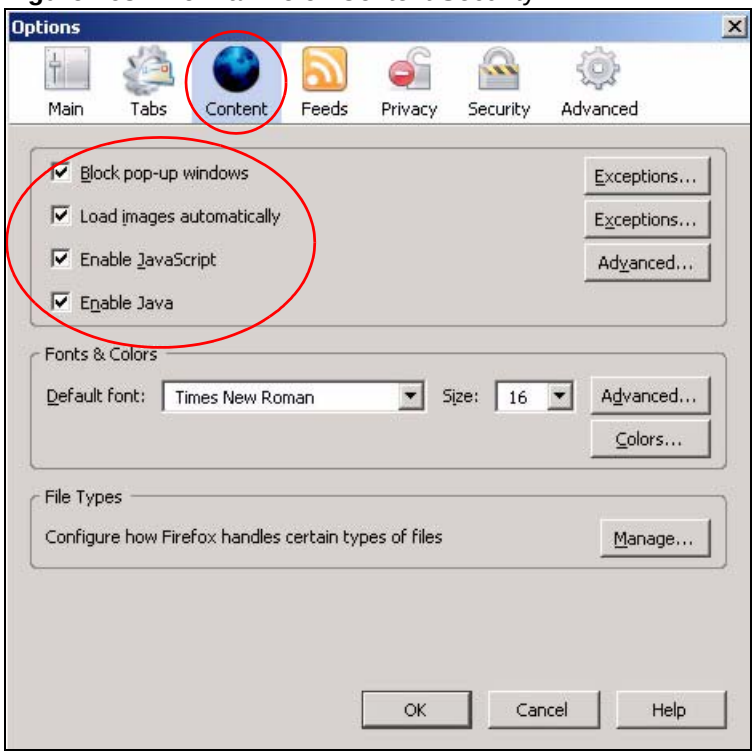
Mozilla Firefox 2.0 screens are used here. Screens for other versions may vary.

You can enable Java, Javascripts and pop-ups in one screen. Click **Tools,** then click **Options** in the screen that appears.

**Figure 167** Mozilla Firefox: TOOLS > Options


Click **Content**.to show the screen below. Select the check boxes as shown in the following screen.

**Figure 168** Mozilla Firefox Content Security



D

# IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

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

## Introduction to IP Addresses

One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

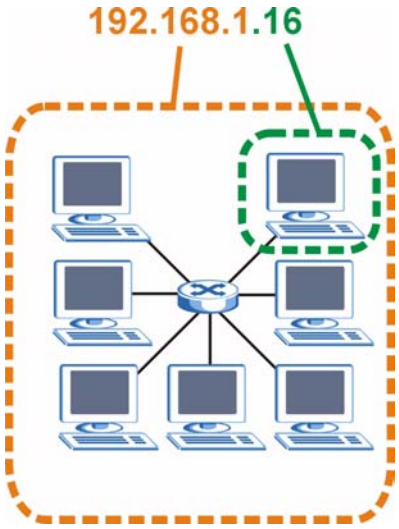
## Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.100.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

**Figure 169** Network Number and Host ID




How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

## Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term "subnet" is short for "sub-network".

A subnet mask has 32 bits. If a bit in the subnet mask is a "1" then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is "0" then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

**Table 113** IP Address Network Number and Host ID Example

| | 1ST OCTET: (192) | 2ND OCTET: (168) | 3RD OCTET: (1) | 4TH OCTET (2) |
|---|---|---|---|---|
| IP Address (Binary) | 11000000 | 10101000 | 00000001 | 00000010 |
| Subnet Mask (Binary) | **11111111** | **11111111** | **11111111** | 00000000 |
| Network Number | **11000000** | **10101000** | **00000001** | |
| Host ID | | | | 00000010 |

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a “1” value). For example, an “8-bit mask” means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

**Table 114** Subnet Masks

| | BINARY | | | | DECIMAL |
|---|---|---|---|---|---|
| | 1ST OCTET | 2ND OCTET | 3RD OCTET | 4TH OCTET | |
| 8-bit mask | 11111111 | 00000000 | 00000000 | 00000000 | 255.0.0.0 |
| 16-bit mask | 11111111 | 11111111 | 00000000 | 00000000 | 255.255.0.0 |
| 24-bit mask | 11111111 | 11111111 | 11111111 | 00000000 | 255.255.255.0 |
| 29-bit mask | 11111111 | 11111111 | 11111111 | 11111000 | 255.255.255.248 |

### Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

**Table 115** Maximum Host Numbers

| SUBNET MASK | | HOST ID SIZE | | MAXIMUM NUMBER OF HOSTS |
|---|---|---|---|---|
| 8 bits | 255.0.0.0 | 24 bits | $2^{24} – 2$ | 16777214 |
| 16 bits | 255.255.0.0 | 16 bits | $2^{16} – 2$ | 65534 |
| 24 bits | 255.255.255.0 | 8 bits | $2^{8} – 2$ | 254 |
| 29 bits | 255.255.255.248 | 3 bits | $2^{3} – 2$ | 6 |

## Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a “/” followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

**Table 116** Alternative Subnet Mask Notation

| SUBNET MASK | ALTERNATIVE NOTATION | LAST OCTET (BINARY) | LAST OCTET (DECIMAL) |
|---|---|---|---|
| 255.255.255.0 | /24 | 0000 0000 | 0 |
| 255.255.255.128 | /25 | 1000 0000 | 128 |
| 255.255.255.192 | /26 | 1100 0000 | 192 |
| 255.255.255.224 | /27 | 1110 0000 | 224 |
| 255.255.255.240 | /28 | 1111 0000 | 240 |
| 255.255.255.248 | /29 | 1111 1000 | 248 |
| 255.255.255.252 | /30 | 1111 1100 | 252 |

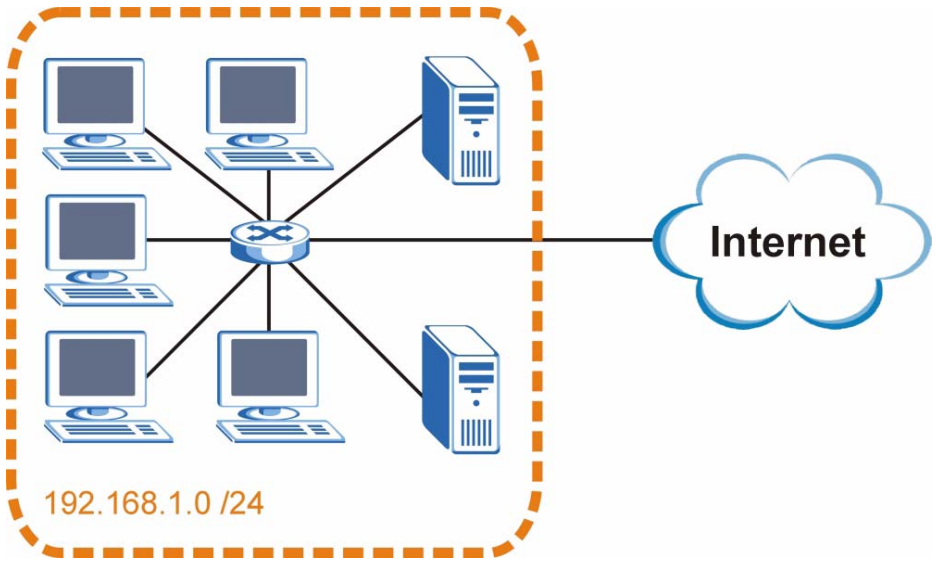
# Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of $2^8 - 2$ or 254 possible hosts.

The following figure shows the company network before subnetting.

**Figure 170** Subnetting Example: Before Subnetting

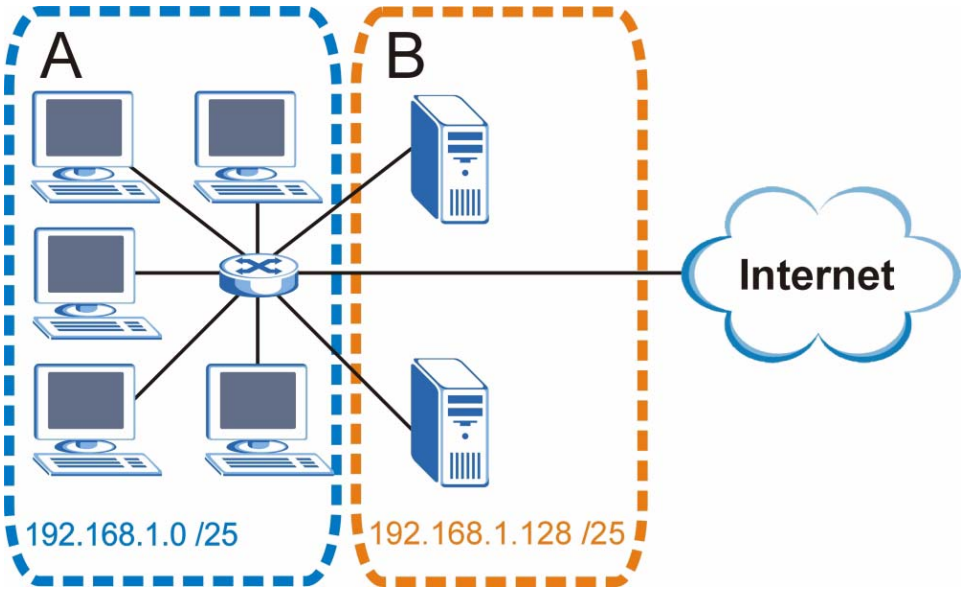



You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The “borrowed” host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.100.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

**Figure 171** Subnetting Example: After Subnetting




In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of $2^7 - 2$ or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.100.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.100.1 and the highest is 192.168.100.126.

Similarly, the host ID range for subnet **B** is 192.168.100.129 to 192.168.1.254.

## Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving $2^6$ - 2 or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

**Table 117** Subnet 1

| IP/SUBNET MASK | NETWORK NUMBER | LAST OCTET BIT VALUE |
|---|---|---|
| IP Address (Decimal) | 192.168.1. | 0 |
| IP Address (Binary) | 11000000.10101000.00000001. | **00**000000 |
| Subnet Mask (Binary) | 11111111.11111111.11111111. | **11**000000 |

**Table 117** Subnet 1 (continued)

| IP/SUBNET MASK | NETWORK NUMBER | LAST OCTET BIT VALUE |
|---|---|---|
| Subnet Address: 192.168.1.0 | Lowest Host ID: 192.168.100.1 | |
| Broadcast Address: 192.168.1.63 | Highest Host ID: 192.168.1.62 | |

**Table 118** Subnet 2

| IP/SUBNET MASK | NETWORK NUMBER | LAST OCTET BIT VALUE |
|---|---|---|
| IP Address | 192.168.1. | 64 |
| IP Address (Binary) | 11000000.10101000.00000001. | **01**000000 |
| Subnet Mask (Binary) | 11111111.11111111.11111111. | **11**000000 |
| Subnet Address: 192.168.1.64 | Lowest Host ID: 192.168.1.65 | |
| Broadcast Address: 192.168.100.127 | Highest Host ID: 192.168.100.126 | |

**Table 119** Subnet 3

| IP/SUBNET MASK | NETWORK NUMBER | LAST OCTET BIT VALUE |
|---|---|---|
| IP Address | 192.168.1. | 128 |
| IP Address (Binary) | 11000000.10101000.00000001. | **10**000000 |
| Subnet Mask (Binary) | 11111111.11111111.11111111. | **11**000000 |
| Subnet Address: 192.168.100.128 | Lowest Host ID: 192.168.100.129 | |
| Broadcast Address: 192.168.100.191 | Highest Host ID: 192.168.100.190 | |

**Table 120** Subnet 4

| IP/SUBNET MASK | NETWORK NUMBER | LAST OCTET BIT VALUE |
|---|---|---|
| IP Address | 192.168.1. | 192 |
| IP Address (Binary) | 11000000.10101000.00000001. | **11**000000 |
| Subnet Mask (Binary) | 11111111.11111111.11111111. | **11**000000 |
| Subnet Address: 192.168.100.192 | Lowest Host ID: 192.168.100.193 | |
| Broadcast Address: 192.168.1.255 | Highest Host ID: 192.168.1.254 | |

## Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

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

**Table 121** Eight Subnets

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

## Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

**Table 122** 24-bit Network Number Subnet Planning

| NO. “BORROWED” HOST BITS | SUBNET MASK | NO. SUBNETS | NO. HOSTS PER SUBNET |
|---|---|---|---|
| 1 | 255.255.255.128 (/25) | 2 | 126 |
| 2 | 255.255.255.192 (/26) | 4 | 62 |
| 3 | 255.255.255.224 (/27) | 8 | 30 |
| 4 | 255.255.255.240 (/28) | 16 | 14 |
| 5 | 255.255.255.248 (/29) | 32 | 6 |
| 6 | 255.255.255.252 (/30) | 64 | 2 |
| 7 | 255.255.255.254 (/31) | 128 | 1 |

The following table is a summary for subnet planning on a network with a 16-bit network number.

