Accton Wireless Broadband Corp.

RG230-2.5
WiMAX 802.16e
Self-Install Residential Gateway

User Guide

User Guide

RG230-2.5

WiMAX 802.16e Self-Install Residential Gateway

with 2.5 GHz Frequency Band Support,
Four LAN (RJ-45) Ports,
Two Optional VoIP (RJ-11) Ports

Compliances

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IMPORTANT NOTE: FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

NCC Statement:「減少電磁波影響，請妥適使用」

About This Guide

Purpose

This guide details the hardware features of the WiMAX Residential Gateway including its physical and performance-related characteristics, and how to install the device and use its configuration software.

Audience

This guide is for PC users with a working knowledge of computers. You should be familiar with basic networking concepts.

Conventions

The following conventions are used throughout this guide to show information:

Note: Emphasizes important information or calls your attention to related features or instructions.

Caution: Alerts you to a potential hazard that could cause loss of data, or damage the system or equipment.

Warning: Alerts you to a potential hazard that could cause personal injury.

Related Publications

The following publication gives basic information on how to install and use the WiMAX Residential Gateway.

Quick Installation Guide

As part of the WiMAX Residential Gateway's software, there is online help that describes all configuration related features.

Revision History

This section summarizes the changes in each revision of this guide.

September 2008 Revision

This is the first revision of this guide. This guide is valid for software release v0.2.0.0.

Table of Contents

Tables

Figures

Chapter 1: Introduction

The RG230-2.5 Wimax 802.16e Self-Install Residential Gateway is a WiMAX subscriber station designed to provide Internet access for a home or small office. The unit provides a gateway function between a WiMAX service provider and a local Ethernet LAN. The device enables a service provider to deliver last mile broadband wireless access as an alternative to wired DSL or cable modems.

The RG230-2.5 includes four RJ-45 Ethernet switch ports for LAN connections and two optional RJ-11 Voice over IP (VoIP) phone ports.

The initial configuration steps can be made through the web browser interface using the Setup Wizard. It is recommended to make the initial changes by connecting a PC directly to one of the RG230's LAN ports.

RG230 Hardware Description

The front of the RG230 provides an array of system status indicators. The back includes four LAN ports for 10/100 Mbps Ethernet connections, two RJ-11 VoIP phone ports (on some models), and a DC power jack.

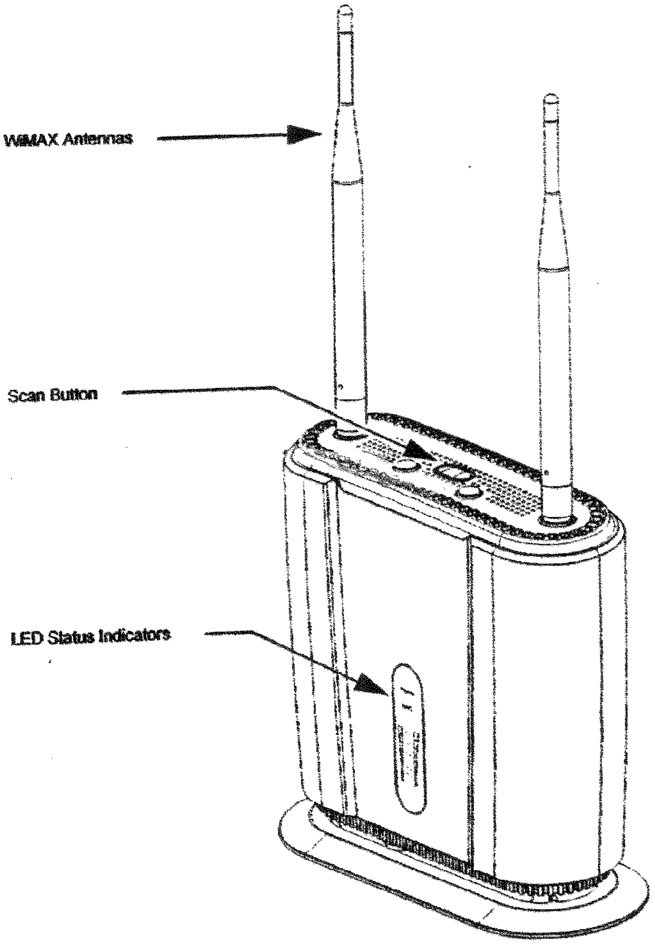


Figure 1-1 Front of the RG230

Scan Button

This button is used to scan WiMAX operating channels. When you press the button, the unit will perform a scan to find the best of the known frequency channels.

WiMAX Antennas

Two antennas are included with the RG230 for WiMAX communications. The omnidirectional antennas transmit and receive signals in all directions equally.

Power Status Indicator LED

The RG230 includes a Power LED indicator that simplifies installation and WiMAX network troubleshooting. The LED, which is located on the front panel, is described in the following table.

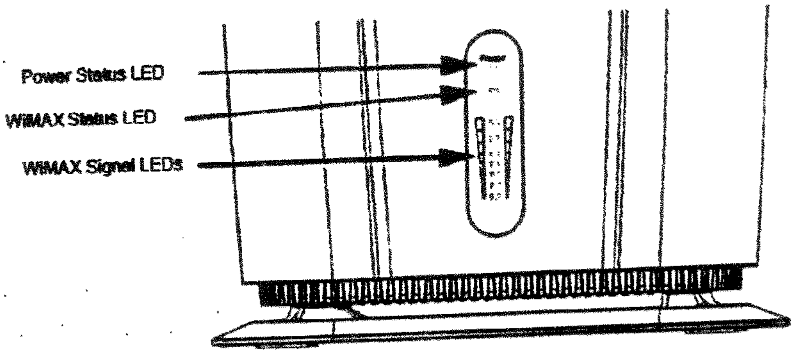


Figure 1-2 RG230 LED Indicators

Table 1-2 Power Status LED

Status	Description
On Green	The unit has completed entry to a WiMAX network.
Flashing Green	Indicates one of the following conditions: - When flashing with three of the WiMAX signal LEDs turned on, indicates authentication has failed. - When flashing with one of the WiMAX signal LEDs turned on, indicates authentication has timed out.

Table 1-2 Power Status LED (Continued)

Status	Description
On Orange	Indicates one of the following conditions: • After power on, indicates the unit is running its self test. • The unit is in scan mode or selecting the base station with the strongest signal. • Indicates the network entry process has restarted.
Flashing Orange	The unit is being reset to factory defaults.
On Red	A system failure has occured.
Off	No power is being supplied to the unit.

WiMAX Signal Indicator LEDs

The RG230 includes seven WiMAX signal strength LED indicators that display the current WiMAX receive signal status. The LEDs, which are located on the front panel, are described in the following table.

Table 1-4 WiMAX Signal Status LEDs

LED	Status	Description
1	On Green	Indicates the receive signal is 5 dB or more.
2	On Green	Indicates the receive signal is 8 dB or more.
3	On Green	Indicates the receive signal is 12 dB or more.
4	On Green	Indicates the receive signal is 15 dB or more.
5	On Green	Indicates the receive signal is 18 dB or more.
6	On Green	Indicates the receive signal is 20 dB or more.
7	On Green	Indicates the receive signal is 25 dB or more.
1 to 7 in sequence	Cycle On/Off Green	A full frequency scan is in progress.
4, 3&5, 2&6, 1&7 in sequence	Cycle On/Off Green	Selecting a detected base station with the strongest signal.

