

# HES-309M

WiMAX Outdoor CPE

## User's Guide



### Default Login Details

IP Address: <http://192.168.1.1>

User Name: admin

Password: 1234

Firmware Version 2.00  
Edition 1, 10/2010

[www.zyxel.com](http://www.zyxel.com)

# ZyXEL



# About This User's Guide

## Intended Audience

This manual is intended for people who want to configure the ZyXEL WiMAX Device using the ZyXEL Web Configurator. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

## Related Documentation

- Quick Start Guide

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

- Support Disc

Refer to the included CD for support documents.

- ZyXEL Web Site

Please refer to [www.zyxel.com](http://www.zyxel.com) for additional support documentation and product certifications.

## Documentation Feedback

Send your comments, questions or suggestions to: [techwriters@zyxel.com.tw](mailto:techwriters@zyxel.com.tw)

Thank you!

The Technical Writing Team, ZyXEL Communications Corp.,  
6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 30099, Taiwan.

## Need More Help?

More help is available at [www.zyxel.com](http://www.zyxel.com).



- Download Library

Search for the latest product updates and documentation from this link. Read the Tech Doc Overview to find out how to efficiently use the documentation in order to better understand how to use your product.

- Knowledge Base

If you have a specific question about your product, the answer may be here. This is a collection of answers to previously asked questions about ZyXEL products.

- Forum

This contains discussions on ZyXEL products. Learn from others who use ZyXEL products and share your experiences as well.

## **Customer Support**

Should problems arise that cannot be solved by the methods listed above, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device.

See [http://www.zyxel.com/web/contact\\_us.php](http://www.zyxel.com/web/contact_us.php) for contact information. Please have the following information ready when you contact an office.

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

---

# Document Conventions

## Warnings and Notes

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

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

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





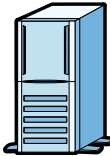






## Syntax Conventions

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

## Icons Used in Figures

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

**Table 1** Common Icons

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

# Safety Warnings

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

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

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

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

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





# Contents Overview

<b>User's Guide .....</b>	<b>15</b>
Getting Started .....	17
The Web Configurator .....	19
Setup Wizard .....	23
Tutorials .....	29
<b>Technical Reference .....</b>	<b>45</b>
System Status .....	47
WiMAX .....	51
Network Settings .....	73
Security .....	105
Maintenance .....	111
Troubleshooting .....	137
Product Specifications .....	143



# Table of Contents

<b>About This User's Guide .....</b>	<b>3</b>
<b>Document Conventions.....</b>	<b>5</b>
<b>Safety Warnings.....</b>	<b>7</b>
<b>Contents Overview .....</b>	<b>9</b>
<b>Table of Contents.....</b>	<b>11</b>
<b>Part I: User's Guide.....</b>	<b>15</b>
<b>Chapter 1</b>	
<b>Getting Started .....</b>	<b>17</b>
1.1 About Your WiMAX Device .....	17
1.1.1 WiMAX Internet Access .....	17
1.2 WiMAX Device Hardware .....	18
1.2.1 LEDs .....	18
1.3 Good Habits for Device Management .....	18
<b>Chapter 2</b>	
<b>The Web Configurator .....</b>	<b>19</b>
2.1 Overview .....	19
2.1.1 Accessing the Web Configurator .....	19
2.1.2 The Reset Button .....	20
2.1.3 Saving and Canceling Changes .....	20
2.1.4 Working with Tables .....	21
2.2 The Main Screen .....	22
<b>Chapter 3</b>	
<b>Setup Wizard .....</b>	<b>23</b>
3.1 Overview .....	23
3.1.1 Welcome to the Setup Wizard .....	23
3.1.2 LAN Settings .....	24
3.1.3 WiMAX Frequency Settings .....	25
3.1.4 WiMAX Authentication Settings .....	27
3.1.5 Setup Complete .....	28

<b>Chapter 4</b>	
<b>Tutorials</b>	<b>29</b>
4.1 Overview	29
4.2 WiMAX Connection Settings	29
4.3 Configuring LAN DHCP	30
4.4 Changing Certificate	32
4.5 Blocking Web Access	33
4.6 Configuring the MAC Address Filter	34
4.7 Setting Up NAT Port Forwarding	36
4.8 Access the WiMAX Device Using DDNS	39
4.8.1 Registering a DDNS Account on www.dyndns.org	39
4.8.2 Configuring DDNS on Your WiMAX Device	40
4.8.3 Testing the DDNS Setting	40
4.9 Configuring Static Route for Routing to Another Network	40
4.10 Remotely Managing Your WiMAX Device	43
<b>Part II: Technical Reference</b>	<b>45</b>
<b>Chapter 5</b>	
<b>System Status</b>	<b>47</b>
5.1 Overview	47
5.2 System Status	47
<b>Chapter 6</b>	
<b>WiMAX</b>	<b>51</b>
6.1 Overview	51
6.1.1 What You Need to Know	51
6.2 Connection Settings	55
6.3 Frequency Settings	57
6.4 Authentication Settings	60
6.5 Connect	63
6.6 Wide Scan	66
6.7 Link Status	67
6.8 Link Statistics	69
6.9 Connection Info	70
6.10 Service Flow	70
6.11 Buzzer	71
<b>Chapter 7</b>	
<b>Network Settings</b>	<b>73</b>
7.1 Overview	73

7.1.1 What You Need to Know .....	73
7.2 WAN .....	78
7.3 PPPoE .....	80
7.4 GRE .....	82
7.5 EtherIP .....	82
7.6 IP .....	83
7.7 DHCP .....	84
7.8 Static Route .....	85
7.9 RIP .....	86
7.10 Port Forwarding .....	87
7.10.1 Port Forwarding Wizard .....	89
7.11 Port Trigger .....	90
7.11.1 Port Trigger Wizard .....	91
7.11.2 Trigger Port Forwarding Example .....	92
7.12 DMZ .....	93
7.13 ALG .....	94
7.14 UPnP .....	95
7.14.1 Installing UPnP in Windows XP .....	95
7.14.2 Web Configurator Easy Access .....	99
7.15 DDNS .....	101
7.16 Content Filter .....	102
<b>Chapter 8</b>	
<b>Security.....</b>	<b>105</b>
8.1 Overview .....	105
8.1.1 What You Need to Know .....	105
8.2 IP Filter .....	106
8.3 MAC Filter .....	107
8.4 DDOS .....	108
<b>Chapter 9</b>	
<b>Maintenance .....</b>	<b>111</b>
9.1 Overview .....	111
9.1.1 What You Need to Know .....	111
9.2 Password .....	118
9.3 HTTP .....	119
9.4 Telnet .....	120
9.5 SSH .....	121
9.6 SNMP .....	122
9.7 CWMP .....	123
9.8 OMA-DM .....	125
9.9 Date .....	127
9.10 Time Zone .....	128

9.11 Upgrade File .....	128
9.11.1 The Firmware Upload Process .....	129
9.12 Upgrade Link .....	130
9.13 CWMP Upgrade .....	130
9.14 Backup .....	131
9.15 Restore .....	132
9.15.1 The Restore Configuration Process .....	132
9.16 Factory Defaults .....	133
9.17 Log Setting .....	133
9.18 Log Display .....	134
9.19 About .....	135
9.20 Reboot .....	135
<b>Chapter 10</b>	
<b>Troubleshooting.....</b>	<b>137</b>
10.1 Power, Hardware Connections, and LEDs .....	137
10.2 WiMAX Device Access and Login .....	138
10.3 Internet Access .....	140
10.4 Reset the WiMAX Device to Its Factory Defaults .....	141
10.4.1 Pop-up Windows, JavaScript and Java Permissions .....	142
<b>Chapter 11</b>	
<b>Product Specifications.....</b>	<b>143</b>
Appendix A WiMAX Security.....	147
Appendix B Setting Up Your Computer's IP Address.....	151
Appendix C Pop-up Windows, JavaScript and Java Permissions.....	179
Appendix D IP Addresses and Subnetting .....	189
Appendix E Importing Certificates .....	201
Appendix F Common Services.....	233
Appendix G Legal Information.....	237
<b>Index.....</b>	<b>241</b>

---

# **PART I**

## **User's Guide**

---





# Getting Started

## 1.1 About Your WiMAX Device

The WiMAX Device that allows you to access the Internet by connecting to a WiMAX wireless network. You can configure firewall and content filtering as well as a host of other features and the browser-based user interface -- the Web Configurator -- provides easy management.

See [Chapter 11 on page 143](#) for a complete list of features for your model.

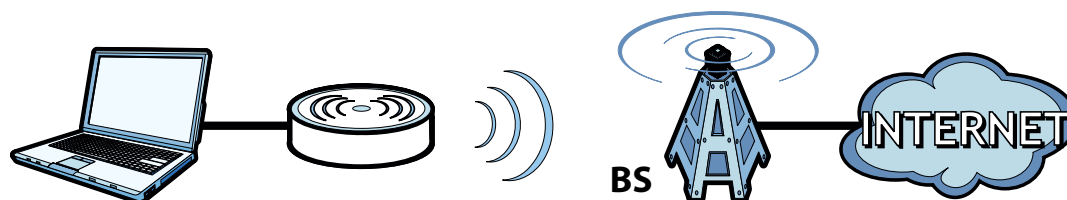
### 1.1.1 WiMAX Internet Access

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

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 (**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.

## 1.2 WiMAX Device Hardware

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

### 1.2.1 LEDs

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

## 1.3 Good Habits for Device Management

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.

# 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 179](#) 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 "" as the URL.
- 4 Enter the default **Username** (admin) and **Password** (1234), then click **Login**. The **Main** screen displays.

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 The Reset Button

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

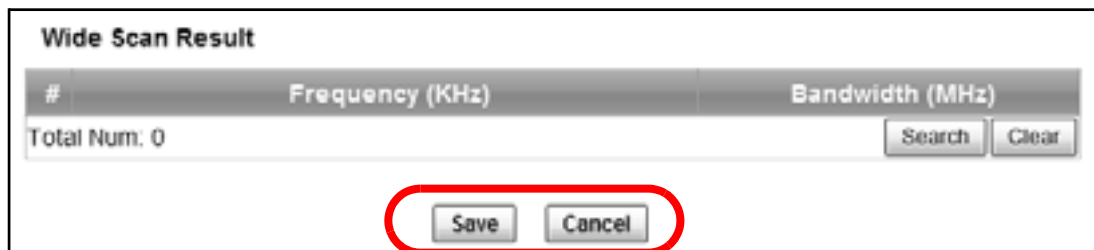
### 2.1.2.1 Using The Reset Button

- 1 Make sure the **Power** light is on (not blinking).
- 2 To set the device back to the factory default settings, press the **Reset** button for five seconds or until all LED lights blink one time, then release it. The device restarts when the defaults have been restored.
- 3 Reconfigure the WiMAX Device following the steps in your Quick Start Guide.

## 2.1.3 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 2** 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 disregarded.

## 2.1.4 Working with Tables

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

**Figure 3** Tables Example



This screen contains the following fields:

**Table 3** Saving and Canceling Changes

LABEL	DESCRIPTION
<input type="text" value="10"/> ▾ per page	<b>Items per Page</b> This displays the number of items displayed per table page. Use the menu to change this value.
⏪	<b>First Page</b> Click this to go to the first page in the table.
◀	<b>Previous Page</b> Click this to go to the previous page in the table.
<input type="text" value="0"/> ▾ page	<b>Page Indicator / Jump to Page</b> 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.
▶	<b>Next Page</b> Click this to go to the previous page in the table.
⏩	<b>Last Page</b> 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.





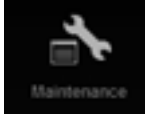
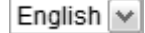


## 2.2 The Main Screen

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 firmware version and/or configuration.

The following table describes the icons in this screen.

**Table 4** Main > Icons

ICON	DESCRIPTION
	<p>System Status</p> <p>Click this to open the Main screen, which shows your WiMAX Device status and other information.</p>
	<p>WiMAX</p> <p>Click this to open the WiMAX menu, which gives you options for configuring your WiMAX settings.</p>
	<p>Network Setting</p> <p>Click this to open the Network menu, which gives you options for configuring your network settings.</p>
	<p>Security</p> <p>Click this to open the Security menu, which gives you options for configuring your firewall and security settings.</p>
	<p>Maintenance</p> <p>Click this to open the Maintenance menu, which gives you options for maintaining your WiMAX Device.</p>
	<p>Language</p> <p>Use this menu to select the Web Configurator's language.</p>
	<p>Setup Wizard</p> <p>Click this to open the Setup Wizard, where you can configure the most essential settings for your WiMAX Device to work.</p>
	<p>Logout</p> <p>Click this to log out of the Web Configurator.</p>

# Setup Wizard

## 3.1 Overview

This chapter provides information on the ZyXEL Setup Wizard. The wizard guides you through several steps for onfiguring 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.

**Figure 4** Setup Wizard > Welcome



## 3.1.2 LAN Settings

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

**Figure 5** 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.



**Table 5** Setup Wizard > LAN Settings (continued)

LABEL	DESCRIPTION
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.
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: These settings should be provided by your ISP.

**Figure 6** Setup Wizard > WiMAX Frequency Settings

Setup Wizard

Step 2: WiMAX Frequency Settings

**Set Frequency**

Setting Type: By List

Bandwidth: 10 MHz

#	Frequency(MHz)
1	3550

Total Num: 1

Valid Band Info:

#	Band Start(KHz)	Band End(KHz)
1	3300000	3600000

Total Num: 1

Back Next

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. <ul style="list-style-type: none"> <li>• <b>By Range</b> - Select this to set up the frequency based on a range of MHz.</li> <li>• <b>By List</b> - Select this to set up the frequency on an individual MHz basis. You can add multiple MHz values to the list.</li> </ul>
Step	Enter the increments in MHz by which to increase the frequency range.  Note: This field only appears when you select <b>By Range</b> under <b>Setting Type</b> .
Start Frequency	Enter the frequency value at the beginning of the frequency range to use. The frequency is increased in increments equal to the <b>Step</b> value until the <b>End Frequency</b> is reached, at which time the cycle starts over with the <b>Start Frequency</b> .  Note: This field only appears when you select <b>By Range</b> under <b>Setting Type</b> .
End Frequency	Enter the frequency value at the end of the frequency range to use.  Note: This field only appears when you select <b>By Range</b> under <b>Setting Type</b> .
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.

**Figure 7** Setup Wizard > WiMAX Authentication Settings

The screenshot shows a window titled "Setup Wizard" with a close button in the top right corner. The main content area is titled "Step 3: WiMAX Authentication Settings". Below this title, there are two sections: "Authentication" and "EAP Supplicant".

- Authentication:** The "Authentication Mode" is set to "User and device authentication" via a dropdown menu.
- EAP Supplicant:**
  - "EAP Mode" is set to "EAP-TTLS" via a dropdown menu.
  - "Anonymous ID" is an empty text input field.
  - "Inner Mode" is set to "MS-CHAPv2" via a dropdown menu.
  - "Username" is an empty text input field.
  - "Password" is an empty password input field with masked characters.

At the bottom right of the window, there are two buttons: "Back" and "Next".

The following table describes the labels in this screen.

**Table 7** Setup Wizard > WiMAX Authentication Settings

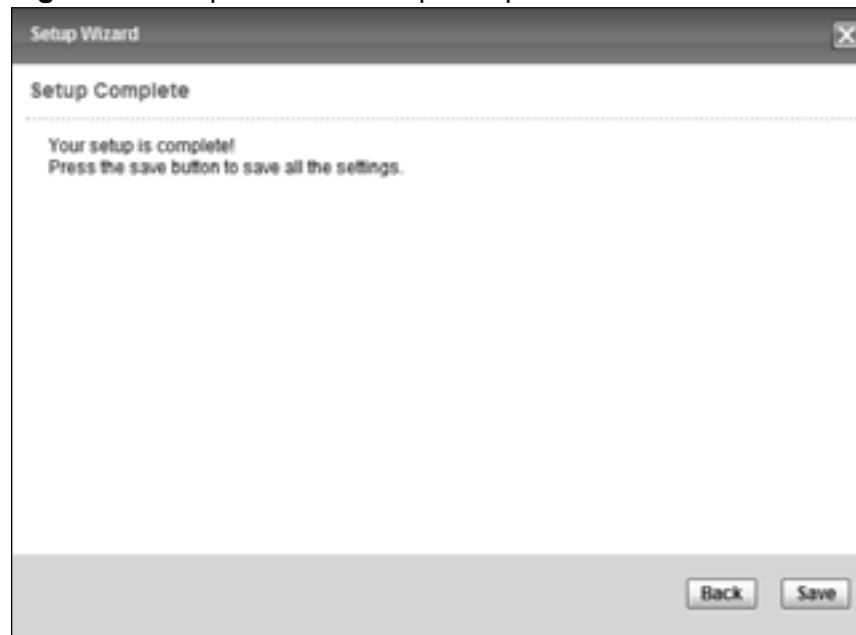
LABEL	DESCRIPTION
Authentication	
Authentication Mode	Select a WiMAX authentication mode for authentication network sessions with the ISP. Options are: <ul style="list-style-type: none"> <li>No authentication</li> <li>User authentication</li> <li>Device authentication</li> <li>User and Device authentication</li> </ul>
EAP Supplication	
EAP Mode	Select an EAP authentication mode.
Anonymous Id	Enter your anonymous ID.  Note: Some modes may not require this.
Inner Mode	Select an inner authentication mode.  Note: Some modes may not require this.

**Table 7** Setup Wizard > WiMAX Authentication Settings (continued)

LABEL	DESCRIPTION
Username	Enter your authentication username.  Note: Some modes may not require this.
Password	Enter your authentication password.  Note: Some modes may not require this.
Back	Click to display the previous screen.
Next	Click to proceed to the next screen.

### 3.1.5 Setup Complete

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

**Figure 8** Setup Wizard > Setup Complete

Launch your web browser and navigate to [www.zyxel.com](http://www.zyxel.com). If everything was configured properly, the web page should display. You can now surf the Internet!

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

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

# Tutorials

## 4.1 Overview

This chapter shows you how to configure some of the WiMAX Device's features.

Note: Be sure to read [The Web Configurator on page 19](#) 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 29](#)
- [Configuring LAN DHCP on page 30](#)
- [Changing Certificate on page 32](#)
- [Blocking Web Access on page 33](#)
- [Configuring the MAC Address Filter, see page 34](#)
- [Setting Up NAT Port Forwarding, see page 36](#)
- [Access the WiMAX Device Using DDNS, see page 39](#)
- [Configuring Static Route for Routing to Another Network, see page 40](#)
- [Remotely Managing Your WiMAX Device on page 43](#)

## 4.2 WiMAX Connection Settings

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

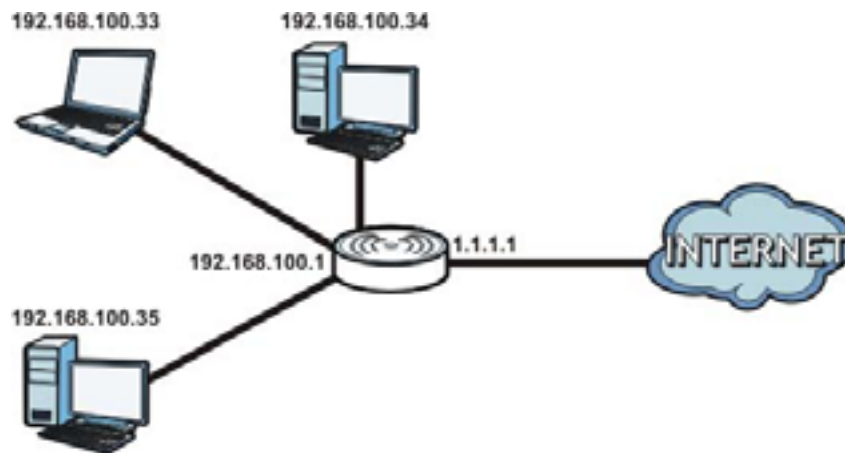
- 1 Connect the WiMAX Device to the ISP's nearest base station. See [Section 6.2 on page 55](#).
- 2 Configure the WiMAX Device's broadcast frequency. [Section 6.3 on page 57](#).
- 3 Configure the WiMAX Device to connect securely to the ISP's authentication servers. See [Section 6.4 on page 60](#).

- 4 Check the WiMAX Device's connection status to ensure everything is working properly. See [Section 6.7 on page 67](#).

## 4.3 Configuring LAN DHCP

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	<a href="#">Chapter 7 on page 83</a>
Starting IP Address	192.168.100.10	<a href="#">Chapter 7 on page 84</a>
Ending IP Address	192.168.100.30	
DNS Servers	From ISP	

- 1 In the Web Configurator, open the **Networking 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**.

The screenshot shows a web form for configuring LAN settings. It has two input fields: 'IP Address' with the value '192.168.100.1' and 'IP Subnet Mask' with the value '255.255.255.0'. At the bottom right, there are two buttons: 'Save' and 'Cancel'.

- 2 Manually change the IP address of your computer that you 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 **Networking Setting > LAN > DHCP** screen.

**DHCP Server**

DHCP Mode:

Start IP:

End IP:

Lease Time:  (minutes)

Relay IP:

**DNS Server assigned by DHCP Server**

First DNS Server:

Second DNS Server:

Third DNS Server:

**Static DHCP**

10 per page

#	MAC Address	IP Address
Total Num: 0		

Add OK

- 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 **Networking Setting > WAN** screen and select **NAT** in the **Operation Mode** field. Click **Save**.

**Operation Mode**

WAN Protocol:

Bridging LAN ARP:

Get IP Method:

WAN IP Request Timeout:  seconds (0-600, default: 120, infinite: 0)

WAN IP Address:

WAN IP Subnet Mask:

Gateway IP Address:

MTU:

Clone MAC Address:

**WAN DNS**

First DNS Server:

Second DNS Server:

Third DNS Server:

Save Cancel

- 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 151](#).

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 23](#)), which walks you through the process.

## 4.4 Changing Certificate

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

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

**See Also:** [Appendix E on page 201](#).

- 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.

Options	
Enable Auth Mode Decoration in EAP Outer ID	<input type="checkbox"/>
Enable Service Mode Decoration in EAP Outer ID	<input type="checkbox"/>
Random Outer ID	<input type="checkbox"/>
Ignore Cert Verification	<input type="checkbox"/>
Same EAP OuterID in ReAuth	<input type="checkbox"/>
MAC address in EAP-TLS outer ID	<input type="checkbox"/>
Delete existed Root Certificate file	<input type="checkbox"/>
Delete existed Device Certificate file	<input type="checkbox"/>
Delete existed Private Key	<input type="checkbox"/>

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

## 4.5 Blocking Web Access

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 7.16 on page 102](#).

- 1 Open the **Networking 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 Configuring the MAC Address Filter

This tutorial shows you how to use the MAC filter to block a DHCP client's access to hosts and 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).

**DHCP Server**

DHCP Mode: Server

Start IP: 192.168.100.2

End IP: 192.168.100.254

Lease Time: 1440 (minutes)

Relay IP: 0.0.0.0

**DNS Server assigned by DHCP Server**

First DNS Server: From ISP 0.0.0.0

Second DNS Server: From ISP 0.0.0.0

Third DNS Server: From ISP 0.0.0.0

**Static DHCP**

Total Num: 0

**DHCP Leased Hosts**

#	MAC Address	IP Address	Remaining Time
1	00:02:E3:57:9A:1C	192.168.100.2	23:57:44
2	00:02:E3:53:16:95	192.168.100.3	23:57:50

Total Num: 2

Save Cancel

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

**MAC List**

Blacklist/Whitelist: Blacklist

**MAC Filter Rules**

#	Active	Source MAC	Destination MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time
Total Num: 0												

Add

Save Cancel

- 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**.

MAC List

Blacklist/Whitelist:

MAC Filter Rules

10 per page 1 page

#	Active	Source MAC	Destination MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time
1	<input checked="" type="checkbox"/>	00:02:E3:53:16:95		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59

Total Num: 1

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

## 4.7 Setting Up NAT Port Forwarding

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

- 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.

DHCP Leased Hosts

10 per page 0 page

#	MAC Address	IP Address	Remaining Time
1	00:02:E3:53:16:95	192.168.100.2	23:57:44
2	00:1E:52:C3:56:95	192.168.100.3	23:57:50

Total Num: 2

- 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**.

The screenshot shows the WAN configuration interface. The 'Operation Mode' dropdown menu is highlighted with a red circle and set to 'NAT'. Other fields include WAN Protocol (Ethernet), Bridging LAN ARP (No), Get IP Method (From ISP), WAN IP Request Timeout (120 seconds), WAN IP Address (1.0.0.0), WAN IP Subnet Mask (1.0.0.0), Gateway IP Address (1.0.0.0), MTU (1400), Clone MAC Address (00:0C:EF:0B:01:01), and WAN DNS servers (all set to From ISP and 1.0.0.0). 'Save' and 'Cancel' buttons are at the bottom.

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

The screenshot shows the Port Forwarding table with 5 entries. The first entry is highlighted with a red circle. A tooltip 'Click to edit or delete' is visible over the first entry's edit/delete icon.

#	Active	Name	Protocol	Incoming Port(s)		Forward Port(s)		Server IP
				Start Port	End Port	Start Port	End Port	
1	N	Name1	TCP	0	0	0	0	1.1.1.1
2	N	Name2	TCP	0	0	0	0	1.1.1.1
3	N	Name3	TCP	0	0	0	0	1.1.1.1
4	N	Name4	TCP	0	0	0	0	1.1.1.1
5	N	Name5	TCP	0	0	0	0	1.1.1.1

Total Num: 5

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

The screenshot shows the Port Forwarding table with 5 entries. The first entry is configured for Xbox 360, with the 'Active' checkbox checked and the protocol set to TCP. The incoming and forward ports are all set to 53. The server IP is 192.168.1.34.

#	Active	Name	Protocol	Incoming Port(s)		Forward Port(s)		Server IP
				Start Port	End Port	Start Port	End Port	
1	<input checked="" type="checkbox"/>	Xbox 360	TCP	53	53	53	53	192.168.1.34
2	N	Name2	TCP	0	0	0	0	1.1.1.1
3	N	Name3	TCP	0	0	0	0	1.1.1.1
4	N	Name4	TCP	0	0	0	0	1.1.1.1
5	N	Name5	TCP	0	0	0	0	1.1.1.1

Total Num: 5

- 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.

#	Active	Name	Protocol	Incoming Port(s)		Forward Port(s)		Server IP
				Start Port	End Port	Start Port	End Port	
1	Y	Xbox 360	TCP	53	53	53	53	192.168.1.34
2	Y	Xbox 360	TCP	80	80	80	80	192.168.1.34
3	Y	Xbox 360	TCP	88	88	88	88	192.168.1.34
4	Y	Xbox 360	TCP	3074	3074	3074	3074	192.168.1.34
5	N	Name5	TCP	0	0	0	0	1.1.1.1

Total Num: 5

Wizard Add OK Save Cancel

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

**HTTP Server**

Enable

Port Number

**HTTPS Server**

Enable

Port Number

**HTTP and HTTPS**

Allow Connection from WAN

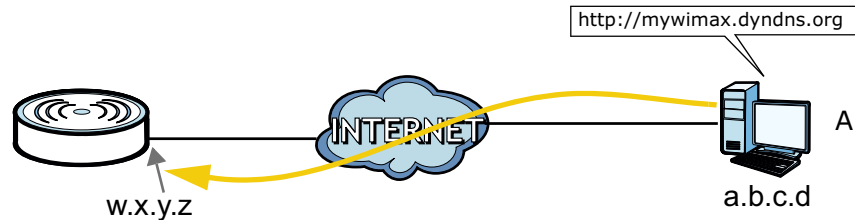
**HTTP Session Timeout**

Session Timeout  minutes (0-99, default 5, 0 means disabled)

Save Cancel

## 4.8 Access the WiMAX Device Using DDNS

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](http://www.dyndns.org).

This tutorial covers:

- [Registering a DDNS Account on \[www.dyndns.org\]\(http://www.dyndns.org\)](#)
- [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 198](#)), then you cannot use DDNS.

