WiMAX CPE Series

MAX208M, MAX218M, MAX208M2W, MAX218M2W, MAX218M1W, MAX218MW, MAX318M2W, MAX308M, MAX318M

User's Guide

Default Login Details

IP Address	http://192.168.1.1
Admin's User Name /Password	admin / 1234
Guest's User Name /Password	guest / guest

Firmware Version 2.00
Edition 1, 8/2011

www.zyxel.com

Copyright © 2011
ZyXEL Communications Corporation

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the WiMAX Device. See the product-specific QSG for hardware setup.

Note: This is a configuration manual for a series of products. Therefore, some features or options in this guide may not be available in your product.

Related Documentation

- Quick Start Guide

  The Quick Start Guide is designed to help you get your WiMAX Device up and running right away. It contains information on setting up your network and configuring for Internet access.

- Web Configurator Online Help

  The embedded Web Help contains descriptions of individual screens and supplementary information.

- Support Disc

  Refer to the included CD for support documents.

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 device.

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

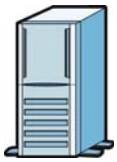
Syntax Conventions

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

Icons Used in Figures

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

Graphics in this book may differ slightly from the product due to differences in operating systems, operating system versions, or if you installed updated firmware/software for your device. Every effort has been made to ensure that the information in this manual is accurate.

WiMAX Device 	Computer 	Notebook computer 
Server 	Base Station 	Firewall 
Router 	Switch 	Telephone 
Internet 	Wireless Signal 	

Safety Warnings

- 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.
- ONLY qualified service personnel should service or disassemble this device.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT 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 power outlet.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- For indoor devices, 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

PART I
User's Guide

1

Introduction to the Series

1.1 About Your WiMAX Device

The WiMAX Device allows you to access the Internet by connecting to a WiMAX wireless network. For some models, you can use a traditional analog telephone to make Internet calls using the WiMAX Device's Voice over IP (VoIP) communication capabilities.

Additionally, The web browser-based Graphical User Interface (GUI), also known as the web configurator, provides easy management of the device and its features.

Please refer to the following description of the product name format.

- Models starting with "2" (for example MAX208M2W) denote an indoor CPE device; models starting with "3" (for example MAX318M2W) denote an outdoor CPE device.
- Models with the second number as "0" (for example MAX208M2W) denote that its frequency band is 2.5GHz ~ 2.7GHz; models with the second number as "1" (for example MAX218M2W) denote that its frequency band is 3.4GHz ~ 3.6GHz.
- The number after the letter "M" denote the number of VoIP ports that the device has. For example, MAX208M2W has 2 VoIP ports; MAX218M has no VoIP port.
- Models ending with "W" (for example MAX208M2W) denote WiFi functionality, including 802.11n mode.

See the following table for the main features for each specific model:

Table 1 Main Features

FEATURE / MODEL	FREQUENCY BAND	NUMBER OF PHONE PORTS	WIFI FUNCTION	INDOOR DEVICE	OUTDOOR DEVICE
MAX208M	2.5 ~ 2.7 GHz	N/A	N/A	✓	
MAX218M	3.4 ~ 3.6 GHz	N/A	N/A	✓	
MAX208M2W	2.5 ~ 2.7 GHz	2	✓	✓	
MAX218M2W	3.4 ~ 3.6 GHz	2	✓	✓	
MAX218M1W	3.4 ~ 3.6 GHz	1	✓	✓	
MAX218MW	3.4 ~ 3.6 GHz	N/A	✓	✓	
MAX318M2W	3.4 ~ 3.6 GHz	2	✓		✓
MAX308M	2.5 ~ 2.7 GHz	N/A	N/A		✓
MAX318M	3.4 ~ 3.6 GHz	N/A	N/A		✓

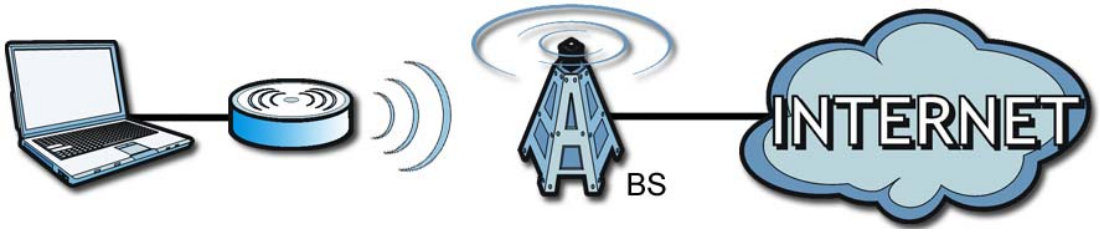
1.1.1 WiMAX Internet Access

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

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

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

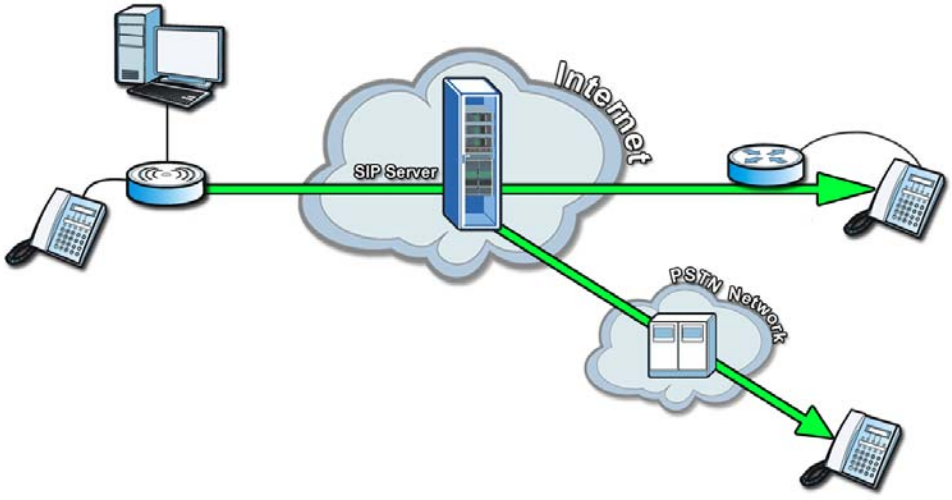
Use content filtering to block access to web sites with URLs containing keywords that you specify. You can define time periods and days during which content filtering is enabled and include or exclude particular computers on your network from content filtering. For example, you could block access to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

1.1.2 Models with Phone Ports

For models with phone ports, you can use the WiMAX Device to make and receive Voice over Internet Phone (VoIP) telephone calls:

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

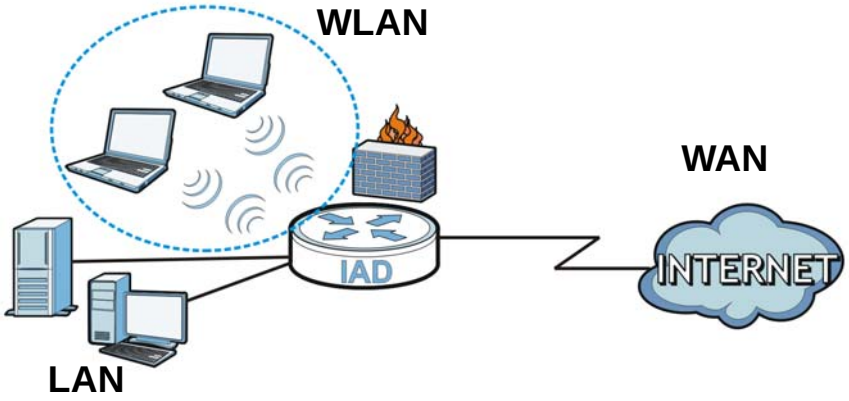
Figure 2 Calls via VoIP Service Provider



1.1.3 Models with WiFi

For WiFi models, IEEE 802.11b/g/n compliant clients can wirelessly connect to the WiMAX Device to access network resources. You can set up a wireless network with WPS (WiFi Protected Setup) or manually add a client to your wireless network.

Figure 3 WiFi Connection Application



1.2 Good Habits for Managing the WiMAX Device

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

- Change 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 Device becomes unstable or even crashes. If you forget your password, you will have to reset the WiMAX Device to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the WiMAX Device. You could simply restore your last configuration.

2

Introduction to 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 233 for more information on configuring your web browser.

2.1.1 Accessing the Web Configurator

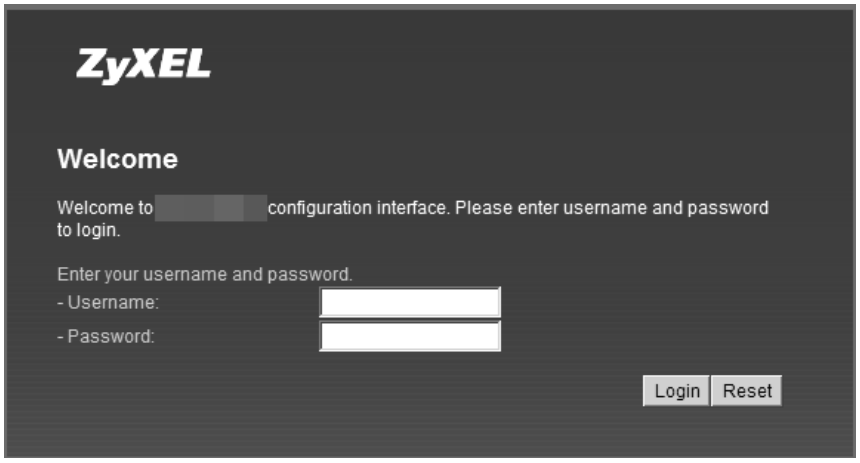
1 Make sure your WiMAX Device hardware is properly connected (refer to the Quick Start Guide for more information).

2 Launch your web browser.

3 Enter 192.168.1.1192.168.1.1" as the URL.

4 A login screen displays. Enter the default **Username** (admin) and **Password** (1234), then click **Login**.

Figure 4 Login screen

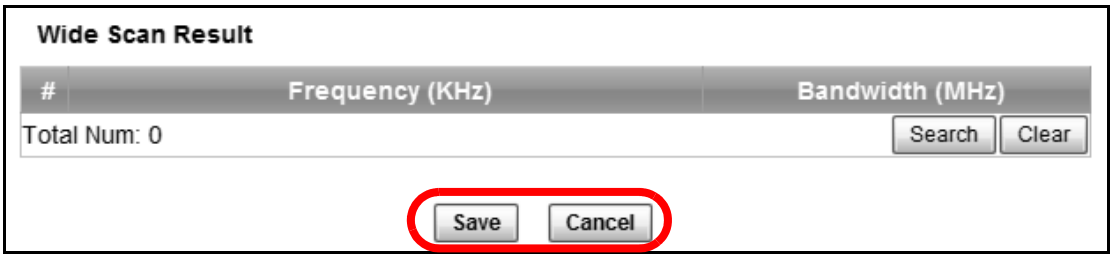


Note: For security reasons, the WiMAX Device automatically logs you out if you do not use the Web Configurator for five minutes. If this happens, log in again.

2.1.2 Saving and Canceling Changes

All screens to which you can make configuration changes must be saved before those changes can go into effect. If you make a mistake while configuring the WiMAX Device, you can cancel those changes and start over.

Figure 5 Saving and Canceling Changes



This screen contains the following fields:

Table 2 Saving and Canceling Changes

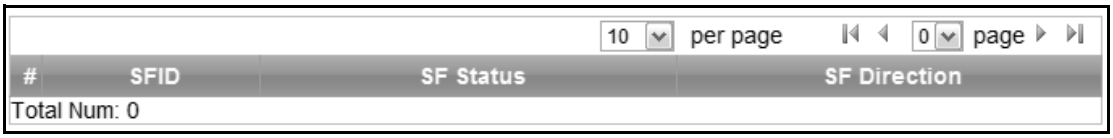
LABEL	DESCRIPTION
Save	Click this to save your changes.
Cancel	Click this to restore the settings on this page to their last saved values.

Note: If you make changes to a page but do not save before switching to another page or exiting the Web Configurator, those changes are discarded.

2.1.3 Working with Tables

Many screens in the WiMAX Device contain tables to provide information or additional configuration options.

Figure 6 Tables Example



This screen contains the following fields:

Table 3 Saving and Canceling Changes

LABEL	DESCRIPTION
10 per page	Items per Page This displays the number of items displayed per table page. Use the menu to change this value.
	First Page Click this to go to the first page in the table.

Table 3 Saving and Canceling Changes (continued)

LABEL	DESCRIPTION
	Previous Page Click this to go to the previous page in the table.
	Page Indicator / Jump to Page This indicates which page is currently displayed in the table. Use the menu to jump to another page. You can only jump to other pages if those pages exist.
	Next Page Click this to go to the previous page in the table.
	Last Page Click this to go to the last page in the table.
#	This indicates an item's position in the table. It has no bearing on that item's importance or lack there of.
Total Num	This indicates the total number of items in the table, including items on pages that are not visible.

2.2 The Main Screen

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

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

Note: The available menus and screens vary depending on the type of account (admin or guest) you use for login.

Figure 7 Main Screen

The following table describes the menus in this screen.

Table 4 Main > Menu

MENU	DESCRIPTION
Language	Use this menu to select the Web Configurator's language.
Setup Wizard	Click this to open the Setup Wizard, where you can configure the most essential settings for your WiMAX Device to work.
Logout	Click this to log out of the Web Configurator.
System Status	Click this to open the **Main** screen, which shows your WiMAX Device status and other information.
WiMAX	Click this to open the WiMAX menu, which gives you options for configuring your WiMAX settings.
Network Setting	Click this to open the Network menu, which gives you options for configuring your WAN/LAN/WiFi network settings.
Security	Click this to open the Security menu, which gives you options for configuring your firewall and security settings.
VoIP	Click this icon to open the VoIP menu, which gives you options on how to make telephone calls over the Internet via the WiMAX Device.
Maintenance	Click this to open the Maintenance menu, which gives you options for maintaining your WiMAX Device and performing basic network connectivity tests.

3

Setup Wizard

3.1 Overview

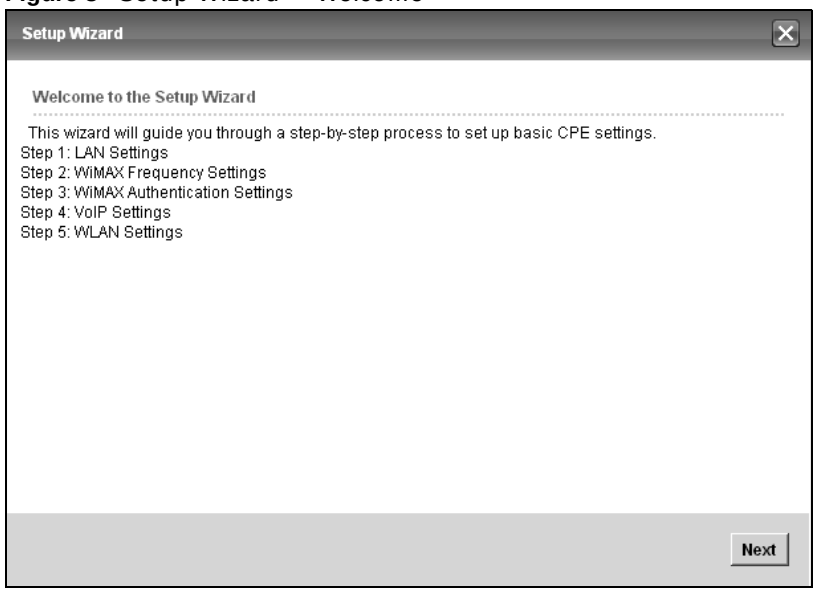
This chapter provides information on the Setup Wizard. The wizard guides you through several steps for configuring your network settings.

3.1.1 Welcome to the Setup Wizard

This screen provides a quick summary of the configuration tasks the wizard helps you to perform. They are:

1. Set up your Local Area Network (LAN) options, which determine how the devices in your home or office connect to the WiMAX Device.
2. Set up your WiMAX Device's broadcast frequency, which is the radio channel it uses to communicate with the ISP's base station.
3. Set up your WiMAX Device's login options, which are used to connect your LAN to the ISP's network and verify your account.
4. For models with VoIP feature, set up your WiMAX Device's VoIP Settings, which will allow you to make calls over the Internet.
5. For models with WiFi feature, set up your WiMAX Device's wireless LAN so that other devices, such as a laptop or a smartphone, can connect wirelessly to the Internet using the WiMAX Device.

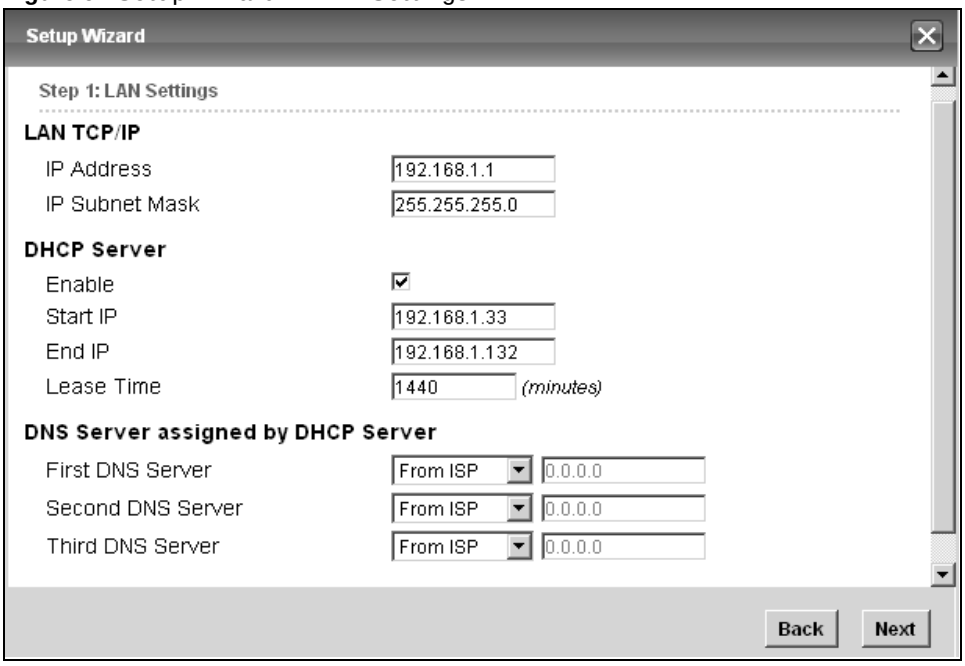
Figure 8 Setup Wizard > Welcome



3.1.2 LAN Settings

The LAN Settings screen allows you to configure your local network options.

Figure 9 Setup Wizard > LAN Settings



The following table describes the labels in this screen.

Table 5 Setup Wizard > LAN Settings

LABEL	DESCRIPTION
LAN TCP/IP	
IP Address	Enter the IP address of the WiMAX Device on the LAN. Note: This field is the IP address you use to access the WiMAX Device on the LAN. If the web configurator is running on a computer on the LAN, you lose access to it as soon as you change this field. 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.
DHCP Server	
Enable	Select this if you want the WiMAX Device to be the DHCP server on the LAN. As a DHCP server, the WiMAX Device assigns IP addresses to DHCP clients on the LAN and provides the subnet mask and DNS server information.
Start IP	Enter the IP address from which the WiMAX Device begins allocating IP addresses.
End IP	Enter the IP address at which the WiMAX Device stops allocating IP addresses.
Lease Time	Enter the duration in minutes before the device requests a new IP address from the DHCP server.
DNS Server assigned by DHCP Server	
First DNS Server	Specify the first IP address of three DNS servers that the network can use. The WiMAX Device provides these IP addresses to DHCP clients.

Table 5 Setup Wizard > LAN Settings (continued)

LABEL	DESCRIPTION
Second DNS Server	Specify the second IP address of three DNS servers that the network can use. The WiMAX Device provides these IP addresses to DHCP clients.
Third DNS Server	Specify the third IP address of three DNS servers that the network can use. The WiMAX Device provides these IP addresses to DHCP clients.
Back	Click to display the previous screen.
Next	Click to proceed to the next screen.

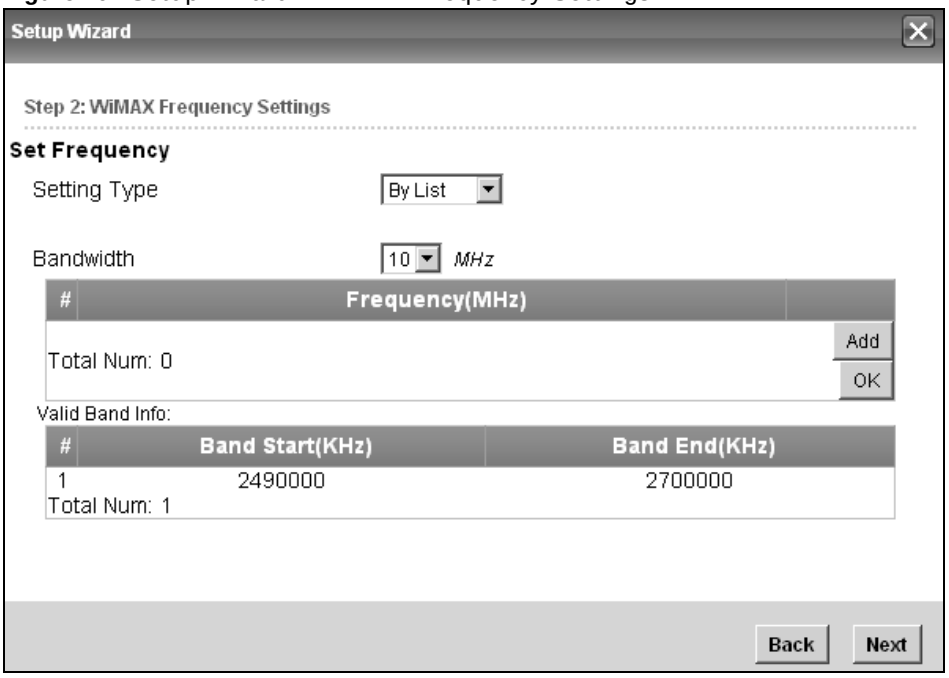
3.1.3 WiMAX Frequency Settings

The WiMAX Frequency Settings screen allows you to configure the broadcast radio frequency used by the WiMAX Device.

Note: The frequency band varies for different models. See Section 1.1 on page 17 for more information.

Note: These settings should be provided by your ISP.

Figure 10 Setup Wizard > WiMAX Frequency Settings



The following table describes the labels in this screen.

Table 6 Setup Wizard > WiMAX Frequency Settings

LABEL	DESCRIPTION
Setting Type	Select the WiMAX frequency setting type from the list. • **By Range** - Select this to set up the frequency based on a range of MHz. • **By List** - Select this to set up the frequency on an individual MHz basis. You can add multiple MHz values to the list.
Step	Enter the increments in MHz by which to increase the frequency range. Note: This field only appears when you select **By Range** under **Setting Type**.
Start Frequency	Enter the frequency value at the beginning of the frequency range to use. The frequency is increased in increments equal to the **Step** value until the **End Frequency** is reached, at which time the cycle starts over with the **Start Frequency**. Note: This field only appears when you select **By Range** under **Setting Type**.
End Frequency	Enter the frequency value at the end of the frequency range to use. Note: This field only appears when you select **By Range** under **Setting Type**.
Bandwidth	Set the frequency bandwidth in MHz that this WiMAX Device uses.
#	This is an index number for enumeration purposes only.
Frequency (MHz)	Displays the frequency MHz for the item in the list.
Total Num	Displays the total number of items in the list.
Delete	Click this to remove an item from the list.
Add	Click this to add an item to the list.
OK	Click this to save an newly added item to the list.
#	This is an index number for enumeration purposes only.
Band Start (KHz)	Indicates the beginning of the frequency band in KHz.
Band End (KHz)	Indicates the end of the frequency band in KHz.
Total Num	Displays the total number of items in the list.
Back	Click to display the previous screen.
Next	Click to proceed to the next screen.

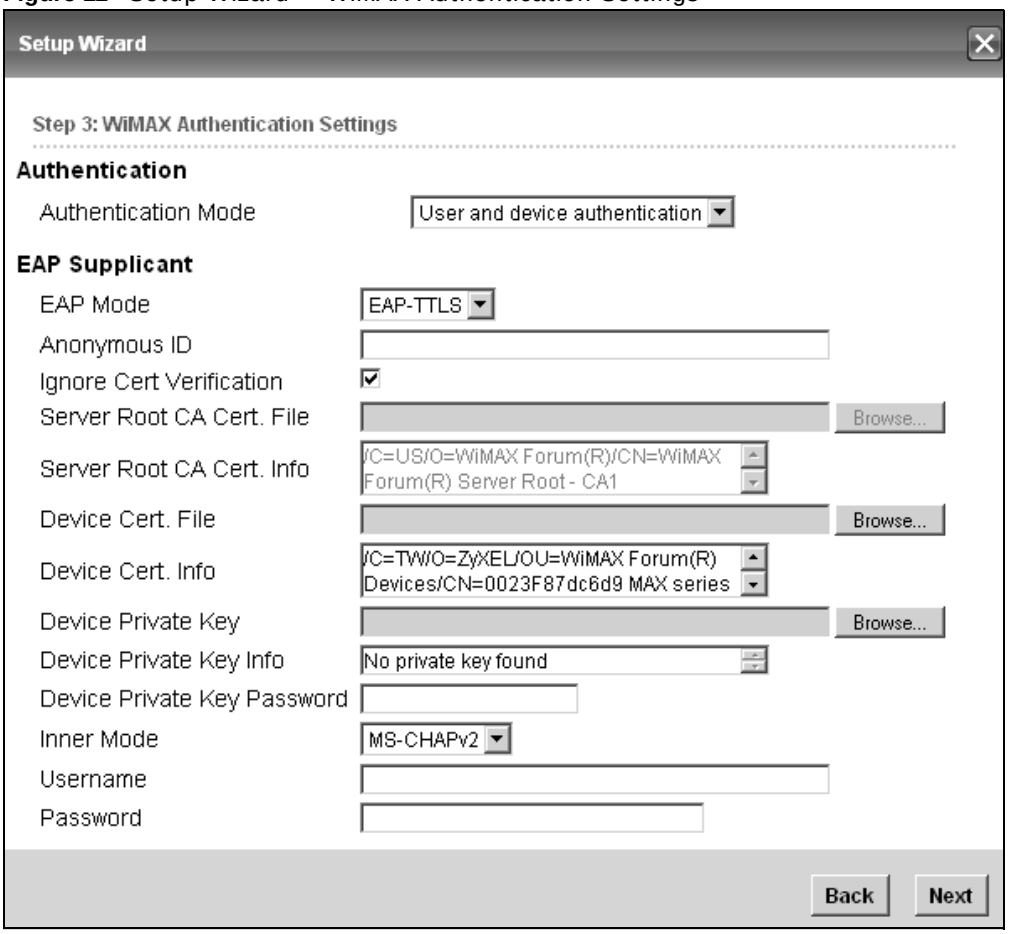
3.1.4 WiMAX Authentication Settings

The WiMAX Authentication Settings screen allows you to configure how your WiMAX Device logs into the service provider's network.

Note: These settings should be provided by your ISP.

Note: The EAP supplicant settings on this screen vary depending on the authentication mode your select.

Figure 11 Setup Wizard > WiMAX Authentication Settings



The following table describes the labels in this screen.

Table 7 Setup Wizard > WiMAX Authentication Settings

LABEL	DESCRIPTION
Authentication	
Authentication Mode	Select a WiMAX authentication mode for authentication network sessions with the ISP. Options are: • No authentication • User authentication • Device authentication • User and Device authentication
EAP Supplication	
EAP Mode	Select an EAP authentication mode. See Table 14 on page 76 if you need more information.
Anonymous Id	Enter your anonymous ID. Note: Some modes may not require this.
Ignore Cert Verification	Select this to ignore base station certification verification when a certificate is received during EAP-TLS or EAP-TTLS.

Table 7 Setup Wizard > WiMAX Authentication Settings (continued)

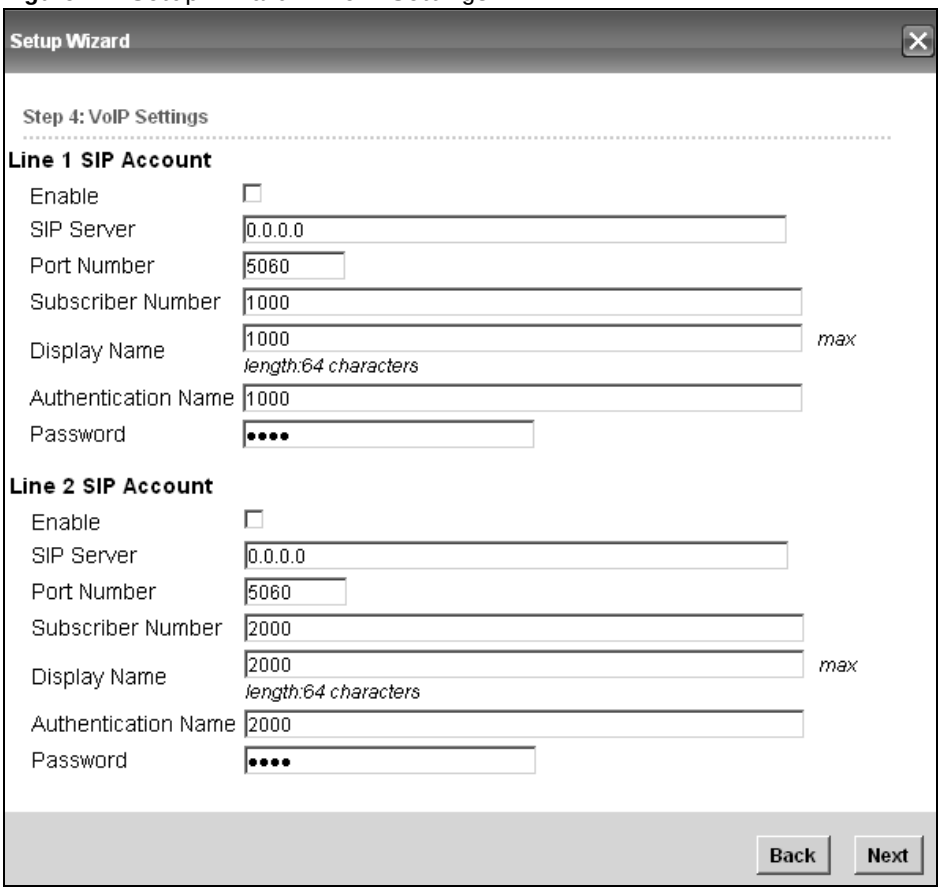
LABEL	DESCRIPTION
Server Root CA Cert. File	Browse for and choose a server root certificate file, if required.
Server Root CA Cert. Info	This field displays information about the assigned server root certificate.
Device Cert. File	Browse for and choose a device certificate file, if required.
Device Cert. Info.	This field displays information about the assigned device certificate.
Device Private Key	Browse for and choose a device private key, if required.
Device Private Key Info	This field displays information about the assigned device private key.
Device Private Key Password	Enter the device private key, if required.
Inner Mode	Select an inner authentication mode (MS-CHAP, MS-CHAPV2, CHAP, MD5, PAP. See Table 14 on page 76 if you need more information.
Username	Enter your authentication username.
Password	Enter your authentication password.
Back	Click to display the previous screen.
Next	Click to proceed to the next screen.

3.1.5 VoIP Settings

For models with VoIP feature, you can configure your VoIP settings in the **Setup Wizard**. The VoIP Settings screen allows you to configure how your WiMAX Device connects to the VoIP service provider's network and makes calls over the Internet.

Note: This settings should be provided by your VoIP service provider.

Figure 12 Setup Wizard > VoIP Settings



The following table describes the labels in this screen.

Table 8 Setup Wizard > VoIP Settings

LABEL	DESCRIPTION
Line 1/2 SIP Account - Configure this section to use the **PHONE 1** and/or **PHONE 2** port.	
Enable	Select this to activate the SIP account.
SIP Server	Enter the IP address or domain name of the SIP server.
Port Number	Enter the SIP server's listening port number.
Subscriber Number	Enter your SIP number. In the full SIP URI, this is the part before the @ symbol.
Display Name	Enter the name that appears on the other party's device if they have Caller ID enabled.
Authentication Name	Type the SIP user name associated with this account for authentication to the SIP server.
Password	Type the SIP password associated with this account.
Back	Click to display the previous screen.
Next	Click to proceed to the next screen.

3.1.6 WLAN Settings

For models with WiFi wireless feature, you can configure your WLAN settings in the **Setup Wizard**. The WLAN Settings screen lets you set up how other devices connect to the Internet wirelessly using the WiMAX Device.

Figure 13 Setup Wizard > WLAN Settings

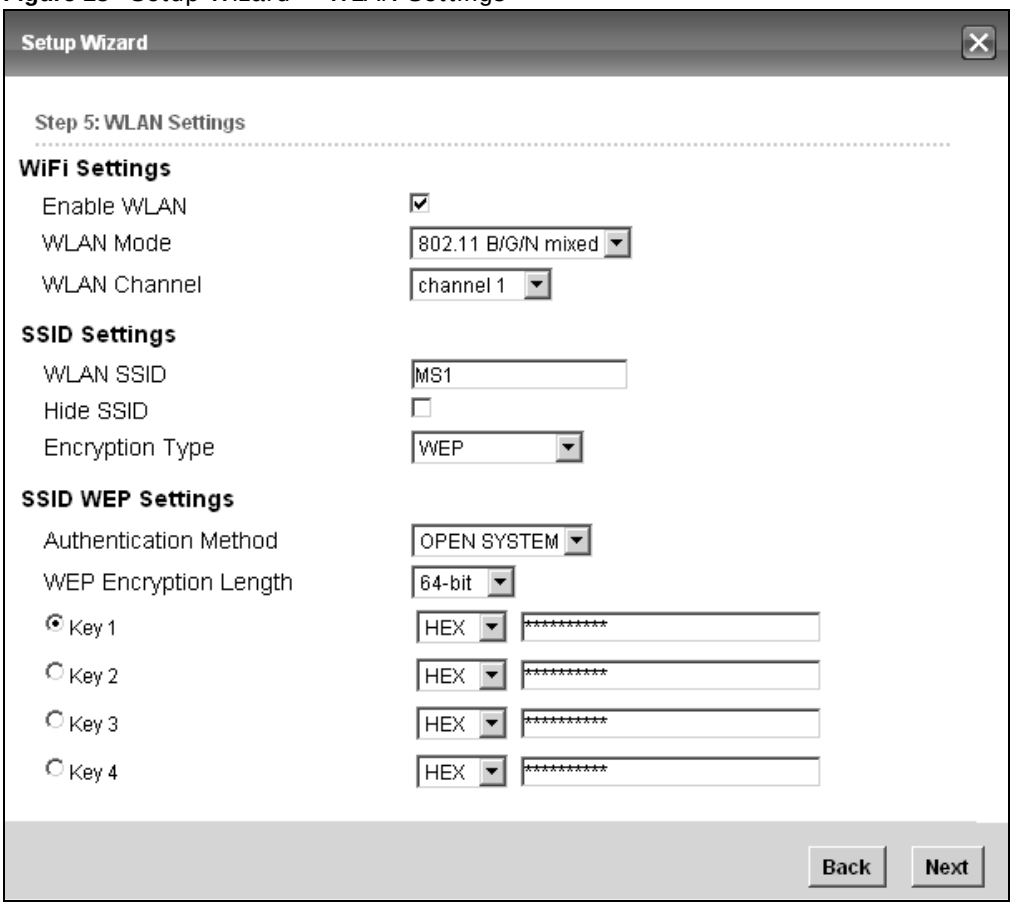
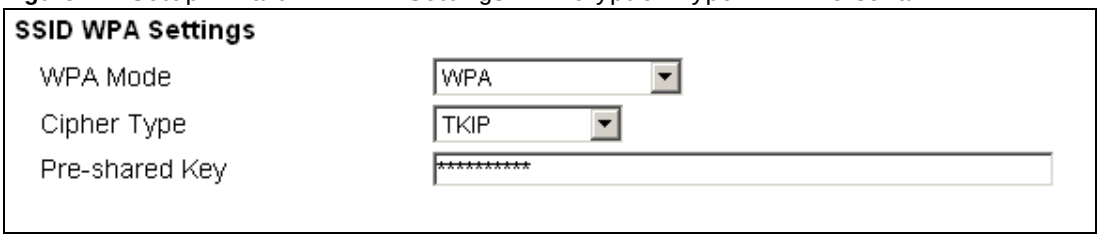


Figure 14 Setup Wizard > WLAN Settings > Encryption Type: WPA Personal



The following table describes the labels in this screen.

Table 9 Setup Wizard > WLAN Settings

LABEL	DESCRIPTION
Wifi Settings	
Enable WLAN	Select this box to enable the wireless service and allow other wireless clients to connect to the Internet using the WiMAX Device.

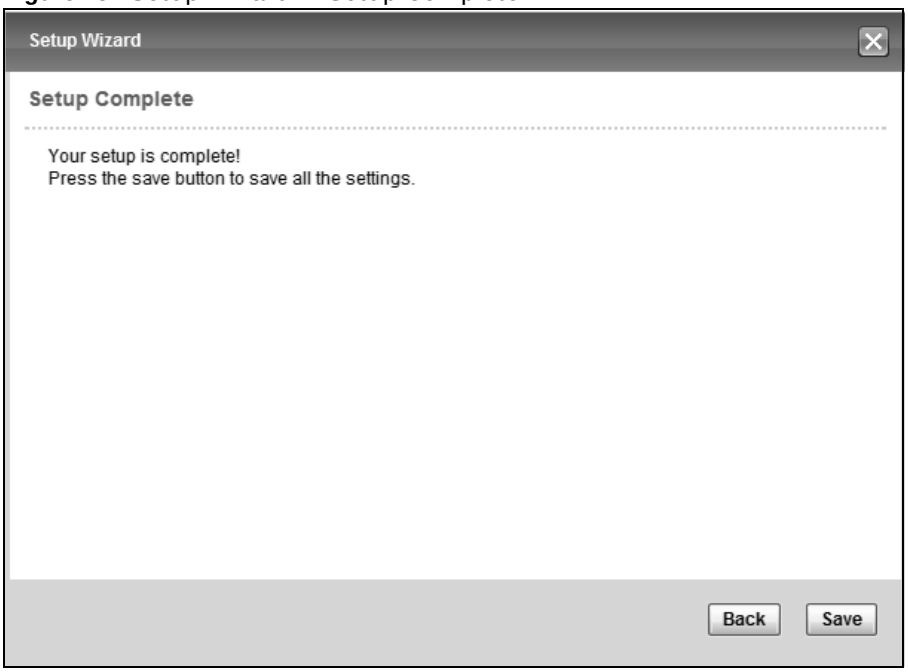
Table 9 Setup Wizard > WLAN Settings (continued)

LABEL	DESCRIPTION
WLAN Mode	Select the mode that the WiMAX Device will be using to communicate: **802.11 B/G mixed**, **802.11 B only**, **802.11 G only**, **802.11 N only,** or **802.11 B/G/ N mixed**.
WLAN Channel	Select one channel from 1 to 13 for wireless communications with the wireless stations.
SSID Settings	
WLAN SSID	This field displays the name of the wireless network associated with the WiMAX Device.
Hide SSID	Select this option if you wish to keep the name of the wireless network hidden.
Encryption Type	Select the type of encryption that the network will be using: **None**, **WEP**, or **WPA Personal**.
SSID WEP Settings Note: You will only see this options if you selected **WEP** as the **Encryption Type**.	
Authentication Method	Select the type of authentication used to join the network: **Open System** or **Shared Key**.
WEP Encryption Length	Select the length of the encryption key: 64-bit or 128-bit.
Key 1 - 4	Pick one of four available keys. The key can be in either Hexagecimal (HEX) or ASCII format. Type the key using any letters and numbers. The field is case sensitive and the length must match the length picked in the step above (64-bit or 128-bit). A warning message will appear if you fail to do this.
SSID WPA Settings Note: You will only see this options if you selected **WPA Personal** as the **Encryption Type**.	
WPA Mode	Select either **WPA**, **WPA2** or **Auto (WPA or WPA2)**.
Cipher Type	Select the type of authentication that you wish to use for your network: **TKIP**, **AES** or **TKIP and AES**. **AES** is more secure.
Pre Shared Key	Type the pre-shared key or PSK previously shared between the two parties.

3.1.7 Setup Complete

Click **Save** to save the Setup Wizard settings and close it.

Figure 15 Setup Wizard > Setup Complete



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

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

Note: If you cannot access the Internet, open the web configurator again to confirm that the Internet settings you configured in the **Wizard Setup** are correct.

4

Tutorials

4.1 Overview

Run the Setup Wizard for the basic setup of your WiMAX Device. This chapter shows you how to configure some of the advanced settings WiMAX Device's features.

Note: Be sure to read Introduction to the Web Configurator on page 20 before working through the tutorials presented here. For field descriptions for individual screens, see the related technical reference in this User's Guide.

This chapter includes the following configuration examples:

- WiMAX Connection Settings on page 35
- Setting Up a Small Network for the LAN on page 36
- Making a Telephone Call Over the Internet on page 38
- Blocking Web Access from the WiMAX Device on page 40
- Restricting Wireless Access to the WiMAX Device on page 40
- Allowing Internet Users to use Internal Servers, see page 42
- Access the WiMAX Device with a Domain Name, see page 44
- Configuring Static Route for Routing to Another Network, see page 46
- Remotely Managing Your WiMAX Device on page 48
- Changing Certificate to Communicate with Other Networks on page 49
- Using Virtual Networks on page 50

4.2 WiMAX Connection Settings

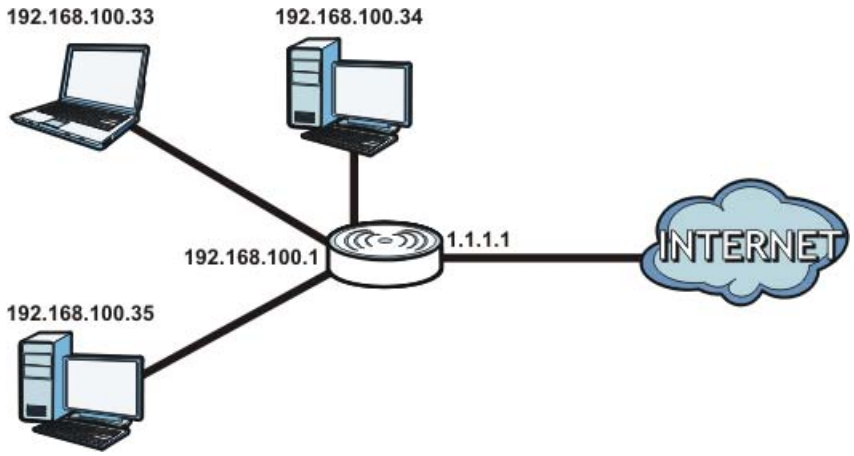
This tutorial provides you with pointers for configuring the WiMAX Device to connect to an ISP.

1. Connect the WiMAX Device to the ISP's nearest base station. See Section 6.2 on page 70.
2. Configure the WiMAX Device's broadcast frequency. Section 6.3 on page 72.
3. Configure the WiMAX Device to connect securely to the ISP's authentication servers. See Section 6.4 on page 74.
4. Check the WiMAX Device's connection status to ensure everything is working properly. See Section 6.11 on page 87.

4.3 Setting Up a Small Network for the LAN

This tutorial shows you how to set up a small network in your office or home.

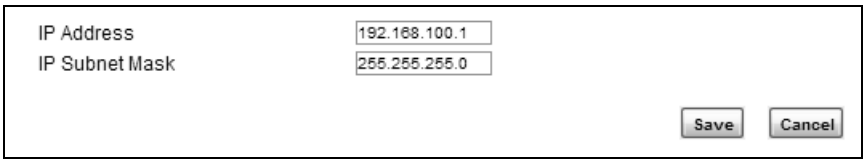
Goal: Connect three computers to your WiMAX Device to form a small network.



Required: The following table provides a summary of the information you will need to complete the tasks in this tutorial.

INFORMATION	VALUE	SEE ALSO
LAN IP Address	192.168.100.1	Chapter 7 on page 98
Starting IP Address	192.168.100.10	Chapter 7 on page 99
Ending IP Address	192.168.100.30	
DNS Servers	From ISP	

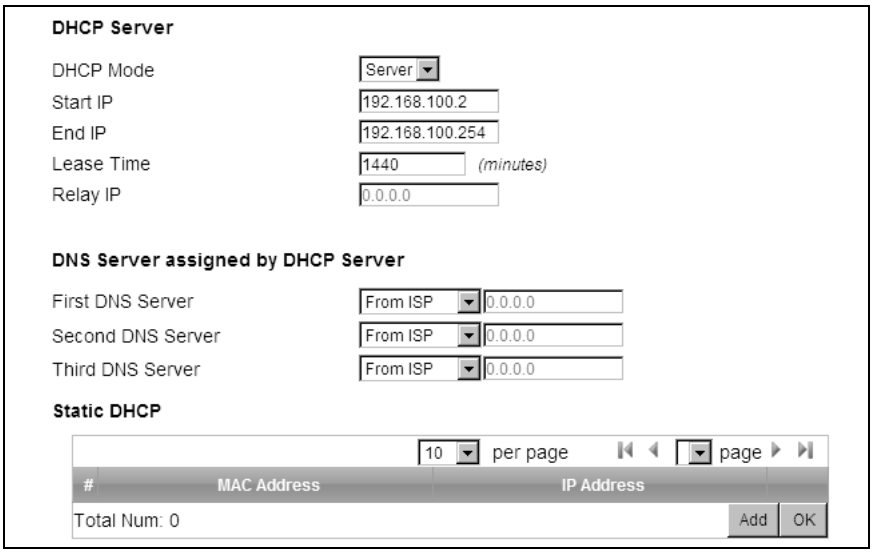
1 In the Web Configurator, open the **Network Setting > LAN** screen and set the IP Address to 192.168.100.1. Use the default **IP Subnet Mask** of 255.255.255.0. Click **Save**.



2 Manually change the IP address of your computer that your are using to 192.168.100.x (for example, 192.168.100.5) and keep the subnet set to 255.255.255.0.

3 Type http://192.168.100.1 in your browser after the WiMAX Device finishes starting up completely.

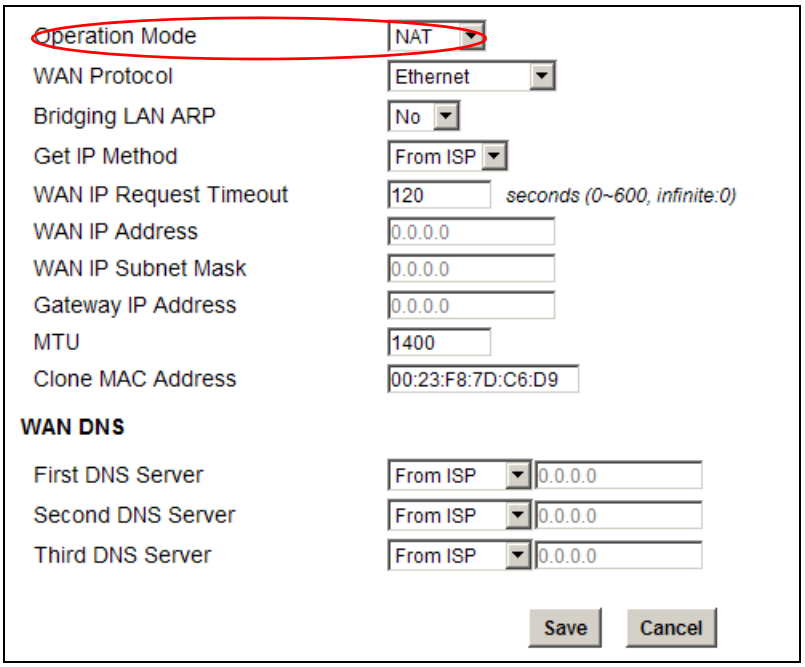
4 Log into the Web Configurator and open the **Network Setting > LAN > DHCP** screen.



5 Select **Server** for the DHCP mode, then enter 192.168.100.10 and 192.168.100.30 as your DHCP starting and ending IP addresses.

6 Leave the other settings as their defaults and click **Save**.

7 Next, go to the **Network Setting > WAN** screen and select **NAT** in the **Operation Mode** field. Click **Save**.



8 Connect your computers to the WiMAX Device's Ethernet ports and you're all set!

Note: You may need to configure the computers on your LAN to automatically obtain IP addresses. For information on how to do this, see Appendix B on page 209.

Once your network is configured and hooked up, you will want to connect it to the Internet next. To do this, just run the **Internet Connection Wizard** (Chapter 3 on page 25), which walks you through the process.

4.4 Making a Telephone Call Over the Internet

For models with phone port(s), you can make a call over the Internet using the WiMAX Device.

4.4.1 Configure Your SIP Account

Your WiMAX Device needs to be configured with the details of your SIP account before you can use it to make calls over the Internet.

Once you have connected the WiMAX Device to your computer and accessed the Web Configurator, follow the steps below to configure your SIP settings.

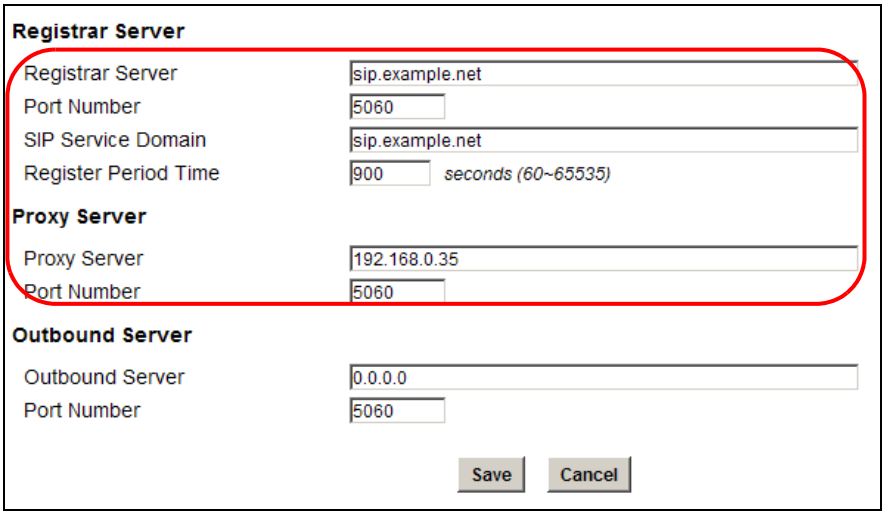
For some models (see Section 1.1 on page 17 for the specific models) that have 2 phone ports, you can configure 2 SIP accounts. The following example uses only 1 SIP account, as the configuration steps are the same for the second account if there is one.

The following parameters are used in this example:

Registrar Server	sip.example.net
Proxy Server	192.168.0.35
Subscriber Number	12345678
Authentication Name	ChangeMe
Password	ThisIsMySIP

1 Click **VoIP > Account > Server**.

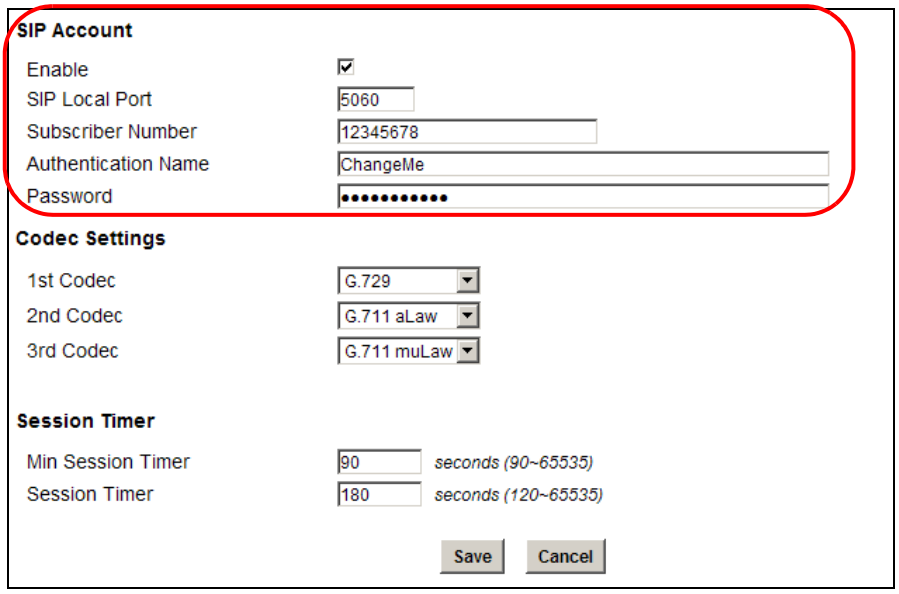
2 Enter the fields in the screen according to the parameters provided. For field information that is not provided, leave it as the default setting.



3 Click **Save** to save your settings.

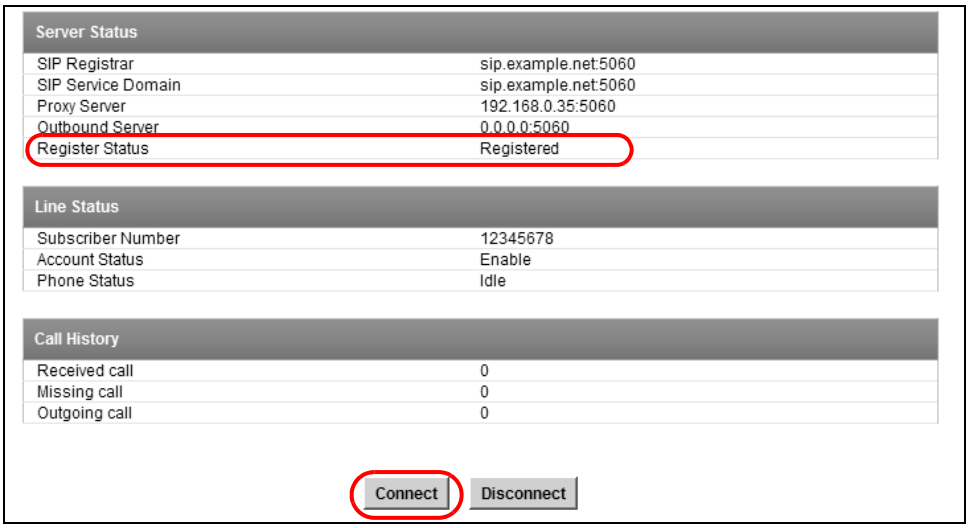
4 Click **VoIP > Account > SIP**.

5 Select the **Enable** checkbox and enter the parameters provided in the **SIP Account** section.



6 Click **Save** to save your settings.

7 Click **VoIP > Account > Status**. Click **Connect** to to register the WiMAX Device to the register server. If the **Register Status** is **Registered**, it is ready to use. If this field shows **Register Fail**, contact your VoIP provider to confirm that you have the correct settings and that your account is active.



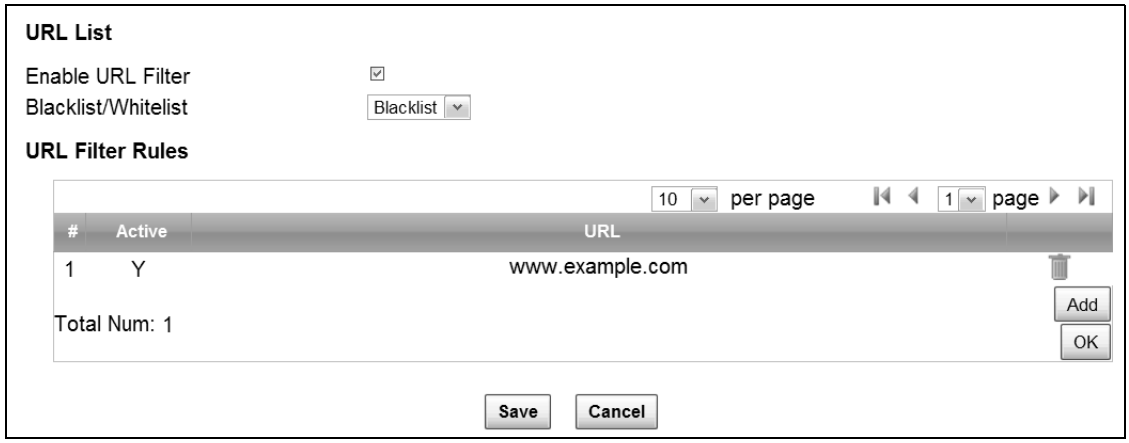
4.5 Blocking Web Access from the WiMAX Device

If your WiMAX Device is in a home or office environment you may decide that you want to block an Internet website access. You may need to block both the website's IP address and domain name.

Goal: Configure the WiMAX Device's content filter to block a website with a domain name www.example.com.

See Also: Section 7.23 on page 123.

1. Open the **Network Setting > Content Filter**.
2. Select **Enable URL Filter**.
3. Select **Blacklist**.
4. Click **Add** and configure a URL filter rule by selecting **Active** and entering www.example.com as the URL.
5. Click **OK**.
6. Click **Save**.

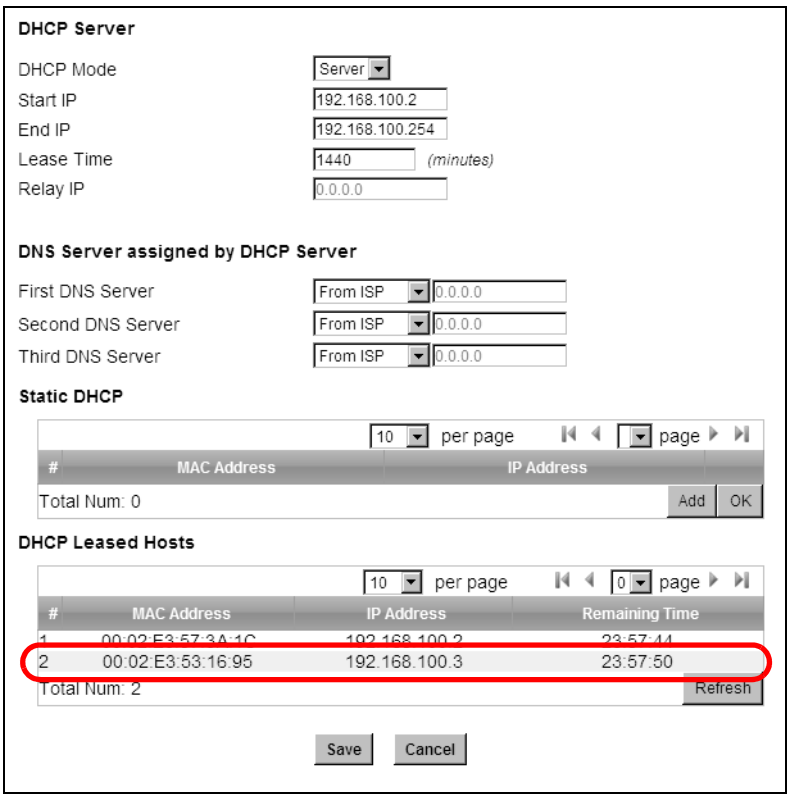


Open a browser from your computer in the WiMAX Device's LAN network, you should get an "**Access Violation**" message when you try to access to http://www.example.com. You may also need to block the IP address of the website if you do not want users to access to the website through its IP address.

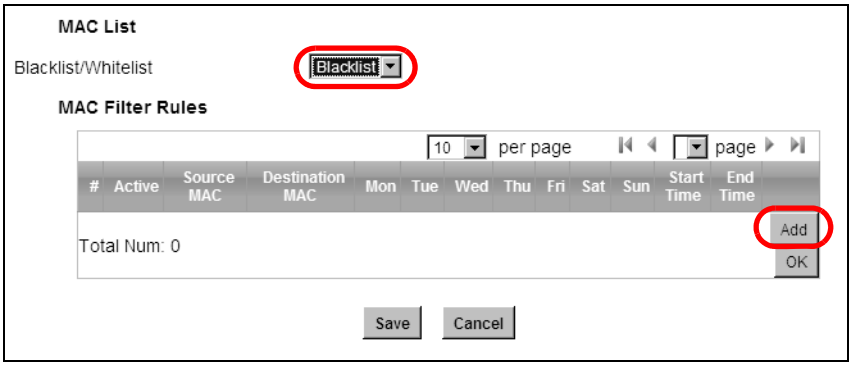
4.6 Restricting Wireless Access to the WiMAX Device

This tutorial shows you how to use the MAC filter to block a DHCP client's access to the WiMAX network.

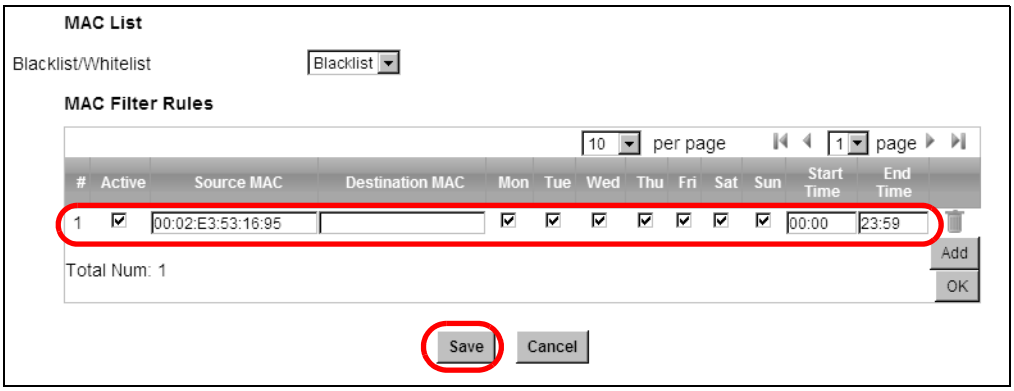
1 First of all, you have to know the MAC address of the computer. If not, you can look for the MAC address in the **Network Setting** > **LAN** > **DHCP** screen. (192.168.100.3 mapping to 00:02:E3:53:16:95 in this example).