**Table 123** 16-bit Network Number Subnet Planning

| NO. “BORROWED” HOST BITS | SUBNET MASK | NO. SUBNETS | NO. HOSTS PER SUBNET |
|---|---|---|---|
| 1 | 255.255.128.0 (/17) | 2 | 32766 |
| 2 | 255.255.192.0 (/18) | 4 | 16382 |
| 3 | 255.255.224.0 (/19) | 8 | 8190 |
| 4 | 255.255.240.0 (/20) | 16 | 4094 |
| 5 | 255.255.248.0 (/21) | 32 | 2046 |

**Table 123** 16-bit Network Number Subnet Planning (continued)

| NO. "BORROWED" HOST BITS | SUBNET MASK | NO. SUBNETS | NO. HOSTS PER SUBNET |
|---|---|---|---|
| 6 | 255.255.252.0 (/22) | 64 | 1022 |
| 7 | 255.255.254.0 (/23) | 128 | 510 |
| 8 | 255.255.255.0 (/24) | 256 | 254 |
| 9 | 255.255.255.128 (/25) | 512 | 126 |
| 10 | 255.255.255.192 (/26) | 1024 | 62 |
| 11 | 255.255.255.224 (/27) | 2048 | 30 |
| 12 | 255.255.255.240 (/28) | 4096 | 14 |
| 13 | 255.255.255.248 (/29) | 8192 | 6 |
| 14 | 255.255.255.252 (/30) | 16384 | 2 |
| 15 | 255.255.255.254 (/31) | 32768 | 1 |

# Configuring IP Addresses

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. 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. You must also enable Network Address Translation (NAT) on the WiMAX Modem.

Once you have decided on the network number, pick an IP address for your WiMAX Modem that is easy to remember (for instance, 192.168.100.1) 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.

## Private IP Addresses

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

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

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

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

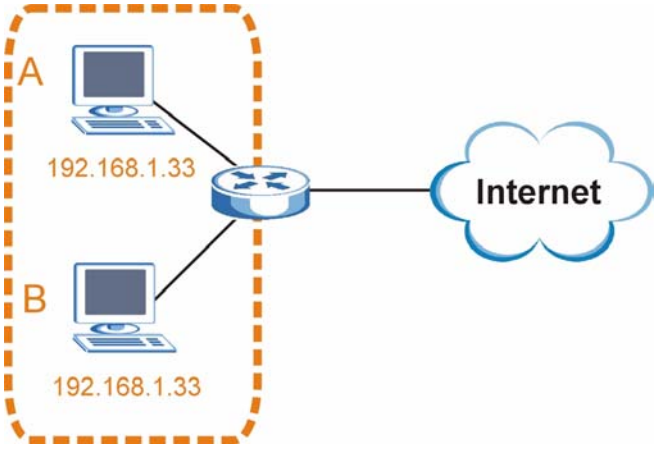
# IP Address Conflicts

Each device on a network must have a unique IP address. Devices with duplicate IP addresses on the same network will not be able to access the Internet or other resources. The devices may also be unreachable through the network.

## Conflicting Computer IP Addresses Example

More than one device can not use the same IP address. In the following example computer **A** has a static (or fixed) IP address that is the same as the IP address that a DHCP server assigns to computer **B** which is a DHCP client. Neither can access the Internet. This problem can be solved by assigning a different static IP address to computer **A** or setting computer **A** to obtain an IP address automatically.

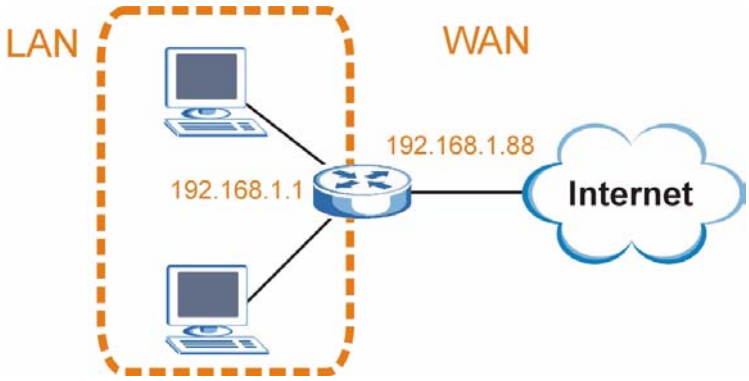
**Figure 172** Conflicting Computer IP Addresses Example



## Conflicting Router IP Addresses Example

Since a router connects different networks, it must have interfaces using different network numbers. For example, if a router is set between a LAN and the Internet (WAN), the router's LAN and WAN addresses must be on different subnets. In the following example, the LAN and WAN are on the same subnet. The LAN computers cannot access the Internet because the router cannot route between networks.

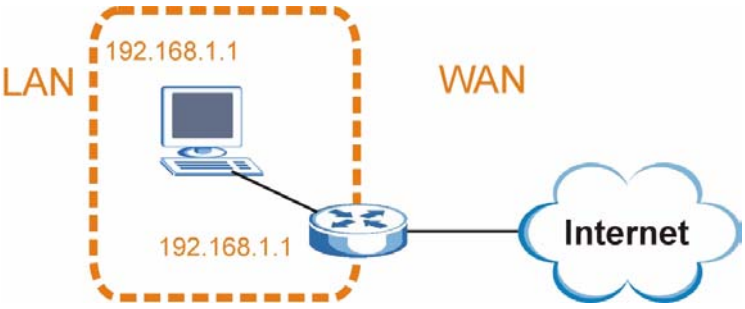
**Figure 173** Conflicting Computer IP Addresses Example




## Conflicting Computer and Router IP Addresses Example

More than one device can not use the same IP address. In the following example, the computer and the router's LAN port both use 192.168.100.1 as the IP address. The computer cannot access the Internet. This problem can be solved by assigning a different IP address to the computer or the router's LAN port.

**Figure 174** Conflicting Computer and Router IP Addresses Example



E

# Importing Certificates

This appendix shows you how to import public key certificates into your web browser.

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 the site to be issued to all visiting web browsers to let them know that the site is legitimate.

Many ZyXEL products, such as the NSA-2401, issue their own public key certificates. These can be used by web browsers on a LAN or WAN to verify that they are in fact connecting to the legitimate device and not one masquerading as it. However, because the certificates were not issued by one of the several organizations officially recognized by the most common web browsers, you will need to import the ZyXEL-created certificate into your web browser and flag that certificate as a trusted authority.

You can see if you are browsing on a secure website if the URL in your web browser's address bar begins with `https://` or there is a sealed padlock icon (  ) somewhere in the main browser window (not all browsers show the padlock in the same location.)

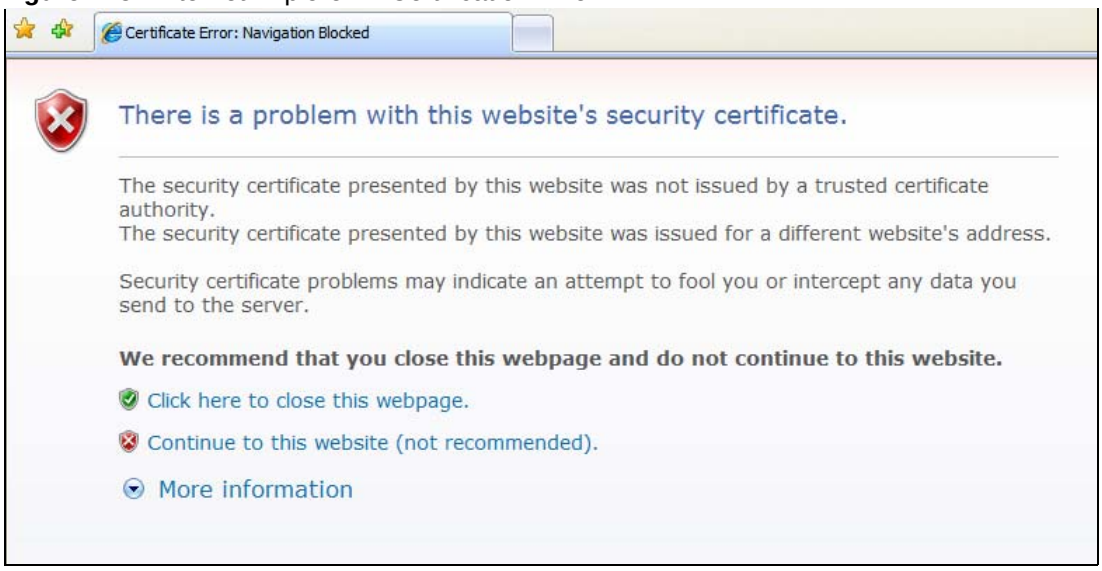
In this appendix, you can import a public key certificate for:

# Internet Explorer

The following example uses Microsoft Internet Explorer 7 on Windows XP Professional; however, they can also apply to Internet Explorer on Windows Vista.

1 If your device's web configurator is set to use SSL certification, then the first time you browse to it you are presented with a certification error.

