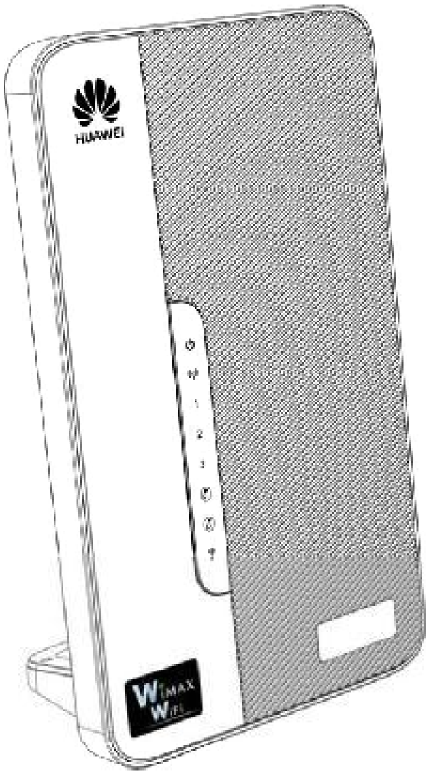
BM2022w, HES-209M2W

WiMAX IEEE 802.16 Indoor WiFi CPE

Tradmark	Model
Huawei	BM2022w
Mitrastar	HES-209M2W

User's Guide



Default Login Details

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

Software Version 2.00
Edition 1, 11/2011

www.huawei.com

HUAWEI

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the BM2022w using the Web Configurator. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

Related Documentation

- Quick Start Guide

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

  Refer to the included CD for support documents.
- Huawei Web Site

  Please refer to www.huawei.com for additional support documentation and product certifications.

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 BM2022w.

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

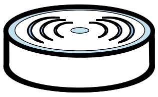
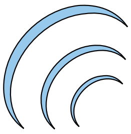
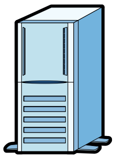
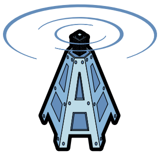
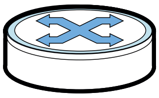
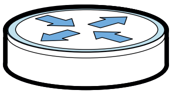
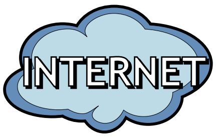
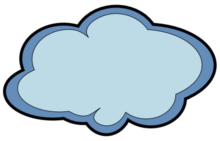
Syntax Conventions

- The product(s) described in this book may be referred to as the "BM2022w", 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 BM2022w icon is not an exact representation of your product.

Table 1 Common Icons

BM2022w 	Computer 	Wireless Signal 
Notebook 	Server 	Base Station 
Telephone 	Switch 	Router 
Internet Cloud  	Network Cloud 	

Safety Warnings

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

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

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

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

Contents Overview

Table of Contents

Chapter 9

Chapter 10

Chapter 11

Chapter 12

PART I
User's Guide

1

Getting Started

1.1 About Your BM2022w

The BM2022w has a built-in switch and two phone ports. It allows you to access the Internet by connecting to a WiMAX wireless network. You can use a traditional analog telephone to make Internet calls using the BM2022w's Voice over IP (VoIP) communication capabilities.

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

See Chapter 14 on page 209 for a complete list of features for your model.

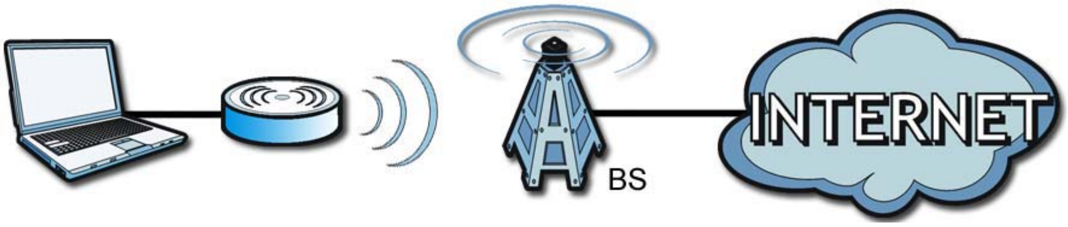
1.1.1 WiMAX Internet Access

Connect your computer or network to the BM2022w for WiMAX Internet access. See the Quick Start Guide for instructions on hardware connection.

In a wireless metropolitan area network (MAN), the BM2022w connects to a WiMAX base station (BS) for Internet access.

The following diagram shows a notebook computer equipped with the BM2022w connecting to the Internet through a WiMAX base station (marked **BS**).

Figure 1 Mobile Station and Base Station



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

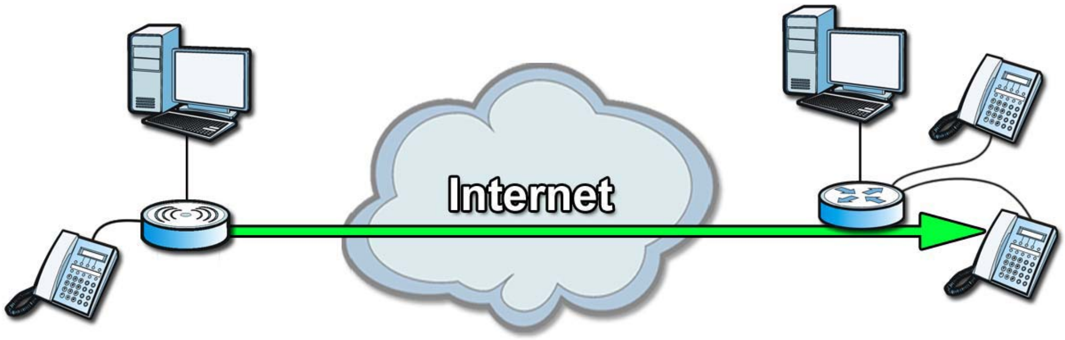
Use content filtering to block access to web sites with URLs containing keywords that you specify. You can define time periods and days during which content filtering is enabled and include or exclude particular computers on your network from content filtering. For example, you could block access to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

1.1.2 Make Calls via Internet Telephony Service Provider

In a home or small office environment, you can use the BM2022w to make and receive the following types of VoIP telephone calls:

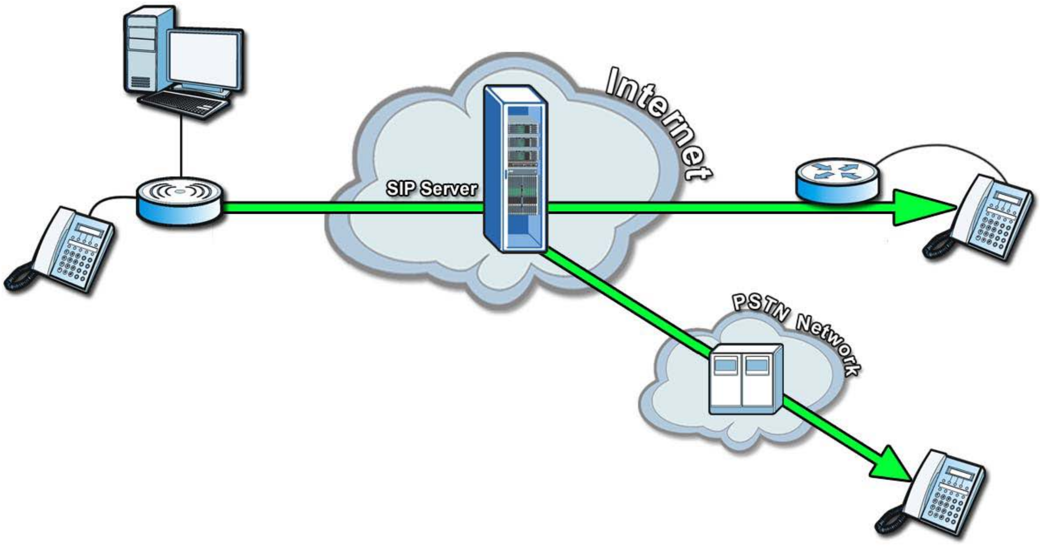
- Peer-to-Peer calls - Use the BM2022w to make a call directly to the recipient's IP address without using a SIP proxy server.

Figure 2 VoIP Features - Peer-to-Peer Calls



- Calls via a VoIP service provider - The BM2022w sends your call to a VoIP service provider's SIP server which forwards your calls to either VoIP or PSTN phones.

Figure 3 Calls via VoIP Service Provider



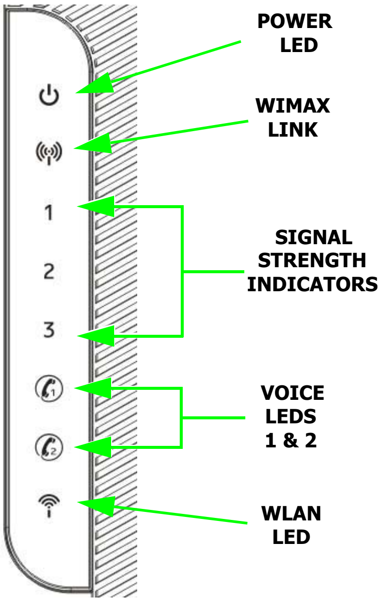
1.2 BM2022w Hardware

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 BM2022w.

Figure 4 The BM2022w's LEDs



The following table describes your BM2022w's LEDs (from top to bottom).

Table 2 The BM2022w LEDs behavior

LED	STATE	DESCRIPTION
Power	Off	The BM2022w is not receiving power.
	Red	The BM2022w is receiving power but has been unable to start up correctly or is not receiving enough power. See the Troubleshooting section for more information.
	Green	**Solid**: The BM2022w is receiving power and functioning correctly. **Flashing**: the device is self-testing (startup)
WiMAX Link	Off	The BM2022w is not connected to a wireless (WiMAX) network.
	Green	The BM2022w is successfully connected to a wireless (WiMAX) network.
	Green (Blinking Slowly)	The BM2022w is searching for a wireless (WiMAX) network.
	Green (Blinking Quickly)	The BM2022w has found a wireless (WiMAX) network and is connecting.
Signal Strength Indicator	The Strength Indicator LEDs display the Interference-plus-Noise Ratio (CINR) of the wireless (WiMAX) connection.	
	Signal 1 On	The signal strength is in the range between 5 and 15.
	Signal 2 On	The signal strength is in the range between 16 and 24.
	Signal 3 On	The signal strength is greater than or equal to 25 dBm

Table 2 The BM2022w LEDs behavior

LED	STATE	DESCRIPTION
Voice 1 & 2	Off	No SIP account is registered, or the BM2022w is not receiving power.
	Green	A SIP account is registered.
	Green (Blinking)	A SIP account is registered, and the phone attached to the VoIP port is in use (off the hook).
	Yellow	A SIP account is registered and has a voice message on the SIP server.
	Yellow (Blinking)	A SIP account is registered and has a voice message on the SIP server, and the phone attached to the VoIP port is in use (off the hook).
WLAN	Off	The Wi-Fi network is not operational.
	Green	The Wi-Fi network is operational.
	Blinking Green	The WiMAX Device is sending and receiving data across the Wi-Fi network.

1.3 Good Habits for Managing the BM2022w

Do the following things regularly to make the BM2022w more secure and to manage the BM2022w 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 BM2022w becomes unstable or even crashes. If you forget your password, you will have to reset the BM2022w to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the BM2022w. You could simply restore your last configuration.

Introducing the Web Configurator

2.1 Overview

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

In order to use the Web Configurator you need to allow:

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

See the Appendix C on page 243 for more information on configuring your web browser.

2.1.1 Accessing the Web Configurator

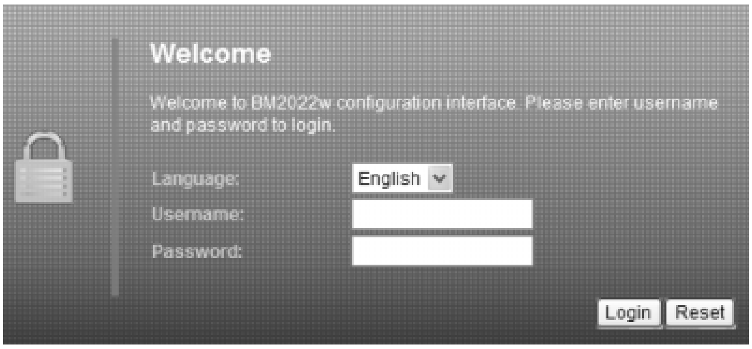
1 Make sure your BM2022w hardware is properly connected (refer to the Quick Start Guide for more information).

2 Launch your web browser.

3 Enter 192.168.1.1192.168.1.1" as the URL.

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

Figure 5 Login screen



Welcome

Welcome to BM2022w configuration interface. Please enter username and password to login.

Language: English

Username:

Password:

Note: For security reasons, the BM2022w 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".

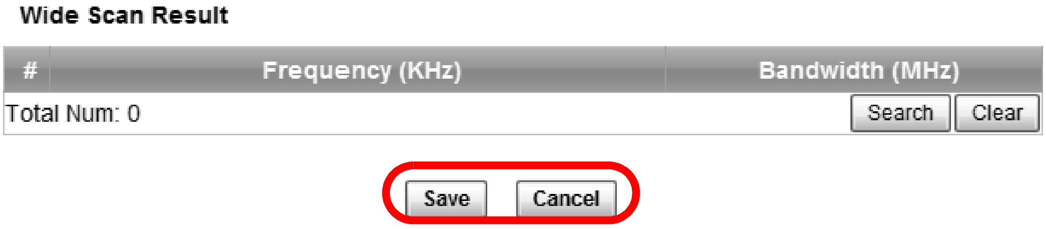
2.1.2.1 Using The Reset Button

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 BM2022w 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 BM2022w, you can cancel those changes and start over.

Figure 6 Saving and Canceling Changes



Wide Scan Result

#	Frequency (KHz)	Bandwidth (MHz)
Total Num: 0		

This screen contains the following fields:

Table 3 Saving and Canceling Changes

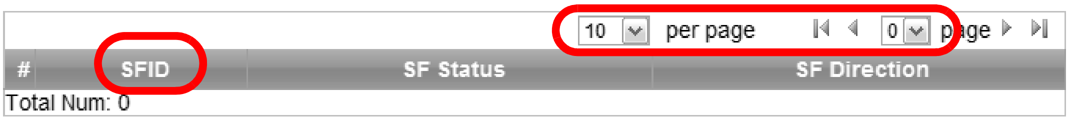
LABEL	DESCRIPTION
Save	Click this to save your changes.
Cancel	Click this to restore the settings on this page to their last saved values.

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 BM2022w contain tables to provide information or additional configuration options.

Figure 7 Tables Example



This screen contains the following fields:

Table 4 Saving and Canceling Changes

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

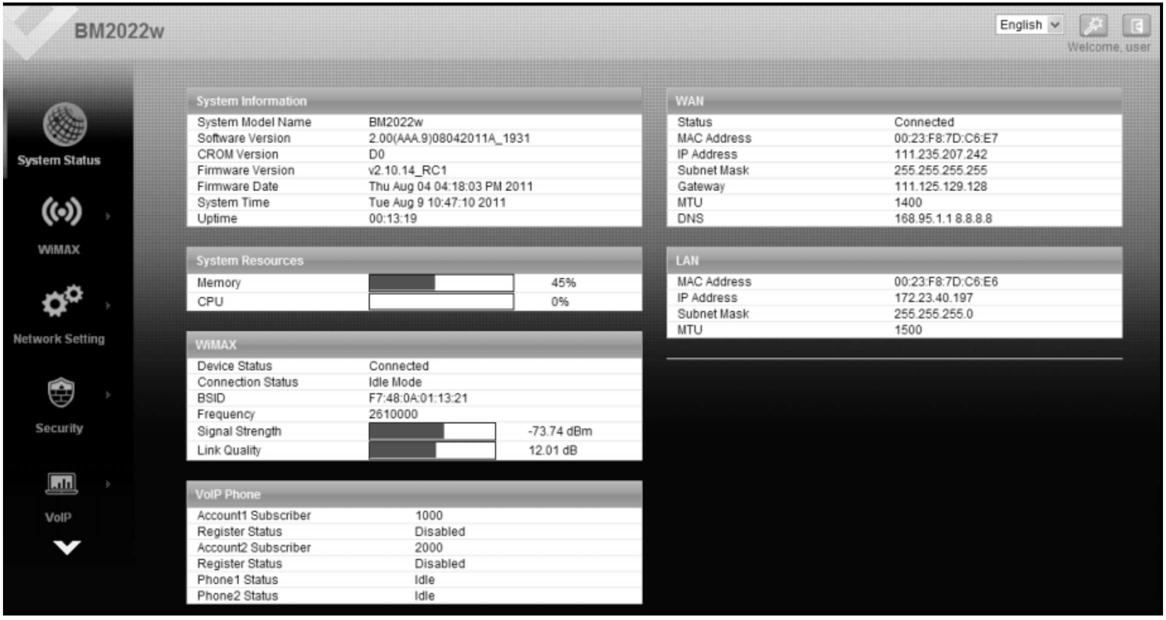
2.2 The Main Screen

When you first log into the Web Configurator, the Main screen appears. Here you can view a summary of your BM2022w'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.

Note: The available menus and screens vary depending on the user account you use for login.

Figure 8 Main Screen



System Information

System Model Name	BM2022w
Software Version	2.00(AAA.9)08042011A_1931
CROM Version	D0
Firmware Version	v2.10.14_RC1
Firmware Date	Thu Aug 04 04:18:03 PM 2011
System Time	Tue Aug 9 10:47:10 2011
Uptime	00:13:19

System Resources

Memory	45%
CPU	0%

WiMAX

Device Status	Connected
Connection Status	Idle Mode
BSID	F7:48:0A:01:13:21
Frequency	2610000
Signal Strength	-73.74 dBm
Link Quality	12.01 dB

VoIP Phone

Account1 Subscriber	1000
Register Status	Disabled
Account2 Subscriber	2000
Register Status	Disabled
Phone1 Status	Idle
Phone2 Status	Idle

WAN

Status	Connected
MAC Address	00:23:F8:7D:C6:E7
IP Address	111.235.207.242
Subnet Mask	255.255.255.255
Gateway	111.125.129.128
MTU	1400
DNS	168.95.1.1 8.8.8.8

LAN

MAC Address	00:23:F8:7D:C6:E6
IP Address	172.23.40.197
Subnet Mask	255.255.255.0
MTU	1500

The following table describes the icons in this screen.

Table 5 Main > Icons

ICON	DESCRIPTION
System Status	System Status Click this to open the Main screen, which shows your BM2022w status and other information.
WiMAX	WiMAX Click this to open the WiMAX menu, which gives you options for configuring your WiMAX settings.
Network Setting	Network Setting Click this to open the Network menu, which gives you options for configuring your network settings.
Security	Security Click this to open the Security menu, which gives you options for configuring your firewall and security settings.
VoIP	VoIP Click this icon to open the VoIP menu, which gives you options on how to use the device to make phone calls.

Table 5 Main > Icons (continued)

ICON	DESCRIPTION
Maintenance	Maintenance Click this to open the Maintenance menu, which gives you options for maintaining your BM2022w and performing basic network connectivity tests.
English ▾	Language Use this menu to select the Web Configurator’s language.
🪄	Setup Wizard Click this to open the Setup Wizard, where you can configure the most essential settings for your BM2022w to work.
⇦	Logout Click this to log out of the Web Configurator.

Setup Wizard

3.1 Overview

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

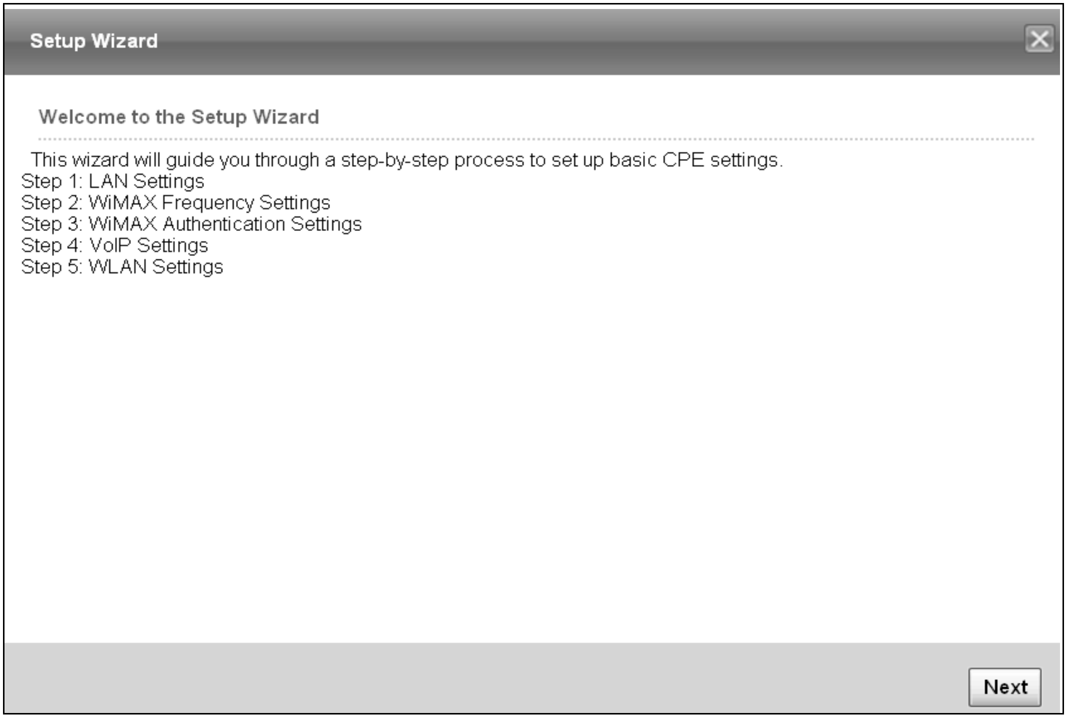
3.1.1 Welcome to the Setup Wizard

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

1. Set up your Local Area Network (LAN) options, which determine how the devices in your home or office connect to the BM2022w.
2. Set up your BM2022w's broadcast frequency, which is the radio channel it uses to communicate with the ISP's base station.
3. Set up your BM2022w's login options, which are used to connect your LAN to the ISP's network and verify your account.
4. Set up your BM2022w's VoIP Settings, which will allow you to make calls over the Internet.

5 Set up your BM2022w's WLAN so that other devices, such as a laptop or a smartphone, can connect wirelessly to the Internet using the BM2022w.

Figure 9 Setup Wizard > Welcome



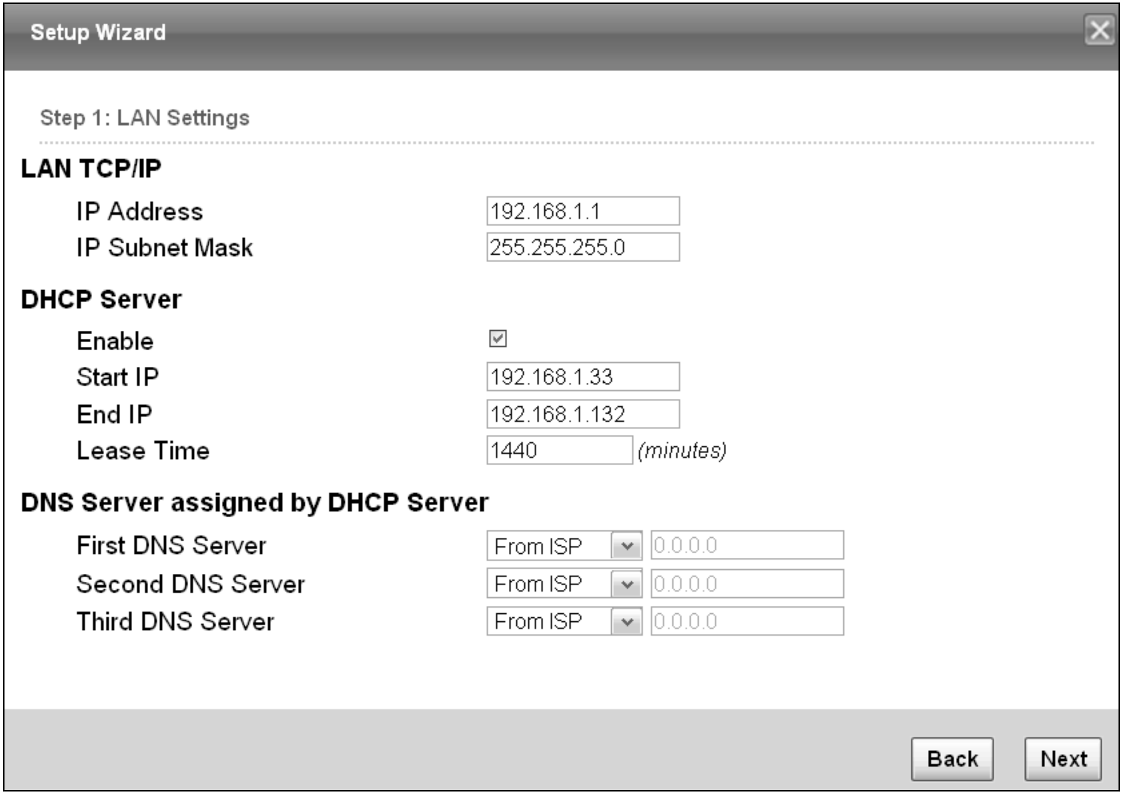
Welcome to the Setup Wizard

This wizard will guide you through a step-by-step process to set up basic CPE settings.
Step 1: LAN Settings
Step 2: WiMAX Frequency Settings
Step 3: WiMAX Authentication Settings
Step 4: VoIP Settings
Step 5: WLAN Settings

3.1.2 LAN Settings

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

Figure 10 Setup Wizard > LAN Settings



Setup Wizard

Step 1: LAN Settings

LAN TCP/IP

IP Address: 192.168.1.1

IP Subnet Mask: 255.255.255.0

DHCP Server

Enable: ☑

Start IP: 192.168.1.33

End IP: 192.168.1.132

Lease Time: 1440 (minutes)

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

The following table describes the labels in this screen.

Table 6 Setup Wizard > LAN Settings

LABEL	DESCRIPTION
LAN TCP/IP	
IP Address	Enter the IP address of the BM2022w on the LAN. Note: This field is the IP address you use to access the BM2022w 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 BM2022w to be the DHCP server on the LAN. As a DHCP server, the BM2022w 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 BM2022w begins allocating IP addresses.
End IP	Enter the IP address at which the BM2022w stops allocating IP addresses.
Lease Time	Enter the duration in minutes before the device requests a new IP address from the DHCP server.

Table 6 Setup Wizard > LAN Settings (continued)

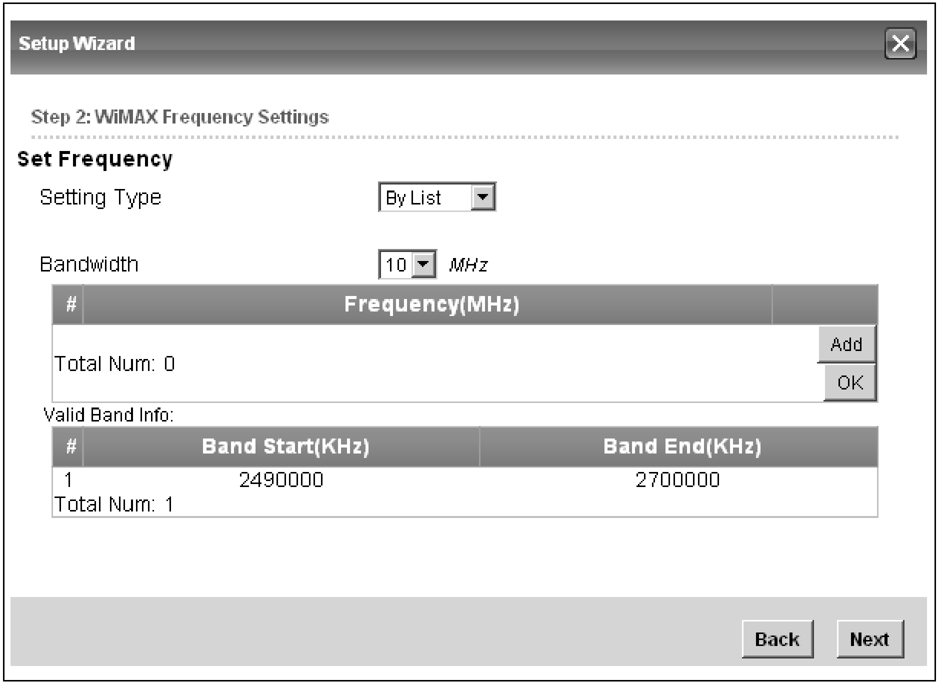
LABEL	DESCRIPTION
DNS Server assigned by DHCP Server	
First DNS Server	Specify the first IP address of three DNS servers that the network can use. The BM2022w provides these IP addresses to DHCP clients.
Second DNS Server	Specify the second IP address of three DNS servers that the network can use. The BM2022w 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 BM2022w 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 BM2022w.

Note: These settings should be provided by your ISP.

Figure 11 Setup Wizard > WiMAX Frequency Settings



Setup Wizard

Step 2: WiMAX Frequency Settings

Set Frequency

Setting Type: By List

Bandwidth: 10 MHz

#	Frequency(MHz)	
Total Num: 0		

Valid Band Info:

#	Band Start(KHz)	Band End(KHz)
1	2490000	2700000
Total Num: 1		

The following table describes the labels in this screen.

Table 7 Setup Wizard > WiMAX Frequency Settings

LABEL	DESCRIPTION
Setting Type	Select the WiMAX frequency setting type from the list. • **By Range** - Select this to set up the frequency based on a range of MHz. • **By List** - Select this to set up the frequency on an individual MHz basis. You can add multiple MHz values to the list.
Step	Enter the increments in MHz by which to increase the frequency range. Note: This field only appears when you select **By Range** under **Setting Type**.
Start Frequency	Enter the frequency value at the beginning of the frequency range to use. The frequency is increased in increments equal to the **Step** value until the **End Frequency** is reached, at which time the cycle starts over with the **Start Frequency**. Note: This field only appears when you select **By Range** under **Setting Type**.
End Frequency	Enter the frequency value at the end of the frequency range to use. Note: This field only appears when you select **By Range** under **Setting Type**.
Bandwidth	Set the frequency bandwidth in MHz that this BM2022w 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.

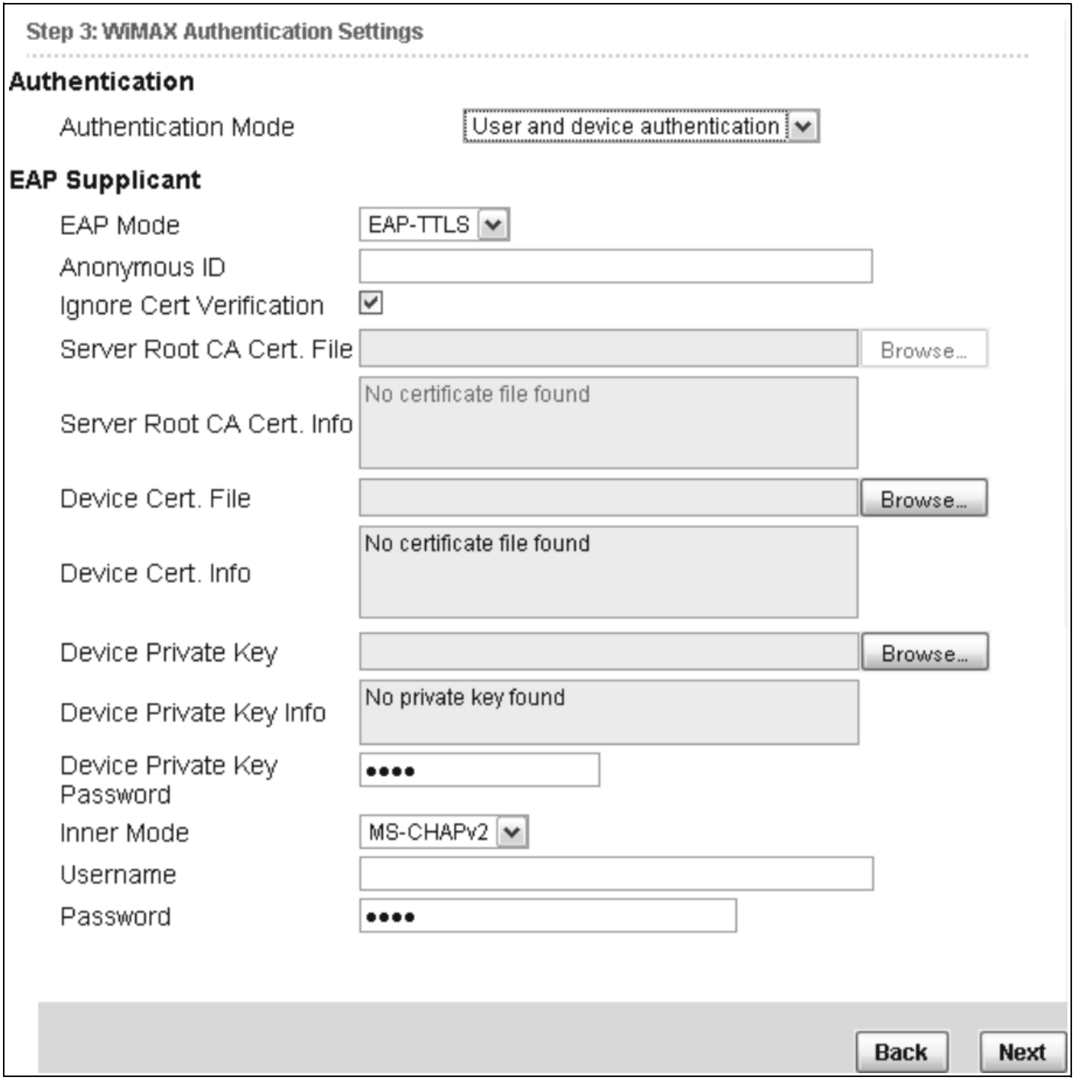
3.1.4 WiMAX Authentication Settings

The WiMAX Authentication Settings screen allows you to configure how your BM2022w logs into the service provider’s network.

Note: These settings should be provided by your ISP.

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

Figure 12 Setup Wizard > WiMAX Authentication Settings



Step 3: WiMAX Authentication Settings

Authentication

Authentication Mode: User and device authentication

EAP Supplicant

EAP Mode: EAP-TTLS

Anonymous ID:

Ignore Cert Verification: ☑

Server Root CA Cert. File:

Server Root CA Cert. Info: No certificate file found

Device Cert. File:

Device Cert. Info: No certificate file found

Device Private Key:

Device Private Key Info: No private key found

Device Private Key Password: ●●●●

Inner Mode: MS-CHAPv2

Username:

Password: ●●●●

The following table describes the labels in this screen.

Table 8 Setup Wizard > WiMAX Authentication Settings

LABEL	DESCRIPTION
Authentication	
Authentication Mode	Select a WiMAX authentication mode for authentication network sessions with the ISP. Options are: • No authentication • User authentication • Device authentication • User and Device authentication
EAP Supplication	
EAP Mode	Select an EAP authentication mode. See Table 15 on page 78 if you need more information.

Table 8 Setup Wizard > WiMAX Authentication Settings (continued)

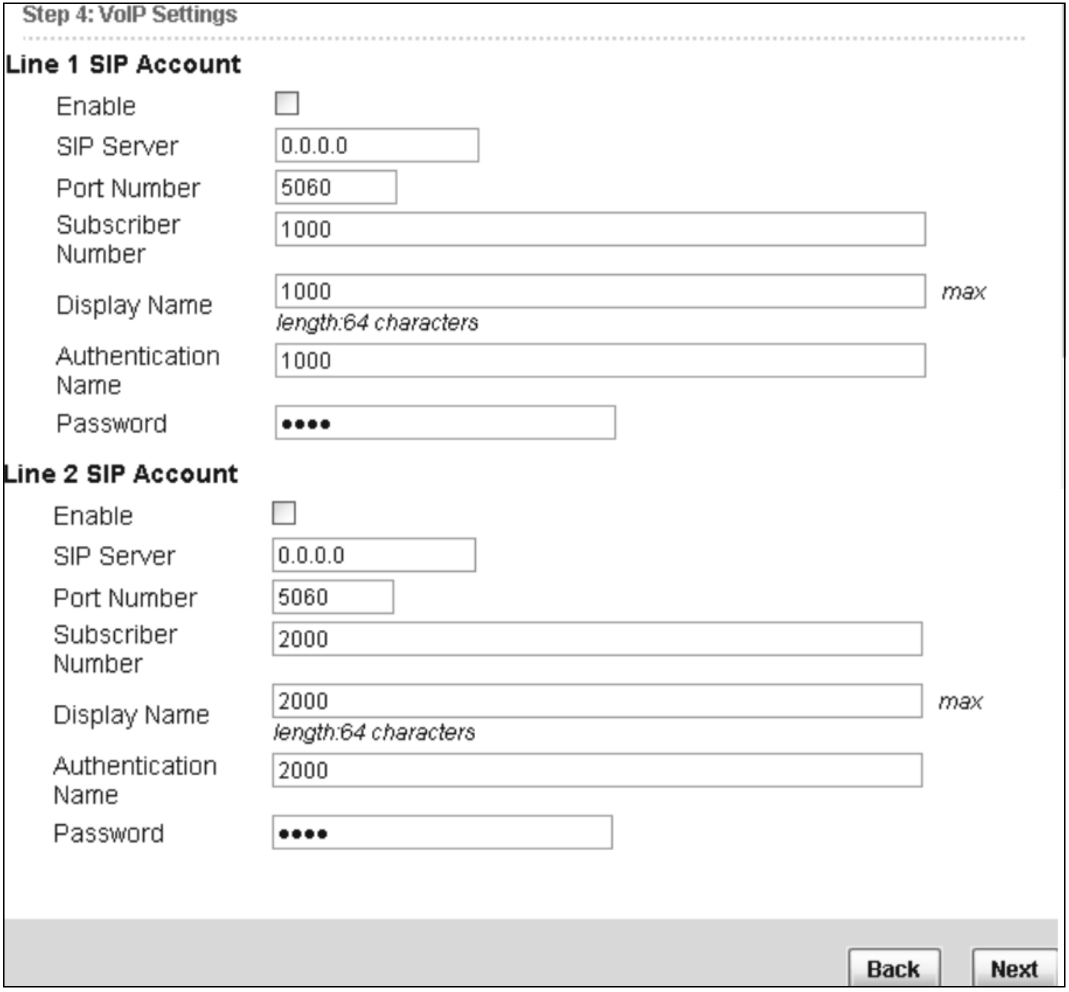
LABEL	DESCRIPTION
Anonymous Id	Enter your anonymous ID. Note: Some modes may not require this.
Ignore Cert Verification	Select this to ignore base station certification verification when a certificate is received during EAP-TLS or EAP-TTLS.
Server Root CA Cert. File	Browse for and choose a server root certificate file, if required.
Server Root CA Cert. Info	This field displays information about the assigned server root certificate.
Device Cert. File	Browse for and choose a device certificate file, if required. Before you import certificate from WebGUI, the certificate file must be signed by chipset vendor due to security reason.
Device Cert. Info.	This field displays information about the assigned device certificate.
Device Private Key	Browse for and choose a device private key, if required.
Device Private Key Info	This field displays information about the assigned device private key.
Device Private Key Password	Enter the device private key, if required.
Inner Mode	Select an inner authentication mode (MS-CHAP, MS-CHAPV2, CHAP, MD5, PAP). See Table 15 on page 78 if you need more information.
Username	Enter your authentication username.
Password	Enter your authentication password.
Back	Click to display the previous screen.
Next	Click to proceed to the next screen.