2 Click **Security** > **Firewall** > **MAC Filter**. Select **Blacklist** and click the **Add** button in the **MAC Filter Rules** table.



3 An empty entry appears. Enter the computer's MAC address in the **Source MAC** field and leave the other fields set to their defaults. Click **Save**.



The computer will no longer be able to access any host on the WiMAX network through the WiMAX Device.

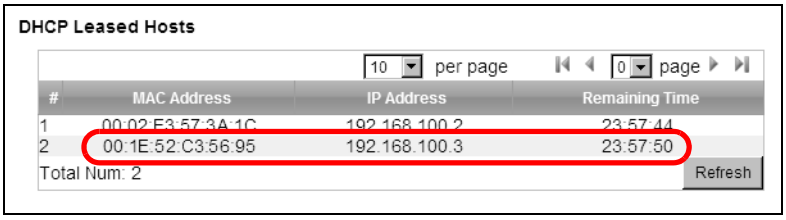
4.7 Allowing Internet Users to use Internal Servers

Thomas recently received an Xbox 360 as his birthday gift. His friends invited him to play online games with them on Xbox LIVE. In order to communicate and play with other gamers on Xbox LIVE, Thomas needs to configure the port settings on his WiMAX Device.

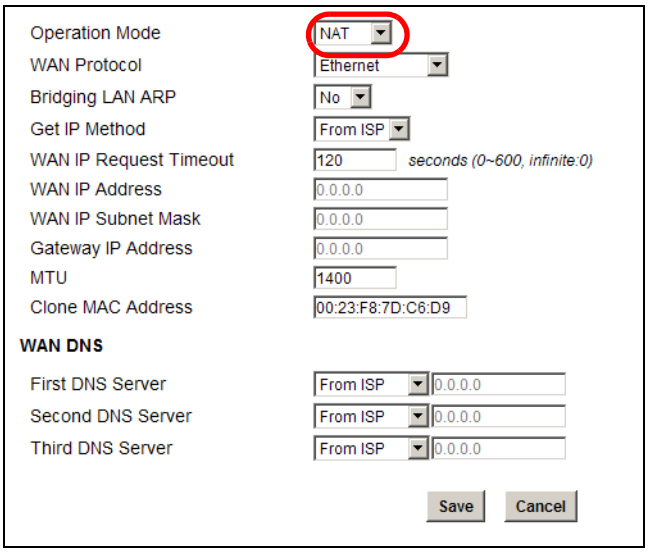
Xbox 360 requires the following ports to be available in order to operate Xbox LIVE correctly:

TCP: 53, 80, 3074
UDP: 53, 88, 3074

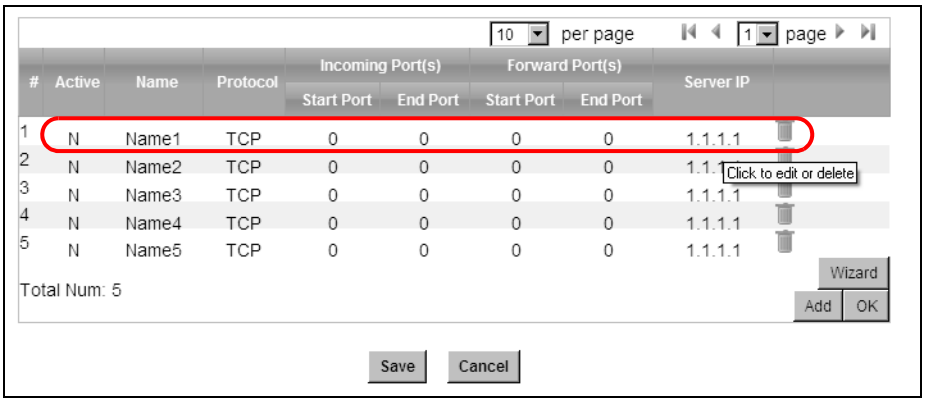
1 You have to know the Xbox 360's IP address first. You can check it through the Xbox 360 console. You may be able to check the IP address on the WiMAX Device if the WiMAX Device has assigned a DHCP IP address to the Xbox 360. Check the **DHCP Leased Hosts** table in the **Network** > **LAN** > **DHCP** screen. Look for the IP address for the Xbox 360.



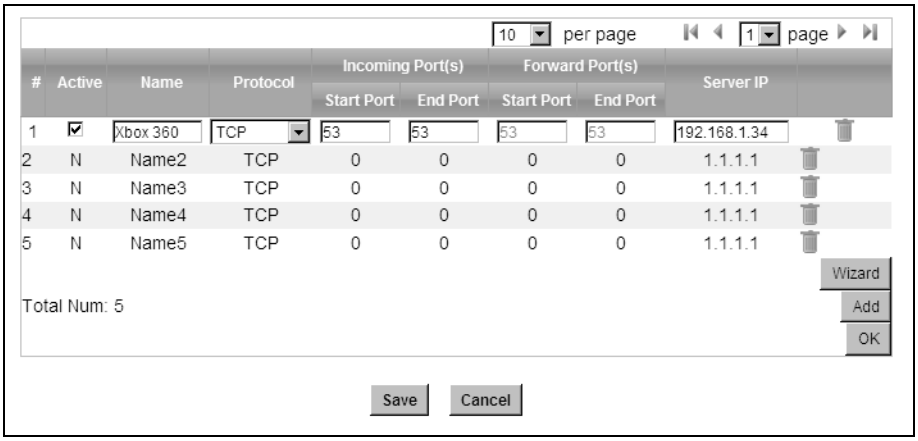
2 NAT mode is required to use port forwarding. Click **Network Setting** > **WAN** and make sure **NAT** is selected in the **Operation Mode** field. Click **Save**.



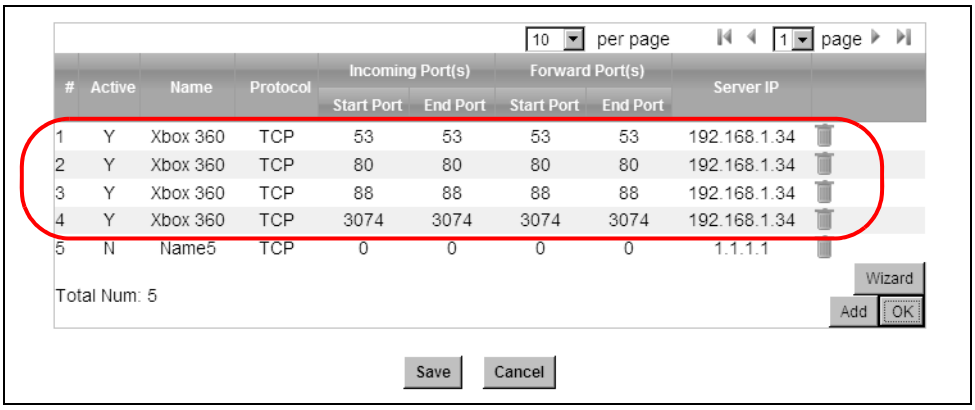
3 Click **Network Setting** > **NAT** > **Port Forwarding** and then click the first entry to edit the rule.



4 Configure the screen as follows to open TCP/UDP port 53 for the Xbox 360. Click **OK**.



5 Repeat steps 2 and 3 to open the rest of the ports for the Xbox 360. The port forwarding settings you configured are listed in the **Port Forwarding** screen.

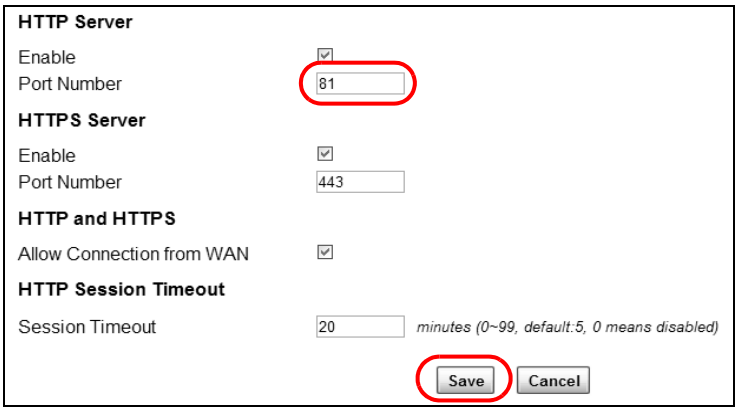


6 Click **Save**.

Thomas can then connect his Xbox 360 to the Internet and play online games with his friends.

In this tutorial, all port 80 traffic is forwarded to the Xbox 360, but port 80 is also the default listening port for remote management via WWW. If Thomas also wants to manage the WiMAX Device from the Internet, he has to assign an unused port to WWW remote access.

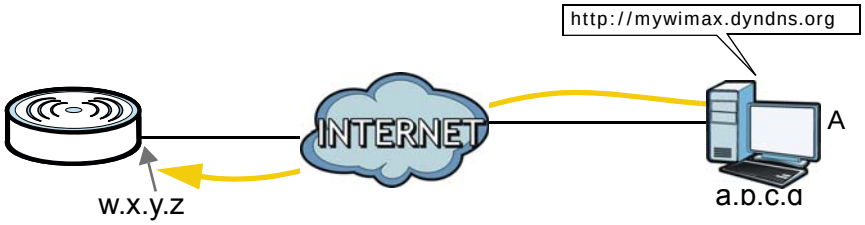
Click **Maintenance** > **Remote MGMT**. Enter an unused port in the **Port** field (81 in this example). Click **Save**.



4.8 Access the WiMAX Device with a Domain Name

If you connect your WiMAX Device to the Internet and it uses a dynamic WAN IP address, it is inconvenient for you to manage the device from the Internet. The WiMAX Device's WAN IP address

changes dynamically. Dynamic DNS (DDNS) allows you to access the WiMAX Device using a domain name.



To use this feature, you have to apply for DDNS service at www.dyndns.org.

This tutorial covers:

- Registering a DDNS Account on www.dyndns.org
- Configuring DDNS on Your WiMAX Device
- Testing the DDNS Setting

Note: If you have a private WAN IP address (see Private IP Addresses on page 250), then you cannot use DDNS.

4.8.1 Registering a DDNS Account on www.dyndns.org

1 Open a browser and type **http://www.dyndns.org**.

2 Apply for a user account. This tutorial uses **UserName1** and **12345** as the username and password.

3 Log into www.dyndns.org using your account.

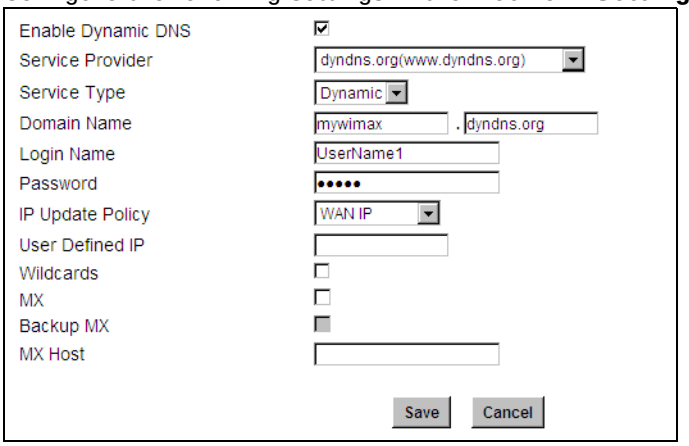
4 Add a new DDNS host name. This tutorial uses the following settings as an example.

- Hostname: **mywimax.dyndns.org**
- Service Type: **Host with IP address**
- IP Address: Enter the WAN IP address that your WiMAX Device is currently using. You can find the IP address on the WiMAX Device's Web Configurator **Status** page.

Then you will need to configure the same account and host name on the WiMAX Device later.

4.8.2 Configuring DDNS on Your WiMAX Device

Configure the following settings in the **Network Setting** > **DDNS** screen.



1 Select **Enable Dynamic DNS**.

2 Select **dyndns.org** for the service provider.

3 Select **Dynamic** for the service type.

4 Type **mywimax.dyndns.org** in the **Domain Name** field.

5 Enter the user name (**UserName1**) and password (**12345**).

6 Select **WAN IP** for the IP update policy.

7 Click **Save**.

4.8.3 Testing the DDNS Setting

Now you should be able to access the WiMAX Device from the Internet. To test this:

1 Open a web browser on the computer (using the IP address **a.b.c.d**) that is connected to the Internet.

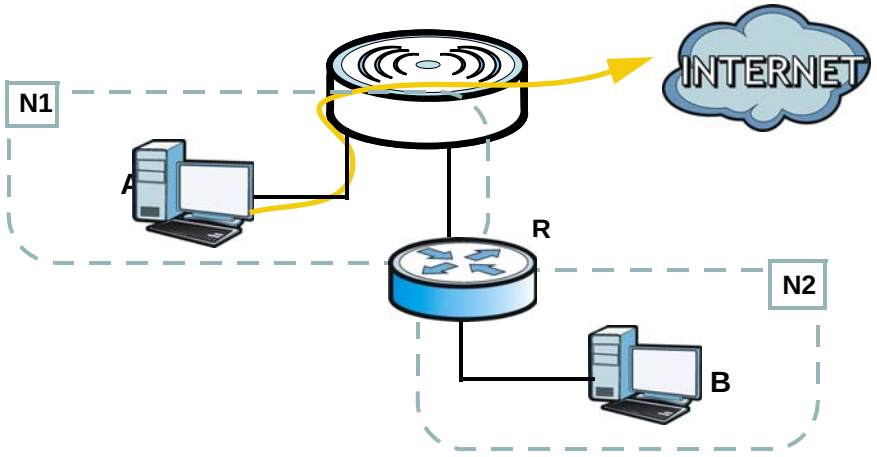
2 Type **http://mywimax.dyndns.org** and press [Enter].

3 The WiMAX Device's login page should appear. You can then log into the WiMAX Device and manage it.

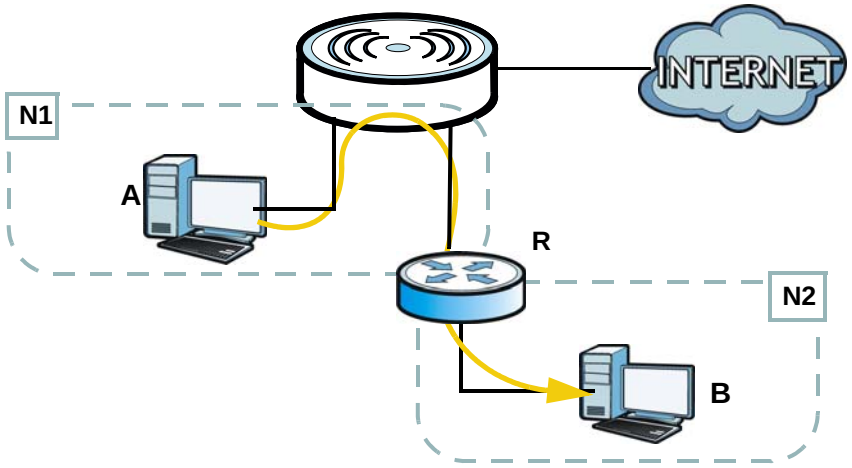
4.9 Configuring Static Route for Routing to Another Network

In order to extend your Intranet and control traffic flowing directions, you may connect a router to the WiMAX Device's LAN. The router may be used to separate two department networks. This tutorial shows how to configure a static routing rule for two network routings.

In the following figure, router **R** is connected to the WiMAX Device's LAN. **R** connects to two networks, **N1** (192.168.1.x/24) and **N2** (192.168.10.x/24). If you want to send traffic from computer **A** (in **N1** network) to computer **B** (in **N2** network), the traffic is sent to the WiMAX Device's WAN default gateway by default. In this case, computer **B** will never receive the traffic.



You need to specify a static routing rule on the WiMAX Device to specify **R** as the router in charge of forwarding traffic to **N2**. In this case, the WiMAX Device routes traffic from computer **A** to **R** and then **R** routes the traffic to computer **B**.



This tutorial uses the following example IP settings:

Table 10 IP Settings in this Tutorial

DEVICE / COMPUTER	IP ADDRESS
The WiMAX Device's WAN	172.16.1.1
The WiMAX Device's LAN	192.168.1.1
A	192.168.1.34
R's IP address on N1	192.168.1.253

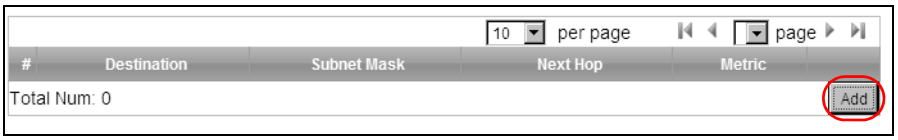
Table 10 IP Settings in this Tutorial

DEVICE / COMPUTER	IP ADDRESS
R's IP address on N2	192.168.10.2
B	192.168.10.33

To configure a static route to route traffic from **N1** to **N2**:

1 Click **Network Setting** > **Route** > **Static Route**.

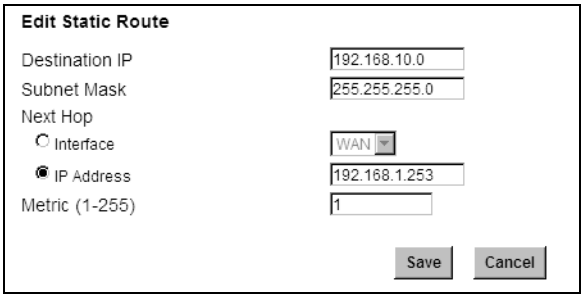
2 Click **Add** to create a new route.



3 Configure the **Edit Static Route** screen using the following settings:

3a Enter **192.168.10.0** and subnet mask **255.255.255.0** for the destination, **N2**.

3b Enter **192.168.1.253** (**R**'s IP address on N1) in the **IP Address** field under **Next Hop**.



3a Click **Save**.

Now computer **B** should be able to receive traffic from computer **A**. You may need to additionally configure **R**'s firewall settings to accept specific traffic to pass through.

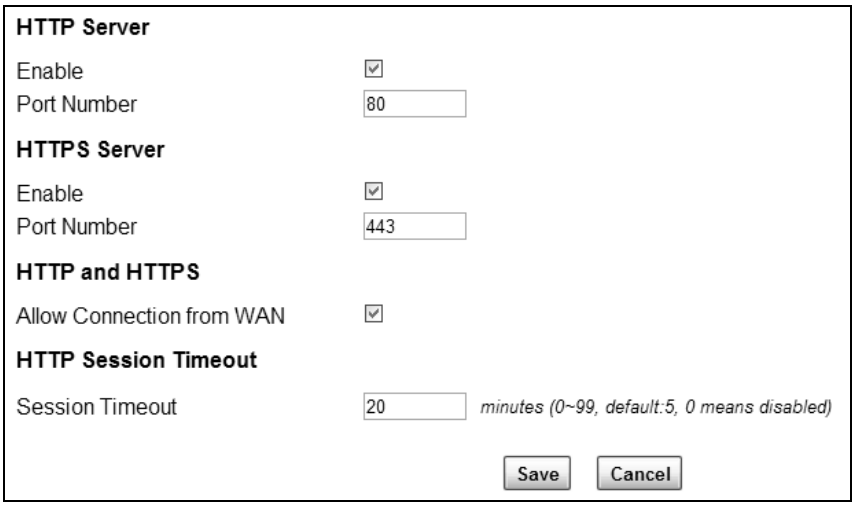
4.10 Remotely Managing Your WiMAX Device

The remote management feature allows you to log into the device through the Internet.

Goal: Set up the WiMAX Device to allow management requests from the WAN (Internet).

See Also: Section 7.20 on page 119.

1 Open the **Maintenance > Remote MGMT > HTTP** screen.



2 Select **Enable** in both **HTTP Server** and **HTTPS Server** sections and leave the **Port Number** settings as “80” and “443”.

3 Select **Allow Connection from WAN**. This allows remote management connections not only from the local network but also the WAN network (Internet).

4 Click **Save**.

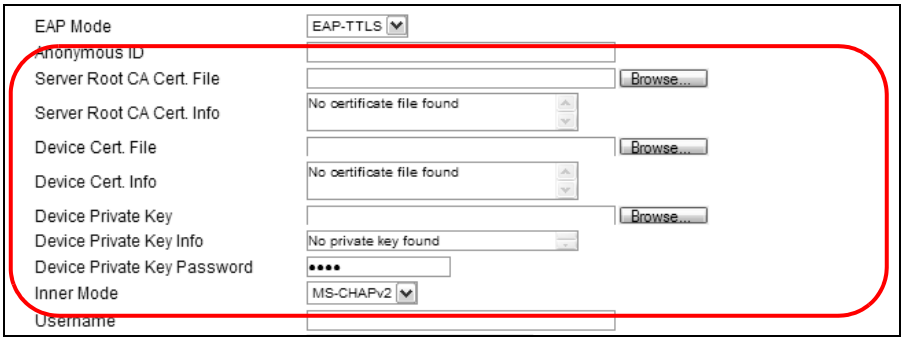
4.11 Changing Certificate to Communicate with Other Networks

This tutorial shows you how to import a new security certificate, which allows your device to communicate with other network servers.

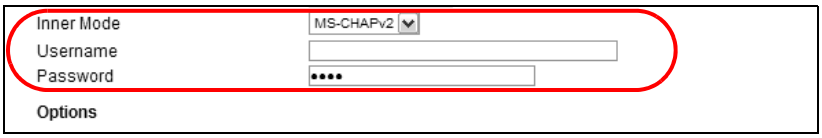
Goal: Import a new security certificate into the WiMAX Device.

See Also: Appendix B on page 211.

1 Go to the **WiMAX > Profile > Authentication Settings** screen. In the **EAP Supplicant** section, click each **Browse** button and locate the security certificates that were provided by your new ISP.

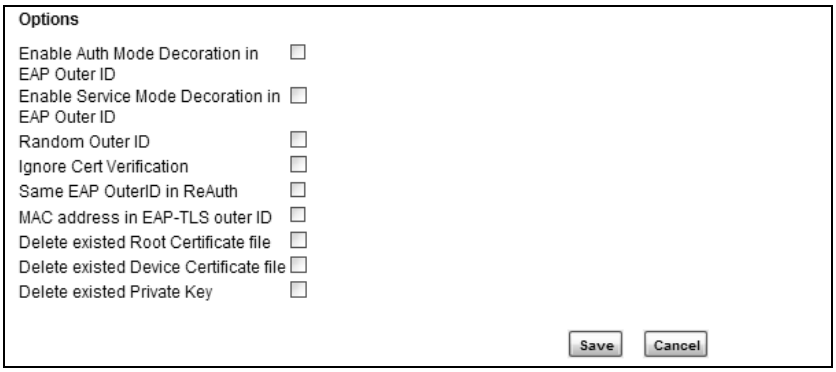


2 Configure your new Internet access settings based on the information provided by the ISP.



Note: You can also use the Internet Connection Wizard to configure the Internet access settings.

3 You may need to configure the **Options** section according to the information provided by the ISP.



4 Click **Save**. You should now be able to connect to the Internet through your new service provider!

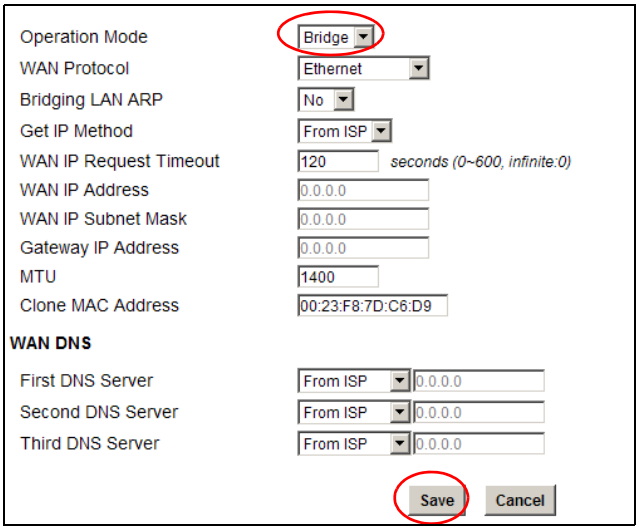
4.12 Using Virtual Networks

This section shows VLAN configuration scenarios.

See Section 7.20 on page 119 if you need more information about VLAN.

Before enabling VLANs you will need to change the WiMAX Device to bridge mode.

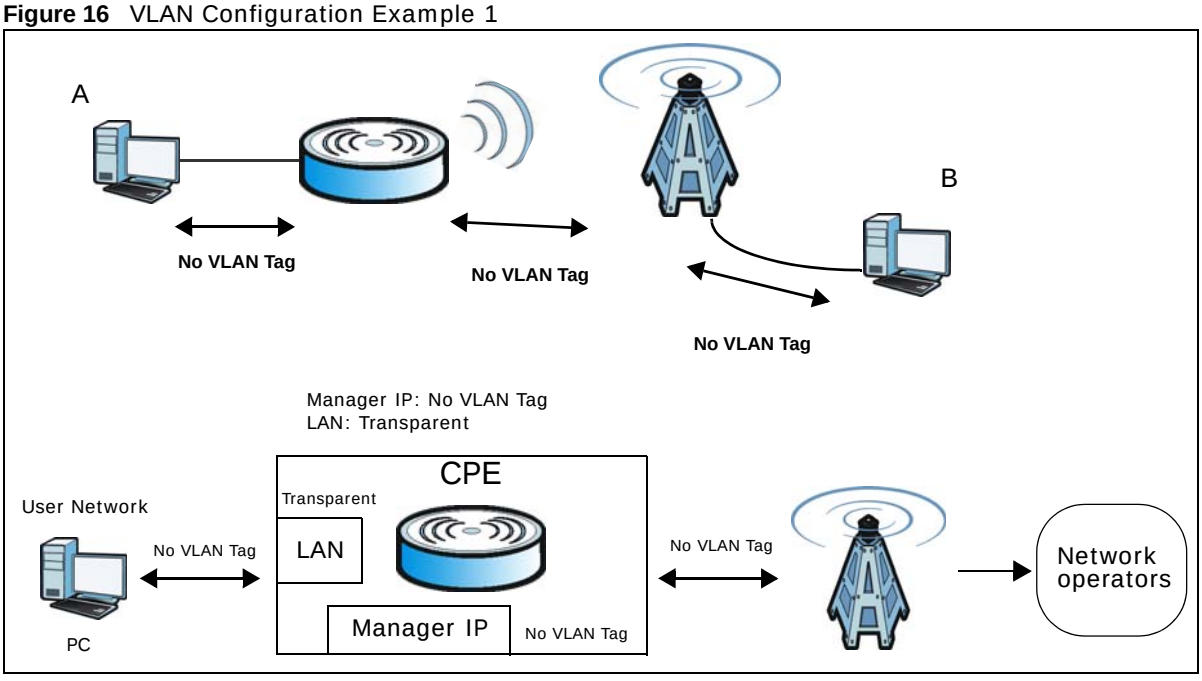
Click **Network Setting** > **WAN**. Change the WiMAX Device to bridge mode and then click **Save**. If you cannot obtain IP address settings from a WAN DHCP server, select **User** as the **Get IP Method** and enter the **WAN IP Address**, **WAN IP Subnet Mask** and **Gateway IP Address**.



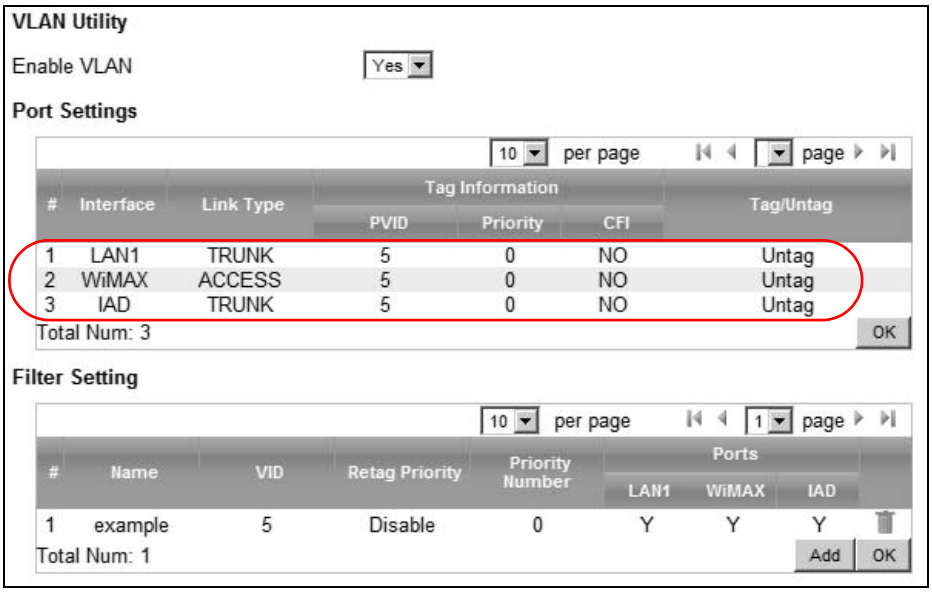
4.12.1 Scenario 1

In this scenario, PC A is connected directly to interface LAN1 on the WiMAX Device. PC B is connected to interface WiMAX and interface IAD for managing the WiMAX Device.

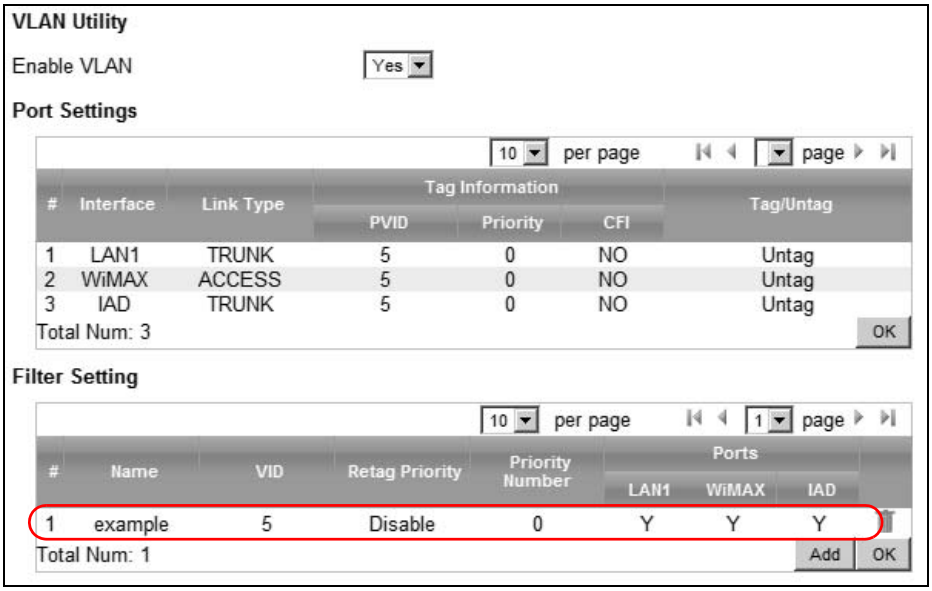
Figure 16 VLAN Configuration Example 1



1 Configure the **Link Type**, **PVID** and **Tag/Untag** settings for the interfaces as below by clicking each row. Then press **OK**.



2 Next, configure the **Name**, **VID** and **Ports** for the **Filter Setting**. The WiMAX Device will tag packets it receives on each interface so that they are recognized in VLAN 5. Tagged packets will be untagged when they are forwarded out of each interface since the devices attached to these interfaces do not support VLAN tagged packets.

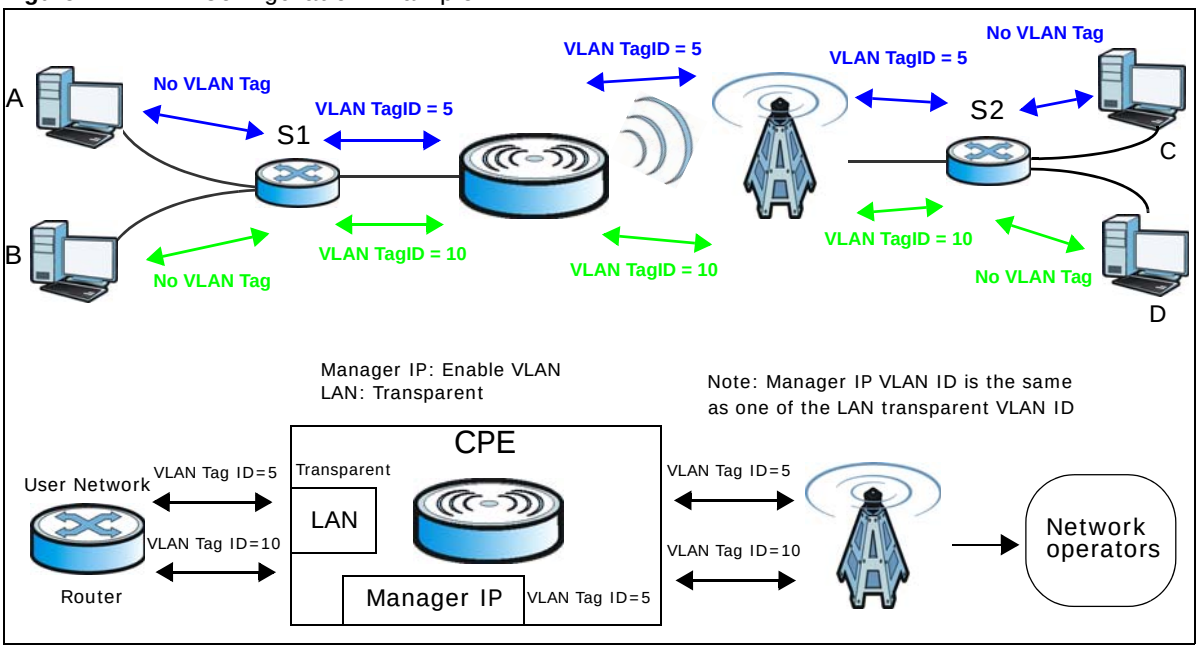


4.12.2 Scenario 2

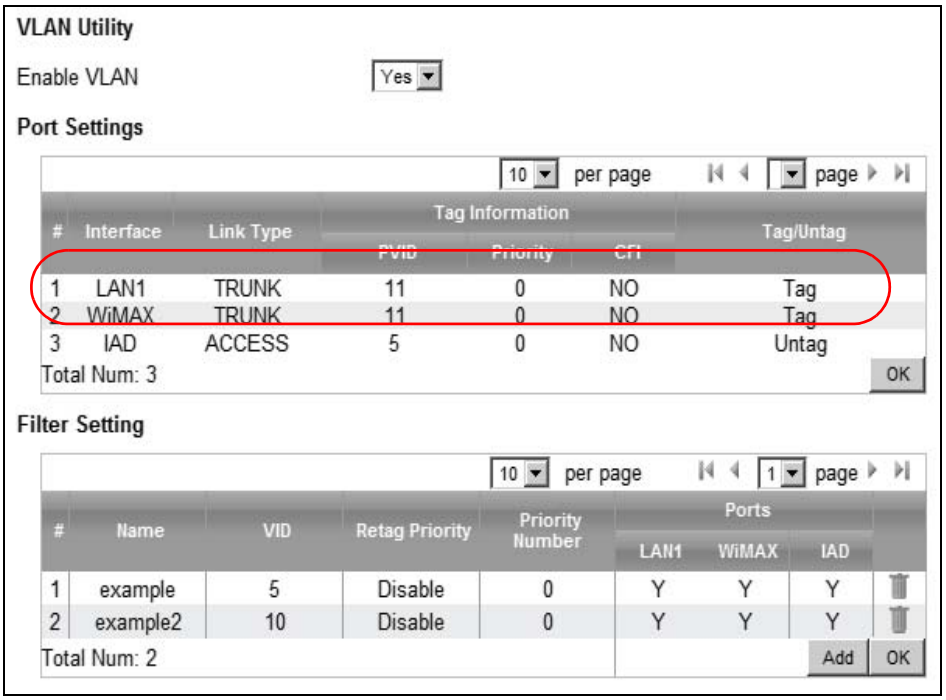
In this scenario, PC A and PC C are on VLAN 5, while PC B and PC D are on VLAN 10. PC A and PC B are connected to interface LAN1 through VLAN supporting switch S1. PC C is connected to interface WiMAX and interface IAD for managing the WiMAX Device, through VLAN supporting switch S2. PC D is connected to interface WiMAX through VLAN supporting switch S2.

Note: You will need to configure the VLAN supporting switches to tag the received packets with the appropriate VLAN IDs. For example, packets received on switch S1 from PC A on the LAN would be tagged to VLAN 5.

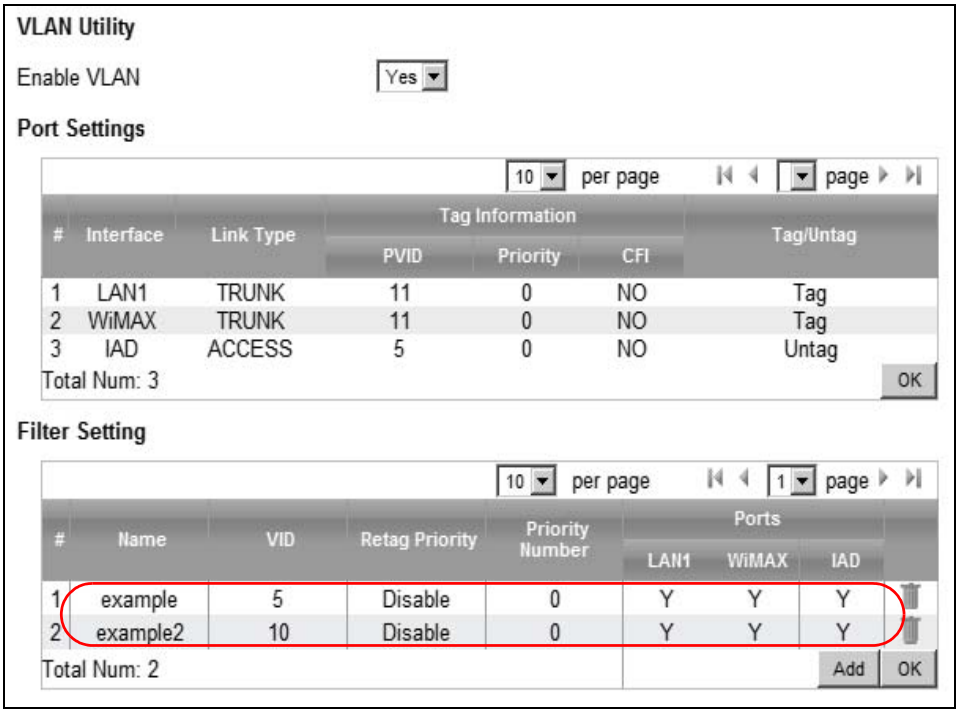
Figure 17 VLAN Configuration Example 2



1 Configure the **Link Type**, **PVID** and **Tag/Untag** settings for the interfaces as below by clicking each row. Then press **OK**.



2 Next, configure the **Name**, **VID** and **Ports** for the **Filter Setting**. Interfaces **LAN1** and **WiMAX** are Trunk links, so the WiMAX Device will recognize VLAN 5 and VLAN 10 tagged packets it receives on these interfaces from the VLAN supporting switches. VLAN tagged packets will also be forwarded out of these interfaces. Interface **IAD** is configured as an Access port, so tagged packets will be untagged when they are forwarded.

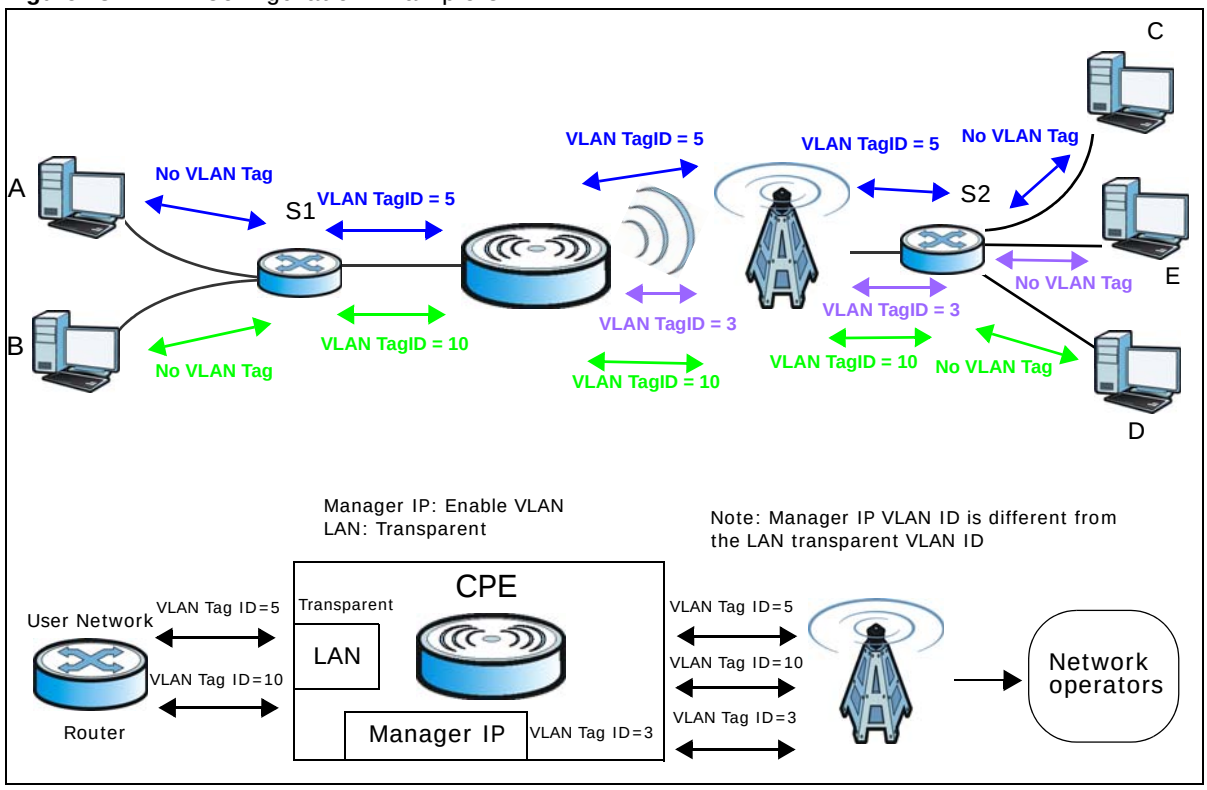


4.12.3 Scenario 3

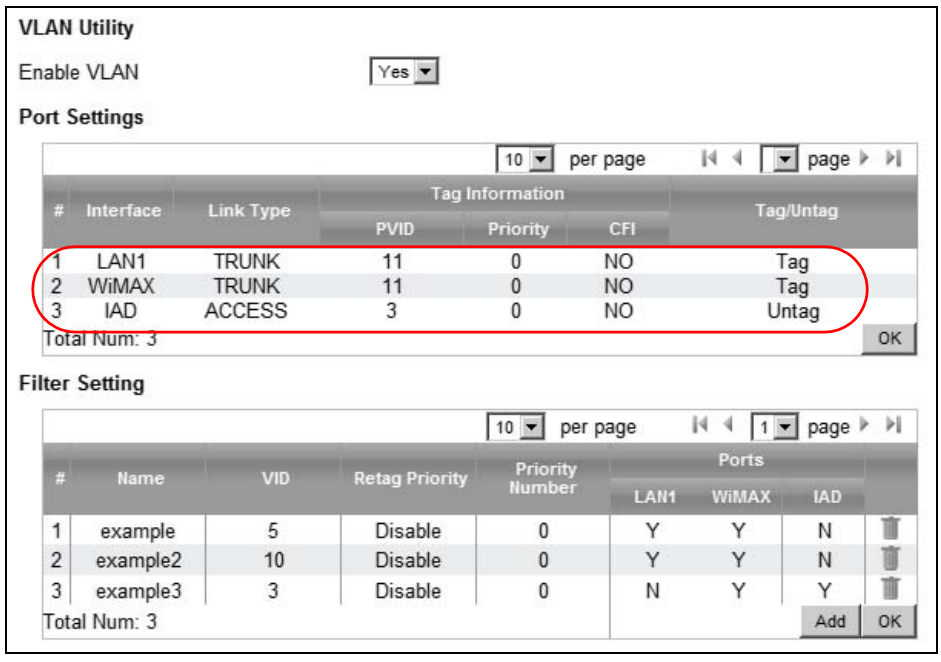
In this scenario, PC A and PC C are on VLAN 5, PC B and PC D are on VLAN 10, and PC E is on VLAN 3. PC A and PC B are connected to interface LAN1 through VLAN supporting switch S1. PC C and PC D are connected to interface WiMAX through VLAN supporting switch S2. PC E is connected to interface IAD through VLAN supporting switch S2 for managing the WiMAX Device.

Note: You will need to configure the VLAN supporting switches to tag the received packets with the appropriate VLAN IDs. For example, packets received on switch S1 from PC A on the LAN would be tagged to VLAN 5.

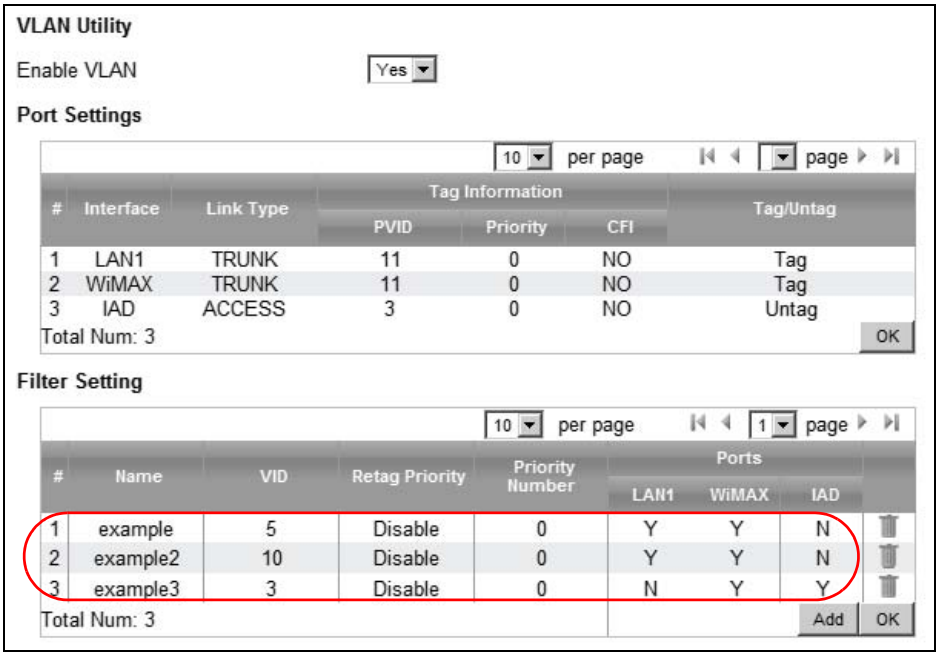
Figure 18 VLAN Configuration Example 3



1 Configure the **Link Type**, **PVID** and **Tag/Untag** settings for the interfaces as below by clicking each row. Then press **OK**.



2 Next, configure the **Name**, **VID** and **Ports** for the **Filter Setting**. Interfaces **LAN1** and **WiMAX** are Trunk links, so the WiMAX Device will recognize VLAN 5 and VLAN 10 tagged packets it receives on these interfaces from the VLAN supporting switches. VLAN tagged packets will also be forwarded out of these interfaces. Interface **IAD** is configured as an Access port, so tagged packets will be untagged when they are forwarded.

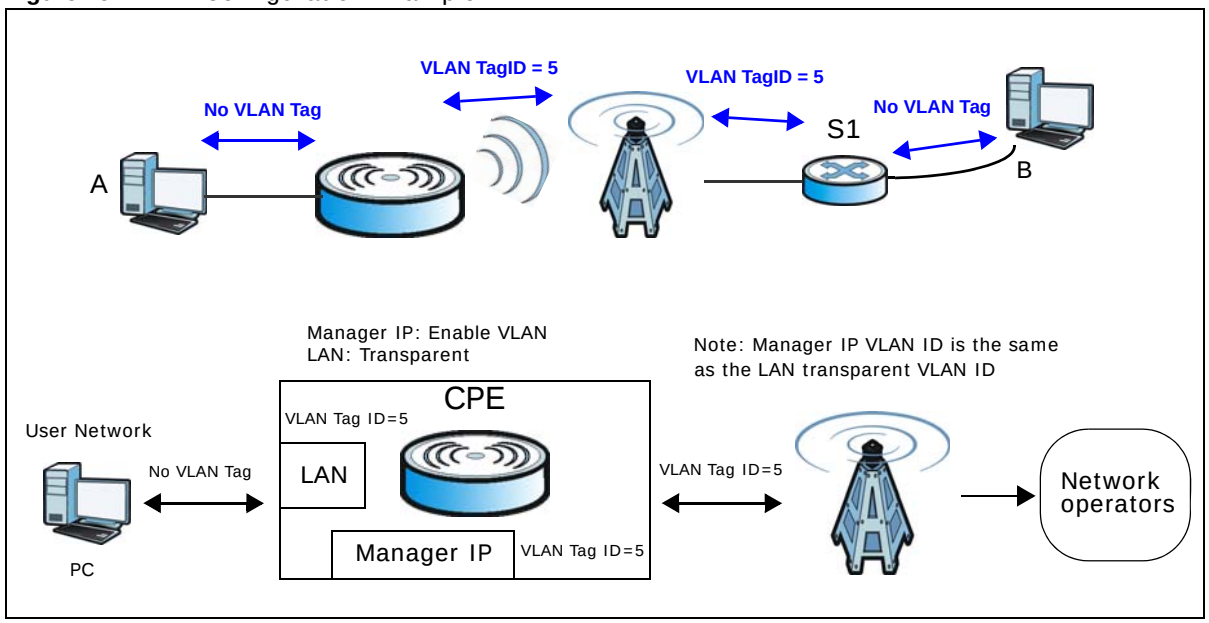


4.12.4 Scenario 4

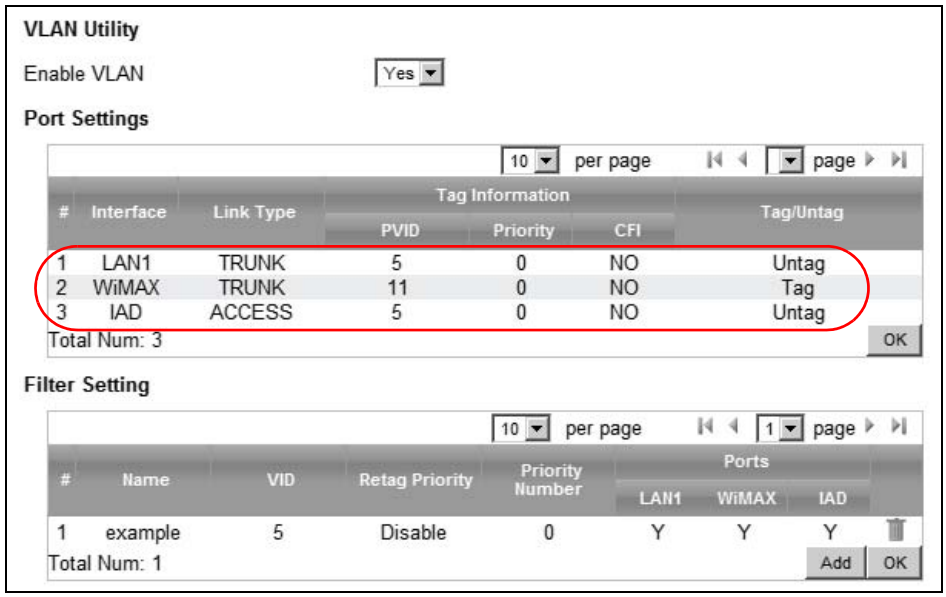
In this scenario, PC A is connected directly to interface LAN1 on the WiMAX Device, while PC B is on VLAN 5. PC B is connected to interface WiMAX and interface IAD for managing the WiMAX Device, through VLAN supporting switch S1.

Note: You will need to configure the VLAN supporting switches to tag the received packets with the appropriate VLAN IDs. For example, packets received on switch S1 from PC B on the LAN would be tagged to VLAN 5.

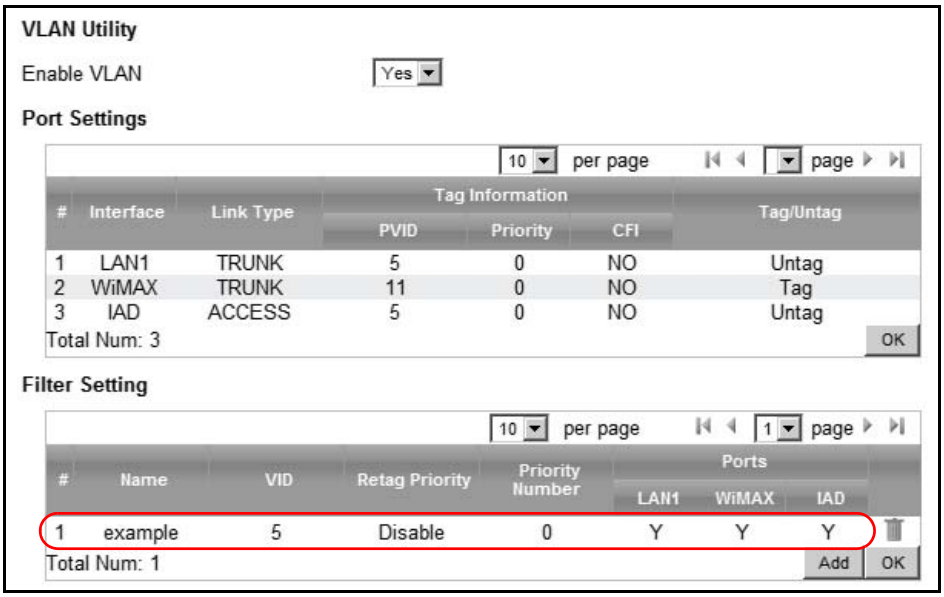
Figure 19 VLAN Configuration Example 4



1 Configure the **Link Type**, **PVID** and **Tag/Untag** settings for the interfaces as below by clicking each row. Then press **OK**.



2 Next, configure the **Name**, **VID** and **Ports** for the **Filter Setting**. Interfaces **LAN1** and **WiMAX** are Trunk links. On the WiMAX interface, the WiMAX Device will recognize VLAN 5 tagged packets it receives from the VLAN supporting switch. VLAN tagged packets will also be forwarded out of this interface. On the LAN1 interface, the WiMAX Device will tag packets it receives so that they are recognized in VLAN 5. On LAN1, tagged packets will be untagged when they are forwarded out since PC A does not support VLAN tagged packets. Interface **IAD** is configured as an Access port, so tagged packets will be untagged when they are forwarded.

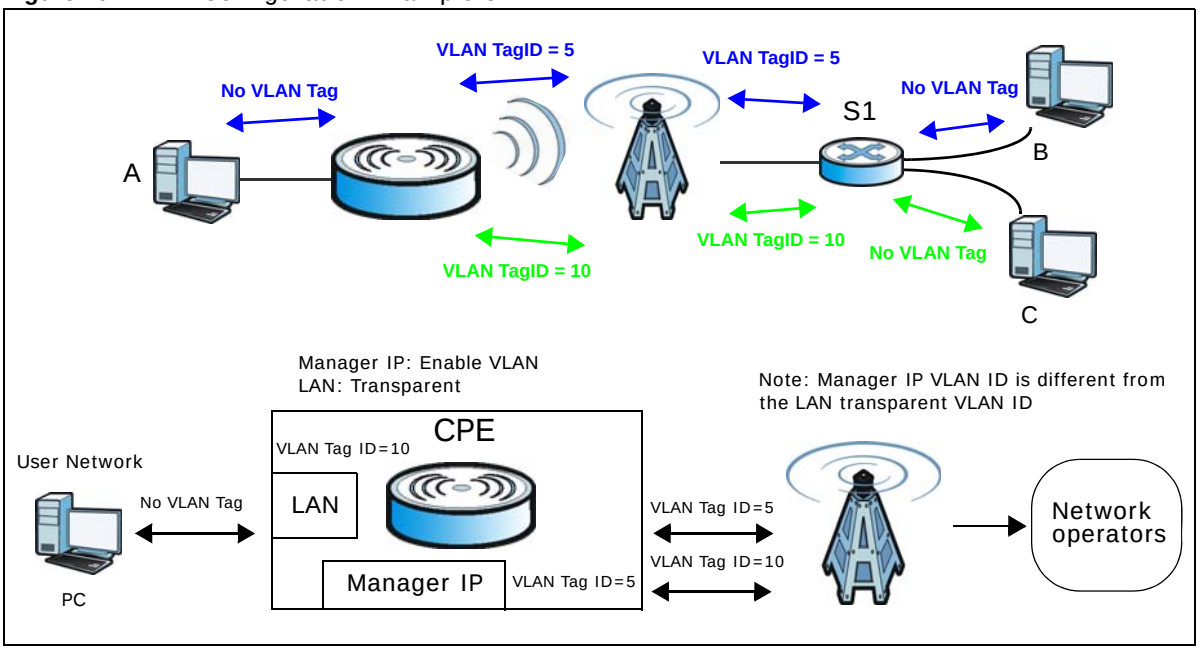


4.12.5 Scenario 5

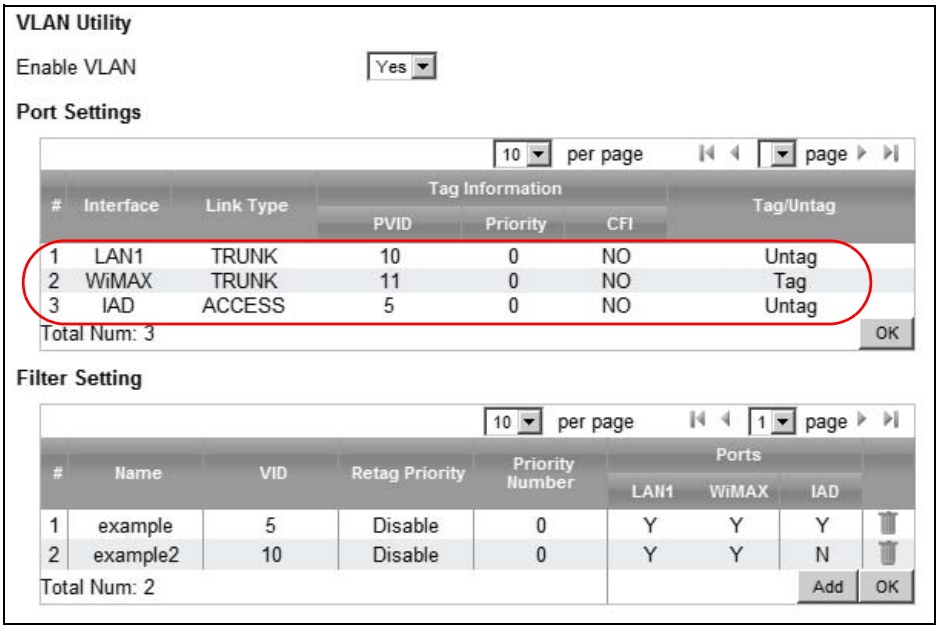
In this scenario, PC A is directly connected to interface LAN1 on the WiMAX Device. PC B is on VLAN 5 while PC C is on VLAN 10. PC B is connected to interface WiMAX and interface IAD for managing the WiMAX Device, through VLAN supporting switch S1. PC C is connected to interface WiMAX through VLAN supporting switch S1.

Note: You will need to configure the VLAN supporting switches to tag the received packets with the appropriate VLAN IDs. For example, packets received on switch S1 from PC C on the LAN would be tagged to VLAN 10.

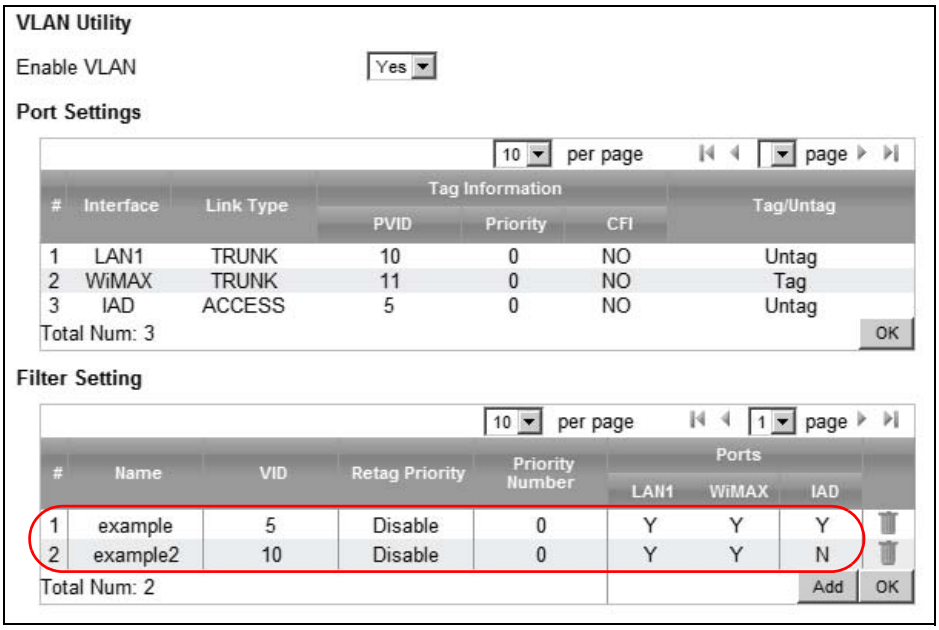
Figure 20 VLAN Configuration Example 5



1 Configure the **Link Type**, **PVID** and **Tag/Untag** settings for the interfaces as below by clicking each row. Then press **OK**.



2 Next, configure the **Name**, **VID** and **Ports** for the **Filter Setting**. Interfaces **LAN1** and **WiMAX** are Trunk links. On the WiMAX interface the WiMAX Device will recognize VLAN 5 and VLAN 10 tagged packets it receives from the VLAN supporting switch. VLAN tagged packets will also be forwarded out of these interfaces. On the LAN1 interface, the WiMAX Device will tag packets it receives so that they are recognized in VLAN 10. On LAN1, tagged packets will be untagged when they are forwarded out, since PC A does not support VLAN tagged packets. Interface **IAD** is configured as an Access port, so tagged packets will be untagged when they are forwarded.