### 4.8.1 Registering a DDNS Account on [www.dyndns.org](http://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](http://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:

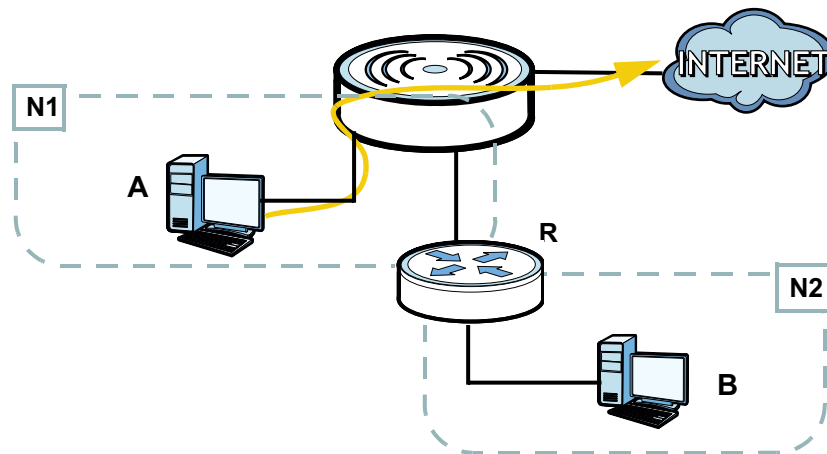
- 1 Open a web browser on the computer (using the IP address **a.b.c.d**) that is connected to the Internet.
- 2 Type **http://mywimax.dyndns.org** and press [Enter].
- 3 The WiMAX Device's login page should appear. You can then log into the WiMAX Device and manage it.

## 4.9 Configuring Static Route for Routing to Another Network

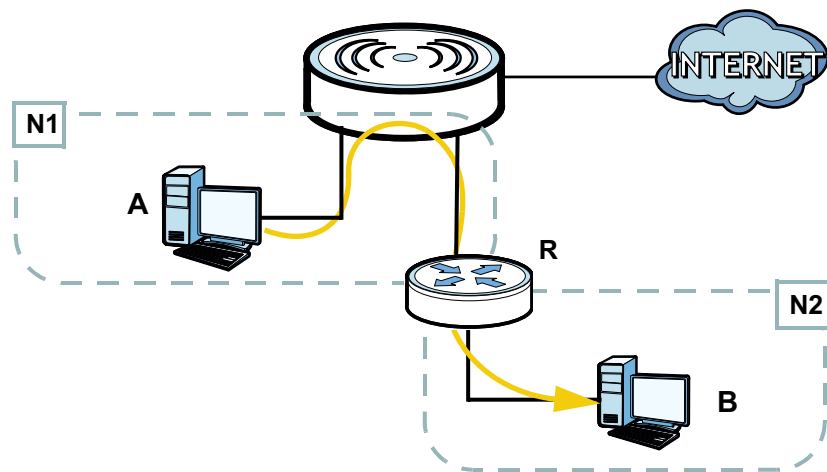
In order to extend your Intranet and control traffic flowing directions, you may connect a router to the WiMAX Device's LAN. The router may be used to separate two department networks. This tutorial shows how to configure a static routing rule for two network routings.



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 8** 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
<b>A</b>	192.168.1.34
<b>R</b> 's IP address on N1	192.168.1.253
<b>R</b> 's IP address on N2	192.168.10.2
<b>B</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 9.3 on page 119](#).

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

**HTTP Server**  
Enable   
Port Number

**HTTPS Server**  
Enable   
Port Number

**HTTP and HTTPS**  
Allow Connection from WAN

**HTTP Session Timeout**  
Session Timeout  minutes (0-99, default 5, 0 means disabled)

- 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**.



---

# **PART II**

## **Technical Reference**

---



# 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 9** System Status



The following tables describe the labels in this screen.

**Table 9** 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.
Firmware Version	This field displays the current version of the firmware inside the device.
Firmware Build Time	This field shows the date the firmware version was created.
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.  <b>Scanning</b> - The WiMAX Device is scanning for available base stations.  <b>Ready</b> - The WiMAX Device has finished a scanning and you can connect to a base station.  <b>Connecting</b> - The WiMAX Device attempts to connect to the selected base station.  <b>Connected</b> - 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.  <b>Network Search</b> - The WiMAX Device is scanning for any available WiMAX connections.  <b>Disconnected</b> - No WiMAX connection is available.  <b>Network Entry</b> - A WiMAX connection is initializing.  <b>Normal</b> - The WiMAX connection has successfully established.



**Table 9** Status (continued)

<b>LABEL</b>	<b>DESCRIPTION</b>
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.
<b>WAN</b>	
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.
<b>LAN</b>	
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.



## 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 10** 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 11** 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 12** Using an AAA Server

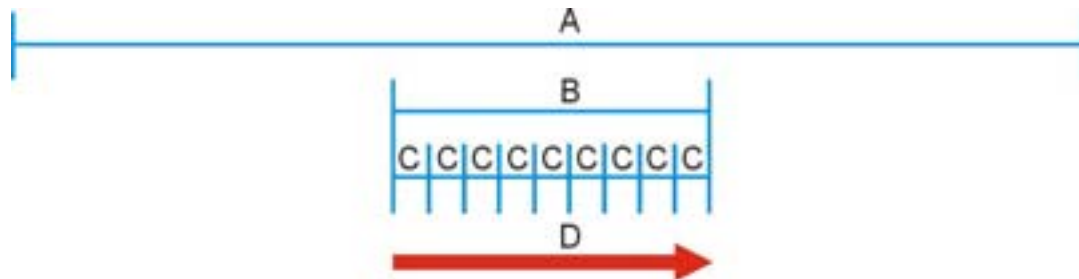


In this figure, the dashed arrow shows the PKM (Privacy Key Management) secured connection between the mobile station and the base station, and the solid arrow shows the EAP secured connection between the mobile station, the base station and the AAA server. See the WiMAX security appendix for more details.

## Frequency Ranges

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

**Figure 13** 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 PKCS#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 bursts. 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 14** Connection Settings Screen

**Connect Option Settings**

Auto Reconnect: 3 seconds (0-60, default 3, 0 means disabled)

Auto Connect Mode: by CINR

Enable Handover:

Enable Idle Mode:

Idle Mode Interval: 60 seconds (default 60)

CINR & RSSI Refresh Interval: 1000 msec (default 1000)

LDRP(Low Data Rate Protection) Time: 20000 msec (default 20000 ; 0 means disabled)

LDRP TX Rate: 10000 bytes/sec (default 10000)

LDRP RX Rate: 10000 bytes/sec (default 10000)

**Connect Type Settings**

Auto Connect Mode:

#	BSID	Preamble ID	Frequency (MHz)	Bandwidth (MHz)	RSSI (dBm)	CINR (dB) R3/R1
Total Num: 0						

This screen contains the following fields:

**Table 10** 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. <ul style="list-style-type: none"> <li>• <b>By channel power</b> - Auto connects to the base station if the signal strength of the channel is sufficient for the WiMAX Device.</li> <li>• <b>By CINR</b> - Auto connects to the base station if the signal-to-noise ratio is sufficient for the WiMAX Device.</li> </ul>
Enable Handover	Select this to maintain connectivity while the WiMAX Device switches its connection from one base station to another base station.
Enable 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.

**Table 10** Connection Settings (continued)

LABEL	DESCRIPTION
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	
Mode Select	Select how the WiMAX Device connects to the base station. <ul style="list-style-type: none"> <li>• <b>Auto Connect Mode</b> - The device connects automatically to the first base station in range.</li> <li>• <b>Network Search Mode</b> - The device scans for available base stations then connects to the best one it can.</li> </ul>
BSID	This displays the MAC address of a base station within range of the WiMAX Device.
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 station'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.

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

**Figure 15** Frequency Settings Screen (By List)

The screenshot shows the 'Frequency Settings (By List)' screen. At the top, 'Setting Type' is set to 'By List', 'Join Wide Scan Result' is 'No', and 'Default Bandwidth' is '10 MHz'. A table with one row is highlighted with a red circle labeled 'A'. Below it, 'Valid Band Info' is shown with a table also highlighted with a red circle labeled 'B'. Buttons for 'Add', 'OK', and 'Total Num: 1' are visible.

#	Frequency(KHz)	Bandwidth(MHz)
1	3550000	10

Total Num: 1

#	Band Start(KHz)	Band End(KHz)
1	3300000	3600000

Total Num: 1

**Figure 16** Frequency Settings Screen (By Range)

The screenshot shows the 'Frequency Settings (By Range)' screen. 'Setting Type' is set to 'By Range'. A table with one row is highlighted with a red circle labeled 'A'. Below it, 'Valid Band Info' is shown with a table also highlighted with a red circle labeled 'B'. Buttons for 'OK' and 'Total Num: 1' are visible.

#	Start Frequency (KHz)	End Frequency (KHz)	Step (KHz)	Bandwidth (MHz)
1				0

Total Num: 1

#	Band Start(KHz)	Band End(KHz)
1	3300000	3600000

Total Num: 1

This screen contains the following fields:

**Table 11** Frequency Settings

LABEL	DESCRIPTION
Setting Type	<p>Select whether to scan base stations by entering specific frequency(-ies) (<b>By List</b>) or a range of frequencies (<b>By Range</b>).</p> <p>Note: When you select <b>By Range</b>, you can only configure one range of frequencies in this screen. To configure multiple frequency ranges, use the <b>WiMAX &gt; Wide Scan</b> screen.</p> <p>Note: Some settings in this screen are only available depending on the <b>Setting Type</b> selected.</p>
Join Wide Scan Result	<p>The scanning result of the frequency to scan you configured in this screen will be shown in the <b>WiMAX &gt; Connect</b> screen. Select this option to determine whether to also append the wide scanning result (configured in the <b>WiMAX &gt; Wide Scan</b> screen) to the same table.</p>
Default Bandwidth	<p>Select the default bandwidth (size) per frequency band you specify in table <b>A</b>.</p>
<b>A</b> (When <b>By List</b> is selected in the <b>Setting Type</b> field)	
Frequency (KHz)	<p>This displays the center frequency of an frequency band in kilohertz (KHz).</p> <p>Click the number to modify it.</p> <p>Enter the center frequency in this field when you are adding an entry.</p>
Bandwidth (MHz)	<p>This displays the bandwidth of the frequency band in megahertz (MHz). If you set a center frequency to 3400000 KHz with the bandwidth of 10 MHz, then the frequency band is from 3300500 to 3400500 KHz.</p> <p>Click the number to modify it.</p> <p>Enter the bandwidth of the frequency band in this field when you are adding an entry.</p>
Delete	<p>Click this button to remove an item from the list.</p>
Add	<p>Click this button to add an item to the list.</p>
OK	<p>Click this button to save any changes made to the list.</p>
<b>A</b> (When <b>By Range</b> is selected in the <b>Setting Type</b> field)	
Start Frequency (KHz)	<p>This indicates the beginning of a frequency band in kilohertz (KHz).</p> <p>Click this field to modify it.</p> <p>Enter the beginning frequency when you are adding an entry.</p>
End Frequency (KHz)	<p>This indicates the end of the frequency band in kilohertz (KHz).</p> <p>Click this field to modify it.</p>
Step (KHz)	<p>This indicates the frequency step within each band in kilohertz (KHz).</p> <p>Click this field to modify it.</p>
Bandwidth (MHz)	<p>This indicates the bandwidth in megahertz (MHz).</p> <p>Click this field to modify it.</p>

**Table 11** Frequency Settings (continued)

LABEL	DESCRIPTION
OK	Click this button to save any changes made to the list.
<b>Valid Band Info (B)</b>  This table displays the entire frequency band the WiMAX Device supports. The frequenc(ies) to scan that you configured in table <b>A</b> 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 17** Authentication Settings Screen

Authentication Mode	User authentication
Data Encryption	
AES-CCM	<input checked="" type="checkbox"/>
AES-CBC	<input checked="" type="checkbox"/>
Key Encryption	
AES-key wrap	<input checked="" type="checkbox"/>
AES-ECB	<input checked="" type="checkbox"/>
<b>EAP Supplicant</b>	
EAP Mode	EAP-TLS
Anonymous ID	<input type="text"/>
Server Root CA Cert. File	<input type="text"/> Browse...
Server Root CA Cert. Info	No certificate file found
Device Cert. File	<input type="text"/> Browse...
Device Cert. Info	No certificate file found
Device Private Key	<input type="text"/> Browse...
Device Private Key Info	No private key found
Device Private Key Password	.....
Inner Mode	MS-CHAPv2
Username	<input type="text"/>
Password	.....
<b>Options</b>	
Enable Auth Mode Decoration in EAP Outer ID	<input type="checkbox"/>
Enable Service Mode Decoration in EAP Outer ID	<input type="checkbox"/>
Random Outer ID	<input type="checkbox"/>
Ignore Cert Verification	<input checked="" type="checkbox"/>
Same EAP OuterID in ReAuth	<input type="checkbox"/>
MAC address in EAP-TLS outer ID	<input type="checkbox"/>
Delete existed Root Certificate file	<input type="checkbox"/>
Delete existed Device Certificate file	<input type="checkbox"/>
Delete existed Private Key	<input type="checkbox"/>

This screen contains the following fields:

**Table 12** Authentication Settings

LABEL	DESCRIPTION
Authentication Mode	Select the authentication mode from the list.  The WiMAX Device supports the following authentication modes: <ul style="list-style-type: none"> <li>• No authentication</li> <li>• User authentication</li> <li>• Device authentication</li> <li>• User and device authentication</li> </ul>
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 to 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: <ul style="list-style-type: none"> <li>• <b>EAP-TLS</b> - 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.</li> <li>• <b>EAP-TTLS</b> - 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.</li> </ul>
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.
Device Cert Info	This field displays information about the assigned device certificate.

**Table 12** Authentication Settings (continued)

LABEL	DESCRIPTION
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	<p>Sets the EAP-TTLS inner mode.</p> <p>The WiMAX Device supports the following:</p> <ul style="list-style-type: none"> <li>• <b>MS-CHAP v2</b> - This is version 2 of Microsoft's variant of Challenge Handshake Authentication Protocol (CHAP). It allows for mutual authentication between devices.</li> <li>• <b>MS-CHAP</b> - This is Microsoft's variant of Challenge Handshake Authentication Protocol (CHAP). It allows for mutual authentication between devices.</li> <li>• <b>CHAP</b> - The Challenge Handshake Authentication Protocol (CHAP) uses PPP to authenticate remote devices using a three-way handshake and shared secret verification.</li> <li>• <b>MD5</b> - 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.</li> <li>• <b>PAP</b> - 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.</li> </ul>
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.

**Table 12** Authentication Settings (continued)

LABEL	DESCRIPTION
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 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 18** Connect Screen

Applied Frequency Information								
#	Frequency(KHz)	Bandwidth(MHz)						
1	3550000	10						
Total Num: 1								
Available Network List								
					Auto Connect Mode	▼	Connect	Disconnect
#	BSID	Preamble ID	Frequency (MHz)	Bandwidth (MHz)	RSSI (dBm)	CINR (dB) R3/R1		
1	F7:48:0A:01:13:21	42	3550	10	-78.82	18.95/14.59		
Total Num: 1							Search	
Connected BS Info								
#	Device Status	UMAC State	BSID	Frequency(MHz)	RSSI(dBm)	CINR(dB)		
1	Ready	Disconnected	00:00:00:00:00	0	0.00	0.00		
Total Num: 1								

This screen contains the following fields:

**Table 13** Connect

LABEL	DESCRIPTION
Applied Frequency Information	
This table shows the scanning result you made in the <b>WiMAX &gt; Profile &gt; Frequency Settings</b> and <b>WiMAX &gt; Wide Scan</b> screens.	
Note: You cannot see the wide scanning result that you made in <b>WiMAX &gt; Wide Scan</b> screen if the <b>Join Wide Scan Result</b> is set to <b>No</b> in the <b>WiMAX &gt; Profile &gt; Frequency Settings</b> screen.	
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: <ul style="list-style-type: none"> <li>• <b>Auto Connect Mode</b> - This allows the WiMAX Device to connect to any of the base stations on the list automatically.</li> <li>• <b>Network Search Mode</b> - This allows the WiMAX Device to connect to a user-specified base station. Select this option, choose a base station, click <b>Connect</b>.</li> </ul>
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.
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' 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).
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 <b>Applied Frequency Information</b> table.
Connected BS Info	



**Table 13** Connect (continued)

LABEL	DESCRIPTION
Device Status	<p>This field displays the WiMAX Device current status for connecting to the selected base station.</p> <p><b>Scanning</b> - The WiMAX Device is scanning for available base stations.</p> <p><b>Ready</b> - The WiMAX Device has finished scanning and you can connect to a base station.</p> <p><b>Connecting</b> - The WiMAX Device attempts to connect to the selected base station.</p> <p><b>Connected</b> - The WiMAX Device has successfully connected to the selected base station.</p>
UMAC State	<p>This field displays the status of the WiMAX connection between the WiMAX Device and the base station.</p> <p><b>Network Search</b> - The WiMAX Device is scanning for any available WiMAX connections.</p> <p><b>Disconnected</b> - No WiMAX connection is available.</p> <p><b>Network Entry</b> - A WiMAX connection is initializing.</p> <p><b>Normal</b> - The WiMAX connection has been successfully established.</p>
BSID	<p>This field displays the MAC address of the base station to which the WiMAX Device is connected.</p>
Frequency (MHz)	<p>This field displays the frequency the base station uses in megahertz (MHz).</p>
RSSI (dBm)	<p>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.</p>
CINR (dB)	<p>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.</p>

## 6.6 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 19** Wide Scan Screen

**Wide Scan Settings**

Auto Wide Scan  ▾

Wide Scan Range

#	Start Frequency (KHz)	End Frequency (KHz)	Step (KHz)	Bandwidth (MHz)
1	3500000	3600000	250	10

Total Num: 1

**Wide Scan Result**

#	Frequency (KHz)	Bandwidth (MHz)
1	3550000	10
2	3570000	10

Total Num: 2

This screen contains the following fields:

**Table 14** Wide Scan

LABEL	DESCRIPTION
Wide Scan Settings	
Auto Wide Scan	Use this to enable ( <b>Yes</b> ) or disable ( <b>No</b> ) 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.	

**Table 14** Wide Scan (continued)

LABEL	DESCRIPTION
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.

## 6.7 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 20** Link Status Screen

Connection Status	
Profile	Wimax
BSID	00:00:00:00:00:00
RSSI	0.00 dBm
CINR R3	0.00 dB
CINR R1	0.00 dB
CINR Std Dev	0.00 dB
Frequency	0 KHz
TX Power	0 dBm
UL MCS	QPSK [CC] 1/2
DL MCS	QPSK [CC] 1/2
RF Temperature	19 C

This screen contains the following fields:

**Table 15** 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.

**Table 15** Link Status (continued)

<b>LABEL</b>	<b>DESCRIPTION</b>
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 of the WiMAX Device's RF circuit.

## 6.8 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 21** 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
PSD Ratio	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 16** 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

## 6.9 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 22** Connection Info Screen



This screen contains the following fields:

**Table 17** 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.

## 6.10 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 23** Service Flow Screen



This screen contains the following fields:

**Table 18** 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.

## 6.11 Buzzer

This screen allows you to enable or disable the WiMAX Device's buzzer. See [Section 1.2.1 on page 18](#) for a description of buzzer states.

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

**Figure 24** Buzzer Screen



This screen contains the following fields:

**Table 19** Buzzer

LABEL	DESCRIPTION
Enable Buzzer	Select this to enable the buzzer. Whenever a connection is made to a WiMAX signal, the device emits a small buzz.





# Network Settings

## 7.1 Overview

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

### 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

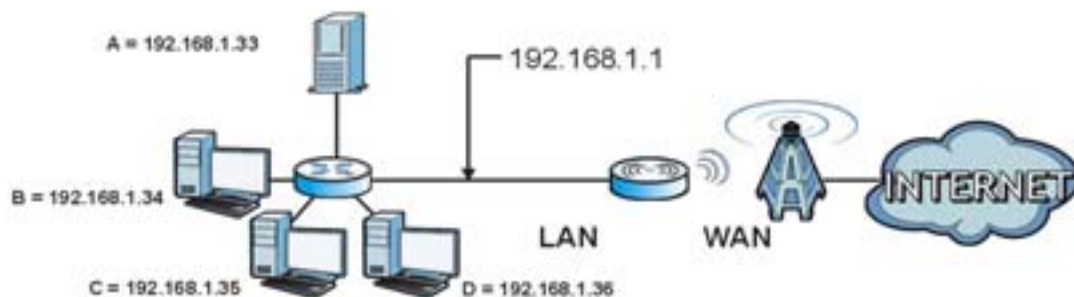
A NAT server set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make accessible to the outside world even though NAT makes your whole inside network appear as a single machine to the outside world.

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 25** 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 26** WAN Screen

Operation Mode	NAT
WAN Protocol	Ethernet
Bridging LAN ARP	No
Get IP Method	From ISP
WAN IP Request Timeout	120 <small>seconds (0~600, default:120, infinite:0)</small>
WAN IP Address	0.0.0.0
WAN IP Subnet Mask	0.0.0.0
Gateway IP Address	0.0.0.0
MTU	1500
Clone MAC Address	00:0C:E7:0B:01:01
<b>WAN DNS</b>	
First DNS Server	From ISP 0.0.0.0
Second DNS Server	From ISP 0.0.0.0
Third DNS Server	From ISP 0.0.0.0

This screen contains the following fields:

**Table 20** WAN

LABEL	DESCRIPTION
Operation Mode	Select the WiMAX Device's operational mode. <ul style="list-style-type: none"> <li>• <b>Bridge</b> - 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.</li> <li>• <b>NAT</b> - 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.</li> </ul>
WAN Protocol	Select the protocol the WiMAX Device uses to connect to the WAN. The options are: <ul style="list-style-type: none"> <li>• <b>Ethernet</b> - Select this if you have a persistent connection to the network.</li> <li>• <b>PPPoE</b> - Select this if must log into the network before initiating a persistent connection.</li> <li>• <b>GRE Tunnel</b> - Select this if you connect to the network using Point-to-Point Protocol to create VPNs.</li> <li>• <b>EtherIP</b> - Select this if you need to tunnel Ethernet and IEEE 802.3 MAC frames across an IP Internet.</li> </ul>
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. <ul style="list-style-type: none"> <li>• <b>User</b> - Select this to manually enter the IP address the WiMAX Device uses.</li> <li>• <b>From ISP</b> - Select to automatically get the IP address the WiMAX Device uses from the ISP.</li> </ul>
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.

**Table 20** WAN (continued)

LABEL	DESCRIPTION
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.
First~Third DNS Server	Select how the WiMAX Device acquires its DNS server address. <ul style="list-style-type: none"> <li>• <b>From ISP</b> - Select this to have the WiMAX Device acquire its DNS server address from the ISP.</li> <li>• <b>User Define</b> - Select this to manually enter the DNS server used by the WiMAX Device.</li> </ul>

## 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 27** PPPoE Screen

**PPPoE**

User Name

Password

Retype Password

Auth Protocol  PAP  CHAP  MSCHAPv1  MSCHAPv2

Encryption

Idle Timeout  (seconds; enter 0 to never timeout)

AC Name

DNS overwrite

MPPE\_Stateful

Connection Trigger

Connection Timeout  (seconds; enter 0 to never timeout)



This screen contains the following fields:

**Table 21** 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: <ul style="list-style-type: none"> <li>• <b>CHAP</b> - The Challenge Handshake Authentication Protocol (CHAP) uses PPP to authenticate remote devices using a three-way handshake and shared secret verification.</li> <li>• <b>PAP</b> - 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.</li> <li>• <b>MS-CHAP v1/2</b> -This is Microsoft's variant of Challenge Handshake Authentication Protocol (CHAP). It allows for mutual authentication between devices.</li> </ul>
Encryption	Use this option to enable or disable authentication.
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.
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.
Connection Trigger	Set whether the WiMAX Device is persistently connected to the WAN ( <b>AlwaysOn</b> ) or you must click the PPPoE Connect button each time you want to get on the WAN ( <b>Manual</b> ).
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 28** GRE Screen

**GRE Peer**

Peer IP Address

This screen contains the following fields:

**Table 22** 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 29** EtherIP Screen

**EtherIP Tunnel Bridge**

Peer IP Address

This screen contains the following fields:

**Table 23** 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 30** IP Screen

IP Address	<input type="text" value="192.168.1.1"/>
IP Subnet Mask	<input type="text" value="255.255.255.0"/>

This screen contains the following fields:

**Table 24** IP

LABEL	DESCRIPTION
IP address	Enter the IP address of the LAN interface for the WiMAX Device.
IP Subnet Mask	Enter the IP subnet masks 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 31** DHCP Screen

This screen contains the following fields:

**Table 25** DHCP

LABEL	DESCRIPTION
DHCP Server	
DHCP Mode	<p>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.</p> <ul style="list-style-type: none"> <li>• <b>None</b> - This disables DHCP mode for the WiMAX Device.</li> <li>• <b>Server</b> - This sets the WiMAX Device as a DHCP server for the LAN.</li> <li>• <b>Relay</b> - 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.</li> </ul>

**Table 25** DHCP (continued)

LABEL	DESCRIPTION
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.
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. <ul style="list-style-type: none"> <li>• <b>None</b> - Select this to not use a DNS server.</li> <li>• <b>From ISP</b> - Select this to have the WiMAX Device acquire its DNS server address from the ISP.</li> <li>• <b>User Define</b> - Select this to manually enter the DNS server used by the WiMAX Device.</li> </ul>
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 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 32** Static Route Screen

This screen contains the following fields:

**Table 26** 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.

## 7.9 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 33** RIP Screen

The screenshot shows the RIP configuration interface. It is divided into several sections:

- General Setup:** Contains an 'Enable' checkbox which is currently unchecked.
- Redistribute:** Contains a table with columns 'Active', 'Type', and 'Metric(0-16)'. The table shows one entry with 'Active' set to 'Y', 'Type' set to 'static route', and 'Metric' set to '7'. Below the table, it says 'Total Num: 1' and has 'Edit' and 'OK' buttons.
- LAN:** Contains configuration options for the LAN interface:
  - Direction: R/TX (dropdown)
  - Version: RIP-2M (dropdown)
  - Authentication: None (dropdown)
  - Authentication ID: (text input)
  - Authentication Key: (text input)
- WAN:** Contains configuration options for the WAN interface:
  - Direction: R/TX (dropdown)
  - Version: RIP-2M (dropdown)
  - Authentication: None (dropdown)
  - Authentication ID: (text input)
  - Authentication Key: (text input)

This screen contains the following fields:

**Table 27** 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.
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.

## 7.10 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 34** Port Forwarding Screen

#	Active	Name	Protocol	Incoming Port(s)		Forward Port(s)		Server IP
				Start Port	End Port	Start Port	End Port	
1	N	Name1	TCP	0	0	0	0	1.1.1.1
2	N	Name2	TCP	0	0	0	0	1.1.1.1
3	N	Name3	TCP	0	0	0	0	1.1.1.1
4	N	Name4	TCP	0	0	0	0	1.1.1.1
5	N	Name5	TCP	0	0	0	0	1.1.1.1

Total Num: 5

Buttons: Wizard, Add, OK

This screen contains the following fields:

**Table 28** 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 <b>Start Port</b> , 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.



## 7.10.1 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 35** Port Forwarding Wizard Screen

**Edit Port Forwarding Rule**

Active

Port Forward Rule

Rule Name

Protocol

Incoming Start Port

Incoming End Port

Forwarding Start Port

Forwarding End Port

Server IP

This screen contains the following fields:

**Table 29** 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.

## 7.11 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 36** Port Trigger Screen



This screen contains the following fields:

**Table 30** 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	<p>This displays the start / end trigger port for the port trigger rule.</p> <p>Click <b>Add</b> 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.</p> <p>To forward one port number, enter the port number in the <b>Start Port</b> and <b>End Port</b> fields.</p> <p>To forward a range of ports,</p> <ul style="list-style-type: none"> <li>enter the port number at the beginning of the range in the <b>Start Port</b> field</li> <li>enter the port number at the end of the range in the <b>End Port</b> field.</li> </ul> <p>If you want to delete this rule, click the <b>Delete</b> icon.</p>
Open Protocol	This indicates which protocol is used to open the port trigger ports.
Open Port(s)	

**Table 30** Port Trigger (continued)

LABEL	DESCRIPTION
Start / End Port	<p>This displays the start / end open port for the port trigger rule.</p> <p>Click <b>Add</b> 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).</p> <p>To select one port number, enter the port number in the <b>Start Port</b> and <b>End Port</b> fields.</p> <p>To select a range of ports,</p> <ul style="list-style-type: none"> <li>enter the port number at the beginning of the range in the <b>Start Port</b> field</li> <li>enter the port number at the end of the range in the <b>End Port</b> field.</li> </ul> <p>If you want to delete this rule, click the <b>Delete</b> icon.</p>
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.