3.1.5 VoIP Settings

The VoIP Settings screen allows you to configure how your BM2022w connects to up to two VoIP service providers’ network and makes calls over the Internet.

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

Figure 13 Setup Wizard > VoIP Settings



Step 4: VoIP Settings

Line 1 SIP Account

Enable	□
SIP Server	0.0.0.0
Port Number	5060
Subscriber Number	1000
Display Name	1000 max length:64 characters
Authentication Name	1000
Password	●●●●

Line 2 SIP Account

Enable	□
SIP Server	0.0.0.0
Port Number	5060
Subscriber Number	2000
Display Name	2000 max length:64 characters
Authentication Name	2000
Password	●●●●

The following table describes the labels in this screen.

Table 9 Setup Wizard > VoIP Settings

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

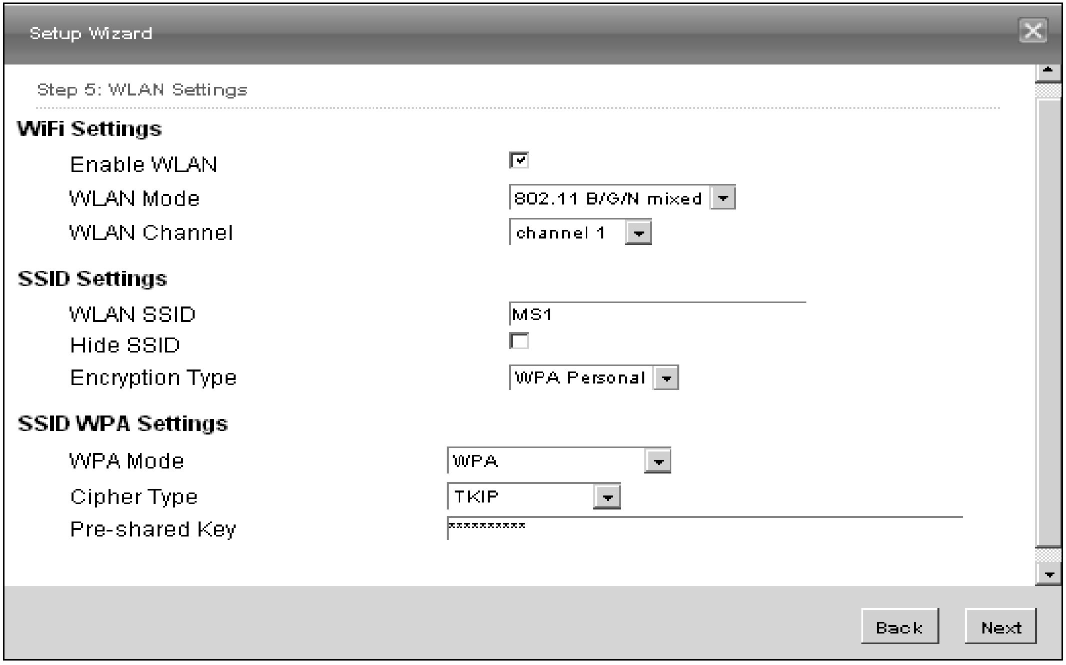
Table 9 Setup Wizard > VoIP Settings (continued)

LABEL	DESCRIPTION
Back	Click to display the previous screen.
Next	Click to proceed to the next screen.

3.1.6 WLAN Settings

The WLAN Settings screen lets you set up how other devices connect to the Internet wirelessly using the BM2022w.

Figure 14 Setup Wizard > WLAN Settings



Setup Wizard

Step 5: WLAN Settings

WiFi Settings

- Enable WLAN ☑
- WLAN Mode: 802.11 B/G/N mixed
- WLAN Channel: channel 1

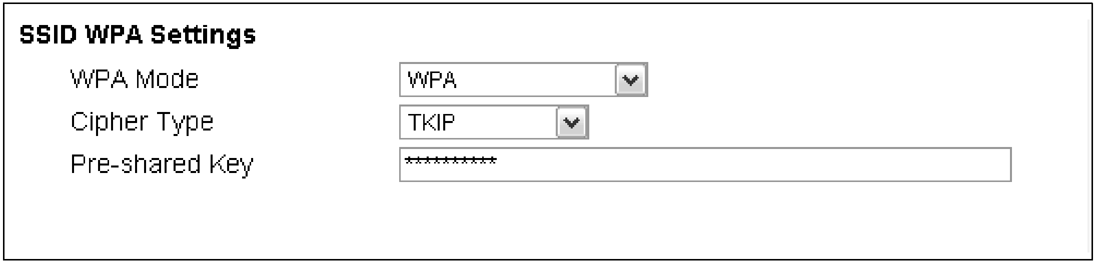
SSID Settings

- WLAN SSID: MS1
- Hide SSID ☐
- Encryption Type: WPA Personal

SSID WPA Settings

- WPA Mode: WPA
- Cipher Type: TKIP
- Pre-shared Key: **********

Figure 15 Setup Wizard > WLAN Settings > Encryption Type: WPA Personal



SSID WPA Settings

- WPA Mode: WPA
- Cipher Type: TKIP
- Pre-shared Key: ***********

The following table describes the labels in this screen.

Table 10 Setup Wizard > WLAN Settings

LABEL	DESCRIPTION
WiFi Settings	
Enable WLAN	Select this box to enable the wireless service and allow other wireless clients to connect to the Internet using the BM2022w.

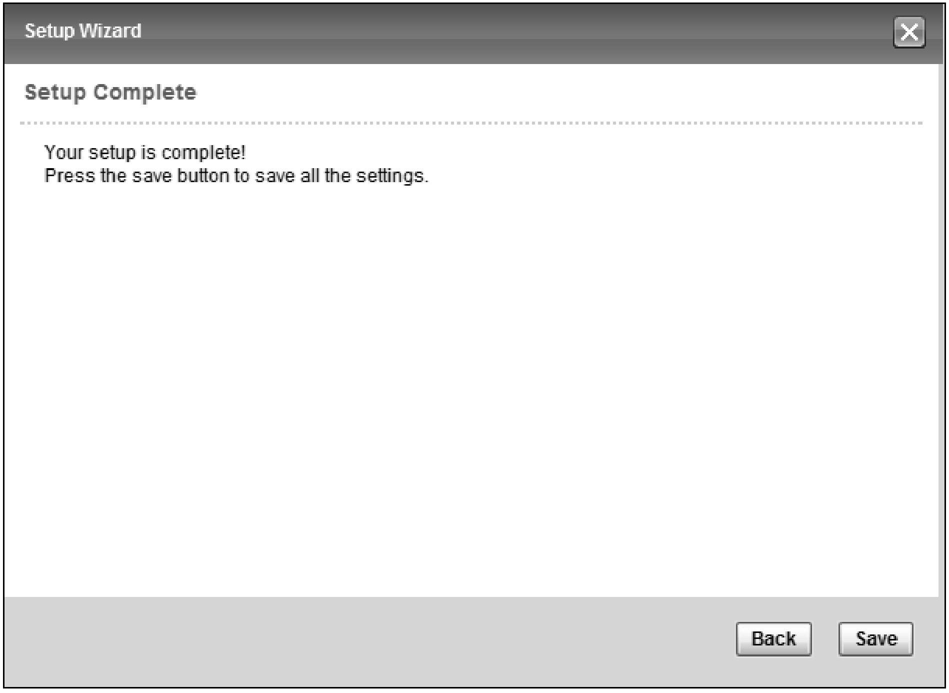
Table 10 Setup Wizard > WLAN Settings (continued)

LABEL	DESCRIPTION
WLAN Mode	Select the mode that the BM2022w will be using to communicate: 802.11 B/G/N mixed, 802.11 B/G mixed, 802.11 B only, 802.11 G only, or 802.11 N only.
WLAN Channel	Select one channel from 1 to 11 for wireless communications with the wireless stations.
SSID Settings	
WLAN SSID	This field displays the name of the wireless network associated with the BM2022w.
Hide SSID	Select this option if you wish to keep the name of the wireless network hidden.
Encryption Type	Select the type of encryption that the network will be using: None, WEP, or WPA Personal.
SSID WEP Settings Note: You will only see this options if you selected WEP as the Encryption Type.	
Authentication Method	Select the type of authentication used to join the network: Open System or Shared Key.
WEP Encryption Length	Select the length of the encryption key: 64-bit or 128-bit.
Key 1 - 4	Pick one of four available keys. The key can be in either Hexadecimal (HEX) or ASCII format. Type the key using any letters and numbers. The field is case sensitive and the length must match the length picked in the step above (64-bit or 128-bit). A warning me sage will appear if you fail to do this.
SSID WPA Settings	
WPA Mode	Select either WPA, WPA2 or Auto (WPA or WPA2).
Cipher Type	Select the type of authentication that you wish to use for your network: TKIP, AES or both. AES is more secure.
Pre Shared Key	Type the pre-shared key or PSK previously shared between the two parties.

3.1.7 Setup Complete

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

Figure 16 Setup Wizard > Setup Complete



Your setup is complete!
Press the save button to save all the settings.

Launch your web browser and navigate to www.huawei.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 BM2022w features available in the more advanced web configurator.

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

4

Tutorials

4.1 Overview

This chapter shows you how to configure some of the BM2022w's features.

Note: Be sure to read Introducing the Web Configurator on page 21 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 39
- Configuring LAN DHCP on page 40
- Changing Certificate on page 42
- Blocking Web Access on page 43
- Configuring the MAC Address Filter, see page 43
- Setting Up NAT Port Forwarding, see page 45
- Access the BM2022w Using DDNS, see page 47
- Configuring Static Route for Routing to Another Network, see page 49
- Remotely Managing Your BM2022w on page 51
- VLAN Configuration Examples on page 52

4.2 WiMAX Connection Settings

This tutorial provides you with pointers for configuring the BM2022w to connect to an ISP.

1 Connect the BM2022w to the ISP's nearest base station. See Section 6.2 on page 72.

2 Configure the BM2022w's broadcast frequency. Section 6.3 on page 74.

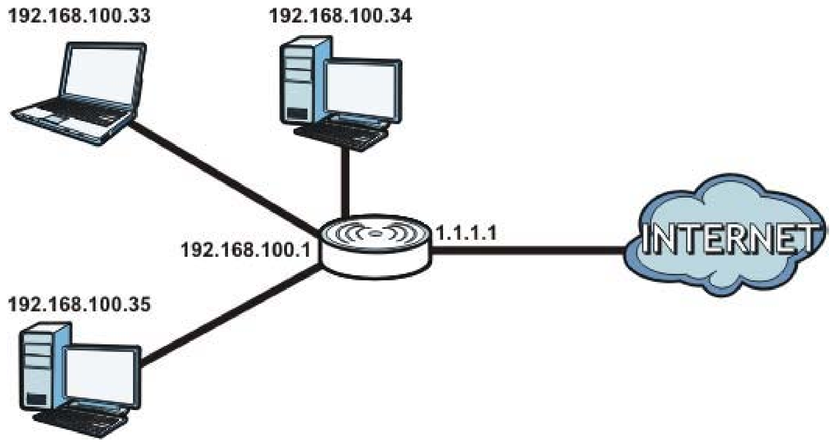
3 Configure the BM2022w to connect securely to the ISP's authentication servers. See Section 6.4 on page 76.

4 Check the BM2022w's connection status to ensure everything is working properly. See Section 6.10 on page 90.

4.3 Configuring LAN DHCP

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

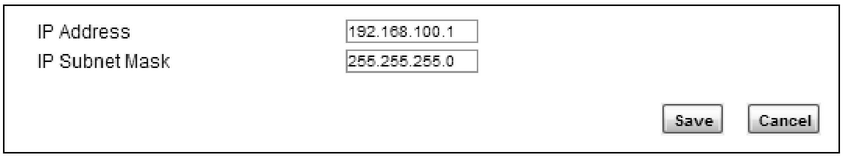
Goal: Connect three computers to your BM2022w to form a small network.



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

INFORMATION	VALUE	SEE ALSO
LAN IP Address	192.168.100.1	Chapter 7 on page 102
Starting IP Address	192.168.100.10	Chapter 7 on page 103
Ending IP Address	192.168.100.30	
DNS Servers	From ISP	

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

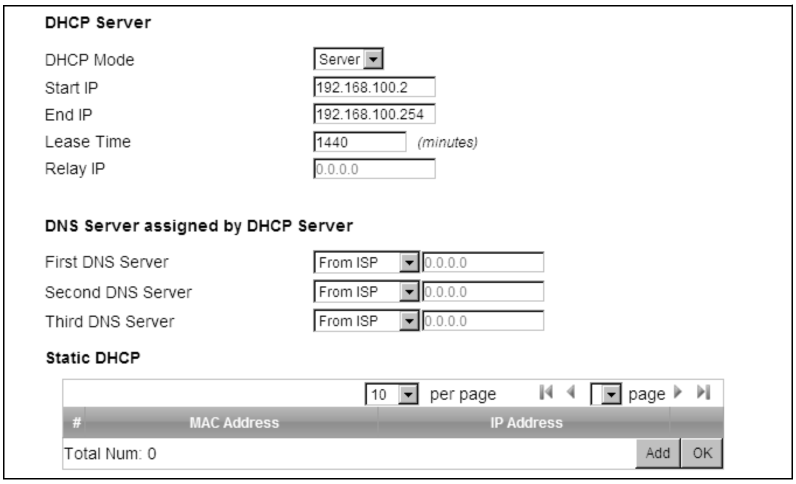


IP Address: 192.168.100.1
IP Subnet Mask: 255.255.255.0

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

3 Type http://192.168.100.1 in your browser after the BM2022w finishes starting up completely.

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



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

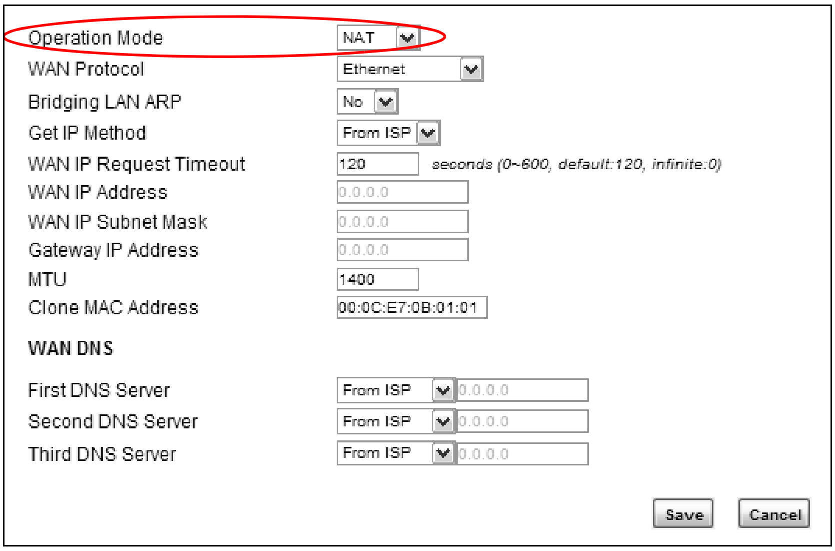
#	MAC Address	IP Address

Total Num: 0

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

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

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



Operation Mode	NAT
WAN Protocol	Ethernet
Bridging LAN ARP	No
Get IP Method	From ISP
WAN IP Request Timeout	120 *seconds (0~600, default:120, infinite:0)*
WAN IP Address	0.0.0.0
WAN IP Subnet Mask	0.0.0.0
Gateway IP Address	0.0.0.0
MTU	1400
Clone MAC Address	00:0C:E7:0B:01:01

WAN DNS

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

8 Connect your computers to the BM2022w'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 219.

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 27), which walks you through the process.

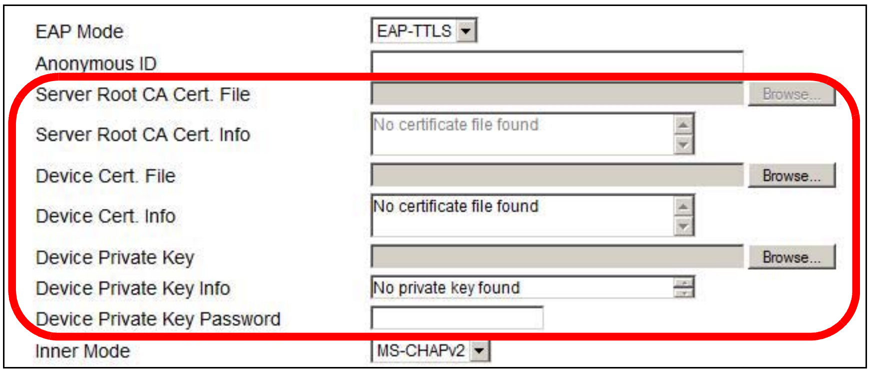
4.4 Changing Certificate

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 BM2022w.

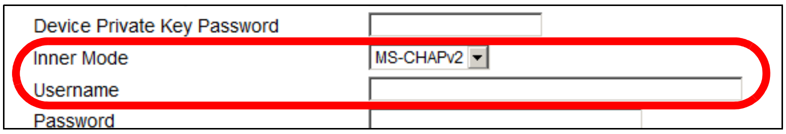
See Also: Appendix E on page 263.

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.



EAP Mode	EAP-TTLS
Anonymous ID	
Server Root CA Cert. File	Browse...
Server Root CA Cert. Info	No certificate file found
Device Cert. File	Browse...
Device Cert. Info	No certificate file found
Device Private Key	Browse...
Device Private Key Info	No private key found
Device Private Key Password	
Inner Mode	MS-CHAPv2

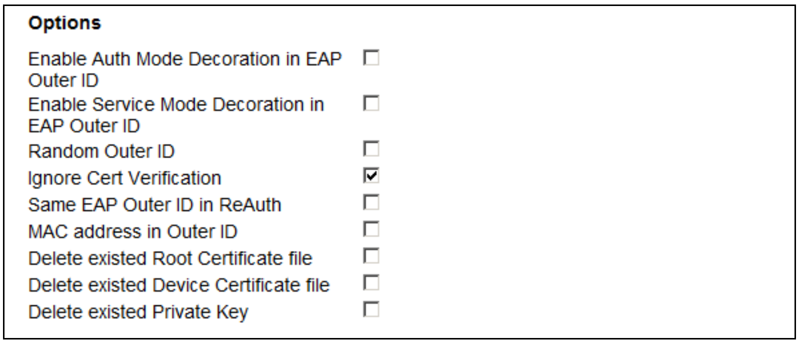
2 Configure your new Internet access settings based on the information provided by the ISP.



Device Private Key Password	
Inner Mode	MS-CHAPv2
Username	
Password	

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	☐
Enable Service Mode Decoration in EAP Outer ID	☐
Random Outer ID	☐
Ignore Cert Verification	☑
Same EAP Outer ID in ReAuth	☐
MAC address in Outer ID	☐
Delete existed Root Certificate file	☐
Delete existed Device Certificate file	☐
Delete existed Private Key	☐

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 BM2022w 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 BM2022w’s content filter to block a website with a domain name www.example.com.

See Also: Section 7.23 on page 126.

1 Open the **Network Setting > Content Filter**.

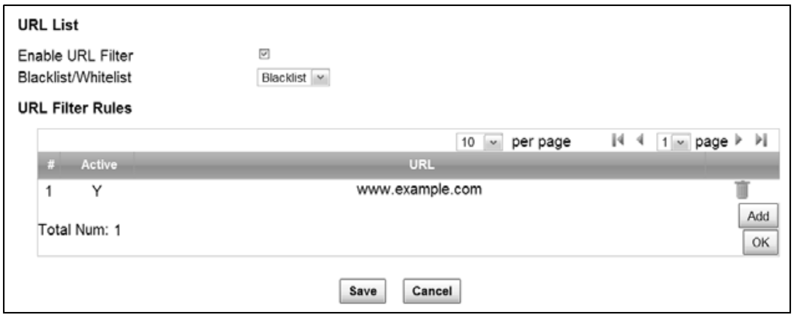
2 Select **Enable URL Filter**.

3 Select **Blacklist**.

4 Click **Add** and configure a URL filter rule by selecting **Active** and entering www.example.com as the URL.

5 Click **OK**.

6 Click **Save**.



URL List

Enable URL Filter ☑

Blacklist/Whitelist Blacklist

URL Filter Rules

#	Active	URL
1	Y	www.example.com

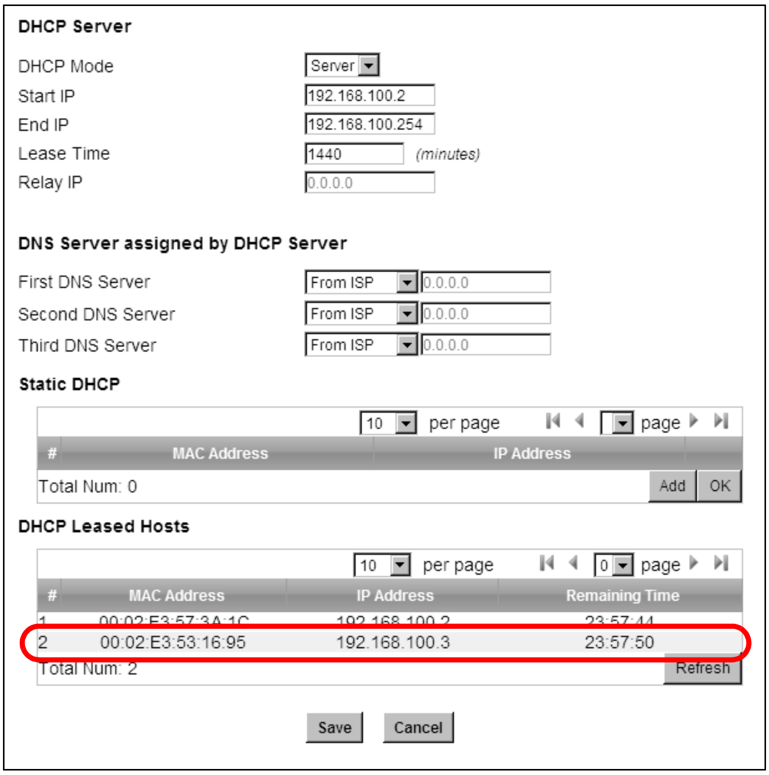
Total Num: 1

Open a browser from your computer in the BM2022w’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

10 per page | page

#	MAC Address	IP Address

Total Num: 0

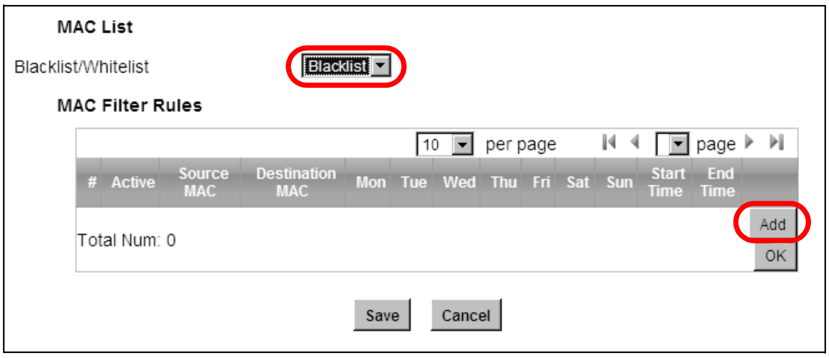
DHCP Leased Hosts

10 per page | 0 page

#	MAC Address	IP Address	Remaining Time
1	00:02:E3:57:3A: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

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



MAC List

Blacklist/Whitelist: Blacklist

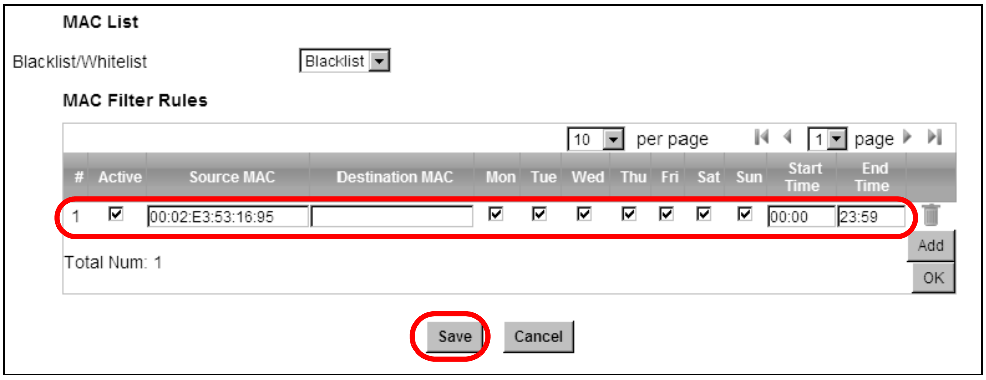
MAC Filter Rules

10 per page | page

#	Active	Source MAC	Destination MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time

Total Num: 0

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



MAC List

Blacklist/Whitelist: Blacklist

MAC Filter Rules

#	Active	Source MAC	Destination MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time
1	☑	00:02:E3:53:16:95		☑	☑	☑	☑	☑	☑	☑	00:00	23:59

Total Num: 1

The computer will no longer be able to access any host on the WiMAX network through the BM2022w.

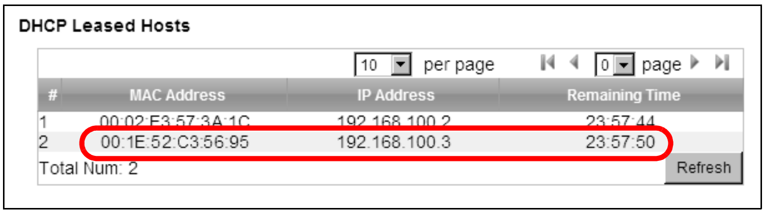
4.7 Setting Up NAT Port Forwarding

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 BM2022w.

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

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

1 You have to know the Xbox 360's IP address first. You can check it through the Xbox 360 console. You may be able to check the IP address on the BM2022w if the BM2022w 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.

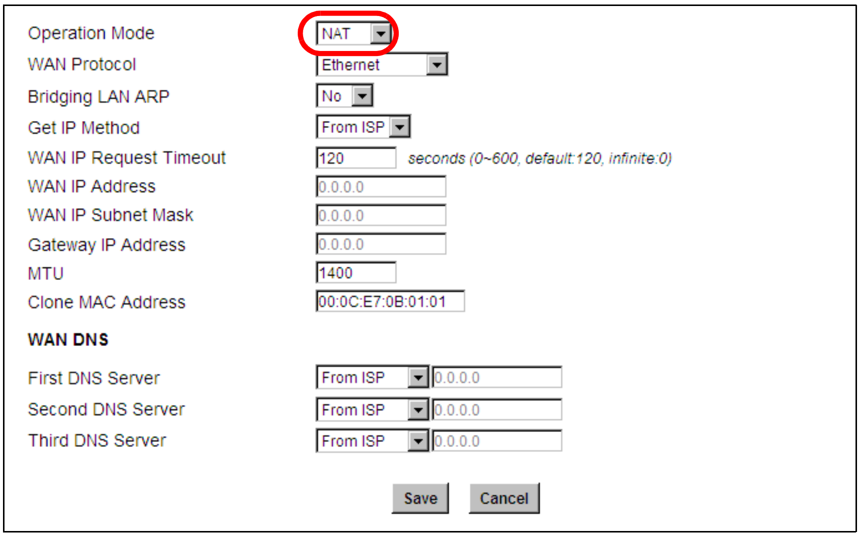


DHCP Leased Hosts

#	MAC Address	IP Address	Remaining Time
1	00:02:E3:57:3A:1C	192.168.100.2	23:57:44
2	00:1E:52:C3:56:95	192.168.100.3	23:57:50

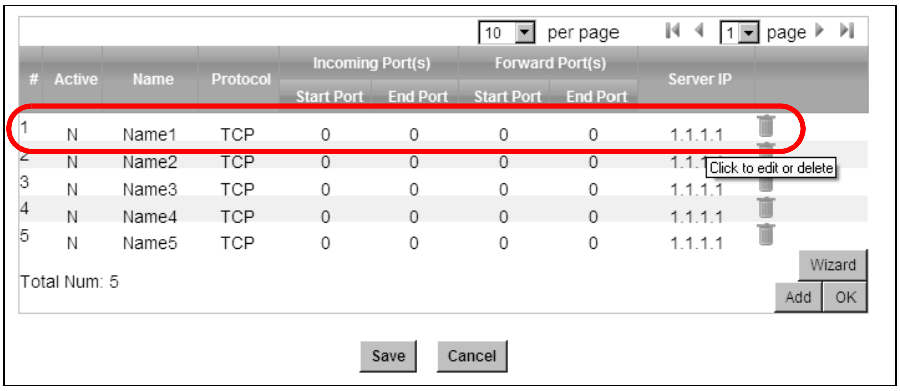
Total Num: 2

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**.



Operation Mode	NAT	
WAN Protocol	Ethernet	
Bridging LAN ARP	No	
Get IP Method	From ISP	
WAN IP Request Timeout	120	*seconds (0~600, default:120, infinite:0)*
WAN IP Address	0.0.0.0	
WAN IP Subnet Mask	0.0.0.0	
Gateway IP Address	0.0.0.0	
MTU	1400	
Clone MAC Address	00:0C:E7:0B:01:01	
WAN DNS		
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

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

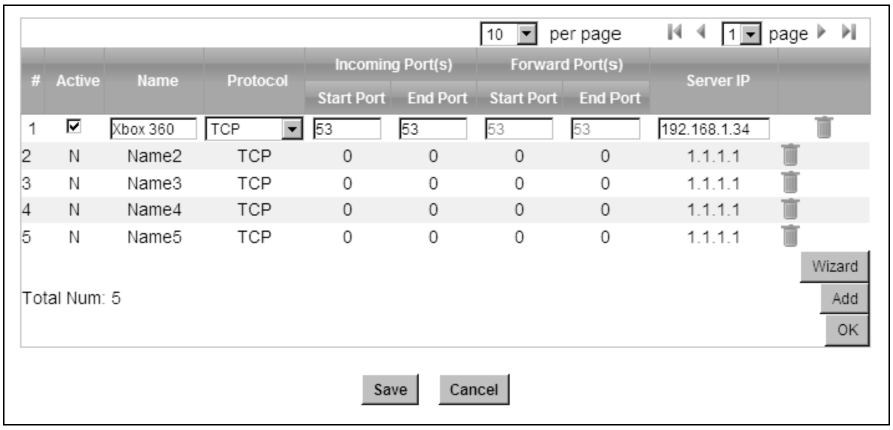


10 per page | 1 page

#	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
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**.

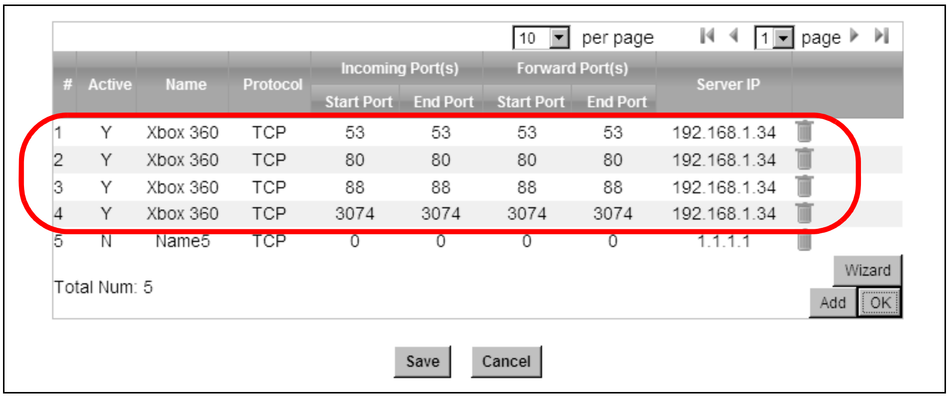


10 per page | 1 page

#	Active	Name	Protocol	Incoming Port(s)		Forward Port(s)		Server IP
				Start Port	End Port	Start Port	End Port	
1	☑	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.



10 per page 1 page

#	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	🗑

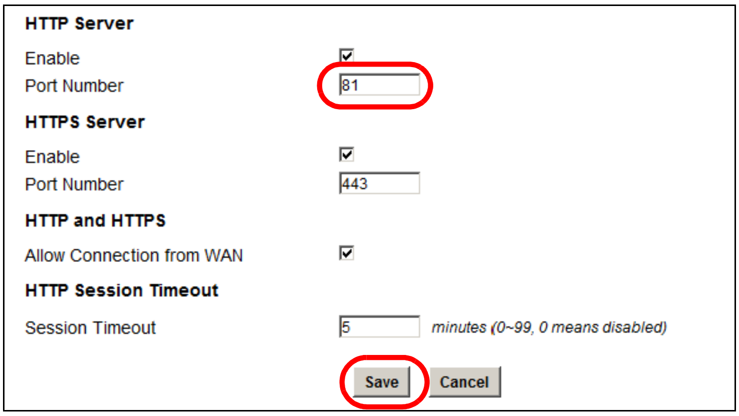
Total Num: 5

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 BM2022w from the Internet, he has to assign an unused port to WWW remote access.

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



HTTP Server

Enable	☑
Port Number	81

HTTPS Server

Enable	☑
Port Number	443

HTTP and HTTPS

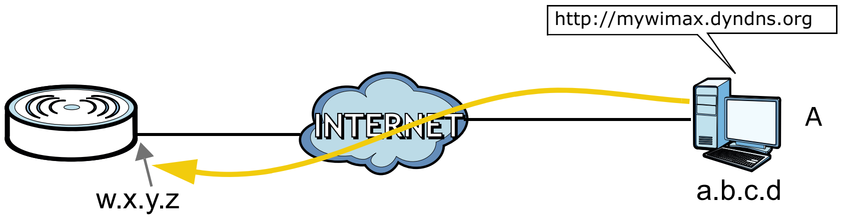
Allow Connection from WAN	☑

HTTP Session Timeout

Session Timeout	5 *minutes (0~99, 0 means disabled)*

4.8 Access the BM2022w Using DDNS

If you connect your BM2022w to the Internet and it uses a dynamic WAN IP address, it is inconvenient for you to manage the device from the Internet. The BM2022w's WAN IP address changes dynamically. Dynamic DNS (DDNS) allows you to access the BM2022w using a domain name.



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

This tutorial covers:

- Registering a DDNS Account on www.dyndns.org
- Configuring DDNS on Your BM2022w
- Testing the DDNS Setting

Note: If you have a private WAN IP address (see Private IP Addresses on page 260), then you cannot use DDNS.

4.8.1 Registering a DDNS Account on www.dyndns.org

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

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

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

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

- Hostname: **mywimax.dyndns.org**
- Service Type: **Host with IP address**
- IP Address: Enter the WAN IP address that your BM2022w is currently using. You can find the IP address on the BM2022w's Web Configurator **Status** page.

Then you will need to configure the same account and host name on the BM2022w later.

4.8.2 Configuring DDNS on Your BM2022w

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

1 Select **Enable Dynamic DNS**.

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

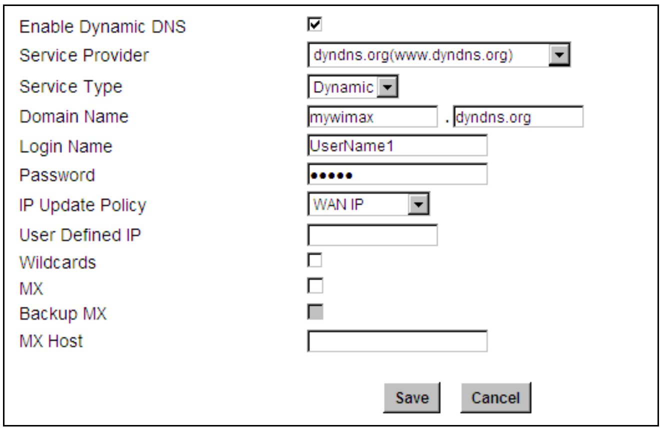
3 Select **Dynamic** for the service type.

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**.



Enable Dynamic DNS	☑
Service Provider	dyndns.org(www.dyndns.org)
Service Type	Dynamic
Domain Name	mywimax . dyndns.org
Login Name	UserName1
Password	●●●●●
IP Update Policy	WAN IP
User Defined IP	
Wildcards	□
MX	□
Backup MX	□
MX Host	

4.8.3 Testing the DDNS Setting

Now you should be able to access the BM2022w 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].

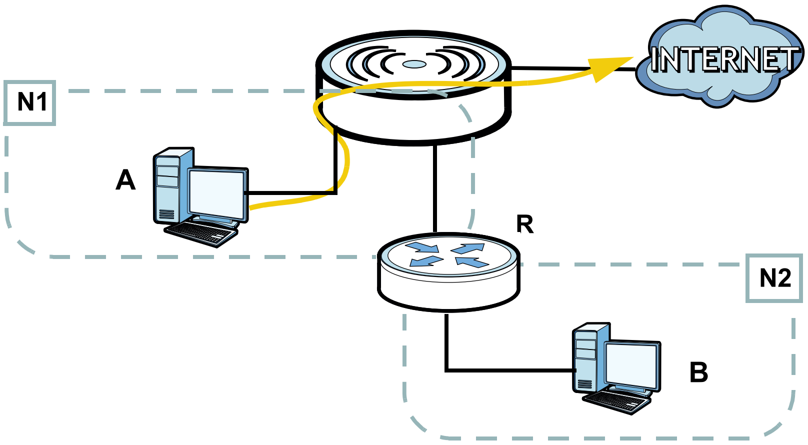
3 The BM2022w's login page should appear. You can then log into the BM2022w and manage it.