Table 1-4 WiMAX Signal Status LEDs (Continued)

LED	Status	Description
All 7 LEDs	Flashing Green	Indicates the receive signal strength is too high (has reached saturation).
All 7 LEDs	Off	No power is being supplied to the unit.

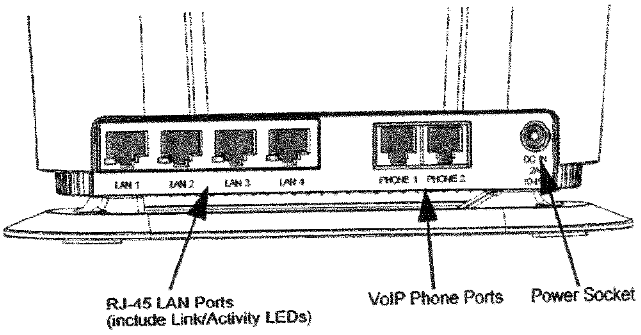


Figure 1-3 Back of the RG230

10BASE-T/100BASE-TX LAN Ports

The RG230 provides four 10BASE-T/100BASE-TX RJ-45 ports. These LAN ports are standard RJ-45 Ethernet network ports that connect directly to PCs. They can also be connected to an Ethernet switch or hub to support more users.

All ports support automatic MDI/MDI-X operation, so you can use straight-through cables for all network connections to PCs or servers, or to other switches or hubs. Each of these ports support auto-negotiation, so the optimum transmission mode (half or full duplex), and data rate (10 or 100 Mbps) is selected automatically.

Each RJ-45 port includes a built-in LED indicator. This LED indicator is described in the following table.

Table 1-5 LAN Port Status LEDs

LED	Status	Description
Link/Activity	On Green	Ethernet port has a valid link with an attached device.
	Flashing Green	The port is transmitting or receiving data.
	Off	Ethernet port has no link with another device.

VoIP Phone Ports

Some RG230 models optionally provide two RJ-11 telephone ports that connect directly to a standard (analog) telephone set. This allows a regular telephone to be used for making VoIP calls over the Internet.

Power Adapter Socket — Asian Power Devices Inc._NB-65B19

The power socket is located on the rear panel of the RG230. The power socket is for the AC power adapter connection.

The unit is powered on when connected to its AC power adapter, and the power adapter is connected to an AC power source between 100-240 volts at 50-60Hz.

Reset Button

This button is used to reset the RG230 or restore the factory default configuration. If you press the button for less than 1 second, the unit will perform a hardware reset. If you press and hold down the button for 5 seconds or more, any configuration changes you may have made are removed, and the factory default configuration is restored to the unit.

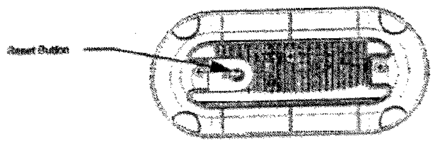


Figure 1-4. Base of the RG230

Chapter 2: Installing the RG230

This section describes how to install and connect the RG230 WiMAX Residential Gateway.

Package Checklist

The RG230 package includes:

- RG230-2.5 unit
- RJ-45 Category 5 network cable
- AC power adapter
- Quick Installation Guide
- User Guide CD

Installation Overview

Before installing the RG230, verify that you have all the items listed in the package checklist above. If any of the items are missing or damaged, contact your local dealer. Also, be sure you have all the necessary tools and cabling before installing the RG230.

Select a Location

The RG230 can be installed indoors on any horizontal surface, such as a desktop or shelf.

When selecting a suitable location for the device, consider these guidelines:

- Select a cool, dry place, which is out of direct sunlight.
- The device should have adequate space (approximately two inches) on all sides for proper air flow.
- The device must be near an AC power outlet that provides 100 to 240 V, 50 to 60 Hz.
- The device should be accessible for network cabling and allow the status LED indicators to be clearly visible.

Note: If the RG230 displays a weak WiMAX receive signal, try moving it to another location. Alternatively, you can connect optional external antennas to the unit to improve performance.

Cable Connections

The RG230 is a plug-and-play device, so once it has been connected to your PC and powered up, it is fully operable.

Functioning as a gateway, the unit routes traffic between a WiMAX service provider's base station and PCs or notebooks in the local network.

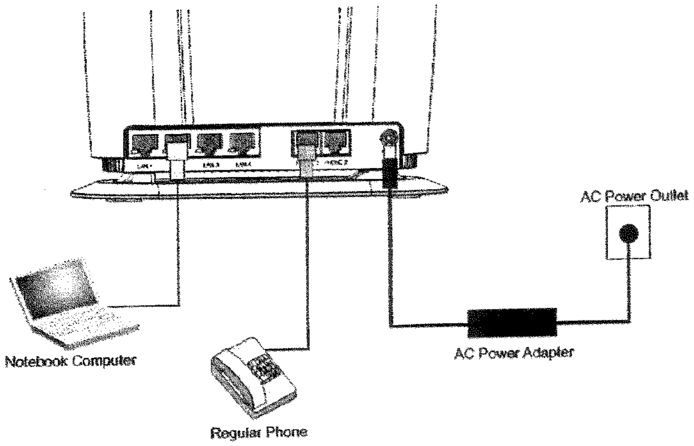


Figure 2-1 RG230 Connections

To connect the RG230, follow these steps:

1. Power on the RG230 by by first connecting the AC power adapter to the unit's power socket, and then connecting the adapter to an AC power source.

Caution: Use ONLY the power adapter supplied with the RG230. Otherwise, the product may be damaged.

2. Observe the Indicator LEDs. When you power on the RG230, verify that the Power LED turns on and that the other LED indicators start functioning as described under "RG230 Hardware Description" on page 1-2.

3. Connect Category 5 or better Ethernet cables from the RG230's LAN ports to the network ports of your PCs. Alternatively, you can connect the LAN ports to an Ethernet switch or other devices. Make sure the length of each cable does not exceed 100 meters (328 ft).

   If your PCs are powered on, the RJ-45 LAN port LEDs on the RG230 should turn on to indicate valid links.

4. (Optional) Connect one or two standard (analog) telephone sets to the RG230's VoIP ports using standard telephone cable with RJ-11 plugs.

The RG230 enables VoIP calls to be made through the unit using a standard (analog) telephone set connected to a VoIP port, or from PCs or other network devices connected to the LAN ports. Standard Session Initiation Protocol (SIP) technology is used to make VoIP calls. You must access the web interface and configure settings for your SIP service provider before being able to make VoIP calls.

5. Use your PC's web browser to access the unit's management interface and run the Setup Wizard to make any configuration changes. For more information, see Chapter 3, "Initial Configuration."