PART II
Technical Reference

5

System Status

5.1 Overview

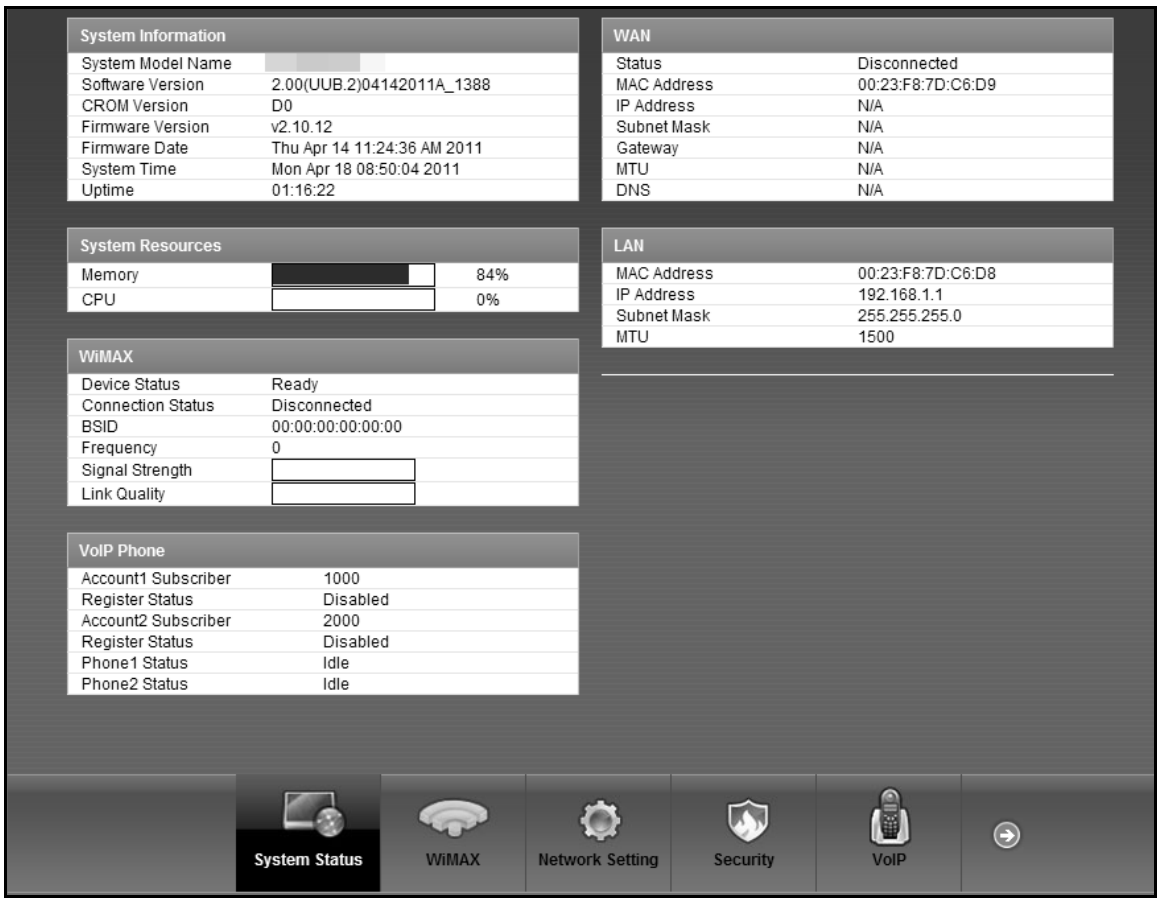
Use this screen to view a summary of your WiMAX Device connection status.

5.2 System Status

This screen allows you to view the current status of the device, system resources, and interfaces (LAN and WAN).

Click **System Status** to open this screen as shown next.

Figure 21 System Status



The following tables describe the labels in this screen.

Table 11 Status

LABEL	DESCRIPTION
System Information	
System Model Name	This field displays the WiMAX Device system model name. It is used for identification.
Software Version	This field displays the Web Configurator version number.
CROM Version	This field displays the CROM version number.
Firmware Version	This field displays the current version of the firmware inside the device.
Firmware Date	This field shows the date the firmware version was created.
System Time	This field displays the current system time.
Uptime	This field displays how long the WiMAX Device has been running since it last started up.
System Resources	
Memory	This field displays what percentage of the WiMAX Device's memory is currently used. The higher the memory usage, the more likely the WiMAX Device is to slow down. Some memory is required just to start the WiMAX Device and to run the web configurator. You can reduce the memory usage by disabling some services; 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.
CPU	This field displays what percentage of the WiMAX Device's CPU is currently used. The higher the CPU usage, the more likely the WiMAX Device is to slow down.
WiMAX	
Device Status	This field displays the WiMAX Device current status for connecting to the selected base station. • **Scanning** - The WiMAX Device is scanning for available base stations. • **Ready** - The WiMAX Device has finished a scanning and you can connect to a base station. • **Connecting** - The WiMAX Device attempts to connect to the selected base station. • **Connected** - The WiMAX Device has successfully connected to the selected base station.
Connection Status	This field displays the status of the WiMAX connection between the WiMAX Device and the base station. • **Network Search** - The WiMAX Device is scanning for any available WiMAX connections. • **Disconnected** - No WiMAX connection is available. • **Network Entry** - A WiMAX connection is initializing. • **Normal** - The WiMAX connection has successfully established.
BSID	This field displays the MAC address of the base station to which the device is connected.
Frequency	This field indicates the frequency the WiMAX Device is using.
Signal Strength	This field indicates the strength of the connection that the WiMAX Device has with the base station.
Link Quality	This field indicates the relative quality of the link the WiMAX Device has with the base station.
WAN	

Table 11 Status (continued)

LABEL	DESCRIPTION
Status	This field indicates the status of the WAN connection to the WiMAX Device.
MAC Address	This field indicates the MAC address of the port making the WAN connection on the WiMAX Device.
IP Address	This field indicates the current IP address of the WiMAX Device in the WAN.
Subnet Mask	This field indicates the current subnet mask on the WAN.
Gateway	This field indicates the IP address of the gateway to which the WiMAX Device is connected.
MTU	This field indicates the Maximum Transmission Unit (MTU) between the WiMAX Device and the ISP servers to which it is connected.
DNS	This field indicates the Domain Name Server (DNS) to which your WiMAX Device is connected.
LAN	
MAC Address	This field indicates the MAC address of the port making the LAN connection on the WiMAX Device.
IP Address	This field displays the current IP address of the WiMAX Device in the LAN.
Subnet Mask	This field displays the current subnet mask in the LAN.
MTU	This field indicates the Maximum Transmission Unit (MTU) between the WiMAX Device and the client devices to which it is connected.
VOIP Phone	
Account1/2 Subscriber	This field displays the SIP number for the SIP account. If your WiMAX Device has only one phone port, there is only one account.
Registered Status	This field displays whether the SIP account is already registered with a SIP server (**Up** or **Disabled**).
Phone1/2 Status	This field displays whether the phone line (mapping to the **VoIP** port) is in use or not (idle). If your WiMAX Device has only one phone port, there is only one phone line.

6

WiMAX

6.1 Overview

This chapter shows you how to set up and manage the connection between the WiMAX Device and your ISP's base stations.

6.1.1 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 22 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 23 WiMAX: Multiple Mobile Stations

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

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

Authentication

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

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

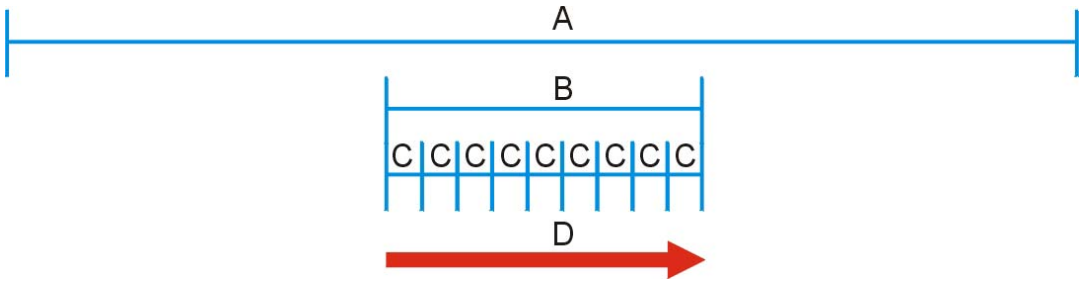
Figure 24 Using an AAA Server

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.

Frequency Ranges

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

Figure 25 Frequency Ranges



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

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

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

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

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

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

Certification Authority

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. You can use the WiMAX Device to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

Certificate File Formats

The certification authority 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. The WiMAX Device currently allows the importation of a PKS#7 file that contains a single certificate.

- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses 64 ASCII characters to convert a binary PKCS#7 certificate into a printable form.

CINR

Carrier to Interference-plus-Noise Ratio (CINR) measures the effectiveness of a wireless signal and plays an important role in allowing the WiMAX Device to decode signal burst. If a burst has a high signal strength and a high interference-plus-noise ratio, it can use Digital Signal Processing (DSP) to decode it; if the signal strength is lower, it can switch to an alternate burst profile.

RSSI

Received Signal Strength Indicator (RSSI) measures the relative strength of a given wireless signal. This is important in determining if a signal is below the Clear-To-Send (CTS) threshold. If it is below the arbitrarily specified threshold, then WiMAX Device is free to transmit any data packets.

EAP Authentication

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

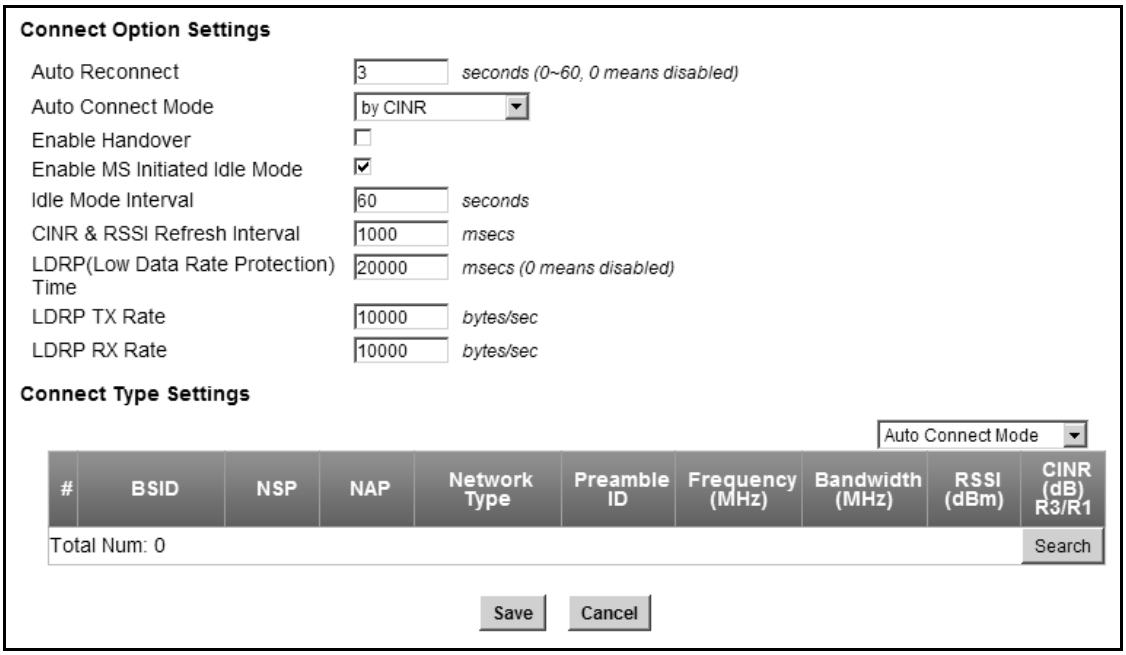
The WiMAX Device supports EAP-TLS and EAP-TTLS (at the time of writing, TTLS is not available in Windows Vista). For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). Certificates (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

6.2 Connection Settings

This screen allows you to configure how the WiMAX Device connects to the base stations on the WiMAX network.

Click **WiMAX > Profile > Connection Settings** to open this screen as shown next.

Figure 26 Connection Settings Screen



This screen contains the following fields:

Table 12 Connection Settings

LABEL	DESCRIPTION
Connection Option Settings	
Auto Reconnect	Select the interval in seconds that the WiMAX Device waits after getting disconnected from the base station before attempting to reconnect.
Auto Connect Mode	Select the auto connect mode. • **By channel power** - Auto connects to the base station if the signal strength of the channel is sufficient for the WiMAX Device. • **By CINR** - Auto connects to the base station if the signal-to-noise ratio is sufficient for the WiMAX Device.
Enable Handover	Select this to maintain connectivity while the WiMAX Device switches its connection from one base station to another base station.
Enable MS Initiated Idle Mode	Select this to have the WiMAX Device enter the idle mode after it has no traffic passing through for a pre-defined period. Make sure your base station also supports this before selecting this.
Idle Mode Interval	Set the idle duration in minutes. This is how long the WiMAX Device waits during periods of no activity before going into idle mode.
CINR & RSSI Refresh Interval	Set the refresh interval in milliseconds for calculating the signal-to-noise measurement (CINR) and signal strength measurement (RSSI) of the WiMAX Device.
LDRP (Low Data Rate Protection)	Enter the Low Data Rate Protection (LDRP) time in milliseconds. If the uplink/ downlink data rate is smaller than the LDRP time, the WiMAX Device sends a disconnect request to the base station.
LDRP TX Rate	Enter the outgoing data rates for LDRP in bytes per second.
LDRP RX Rate	Enter the incoming data rates for LDRP in bytes per second.
Connection Type Settings	

Table 12 Connection Settings (continued)

LABEL	DESCRIPTION
Mode Select	Select how the WiMAX Device connects to the base station. • **Auto Connect Mode** - The device connects automatically to the first base station in range. • **Network Search Mode** - The device scans for available base stations then connects to the best one it can. • **NSP Mode** - This allows the WiMAX Device to connect to a base station with a user-specified NSP ID. To specify the NSP ID, select a result in the list and click **Connect**. The WiMAX Device will automatically connect to a base station with the same NSP ID, and the best CINR or RSSI. • **NSP/NAP Mode** - This allows the WiMAX Device to connect to a base station with a user-specified NSP ID and NAP ID. To specify the NSP ID and NAP ID, select a result in the list and click **Connect**. The WiMAX Device will automatically connect to a base station with the same NSP ID and NAP ID, and the best CINR or RSSI. • **NSP/NAP/BSID Mode** - This allows the WiMAX Device to connect to a base station with a user-specified NSP ID, NAP ID and BSID. To specify the NSP ID, NAP ID and BSID, select a result in the list and click **Connect**. The WiMAX Device will automatically connect to a base station with the same NSP ID, NAP ID and BSID, and the best CINR or RSSI.
BSID	This displays the MAC address of a base station within range of the WiMAX Device.
NSP	This field displays the NSP ID.
NAP	This field displays the NAP ID.
Preamble ID	The preamble ID is the index identifier in the header of the base station's broadcast messages. In the beginning of a mobile stations's network entry process, it searches for the preamble and uses it to additional channel information. The preamble ID is used to synchronize the upstream and downstream transmission timing with the base station.
Frequency (MHz)	This field displays the radio frequency of the WiMAX Device's connection to the base station.
Bandwidth (MHz)	This field displays the bandwidth of the base station in megahertz (MHz).
RSSI (dBm)	This field displays the Received Signal Strength Indication (RSSI), which is an overall measurement of radio signal strength. A higher RSSI level indicates a stronger signal.
CINR (dB) R3/R1	This field displays the average Carrier to Interference plus Noise Ratio for the current connection. This value is an indication of overall radio signal quality, where a higher value means a better quality signal.
Search	Click this to have the WiMAX Device scan for base stations.

6.3 Frequency Settings

Use this screen to have the WiMAX Device to scan one or more specific radio frequencies (given by your WiMAX service provider) to find available connections to base stations.

Note: The frequency band varies for different models. See Section 1.1 on page 17 for more information.

Click **WiMAX > Profile > Frequency Settings** to open this screen as shown next.

Figure 27 Frequency Settings Screen (By List)

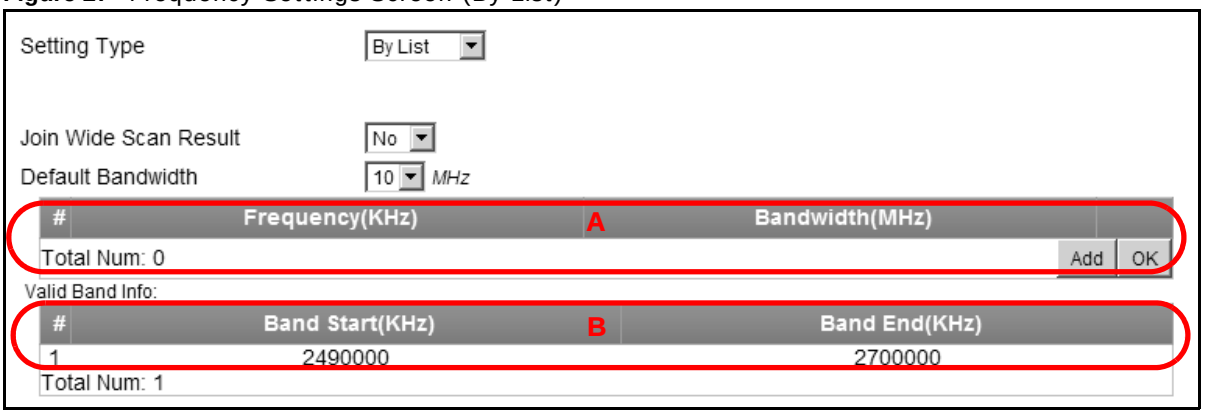
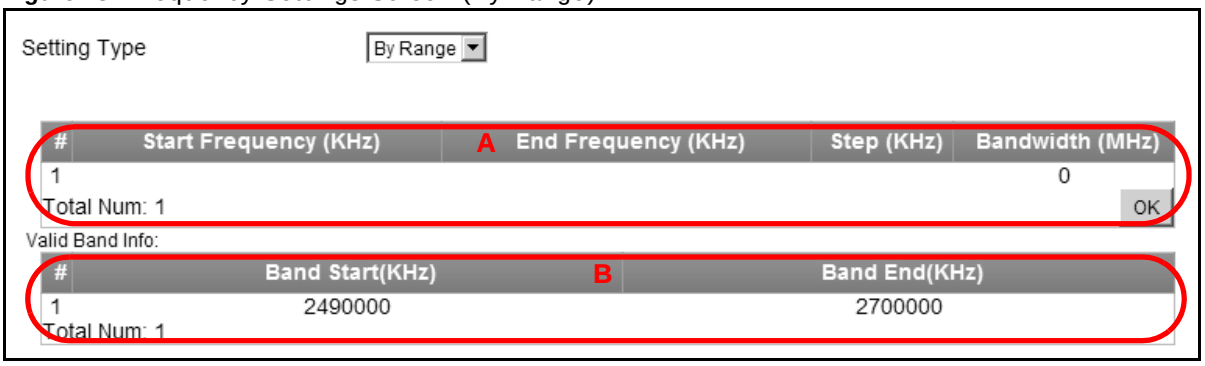


Figure 28 Frequency Settings Screen (By Range)



This screen contains the following fields:

Table 13 Frequency Settings

LABEL	DESCRIPTION
Setting Type	Select whether to scan base stations by entering specific frequency(-ies) (**By List**) or a range of frequencies (**By Range**). Note: When you select **By Range**, you can only configure one range of frequencies in this screen. To configure multiple frequency ranges, use the **WiMAX > Wide Scan** screen. Note: Some settings in this screen are only available depending on the **Setting Type** selected.
Join Wide Scan Result	The scanning result of the frequency to scan you configured in this screen will be shown in the **WiMAX > Connect** screen. Select this option to determine whether to also append the wide scanning result (configured in the **WiMAX > Wide Scan** screen) to the same table.
Default Bandwidth	Select the default bandwidth (size) per frequency band you specify in table **A**.
A (When **By List** is selected in the **Setting Type** field)	
Frequency (KHz)	This displays the center frequency of an frequency band in kilohertz (KHz). Click the number to modify it. Enter the center frequency in this field when you are adding an entry.

Table 13 Frequency Settings (continued)

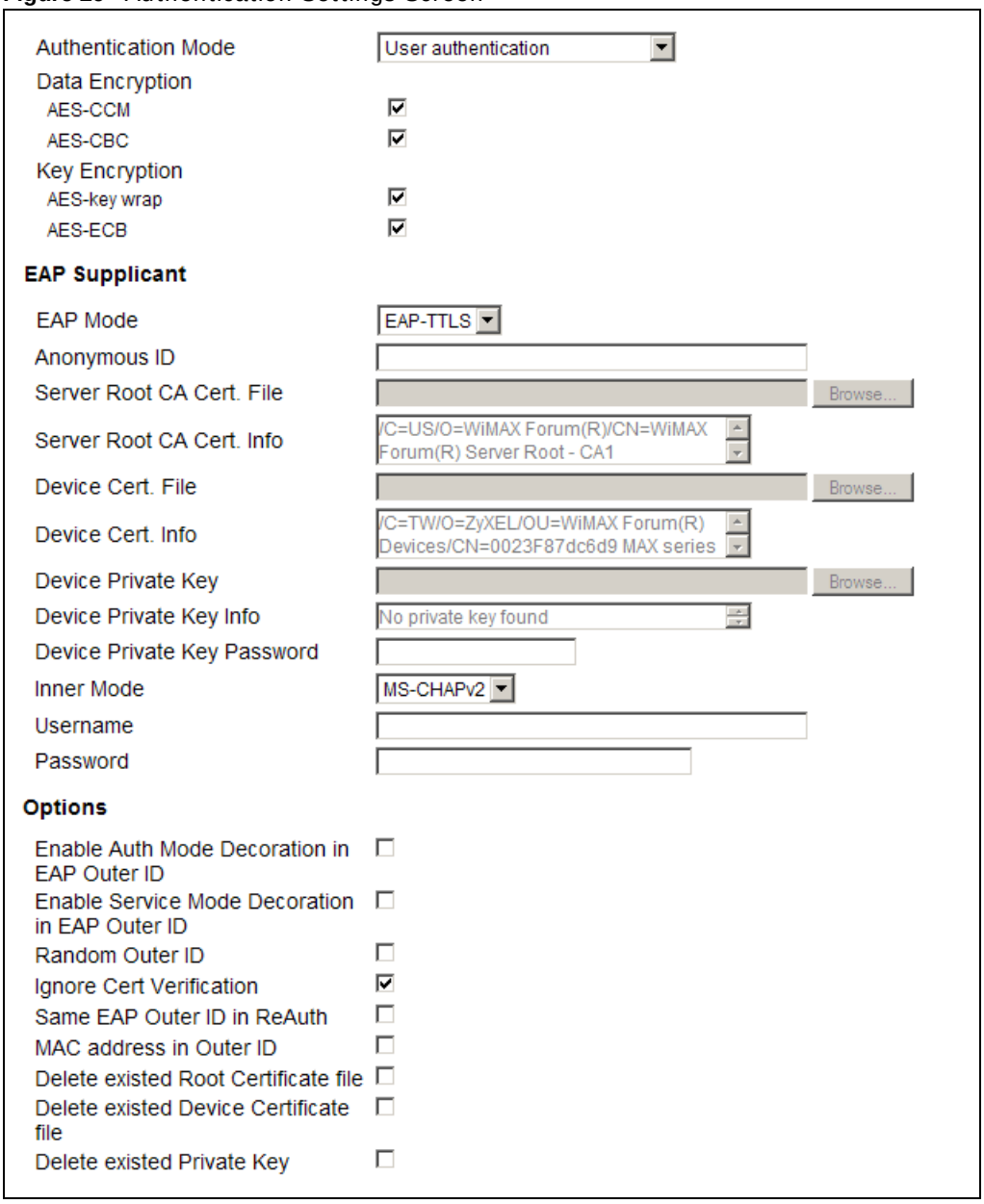
LABEL	DESCRIPTION
Bandwidth (MHz)	This displays the bandwidth of the frequency band in megahertz (MHz). If you set a center frequency to 2600000 KHz with the bandwidth of 10 MHz, then the frequency band is from 2595000 to 2605000 KHz. Click the number to modify it. Enter the bandwidth of the frequency band in this field when you are adding an entry.
Delete	Click this button to remove an item from the list.
Add	Click this button to add an item to the list.
OK	Click this button to save any changes made to the list.
A (When **By Range** is selected in the **Setting Type** field)	
Start Frequency (KHz)	This indicates the beginning of a frequency band in kilohertz (KHz). Click this field to modify it. Enter the beginning frequency when you are adding an entry.
End Frequency (KHz)	This indicates the end of the frequency band in kilohertz (KHz). Click this field to modify it.
Step (KHz)	This indicates the frequency step within each band in kilohertz (KHz). Click this field to modify it.
Bandwidth (MHz)	This indicates the bandwidth in megahertz (MHz). Click this field to modify it.
OK	Click this button to save any changes made to the list.
Valid Band Info (**B**) This table displays the entire frequency band the WiMAX Device supports. The frequenc(ies) to scan that you configured in table **A** must be within this range.	
Band Start (KHz)	This indicates the beginning of the frequency band in kilohertz (KHz).
Band End (KHz)	This indicates the end of the frequency band in kilohertz (KHz).

6.4 Authentication Settings

These settings allow the WiMAX Device to establish a secure (authenticated) connection with the service provider.

Click **WiMAX > Profile > Authentication Settings** to open this screen as shown next.

Figure 29 Authentication Settings Screen



This screen contains the following fields:

Table 14 Authentication Settings

LABEL	DESCRIPTION
Authentication Mode	Select the authentication mode from the list. The WiMAX Device supports the following authentication modes: • No authentication • User authentication • Device authentication • User and device authentication
Data Encryption	
AES-CCM	Select this to enable AES-CCM encryption. CCM combines counter-mode encryption with CBC-MAC authentication.
AES-CBC	Select this to enable AES-CBC encryption. CBC creates message authentication code from a block cipher.
Key Encryption	
AES-key wrap	Select this encapsulate cryptographic keys in a symmetric encryption algorithm.
AES-ECB	Select this to divide cryptographic keys into blocks and encrypt them separately.
EAP Supplicant	
EAP Mode	Select an Extensible Authentication Protocol (EAP) mode. The WiMAX Device supports the following: • **EAP-TLS** - In this protocol, digital certifications are needed by both the server and the wireless clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead. • **EAP-TTLS** - This protocol is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.
Anonymous ID	Enter the anonymous ID used for EAP supplicant authentication.
Server Root CA Cert File	Browse for and choose a server root certificate file, if required.
Server Root CA Info	This field displays information about the assigned server root certificate.
Device Cert File	Browse for and choose a device certificate file, if required. Before you import certificate from WebGUI, the certificate file must be signed by chipset vendor due to security reason.
Device Cert Info	This field displays information about the assigned device certificate.
Device Private Key	Browse for and choose a device private key, if required.
Device Private Key Info	This field displays information about the assigned device private key.
Device Private Key Password	Enter the device private key, if required.

Table 14 Authentication Settings (continued)

LABEL	DESCRIPTION
Inner Mode	Sets the EAP-TTLS inner mode. The WiMAX Device supports the following: • **MS-CHAP v2** - This is version 2 of Microsoft's variant of Challenge Handshake Authentication Protocol (CHAP). It allows for mutual authentication between devices. • **MS-CHAP** - This is Microsoft's variant of Challenge Handshake Authentication Protocol (CHAP). It allows for mutual authentication between devices. • **CHAP** - The Challenge Handshake Authentication Protocol (CHAP) uses PPP to authenticate remote devices using a three-way handshake and shared secret verification. • **MD5** - Message-Digest, algorithm 5, (MD5) encryption is typically used for checking file integrity. Because this encryption protocol contains a number of serious security flaws it is generally not recommended that you use it for authentication security. • **PAP** - Password Authentication Protocol uses unencrypted plaintext to send a passwords for authentication over the network. It's probably not a good idea to rely on this for security.
Username	Enter the username required for the EAP-TTLS inner method.
Password	Enter the password required for the EAP-TTLS inner method.
Options	
Enable Auth Mode Decoration in EAP Outer ID	Select this to enable authentication mode.
Enable Service Mode Decoration in EAP Outer ID	Select this to enable service mode.
Random Outer ID	Select this to allow the WiMAX Device to generate a 16-byte random number as a username for the EAP Identity Response message.
Ignore Cert Verification	Select this to ignore base station certification verification when a certificate is received during EAP-TLS or EAP-TTLS.
Same EAP OuterID in ReAuth	Select this to use the same EAP to the outer ID when reauthenticating.
MAC address in EAP-TLS outer Id	Adds the MAC address of the WiMAX Device to the outer ID while the EAP mode is set to EAP-TLS.
Delete existed Root Certificate file	Select this to delete an existing root certificate file from the WiMAX Device.
Delete existed Device Certificate file	Select this to delete an existing device certificate file from the WiMAX Device.
Delete existed Private Key	Select this to delete an existing private key from the WiMAX Device.

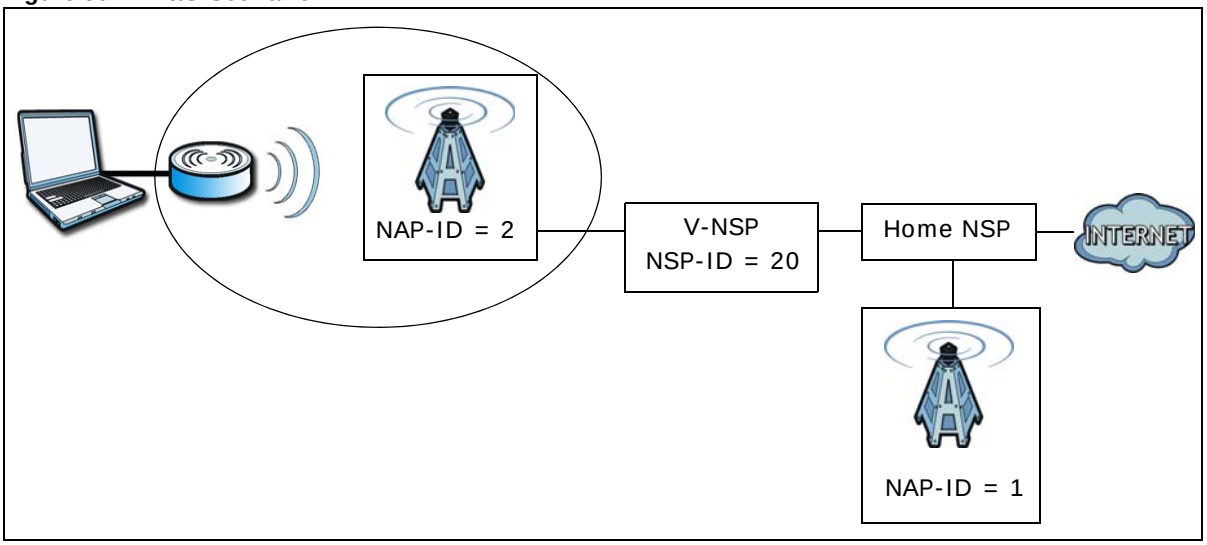
6.5 Channel Plan Settings

This screen allows you to specify channel plan settings for Network Discovery and Selection (ND&S). The WiMAX Device uses ND&S to establish connections when it is roaming. To do this, the WiMAX Device will scan for base stations that are operated by Network Access Providers (NAP) that have service agreements with the subscriber's service provider (Home-Network Service Provider or

Home NSP). Through the NAP's base station, which is identified by a NAP-ID, the subscriber's WiMAX Device can access the Internet through a network service provider (NSP). Access can be through another network service provider (Visited-Network Service Provider or V-NSP) or his own network service provider (Home NSP), depending on his service agreement.

In the following scenario, the subscriber's WiMAX Device cannot reach a base station owned by his Home NSP (base station with NAP-ID = 1). The WiMAX Device uses ND&S and is able to access another base station with NAP-ID = 2. This base station is associated with another service provider (V-NSP with NSP-ID = 20). The subscriber's service agreement specifies to route traffic from the other service provider to the Home NSP, so the Home NSP authenticates and authorizes the connection.

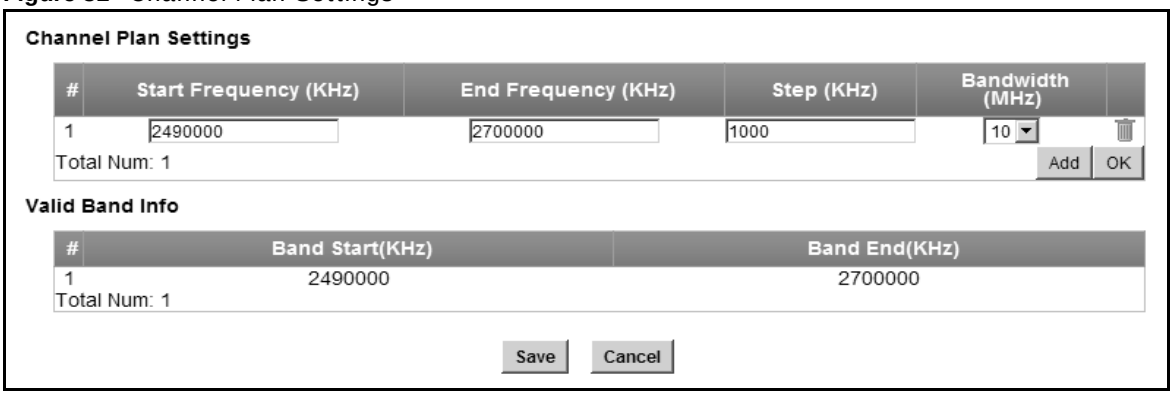
Figure 30 ND&S Scenario



The channel plan settings specify the allowed frequency range to search for a NAP. The channel plan is necessary to speed up the network discovery process.

Click **WiMAX > ND&S > Channel Plan Settings** to open this screen as shown next.

Figure 31 Channel Plan Settings



This screen contains the following fields:

Table 15 Channel Plan Settings

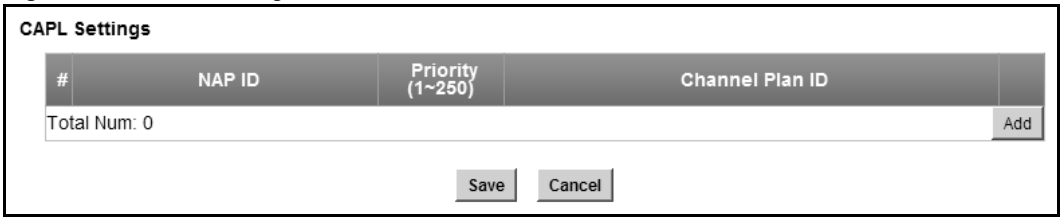
LABEL	DESCRIPTION
Channel Plan Settings - You can configure multiple ranges of frequencies to scan for different NAPs. The configured frequency ranges to scan must be within the Valid Band. Specify the Channel Plan to scan for each NAP on the CAPL Settings: Add screen (Section 6.6.1 on page 80).	
Start Frequency (KHz)	This indicates the beginning of a frequency band in kilohertz (KHz). Click this field to modify it. Enter the beginning frequency when you are adding an entry.
End Frequency (KHz)	This indicates the end of the frequency band in kilohertz (KHz). Click this field to modify it.
Step (KHz)	This indicates the frequency step within each band in kilohertz (KHz). Click this field to modify it. The minimum step is 250KHz and the maximum step is the difference between the start frequency and end frequency.
Bandwidth (MHz)	This indicates the bandwidth in megahertz (MHz). Click this field to modify it.
Delete	Click this button to remove an item from the list.
Add	Click this button to add an item to the list.
OK	Click this button to save any changes made to the list.
Valid Band Info - This table displays the entire frequency band the WiMAX Device supports. The frequency ranges to scan that you configured in Channel Plan Settings must be within this range.	
Band Start (KHz)	This indicates the beginning of the frequency band in kilohertz (KHz).
Band End (KHz)	This indicates the end of the frequency band in kilohertz (KHz).
Save	Click this to save the changes made.
Cancel	Click this avoid any changes made from being saved to your configuration.

6.6 CAPL Settings

This screen allows you to view the Contractual Agreement Preference List (CAPL) of NAPs for base stations that are preferred for establishing connections. The CAPL is a list of NAPs that are affiliated with the Home NSP through contractual agreements.

Click **WiMAX > ND&S > CAPL Settings** to open this screen as shown next.

Figure 32 CAPL Settings



This screen contains the following fields:

Table 16 CAPL Settings

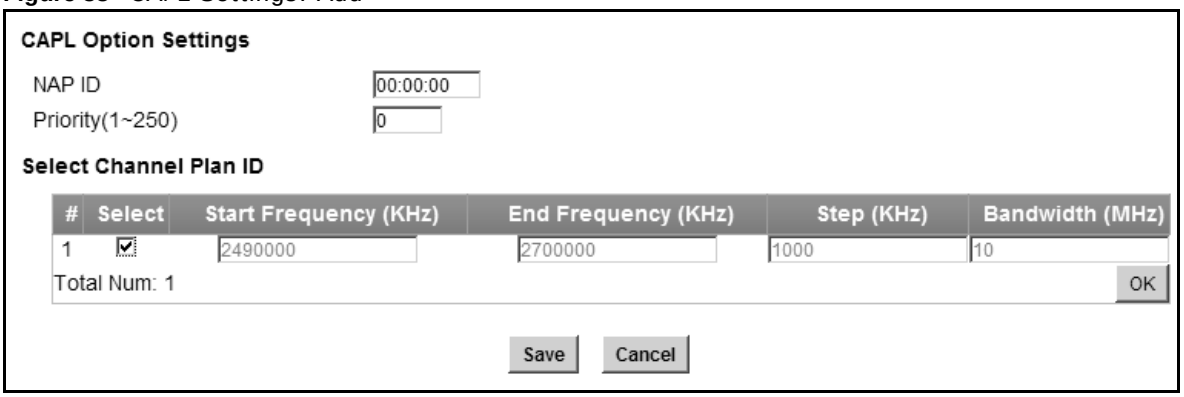
LABEL	DESCRIPTION
NAP ID	This displays the NAP ID.
Priority	This displays the priority for the NAP ID.
Channel Plan ID	This displays the Channel Plan ID.
Delete	Click this button to remove an item from the list.
Add	Click this button to add an item to the list.
Save	Click this to save the changes made.
Cancel	Click this avoid any changes made from being saved to your configuration.

6.6.1 CAPL Settings: Add

This screen allows you to specify the Contractual Agreement Preference List (CAPL) of NAPs, and the corresponding channel plan to search for the NAP.

Click **WiMAX > ND&S > CAPL Settings: Add** to open this screen as shown next.

Figure 33 CAPL Settings: Add



This screen contains the following fields:

Table 17 CAPL Settings: Add

LABEL	DESCRIPTION
NAP ID	Specify the NAP ID in the format XX:XX:XX where X is a hexadecimal character. The NAP ID is typically the first three blocks of the BSID of the base station.
Priority	Specify the priority for the NAP ID. Enter 1-250 where 1 is the highest priority. The WiMAX Device will search for NAPs according to the priority specified. Priority may be determined by the number of base stations an NAP has, with a NAP having more base stations being assigned a higher priority. If the same priority is assigned to a NAP ID, the WiMAX Device will consider them as having equal priority.
Select Channel Plan ID	
Select	After clicking a Channel Plan ID entry in the list, you can click this check box to select it.
Start Frequency (KHz)	This indicates the beginning of a frequency band in kilohertz (KHz).

Table 17 CAPL Settings: Add (continued)

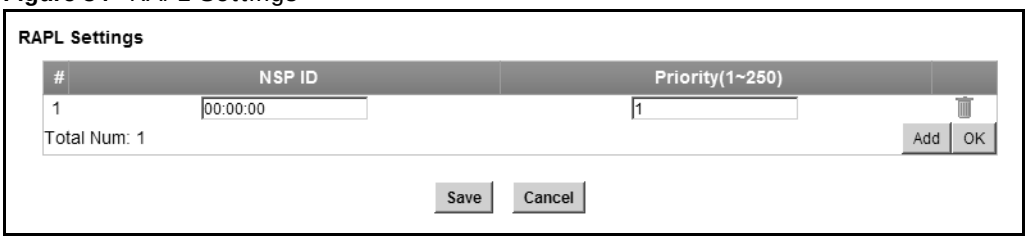
LABEL	DESCRIPTION
End Frequency (KHz)	This indicates the end of the frequency band in kilohertz (KHz).
Step (KHz)	This indicates the frequency step within each band in kilohertz (KHz).
Bandwidth (MHz)	This indicates the bandwidth in megahertz (MHz).
OK	Click this button to save any changes made to the list.
Save	Click this to save the changes made.
Cancel	Click this avoid any changes made from being saved to your configuration.

6.7 RAPL Settings

This screen allows you to specify the Roaming Agreement Preference List (RAPL) of preferred NSPs for establishing connections to the Home NSP. The RAPL is a list of NSPs that are affiliated with the Home NSP through roaming agreements. A NSP specified in the RAPL is a V-NSP and can route data to the Home NSP.

Click **WiMAX > ND&S > RAPL Settings** to open this screen as shown next.

Figure 34 RAPL Settings



This screen contains the following fields:

Table 18 RAPL Settings

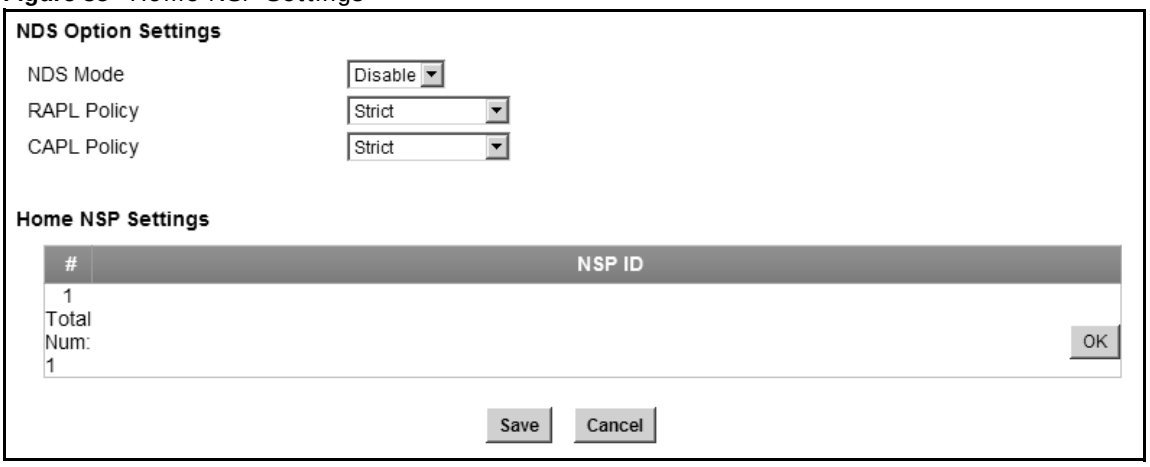
LABEL	DESCRIPTION
NSP ID	Specify the Network Service Provider (NSP) ID in the format XX:XX:XX where X is a hexadecimal character. If the Home NSP ID is entered in this list, the WiMAX Device will try to use it to establish a connection.
Priority	Specify the priority for the NSP. Enter 1-250 where 1 is the highest priority.
Delete	Click this button to remove an item from the list.
Add	Click this button to add an item to the list.
OK	Click this button to save any changes made to the list.
Save	Click this to save the changes made.
Cancel	Click this avoid any changes made from being saved to your configuration.

6.8 Home NSP Settings

On this screen, you can configure settings for the Home NSP. The Home NSP can authenticate and authorize connections and may support roaming through relationships with other NSPs.

Click **WiMAX > ND&S > Home NSP Settings** to open this screen as shown next.

Figure 35 Home NSP Settings



This screen contains the following fields:

Table 19 Home NSP Settings

LABEL	DESCRIPTION
NDS Option Settings	
NDS Mode	Select **Enable** to use NDS to establish connections to the Home NSP.
RAPL Policy	Select **Strict** to only allow V-NSPs specified in the RAPL to be used for establishing connections to the H-NSP. Select **Partially Flexible** to allow the WiMAX Device to use V-NSPs not specified in the RAPL to connect to the H-NSP. Before attempting V-NSPs not specified in the RAPL the WiMAX Device will first try the V-NSPs specified in the RAPL to connect to the H-NSP. Select **Flexible** to allow the WiMAX Device to use any V-NSPs for establishing connections to the H-NSP. V-NSPs specified in the RAPL will have the same priority as V-NSPs not specified in the RAPL.
CAPL Policy	Select **Strict** to only allow NAPs specified in the CAPL to be used for establishing connections to the H-NSP. Select **Partially Flexible** to allow the WiMAX Device to use NAPs not specified in the CAPL to connect to the H-NSP. Before attempting NAPs not specified in the CAPL the WiMAX Device will first try the NAPs specified in the CAPL to connect to the H-NSP. Select **Flexible** to allow the WiMAX Device to use any NAPs for establishing connections to the H-NSP. NAPs specified in the CAPL will have the same priority as NAPs not specified in the CAPL.
Home NSP Settings	
NSP ID	After clicking the entry in the NSP ID list, you can enter the NSP ID for the Home NSP here in the format XX:XX:XX where X is a hexadecimal character. Only one Home NSP can be entered.
OK	Click this button to save any changes made to the list.

Table 19 Home NSP Settings (continued)

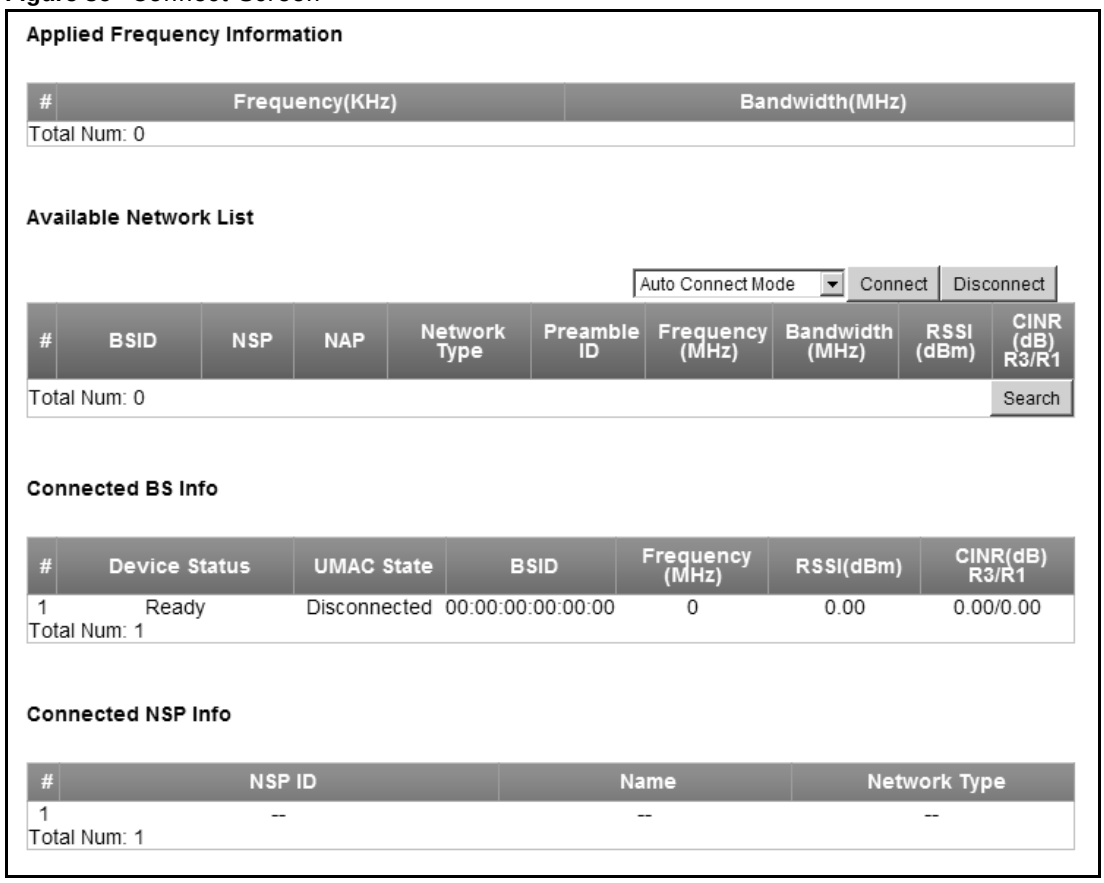
LABEL	DESCRIPTION
Save	Click this button to save any changes made to the list. Note: If you change the **NDS Mode**, the WiMAX Device will reboot when you click save.
Cancel	Click this avoid any changes made from being saved to your configuration.

6.9 Connect

This screen allows you to view the available WiMAX frequency band(s) and base station(s) the WiMAX Device found through scanning and choose a base station to which to connect.

Click **WiMAX > Connect** to open this screen as shown next.

Figure 36 Connect Screen



This screen contains the following fields:

Table 20 Connect

LABEL	DESCRIPTION
Applied Frequency Information This table shows the scanning result you made in the **WiMAX > Profile > Frequency Settings** and **WiMAX > Wide Scan** screens. Note: You cannot see the wide scanning result that you made in **WiMAX > Wide Scan** screen if the **Join Wide Scan Result** is set to **No** in the **WiMAX > Profile > Frequency Settings** screen.	
Applied Frequency Information	
Frequency (KHz)	This field displays the available center frequency of a frequency band in kilohertz (KHz).
Bandwidth (MHz)	This field displays the bandwidth of the frequency band in megahertz (MHz).
Available Network List	
Connected Mode	Select a connect mode: • **Auto Connect Mode** - This allows the WiMAX Device to connect to any of the base stations on the list automatically. • **Network Search Mode** - This allows the WiMAX Device to connect to a user-specified base station. Select this option, choose a base station, click **Connect**. • **NSP Mode** - This allows the WiMAX Device to connect to a base station with a user-specified NSP ID. To specify the NSP ID, select a result in the list and click **Connect**. The WiMAX Device will automatically connect to a base station with the same NSP ID, and the best CINR or RSSI. • **NSP/NAP Mode** - This allows the WiMAX Device to connect to a base station with a user-specified NSP ID and NAP ID. To specify the NSP ID and NAP ID, select a result in the list and click **Connect**. The WiMAX Device will automatically connect to a base station with the same NSP ID and NAP ID, and the best CINR or RSSI. • **NSP/NAP/BSID Mode** - This allows the WiMAX Device to connect to a base station with a user-specified NSP ID, NAP ID and BSID. To specify the NSP ID, NAP ID and BSID, select a result in the list and click **Connect**. The WiMAX Device will automatically connect to a base station with the same NSP ID, NAP ID and BSID, and the best CINR or RSSI.
Connect	Click this to connect to the selected base station.
Disconnect	Click this to disconnect from the selected base station.
BSID	This field displays the base station MAC address.
NSP	This field displays the NSP ID.
NAP	This field displays the NAP ID.
Network Type	This field displays the network type.
Preamble ID	This field displays the preamble ID. The preamble ID is the index identifier in the header of the base station's broadcast messages. In the beginning of a mobile stations's network entry process, it searches for the preamble and uses it to additional channel information. The preamble ID is used to synchronize the upstream and downstream transmission timing with the base station.
Frequency (MHz)	This field displays the center frequency the base station uses in kilohertz (KHz).
Bandwidth (MHz)	This field displays the frequency band bandwidth the base station uses in megahertz (MHz).

Table 20 Connect (continued)

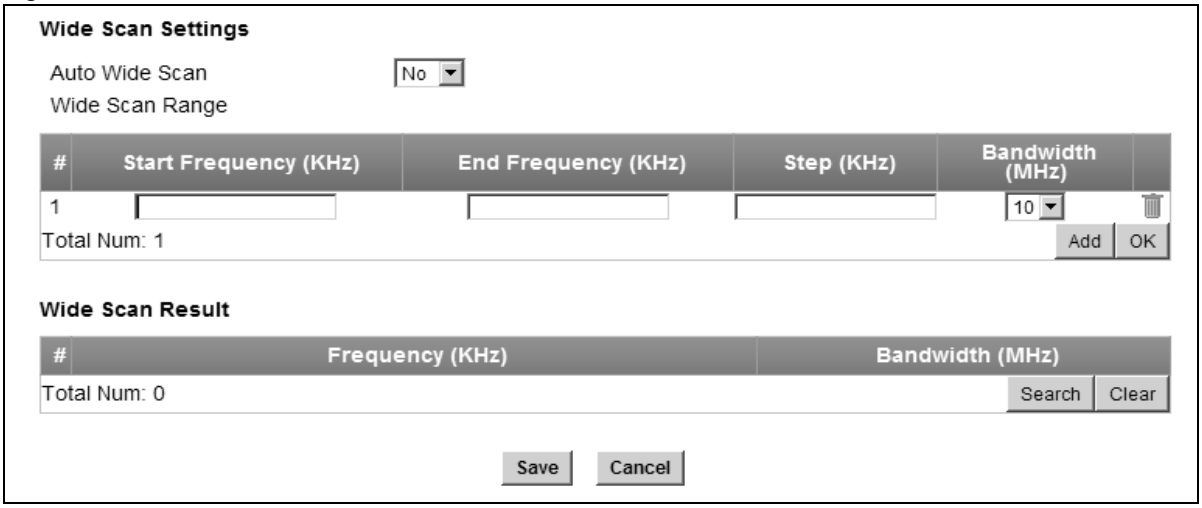
LABEL	DESCRIPTION
RSSI (dBm)	This field displays the Received Signal Strength Indication (RSSI), which is an overall measurement of radio signal strength. A higher RSSI level indicates a stronger signal.
CINR (dB) R3/ R1	This field displays the average Carrier to Interference plus Noise Ratio for the current connection. This value is an indication of overall radio signal quality, where a higher value means a better quality signal.
Search	Click this to have the WiMAX Device scan for base stations in the frequency band(s) listed in the **Applied Frequency Information** table.
Connected BS Info	
Device Status	This field displays the WiMAX Device current status for connecting to the selected base station. • **Scanning** - The WiMAX Device is scanning for available base stations. • **Ready** - The WiMAX Device has finished scanning and you can connect to a base station. • **Connecting** - The WiMAX Device attempts to connect to the selected base station. • **Connected** - The WiMAX Device has successfully connected to the selected base station.
UMAC State	This field displays the status of the WiMAX connection between the WiMAX Device and the base station. • **Network Search** - The WiMAX Device is scanning for any available WiMAX connections. • **Disconnected** - No WiMAX connection is available. • **Network Entry** - A WiMAX connection is initializing. • **Normal** - The WiMAX connection has been successfully established.
BSID	This field displays the MAC address of the base station to which the WiMAX Device is connected.
Frequency (MHz)	This field displays the frequency the base station uses in megahertz (MHz).
RSSI (dBm)	This field displays the Received Signal Strength Indication (RSSI), which is an overall measurement of radio signal strength. A higher RSSI level indicates a stronger signal.
CINR (dB)	This field displays the average Carrier to Interference plus Noise Ratio for the current connection. This value is an indication of overall radio signal quality, where a higher value means a better quality signal.
Connected NSP Info	
NSP ID	This field displays the NSP ID of the connected NSP.
Name	This field displays the name of the connected NSP.
Network Type	This field displays the network type of the connected NSP.

6.10 Wide Scan

This screen allows you to discover base stations by entering one or more frequency ranges and bandwidth on which to scan.

Click **WiMAX > Wide Scan** to open this screen as shown next.

Figure 37 Wide Scan Screen



This screen contains the following fields:

Table 21 Wide Scan

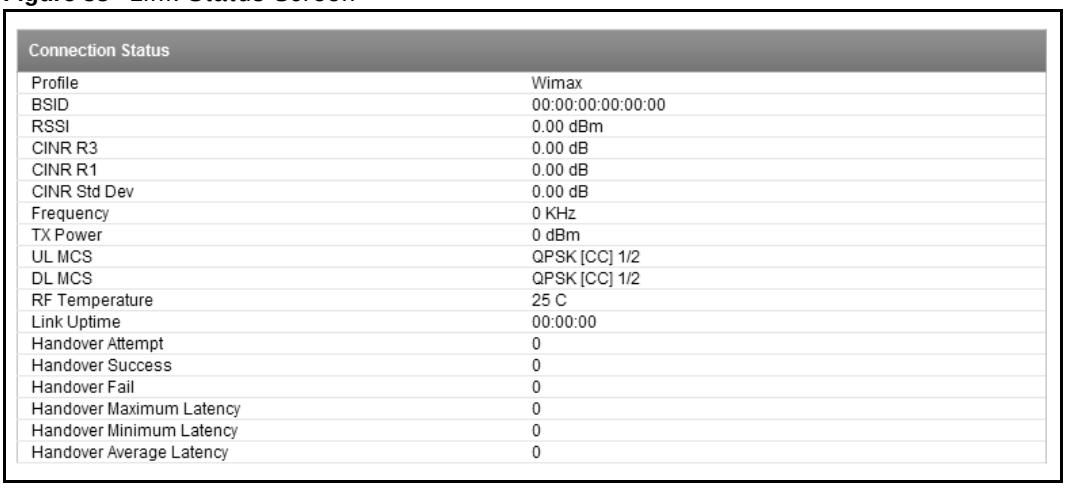
LABEL	DESCRIPTION
Wide Scan Settings	
Auto Wide Scan	Use this to enable (**Yes**) or disable (**No**) automatically scanning for base stations.
Wide Scan Range	
Start Frequency (KHz)	Enter the start frequency in kilohertz (KHz) for a wide scan range.
End Frequency (KHz)	Enter the end frequency in kilohertz (KHz) for a wide scan range.
Step (KHz)	Enter the step increment in kilohertz (KHz) that the wide scan jumps each time it scans between the start and end frequencies.
Bandwidth (MHz)	Enter the frequency bandwidth to be scanned.
Delete	Click this to remove a range of frequencies from the wide scan range list.
Add	Click this to add a range of frequencies to the wide scan range list.
OK	Click this so save any changes to the wide scan range list.
Wide Scan Result This table displays the available frequency band(s) found through the wide scan.	
Frequency (KHz)	This field displays the frequency in kilohertz (KHz).
Bandwidth (MHz)	This field displays the bandwidth in megahertz (MHz).
Search	Click this to initiate a wide scan.
Clear	Click this to clear the wide scan results.

6.11 Link Status

This screen provides a general overview of the current WiMAX connection with the service provider.

Click **WiMAX > Link Status** to open this screen as shown next.

Figure 38 Link Status Screen



This screen contains the following fields:

Table 22 Link Status

LABEL	DESCRIPTION
Profile	This field displays the profile name.
BSID	This field displays the MAC address of the base station to which the WiMAX Device is currently connected.
RSSI	This field displays the Received Signal Strength Indication (RSSI), which is an overall measurement of radio signal strength. A higher RSSI level indicates a stronger signal.
CINR R3	This field displays the average Carrier to Interference plus Noise Ratio (R3) for the current connection. This value is an indication of overall radio signal quality, where a higher value means a better quality signal.
CINR R1	This field displays the average Carrier to Interference plus Noise Ratio (R1) for the current connection. This value is an indication of overall radio signal quality, where a higher value means a better quality signal.
CINR Std Dev	This field displays the average Carrier to Interference plus Noise Ratio (Std Dev) for the current connection. This value is an indication of overall radio signal quality, where a higher value means a better quality signal.
Frequency	This field displays the frequency in kilohertz (KHz).
TX Power	This field displays the transmission power of the WiMAX Device in dBm.
UL MCS	This field displays the Uplink Modulation and Coding Sequence (UL MCS).
DL MCS	This field displays the Downlink Modulation and Coding Sequence (DL MCS).
RF Temperature	This field displays the temperature in centigrade of the WiMAX Device's RF circuit.
Link Uptime	This field displays the length of time the current connection has been up.
Handover Success	This field displays how many times the WiMAX Device had ever successfully switched its connection from one base station to another base station, since the WiMAX Device last restarted.