### 7.11.1 Port Trigger Wizard

Use the wizard to create a port trigger rules that will allow the WiMAX Device to 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 37** Port Trigger Wizard Screen

**Edit Port Trigger Rule**

Active

Port Trigger Rule

Rule Name

Trigger Protocol

Trigger Start Port

Trigger End Port

Open Protocol

Open Start Port

Open End Port

This screen contains the following fields:

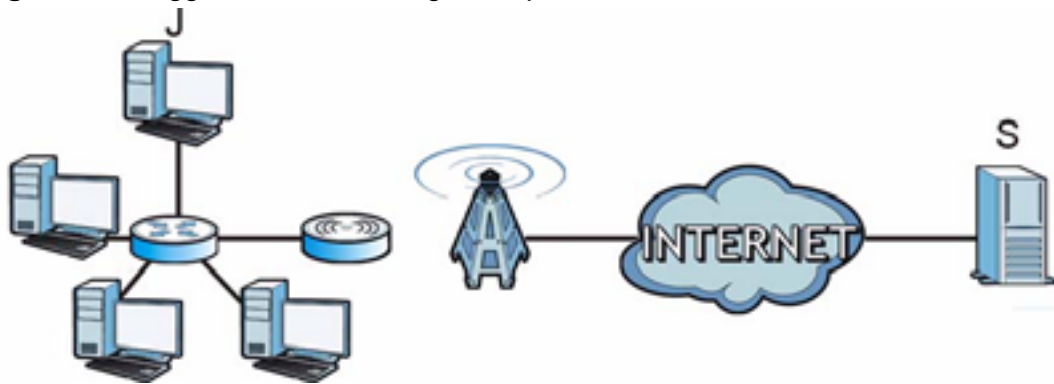
**Table 31** Port Trigger Wizard

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.

## 7.11.2 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 38** Trigger Port Forwarding Example



- 1 Jane requests a file from the Real Audio server (port 7070).
- 2 Port 7070 is a "trigger" port and causes the WiMAX 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.

## 7.12 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 39** DMZ Screen

The screenshot shows a configuration screen for DMZ. It features a label 'DMZ Host' on the left and a text input field on the right containing the IP address '0.0.0.0'. The entire configuration area is enclosed in a rectangular border.

This screen contains the following fields:

**Table 32** DMZ

LABEL	DESCRIPTION
DMZ Host	Enter the IP address of your network DMZ host, if you have one. <b>0.0.0.0</b> means this feature is disabled.

## 7.13 ALG

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

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

**Figure 40** ALG Screen

Enable FTP ALG	<input checked="" type="checkbox"/>
Enable H.323 ALG	<input checked="" type="checkbox"/>
Enable IPsec ALG	<input checked="" type="checkbox"/> <i>(Allow IPsec pass through)</i>
Enable L2TP ALG	<input checked="" type="checkbox"/> <i>(Allow L2TP pass through)</i>
Enable PPTP ALG	<input checked="" type="checkbox"/> <i>(Allow PPTP pass through)</i>
Enable RTSP ALG	<input checked="" type="checkbox"/> <i>(Allow RTSP pass through)</i>
Enable SIP ALG	<input checked="" type="checkbox"/>
SIP Port	<input type="text" value="5060"/>

This screen contains the following fields:

**Table 33** 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.
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.

## 7.14 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 41** UPnP Screen

Enable UPnP	<input type="checkbox"/>
Enable NAT-PMP	<input type="checkbox"/>

This screen contains the following fields:

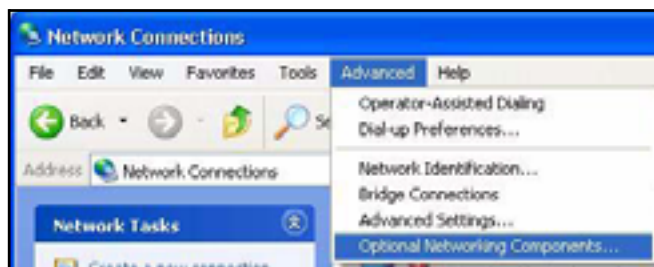
**Table 34** UPnP

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.

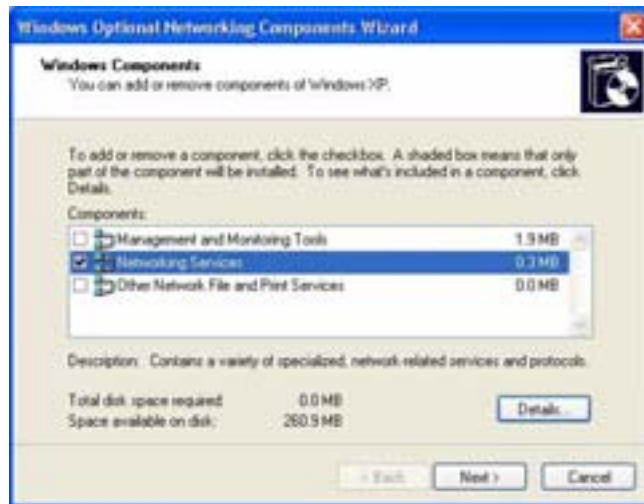
### 7.14.1 Installing UPnP in Windows XP

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

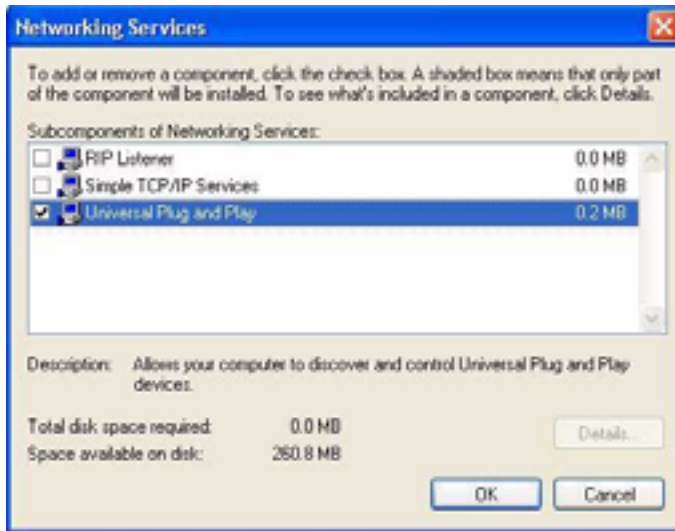
- 1 Click **Start > Control Panel**.
- 2 Double-click **Network Connections**.
- 3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ...**



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



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



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



### 7.14.1.1 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.

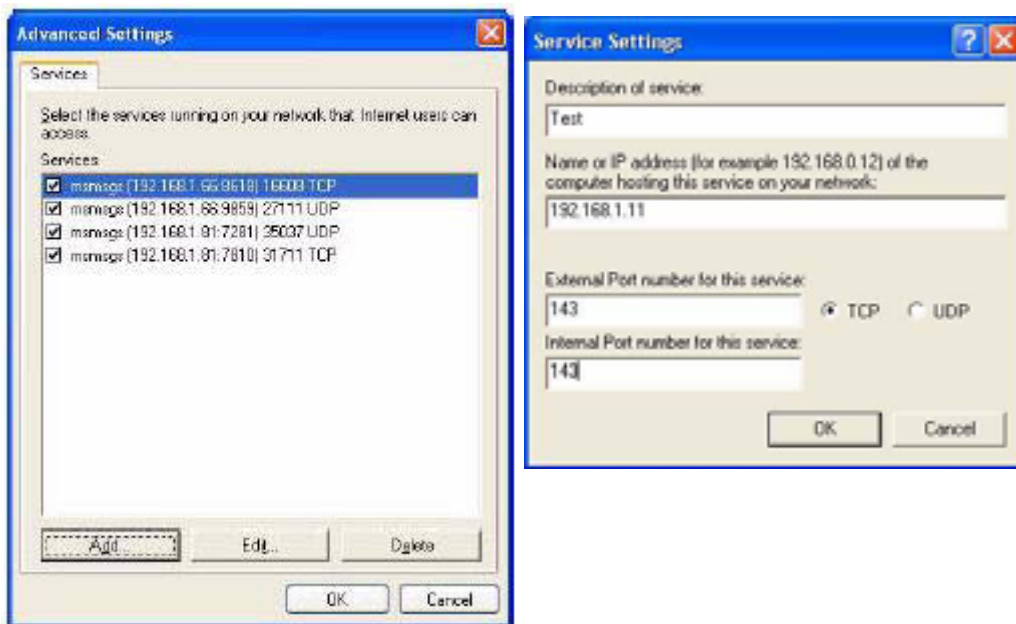
- 1 Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.
- 2 Right-click the icon and select **Properties**.



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

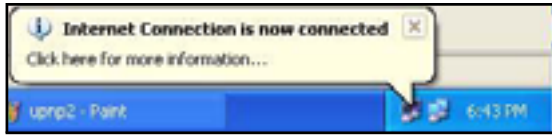


- 4 You may edit or delete the port mappings or click **Add** to manually add port mappings.



- 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.



## 7.14.2 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.



## 7.15 DDNS

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

Click Network Setting > DDNS

**Figure 42** DDNS Screen

Enable Dynamic DNS	<input type="checkbox"/>
Service Provider	dyndns.org(www.dyndns.org) ▼
Service Type	Dynamic ▼
Domain Name	<input type="text"/> . <input type="text"/>
Login Name	<input type="text"/>
Password	<input type="text"/>
IP Update Policy	Auto Detect ▼
User Defined IP	<input type="text"/>
Wildcards	<input type="checkbox"/>
MX	<input type="checkbox"/>
Backup MX	<input type="checkbox"/>
MX Host	<input type="text"/>

This screen contains the following fields:

**Table 35** DDNS

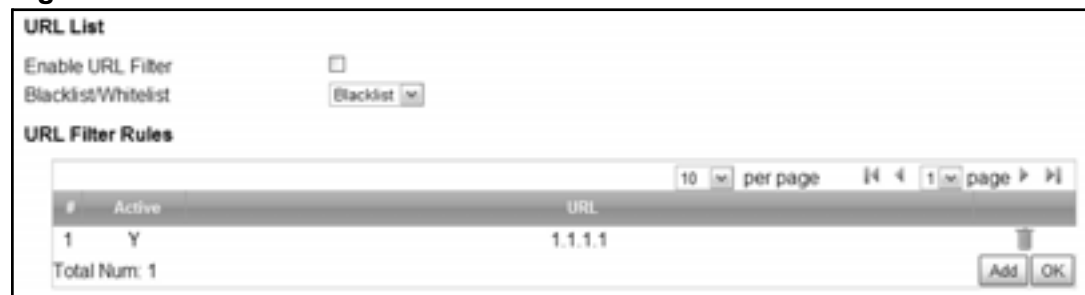
LABEL	DESCRIPTION
Enable Dynamic DNS	Select this to enable dynamic DNS on the WiMAX Device.
Service Provider	Select the dynamic DNS service provider for the WiMAX Device.
Service Type	Select the dynamic DNS service type.
Domain Name	Enter the domain name.
Login Name	Enter the user name.
Password	Enter the password.
IP Update Policy	Select the policy used by the WiMAX Device. Options are: <ul style="list-style-type: none"> <li>• Auto Detect</li> <li>• WAN</li> <li>• User Defined</li> </ul>
User Defined IP	If chose "User Defined" for the <b>IP Update Policy</b> , 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 DYDNS service provider.
Backup MX	Select this to enable a secondary mail routing, if supported by the specified DYDNS service provider.
MX Host	Enter the host to which mail is routed when the MX option is selected.

## 7.16 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 43** Content Filter Screen



This screen contains the following fields:

**Table 36** 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.





# 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 44** IP Filter Screen



This screen contains the following fields:

**Table 37** 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 <b>Add</b> 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 <b>Delete</b> icon.
Source Port	This displays the source port number for the IP filter rule. Click <b>Add</b> 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 <b>Delete</b> icon.
Destination IP	This displays the destination IP address for the IP filter rule. Click <b>Add</b> 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 <b>Delete</b> icon.
Destination Port	This displays the destination port number for the IP filter rule. Click <b>Add</b> 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 <b>Delete</b> icon.
Protocol	This displays the protocol blocked by the IP filter rule. Click <b>Add</b> 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 <b>Delete</b> 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 45** MAC Filter Screen



This screen contains the following fields:

**Table 38** 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 <b>Add</b> 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 <b>Delete</b> icon.
Destination MAC	This displays the destination MAC for the MAC filter rule. Click <b>Add</b> 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 <b>Delete</b> 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 46** DDOS Screen

Prevent from TCP SYN Flood	<input type="checkbox"/>
Prevent from UDP Flood	<input type="checkbox"/>
Prevent from ICMP Flood	<input type="checkbox"/>
Prevent from Port Scan	<input type="checkbox"/>
Prevent from LAND Attack	<input type="checkbox"/>
Prevent from IP Spoof	<input type="checkbox"/>
Prevent from ICMP redirect	<input type="checkbox"/>
Prevent from PING of Death	<input type="checkbox"/>
Prevent from PING from WAN	<input type="checkbox"/>

This screen contains the following fields:

**Table 39** 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.

**Table 39** DDOS (continued)

LABEL	DESCRIPTION
Prevent from IP Spoof	<p>Select this to monitor for and block IP address spoof attacks.</p> <p>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.</p>
Prevent from ICMP redirect	<p>Select this to monitor for and block ICMP redirect attacks.</p> <p>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.</p>
Prevent from PING of Death	<p>Select this to monitor for and block ping of death attacks.</p> <p>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.</p>
Prevent from PING from WAN	<p>Select this to ignore ping requests from the WAN.</p>



# Maintenance

## 9.1 Overview

Use these screens to manage and maintain your WiMAX Device.

### 9.1.1 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.

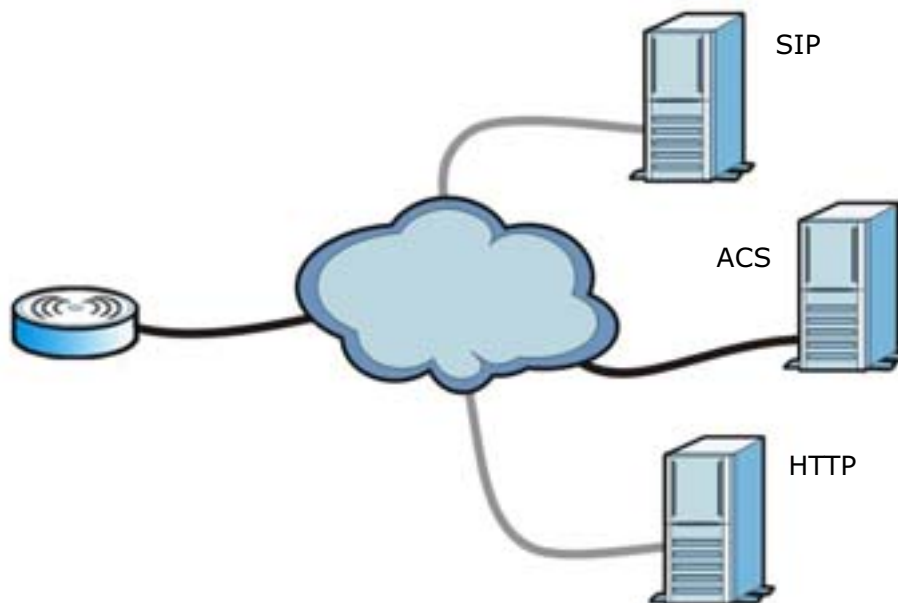


## TR-069

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 47** TR-069 Example



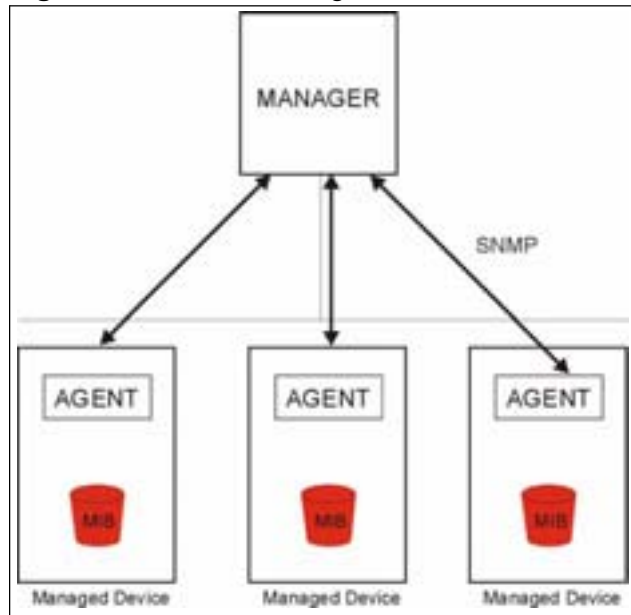
In this example, the WiMAX Device receives data from at least 3 sources: A SIP server for handling voice calls, an HTTP server for handling web services, and an ACS, for configuring the WiMAX Device remotely. All three servers are owned and operated by the client's Internet Service Provider. However, 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 48** 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 40** SNMP Traps

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

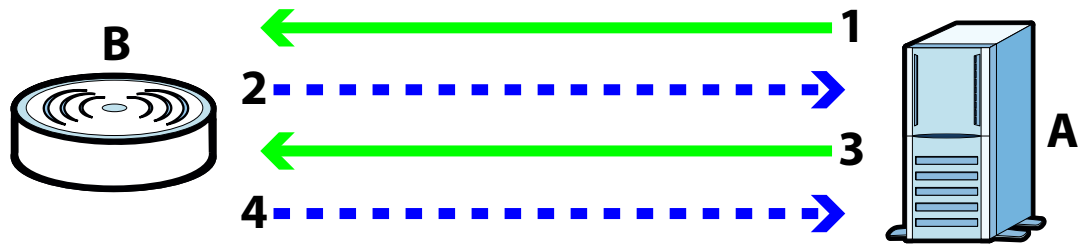
When the WiMAX Device initiates communication with the server (often times at start up or after the first time you turn it on), the server uploads commands, new files (if any), and other information used by a service provider to customize the WiMAX Device's features.

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 49** 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.

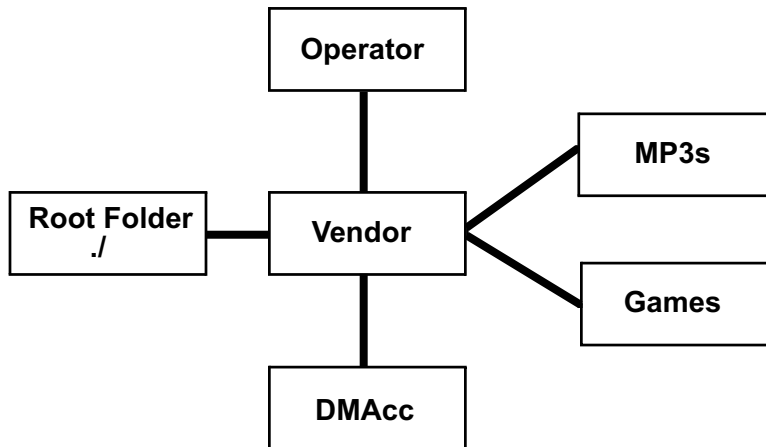
**Digest Access Authentication** – This protocol was designed to replace basic access authentication. Instead of encoding a user name and password in plaintext, this protocol uses what is known as an MD5 message authentication code. It allows the server to issue a single-use, randomly generated number (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 50** 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.

## 9.2 Password

Use this screen to set up user and admin accounts for logging into and managing the WiMAX Device.

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

**Figure 51** Password Screen

**Change Password**

Group  ▼

Old Password

New Password

Retype

**Change Username**

Group  ▼

Old Username

New Username

Password

This screen contains the following fields:

**Table 41** Password

LABEL	DESCRIPTION
Change Password	
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.
Change User name	
Group	Select a group for which want to change a username.
Old Username	Enter the username to be changed.

**Table 41** Password (continued)

LABEL	DESCRIPTION
New Username	Enter the new username.
Password	Enter the password for this username.

## 9.3 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 52** HTTP Screen

The screenshot shows the following configuration options:

- HTTP Server**
  - Enable:
  - Port Number:
- HTTPS Server**
  - Enable:
  - Port Number:
- HTTP and HTTPS**
  - Allow Connection from WAN:
- HTTP Session Timeout**
  - Session Timeout:  minutes (0-99, default 5, 0 means disabled)

This screen contains the following fields:

**Table 42** 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	

**Table 42** HTTP (continued)

LABEL	DESCRIPTION
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).

## 9.4 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 53** Telnet Screen

Enable	<input checked="" type="checkbox"/>
Port Number	<input type="text" value="23"/>
Allow Connection from WAN	<input checked="" type="checkbox"/>
Allow Connection from LAN	<input checked="" type="checkbox"/>

This screen contains the following fields:

**Table 43** 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.



## 9.5 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 54** SSH Screen

Enable	<input checked="" type="checkbox"/>
Port Number	<input type="text" value="22"/>
Allow Connection from WAN	<input checked="" type="checkbox"/>
Allow Connection from LAN	<input checked="" type="checkbox"/>

This screen contains the following fields:

**Table 44** 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.

## 9.6 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 55** SNMP Screen

Enable	<input type="checkbox"/>
Location	<input type="text"/>
Contact	<input type="text"/>
Read Community	<input type="text" value="public"/>
Write Community	<input type="text" value="private"/>
Trap Server	<input type="text" value="192.168.0.1"/>
Trap Community	<input type="text" value="test"/>

This screen contains the following fields:

**Table 45** 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.

## 9.7 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 56** CWMP Screen

This screen contains the following fields:

**Table 46** 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.

**Table 46** CWMP (continued)

LABEL	DESCRIPTION
Periodical Inform Enable	<p>Select this to allow the WiMAX Device to periodically connect to the ACS and check for configuration updates.</p> <p>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.</p>
Periodical Inform Interval	<p>Enter the time interval (in seconds) at which the WiMAX Device connects to the auto-configuration server.</p>
Connection Request Username	<p>Enter the connection request user name that the ACS must send to the WiMAX Device when it requests a connection.</p> <p>You can enter up to 31 alphanumeric characters (a-z, A-Z, 0-9) and underscores but spaces are not allowed.</p> <p><b>Note:</b> This must be provided by the ACS administrator.</p>
Connection Request Password	<p>Enter the connection request password that the ACS must send to the WiMAX Device when it requests a connection.</p> <p>You can enter up to 31 alphanumeric characters (a-z, A-Z, 0-9) and underscores but spaces are not allowed.</p> <p><b>Note:</b> This must be provided by the ACS administrator.</p>
CA Certificate File	<p>Click <b>Browse</b> to upload a Certificate Authority (CA) certificate to the WiMAX Device.</p>
CA Certificate Info	<p>This displays information about the currently active CA certificate.</p>
Client Certificate File	<p>Click <b>Browse</b> to upload a client certificate to the WiMAX Device.</p>
Client Certificate Info	<p>This displays information about the currently active client certificate.</p>

## 9.8 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 57** OMA-DM Screen

Enable	<input type="checkbox"/>
Server URL	<input type="text"/>
Server Port	<input type="text" value="80"/>
Server Auth Type	<input type="text" value="NONE"/>
Server ID	<input type="text"/>
Server Password	<input type="text"/>
Client Auth Type	<input type="text" value="NONE"/>
Client ID	<input type="text"/>
Client Password	<input type="text"/>
Periodical Client-initiated Enable	<input checked="" type="checkbox"/>
Periodical Client-initiated Interval	<input type="text" value="3600"/>

This screen contains the following fields:

**Table 47** 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.
Server Port	Enter the port number for the IP address of the OMA-DM server set up in the preceding field.
Server Auth Type	<p>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.</p> <ul style="list-style-type: none"> <li>• <b>None</b> - No authentication.</li> <li>• <b>Basic</b> - Server ID and Password are encoded using a Basic Access Authentication Code.</li> <li>• <b>Digest (MD5)</b> - Server ID and Password are encoded using a Digest Access Authentication Code.</li> <li>• <b>HMAC</b> - Server ID and Password are encoded using a keyed Hash Message Authentication Code.</li> </ul>
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.

**Table 47** OMA-DM (continued)

LABEL	DESCRIPTION
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.
Client Auth Type	<p>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.</p> <ul style="list-style-type: none"> <li>• <b>None</b> - No authentication.</li> <li>• <b>Basic</b> - Server ID and Password are encoded using a Basic Access Authentication Code.</li> <li>• <b>Digest (MD5)</b> - Server ID and Password are encoded using a Digest Access Authentication Code.</li> <li>• <b>HMAC</b> - Server ID and Password are encoded using a keyed Hash Message Authentication Code.</li> </ul> <p>Note: Make sure that the scheme selected here matches the the <b>Server Auth Type</b>.</p>
Client ID	Enter the client name for the WiMAX Device.
Client Password	Enter the password for the WiMAX Device's client name.
Periodical Client-Initiated Enable	<p>Select this to allow the WiMAX Device to periodically connect to the OMA-DM server and check for configuration updates.</p> <p>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.</p>
Periodical Client-Initiated Interval	Enter the time interval (in seconds) at which the WiMAX Device connects to the OMA-DM server.

## 9.9 Date

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 58** Date Screen

Current System Time	Tue Jan 13 13:21:04 1970		
<input type="radio"/> Manual			
New Time(hh:mm:ss)	<input type="text" value="15"/>	: <input type="text" value="42"/>	: <input type="text" value="02"/>
New Date(mm-dd-yyyy)	<input type="text" value="07"/>	- <input type="text" value="26"/>	- <input type="text" value="2010"/>
<input checked="" type="radio"/> Get from Time Server			
Time Protocol	<input type="text" value="NTP (RFC-1305) ▼"/>		
Time Server Address 1	<input type="text" value="1.my.pool.ntp.org"/>		
Time Server Address 2	<input type="text" value="2.my.pool.ntp.org"/>		
Time Server Address 3	<input type="text" value="3.my.pool.ntp.org"/>		
Time Server Address 4	<input type="text" value="4.my.pool.ntp.org"/>		

This screen contains the following fields:

**Table 48** 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. <ul style="list-style-type: none"> <li>• <b>NTP (RFC 1305)</b> - This format is similar to Time (RFC 868).</li> </ul>
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.

## 9.10 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 59** Time Zone Screen

Time Zone	(GMT+08:00) Kuala Lumpur, Singapore
Enable Daylight Saving	<input type="checkbox"/>
Start Date	First Sunday of April at 2 o'clock
End Date	Last Sunday of October at 2 o'clock

This screen contains the following fields:

**Table 49** 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.

## 9.11 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 60** Upgrade File Screen

This screen contains the following fields:

**Table 50** Upgrade File

LABEL	DESCRIPTION
Upgrade File	Click <b>Browse</b> 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!

### 9.11.1 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.

## 9.12 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 61** Upgrade Link Screen

The screenshot shows a web interface with a title 'Upgrade Link' on the left. To the right is a large, empty text input field. Below the input field is a rectangular button with the text 'Upgrade' centered on it.

This screen contains the following fields:

**Table 51** 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!

## 9.13 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 62** CWMP Upgrade Screen

The screenshot shows a web interface with a title 'Upgrade Firmware via CWMP Request Download' at the top. Below the title is a large, empty rectangular area. In the bottom right corner of this area is a rectangular button with the text 'Upgrade' centered on it.

This screen contains the following fields:

**Table 52** CWMP Upgrade

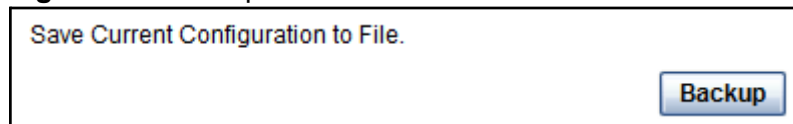
LABEL	DESCRIPTION
Upgrade	<p>Click this to begin upgrading firmware using CWMP Request. This may take up to two minutes.</p> <p>Note: Do not turn off the device while firmware upload is in progress!</p>

## 9.14 Backup

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 63** Backup/Restore Screen



This screen contains the following fields:

**Table 53** Backup/Restore

LABEL	DESCRIPTION
Backup	<p>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.</p>

## 9.15 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 64** Restore Screen

This screen contains the following fields:

**Table 54** Restore

LABEL	DESCRIPTION
Configuration File	Click <b>Choose File</b> then browse to the location of a firmware upgrade file and select it.  Click <b>File Restore</b> 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 <b>URL Restore</b> to upload the specified configuration to the WiMAX Device and replace the current settings.

### 9.15.1 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.

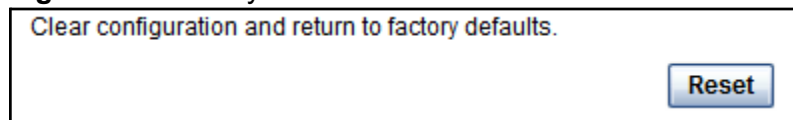
If the upload was not successful, you are notified with an error message.