4.9 Configuring Static Route for Routing to Another Network

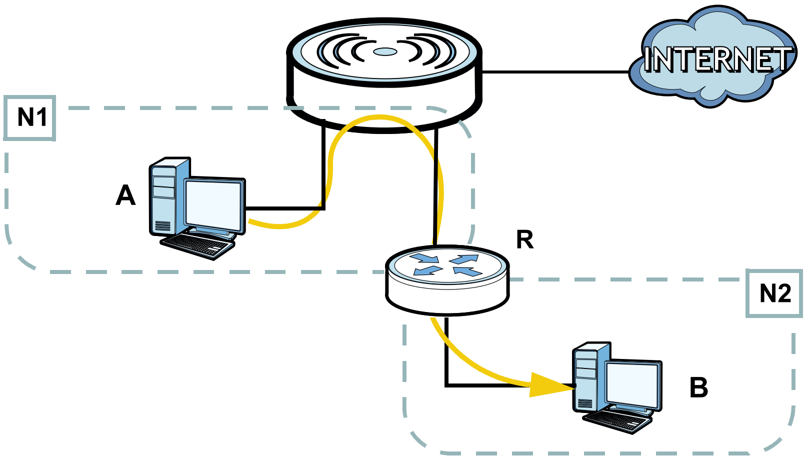
In order to extend your Intranet and control traffic flowing directions, you may connect a router to the BM2022w's LAN. The router may be used to separate two department networks. This tutorial shows how to configure a static routing rule for two network routings.

In the following figure, router **R** is connected to the BM2022w'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 BM2022w'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 BM2022w to specify **R** as the router in charge of forwarding traffic to **N2**. In this case, the BM2022w 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 11 IP Settings in this Tutorial

DEVICE / COMPUTER	IP ADDRESS
The BM2022w's WAN	172.16.1.1
The BM2022w's LAN	192.168.1.1
A	192.168.1.34
R's IP address on N1	192.168.1.253

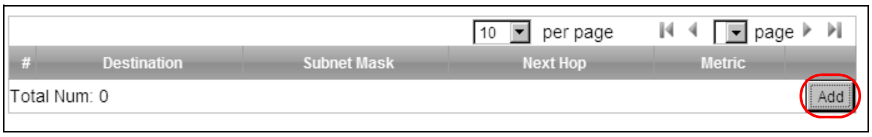
Table 11 IP Settings in this Tutorial

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

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

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

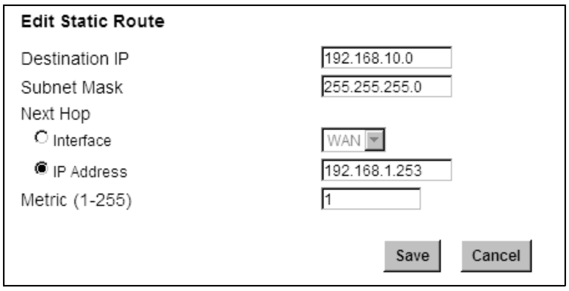
2 Click **Add** to create a new route.



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

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

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



Edit Static Route

Destination IP	192.168.10.0
Subnet Mask	255.255.255.0
Next Hop	
○ Interface	WAN
● IP Address	192.168.1.253
Metric (1-255)	1

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.

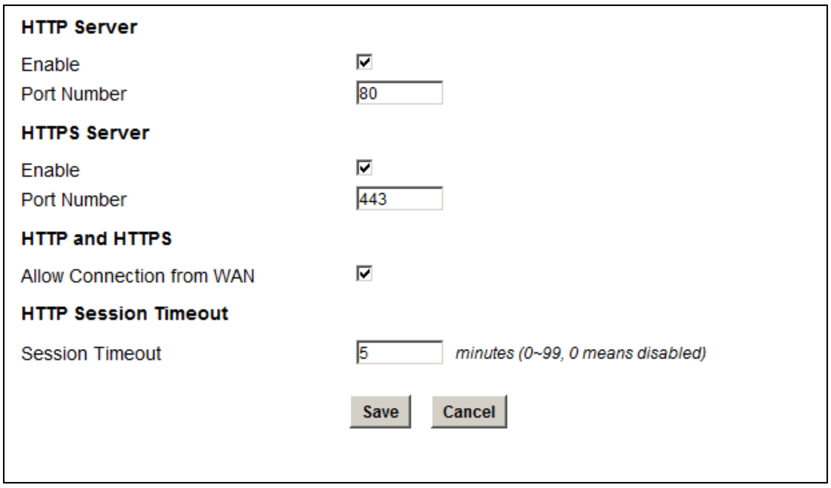
4.10 Remotely Managing Your BM2022w

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

Goal: Set up the BM2022w to allow management requests from the WAN (Internet).

See Also: Section 12.3 on page 187.

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



HTTP Server

Enable ☑

Port Number 80

HTTPS Server

Enable ☑

Port Number 443

HTTP and HTTPS

Allow Connection from WAN ☑

HTTP Session Timeout

Session Timeout 5 *minutes (0~99, 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**.

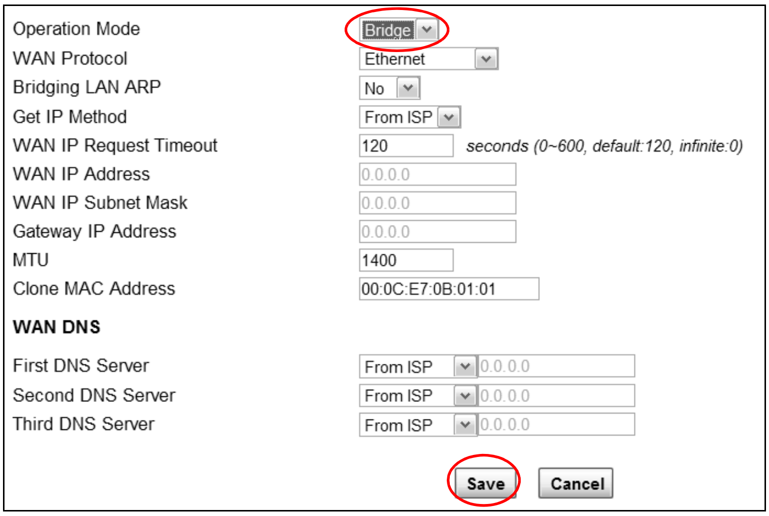
4.11 VLAN Configuration Examples

This section shows VLAN configuration scenarios.

See Section 7.20 on page 122 if you need more information about VLAN.

Before enabling VLANs you will need to change the BM2022w to bridge mode.

Click **Network Setting** > **WAN**. Change the BM2022w to bridge mode and then click **Save**. If you cannot obtain IP address settings from a WAN DHCP server, select **User** as the **Get IP Method** and enter the **WAN IP Address**, **WAN IP Subnet Mask** and **Gateway IP Address**.

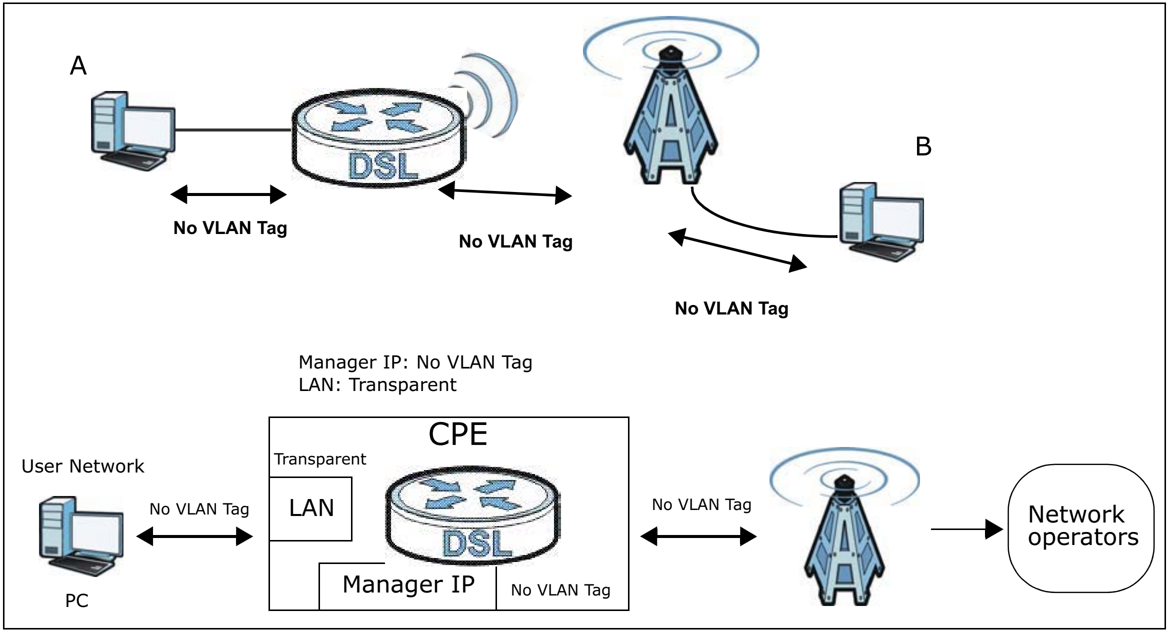


Operation Mode	Bridge	
WAN Protocol	Ethernet	
Bridging LAN ARP	No	
Get IP Method	From ISP	
WAN IP Request Timeout	120	*seconds (0~600, default:120, infinite:0)*
WAN IP Address	0.0.0.0	
WAN IP Subnet Mask	0.0.0.0	
Gateway IP Address	0.0.0.0	
MTU	1400	
Clone MAC Address	00:0C:E7:0B:01:01	
WAN DNS		
First 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

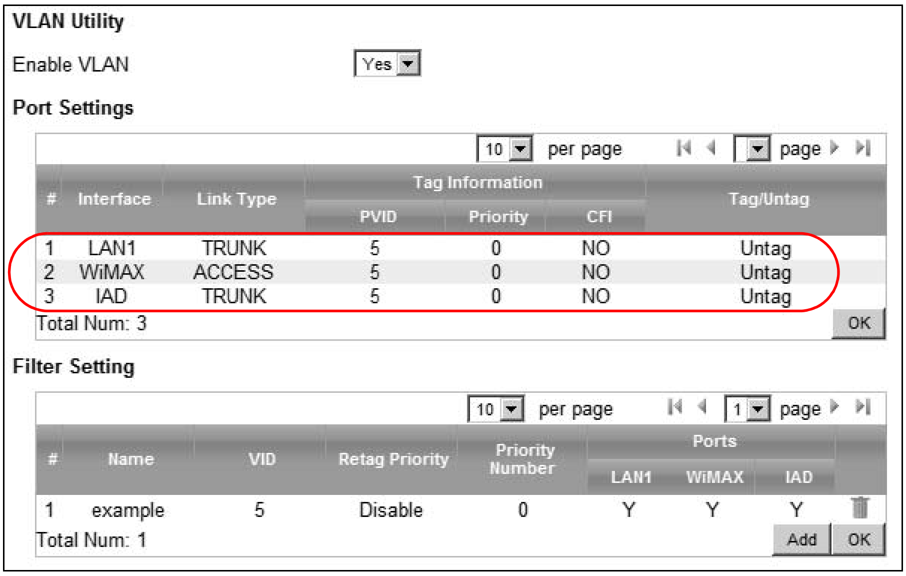
4.11.1 Scenario 1

In this scenario, PC A is connected directly to interface LAN1 on the BM2022w. PC B is connected to interface WiMAX and interface IAD for managing the BM2022w.

Figure 17 VLAN Configuration Example 1



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



VLAN Utility

Enable VLAN: Yes

Port Settings

10 per page | 1 page

#	Interface	Link Type	Tag Information			Tag/Untag
			PVID	Priority	CFI	
1	LAN1	TRUNK	5	0	NO	Untag
2	WiMAX	ACCESS	5	0	NO	Untag
3	IAD	TRUNK	5	0	NO	Untag

Total Num: 3 OK

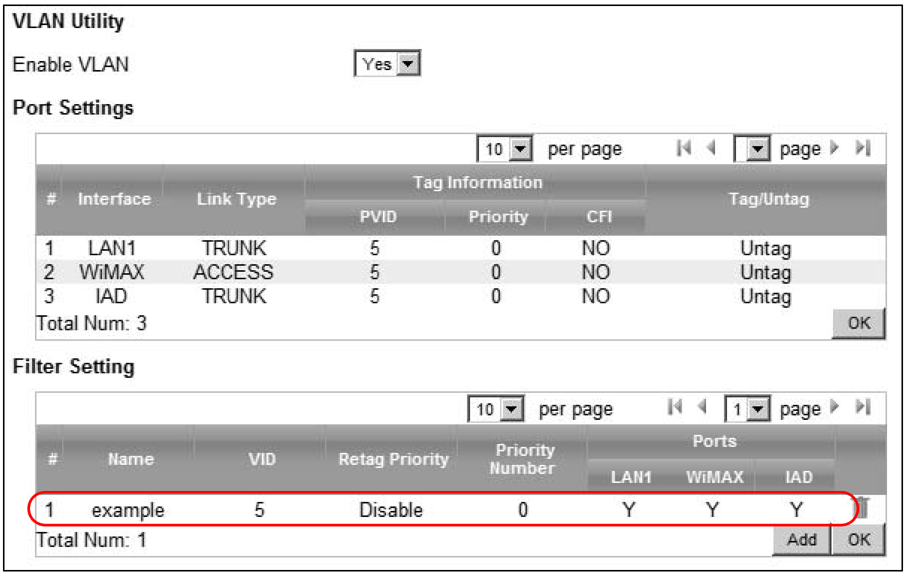
Filter Setting

10 per page | 1 page

#	Name	VID	Retag Priority	Priority Number	Ports		
					LAN1	WiMAX	IAD
1	example	5	Disable	0	Y	Y	Y

Total Num: 1 Add OK

2 Next, configure the **Name**, **VID** and **Ports** for the **Filter Setting**. The BM2022w will tag packets it receives on each interface so that they are recognized in VLAN 5. Tagged packets will be untagged when they are forwarded out of each interface since the devices attached to these interfaces do not support VLAN tagged packets.



VLAN Utility

Enable VLAN: Yes

Port Settings

10 per page | 1 page

#	Interface	Link Type	Tag Information			Tag/Untag
			PVID	Priority	CFI	
1	LAN1	TRUNK	5	0	NO	Untag
2	WiMAX	ACCESS	5	0	NO	Untag
3	IAD	TRUNK	5	0	NO	Untag

Total Num: 3 OK

Filter Setting

10 per page | 1 page

#	Name	VID	Retag Priority	Priority Number	Ports		
					LAN1	WiMAX	IAD
1	example	5	Disable	0	Y	Y	Y

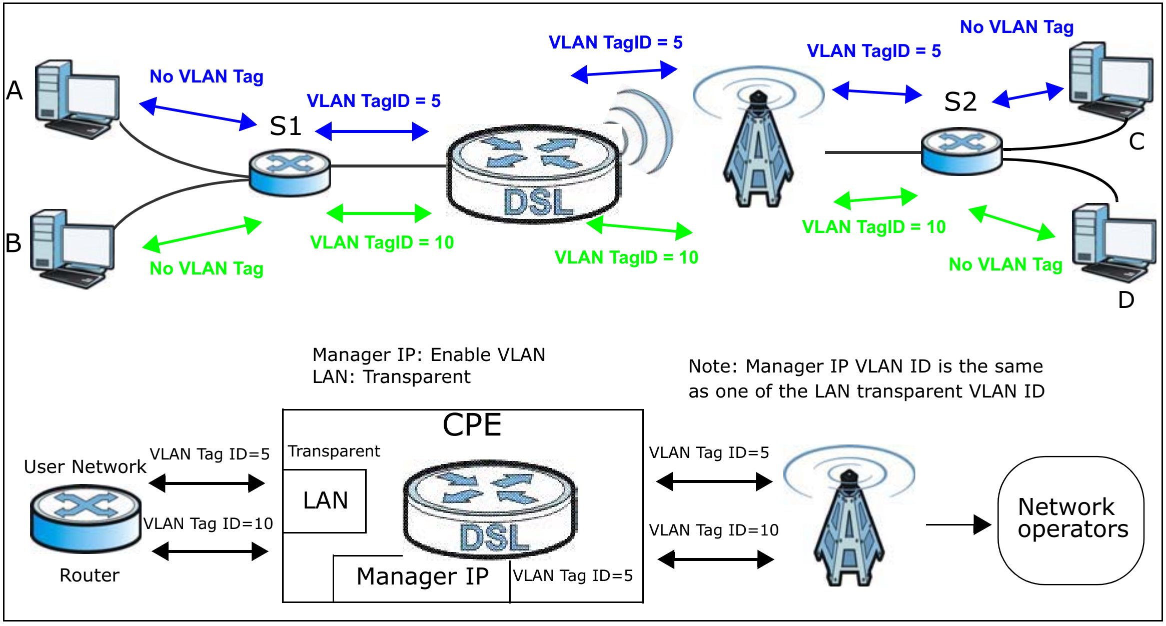
Total Num: 1 Add OK

4.11.2 Scenario 2

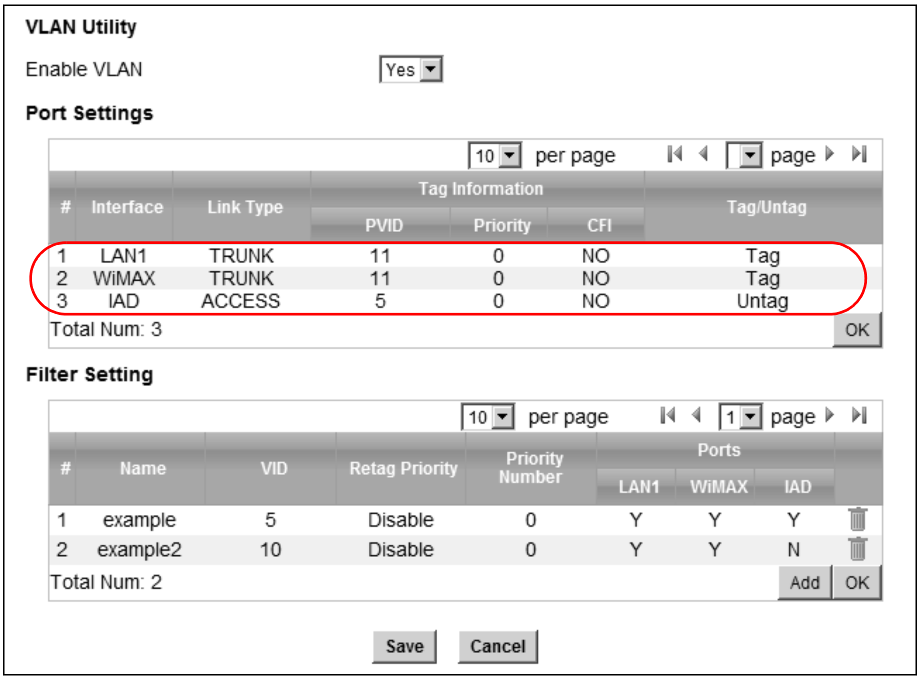
In this scenario, PC A and PC C are on VLAN 5, while PC B and PC D are on VLAN 10. PC A and PC B are connected to interface LAN1 through VLAN supporting switch S1. PC C is connected to interface WiMAX and interface IAD for managing the BM2022w, through VLAN supporting switch S2. PC D is connected to interface WiMAX through VLAN supporting switch S2.

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

Figure 18 VLAN Configuration Example 2



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



VLAN Utility

Enable VLAN: Yes

Port Settings

10 per page | page

#	Interface	Link Type	Tag Information			Tag/Untag
			PVID	Priority	CFI	
1	LAN1	TRUNK	11	0	NO	Tag
2	WiMAX	TRUNK	11	0	NO	Tag
3	IAD	ACCESS	5	0	NO	Untag

Total Num: 3

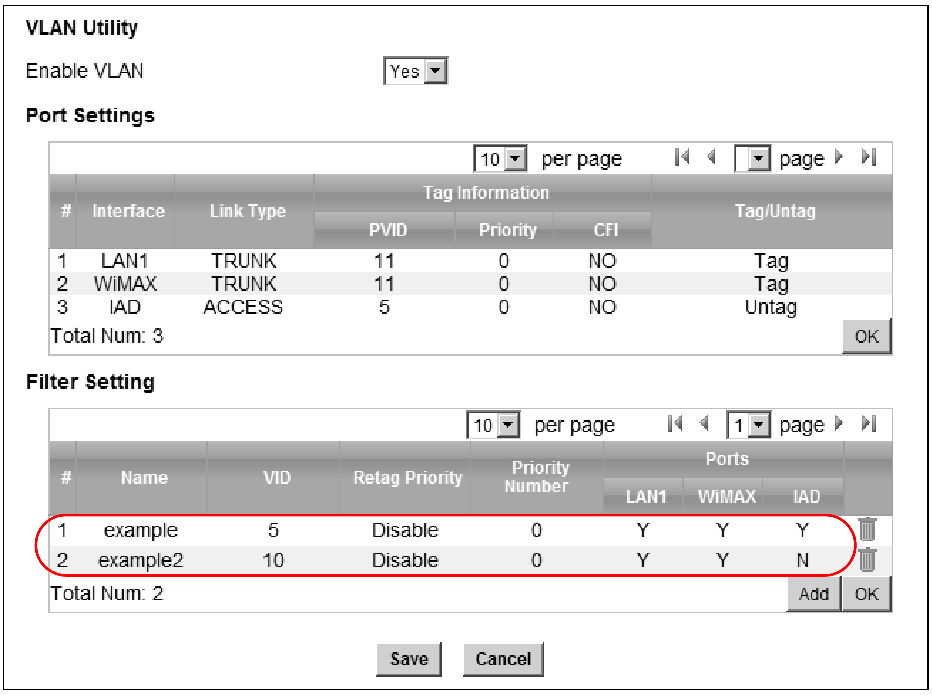
Filter Setting

10 per page | 1 page

#	Name	VID	Retag Priority	Priority Number	Ports		
					LAN1	WiMAX	IAD
1	example	5	Disable	0	Y	Y	Y
2	example2	10	Disable	0	Y	Y	N

Total Num: 2

2 Next, configure the **Name**, **VID** and **Ports** for the **Filter Setting**. Interfaces **LAN1** and **WiMAX** are Trunk links, so the BM2022w will recognize VLAN 5 and VLAN 10 tagged packets it receives on these interfaces from the VLAN supporting switches. VLAN tagged packets will also be forwarded out of these interfaces. Interface **IAD** is configured as an Access port, so tagged packets will be untagged when they are forwarded.



VLAN Utility

Enable VLAN: Yes

Port Settings

#	Interface	Link Type	Tag Information			Tag/Untag
			PVID	Priority	CFI	
1	LAN1	TRUNK	11	0	NO	Tag
2	WiMAX	TRUNK	11	0	NO	Tag
3	IAD	ACCESS	5	0	NO	Untag

Total Num: 3

Filter Setting

#	Name	VID	Retag Priority	Priority Number	Ports		
					LAN1	WiMAX	IAD
1	example	5	Disable	0	Y	Y	Y
2	example2	10	Disable	0	Y	Y	N

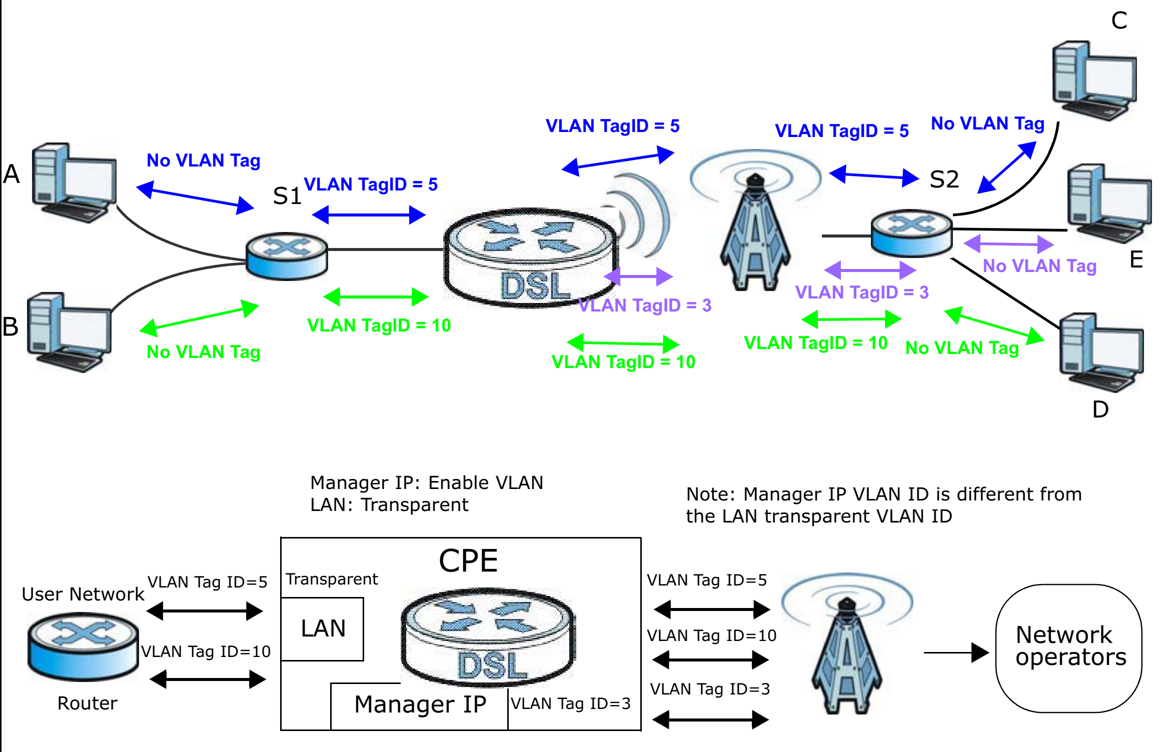
Total Num: 2

4.11.3 Scenario 3

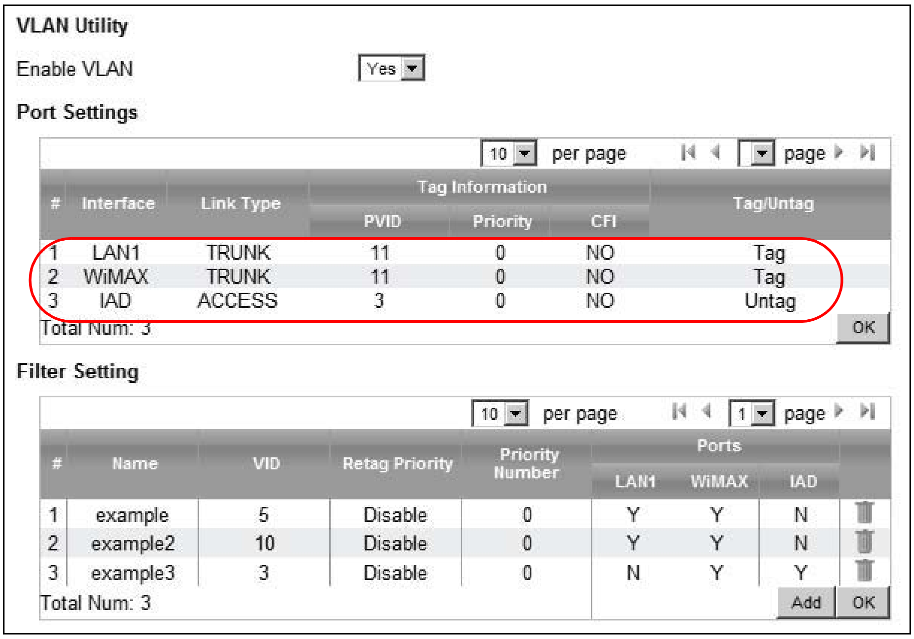
In this scenario, PC A and PC C are on VLAN 5, PC B and PC D are on VLAN 10, and PC E is on VLAN 3. PC A and PC B are connected to interface LAN1 through VLAN supporting switch S1. PC C and PC D are connected to interface WiMAX through VLAN supporting switch S2. PC E is connected to interface IAD through VLAN supporting switch S2 for managing the BM2022w.

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

Figure 19 VLAN Configuration Example 3



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



VLAN Utility

Enable VLAN: Yes

Port Settings

10 per page | page

#	Interface	Link Type	Tag Information			Tag/Untag
			PVID	Priority	CFI	
1	LAN1	TRUNK	11	0	NO	Tag
2	WiMAX	TRUNK	11	0	NO	Tag
3	IAD	ACCESS	3	0	NO	Untag

Total Num: 3

OK

Filter Setting

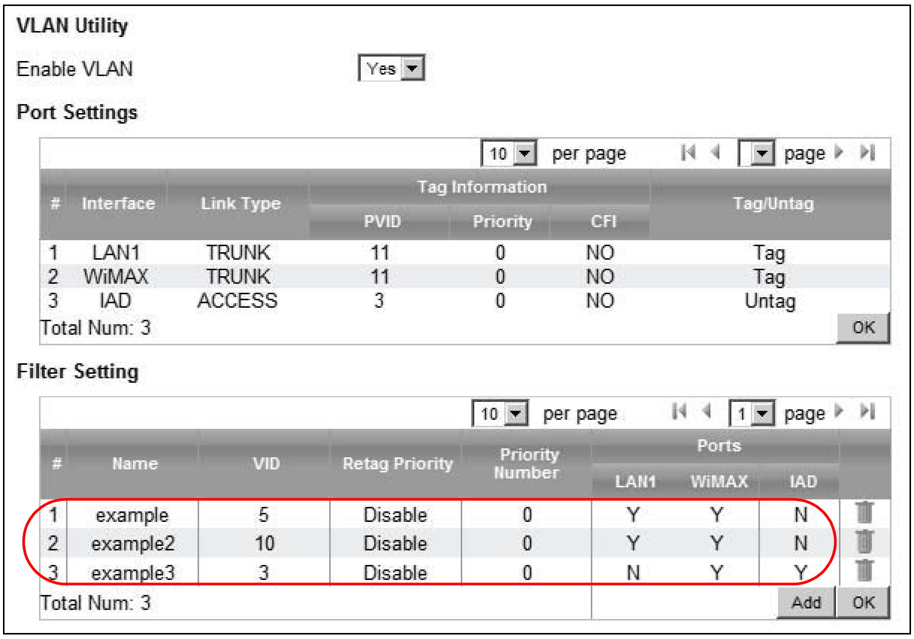
10 per page | 1 page

#	Name	VID	Retag Priority	Priority Number	Ports		
					LAN1	WiMAX	IAD
1	example	5	Disable	0	Y	Y	N
2	example2	10	Disable	0	Y	Y	N
3	example3	3	Disable	0	N	Y	Y

Total Num: 3

Add OK

2 Next, configure the **Name**, **VID** and **Ports** for the **Filter Setting**. Interfaces **LAN1** and **WiMAX** are Trunk links, so the BM2022w will recognize VLAN 5 and VLAN 10 tagged packets it receives on these interfaces from the VLAN supporting switches. VLAN tagged packets will also be forwarded out of these interfaces. Interface **IAD** is configured as an Access port, so tagged packets will be untagged when they are forwarded.



VLAN Utility

Enable VLAN: Yes

Port Settings

10 per page, page

#	Interface	Link Type	Tag Information			Tag/Untag
			PVID	Priority	CFI	
1	LAN1	TRUNK	11	0	NO	Tag
2	WiMAX	TRUNK	11	0	NO	Tag
3	IAD	ACCESS	3	0	NO	Untag

Total Num: 3

Filter Setting

10 per page, 1 page

#	Name	VID	Retag Priority	Priority Number	Ports		
					LAN1	WiMAX	IAD
1	example	5	Disable	0	Y	Y	N
2	example2	10	Disable	0	Y	Y	N
3	example3	3	Disable	0	N	Y	Y

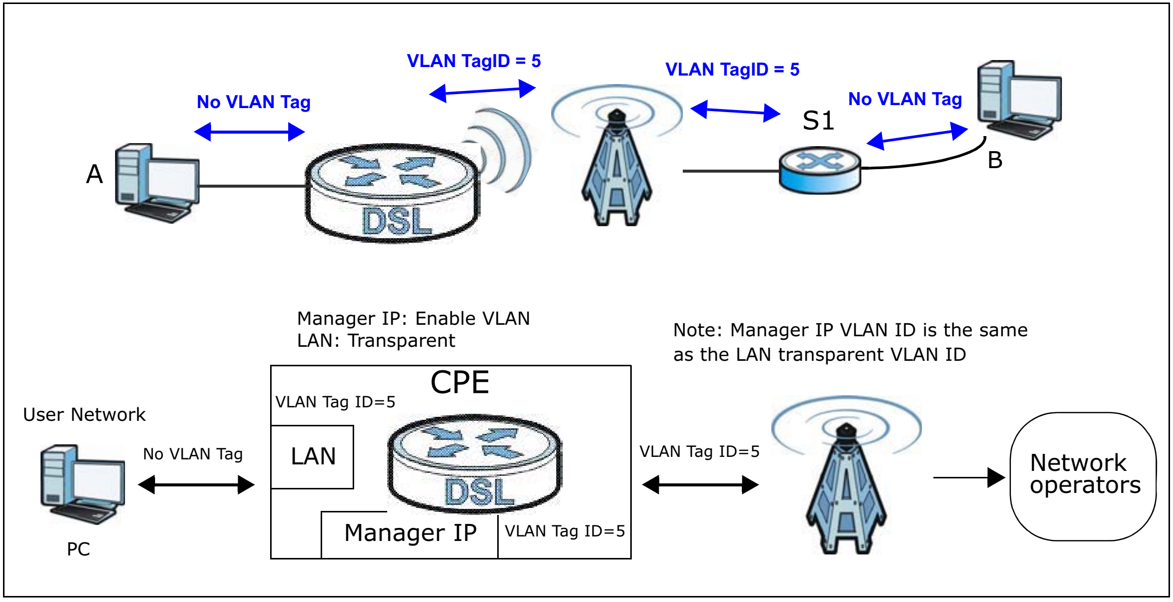
Total Num: 3

4.11.4 Scenario 4

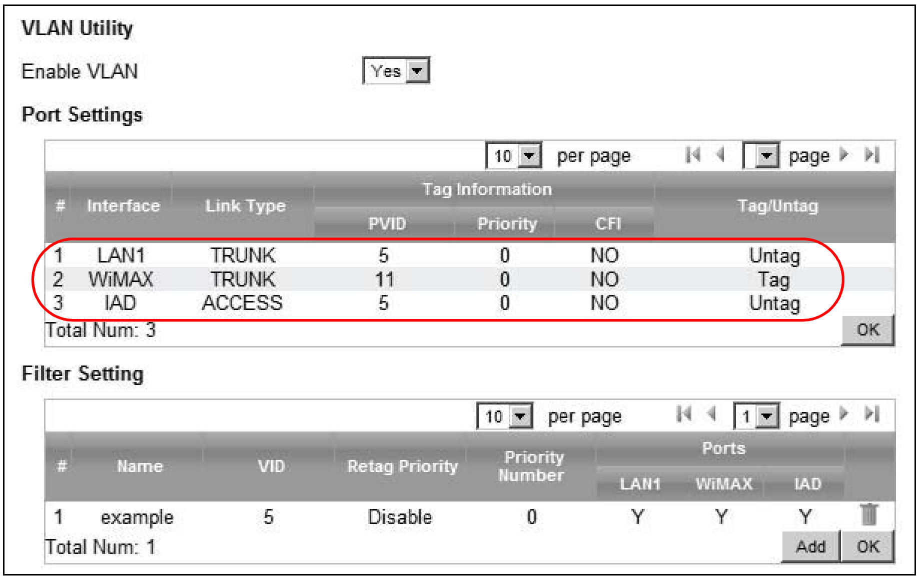
In this scenario, PC A is connected directly to interface LAN1 on the BM2022w, while PC B is on VLAN 5. PC B is connected to interface WiMAX and interface IAD for managing the BM2022w, through VLAN supporting switch S1.

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

Figure 20 VLAN Configuration Example 4



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



VLAN Utility

Enable VLAN: Yes

Port Settings

10 per page | 1 page

#	Interface	Link Type	Tag Information			Tag/Untag
			PVID	Priority	CFI	
1	LAN1	TRUNK	5	0	NO	Untag
2	WiMAX	TRUNK	11	0	NO	Tag
3	IAD	ACCESS	5	0	NO	Untag

Total Num: 3

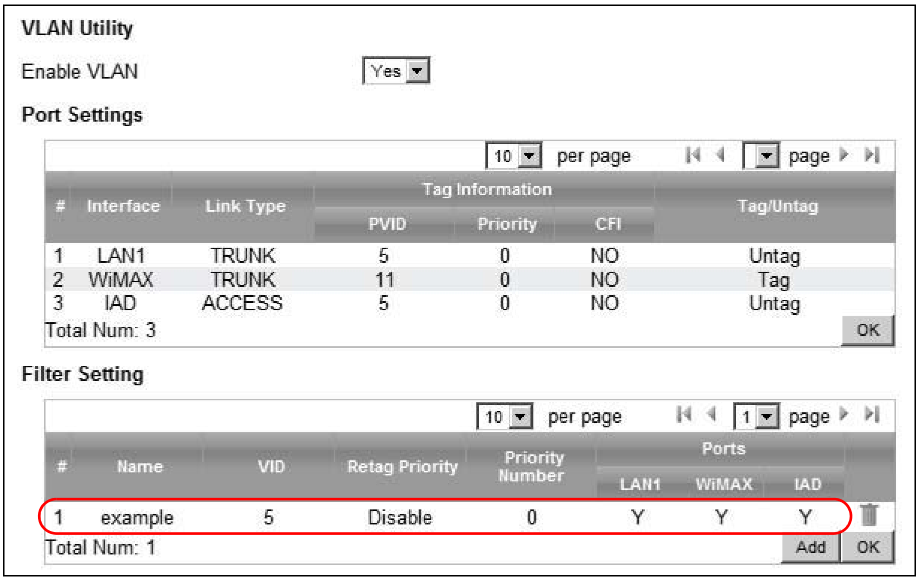
Filter Setting

10 per page | 1 page

#	Name	VID	Retag Priority	Priority Number	Ports		
					LAN1	WiMAX	IAD
1	example	5	Disable	0	Y	Y	Y

Total Num: 1

2 Next, configure the **Name**, **VID** and **Ports** for the **Filter Setting**. Interfaces **LAN1** and **WiMAX** are Trunk links. On the WiMAX interface, the BM2022w will recognize VLAN 5 tagged packets it receives from the VLAN supporting switch. VLAN tagged packets will also be forwarded out of this interface. On the LAN1 interface, the BM2022w will tag packets it receives so that they are recognized in VLAN 5. On LAN1, tagged packets will be untagged when they are forwarded out since PC A does not support VLAN tagged packets. Interface **IAD** is configured as an Access port, so tagged packets will be untagged when they are forwarded.