**Figure 175** Internet Explorer 7: Certification Error

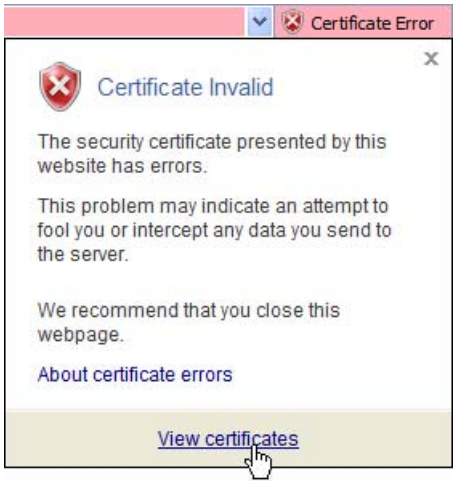



2 Click **Continue to this website (not recommended)**.

**Figure 176** Internet Explorer 7: Certification Error

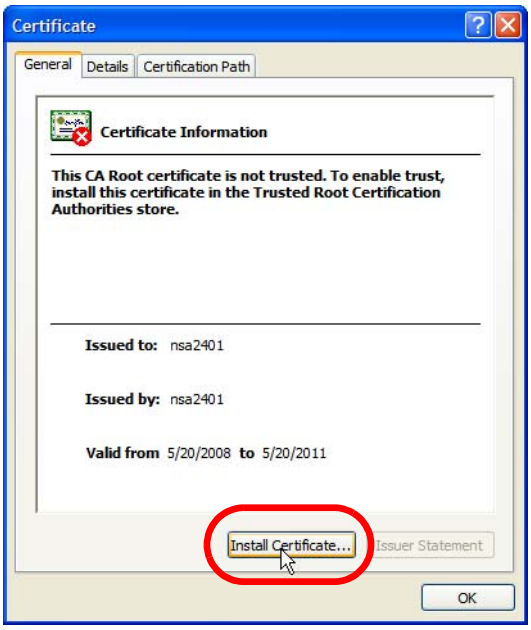

3 In the **Address Bar**, click **Certificate Error** > **View certificates**.

**Figure 177** Internet Explorer 7: Certificate Error



4 In the **Certificate** dialog box, click **Install Certificate**.

**Figure 178** Internet Explorer 7: Certificate

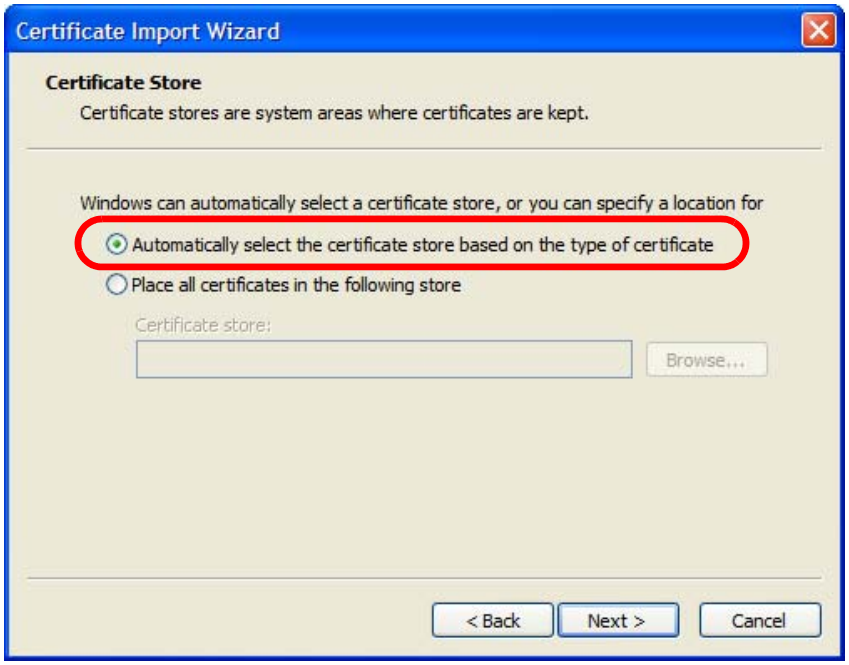



5 In the **Certificate Import Wizard**, click **Next**.

**Figure 179** Internet Explorer 7: Certificate Import Wizard

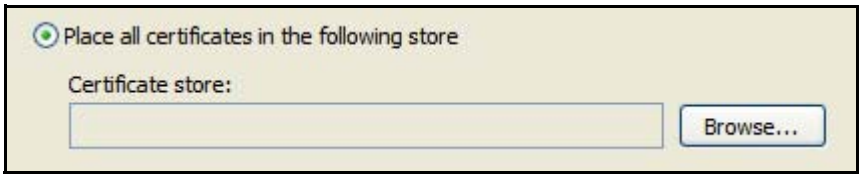
6 If you want Internet Explorer to **Automatically select certificate store based on the type of certificate**, click **Next** again and then go to step 9.

**Figure 180** Internet Explorer 7: Certificate Import Wizard




7 Otherwise, select **Place all certificates in the following store** and then click **Browse**.

**Figure 181** Internet Explorer 7: Certificate Import Wizard

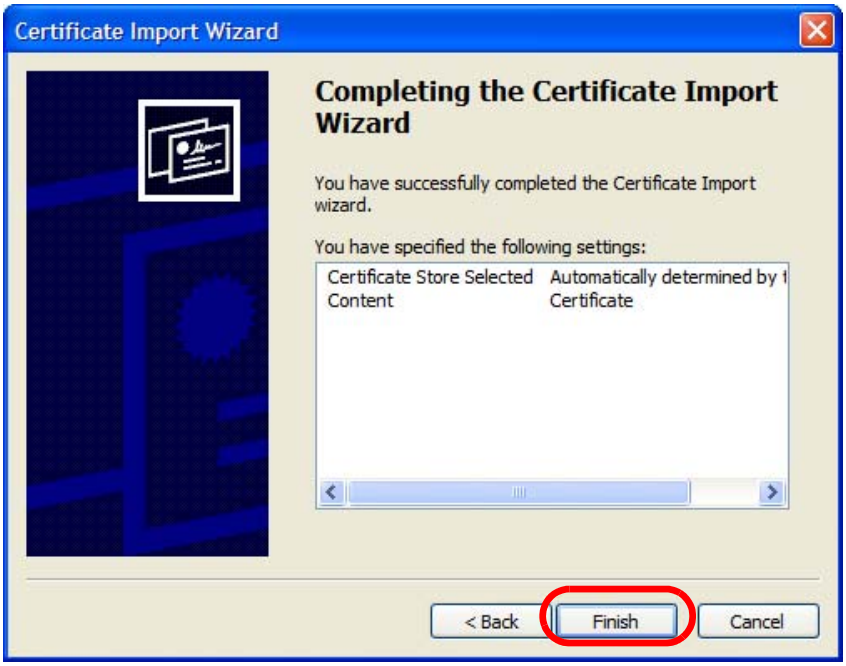



8 In the **Select Certificate Store** dialog box, choose a location in which to save the certificate and then click **OK**.

**Figure 182** Internet Explorer 7: Select Certificate Store

**9** In the **Completing the Certificate Import Wizard** screen, click **Finish**.

**Figure 183** Internet Explorer 7: Certificate Import Wizard




**10** If you are presented with another **Security Warning**, click **Yes**.

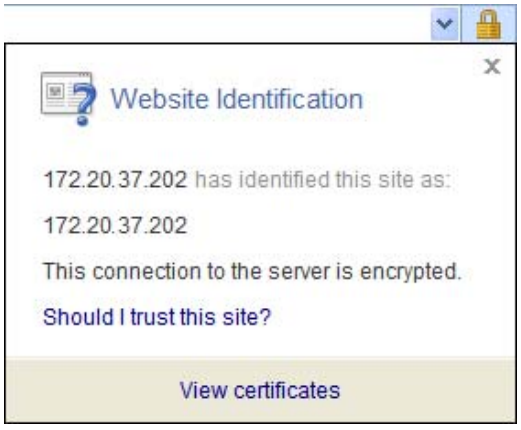
**Figure 184** Internet Explorer 7: Security Warning

**11** Finally, click **OK** when presented with the successful certificate installation message.

**Figure 185** Internet Explorer 7: Certificate Import Wizard


**12** The next time you start Internet Explorer and go to a ZyXEL web configurator page, a sealed padlock icon appears in the address bar. Click it to view the page's **Website Identification** information.

**Figure 186** Internet Explorer 7: Website Identification



## Installing a Stand-Alone Certificate File in Internet Explorer

Rather than browsing to a ZyXEL web configurator and installing a public key certificate when prompted, you can install a stand-alone certificate file if one has been issued to you.

1 Double-click the public key certificate file.

**Figure 187** Internet Explorer 7: Public Key Certificate File


2 In the security warning dialog box, click **Open**.

**Figure 188** Internet Explorer 7: Open File - Security Warning


3 Refer to steps 4-12 in the Internet Explorer procedure beginning on page 278 to complete the installation process.

## Removing a Certificate in Internet Explorer

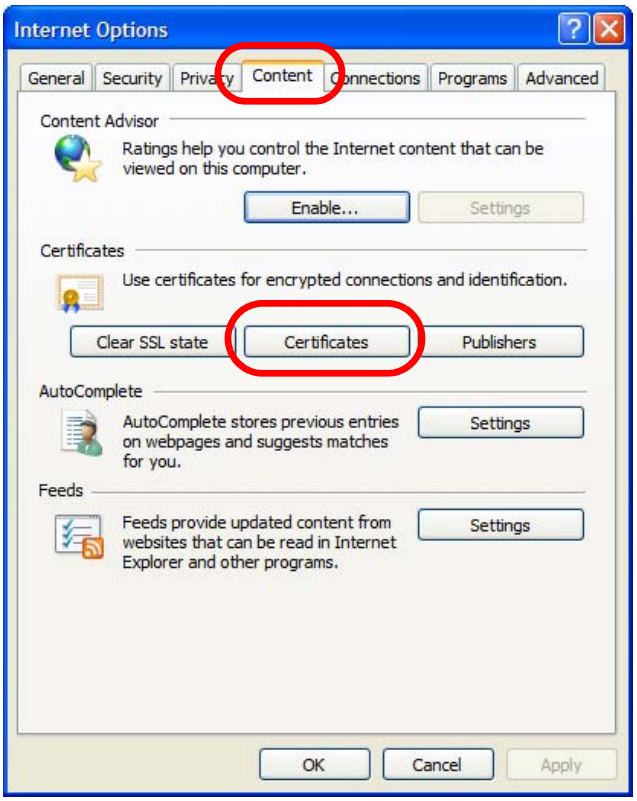
This section shows you how to remove a public key certificate in Internet Explorer 7.

1 Open **Internet Explorer** and click **TOOLS** > **Internet Options**.

**Figure 189** Internet Explorer 7: Tools Menu

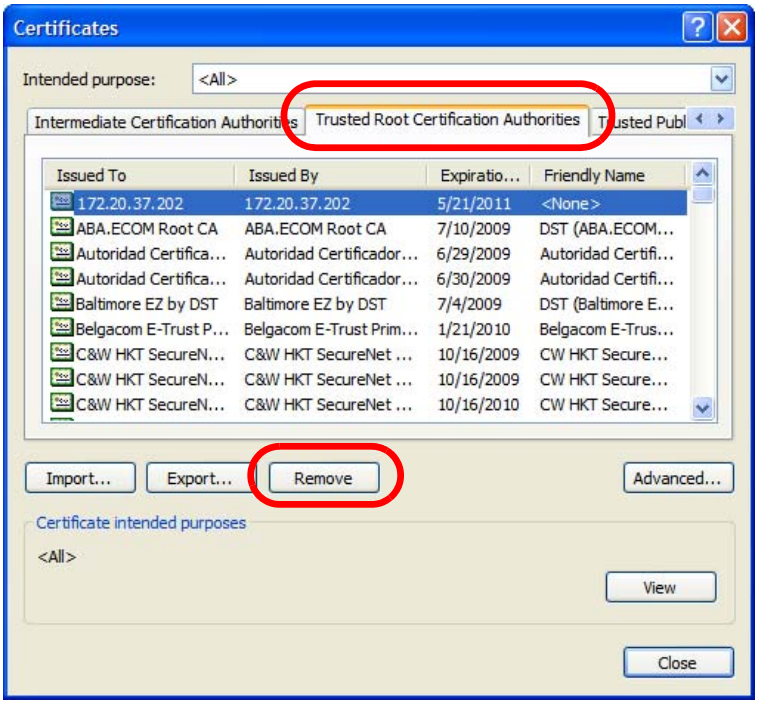

2 In the **Internet Options** dialog box, click **Content** > **Certificates**.

**Figure 190** Internet Explorer 7: Internet Options



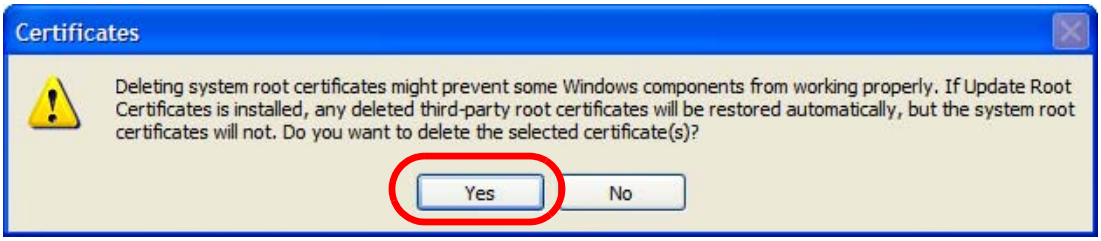
3 In the **Certificates** dialog box, click the **Trusted Root Certificates Authorities** tab, select the certificate that you want to delete, and then click **Remove**.