Table 22 Link Status (continued)

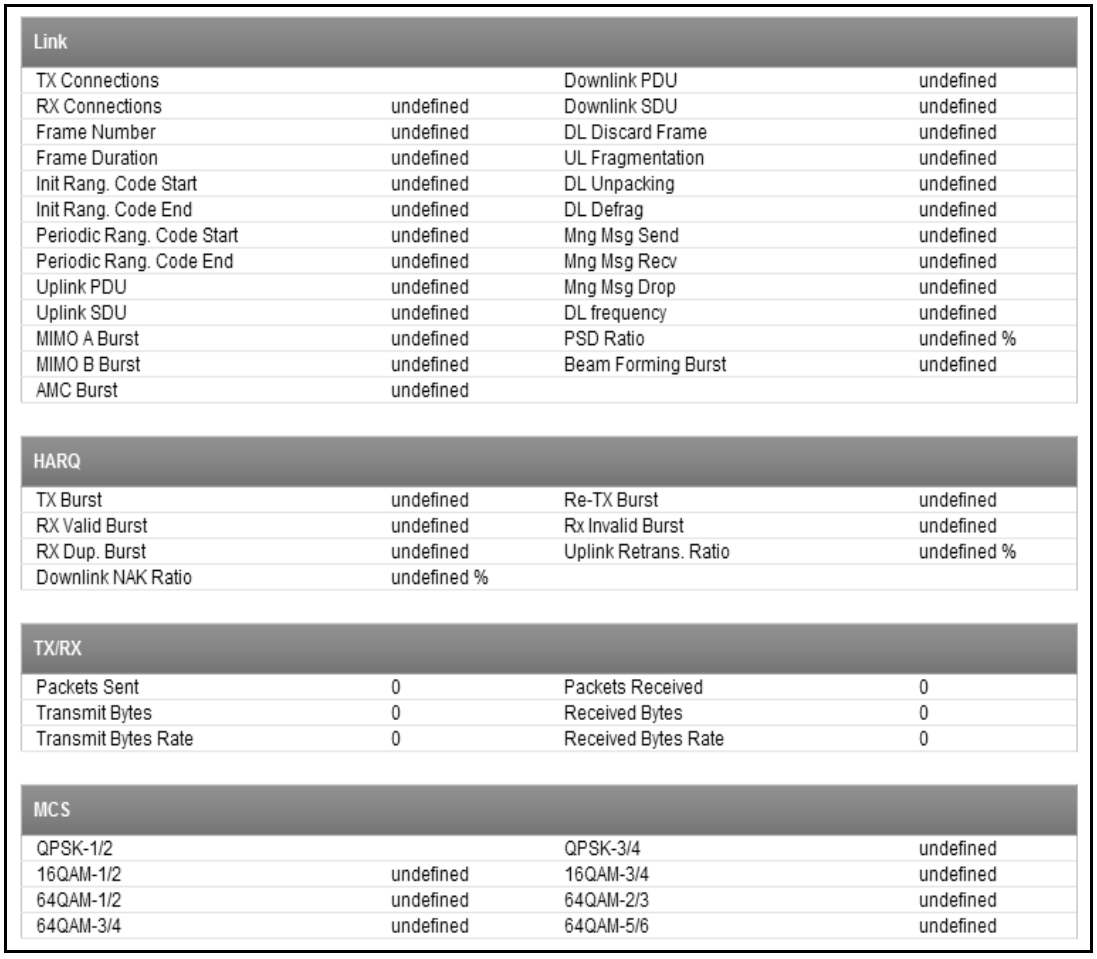
LABEL	DESCRIPTION
Handover Fail	This field displays how many times the WiMAX Device had been failed to switch its connection from one base station to another base station, since the WiMAX Device last restarted.
Handover Maximum Latency	This field displays the maximum latency for switching connections from one base station to another base station, since the WiMAX Device last restarted.
Handover Minimum Latency	This field displays the minimum latency for switching connections from one base station to another base station, since the WiMAX Device last restarted.
Handover Average Latency	This field displays the average latency for switching connections from one base station to another base station, since the WiMAX Device last restarted.

6.12 Link Statistics

This screen provides a detailed overview of the current WiMAX connection with the service provider.

Click **WiMAX > Link Statistics** to open this screen as shown next.

Figure 39 Link Statistics Screen



Link			
TX Connections		Downlink PDU	undefined
RX Connections	undefined	Downlink SDU	undefined
Frame Number	undefined	DL Discard Frame	undefined
Frame Duration	undefined	UL Fragmentation	undefined
Init Rang. Code Start	undefined	DL Unpacking	undefined
Init Rang. Code End	undefined	DL Defrag	undefined
Periodic Rang. Code Start	undefined	Mng Msg Send	undefined
Periodic Rang. Code End	undefined	Mng Msg Recv	undefined
Uplink PDU	undefined	Mng Msg Drop	undefined
Uplink SDU	undefined	DL frequency	undefined
MIMO A Burst	undefined	PSD Ratio	undefined %
MIMO B Burst	undefined	Beam Forming Burst	undefined
AMC Burst	undefined		

HARQ			
TX Burst	undefined	Re-TX Burst	undefined
RX Valid Burst	undefined	Rx Invalid Burst	undefined
RX Dup. Burst	undefined	Uplink Retrans. Ratio	undefined %
Downlink NAK Ratio	undefined %		

TX/RX			
Packets Sent	0	Packets Received	0
Transmit Bytes	0	Received Bytes	0
Transmit Bytes Rate	0	Received Bytes Rate	0

MCS			
QPSK-1/2		QPSK-3/4	undefined
16QAM-1/2	undefined	16QAM-3/4	undefined
64QAM-1/2	undefined	64QAM-2/3	undefined
64QAM-3/4	undefined	64QAM-5/6	undefined

This screen contains the following sections:

Table 23 Link Statistics

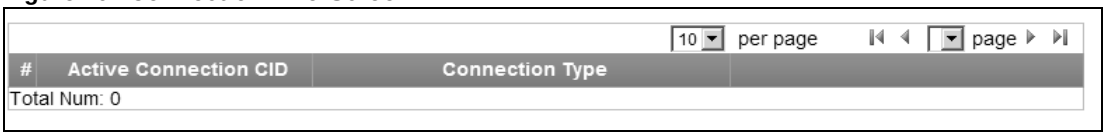
LABEL	DESCRIPTION
Link	This section provides a detailed overview of link statistics.
HARQ	This section provides a detailed overview of Hybrid Automatic Repeat Request link statistics.
TX/RX	This section provides a detailed overview of transmission and receiving link statistics.
MCS	This section provides a detailed overview of Modulation and Coding Sequence (MCS) link statistics

6.13 Connection Info

This screen displays all of the connections made through the WiMAX device since its last reboot.

Click **WiMAX > Connection Info** to open this screen as shown next.

Figure 40 Connection Info Screen



This screen contains the following fields:

Table 24 Connection Info

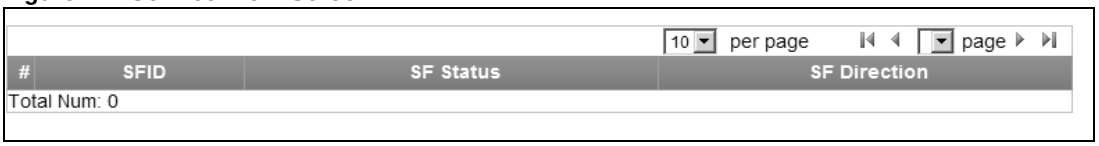
LABEL	DESCRIPTION
Active Connection CID	This displays the unique, unidirectional 16-bit Connection Identifier (CID) for an active connection.
Connection Type	This displays the type of connection.

6.14 Service Flow

This screen displays data priority information for all of the connections made through the WiMAX device since its last reboot.

Click **WiMAX > Service Flow** to open this screen as shown next.

Figure 41 Service Flow Screen



This screen contains the following fields:

Table 25 Service Flow

LABEL	DESCRIPTION
SFID	This displays a 32-bit service flow identifier.
SF Status	This display the service flow status.
SF Direction	This displays the service flow direction.

7

Network Setting

7.1 Overview

This chapter shows you how to configure the WiMAX Device's network setting.

7.1.1 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.

DHCP

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

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; otherwise, leave them blank.

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

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

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

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:

- **RX/TX -** the WiMAX Device will broadcast its routing table periodically and incorporate the RIP information that it receives.
- **RX Only -** the WiMAX Device will not send any RIP packets but will accept all RIP packets received.
- **TX Only -** the WiMAX Device will send out RIP packets but will not accept any RIP packets received.
- **None -** the WiMAX Device will not send any RIP packets and will ignore any RIP packets received.

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

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

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.

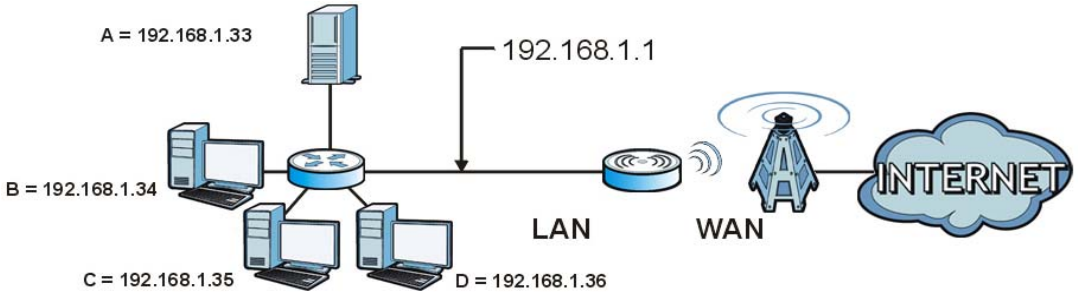
With port forwarding, you can forward incoming service requests to the server(s) on your local network. You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 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 42 Multiple Servers Behind NAT Example



Trigger Ports

Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address,

Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The WiMAX Device records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the WiMAX Device's WAN port receives a response with a specific port number and protocol ("incoming" port), the WiMAX Device forwards the traffic to the LAN IP address of the computer that sent the request. After that computer’s connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

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.

UPnP

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.

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.

Cautions with UPnP

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

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

UPnP and ZyXEL

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

The WiMAX Device only sends UPnP multicasts to the LAN.

Content Filter

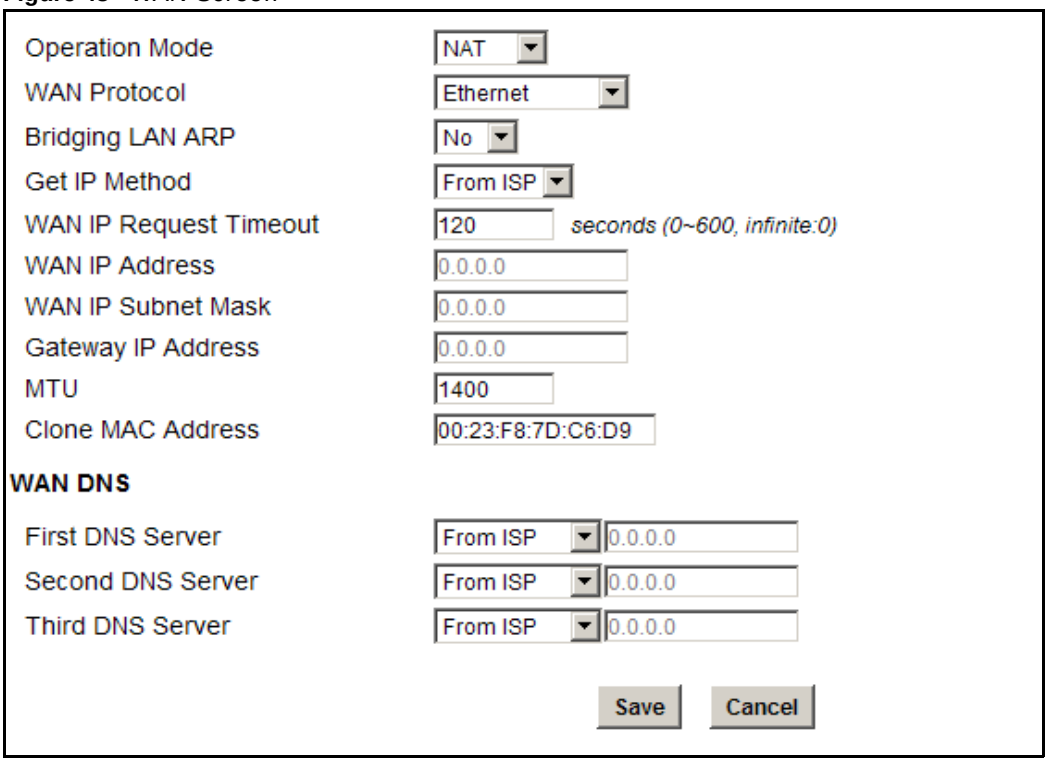
Internet content filtering allows you to create and enforce Internet access policies tailored to their needs. Content filtering is the ability to block certain specific URL keywords.

7.2 WAN

Use these settings to configure the WAN connection between the WiMAX Device and the service provider.

Click **Network Setting > WAN** to open this screen as shown next.

Figure 43 WAN Screen



This screen contains the following fields:

Table 26 WAN

LABEL	DESCRIPTION
Operation Mode	Select the WiMAX Device's operational mode. • **Bridge** - This puts the WiMAX Device in bridge mode, acting as a transparent middle man between devices on the LAN and the devices on the WAN. • **Router** - Select Router from the drop-down list box if your ISP gives you one IP address only and you want multiple computers to share an Internet account. • **NAT** - This allows the WiMAX Device to tag frames for NAT, allowing devices on the LAN to use their own internal IP addresses while communicating with devices on the WAN.
WAN Protocol	Select the protocol the WiMAX Device uses to connect to the WAN. The options are: • **Ethernet** - Select this if you have a persistent connection to the network. • **PPPoE** - Select this if must log into the network before initiating a persistent connection. • **GRE Tunnel** - Select this if you connect to the network using Point-to-Point Protocol to create VPNs. • **EtherIP Tunnel** - Select this if you need to tunnel Ethernet and IEEE 802.3 MAC frames across an IP Internet.
Bridging LAN ARP	This option enables or disables allow ARP requests to cross the WiMAX Device.
Get IP Method	Select how the WiMAX Device receives its IP address. • **User** - Select this to manually enter the IP address the WiMAX Device uses. • **From ISP** - Select to automatically get the IP address the WiMAX Device uses from the ISP.

Table 26 WAN (continued)

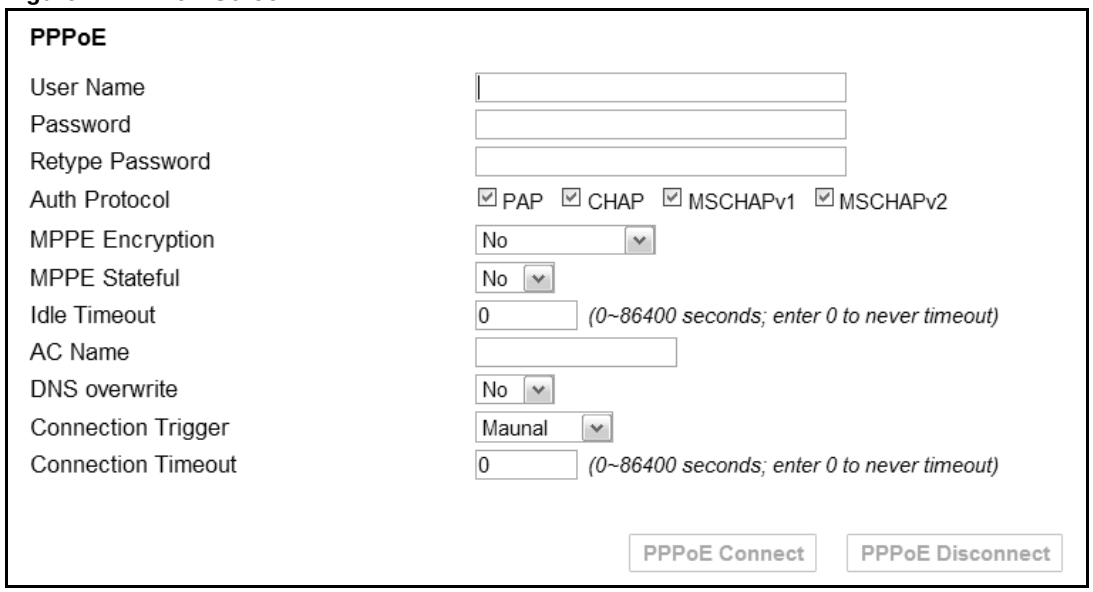
LABEL	DESCRIPTION
WAN IP Request Timeout	Enter the number of seconds the WiMAX Device waits for an IP from the ISP before it times out.
WAN IP Address	If the WiMAX Device gets its IP from the user, enter the IP address it is to use.
WAN IP Subnet Mask	If the WiMAX Device gets its IP from the ISP, enter the IP address it is to use.
Gateway IP Address	If the WiMAX Device gets its gateway IP address from the user, enter the IP address it is to use.
MTU	Enter the Maximum Transmission Unit (MTU) for the WiMAX Device. This is the largest protocol unit that the WiMAX Device allows to pass through it.
Clone MAC Address	Enter a MAC address here for registering bridged devices on the network if their current MAC addresses are causing problems. For example, this can happen when a desktop computer swaps network interface cards; the original NIC may have used its MAC address to register itself on the network and now the new NIC is unrecognized. Using a MAC address that you know is valid, i.e. a “clone”, allows that device to stay registered.
WAN DNS	
First~Third DNS Server	Select how the WiMAX Device acquires its DNS server address. • **From ISP** - Select this to have the WiMAX Device acquire its DNS server address from the ISP. • **User Define** - Select this to manually enter the DNS server used by the WiMAX Device.

7.3 PPPoE

Use these settings to configure the PPPoE connection between the WiMAX Device and the service provider.

Click Network Setting > WAN > PPPoE.

Figure 44 PPPoE Screen



This screen contains the following fields:

Table 27 PPPoE

LABEL	DESCRIPTION
User Name	Enter the username for PPPoE login into the WAN network.
Password	Enter the password for PPPoE login into the WAN network.
Retype Password	Retype the password to confirm it.
Auth Protocol	Select a PPPoE authentication protocol. The WiMAX Device supports the following: • **PAP** - Password Authentication Protocol uses unencrypted plaintext to send a passwords for authentication over the network. It's probably not a good idea to rely on this for security. • **CHAP** - The Challenge Handshake Authentication Protocol (CHAP) uses PPP to authenticate remote devices using a three-way handshake and shared secret verification. • **MS-CHAP v1 / 2** -This is Microsoft's variant of Challenge Handshake Authentication Protocol (CHAP). It allows for mutual authentication between devices.
MPPE Encryption	Use this option to enable or disable authentication through Microsoft Point-To-Point Encryption (MPPE) protocol.
MPPE Stateful	Use this option to allow or disallow the WiMAX Device to use the Microsoft Point-To-Point Encryption (MPPE) protocol for stateful peer negotiation.
Idle Timeout	Enter the number of second the WiMAX Device waits during authentication before timing out.
AC Name	Enter the access concentrator name for the PPPoE interface if your ISP uses an AC PPPoE service.
DNS Overwrite	Use this option to allow or disallow the WiMAX Device to overwrite DNS static DNS entries on client devices.
Connection Trigger	Set whether the WiMAX Device is persistently connected to the WAN (**AlwaysOn**) or you must click the PPPoE Connect button each time you want to get on the WAN (**Manual**).
Connection Timeout	Enter in seconds the duration the WiMAX Device waits for idle activity before disconnecting from the WAN.
PPPoE Connect	Click this to connect to the WAN using PPPoE.
PPPoE Disconnect	Click this to disconnect from the WAN.

7.4 GRE

Use these settings to configure the peer setting of the Generic Routing Encapsulation (GRE) tunnel between the WiMAX Device and another GRE peer.

Click **Network Setting > WAN > GRE** to open this screen as shown next.

Figure 45 GRE Screen

This screen contains the following fields:

Table 28 GRE

LABEL	DESCRIPTION
Peer IP Address	Enter the IP address of the GRE peer.

7.5 EtherIP

Use these settings to configure the peer setting of the EtherIP tunnel between the WiMAX Device and another EtherIP peer.

Click **Network Setting > WAN > EtherIP** to open this screen as shown next.

Figure 46 EtherIP Screen

This screen contains the following fields:

Table 29 EtherIP

LABEL	DESCRIPTION
Peer IP Address	Enter the IP address of the EtherIP peer.

7.6 IP

Use these settings to configure the LAN connection between the WiMAX Device and your local network.

Click **Network Setting > LAN > IP** to open this screen as shown next.

Figure 47 IP Screen

This screen contains the following fields:

Table 30 IP

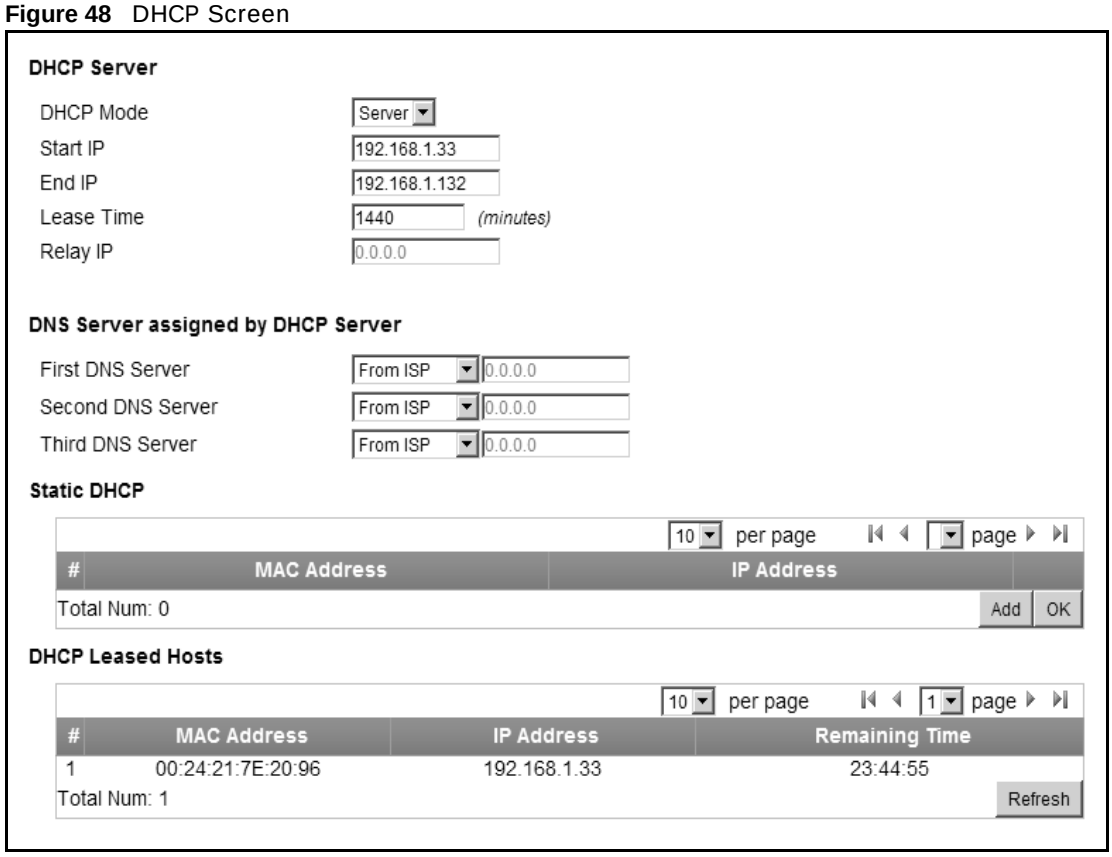
LABEL	DESCRIPTION
IP address	Enter the IP address of the LAN interface for the WiMAX Device.
IP Subnet Mask	Enter the IP subnet mask of the LAN interface for the WiMAX Device.

7.7 DHCP

Use these settings to configure whether the WiMAX Device functions as a DHCP server for your local network, or a DHCP relay between the local network and the service provider. You can also disable the DHCP functions.

Click **Network Setting > LAN > DHCP** to open this screen as shown next.

Figure 48 DHCP Screen



This screen contains the following fields:

Table 31 DHCP

LABEL	DESCRIPTION
DHCP Server	
DHCP Mode	Select this if you want the WiMAX Device to be the DHCP server on the LAN. As a DHCP server, the WiMAX Device assigns IP addresses to DHCP clients on the LAN and provides the subnet mask and DNS server information. • **None** - This disables DHCP mode for the WiMAX Device. • **Server** - This sets the WiMAX Device as a DHCP server for the LAN. • **Relay** - This sets the WiMAX Device as a DHCP relay for the LAN, allowing it to pass-through IP addresses assigned to LAN devices from the ISP servers.
Start IP	Enter the start IP address from which the WiMAX Device begins allocating IP addresses.
End IP	Enter the end IP address at which the WiMAX Device ceases allocating IP addresses.

Table 31 DHCP (continued)

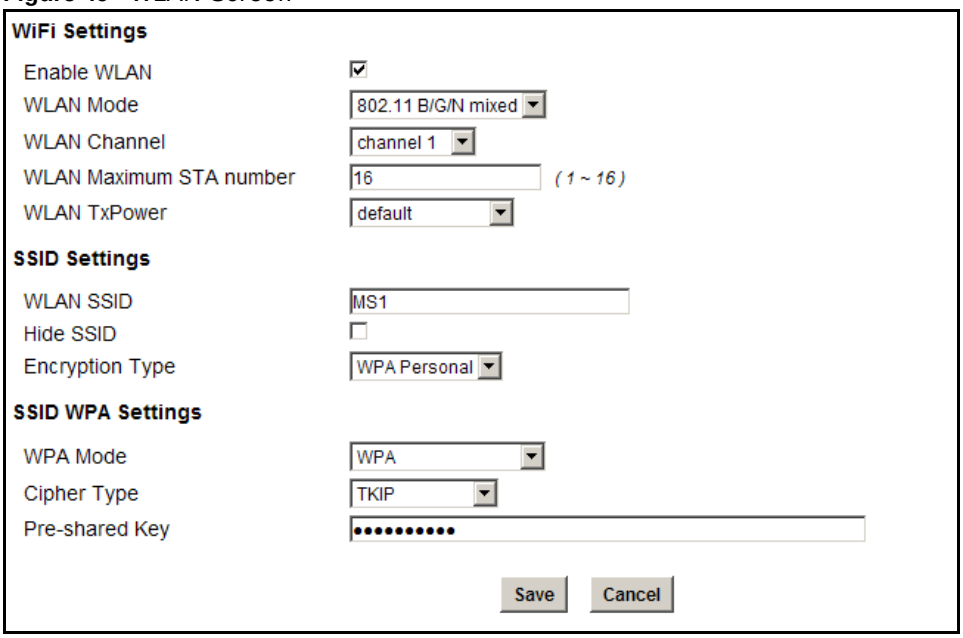
LABEL	DESCRIPTION
Lease Time	Enter the duration in minutes that devices on the LAN retain their DHCP-issued IP addresses. At the end of the lease time, they poll the WiMAX Device for a renewed or replacement IP.
Relay IP	Enter the name of the IP address to be used.
DNS Server Assigned by the DHCP Server	
First~Third DNS Server	Select how the WiMAX Device acquires its DNS server address. • **None** - Select this to not use a DNS server. • **From ISP** - Select this to have the WiMAX Device acquire its DNS server address from the ISP. • **User Define** - Select this to manually enter the DNS server used by the WiMAX Device.
Static DHCP	
MAC Address	This field displays the MAC address of the static DHCP client connected to the WiMAX Device.
IP Address	This field displays the IP address of the static DHCP client connected to the WiMAX Device.
Add	Click this to add a new static DHCP entry.
OK	Click this to save any changes made to this list.
DHCP Leased Hosts	
MAC Address	This displays the MAC address of the DHCP leased host.
IP Address	This displays the IP address of the DHCP leased host.
Remaining Time	This displays the how much time is left on the host's lease.
Refresh	Click this to refresh the list.

7.8 WLAN

This screen is available for models with WiFi wireless feature. Use the **WLAN** screen to configure the connections between the WiMAX Device and the wireless clients that want to access the Internet.

Click **Network Setting > WLAN** to open this screen as shown next.

Figure 49 WLAN Screen



This screen contains the following fields:

Table 32 WLAN

LABEL	DESCRIPTION
WiFi Settings	
Enable WLAN	Select this to activate the wireless LAN.
WLAN Mode	Select **802.11B/G mixed** to allow both IEEE802.11b and IEEE802.11g compliant WLAN devices to associate with the WiMAX Device. Select **802.11B only** to allow only IEEE 802.11b compliant WLAN devices to associate with the WiMAX Device. Select **802.11A only** to allow only IEEE 802.11a compliant WLAN devices to associate with the WiMAX Device. Select **802.11G only** to allow only IEEE 802.11g compliant WLAN devices to associate with the WiMAX Device.
WLAN Channel	Select this option and set the operating frequency/channel depending on your particular region. Select **Auto** to have the WiMAX Device scan and find an available channel.
WLAN Maximum STA number	Enter the maximum number of wireless stations that is allowed to associate with the WiMAX Device.
WLAN TxPower	Select a number between 1 and 24 dB in the drop down box to control the strength of the connection signal, or leave it as **default** to let the WiMAX Device control this feature.
SSID Settings	
WLAN SSID	This field displays the name of the wireless network and it will appear to other computers that wish to connect wirelessly to the Internet.
Hide SSID	Select this to make the name of the network invisible to others.
Encryption Type	Select the type of encryption that the network will use: **None**, **WEP** or **WPA Personal**.

Table 32 WLAN (continued)

LABEL	DESCRIPTION
SSID WEP Settings Note: You will only see these options if you selected **WEP** as the Encryption Type.	
Authentication Method	Select the type of authentication used to join the network: **OPEN SYSTEM** or **SHARED KEY**.
WEP Encryption Length	Select the length of the encryption key: 64-bit or 128-bit.
Key 1 - 4	Pick one of four available keys. The key can be in either HexaDecimal (**HEX**) or **ASCII** format. Type the key using any letters and numbers. The field is case sensitive and the length must match the length picked in the step above (64-bit or 128-bit). A warning message will appear if you fail to do this.
SSID WPA Settings Note: You will only see these options if you selected **WPA Personal** as the Encryption Type.	
WPA Mode	Select either **WPA**, **WPA2** or **Auto (WPA or WPA2)**.
Cipher Type	Select the type of authentication that you wish to use for your network: **TKIP**, **AES** or **TKIP and AES**. AES is more secure.
Pre-shared Key	Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).

7.9 WPS

This screen is available for models with WiFi wireless feature. Use the WPS screen to configure WiFi Protected Setup (WPS) on your WiMAX Device.

WPS allows you to quickly set up a wireless network with strong security without having to configure security settings manually. Set up each WPS connection between two devices. Both devices have to support WPS.

Click **Network Setting > WLAN > WPS** to open this screen as shown next.

Figure 50 WPS Screen

This screen contains the following fields:

Table 33 WPS

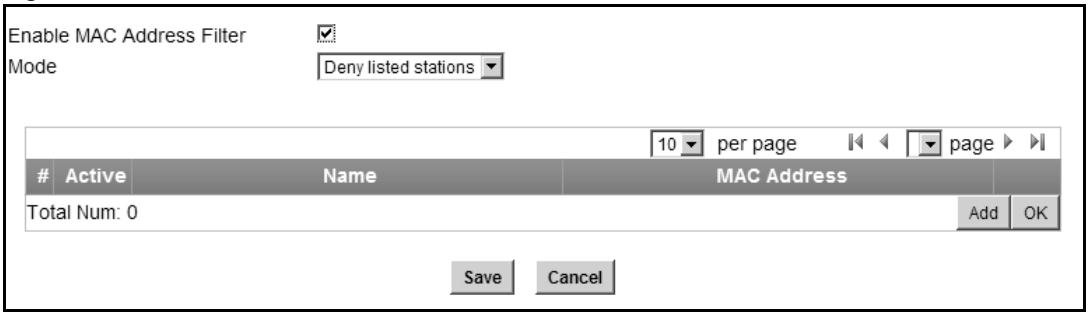
LABEL	DESCRIPTION
Enable WPS	Select **Enable** and click **Apply** to activate WPS on the WiMAX Device. Select **Disable** and click **Apply** to deactivate WPS.
Start WPS PBC	This field is available after you select **Enable** in the **Enable WPS** field and click **Apply**. Click this to activate the Push Button Configuration. After clicking this you will be able to use the WPS button at the back of the device to add new wireless clients. Note: You must press the WPS buttons within two minutes of each other.

7.10 MAC Address Filter

This screen is available for models with WiFi wireless feature. Use this screen to restrict access to the WiFi network by device ID (MAC address).

Click on **Network Setting > WLAN > MAC Address Filter**. The screen appears as shown.

Figure 51 MAC Address Filter Screen



This screen contains the following fields:

Table 34 MAC Address Filter

LABEL	DESCRIPTION
Enable MAC Address Filter	Select the check box to enable MAC address filtering. Then, the following fields display.
Mode	Define the filter action for the list of MAC addresses in the MAC address table. Select **Allow listed stations** to permit access to the WiMAX Device only to addresses listed. MAC addresses not listed will be denied access to the WiMAX Device. Select **Deny listed stations** to block access to the WiMAX Device to the computers or devices listed in this list.
#	This is the index number of the MAC address.
Active	Select this box to make the policy effective or ineffective for a particular device.
Name	Type the name of the device. The name can be up to 20 characters long, and any combination of letters, numbers or symbols.

Table 34 MAC Address Filter (continued)

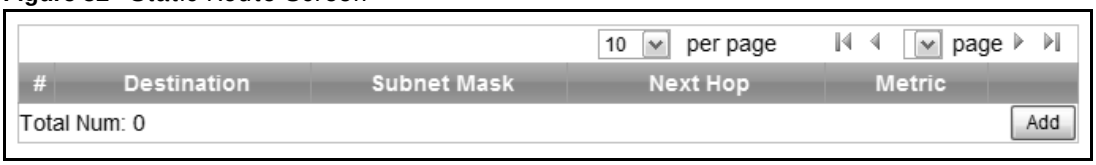
LABEL	DESCRIPTION
MAC Address	Enter the MAC addresses of the wireless devices that are allowed or denied access to the WiMAX Device in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Delete	Click to delete a specific MAC address from the list.
Add	Click to add a MAC address to the list.
OK	Click this button when you are done adding a MAC Address.

7.11 Static Route

Use these settings to create fixed paths through the network.

Click **Network Setting > Route > Static Route** to open this screen as shown next.

Figure 52 Static Route Screen



This screen contains the following fields:

Table 35 Static Route

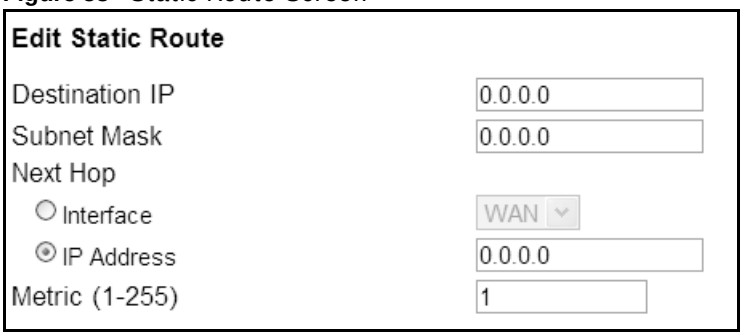
LABEL	DESCRIPTION
Destination	This field displays the destination IP address of the static route.
Subnet Mask	This field displays the subnet mask of the static route.
Next Hop	This field displays next hop information of the static route.
Metric	This field displays the static route metric.
Add	Click this to add a new static route to the list.

7.12 Static Route Add

Use these settings to configure a static route.

Click **Add** in the **Network Setting > Route > Static Route** screen to open this screen as shown next.

Figure 53 Static Route Screen



This screen contains the following fields:

Table 36 Static Route

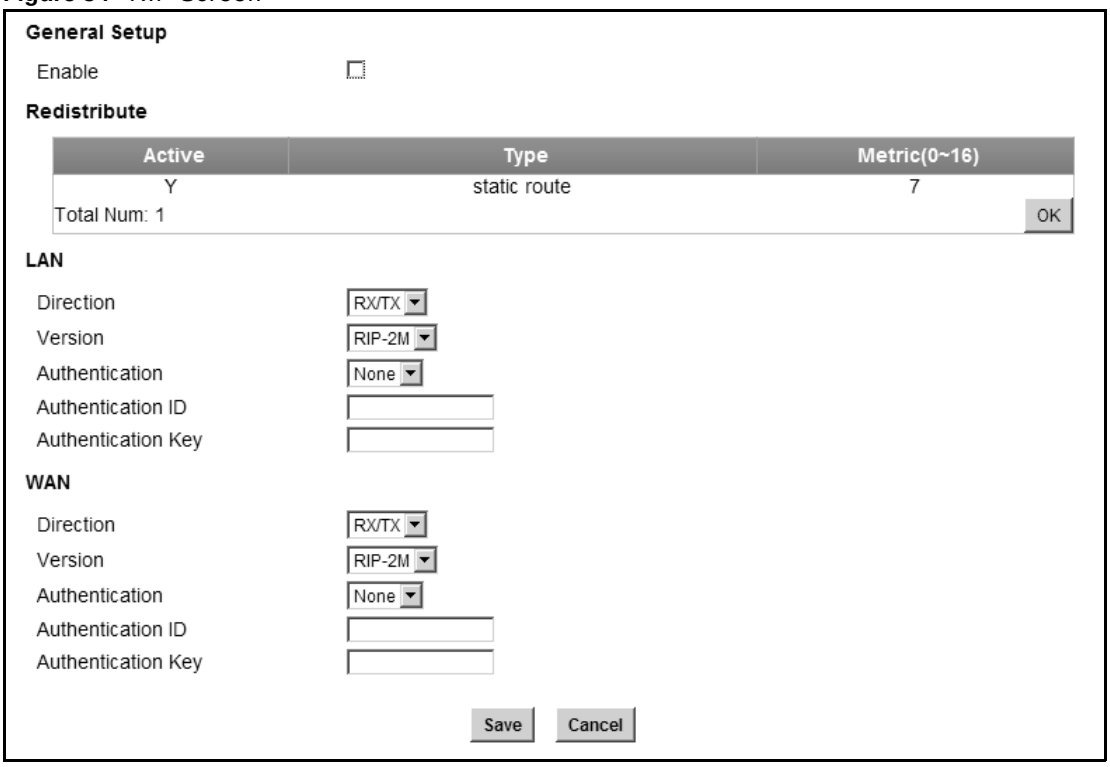
LABEL	DESCRIPTION
Destination IP	Enter the destination IP address of the static route.
Subnet Mask	Enter the subnet mask of the static route.
Next Hop	Select **Interface** and then select **WAN** or **LAN** for the next hop of the static route. If the next hop is an IP address rather than an interface on the WiMAX Device, select **IP Address** and enter the IP address.
Metric	Enter the static route metric.

7.13 RIP

Use these settings to configure how the WiMAX Device exchanges information with other routers.

Click **Network Setting > Route > RIP** to open this screen as shown next.

Figure 54 RIP Screen



This screen contains the following fields:

Table 37 RIP

LABEL	DESCRIPTION
General Setup	
Enable	Select this to enable RIP on the WiMAX Device.
Redistribute	
Active	This indicates whether a route is being redistributed.
Type	This indicates what type of route is being redistributed.
Metric	This indicates the metric that is being used for redistribution.
Edit	Click this to edit a selected route.
OK	Click this to save any changes to the redistribution table.
LAN	
Direction	Set the LAN network direction to use with RIP.
Version	Set the RIP version to use.
Authentication	Use this option to enable or disable RIP authentication.
Authentication ID	Enter the authentication ID to use for RIP authentication.
Authentication Key	Enter the authentication key to use for RIP authentication.
WAN	
Direction	Set the WAN network direction to use with RIP.
Version	Set the RIP version to use.

Table 37 RIP (continued)

LABEL	DESCRIPTION
Authentication	Use this option to enable or disable RIP authentication.
Authentication ID	Enter the authentication ID to use for RIP authentication.
Authentication Key	Enter the authentication key to use for RIP authentication.

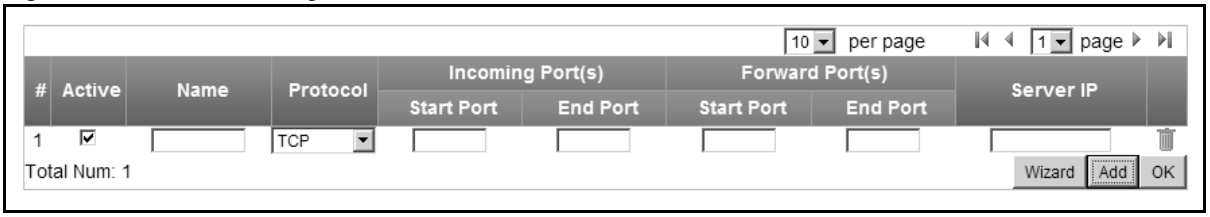
7.14 Port Forwarding

Use these settings to forward incoming service requests to the ports on your local network.

Note: Make sure you did not configure a DMZ host in the **Network Setting > NAT > DMZ** screen if you want to make the settings of this screen work.

Click **Network Setting > NAT > Port Forwarding** to open this screen as shown next.

Figure 55 Port Forwarding Screen



This screen contains the following fields:

Table 38 Port Forwarding

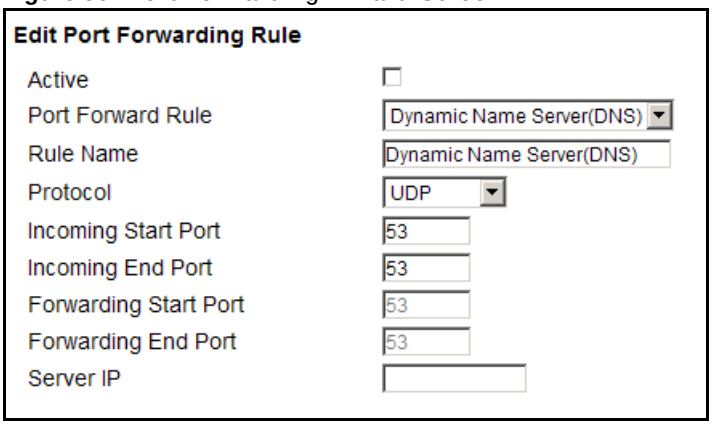
LABEL	DESCRIPTION
Active	This indicates whether the port forwarding rule is active or not.
Name	The displays the name of the port forwarding rule.
Protocol	This displays the protocol to which the port forwarding rule applies.
Incoming Port(s)	
Start Port	This displays the starting port number for incoming traffic for the port forwarding rule.
End Port	This displays the ending port number for incoming traffic for the port forwarding rule.
Forward Port(s)	
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	This displays the IP address of the server to which packet for the selected port(s) are forwarded.
Delete	Click this to delete a specified rule.
Wizard	Click this to open the port forwarding “wizard”.
Add	Click this to add a new port forwarding rule.
OK	Click this to save any changes made to the port forwarding list.

7.14.1 Port Forwarding Wizard

Use this wizard to set up a port forwarding rule for incoming service requests to the ports on your local network.

Click **Network Setting > NAT > Port Forwarding > Wizard** to open this screen as shown next.

Figure 56 Port Forwarding Wizard Screen



This screen contains the following fields:

Table 39 Port Forwarding Wizard

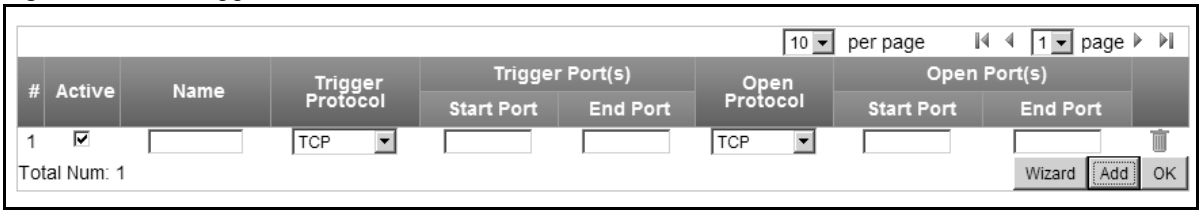
LABEL	DESCRIPTION
Active	Select this to make this port forwarding rule active.
Port Forward Rule	Select the type of port forwarding rule.
Rule Name	Enter a name for the port forwarding rule.
Protocol	Select the port forwarding protocol.
Incoming Start Port	Enter the starting port number for incoming traffic for the port forwarding rule.
Incoming End Port	Enter the ending port number for incoming traffic for the port forwarding rule.
Forwarding Start Port	Enter the starting port number for forwarded traffic for the port forwarding rule.
Forwarding End Port	Enter the ending port number for forwarded traffic for the port forwarding rule.
Server IP	Enter the port forwarding server IP address.

7.15 Port Trigger

Use these settings to automate port forwarding and allow computers on local network to provide services that would normally require a fixed address on the local network.

Click **Network Setting > NAT > Port Trigger** to open this screen as shown next.

Figure 57 Port Trigger Screen



This screen contains the following fields:

Table 40 Port Trigger

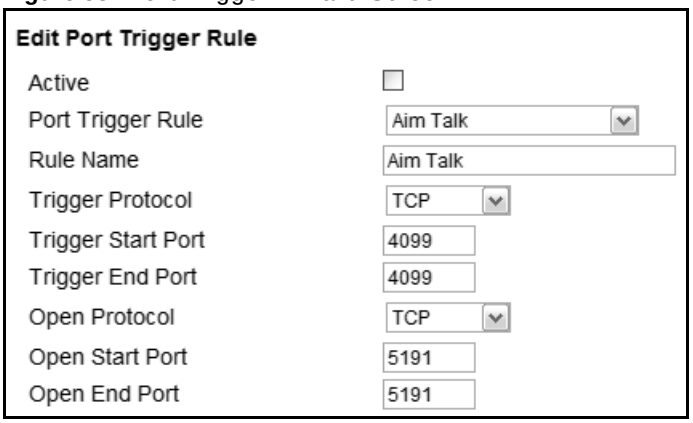
LABEL	DESCRIPTION
Active	This indicates whether the port trigger rule is active or not.
Name	The displays the name of the port trigger rule.
Trigger Protocol	This displays the protocol to which the port trigger rule applies.
Trigger Port(s)	
Start / End Port	This displays the start / end trigger port for the port trigger rule. Click **Add** to create a new, empty rule, then enter the incoming port number or range of port numbers you want to forward to the IP address the WiMAX Device records. To forward one port number, enter the port number in the **Start Port** and **End Port** fields. To forward a range of ports, • enter the port number at the beginning of the range in the **Start Port** field • enter the port number at the end of the range in the **End Port** field. If you want to delete this rule, click the **Delete** icon.
Open Protocol	This indicates which protocol is used to open the port trigger ports.
Open Port(s)	
Start / End Port	This displays the start / end open port for the port trigger rule. Click **Add** to create a new, empty rule, then enter the outgoing port number or range of port numbers that makes the WiMAX Device record the source IP address and assign it to the selected incoming port number(s). To select one port number, enter the port number in the **Start Port** and **End Port** fields. To select a range of ports, • enter the port number at the beginning of the range in the **Start Port** field • enter the port number at the end of the range in the **End Port** field. If you want to delete this rule, click the **Delete** icon.
Delete	Click this to delete a specified rule.
Wizard	Click this to open the port trigger “wizard”.
Add	Click this to add a new port trigger rule.
OK	Click this to save any changes made to the port trigger list.

7.15.1 Port Trigger Wizard

Use the wizard to create a port trigger rules that will allow the WiMAX Device to automate port forwarding and allow computers on local network to provide services that would normally require a fixed address on the local network.

Click Network Setting > NAT > Port Trigger > Wizard

Figure 58 Port Trigger Wizard Screen



This screen contains the following fields:

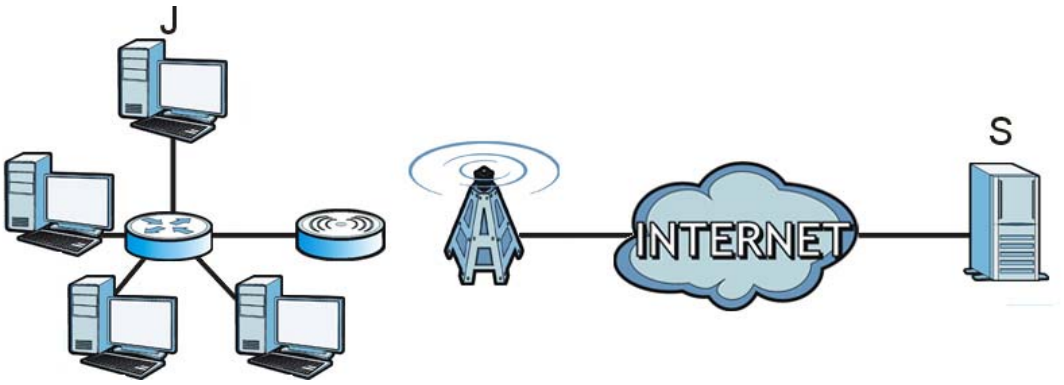
Table 41 Port Trigger Wizard

LABEL	DESCRIPTION
Active	Select this to make this port trigger rule active.
Port Trigger Rule	Select the type of port trigger rule.
Rule Name	Enter a name for the port trigger rule.
Trigger Protocol	Select the type of port trigger protocol.
Trigger Start Port	Enter the port trigger start port.
Trigger End Port	Enter the port trigger end port.
Open Protocol	Select the type of open protocol for the port trigger rule.
Open Start Port	Select the starting open port for the port trigger rule.
Open End Port	Select the ending open port number for the port trigger rule.

7.15.2 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 59 Trigger Port Forwarding Example



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

Two points to remember about trigger ports:

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

7.16 DMZ

Use this page to set the IP address of your network DMZ (if you have one) for the WiMAX Device. All incoming packets received by this WiMAX Device's WAN interface will be forwarded to the DMZ host you set.

Click **Network Setting > NAT > DMZ** to open this screen as shown next.

Note: The configuration you set in this screen takes priority than the **Network Setting > NAT > Port Forwarding** screen.

Figure 60 DMZ Screen

This screen contains the following fields:

Table 42 DMZ

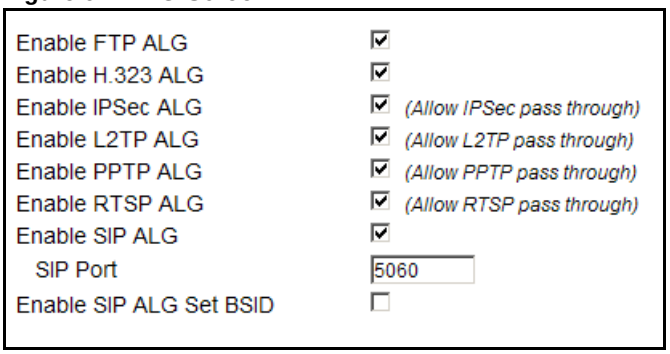
LABEL	DESCRIPTION
DMZ Enable	Click this check box to enable DMZ.
DMZ Host	Enter the IP address of your network DMZ host, if you have one. **0.0.0.0** means this feature is disabled.

7.17 ALG

Use these settings to bypass NAT on your WiMAX Device for those applications that are "NAT unfriendly".

Click **Network Setting > NAT > ALG** to open this screen as shown next.

Figure 61 ALG Screen



This screen contains the following fields:

Table 43 ALG

LABEL	DESCRIPTION
Enable FTP ALG	Turns on the FTP ALG to detect FTP (File Transfer Program) traffic and helps build FTP sessions through the WiMAX Device's NAT.
Enable H.323 ALG	Turns on the H.323 ALG to detect H.323 traffic (used for audio communications) and helps build H.323 sessions through the WiMAX Device's NAT.
Enable IPsec ALG	Turns on the IPsec ALG to detect IPsec traffic and helps build IPsec sessions through the WiMAX Device's NAT.
Enable L2TP ALG	Turns on the L2TP ALG to detect L2TP traffic and helps build L2TP sessions through the WiMAX Device's NAT.
Enable PPTP ALG	Turns on the PPTP ALG to detect PPTP traffic and helps build PPTP sessions through the WiMAX Device's NAT.

Table 43 ALG (continued)

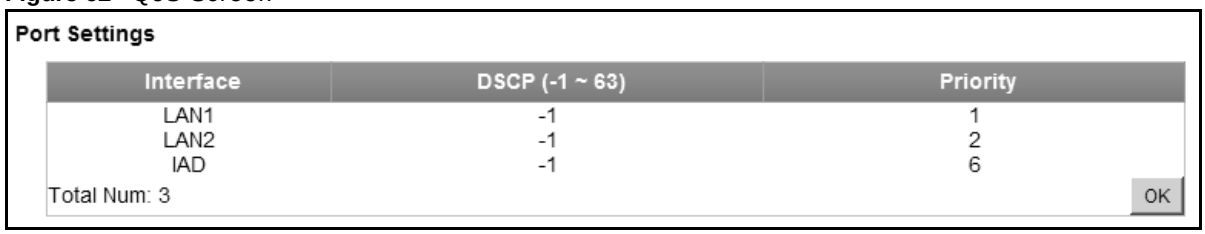
LABEL	DESCRIPTION
Enable RTSP ALG	Turns on the RTSP ALG to detect RTSP traffic and helps build RTSP sessions through the WiMAX Device's NAT.
Enable SIP ALG	Turns on the SIP ALG to detect SIP traffic and helps build SIP sessions through the WiMAX Device's NAT.
SIP Port	If you are using a custom UDP port number (not 5060) for SIP traffic, enter it here.
Enable SIP ALG Set BSID	Check this box to add the base station ID to the outgoing SIP messages. Select this option only if the media server forwarding calls requires this information.

7.18 QoS

Use this page to configure QoS settings on the WiMAX Device.

Click **Network Setting > QoS** to open this screen as shown next.

Figure 62 QoS Screen



This screen contains the following fields:

Table 44 QoS

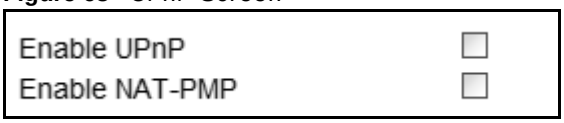
LABEL	DESCRIPTION
Interface	This displays the interface for the QoS rule. The **IAD** interface is for device management. Configure DiffServ Code Point (DSCP) and/or Priority marking based on which method is supported within your network. With DSCP you can use 64 (0-63) different markings, compared to 6 (1-6) with Priority marking.
DSCP	Specify a DiffServ Code Point (**DSCP**) classification identification number (-1-63) to mark traffic that passes through this interface. Setting the **DSCP** to -1 indicates marking is not enabled. A higher number indicates higher priority. The **DSCP** allows marked packets to receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow.
Priority	Select a priority level (1 to 6) to assign a priority to traffic that passes through this interface. A higher number indicates higher priority. Like DSCP, this marking is used to identify traffic for specific treatment.
OK	Click this to save any changes made to the QoS rules.

7.19 UPnP

Use this page to enable the UPnP networking protocol on your WiMAX Device and allow easy network connectivity with other UPnP-compatible devices.

Click **Network Setting > UPnP** to open this screen as shown next.

Figure 63 UPnP Screen



This screen contains the following fields:

Table 45 UPnP

LABEL	DESCRIPTION
Enable UPnP	Select this to enable UPnP on the WiMAX Device.
Enable NAT-PMP	Select this to enable NAT Port Mapping Protocol on the WiMAX Device.

7.19.1 Installing UPnP in Windows XP

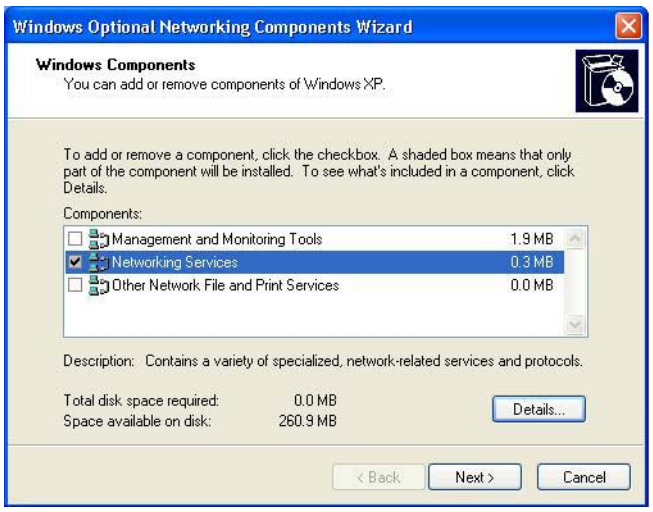
Follow the steps below to install the UPnP in Windows XP.

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

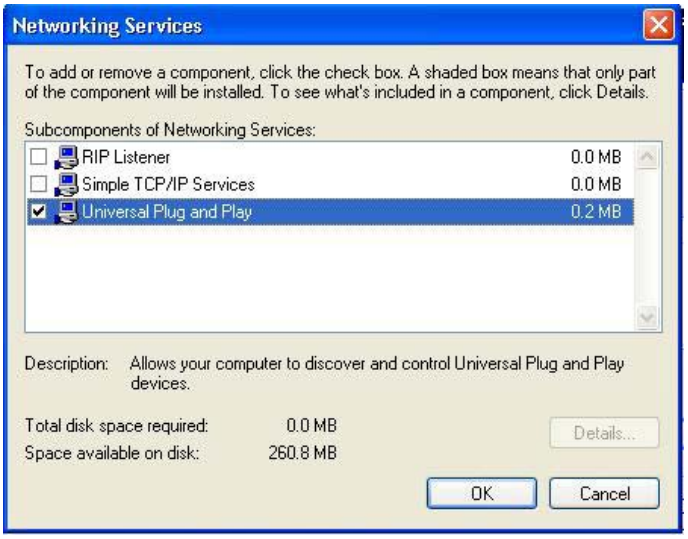
2 Double-click **Network Connections**.

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

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



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



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

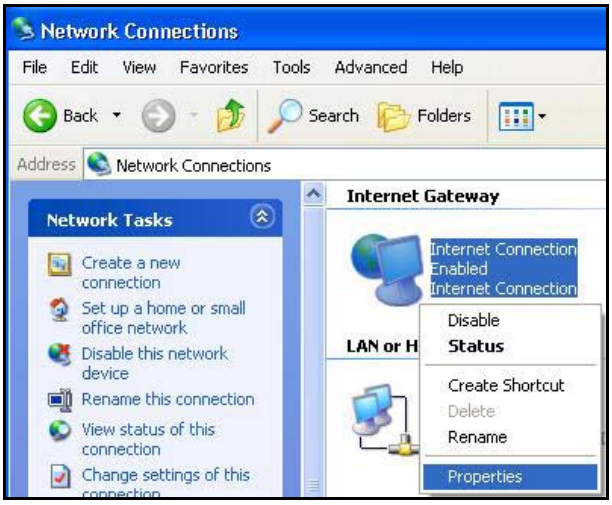
7.19.1.1 Auto-discover Your UPnP-enabled Network Device in Windows XP

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

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

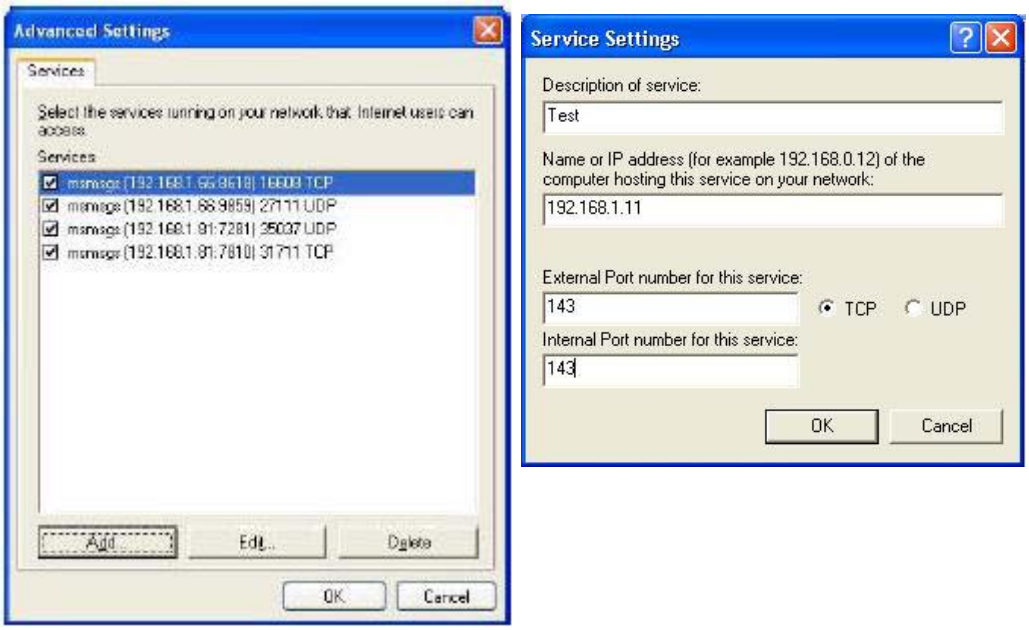
1 Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.

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



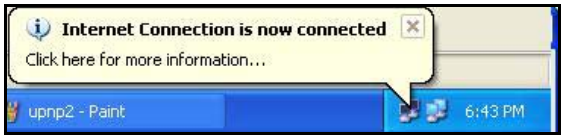
3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings there were automatically created.

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



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.



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

7.19.2 Web Configurator Easy Access

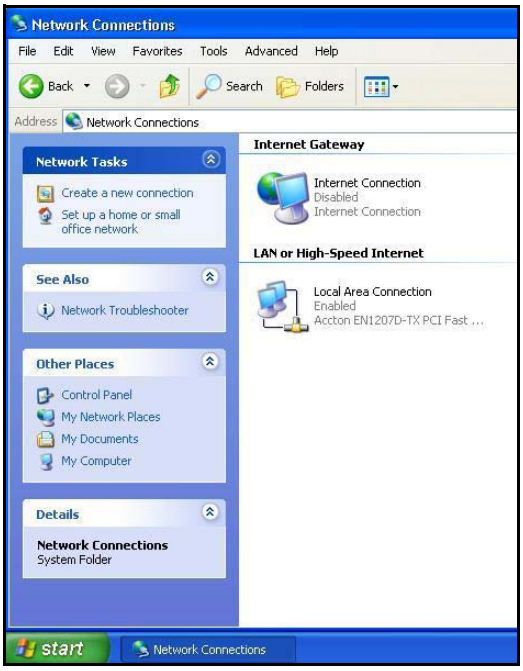
With UPnP, you can access the web-based configurator on the WiMAX Device without finding out the IP address of the WiMAX Device first. This becomes helpful if you do not know the IP address of the WiMAX Device.

Follow the steps below to access the web configurator:

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

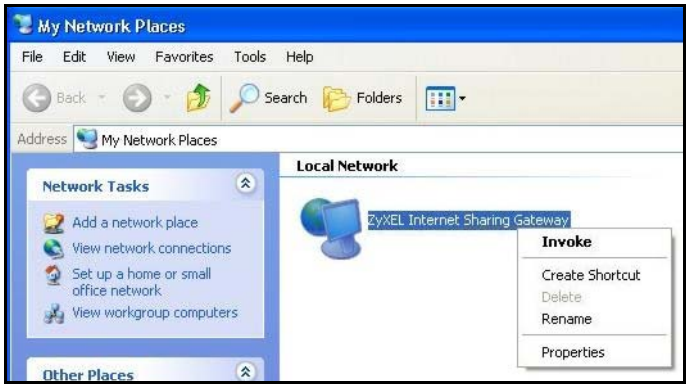
2 Double-click **Network Connections**.