VLAN Utility

Enable VLAN: Yes

Port Settings

10 per page, page

#	Interface	Link Type	Tag Information			Tag/Untag
			PVID	Priority	CFI	
1	LAN1	TRUNK	5	0	NO	Untag
2	WiMAX	TRUNK	11	0	NO	Tag
3	IAD	ACCESS	5	0	NO	Untag

Total Num: 3

Filter Setting

10 per page, 1 page

#	Name	VID	Retag Priority	Priority Number	Ports		
					LAN1	WiMAX	IAD
1	example	5	Disable	0	Y	Y	Y

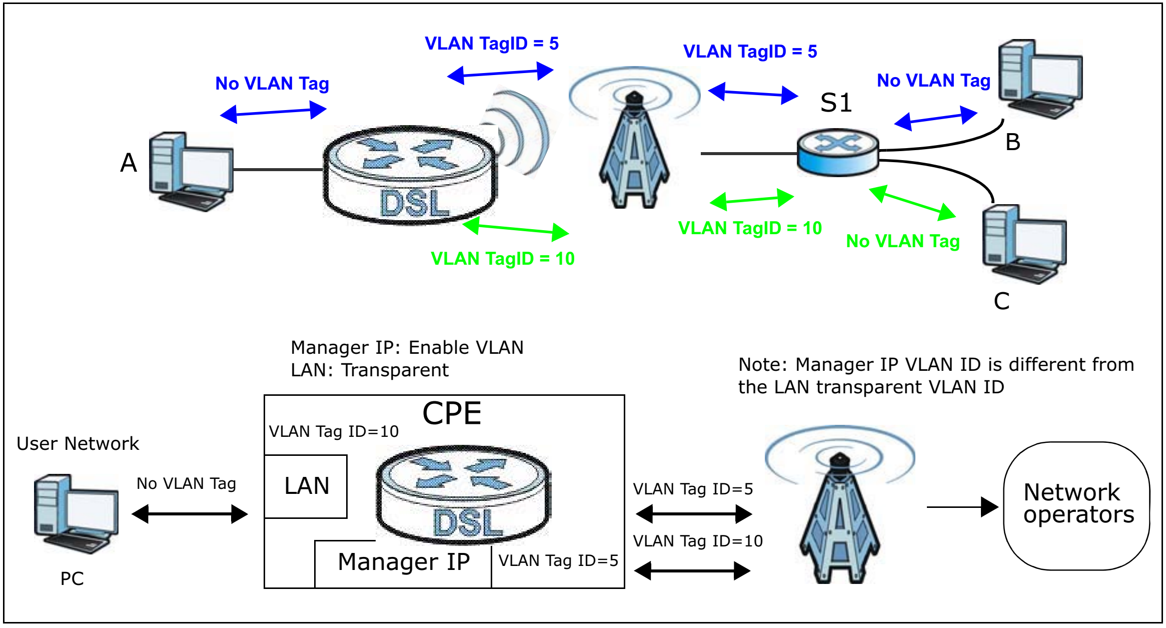
Total Num: 1

4.11.5 Scenario 5

In this scenario, PC A is directly connected to interface LAN1 on the BM2022w. PC B is on VLAN 5 while PC C is on VLAN 10. PC B is connected to interface WiMAX and interface IAD for managing the BM2022w, through VLAN supporting switch S1. PC C is connected to interface WiMAX through VLAN supporting switch S1.

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

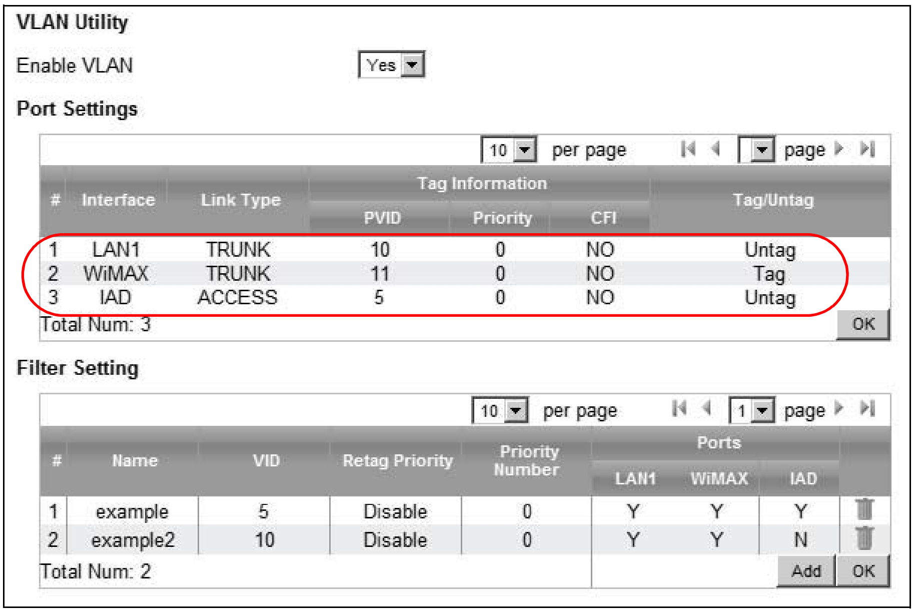
Figure 21 VLAN Configuration Example 5



Manager IP: Enable VLAN
LAN: Transparent

Note: Manager IP VLAN ID is different from the LAN transparent VLAN ID

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


VLAN Utility

Enable VLAN: Yes

Port Settings

10 per page | page

#	Interface	Link Type	Tag Information			Tag/Untag
			PVID	Priority	CFI	
1	LAN1	TRUNK	10	0	NO	Untag
2	WiMAX	TRUNK	11	0	NO	Tag
3	IAD	ACCESS	5	0	NO	Untag

Total Num: 3

OK

Filter Setting

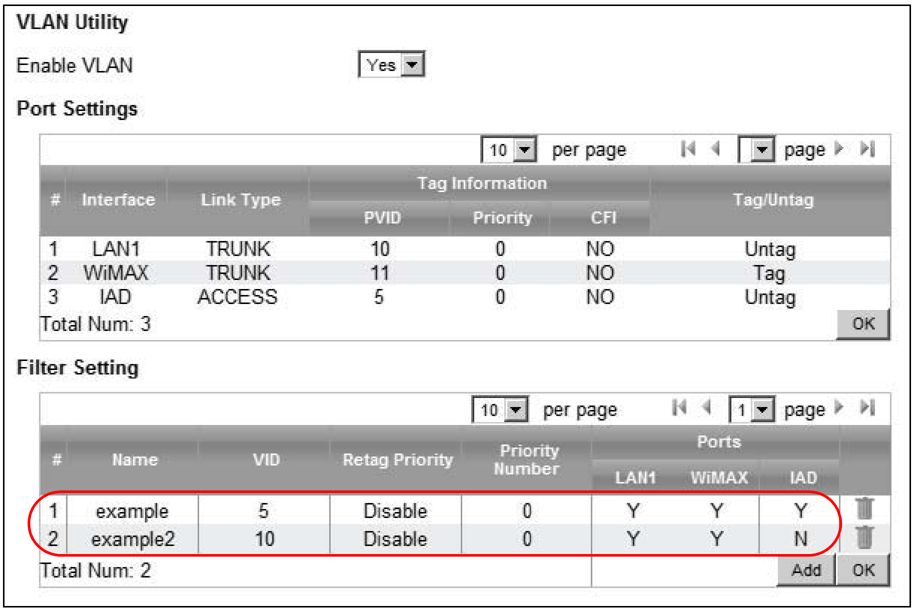
10 per page | 1 page

#	Name	VID	Retag Priority	Priority Number	Ports			
					LAN1	WiMAX	IAD	
1	example	5	Disable	0	Y	Y	Y	🗑
2	example2	10	Disable	0	Y	Y	N	🗑

Total Num: 2

Add OK

2 Next, configure the **Name**, **VID** and **Ports** for the **Filter Setting**. Interfaces **LAN1** and **WiMAX** are Trunk links. On the WiMAX interface the BM2022w will recognize VLAN 5 and VLAN 10 tagged packets it receives from the VLAN supporting switch. VLAN tagged packets will also be forwarded out of these interfaces. On the LAN1 interface, the BM2022w will tag packets it receives so that they are recognized in VLAN 10. On LAN1, tagged packets will be untagged when they are forwarded out, since PC A does not support VLAN tagged packets. Interface **IAD** is configured as an Access port, so tagged packets will be untagged when they are forwarded.



VLAN Utility

Enable VLAN: Yes

Port Settings

#	Interface	Link Type	Tag Information			Tag/Untag
			PVID	Priority	CFI	
1	LAN1	TRUNK	10	0	NO	Untag
2	WiMAX	TRUNK	11	0	NO	Tag
3	IAD	ACCESS	5	0	NO	Untag

Total Num: 3

Filter Setting

#	Name	VID	Retag Priority	Priority Number	Ports		
					LAN1	WiMAX	IAD
1	example	5	Disable	0	Y	Y	Y
2	example2	10	Disable	0	Y	Y	N

Total Num: 2

PART II
Technical Reference

5

System Status

5.1 Overview

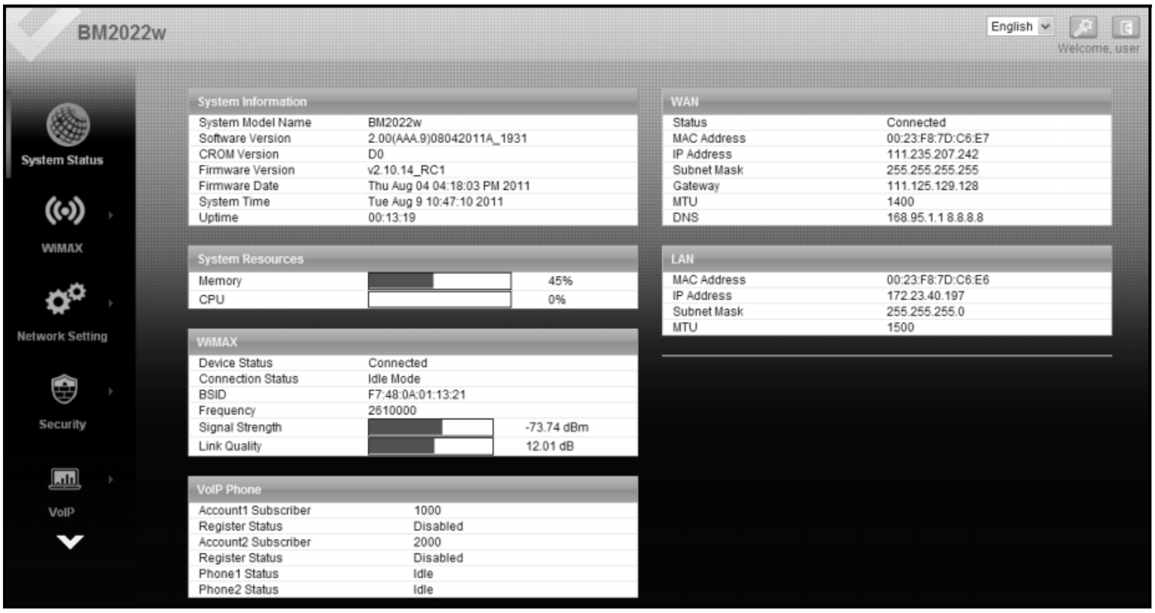
Use this screen to view a summary of your BM2022w connection status.

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 22 System Status



System Information

System Model Name	BM2022w
Software Version	2.00(AAA.9)08042011A_1931
CROM Version	D0
Firmware Version	v2.10.14_RC1
Firmware Date	Thu Aug 04 04:18:03 PM 2011
System Time	Tue Aug 9 10:47:10 2011
Uptime	00:13:19

System Resources

Memory	45%
CPU	0%

WiMAX

Device Status	Connected
Connection Status	Idle Mode
BSID	F7:48:0A:01:13:21
Frequency	2610000
Signal Strength	-73.74 dBm
Link Quality	12.01 dB

VoIP Phone

Account1 Subscriber	1000
Register Status	Disabled
Account2 Subscriber	2000
Register Status	Disabled
Phone1 Status	Idle
Phone2 Status	Idle

WAN

Status	Connected
MAC Address	00:23:F8:7D:C6:E7
IP Address	111.235.207.242
Subnet Mask	255.255.255.255
Gateway	111.125.129.128
MTU	1400
DNS	168.95.1.1 8.8.8.8

LAN

MAC Address	00:23:F8:7D:C6:E6
IP Address	172.23.40.197
Subnet Mask	255.255.255.0
MTU	1500

The following tables describe the labels in this screen.

Table 12 Status

LABEL	DESCRIPTION
System Information	
System Model Name	This field displays the BM2022w system model name. It is used for identification.
Software Version	This field displays the Web Configurator version number.

Table 12 Status (continued)

LABEL	DESCRIPTION
CROM Version	This field displays the CROM version number.
Firmware Version	This field displays the current version of the firmware inside the device.
Firmware Date	This field shows the date the firmware version was created.
System Time	This field displays the current system time.
Uptime	This field displays how long the BM2022w has been running since it last started up.
System Resources	
Memory	This field displays what percentage of the BM2022w's memory is currently used. The higher the memory usage, the more likely the BM2022w is to slow down. Some memory is required just to start the BM2022w 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 BM2022w's CPU is currently used. The higher the CPU usage, the more likely the BM2022w is to slow down.
WiMAX	
Device Status	This field displays the BM2022w current status for connecting to the selected base station. **Scanning** - The BM2022w is scanning for available base stations. **Ready** - The BM2022w has finished a scanning and you can connect to a base station. **Connecting** - The BM2022w attempts to connect to the selected base station. **Connected** - The BM2022w has successfully connected to the selected base station.
Connection Status	This field displays the status of the WiMAX connection between the BM2022w and the base station. **Network Search** - The BM2022w is scanning for any available WiMAX connections. **Disconnected** - No WiMAX connection is available. **Network Entry** - A WiMAX connection is initializing. **Normal** - The WiMAX connection has successfully established.
BSID	This field displays the MAC address of the base station to which the device is connected.
Frequency	This field indicates the frequency the BM2022w is using.
Signal Strength	This field indicates the strength of the connection that the BM2022w has with the base station.
Link Quality	This field indicates the relative quality of the link the BM2022w has with the base station.
WAN	
Status	This field indicates the status of the WAN connection to the BM2022w.
MAC Address	This field indicates the MAC address of the port making the WAN connection on the BM2022w.
IP Address	This field indicates the current IP address of the BM2022w in the WAN.

Table 12 Status (continued)

LABEL	DESCRIPTION
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 BM2022w is connected.
MTU	This field indicates the Maximum Transmission Unit (MTU) between the BM2022w and the ISP servers to which it is connected.
DNS	This field indicates the Domain Name Server (DNS) to which your BM2022w is connected.
LAN	
MAC Address	This field indicates the MAC address of the port making the LAN connection on the BM2022w.
IP Address	This field displays the current IP address of the BM2022w 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 BM2022w and the client devices to which it is connected.
VoIP Phone	
Account1 Subscriber	This field displays the SIP number for SIP account 1.
Register Status	This field displays whether SIP account 1 is already registered with a SIP server (**Up** or **Disabled**).
Account2 Subscriber	This field displays the SIP number for SIP account 2.
Register Status	This field displays whether SIP account 2 is already registered with a SIP server (**Up** or **Disabled**).
Phone1 Status	This field displays whether phone line 1 (mapping to the **VoIP1** port) is in use or not (idle).
Phone2 Status	This field displays whether phone line 2 (mapping to the **VoIP2** port) is in use or not (idle).

6

WiMAX

6.1 Overview

This chapter shows you how to set up and manage the connection between the BM2022w and your ISP's base stations.

6.1.1 What You Need to Know

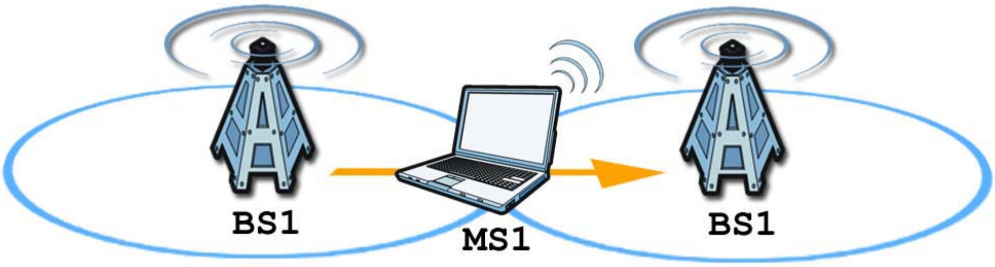
The following terms and concepts may help as you read through this chapter.

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). Huawei is a member of the WiMAX Forum, the industry group dedicated to promoting and certifying interoperability of wireless broadband products.

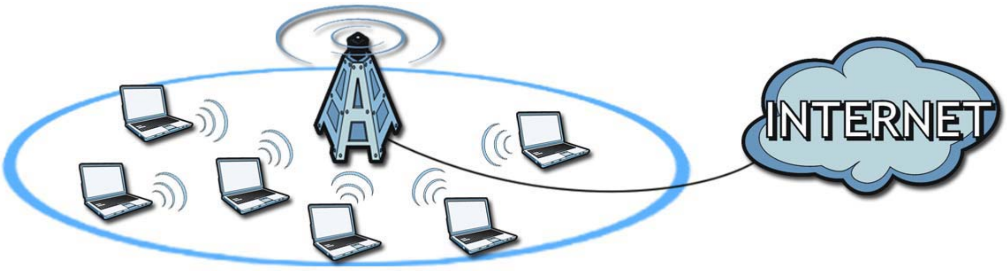
In a wireless MAN, a wireless-equipped computer is known either as a mobile station (MS) or a subscriber station (SS). Mobile stations use the IEEE 802.16e standard and are able to maintain connectivity while switching their connection from one base station to another base station (handover) while subscriber 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 23 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 24 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.

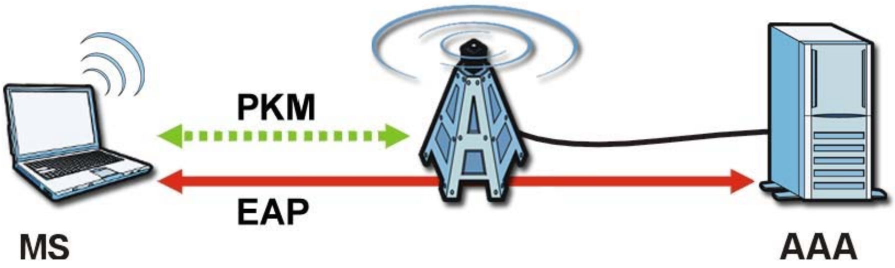
The radio frequency and bandwidth of the link between the BM2022w and the base station are controlled by the base station. The BM2022w follows the base station's configuration.

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 25 Using an AAA Server

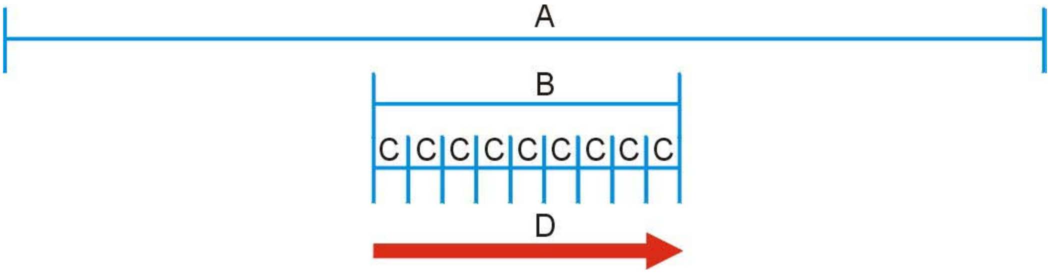


In this figure, the dashed arrow shows the PKM (Privacy Key Management) secured connection between the mobile station and the base station, and the solid arrow shows the EAP secured connection between the mobile station, the base station and the AAA server. See the WiMAX security appendix for more details.

Frequency Ranges

The following figure shows the BM2022w searching a range of frequencies to find a connection to a base station.

Figure 26 Frequency Ranges



In this figure, **A** is the WiMAX frequency range. "WiMAX frequency range" refers to the entire range of frequencies the BM2022w 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 BM2022w searching for a connection.

Have the BM2022w 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 BM2022w 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 BM2022w 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 BM2022w currently allows the importation of a PKS#7 file that contains a single certificate.

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

CINR

Carrier to Interference-plus-Noise Ratio (CINR) measures the effectiveness of a wireless signal and plays an important role in allowing the BM2022w to decode signal burst. If a burst has a high signal strength and a high interference-plus-noise ratio, it can use Digital Signal Processing (DSP) to decode it; if the signal strength is lower, it can switch to an alternate burst profile.

RSSI

Received Signal Strength Indicator (RSSI) measures the relative strength of a given wireless signal. This is important in determining if a signal is below the Clear-To-Send (CTS) threshold. If it is below the arbitrarily specified threshold, then BM2022w 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.

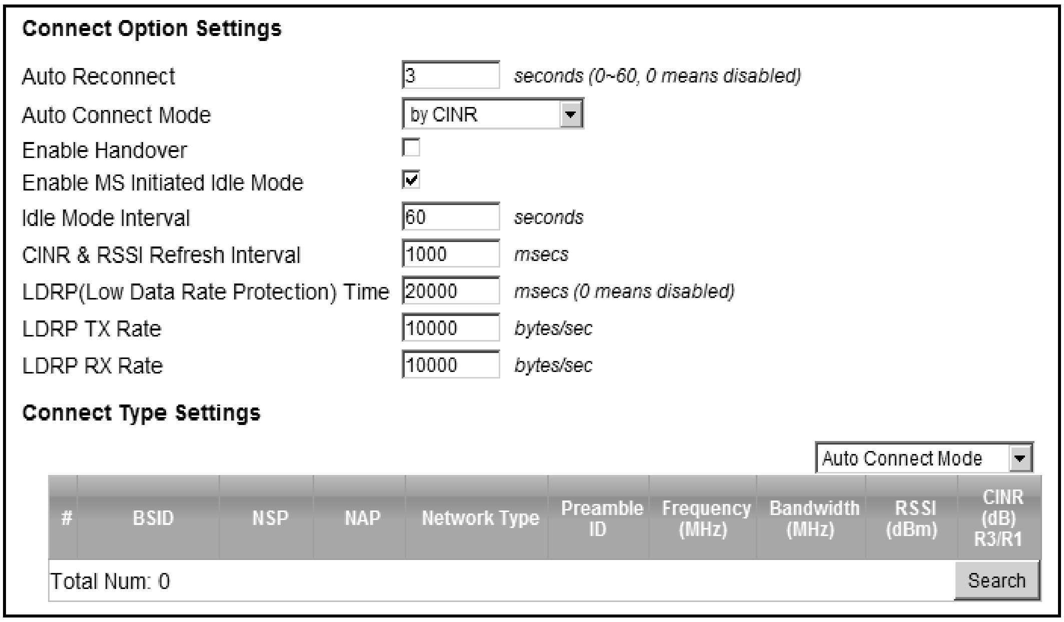
The BM2022w supports EAP-TLS and EAP-TTLS (at the time of writing, TTLS is not available in Windows Vista). For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). Certificates (also called digital IDs) can 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 BM2022w connects to the base stations on the WiMAX network.

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

Figure 27 Connection Settings Screen



Connect Option Settings

Auto Reconnect: 3 *seconds (0~60, 0 means disabled)*

Auto Connect Mode: by CINR

Enable Handover: □

Enable MS Initiated Idle Mode: ☑

Idle Mode Interval: 60 *seconds*

CINR & RSSI Refresh Interval: 1000 *msecs*

LDRP(Low Data Rate Protection) Time: 20000 *msecs (0 means disabled)*

LDRP TX Rate: 10000 *bytes/sec*

LDRP RX Rate: 10000 *bytes/sec*

Connect Type Settings

Auto Connect Mode

#	BSID	NSP	NAP	Network Type	Preamble ID	Frequency (MHz)	Bandwidth (MHz)	RSSI (dBm)	CINR (dB) R3/R1

Total Num: 0

This screen contains the following fields:

Table 13 Connection Settings

LABEL	DESCRIPTION
Connection Option Settings	
Auto Reconnect	Select the interval in seconds that the BM2022w waits after getting disconnected from the base station before attempting to reconnect.
Auto Connect Mode	Select the auto connect mode. • **By channel power** - Auto connects to the base station if the signal strength of the channel is sufficient for the BM2022w. • **By CINR** - Auto connects to the base station if the signal-to-noise ratio is sufficient for the BM2022w.
Enable Handover	Select this to maintain connectivity while the BM2022w switches its connection from one base station to another base station.
Enable MS Initiated Idle Mode	Select this to have the BM2022w 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 BM2022w waits during periods of no activity before going into idle mode.
CINR & RSSI Refresh Interval	Set the refresh interval in milliseconds for calculating the signal-to-noise measurement (CINR) and signal strength measurement (RSSI) of the BM2022w.
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 BM2022w sends a disconnect request to the base station.
LDRP TX Rate	Enter the outgoing data rates for LDRP in bytes per second.
LDRP RX Rate	Enter the incoming data rates for LDRP in bytes per second.
Connection Type Settings	

Table 13 Connection Settings (continued)

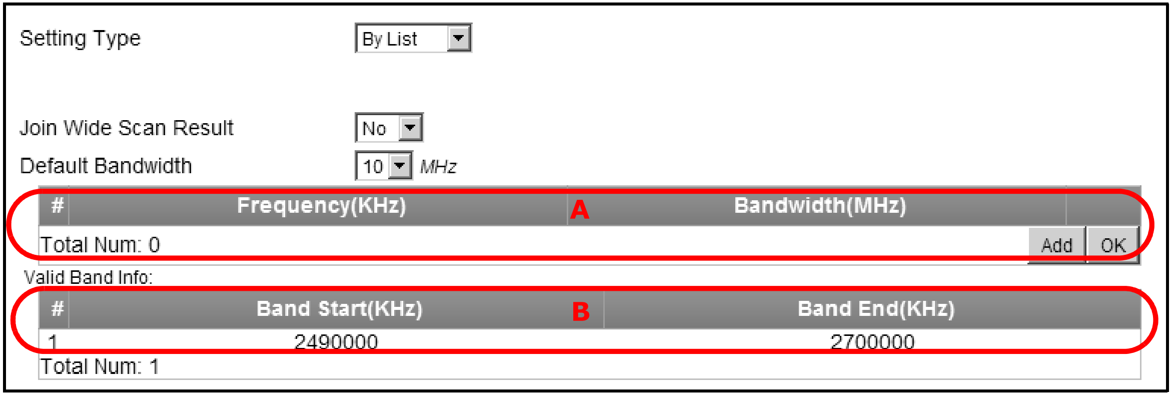
LABEL	DESCRIPTION
Mode Select	Select how the BM2022w connects to the base station. • **Auto Connect Mode** - The device connects automatically to the first base station in range. • **Network Search Mode** - The device scans for available base stations then connects to the best one it can.
BSID	This displays the MAC address of a base station within range of the BM2022w.
Preamble ID	The preamble ID is the index identifier in the header of the base station's broadcast messages. In the beginning of a mobile stations's network entry process, it searches for the preamble and uses it to additional channel information. The preamble ID is used to synchronize the upstream and downstream transmission timing with the base station.
Frequency (MHz)	This field displays the radio frequency of the BM2022w'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 BM2022w 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 28 Frequency Settings Screen (By List)



Setting Type: By List

Join Wide Scan Result: No

Default Bandwidth: 10 MHz

#	Frequency(KHz)	Bandwidth(MHz)

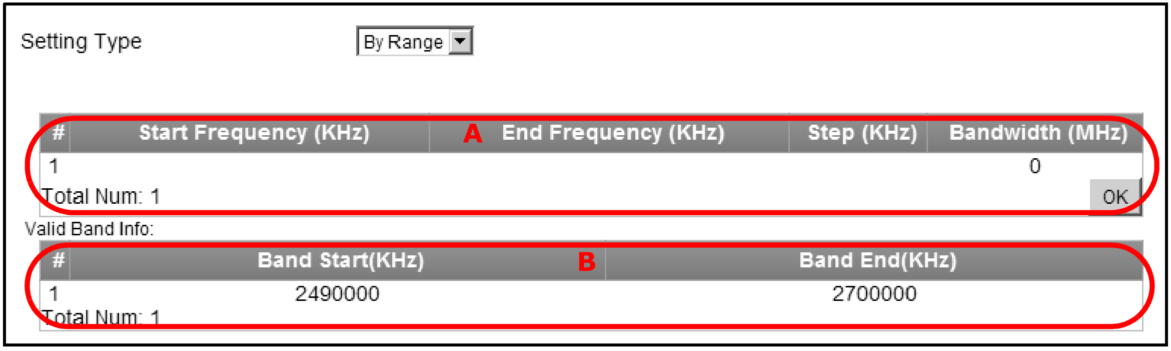
Total Num: 0

Valid Band Info:

#	Band Start(KHz)	Band End(KHz)
1	2490000	2700000

Total Num: 1

Figure 29 Frequency Settings Screen (By Range)



Setting Type: By Range

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

Total Num: 1

Valid Band Info:

#	Band Start(KHz)	Band End(KHz)
1	2490000	2700000

Total Num: 1

This screen contains the following fields:

Table 14 Frequency Settings

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

Table 14 Frequency Settings (continued)

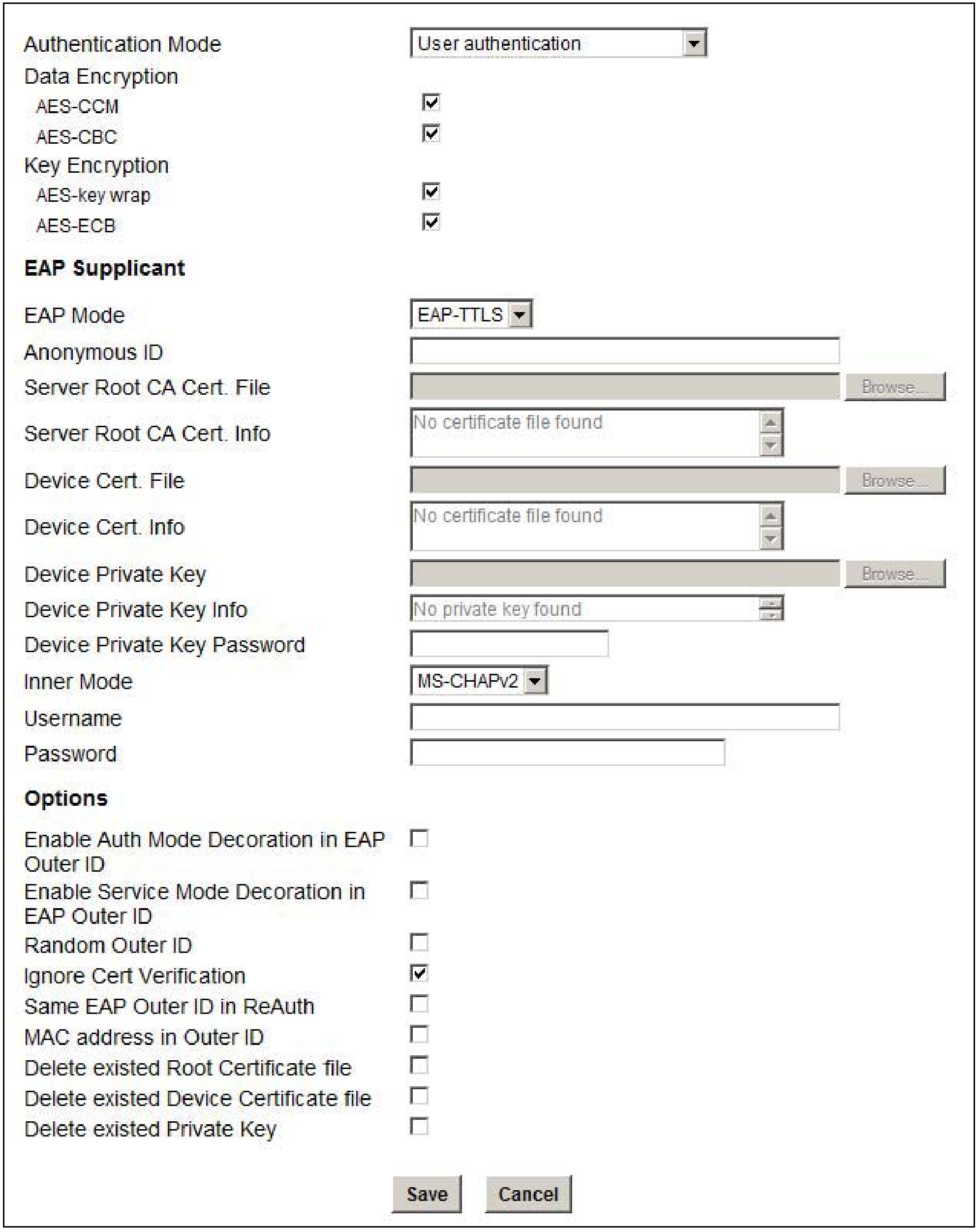
LABEL	DESCRIPTION
Bandwidth (MHz)	This displays the bandwidth of the frequency band in megahertz (MHz). If you set a center frequency to 2600000 KHz with the bandwidth of 10 MHz, then the frequency band is from 2595000 to 2605000 KHz. Click the number to modify it. Enter the bandwidth of the frequency band in this field when you are adding an entry.
Delete	Click this button to remove an item from the list.
Add	Click this button to add an item to the list.
OK	Click this button to save any changes made to the list.
A (When **By Range** is selected in the **Setting Type** field)	
Start Frequency (KHz)	This indicates the beginning of a frequency band in kilohertz (KHz). Click this field to modify it. Enter the beginning frequency when you are adding an entry.
End Frequency (KHz)	This indicates the end of the frequency band in kilohertz (KHz). Click this field to modify it.
Step (KHz)	This indicates the frequency step within each band in kilohertz (KHz). Click this field to modify it.
Bandwidth (MHz)	This indicates the bandwidth in megahertz (MHz). Click this field to modify it.
OK	Click this button to save any changes made to the list.
Valid Band Info (**B**) This table displays the entire frequency band the BM2022w supports. The frequenc(ies) to scan that you configured in table **A** must be within this range.	
Band Start (KHz)	This indicates the beginning of the frequency band in kilohertz (KHz).
Band End (KHz)	This indicates the end of the frequency band in kilohertz (KHz).

6.4 Authentication Settings

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

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

Figure 30 Authentication Settings Screen



Authentication Mode	User authentication
Data Encryption	
AES-CCM	☑
AES-CBC	☑
Key Encryption	
AES-key wrap	☑
AES-ECB	☑
EAP Supplicant	
EAP Mode	EAP-TTLS
Anonymous ID	
Server Root CA Cert. File	Browse...
Server Root CA Cert. Info	No certificate file found
Device Cert. File	Browse...
Device Cert. Info	No certificate file found
Device Private Key	Browse...
Device Private Key Info	No private key found
Device Private Key Password	
Inner Mode	MS-CHAPv2
Username	
Password	
Options	
Enable Auth Mode Decoration in EAP Outer ID	□
Enable Service Mode Decoration in EAP Outer ID	□
Random Outer ID	□
Ignore Cert Verification	☑
Same EAP Outer ID in ReAuth	□
MAC address in Outer ID	□
Delete existed Root Certificate file	□
Delete existed Device Certificate file	□
Delete existed Private Key	□

This screen contains the following fields:

Table 15 Authentication Settings

LABEL	DESCRIPTION
Authentication Mode	Select the authentication mode from the list. The BM2022w supports the following authentication modes: • No authentication • User authentication • Device authentication • User and device authentication
Data Encryption	
AES-CCM	Select this to enable AES-CCM encryption. CCM combines counter-mode encryption with CBC-MAC authentication.
AES-CBC	Select this to enable AES-CBC encryption. CBC creates message authentication code from a block cipher.
Key Encryption	
AES-key wrap	Select this encapsulate cryptographic keys in a symmetric encryption algorithm.
AES-ECB	Select this to divide cryptographic keys into blocks and encrypt them separately.
EAP Supplicant	
EAP Mode	Select an Extensible Authentication Protocol (EAP) mode. The BM2022w supports the following: • **EAP-TLS** - In this protocol, digital certifications are needed by both the server and the wireless clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead. • **EAP-TTLS** - This protocol is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.
Anonymous ID	Enter the anonymous ID used for EAP supplicant authentication.
Server Root CA Cert File	Browse for and choose a server root certificate file, if required.
Server Root CA Info	This field displays information about the assigned server root certificate.
Device Cert File	Browse for and choose a device certificate file, if required. Before you import certificate from WebGUI, the certificate file must be signed by chipset vendor due to security reason.
Device Cert Info	This field displays information about the assigned device certificate.
Device Private Key	Browse for and choose a device private key, if required.
Device Private Key Info	This field displays information about the assigned device private key.
Device Private Key Password	Enter the device private key, if required.

Table 15 Authentication Settings (continued)

LABEL	DESCRIPTION
Inner Mode	Sets the EAP-TTLS inner mode. The BM2022w supports the following: • **MS-CHAP v2** - This is version 2 of Microsoft's variant of Challenge Handshake Authentication Protocol (CHAP). It allows for mutual authentication between devices. • **MS-CHAP** - This is Microsoft's variant of Challenge Handshake Authentication Protocol (CHAP). It allows for mutual authentication between devices. • **CHAP** - The Challenge Handshake Authentication Protocol (CHAP) uses PPP to authenticate remote devices using a three-way handshake and shared secret verification. • **MD5** - Message-Digest, algorithm 5, (MD5) encryption is typically used for checking file integrity. Because this encryption protocol contains a number of serious security flaws it is generally not recommended that you use it for authentication security. • **PAP** - Password Authentication Protocol uses unencrypted plaintext to send a passwords for authentication over the network. It's probably not a good idea to rely on this for security.
Username	Enter the username required for the EAP-TTLS inner method.
Password	Enter the password required for the EAP-TTLS inner method.
Options	
Enable Auth Mode Decoration in EAP Outer ID	Select this to enable authentication mode.
Enable Service Mode Decoration in EAP Outer ID	Select this to enable service mode.
Random Outer ID	Select this to allow the BM2022w 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 BM2022w to the outer ID while the EAP mode is set to EAP-TLS.
Delete existed Root Certificate file	Select this to delete an existing root certificate file from the BM2022w.
Delete existed Device Certificate file	Select this to delete an existing device certificate file from the BM2022w.
Delete existed Private Key	Select this to delete an existing private key from the BM2022w.