## 9.16 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 65** Factory Defaults Screen



This screen contains the following fields:

**Table 55** 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.

## 9.17 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 66** Log Setting Screen

The screenshot shows a form with five rows of settings. Each row has a label on the left and a control on the right. The controls are: a checked checkbox, a dropdown menu, an unchecked checkbox, an empty text input field, and a text input field containing the number "514".

Enable Log	<input checked="" type="checkbox"/>
Log Level	Info <input type="button" value="v"/>
Enable Remote Log	<input type="checkbox"/>
Remote Log Host	<input type="text"/>
Remote Log Port	514 <input type="text"/>

This screen contains the following fields:

**Table 56** Log Setting

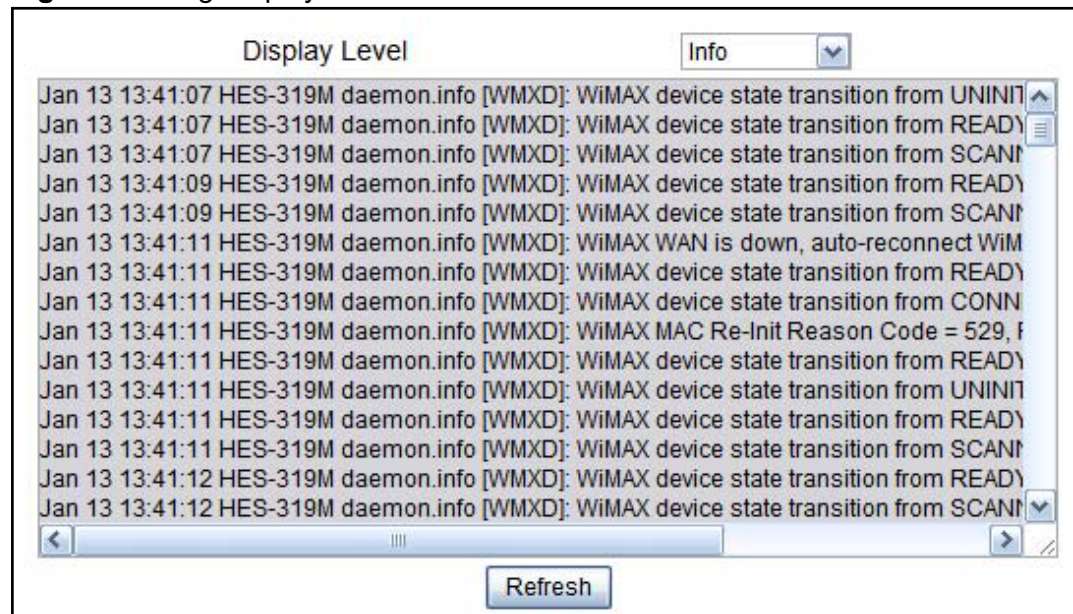
LABEL	DESCRIPTION
Enable Log	Select this to have the WiMAX Device log network activity according to the selected <b>Log Level</b> .
Log Level	Select the type of logs to record.
Enable Remote Log	Select this to allow logs to be recorded and stored on a remote logs server.
Remote Log Host	Enter the remote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

## 9.18 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 67** Log Display Screen



This screen contains the following fields:

**Table 57** Log Display

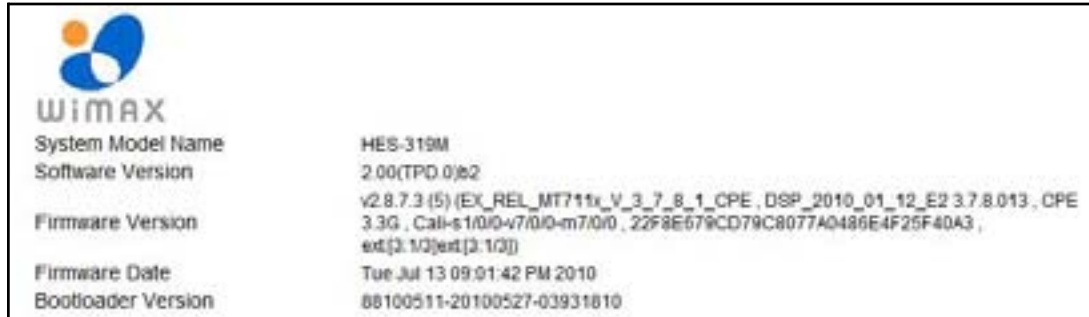
LABEL	DESCRIPTION
Display Level	Select the type of logs to display from this menu.
Refresh	Click this to refresh the logs in the display window.

## 9.19 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 68** About Screen



This screen contains the following fields:

**Table 58** About

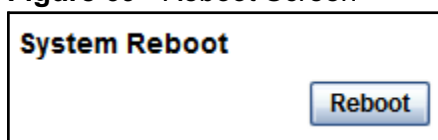
LABEL	DESCRIPTION
System Model Name	This field displays the WiMAX Device system name. It is used for identification.
Software Version	This field displays the Web Configurator software version that the WiMAX Device is currently running.
Firmware Version	This field displays the current version of the firmware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

## 9.20 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 69** Reboot Screen



This screen contains the following fields:

**Table 59** Reboot

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



# 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](#)

## 10.1 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 [Section 1.2.1 on page 18](#) 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.

## 10.2 WiMAX Device Access and Login

---

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

---

- 1 The default IP address is .
- 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 9.16 on page 133](#).

---

### 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 9.16 on page 133](#).

---

### 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 .
  - If you changed the IP address ([Section 7.6 on page 83](#)), 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 [Section 1.2.1 on page 18](#).
  - 3 Make sure your Internet browser does not block pop-up windows and has JavaScript and Java enabled. See [Appendix C on page 179](#).
  - 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. See [Appendix D on page 189](#).
  - 5 Reset the WiMAX Device to its factory defaults, and try to access the WiMAX Device with the default IP address. See [Chapter 2 on page 19](#).
  - 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 9.16 on page 133](#).

---

### 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.

## 10.3 Internet Access

---

### I cannot access the Internet.

---

- 1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and [Section 1.2.1 on page 18](#).
- 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 105](#).
- 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 51](#). If you are unsure of the correct values, contact your service provider.
- 5 If you are trying to access the Internet wirelessly, make sure the wireless settings in the wireless client are the same as the settings in the AP.
- 6 Disconnect all the cables from your WiMAX Device, and follow the directions in the Quick Start Guide again.
- 7 If the problem continues, contact your ISP.

---

### I cannot access the Internet any more. I had access to the Internet (with the WiMAX 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 [Section 1.2.1 on page 18](#).
- 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 [Section 1.2.1 on page 18](#). 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.

## 10.4 Reset the WiMAX Device to Its Factory Defaults

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

---

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

---

To reset the WiMAX 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.

### 10.4.1 Pop-up Windows, JavaScript and Java Permissions

Please see [Appendix C on page 179](#).

# Product Specifications

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

FEATURE	DESCRIPTION
Operation Requirements	<ul style="list-style-type: none"> <li>Storage conditions: -40°C to 60°C, 10% to 95% humidity</li> <li>Operation conditions: -40°C to 65°C, 10% to 90% humidity (non condensing)</li> <li>Operating Humidity: 10% to 95% RH</li> </ul>
Power Supply Requirement	<ul style="list-style-type: none"> <li>DC 48 V, 0.32 A on PoE</li> <li>100 V ~ 240 V ± 10% AC input</li> </ul>
LAN Port	<ul style="list-style-type: none"> <li>RJ-45 Interface</li> <li>1 Port</li> <li>10/100BaseT</li> <li>AUTO MDI/MDIX</li> </ul>
Reset Button / Restore to Factory Default Button	<ul style="list-style-type: none"> <li>System Reset</li> <li>System configuration can be restored to factory default if hold the Reset Button longer than 5 seconds</li> </ul>
LAN Status LED (Green / Yellow)	<p>Green LED for 10M</p> <ul style="list-style-type: none"> <li>ON: Linked</li> <li>Blinking: Data transmitting</li> <li>OFF: Link off</li> </ul> <p>Yellow LED for 100M</p> <ul style="list-style-type: none"> <li>ON: Linked</li> <li>Blinking: Data transmitting</li> <li>OFF: Link off</li> </ul>
RSSI LED (Green)	<p>5 LED bar : LED 1~5 indicates RSSI (Power level reception, only on when connected)</p> <ul style="list-style-type: none"> <li>5 LED : -50dBm &lt; RSSI</li> <li>4 LED : -50dBm &lt;= RSSI &gt; -60dBm</li> <li>3 LED : -60dBm &lt;= RSSI &gt; -70dBm</li> <li>2 LED : -70dBm &lt;= RSSI &gt; -80dBm</li> <li>1 LED : -80dBm &lt;= RSSI &gt; -90dBm</li> <li>0 LED : -90dBm &gt;= RSSI</li> </ul>

FEATURE	DESCRIPTION
Buzzer behavior	<ul style="list-style-type: none"> <li>• 5 Counts (5 sec) : -50dBm &lt; RSSI</li> <li>• 4 Counts (4 sec) : -50dBm ≤ RSSI &lt; -60dBm</li> <li>• 3 Counts (3 sec) : -60dBm ≤ RSSI &lt; -70dBm</li> <li>• 2 Counts (2 sec) : -70dBm ≤ RSSI &lt; -80dBm</li> <li>• 1 Counts (1 sec) : -80dBm ≤ RSSI &lt; -90dBm</li> <li>• 0 Counts no buzzer : -90dBm ≥ RSSI</li> </ul>
Antenna	<ul style="list-style-type: none"> <li>• Center Frequency: 3500 MHz (HES-319M), 2300 MHz (HES-339M), 2600 MHz (HES-309M)</li> <li>• Frequency Range: 3300 MHz~3600 MHz (HES-319M), 2300 MHz~2400 MHz (HES-339M), 2500 MHz~2700 MHz (HES-309M)</li> <li>• Bandwidth: 300 MHz</li> <li>• Peak Gain: 15 dBi (HES-319M), 12 dBi (HES-339M), 13 dBi (HES-309M)</li> <li>• H-Plane Average Gain: 3.5 dBi</li> <li>• VSWR: 2</li> <li>• Polarization: Linear, Vertical</li> <li>• H-Plane HPBW: 180°</li> <li>• V-Plane HPBW: 25°</li> <li>• Down tilt: 0°</li> <li>• Impedance: 50</li> <li>• Connector: IPEX female</li> </ul>
WiMAX compliance	Fully compliant with IEEE 802.16e Mobile WiMAX corrigendum 1 & 2 and WiMAX Forum Wave 2 System Profiles
Operating Frequency Band	3.3GHz~3.6GHz (HES-319M), 2.3GHz~2.4GHz (HES-339M), 2.5GHz~2.7GHz (HES-309M)
Certification Profile	Support WF profiles: 1A, 2A, 3A, 5A, 5AL, 5BL (5MHz, 7MHz, 10MHz bandwidth)
Maximum nominal Transmission Power	Maximum nominal Tx power at the antenna connector: 26dBm.
Transmitter Power Control	Transmit power control by step of 1dB, relative accuracy of +/- 0.5dB (as per IEEE 802.16e-2005, §8.4.12.1).
Transmitter spectral flatness	Transmitter spectral flatness as defined in IEEE 802.16e-2005, §8.4.12.2.
Transmitter Error Vector Magnitude (EVM)	Transmitter relative constellation error (EVM) as defined in IEEE 802.16e-2005, §8.4.12.3.
Receiver SNR	Compliant to IEEE 802.16e-2005 section §8.4.13.1
Receiver Sensitivity	The receiver minimum sensitivity level $R_{ss}$ , measured under the conditions defined in IEEE 802.16e-2005.



FEATURE	DESCRIPTION
Cumulated Noise Figure and Implementation Loss of the Receiver	Lower than 6.4dB
Receiver SNR	Compliant to IEEE 802.16e-2005 section §8.4.13.1
Receiver Sensitivity	The receiver minimum sensitivity level $R_{ss}$ , measured under the conditions defined in IEEE 802.16e-2005.
Receiver Diversity	Maximum Ratio Combining (MRC)
Receiver Adjacent Channel Rejection	The receiver adjacent channel rejection measured under the conditions defined in IEEE 802.16e-2005 is at least: 25dB for QPSK $\frac{1}{2}$ , 14dB for 16QAM $\frac{3}{4}$ , 7dB for 64QAM $\frac{3}{4}$ .
Receiver Non-Adjacent Channel Rejection	The receiver non-adjacent channel rejection measured under the conditions defined in IEEE 802.16e-2005 is at least: 38dB for QPSK $\frac{1}{2}$ , 33dB for 16QAM $\frac{3}{4}$ , 26dB for 64QAM $\frac{3}{4}$ .



# 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.

# Setting Up Your Computer's IP Address

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

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

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

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

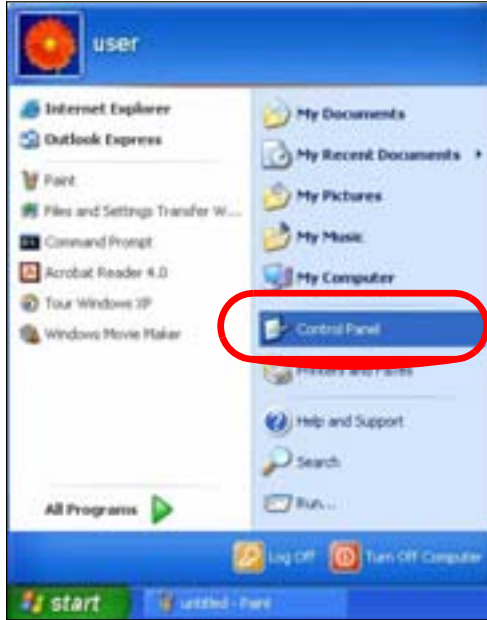
- [Windows XP/NT/2000](#) on [page 152](#)
- [Windows Vista](#) on [page 155](#)
- [Mac OS X: 10.3 and 10.4](#) on [page 159](#)
- [Mac OS X: 10.5](#) on [page 163](#)
- [Linux: Ubuntu 8 \(GNOME\)](#) on [page 166](#)
- [Linux: openSUSE 10.3 \(KDE\)](#) on [page 172](#)

## Windows XP/NT/2000

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

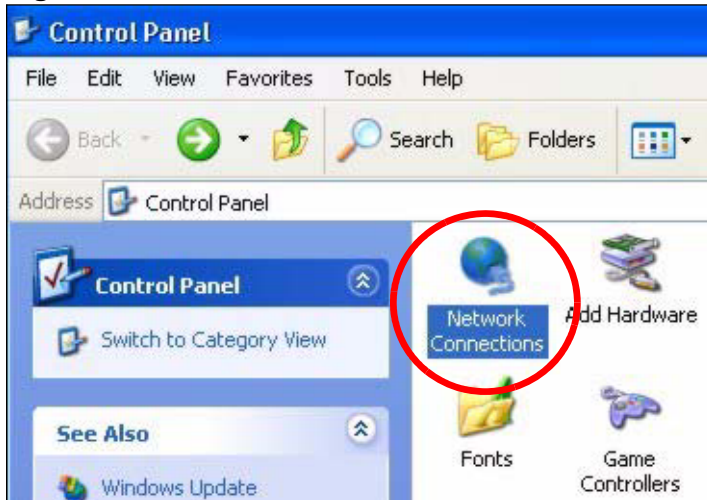
- 1 Click **Start > Control Panel**.

**Figure 70** Windows XP: Start Menu



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

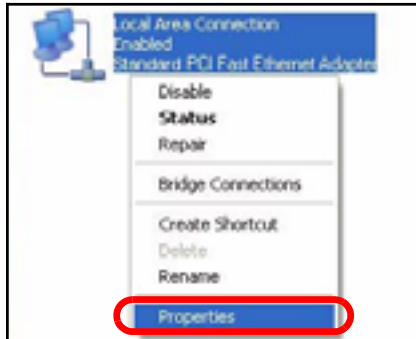
**Figure 71** Windows XP: Control Panel





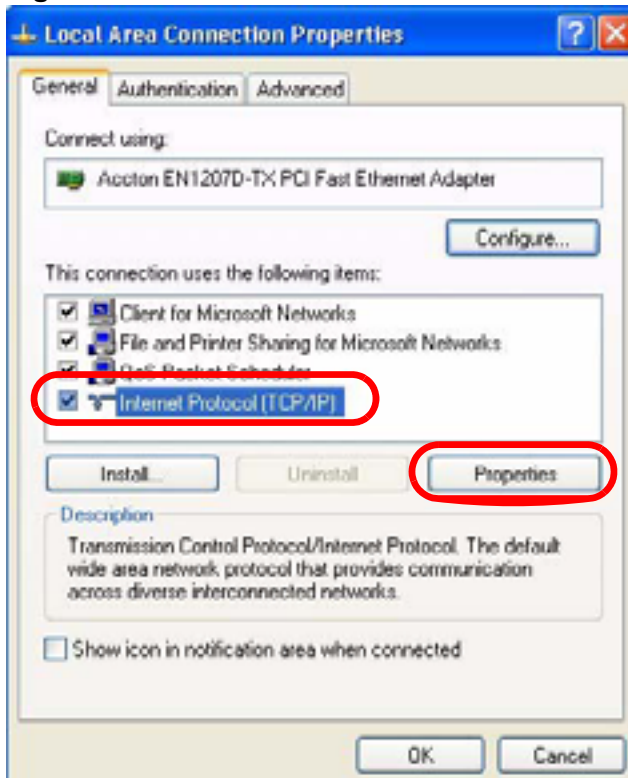
- 3 Right-click **Local Area Connection** and then select **Properties**.

**Figure 72** Windows XP: Control Panel > Network Connections > Properties



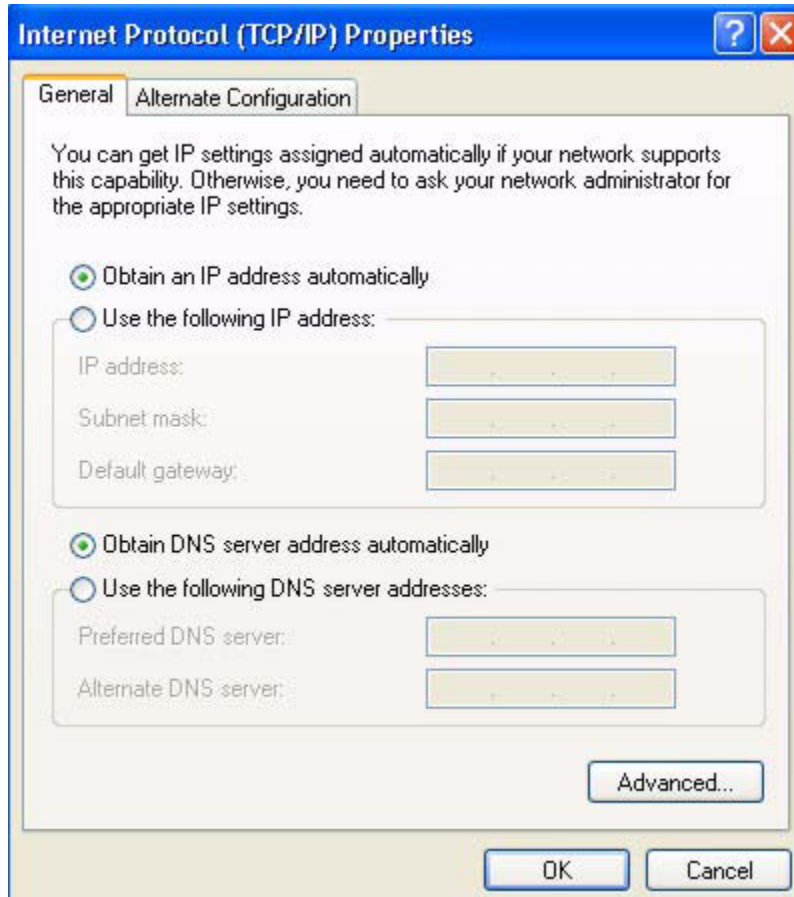
- 4 On the **General** tab, select **Internet Protocol (TCP/IP)** and then click **Properties**.

**Figure 73** Windows XP: Local Area Connection Properties



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

**Figure 74** Windows XP: Internet Protocol (TCP/IP) Properties



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

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

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

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

- 1 Click **Start > All Programs > Accessories > Command Prompt**.
- 2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

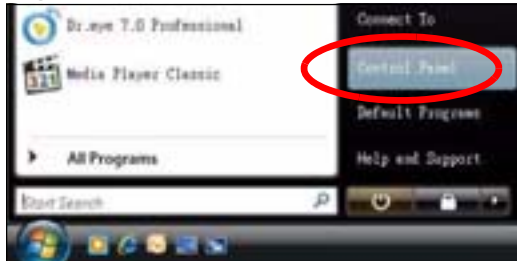
You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

## Windows Vista

This section shows screens from Windows Vista Professional.

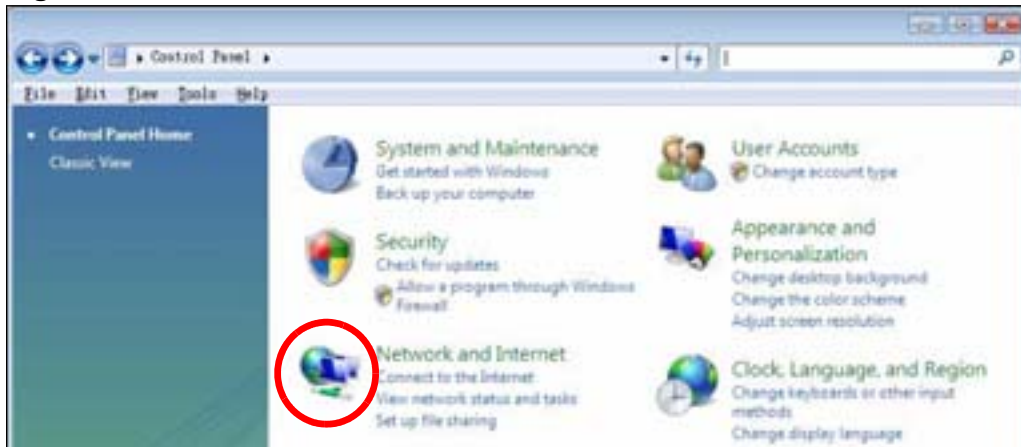
- 1 Click **Start > Control Panel**.

**Figure 75** Windows Vista: Start Menu



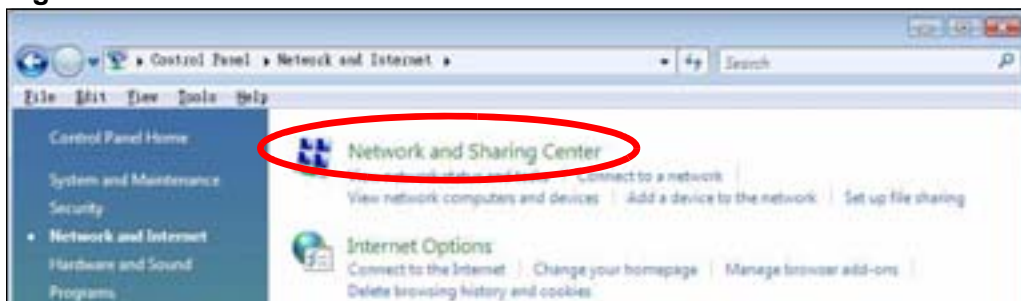
- 2 In the **Control Panel**, click the **Network and Internet** icon.

**Figure 76** Windows Vista: Control Panel



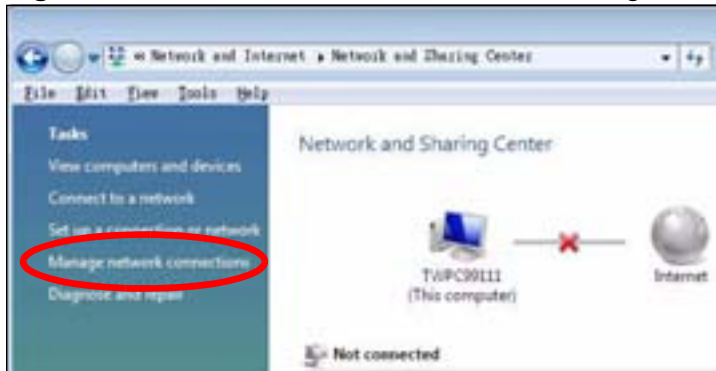
- 3 Click the **Network and Sharing Center** icon.

**Figure 77** Windows Vista: Network And Internet



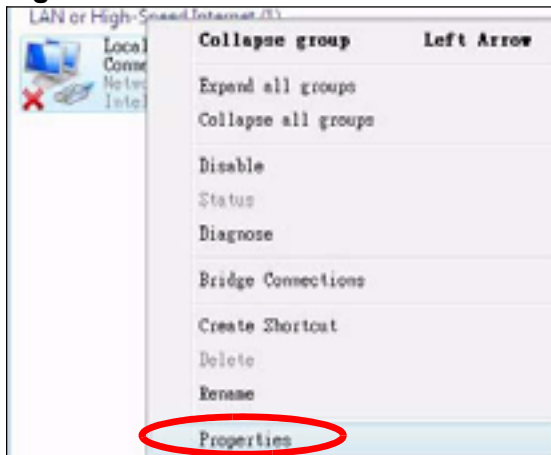
- 4 Click **Manage network connections**.

**Figure 78** Windows Vista: Network and Sharing Center



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

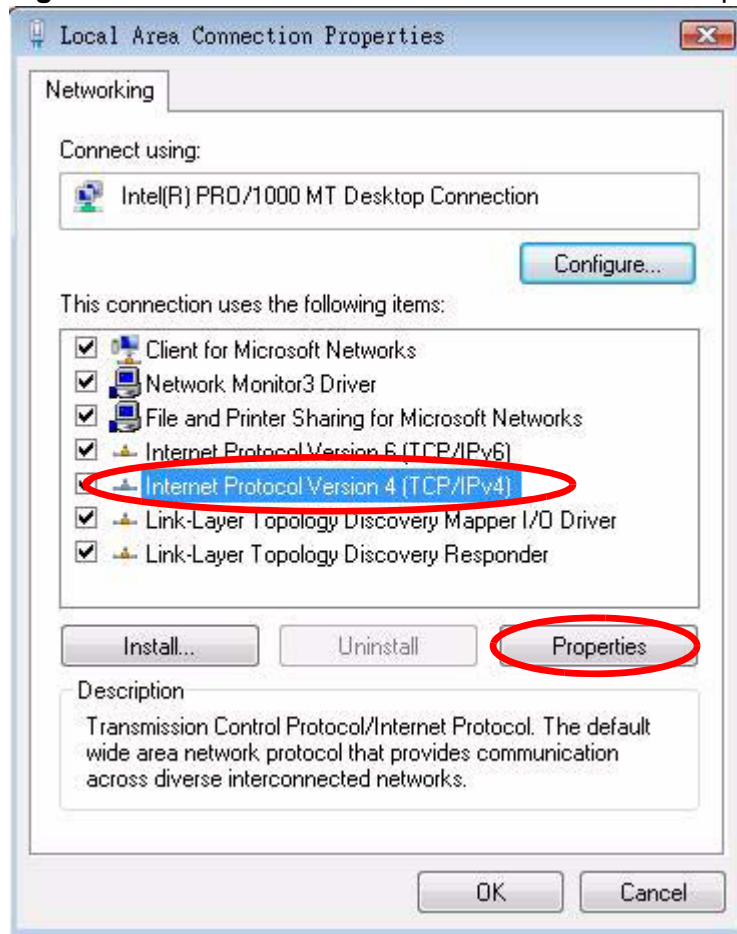
**Figure 79** Windows Vista: Network and Sharing Center



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

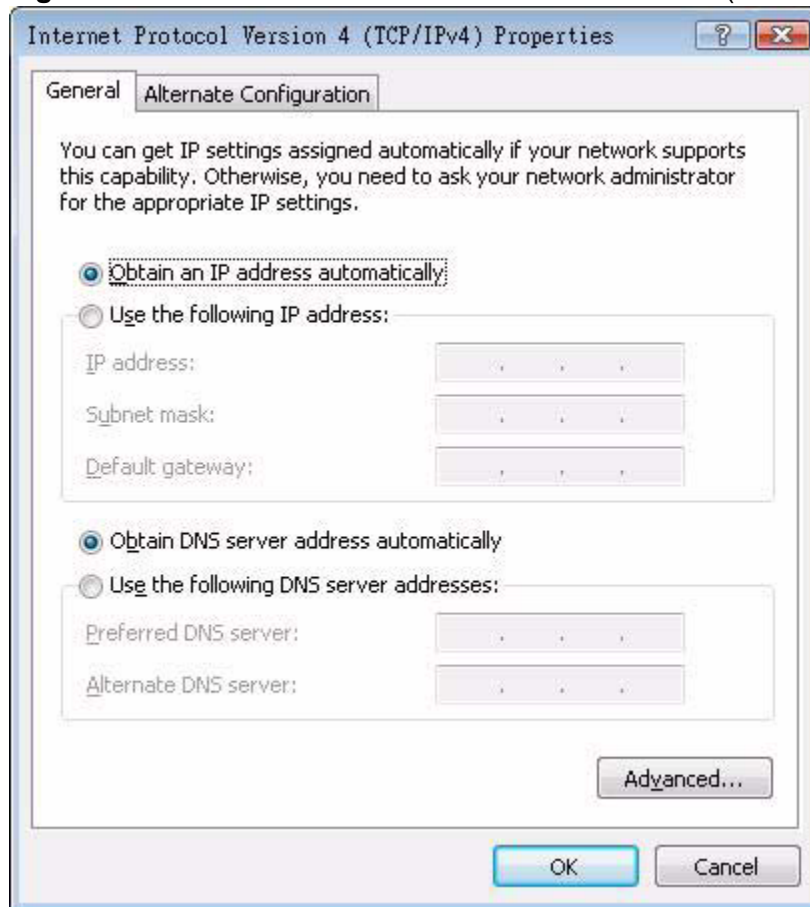
- 6 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.