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



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

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



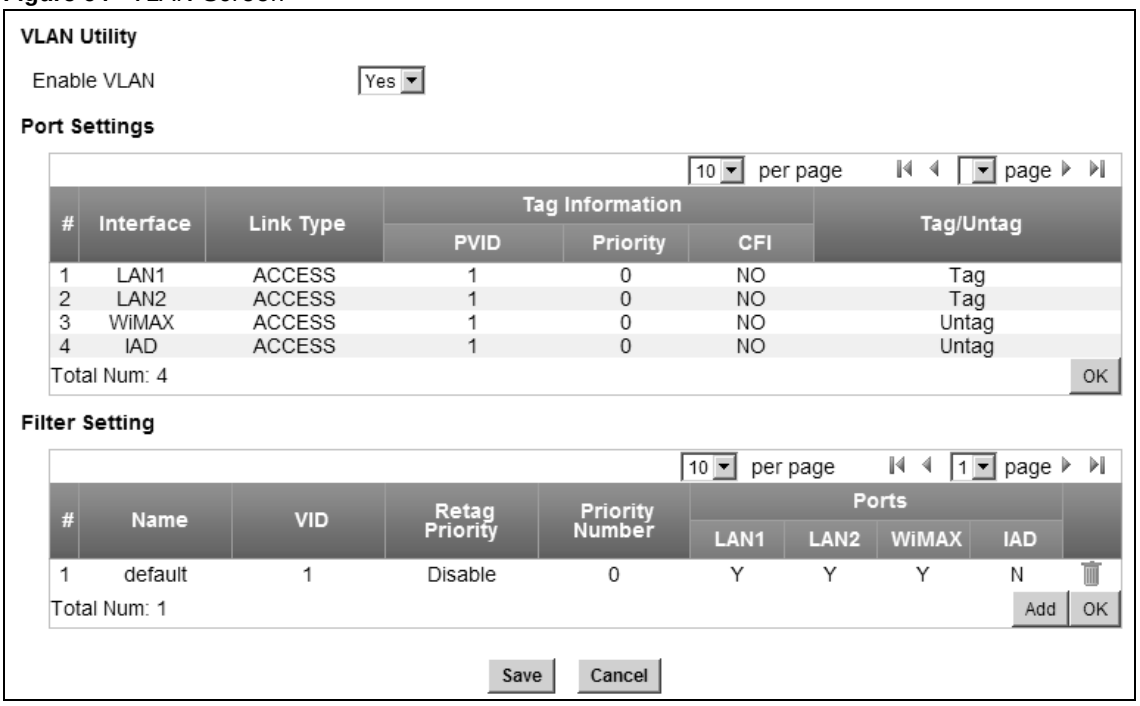
6 Right-click on the icon for your WiMAX Device and select **Properties**. A properties window displays with basic information about the WiMAX Device.

7.20 VLAN

Use this screen to configure port-based VLAN settings on the WiMAX Device. This screen allows you to assign port(s) to specific virtual LAN(s) in order to isolate traffic from different VLAN groups. See Section 4.12 on page 50 for example configurations for VLANs.

Click **Network Setting > VLAN** to open the screen as shown next.

Figure 64 VLAN Screen



This screen contains the following fields:

Table 46 VLAN

LABEL	DESCRIPTION
VLAN Utility	
Enable VLAN	Select **Yes** to enable the VLAN function on the WiMAX Device. Note: To use VLAN on the WiMAX Device, you must switch the operation mode to "bridge" on the **Network Setting > WAN** screen. It will then require system restart to take effect.
Port Settings	
#	This is the index number of the port setting.
Interface	This displays the interface that the port setting applies to.
Link Type	Select **Access** if this port forwards traffic for only one VLAN. The device connected to an access port does not support VLAN tagged packets, so the WiMAX Device will remove packets forwarded out of this port. Packets received on access ports will be tagged with the specified PVID. Select **Trunk** to allow packets belonging to different VLAN groups to pass through the port. The device connected to this port should support VLAN tagged packets. You must configure **Filter Settings** for the port and VLAN ID for tagged packets to be forwarded. If received packets are already tagged, the PVID set for this port should not be the same as the VLAN IDs configured in **Filter Settings**. This will allow the tagged packets to be forwarded to the specified VLANs. If received packets are not tagged, the WiMAX Device will tag them with the PVID. Select **Hybrid** to allow the port to function as an access port and trunk port.
PVID	A **PVID** (Port VLAN ID) is a tag that adds to incoming untagged packets received on a port so that the packets are forwarded to the VLAN group that the tag defines. Enter a number between 1and 4094 as the port VLAN ID.

Table 46 VLAN (continued)

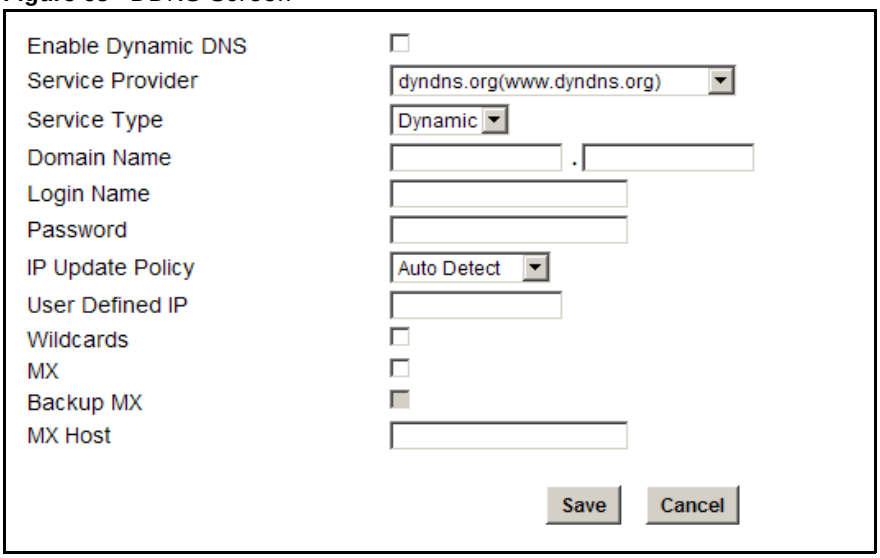
LABEL	DESCRIPTION
Priority	Enter a priority level (1~7) that the WiMAX Device assigns to packets belonging to this VLAN. Enter "0" for no priority assigned.
CFI	Select **Yes** if the CFI (Canonical Format Indicator) field in a received packet is set to 1, indicating non-Canonical Format. In this case, the packet should not be forwarded as it is to an untagged port.
Tag/Untag	You can only select **Tag** if the port is configured as a **Trunk** or **Hybrid** port. The WiMAX Device will receive and forward VLAN tagged packets. Untagged packets will be tagged with the PVID. If you select **Untag** the WiMAX Device will remove tags from tagged packets it forwards out of the port. Untagged packets received will be forwarded. If the port is an **Access** port, the WiMAX Device will add tags to untagged packets it receives and drop tagged packets it receives. If the port is a **Trunk** port, the WiMAX Device will add tags to untagged packets it receives and retag tagged packets.
OK	Click this to save the changes in the **Port Setting** section.
Filter Setting	
#	This is the index number of a filter.
Name	This is the name of a filter rule.
VID	This field displays the VLAN ID for the filter. Click this field to change the VLAN ID.
Retag Priority	Select **Yes** to retag the priority of a packet received on a **Trunk** or **Hybrid** port.
Priority Number	If Retag Priority is enabled, specify the new priority level (1~7) to tag. Enter "0" for no priority assigned.
Ports	This field displays the ports included in the filter. Click this field to select which ports to include.
Delete	Click this button to remove an item from the list.
Add	Click this button to add an item to the list.
OK	Click this button to save any changes made to the list.
Save	Click this to save the changes made.
Cancel	Click this avoid any changes made from being saved to your configuration.

7.21 DDNS

Use this page to configure the WiMAX Device as a dynamic DNS client.

Click Network Setting > DDNS

Figure 65 DDNS Screen



This screen contains the following fields:

Table 47 DDNS

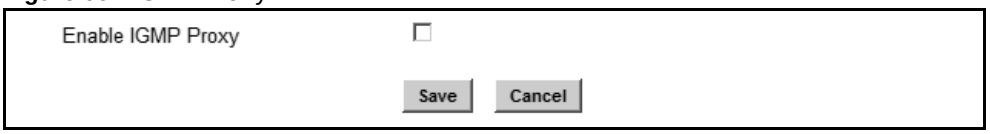
LABEL	DESCRIPTION
Enable Dynamic DNS	Select this to enable dynamic DNS on the WiMAX Device.
Service Provider	Select the dynamic DNS service provider for the WiMAX Device.
Service Type	Select the dynamic DNS service type.
Domain Name	Enter the domain name.
Login Name	Enter the user name.
Password	Enter the password.
IP Update Policy	Select the policy used by the WiMAX Device. Options are: • Auto Detect • WAN • User Defined
User Defined IP	If chose “User Defined” for the **IP Update Policy**, enter the user defined IP address.
Wildcards	Select this to allow a hostname to use wildcards such as “*”.
MX	Select this to enable mail routing, if supported by the specified DYNDNS service provider.
Backup MX	Select this to enable a secondary mail routing, if supported by the specified DYNDNS service provider.
MX Host	Enter the host to which mail is routed when the MX option is selected.

7.22 IGMP Proxy

IGMP proxy allows the WiMAX Device to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly. Use this screen to enable IGMP Proxy on the WiMAX Device.

Click **Network Setting > IGMP Proxy** to open this screen as shown next.

Figure 66 IGMP Proxy



This screen contains the following fields:

Table 48 IGMP Proxy

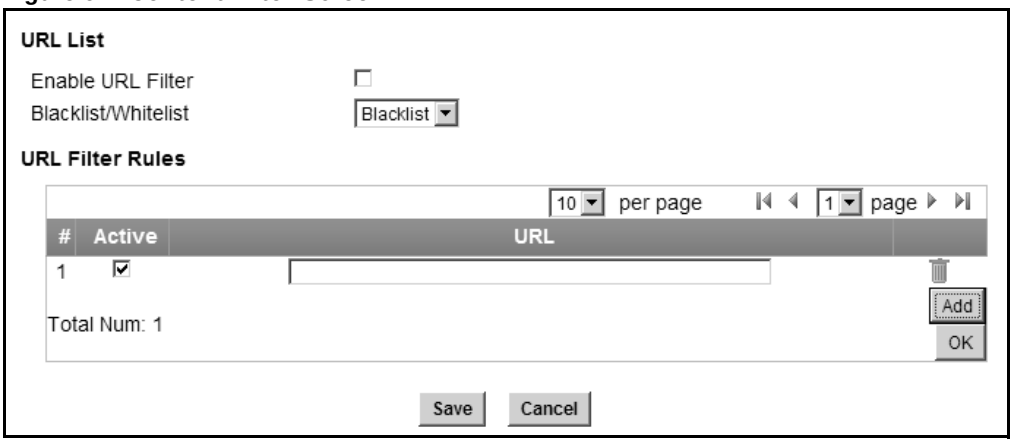
LABEL	DESCRIPTION
Enable IGMP Proxy	Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. Select this option to have the WiMAX Device act as an IGMP proxy. This allows the WiMAX Device to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Save	Click this to save the changes made.
Cancel	Click this avoid any changes made from being saved to your configuration.

7.23 Content Filter

Use these settings to allow ("whitelist") or block ("blacklist") connections to and from specific web sites through the WiMAX Device.

Click **Network Setting > Content Filter** to open this screen as shown next.

Figure 67 Content Filter Screen



This screen contains the following fields:

Table 49 Content Filter

LABEL	DESCRIPTION
URL List	
Enable URL Filter	Select this employ the content filter to allow (“whitelist”) or block (“blacklist”) specific URL connections made through the WiMAX Device.
Blacklist/ Whitelist	Select whether the current filtering applies to the blacklist (sites that are blocked) or the whitelist (sites that are allowed).
URL Filter Rule	
Active	Indicates whether the current URL filter is active or not.
URL	Indicates the URL to be filtered according to blacklist or whitelist rules.
Delete	Click this to delete a specified rule.
Add	Click this to add a new filter rule.
OK	Click this to save any changes made to the list.

8

Security

8.1 Overview

This chapter shows you how to configure the WiMAX Device's network settings.

8.1.1 What You Need to Know

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

About the WiMAX Device's Security Features

The WiMAX Device security features are designed to protect against Denial of Service attacks when activated as well as block access to and from specific URLs and MAC addresses. Its purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The WiMAX Device can be used to prevent theft, destruction and modification of data.

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

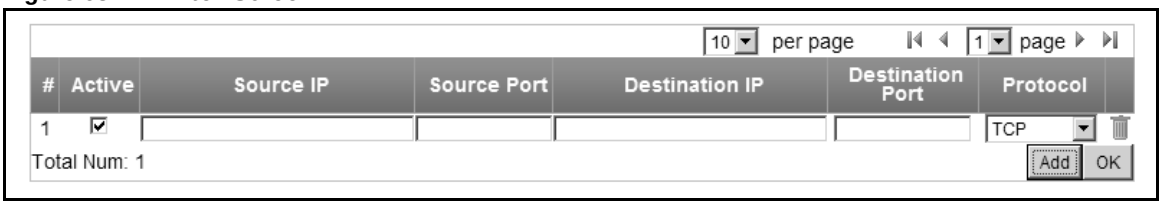
The WiMAX Device has one Ethernet (LAN) port. The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers will have access to Internet services such as e-mail, FTP and the World Wide Web. However, "inbound access" is not allowed (by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

8.2 IP Filter

Use this screen to block incoming connections from specific IP addresses.

Click **Security > Firewall > IP Filter** to open this screen as shown next.

Figure 68 IP Filter Screen



This screen contains the following fields:

Table 50 IP Filter

LABEL	DESCRIPTION
Active	Indicates whether the current IP filter is active or not.
Source IP	This displays the source IP address for the IP filter rule. Click **Add** to create a new, empty rule, then enter the incoming IP address for the WiMAX Device to block. If you want to delete this rule, click the **Delete** icon.
Source Port	This displays the source port number for the IP filter rule. Click **Add** to create a new, empty rule, then enter the incoming port number for the WiMAX Device to block. If you want to delete this rule, click the **Delete** icon.
Destination IP	This displays the destination IP address for the IP filter rule. Click **Add** to create a new, empty rule, then enter the outgoing IP address for the WiMAX Device to block. If you want to delete this rule, click the **Delete** icon.
Destination Port	This displays the destination port number for the IP filter rule. Click **Add** to create a new, empty rule, then enter the outgoing port number for the WiMAX Device to block. If you want to delete this rule, click the **Delete** icon.
Protocol	This displays the protocol blocked by the IP filter rule. Click **Add** to create a new, empty rule, then select the protocol type for the WiMAX Device to block. If you want to delete this rule, click the **Delete** icon.
Delete	Click this to delete a specified rule.
Add	Click this to add a new filter rule.
OK	Click this to save any changes made to the list.

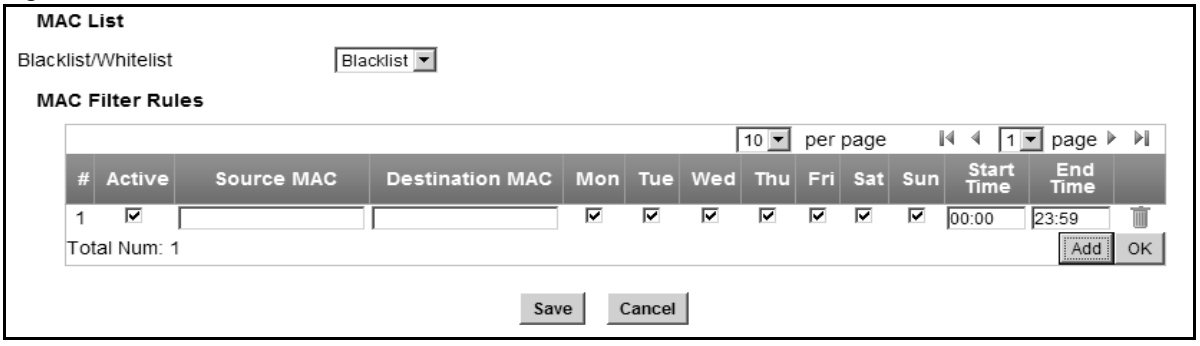
8.3 MAC Filter

Use this screen to allow ("whitelist") or block ("blacklist") connections to and from specific devices on the network based on their unique MAC addresses.

Note: This feature only works when the WiMAX Device is in bridge mode.

Click **Security > Firewall > MAC Filter** to open this screen as shown next.

Figure 69 MAC Filter Screen



This screen contains the following fields:

Table 51 MAC Filter

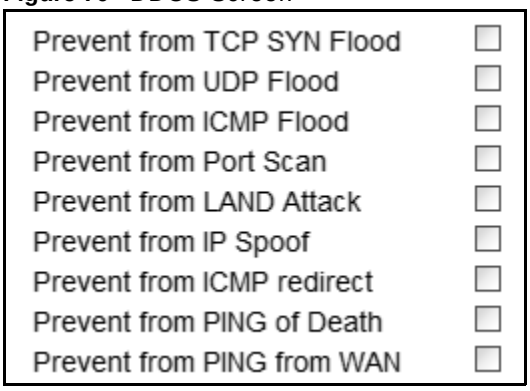
LABEL	DESCRIPTION
Blacklist/Whitelist	Select either whitelist or blacklist for viewing and editing.
Source MAC	This displays the source MAC for the MAC filter rule. Click **Add** to create a new, empty rule, then enter the incoming MAC address for the WiMAX Device to block. If you want to delete this rule, click the **Delete** icon.
Destination MAC	This displays the destination MAC for the MAC filter rule. Click **Add** to create a new, empty rule, then enter the outgoing MAC address for the WiMAX Device to block. If you want to delete this rule, click the **Delete** icon.
Mon ~ Sun	Select which days of the week you want the filter rule to be effective.
Start / End Time	Select what time each day you want the filter rule to be effective. Enter times in 24-hour format; for example, 3:00pm should be entered as 15:00.
Add	Click this to add a new filter rule.
OK	Click this to save any changes made to the list.

8.4 DDOS

Use these settings to potentially block specific types of Denial of Service attacks directed at your WiMAX Device.

Click **Security > Firewall > DDOS** to open this screen as shown next.

Figure 70 DDOS Screen



This screen contains the following fields:

Table 52 DDOS

LABEL	DESCRIPTION
Prevent from TCP SYN Flood	Select this to monitor for and block TCP SYN flood attacks. A SYN flood is one type of denial of service attack where an overwhelming number of SYN requests assault a client device.
Prevent from UDP Flood	Select this to monitor for and block UDP flood attacks. An UDP flood is a type of denial of service attack where an overwhelming number of UDP packets assault random ports on a client device. Because the device is forced to analyze and respond to each packet, it quickly becomes unreachable to other devices.
Prevent from ICMP Flood	Select this to monitor for and block ICMP flood attacks. An ICMP flood is a type of denial of service attack where an overwhelming number of ICMP ping assault a client device, locking it down and preventing it from responding to requests from other servers.
Prevent from Port Scan	Select this to monitor for and block port scan attacks. A port scan attack is typically the precursor to a full-blown denial of service attack wherein each port on a device is probed for security holes that can be exploited. Once a security flaw is discovered, an attacker can initiate the appropriate denial of service attack or intrusion attack against the client device.
Prevent from LAND Attack	Select this to monitor for and block LAND attacks. A Local Area Network Denial (LAND) attack is a type of denial of service attack where a spoofed TCP SYN packet targets a client device's IP address and forces it into an infinite recursive loop of querying itself and then replying, effectively locking it down.
Prevent from IP Spoof	Select this to monitor for and block IP address spoof attacks. An IP address spoof is an attack whereby the source IP address in the incoming IP packets allows a malicious party to masquerade as a legitimate user and gain access to the client device.
Prevent from ICMP redirect	Select this to monitor for and block ICMP redirect attacks. An ICMP redirect attack is one where forged ICMP redirect messages can force the client device to route packets for certain connections through an attacker's host.

Table 52 DDOS (continued)

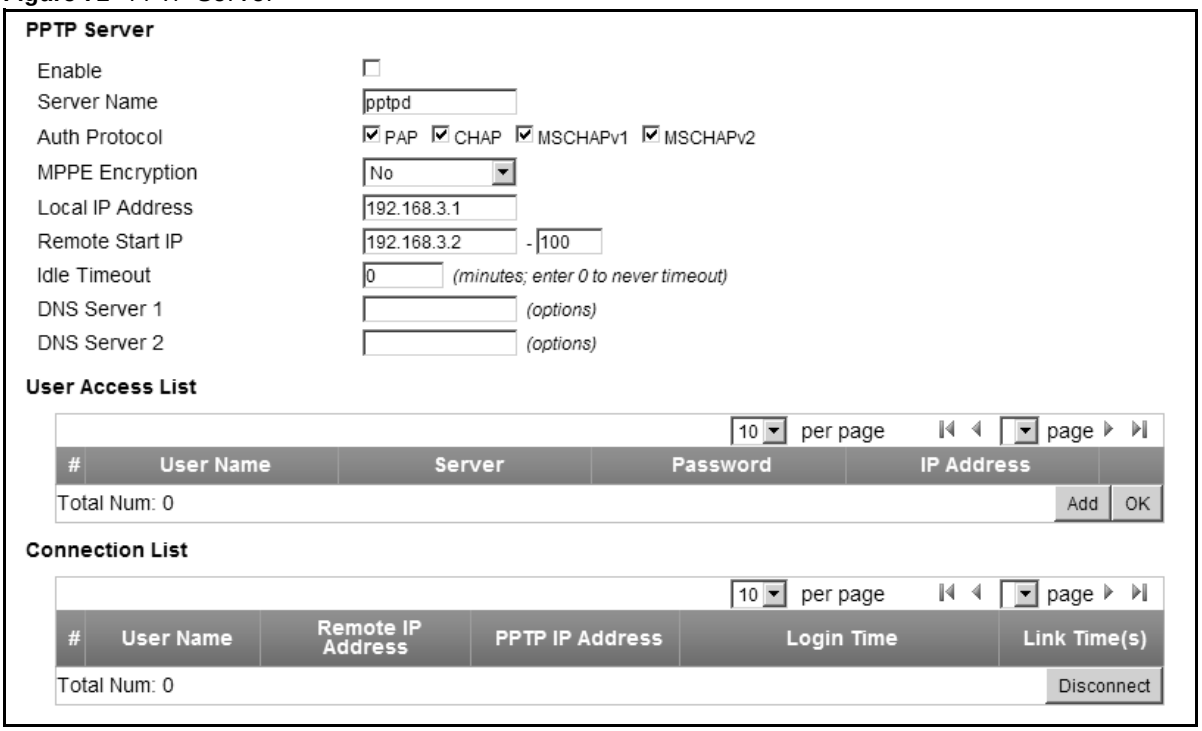
LABEL	DESCRIPTION
Prevent from PING of Death	Select this to monitor for and block ping of death attacks. A Ping of Death (POD) attack is one where larger-than-allowed ping packets are fragmented then sent against a client device. This results in the client device suffering from a buffer overflow and subsequent system crash.
Prevent from PING from WAN	Select this to ignore ping requests from the WAN.

8.5 PPTP VPN Server

Use this screen to configure settings for a Point to Point Tunneling Protocol (PPTP) server.

Click **Security > PPTP VPN > PPTP Server** to open this screen as shown next.

Figure 71 PPTP Server



This screen contains the following fields:

Table 53 PPTP Server

LABEL	DESCRIPTION
PPTP Server	
Enable	Use this field to turn the WiMAX Device'S PPTP VPN function on or off.
Server Name	Enter the server name for the PPTP VPN connection.

Table 53 PPTP Server (continued)

LABEL	DESCRIPTION
Auth Protocol	Select the Authentication Protocol allowed for the connection. Options are: • **PAP** - Password Authentication Protocol (PAP) authentication occurs in clear text and does not use encryption. It's probably not a good idea to rely on this for security. • **CHAP** - Challenge Handshake Authentication Protocol (CHAP) provides authentication through a shared secret key and uses a three way handshake. • **MSCHAPv1** - Microsoft CHAP v1 (MSCHAPv1) provides authentication through a shared secret key and uses a three way handshake. It provides improved usability with Microsoft products. • **MSCHAPv2** - Microsoft CHAP v2 (MSCHAPv2) provides encryption through a shared secret key and uses a three way handshake. It provides additional security over **MSCHAPv1**, including two-way authentication.
MPPE Encryption	If **MSCHAPv1** or **MSCHAPv2** is selected as an **Auth Protocol**, use the drop-down list box to select the type of Microsoft Point-to-Point Encryption (MPPE). Options are: • **MPPE 40 bits -** MPPE with 40 bit session key length • **MPPE 128 bits -** MPPE with 128 bit session key length • Auto - Automatically select either MPPE 40 bits or MPPE 128 bits
Local IP Address	Enter the local endpoint for the PPTP connection.
Remote Start IP	Enter the local IP address range the WiMAX Device assigns to remote users if the remote client device is set to obtain an IP address automatically.
Idle Timeout	Enter the time in minutes to timeout PPTP connections.
DNS Server 1 DNS Server 2	Specify the IP addresses of DNS servers to assign to the remote users.
User Access List	
User Name	Enter the user name for the remote user.
Server	Select the server that the remote user has access to: **PPTPD**, **L2TPD** or **Both**.
Password	Enter the password for the remote user.
IP Address	Enter the local IP address the WiMAX Device assigns to the remote user. Entering 0.0.0.0 indicates the local IP address will be dynamically assigned.
Delete	Select an entry and click this to delete it.
Add	Click this to create a new entry.
OK	Click this to save the changes.
Connection List	
User Name	This displays the user name for the remote user.
Remote IP Address	This displays the remote endpoint IP address of the remote user.
PPTP IP Address	This displays the local IP address of the PPTP server.
Login Time	This displays the time the PPTP connection started.
Link Time(s)	This displays the duration of the PPTP connection.

8.6 PPTP VPN Client

Use this screen to view settings for Point to Point Tunneling Protocol (PPTP) clients.

Click **Security > PPTP VPN > PPTP Client** to open this screen as shown next.

Figure 72 PPTP Client

This screen contains the following fields:

Table 54 PPTP Client

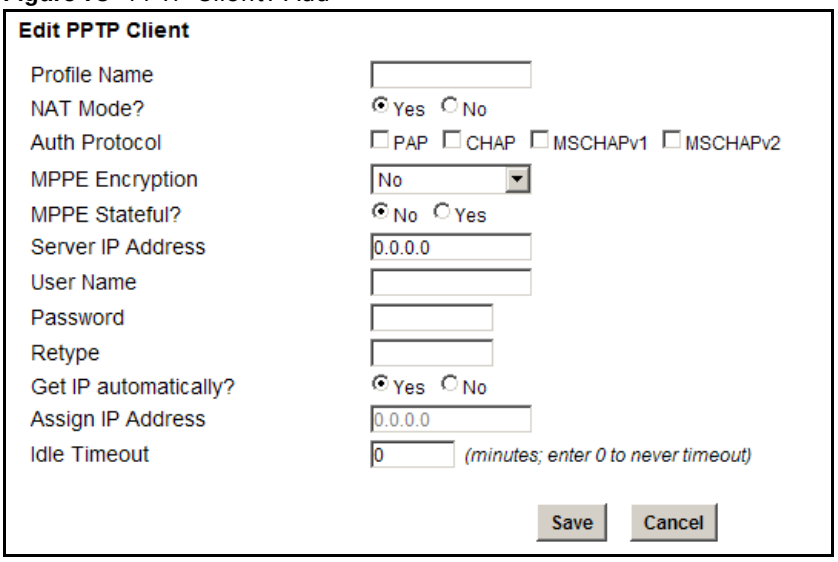
LABEL	DESCRIPTION
#	This is the index number of the connection.
Profile Name	This is the name of this client connection.
Server IP	This is the IP address of the PPTP VPN server.
Assign IP	This is the local IP address the client assigns to itself or is assigned by the server.
MTU	This field indicates the Maximum Transmission Unit (MTU) for the connection.
Status	This is the connection status.
Add	Click this to add a VPN client profile.
Edit	Click this to edit an existing VPN client profile.
Connect	Select a VPN client connection and click this to connect.
Disconnect	Select a VPN client connection and click this to disconnect.

8.7 PPTP VPN Client: Add

Use this screen to configure settings for Point to Point Tunneling Protocol (PPTP) clients.

Click **Security > PPTP VPN > PPTP Client > Add** to open this screen as shown next.

Figure 73 PPTP Client: Add



This screen contains the following fields:

Table 55 PPTP Client: Add

LABEL	DESCRIPTION
Profile Name	Enter the name for this client connection.
NAT Mode?	Select **Yes** if the client will be located behind a NAT enabled router. This will allow multiple clients using NAT to connect with PPTP at the same time.
Auth Protocol	Select the Authentication Protocol allowed for the connection. Options are: • **PAP** - Password Authentication Protocol (PAP) authentication occurs in clear text and does not use encryption. It's probably not a good idea to rely on this for security. • **CHAP** - Challenge Handshake Authentication Protocol (CHAP) provides authentication through a shared secret key and uses a three way handshake. • **MSCHAPv1** - Microsoft CHAP v1 (MSCHAPv1) provides authentication through a shared secret key and uses a three way handshake. It provides improved usability with Microsoft products. • **MSCHAPv2** - Microsoft CHAP v2 (MSCHAPv2) provides encryption through a shared secret key and uses a three way handshake. It provides additional security over **MSCHAPv1**, including two-way authentication.
MPPE Encryption	If **MSCHAPv1** or **MSCHAPv2** is selected as an **Auth Protocol**, use the drop-down list box to select the type of Microsoft Point-to-Point Encryption (MPPE). Options are: • **MPPE 40 -** MPPE with 40 bit session key length. • **MPPE 128 -** MPPE with 128 bit session key length. • **Auto -** Automatically select either **MPPE 40** or **MPPE 128**.
MPPE Stateful?	Select **Yes** to enable stateful MPPE encryption. This can increase performance over stateless MPPE, but should not be used in lossy network environments like layer two tunnels over the Internet.
Server IP Address	Enter the IP address of the PPTP server.
User Name	Enter the user name for connecting to the PPTP server.
Password	Enter the password for connecting to the PPTP server.
Retype	Retype the password for connecting to the PPTP server.

Table 55 PPTP Client: Add (continued)

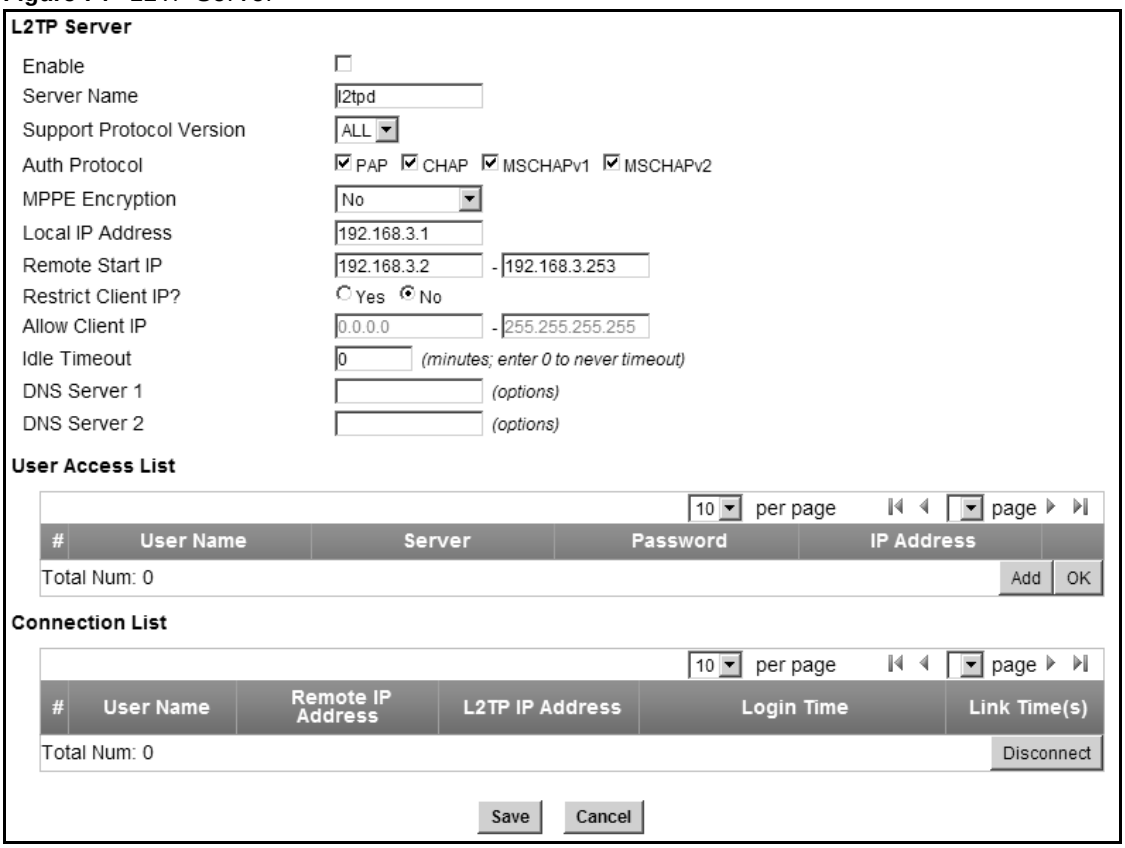
LABEL	DESCRIPTION
Get IP automatically	Select **Yes** to have the PPTP server assign a local IP address to the client.
Assign IP Address	Enter the IP address for the client. Ensure that the IP address is configured to be allowed on the PPTP server.
Idle Timeout	Enter the time in minutes to timeout PPTP connections.

8.8 L2TP VPN Server

Use this screen to configure settings for Layer 2 Tunneling Protocol (L2TP) server.

Click **Security > L2TP VPN > L2TP Server** to open this screen as shown next.

Figure 74 L2TP Server



This screen contains the following fields:

Table 56 L2TP Server

LABEL	DESCRIPTION
L2TP Server	
Enable	Use this field to turn the WiMAX Device'S L2TP VPN function on or off.
Server Name	Enter the server name for the L2TP VPN connection.

Table 56 L2TP Server (continued)

LABEL	DESCRIPTION
Support Protocol Version	Select the L2TP Protocol Version: **All**, **2**, or **3**. L2TPv2 is a standard method for tunneling Point-to-Point Protocol (PPP) while L2TPv3 provides improved support for other types of networks including frame relay and ATM.
Auth Protocol	Select the Authentication Protocol allowed for the connection. Options are: • **PAP** - Password Authentication Protocol (PAP) authentication occurs in clear text and does not use encryption. It's probably not a good idea to rely on this for security. • **CHAP** - Challenge Handshake Authentication Protocol (CHAP) provides authentication through a shared secret key and uses a three way handshake. • **MSCHAPv1** - Microsoft CHAP v1 (MSCHAPv1) provides authentication through a shared secret key and uses a three way handshake. It provides improved usability with Microsoft products. • **MSCHAPv2** - Microsoft CHAP v2 (MSCHAPv2) provides encryption through a shared secret key and uses a three way handshake. It provides additional security over **MSCHAPv1**, including two-way authentication.
MPPE Encryption	If **MSCHAPv1** or **MSCHAPv2** is selected as an **Auth Protocol**, use the drop-down list box to select the type of Microsoft Point-to-Point Encryption (MPPE). Options are: • **MPPE 40 -** MPPE with 40 bit session key length • **MPPE 128 -** MPPE with 128 bit session key length • Auto - Automatically select either MPPE 40 or MPPE 128
Local IP Address	Enter the local endpoint for the L2TP connection.
Remote Start IP	Enter the local IP address range the WiMAX Device assigns to remote users if the remote client device is set to obtain an IP address automatically.
Restrict Client IP?	Select **Yes** to restrict the remote client device local IP address.
Allow Client IP	Enter the local IP address range the remote client device is restricted to. If the client device is configured with a static IP address, it should be in this range.
Idle Timeout	Enter the time in minutes to timeout L2TP connections.
DNS Server 1 DNS Server 2	Specify the IP addresses of DNS servers to assign to the remote users.
User Access List	
User Name	Enter the user name for the remote user.
Server	Select the server that the remote user has access to: **PPTPD**, **L2TPD** or **Both**.
Password	Enter the password for the remote user.
IP Address	Enter the local IP address the WiMAX Device assigns to the remote user. Entering 0.0.0.0 indicates the local IP address will be dynamically assigned.
Delete	Select an entry and click this to delete it.
Add	Click this to create a new entry.
OK	Click this to save the changes.
Connection List	
User Name	This displays the user name for the remote user.
Remote IP Address	This displays the remote endpoint IP address of the remote user.
L2TP IP Address	This displays the local IP address of the L2TP server.
Login Time	This displays the time the L2TP connection started.

Table 56 L2TP Server (continued)

LABEL	DESCRIPTION
Link Time(s)	This displays the duration of the L2TP connection.
Disconnect	Select a client and click this button to disconnect the selected client.

8.9 L2TP VPN Client

Use this screen to view settings for Layer 2 Tunneling Protocol (L2TP) clients.

Click **Security > L2TP VPN > L2TP Client** to open this screen as shown next.

Figure 75 L2TP Client

This screen contains the following fields:

Table 57 L2TP Client

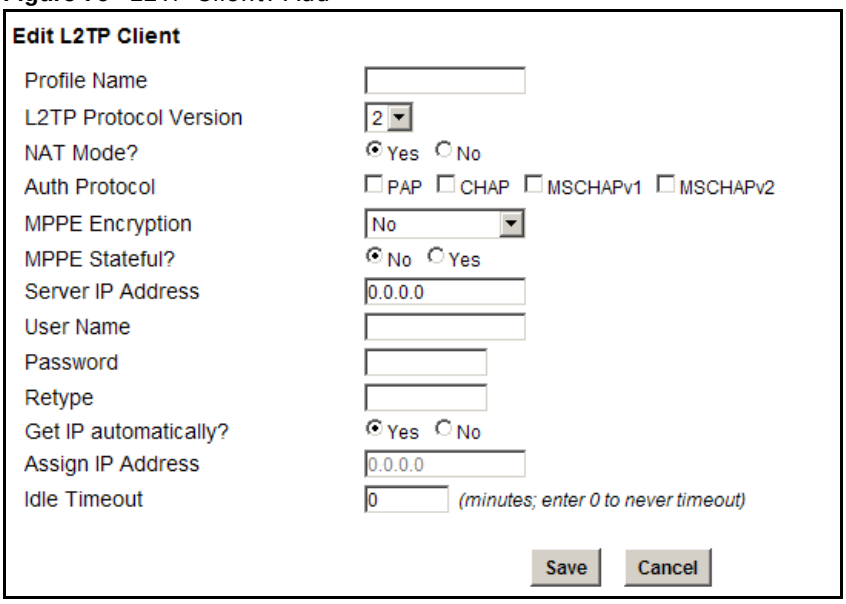
LABEL	DESCRIPTION
#	This is the index number of the connection.
Profile Name	This is the name of this client connection.
Server IP	This is the IP address of the L2TP VPN server.
Assign IP	This is the local IP address the client assigns to itself or is assigned by the server.
MTU	This field indicates the Maximum Transmission Unit (MTU) for the connection.
Status	This is the connection status.
Add	Click this to add a VPN client profile.
Edit	Click this to edit an existing VPN client profile.
Connect	Select a VPN client connection and click this to connect.
Disconnect	Select a VPN client connection and click this to disconnect.

8.10 L2TP VPN Client: Add

Use this screen to configure settings for Layer 2 Tunneling Protocol (L2TP) clients.

Click **Security > L2TP VPN > L2TP Client > Add** to open this screen as shown next.

Figure 76 L2TP Client: Add



This screen contains the following fields:

Table 58 L2TP Client: Add

LABEL	DESCRIPTION
Profile Name	Enter the name for this client connection.
L2TP Protocol Version	Select the L2TP Protocol Version **2** or **3**. L2TPv2 is a standard method for tunneling Point-to-Point Protocol (PPP) while L2TPv3 provides improved support for other types of networks including frame relay and ATM.
NAT Mode?	Select **Yes** if the client will be located behind a NAT enabled router. This will allow multiple clients using NAT to connect with L2TP at the same time.
Auth Protocol	Select the Authentication Protocol allowed for the connection. Options are: • **PAP** - Password Authentication Protocol (PAP) authentication occurs in clear text and does not use encryption. It's probably not a good idea to rely on this for security. • **CHAP** - Challenge Handshake Authentication Protocol (CHAP) provides authentication through a shared secret key and uses a three way handshake. • **MSCHAPv1** - Microsoft CHAP v1 (MSCHAPv1) provides authentication through a shared secret key and uses a three way handshake. It provides improved usability with Microsoft products. • **MSCHAPv2** - Microsoft CHAP v2 (MSCHAPv2) provides encryption through a shared secret key and uses a three way handshake. It provides additional security over **MSCHAPv1**, including two-way authentication.
MPPE Encryption	If **MSCHAPv1** or **MSCHAPv2** is selected as an **Auth Protocol**, use the drop-down list box to select the type of Microsoft Point-to-Point Encryption (MPPE). Options are: • **MPPE 40 bits -** MPPE with 40 bit session key length • **MPPE 128 bits -** MPPE with 128 bit session key length • **Auto -** Automatically select either **MPPE 40 bits** or **MPPE 128 bits**
MPPE Stateful?	Select **Yes** to enable stateful MPPE encryption. This can increase performance over stateless MPPE, but should not be used in lossy network environments like layer two tunnels over the Internet.
Server IP Address	Enter the IP address of the L2TP server.
User Name	Enter the user name for connecting to the L2TP server.

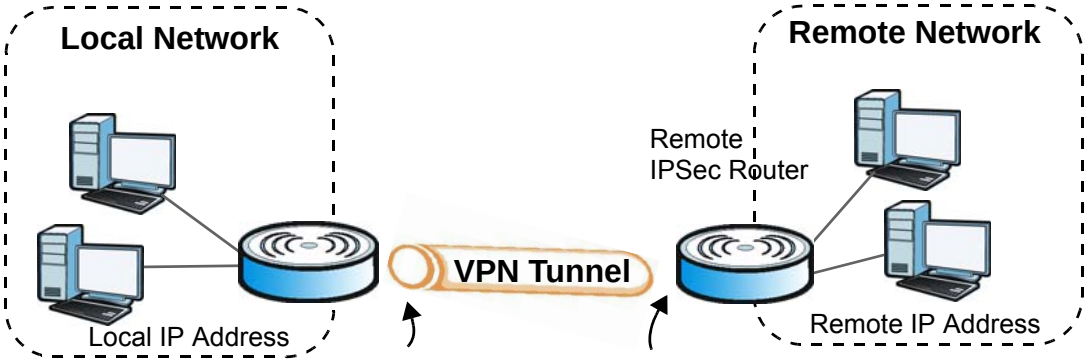
Table 58 L2TP Client: Add (continued)

LABEL	DESCRIPTION
Password	Enter the password for connecting to the L2TP server.
Retype	Retype the password for connecting to the L2TP server.
Get IP automatically	Select **Yes** to have the L2TP server assign a local IP address to the client.
Assign IP Address	Enter the IP address for the client. Ensure that the IP address is configured to be allowed on the L2TP server.
Idle Timeout	Enter the time in minutes to timeout L2TP connections.

8.11 IPSec VPN

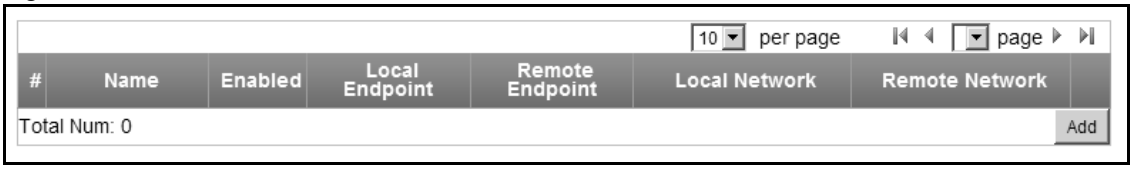
The following figure helps explain the main fields in the web configurator.

Figure 77 IPSec Fields Summary



Click **Security > IPSec VPN** to open the **General** screen as shown next.

Figure 78 IPSec VPN



This screen contains the following fields:

Table 59 IPSec VPN

LABEL	DESCRIPTION
#	This is the VPN policy index number.
Name	Enter the name of the VPN connection.
Enabled	This displays if the VPN policy is enabled.
Local Endpoint	This displays the IP address of the WiMAX Device.
Remote Endpoint	This displays the IP address of the remote IPSec router.
Local Network	This displays the single (static) IP address on the LAN behind your WiMAX Device or the IP address and subnet mask of a network behind your WiMAX Device.

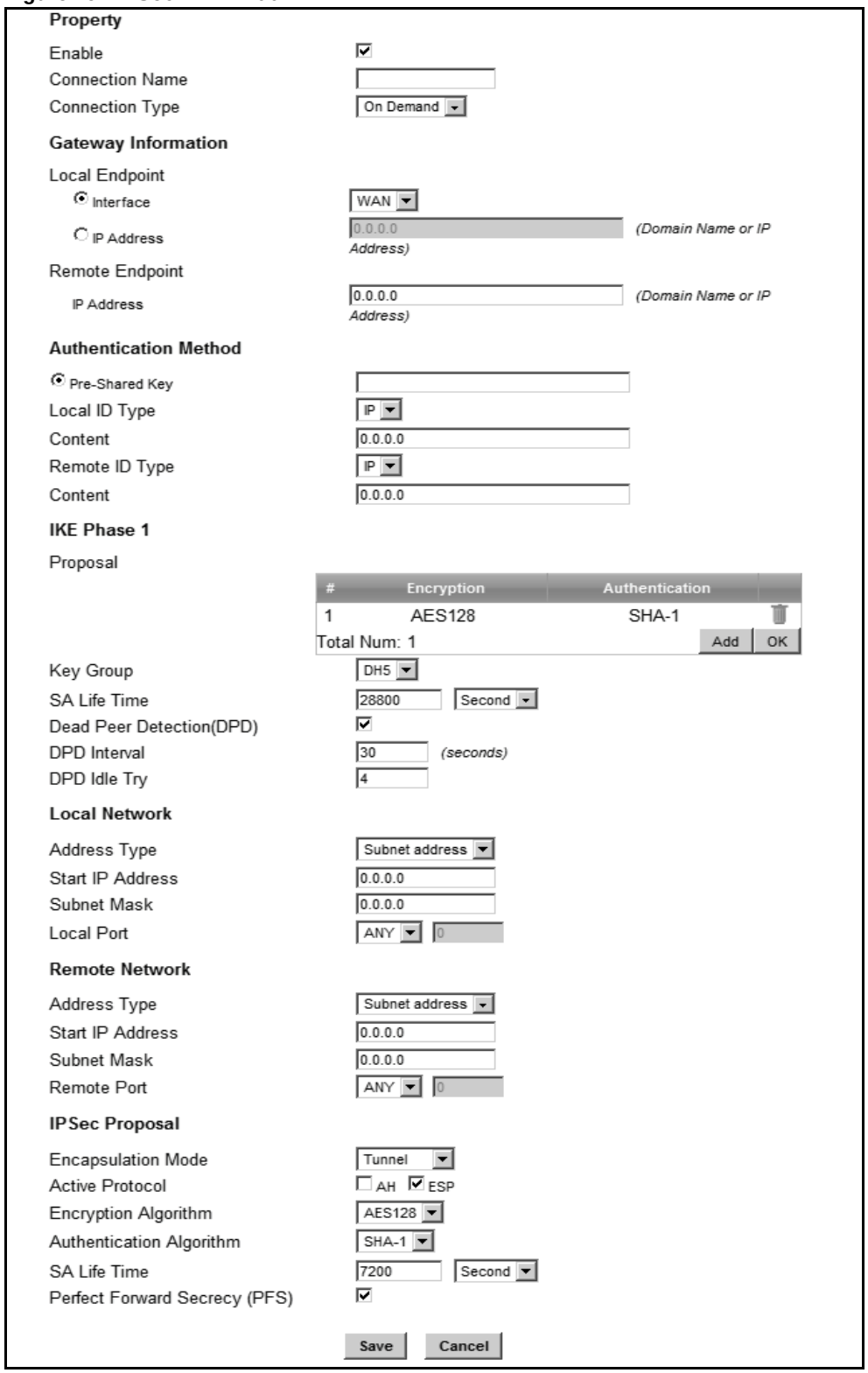
Table 59 IPSec VPN (continued)

LABEL	DESCRIPTION
Remote Network	This displays the single (static) IP address on the LAN behind the remote IPSec router or the IP address and subnet mask of a network behind the remote IPSec router.
Add	Click this button to add an item to the list.

8.11.1 IPSec VPN: Add

Use these settings. Click **Security > IPSec VPN > Add** to open this screen as shown next.

Figure 79 IPSec VPN: Add



This screen contains the following fields:

Table 60 IPSec VPN: Add

LABEL	DESCRIPTION
Property	
Enable	Select **Enable** to activate this VPN policy.
Connection Name	Enter the name of the VPN connection.
Connection Type	Select the scenario that best describes your intended VPN connection. • **Initiator** - Choose this to connect to an IPSec server. The WiMAX Device is the client (dial-in user) and can initiate the VPN connection. • On Demand - Choose this if the remote IPSec router has a static IP address or a domain name. This WiMAX Device can initiate the VPN tunnel. • Responder - Choose this to allow incoming connections from IPSec VPN clients. The clients can have dynamic IP addresses and are also known as dial-in users. Only the clients can initiate the VPN tunnel.
Gateway Information	
Local Endpoint	
Interface	Select the interface for the VPN gateway.
IP Address	Enter the IP address of the WiMAX Device in the IKE SA.
Remote Endpoint	
IP Address	Enter the IP address of the remote IPSec router in the IKE SA.
Authentication Method	
Pre-Shared Key	Type your pre-shared key in this field. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. You must precede a hexadecimal key with a "0x" (zero x), which is not counted as part of the 16 to 62 character range for the key. For example, in "0x0123456789ABCDEF", “0x” denotes that the key is hexadecimal and “0123456789ABCDEF” is the key itself.
Local ID Type	Select **IP** to identify the WiMAX Device by its IP address. Select **Domain Name** to identify this WiMAX Device by a domain name. Select **E-mail** to identify this WiMAX Device by an e-mail address.
Content	When you select IP in the **Local ID Type** field, type the IP address of your computer in the **Content** field. If you configure the **Content** field to 0.0.0.0 or leave it blank, the WiMAX Device automatically uses the **Pre-Shared Key** (refer to the **Pre-Shared Key** field description). It is recommended that you type an IP address other than 0.0.0.0 in the **Content** field or use the **Domain Name** or **E-mail ID** type in the following situations. • When there is a NAT router between the two IPSec routers. • When you want the remote IPSec router to be able to distinguish between VPN connection requests that come in from IPSec routers with dynamic WAN IP addresses. When you select **Domain Name** or **E-mail** in the **Local ID Type** field, type a domain name or e-mail address by which to identify this WiMAX Device in the **Local Content** field. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string.

Table 60 IPSec VPN: Add (continued)

LABEL	DESCRIPTION
Remote ID Type	Select **IP** to identify the remote IPSec router by its IP address. Select **Domain Name** to identify the remote IPSec router by a domain name. Select **E-mail** to identify the remote IPSec router by an e-mail address.
Content	The configuration of the remote content depends on the remote ID type. For **IP**, type the IP address of the computer with which you will make the VPN connection. If you configure this field to 0.0.0.0 or leave it blank, the WiMAX Device will use the address in the **Remote Endpoint** field (refer to the **Remote Endpoint** field description). For **Domain Name** or **E-mail**, type a domain name or e-mail address by which to identify the remote IPSec router. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string. It is recommended that you type an IP address other than 0.0.0.0 or use the **Domain Name** or **E-mail** ID type in the following situations: • When there is a NAT router between the two IPSec routers. • When you want the WiMAX Device to distinguish between VPN connection requests that come in from remote IPSec routers with dynamic WAN IP addresses.
IKE Phase 1	
Proposal	
#	This field is a sequential value, and it is not associated with a specific proposal. The sequence of proposals should not affect performance significantly.
Encryption	Select which key size and encryption algorithm to use in the IKE SA. Choices are: • **DES** - a 56-bit key with the DES encryption algorithm • **3DES** - a 168-bit key with the DES encryption algorithm • **AES128** - a 128-bit key with the AES encryption algorithm • **AES192** - a 192-bit key with the AES encryption algorithm • **AES256** - a 256-bit key with the AES encryption algorithm The WiMAX Device and the remote IPSec router must use the same key size and encryption algorithm. Longer keys require more processing power, resulting in increased latency and decreased throughput.
Authentication	Select which hash algorithm to use to authenticate packet data. Choices are **SHA1** and **MD5**. **SHA1** is generally considered stronger than **MD5**, but it is also slower.
Remove	Select an entry and click this to delete it.
Add	Click this to create a new entry.
OK	Click this to save the changes.
Key Group	Select which Diffie-Hellman key group (DHx) you want to use for encryption keys. Choices are: • **DH1** - use a 768-bit random number • **DH2** - use a 1024-bit random number • **DH5** - use a 1536-bit random number The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. Both routers must use the same DH key group.

Table 60 IPSec VPN: Add (continued)

LABEL	DESCRIPTION
SA Life Time	Type the maximum number of seconds the IKE SA can last. When this time has passed, the WiMAX Device and remote IPSec router have to update the encryption and authentication keys and re-negotiate the IKE SA. This does not affect any existing IPSec SAs, however.
Dead Peer Detection (DPD)	Select this check box if you want the WiMAX Device to make sure the remote IPSec router is there before it transmits data through the IKE SA. The remote IPSec router must support DPD. If the remote IPSec router does not respond, the WiMAX Device shuts down the IKE SA. If the remote IPSec router does not support DPD, see if you can use the VPN connection connectivity check.
DPD Interval	Specify the time interval for the WiMAX Device to send a DPD message to the remote IPSec router.
DPD Idle Try	Specify the maximum number of times the WiMAX Device sends the DPD message.
Local Network	Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses. Two active SAs can have the same configured local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time. In order to have more than one active rule with the **Remote Endpoint** field set to 0.0.0.0, the ranges of the local IP addresses cannot overlap between rules. If you configure an active rule with 0.0.0.0 in the **Remote Endpoint** field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the **Remote Endpoint** field set to 0.0.0.0.
Address Type	Select **Single address** or **Subnet address** to specify if the VPN connection begins at an IP address or subnet.
Start IP Address	If **Single address** is selected, enter a (static) IP address on the LAN behind your WiMAX Device. If **Subnet address** is selected, specify IP addresses on a network by their subnet mask by entering a (static) IP address on the LAN behind your WiMAX Device. Then enter the subnet mask to identify the network address.
Subnet Mask	If **Subnet address** is selected, enter the subnet mask to identify the network address.
Local Port	Select how the WiMAX Device checks the connection. The peer must be configured to respond to the method you select. Select **icmp** to have the WiMAX Device regularly ping the address you specify to make sure traffic can still go through the connection. You may need to configure the peer to respond to pings. Select **tcp** or **udp** to have the WiMAX Device regularly perform a TCP or UDP handshake with the address you specify to make sure traffic can still go through the connection. You may need to configure the peer to accept the TCP or UDP connection. If you select **tcp** or **udp**, specify the port number to use for the connectivity check.
Remote Network	Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses. The remote fields do not apply when the **Remote Endpoint** field is configured to 0.0.0.0. In this case only the remote IPSec router can initiate the VPN. Two active SAs cannot both have the same local and remote IP address(es). Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.

Table 60 IPSec VPN: Add (continued)

LABEL	DESCRIPTION
Address Type	Select **Single address** or **Subnet address** to specify if the VPN connection terminates at an IP address or subnet.
Start IP Address	If **Single address** is selected, enter a (static) IP address on the LAN behind the remote IPSec's router. If **Subnet address** is selected, specify IP addresses on a network by their subnet mask by entering a (static) IP address on the LAN behind the remote IPSec's router. Then enter the subnet mask to identify the network address.
Subnet Mask	If **Subnet address** is selected, enter the subnet mask to identify the network address.
Remote Port	Select how the WiMAX Device checks the connection. The peer must be configured to respond to the method you select. Select **icmp** to have the WiMAX Device regularly ping the address you specify to make sure traffic can still go through the connection. You may need to configure the peer to respond to pings. Select **tcp** or **udp** to have the WiMAX Device regularly perform a TCP or UDP handshake with the address you specify to make sure traffic can still go through the connection. You may need to configure the peer to accept the TCP or UDP connection. If you select **tcp** or **udp**, specify the port number to use for the connectivity check.
IPSec Proposal	
Encapsulation Mode	Select **Tunnel** mode or **Transport** mode from the drop-down list box.
Active Protocol	Select the security protocols used for an SA. Both **AH** and **ESP** increase processing requirements and communications latency (delay). If you select **ESP** here, you must select options from the **Encryption Algorithm** and **Authentication Algorithm** fields (described below).
Encryption Algorithm	Select which key size and encryption algorithm to use in the IPSec SA. Choices are: • **DES** - a 56-bit key with the DES encryption algorithm • **3DES** - a 168-bit key with the DES encryption algorithm • **AES128** - a 128-bit key with the AES encryption algorithm • **AES192** - a 192-bit key with the AES encryption algorithm • **AES256** - a 256-bit key with the AES encryption algorithm The WiMAX Device and the remote IPSec router must use the same key size and encryption algorithm. Longer keys require more processing power, resulting in increased latency and decreased throughput.
Authentication Algorithm	Select which hash algorithm to use to authenticate packet data. Choices are **SHA1** and **MD5**. **SHA1** is generally considered stronger than **MD5**, but it is also slower.
SA Life Time	Define the length of time before an IPSec SA automatically renegotiates in this field. A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.

Table 60 IPSec VPN: Add (continued)

LABEL	DESCRIPTION
Perfect Forward Secrecy (PFS)	Select whether or not you want to enable Perfect Forward Secrecy (PFS). PFS changes the root key that is used to generate encryption keys for each IPSec SA. The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. Both routers must use the same DH key group.
Save	Click **Apply** to save your changes back to the WiMAX Device.
Cancel	Click **Cancel** to restore your previous settings.

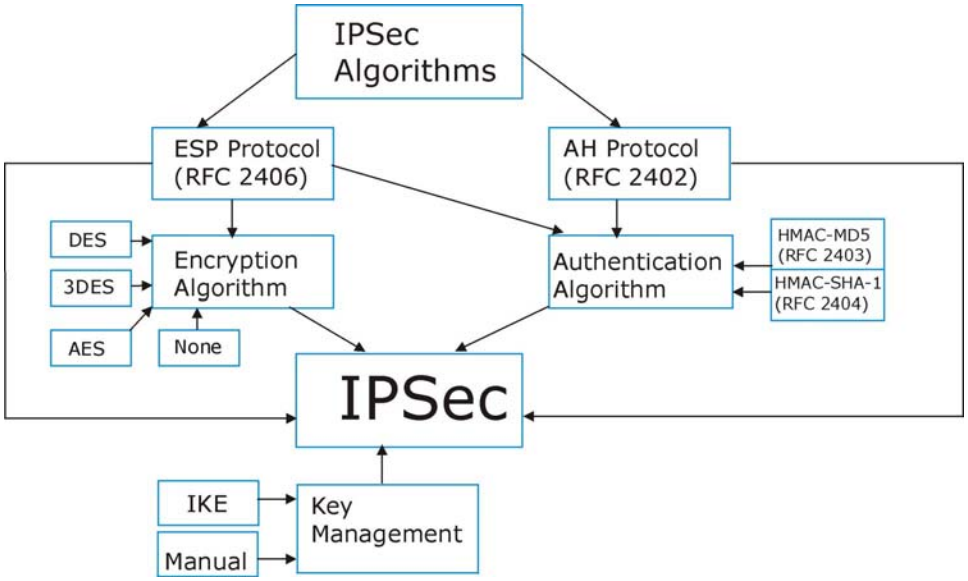
8.12 Technical Reference

This section provides some technical background information about the topics covered in this section.

8.12.1 IPSec Architecture

The overall IPSec architecture is shown as follows.

Figure 80 IPSec Architecture



IPSec Algorithms

The **ESP** (Encapsulating Security Payload) Protocol (RFC 2406) and **AH** (Authentication Header) protocol (RFC 2402) describe the packet formats and the default standards for packet structure (including implementation algorithms).

The Encryption Algorithm describes the use of encryption techniques such as DES (Data Encryption Standard) and Triple DES algorithms.

The Authentication Algorithms, HMAC-MD5 (RFC 2403) and HMAC-SHA-1 (RFC 2404, provide an authentication mechanism for the **AH** and **ESP** protocols.

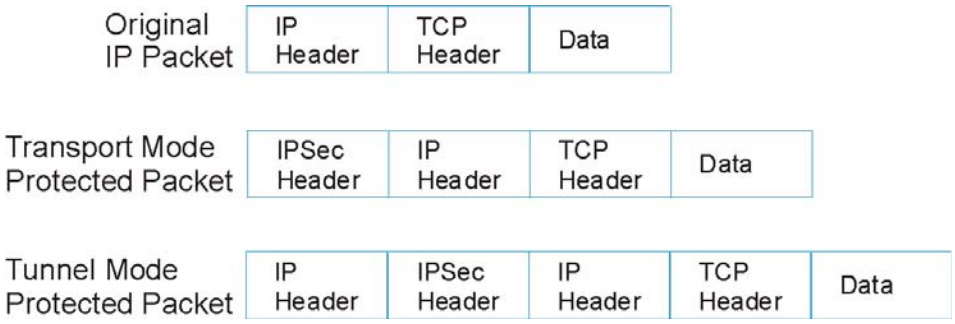
Key Management

Key management allows you to determine whether to use IKE (ISAKMP) or manual key configuration in order to set up a VPN.