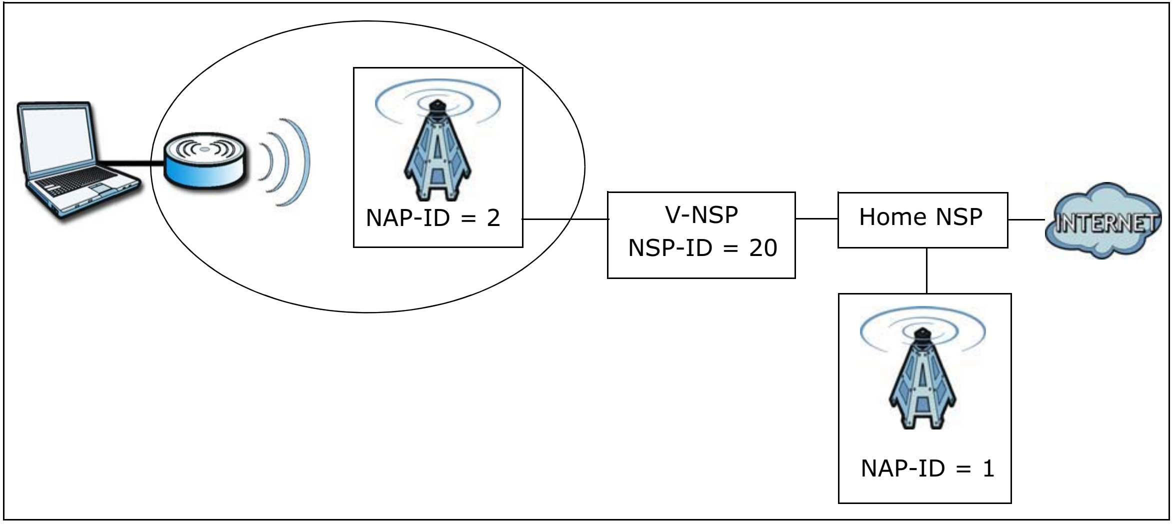
6.5 Channel Plan Settings

This screen allows you to specify channel plan settings for Network Discovery and Selection (ND&S). The BM2022w uses ND&S to establish connections when it is roaming. To do this, the BM2022w will scan for base stations that are operated by Network Access Providers (NAP) that have service agreements with the subscriber's service provider (Home-Network Service Provider or

Home NSP). Through the NAP's base station, which is identified by a NAP-ID, the subscriber's BM2022w can access the Internet through a network service provider (NSP). Access can be through another network service provider (Visited-Network Service Provider or V-NSP) or his own network service provider (Home NSP), depending on his service agreement.

In the following scenario, the subscriber's BM2022w cannot reach a base station owned by his Home NSP (base station with NAP-ID = 1). The BM2022w uses ND&S and is able to access another base station with NAP-ID = 2. This base station is associated with another service provider (V-NSP with NSP-ID = 20). The subscriber's service agreement specifies to route traffic from the other service provider to the Home NSP, so the Home NSP authenticates and authorizes the connection.

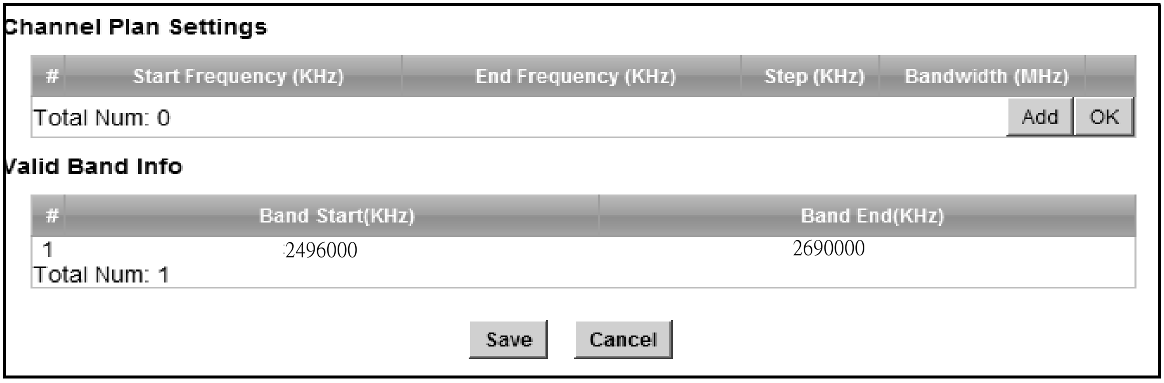
Figure 31 ND&S Scenario



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

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

Figure 32 Channel Plan Settings



Channel Plan Settings

#	Start Frequency (KHz)	End Frequency (KHz)	Step (KHz)	Bandwidth (MHz)
Total Num: 0				

Valid Band Info

#	Band Start(KHz)	Band End(KHz)
1	2496000	2690000
Total Num: 1		

This screen contains the following fields:

Table 16 Channel Plan Settings

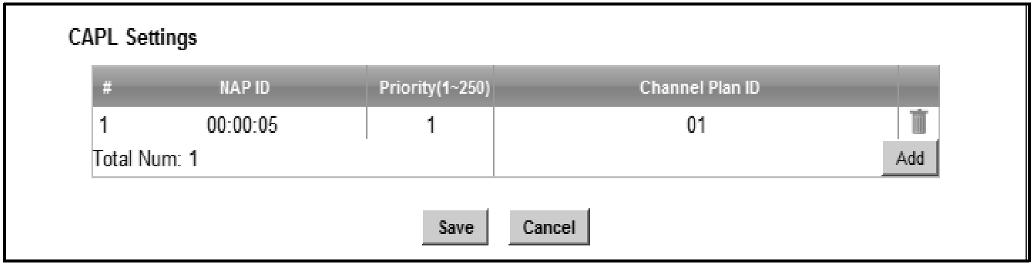
LABEL	DESCRIPTION
Channel Plan Settings - You can configure multiple ranges of frequencies to scan for different NAPs. The configured frequency ranges to scan must be within the Valid Band. Specify the Channel Plan to scan for each NAP on the CAPL Settings: Add screen (Section 6.6.1 on page 82).	
Start Frequency (KHz)	This indicates the beginning of a frequency band in kilohertz (KHz). Click this field to modify it. Enter the beginning frequency when you are adding an entry.
End Frequency (KHz)	This indicates the end of the frequency band in kilohertz (KHz). Click this field to modify it.
Step (KHz)	This indicates the frequency step within each band in kilohertz (KHz). Click this field to modify it. The minimum step is 250KHz and the maximum step is the difference between the start frequency and end frequency.
Bandwidth (MHz)	This indicates the bandwidth in megahertz (MHz). Click this field to modify it.
Delete	Click this button to remove an item from the list.
Add	Click this button to add an item to the list.
OK	Click this button to save any changes made to the list.
Valid Band Info - This table displays the entire frequency band the BM2022w supports. The frequency ranges to scan that you configured in Channel Plan Settings must be within this range.	
Band Start (KHz)	This indicates the beginning of the frequency band in kilohertz (KHz).
Band End (KHz)	This indicates the end of the frequency band in kilohertz (KHz).
Save	Click this to save the changes made.
Cancel	Click this avoid any changes made from being saved to your configuration.

6.6 CAPL Settings

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

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

Figure 33 CAPL Settings



CAPL Settings

#	NAP ID	Priority(1~250)	Channel Plan ID	
1	00:00:05	1	01	🗑

Total Num: 1

This screen contains the following fields:

Table 17 CAPL Settings

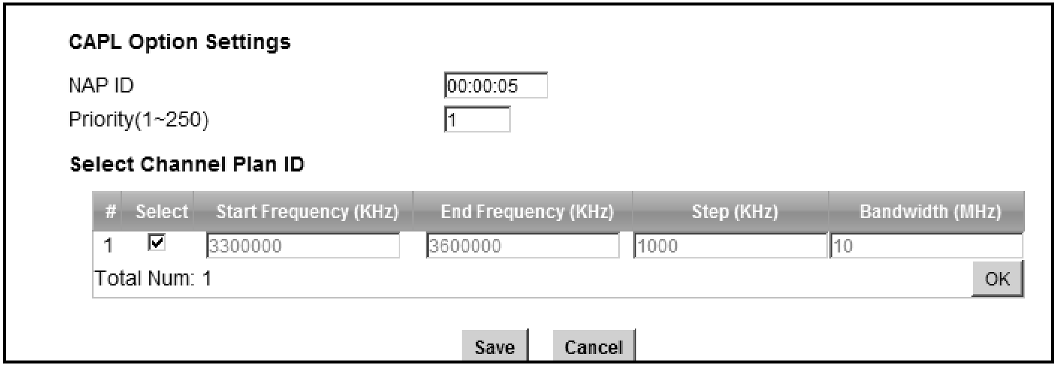
LABEL	DESCRIPTION
NAP ID	This displays the NAP ID.
Priority	This displays the priority for the NAP ID.
Channel Plan ID	This displays the Channel Plan ID.
Delete	Click this button to remove an item from the list.
Add	Click this button to add an item to the list.
Save	Click this to save the changes made.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

6.6.1 CAPL Settings: Add

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

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

Figure 34 CAPL Settings: Add



CAPL Option Settings

NAP ID: 00:00:05

Priority(1~250): 1

Select Channel Plan ID

#	Select	Start Frequency (KHz)	End Frequency (KHz)	Step (KHz)	Bandwidth (MHz)
1	☑	3300000	3600000	1000	10

Total Num: 1

This screen contains the following fields:

Table 18 CAPL Settings: Add

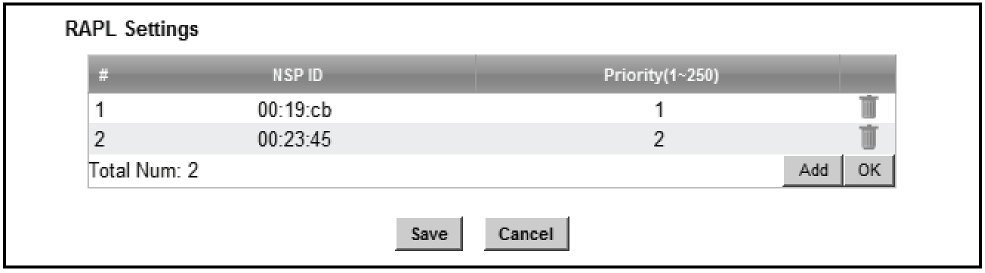
LABEL	DESCRIPTION
NAP ID	Specify the NAP ID in the format XX:XX:XX where X is a hexadecimal character. The NAP ID is typically the first three blocks of the BSID of the base station.
Priority	Specify the priority for the NAP ID. Enter 1-250 where 1 is the highest priority. The BM2022w will search for NAPs according to the priority specified. Priority may be determined by the number of base stations an NAP has, with a NAP having more base stations being assigned a higher priority. If the same priority is assigned to a NAP ID, the BM2022w will consider them as having equal priority.
Select Channel Plan ID	
Select	After clicking a Channel Plan ID entry in the list, you can click this check box to select it.
Start Frequency (KHz)	This indicates the beginning of a frequency band in kilohertz (KHz).
End Frequency (KHz)	This indicates the end of the frequency band in kilohertz (KHz).
Step (KHz)	This indicates the frequency step within each band in kilohertz (KHz).
Bandwidth (MHz)	This indicates the bandwidth in megahertz (MHz).
OK	Click this button to save any changes made to the list.
Save	Click this to save the changes made.
Cancel	Click this avoid any changes made from being saved to your configuration.

6.7 RAPL Settings

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

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

Figure 35 RAPL Settings



RAPL Settings

#	NSP ID	Priority(1~250)	
1	00:19:cb	1	
2	00:23:45	2	

Total Num: 2

This screen contains the following fields:

Table 19 RAPL Settings

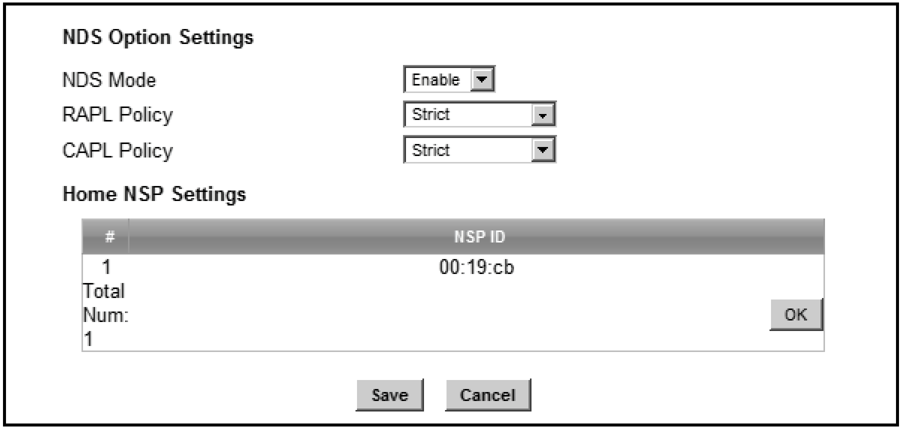
LABEL	DESCRIPTION
NSP ID	Specify the Network Service Provider (NSP) ID in the format XX:XX:XX where X is a hexadecimal character. If the Home NSP ID is entered in this list, the BM2022w will try to use it to establish a connection.
Priority	Specify the priority for the NSP. Enter 1-250 where 1 is the highest priority.
Delete	Click this button to remove an item from the list.
Add	Click this button to add an item to the list.
OK	Click this button to save any changes made to the list.
Save	Click this to save the changes made.
Cancel	Click this avoid any changes made from being saved to your configuration.

6.8 Home NSP Settings

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

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

Figure 36 Home NSP Settings



NDS Option Settings

NDS Mode: Enable

RAPL Policy: Strict

CAPL Policy: Strict

Home NSP Settings

#	NSP ID
1	00:19:cb

Total Num: 1

This screen contains the following fields:

Table 20 Home NSP Settings

LABEL	DESCRIPTION
NDS Option Settings	
NDS Mode	Select **Enable** to use NDS to establish connections to the Home NSP.

Table 20 Home NSP Settings (continued)

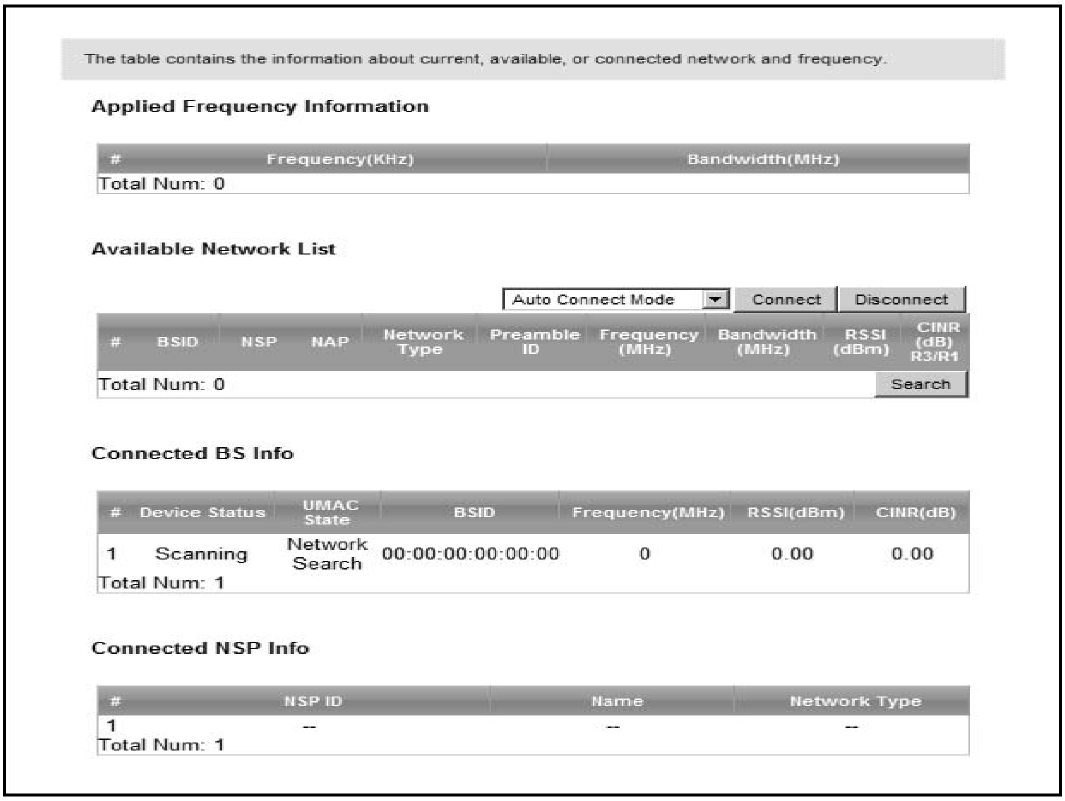
LABEL	DESCRIPTION
RAPL Policy	Select **Strict** to only allow V-NSPs specified in the RAPL to be used for establishing connections to the H-NSP. Select **Partially Flexible** to allow the BM2022w to use V-NSPs not specified in the RAPL to connect to the H-NSP. Before attempting V-NSPs not specified in the RAPL the BM2022w will first try the V-NSPs specified in the RAPL to connect to the H-NSP. Select **Flexible** to allow the BM2022w to use any V-NSPs for establishing connections to the H-NSP. V-NSPs specified in the RAPL will have the same priority as V-NSPs not specified in the RAPL.
CAPL Policy	Select **Strict** to only allow NAPs specified in the CAPL to be used for establishing connections to the H-NSP. Select **Partially Flexible** to allow the BM2022w to use NAPs not specified in the CAPL to connect to the H-NSP. Before attempting NAPs not specified in the CAPL the BM2022w will first try the NAPs specified in the CAPL to connect to the H-NSP. Select **Flexible** to allow the BM2022w to use any NAPs for establishing connections to the H-NSP. NAPs specified in the CAPL will have the same priority as NAPs not specified in the CAPL.
Home NSP Settings	
NSP ID	After clicking the entry in the NSP ID list, you can enter the NSP ID for the Home NSP here in the format XX:XX:XX where X is a hexadecimal character. Only one Home NSP can be entered.
OK	Click this button to save any changes made to the list.
Save	Click this button to save any changes made to the list. Note: If you change the **NDS Mode**, the BM2022w will reboot when you click save.
Cancel	Click this avoid any changes made from being saved to your configuration.

6.9 Connect

This screen allows you to view the available WiMAX frequency band(s) and base station(s) the BM2022w found through scanning and choose a base station to which to connect.

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

Figure 37 Connect Screen



The table contains the information about current, available, or connected network and frequency.

Applied Frequency Information

#	Frequency(KHz)	Bandwidth(MHz)
Total Num: 0		

Available Network List

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

Connected BS Info

#	Device Status	UMAC State	BSID	Frequency(MHz)	RSSI(dBm)	CINR(dB)
1	Scanning	Network Search	00:00:00:00:00:00	0	0.00	0.00
Total Num: 1						

Connected NSP Info

#	NSP ID	Name	Network Type
1	--	--	--
Total Num: 1			

This screen contains the following fields:

Table 21 Connect

LABEL	DESCRIPTION
Applied Frequency Information This table shows the scanning result you made in the **WiMAX > Profile > Frequency Settings** and **WiMAX > Wide Scan** screens. Note: You cannot see the wide scanning result that you made in **WiMAX > Wide Scan** screen if the **Join Wide Scan Result** is set to **No** in the **WiMAX > Profile > Frequency Settings** screen.	
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	

Table 21 Connect (continued)

LABEL	DESCRIPTION
Connected Mode	Select a connect mode: • **Auto Connect Mode** - This allows the BM2022w to connect to any of the base stations on the list automatically. • **Network Search Mode** - This allows the BM2022w to connect to a user-specified base station. Select this option, choose a base station, click **Connect**. • **NSP Mode** - This allows the BM2022w to connect to a base station with a user-specified NSP ID. To specify the NSP ID, select a result in the list and click **Connect**. The BM2022w will automatically connect to a base station with the same NSP ID, and the best CINR or RSSI. • **NSP/NAP Mode** - This allows the BM2022w to connect to a base station with a user-specified NSP ID and NAP ID. To specify the NSP ID and NAP ID, select a result in the list and click **Connect**. The BM2022w will automatically connect to a base station with the same NSP ID and NAP ID, and the best CINR or RSSI. • **NSP/NAP/BSID Mode** - This allows the BM2022w to connect to a base station with a user-specified NSP ID, NAP ID and BSID. To specify the NSP ID, NAP ID and BSID, select a result in the list and click **Connect**. The BM2022w will automatically connect to a base station with the same NSP ID, NAP ID and BSID, and the best CINR or RSSI.
Connect	Click this to connect to the selected base station.
Disconnect	Click this to disconnect from the selected base station.
BSID	This field displays the base station MAC address.
NSP	This field displays the NSP ID.
NAP	This field displays the NAP ID.
Network Type	This field displays the network type.
Preamble ID	This field displays the preamble ID. The preamble ID is the index identifier in the header of the base station’s broadcast messages. In the beginning of a mobile stations’s network entry process, it searches for the preamble and uses it to additional channel information. The preamble ID is used to synchronize the upstream and downstream transmission timing with the base station.
Frequency (MHz)	This field displays the center frequency the base station uses in kilohertz (KHz).
Bandwidth (MHz)	This field displays the frequency band bandwidth the base station uses in megahertz (MHz).
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 BM2022w scan for base stations in the frequency band(s) listed in the **Applied Frequency Information** table.
Connected BS Info	

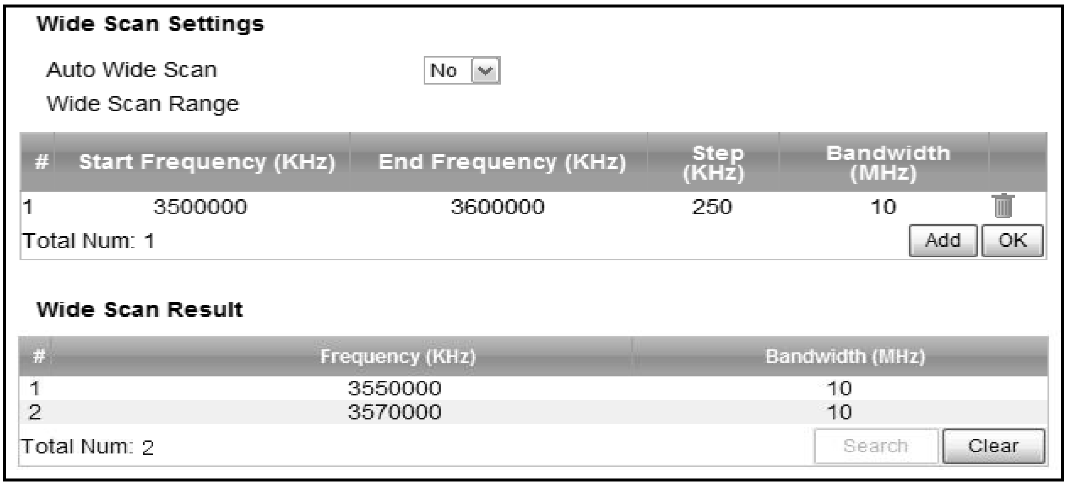
Table 21 Connect (continued)

LABEL	DESCRIPTION
Device Status	This field displays the BM2022w current status for connecting to the selected base station. **Scanning** - The BM2022w is scanning for available base stations. **Ready** - The BM2022w has finished scanning and you can connect to a base station. **Connecting** - The BM2022w attempts to connect to the selected base station. **Connected** - The BM2022w has successfully connected to the selected base station.
UMAC State	This field displays the status of the WiMAX connection between the BM2022w and the base station. **Network Search** - The BM2022w is scanning for any available WiMAX connections. **Disconnected** - No WiMAX connection is available. **Network Entry** - A WiMAX connection is initializing. **Normal** - The WiMAX connection has been successfully established.
BSID	This field displays the MAC address of the base station to which the BM2022w is connected.
Frequency (MHz)	This field displays the frequency the base station uses in megahertz (MHz).
RSSI (dBm)	This field displays the Received Signal Strength Indication (RSSI), which is an overall measurement of radio signal strength. A higher RSSI level indicates a stronger signal.
CINR (dB)	This field displays the average Carrier to Interference plus Noise Ratio for the current connection. This value is an indication of overall radio signal quality, where a higher value means a better quality signal.
Connected NSP Info	
NSP ID	This field displays the NSP ID of the connected NSP.
Name	This field displays the name of the connected NSP.
Network Type	This field displays the network type of the connected NSP.

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.



Wide Scan Settings

Auto Wide Scan: No

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

Figure 38 Wide Scan Screen

This screen contains the following fields:

Table 22 Wide Scan

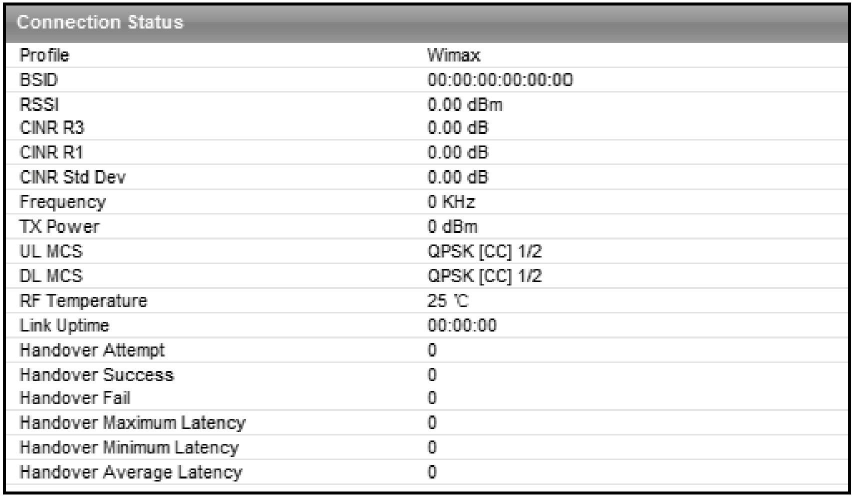
LABEL	DESCRIPTION
Wide Scan Settings	
Auto Wide Scan	Use this to enable (**Yes**) or disable (**No**) automatically scanning for base stations.
Wide Scan Range	
Start Frequency (KHz)	Enter the start frequency in kilohertz (KHz) for a wide scan range.
End Frequency (KHz)	Enter the end frequency in kilohertz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

6.10 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 39 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	25 ℃
Link Uptime	00:00:00
Handover Attempt	0
Handover Success	0
Handover Fail	0
Handover Maximum Latency	0
Handover Minimum Latency	0
Handover Average Latency	0

This screen contains the following fields:

Table 23 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 BM2022w is currently connected.
RSSI	This field displays the Received Signal Strength Indication (RSSI), which is an overall measurement of radio signal strength. A higher RSSI level indicates a stronger signal.
CINR R3	This field displays the average Carrier to Interference plus Noise Ratio (R3) for the current connection. This value is an indication of overall radio signal quality, where a higher value means a better quality signal.
CINR R1	This field displays the average Carrier to Interference plus Noise Ratio (R1) for the current connection. This value is an indication of overall radio signal quality, where a higher value means a better quality signal.
CINR Std Dev	This field displays the average Carrier to Interference plus Noise Ratio (Std Dev) for the current connection. This value is an indication of overall radio signal quality, where a higher value means a better quality signal.
Frequency	This field displays the frequency in kilohertz (KHz).
TX Power	This field displays the transmission power of the BM2022w in dBm.
UL MCS	This field displays the Uplink Modulation and Coding Sequence (UL MCS).
DL MCS	This field displays the Downlink Modulation and Coding Sequence (DL MCS).
RF Temperature	This field displays the temperature in centigrade of the BM2022w’s RF circuit.
Link Uptime	This field displays the length of time the current connection has been up.
Handover Success	This field displays how many times the BM2022w had ever successfully switched its connection from one base station to another base station, since the BM2022w last restarted.

Table 23 Link Status (continued)

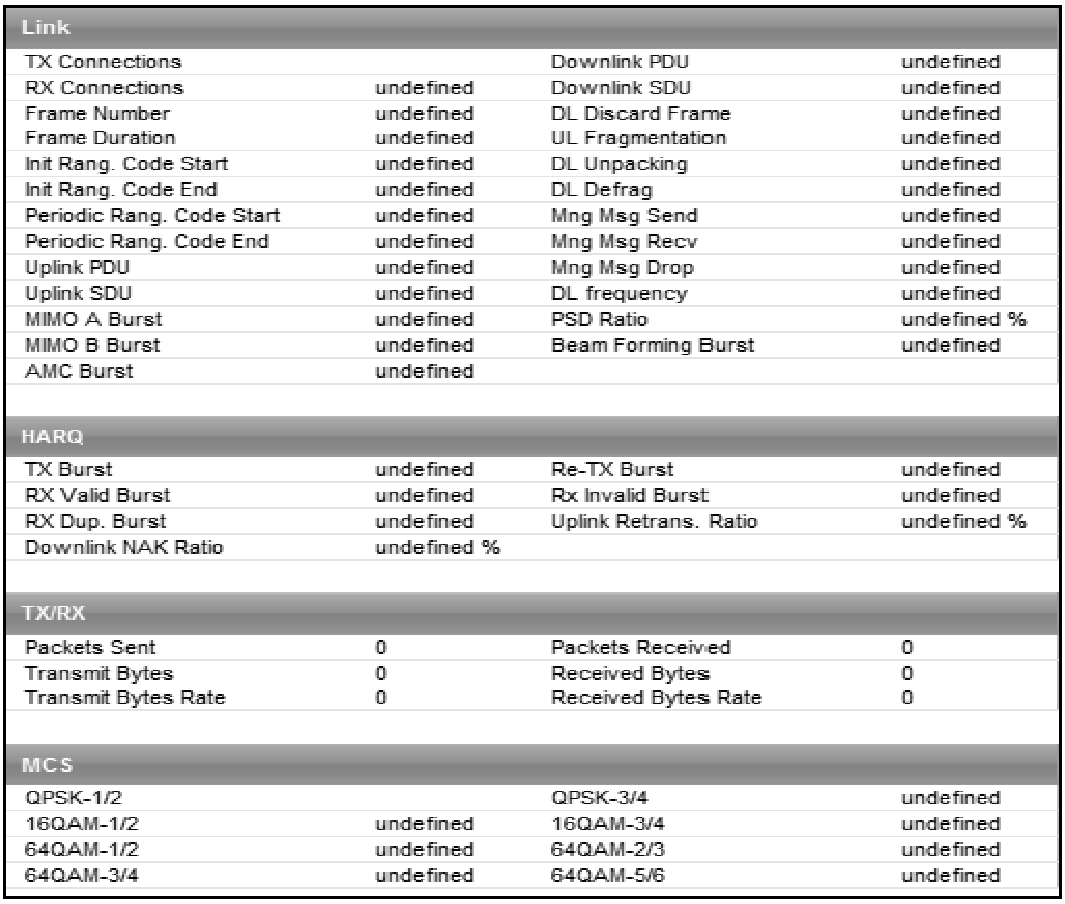
LABEL	DESCRIPTION
Handover Fail	This field displays how many times the BM2022w had been failed to switch its connection from one base station to another base station, since the BM2022w last restarted.
Handover Maximum Latency	This field displays the maximum latency for switching connections from one base station to another base station, since the BM2022w last restarted.
Handover Minimum Latency	This field displays the minimum latency for switching connections from one base station to another base station, since the BM2022w last restarted.
Handover Average Latency	This field displays the average latency for switching connections from one base station to another base station, since the BM2022w last restarted.

6.11 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 40 Link Statistics Screen



Link

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

HARQ

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

TX/RX

Packets Sent	0	Packets Received	0
Transmit Bytes	0	Received Bytes	0
Transmit Bytes Rate	0	Received Bytes Rate	0

MCS

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

This screen contains the following sections:

Table 24 Link Statistics

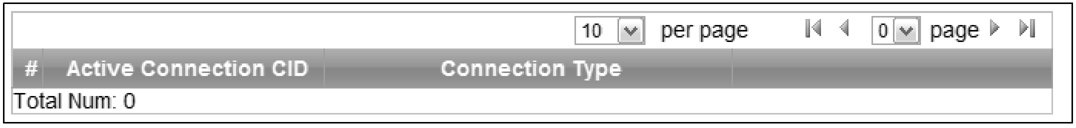
LABEL	DESCRIPTION
Link	This section provides a detailed overview of link statistics.
HARQ	This section provides a detailed overview of Hybrid Automatic Repeat Request link statistics.
TX/RX	This section provides a detailed overview of transmission and receiving link statistics.
MCS	This section provides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

6.12 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 41 Connection Info Screen



This screen contains the following fields:

Table 25 Connection Info

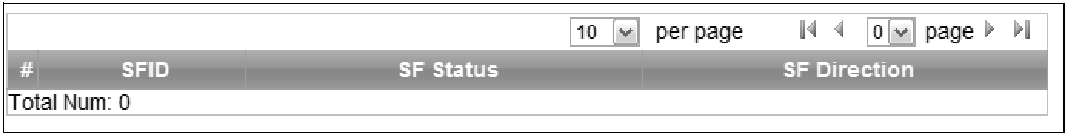
LABEL	DESCRIPTION
Active Connection CID	This displays the unique, unidirectional 16-bit Connection Identifier (CID) for an active connection.
Connection Type	This displays the type of connection.

6.13 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 42 Service Flow Screen



This screen contains the following fields:

Table 26 Service Flow

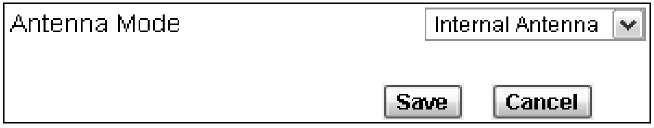
LABEL	DESCRIPTION
SFID	This displays a 32-bit service flow identifier.
SF Status	This display the service flow status.
SF Direction	This displays the service flow direction.

6.14 Antenna

This option lets you choose which type of antenna you wish to use in the device: Internal or External. The device has both and switching between them might give you a better connection.

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

Figure 43 Antenna Screen



Antenna Mode: Internal Antenna

This screen contains the following fields:

Table 27 Antenna

LABEL	DESCRIPTION
Antenna Mode	Select the type of Antenna that you wish to use: Internal or External
Save	Click this to save the changes made
Cancel	Click this avoid any changes made from being saved to your configuration.

7

Network Setting

7.1 Overview

This chapter shows you how to configure the BM2022w's network setting.

7.1.1 What You Need to Know

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

IP Address

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

Subnet Masks

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

DHCP

A DHCP (Dynamic Host Configuration Protocol) server can assign your BM2022w 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 BM2022w 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 BM2022w tells the DHCP clients that it itself is the DNS server. When a computer sends a DNS query to the BM2022w, the BM2022w 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 BM2022w can pass the DNS servers to the computers and the computers can query the DNS server directly without the BM2022w'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 BM2022w will broadcast its routing table periodically and incorporate the RIP information that it receives.
- **RX Only -** the BM2022w will not send any RIP packets but will accept all RIP packets received.
- **TX Only -** the BM2022w will send out RIP packets but will not accept any RIP packets received.
- **None -** the BM2022w 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 BM2022w 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.

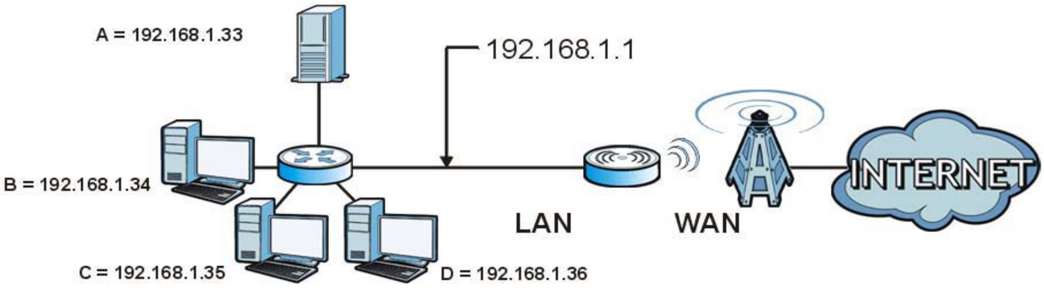
With port forwarding, you can forward incoming service requests to the server(s) on your local network. You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 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 44 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 BM2022w 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 BM2022w's WAN port receives a response with a specific port number and protocol ("incoming" port), the BM2022w 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 Huawei

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

The BM2022w only sends UPnP multicasts to the LAN.

Content Filter

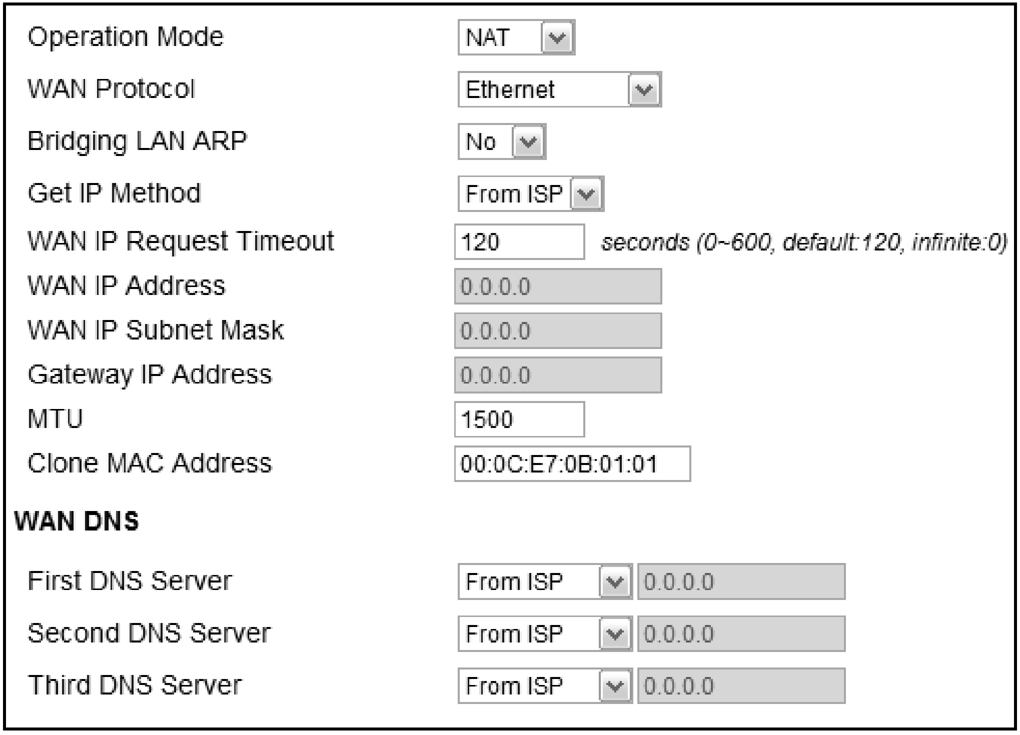
Internet content filtering allows you to create and enforce Internet access policies tailored to their needs. Content filtering is the ability to block certain specific URL keywords.