**Figure 80** Windows Vista: Local Area Connection Properties



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

**Figure 81** Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties



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

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

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

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

- 1 Click **Start > All Programs > Accessories > Command Prompt**.
- 2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

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

## Mac OS X: 10.3 and 10.4

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

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

**Figure 82** Mac OS X 10.4: Apple Menu



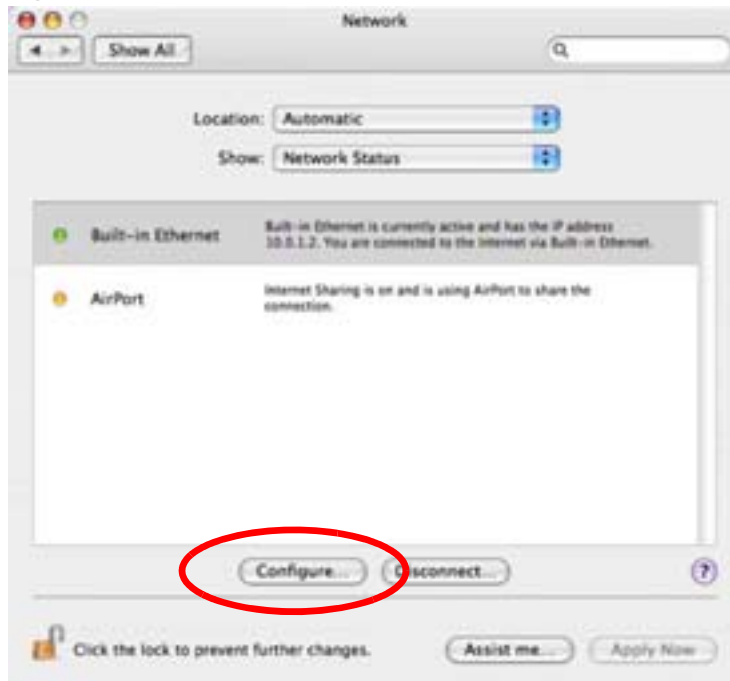
- 2 In the **System Preferences** window, click the **Network** icon.

**Figure 83** Mac OS X 10.4: System Preferences



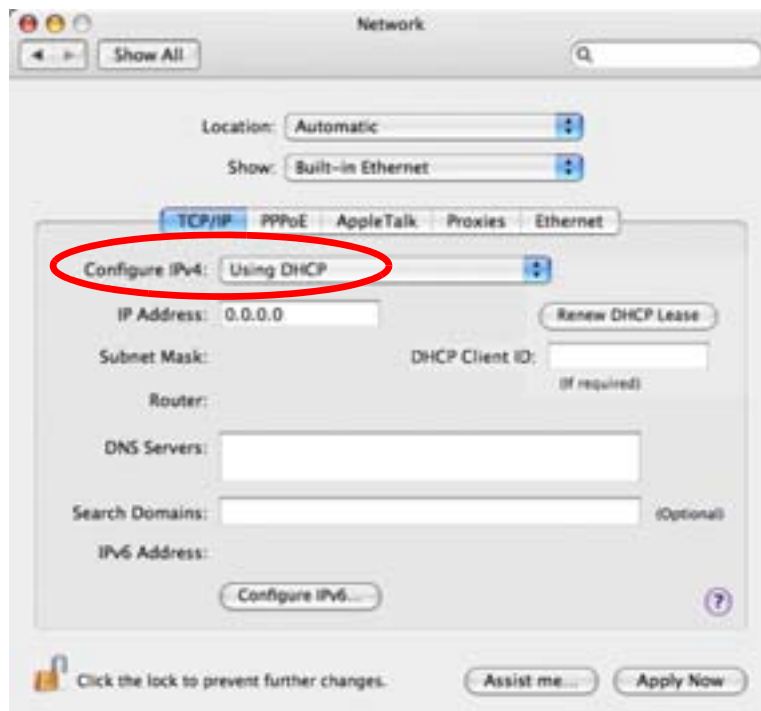
- 3 When the **Network** preferences pane opens, select **Built-in Ethernet** from the network connection type list, and then click **Configure**.

**Figure 84** Mac OS X 10.4: Network Preferences



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

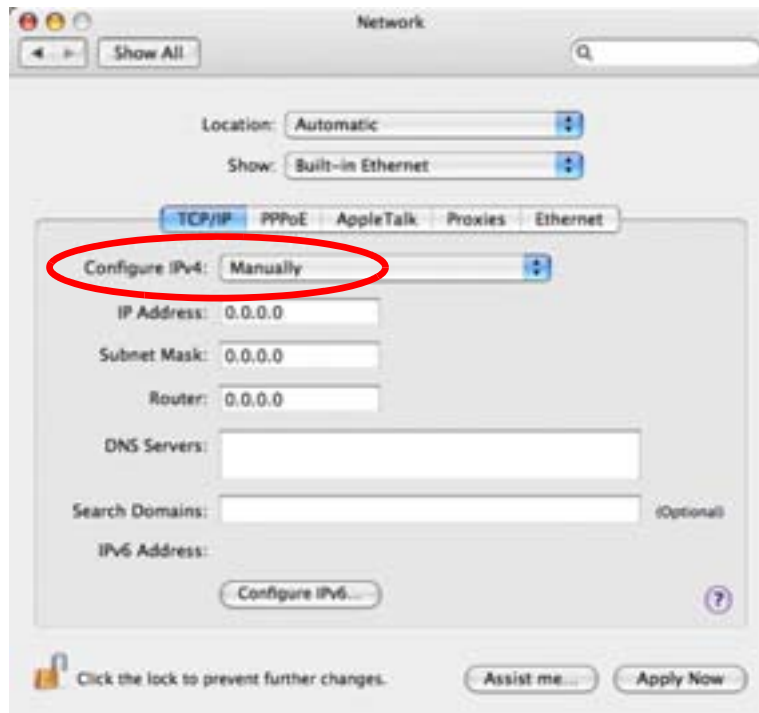
**Figure 85** Mac OS X 10.4: Network Preferences > TCP/IP Tab.





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

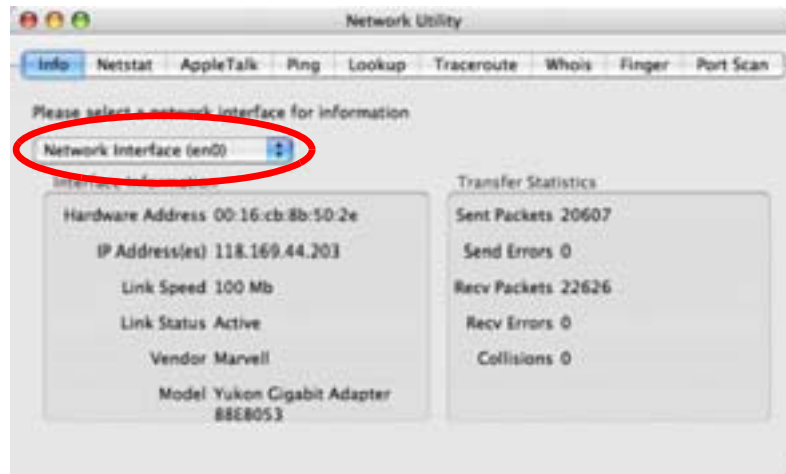
**Figure 86** Mac OS X 10.4: Network Preferences > Ethernet



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

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

**Figure 87** Mac OS X 10.4: Network Utility



## Mac OS X: 10.5

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

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

**Figure 88** Mac OS X 10.5: Apple Menu



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

**Figure 89** Mac OS X 10.5: Systems Preferences



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

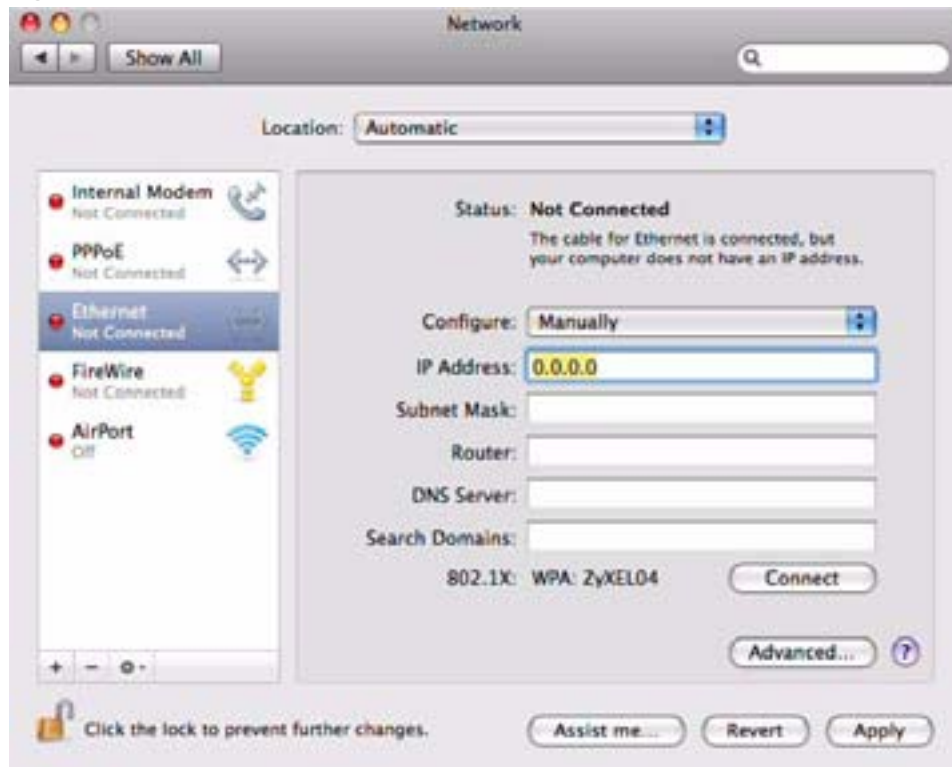
**Figure 90** Mac OS X 10.5: Network Preferences > Ethernet



- 4 From the **Configure** list, select **Using DHCP** for dynamically assigned settings.
- 5 For statically assigned settings, do the following:
  - From the **Configure** list, select **Manually**.
  - In the **IP Address** field, enter your IP address.
  - In the **Subnet Mask** field, enter your subnet mask.

- In the **Router** field, enter the IP address of your WIMAX Device.

**Figure 91** Mac OS X 10.5: Network Preferences > Ethernet

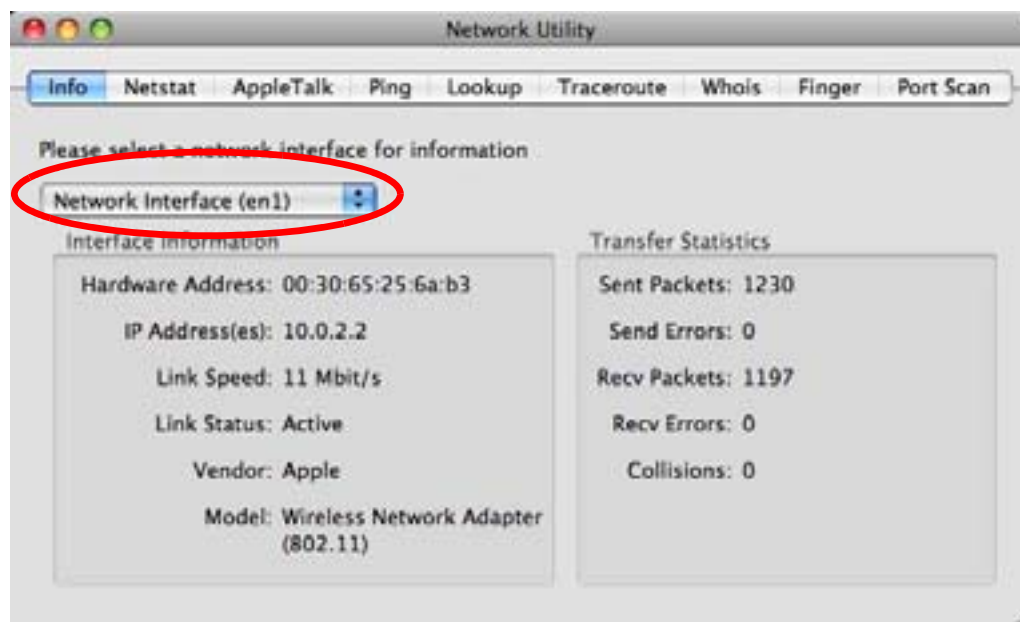


- 6 Click **Apply** and close the window.

## Verifying Settings

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

**Figure 92** Mac OS X 10.5: Network Utility



## Linux: Ubuntu 8 (GNOME)

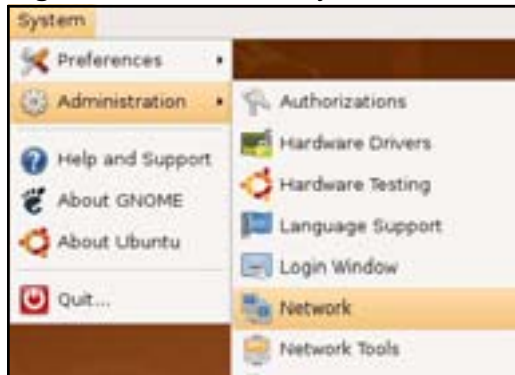
This section shows you how to configure your computer's TCP/IP settings in the GNU Object Model Environment (GNOME) using the Ubuntu 8 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following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

Note: Make sure you are logged in as the root administrator.

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

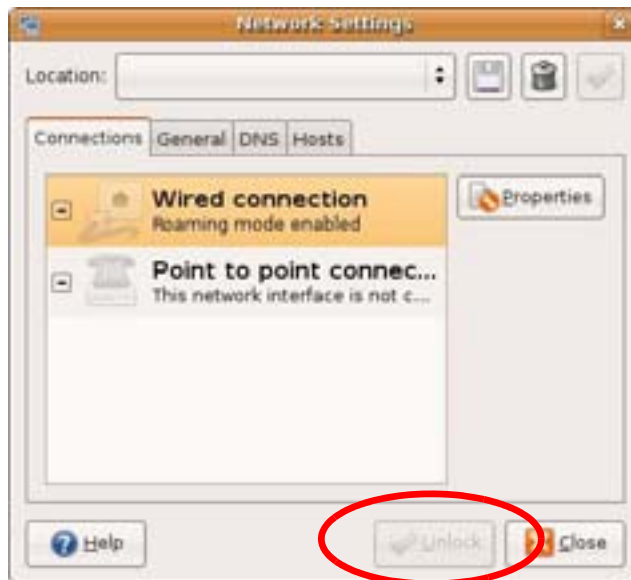
- 1 Click **System > Administration > Network**.

**Figure 93** Ubuntu 8: System > Administration Menu



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

**Figure 94** Ubuntu 8: Network Settings > Connections



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

**Figure 95** Ubuntu 8: Administrator Account Authentication



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

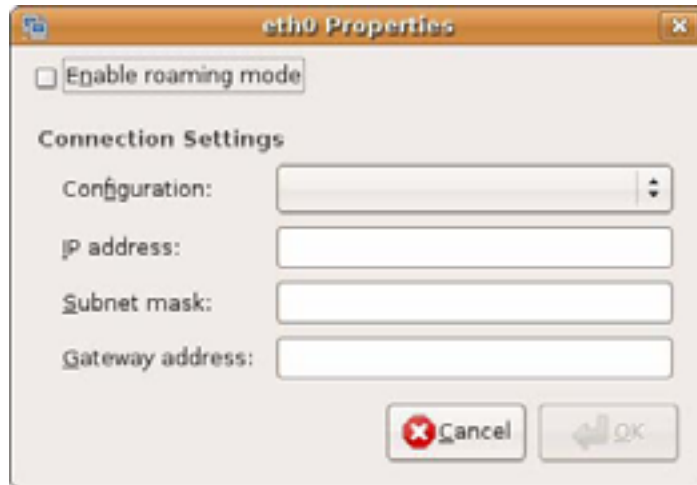
**Figure 96** Ubuntu 8: Network Settings > Connections





- 5 The **Properties** dialog box opens.

**Figure 97** Ubuntu 8: Network Settings > Properties



- In the **Configuration** list, select **Automatic Configuration (DHCP)** if you have a dynamic IP address.
  - In the **Configuration** list, select **Static IP address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Gateway address** fields.
- 6 Click **OK** to save the changes and close the **Properties** dialog box and return to the **Network Settings** screen.

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

**Figure 98** Ubuntu 8: Network Settings > DNS



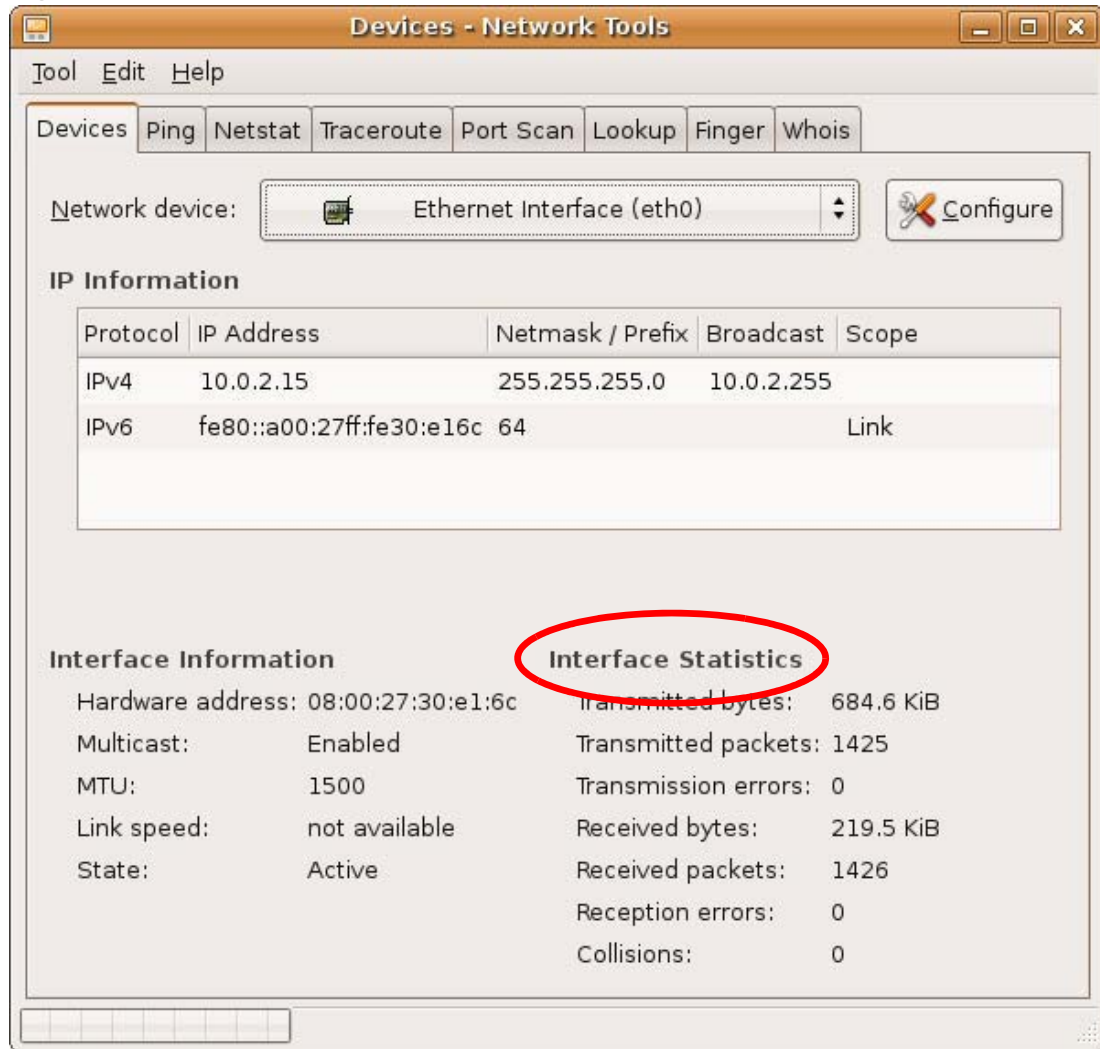
- 8 Click the **Close** button to apply the changes.

## Verifying Settings

Check your TCP/IP properties by clicking **System > Administration > Network Tools**, and then selecting the appropriate **Network device** from the **Devices**

tab. The **Interface Statistics** column shows data if your connection is working properly.

**Figure 99** Ubuntu 8: Network Tools



## Linux: openSUSE 10.3 (KDE)

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

Note: Make sure you are logged in as the root administrator.

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

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

**Figure 100** openSUSE 10.3: K Menu > Computer Menu



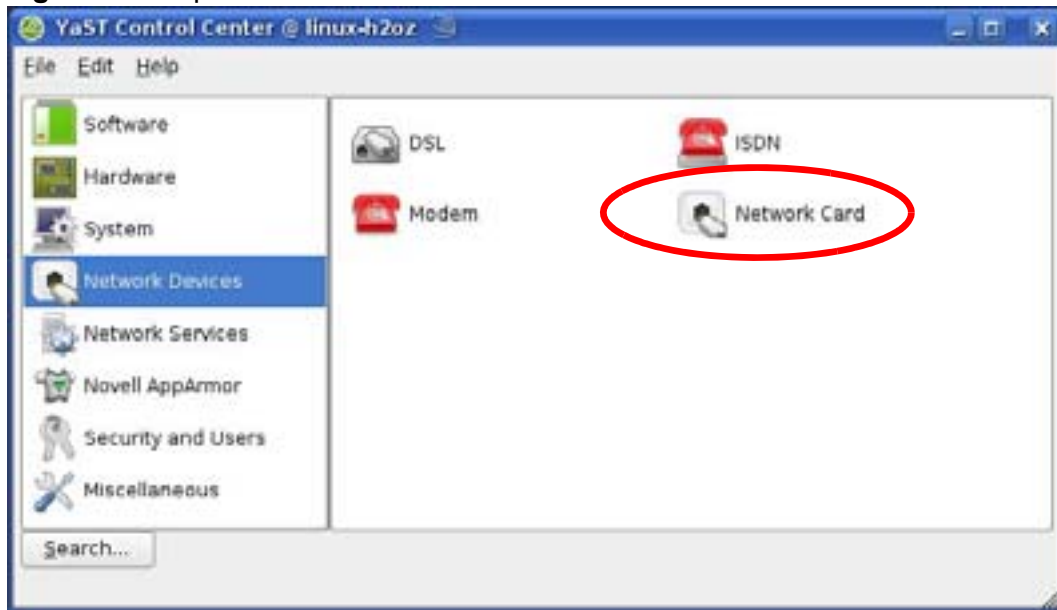
- 2 When the **Run as Root - KDE su** dialog opens, enter the admin password and click **OK**.

**Figure 101** openSUSE 10.3: K Menu > Computer Menu



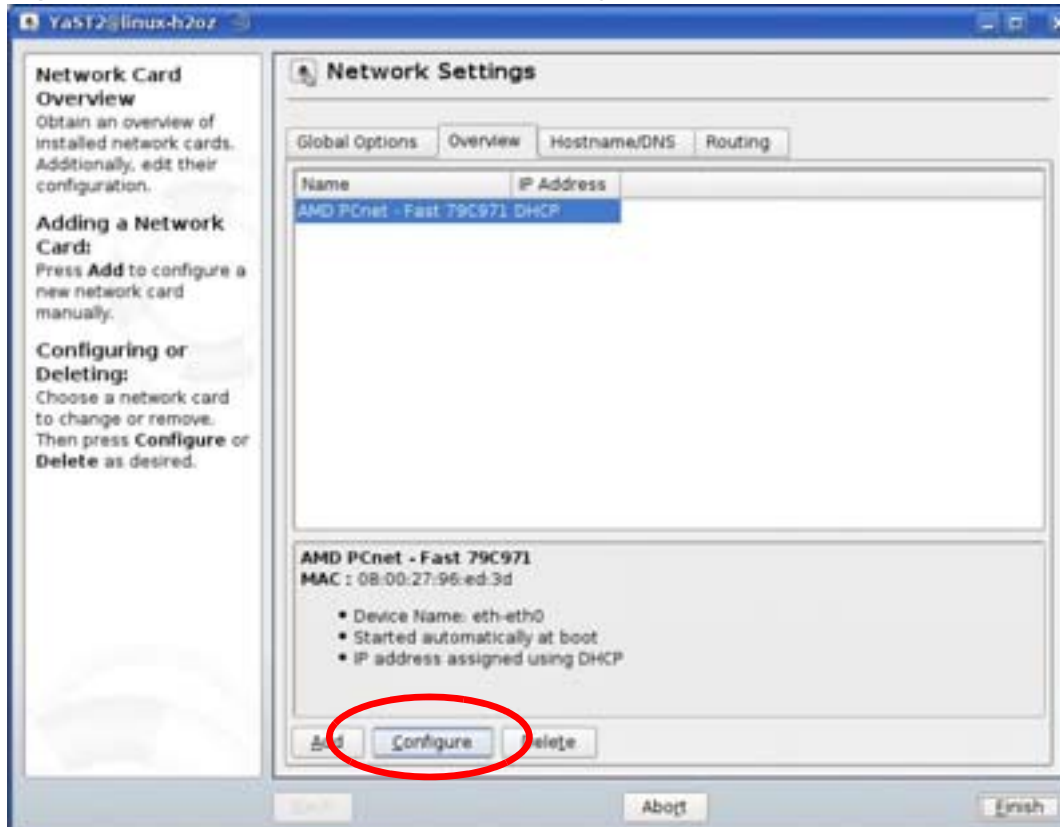
- 3 When the **YaST Control Center** window opens, select **Network Devices** and then click the **Network Card** icon.

**Figure 102** openSUSE 10.3: YaST Control Center



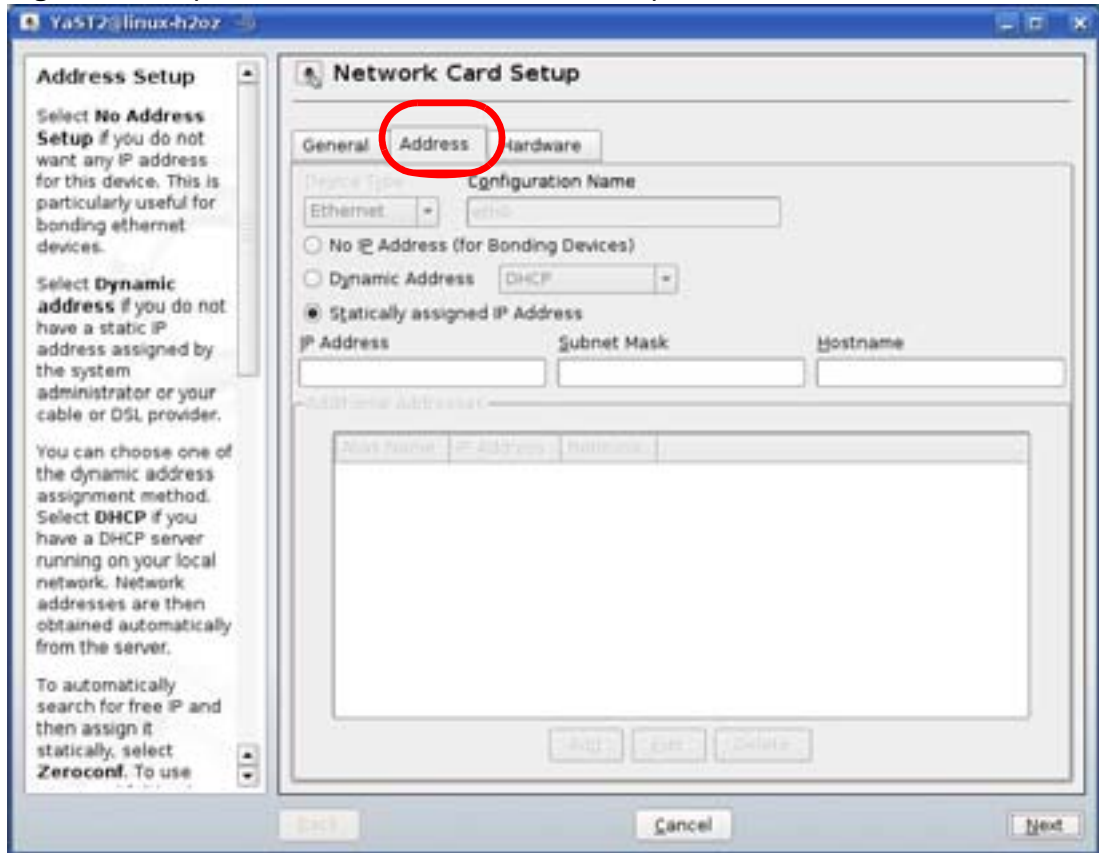
- 4 When the **Network Settings** window opens, click the **Overview** tab, select the appropriate connection **Name** from the list, and then click the **Configure** button.