8.12.2 Encapsulation

The two modes of operation for IPSec VPNs are **Transport** mode and **Tunnel** mode. At the time of writing, the WiMAX Device supports **Tunnel** mode only.

Figure 81 Transport and Tunnel Mode IPSec Encapsulation



Transport Mode

Transport mode is used to protect upper layer protocols and only affects the data in the IP packet. In **Transport** mode, the IP packet contains the security protocol (**AH** or **ESP**) located after the original IP header and options, but before any upper layer protocols contained in the packet (such as TCP and UDP).

With **ESP,** protection is applied only to the upper layer protocols contained in the packet. The IP header information and options are not used in the authentication process. Therefore, the originating IP address cannot be verified for integrity against the data.

With the use of **AH** as the security protocol, protection is extended forward into the IP header to verify the integrity of the entire packet by use of portions of the original IP header in the hashing process.

Tunnel Mode

Tunnel mode encapsulates the entire IP packet to transmit it securely. A **Tunnel** mode is required for gateway services to provide access to internal systems. **Tunnel** mode is fundamentally an IP tunnel with authentication and encryption. This is the most common mode of operation. **Tunnel** mode is required for gateway to gateway and host to gateway communications. **Tunnel** mode communications have two sets of IP headers:

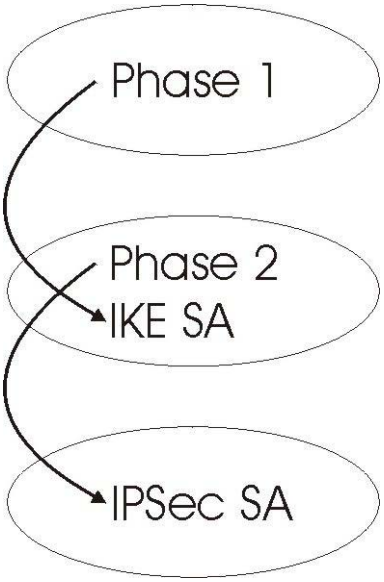
- **Outside header**: The outside IP header contains the destination IP address of the VPN gateway.

- **Inside header**: The inside IP header contains the destination IP address of the final system behind the VPN gateway. The security protocol appears after the outer IP header and before the inside IP header.

8.12.3 IKE Phases

There are two phases to every IKE (Internet Key Exchange) negotiation – phase 1 (Authentication) and phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA and the second one uses that SA to negotiate SAs for IPSec.

Figure 82 Two Phases to Set Up the IPSec SA



In phase 1 you must:

- Choose a negotiation mode.
- Authenticate the connection by entering a pre-shared key.
- Choose an encryption algorithm.
- Choose an authentication algorithm.
- Choose a Diffie-Hellman public-key cryptography key group (**DH1** or **DH2**).
- Set the IKE SA lifetime. This field allows you to determine how long an IKE SA should stay up before it times out. An IKE SA times out when the IKE SA lifetime period expires. If an IKE SA times out when an IPSec SA is already established, the IPSec SA stays connected.

In phase 2 you must:

- Choose an encryption algorithm.
- Choose an authentication algorithm
- Choose a Diffie-Hellman public-key cryptography key group.
- Set the IPSec SA lifetime. This field allows you to determine how long the IPSec SA should stay up before it times out. The WiMAX Device automatically renegotiates the IPSec SA if there is traffic when the IPSec SA lifetime period expires. If an IPSec SA times out, then the IPSec router must renegotiate the SA the next time someone attempts to send traffic.

8.12.4 Negotiation Mode

The phase 1 **Negotiation Mode** you select determines how the Security Association (SA) will be established for each connection through IKE negotiations.

- **Main Mode** ensures the highest level of security when the communicating parties are negotiating authentication (phase 1). It uses 6 messages in three round trips: SA negotiation, Diffie-Hellman exchange and an exchange of nonces (a nonce is a random number). This mode features identity protection (your identity is not revealed in the negotiation).
- **Aggressive Mode** is quicker than **Main Mode** because it eliminates several steps when the communicating parties are negotiating authentication (phase 1). However the trade-off is that faster speed limits its negotiating power and it also does not provide identity protection. It is useful in remote access situations where the address of the initiator is not know by the responder and both parties want to use pre-shared key authentication.

8.12.5 IPSec and NAT

Read this section if you are running IPSec on a host computer behind the WiMAX Device.

NAT is incompatible with the **AH** protocol in both **Transport** and **Tunnel** mode. An IPSec VPN using the **AH** protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet. When using **AH** protocol, packet contents (the data payload) are not encrypted.

A NAT device in between the IPSec endpoints will rewrite either the source or destination address with one of its own choosing. The VPN device at the receiving end will verify the integrity of the incoming packet by computing its own hash value, and complain that the hash value appended to the received packet doesn't match. The VPN device at the receiving end doesn't know about the NAT in the middle, so it assumes that the data has been maliciously altered.

IPSec using **ESP** in **Tunnel** mode encapsulates the entire original packet (including headers) in a new IP packet. The new IP packet's source address is the outbound address of the sending VPN gateway, and its destination address is the inbound address of the VPN device at the receiving end. When using **ESP** protocol with authentication, the packet contents (in this case, the entire original packet) are encrypted. The encrypted contents, but not the new headers, are signed with a hash value appended to the packet.

Tunnel mode **ESP** with authentication is compatible with NAT because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device.

Transport mode **ESP** with authentication is not compatible with NAT.

Table 61 VPN and NAT

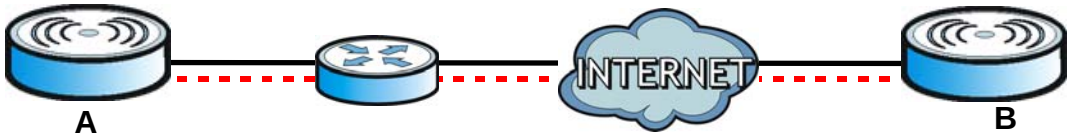
SECURITY PROTOCOL	MODE	NAT
AH	Transport	N
AH	Tunnel	N
ESP	Transport	N
ESP	Tunnel	Y

8.12.6 VPN, NAT, and NAT Traversal

NAT is incompatible with the AH protocol in both transport and tunnel mode. An IPSec VPN using the AH protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet, but a NAT device between the IPSec endpoints rewrites the source or destination address. As a result, the VPN device at the receiving end finds a mismatch between the hash value and the data and assumes that the data has been maliciously altered.

NAT is not normally compatible with ESP in transport mode either, but the WiMAX Device's **NAT Traversal** feature provides a way to handle this. NAT traversal allows you to set up an IKE SA when there are NAT routers between the two IPSec routers.

Figure 83 NAT Router Between IPSec Routers



Normally you cannot set up an IKE SA with a NAT router between the two IPSec routers because the NAT router changes the header of the IPSec packet. NAT traversal solves the problem by adding a UDP port 500 header to the IPSec packet. The NAT router forwards the IPSec packet with the UDP port 500 header unchanged. In the above figure, when IPSec router **A** tries to establish an IKE SA, IPSec router **B** checks the UDP port 500 header, and IPSec routers **A** and **B** build the IKE SA.

For NAT traversal to work, you must:

- Use ESP security protocol (in either transport or tunnel mode).
- Use IKE keying mode.
- Enable NAT traversal on both IPSec endpoints.
- Set the NAT router to forward UDP port 500 to IPSec router **A**.

Finally, NAT is compatible with ESP in tunnel mode because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device. The compatibility of AH and ESP with NAT in tunnel and transport modes is summarized in the following table.

Table 62 VPN and NAT

SECURITY PROTOCOL	MODE	NAT
AH	Transport	N
AH	Tunnel	N
ESP	Transport	Y*
ESP	Tunnel	Y

Y* - This is supported in the WiMAX Device if you enable NAT traversal.

8.12.7 ID Type and Content

With aggressive negotiation mode (see Section 8.12.4 on page 147), the WiMAX Device identifies incoming SAs by ID type and content since this identifying information is not encrypted. This

enables the WiMAX Device to distinguish between multiple rules for SAs that connect from remote IPSec routers that have dynamic WAN IP addresses.

Regardless of the ID type and content configuration, the WiMAX Device does not allow you to save multiple active rules with overlapping local and remote IP addresses.

With main mode (see Section 8.12.4 on page 147), the ID type and content are encrypted to provide identity protection. In this case the WiMAX Device can only distinguish between up to 12 different incoming SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. The WiMAX Device can distinguish up to 48 incoming SAs because you can select between three encryption algorithms (DES, 3DES and AES), two authentication algorithms (MD5 and SHA1) and eight key groups when you configure a VPN rule (see Section on page 137). The ID type and content act as an extra level of identification for incoming SAs.

The type of ID can be a domain name, an IP address or an e-mail address. The content is the IP address, domain name, or e-mail address.

Table 63 Local ID Type and Content Fields

LOCAL ID TYPE=	CONTENT=
IP	Type the IP address of your computer.
DNS	Type a domain name (up to 31 characters) by which to identify this WiMAX Device.
E-mail	Type an e-mail address (up to 31 characters) by which to identify this WiMAX Device.
	The domain name or e-mail address that you use in the **Local ID Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address.

8.12.7.1 ID Type and Content Examples

Two IPSec routers must have matching ID type and content configuration in order to set up a VPN tunnel.

The two WiMAX Devices in this example can complete negotiation and establish a VPN tunnel.

Table 64 Matching ID Type and Content Configuration Example

WiMAX Device A	WiMAX Device B
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2
Remote ID type: IP	Remote ID type: E-mail
Remote ID content: 1.1.1.2	Remote ID content: tom@yourcompany.com

The two WiMAX Devices in this example cannot complete their negotiation because WiMAX Device B's **Local ID type** is **IP**, but WiMAX Device A's **Remote ID type** is set to **E-mail**. An "ID mismatched" message displays in the IPSEC LOG.

Table 65 Mismatching ID Type and Content Configuration Example

WIMAX DEVICE A	WIMAX DEVICE B
Local ID type: IP	Local ID type: IP
Local ID content: 1.1.1.10	Local ID content: 1.1.1.2
Remote ID type: E-mail	Remote ID type: IP
Remote ID content: aa@yahoo.com	Remote ID content: 1.1.1.0

8.12.8 Pre-Shared Key

A pre-shared key identifies a communicating party during a phase 1 IKE negotiation (see Section 8.12.3 on page 146 for more on IKE phases). It is called “pre-shared” because you have to share it with another party before you can communicate with them over a secure connection.

8.12.9 Diffie-Hellman (DH) Key Groups

Diffie-Hellman (DH) is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communications channel. Diffie-Hellman is used within IKE SA setup to establish session keys. 768-bit, 1024-bit 1536-bit, 2048-bit, and 3072-bit Diffie-Hellman groups are supported. Upon completion of the Diffie-Hellman exchange, the two peers have a shared secret, but the IKE SA is not authenticated. For authentication, use pre-shared keys.

9

The VoIP General Screens

9.1 VoIP Overview

The features mentioned in this chapter are for models that has phone port(s) and you can make telephone calls over the Internet using the WiMAX Device.

The **VOICE > General** screens allow you to set up global SIP and Quality of Service (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.

9.1.1 What You Need to Know

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

Voice Coding

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

- **G.711** is a Pulse Code Modulation (PCM) waveform codec. PCM measures analog signal amplitudes at regular time intervals (sampling) and converts them into digital bits (quantization). Quantization "reads" the analog signal and then "writes" it to the nearest digital value. For this reason, a digital sample is usually slightly different from its analog original (this difference is known as "quantization noise"). G.711 provides excellent sound quality but requires 64kbps of bandwidth.
- **G.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.

Quality of Service (QoS)

Quality of Service (QoS) 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.

Type Of Service (ToS)

Network traffic can be classified by setting the ToS (Type Of Service) values at the data source (for example, at the WiMAX Device) so a server can decide the best method of delivery, that is the least cost, fastest route and so on. The ToS field is consist of 8 bits. The first 3 bits indicate the priority of the packet.

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.

DiffServ uses the first 6 bits of the 8-bit ToS value so that it can be backward compatible with non-DiffServ compliant but ToS-enabled network device. See Section 9.6.1 on page 156 for more information.

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.

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.

Speed Dial

Speed dial provides shortcuts for dialing frequently used phone numbers. You can map a phone number to a self-defined key(s) and then use that key(s) to call the phone number. For example, you can map 123456 to #01. When you press #01 it means that you press 123456.

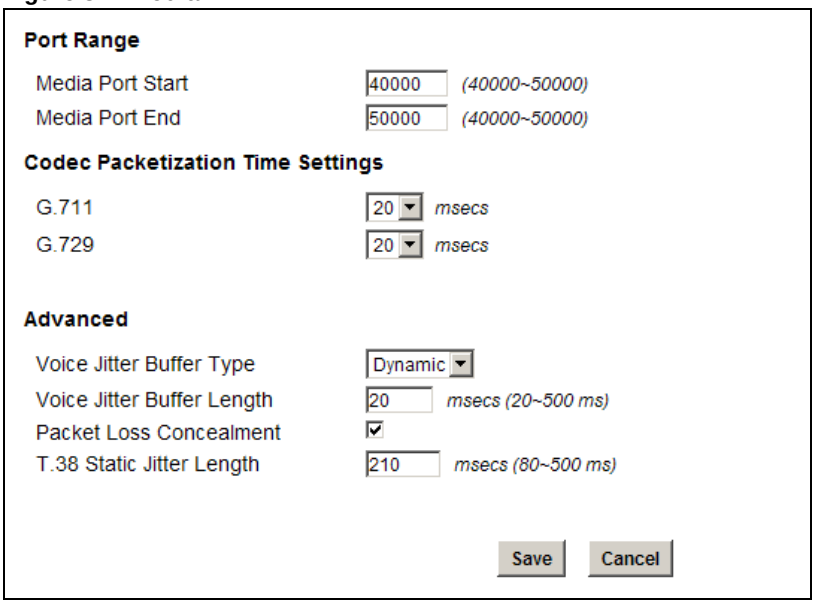
9.1.2 Before you Begin

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

9.2 Media

Click **VoIP > General > Media** to set up and maintain global VoIP settings.

Figure 84 Media



The following table describes the labels in this screen.

Table 66 Media

LABEL	DESCRIPTION
Port Range	
Media Port Start Media Port End	Enter the listening port number(s) for RTP traffic on the WiMAX Device, if your VoIP service provider gave you this information. Otherwise, keep the default values. To enter one port number, enter the port number in the both **Media Port Start** and **Media Port End** fields. To enter a range of ports, enter the beginning port number of the range in the **Media Port Start** field and the ending port number in the **Media Port End** field.
Codec Packetization Time Settings	
G.711, G.729	Select how often (**10** to **60** msecs) the WiMAX Device sends an RTP packet for each type of voice coder/decoder (codec) **G.711** and **G.729**.
Advanced	
Voice Jitter Buffer Type	Voice jitter is a variation in delay of RTP packets delivery. This could cause strange sound effects. The WiMAX Device can utilize the following types of jitter buffer to minimize the effects of jitter. **Dynamic** - Jitter buffer size is dynamically changed by RTP packets delivery status. **Static** - Jitter buffer size is fixed.
Voice Jitter Buffer Length	Select the maximum number of milliseconds of voice traffic the WiMAX Device can help to smooth out the jitter in order to ensure good voice quality for your conversations.

Table 66 Media (continued)

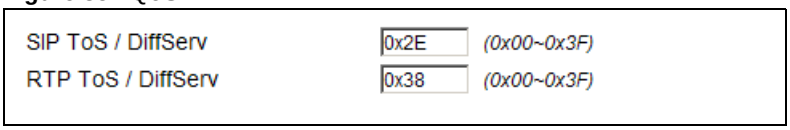
LABEL	DESCRIPTION
Packet Loss Concealment	Packets may be dropped due to an overwhelming amount of traffic on the network. Some degree of packet loss will not be noticeable to the end user, but as packet loss increases the quality of sound degrades. Select this to have the WiMAX Device to improve the voice quality when packet loss occurs.
T.38 Static Jitter Length	T.38 is an ITU-T standard that VoIP devices use to send fax messages over the Internet. Select the number of milliseconds for the jitter buffer size used for transmitting T.38 fax messages.

9.3 QoS

This section describes the features of the Quality of Service (QoS) screen.

Click **VoIP > General > QoS** to set up Type of Service (ToS) and Differentiated Services (Diffserv) settings for voice traffic transmission through the WiMAX Device.

Figure 85 QoS



The following table describes the labels in this screen.

Table 67 QoS

LABEL	DESCRIPTION
SIP ToS/DiffServ	Enter the DSCP value you want to mark on all outgoing SIP packets generated by the WiMAX Device for DiffServ-enabled networks. Since DiffServ uses the first 6 bits of the 8-bit IP ToS field to represent the DSCP value, enter here the 6-bit DSCP value you want to mark in hexadecimal (in a format of 0x00), and the WiMAX Device will then automatically append 2 bits '0' to make a whole 8-bit ToS field value for all outgoing SIP packets. For example, if you enter 0x2E, it is 101110 in binary for DSCP. The WiMAX Device converts it to 10111000 in binary and marks on the IP ToS field of all the outgoing SIP packets.
RTP ToS/DiffServ	Enter the DSCP value you want to mark on all outgoing VoIP data packets (including both RTP and T.38 UDPTL packets) generated by the WiMAX Device for DiffServ-enabled networks.

9.4 SIP Settings

Click **VoIP > General > SIP** to set up session timer on the WiMAX Device. See Section 10.8 on page 167 for more information on SIP.

Figure 86 SIP

The following table describes the labels in this screen.

Table 68 SIP

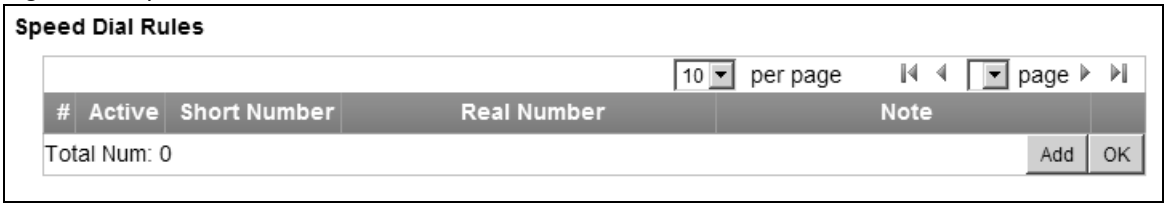
LABEL	DESCRIPTION
Session Timer Enable	Select this to activate the WiMAX Device's SIP Session Timer. SIP Session Timer is a function used by both of the communication peers to determine if the call session is still active (alive) or not. It uses the method specified in the following **Refresh Method** field to periodically refresh the SIP sessions.
Refresh Method	Select the method to be used for periodically refreshing SIP sessions, to determine if the session is still active. Select **UPDATE** to use Update requests to refresh the session and select **INVITE** to use Re-Invite requests. You should use the same method as the peer device. The Update method uses less overhead than Re-Invite, but is not as widely supported as Re-Invite. By default the WiMAX Device is set to use the **UPDATE** method. When set to **UPDATE**, the WiMAX Device can also revert to using the **INVITE** method for SIP session refresh, depending on the method supported and allowed by the peer device.

9.5 Speed Dial

Speed dial allows you to use a shorter number for dialing frequently used phone numbers.

Click **VoIP > General > Speed Dial** to add, edit, or remove speed-dial rules.

Figure 87 Speed Dial



The following table describes the labels in this screen.

Table 69 Speed Dial

LABEL	DESCRIPTION
Speed Dial Rules - This is a list of speed dial numbers. To edit an existing speed dial rule, you can click the row for the rule and editable fields will appear.	
Active	This field displays whether the rule is activated or not.

Table 69 Speed Dial (continued)

LABEL	DESCRIPTION
Short Number	This field displays the abbreviated number you want to use to substitute for the real (actual) phone number in the following **Real Number** field. When the rule is activated, you can press the assigned **Short Number** to dial the **Real Number**.
Real Number	This field displays the actual phone number you want the WiMAX Device to call when you use the specified **Short Number**. Enter the actual phone number you want the WiMAX Device to call when you use the specified **Short Number** if you are editing the entry.
Notes	This field displays additional information for this speed-dial rule. Enter additional information or any remark for this speed-dial rule if your are editing the entry.
Remove	Click this to remove the rule.
Add	Click this to add a new speed-dial rule.
OK	Click this to save the changes you made in this table.

9.6 Technical Reference

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

9.6.1 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 88 DiffServ: Differentiated Service Field

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

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

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

10

The VoIP Account Screens

10.1 Overview

The features mentioned in this chapter are for models with VoIP function.

Use the **VoIP > Account 1 (or Account 2)** screens to configure your VoIP account information on the WiMAX Device. You need to have a VoIP account set up first.

Note: If your WiMAX Device has only one phone port, there is only one account.

Note: You can identify the number of phone ports available on your WiMAX Device by its model name. See Section 1.1 on page 17 for more information.

10.1.1 What You Need to Know

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

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.

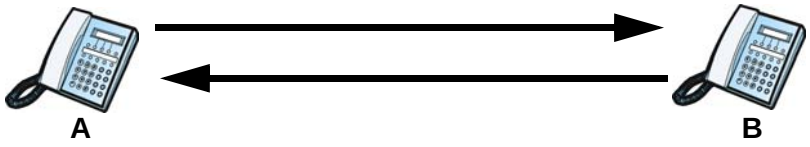
SIP Register Server

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.

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 89 SIP User Agent



SIP Proxy Server

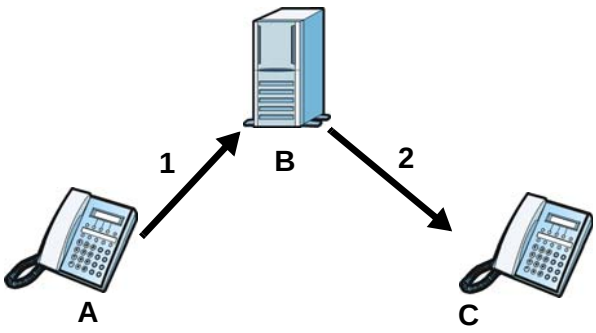
A SIP proxy server receives requests from clients and forwards them to another server.

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 90 SIP Proxy Server



STUN

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

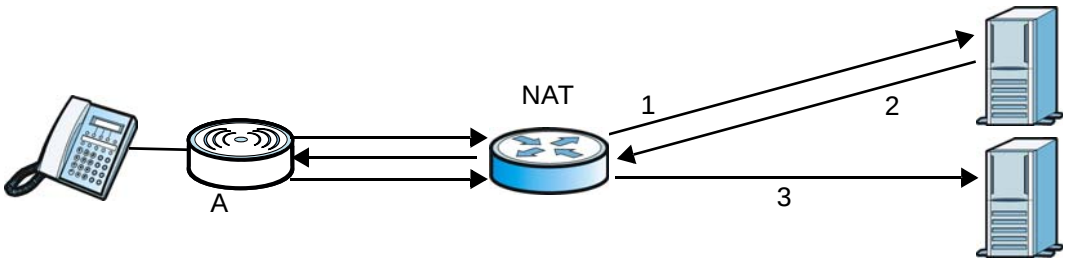
The following figure shows how STUN works.

1 The WiMAX Device (**A**) sends SIP packets to the STUN server (**B**).

2 The STUN server (**B**) finds the public IP address and port number that the NAT router used on the WiMAX Device's SIP packets and sends them to the WiMAX Device.

3 The WiMAX Device uses the public IP address and port number in the SIP packets that it sends to the SIP server (**C**).

Figure 91 STUN



Outbound Proxy

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

NAT and SIP

The WiMAX Device must register its public IP address with a SIP register server. If there is a NAT router between the WiMAX Device and the SIP register server, the WiMAX Device probably has a private IP address. The WiMAX Device lists its IP address in the SIP message that it sends to the SIP register server. NAT does not translate this IP address in the SIP message. The SIP register server gets the WiMAX Device's IP address from inside the SIP message and maps it to your SIP identity. If the WiMAX Device has a private IP address listed in the SIP message, the SIP server cannot map it to your SIP identity.

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

DTMF

Dual-Tone Multi-Frequency (DTMF) telephone call signaling uses pairs of frequencies (one lower frequency and one higher frequency) to set up calls. It is also known as Touch Tone. Each of the keys on a DTMF telephone corresponds to a different pair of frequencies.

Supplementary Phone Services Overview

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

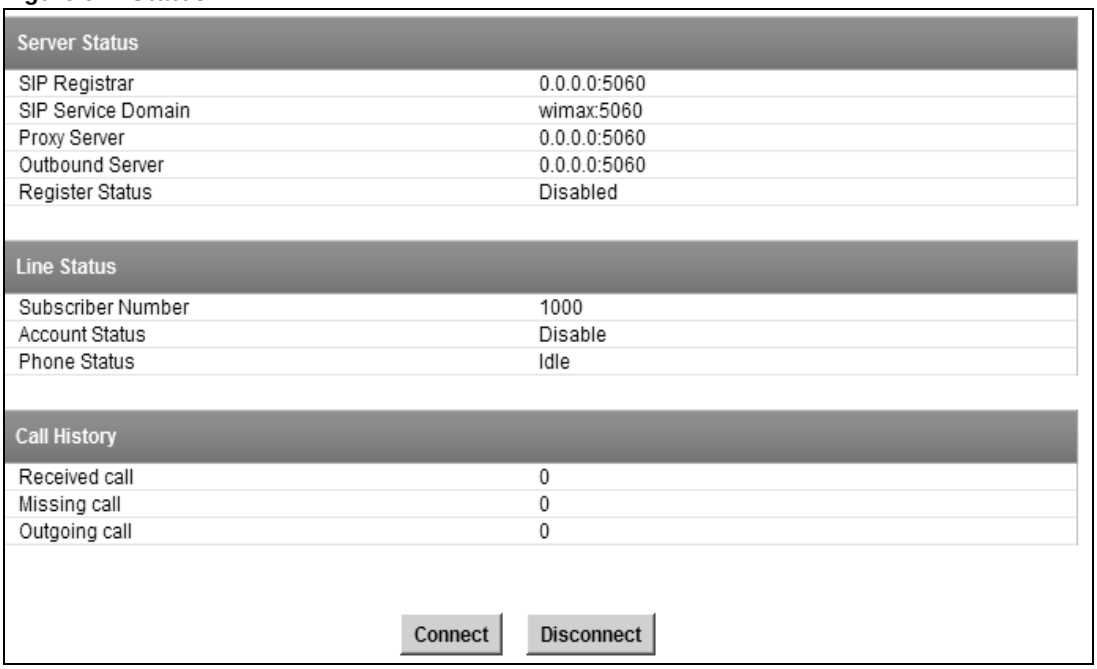
- Call Waiting
- Call Forwarding
- Caller ID

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

10.2 Status

Click **VoIP > Account 1 (or Account 2) > Status** to view VoIP settings and current status.

Figure 92 Status



The following table describes the labels in this screen.

Table 70 Status

LABEL	DESCRIPTION
Server Status	
SIP Register	This field displays the IP address (or domain name) and service port number of the register server, if you have configured one.
SIP Service Domain	This field displays the SIP service domain and port number of the SIP server, if you have configured one.
Proxy Server	This field displays the IP address (or domain name) and service port number of the SIP proxy server, if you have configured one.
Outbound Server	This field displays the IP address (or domain name) and service port number of the outbound proxy server, if you have configured one.
Register Status	This field displays **Disabled** if the SIP account (set up in Section 10.4 on page 163) is disabled or de-registered from the registrar server. It displays **Registering** (or **Unregistering**) after sending out the SIP register (or unregister) message to make registration (or de-registration) at (or from) the SIP registrar server. If the registration fails, for example, rejected by SIP registrar server (due to wrong authentication data) or timeout to get response from the server, **Error** would be displayed. It displays **Up** if the SIP account is registered at the registrar server successfully.
Line Status	
Subscriber Number	This field displays the SIP phone number for the phone line.

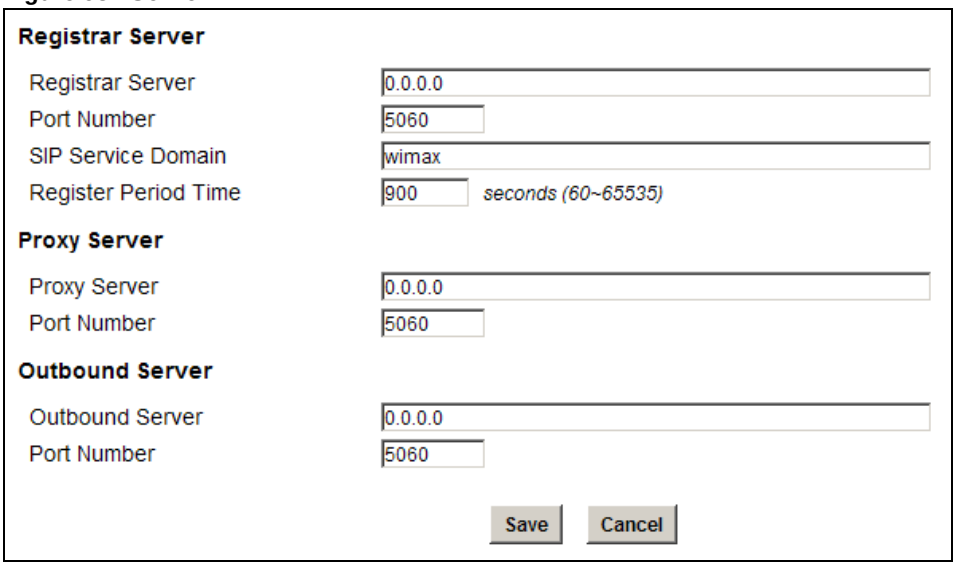
Table 70 Status (continued)

LABEL	DESCRIPTION
Account Status	This indicates whether the SIP account is activated or not. **Enable** means activated and **Disable** means deactivated.
Phone Status	This field displays the phone status, such as **Idle**, **Calling**, **Ringing**, **Connecting**, **InCall**, **Hold**, and **Disconnecting**.
Call History	
Received call	This field displays the number of calls you have received through the connected phone since the WiMAX Device last restarted or was turned on.
Missing call	This field displays the number of calls you have missed since the WiMAX Device last restarted or was turned on.
Outgoing call	This field displays the number of calls you have made through the connected phone since the WiMAX Device last restarted or was turned on.
Connect	Click this to register the WiMAX Device to the specified register server.
Disconnect	Click this to de-register the WiMAX Device with the register server.

10.3 Server

Click **VoIP > Account 1 (or Account 2) > Server** to configure the registrar server, proxy server and outbound proxy server for this SIP account.

Figure 93 Server



The following table describes the labels in this screen.

Table 71 Server

LABEL	DESCRIPTION
Registrar Server	
Registrar Server	Enter the IP address or domain name of a register server. You can use up to 63 printable ASCII characters.
Port Number	Enter the SIP server's listening port number. Keep the default value, if you are not sure of this value.

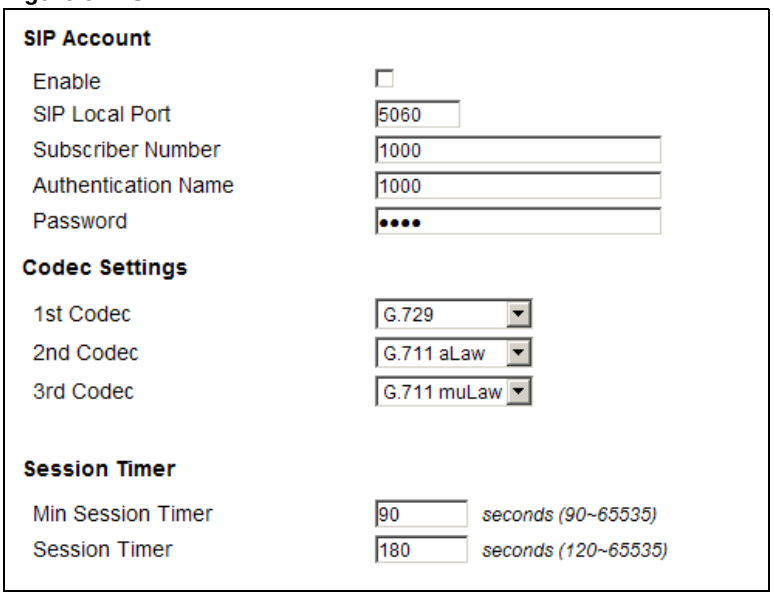
Table 71 Server (continued)

LABEL	DESCRIPTION
SIP Service Domain	Enter the IP address or domain name of a SIP server, if your VoIP service provider gave you one. Otherwise, enter the same address that you have entered in the **Registrar Server** field. You can use up to 63 printable ASCII characters.
Register Period Time	Enter the registration expiry time in seconds for the SIP account specified in Section 10.4 on page 163. The allowable range is 60~65535 seconds. However, this value is just a default preference value by user, the actual registration expiry time used by the SIP account is determined by the registrar server after the registration process. Once the SIP account has registered at the registrar server successfully, the WiMAX Device will send a re-register message to keep alive the successfully registered status at every half of the registration expiry time determined by the registrar server. If the keep-alive action failed, the register status described in Section 10.2 on page 160 will become **Error** state and you can not make any call in this status. However, after 512 seconds (fixed value), the WiMAX Device will send a register message again to try to recover a successfully registered status.
Proxy Server	
Proxy Server	Enter the IP address or domain name of the SIP proxy server provided by your VoIP service provider. You can use up to 63 printable ASCII characters.
Port Number	Enter the SIP proxy server's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.
Outbound Server	
Outbound Server	Enter the IP address or domain name of the outbound proxy server provided by your VoIP service provider. You can use up to 63 printable ASCII characters. If you choose not to use an outbound proxy server, set this to **0.0.0.0**.
Port Number	Enter the outbound proxy's listening port number, if your VoIP service provider gave you one. Otherwise, leave it as the default '5060'. If the outbound proxy is disabled (set to **0.0.0.0**), then this port will be ignored.

10.4 SIP

Click **VoIP > Account 1 (or Account 2) > SIP** to configure SIP settings.

Figure 94 SIP



The following table describes the labels in this screen.

Table 72 SIP

LABEL	DESCRIPTION
SIP Account	
Enable	Select this if you want the WiMAX Device to use this account. Clear it if you do not want the WiMAX Device to use this account.
SIP Local Port	Enter the WiMAX Device's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.
Subscriber Number	Enter your SIP number. In the full SIP URI, this is the part before the @ symbol. You can use up to 1-31 printable ASCII characters.
Authentication Name	Type the SIP user name associated with this account for authentication to the SIP register server. This field can be 1-31 printable characters (A-Z, a-z, 0-9).
Password	Type the SIP password associated with this account. This field can be 0-31 printable characters (A-Z, a-z, 0-9), underscores (_), pluses (+), periods (.), and "at" symbols (@).
Codec Settings	

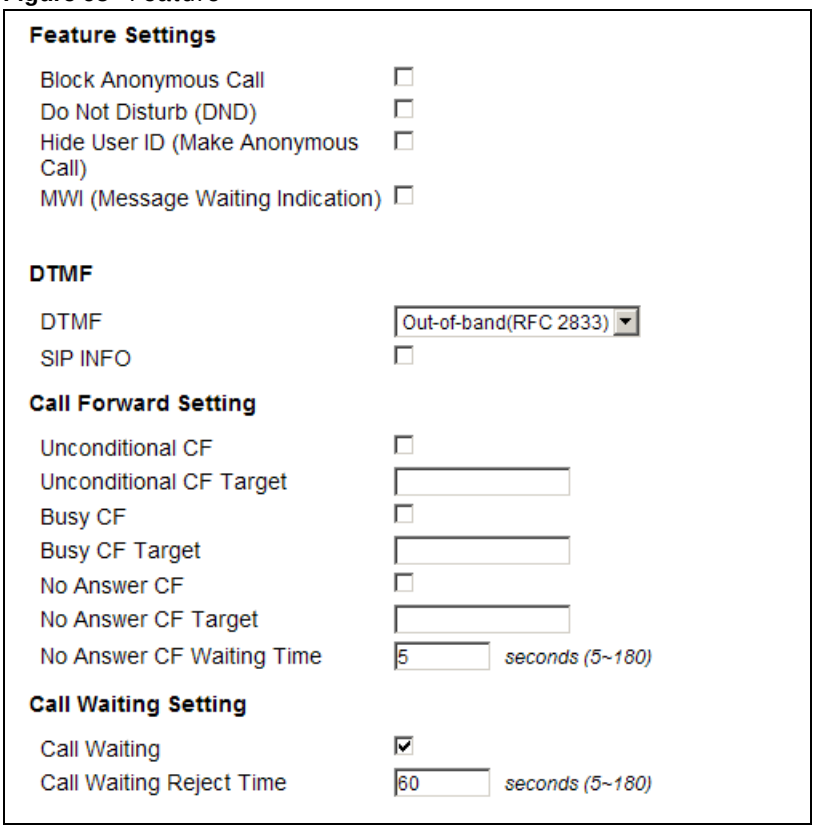
Table 72 SIP (continued)

LABEL	DESCRIPTION
1st Codec, 2nd Codec, 3rd Codec	Select the WiMAX Device's first, second, and third choices of the type of voice coder/decoder (codec) that you want the phone line to use when communicating with the SIP server. The following codecs (shown in highest quality to lowest quality order) are supported by the WiMAX Device: • **G.711 aLaw** (typically used in Europe) • **G.711 muLaw** (typically used in North America and Japan) • **G.729** You can also select **NONE** for the 2nd and 3rd codecs if your VoIP service provider only gave you one or two codec settings. When two SIP devices start a SIP session, they must agree on a codec.
Session Timer	
Min Session Timer	Enter the minimum session expiry time in seconds. The allowable range is 90~65535 seconds. When an incoming call requests a session expiry time that is lower than this value, the WiMAX Device will respond with a "423 session timer too small" message and tell the peer to use this value as the minimum bound.
Session Timer	Enter the session expiry time in seconds for all phone connections on this trunk. The allowable range is 120~65535 seconds. This value cannot be lower than the **Min Session Timer**. The WiMAX Device will use INVITE or UPDATE method to keep alive a session every half of the session expiry time during a call. If the keep-alive action is successful, the WiMAX Device will re-start the timer and do another keep-alive action after it reaches half of the session expiry time. If the keep-alive action failed, the call will terminate automatically. See Section 9.4 on page 155 to configure the Refresh Method with the INVITE or UPDATE method.

10.5 Feature

Click **VoIP > Account 1 (or Account 2) > Feature** to configure advanced VoIP features such as DTMF, Call Forwarding and Call Waiting.

Figure 95 Feature



The following table describes the labels in this screen.

Table 73 Feature

LABEL	DESCRIPTION
Feature Settings	
Block Anonymous Call	Select this to have the WiMAX Device block all incoming calls from phone that do not send caller ID.
Do Not Disturb (DND)	Select this to have the WiMAX Device not forward calls to the phone line while processing incoming calls. Thus, for any incoming call, the remote peer can hear ringback tone, but the phone connected on the WiMAX Device would not ring. Meanwhile, the WiMAX Device can still make outgoing calls as usual. Note: The DND function should be used very carefully, since enabling DND makes the WiMAX Device not forward any incoming call to the phone line so the user would never know whether there are any incoming calls.
Hide User ID (Make Anonymous Call)	Select this to not have your Caller ID (number) displayed on the callee's screen.

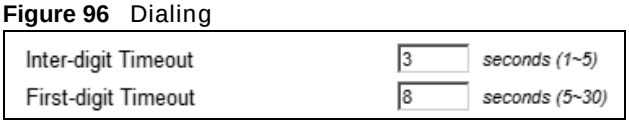
Table 73 Feature (continued)

LABEL	DESCRIPTION
MWI (Message Waiting Indication)	Select this to enable Message Waiting Indicator (MWI) function for this SIP account specified in Section 10.4 on page 163. When there is at least one new voice mail for the SIP account, the voice LED turns yellow and the WiMAX Device sends a beeping tone to the phone while user picks-up the phone to make calls.
DTMF	
DTMF	Control how the WiMAX Device handles the DTMF tone relay to the communication peer. The DTMF tone is generated by the phone when you push its digit buttons during a call. One application is to send numbers when trying to do IVR (Interactive Voice Response) service with server. You should use the same mode as your VoIP service provider. The choices are: • **Out-of-band(RFC 2833)** - Follow the RFC 2833 standard and send the DTMF tones in RTP packets. • **In Band** - Send the DTMF tones in the voice data stream. This works best when you are using a codec that does not use compression (like G.711). Codecs that use compression (like G.729) can distort the tones.
SIP INFO	Select this to have the WiMAX Device send the DTMF tones in SIP messages.
Call Forward Setting	
Unconditional CF, Unconditional CF Target	Select this if you want the WiMAX Device to forward all incoming calls to the specified phone number, regardless of other rules in this Call Forward Setting section. Specify the phone number in the **Unconditional CF Target** field. Note: The Unconditional CF function should be used very carefully, since enabling this function makes the WiMAX Device forward all incoming calls to another phone number, so the user would never know if there are any incoming calls.
Busy CF, Busy CF Target	Select this if you want the WiMAX Device to forward incoming calls to the specified phone number if the phone port is busy. Specify the phone number in the **Busy CF Target** field. 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 CF, No Answer CF Target, No Answer CF Waiting Time	Select this if you want the WiMAX Device to forward incoming calls to the specified phone number if the call is unanswered. Specify the phone number in the **No Answer CF Target** field on the right. Specify the time to wait before forwarding incoming calls in the **No Answer CF Waiting Time** field.
Call Waiting Setting	
Call Waiting	Select this to enable call waiting for this SIP account on the WiMAX Device.
Call Waiting Reject Time	Enter time to wait before rejecting a call when call waiting is enabled.

10.6 Dialing

Click **VoIP > Account 1 (or Account 2) > Dialing** to configure dialing timeout values.

Figure 96 Dialing



The following table describes the labels in this screen.

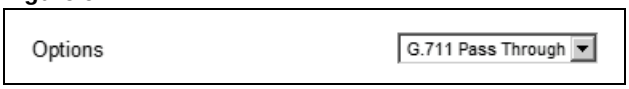
Table 74 Dialing

LABEL	DESCRIPTION
Inter-digit Timeout	Set the time in seconds (1~5) the WiMAX Device waits for each digit input of a complete callee number after you press the first key on the phone. If the WiMAX Device cannot receive the next digit entered within this time period, the WiMAX Device processes digits you have dialed.
First-digit Timeout	Set the number of seconds (5~30) for the WiMAX Device to wait for you to start dialing a number after you pick up the telephone receiver. If you do not dial any number within that time period, the dial tone becomes a busy signal. Put back the receiver and pick it up again if you want to make a new call.

10.7 FAX

Click **VoIP > Account 1 (or Account 2) > FAX** to configure which standard the account uses for fax services.

Figure 97 FAX



The following table describes the labels in this screen.

Table 75 FAX

LABEL	DESCRIPTION
Options	Select which standard the WiMAX Device uses to handle faxes. The peer devices must also use standard. **G.711A Pass Through** - Select this option to send and receive fax messages over the network or Internet using VoIP (G.711a). By encoding fax data as audio data, faxes may be susceptible to packet loss and other errors. However, as this standard is considerably older than T.38, it is more compatible with older obsolete systems. **T.38 FAX Relay** - WiMAX Device encodes fax messages to T.38 packets and sends as UDP packets through IP networks. This provides better quality, but it may have interoperability problems.

10.8 Technical Reference

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

10.8.1 SIP Call Progression with Session Timer

The following figure displays the basic steps in the setup and tear down of a SIP call with session timer supported by both peers. The UPDATE method is used to refresh the session. A calls B and

uses proxy server P. Messages include Session Expiry (SE) and Minimum Session Expiry (MSE) time values. When the duration of the call reaches half of the SE time period, the session is refreshed.

Table 76 SIP Call Progression

A	P	B
1. INVITE SE: 60 ---------->		
	2. 422 MSE: 3600 <----------	
3. ACK ---------->		
4. INVITE SE: 3600 MSE: 3600 ---------->		
	5. INVITE SE: 3600 MSE: 3600<br---------->	
		6. INVITE SE: 3600 MSE: 3600<br---------->
		7. OK SE: 3600 <----------
	8. OK SE: 3600 <----------	
9. OK SE: 3600 <----------		
10. ACK ---------->		
	11. ACK ---------->	---------->
	12. Dialogue (voice traffic)	

Table 76 SIP Call Progression (continued)

A	P	B
13. UPDATE SE: 3600 ---------->		
	14. UPDATE SE:3600 ---------->	---------->
	<----------	15. OK SE: 3600 <----------
16. OK SE: 3600 <----------		
17. BYE ---------->		
		18. OK <----------

1 A sends a SIP INVITE request. This message is an invitation for B to participate in a SIP telephone call. A's INVITE specifies a SE of 60 seconds.

2 A's request arrives at P but is below the minimum allowed value of 3600, so it is rejected with a 422 message, which contains the MSE of 3600.

3 A sends an ACK to acknowledge the message was received.

4 A retries the INVITE request with SE of 3600 and MSE of 3600.

5 The SE in the new INVITE is acceptable so P forwards it to B.

6 B receives the INVITE.

7 B responds with an OK message which includes the SE of 3600.

8 P forwards the OK message to A.

9 A receives the OK.

10 A then sends an ACK message to acknowledge that the call is established completely.

11 The proxy server forwards the ACK message to B.

12 Now A and B exchange voice media (talk).

13 After around half of the SE time period is reached, or 1800 seconds in this case, A sends an UPDATE request to refresh the session.

14 The UPDATE request is forwarded by P to B.

15 B receives the UPDATE request and responds with an OK message.

16 The OK message is received by A.

17 After talking, A hangs up and sends a BYE request.

18 B replies with an OK response confirming receipt of the BYE request and the call is terminated.

10.8.2 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.

For more information on the SIP protocol, please refer to RFC 3261.

11

The VoIP Line Screens

11.1 Overview

The features mentioned in this chapter are for models with VoIP function.

The **VoIP > Line 1 (or Line 2)** screens allow you to configure the volume, echo cancellation, VAD settings and custom tones for the phone port which maps to the SIP account (see Chapter 10 on page 157).

Note: If your WiMAX Device has only one phone port, there is only one line.

Note: You can identify the number of phone ports available on your WiMAX Device by its model name. See Section 1.1 on page 17 for more information.

11.1.1 What You Need to Know

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

Voice Activity Detection/Silence Suppression/Comfort Noise

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

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

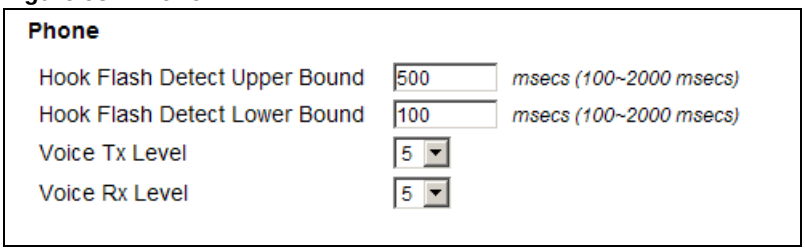
Echo Cancellation

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

11.2 Phone

Click **VoIP > Line 1 (or Line 2) > Phone** to configure phone related settings.

Figure 98 Phone



The following table describes the labels in this screen.

Table 77 Phone

LABEL	DESCRIPTION
Phone	
Hook Flash Detect Upper Bound	Enter the number of milliseconds for the upper bound of a quick on-hook and off-hook cycle in order to recognize a hook flash event.
Hook Flash Detect Lower Bound	Enter the number of milliseconds for the lower bound of a quick on-hook and off-hook cycle in order to recognize a hook flash event.
Voice Tx Level	Select the volume level transmitted by the WiMAX Device. -9 is the quietest, and 9 is the loudest.
Voice Rx Level	Select the volume level transmitted to the WiMAX Device. -9 is the quietest, and 9 is the loudest.

11.3 Voice

Click **VoIP > Line 1 (or Line 2) > Voice** to configure voice settings.

Figure 99 Voice

The following table describes the labels in this screen.

Table 78 Voice

LABEL	DESCRIPTION
VAD - Voice Activity Detection	
Enable VAD	Enable Voice Active Detector (VAD) to have the WiMAX Device stop transmitting voice traffic when you are not speaking using the detection method. This reduces the bandwidth the WiMAX Device uses.

Table 78 Voice (continued)

LABEL	DESCRIPTION
LEC - Line Echo Cancellation	
Line Echo Canceller Tail Length	Select the maximum number of milliseconds of an echo length (16 ms, 32 ms or 48 ms) the WiMAX Device can handle and eliminate the effect. An echo is normally caused by the sound of your voice reverberating in the telephone receiver while you talk. Select **Disable** to turn this feature off.

11.4 Region

Click **VoIP > Line 1 (or Line 2) > Region** to maintain settings that depend on which region of the world the WiMAX Device is in.

Figure 100 Region

The following table describes the labels in this screen.

Table 79 Region

LABEL	DESCRIPTION
Country Profile	Select the place in which the WiMAX Device is located, **USA** (Default) or any other country.

12

Maintenance

12.1 Overview

Use these screens to manage and maintain your WiMAX Device.

12.1.1 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. You have disabled that service in one of the remote management screens.
2. The IP address in the **Secured Client IP** field does not match the client IP address. If it does not match, the WiMAX Device will disconnect the session immediately.
3. There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.

Remote Management and NAT

When NAT is enabled:

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

System Timeout

There is a default system management idle timeout of five minutes. The WiMAX Device automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling.

SNMP

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

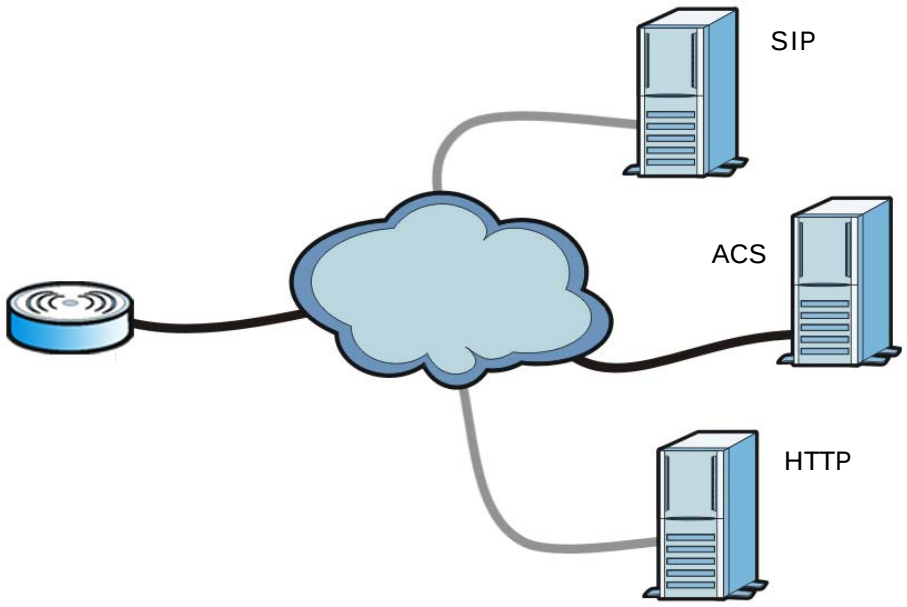
Note: SNMP is only available if TCP/IP is configured.

TR-069

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

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

Figure 101 TR-069 Example



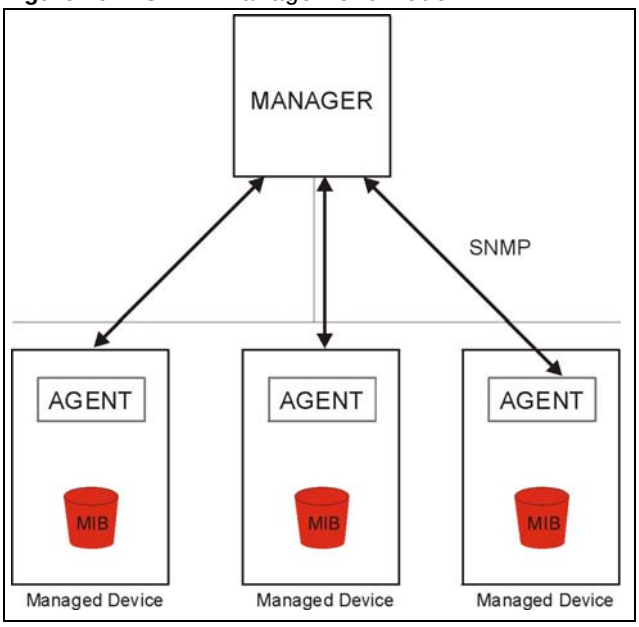
In this example, the WiMAX Device receives data from at least 3 sources: A SIP server for handling voice calls, an HTTP server for handling web services, and an ACS, for configuring the WiMAX Device remotely. All three servers are owned and operated by the client’s Internet Service Provider. However,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

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

SNMP

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

Figure 102 SNMP Management Model



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

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

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

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

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

Table 80 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	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.

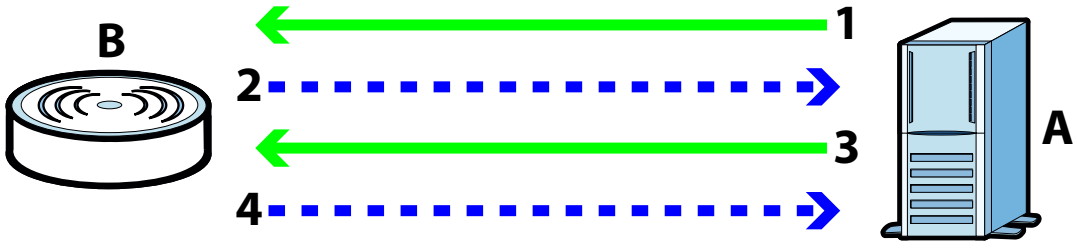
OMA-DM

When the WiMAX Device initiates communication with the server (often times at start up or after the first time you turn it on), the server uploads commands, new files (if any), and other information used by a service provider to customize the WiMAX Device's features.

Device management works as follows:

1. The server (**A**) sends out the query (**1**) to the WiMAX Device (**B**).
2. The WiMAX Device responds by sending back its credentials (**2**), to which the server responds with its credentials along with a string of management operations (**3**).
3. The client responds to the management operations (**4**), perhaps confirming file alterations or confirming receipt of file uploads and so on.
4. The server disconnects from the WiMAX Device once all of its management operations have been carried out.

Figure 103 OMA-DM Data Management



OMA-DM Authentication

In order to ensure the integrity of the connection between an OMA-DM server and the WiMAX Device, communication between the two is encoded using one of three common algorithms. They are not intended to be used in lieu of proper digital security, but instead as a means of transmitting

multiple disparate types of data over HTTP. Security encryption for communication is handled by different processes configured elsewhere in the WiMAX Device's web configurator

Basic Access Authentication — Sends a person's user name and password in Base64. This authentication protocol is supported by all browsers that are HTTP 1.0/1.1 compliant. Although converted to Base64 for the sake of cross-compatibility, credentials are nonetheless passed between the web browser and the server in plaintext, making it extremely easy to intercept and read. As such, it is rarely used anymore.

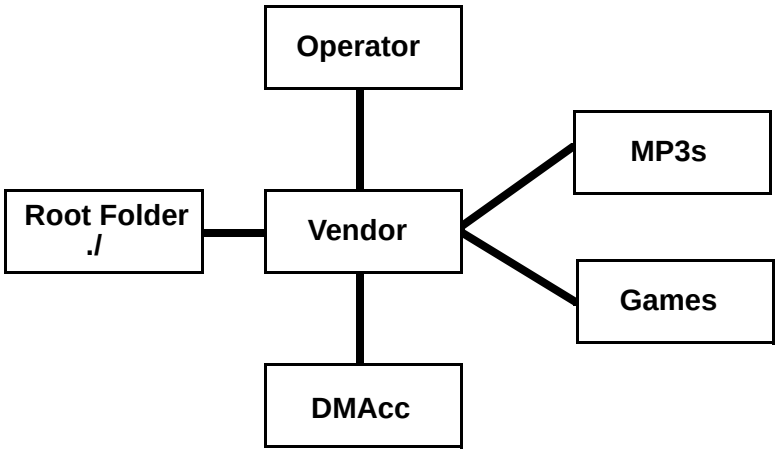
Digest Access Authentication — This protocol was designed to replace basic access authentication. Instead of encoding a user name and password in plaintext, this protocol uses what is known as an MD5 message authentication code. It allows the server to issue a single-use, randomly generated number (known as a 'nonce') to the client (in this case, the web browser), which then uses the number as the 'public key' for encrypting its data. When the server receives the encrypted data, it unlocks it using the 'key' that was just provided. While stronger than basic access authentication, this protocol is not as strong as, say, HMAC, or as secure as the client using a client-side private key encryption scheme.

Hash Message Authentication Code — Also known as HMAC, this code relies on cryptographic hash functions to bolster an existing protocol, such as MD5. It is a method for generating a stronger, significantly higher encryption key.

OMA-DM Data Model

Each device that conforms to the current OMA-DM standard has an identical data structure embedded in its controlling firmware. This allows a similarly conforming OMA-DM server to navigate the folder structure and to make file alterations where appropriate or required.

Figure 104 OMA-DM Data Model



In the example data model shown here, the parent folders must conform to the OMA-DM standard. The child folders, on the other hand, can be customized on an individual basis. This allows the parent folders to all maintain a consistent URI (Uniform Resource Identifier) across all devices that meet the OMA-DM standard's requirements.

For example, in the preceding figure the URI for the "Games" folder is "./Vendor/Games/". The "./Vendor/" portion of the URI exists on all devices that conform to the OMA-DM standard. The "Games" folder, however, may or may not exist depending on the services provided by the company managing the device.

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

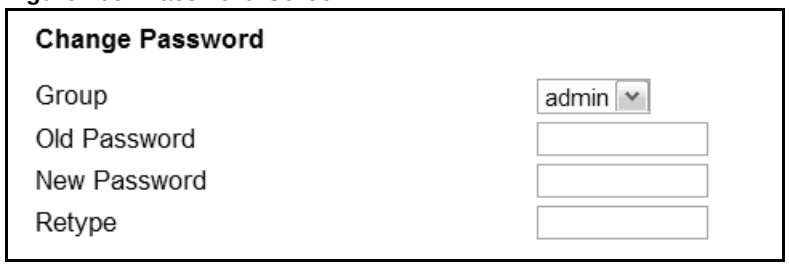
NTP stands for Network Time Protocol. It is employed by devices connected to the Internet in order to obtain a precise time setting from an official time server. These time servers are accurate to within 200 microseconds.

12.2 Password

Use this screen to set up admin and guest accounts for logging into and managing the WiMAX Device. The “admin” user can access and configure all screens. The “guest” user can only perform some basic settings such as viewing the system status information, configuring LAN, NAT, DDNS, and Firewall settings and reset the WiMAX Device to factory defaults and restart the WiMAX Device.

Click **Maintenance > Password** to open this screen as shown next.

Figure 105 Password Screen



This screen contains the following fields:

Table 81 Password

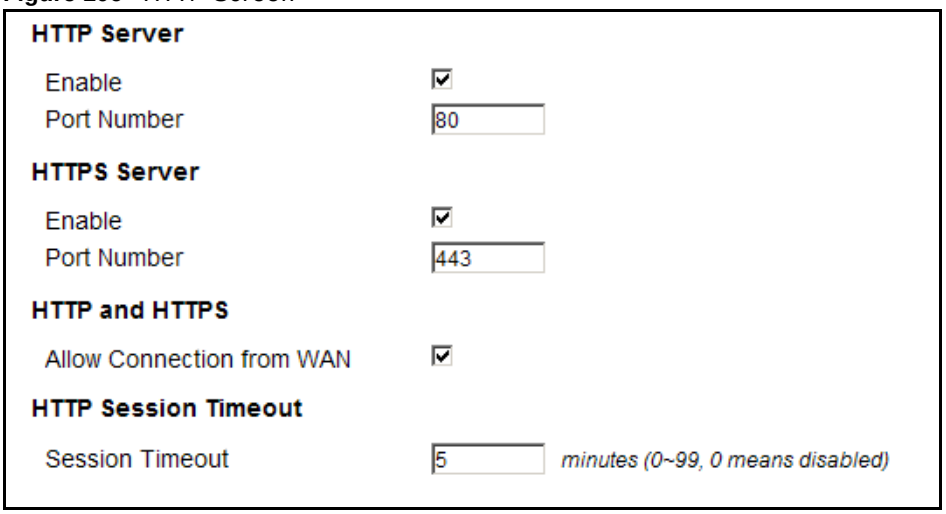
LABEL	DESCRIPTION
Group	Select the group for which you want to change the login password.
Old Password	Enter the old password for the login group.
New Password	Enter the new password for the login group.
Retype	Retype the new password for the login group.

12.3 HTTP

Use this screen to allow remote access to the WiMAX Device from a network connection over HTTP.

Click **Maintenance > Remote MGMT > HTTP** to open this screen as shown next.

Figure 106 HTTP Screen



This screen contains the following fields:

Table 82 HTTP

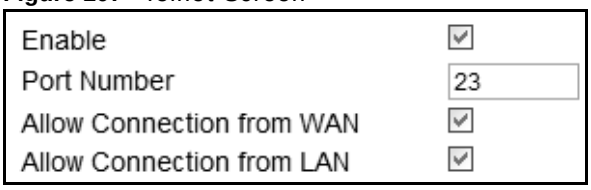
LABEL	DESCRIPTION
HTTP Server	
Enable	Select this to enable remote management using this service.
Port Number	Enter the port number this service can use to access the WiMAX Device. The computer must use the same port number.
HTTPS Server	
Enable	Select this to enable remote management using this service.
Port Number	Enter the port number this service can use to access the WiMAX Device. The computer must use the same port number.
HTTP and HTTPS	
Allow Connection from WAN	Select this to allow incoming connections from the WAN over either HTTP or HTTPS.
HTTP Session Timeout	
Session Timeout	Enter the number of minutes (0-99) the WiMAX Device waits to delete an inactive web connection (HTTP or HTTPS).

12.4 Telnet

Use this screen to allow remote access to the WiMAX Device from a network connection over Telnet.