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 45 WAN Screen



Operation Mode	NAT
WAN Protocol	Ethernet
Bridging LAN ARP	No
Get IP Method	From ISP
WAN IP Request Timeout	120 *seconds (0~600, default:120, infinite:0)*
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
WAN DNS	
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 28 WAN

LABEL	DESCRIPTION
Operation Mode	Select the BM2022w's operational mode. • **Bridge** - This puts the BM2022w in bridge mode, acting as a transparent middle man between devices on the LAN and the devices on the WAN. • **Router** - Select Router from the drop-down list box if your ISP gives you one IP address only and you want multiple computers to share an Internet account. • **NAT** - This allows the BM2022w to tag frames for NAT, allowing devices on the LAN to use their own internal IP addresses while communicating with devices on the WAN.
WAN Protocol	Select the protocol the BM2022w uses to connect to the WAN. The options are: • **Ethernet** - Select this if you have a persistent connection to the network. • **PPPoE** - Select this if must log into the network before initiating a persistent connection. • **GRE Tunnel** - Select this if you connect to the network using Point-to-Point Protocol to create VPNs. • **EtherIP** - Select this if you need to tunnel Ethernet and IEEE 802.3 MAC frames across an IP Internet.
Bridging LAN ARP	This option enables or disables allow ARP requests to cross the BM2022w.
Get IP Method	Select how the BM2022w receives its IP address. • **User** - Select this to manually enter the IP address the BM2022w uses. • **From ISP** - Select to automatically get the IP address the BM2022w uses from the ISP.

Table 28 WAN (continued)

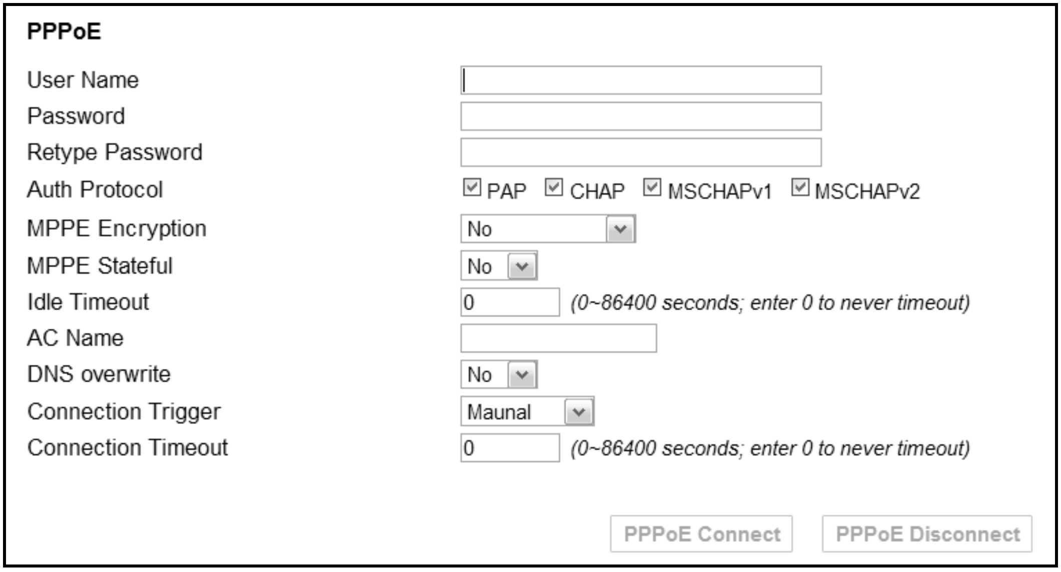
LABEL	DESCRIPTION
WAN IP Request Timeout	Enter the number of seconds the BM2022w waits for an IP from the ISP before it times out.
WAN IP Address	If the BM2022w gets its IP from the user, enter the IP address it is to use.
WAN IP Subnet Mask	If the BM2022w gets its IP from the ISP, enter the IP address it is to use.
Gateway IP Address	If the BM2022w 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 BM2022w. This is the largest protocol unit that the BM2022w allows to pass through it.
Clone MAC Address	Enter a MAC address here for registering bridged devices on the network if their current MAC addresses are causing problems. For example, this can happen when a desktop computer swaps network interface cards; the original NIC may have used its MAC address to register itself on the network and now the new NIC is unrecognized. Using a MAC address that you know is valid, i.e. a "clone", allows that device to stay registered.
First~Third DNS Server	Select how the BM2022w acquires its DNS server address. • **From ISP** - Select this to have the BM2022w acquire its DNS server address from the ISP. • **User Define** - Select this to manually enter the DNS server used by the BM2022w.

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 46 PPPoE Screen



PPPoE

User Name	
Password	
Retype Password	
Auth Protocol	☑ PAP ☑ CHAP ☑ MSCHAPv1 ☑ MSCHAPv2
MPPE Encryption	No
MPPE Stateful	No
Idle Timeout	0 *(0~86400 seconds; enter 0 to never timeout)*
AC Name	
DNS overwrite	No
Connection Trigger	Maunal
Connection Timeout	0 *(0~86400 seconds; enter 0 to never timeout)*

This screen contains the following fields:

Table 29 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 BM2022w supports the following: • **CHAP** - The Challenge Handshake Authentication Protocol (CHAP) uses PPP to authenticate remote devices using a three-way handshake and shared secret verification. • **PAP** - Password Authentication Protocol uses unencrypted plaintext to send a passwords for authentication over the network. It's probably not a good idea to rely on this for security. • **MS-CHAP v1/2** -This is Microsoft's variant of Challenge Handshake Authentication Protocol (CHAP). It allows for mutual authentication between devices.
MPPE Encryption	Use this option to enable or disable authentication through Microsoft Point-To-Point Encryption (MPPE) protocol.through Microsoft Point-To-Point Encryption (MPPE) protocol.
MPPE Stateful	Use this option to allow or disallow the BM2022w to use the Microsoft Point-To-Point Encryption (MPPE) protocol for stateful peer negotiation.
Idle Timeout	Enter the number of second the BM2022w 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 BM2022w to overwrite DNS static DNS entries on client devices.
Connection Trigger	Set whether the BM2022w is persistently connected to the WAN (**AlwaysOn**) or you must click the PPPoE Connect button each time you want to get on the WAN (**Manual**).
Connection Timeout	Enter in seconds the duration the BM2022w 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 47 GRE Screen

GRE Peer

Peer IP Address 0.0.0.0

This screen contains the following fields:

Table 30 GRE

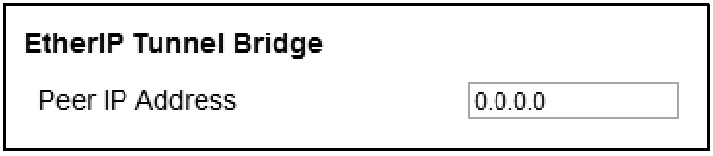
LABEL	DESCRIPTION
Peer IP Address	Enter the IP address of the GRE peer.

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 48 EtherIP Screen



EtherIP Tunnel Bridge

Peer IP Address: 0.0.0.0

This screen contains the following fields:

Table 31 EtherIP

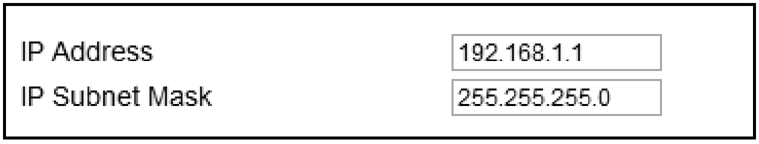
LABEL	DESCRIPTION
Peer IP Address	Enter the IP address of the EtherIP peer.

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 49 IP Screen



IP Address: 192.168.1.1

IP Subnet Mask: 255.255.255.0

This screen contains the following fields:

Table 32 IP

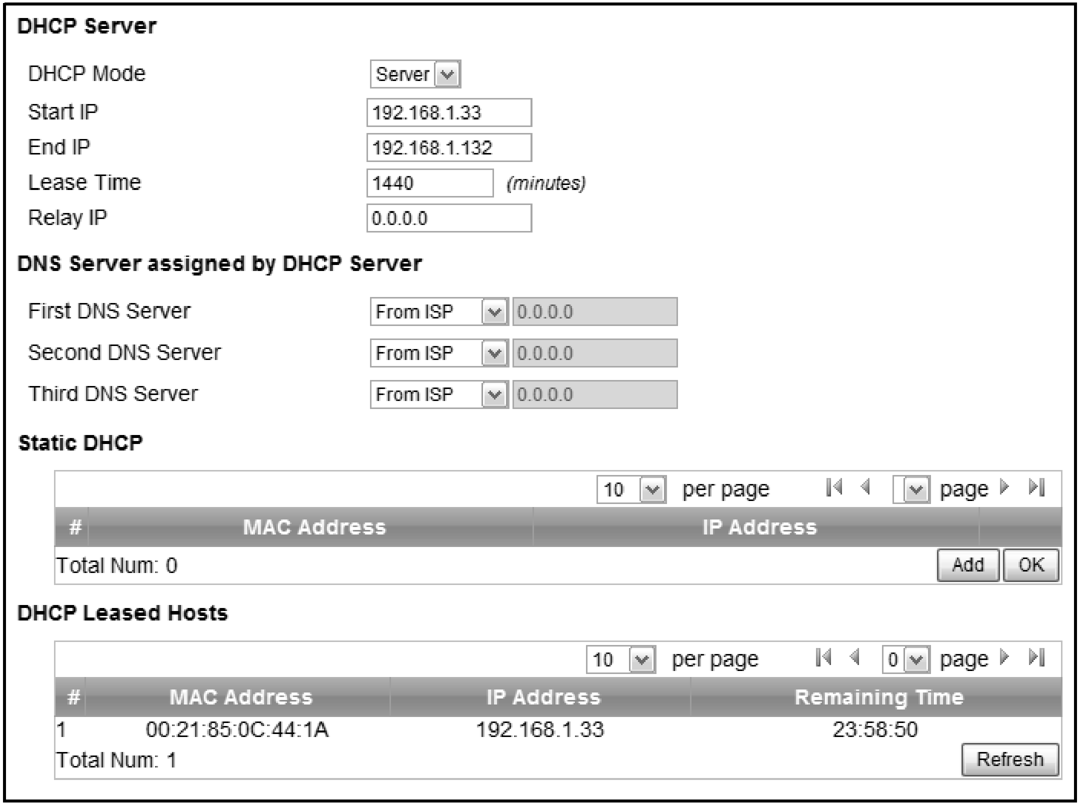
LABEL	DESCRIPTION
IP address	Enter the IP address of the LAN interface for the BM2022w.
IP Subnet Mask	Enter the IP subnet mask of the LAN interface for the BM2022w.

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 50 DHCP Screen



DHCP Server

DHCP Mode: Server
Start IP: 192.168.1.33
End IP: 192.168.1.132
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

10 per page, page

#	MAC Address	IP Address

Total Num: 0

DHCP Leased Hosts

10 per page, 0 page

#	MAC Address	IP Address	Remaining Time
1	00:21:85:0C:44:1A	192.168.1.33	23:58:50

Total Num: 1

This screen contains the following fields:

Table 33 DHCP

LABEL	DESCRIPTION
DHCP Server	
DHCP Mode	Select this if you want the BM2022w to be the DHCP server on the LAN. As a DHCP server, the BM2022w assigns IP addresses to DHCP clients on the LAN and provides the subnet mask and DNS server information. • **None** - This disables DHCP mode for the BM2022w. • **Server** - This sets the BM2022w as a DHCP server for the LAN. • **Relay** - This sets the BM2022w as a DHCP relay for the LAN, allowing it to pass-through IP addresses assigned to LAN devices from the ISP servers.
Start IP	Enter the start IP address from which the BM2022w begins allocating IP addresses.
End IP	Enter the end IP address at which the BM2022w ceases allocating IP addresses.

Table 33 DHCP (continued)

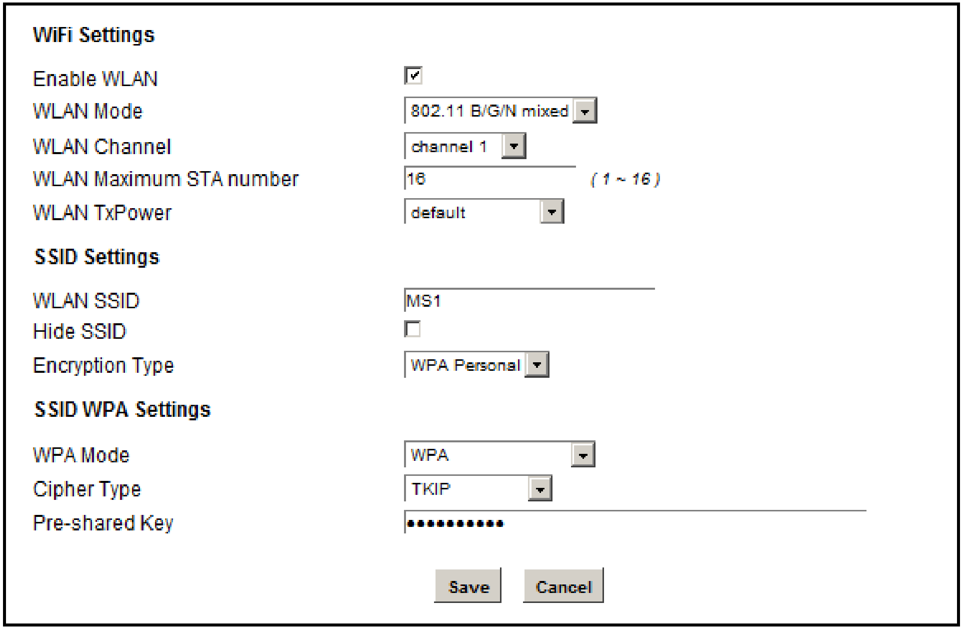
LABEL	DESCRIPTION
Lease Time	Enter the duration in minutes that devices on the LAN retain their DHCP-issued IP addresses. At the end of the lease time, they poll the BM2022w for a renewed or replacement IP.
Relay IP	Enter the name of the IP address to be used.
DNS Server Assigned by the DHCP Server	
First~Third DNS Server	Select how the BM2022w acquires its DNS server address. • **None** - Select this to not use a DNS server. • **From ISP** - Select this to have the BM2022w acquire its DNS server address from the ISP. • **User Define** - Select this to manually enter the DNS server used by the BM2022w.
Static DHCP	
MAC Address	This field displays the MAC address of the static DHCP client connected to the BM2022w.
IP Address	This field displays the IP address of the static DHCP client connected to the BM2022w.
Add	Click this to add a new static DHCP entry.
OK	Click this to save any changes made to this list.
DHCP Leased Hosts	
MAC Address	This displays the MAC address of the DHCP leased host.
IP Address	This displays the IP address of the DHCP leased host.
Remaining Time	This displays the how much time is left on the host’s lease.
Refresh	Click this to refresh the list.

7.8 WLAN

Use this screen to configure the connections between the BM2022w and the wireless clients that want to access the Internet.

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

Figure 51 WLAN Screen



WiFi Settings

Enable WLAN ☑

WLAN Mode 802.11 B/G/N mixed

WLAN Channel channel 1

WLAN Maximum STA number 16 (1 ~ 16)

WLAN TxPower default

SSID Settings

WLAN SSID MS1

Hide SSID □

Encryption Type WPA Personal

SSID WPA Settings

WPA Mode WPA

Cipher Type TKIP

Pre-shared Key ●●●●●●●●●●●

This screen contains the following fields:

Table 34 Network Setting > WLAN

LABEL	DESCRIPTION
WiFi Settings	
Enable WLAN	Select this to activate the wireless LAN.
WLAN Mode	Select **802.11B/G mixed** to allow both IEEE802.11b and IEEE802.11g compliant WLAN devices to associate with the BM2022w. Select **802.11B only** to allow only IEEE 802.11b compliant WLAN devices to associate with the BM2022w. Select **802.11A only** to allow only IEEE 802.11a compliant WLAN devices to associate with the BM2022w. Select **802.11G only** to allow only IEEE 802.11g compliant WLAN devices to associate with the BM2022w.
WLAN Channel	Select this option and set the operating frequency/channel depending on your particular region. Select **Auto** to have the BM2022w scan and find an available channel.
WLAN Maximum STA number	Enter the maximum number of wireless stations that is allowed to associate with the BM2022w.
WLAN TxPower	Select a number between 1 and 24 dB in the drop down box to control the strength of the connection signal, or leave it as **default** to let the BM2022w control this feature.
SSID Settings	
WLAN SSID	This field displays the name of the wireless network and it will appear to other computers that wish to connect wirelessly to the Internet.
Hide SSID	Select this to make the name of the network invisible to others.
Encryption Type	Select the type of encryption that the network will use: **None**, **WEP** or **WPA Personal**.

Table 34 Network Setting > WLAN

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

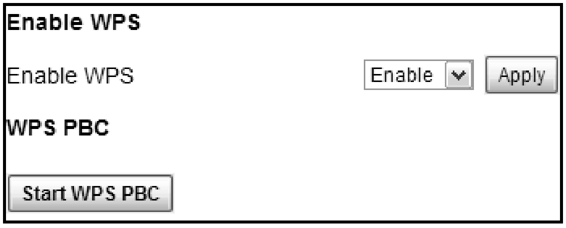
7.9 WPS

Use this screen to configure WiFi Protected Setup (WPS) on your BM2022w.

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

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

Figure 52 WPS Screen



Enable WPS

Enable WPS: Enable

WPS PBC

This screen contains the following fields:

Table 35 WPS

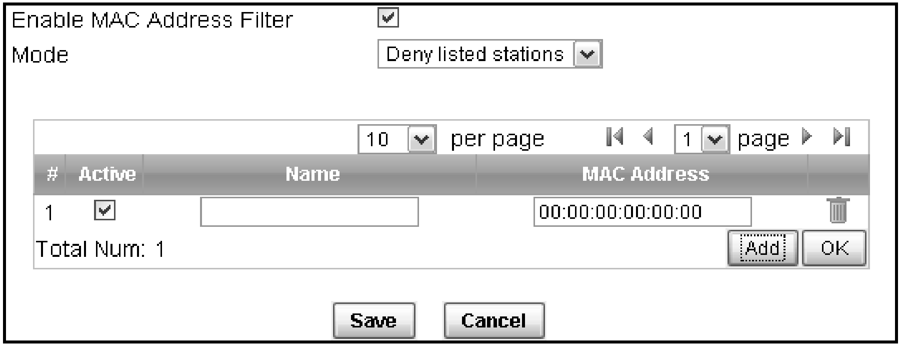
LABEL	DESCRIPTION
Enable WPS	Select **Enable** and click **Apply** to activate WPS on the BM2022w. Select **Disable** and click **Apply** to deactivate WPS.
Start WPS PBC	This field is available after you select **Enable** in the **Enable WPS** field and click **Apply**. Click this to activate the Push Button Configuration. After clicking this you will be able to use the WPS button at the back of the device to add new wireless clients. Note: You must press the WPS buttons within two minutes of each other.

7.10 MAC Address Filter

Use these screens to configure a MAC (Media Access Control) address filter to restrict access to the network.

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

Figure 53 MAC Address Filter Screen



Enable MAC Address Filter ☑

Mode: Deny listed stations

#	Active	Name	MAC Address
1	☑		00:00:00:00:00:00

Total Num: 1

This screen contains the following fields:

Table 36 MAC Address Filter

LABEL	DESCRIPTION
Enable MAC Address Filter	Select the check box to enable MAC address filtering. Then, the following fields display.
Mode	Define the filter action for the list of MAC addresses in the MAC address table. Select **Allow listed stations** to permit access to the BM2022w only to addresses listed. MAC addresses not listed will be denied access to the BM2022w. Select **Deny listed stations** to block access to the BM2022w to the computers or devices listed in this list.
#	This is the index number of the MAC address.
Active	Select this box to make the policy effective or ineffective for a particular device.

Table 36 MAC Address Filter

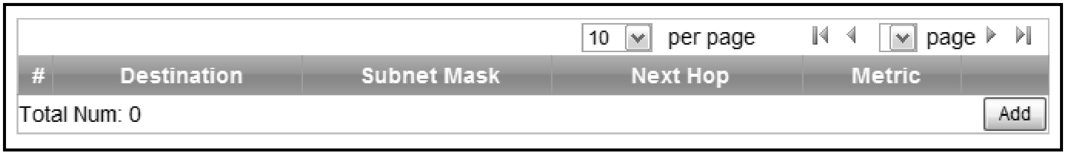
LABEL	DESCRIPTION
Name	Type the name of the device. The name can be up to 20 characters long, and any combination of letters, numbers or symbols.
MAC Address	Enter the MAC addresses of the wireless devices that are allowed or denied access to the BM2022w in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Delete	Click to delete a specific MAC address from the list.
Add	Click to add a MAC address to the list.
OK	Click this button when you are done adding a MAC Address.

7.11 Static Route

Use these settings to create fixed paths through the network.

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

Figure 54 Static Route Screen



This screen contains the following fields:

Table 37 Static Route

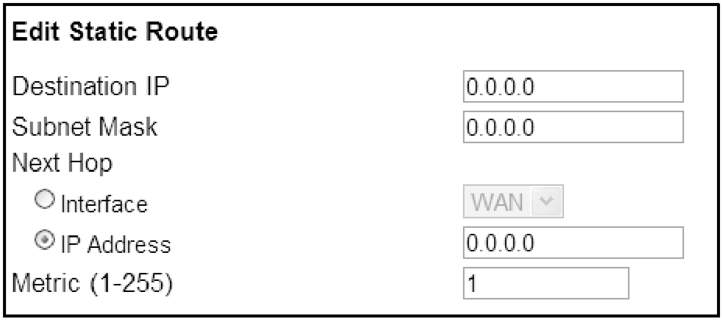
LABEL	DESCRIPTION
Destination	This field displays the destination IP address of the static route.
Subnet Mask	This field displays the subnet mask of the static route.
Next Hop	This field displays next hop information of the static route.
Metric	This field displays the static route metric.
Add	Click this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

7.12 Static Route Add

Use these settings to configure a static route.

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

Figure 55 Static Route Screen



Edit Static Route

Destination IP	0.0.0.0
Subnet Mask	0.0.0.0
Next Hop	
○ Interface	WAN
● IP Address	0.0.0.0
Metric (1-255)	1

This screen contains the following fields:

Table 38 Static Route

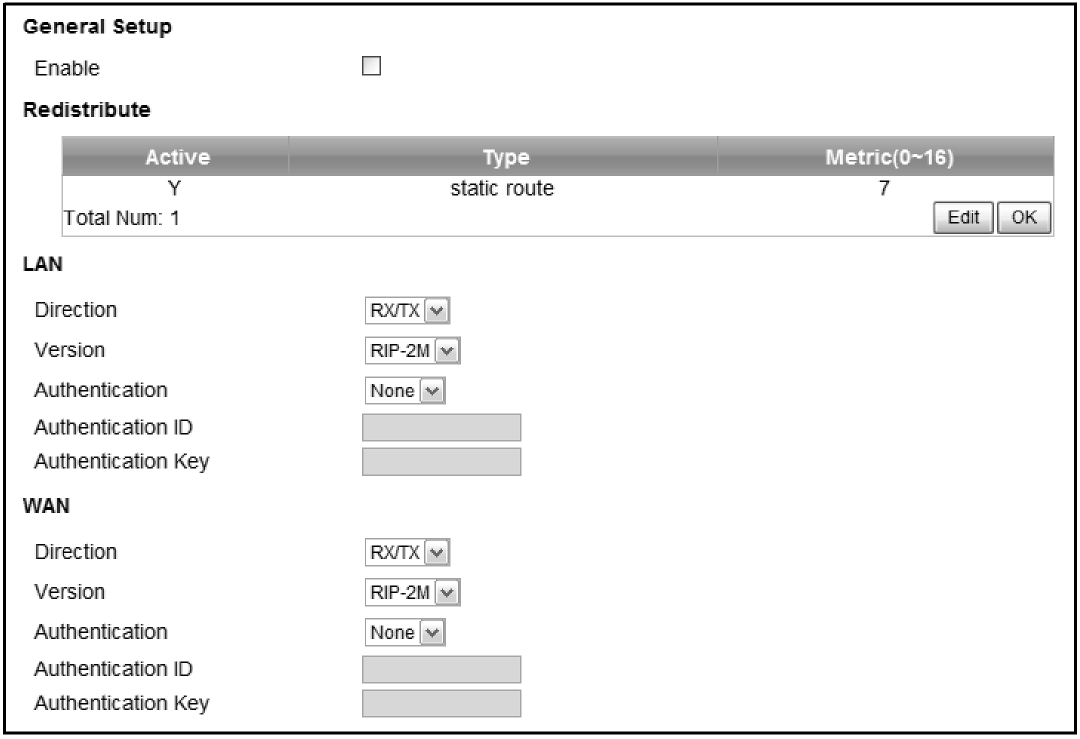
LABEL	DESCRIPTION
Destination IP	Enter the destination IP address of the static route.
Subnet Mask	Enter the subnet mask of the static route.
Next Hop	Select **Interface** and then select **WAN** or **LAN** for the next hop of the static route. If the next hop is an IP address rather than an interface on the BM2022w, select **IP Address** and enter the IP address.
Metric	Enter the static route metric.

7.13 RIP

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

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

Figure 56 RIP Screen



General Setup

Enable □

Redistribute

Active	Type	Metric(0~16)
Y	static route	7

Total Num: 1

LAN

Direction: RX/TX

Version: RIP-2M

Authentication: None

Authentication ID

Authentication Key

WAN

Direction: RX/TX

Version: RIP-2M

Authentication: None

Authentication ID

Authentication Key

This screen contains the following fields:

Table 39 RIP

LABEL	DESCRIPTION
General Setup	
Enable	Select this to enable RIP on the BM2022w.
Redistribute	
Active	This indicates whether a route is being redistributed.
Type	This indicates what type of route is being redistributed.
Metric	This indicates the metric that is being used for redistribution.
Edit	Click this to edit a selected route.
OK	Click this to save any changes to the redistribution table.
LAN	
Direction	Set the LAN network direction to use with RIP.
Version	Set the RIP version to use.
Authentication	Use this option to enable or disable RIP authentication.
Authentication ID	Enter the authentication ID to use for RIP authentication.
Authentication Key	Enter the authentication key to use for RIP authentication.
WAN	
Direction	Set the WAN network direction to use with RIP.
Version	Set the RIP version to use.

Table 39 RIP (continued)

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

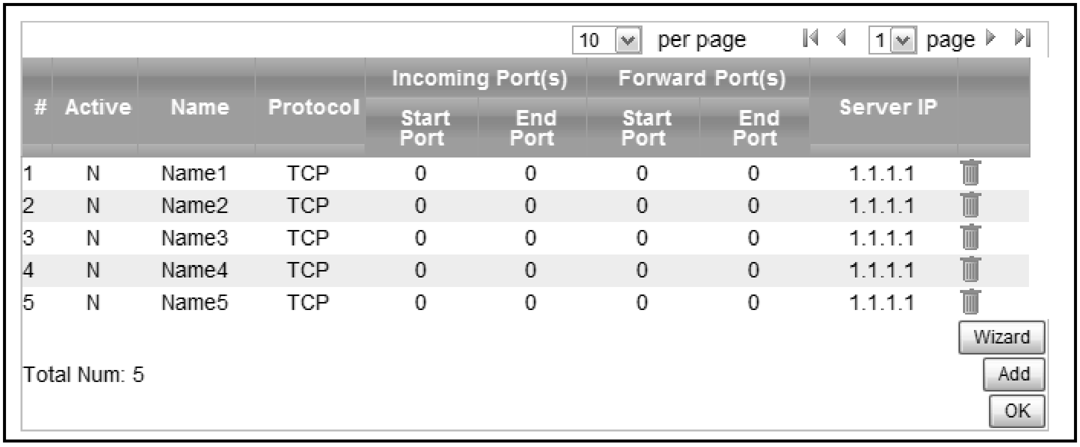
7.14 Port Forwarding

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

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

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

Figure 57 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

This screen contains the following fields:

Table 40 Port Forwarding

LABEL	DESCRIPTION
Active	This indicates whether the port forwarding rule is active or not.
Name	The displays the name of the port forwarding rule.
Protocol	This displays the protocol to which the port forwarding rule applies.
Incoming Port(s)	
Start Port	This displays the starting port number for incoming traffic for the port forwarding rule.
End Port	This displays the ending port number for incoming traffic for the port forwarding rule.
Forward Port(s)	
Start Port	This field displays the beginning of the range of port numbers forwarded by this rule.
End Port	This field displays the end of the range of port numbers forwarded by this rule. If it is the same as the **Start Port**, only one port number is forwarded.

Table 40 Port Forwarding (continued)

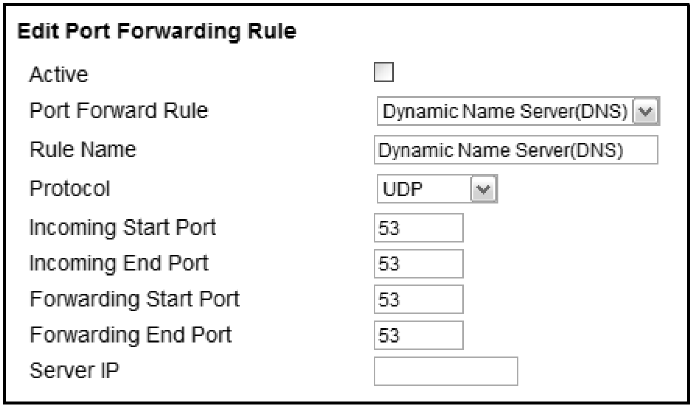
LABEL	DESCRIPTION
Server IP	This displays the IP address of the server to which packet for the selected port(s) are forwarded.
Delete	Click this to delete a specified rule.
Wizard	Click this to open the port forwarding "wizard".
Add	Click this to add a new port forwarding rule.
OK	Click this to save any changes made to the port forwarding list.

7.14.1 Port Forwarding Wizard

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

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

Figure 58 Port Forwarding Wizard Screen



Edit Port Forwarding Rule

Active	□
Port Forward Rule	Dynamic Name Server(DNS)
Rule Name	Dynamic Name Server(DNS)
Protocol	UDP
Incoming Start Port	53
Incoming End Port	53
Forwarding Start Port	53
Forwarding End Port	53
Server IP	

This screen contains the following fields:

Table 41 Port Forwarding Wizard

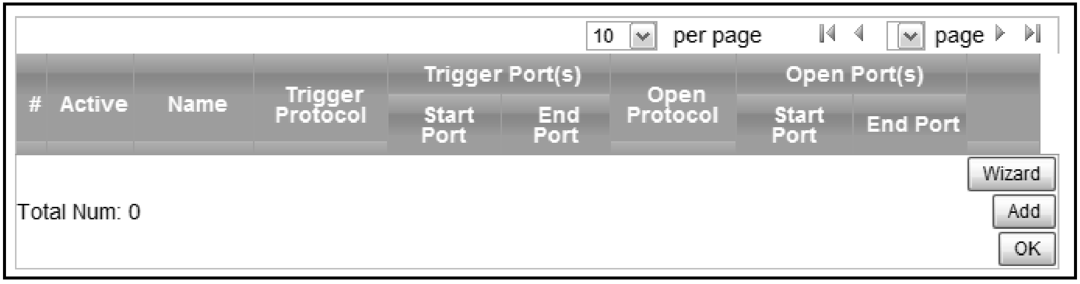
LABEL	DESCRIPTION
Active	Select this to make this port forwarding rule active.
Port Forward Rule	Select the type of port forwarding rule.
Rule Name	Enter a name for the port forwarding rule.
Protocol	Select the port forwarding protocol.
Incoming Start Port	Enter the starting port number for incoming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

7.15 Port Trigger

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

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

Figure 59 Port Trigger Screen



#	Active	Name	Trigger Protocol	Trigger Port(s)		Open Protocol	Open Port(s)	
				Start Port	End Port		Start Port	End Port

Total Num: 0

This screen contains the following fields:

Table 42 Port Trigger

LABEL	DESCRIPTION
Active	This indicates whether the port trigger rule is active or not.
Name	The displays the name of the port trigger rule.
Trigger Protocol	This displays the protocol to which the port trigger rule applies.
Trigger Port(s)	
Start / End Port	This displays the start / end trigger port for the port trigger rule. Click **Add** to create a new, empty rule, then enter the incoming port number or range of port numbers you want to forward to the IP address the BM2022w records. To forward one port number, enter the port number in the **Start Port** and **End Port** fields. To forward a range of ports, • enter the port number at the beginning of the range in the **Start Port** field • enter the port number at the end of the range in the **End Port** field. If you want to delete this rule, click the **Delete** icon.
Open Protocol	This indicates which protocol is used to open the port trigger ports.
Open Port(s)	
Start / End Port	This displays the start / end open port for the port trigger rule. Click **Add** to create a new, empty rule, then enter the outgoing port number or range of port numbers that makes the BM2022w record the source IP address and assign it to the selected incoming port number(s). To select one port number, enter the port number in the **Start Port** and **End Port** fields. To select a range of ports, • enter the port number at the beginning of the range in the **Start Port** field • enter the port number at the end of the range in the **End Port** field. If you want to delete this rule, click the **Delete** icon.

Table 42 Port Trigger (continued)

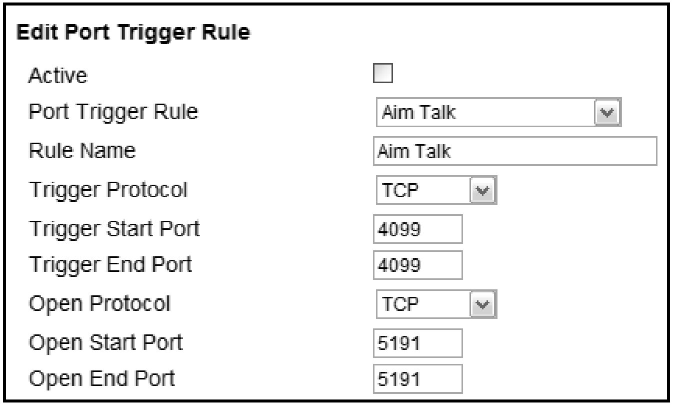
LABEL	DESCRIPTION
Delete	Click this to delete a specified rule.
Wizard	Click this to open the port trigger “wizard”.
Add	Click this to add a new port trigger rule.
OK	Click this to save any changes made to the port trigger list.

7.15.1 Port Trigger Wizard

Use the wizard to create a port trigger rules that will allow the BM2022w 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 60 Port Trigger Wizard Screen



Edit Port Trigger Rule

Active	□
Port Trigger Rule	Aim Talk
Rule Name	Aim Talk
Trigger Protocol	TCP
Trigger Start Port	4099
Trigger End Port	4099
Open Protocol	TCP
Open Start Port	5191
Open End Port	5191

This screen contains the following fields:

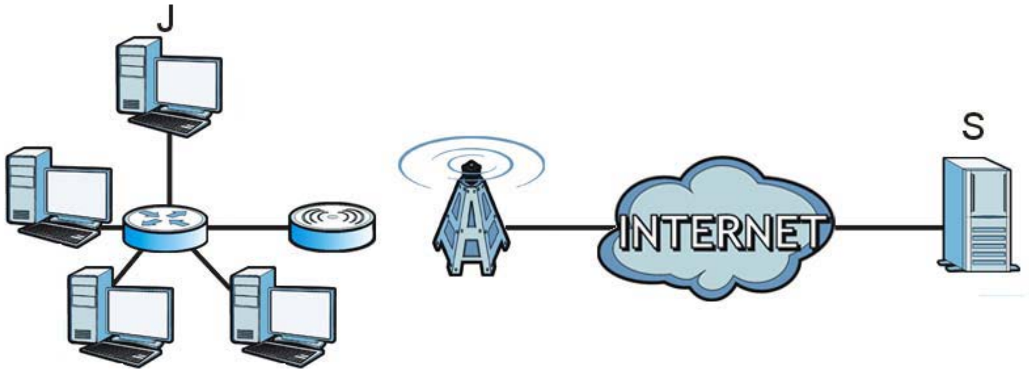
Table 43 Port Trigger Wizard

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

7.15.2 Trigger Port Forwarding Example

The following is an example of trigger port forwarding. In this example, **J** is Jane's computer and **S** is the Real Audio server.

Figure 61 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 BM2022w to record Jane's computer IP address. The BM2022w 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 BM2022w 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 BM2022w 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 BM2022w and going to the outside.

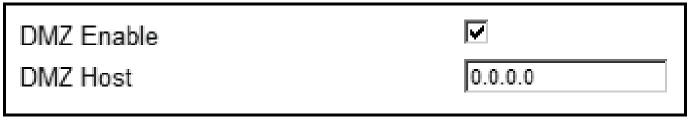
2 If an application needs a continuous data stream, that port (range) will be tied up so that another computer on the LAN can't trigger it.

7.16 DMZ

Use this page to set the IP address of your network DMZ (if you have one) for the WiMAX Device. All incoming packets received by this BM2022w'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.