**Figure 191** Internet Explorer 7: Certificates



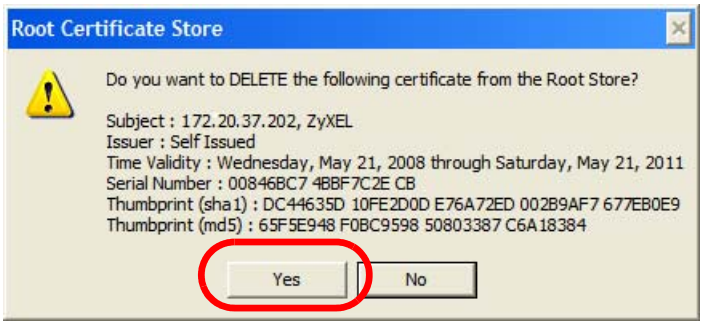

4 In the **Certificates** confirmation, click **Yes**.

**Figure 192** Internet Explorer 7: Certificates




5 In the **Root Certificate Store** dialog box, click **Yes**.

**Figure 193** Internet Explorer 7: Root Certificate Store



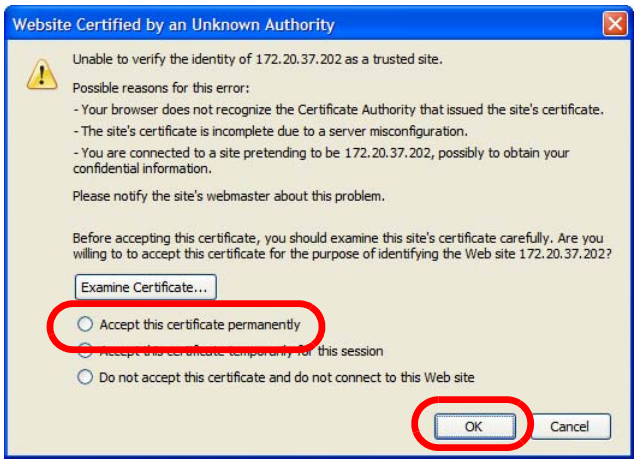

6 The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.

# Firefox

The following example uses Mozilla Firefox 2 on Windows XP Professional; however, the screens can also apply to Firefox 2 on all platforms.

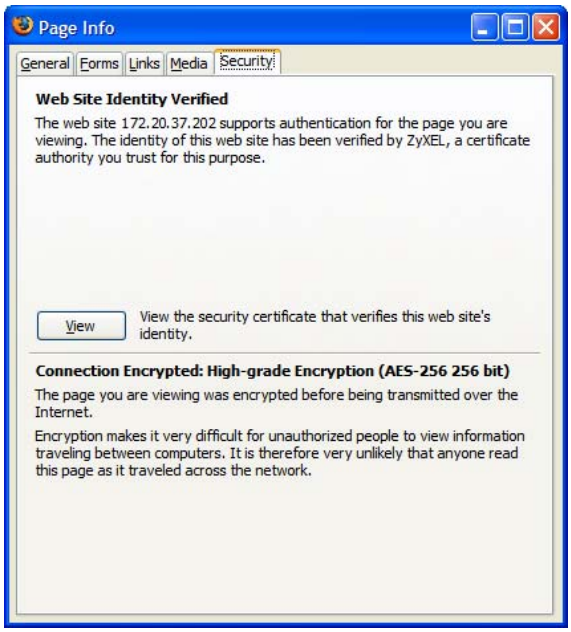
1. If your device's web configurator is set to use SSL certification, then the first time you browse to it you are presented with a certification error.
2. Select **Accept this certificate permanently** and click **OK.**

**Figure 194** Firefox 2: Website Certified by an Unknown Authority




3. The certificate is stored and you can now connect securely to the web configurator. A sealed padlock appears in the address bar, which you can click to open the **Page Info** > **Security** window to view the web page's security information.

**Figure 195** Firefox 2: Page Info

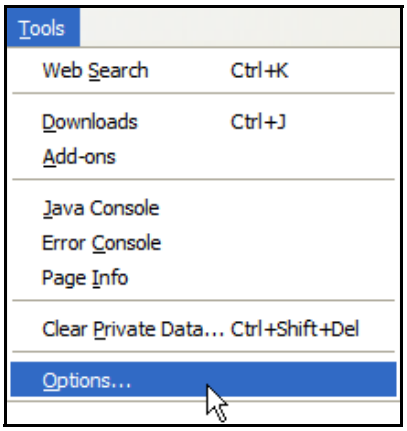


## Installing a Stand-Alone Certificate File in Firefox

Rather than browsing to a ZyXEL web configurator and installing a public key certificate when prompted, you can install a stand-alone certificate file if one has been issued to you.

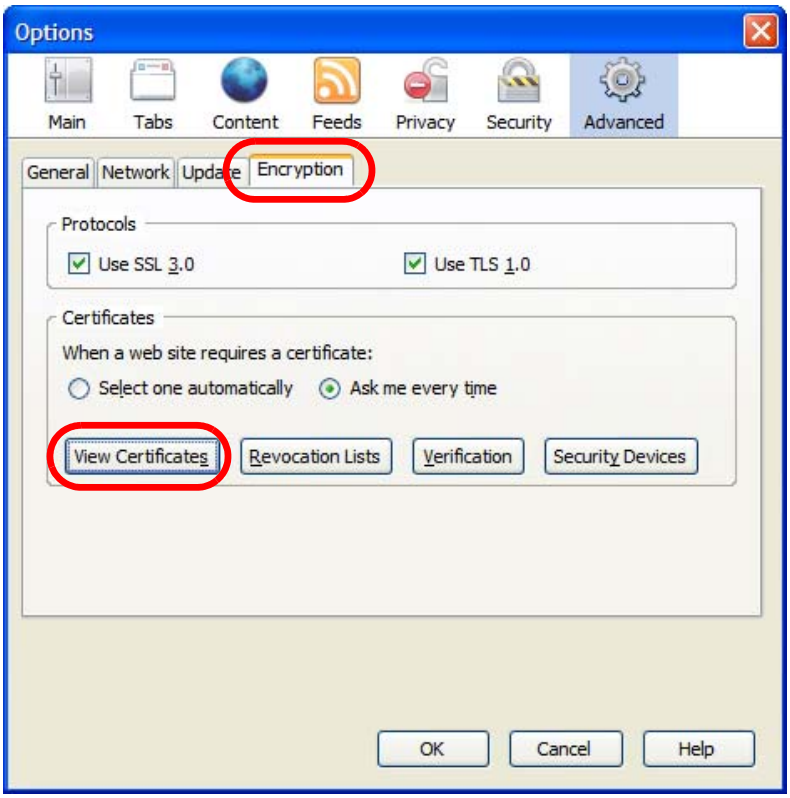
1 Open **Firefox** and click **TOOLS** > **Options**.

**Figure 196** Firefox 2: Tools Menu



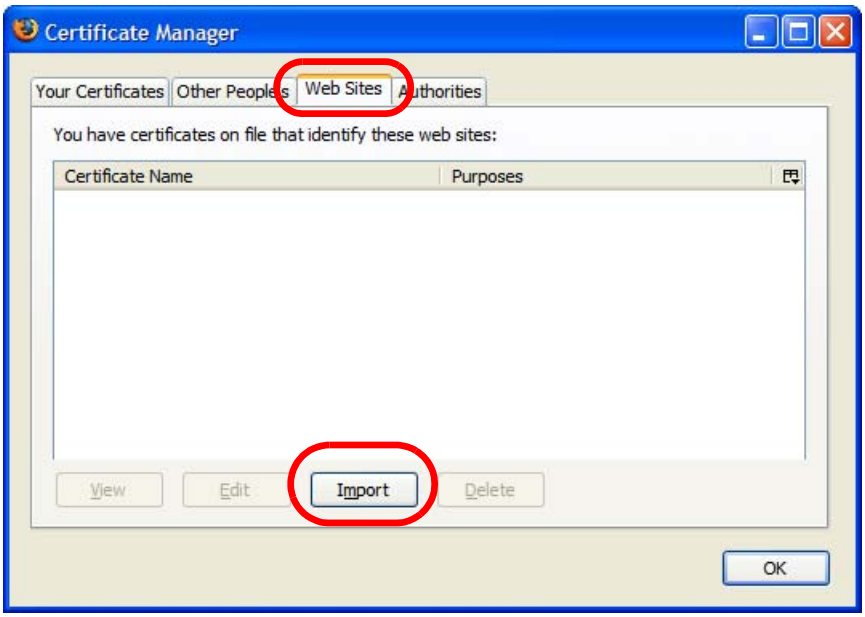

2 In the **Options** dialog box, click **ADVANCED** > **Encryption** > **View Certificates**.

**Figure 197** Firefox 2: Options



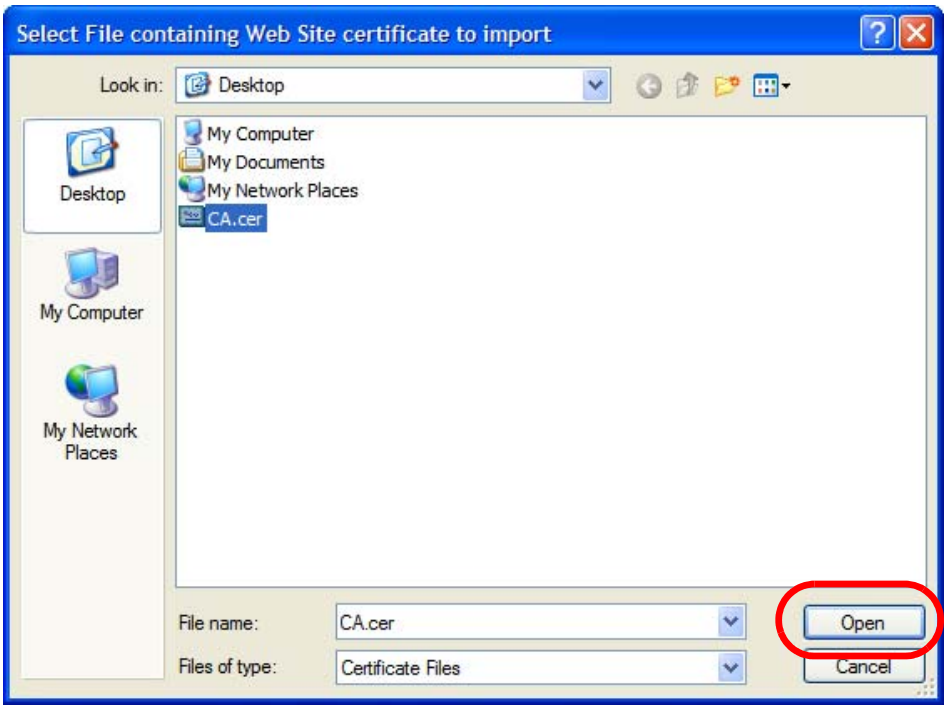
3 In the **Certificate Manager** dialog box, click **Web Sites** > **Import**.

**Figure 198** Firefox 2: Certificate Manager




4 Use the **Select File** dialog box to locate the certificate and then click **Open**.

**Figure 199** Firefox 2: Select File



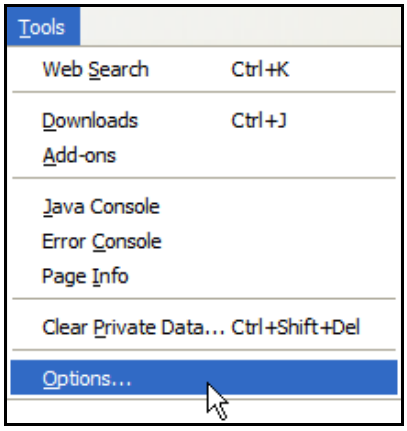

5 The next time you visit the web site, click the padlock in the address bar to open the **Page Info** > **Security** window to see the web page's security information.

## Removing a Certificate in Firefox

This section shows you how to remove a public key certificate in Firefox 2.