Chapter 3: Initial Configuration

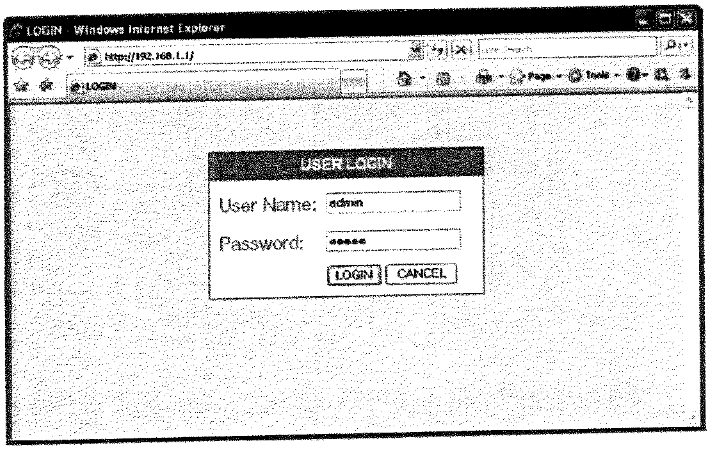
The RG230 can be configured through its web management interface. The web interface provides a simple Setup Wizard or Advanced Setup options.

Accessing the Web Management Interface

The RG230 has a default IP address of 192.168.1.1 and a subnet mask of 255.255.255.0. If your PC is set to have an IP address assigned by DHCP (Dynamic Host Configuration Protocol), you can connect immediately to the web management interface. Otherwise, you must first check if your PC's IP address is set on the same subnet as the RG230 (that is, the PC's IP address starts 192.168.1.x).

In the web browser's address bar, type the default IP address: http://192.168.1.1.

The web browser displays the RG230's login page.

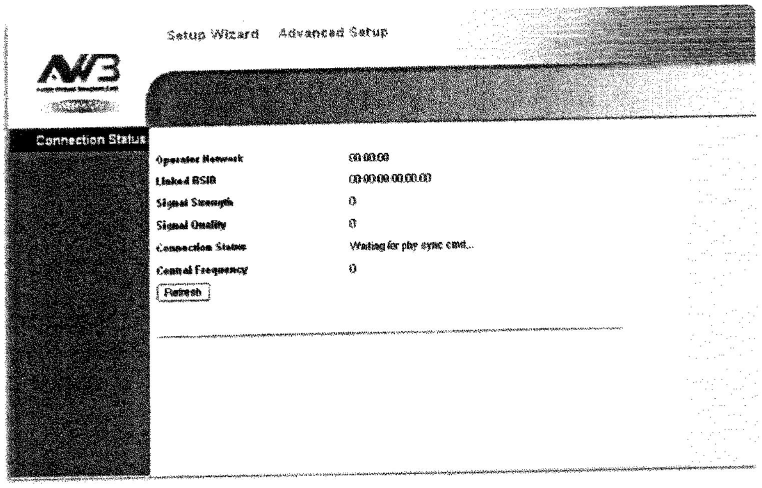


User Name: admin

Password: •••••

Figure 3-1 Login Page

Logging In – Type the default User Name "admin" and Password "admin," then click Login. The home page displays.



Operator Network	00:00:00
Linked BSID	00:00:00:00:00:00
Signal Strength	0
Signal Quality	0
Connection Status	Waiting for phy sync cmd...
Central Frequency	0

Figure 3-2 Home Page

To configure basic settings for the current operating mode, click Setup Wizard. For more information, see "Initial Configuration" on page 3-1.

Alternatively, to configure more detailed settings, click Advanced Setup. For more information, see "The Advanced Setup Menu" on page 3-13.

Note: It is recommended that you configure a user password as the first step under "Administrator Settings" on page 4-3 to control management access to the unit.

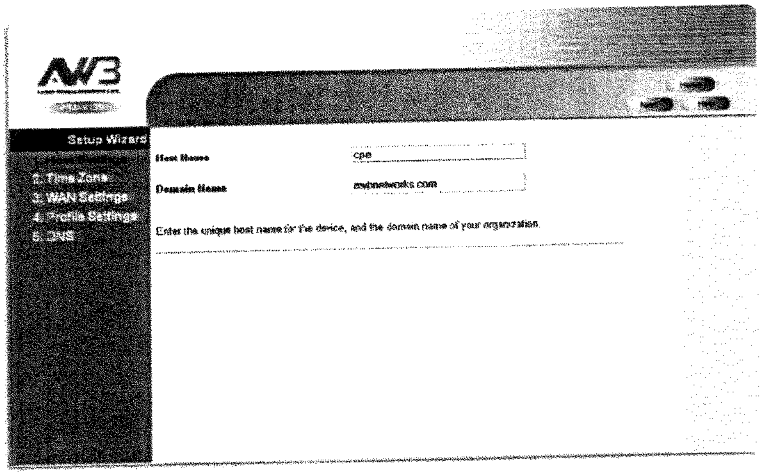
Using the Setup Wizard

The Setup Wizard takes you through the basic configuration steps for the current operating mode.

Launching the Setup Wizard – To perform basic configuration, click Setup Wizard on the home page.

When configuring the unit through the Setup Wizard you will need to proceed through the following steps:

1. **Host Settings** – The Host Settings page defines a name that identifies your unit and the domain name used by the local network.



Host Name: cpe

Domain Name: awbnetworks.com

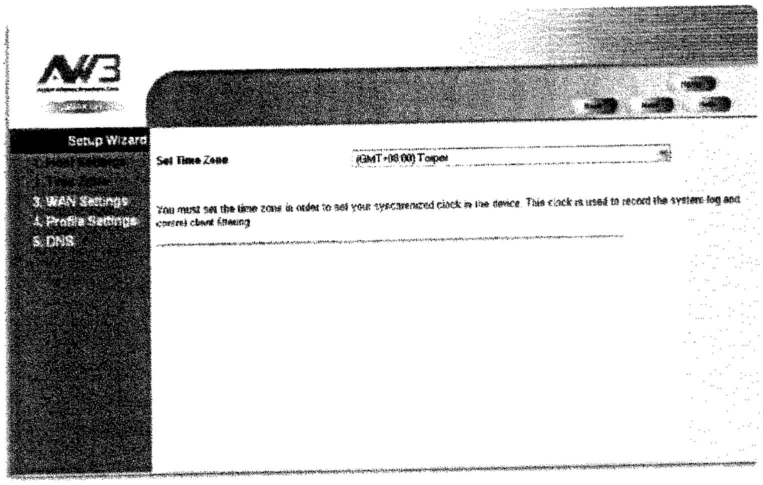
Enter the unique host name for the device, and the domain name of your organization.

Figure 3-3 Host Settings

Host Name – The name that uniquely identifies the unit.

Domain Name – The name that uniquely identifies the domain to which the unit belongs.

2. **Time Zone** – The time zone for the country in which the unit is being used, expressed in GMT format.