**Figure 103** openSUSE 10.3: Network Settings



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

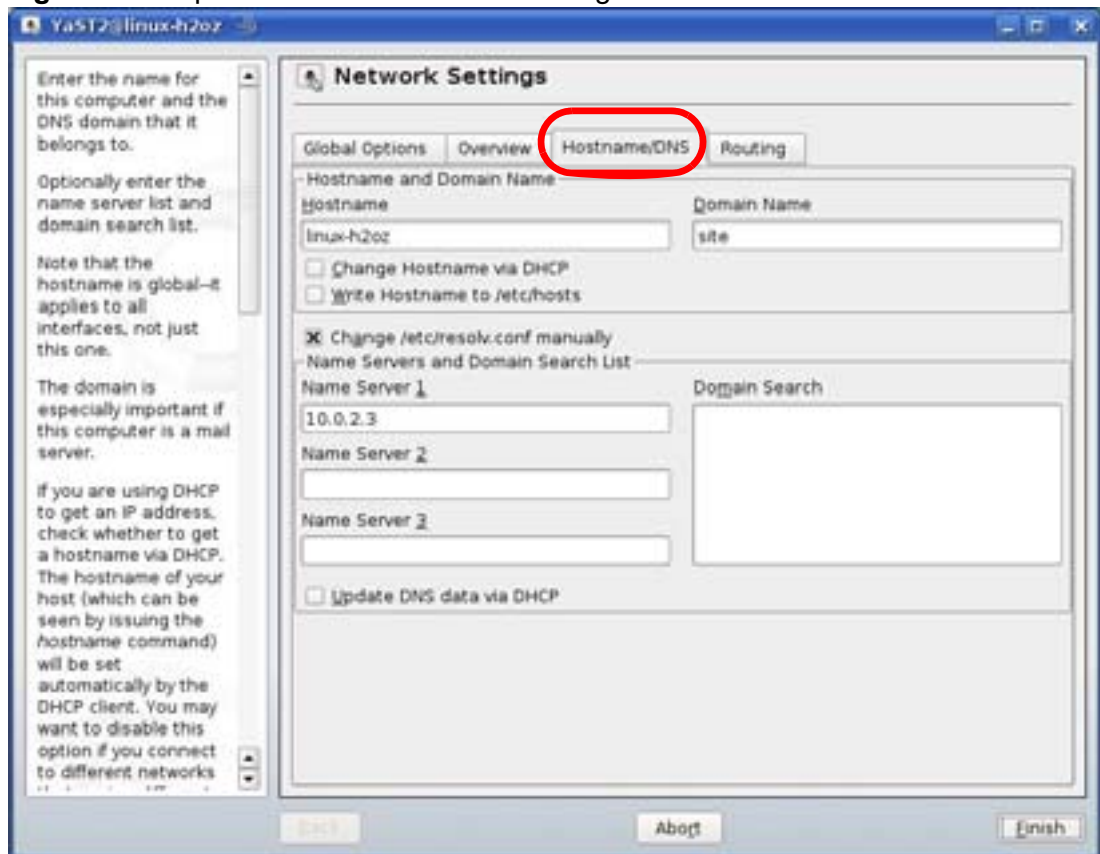
**Figure 104** openSUSE 10.3: Network Card Setup



- 6 Select **Dynamic Address (DHCP)** if you have a dynamic IP address.  
Select **Statically assigned IP Address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Hostname** fields.
- 7 Click **Next** to save the changes and close the **Network Card Setup** window.

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

**Figure 105** openSUSE 10.3: Network Settings



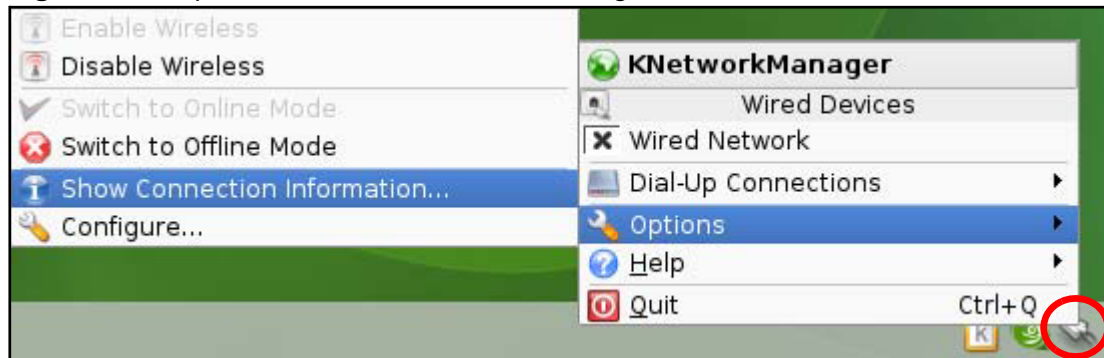
- 9 Click **Finish** to save your settings and close the window.



## Verifying Settings

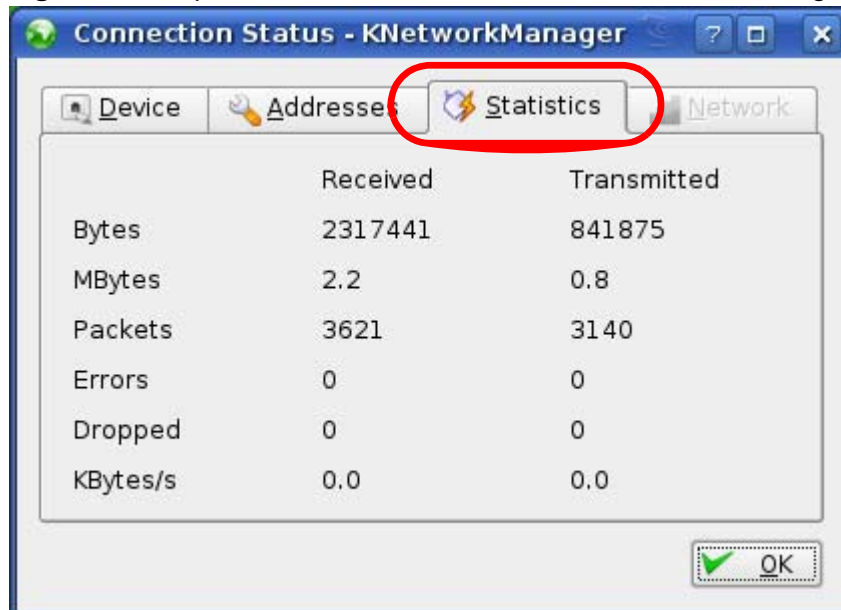
Click the **KNetwork Manager** icon on the **Task bar** to check your TCP/IP properties. From the **Options** sub-menu, select **Show Connection Information**.

**Figure 106** openSUSE 10.3: KNetwork Manager



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

**Figure 107** openSUSE: Connection Status - KNetwork Manager





# Pop-up Windows, JavaScript and Java Permissions

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

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

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

## Internet Explorer Pop-up Blockers

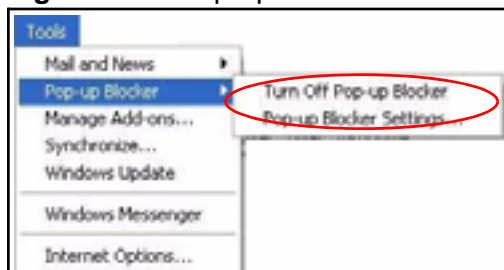
You may have to disable pop-up blocking to log into your device.

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

### Disable Pop-up Blockers

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

**Figure 108** Pop-up Blocker



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

- 1 In Internet Explorer, select **Tools, Internet Options, Privacy**.
- 2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

**Figure 109** Internet Options: Privacy



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

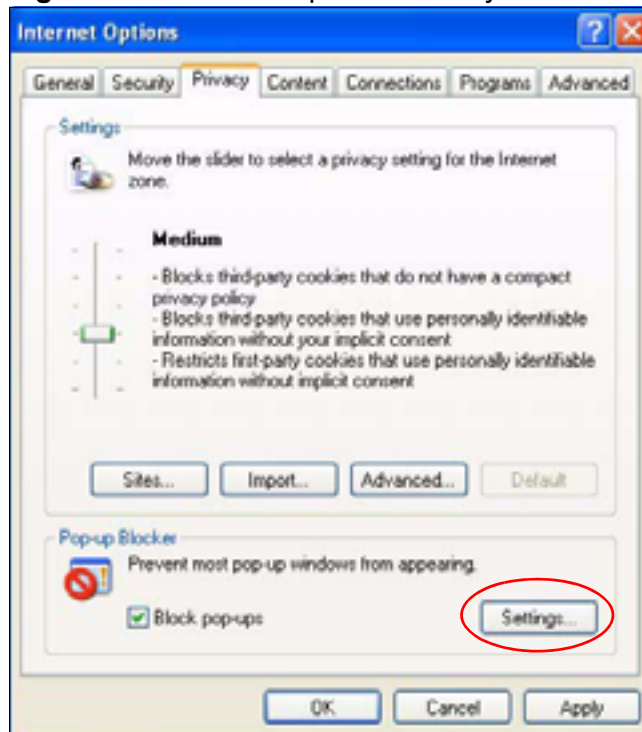
### Enable Pop-up Blockers with Exceptions

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

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

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

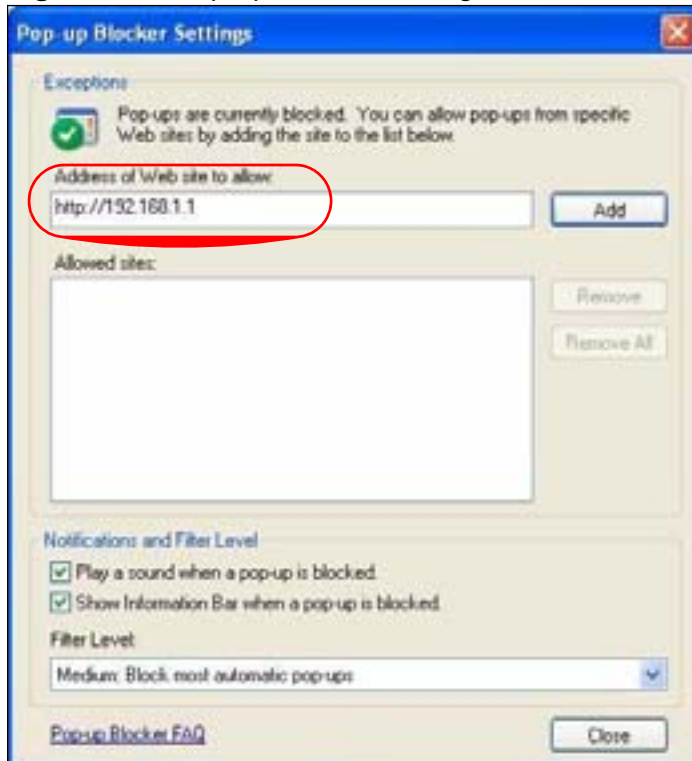
**Figure 110** Internet Options: Privacy



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

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

**Figure 111** Pop-up Blocker Settings



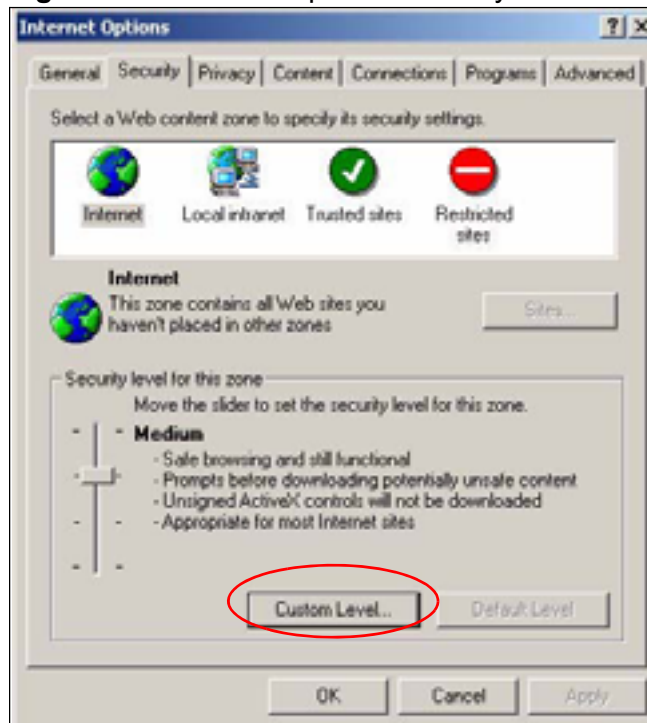
- 5 Click **Close** to return to the **Privacy** screen.
- 6 Click **Apply** to save this setting.

## JavaScript

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

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

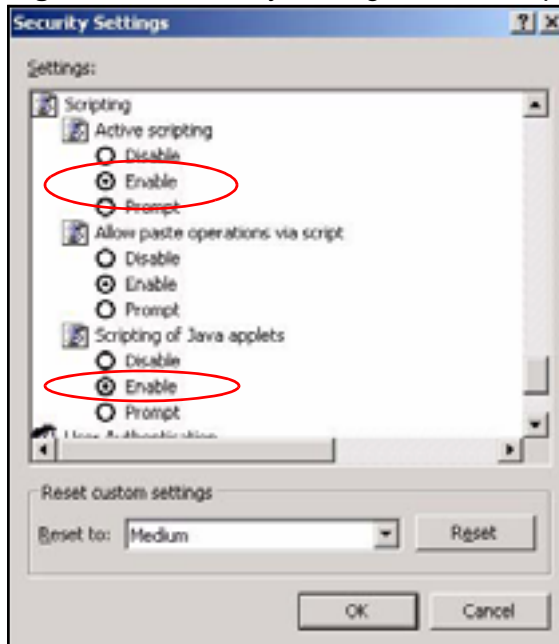
**Figure 112** Internet Options: Security



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

- 6 Click **OK** to close the window.

**Figure 113** Security Settings - Java Scripting



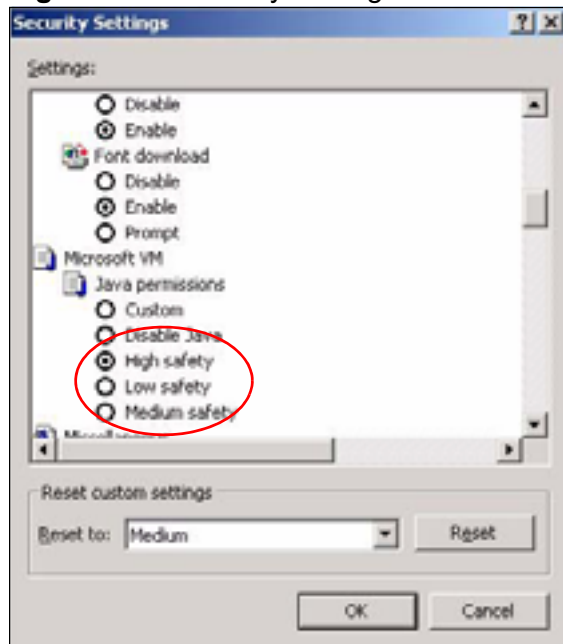
## Java Permissions

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



- 5 Click **OK** to close the window.

**Figure 114** Security Settings - Java

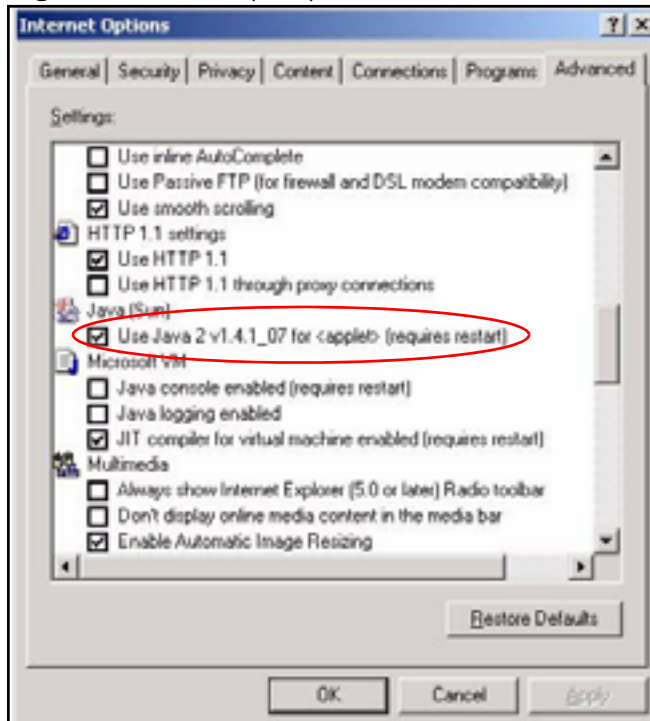


## JAVA (Sun)

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

- 3 Click **OK** to close the window.

**Figure 115** Java (Sun)

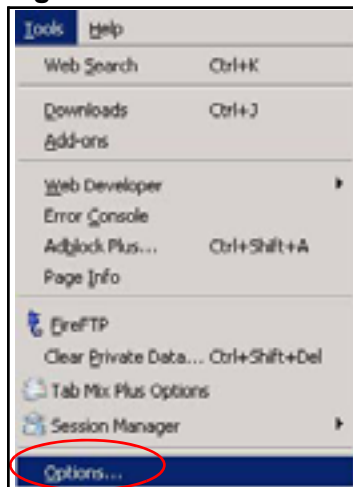


## Mozilla Firefox

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

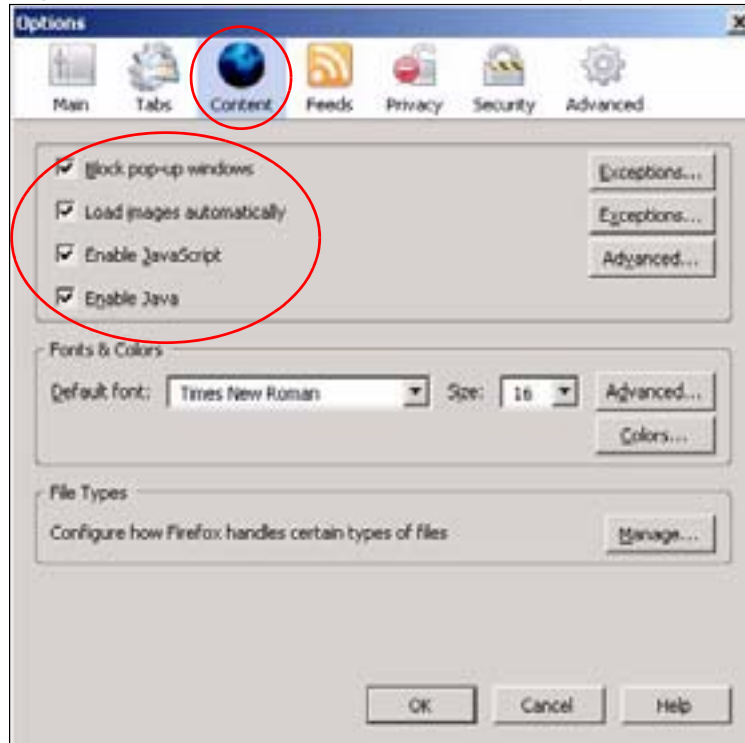
You can enable Java, Javascript and pop-ups in one screen. Click **Tools**, then click **Options** in the screen that appears.

**Figure 116** Mozilla Firefox: TOOLS > Options



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

**Figure 117** Mozilla Firefox Content Security





# IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

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

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

## Introduction to IP Addresses

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

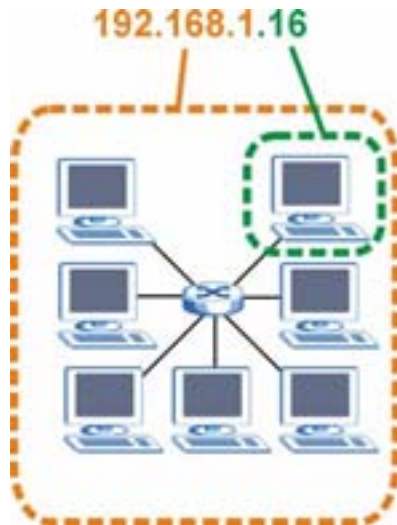
## Structure

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

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

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

**Figure 118** Network Number and Host ID



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

## Subnet Masks

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

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

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

**Table 60** IP Address Network Number and Host ID Example

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

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

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

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

**Table 61** Subnet Masks

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

## Network Size

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

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

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

**Table 62** Maximum Host Numbers

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

## Notation

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

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

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

**Table 63** Alternative Subnet Mask Notation

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

## Subnetting

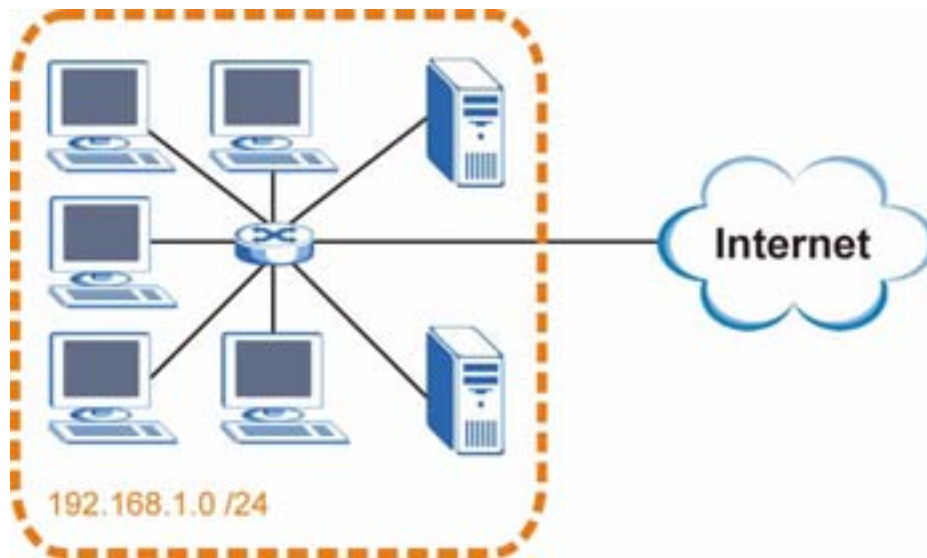
You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

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



The following figure shows the company network before subnetting.

**Figure 119** Subnetting Example: Before Subnetting

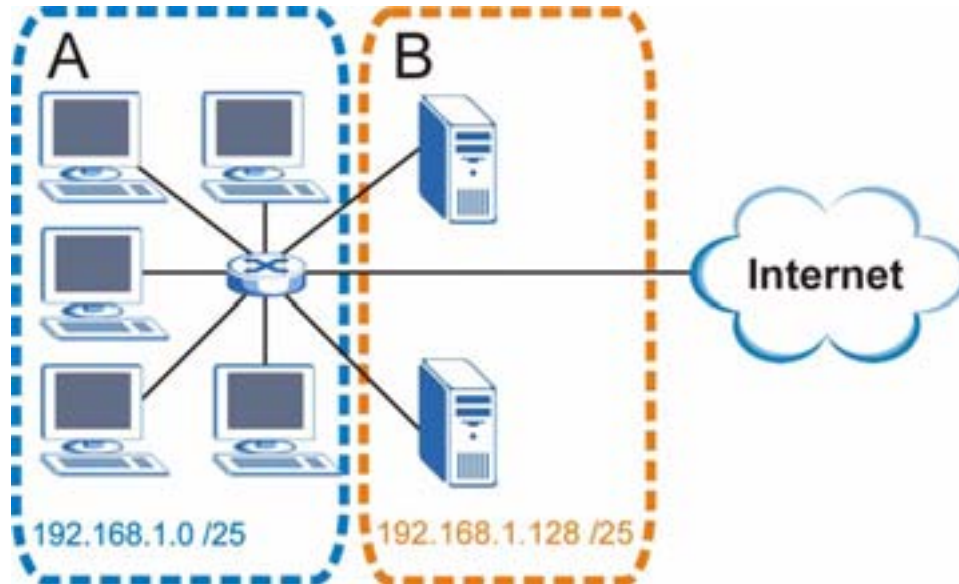


You can “borrow” one of the host ID bits to divide the network `192.168.1.0` into two separate sub-networks. The subnet mask is now 25 bits (`255.255.255.128` or `/25`).

The “borrowed” host ID bit can have a value of either 0 or 1, allowing two subnets; `192.168.1.0 /25` and `192.168.1.128 /25`.

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

**Figure 120** Subnetting Example: After Subnetting



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

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

## Example: Four Subnets

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

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

**Table 64** Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	<b>00000000</b>
Subnet Mask (Binary)	11111111.11111111.11111111.	<b>11000000</b>
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

**Table 65** Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	<b>01000000</b>
Subnet Mask (Binary)	11111111.11111111.11111111.	<b>11000000</b>
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

**Table 66** Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	<b>10000000</b>
Subnet Mask (Binary)	11111111.11111111.11111111.	<b>11000000</b>
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

**Table 67** Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001. .	<b>11000000</b>
Subnet Mask (Binary)	11111111.11111111.11111111. .	<b>11000000</b>

**Table 67** Subnet 4 (continued)

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

## Example: Eight Subnets

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

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

**Table 68** Eight Subnets

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

## Subnet Planning

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

**Table 69** 24-bit Network Number Subnet Planning

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

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

**Table 70** 16-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

## Configuring IP Addresses

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

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the WiMAX Device.

Once you have decided on the network number, pick an IP address for your WiMAX Device that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your WiMAX Device will compute the subnet mask automatically based on the IP

address that you entered. You don't need to change the subnet mask computed by the WiMAX Device unless you are instructed to do otherwise.

## Private IP Addresses

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

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

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

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

## IP Address Conflicts

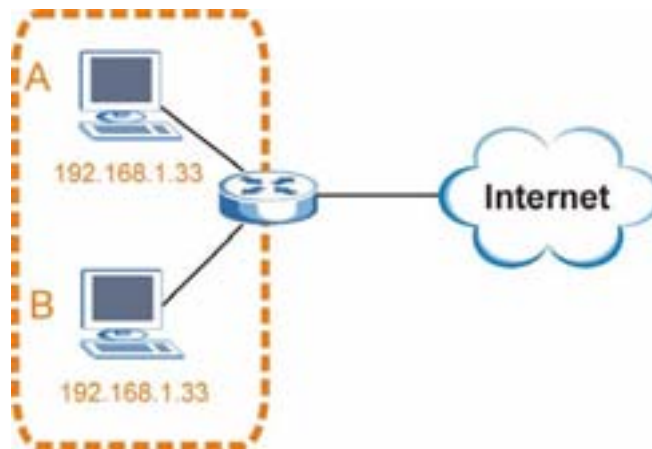
Each device on a network must have a unique IP address. Devices with duplicate IP addresses on the same network will not be able to access the Internet or other resources. The devices may also be unreachable through the network.

### Conflicting Computer IP Addresses Example

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

address to computer **A** or setting computer **A** to obtain an IP address automatically.