Click **Maintenance > Remote MGMT > Telnet** to open this screen as shown next.

Figure 107 Telnet Screen



This screen contains the following fields:

Table 83 Telnet

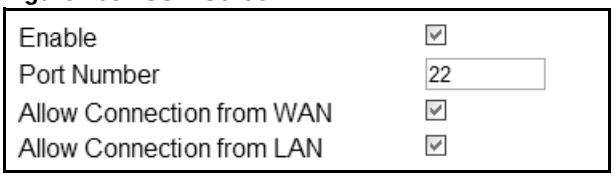
LABEL	DESCRIPTION
Enable	Select this to enable remote management using this service.
Port Number	Enter the port number this service can use to access the WiMAX Device. The computer must use the same port number.
Allow Connection from WAN	Select this to allow connections using this service that originate on the WAN.
Allow Connection from LAN	Select this to allow connection using this service that originate on the LAN.

12.5 SSH

Use this screen to allow remote access to the WiMAX Device from a network connection over SSH.

Click **Maintenance > Remote MGMT > SSH** to open this screen as shown next.

Figure 108 SSH Screen



This screen contains the following fields:

Table 84 SSH

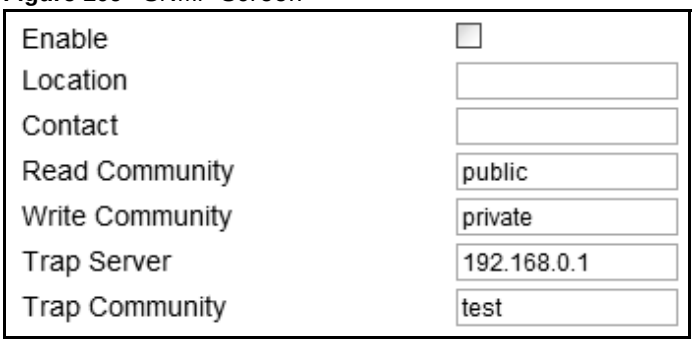
LABEL	DESCRIPTION
Enable	Select this to enable remote management using this service.
Port Number	Enter the port number this service can use to access the WiMAX Device. The computer must use the same port number.
Allow Connection from WAN	Select this to allow connections using this service that originate on the WAN.
Allow Connection from LAN	Select this to allow connection using this service that originate on the LAN.

12.6 SNMP

Use this screen to allow remote access to the WiMAX Device from a network connection over SNMP.

Click **Maintenance > Remote MGMT > SNMP** to open this screen as shown next.

Figure 109 SNMP Screen



This screen contains the following fields:

Table 85 SNMP

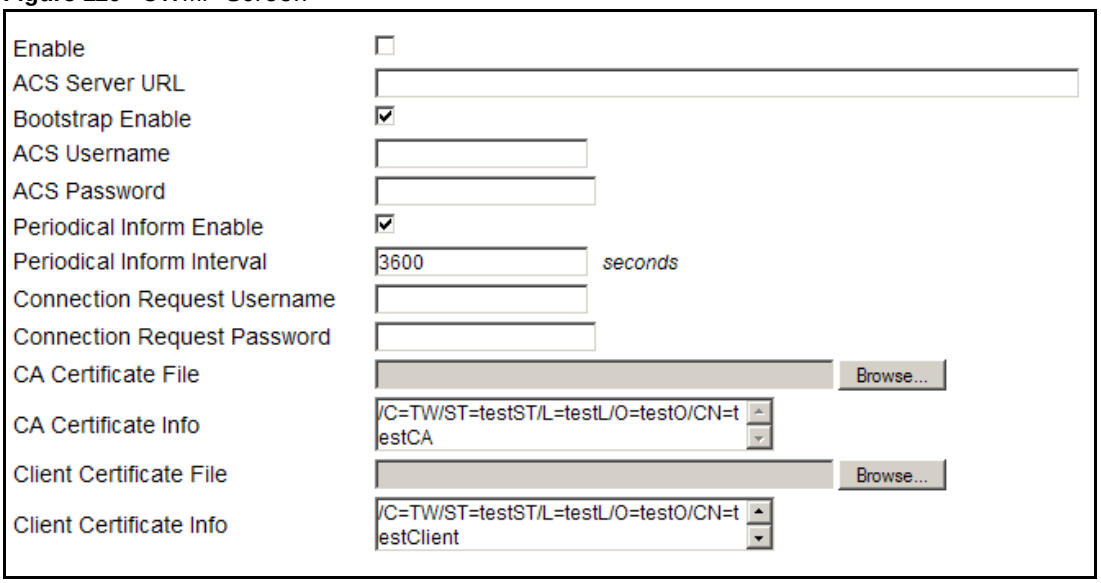
LABEL	DESCRIPTION
Enable	Select this to enable remote management using this service.
Location	Enter the location of the SNMP server (for example, “Engineering Dept., Floor 6, Building A, New York City”).
Contact	Enter contact information for the administrator managing the SNMP server (for example, “Bill Smith, IT Dept., (555) 555-5454”).
Read Community	Enter the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Write Community	Enter the password for incoming Set requests from the management station. The default is public and allows all requests.
Trap Server	Enter the IP address of the station to send your SNMP traps to.
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.

12.7 CWMP

Use this screen to allow CWMP connections for remote management, firmware upgrades and troubleshooting.

Click **Maintenance > Remote MGMT > CWMP** to open this screen as shown next.

Figure 110 CWMP Screen



This screen contains the following fields:

Table 86 CWMP

LABEL	DESCRIPTION
Enable	Select this to enable remote management using this service.
ACS Server URL	Enter the URL or IP address of the auto-configuration server.
Bootstrap Enable	Select this to enable bootstrap events.
ACS Username	Enter the user name sent when the WiMAX Device connects to the ACS and which is used for authentication. You can enter up to 31 alphanumeric characters (a-z, A-Z, 0-9) and underscores but spaces are not allowed.
ACS Password	Enter the password sent when the WiMAX Device connects to an ACS and which is used for authentication. You can enter up to 31 alphanumeric characters (a-z, A-Z, 0-9) and underscores but spaces are not allowed.
Periodical Inform Enable	Select this to allow the WiMAX Device to periodically connect to the ACS and check for configuration updates. If you do not enable this feature then the WiMAX Device can only be updated automatically when the ACS initiates contact with it and if you selected the checkbox on this screen.
Periodical Inform Interval	Enter the time interval (in seconds) at which the WiMAX Device connects to the auto-configuration server.
Connection Request Username	Enter the connection request user name that the ACS must send to the WiMAX Device when it requests a connection. You can enter up to 31 alphanumeric characters (a-z, A-Z, 0-9) and underscores but spaces are not allowed. Note: This must be provided by the ACS administrator.

Table 86 CWMP (continued)

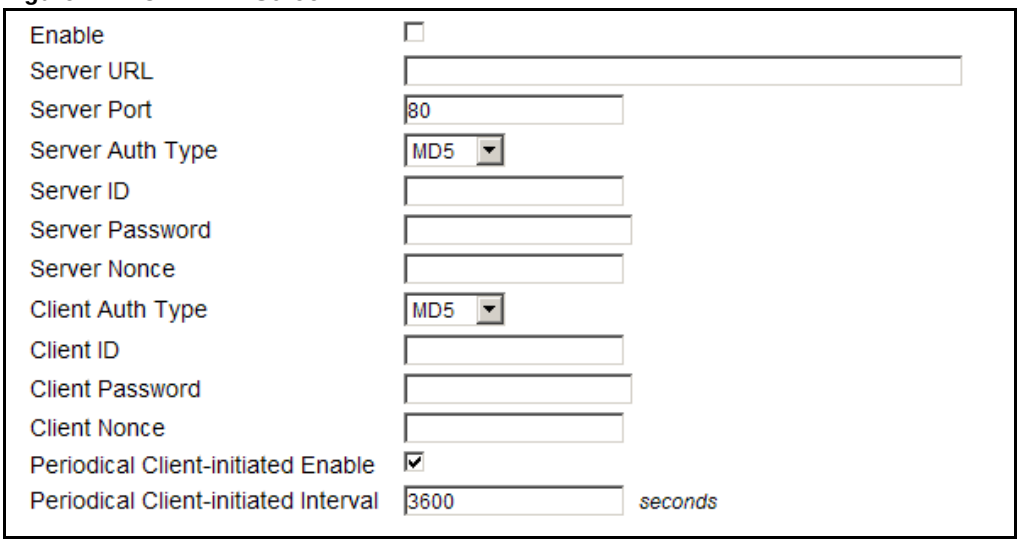
LABEL	DESCRIPTION
Connection Request Password	Enter the connection request password that the ACS must send to the WiMAX Device when it requests a connection. You can enter up to 31 alphanumeric characters (a-z, A-Z, 0-9) and underscores but spaces are not allowed. Note: This must be provided by the ACS administrator.
CA Certificate File	Click **Browse** to upload a Certificate Authority (CA) certificate to the WiMAX Device.
CA Certificate Info	This displays information about the currently active CA certificate.
Client Certificate File	Click **Browse** to upload a client certificate to the WiMAX Device.
Client Certificate Info	This displays information about the currently active client certificate.

12.8 OMA-DM

Use this screen to allow remote access to the WiMAX Device from a network connection over OMA-DM.

Click **Maintenance > Remote MGMT > OMA-DM** to open this screen as shown next.

Figure 111 OMA-DM Screen



This screen contains the following fields:

Table 87 OMA-DM

LABEL	DESCRIPTION
Enable	Select this to enable remote management using this service.
Server URL	Enter the IP address or URL of the OMA-DM server that you intend to use to manage this device.

Table 87 OMA-DM (continued)

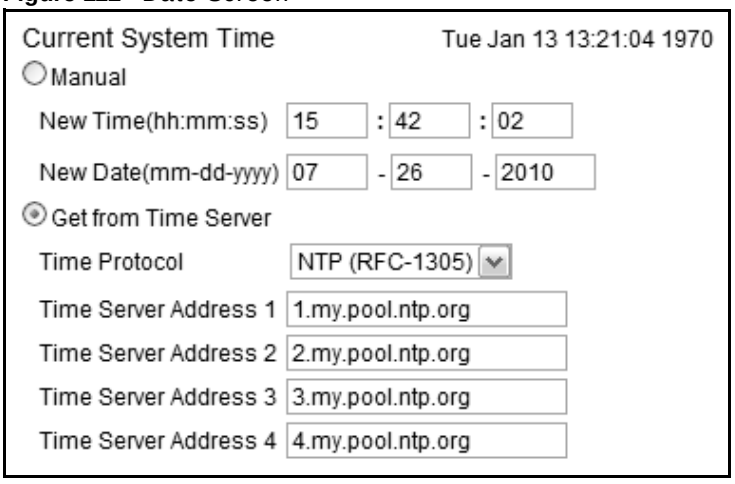
LABEL	DESCRIPTION
Server Port	Enter the port number for the IP address of the OMA-DM server set up in the preceding field.
Server Auth Type	Select the encryption algorithm scheme used by the OMA-DM server to communicate with client devices. If the scheme selected here does not match the actual scheme used by the server, then server will challenge the WiMAX Device to automatically update its settings. • **None** - No authentication. • **Basic** - Server ID and Password are encoded using a Basic Access Authentication Code. • **Digest (MD5)** - Server ID and Password are encoded using a Digest Access Authentication Code. • **HMAC** - Server ID and Password are encoded using a keyed Hash Message Authentication Code.
Server ID	Enter the identification code for the server. This is used by the WiMAX Device during the communication handshake process to identify the server.
Server Password	Enter the password for the server's identification code. This shared public key is used by the WiMAX Device during the communication handshake process to identify the server.
Server Nonce	The WiMAX Device and the OMA-DM server use nonces to authenticate each other if you select **MD5** as the authentication algorithm in the **Server Auth Type** field. Nonce is an abbreviation of 'number used once'. It is normally a random or pseudo-random number applied in an authentication protocol to protect existing communications from being reused in 'replay attacks'. Type up to 20 digits for the OMA-DM server nonce.
Client Auth Type	Select the encryption algorithm scheme used by the OMA-DM server to communicate with client devices. If the scheme selected here does not match the actual scheme used by the server, then server will challenge the WiMAX Device to automatically update its settings. • **None** - No authentication. • **Basic** - Server ID and Password are encoded using a Basic Access Authentication Code. • **Digest (MD5)** - Server ID and Password are encoded using a Digest Access Authentication Code. • **HMAC** - Server ID and Password are encoded using a keyed Hash Message Authentication Code. Note: Make sure that the scheme selected here matches the **Server Auth Type**.
Client ID	Enter the client name for the WiMAX Device.
Client Password	Enter the password for the WiMAX Device's client name.
Client Nonce	The WiMAX Device and the OMA-DM server use nonces to authenticate each other if you select **MD5** as the authentication algorithm in the **Client Auth Type** field. Type up to 20 digits for the OMA-DM client nonce.
Periodical Client-Initiated Enable	Select this to allow the WiMAX Device to periodically connect to the OMA-DM server and check for configuration updates. If you do not enable this feature then the WiMAX Device can only be updated automatically when the OM-DM server initiates contact with it and if you selected the checkbox on this screen.
Periodical Client-Initiated Interval	Enter the time interval (in seconds) at which the WiMAX Device connects to the OMA-DM server.

12.9 Date/Time

Use these settings to set the system time or configure an NTP server for automatic time synchronization.

Click **Maintenance > Date/Time > Date** to open this screen as shown next.

Figure 112 Date Screen



This screen contains the following fields:

Table 88 Date

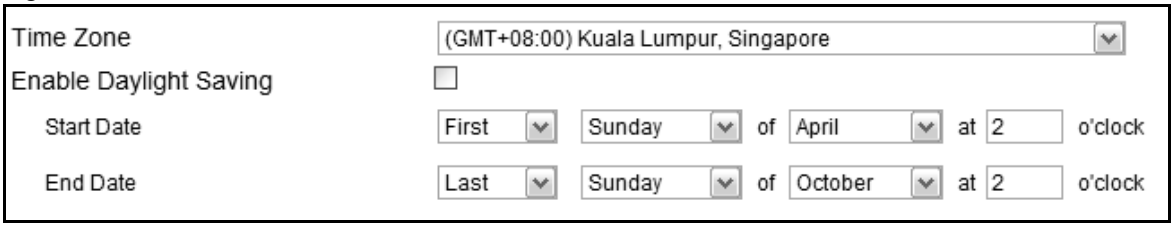
LABEL	DESCRIPTION
Manual	
New Time	Enter the new time in this field.
New Date	Enter the new date in this field.
Get from Time Server	
Time Protocol	Select the time service protocol that your time server uses.Check with your ISP or network administrator, or use trial-and-error to find a protocol that works. • **NTP (RFC 1305)** - This format is similar to Time (RFC 868).
Time Server Address 1~4	Enter the IP address or URL of your time server. Check with your ISP or network administrator if you are unsure of this information.

12.10 Time Zone

Use this screen to set the time zone in which the WiMAX device is physically located.

Click **Maintenance > Date/Time > Time Zone** to open this screen as shown next.

Figure 113 Time Zone Screen



This screen contains the following fields:

Table 89 Time Zone

LABEL	DESCRIPTION
Time Zone	Select the time zone at your location.
Enable Daylight Savings Time	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.

12.11 Upgrade File

Use this screen to browse to a firmware file on a local computer and upload it to the WiMAX Device. Firmware files usually use the system model name with a "*.bin" extension, such as "WiMAX Device.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system restarts.

Contact your service provider for information on available firmware upgrades.

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

Click **Maintenance > Firmware Upgrade > Upgrade File** to open this screen as shown next.

Figure 114 Upgrade File Screen

This screen contains the following fields:

Table 90 Upgrade File

LABEL	DESCRIPTION
Upgrade File	Click **Browse** then browse to the location of a firmware upgrade file and select it.
Upgrade	Click this to begin uploading the selected file. This may take up to two minutes. Note: Do not turn off the device while firmware upload is in progress!

12.11.1 The Firmware Upload Process

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

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

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

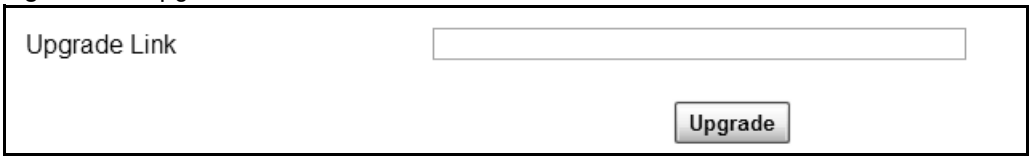
If the upload is not successful, you will be notified by error message.

12.12 Upgrade Link

Use this screen to set the URL of a firmware file on a remote computer and upload it to the WiMAX Device.

Click **Maintenance > Firmware Upgrade > Upgrade Link** to open this screen as shown next.

Figure 115 Upgrade Link Screen



This screen contains the following fields:

Table 91 Upgrade Link

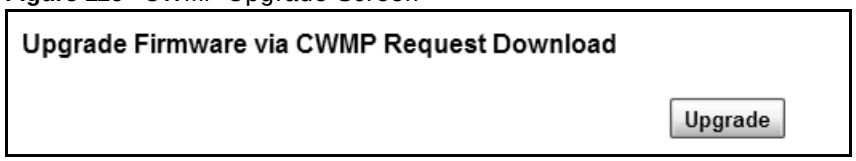
LABEL	DESCRIPTION
Upgrade Link	Enter the URL or IP address of the firmware's upgrade location on the network.
Upgrade	Click this to begin uploading the selected file. This may take up to two minutes. Note: Do not turn off the device while firmware upload is in progress!

12.13 CWMP Upgrade

Use this screen to upgrade the firmware on the WiMAX Device using CWMP Request Download.

Click **Maintenance > Firmware Upgrade > CWMP Upgrade** to open this screen as shown next.

Figure 116 CWMP Upgrade Screen



This screen contains the following fields:

Table 92 CWMP Upgrade

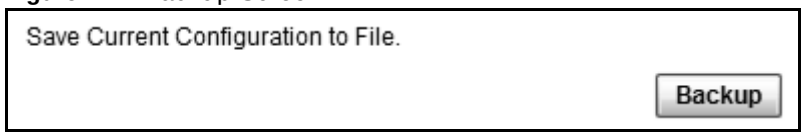
LABEL	DESCRIPTION
Upgrade	Click this to begin upgrading firmware using CWMP Request. This may take up to two minutes. Note: Do not turn off the device while firmware upload is in progress!

12.14 Backup/Restore

Use this screen to backup your current WiMAX Device settings to a local computer.

Click **Maintenance > Backup / Restore > Backup** to open this screen as shown next.

Figure 117 Backup Screen



This screen contains the following fields:

Table 93 Backup

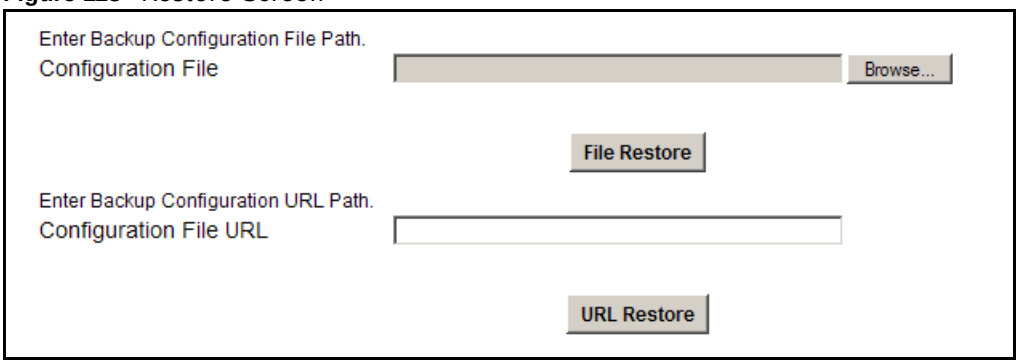
LABEL	DESCRIPTION
Backup	Click this to save the WiMAX Device's current configuration to a file on your computer. Once your device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file is useful if you need to return to your previous settings.

12.15 Restore

Use this screen to restore your WiMAX Device settings from a backup file on a local computer.

Click **Maintenance > Backup/Restore > Restore** to open this screen as shown next.

Figure 118 Restore Screen



This screen contains the following fields:

Table 94 Restore

LABEL	DESCRIPTION
Configuration File	Click **Browse...** then browse to the location of a firmware upgrade file and select it. Click **File Restore** to upload the specified configuration to the WiMAX Device and replace the current settings.
Backup Configuration File URL	Enter the URL or IP address of the backup configuration file's location on the network. Click **URL Restore** to upload the specified configuration to the WiMAX Device and replace the current settings.

12.15.1 The Restore Configuration Process

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

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

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

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

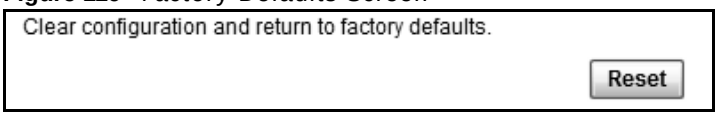
If the upload was not successful, you are notified with an error message.

12.16 Factory Defaults

Use this screen to restore the WiMAX Device to its factory default settings.

Click **Maintenance > Backup/Restore > Factory Defaults** to open this screen as shown next.

Figure 119 Factory Defaults Screen



This screen contains the following fields:

Table 95 Factory Defaults

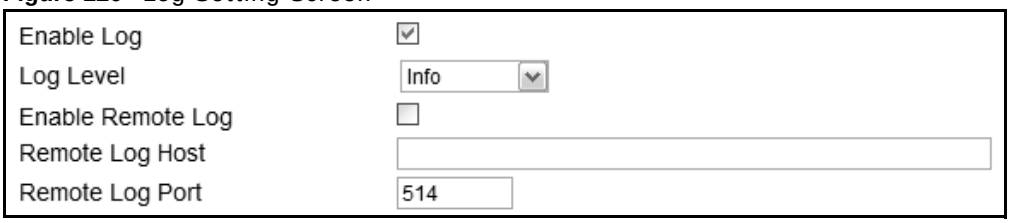
LABEL	DESCRIPTION
Reset	Click this to clear all user-entered configuration information and return the WiMAX Device to its factory defaults. There is no warning screen.

12.17 Log Setting

Use this screen to configure which type of events on the WiMAX Device are logged.

Click **Maintenance > LOG > Log Setting** to open this screen as shown next.

Figure 120 Log Setting Screen



This screen contains the following fields:

Table 96 Log Setting

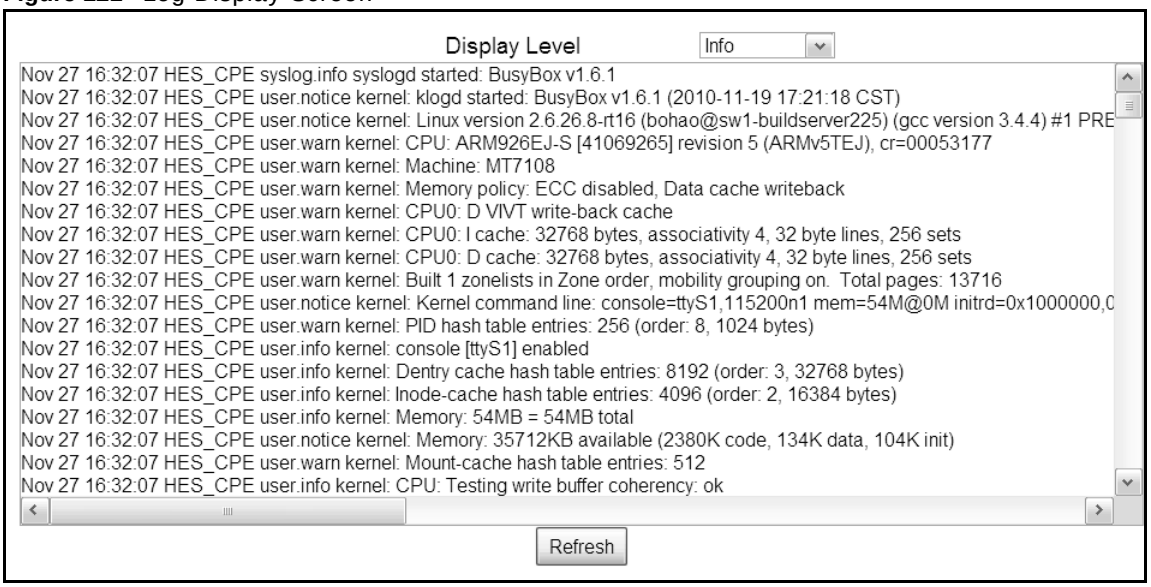
LABEL	DESCRIPTION
Enable Log	Select this to have the WiMAX Device log network activity according to the selected **Log Level**.
Log Level	Select the type of logs to record.
Enable Remote Log	Select this to allow logs to be recorded and stored on a remote logs server.
Remote Log Host	Enter the remote log host IP address if **Enable Remote Log** is selected.
Remote Log Port	Enter the remote log host port if **Enable Remote Log** is selected.

12.18 Log Display

Use this screen to view the log messages of the WiMAX Device.

Click **Maintenance > LOG > Log Display** to open this screen as shown next.

Figure 121 Log Display Screen



This screen contains the following fields:

Table 97 Log Display

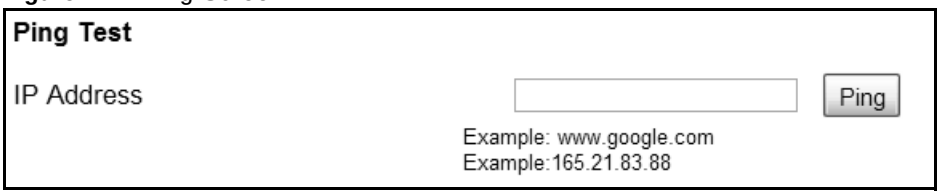
LABEL	DESCRIPTION
Display Level	Select the type of logs to display from this menu.
Refresh	Click this to refresh the logs in the display window.

12.19 Network Test

Use this screen to test network connectivity using ping.

Click **Maintenance > Network Test > Ping** to open this screen as shown next.

Figure 122 Ping Screen



This screen contains the following fields:

Table 98 Ping

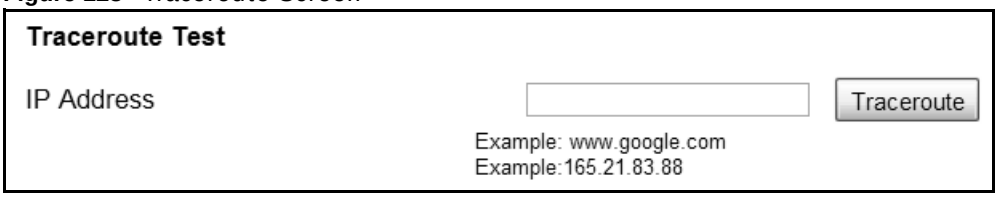
LABEL	DESCRIPTION
IP Address	Enter the IP address or domain name of a target device to which this test will send.
Ping	Click this to start the test. The result will show at the bottom of the screen.

12.20 Traceroute

Use this screen to test network connectivity using traceroute.

Click **Maintenance > Network Test > Traceroute** to open this screen as shown next.

Figure 123 Traceroute Screen



This screen contains the following fields:

Table 99 Traceroute

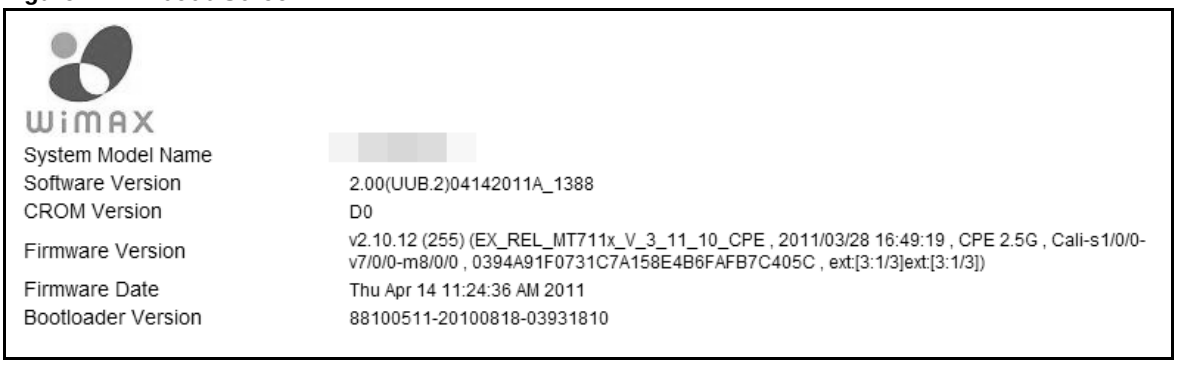
LABEL	DESCRIPTION
IP Address	Enter the IP address or domain name of a target device to which this test will send.
Traceroute	Click this to start the test. The result will show at the bottom of the screen.

12.21 About

This screen displays information about the WiMAX Device that can be useful when upgrading firmware, considering deployment options, and working with technical support if the device encounters difficulties.

Click **Maintenance > About** to open this screen as shown next.

Figure 124 About Screen



This screen contains the following fields:

Table 100 About

LABEL	DESCRIPTION
System Model Name	This field displays the WiMAX Device system name. It is used for identification.
Software Version	This field displays the Web Configurator software version that the WiMAX Device is currently running.
CROM Version	This field displays the CROM version number.
Firmware Version	This field displays the current version of the firmware inside the device.
Firmware Date	This field displays the date the firmware version was created.
Bootloader Version	This field displays the bootloader version.

12.22 Reboot

Use this screen to perform a software restart of the WiMAX Device. You may log in again within a few minutes of using the reboot button.

Click **Maintenance > Reboot** to open this screen as shown next.

Figure 125 Reboot Screen

This screen contains the following fields:

Table 101 Reboot

LABEL	DESCRIPTION
Reboot	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. Note: Wait one minute before logging back into the WiMAX Device after a restart.

13

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 Device Access and Login
- Internet Access
- Reset the WiMAX Device to Its Factory Defaults

13.1 Power, Hardware Connections, and LEDs

The WiMAX Device 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 Device.
2. Make sure the power adapter or cord is connected to the WiMAX Device 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 Device.
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 Chapter 14 on page 203 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 Device.
5. If the problem continues, contact the vendor.

13.2 WiMAX Device Access and Login

I forgot the IP address for the WiMAX Device.

1 The default IP address is **192.168.1.1**http://192.168.1.1.

2 If you changed the IP address and have forgotten it, you might get the IP address of the WiMAX Device 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 Device (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 Device to its factory defaults. See Section 13.6 on page 202.

I forgot the password.

1 The default password is **1234**.

2 If this does not work, you have to reset the WiMAX Device to its factory defaults. See Section 13.6 on page 202.

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://192.168.1.1**.
- If you changed the IP address (Section 7.6 on page 98), 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 Device.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Chapter 14 on page 203.

3 Make sure your Internet browser does not block pop-up windows and has JavaScript and Java enabled.

4 If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. Your WiMAX Device 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 Device.

5 Reset the WiMAX Device to its factory defaults, and try to access the WiMAX Device with the default IP address. See Section 13.6 on page 202..

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 Device using another service, such as Telnet. If you can access the WiMAX Device, check the remote management settings and firewall rules to find out why the WiMAX Device 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 Device.

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 Device. Log out of the WiMAX Device 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 Device.

4 If this does not work, you have to reset the WiMAX Device to its factory defaults. See Section 13.6 on page 202.

I cannot Telnet to the WiMAX Device.

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

13.3 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 Chapter 14 on page 203.

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. See Chapter 8 on page 125.

4 Check your WiMAX settings. The WiMAX Device may have been set to search the wrong frequencies for a wireless connection. See Chapter 6 on page 72. If you are unsure of the correct values, contact your service provider.

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

6 If the problem continues, contact your ISP.

I cannot access the Internet any more. I had access to the Internet (with the WiMAX Device), 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 Chapter 14 on page 203.

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

3 If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

1 The quality of the WiMAX Device's wireless connection to the base station may be poor. Poor signal reception may be improved by moving the WiMAX Device 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 Device away or switch the other devices off. Weather conditions may also affect signal quality.

3 There might be a lot of traffic on the network. Look at the LEDs, and check Chapter 14 on page 203. If the WiMAX Device is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.

4 Disconnect and re-connect the power adapter to the WiMAX Device.

5 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 **Strength Indicator** LEDs on the device.

2 Contact your ISP if the problem persists.

13.4 Wireless Internet Access (for Models with WiFi)

What factors may cause intermittent or unstabled wireless connection? How can I solve this problem?

The following factors may cause interference:

- Obstacles: walls, ceilings, furniture, and so on.
- Building Materials: metal doors, aluminum studs.
- Electrical devices: microwaves, monitors, electric motors, cordless phones, and other wireless devices.

To optimize the speed and quality of your wireless connection, you can:

- Move your WiMAX Device closer to the AP if the signal strength is low.
- Reduce wireless interference that may be caused by other wireless networks or surrounding wireless electronics such as cordless phones.
- Place the AP where there are minimum obstacles (such as walls and ceilings) between the AP and the wireless client.
- Reduce the number of wireless clients connecting to the same AP simultaneously, or add additional APs if necessary.
- Try closing some programs that use the Internet, especially peer-to-peer applications. If the wireless client is sending or receiving a lot of information, it may have too many programs open that use the Internet.

13.5 Phone Calls and VoIP (for Models with Phone Ports)

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

Check the telephone connections and telephone wire.

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

1. The **PHONE** LED should come on. Make sure that your telephone is connected to the **PHONE** port.
2. You can also check the VoIP status in the **VoIP > Account > Status** screen.
3. Make sure your settings for your VoIP account are correct. If your phone still cannot work, contact your VoIP service provider to make sure the account is active.

13.6 Reset the WiMAX Device to Its Factory Defaults

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**.

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

To reset the WiMAX Device,

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

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

13.6.1 Pop-up Windows, JavaScript and Java Permissions

Please see Appendix C on page 233.

Product Specifications

Table 102 LEDs Status for Indoor Device

LED	STATE	DESCRIPTION
Power 	Off	The WiMAX Device is not receiving power.
	Red	The WiMAX Device is receiving power but has been unable to start up correctly or is not receiving enough power. See the Troubleshooting section for more information.
	Green	**Solid**: The WiMAX Device is receiving power and functioning correctly. **Flashing**: the device is self-testing (startup).
WiMAX Link 	Off	The WiMAX Device is not connected to a wireless (WiMAX) network.
	Green	The WiMAX Device is successfully connected to a wireless (WiMAX) network.
	Green (Blinking Slowly)	The WiMAX Device is searching for a wireless (WiMAX) network.
	Green (Blinking Quickly)	The WiMAX Device has found a wireless (WiMAX) network and is connecting.
Signal Strength 1,2,3 	The Strength Indicator LEDs display the Interference-plus-Noise Ratio (CINR) of the wireless (WiMAX) connection.	
	No Signal LEDs On	There is no WiMAX connection.
	Signal 1 On	The signal strength is between -80dBm and -90dBm.
	Signal 1 and 2 On	The signal strength is between -70dBm and -80dBm.
	Signal 1, 2 and 3 On	The signal strength is greater than or equal to -70dBm.
Phone 1,2 (for models with VoIP feature) 	Off	No SIP account is registered, or the WiMAX Device is not receiving power.
	Green	A SIP account is registered.
	Green (Blinking)	A SIP account is registered, and the phone attached to the VoIP 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 VoIP port is in use (off the hook).
WLAN (for models with WLAN feature) 	Off	The Wi-Fi network is not operational.
	Green	The Wi-Fi network is operational.
	Green (Blinking)	The WiMAX Device is sending and receiving data across the Wi-Fi network.

Table 103 LEDs Status for Outdoor Device

LED	STATE	DESCRIPTION
Strength Indicator	The Strength Indicator LEDs display the Received Signal Strength Indication (RSSI) of the wireless (WiMAX) connection.	
	5 Signal LEDs	The signal strength is greater than or equal to -50 dBm.
	4 Signal LEDs	The signal strength is between -50 and -60 dBm.
	3 Signal LEDs	The signal strength is between -60 and -70 dBm.
	2 Signal LEDs	The signal strength is between -70 and -80 dBm.
	1 Signal LED	The signal strength is between -80 and -90 dBm.
	0 Signal LEDs	The signal strength is less than -90 dBm.
Buzzer Behavior	The buzzer uses sound to alert users to the Received Signal Strength Indication (RSSI) of the wireless (WiMAX) connection.	
	5 Counts (5 sec.)	The signal strength is greater than or equal to -50 dBm.
	4 Counts (4 sec.)	The signal strength is between -50 and -60 dBm.
	3 Counts (3 sec.)	The signal strength is between -60 and -70 dBm.
	2 Counts (2 sec.)	The signal strength is between -70 and -80 dBm.
	1 Count (1 sec.)	The signal strength is between -80 and -90 dBm.
	0 Counts	The signal strength is less than -90 dBm.
Activity Indicator	Off	The WiMAX Device is not ready.
	Green	The WiMAX Device is connected to the network.
	Blinking	The WiMAX Device system is seeking a viable signal.

The following table is for models with VoIP feature.

Table 104 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. 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. 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 Device 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 Device 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 Device 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 Device wait a specified length of time before dialing the number.

Table 104 Voice Features

Phone config	The phone configuration table allows you to customize the phone keypad combinations you use to access certain features on the WiMAX Device, such as call waiting, call return, call forward, etc. The phone configuration 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 Device. Enter *99# in your phone's keypad to have the WiMAX Device 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 Device 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 Device 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.
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) SDP (Session Description Protocol RFC 2327) RTP (RFC 1889) RTCP (RFC 1890) Voice codecs (coder/decoders) G.711, G.726, G.729 Fax and data modem discrimination DTMF Detection and Generation DTMF: In-band and Out-band traffic (RFC 2833),(PCM), (SIP INFO) Point-to-point call establishment between two IADs Quick dialing through predefined phone book, which maps the phone dialing number and destination URL. Flexible Dial Plan (RFC3525 section 7.1.14)

Table 105 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

Table 105 Star (*) and Pound (#) Code Support

*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

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

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

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 Device 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

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 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.

Note: 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.)

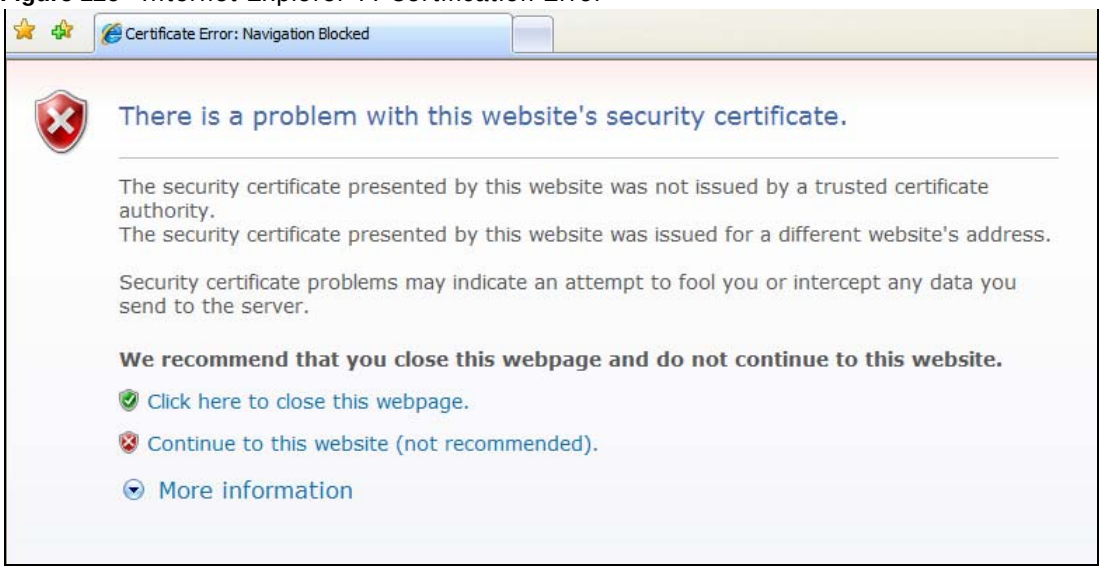
In this appendix, you can import a public key certificate for:

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 126 Internet Explorer 7: Certification Error

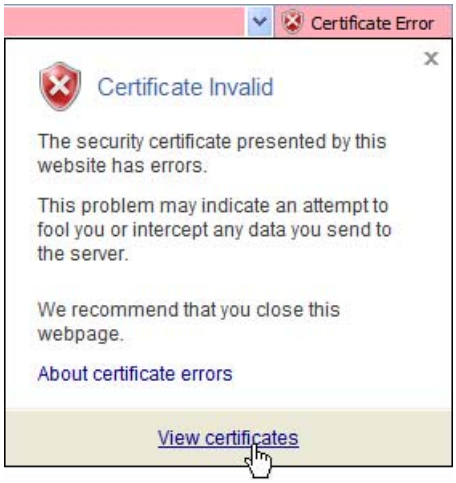


2 Click **Continue to this website (not recommended)**.

Figure 127 Internet Explorer 7: Certification Error

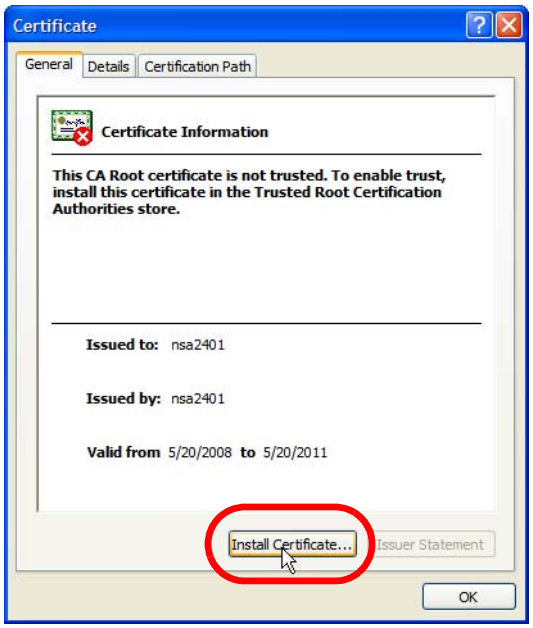
3 In the **Address Bar**, click **Certificate Error** > **View certificates**.

Figure 128 Internet Explorer 7: Certificate Error



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

Figure 129 Internet Explorer 7: Certificate

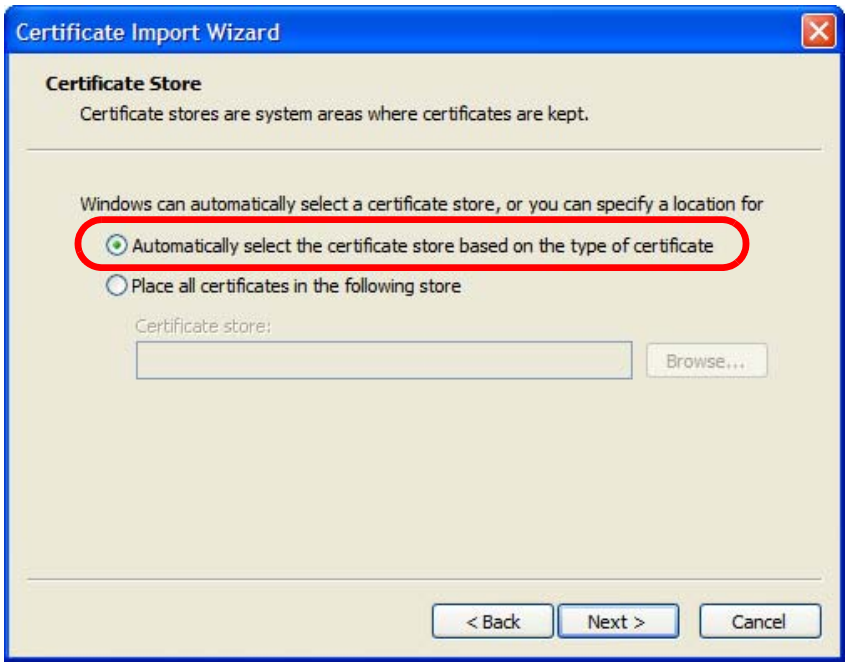


5 In the **Certificate Import Wizard**, click **Next**.

Figure 130 Internet Explorer 7: Certificate Import Wizard

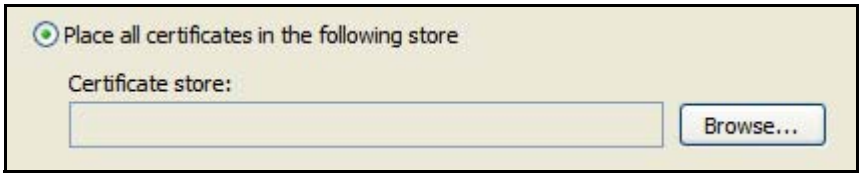
6 If you want Internet Explorer to **Automatically select certificate store based on the type of certificate**, click **Next** again and then go to step 9.

Figure 131 Internet Explorer 7: Certificate Import Wizard



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

Figure 132 Internet Explorer 7: Certificate Import Wizard

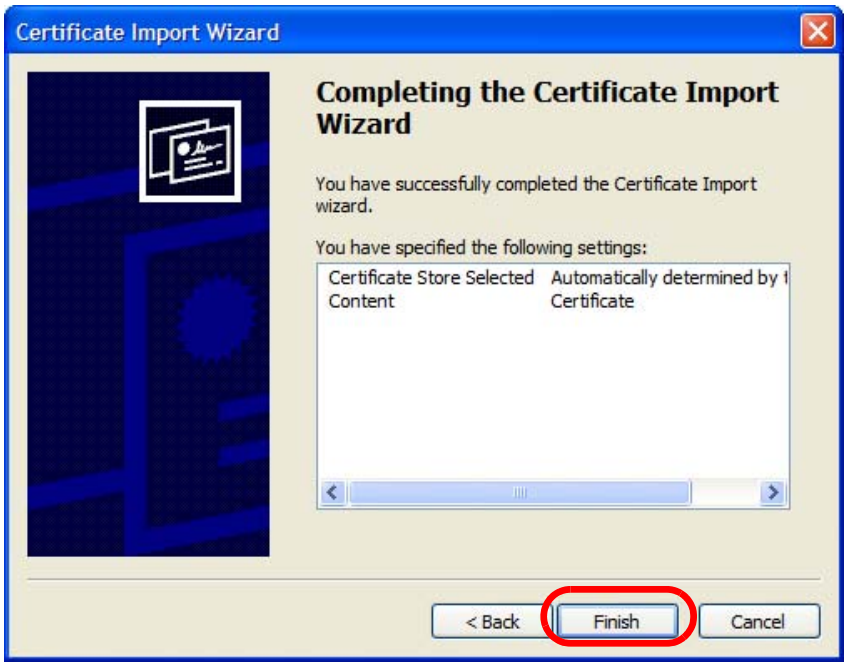


8 In the **Select Certificate Store** dialog box, choose a location in which to save the certificate and then click **OK**.

Figure 133 Internet Explorer 7: Select Certificate Store

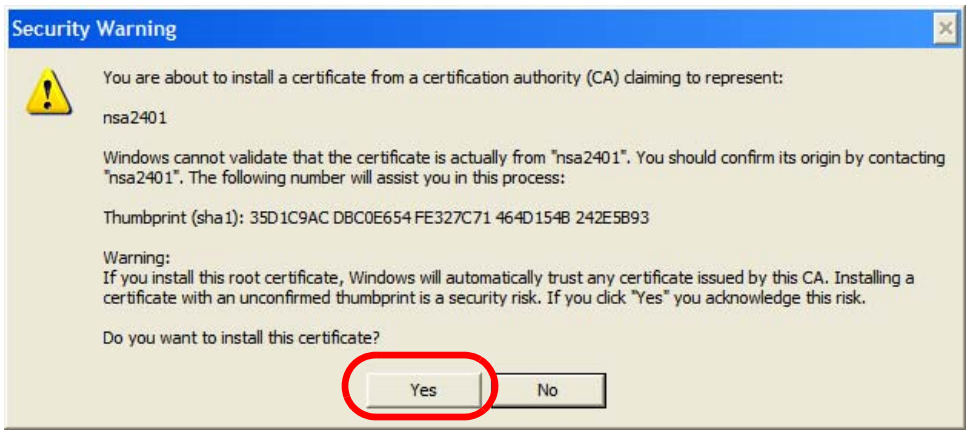
9 In the **Completing the Certificate Import Wizard** screen, click **Finish**.

Figure 134 Internet Explorer 7: Certificate Import Wizard



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

Figure 135 Internet Explorer 7: Security Warning

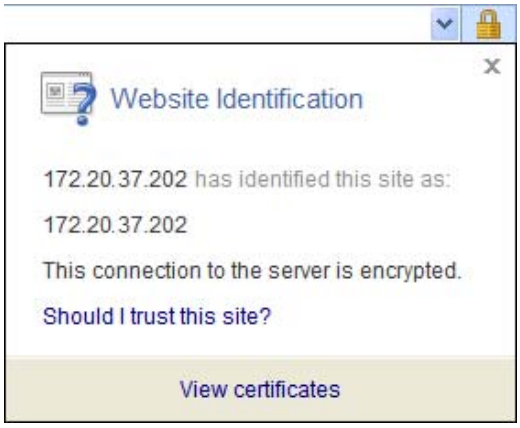


11 Finally, click **OK** when presented with the successful certificate installation message.

Figure 136 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 137 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 138 Internet Explorer 7: Public Key Certificate File

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

Figure 139 Internet Explorer 7: Open File - Security Warning

3 Refer to steps 4-12 in the Internet Explorer procedure beginning on page 212 to complete the installation process.

Removing a Certificate in Internet Explorer

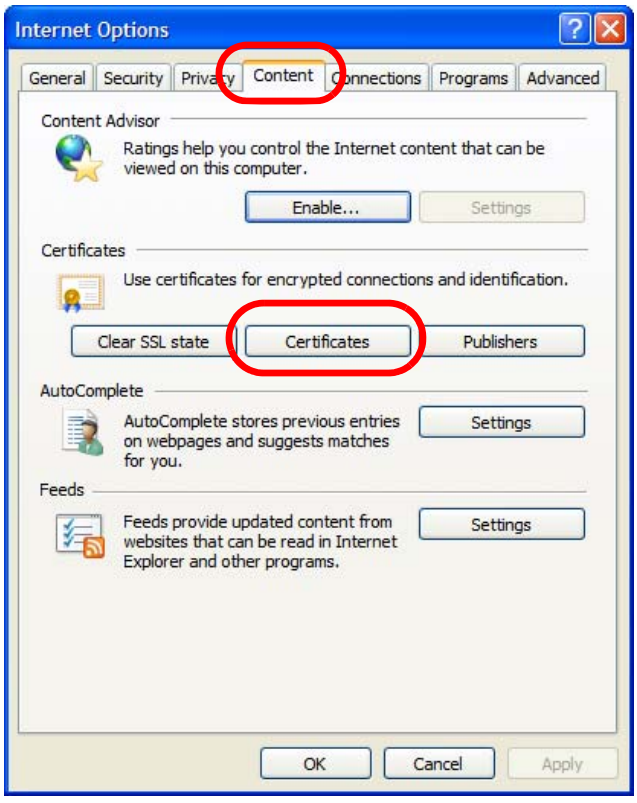
This section shows you how to remove a public key certificate in Internet Explorer 7.

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

Figure 140 Internet Explorer 7: Tools Menu

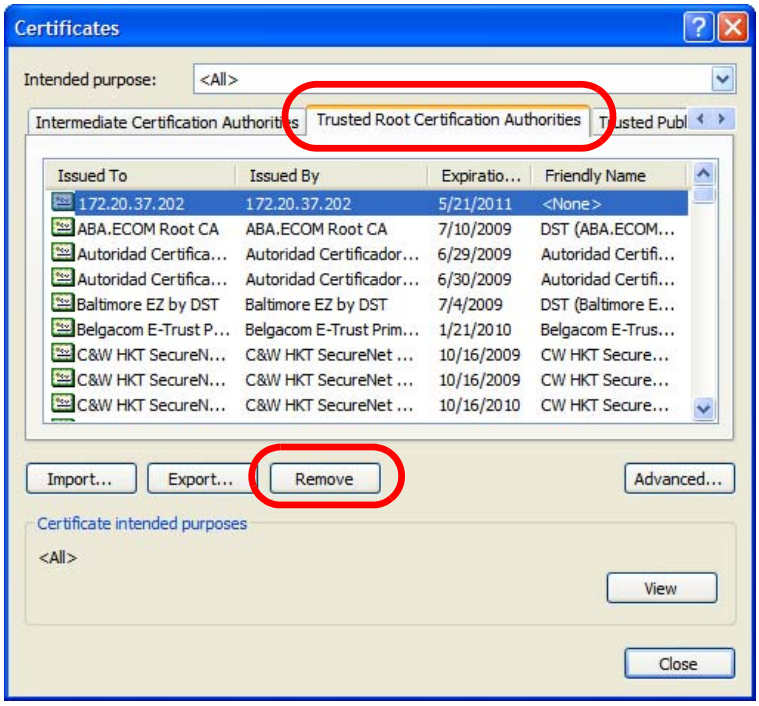
2 In the **Internet Options** dialog box, click **Content** > **Certificates**.

Figure 141 Internet Explorer 7: Internet Options



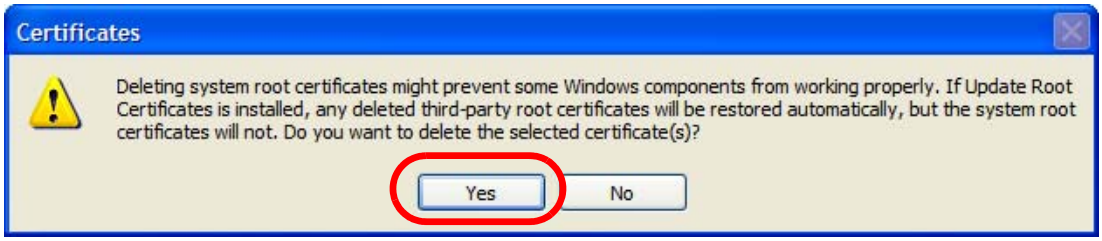
3 In the **Certificates** dialog box, click the **Trusted Root Certificates Authorities** tab, select the certificate that you want to delete, and then click **Remove**.

Figure 142 Internet Explorer 7: Certificates



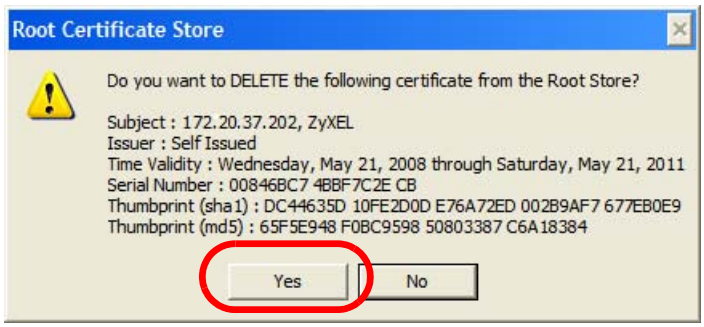
4 In the **Certificates** confirmation, click **Yes**.

Figure 143 Internet Explorer 7: Certificates



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

Figure 144 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.

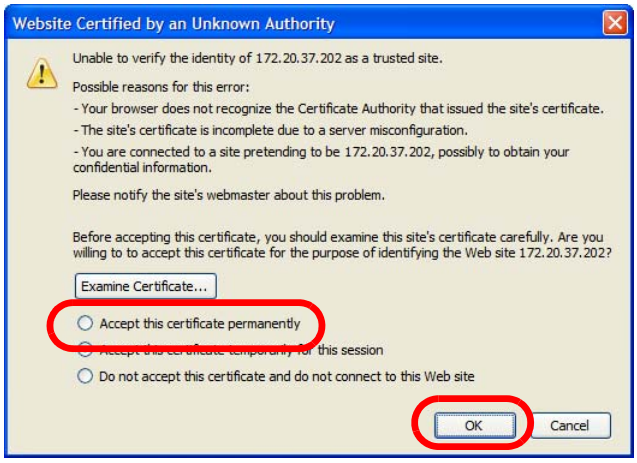
Firefox

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.

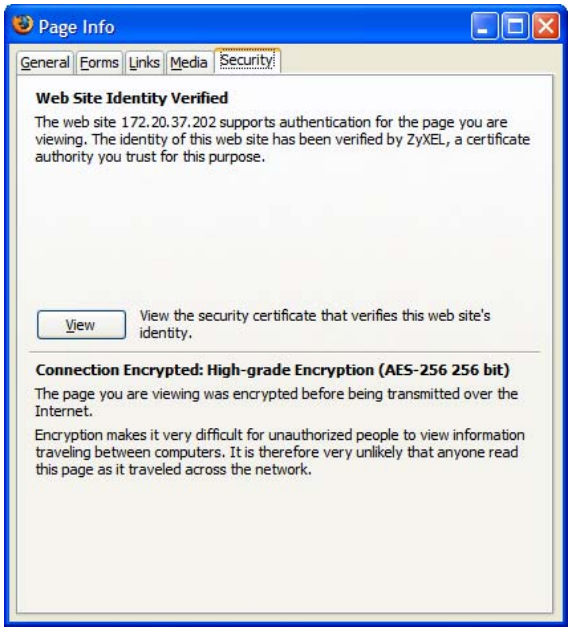
2 Select **Accept this certificate permanently** and click **OK.**

Figure 145 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 146 Firefox 2: Page Info

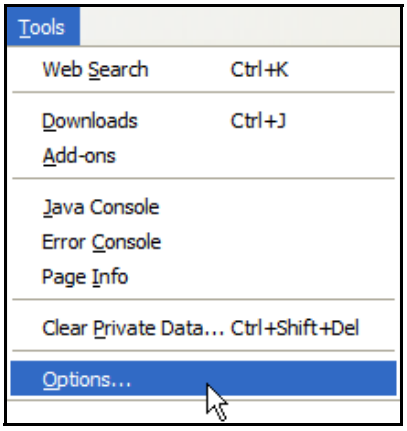


Installing a Stand-Alone Certificate File in Firefox

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.

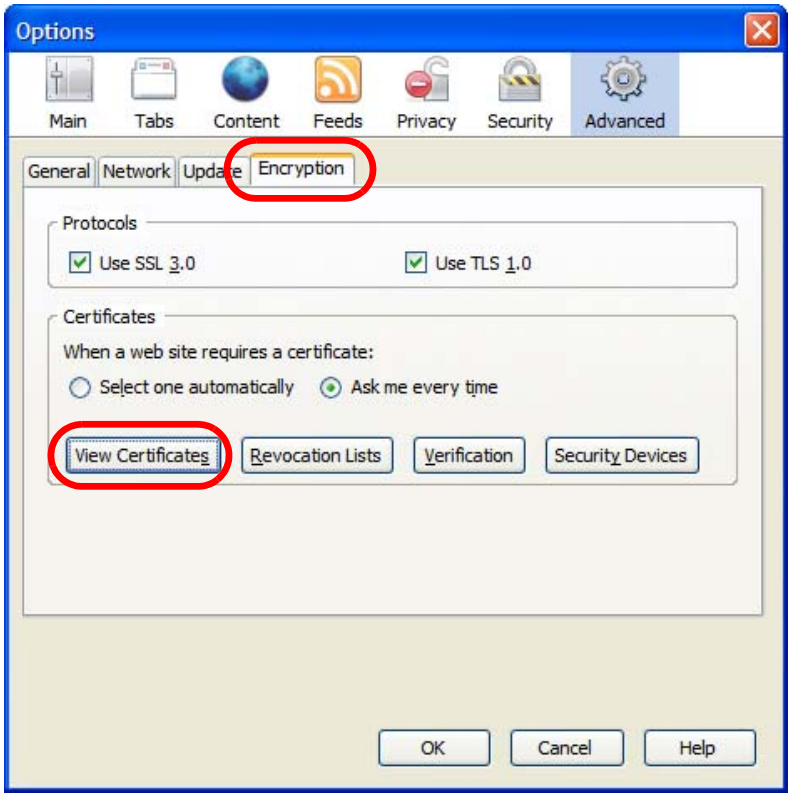
1 Open **Firefox** and click **TOOLS > Options**.

Figure 147 Firefox 2: Tools Menu



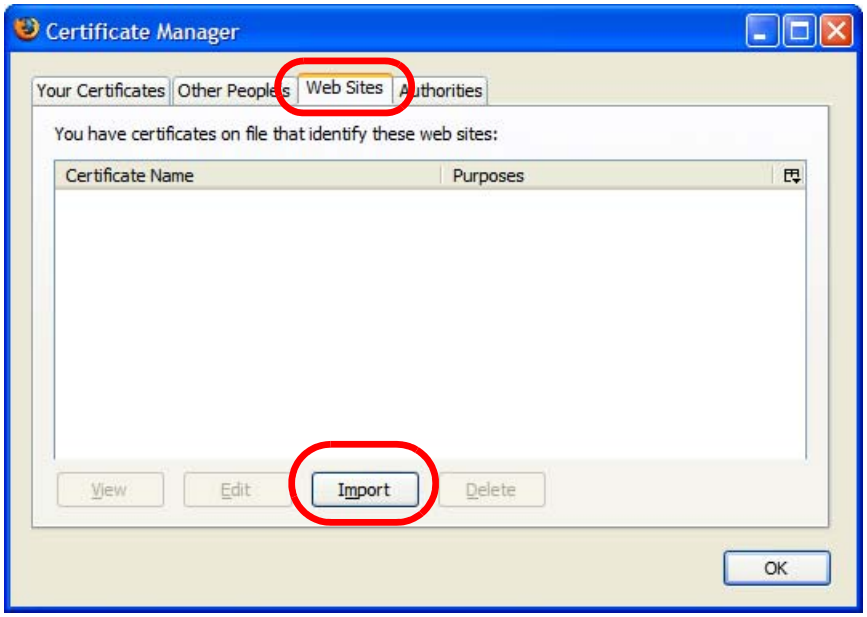
2 In the **Options** dialog box, click **ADVANCED > Encryption** > **View Certificates**.