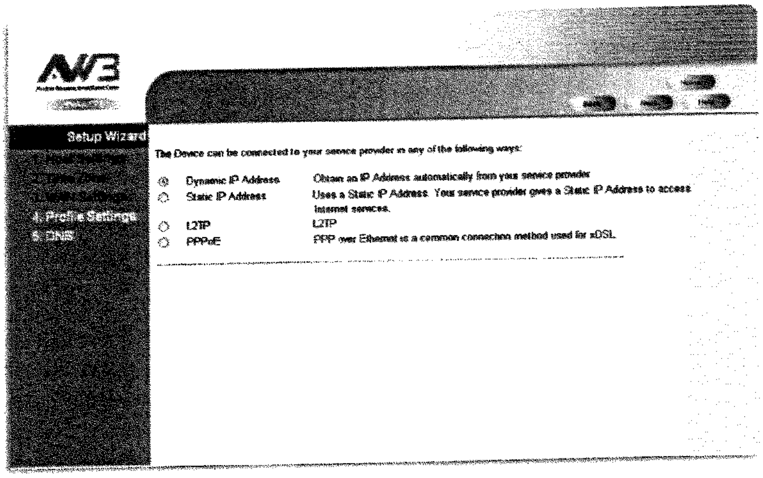
Set Time Zone (GMT+08:00) Taipei

You must set the time zone in order to set your syncaronized clock in the device. This clock is used to record the system log and control client filtering.

Figure 3-4 Time Zone

Set Time Zone – Selects the time zone in which the unit is being used.

3. **WAN Settings** – The WAN Settings page is for specifying the type of connection to your Internet service provider (ISP). When one of the options is selected, the Wizard displays the appropriate configuration parameters.



The Device can be connected to your service provider in any of the following ways:

● Dynamic IP Address Obtain an IP Address automatically from your service provider
○ Static IP Address Uses a Static IP Address. Your service provider gives a Static IP Address to access Internet services.
○ L2TP L2TP
○ PPPoE PPP over Ethernet is a common connection method used for xDSL.

Figure 3-5 WAN Type

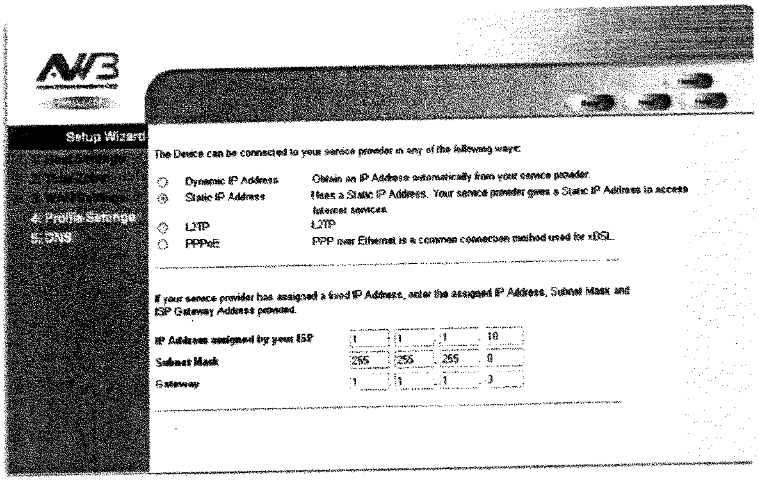
Dynamic IP Address – Selects configuration for an Internet connection using DHCP for IP address assignment.

Static IP Address – Selects configuration for an Internet connection using a fixed IP assignment.

L2TP – Selects configuration for an Internet connection using the Layer 2 Tunneling Protocol, an access protocol often used for virtual private networks.

PPPoE – Selects configuration for an Internet connection using the Point-to-Point Protocol over Ethernet (PPPoE), a common connection method used for DSL access.

Note: For the Dynamic IP Address (DHCP) option, the unit requires no further configuration and you can continue directly to next step. Selecting other WAN types displays the parameters that are required for configuring the connection.



The Device can be connected to your service provider in any of the following ways:

○	Dynamic IP Address	Obtain an IP Address automatically from your service provider.
●	Static IP Address	Uses a Static IP Address. Your service provider gives a Static IP Address to access Internet services.
○	L2TP	L2TP
○	PPPoE	PPP over Ethernet is a common connection method used for xDSL.

If your service provider has assigned a fixed IP Address, enter the assigned IP Address, Subnet Mask and ISP Gateway Address provided.

IP Address assigned by your ISP	1	1	1	10
Subnet Mask	255	255	255	0
Gateway	1	1	1	3

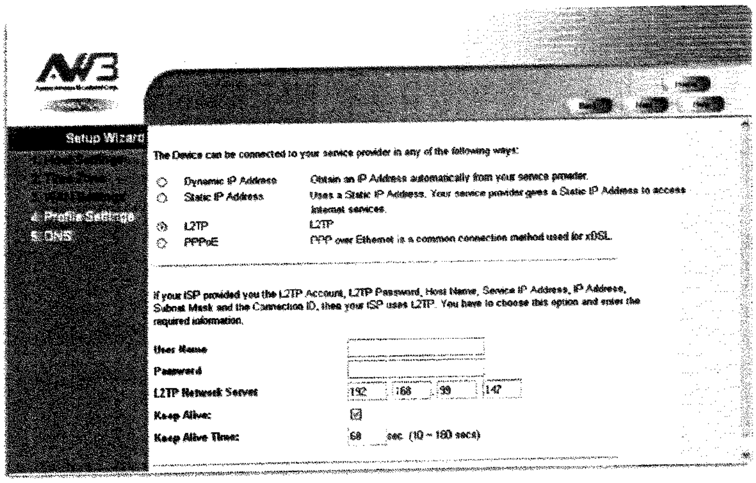
Figure 3-6 WAN Type - Static IP Address

For the static IP option, you are prompted for the following information (as supplied by your ISP):

IP Address – If your ISP has assigned you a fixed IP address, enter the address here.

Subnet Mask – Enter the subnet mask as supplied by your ISP.

ISP Gateway Address – The gateway IP address of your ISP.



The Device can be connected to your service provider in any of the following ways:

○	Dynamic IP Address	Obtain an IP Address automatically from your service provider.
○	Static IP Address	Uses a Static IP Address. Your service provider gives a Static IP Address to access Internet services.
●	L2TP	L2TP
○	PPPoE	PPP over Ethernet is a common connection method used for xDSL.

If your ISP provided you the L2TP Account, L2TP Password, Host Name, Service IP Address, IP Address, Subnet Mask and the Connection ID, then your ISP uses L2TP. You have to choose this option and enter the required information.