DMZ Enable	☑
DMZ Host	0.0.0.0

Figure 62 DMZ Screen

This screen contains the following fields:

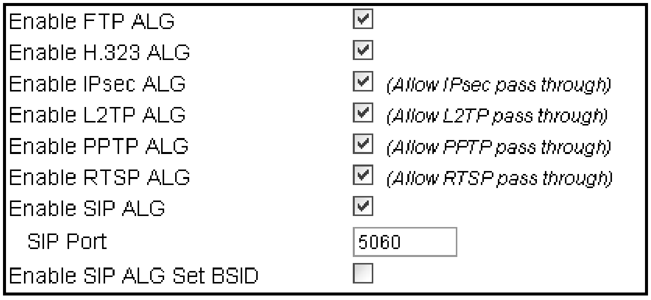
Table 44 DMZ

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

7.17 ALG

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

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



Enable FTP ALG	☑
Enable H.323 ALG	☑
Enable IPsec ALG	☑ *(Allow IPsec pass through)*
Enable L2TP ALG	☑ *(Allow L2TP pass through)*
Enable PPTP ALG	☑ *(Allow PPTP pass through)*
Enable RTSP ALG	☑ *(Allow RTSP pass through)*
Enable SIP ALG	☑
SIP Port	5060
Enable SIP ALG Set BSID	□

Figure 63 ALG Screen

This screen contains the following fields:

Table 45 Network Setting > NAT > 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 BM2022w'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 BM2022w's NAT.
Enable IPsec ALG	Turns on the IPsec ALG to detect IPsec traffic and helps build IPsec sessions through the BM2022w's NAT.
Enable L2TP ALG	Turns on the L2TP ALG to detect L2TP traffic and helps build L2TP sessions through the BM2022w's NAT.
Enable PPTP ALG	Turns on the PPTP ALG to detect PPTP traffic and helps build PPTP sessions through the BM2022w's NAT.

Table 45 Network Setting > NAT **>** ALG (continued)

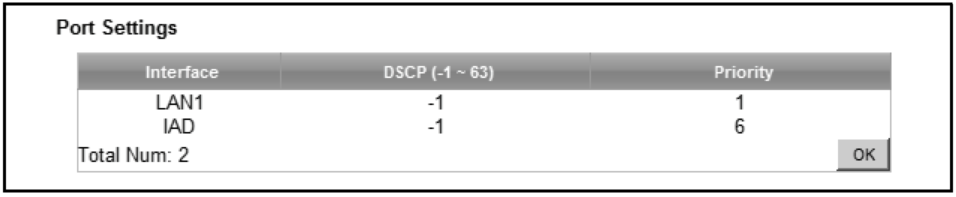
LABEL	DESCRIPTION
Enable RTSP ALG	Turns on the RTSP ALG to detect RTSP traffic and helps build RTSP sessions through the BM2022w's NAT.
Enable SIP ALG	Turns on the SIP ALG to detect SIP traffic and helps build SIP sessions through the BM2022w's NAT.
SIP Port	If you are using a custom UDP port number (not 5060) for SIP traffic, enter it here.
Enable SIP ALG Set BSID	Check this box to add the base station ID to the outgoing SIP messages. Select this option only if the media server forwarding calls requires this information.

7.18 QoS

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

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

Figure 64 QoS Screen



Port Settings

Interface	DSCP (-1 ~ 63)	Priority
LAN1	-1	1
IAD	-1	6

Total Num: 2

This screen contains the following fields:

Table 46 QoS

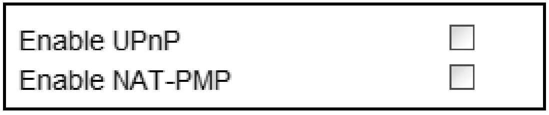
LABEL	DESCRIPTION
Interface	This displays the interface for the QoS rule. The **IAD** interface is for device management. Configure DiffServ Code Point (DSCP) and/or Priority marking based on which method is supported within your network. With DSCP you can use 64 (0-63) different markings, compared to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

7.19 UPnP

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

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

Figure 65 UPnP Screen



Enable UPnP □

Enable NAT-PMP □

This screen contains the following fields:

Table 47 UPnP

LABEL	DESCRIPTION
Enable UPnP	Select this to enable UPnP on the BM2022w.
Enable NAT-PMP	Select this to enable NAT Port Mapping Protocol on the BM2022w.

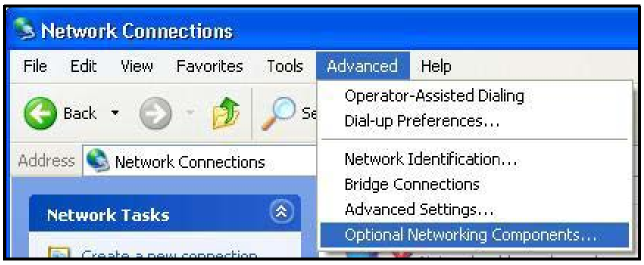
7.19.1 Installing UPnP in Windows XP

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

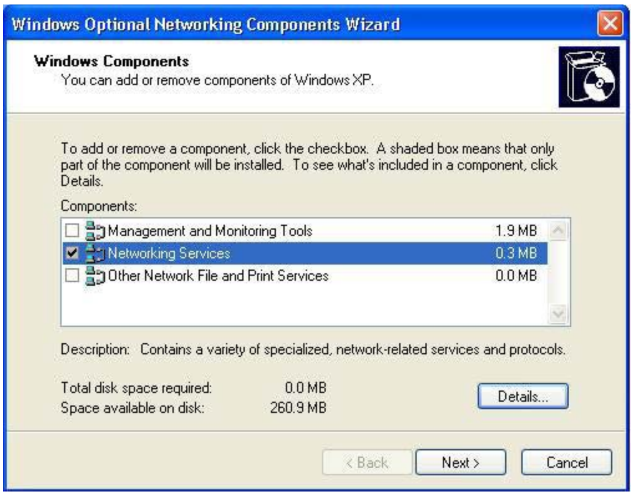
1 Click **Start** > **Control Panel**.

2 Double-click **Network Connections**.

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



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



Windows Optional Networking Components Wizard

Windows Components
You can add or remove components of Windows XP.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

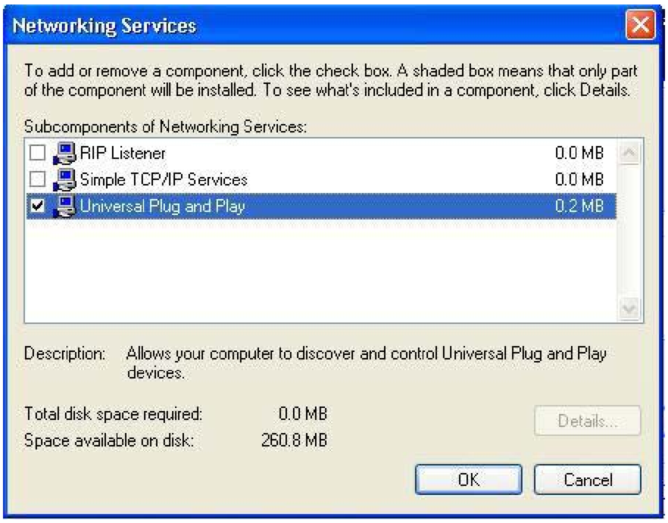
Components:

□	Management and Monitoring Tools	1.9 MB
☑	Networking Services	0.3 MB
□	Other Network File and Print Services	0.0 MB

Description: Contains a variety of specialized, network-related services and protocols.

Total disk space required: 0.0 MB
Space available on disk: 260.9 MB

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



Networking Services

To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Networking Services:

□	RIP Listener	0.0 MB
□	Simple TCP/IP Services	0.0 MB
☑	Universal Plug and Play	0.2 MB

Description: Allows your computer to discover and control Universal Plug and Play devices.

Total disk space required: 0.0 MB
Space available on disk: 260.8 MB

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

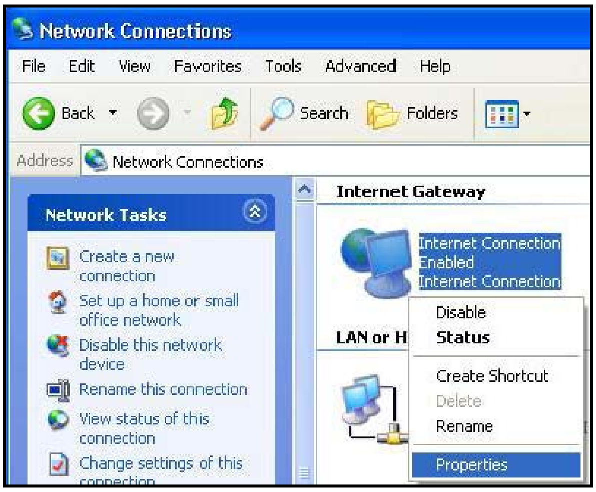
7.19.1.1 Auto-discover Your UPnP-enabled Network Device in Windows XP

This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the BM2022w.

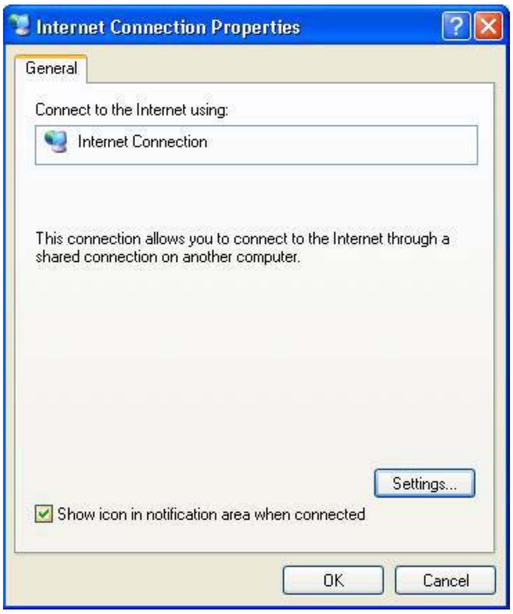
Make sure the computer is connected to a LAN port of the BM2022w. Turn on your computer and the BM2022w.

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.



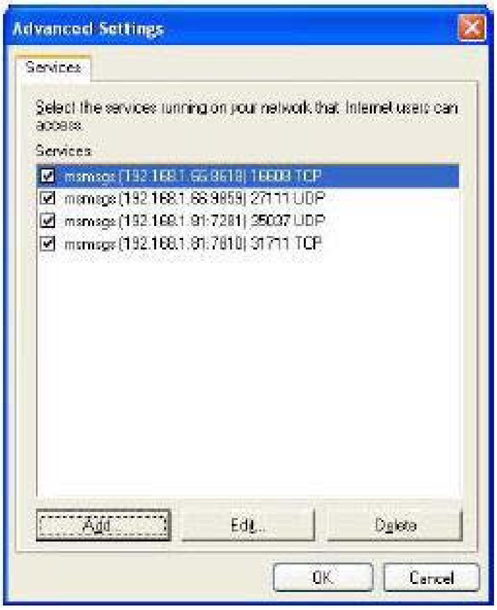
Connect to the Internet using:

Internet Connection

This connection allows you to connect to the Internet through a shared connection on another computer.

☑ Show icon in notification area when connected

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



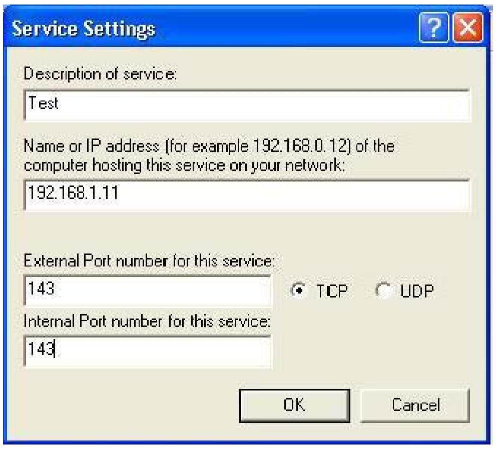
Advanced Settings

Services

Select the services running on your network that Internet users can access.

Services

- ☑ msmsgs (192.168.1.65:9618) 16603 TCP
- ☑ msmsgs (192.168.1.66:9859) 27111 UDP
- ☑ msmsgs (192.168.1.91:7281) 35037 UDP
- ☑ msmsgs (192.168.1.91:7810) 31711 TCP



Service Settings

Description of service: Test

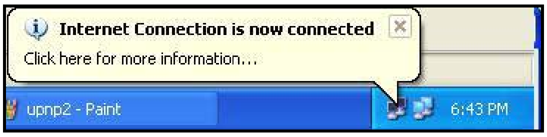
Name or IP address (for example 192.168.0.12) of the computer hosting this service on your network: 192.168.1.11

External Port number for this service: 143 ● TCP ○ UDP

Internal Port number for this service: 143

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

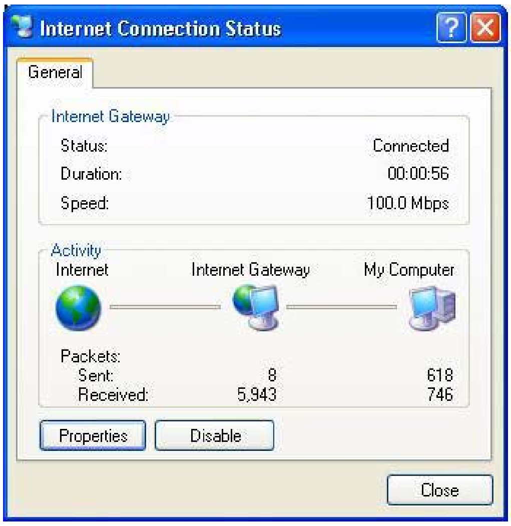
6 Select **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray.



Internet Connection is now connected

Click here for more information...

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



Internet Connection Status

General

Internet Gateway

Status: Connected

Duration: 00:00:56

Speed: 100.0 Mbps

Activity

	Internet Gateway	My Computer
Packets:		
Sent:	8	618
Received:	5,943	746

7.19.2 Web Configurator Easy Access

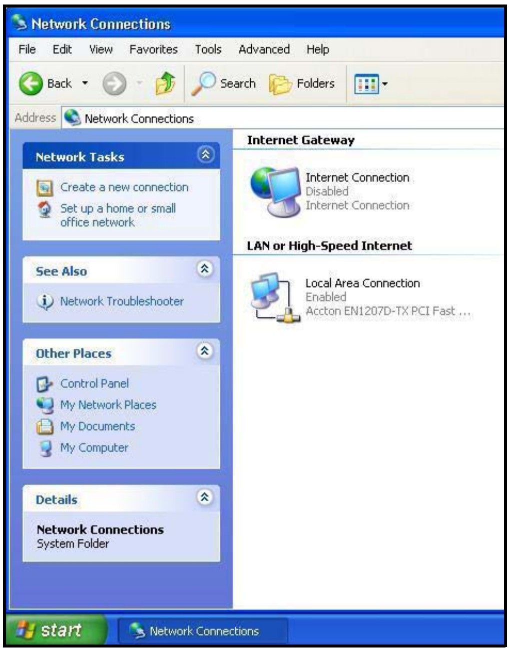
With UPnP, you can access the web-based configurator on the BM2022w without finding out the IP address of the BM2022w first. This becomes helpful if you do not know the IP address of the BM2022w.

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 BM2022w and select **Invoke**. The web configurator login screen displays.

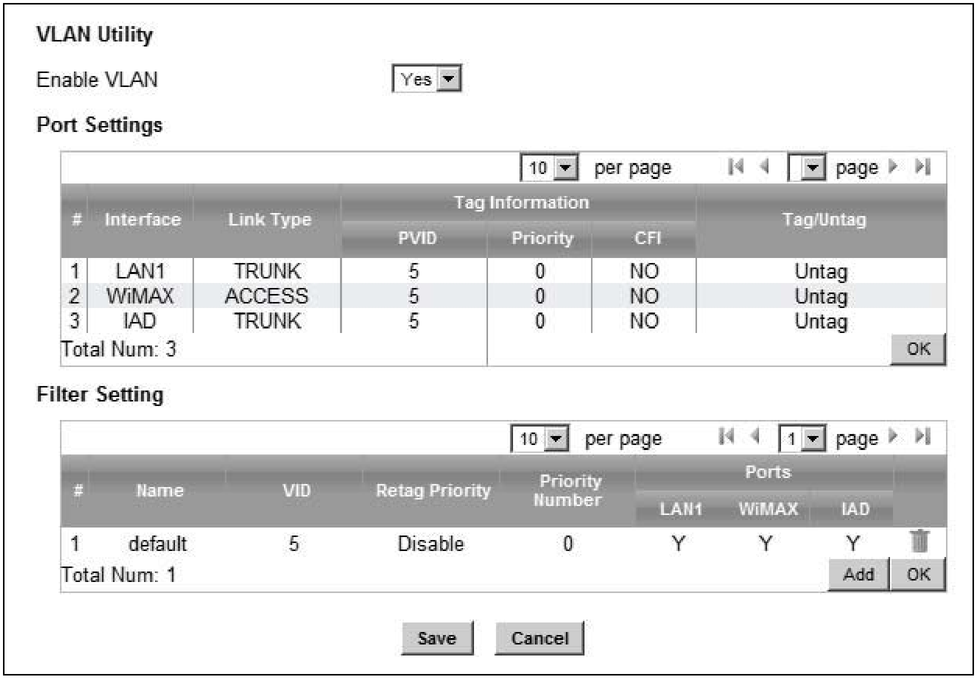
6 Right-click on the icon for your BM2022w and select **Properties**. A properties window displays with basic information about the BM2022w.

7.20 VLAN

Use this screen to configure port-based VLAN settings on the BM2022w. This screen allows you to assign port(s) to specific virtual LAN(s) in order to isolate traffic from different VLAN groups. See Section 4.11 on page 52 for example configurations for VLANs.

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

Figure 66 VLAN Screen



VLAN Utility

Enable VLAN: Yes

Port Settings

10 per page | page

#	Interface	Link Type	Tag Information			Tag/Untag
			PVID	Priority	CFI	
1	LAN1	TRUNK	5	0	NO	Untag
2	WiMAX	ACCESS	5	0	NO	Untag
3	IAD	TRUNK	5	0	NO	Untag

Total Num: 3

Filter Setting

10 per page | 1 page

#	Name	VID	Retag Priority	Priority Number	Ports		
					LAN1	WiMAX	IAD
1	default	5	Disable	0	Y	Y	Y

Total Num: 1

This screen contains the following fields:

Table 48 VLAN

LABEL	DESCRIPTION
VLAN Utility	
Enable VLAN	Select **Yes** to enable the VLAN function on the BM2022w. Note: To use VLAN on the BM2022w, you must switch the operation mode to "bridge" on the **Network Setting > WAN** screen. It will then require system restart to take effect.
Port Settings	
#	This is the index number of the port setting.
Interface	This displays the interface that the port setting applies to.
Link Type	Select **Access** if this port forwards traffic for only one VLAN. The device connected to an access port does not support VLAN tagged packets, so the BM2022w will remove packets forwarded out of this port. Packets received on access ports will be tagged with the specified PVID. Select **Trunk** to allow packets belonging to different VLAN groups to pass through the port. The device connected to this port should support VLAN tagged packets. You must configure **Filter Settings** for the port and VLAN ID for tagged packets to be forwarded. If received packets are already tagged, the PVID set for this port should not be the same as the VLAN IDs configured in **Filter Settings**. This will allow the tagged packets to be forwarded to the specified VLANs. If received packets are not tagged, the BM2022w will tag them with the PVID. Select **Hybrid** to allow the port to function as an access port and trunk port.

Table 48 VLAN

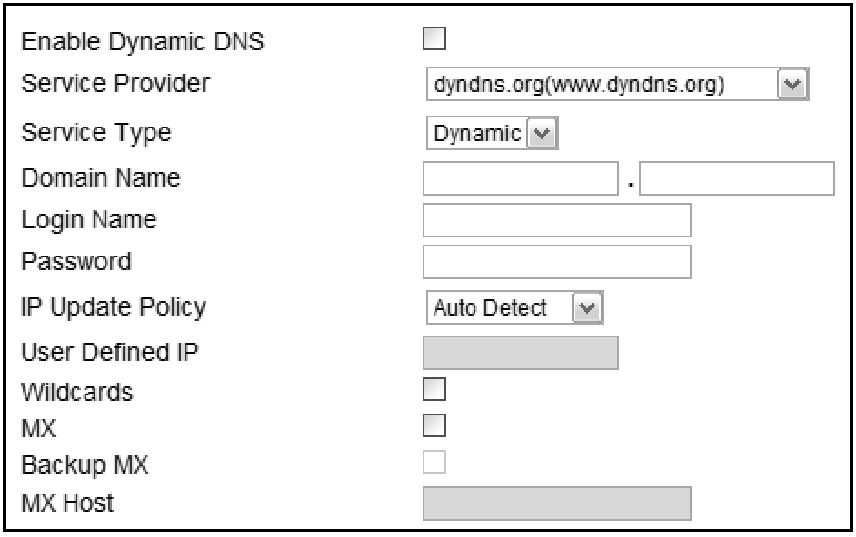
LABEL	DESCRIPTION
PVID	A **PVID** (Port VLAN ID) is a tag that adds to incoming untagged packets received on a port so that the packets are forwarded to the VLAN group that the tag defines. Enter a number between 1and 4094 as the port VLAN ID.
Priority	Enter a priority level (1~7) that the BM2022w assigns to packets belonging to this VLAN. Enter "0" for no priority assigned.
CFI	Select **Yes** if the CFI (Canonical Format Indicator) field in a received packet is set to 1, indicating non-Canonical Format. In this case, the packet should not be forwarded as it is to an untagged port.
Tag/Untag	You can only select **Tag** if the port is configured as a **Trunk** or **Hybrid** port. The BM2022w will receive and forward VLAN tagged packets. Untagged packets will be tagged with the PVID. If you select **Untag** the BM2022w will remove tags from tagged packets it forwards out of the port. Untagged packets received will be forwarded. If the port is an **Access** port, the BM2022w will add tags to untagged packets it receives and drop tagged packets it receives. If the port is a **Trunk** port, the BM2022w will add tags to untagged packets it receives and retag tagged packets.
OK	Click this to save the changes in the **Port Setting** section.
Filter Setting	
#	This is the index number of a filter.
Name	This is the name of a filter rule.
VID	This field displays the VLAN ID for the filter. Click this field to change the VLAN ID.
Retag Priority	Select **Yes** to retag the priority of a packet received on a **Trunk** or **Hybrid** port.
Priority Number	If Retag Priority is enabled, specify the new priority level (1~7) to tag. Enter "0" for no priority assigned.
Ports	This field displays the ports included in the filter. Click this field to select which ports to include.
Delete	Click this button to remove an item from the list.
Add	Click this button to add an item to the list.
OK	Click this button to save any changes made to the list.
Save	Click this to save the changes made.
Cancel	Click this avoid any changes made from being saved to your configuration.

7.21 DDNS

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

Click Network Setting > DDNS

Figure 67 DDNS Screen



Enable Dynamic DNS	□
Service Provider	dyndns.org(www.dyndns.org)
Service Type	Dynamic
Domain Name	.
Login Name	
Password	
IP Update Policy	Auto Detect
User Defined IP	
Wildcards	□
MX	□
Backup MX	□
MX Host	

This screen contains the following fields:

Table 49 DDNS

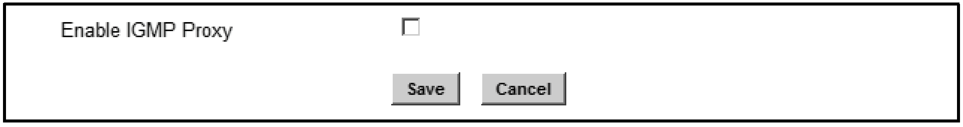
LABEL	DESCRIPTION
Enable Dynamic DNS	Select this to enable dynamic DNS on the BM2022w.
Service Provider	Select the dynamic DNS service provider for the BM2022w.
Service Type	Select the dynamic DNS service type.
Domain Name	Enter the domain name.
Login Name	Enter the user name.
Password	Enter the password.
IP Update Policy	Select the policy used by the BM2022w. Options are: • Auto Detect • WAN • User Defined
User Defined IP	If chose "User Defined" for the **IP Update Policy**, enter the user defined IP address.
Wildcards	Select this to allow a hostname to use wildcards such as "*".
MX	Select this to enable mail routing, if supported by the specified DYNDNS service provider.
Backup MX	Select this to enable a secondary mail routing, if supported by the specified DYNDNS service provider.
MX Host	Enter the host to which mail is routed when the MX option is selected.

7.22 IGMP Proxy

Use this page to enable IGMP Proxy on the WiMAX Device.

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

Figure 68 IGMP Proxy



Enable IGMP Proxy □

This screen contains the following fields:

Table 50 IGMP Proxy

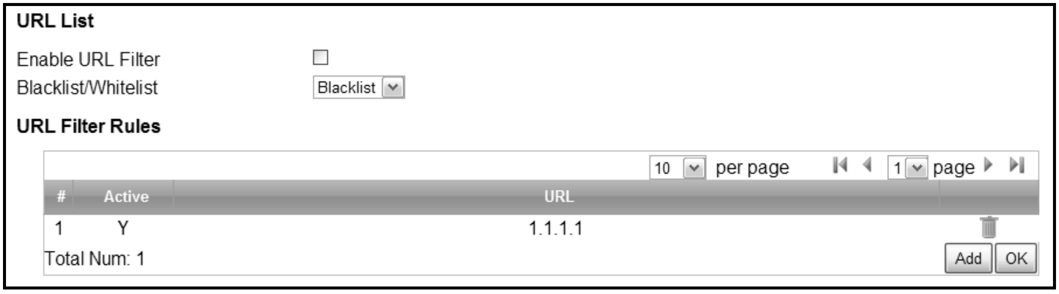
LABEL	DESCRIPTION
Enable IGMP Proxy	Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. Select this option to have the BM2022w act as an IGMP proxy. This allows the BM2022w to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Save	Click this to save the changes made.
Cancel	Click this avoid any changes made from being saved to your configuration.

7.23 Content Filter

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

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

Figure 69 Content Filter Screen



URL List

Enable URL Filter □

Blacklist/Whitelist Blacklist

URL Filter Rules

10 per page 1 page

#	Active	URL
1	Y	1.1.1.1

Total Num: 1

This screen contains the following fields:

Table 51 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 BM2022w.
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.

Table 51 Content Filter (continued)

LABEL	DESCRIPTION
Delete	Click this to delete a specified rule.
Add	Click this to add a new filter rule.
OK	Click this to save any changes made to the list.

8

Security

8.1 Overview

This chapter shows you how to configure the BM2022w'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 BM2022w's Security Features

The BM2022w 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 BM2022w can be used to prevent theft, destruction and modification of data.

The BM2022w 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.

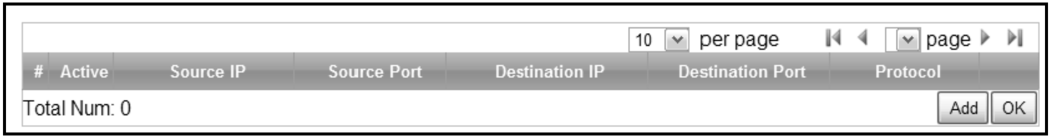
The BM2022w has one Ethernet (LAN) port. The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers will have access to Internet services such as e-mail, FTP and the World Wide Web. However, "inbound access" is not allowed (by default) 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 70 IP Filter Screen



#	Active	Source IP	Source Port	Destination IP	Destination Port	Protocol

Total Num: 0

This screen contains the following fields:

Table 52 IP Filter

LABEL	DESCRIPTION
Active	Indicates whether the current IP filter is active or not.
Source IP	This displays the source IP address for the IP filter rule. Click **Add** to create a new, empty rule, then enter the incoming IP address for the BM2022w to block. If you want to delete this rule, click the **Delete** icon.
Source Port	This displays the source port number for the IP filter rule. Click **Add** to create a new, empty rule, then enter the incoming port number for the BM2022w to block. If you want to delete this rule, click the **Delete** icon.
Destination IP	This displays the destination IP address for the IP filter rule. Click **Add** to create a new, empty rule, then enter the outgoing IP address for the BM2022w to block. If you want to delete this rule, click the **Delete** icon.
Destination Port	This displays the destination port number for the IP filter rule. Click **Add** to create a new, empty rule, then enter the outgoing port number for the BM2022w to block. If you want to delete this rule, click the **Delete** icon.
Protocol	This displays the protocol blocked by the IP filter rule. Click **Add** to create a new, empty rule, then select the protocol type for the BM2022w to block. If you want to delete this rule, click the **Delete** icon.
Delete	Click this to delete a specified rule.
Add	Click this to add a new filter rule.
OK	Click this to save any changes made to the list.

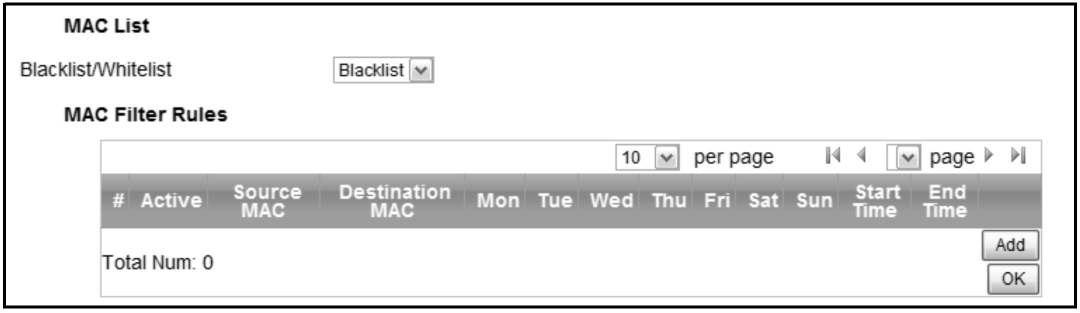
8.3 MAC Filter

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

Note: This feature only works when the BM2022w is in bridge mode.

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

Figure 71 MAC Filter Screen



MAC List

Blacklist/Whitelist: Blacklist

MAC Filter Rules

10 per page | page

#	Active	Source MAC	Destination MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time

Total Num: 0

This screen contains the following fields:

Table 53 MAC Filter

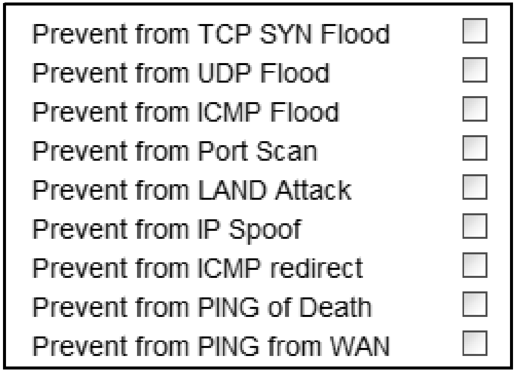
LABEL	DESCRIPTION
Blacklist/Whitelist	Select either whitelist or blacklist for viewing and editing.
Source MAC	This displays the source MAC for the MAC filter rule. Click **Add** to create a new, empty rule, then enter the incoming MAC address for the BM2022w to block. If you want to delete this rule, click the **Delete** icon.
Destination MAC	This displays the destination MAC for the MAC filter rule. Click **Add** to create a new, empty rule, then enter the outgoing MAC address for the BM2022w to block. If you want to delete this rule, click the **Delete** icon.
Mon ~ Sun	Select which days of the week you want the filter rule to be effective.
Start / End Time	Select what time each day you want the filter rule to be effective. Enter times in 24-hour format; for example, 3:00pm should be entered as 15:00.
Add	Click this to add a new filter rule.
OK	Click this to save any changes made to the list.

8.4 DDOS

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

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

Figure 72 DDOS Screen



Prevent from TCP SYN Flood □
Prevent from UDP Flood □
Prevent from ICMP Flood □
Prevent from Port Scan □
Prevent from LAND Attack □
Prevent from IP Spoof □
Prevent from ICMP redirect □
Prevent from PING of Death □
Prevent from PING from WAN □

This screen contains the following fields:

Table 54 DDOS

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

Table 54 DDOS (continued)

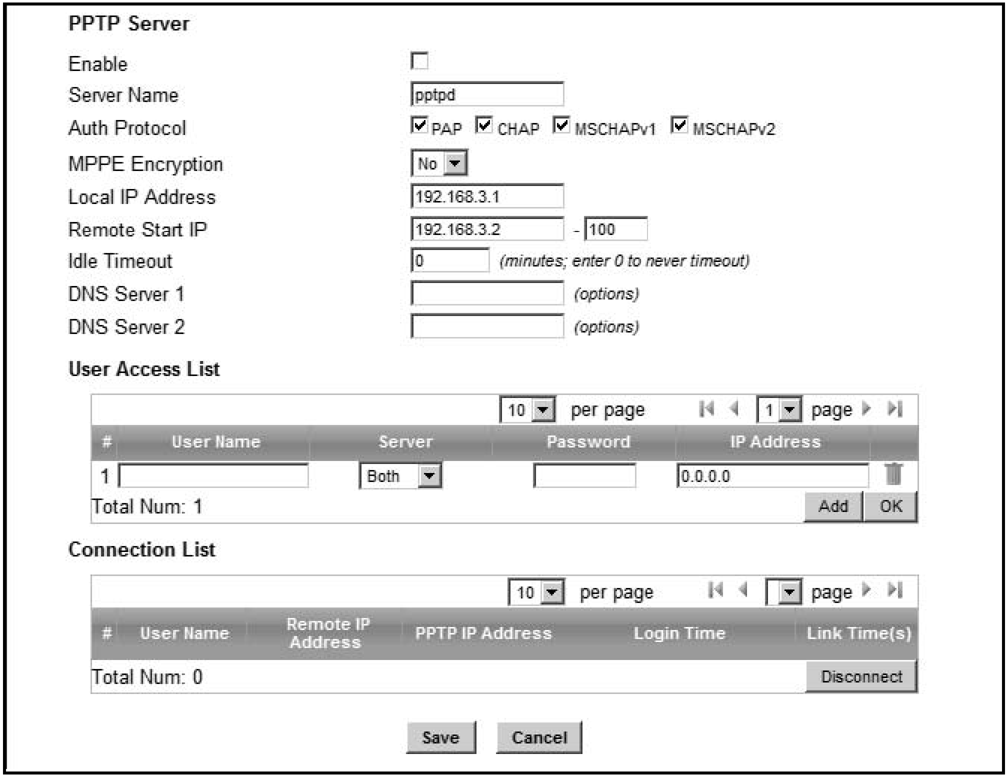
LABEL	DESCRIPTION
Prevent from PING of Death	Select this to monitor for and block ping of death attacks. A Ping of Death (POD) attack is one where larger-than-allowed ping packets are fragmented then sent against a client device. This results in the client device suffering from a buffer overflow and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

8.5 PPTP VPN Server

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

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

Figure 73 PPTP Server



PPTP Server

Enable □

Server Name pptpd

Auth Protocol ☑ PAP ☑ CHAP ☑ MSCHAPv1 ☑ MSCHAPv2

MPPE Encryption No

Local IP Address 192.168.3.1

Remote Start IP 192.168.3.2 - 100

Idle Timeout 0 *(minutes; enter 0 to never timeout)*

DNS Server 1 *(options)*

DNS Server 2 *(options)*

User Access List

10 per page 1 page

#	User Name	Server	Password	IP Address
1		Both		0.0.0.0

Total Num: 1

Connection List

10 per page page

#	User Name	Remote IP Address	PPTP IP Address	Login Time	Link Time(s)

Total Num: 0

This screen contains the following fields:

Table 55 PPTP Server

LABEL	DESCRIPTION
PPTP Server	
Enable	Use this field to turn the BM2022w’S PPTP VPN function on or off.
Server Name	Enter the server name for the PPTP VPN connection.

Table 55 PPTP Server

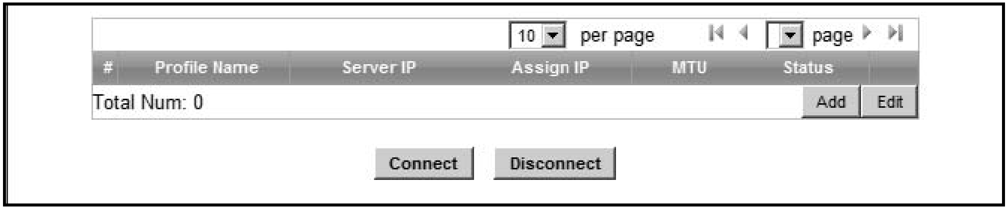
LABEL	DESCRIPTION
Auth Protocol	Select the Authentication Protocol allowed for the connection. Options are: **PAP** - Password Authentication Protocol (PAP) authentication occurs in clear text and does not use encryption. It’s probably not a good idea to rely on this for security. **CHAP** - Challenge Handshake Authentication Protocol (CHAP) provides authentication through a shared secret key and uses a three way handshake. **MSCHAPv1** - Microsoft CHAP v1 (MSCHAPv1) provides authentication through a shared secret key and uses a three way handshake. It provides improved usability with Microsoft products. **MSCHAPv2** - Microsoft CHAP v2 (MSCHAPv2) provides encryption through a shared secret key and uses a three way handshake. It provides additional security over **MSCHAPv1**, including two-way authentication.
MPPE Encryption	If **MSCHAPv1** or **MSCHAPv2** is selected as an **Auth Protocol**, use the drop-down list box to select the type of Microsoft Point-to-Point Encryption (MPPE). Options are: **MPPE 40 -** MPPE with 40 bit session key length **MPPE 128 -** MPPE with 128 bit session key length Auto - Automatically select either MPPE 40 or MPPE 128
Local IP Address	Enter the local endpoint for the PPTP connection.
Remote Start IP	Enter the local IP address range the BM2022w assigns to remote users if the remote client device is set to obtain an IP address automatically.
Idle Timeout	Enter the time in minutes to timeout PPTP connections.
DNS Server 1 DNS Server 2	Specify the IP addresses of DNS servers to assign to the remote users.
User Access List	
User Name	Enter the user name for the remote user.
Server	Select the server that the remote user has access to: **PPTPD**, **L2TPD** or **Both**.
Password	Enter the password for the remote user.
IP Address	Enter the local IP address the BM2022w assigns to the remote user. Entering 0.0.0.0 indicates the local IP address will be dynamically assigned.
Delete	Select an entry and click this to delete it.
Add	Click this to create a new entry.
OK	Click this to save the changes.
Connection List	
User Name	This displays the user name for the remote user.
Remote IP Address	This displays the remote endpoint IP address of the remote user.
PPTP IP Address	This displays the local IP address of the PPTP server.
Login Time	This displays the time the PPTP connection started.
Link Time(s)	This displays the duration of the PPTP connection.