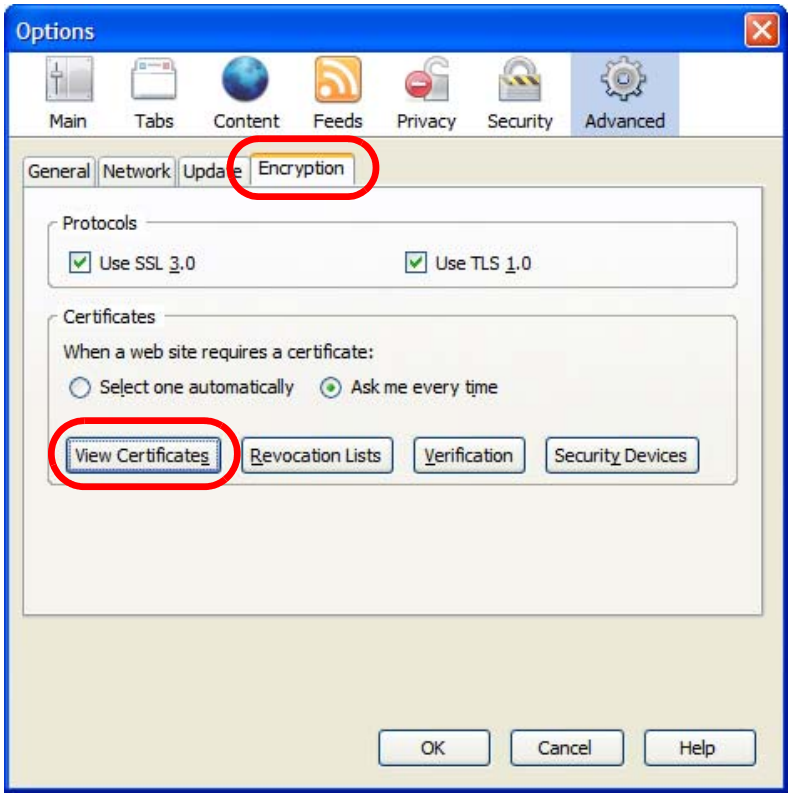
1 Open **Firefox** and click **TOOLS** > **Options**.

**Figure 200** Firefox 2: Tools Menu



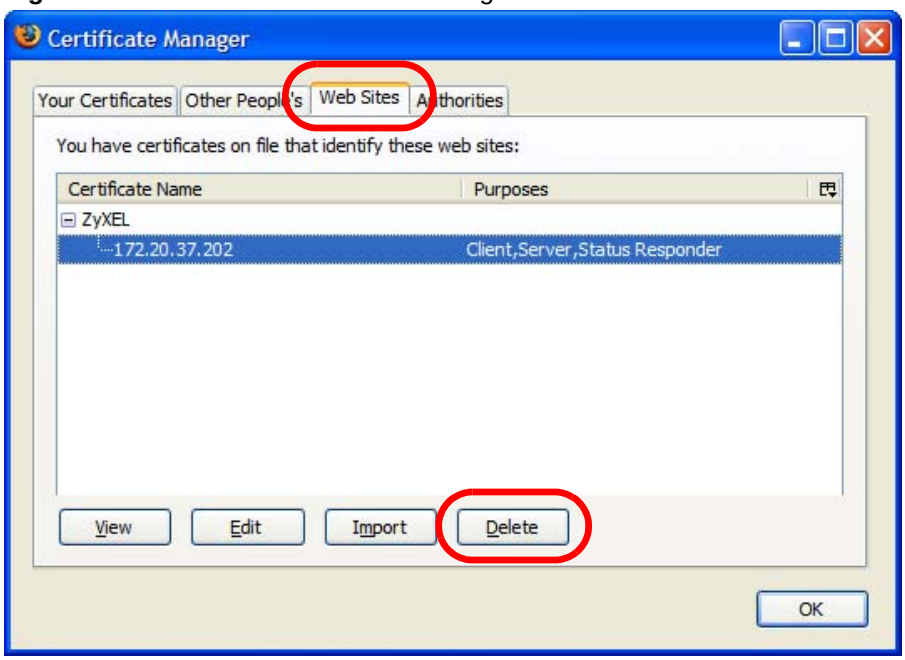

2 In the **Options** dialog box, click **ADVANCED** > **Encryption** > **View Certificates**.

**Figure 201** Firefox 2: Options



3 In the **Certificate Manager** dialog box, select the **Web Sites** tab, select the certificate that you want to remove, and then click **Delete**.

**Figure 202** Firefox 2: Certificate Manager




4 In the **Delete Web Site Certificates** dialog box, click **OK**.

**Figure 203** Firefox 2: Delete Web Site Certificates

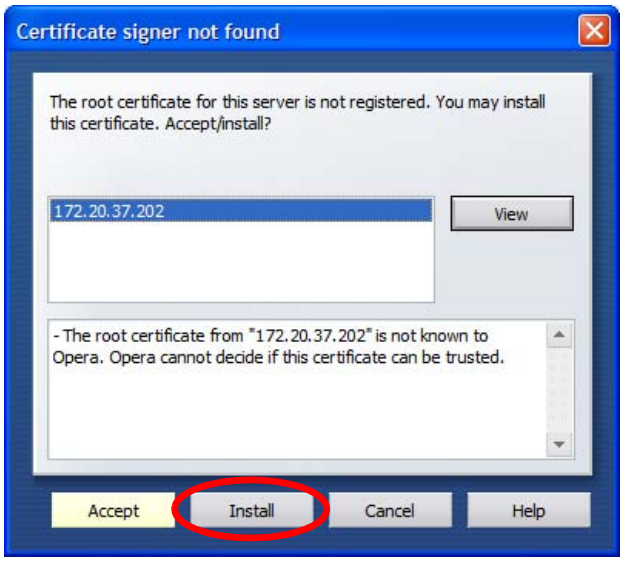

5 The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.

# Opera

The following example uses Opera 9 on Windows XP Professional; however, the screens can apply to Opera 9 on all platforms.

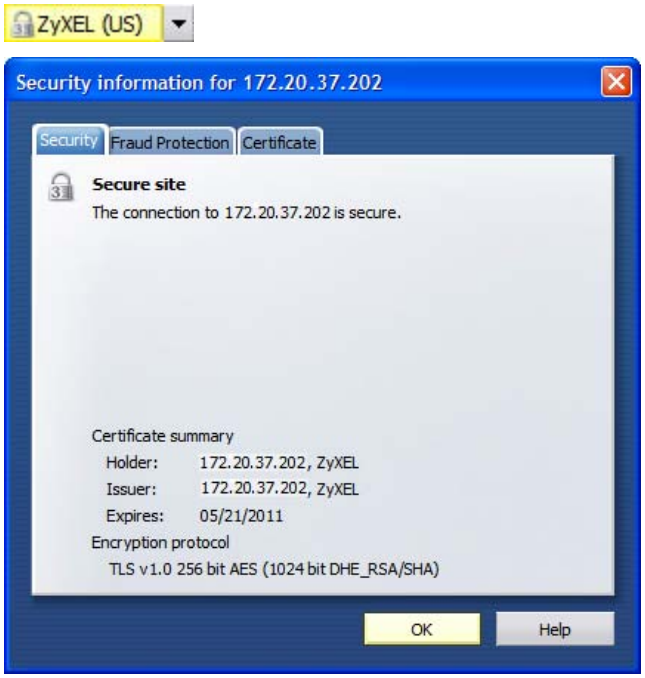
1. If your device's web configurator is set to use SSL certification, then the first time you browse to it you are presented with a certification error.
2. Click **Install** to accept the certificate.

**Figure 204** Opera 9: Certificate signer not found




3. The next time you visit the web site, click the padlock in the address bar to open the **Security information** window to view the web page's security details.

**Figure 205** Opera 9: Security information

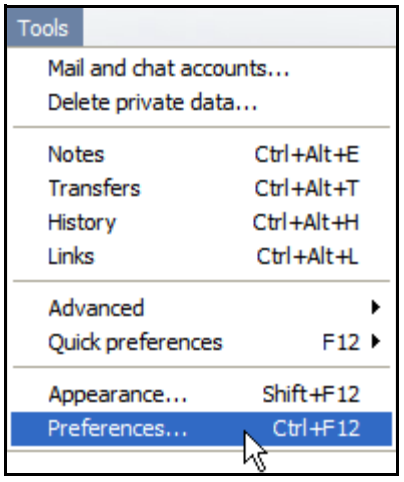


## Installing a Stand-Alone Certificate File in Opera

Rather than browsing to a ZyXEL web configurator and installing a public key certificate when prompted, you can install a stand-alone certificate file if one has been issued to you.

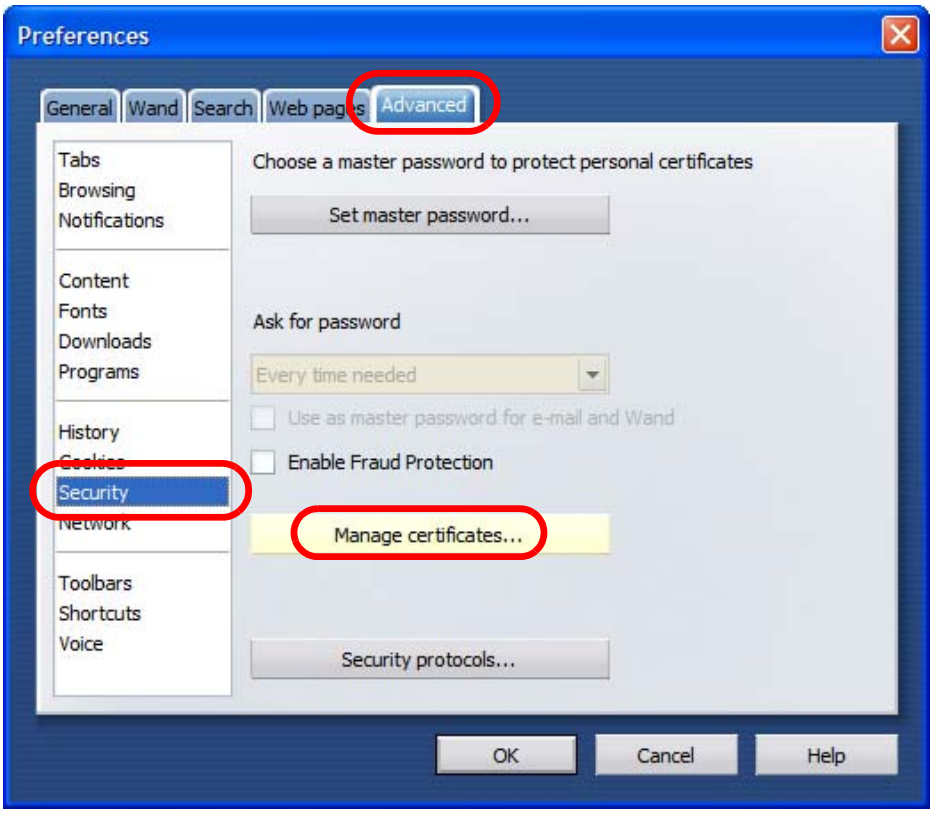
1 Open **Opera** and click **TOOLS** > **Preferences**.