Figure 148 Firefox 2: Options



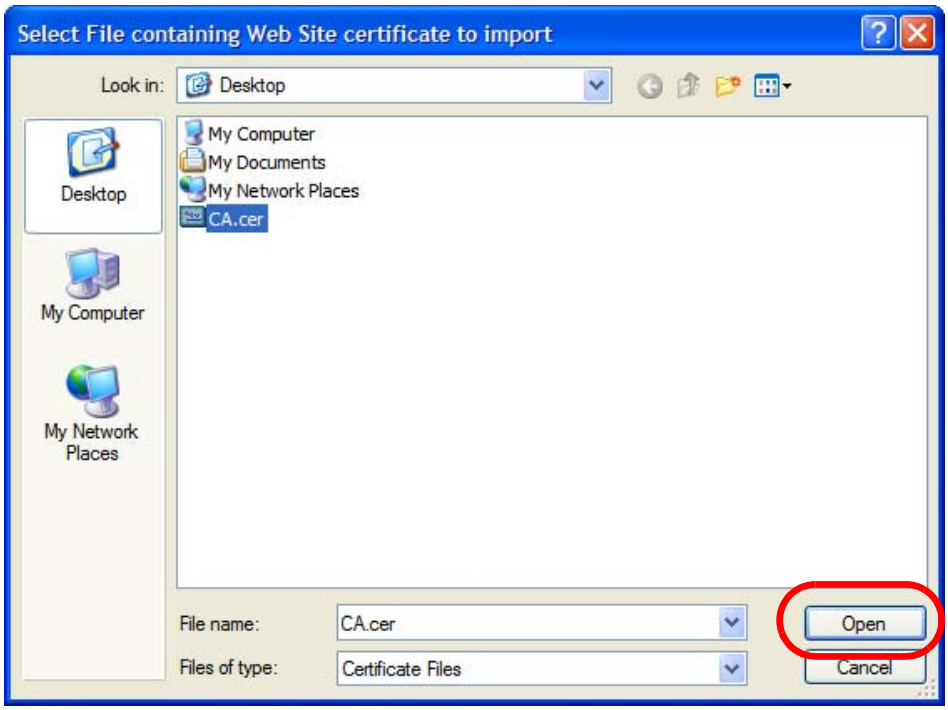
3 In the **Certificate Manager** dialog box, click **Web Sites** > **Import**.

Figure 149 Firefox 2: Certificate Manager



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

Figure 150 Firefox 2: Select File



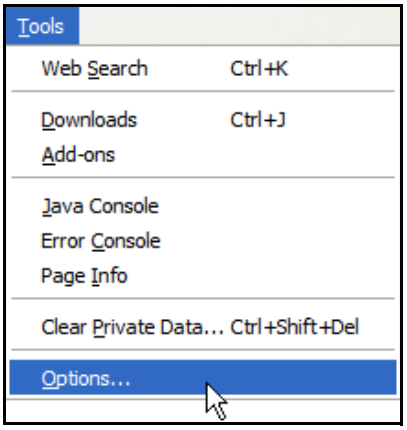
5 The next time you visit the web site, click the padlock in the address bar to open the **Page Info** > **Security** window to see the web page's security information.

Removing a Certificate in Firefox

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

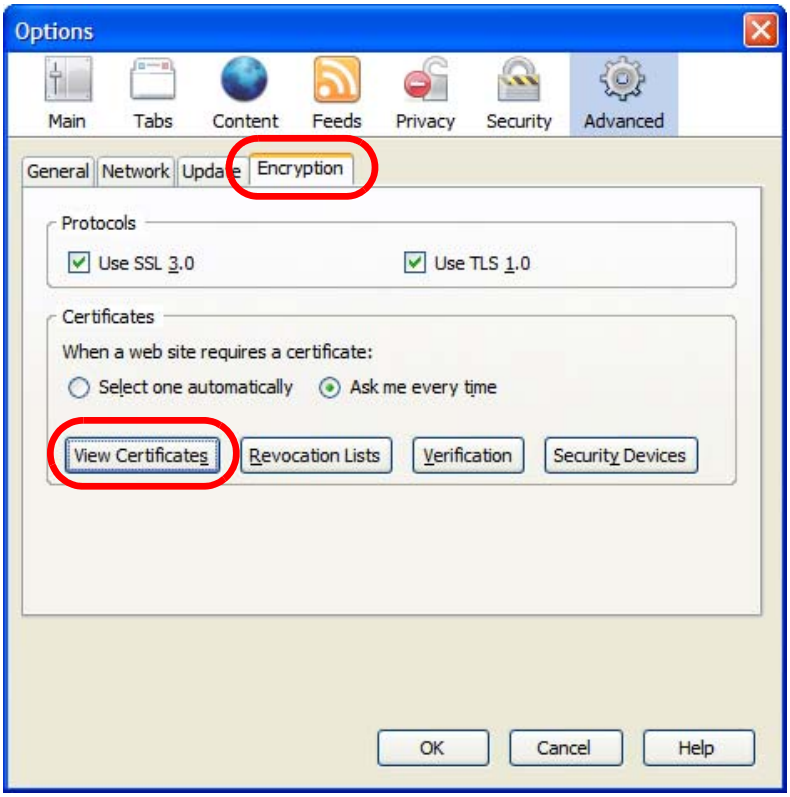
1 Open **Firefox** and click **TOOLS > Options**.

Figure 151 Firefox 2: Tools Menu



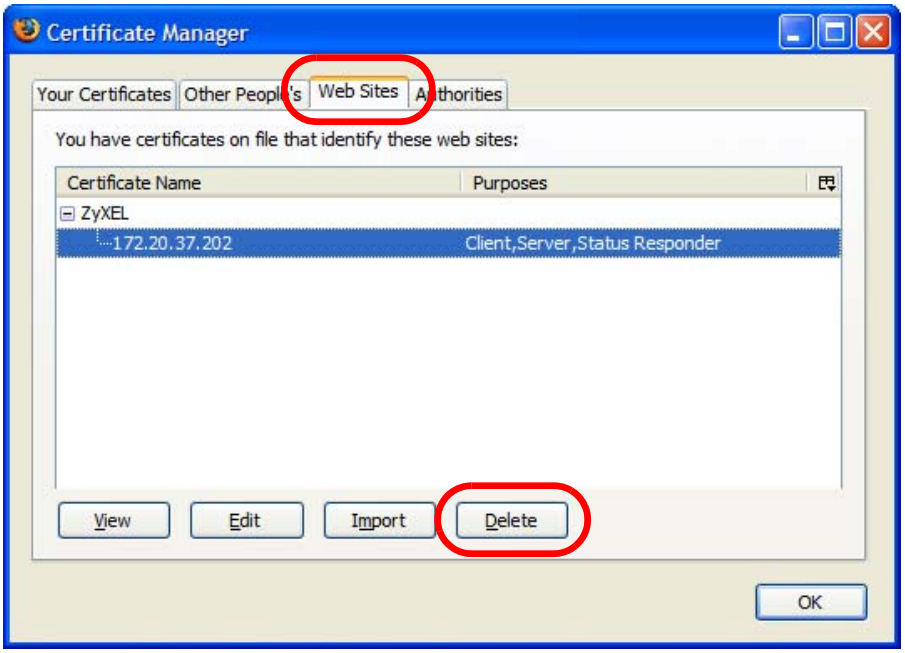
2 In the **Options** dialog box, click **ADVANCED > Encryption** > **View Certificates**.

Figure 152 Firefox 2: Options



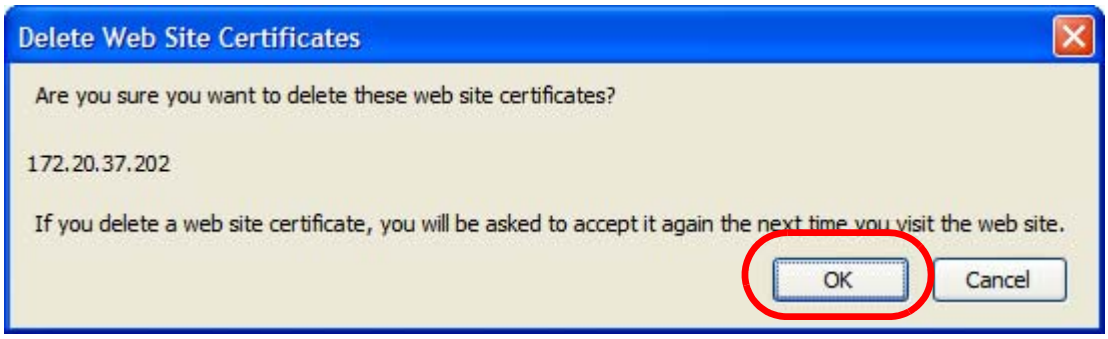
3 In the **Certificate Manager** dialog box, select the **Web Sites** tab, select the certificate that you want to remove, and then click **Delete**.

Figure 153 Firefox 2: Certificate Manager



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

Figure 154 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.

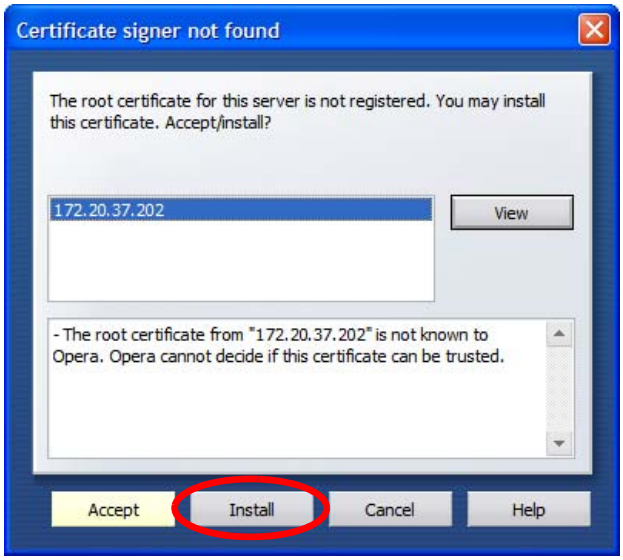
Opera

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.

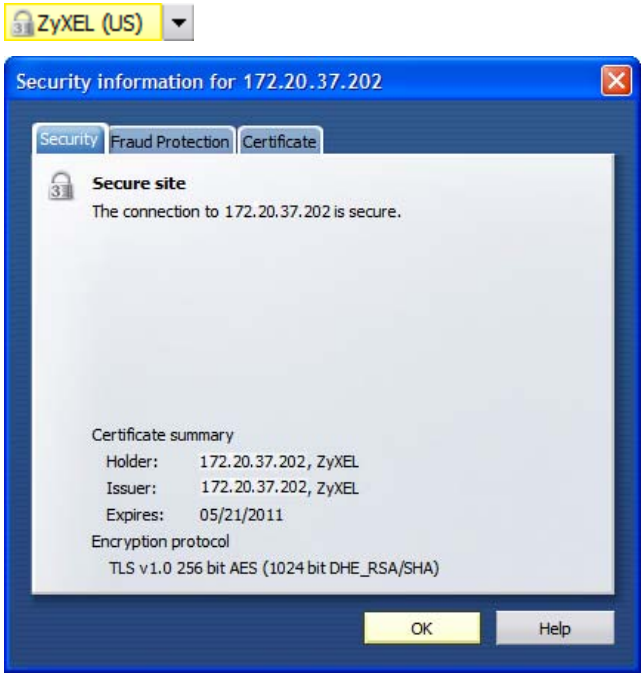
2 Click **Install** to accept the certificate.

Figure 155 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 156 Opera 9: Security information

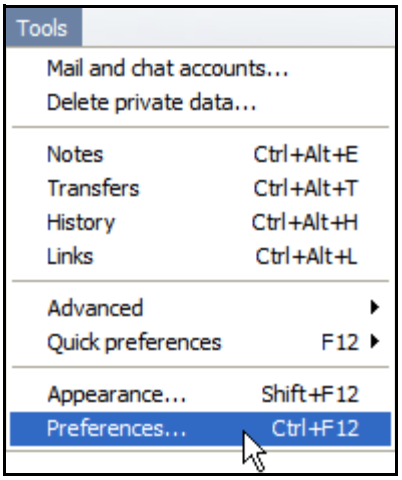


Installing a Stand-Alone Certificate File in Opera

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.

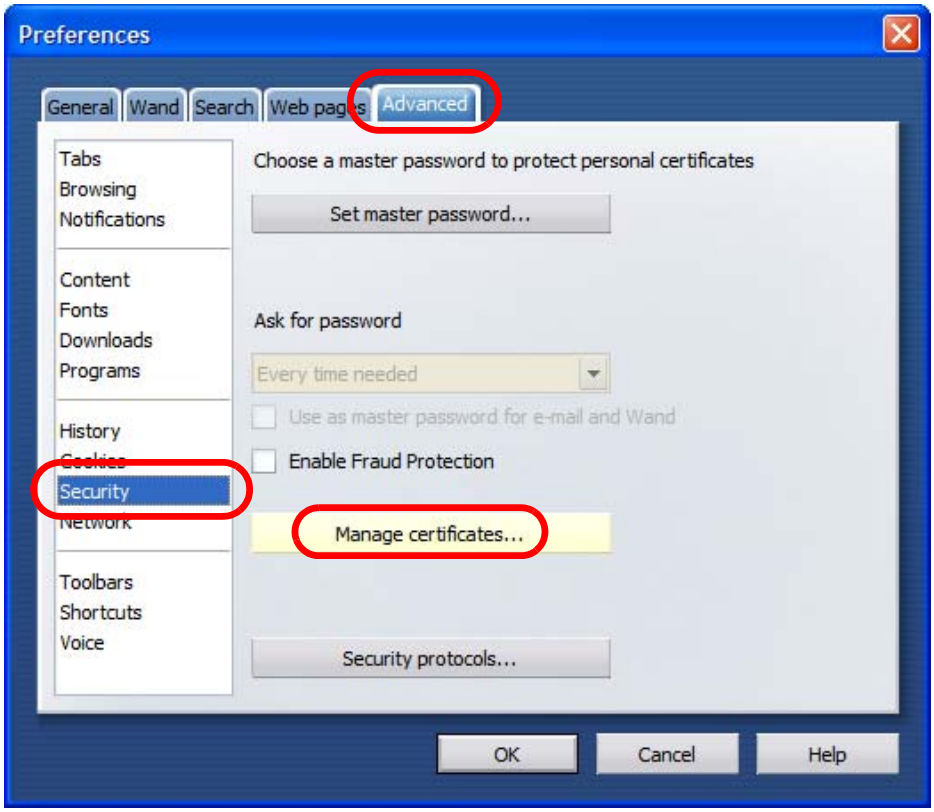
1 Open **Opera** and click **TOOLS > Preferences**.

Figure 157 Opera 9: Tools Menu



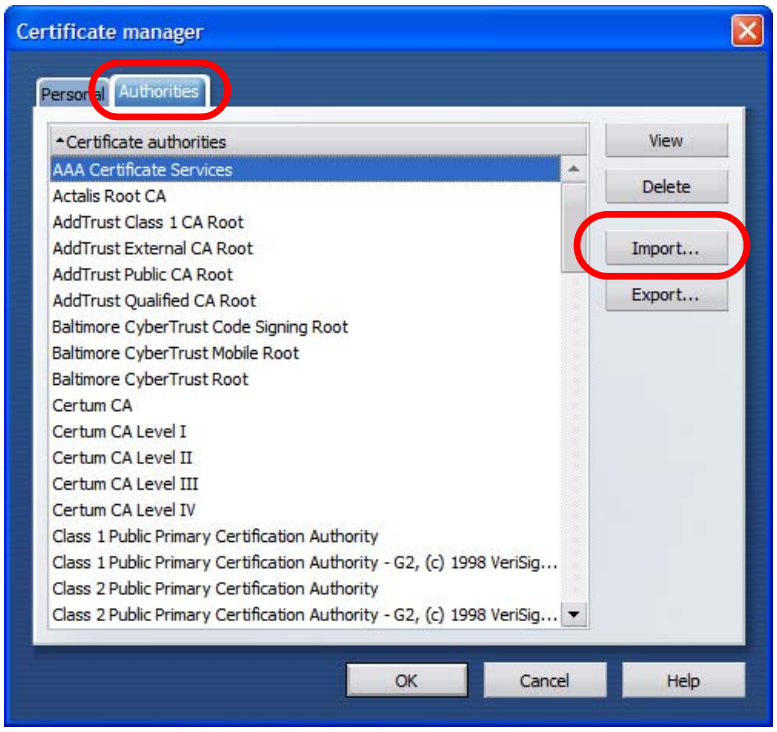
2 In **Preferences**, click **ADVANCED > Security** > **Manage certificates**.

Figure 158 Opera 9: Preferences



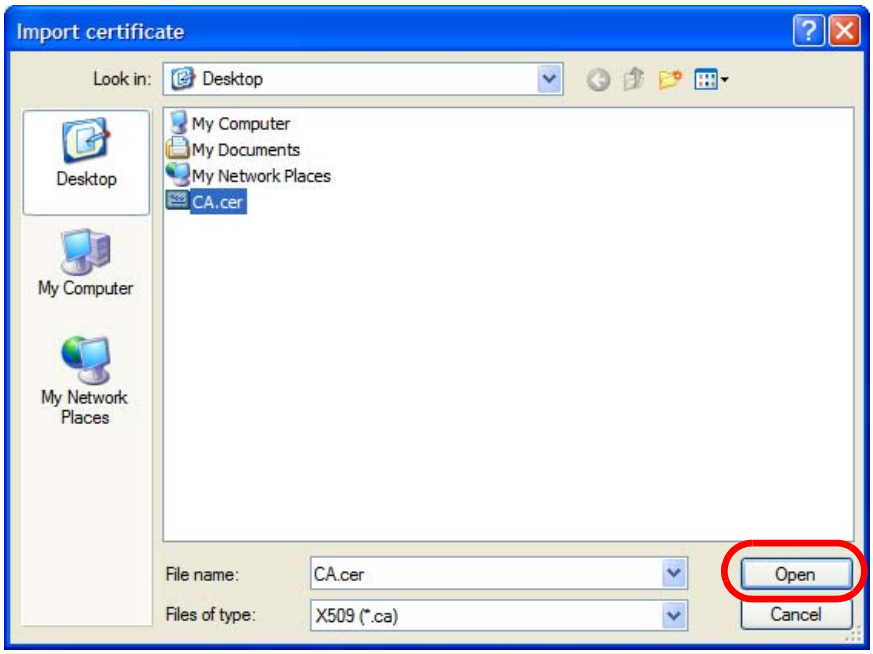
3 In the **Certificates Manager**, click **Authorities** > **Import**.

Figure 159 Opera 9: Certificate manager



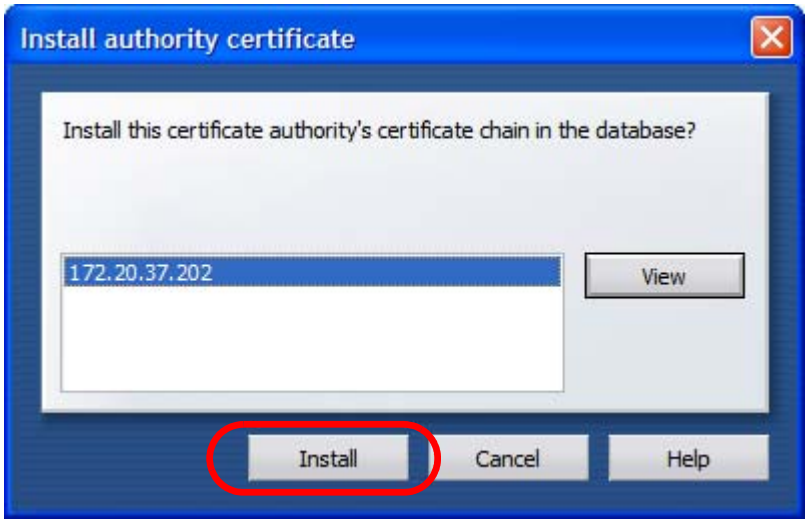
4 Use the **Import certificate** dialog box to locate the certificate and then click **Open.**

Figure 160 Opera 9: Import certificate



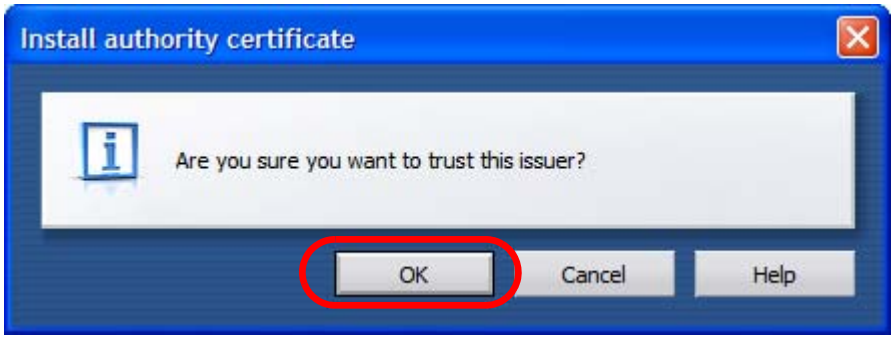
5 In the **Install authority certificate** dialog box, click **Install**.

Figure 161 Opera 9: Install authority certificate



6 Next, click **OK**.

Figure 162 Opera 9: Install authority certificate



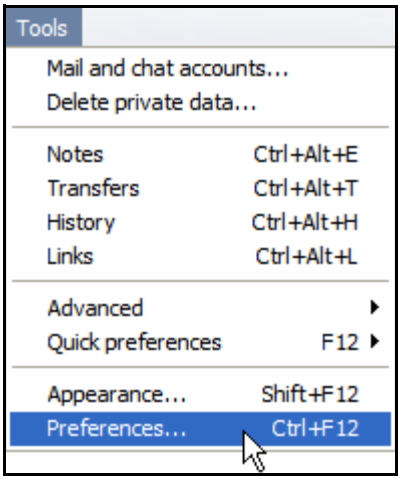
7 The next time you visit the web site, click the padlock in the address bar to open the **Security information** window to view the web page's security details.

Removing a Certificate in Opera

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

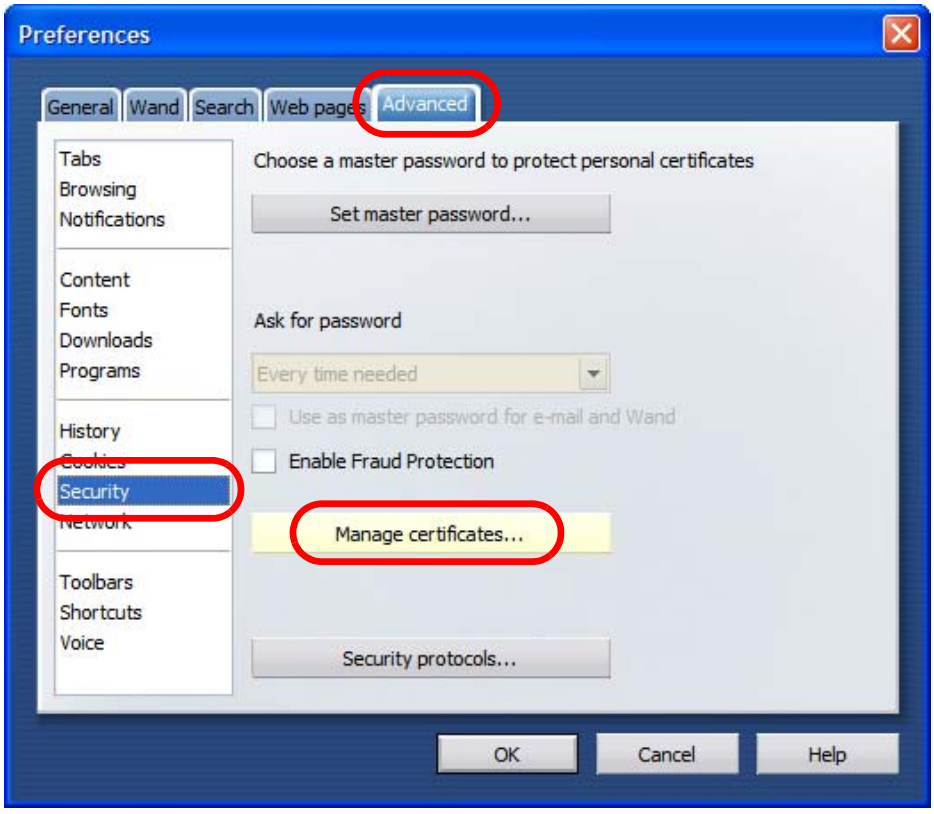
1 Open **Opera** and click **TOOLS > Preferences**.

Figure 163 Opera 9: Tools Menu



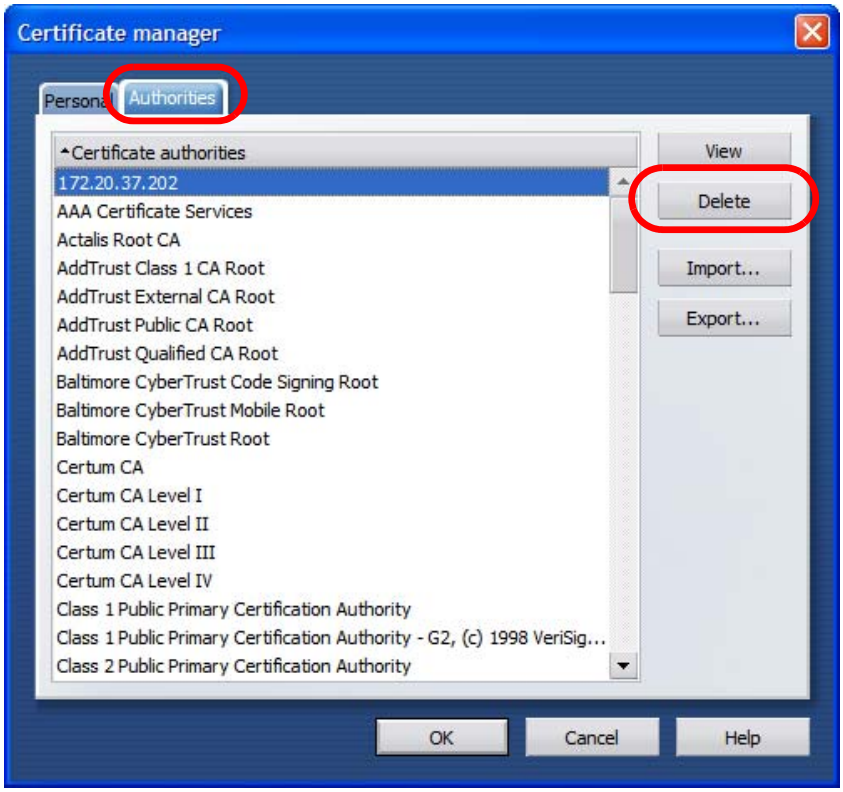
2 In **Preferences**, **ADVANCED > Security** > **Manage certificates**.

Figure 164 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 165 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.

Note: 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.

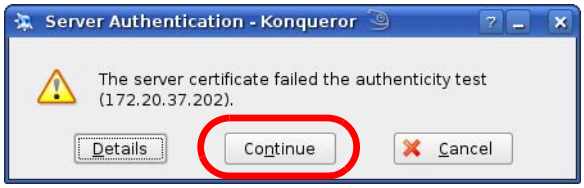
Konqueror

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 166 Konqueror 3.5: Server Authentication

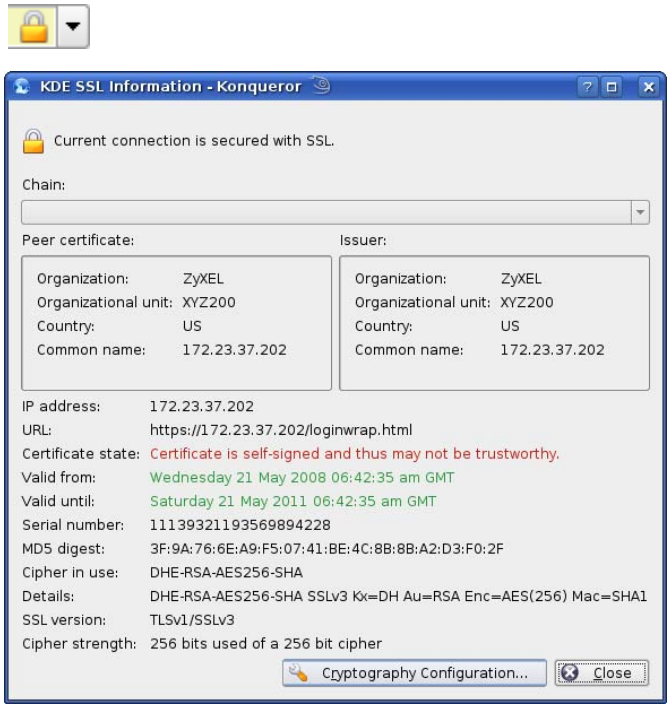


3 Click **Forever** when prompted to accept the certificate.

Figure 167 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 168 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.

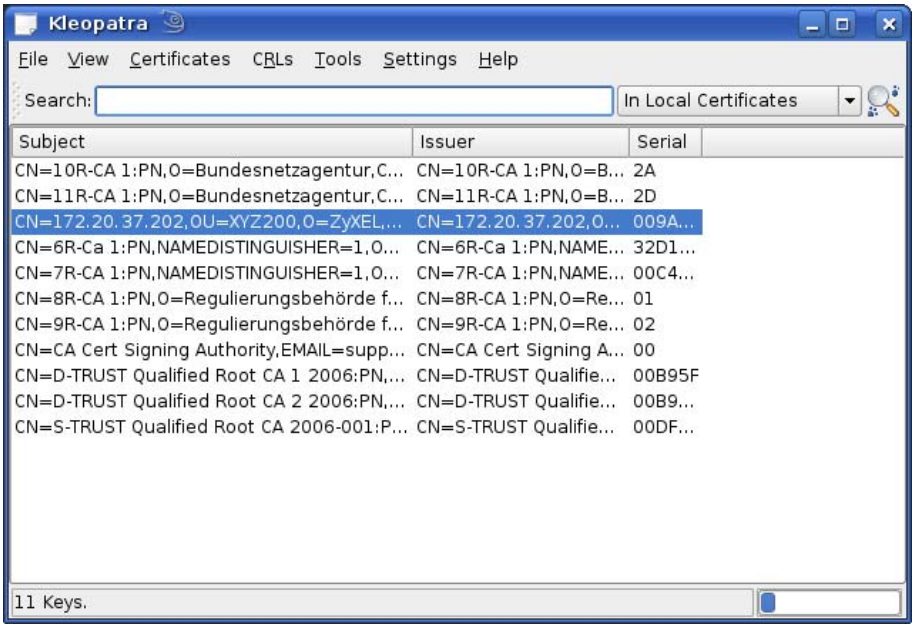
Figure 169 Konqueror 3.5: Public Key Certificate File

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

Figure 170 Konqueror 3.5: Certificate Import Result

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

Figure 171 Konqueror 3.5: Kleopatra



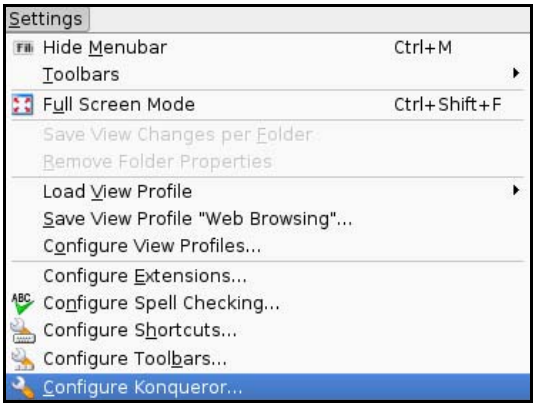
3 The next time you visit the web site, click the padlock in the address bar to open the **KDE SSL Information** window to view the web page's security details.

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**.

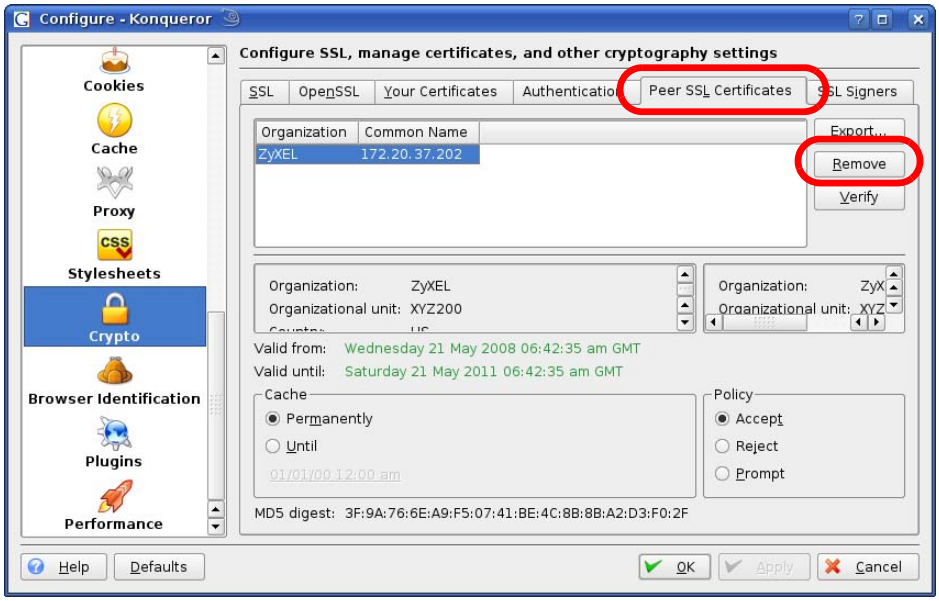
Figure 172 Konqueror 3.5: Settings Menu



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 173 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.

Note: 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.

C

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 106 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 UDP	7648 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.
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.

Table 106 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
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.
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.

Table 106 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
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.

D

Open Software Announcements

End-User License Agreement for "MAX208M, MAX218M, MAX208M2W, MAX218M2W, MAX218M1W, MAX218MW, MAX318M2W, MAX308M, and MAX318M"

WARNING: ZyXEL Communications Corp. IS WILLING TO LICENSE THE SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AS INSTALLING THE SOFTWARE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN ZyXEL IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE UNINSTALLED SOFTWARE AND PACKAGING TO THE PLACE FROM WHICH IT WAS ACQUIRED OR ZyXEL, AND YOUR MONEY WILL BE REFUNDED. HOWEVER, CERTAIN ZYXEL'S PRODUCTS MAY CONTAIN-IN PART-SOME THIRD PARTY'S FREE AND OPEN SOFTWARE PROGRAMS WHICH ALLOW YOU TO FREELY COPY, RUN, DISTRIBUTE, MODIFY AND IMPROVE THE SOFTWARE UNDER THE APPLICABLE TERMS OF SUCH THRID PARTY'S LICENSES ("OPEN-SOURCED COMPONENTS"). THE OPEN-SOURCED COMPONENTS ARE LISTED IN THE NOTICE OR APPENDIX BELOW. ZYXEL MAY HAVE DISTRIBUTED TO YOU HARDWARE AND/OR SOFTWARE, OR MADE AVAILABLE FOR ELECTRONIC DOWNLOADS THESE FREE SOFTWARE PROGRAMS OF THRID PARTIES AND YOU ARE LICENSED TO FREELY COPY, MODIFY AND REDISTIBUTE THAT SOFTWARE UNDER THE APPLICABLE LICENSE TERMS OF SUCH THIRD PARTY. NONE OF THE STATEMENTS OR DOCUMENTATION FROM ZYXEL INCLUDING ANY RESTRICTIONS OR CONDITIONS STATED IN THIS END USER LICENSE AGREEMENT SHALL RESTRICT ANY RIGHTS AND LICENSES YOU MAY HAVE WITH RESPECT TO THE OPEN-SOURCED COMPONENTS UNDER THE APPLICABLE LICENSE TERMS OF SUCH THIRD PARTY.

1.Grant of License for Personal Use

ZyXEL Communications Corp. ("ZyXEL") grants you a non-exclusive, non-sublicense, non-transferable license to use the program with which this license is distributed (the "Software"), including any documentation files accompanying the Software ("Documentation"), for internal business use only, for up to the number of users specified in sales order and invoice. You have the right to make one backup copy of the Software and Documentation solely for archival, back-up or disaster recovery purposes. You shall not exceed the scope of the license granted hereunder. Any rights not expressly granted by ZyXEL to you are reserved by ZyXEL, and all implied licenses are disclaimed.

2.Ownership

You have no ownership rights in the Software. Rather, you have a license to use the Software as long as this License Agreement remains in full force and effect. Ownership of the Software, Documentation and all intellectual property rights therein shall remain at all times with ZyXEL. Any other use of the Software by any other entity is strictly forbidden and is a violation of this License Agreement.

3.Copyright

The Software and Documentation contain material that is protected by international copyright law, trade secret law, international treaty provisions, and the applicable national laws of each respective country. All rights not granted to you herein are expressly reserved by ZyXEL. You may not remove any proprietary notice of ZyXEL or any of its licensors from any copy of the Software or Documentation.

4.Restrictions

You may not publish, display, disclose, sell, rent, lease, modify, store, loan, distribute, or create derivative works of the Software, or any part thereof. You may not assign, sublicense, convey or otherwise transfer, pledge as security or otherwise encumber the rights and licenses granted hereunder with respect to the Software. ZyXEL is not obligated to provide any maintenance, technical or other support for the resultant modified Software. You may not copy, reverse engineer, decompile, reverse compile, translate, adapt, or disassemble the Software, or any part thereof, nor shall you attempt to create the source code from the object code for the Software. Except as and only to the extent expressly permitted in this License, you may not market, co-brand, and private label or otherwise permit third parties to link to the Software, or any part thereof. You may not use the Software, or any part thereof, in the operation of a service bureau or for the benefit of any other person or entity. You may not cause, assist or permit any third party to do any of the foregoing. Portions of the Software utilize or include third party software and other copyright material. Acknowledgements, licensing terms and disclaimers for such material are contained in the License Notice as below for the third party software, and your use of such material is exclusively governed by their respective terms. ZyXEL has provided, as part of the Software package, access to certain third party software as a convenience. To the extent that the Software contains third party software, ZyXEL has no express or implied obligation to provide any technical or other support for such software other than compliance with the applicable license terms of such third party, and makes no warranty (express, implied or statutory) whatsoever with respect thereto. Please contact the appropriate software vendor or manufacturer directly for technical support and customer service related to its software and products.

5.Confidentiality

You acknowledge that the Software contains proprietary trade secrets of ZyXEL and you hereby agree to maintain the confidentiality of the Software using at least as great a degree of care as you use to maintain the confidentiality of your own most confidential information. You agree to reasonably communicate the terms and conditions of this License Agreement to those persons employed by you who come into contact with the Software, and to use reasonable best efforts to ensure their compliance with such terms and conditions, including, without limitation, not knowingly permitting such persons to use any portion of the Software for the purpose of deriving the source code of the Software.

6.No Warranty

THE SOFTWARE IS PROVIDED "AS IS." TO THE MAXIMUM EXTENT PERMITTED BY LAW, ZyXEL DISCLAIMS ALL WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. ZyXEL DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET ANY REQUIREMENTS OR NEEDS YOU MAY HAVE, OR THAT THE SOFTWARE WILL OPERATE ERROR FREE, OR IN AN UNINTERUPTED FASHION, OR THAT ANY DEFECTS OR ERRORS IN THE SOFTWARE WILL BE CORRECTED, OR THAT THE SOFTWARE IS COMPATIBLE WITH ANY PARTICULAR PLATFORM. SOME JURISDICTIONS DO NOT ALLOW THE WAIVER OR EXCLUSION OF IMPLIED WARRANTIES SO THEY MAY NOT APPLY TO YOU. IF THIS EXCLUSION IS HELD TO BE UNENFORCEABLE BY A COURT OF COMPETENT JURISDICTION, THEN ALL EXPRESS AND IMPLIED WARRANTIES SHALL BE LIMITED IN DURATION TO A PERIOD OF

THIRTY (30) DAYS FROM THE DATE OF PURCHASE OF THE SOFTWARE, AND NO WARRANTIES SHALL APPLY AFTER THAT PERIOD.

7.Limitation of Liability

IN NO EVENT WILL ZyXEL BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, INDIRECT, SPECIAL, PUNITIVE, OR EXEMPLARY DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE OR PROGRAM, OR FOR ANY CLAIM BY ANY OTHER PARTY, EVEN IF ZyXEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. ZyXEL's TOTAL AGGREGATE LIABILITY WITH RESPECT TO ITS OBLIGATIONS UNDER THIS AGREEMENT OR OTHERWISE WITH RESPECT TO THE SOFTWARE AND DOCUMENTATION OR OTHERWISE SHALL BE EQUAL TO THE PURCHASE PRICE, BUT SHALL IN NO EVENT EXCEED THE PRODUCT'S PRICE. BECAUSE SOME STATES/COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

8.Export Restrictions

THIS LICENSE AGREEMENT IS EXPRESSLY MADE SUBJECT TO ANY APPLICABLE LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS ON THE EXPORT OF THE SOFTWARE OR INFORMATION ABOUT SUCH SOFTWARE WHICH MAY BE IMPOSED FROM TIME TO TIME. YOU SHALL NOT EXPORT THE SOFTWARE, DOCUMENTATION OR INFORMATION ABOUT THE SOFTWARE AND DOCUMENTATION WITHOUT COMPLYING WITH SUCH LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS. YOU AGREE TO INDEMNIFY ZyXEL AGAINST ALL CLAIMS, LOSSES, DAMAGES, LIABILITIES, COSTS AND EXPENSES, INCLUDING REASONABLE ATTORNEYS' FEES, TO THE EXTENT SUCH CLAIMS ARISE OUT OF ANY BREACH OF THIS SECTION 8.

9.Audit Rights

ZyXEL SHALL HAVE THE RIGHT, AT ITS OWN EXPENSE, UPON REASONABLE PRIOR NOTICE, TO PERIODICALLY INSPECT AND AUDIT YOUR RECORDS TO ENSURE YOUR COMPLIANCE WITH THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT.

10.Termination

This License Agreement is effective until it is terminated. You may terminate this License Agreement at any time by destroying or returning to ZyXEL all copies of the Software and Documentation in your possession or under your control. ZyXEL may terminate this License Agreement for any reason, including, but not limited to, if ZyXEL finds that you have violated any of the terms of this License Agreement. Upon notification of termination, you agree to destroy or return to ZyXEL all copies of the Software and Documentation and to certify in writing that all known copies, including backup copies, have been destroyed. All provisions relating to confidentiality, proprietary rights, and non-disclosure shall survive the termination of this Software License Agreement.

11.General

This License Agreement shall be construed, interpreted and governed by the laws of Republic of China without regard to conflicts of laws provisions thereof. The exclusive forum for any disputes arising out of or relating to this License Agreement shall be an appropriate court or Commercial Arbitration Association sitting in ROC, Taiwan if the parties agree to a binding arbitration. This License Agreement shall constitute the entire Agreement between the parties hereto. This License Agreement, the rights granted hereunder, the Software and Documentation shall not be assigned by you without the prior written consent of ZyXEL. Any waiver or modification of this License

Agreement shall only be effective if it is in writing and signed by both parties hereto. If any part of this License Agreement is found invalid or unenforceable by a court of competent jurisdiction, the remainder of this License Agreement shall be interpreted so as to reasonably effect the intention of the parties.

NOTE: Some components of this product incorporate free software programs covered under the open source code licenses which allows you to freely copy, modify and redistribute the software. For at least three (3) years from the date of distribution of the applicable product or software, we will give to anyone who contacts us at the ZyXEL Technical Support (support@zyxel.com.tw), for a charge of no more than our cost of physically performing source code distribution, a complete machine-readable copy of the complete corresponding source code for the version of the Programs that we distributed to you if we are in possession of such.

Notice

Information herein is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, except the express written permission of ZyXEL Communications Corporation.

This Product includes Bridge-utils, Busybox, Dnrd, Ebtables, Igmpproxy, Iproute2, Iptables, MIPS linux kernel, miniupnpd, Ntpclient, open12tp, Ppp, rp-pppoe, pptp, pptpd, quagga,, Updatedd, Strongswan, termcap, and zebra under below GPL license

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose

authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it. For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software. Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you". Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program. In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, c) Accompany it with the information you received as to the offer to distribute corresponding source code.(This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.) The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the

scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the

operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and

"any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

All other trademarks or trade names mentioned herein, if any, are the property of their respective owners.

This Product includes Dropbear under the MIT-Style License.

The MIT License

Copyright (c) <year> <copyright holders>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is

furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THEAUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHERLIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS INTHE SOFTWARE.

This Product includes Ppp under the license by BSD

BSD

Copyright (c) [dates as appropriate to package]

The Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the University nor of the Laboratory may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This Product includes Mini_httpd under the license by ACME Labs Freeware

ACME Labs Freeware License

All the free software available on the ACME Labs web site has a copyright notice like this one:

Copyright © 2000 by Jef Poskanzer <jef@mail.acme.com>. All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:

1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSEARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLEFOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIALDAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY

This Product includes libnl and gmplib under the LGPL License.

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. [This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you.You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries,

and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License. In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License").

Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables. The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any

associated interface definition files, plus the scripts used to control compilation and installation of the library. Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions: a) The modified work must itself be a software library. b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change. c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License. d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful. (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.) These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library. In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices. Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy. This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software

interchange. If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables. When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law. If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.) Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications. You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things: a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.) b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with. c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution. d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place. e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy. For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form)

with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things: a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above. b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCHDAMAGES.

END OF TERMS AND CONDITIONS.

This Product includes OpenSSL under the OpenSSL License.

OpenSSL Licens

```
/*
=====================================================================
=======
 * Copyright (c) 1998-2008 The OpenSSL Project.  All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 *    software must display the following acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 *    endorse or promote products derived from this software without
 *    prior written permission. For written permission, please contact
 *    openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 *    nor may "OpenSSL" appear in their names without prior written
```

```
 *    permission of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
 *    acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
 *
 * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
 * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
 * PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
 * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
 * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
 * OF THE POSSIBILITY OF SUCH DAMAGE.
 *
================================================================
=======
 *
 * This product includes cryptographic software written by Eric Young
 * (eay@cryptsoft.com).  This product includes software written by Tim
 * Hudson (tjh@cryptsoft.com).
 *
 */
```

Original SSLeay License

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to. The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code. The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the copyright

* notice, this list of conditions and the following disclaimer.

* 2. Redistributions in binary form must reproduce the above copyright

* notice, this list of conditions and the following disclaimer in the

* documentation and/or other materials provided with the distribution.

* 3. All advertising materials mentioning features or use of this software

* must display the following acknowledgement:

* "This product includes cryptographic software written by

* Eric Young (eay@cryptsoft.com)"

* The word 'cryptographic' can be left out if the rouines from the library

* being used are not cryptographic related :-).

* 4. If you include any Windows specific code (or a derivative thereof) from

* the apps directory (application code) you must include an acknowledgement:

* "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

*

* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND

* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE

* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

*

* The licence and distribution terms for any publically available version or

* derivative of this code cannot be changed. i.e. this code cannot simply be

* copied and put under another distribution licence

* [including the GNU Public Licence.]

*/

This Product includes ftpd under the following License.

Ftp Server

* Copyright (c) 1985, 1988, 1990, 1992, 1993, 1994, 2002
* The Regents of the University of California. All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the above copyright
* notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
* notice, this list of conditions and the following disclaimer in the
* documentation and/or other materials provided with the distribution.
* 4. Neither the name of the University nor the names of its contributors
* may be used to endorse or promote products derived from this software
* without specific prior written permission.
*
* THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.

*/

This Product includes net-snmp software under the following license

Various copyrights apply to this package, listed in various separate
parts below. Please make sure that you read all the parts.

---- Part 1: CMU/UCD copyright notice: (BSD like) -----

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000
Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Permission to use, copy, modify and distribute this software and its
documentation for any purpose and without fee is hereby granted,
provided that the above copyright notice appears in all copies and
that both that copyright notice and this permission notice appear in
supporting documentation, and that the name of CMU and The Regents of
the University of California not be used in advertising or publicity
pertaining to distribution of the software without specific written
permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL

WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) -----

Copyright (c) 2001-2003, Networks Associates Technology, Inc
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) -----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----

Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 5: Sparta, Inc copyright notice (BSD) -----

Copyright (c) 2003-2009, Sparta, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR

OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 6: Cisco/BUPTNIC copyright notice (BSD) -----

Copyright (c) 2004, Cisco, Inc and Information Network
Center of Beijing University of Posts and Telecommunications.
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR

CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 7: Fabasoft R&D Software GmbH & Co KG copyright notice (BSD) -----

Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2003

oss@fabasoft.com

Author: Bernhard Penz

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* The name of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries, brand or product names may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 8: Apple Inc. copyright notice (BSD) -----

Copyright (c) 2007 Apple Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of Apple Inc. ("Apple") nor the names of its contributors may be used to endorse or promote products derived

from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY APPLE AND ITS CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL APPLE OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 9: ScienceLogic, LLC copyright notice (BSD) -----

Copyright (c) 2009, ScienceLogic, LLC
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright

notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of ScienceLogic, LLC nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This Product includes sqlite software under below license

SQLite Copyright

All of the deliverable code in SQLite has been dedicated to the public domain by the authors. All code authors, and representatives of the companies they work for, have signed affidavits dedicating their contributions to the public domain and originals of those signed affidavits are stored in a firesafe at the main offices of Hwaci. Anyone is free to copy, modify, publish, use, compile, sell, or distribute the original SQLite code, either in source code form or as a compiled binary, for any purpose, commercial or non-commercial, and by any means.

The previous paragraph applies to the deliverable code in SQLite - those parts of the SQLite library that you actually bundle and ship with a larger application. Portions of the documentation and some code used as part of the build process might fall under other licenses. The details here are unclear. We do not worry about the licensing of the documentation and build code so much because none of these things are part of the core deliverable SQLite library.

All of the deliverable code in SQLite has been written from scratch. No code has been taken from other projects or from the open internet. Every line of code can be traced back to its original author, and all of those authors have public domain dedications on file. So the SQLite code base is clean and is uncontaminated with licensed code from other projects.

Obtaining An Explicit License To Use SQLite

Even though SQLite is in the public domain and does not require a license, some users want to obtain a license anyway. Some reasons for obtaining a license include:

"You are using SQLite in a jurisdiction that does not recognize the public domain.

"You are using SQLite in a jurisdiction that does not recognize the right of an author to dedicate their work to the public domain.

"You want to hold a tangible legal document as evidence that you have the legal right to use and distribute SQLite.

"Your legal department tells you that you have to purchase a license.

If you feel like you really have to purchase a license for SQLite, Hwaci, the company that employs the architect and principal developers of SQLite, will sell you one.

Contributed Code

In order to keep SQLite completely free and unencumbered by copyright, all new contributors to the SQLite code base are asked to dedicate their contributions to the public domain. If you want to send a patch or enhancement for possible inclusion in the SQLite source tree, please accompany the patch with the following statement:

The author or authors of this code dedicate any and all copyright interest in this code to the public domain. We make this dedication for the benefit of the public at large and to the detriment of our heirs and successors. We intend this dedication to be an overt act of relinquishment in perpetuity of all present and future rights to this code under copyright law.

We are not able to accept patches or changes to SQLite that are not accompanied by a statement such as the above. In addition, if you make changes or enhancements as an employee, then a simple statement such as the above is insufficient. You must also send by surface mail a copyright release signed by a company officer. A signed original of the copyright release should be mailed to:

Hwaci

6200 Maple Cove Lane

Charlotte, NC 28269

USA

A template copyright release is available in PDF or HTML. You can use this release to make future changes

Copyright Release for

Contributions To SQLite

SQLite is software that implements an embeddable SQL database engine. SQLite is available for free download from http://www.sqlite.org/. The principal author and maintainer of SQLite has disclaimed all copyright interest in his contributions to SQLite and thus released his contributions into the public domain. In order to keep the SQLite software unencumbered by copyright claims, the principal author asks others who may from time to time contribute changes and enhancements to likewise disclaim their own individual copyright interest.

Because the SQLite software found at http://www.sqlite.org/ is in the public domain, anyone is free to download the SQLite software from that website, make changes to the software, use, distribute, or sell the modified software, under either the original name or under some new name, without any need to obtain permission, pay royalties, acknowledge the original source of the software, or in any other way compensate, identify, or notify the original authors. Nobody is in any way compelled to contribute their SQLite changes and enhancements back to the SQLite website. This document concerns only changes and enhancements to SQLite that are intentionally and deliberately contributed back to the SQLite website.

For the purposes of this document, "SQLite software" shall mean any computer source code, documentation, makefiles, test scripts, or other information that is published on the SQLite website, http://www.sqlite.org/. Precompiled binaries are excluded from the definition of "SQLite software" in this document because the process of compiling the software may introduce information from outside sources which is not properly a part of SQLite.

The header comments on the SQLite source files exhort the reader to share freely and to never take more than one gives. In the spirit of that exhortation I make the following declarations:

1.I dedicate to the public domain any and all copyright interest in the SQLite software that was publicly available on the SQLite website (http://www.sqlite.org/) prior to the date of the signature below and any changes or enhancements to the SQLite software that I may cause to be published on that website in the future. I make this dedication for the benefit of the public at large and to the detriment of my heirs and successors. I intend this dedication to be an overt act of relinquishment in perpetuity of all present and future rights to the SQLite software under copyright law.

2.To the best of my knowledge and belief, the changes and enhancements that I have contributed to SQLite are either originally written by me or are derived from prior works which I have verified are also in the public domain and are not subject to claims of copyright by other parties.

3.To the best of my knowledge and belief, no individual, business, organization, government, or other entity has any copyright interest in the SQLite software as it existed on the SQLite website as of the date on the signature line below.

4.I agree never to publish any additional information to the SQLite website (by CVS, email, scp, FTP, or any other means) unless that information is an original work of authorship by me or is derived from prior published versions of SQLite. I agree never to copy and paste code into the SQLite code base from other sources. I agree never to publish on the SQLite website any information that would violate a law or breach a contract.

Signature:

Date:

Name (printed):

This Product includes Stunnel software under the stunnel license.

stunnel license (see COPYRIGHT.GPL for detailed GPL conditions)

Copyright (C) 1998-2011 Michal Trojnara

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, see <http://www.gnu.org/licenses>.

Linking stunnel statically or dynamically with other modules is making a combined work based on stunnel. Thus, the terms and conditions of the GNU General Public License cover the whole combination.

In addition, as a special exception, the copyright holder of stunnel gives you permission to combine stunnel with free software programs or libraries that are released under the GNU LGPL and with code included in the standard release of OpenSSL under the OpenSSL License (or modified versions of such code, with unchanged license). You may copy and distribute such a system following the terms of the GNU GPL for stunnel and the licenses of the other code concerned.

Note that people who make modified versions of stunnel are not obligated to grant this special exception for their modified versions; it is their choice whether to do so. The GNU General Public License gives permission to release a modified version without this exception; this exception also makes it possible to release a modified version which carries forward this exception.

This Product includes Zlib under the license by Zlib

Zlib License

/* zlib.h -- interface of the 'zlib' general purpose compression library

version 1.2.3, July 18th, 2005

Copyright (C) 1995-2005 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org

Mark Adler mdler@alumni.caltech.edu

E

Legal Information

Copyright

Copyright © 2011 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

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 Device is subject to the terms and conditions of any related service providers.

Do not use the WiMAX Device 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 complies with part 15 of the FCC Rules.
- Operation is subject to the condition that this device does not cause harmful interference.

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 device is designed for the WLAN 2.4 GHz and/or 5 GHz networks throughout the EC region and Switzerland, with restrictions in France.

Ce produit est conçu pour les bandes de fréquences 2,4 GHz et/ou 5 GHz conformément à la législation Européenne. En France métropolitaine, suivant les décisions n°03-908 et 03-909 de l’ARCEP, la puissance d’émission ne devra pas dépasser 10 mW (10 dB) dans le cadre d’une installation WiFi en extérieur pour les fréquences comprises entre 2454 MHz et 2483,5 MHz.

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.

Regulatory Information

European Union

The following information applies if you use the product within the European Union.

Declaration of Conformity with Regard to EU Directive 1999/5/EC (R&TTE Directive)

Compliance Information for 2.4GHz and 5GHz Wireless Products Relevant to the EU and Other Countries Following the EU Directive 1999/5/EC (R&TTE Directive)

[Czech]	ZyXEL tímto prohlašuje, že tento zařízení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/EC.
[Danish]	Undertegnede ZyXEL erklærer herved, at følgende udstyr udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
[German]	Hiermit erklärt ZyXEL, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EU befindet.
[Estonian]	Käesolevaga kinnitab ZyXEL seadme seadmed vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, *ZyXEL* declares that this equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
[Spanish]	Por medio de la presente ZyXEL declara que el equipo cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
[Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ ZyXEL ΔΗΛΩΝΕΙ ΟΤΙ εξοπλισμός ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕC.
[French]	Par la présente ZyXEL déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/EC.

[Italian]	Con la presente ZyXEL dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
[Latvian]	Ar šo ZyXEL deklarē, ka iekārtas atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
[Lithuanian]	Šiuo ZyXEL deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
[Dutch]	Hierbij verklaart ZyXEL dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EC.
[Maltese]	Hawnhekk, ZyXEL, jiddikjara li dan tagħmir jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
[Hungarian]	Alulírott, ZyXEL nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EK irányelv egyéb elõírásainak.
[Polish]	Niniejszym ZyXEL oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
[Portuguese]	ZyXEL declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/EC.
[Slovenian]	ZyXEL izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/EC.
[Slovak]	ZyXEL týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/EC.
[Finnish]	ZyXEL vakuuttaa täten että laitteet tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
[Swedish]	Härmed intygar ZyXEL att denna utrustning står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EC.
[Bulgarian]	С настоящото ZyXEL декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 1999/5/EC.

[Icelandic]	Hér með lýsir, ZyXEL því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 1999/5/EC.
[Norwegian]	Erklærer herved ZyXEL at dette utstyret er I samsvar med de grunnleggende kravene og andre relevante bestemmelser I direktiv 1999/5/EF.
[Romanian]	Prin prezenta, ZyXEL declară că acest echipament este în conformitate cu cerinţele esenţiale şi alte prevederi relevante ale Directivei 1999/5/EC.

National Restrictions

This product may be used in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

Ce produit peut être utilisé dans tous les pays de l'UE (et dans tous les pays ayant transposés la directive 1999/5/CE) sans aucune limitation, excepté pour les pays mentionnés ci-dessous:

Questo prodotto è utilizzabile in tutte i paesi EU (ed in tutti gli altri paesi che seguono le direttive EU 1999/5/EC) senza nessuna limitazione, eccetto per i paesii menzionati di seguito:

Das Produkt kann in allen EU Staaten ohne Einschränkungen eingesetzt werden (sowie in anderen Staaten die der EU Direktive 1995/5/CE folgen) mit Außnahme der folgenden aufgeführten Staaten:

In the majority of the EU and other European countries,the 2,4- and 5-GHz bands have been made available for the use of wireless local area networks (LANs). Later in this document you will find an overview of countries in
which additional restrictions or requirements or both are applicable.
The requirements for any country may evolve. ZyXEL recommends that you check with the local authorities for the latest status of their national regulations for both the 2,4- and 5-GHz wireless LANs.
The following countries have restrictions and/or requirements in addition to those given in the tablelabeled "*Overview of Regulatory Requirements for Wireless LANs*":

Overview of Regulatory Requirements for Wireless LANs

Frequency Band (MHz)	Max Power Level (EIRP)[1] (mW)	Indoor ONLY	Indoor and Outdoor
2400-2483.5	100		V
5150-5350	200	V	
5470-5725	1000		V

Belgium
The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check http://www.bipt.be for more details.

Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie http://www.bipt.be voor meer gegevens.

Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez http://www.ibpt.be pour de plus amples détails.

Denmark
In Denmark, the band 5150 - 5350 MHz is also allowed for outdoor usage.

I Danmark må frekvensbåndet 5150 - 5350 også anvendes udendørs.

France
For 2.4 GHz, the output power is restricted to 10 mW EIRP when the product is used outdoors in the band 2454 - 2483.5 MHz. There are no restrictions when used indoors or in other parts of the 2.4 GHz band. Check http://www.arcep.fr/ for more details.

Pour la bande 2.4 GHz, la puissance est limitée à 10 mW en p.i.r.e. pour les équipements utilisés en extérieur dans la bande 2454 - 2483.5 MHz. Il n'y a pas de restrictions pour des utilisations en intérieur ou dans d'autres parties de la bande 2.4 GHz. Consultez http://www.arcep.fr/ pour de plus amples détails.

R&TTE 1999/5/EC
WLAN 2.4 – 2.4835 GHz
IEEE 802.11 b/g/n

Location	Frequency Range(GHz)	Power (EIRP)
Indoor (No restrictions)	2.4 – 2.4835	100mW (20dBm)
Outdoor	2.4 – 2.454	100mW (20dBm)
	2.454 – 2.4835	10mW (10dBm)

Italy
This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a “general authorization.” Please check http://www.sviluppoeconomico.gov.it/ for more details.

Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all 'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una “Autorizzazione Generale”. Consultare http://www.sviluppoeconomico.gov.it/ per maggiori dettagli.

Latvia
The outdoor usage of the 2.4 GHz band requires an authorization from the Electronic Communications Office. Please check http://www.esd.lv for more details.

2.4 GHz frekvenèu joslas izmantoðanai ârpus telpâm nepiecieðama atïauja no Elektronisko sakaru direkcijas. Vairâk informâcijas: http://www.esd.lv.

Notes:
1. Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 1999/5/EC has also been implemented in those countries.
2. The regulatory limits for maximum output power are specified in EIRP. The EIRP level (in dBm) of a device can be calculated by adding the gain of the antenna used(specified in dBi) to the output power available at the connector (specified in dBm).

Index

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W