User Name	
Password	
L2TP Network Server	192 . 168 . 99 . 147
Keep Alive:	☑
Keep Alive Time:	60 sec. (10 ~ 180 secs)

Figure 3-7 WAN Type - L2TP

For the L2TP option, you are prompted for the following information (specified by the service provider):

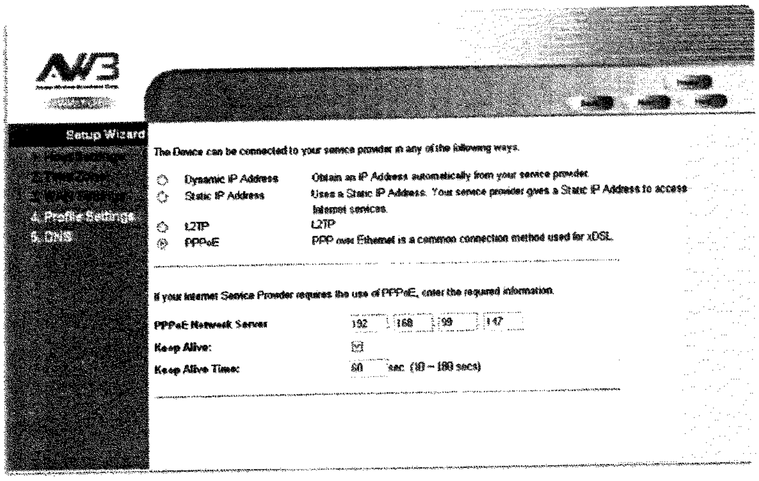
User Name – Enter your user name for connecting to the L2TP service, as supplied by the service provider. (Range: 1-32 characters)

Password – Specify the password for your connection, as supplied by the service provider. (Default: No password)

L2TP Network Server – The IP address of the L2TP server, as specified by the service provider.

Keep Alive – This option enables the unit to check periodically that the L2TP connection is still operating. If the connection is found to be lost, the unit automatically attempts to reconnect to the service provider. (Default: Enabled)

Keep Alive Time – The time period the unit waits before checking that the L2TP connection is still operating. This parameter only applies when Keep Alive is enabled. (Default: 60 seconds; Range: 10-180 seconds)



The Device can be connected to your service provider in any of the following ways.

○ Dynamic IP Address Obtain an IP Address automatically from your service provider.
○ Static IP Address Uses a Static IP Address. Your service provider gives a Static IP Address to access Internet services.
○ L2TP L2TP
● PPPoE PPP over Ethernet is a common connection method used for xDSL.

If your Internet Service Provider requires the use of PPPoE, enter the required information.

PPPoE Network Server 192 . 168 . 99 . 147
Keep Alive: ☒
Keep Alive Time: 60 sec. (10 ~ 180 secs)

Figure 3-8 WAN Type - PPPoE

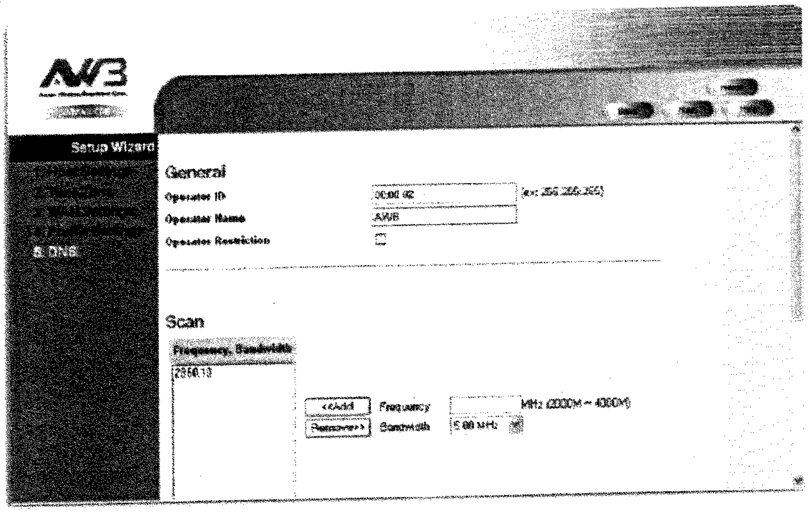
For the PPPoE option, you are prompted for the following information (specified by the service provider):

PPPoE Network Server – The IP address of the PPPoE server, as specified by the service provider.

Keep Alive – This option enables the unit to check periodically that the PPPoE connection is still operating. If the connection is found to be lost, the unit automatically attempts to reconnect to the service provider. (Default: Enabled)

Keep Alive Time – The time period the unit waits before checking that the PPPoE connection is still operating. This parameter only applies when Keep Alive is enabled. (Default: 60 seconds; Range: 10-180 seconds)

4. **Profile Settings** – A profile allows a user to set specific details for connecting to various WiMAX service providers. The RG230 must have at least one profile configured to be able to connect to a WiMAX service.



General

Operator ID: 00:00:02 (ex: 255:255:255)

Operator Name: AWB

Operator Restriction: □

Scan

Frequency, Bandwidth: 2560,10

<<Add | Frequency: MHz (2000M ~ 4000M)

Remove>> | Bandwidth: 5.00 MHz

Figure 3-9 Profile Configuration

Operator ID – The ID number that identifies the WiMAX operator for this profile.

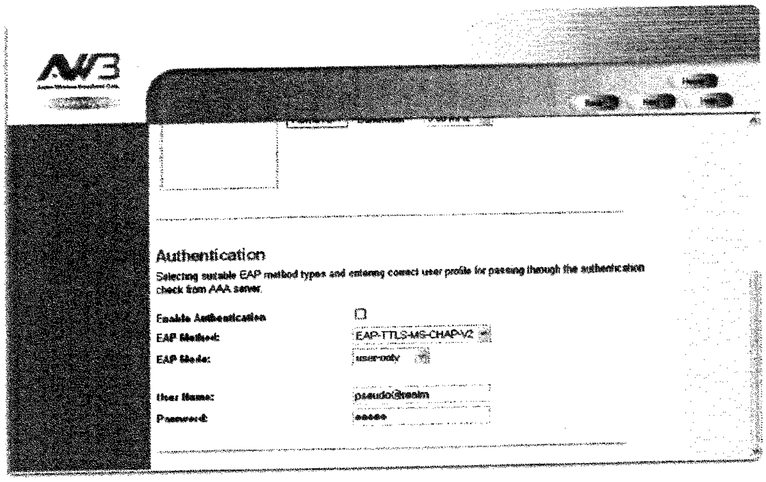
Operator name – The WiMAX operator name.

Operator Restriction – When enabled, the user can only connect to the service provider specified in the profile. The user cannot roam to other networks. When disabled, the operator specified in the profile will be used when base stations are detected, otherwise the user can roam to other networks. (Default: Disabled)

Scan Frequency – Specifies a center frequency to scan.
Range:
FCC_2.5: 2496 – 2690 MHz
Taiwan NCC: 2500 – 2690 MHz
Support for Full Scan and Partial Scan

Scan Bandwidth – Either 5, 7, 8.75, or 10 MHz, depending on model (software configurable). (Options: 5.00, 7.00, 8.75, 10.00 MHz)

2.5 GHz model: 5, and 10 MHz



Authentication

Selecting suitable EAP method types and entering correct user profile for passing through the authentication check from AAA server.