**Figure 206** Opera 9: Tools Menu



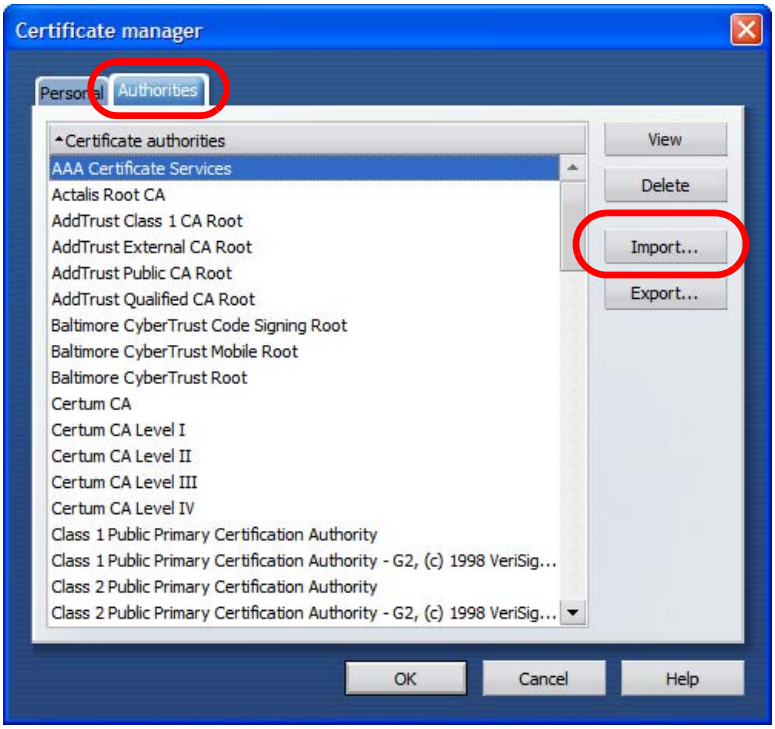

2 In **Preferences**, click **ADVANCED** > **Security** > **Manage certificates**.

**Figure 207** Opera 9: Preferences



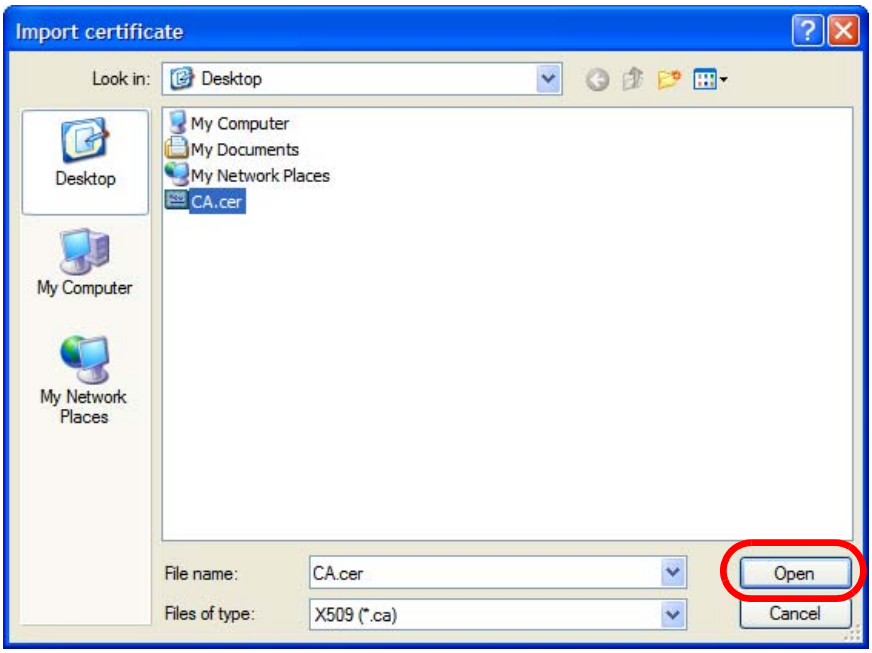
3 In the **Certificates Manager**, click **Authorities** > **Import**.

**Figure 208** Opera 9: Certificate manager



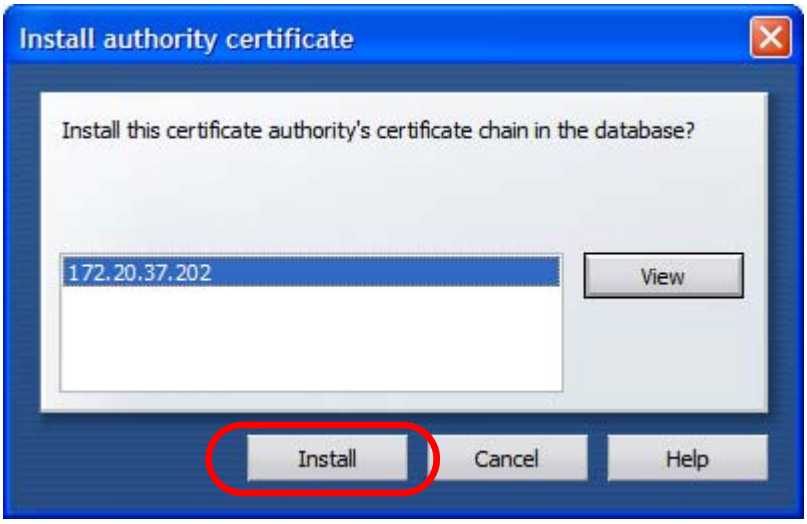

4 Use the **Import certificate** dialog box to locate the certificate and then click **Open.**

**Figure 209** Opera 9: Import certificate



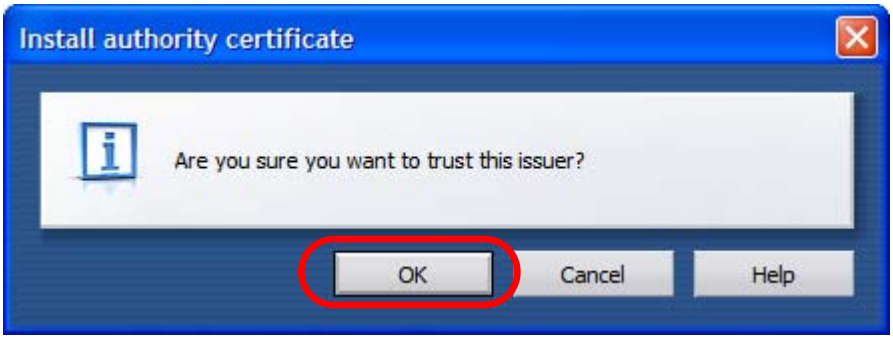
5 In the **Install authority certificate** dialog box, click **Install**.

**Figure 210** Opera 9: Install authority certificate




6 Next, click **OK**.

**Figure 211** Opera 9: Install authority certificate



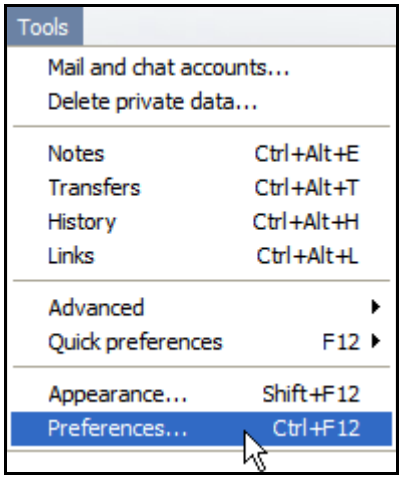

7 The next time you visit the web site, click the padlock in the address bar to open the **Security information** window to view the web page's security details.

## Removing a Certificate in Opera

This section shows you how to remove a public key certificate in Opera 9.

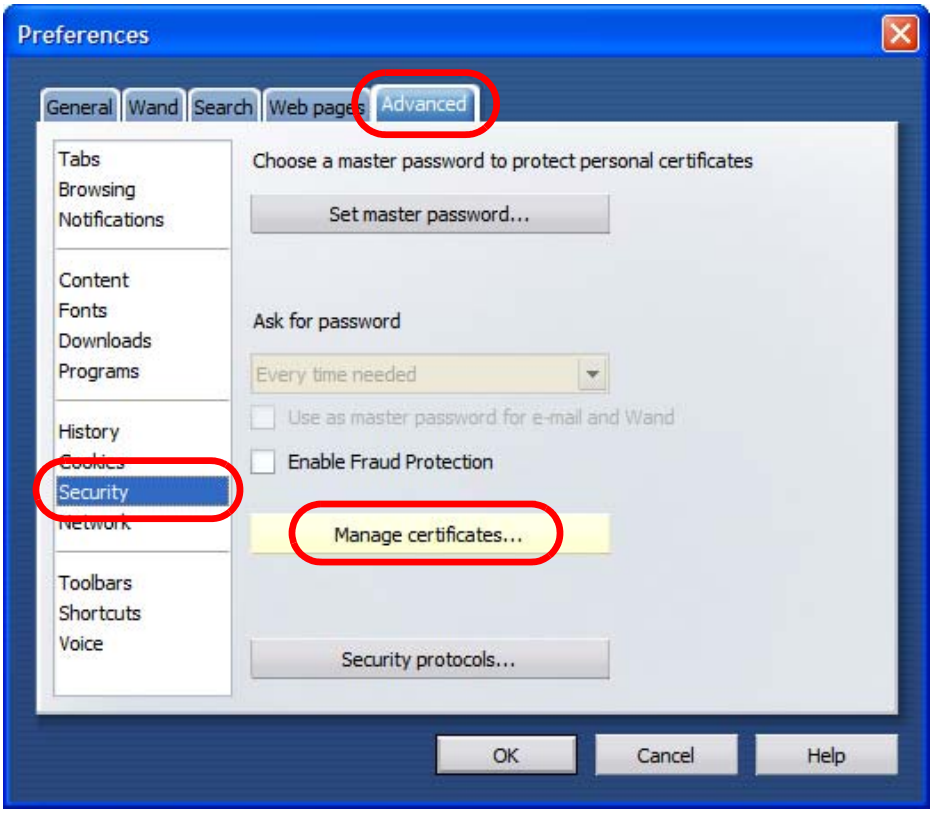
1 Open **Opera** and click **TOOLS > Preferences**.

**Figure 212** Opera 9: Tools Menu



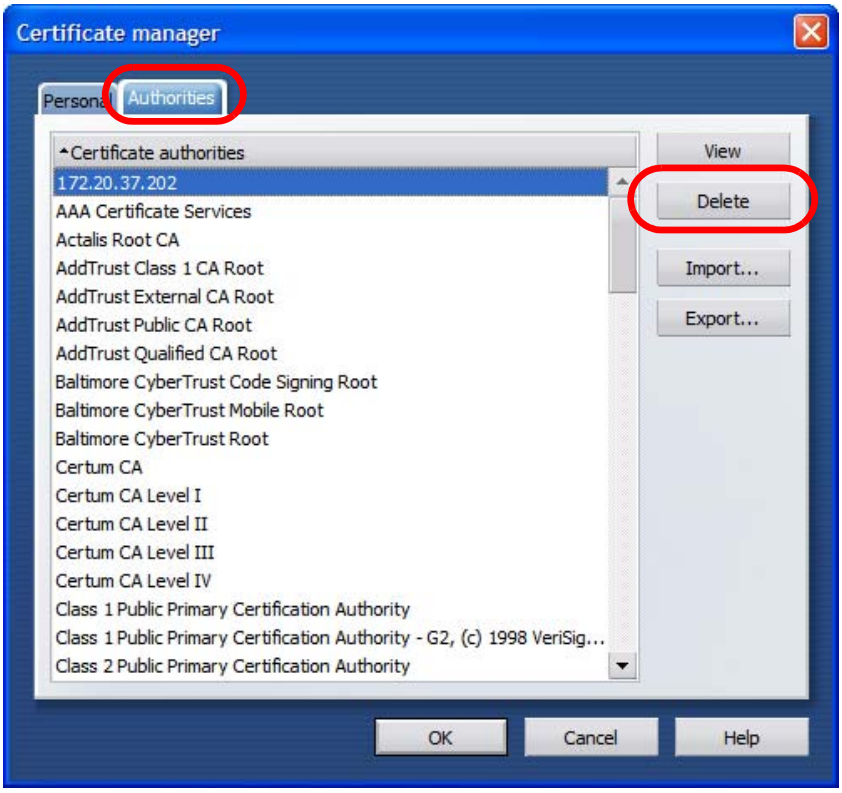

2 In **Preferences**, **ADVANCED > Security** > **Manage certificates**.

**Figure 213** Opera 9: Preferences



3 In the **Certificates manager**, select the **Authorities** tab, select the certificate that you want to remove, and then click **Delete**.