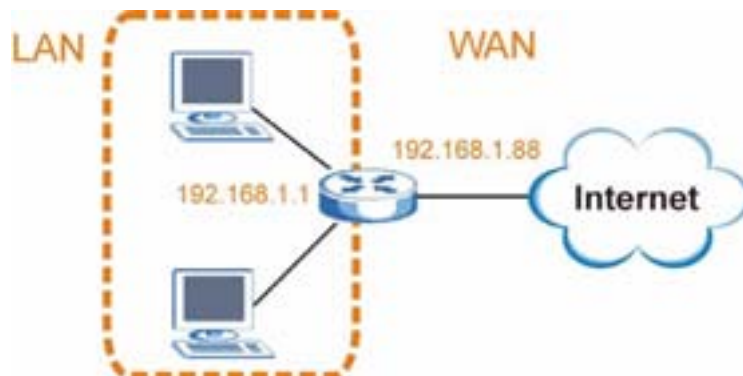
**Figure 121** Conflicting Computer IP Addresses Example



### Conflicting Router IP Addresses Example

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

**Figure 122** Conflicting Computer IP Addresses Example

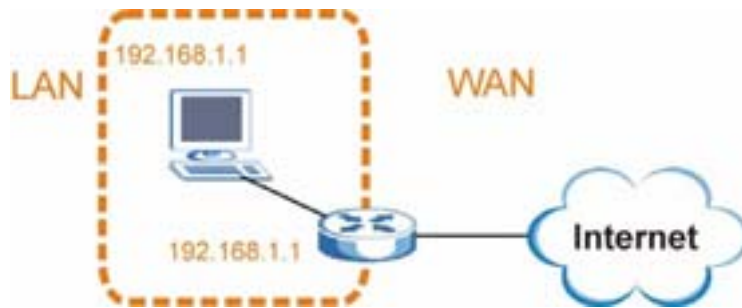


### Conflicting Computer and Router IP Addresses Example

More than one device can not use the same IP address. In the following example, the computer and the router's LAN port both use 192.168.1.1 as the IP address.

The computer cannot access the Internet. This problem can be solved by assigning a different IP address to the computer or the router's LAN port.

**Figure 123** Conflicting Computer and Router IP Addresses Example






# Importing Certificates

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

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

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

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:

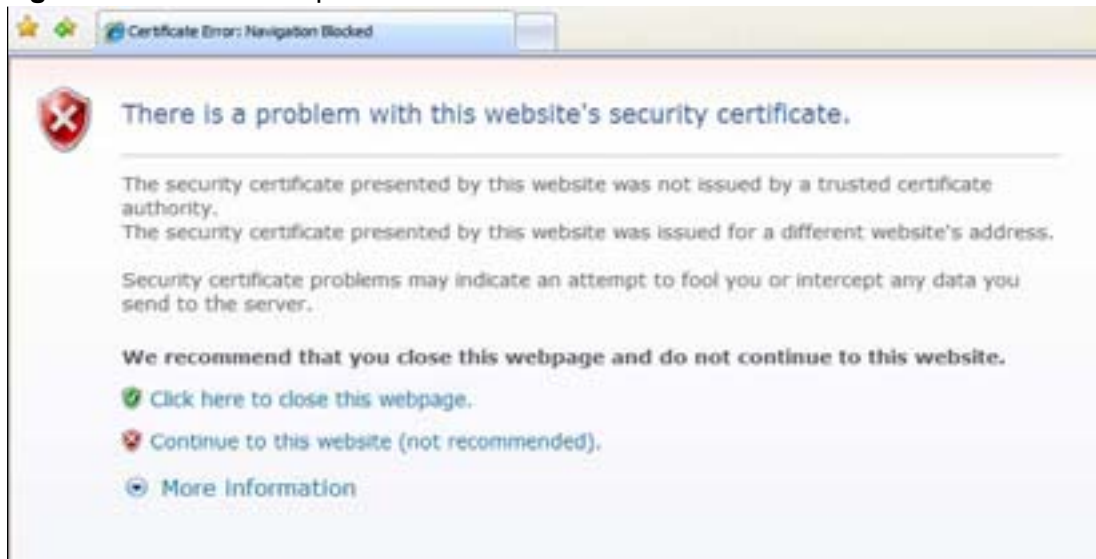
- Internet Explorer on [page 202](#)
- Firefox on [page 212](#)
- Opera on [page 218](#)
- Konqueror on [page 226](#)

## 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 124** Internet Explorer 7: Certification Error



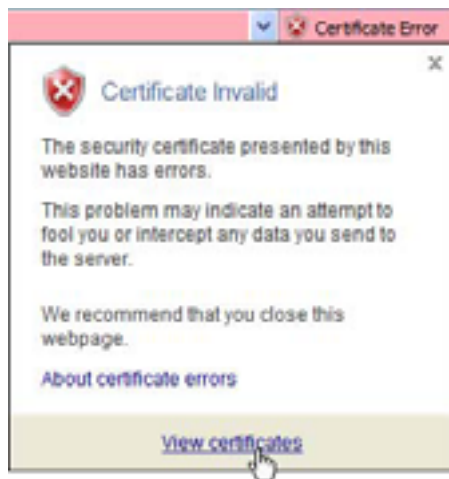
- 2 Click **Continue to this website (not recommended)**.

**Figure 125** Internet Explorer 7: Certification Error



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

**Figure 126** Internet Explorer 7: Certificate Error



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

**Figure 127** Internet Explorer 7: Certificate



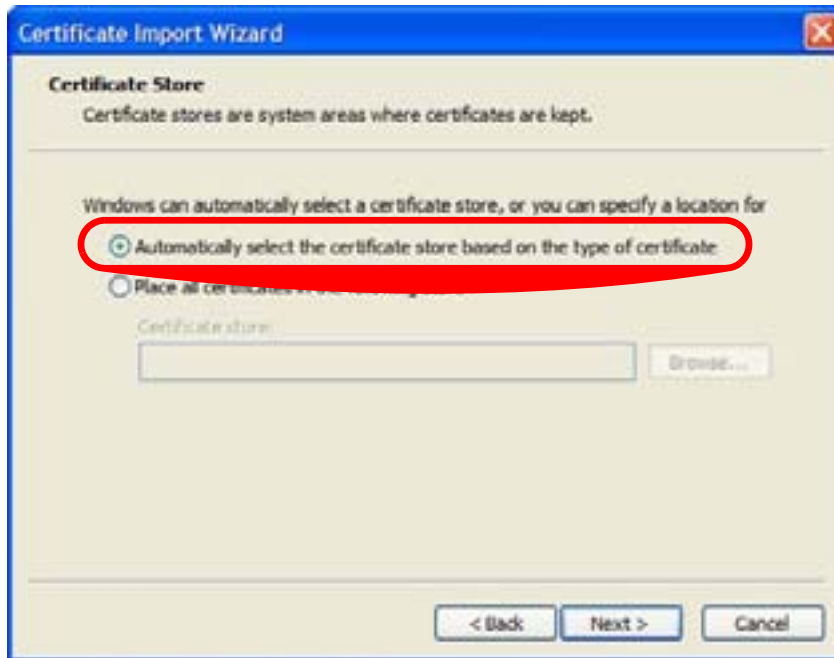
- 5 In the **Certificate Import Wizard**, click **Next**.

**Figure 128** 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 129** Internet Explorer 7: Certificate Import Wizard



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

**Figure 130** 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 131** Internet Explorer 7: Select Certificate Store



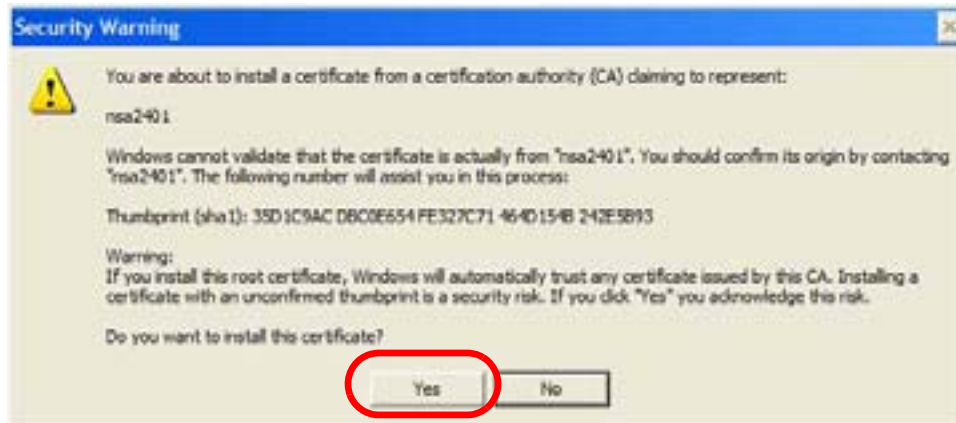
- 9 In the **Completing the Certificate Import Wizard** screen, click **Finish**.

**Figure 132** Internet Explorer 7: Certificate Import Wizard



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

**Figure 133** Internet Explorer 7: Security Warning



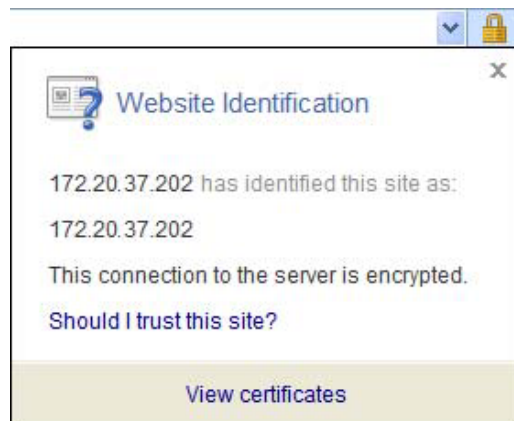
- 11 Finally, click **OK** when presented with the successful certificate installation message.

**Figure 134** 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 135** 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 136** Internet Explorer 7: Public Key Certificate File



CA.cer

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

**Figure 137** Internet Explorer 7: Open File - Security Warning



- 3 Refer to steps 4-12 in the Internet Explorer procedure beginning on [page 202](#) to complete the installation process.

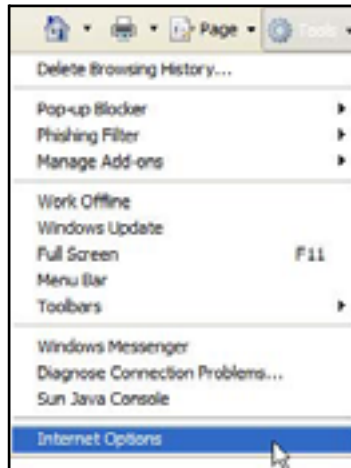


## Removing a Certificate in Internet Explorer

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

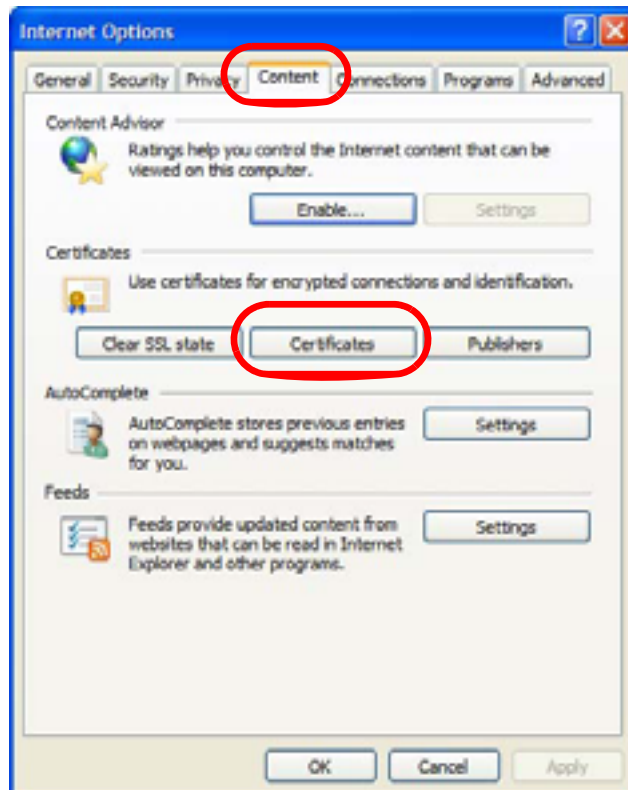
- 1 Open **Internet Explorer** and click **TOOLS > Internet Options**.

**Figure 138** Internet Explorer 7: Tools Menu



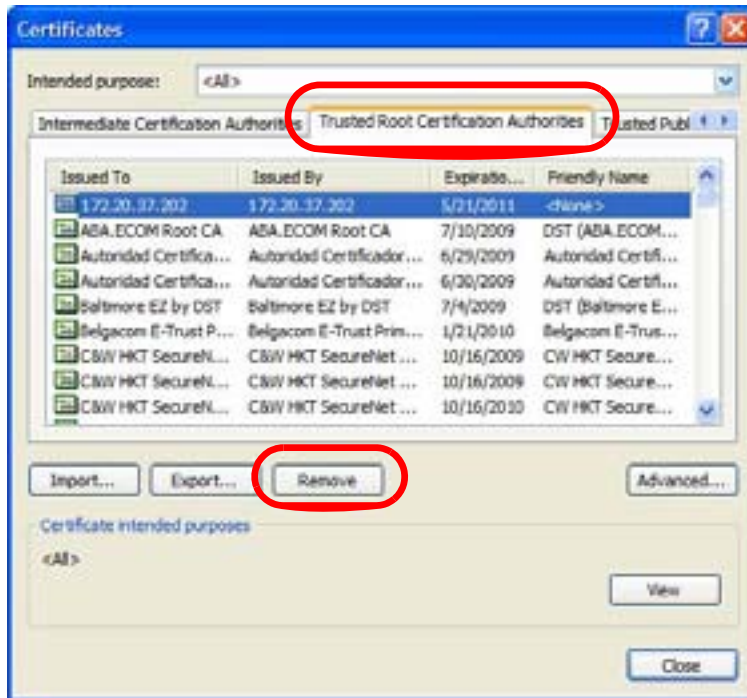
- 2 In the **Internet Options** dialog box, click **Content > Certificates**.

**Figure 139** Internet Explorer 7: Internet Options



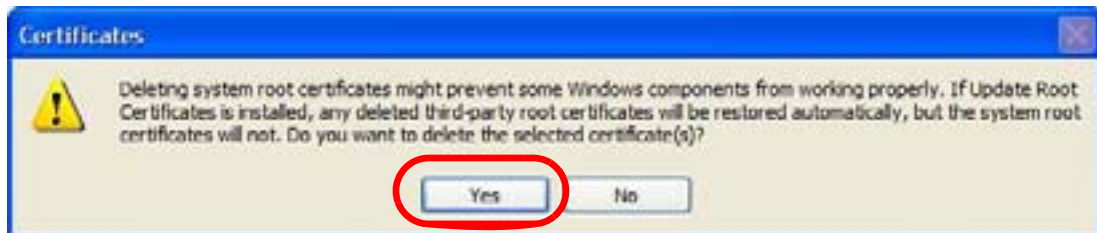
- In the **Certificates** dialog box, click the **Trusted Root Certificates Authorities** tab, select the certificate that you want to delete, and then click **Remove**.

**Figure 140** Internet Explorer 7: Certificates



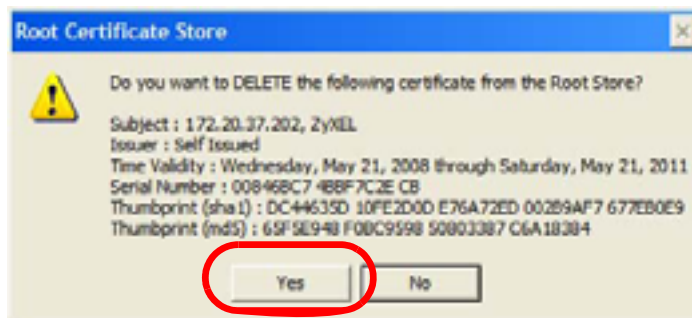
- In the **Certificates** confirmation, click **Yes**.

**Figure 141** Internet Explorer 7: Certificates



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

**Figure 142** 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.

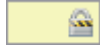
- 1 If your device's web configurator is set to use SSL certification, then the first time you browse to it you are presented with a certification error.
- 2 Select **Accept this certificate permanently** and click **OK**.

**Figure 143** 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 144** Firefox 2: Page Info

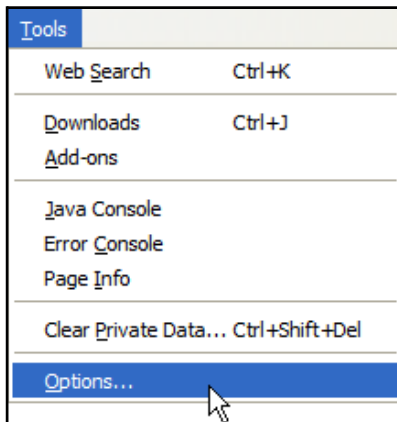


## Installing a Stand-Alone Certificate File in Firefox

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.

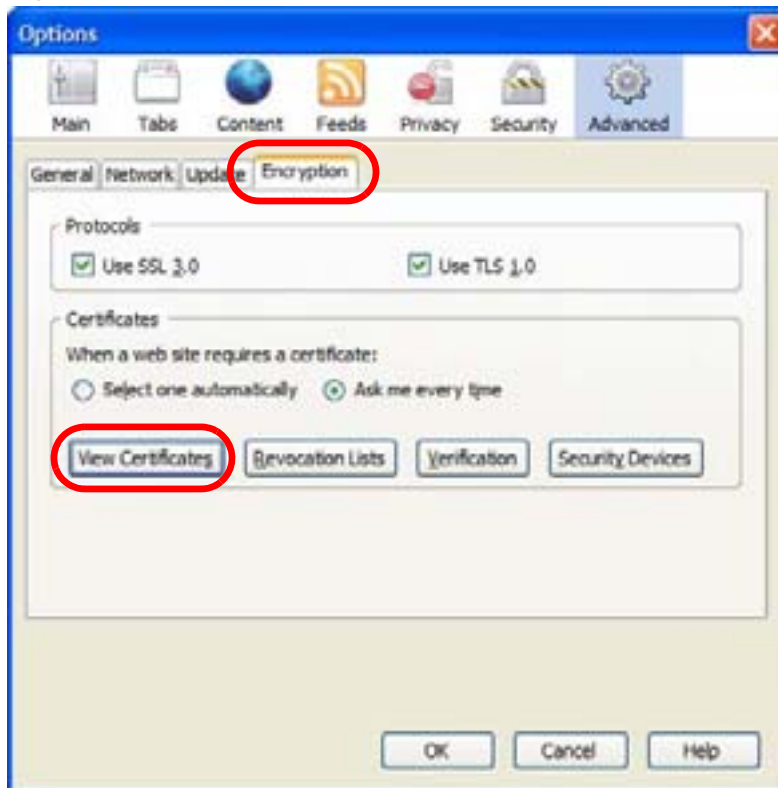
- 1 Open **Firefox** and click **TOOLS > Options**.

**Figure 145** Firefox 2: Tools Menu



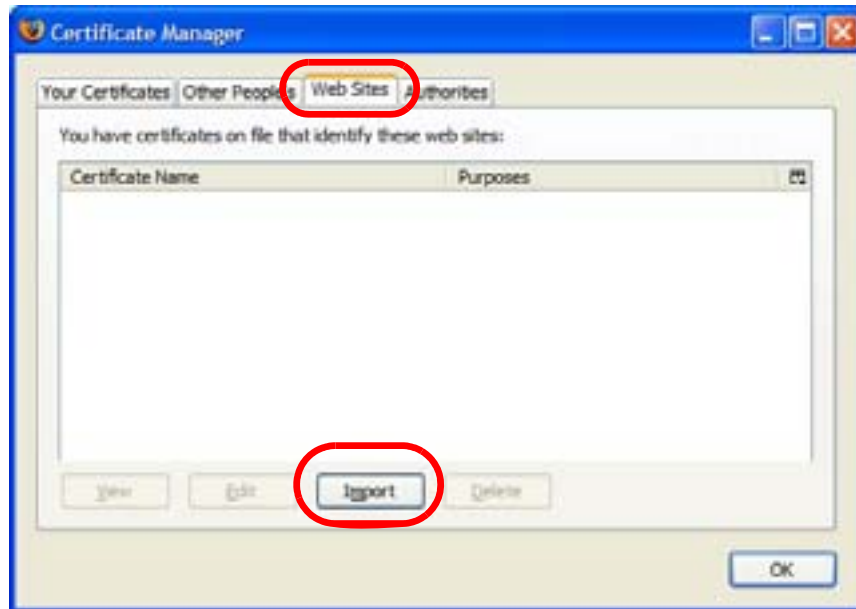
- 2 In the **Options** dialog box, click **ADVANCED > Encryption > View Certificates**.

**Figure 146** Firefox 2: Options



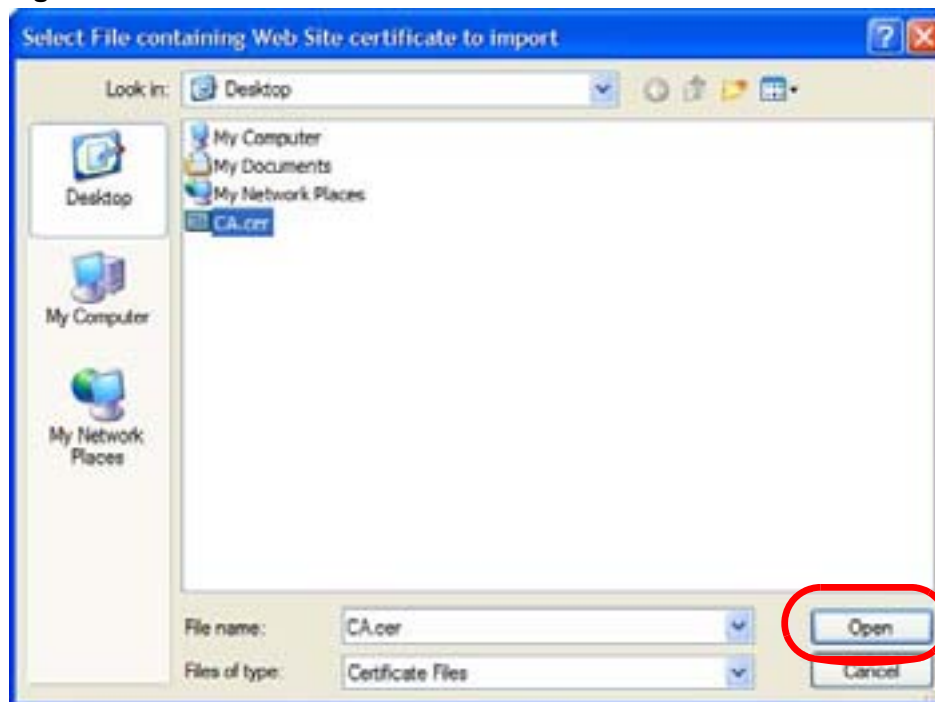
- 3 In the **Certificate Manager** dialog box, click **Web Sites** > **Import**.

**Figure 147** Firefox 2: Certificate Manager



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

**Figure 148** Firefox 2: Select File



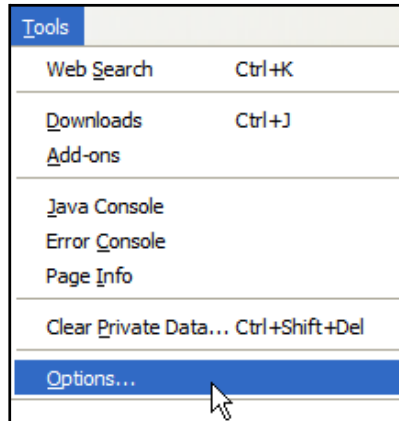
- 5 The next time you visit the web site, click the padlock in the address bar to open the **Page Info** > **Security** window to see the web page's security information.

## Removing a Certificate in Firefox

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

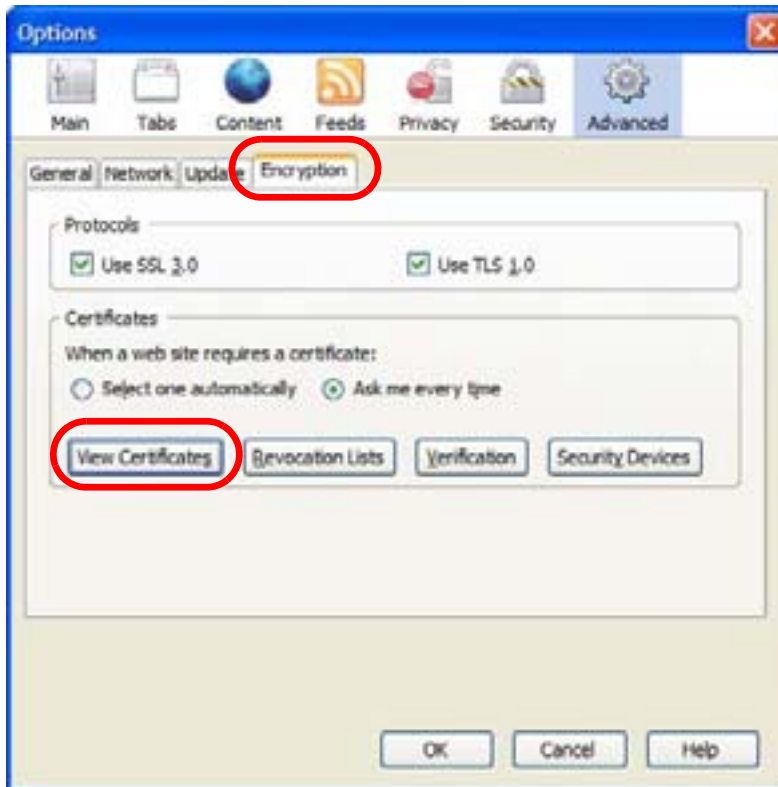
- 1 Open **Firefox** and click **TOOLS > Options**.

**Figure 149** Firefox 2: Tools Menu



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

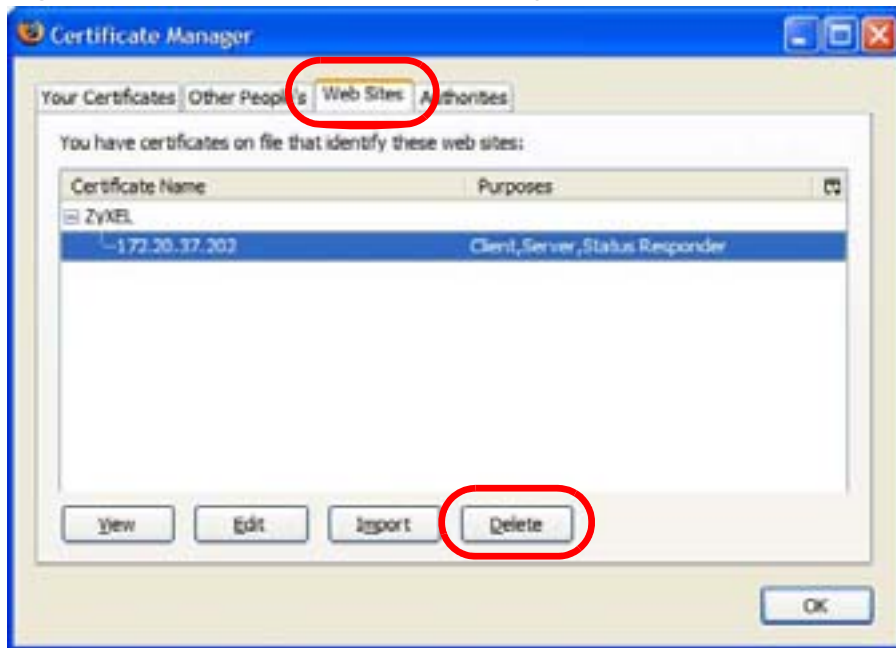
**Figure 150** Firefox 2: Options





- 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 151** Firefox 2: Certificate Manager



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

**Figure 152** Firefox 2: Delete Web Site Certificates



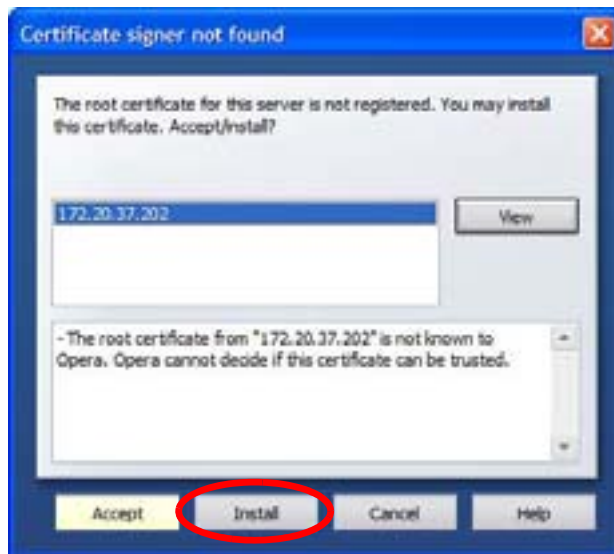
- 5 The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.