Enable Authentication ☐

EAP Method: EAP-TTLS-MS-CHAP-V2

EAP Mode: user-only

User Name: pseudo@realm

Password: *****

Figure 3-10 Profile Configuration — Authentication

Enable Authentication – Enables user authentication for connection to the network. (Default: Disabled)

EAP Method – Selects the Extensible Authentication Protocol (EAP) method to use for authentication. (Default: EAP-TTLS-MSCHAPV2)

- **EAP-TLS** – Transport Layer Security. Provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based encryption keys to secure subsequent communications between the user and the network.
- **EAP-TTLS-CHAP** – Tunneled Transport Layer Security with Challenge-Handshake Authentication Protocol (CHAP). This security method provides for certificate-based, mutual authentication of the client and network through an encrypted channel. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates.
- **EAP-TTLS-MSCHAPV2** – Tunneled Transport Layer Security with Microsoft's version 2 of CHAP.

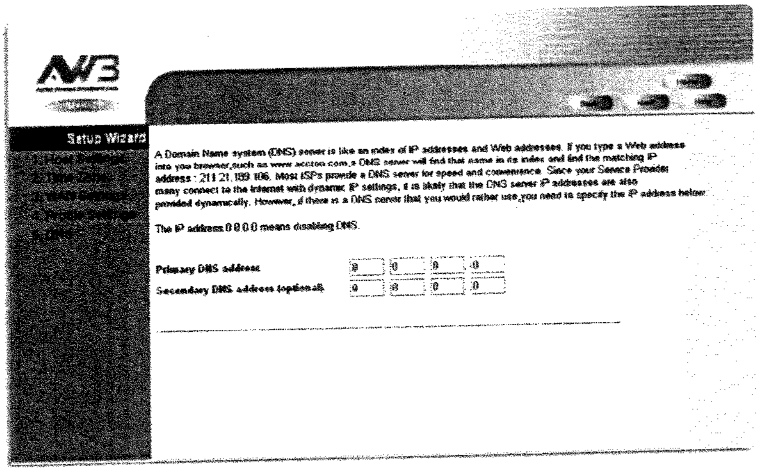
EAP Mode – Selects if only a specific user is to be authenticated (user-only), the subscriber device itself (device-only), or both a user and the device (user-device). Select the option instructed by the WiMAX service operator.

User Name – The user name required for EAP-TTLS authentication. (Default: pseudo@realm)

Password – The user password required for EAP-TTLS authentication. (Default: hello)

MAC Address@domain – An identity that is used to authenticate the WiMAX subscriber device itself. It consists of the MAC address of the RG230 specified in the format xx:xx:xx:xx:xx:xx @ the domain URL of the service provider. For example; 1f:20:30:10:4d:50@service-telecom.

5. **DNS** (Domain Name System) – A DNS server is like an index of IP addresses and Web host name addresses. When you type a Web address into your browser, such as www.awbnetworks.com, a DNS server will find that name in its index and translate it to a matching IP address, such as 211.21.189.106. DNS server addresses are usually provided by service providers, however if you want to specify certain other servers, this page allows you to enter primary and secodary DNS addresses.



A Domain Name system (DNS) server is like an index of IP addresses and Web addresses. If you type a Web address into you browser,such as www.accton.com,a DNS server will find that name in its index and find the matching IP address : 211.21.189.106. Most ISPs provide a DNS server for speed and convenience. Since your Service Provider many connect to the Internet with dynamic IP settings, it is likely that the DNS server IP addresses are also provided dynamically. However, if there is a DNS server that you would rather use,you need to specify the IP address below.

The IP address 0.0.0.0 means disabling DNS.

Primary DNS address: 0 . 0 . 0 . 0

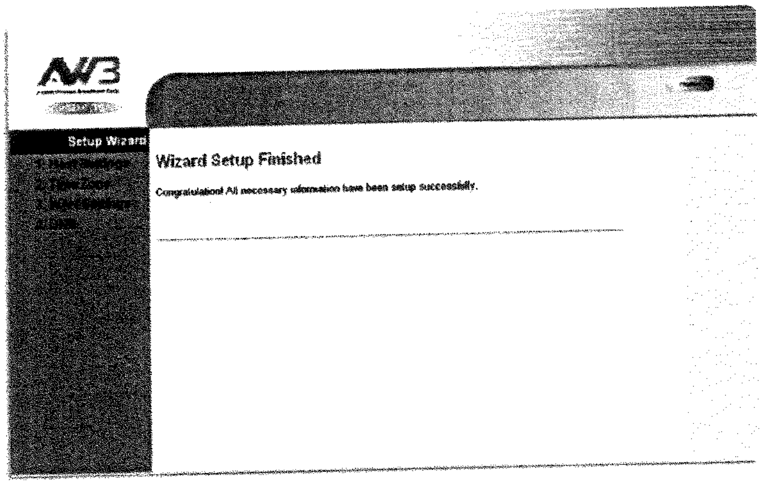
Secondary DNS address (optional): 0 . 0 . 0 . 0

Figure 3-11 DNS Configuration

Primary DNS address – Address of the primary DNS server, specified in the form of 0.0.0.0.

Secondary DNS address – Optional address of a secondary DNS server, specified in the form of 0.0.0.0.

6. **Wizard Setup Finished** – When the wizard set up steps are completed, click on the Home button to return to the Home page.



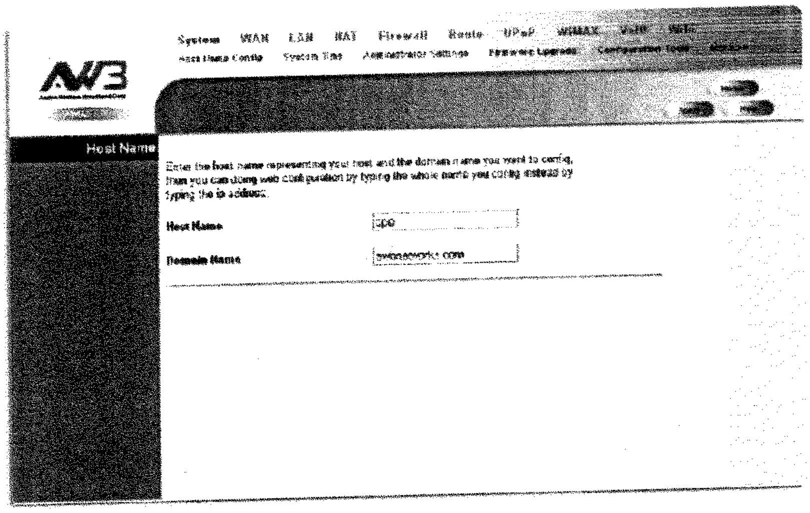
Wizard Setup Finished

Congratulation! All necessary information have been setup successfully.

Figure 3-12 Wizard Setup Finished

The Advanced Setup Menu

The Advanced Setup menu provides access to all the configuration settings available for the RG230.



Enter the host name representing your host and the domain name you want to config, than you can doing web configuration by typing the whole name you config instead by typing the ip address.