**Figure 214** Opera 9: Certificate manager




4 The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.

There is no confirmation when you delete a certificate authority, so be absolutely certain that you want to go through with it before clicking the button.

# Konqueror

The following example uses Konqueror 3.5 on openSUSE 10.3, however the screens apply to Konqueror 3.5 on all Linux KDE distributions.

1. If your device's web configurator is set to use SSL certification, then the first time you browse to it you are presented with a certification error.
2. Click **Continue**.

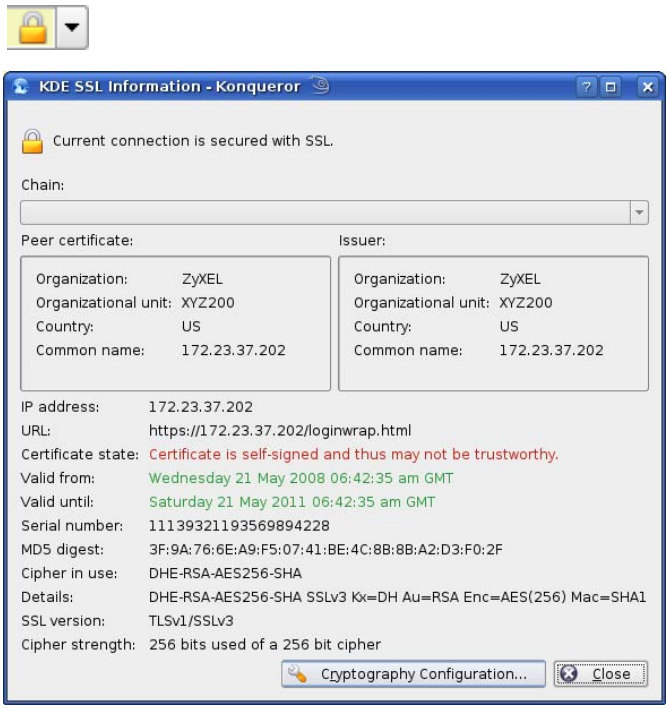
**Figure 215** Konqueror 3.5: Server Authentication


3. Click **Forever** when prompted to accept the certificate.

**Figure 216** Konqueror 3.5: Server Authentication


4. Click the padlock in the address bar to open the **KDE SSL Information** window and view the web page's security details.

**Figure 217** Konqueror 3.5: KDE SSL Information



## Installing a Stand-Alone Certificate File in Konqueror

Rather than browsing to a ZyXEL web configurator and installing a public key certificate when prompted, you can install a stand-alone certificate file if one has been issued to you.

1 Double-click the public key certificate file.

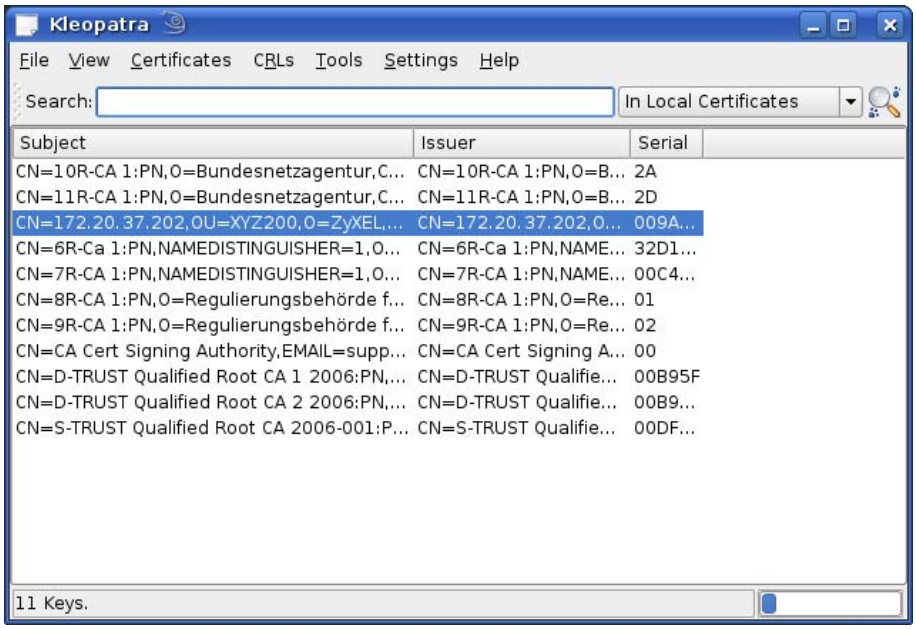
**Figure 218** Konqueror 3.5: Public Key Certificate File


2 In the **Certificate Import Result - Kleopatra** dialog box, click **OK**.

**Figure 219** Konqueror 3.5: Certificate Import Result


The public key certificate appears in the KDE certificate manager, **Kleopatra**.

**Figure 220** Konqueror 3.5: Kleopatra



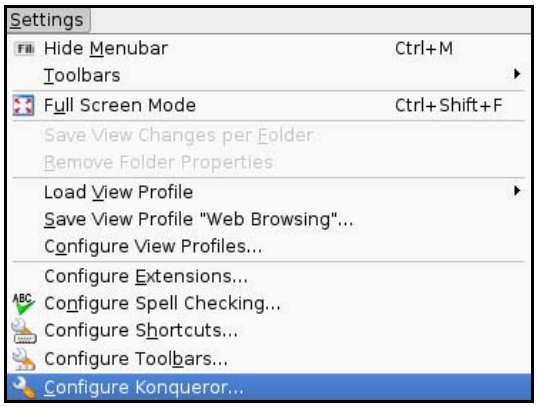

3 The next time you visit the web site, click the padlock in the address bar to open the **KDE SSL Information** window to view the web page's security details.

## Removing a Certificate in Konqueror

This section shows you how to remove a public key certificate in Konqueror 3.5.

1 Open **Konqueror** and click **Settings** > **Configure Konqueror**.

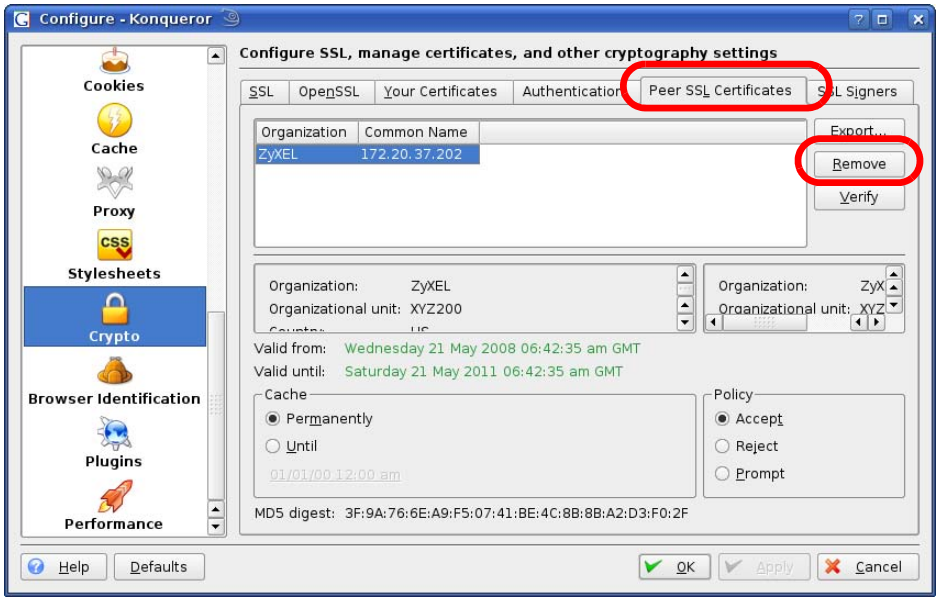
**Figure 221** Konqueror 3.5: Settings Menu




2 In the **Configure** dialog box, select **Crypto**.

3 On the **Peer SSL Certificates** tab, select the certificate you want to delete and then click **Remove**.

**Figure 222** Konqueror 3.5: Configure




4 The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.

There is no confirmation when you remove a certificate authority, so be absolutely certain you want to go through with it before clicking the button.

F

# SIP Passthrough

## Enabling/Disabling the SIP ALG

You can turn off the WiMAX Modem SIP ALG to avoid retranslating the IP address of an existing SIP device that is using STUN. If you want to use STUN with a SIP client device (a SIP phone or IP phone for example) behind the WiMAX Modem, use the `ip alg disable ALG_SIP` command to turn off the SIP ALG.

## Signaling Session Timeout

Most SIP clients have an “expire” mechanism indicating the lifetime of signaling sessions. The SIP UA sends registration packets to the SIP server periodically and keeps the session alive in the WiMAX Modem.

If the SIP client does not have this mechanism and makes no call during the WiMAX Modem SIP timeout default (60 minutes), the WiMAX Modem SIP ALG drops any incoming calls after the timeout period. You can use the `ip alg siptimeout` command to change the timeout value.

## Audio Session Timeout

If no voice packets go through the SIP ALG before the timeout period default (5 minutes) expires, the SIP ALG does not drop the call but blocks all voice traffic and deletes the audio session. You cannot hear anything and you will need to make a new call to continue your conversation.

# G

# Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s**) is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

**Table 124** Commonly Used Services

| NAME | PROTOCOL | PORT(S) | DESCRIPTION |
|---|---|---|---|
| AH (IPSEC_TUNNEL) | User-Defined | 51 | The IPSEC AH (Authentication Header) tunneling protocol uses this service. |
| AIM/New-ICQ | TCP | 5190 | AOL's Internet Messenger service. It is also used as a listening port by ICQ. |
| AUTH | TCP | 113 | Authentication protocol used by some servers. |
| BGP | TCP | 179 | Border Gateway Protocol. |
| BOOTP_CLIENT | UDP | 68 | DHCP Client. |
| BOOTP_SERVER | UDP | 67 | DHCP Server. |
| CU-SEEME | TCP<br>UDP | 7648<br>24032 | A popular videoconferencing solution from White Pines Software. |
| DNS | TCP/UDP | 53 | Domain Name Server, a service that matches web names (for example www.zyxel.com) to IP numbers. |
| ESP (IPSEC_TUNNEL) | User-Defined | 50 | The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service. |
| FINGER | TCP | 79 | Finger is a UNIX or Internet related command that can be used to find out if a user is logged on. |

**Table 124** Commonly Used Services (continued)

| NAME | PROTOCOL | PORT(S) | DESCRIPTION |
|---|---|---|---|
| FTP | TCP<br>TCP | 20<br>21 | File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail. |
| H.323 | TCP | 1720 | NetMeeting uses this protocol. |
| HTTP | TCP | 80 | Hyper Text Transfer Protocol - a client/ server protocol for the world wide web. |
| HTTPS | TCP | 443 | HTTPS is a secured http session often used in e-commerce. |
| ICMP | User-Defined | 1 | Internet Control Message Protocol is often used for diagnostic or routing purposes. |
| ICQ | UDP | 4000 | This is a popular Internet chat program. |
| IGMP (MULTICAST) | User-Defined | 2 | Internet Group Management Protocol is used when sending packets to a specific group of hosts. |
| IKE | UDP | 500 | The Internet Key Exchange algorithm is used for key distribution and management. |
| IRC | TCP/UDP | 6667 | This is another popular Internet chat program. |
| MSN Messenger | TCP | 1863 | Microsoft Networks' messenger service uses this protocol. |
| NEW-ICQ | TCP | 5190 | An Internet chat program. |
| NEWS | TCP | 144 | A protocol for news groups. |
| NFS | UDP | 2049 | Network File System - NFS is a client/ server distributed file service that provides transparent file sharing for network environments. |
| NNTP | TCP | 119 | Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service. |
| PING | User-Defined | 1 | Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable. |
| POP3 | TCP | 110 | Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other). |
| PPTP | TCP | 1723 | Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel. |
| PPTP_TUNNEL (GRE) | User-Defined | 47 | PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel. |
| RCMD | TCP | 512 | Remote Command Service. |
| REAL_AUDIO | TCP | 7070 | A streaming audio service that enables real time sound over the web. |
| REXEC | TCP | 514 | Remote Execution Daemon. |
| RLOGIN | TCP | 513 | Remote Login. |
| RTELNET | TCP | 107 | Remote Telnet. |

**Table 124** Commonly Used Services (continued)

| NAME | PROTOCOL | PORT(S) | DESCRIPTION |
|---|---|---|---|
| RTSP | TCP/UDP | 554 | The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet. |
| SFTP | TCP | 115 | Simple File Transfer Protocol. |
| SMTP | TCP | 25 | Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another. |
| SNMP | TCP/UDP | 161 | Simple Network Management Program. |
| SNMP-TRAPS | TCP/UDP | 162 | Traps for use with the SNMP (RFC:1215). |
| SQL-NET | TCP | 1521 | Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers. |
| SSH | TCP/UDP | 22 | Secure Shell Remote Login Program. |
| STRM WORKS | UDP | 1558 | Stream Works Protocol. |
| SYSLOG | UDP | 514 | Syslog allows you to send system logs to a UNIX server. |
| TACACS | UDP | 49 | Login Host Protocol used for (Terminal Access Controller Access Control System). |
| TELNET | TCP | 23 | Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems. |
| TFTP | UDP | 69 | Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol). |
| VDOLIVE | TCP | 7000 | Another videoconferencing solution. |

# H

# Legal Information

## Copyright



### Disclaimers

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Your use of the WiMAX Modem is subject to the terms and conditions of any related service providers.