## 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 153** 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 154** Opera 9: Security information

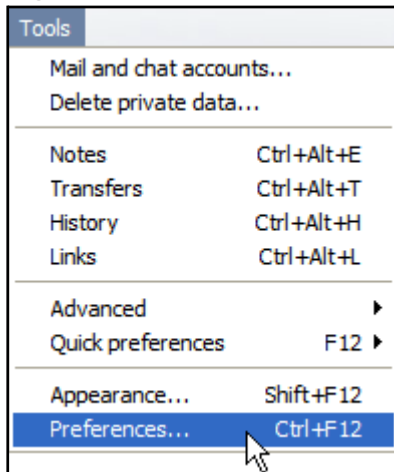


## Installing a Stand-Alone Certificate File in Opera

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.

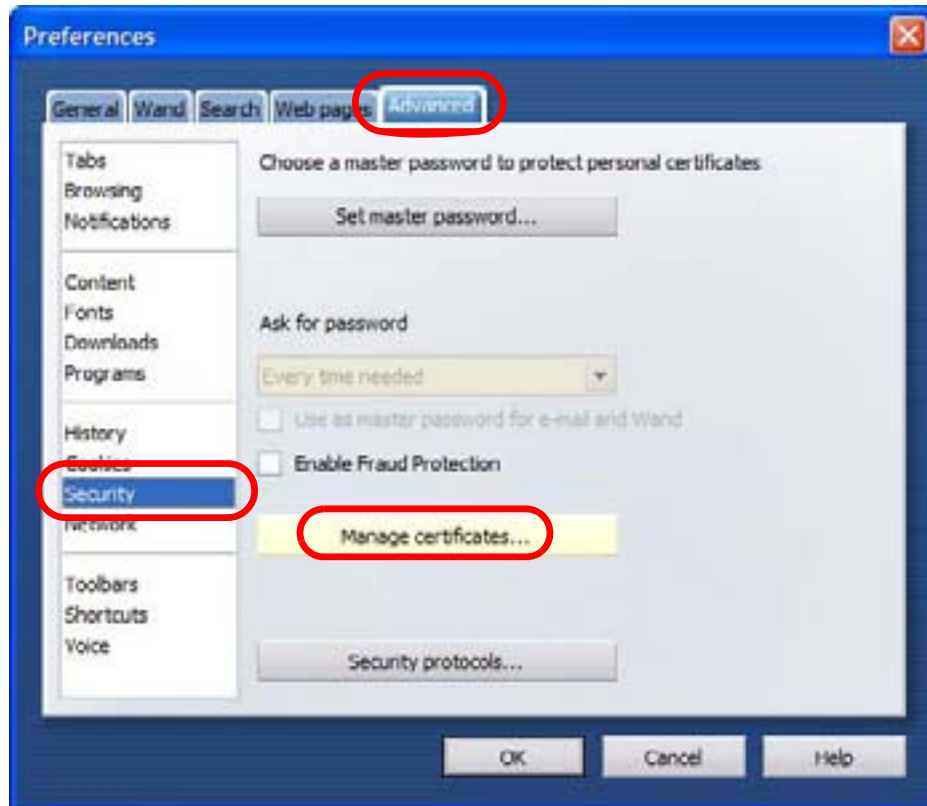
- 1 Open **Opera** and click **TOOLS > Preferences**.

**Figure 155** Opera 9: Tools Menu



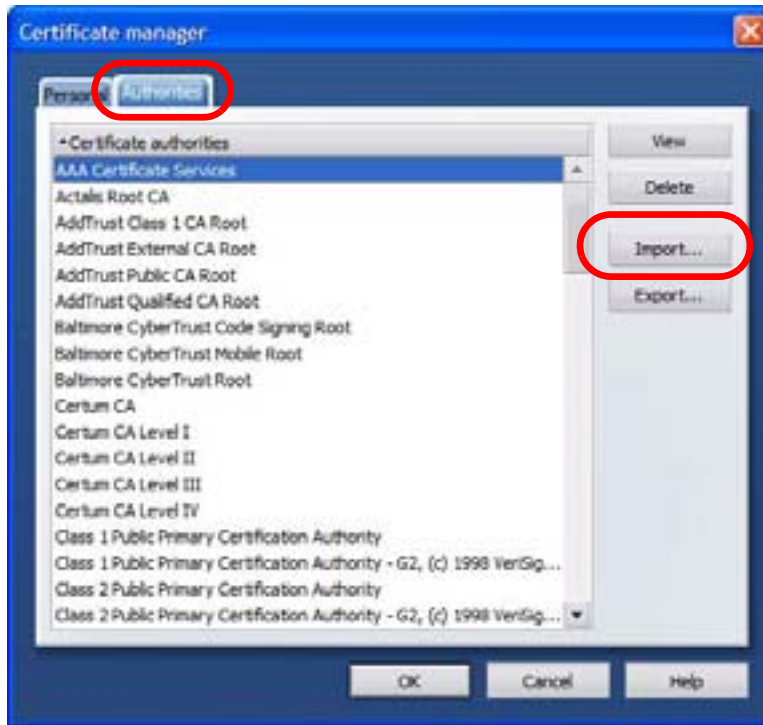
- 2 In **Preferences**, click **ADVANCED > Security > Manage certificates**.

**Figure 156** Opera 9: Preferences



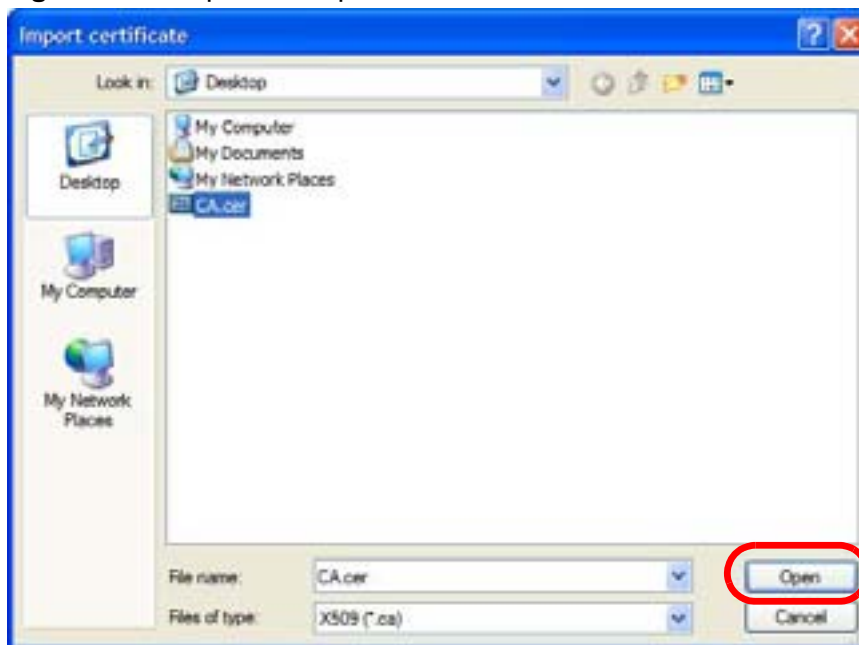
- 3 In the **Certificates Manager**, click **Authorities > Import**.

**Figure 157** Opera 9: Certificate manager



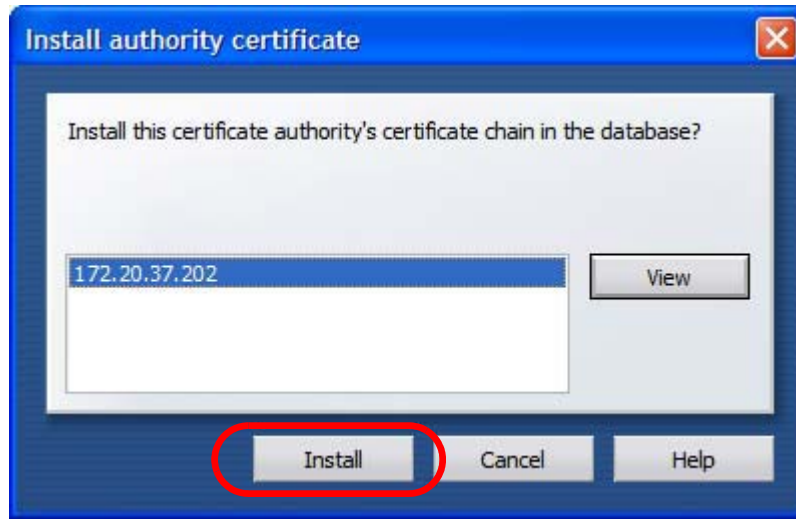
- 4 Use the **Import certificate** dialog box to locate the certificate and then click **Open**.

**Figure 158** Opera 9: Import certificate



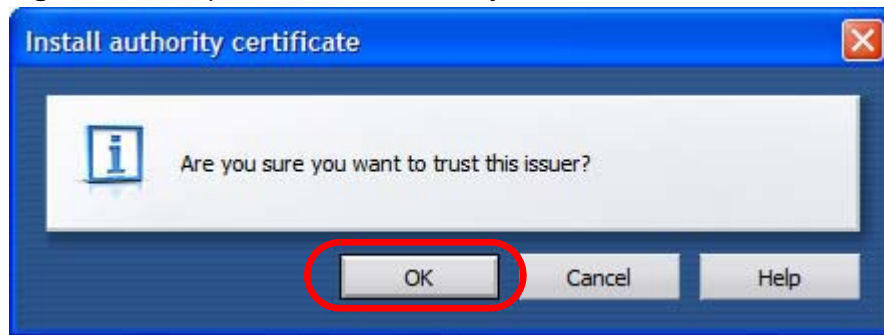
- 5 In the **Install authority certificate** dialog box, click **Install**.

**Figure 159** Opera 9: Install authority certificate



- 6 Next, click **OK**.

**Figure 160** Opera 9: Install authority certificate



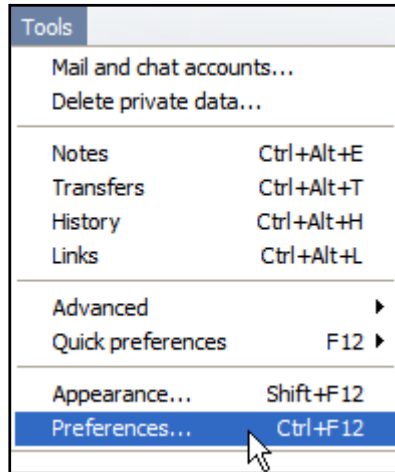
- 7 The next time you visit the web site, click the padlock in the address bar to open the **Security information** window to view the web page's security details.

## Removing a Certificate in Opera

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

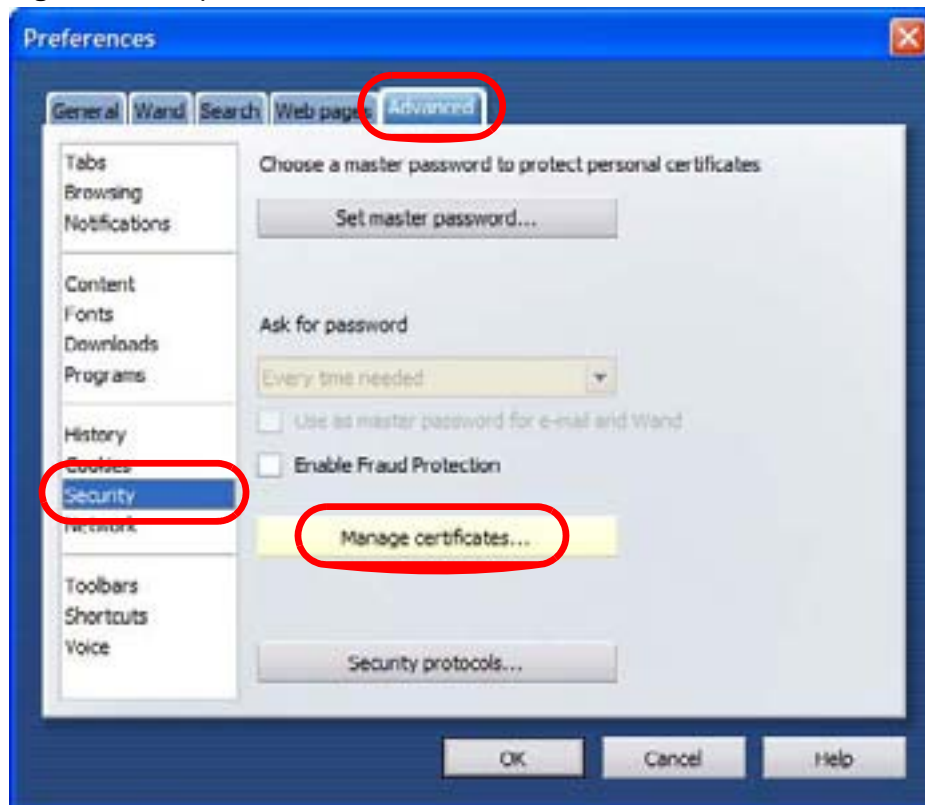
- 1 Open **Opera** and click **TOOLS > Preferences**.

**Figure 161** Opera 9: Tools Menu



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

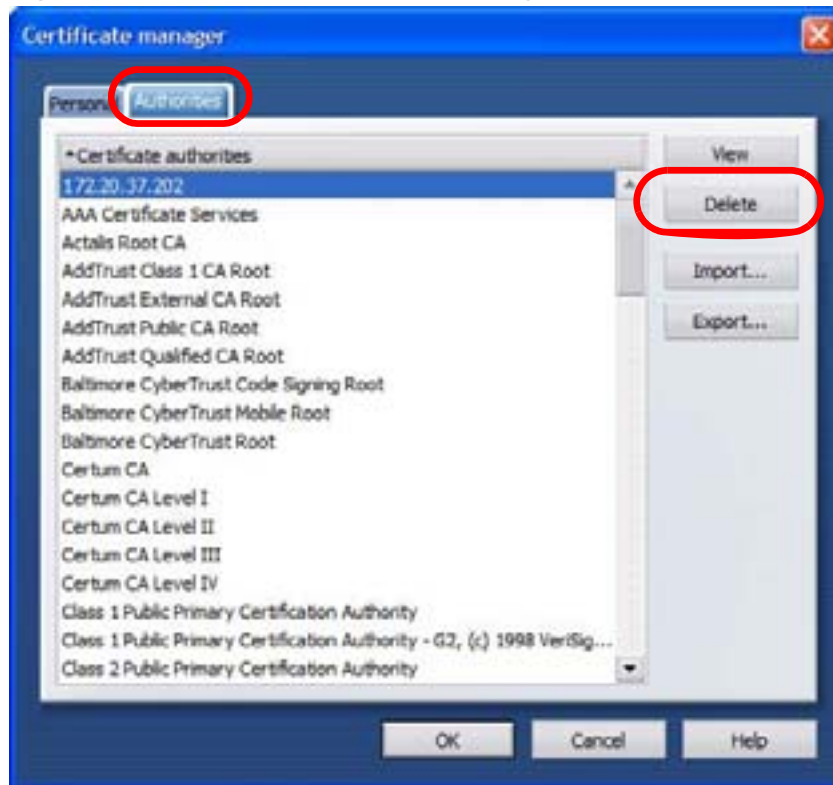
**Figure 162** Opera 9: Preferences





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

**Figure 163** 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.

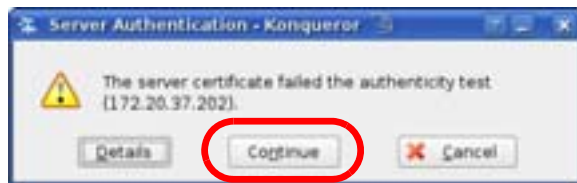
Note: There is no confirmation when you delete a certificate authority, so be absolutely certain that you want to go through with it before clicking the button.

## 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 164** Konqueror 3.5: Server Authentication



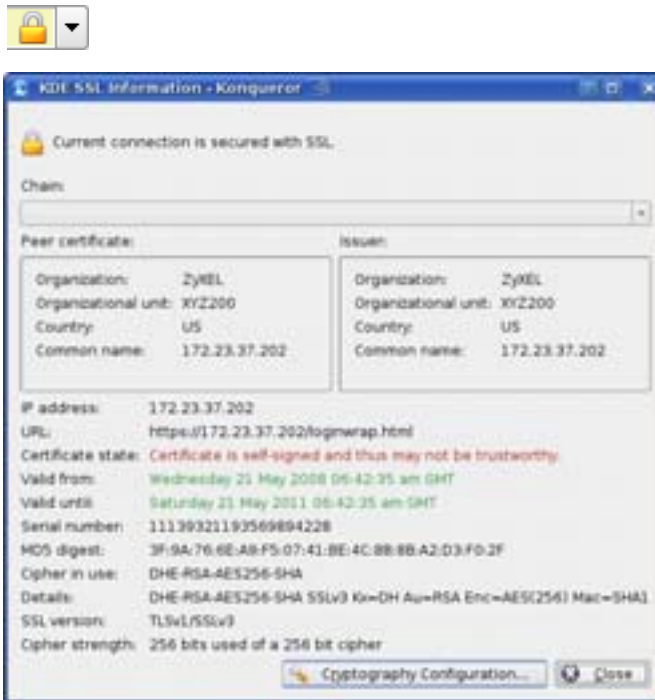
- 3 Click **Forever** when prompted to accept the certificate.

**Figure 165** 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 166** 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.

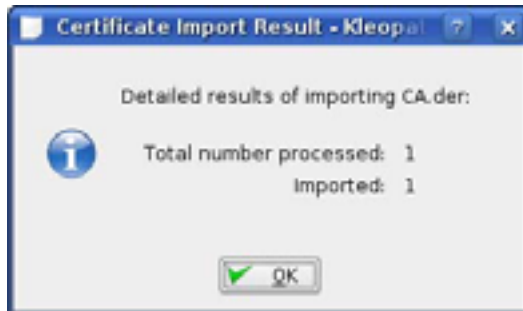
- 1 Double-click the public key certificate file.

**Figure 167** Konqueror 3.5: Public Key Certificate File



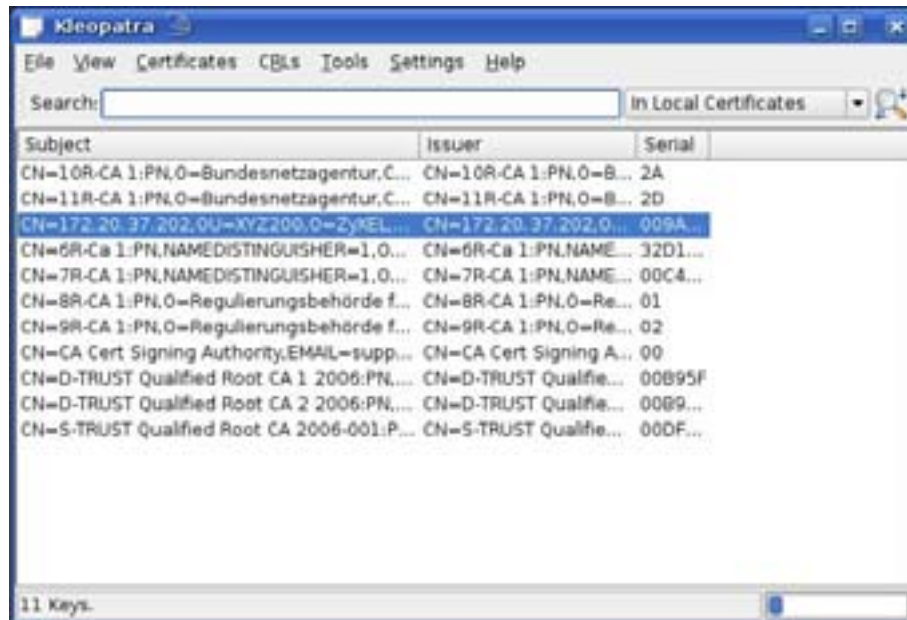
- 2 In the **Certificate Import Result - Kleopatra** dialog box, click **OK**.

**Figure 168** Konqueror 3.5: Certificate Import Result



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

**Figure 169** Konqueror 3.5: Kleopatra



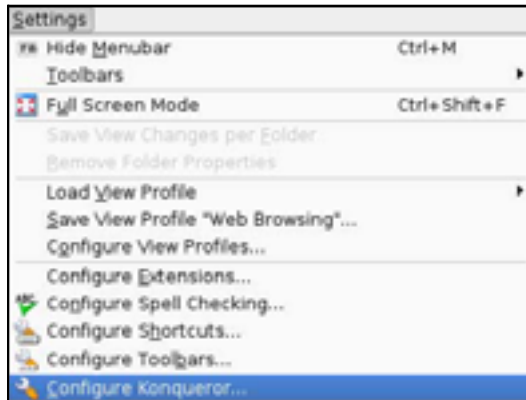
- 3 The next time you visit the web site, click the padlock in the address bar to open the **KDE SSL Information** window to view the web page's security details.

## Removing a Certificate in Konqueror

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

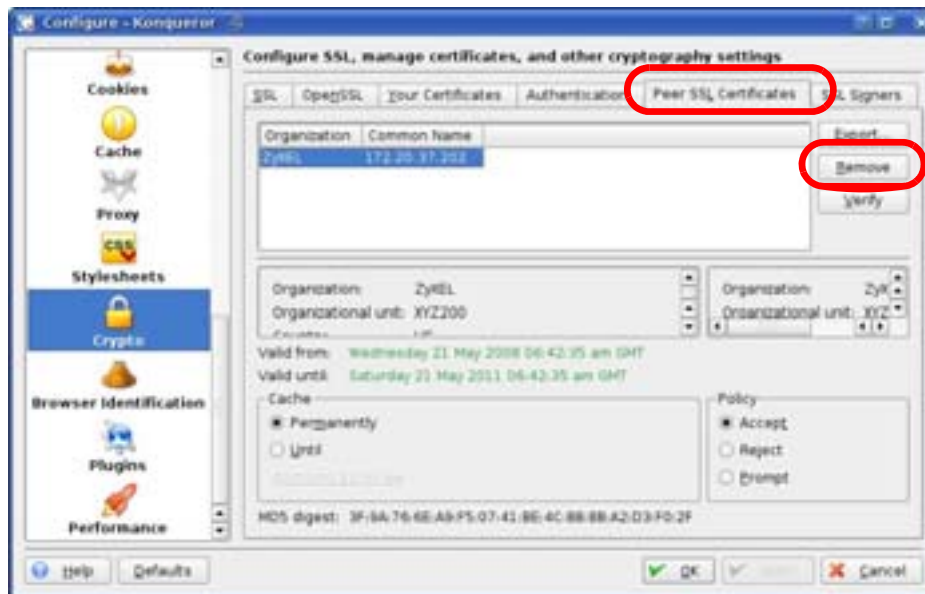
- 1 Open **Konqueror** and click **Settings > Configure Konqueror**.

**Figure 170** 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 171** 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.





# 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 71** 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 <a href="http://www.zyxel.com">www.zyxel.com</a> ) to IP numbers.

**Table 71** Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
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.
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).

**Table 71** Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
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.
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.

**Table 71** Commonly Used Services (continued)

<b>NAME</b>	<b>PROTOCOL</b>	<b>PORT(S)</b>	<b>DESCRIPTION</b>
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.

# Legal Information

## Copyright

Copyright © 2010 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 40 cm must be maintained between the antenna of this device and all persons.

**注意 !**

依據 低功率電波輻射性電機管理辦法

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

本機限在不干擾合法電臺與不受被干擾保障條件下於室內使用。減少電磁波影響，請妥適使用。

## Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

## Viewing Certifications

- 1 Go to <http://www.zyxel.com>.
- 2 Select your product on the ZyXEL home page to go to that product's page.
- 3 Select the certification you wish to view from this page.

## ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

### **Note**

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at [http://www.zyxel.com/web/support\\_warranty\\_info.php](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](http://www.zyxel.com).



# Index

## A

AAA [52](#)  
accounting server  
    see AAA  
activity [52](#)  
Advanced Encryption Standard  
    see AES  
AES [149](#)  
ALG [76](#)  
alternative subnet mask notation [192](#)  
Application Layer Gateway  
    see ALG  
authentication [52](#), [147](#)  
    inner [150](#)  
    key  
    server [52](#)  
    types [150](#)  
authorization [147](#)  
    request and reply [149](#)  
    server [52](#)  
auto-discovery  
    UPnP [97](#)

## B

base station  
    see BS  
BS [51–52](#)  
    links [52](#)

## C

CA [53](#), [54](#)  
CBC-MAC [149](#)  
CCMP [147](#), [149](#)  
cell [51](#)  
certificates [147](#)

CA [53](#)  
    formats [54](#)  
    verification [149](#)  
certification  
    notices [239](#)  
    viewing [239](#)  
Certification Authority, see CA  
chaining [149](#)  
chaining message authentication  
    see CCMP  
CMAC  
    see MAC  
copyright [237](#)  
counter mode  
    see CCMP  
coverage area [51](#)  
cryptography [147](#)

## D

data [147–149](#)  
    decryption [147](#)  
    encryption [147](#)  
    flow [149](#)  
DHCP [73](#)  
    server [73](#)  
diameter [52](#)  
digital ID [54](#), [147](#)  
Dynamic Host Configuration Protocol  
    see DHCP

## E

EAP [52](#)  
EAP (Extensible Authentication Protocol) [54](#)  
EAP-TLS [54](#)  
EAP-TTLS [54](#)  
encryption [147–149](#)

traffic [149](#)  
Ethernet  
  encapsulation [75](#)  
Extensible Authorization Protocol  
  see EAP

## F

FCC interference statement [238](#)  
firewall [105](#)  
FTP [111](#)  
  restrictions [111](#)

## I

IANA [198](#)  
identity [52](#), [147](#)  
idle timeout [112](#)  
IEEE 802.16 [51](#), [147](#)  
IEEE 802.16e [51](#)  
IGD 1.0 [77](#)  
inner authentication [150](#)  
Internet  
  access [52](#)  
  gateway device [77](#)  
Internet Assigned Numbers Authority  
  see IANA [198](#)  
interoperability [51](#)

## K

key [147](#)  
  request and reply [149](#)

## M

MAC [149](#)  
MAN [51](#)  
Management Information Base (MIB) [114](#)  
Message Authentication Code

  see MAC  
message integrity [149](#)  
Metropolitan Area Network  
  see MAN  
microwave [51](#), [52](#)  
mobile station  
  see MS  
MS [52](#)

## N

NAT [197](#)  
  and remote management [112](#)  
  server sets [75](#)  
  traversal [77](#)  
network  
  activity [52](#)  
  services [52](#)

## P

pattern-spotting [149](#)  
PKMv2 [52](#), [147](#), [150](#)  
plain text encryption [149](#)  
Privacy Key Management  
  see PKM  
private key [147](#)  
product registration [240](#)  
public certificate [149](#)  
public key [147](#)

## R

RADIUS [52](#), [54](#), [148](#)  
  Message Types [148](#)  
  Messages [148](#)  
  Shared Secret Key [148](#)  
registration  
  product [240](#)  
related documentation [3](#)  
remote management and NAT [112](#)  
remote management limitations [111](#)

**S**

- safety warnings [7](#)
- secure communication [147](#)
- secure connection [52](#)
- security [147](#)
- security association [149](#)
  - see SA
- services [52](#)
- SIP
  - ALG [76](#)
  - Application Layer Gateway, see ALG
- SNMP [112](#)
  - manager [114](#)
- SS [51](#), [52](#)
- subnet [189](#)
  - mask [190](#)
- subnetting [192](#)
- subscriber station
  - see SS
- syntax conventions [5](#)
- system timeout [112](#)

**T**

- tampering
- TCP/IP configuration [73](#)
- TEK [149](#)
- TFTP restrictions [111](#)
- TLS [147](#)
- transport encryption key
  - see TEK
- transport layer security
  - see TLS
- trigger port forwarding
  - process [92](#)
- TTLS [147](#), [150](#)
- tunneled TLS
  - see TTLS

**U**

- unauthorized device [147](#)
- Universal Plug and Play
  - see UPnP
- UPnP [76](#)
  - application [77](#)
  - auto-discovery [97](#)
  - security issues [77](#)
  - Windows XP [95](#)
- user authentication [147](#)

**V**

- verification [149](#)

**W**

- WiMAX [51–52](#)
  - security [149](#)
  - WiMAX Forum [51](#)
- Wireless Interoperability for Microwave Access
  - see WiMAX
- Wireless Metropolitan Area Network
  - see MAN
- wireless network
  - access [51](#)
  - standard [51](#)
- wireless security [147](#)
- wizard setup [23](#)