8.6 PPTP VPN Client

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

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

Figure 74 PPTP Client



#	Profile Name	Server IP	Assign IP	MTU	Status

Total Num: 0

This screen contains the following fields:

Table 56 PPTP Client

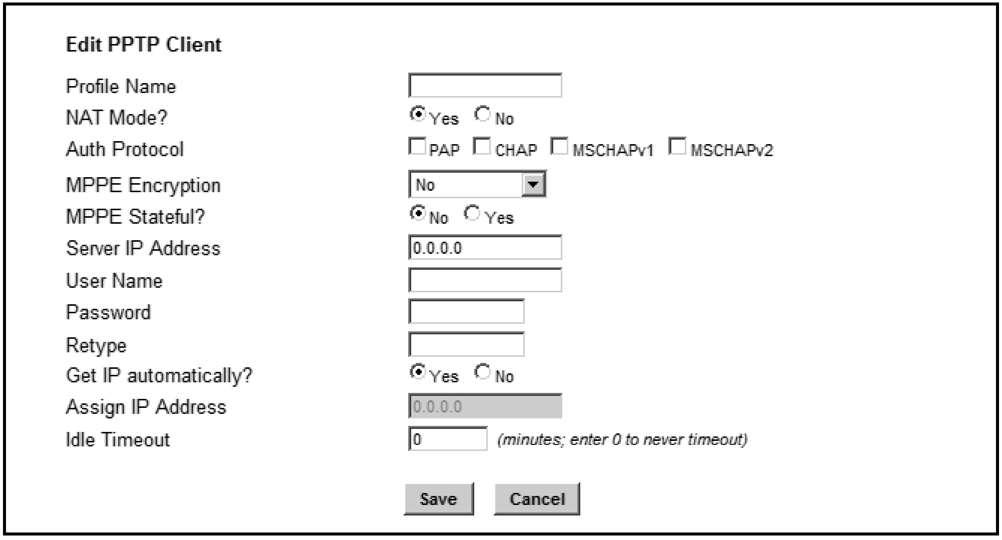
LABEL	DESCRIPTION
#	This is the index number of the connection.
Profile Name	This is the name of this client connection.
Server IP	This is the IP address of the PPTP VPN server.
Assign IP	This is the local IP address the client assigns to itself or is assigned by the server.
MTU	This field indicates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

8.7 PPTP VPN Client: Add

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

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

Figure 75 PPTP Client: Add



Edit PPTP Client

Profile Name	
NAT Mode?	● Yes ○ No
Auth Protocol	□ PAP □ CHAP □ MSCHAPv1 □ MSCHAPv2
MPPE Encryption	No
MPPE Stateful?	● No ○ Yes
Server IP Address	0.0.0.0
User Name	
Password	
Retype	
Get IP automatically?	● Yes ○ No
Assign IP Address	0.0.0.0
Idle Timeout	0 *(minutes; enter 0 to never timeout)*

This screen contains the following fields:

Table 57 PPTP Client: Add

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

Table 57 PPTP Client: Add

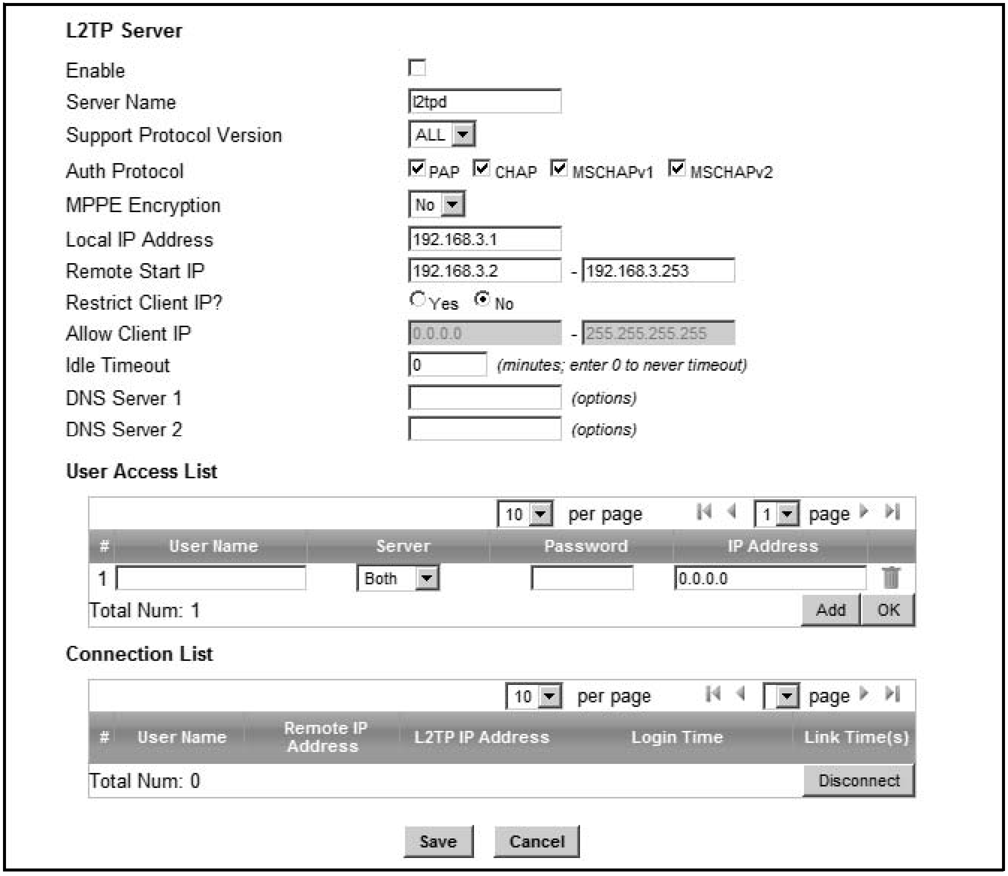
LABEL	DESCRIPTION
Password	Enter the password for connecting to the PPTP server.
Retype	Retype the password for connecting to the PPTP server.
Get IP automatically	Select **Yes** to have the PPTP server assign a local IP address to the client.
Assign IP Address	Enter the IP address for the client. Ensure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

8.8 L2TP VPN Server

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

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

Figure 76 L2TP Server



L2TP Server

Enable	□
Server Name	l2tpd
Support Protocol Version	ALL
Auth Protocol	☑ PAP ☑ CHAP ☑ MSCHAPv1 ☑ MSCHAPv2
MPPE Encryption	No
Local IP Address	192.168.3.1
Remote Start IP	192.168.3.2 - 192.168.3.253
Restrict Client IP?	○ Yes ● No
Allow Client IP	0.0.0.0 - 255.255.255.255
Idle Timeout	0 *(minutes; enter 0 to never timeout)*
DNS Server 1	*(options)*
DNS Server 2	*(options)*

User Access List

10 per page 1 page

#	User Name	Server	Password	IP Address
1		Both		0.0.0.0

Total Num: 1

Connection List

10 per page page

#	User Name	Remote IP Address	L2TP IP Address	Login Time	Link Time(s)

Total Num: 0

This screen contains the following fields:

Table 58 L2TP Server

LABEL	DESCRIPTION
L2TP Server	
Enable	Use this field to turn the BM2022w'S L2TP VPN function on or off.
Server Name	Enter the server name for the L2TP VPN connection.
Support Protocol Version	Select the L2TP Protocol Version **2** or **3**. L2TPv2 is a standard method for tunneling Point-to-Point Protocol (PPP) while L2TPv3 provides improved support for other types of networks including frame relay and ATM.
Auth Protocol	Select the Authentication Protocol allowed for the connection. Options are: **PAP** - Password Authentication Protocol (PAP) authentication occurs in clear text and does not use encryption. It's probably not a good idea to rely on this for security. **CHAP** - Challenge Handshake Authentication Protocol (CHAP) provides authentication through a shared secret key and uses a three way handshake. **MSCHAPv1** - Microsoft CHAP v1 (MSCHAPv1) provides authentication through a shared secret key and uses a three way handshake. It provides improved usability with Microsoft products. **MSCHAPv2** - Microsoft CHAP v2 (MSCHAPv2) provides encryption through a shared secret key and uses a three way handshake. It provides additional security over **MSCHAPv1**, including two-way authentication.
MPPE Encryption	If **MSCHAPv1** or **MSCHAPv2** is selected as an **Auth Protocol**, use the drop-down list box to select the type of Microsoft Point-to-Point Encryption (MPPE). Options are: **MPPE 40 -** MPPE with 40 bit session key length **MPPE 128 -** MPPE with 128 bit session key length Auto - Automatically select either MPPE 40 or MPPE 128
Local IP Address	Enter the local endpoint for the L2TP connection.
Remote Start IP	Enter the local IP address range the BM2022w assigns to remote users if the remote client device is set to obtain an IP address automatically.
Restrict Client IP?	Select **Yes** to restrict the remote client device local IP address.
Allow Client IP	Enter the local IP address range the remote client device is restricted to. If the client device is configured with a static IP address, it should be in this range.
Idle Timeout	Enter the time in minutes to timeout L2TP connections.
DNS Server 1 DNS Server 2	Specify the IP addresses of DNS servers to assign to the remote users.
User Access List	
User Name	Enter the user name for the remote user.
Server	Select the server that the remote user has access to: **PPTPD**, **L2TPD** or **Both**.
Password	Enter the password for the remote user.
IP Address	Enter the local IP address the BM2022w assigns to the remote user. Entering 0.0.0.0 indicates the local IP address will be dynamically assigned.
Delete	Select an entry and click this to delete it.
Add	Click this to create a new entry.
OK	Click this to save the changes.

Table 58 L2TP Server

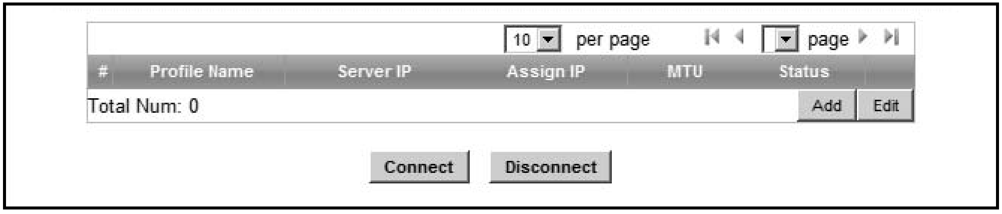
LABEL	DESCRIPTION
Connection List	
User Name	This displays the user name for the remote user.
Remote IP Address	This displays the remote endpoint IP address of the remote user.
L2TP IP Address	This displays the local IP address of the L2TP server.
Login Time	This displays the time the L2TP connection started.
Link Time(s)	This displays the duration of the L2TP connection.
Disconnect	Select a client and click this button to disconnect the selected client.

8.9 L2TP VPN Client

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

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

Figure 77 L2TP Client



#	Profile Name	Server IP	Assign IP	MTU	Status

Total Num: 0

This screen contains the following fields:

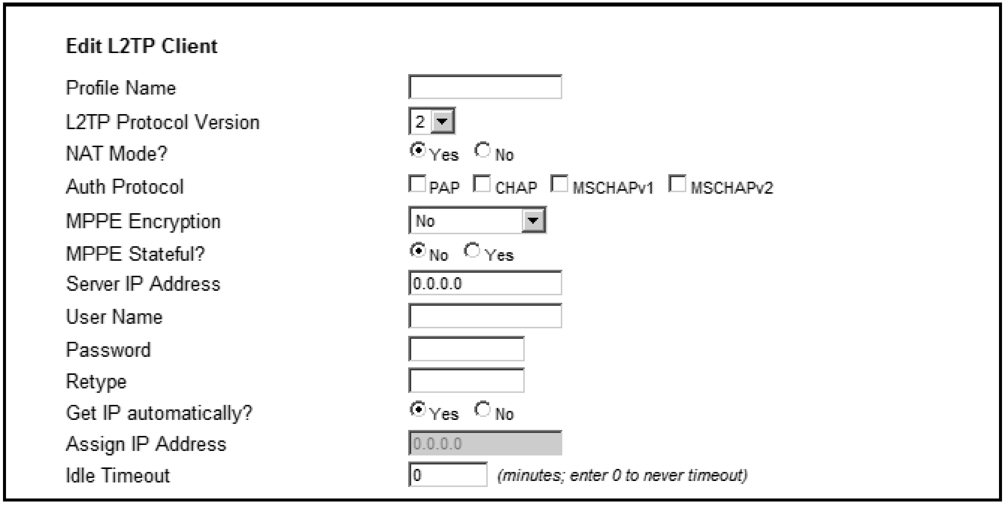
Table 59 L2TP Client

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

8.10 L2TP VPN Client: Add

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

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



Edit L2TP Client

Profile Name	
L2TP Protocol Version	2
NAT Mode?	● Yes ○ No
Auth Protocol	□ PAP □ CHAP □ MSCHAPv1 □ MSCHAPv2
MPPE Encryption	No
MPPE Stateful?	● No ○ Yes
Server IP Address	0.0.0.0
User Name	
Password	
Retype	
Get IP automatically?	● Yes ○ No
Assign IP Address	0.0.0.0
Idle Timeout	0 *(minutes; enter 0 to never timeout)*

Figure 78 L2TP Client: Add

This screen contains the following fields:

Table 60 L2TP Client: Add

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

Table 60 L2TP Client: Add

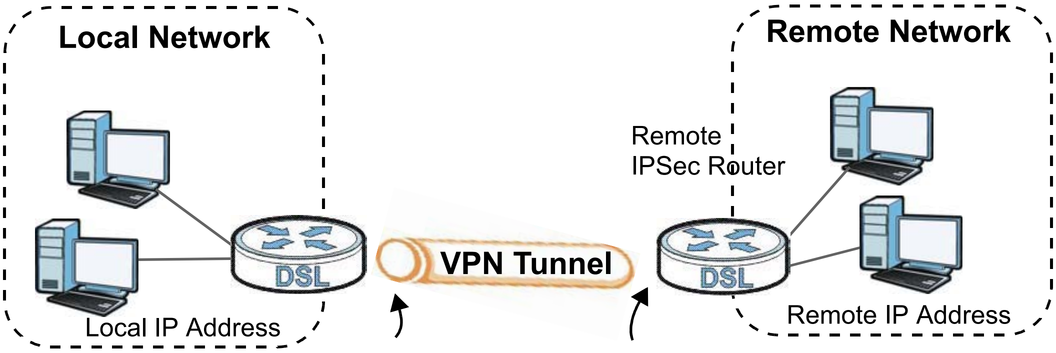
LABEL	DESCRIPTION
User Name	Enter the user name for connecting to the L2TP server.
Password	Enter the password for connecting to the L2TP server.
Retype	Retype the password for connecting to the L2TP server.
Get IP automatically	Select **Yes** to have the L2TP server assign a local IP address to the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

8.11 IPSec VPN

8.11.1 The General Screen

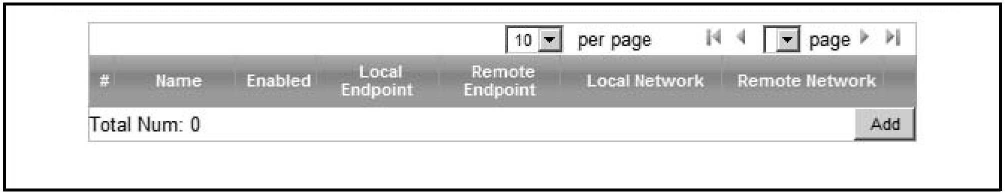
The following figure helps explain the main fields in the web configurator.

Figure 79 IPSec Fields Summary



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

Figure 80 IPSec VPN



#	Name	Enabled	Local Endpoint	Remote Endpoint	Local Network	Remote Network

Total Num: 0

This screen contains the following fields:

Table 61 IPSec VPN

LABEL	DESCRIPTION
#	This is the VPN policy index number.
Name	Enter the name of the VPN connection.
Enabled	This displays if the VPN policy is enabled.

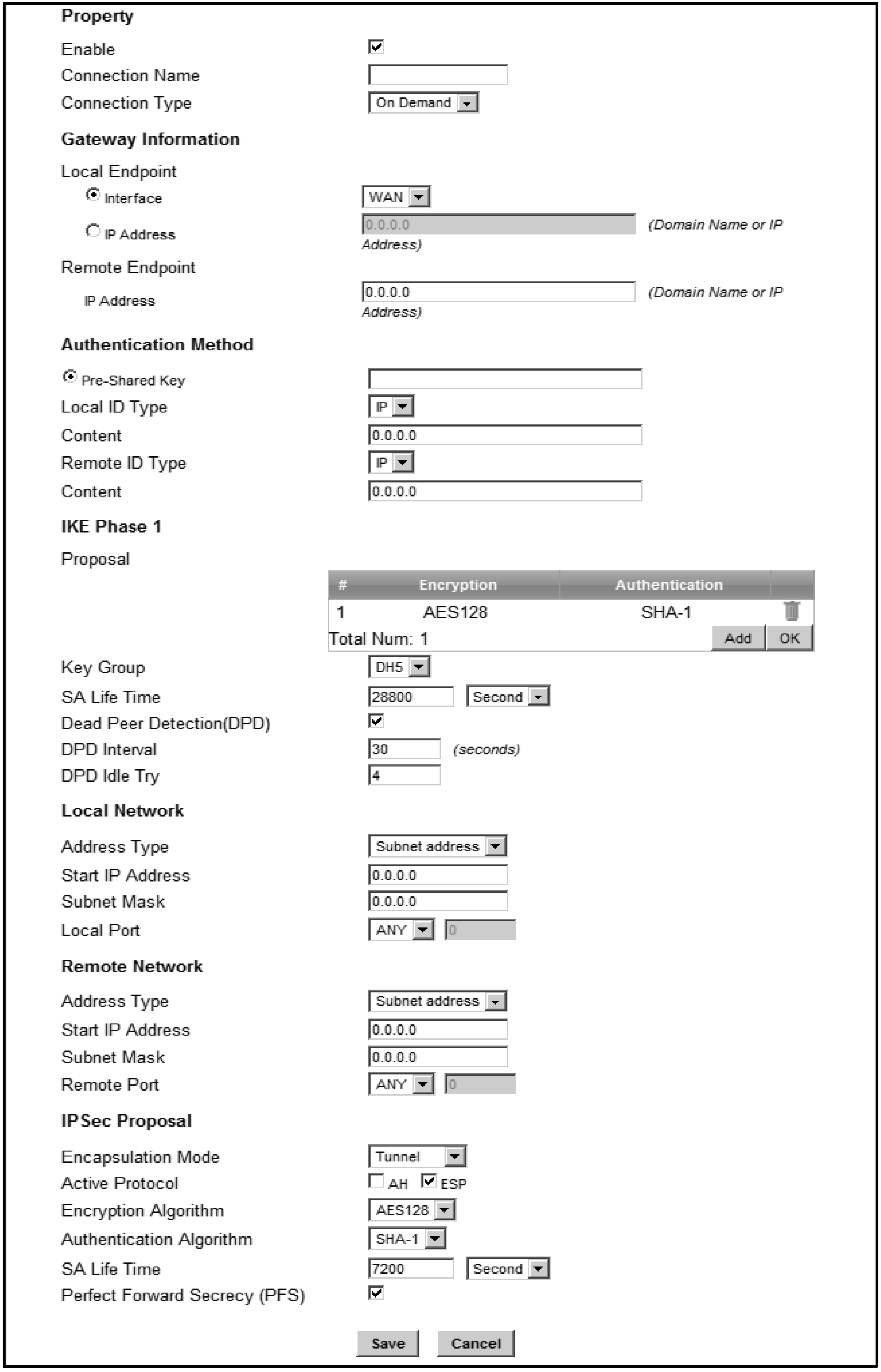
Table 61 IPSec VPN

LABEL	DESCRIPTION
Local Endpoint	This displays the IP address of the BM2022w.
Remote Endpoint	This displays the IP address of the remote IPSec router.
Local Network	This displays the single (static) IP address on the LAN behind your BM2022w or the IP address and subnet mask of a network behind your BM2022w.
Remote Network	This displays the single (static) IP address on the LAN behind the remote IPSec router or the IP address and subnet mask of a network behind the remote IPSec router.
Add	Click this button to add an item to the list.

8.11.2 IPSec VPN: Add

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

Figure 81 IPSec VPN: Add



Property

Enable	☑
Connection Name	
Connection Type	On Demand

Gateway Information

Local Endpoint	
● Interface	WAN
○ IP Address	0.0.0.0 *(Domain Name or IP Address)*
Remote Endpoint	
IP Address	0.0.0.0 *(Domain Name or IP Address)*

Authentication Method

● Pre-Shared Key	
Local ID Type	IP
Content	0.0.0.0
Remote ID Type	IP
Content	0.0.0.0

IKE Phase 1

Proposal

#	Encryption	Authentication
1	AES128	SHA-1

Total Num: 1

Key Group	DH5
SA Life Time	28800 Second
Dead Peer Detection(DPD)	☑
DPD Interval	30 *(seconds)*
DPD Idle Try	4

Local Network

Address Type	Subnet address
Start IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Local Port	ANY 0

Remote Network

Address Type	Subnet address
Start IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Remote Port	ANY 0

IPSec Proposal

Encapsulation Mode	Tunnel
Active Protocol	□ AH ☑ ESP
Encryption Algorithm	AES128
Authentication Algorithm	SHA-1
SA Life Time	7200 Second
Perfect Forward Secrecy (PFS)	☑

This screen contains the following fields:

Table 62 IPSec VPN: Add

LABEL	DESCRIPTION
Property	
Enable	Select **Enable** to activate this VPN policy.
Connection Name	Enter the name of the VPN connection.
Connection Type	Select the scenario that best describes your intended VPN connection. **Initiator** - Choose this to connect to an IPSec server. The BM2022w is the client (dial-in user) and can initiate the VPN connection. On Demand - Choose this if the remote IPSec router has a static IP address or a domain name. This BM2022w can initiate the VPN tunnel. Responder - Choose this to allow incoming connections from IPSec VPN clients. The clients can have dynamic IP addresses and are also known as dial-in users. Only the clients can initiate the VPN tunnel.
Gateway Information	
Local Endpoint	
Interface	Select the interface for the VPN gateway.
IP Address	Enter the IP address of the BM2022w in the IKE SA.
Remote Endpoint	
IP Address	Enter the IP address of the remote IPSec router in the IKE SA.
Authentication Method	
Pre-Shared Key	Type your pre-shared key in this field. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. You must precede a hexadecimal key with a "0x" (zero x), which is not counted as part of the 16 to 62 character range for the key. For example, in "0x0123456789ABCDEF", "0x" denotes that the key is hexadecimal and "0123456789ABCDEF" is the key itself.
Local ID Type	Select **IP** to identify the BM2022w by its IP address. Select **Domain Name** to identify this BM2022w by a domain name. Select **E-mail** to identify this BM2022w by an e-mail address.
Content	When you select IP in the **Local ID Type** field, type the IP address of your computer in the **Content** field. If you configure the **Content** field to 0.0.0.0 or leave it blank, the BM2022w automatically uses the **Pre-Shared Key** (refer to the **Pre-Shared Key** field description). It is recommended that you type an IP address other than 0.0.0.0 in the **Content** field or use the **Domain Name** or **E-mail ID** type in the following situations. • When there is a NAT router between the two IPSec routers. • When you want the remote IPSec router to be able to distinguish between VPN connection requests that come in from IPSec routers with dynamic WAN IP addresses. When you select **Domain Name** or **E-mail** in the **Local ID Type** field, type a domain name or e-mail address by which to identify this BM2022w in the **Local Content** field. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string.

Table 62 IPSec VPN: Add

LABEL	DESCRIPTION
Remote ID Type	Select **IP** to identify the remote IPSec router by its IP address. Select **Domain Name** to identify the remote IPSec router by a domain name. Select **E-mail** to identify the remote IPSec router by an e-mail address.
Content	The configuration of the remote content depends on the remote ID type. For **IP**, type the IP address of the computer with which you will make the VPN connection. If you configure this field to 0.0.0.0 or leave it blank, the BM2022w will use the address in the **Remote Endpoint** field (refer to the **Remote Endpoint** field description). For **Domain Name** or **E-mail**, type a domain name or e-mail address by which to identify the remote IPSec router. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string. It is recommended that you type an IP address other than 0.0.0.0 or use the **Domain Name** or **E-mail** ID type in the following situations: • When there is a NAT router between the two IPSec routers. • When you want the BM2022w to distinguish between VPN connection requests that come in from remote IPSec routers with dynamic WAN IP addresses.
IKE Phase 1	
Proposal	
#	This field is a sequential value, and it is not associated with a specific proposal. The sequence of proposals should not affect performance significantly.
Encryption	Select which key size and encryption algorithm to use in the IKE SA. Choices are: **DES** - a 56-bit key with the DES encryption algorithm **3DES** - a 168-bit key with the DES encryption algorithm **AES128** - a 128-bit key with the AES encryption algorithm **AES192** - a 192-bit key with the AES encryption algorithm **AES256** - a 256-bit key with the AES encryption algorithm The BM2022w and the remote IPSec router must use the same key size and encryption algorithm. Longer keys require more processing power, resulting in increased latency and decreased throughput.
Authentication	Select which hash algorithm to use to authenticate packet data. Choices are **SHA1** and **MD5**. **SHA1** is generally considered stronger than **MD5**, but it is also slower.
Remove	Select an entry and click this to delete it.
Add	Click this to create a new entry.
OK	Click this to save the changes.

Table 62 IPSec VPN: Add

LABEL	DESCRIPTION
Key Group	Select which Diffie-Hellman key group (DHx) you want to use for encryption keys. Choices are: **DH1** - use a 768-bit random number **DH2** - use a 1024-bit random number **DH5** - use a 1536-bit random number The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. Both routers must use the same DH key group.
SA Life Time	Type the maximum number of seconds the IKE SA can last. When this time has passed, the BM2022w and remote IPSec router have to update the encryption and authentication keys and re-negotiate the IKE SA. This does not affect any existing IPSec SAs, however.
Dead Peer Detection (DPD)	Select this check box if you want the BM2022w to make sure the remote IPSec router is there before it transmits data through the IKE SA. The remote IPSec router must support DPD. If the remote IPSec router does not respond, the BM2022w shuts down the IKE SA. If the remote IPSec router does not support DPD, see if you can use the VPN connection connectivity check.
DPD Interval	Specify the time interval for the BM2022w to send a DPD message to the remote IPSec router.
DPD Idle Try	Specify the maximum number of times the BM2022w sends the DPD message.
Local Network	Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses. Two active SAs can have the same configured local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time. In order to have more than one active rule with the **Remote Endpoint** field set to 0.0.0.0, the ranges of the local IP addresses cannot overlap between rules. If you configure an active rule with 0.0.0.0 in the **Remote Endpoint** field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the **Remote Endpoint** field set to 0.0.0.0.
Address Type	Select **Single address** or **Subnet address** to specify if the VPN connection begins at an IP address or subnet.
Start IP Address	If **Single address** is selected, enter a (static) IP address on the LAN behind your BM2022w. If **Subnet address** is selected, specify IP addresses on a network by their subnet mask by entering a (static) IP address on the LAN behind your BM2022w. Then enter the subnet mask to identify the network address.
Subnet Mask	If **Subnet address** is selected, enter the subnet mask to identify the network address.

Table 62 IPSec VPN: Add

LABEL	DESCRIPTION
Local Port	Select how the BM2022w checks the connection. The peer must be configured to respond to the method you select. Select **icmp** to have the BM2022w regularly ping the address you specify to make sure traffic can still go through the connection. You may need to configure the peer to respond to pings. Select **tcp** or **udp** to have the BM2022w regularly perform a TCP or UDP handshake with the address you specify to make sure traffic can still go through the connection. You may need to configure the peer to accept the TCP or UDP connection. If you select **tcp** or **udp**, specify the port number to use for the connectivity check.
Remote Network	Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses. The remote fields do not apply when the **Remote Endpoint** field is configured to 0.0.0.0. In this case only the remote IPSec router can initiate the VPN. Two active SAs cannot both have the same local and remote IP address(es). Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Address Type	Select **Single address** or **Subnet address** to specify if the VPN connection terminates at an IP address or subnet.
Start IP Address	If **Single address** is selected, enter a (static) IP address on the LAN behind the remote IPSec's router. If **Subnet address** is selected, specify IP addresses on a network by their subnet mask by entering a (static) IP address on the LAN behind the remote IPSec's router. Then enter the subnet mask to identify the network address.
Subnet Mask	If **Subnet address** is selected, enter the subnet mask to identify the network address.
Remote Port	Select how the BM2022w checks the connection. The peer must be configured to respond to the method you select. Select **icmp** to have the BM2022w regularly ping the address you specify to make sure traffic can still go through the connection. You may need to configure the peer to respond to pings. Select **tcp** or **udp** to have the BM2022w regularly perform a TCP or UDP handshake with the address you specify to make sure traffic can still go through the connection. You may need to configure the peer to accept the TCP or UDP connection. If you select **tcp** or **udp**, specify the port number to use for the connectivity check.
IPSec Proposal	
Encapsulation Mode	Select **Tunnel** mode or **Transport** mode from the drop-down list box.
Active Protocol	Select the security protocols used for an SA. Both **AH** and **ESP** increase processing requirements and communications latency (delay). If you select **ESP** here, you must select options from the **Encryption Algorithm** and **Authentication Algorithm** fields (described below).

Table 62 IPSec VPN: Add

LABEL	DESCRIPTION
Encryption Algorithm	Select which key size and encryption algorithm to use in the IPSec SA. Choices are: **DES** - a 56-bit key with the DES encryption algorithm **3DES** - a 168-bit key with the DES encryption algorithm **AES128** - a 128-bit key with the AES encryption algorithm **AES192** - a 192-bit key with the AES encryption algorithm **AES256** - a 256-bit key with the AES encryption algorithm The BM2022w and the remote IPSec router must use the same key size and encryption algorithm. Longer keys require more processing power, resulting in increased latency and decreased throughput.
Authentication Algorithm	Select which hash algorithm to use to authenticate packet data. Choices are **SHA1** and **MD5**. **SHA1** is generally considered stronger than **MD5**, but it is also slower.
SA Life Time	Define the length of time before an IPSec SA automatically renegotiates in this field. A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Perfect Forward Secrecy (PFS)	Select whether or not you want to enable Perfect Forward Secrecy (PFS) PFS changes the root key that is used to generate encryption keys for each IPSec SA. The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. Both routers must use the same DH key group.
Save	Click **Apply** to save your changes back to the BM2022w.
Cancel	Click **Cancel** to restore your previous settings.

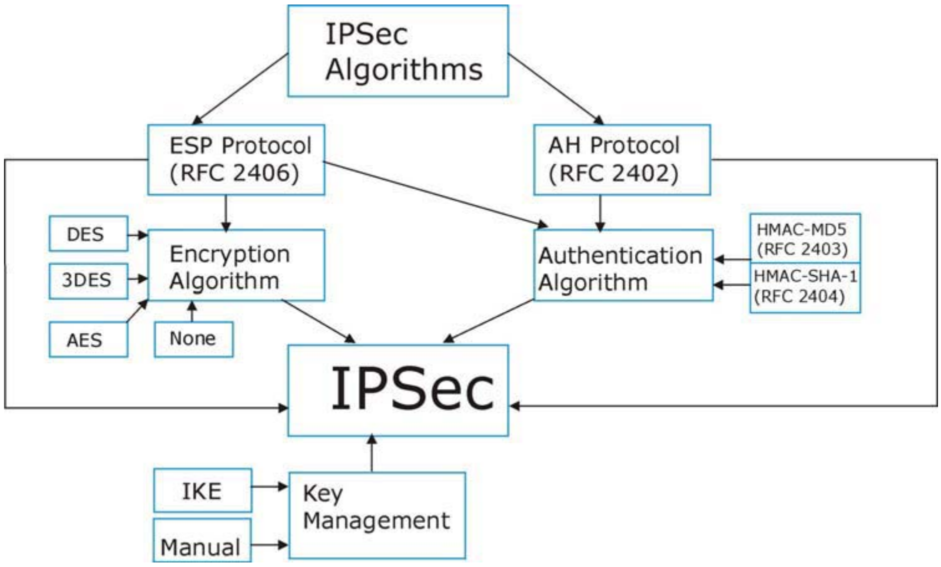
8.12 Technical Reference

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

8.12.1 IPSec Architecture

The overall IPSec architecture is shown as follows.

Figure 82 IPSec Architecture



IPSec Algorithms

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

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

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

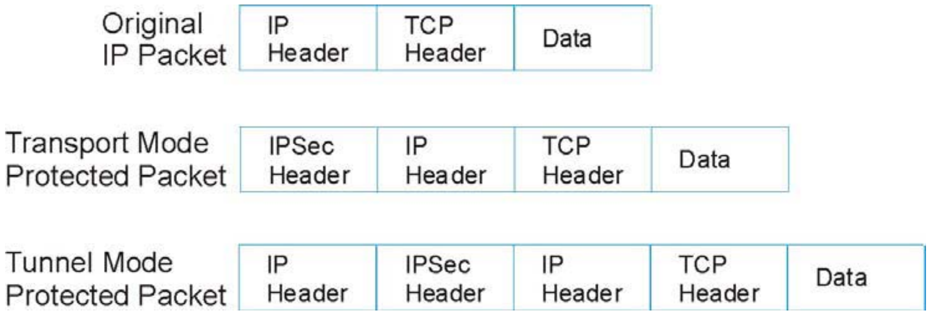
Key Management

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

8.12.2 Encapsulation

The two modes of operation for IPSec VPNs are **Transport** mode and **Tunnel** mode. At the time of writing, the BM2022w supports **Tunnel** mode only.

Figure 83 Transport and Tunnel Mode IPSec Encapsulation



Transport Mode

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

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

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

Tunnel Mode

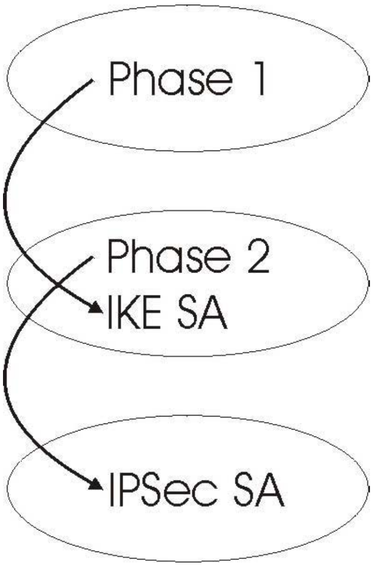
Tunnel mode encapsulates the entire IP packet to transmit it securely. A **Tunnel** mode is required for gateway services to provide access to internal systems. **Tunnel** mode is fundamentally an IP tunnel with authentication and encryption. This is the most common mode of operation. **Tunnel** mode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

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

8.12.3 IKE Phases

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

Figure 84 Two Phases to Set Up the IPSec SA



In phase 1 you must:

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

In phase 2 you must:

- Choose an encryption algorithm.
- Choose an authentication algorithm
- Choose a Diffie-Hellman public-key cryptography key group.
- Set the IPSec SA lifetime. This field allows you to determine how long the IPSec SA should stay up before it times out. The BM2022w automatically renegotiates the IPSec SA if there is traffic when the IPSec SA lifetime period expires. If an IPSec SA times out, then the IPSec router must renegotiate the SA the next time someone attempts to send traffic.

8.12.4 Negotiation Mode

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

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

8.12.5 IPSec and NAT

Read this section if you are running IPSec on a host computer behind the BM2022w.

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

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

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

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

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

Table 63 VPN and NAT

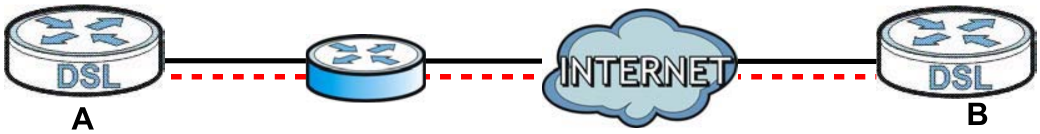
SECURITY PROTOCOL	MODE	NAT
AH	Transport	N
AH	Tunnel	N
ESP	Transport	N
ESP	Tunnel	Y

8.12.6 VPN, NAT, and NAT Traversal

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

NAT is not normally compatible with ESP in transport mode either, but the BM2022w’s **NAT Traversal** feature provides a way to handle this. NAT traversal allows you to set up an IKE SA when there are NAT routers between the two IPSec routers.

Figure 85 NAT Router Between IPSec Routers



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

For NAT traversal to work, you must:

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

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

Table 64 VPN and NAT

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

Y* - This is supported in the BM2022w if you enable NAT traversal.

8.12.7 ID Type and Content

With aggressive negotiation mode (see Section 8.12.4 on page 151), the BM2022w identifies incoming SAs by ID type and content since this identifying information is not encrypted. This enables the BM2022w to distinguish between multiple rules for SAs that connect from remote IPSec routers that have dynamic WAN IP addresses.

Regardless of the ID type and content configuration, the BM2022w does not allow you to save multiple active rules with overlapping local and remote IP addresses.

With main mode (see Section 8.12.4 on page 151), the ID type and content are encrypted to provide identity protection. In this case the BM2022w can only distinguish between up to 12 different incoming SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. The BM2022w can distinguish up to 48 incoming SAs because you can select between three encryption algorithms (DES, 3DES and AES), two authentication algorithms (MD5 and SHA1) and eight key groups when you configure a VPN rule (see Section 8.11.1 on page 141). The ID type and content act as an extra level of identification for incoming SAs.

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

Table 65 Local ID Type and Content Fields

LOCAL ID TYPE=	**CONTENT=**
IP	Type the IP address of your computer.
DNS	Type a domain name (up to 31 characters) by which to identify this BM2022w.
E-mail	Type an e-mail address (up to 31 characters) by which to identify this BM2022w.
	The domain name or e-mail address that you use in the **Local ID Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address.

8.12.7.1 ID Type and Content Examples

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

The two BM2022ws in this example can complete negotiation and establish a VPN tunnel.

Table 66 Matching ID Type and Content Configuration Example

BM2022w A	BM2022w B
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2
Remote ID type: IP	Remote ID type: E-mail
Remote ID content: 1.1.1.2	Remote ID content: tom@yourcompany.com

The two BM2022ws in this example cannot complete their negotiation because BM2022w B's **Local ID type** is **IP**, but BM2022w A's **Remote ID type** is set to **E-mail**. An "ID mismatched" message displays in the IPSEC LOG.

Table 67 Mismatching ID Type and Content Configuration Example

BM2022W A	**BM2022W B**
Local ID type: IP	Local ID type: IP
Local ID content: 1.1.1.10	Local ID content: 1.1.1.2
Remote ID type: E-mail	Remote ID type: IP
Remote ID content: aa@yahoo.com	Remote ID content: 1.1.1.0

8.12.8 Pre-Shared Key

A pre-shared key identifies a communicating party during a phase 1 IKE negotiation (see Section 8.12.3 on page 151 for more on IKE phases). It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection.

8.12.9 Diffie-Hellman (DH) Key Groups

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