Do not use the WiMAX Modem for illegal purposes. Illegal downloading or sharing of files can result in severe civil and criminal penalties. You are subject to the restrictions of copyright laws and any other applicable laws, and will bear the consequences of any infringements thereof. ZyXEL bears NO responsibility or liability for your use of the download service feature.

### Trademarks

Trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

## Certifications

### Federal Communications Commission (FCC) Interference Statement

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

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

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

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

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

### FCC Radiation Exposure Statement

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

## 注意 !

依據　低功率電波輻射性電機管理辦法

第十二條　經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條　低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

本機限在不干擾合法電臺與不受被干擾保障條件下於室內使用。
減少電磁波影響，請妥適使用。

### Notices

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

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

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

### Viewing Certifications

1. Go to http://www.zyxel.com.
2. Select your product on the ZyXEL home page to go to that product's page.
3. Select the certification you wish to view from this page.

# ZyXEL Limited Warranty

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

### Note

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

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

### Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com.

# Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device. Regional offices are listed below (see also http://www.zyxel.com/web/contact_us.php). Please have the following information ready when you contact an office.

### Required Information

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

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

### Corporate Headquarters (Worldwide)

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-3-578-3942
- Fax: +886-3-578-2439
- Web: www.zyxel.com
- Regular Mail: ZyXEL Communications Corp., 6 Innovation Road II, Science Park, Hsinchu 300, Taiwan

### China - ZyXEL Communications (Beijing) Corp.

- Support E-mail: cso.zycn@zyxel.cn
- Sales E-mail: sales@zyxel.cn
- Telephone: +86-010-82800646
- Fax: +86-010-82800587
- Address: 902, Unit B, Horizon Building, No.6, Zhichun Str, Haidian District, Beijing
- Web: http://www.zyxel.cn

### China - ZyXEL Communications (Shanghai) Corp.

- Support E-mail: cso.zycn@zyxel.cn
- Sales E-mail: sales@zyxel.cn
- Telephone: +86-021-61199055
- Fax: +86-021-52069033

- Address: 1005F, ShengGao International Tower, No.137 XianXia Rd., Shanghai
- Web: http://www.zyxel.cn

### Costa Rica

- Support E-mail: soporte@zyxel.co.cr
- Sales E-mail: sales@zyxel.co.cr
- Telephone: +506-2017878
- Fax: +506-2015098
- Web: www.zyxel.co.cr
- Regular Mail: ZyXEL Costa Rica, Plaza Roble Escazú, Etapa El Patio, Tercer Piso, San José, Costa Rica

### Czech Republic

- E-mail: info@cz.zyxel.com
- Telephone: +420-241-091-350
- Fax: +420-241-091-359
- Web: www.zyxel.cz
- Regular Mail: ZyXEL Communications, Czech s.r.o., Modranská 621, 143 01 Praha 4 - Modrany, Ceská Republika

### Denmark

- Support E-mail: support@zyxel.dk
- Sales E-mail: sales@zyxel.dk
- Telephone: +45-39-55-07-00
- Fax: +45-39-55-07-07
- Web: www.zyxel.dk
- Regular Mail: ZyXEL Communications A/S, Columbusvej, 2860 Soeborg, Denmark

### Finland

- Support E-mail: support@zyxel.fi
- Sales E-mail: sales@zyxel.fi
- Telephone: +358-9-4780-8411
- Fax: +358-9-4780-8448
- Web: www.zyxel.fi
- Regular Mail: ZyXEL Communications Oy, Malminkaari 10, 00700 Helsinki, Finland

### France

- E-mail: info@zyxel.fr
- Telephone: +33-4-72-52-97-97
- Fax: +33-4-72-52-19-20
- Web: www.zyxel.fr
- Regular Mail: ZyXEL France, 1 rue des Vergers, Bat. 1 / C, 69760 Limonest, France

### Germany

- Support E-mail: support@zyxel.de
- Sales E-mail: sales@zyxel.de
- Telephone: +49-2405-6909-69
- Fax: +49-2405-6909-99
- Web: www.zyxel.de
- Regular Mail: ZyXEL Deutschland GmbH., Adenauerstr. 20/A2 D-52146, Wuerselen, Germany

### Hungary

- Support E-mail: support@zyxel.hu
- Sales E-mail: info@zyxel.hu
- Telephone: +36-1-3361649
- Fax: +36-1-3259100
- Web: www.zyxel.hu
- Regular Mail: ZyXEL Hungary, 48, Zoldlomb Str., H-1025, Budapest, Hungary

### India

- Support E-mail: support@zyxel.in
- Sales E-mail: sales@zyxel.in
- Telephone: +91-11-30888144 to +91-11-30888153
- Fax: +91-11-30888149, +91-11-26810715
- Web: http://www.zyxel.in
- Regular Mail: India - ZyXEL Technology India Pvt Ltd., II-Floor, F2/9 Okhla Phase -1, New Delhi 110020, India

### Japan

- Support E-mail: support@zyxel.co.jp
- Sales E-mail: zyp@zyxel.co.jp
- Telephone: +81-3-6847-3700
- Fax: +81-3-6847-3705
- Web: www.zyxel.co.jp
- Regular Mail: ZyXEL Japan, 3F, Office T&U, 1-10-10 Higashi-Gotanda, Shinagawa-ku, Tokyo 141-0022, Japan

### Kazakhstan

- Support: http://zyxel.kz/support
- Sales E-mail: sales@zyxel.kz
- Telephone: +7-3272-590-698
- Fax: +7-3272-590-689
- Web: www.zyxel.kz
- Regular Mail: ZyXEL Kazakhstan, 43 Dostyk Ave., Office 414, Dostyk Business Centre, 050010 Almaty, Republic of Kazakhstan

### Malaysia

- Support E-mail: support@zyxel.com.my
- Sales E-mail: sales@zyxel.com.my
- Telephone: +603-8076-9933
- Fax: +603-8076-9833
- Web: http://www.zyxel.com.my
- Regular Mail: ZyXEL Malaysia Sdn Bhd., 1-02 & 1-03, Jalan Kenari 17F, Bandar Puchong Jaya, 47100 Puchong, Selangor Darul Ehsan, Malaysia

### North America

- Support E-mail: support@zyxel.com
- Support Telephone: +1-800-978-7222
- Sales E-mail: sales@zyxel.com
- Sales Telephone: +1-714-632-0882
- Fax: +1-714-632-0858
- Web: www.zyxel.com
- Regular Mail: ZyXEL Communications Inc., 1130 N. Miller St., Anaheim, CA 92806-2001, U.S.A.

### Norway

- Support E-mail: support@zyxel.no
- Sales E-mail: sales@zyxel.no
- Telephone: +47-22-80-61-80
- Fax: +47-22-80-61-81
- Web: www.zyxel.no
- Regular Mail: ZyXEL Communications A/S, Nils Hansens vei 13, 0667 Oslo, Norway

### Poland

- E-mail: info@pl.zyxel.com
- Telephone: +48-22-333 8250
- Fax: +48-22-333 8251
- Web: www.pl.zyxel.com
- Regular Mail: ZyXEL Communications, ul. Okrzei 1A, 03-715 Warszawa, Poland

### Russia

- Support: http://zyxel.ru/support
- Sales E-mail: sales@zyxel.ru
- Telephone: +7-095-542-89-29
- Fax: +7-095-542-89-25
- Web: www.zyxel.ru
- Regular Mail: ZyXEL Russia, Ostrovityanova 37a Str., Moscow 117279, Russia

### Singapore

- Support E-mail: support@zyxel.com.sg
- Sales E-mail: sales@zyxel.com.sg
- Telephone: +65-6899-6678
- Fax: +65-6899-8887
- Web: http://www.zyxel.com.sg
- Regular Mail: ZyXEL Singapore Pte Ltd., No. 2 International Business Park, The Strategy #03-28, Singapore 609930

### Spain

- Support E-mail: support@zyxel.es
- Sales E-mail: sales@zyxel.es
- Telephone: +34-902-195-420
- Fax: +34-913-005-345
- Web: www.zyxel.es
- Regular Mail: ZyXEL Communications, Arte, 21 5ª planta, 28033 Madrid, Spain

### Sweden

- Support E-mail: support@zyxel.se
- Sales E-mail: sales@zyxel.se
- Telephone: +46-31-744-7700
- Fax: +46-31-744-7701
- Web: www.zyxel.se
- Regular Mail: ZyXEL Communications A/S, Sjöporten 4, 41764 Göteborg, Sweden

### Taiwan

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-2-27399889
- Fax: +886-2-27353220
- Web: http://www.zyxel.com.tw
- Address: Room B, 21F., No.333, Sec. 2, Dunhua S. Rd., Da-an District, Taipei

### Thailand

- Support E-mail: support@zyxel.co.th
- Sales E-mail: sales@zyxel.co.th
- Telephone: +662-831-5315
- Fax: +662-831-5395
- Web: http://www.zyxel.co.th
- Regular Mail: ZyXEL Thailand Co., Ltd., 1/1 Moo 2, Ratchaphruk Road, Bangrak-Noi, Muang, Nonthaburi 11000, Thailand.

### Turkey

- Support E-mail: cso@zyxel.com.tr
- Telephone: +90 212 222 55 22
- Fax: +90-212-220-2526
- Web: http:www.zyxel.com.tr
- Address: Kaptanpasa Mahallesi Piyalepasa Bulvari Ortadogu Plaza N:14/13 K:6 Okmeydani/Sisli Istanbul/Turkey

### Ukraine

- Support E-mail: support@ua.zyxel.com
- Sales E-mail: sales@ua.zyxel.com
- Telephone: +380-44-247-69-78
- Fax: +380-44-494-49-32
- Web: www.ua.zyxel.com
- Regular Mail: ZyXEL Ukraine, 13, Pimonenko Str., Kiev 04050, Ukraine

### United Kingdom

- Support E-mail: support@zyxel.co.uk
- Sales E-mail: sales@zyxel.co.uk
- Telephone: +44-1344-303044, 0845 122 0301 (UK only)
- Fax: +44-1344-303034
- Web: www.zyxel.co.uk
- Regular Mail: ZyXEL Communications UK Ltd., 11 The Courtyard, Eastern Road, Bracknell, Berkshire RG12 2XB, United Kingdom (UK)

# Index

## D



## E



## F



## G



## H



## I

## J



## K



## L



## M



## N



## O



## P

## Q



## R



## S

## T



## U



## V



## W