Host Name: cpe

Domain Name: [illegible]

Figure 3-13 Advanced Setup

Each primary menu item is sumarized below with links to the relevant section in this guide where configuration parameters are described in detail:

• **System** – Configures general device settings.	see page 4-1
• **WAN** – Configures WAN port connection settings.	see page 5-2
• **LAN** – Configures LAN settings.	see page 5-7
• **NAT** – Configures Network Address Translation settings.	see page 5-8
• **Firewall** – Configures firewall settings.	see page 5-11
• **Route** – Configures static routing settings.	see page 5-15
• **UPnP** – Enables UPnP.	see page 5-16
• **WIMAX** – Views the wireless connection status.	see page 6-1
• **VoIP** – Configures VoIP SIP settings.	see page 7-1

Chapter 4: System Settings

The RG230's System menu allows you to perform general management functions for the unit, including setting the system time, configuring an access password, and upgrading the system software.

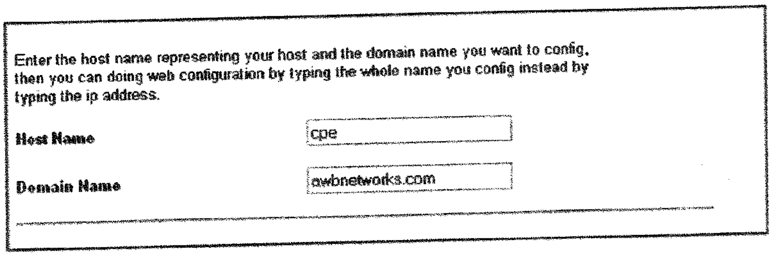
The System pages include the following options.

Table 4-1 System Settings

Menu	Description	Page
Host Name Config	Configures a host name and domain name	4-1
System Time	Configures the system time settings for updates from a time server	4-2
Administrator Settings	Configures user password for management access	4-3
Firmware Upgrade	Updates the current firmware	4-3
Configuration Tools	Restores the factory default settings, or save the unit's current settings	4-4
System Status	Displays WAN and LAN interface information and other system details	4-6
System Log	Displays event log entries	4-8
Reset	Resets the device	4-9

Host Name

The RG230 allows you to define a name that identifies your unit and the domain name used by the local network. Setting a host name enables the web interface to be accessed using an easy-to-remember name instead of its IP address.



Enter the host name representing your host and the domain name you want to config, then you can doing web configuration by typing the whole name you config instead by typing the ip address.

Host Name: cpe

Domain Name: awbnetworks.com

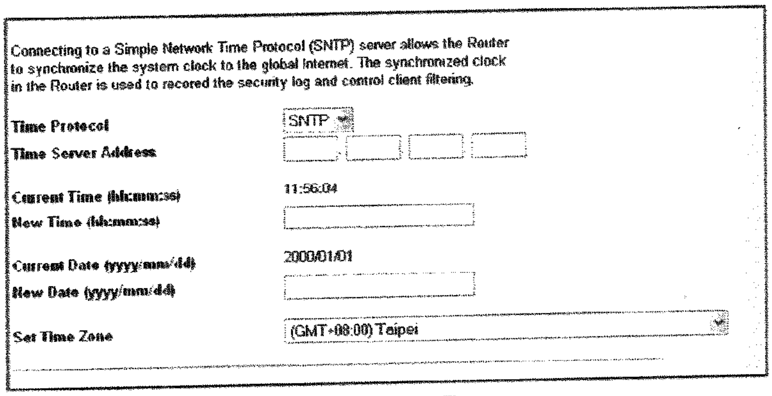
Figure 4-1 System Host Name

- **Host Name** – Enter the name chosen for the unit. (Default: cpe)
- **Domain Name** – Enter the domain to which the unit is connected.

System Time

The RG230 uses the Simple Network Time Protocol (SNTP) to set its internal clock based on periodic updates from a time server. Maintaining an accurate time on the device enables the system log to record meaningful dates and times for event entries.

SNTP uses Coordinated Universal Time (or UTC, formerly Greenwich Mean Time, or GMT) based on the time at the Earth's prime meridian, zero degrees longitude. To display a time corresponding to your local time, you must select your time zone.



Connecting to a Simple Network Time Protocol (SNTP) server allows the Router to synchronize the system clock to the global Internet. The synchronized clock in the Router is used to recored the security log and control client filtering.

Time Protocol	SNTP
Time Server Address	
Current Time (hh:mm:ss)	11:56:04
New Time (hh:mm:ss)	
Current Date (yyyy/mm/dd)	2000/01/01
New Date (yyyy/mm/dd)	
Set Time Zone	(GMT+08:00) Taipei

Figure 4-2 System Time

Time Protocol – Select SNTP to enable the unit to set its internal clock based on periodic updates from a time server. The unit acts as an SNTP client, periodically sending time synchronization requests to a specified time server. Alternatively, you can select "None" and set the time and date manually. (Default: SNTP)

Time Server Address – The IP address of a time server that the unit attempts to poll for a time update. (Default: 192.43.244.18)

Current Time (hh:mm:ss) – Displays the current time of the system clock.

New Time (hh:mm:ss) – Sets the system clock to the time specified.

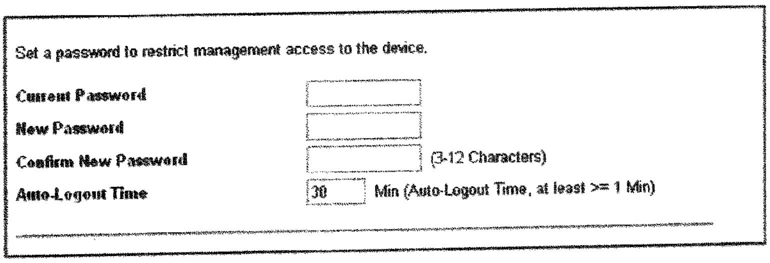
Current Date (yyyy:mm:dd) – Displays the current date of the system clock.

New Date (yyyy:mm:dd) – Sets the system clock to the date specified.

Set Time Zone – SNTP uses Coordinated Universal Time (or UTC, formerly Greenwich Mean Time, or GMT) based on the time at the Earth's prime meridian, zero degrees longitude. To display a time corresponding to your local time, you must select your time zone from the pull-down list. (Default: (GMT+08:00) Taipei)

Administrator Settings

The Administrator Settings page enables you to change the default password for management access to the RG230.



Set a password to restrict management access to the device.

Current Password

New Password

Confirm New Password (3-12 Characters)

Auto-Logout Time 30 Min (Auto-Logout Time, at least >= 1 Min)

Figure 4-3 Setting a Password

Current Password – You need to first enter your current administrator password to be able to configure a new one. (Default: admin)

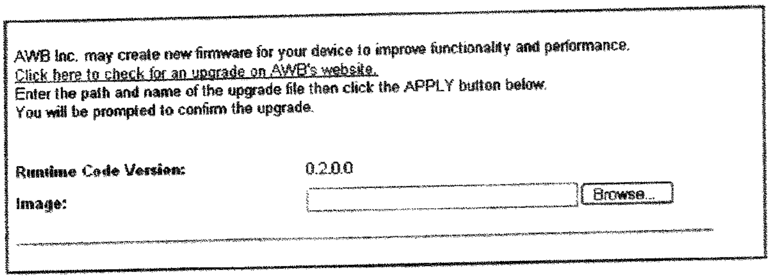
New Password – Enter a new administrator password. (Range: 3~12 characters)

Confirm New Password – Enter the new password again for verification. (Range: 3~12 characters)

Auto-Logout Time – The time of inactivity after which the unit terminates a web management session. (Default: 30 minutes; Range: 1~99 minutes)

Firmware Update

The Firmware Update page enables you to download new software to the unit.



AWB Inc. may create new firmware for your device to improve functionality and performance.
Click here to check for an upgrade on AWB's website.
Enter the path and name of the upgrade file then click the APPLY button below.
You will be prompted to confirm the upgrade.

Runtime Code Version: 0.2.0.0

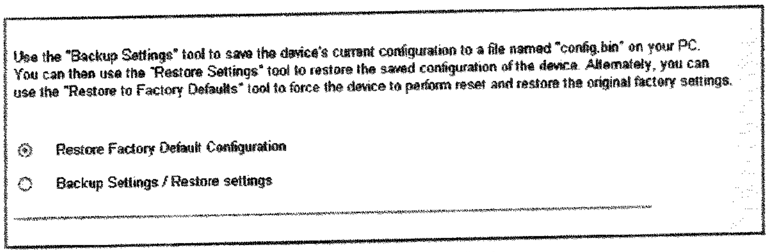
Image:

Figure 4-4 Firmware Update

- **Firmware Update** – Downloads an operation code file from the web management station to the RG230 using HTTP. Use the Browse button to locate the code file locally on the management station and click Apply to proceed.

Configuration Tools

The Configurations Tools page allows you to restore factory default settings, or save and restore the unit's configuration settings to or from a file on the management station.



Use the "Backup Settings" tool to save the device's current configuration to a file named "config.bin" on your PC. You can then use the "Restore Settings" tool to restore the saved configuration of the device. Alternately, you can use the "Restore to Factory Defaults" tool to force the device to perform reset and restore the original factory settings.

● Restore Factory Default Configuration

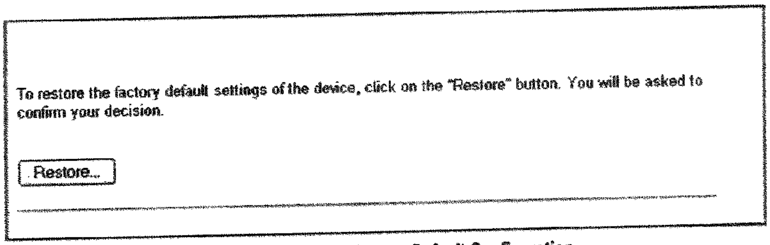
○ Backup Settings / Restore settings

Figure 4-5 Configuration Tools

Restore Factory Default Configuration – Resets the unit to its factory default settings.

Backup Settings/Restore Settings – When selected, prompts either to backup the current configuration to a file, or select a previously backed up file to restore to the unit.

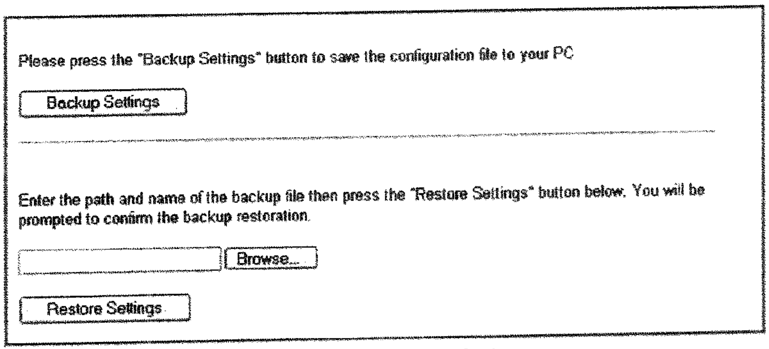
When you select "Restore Factory Default Configuration" and click Apply, a confirmation page displays. Click the Restore button to continue.



To restore the factory default settings of the device, click on the "Restore" button. You will be asked to confirm your decision.

Figure 4-6 Restore Factory Default Configuration

When you select "Backup Settings/Restore Settings" and click Apply, The following page displays.



Please press the "Backup Settings" button to save the configuration file to your PC

Enter the path and name of the backup file then press the "Restore Settings" button below. You will be prompted to confirm the backup restoration.

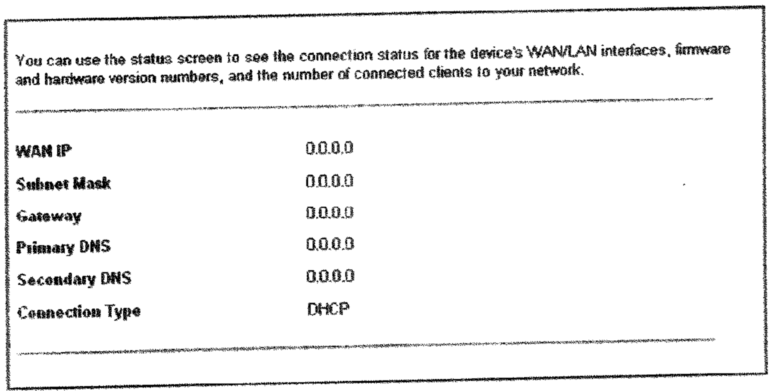
Figure 4-7 Backup/Restore Settings

Backup Settings – Saves the current configuration settings to a file named "config.bin" on the web management station.

Restore Settings – Restores a saved configuration file to the unit. You can use the Browse button to locate the file on the web management station.

System Status

The system status page displays connectivity status information for the unit's WiMAX (WAN) and LAN interfaces, firmware and hardware version numbers, and the number of clients connected to your network.



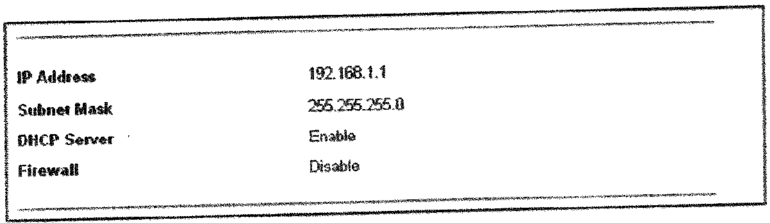
You can use the status screen to see the connection status for the device's WAN/LAN interfaces, firmware and hardware version numbers, and the number of connected clients to your network.

WAN IP	0.0.0.0
Subnet Mask	0.0.0.0
Gateway	0.0.0.0
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
Connection Type	DHCP

Figure 4-8 System Status – Internet

INTERNET – Displays WAN (WiMAX) connection status:

- **WAN IP** – Displays the IP address assigned by the service provider.
- **Subnet Mask** – Displays the WAN subnet mask assigned by the service provider.
- **Gateway** – Displays the WAN gateway address assigned by the service provider.
- **Primary DNS** – Displays the WAN primary DNS address.
- **Secondary DNS** – Displays the WAN secondary DNS address.
- **Connection Type** – Displays the connection type for the WAN. Either FIXED for a static IP setting, or DHCPC for dynamic IP assignment.
- **Release** – Releases the current IP address information.
- **Renew** – Initiates a new DHCP client request for an IP address.

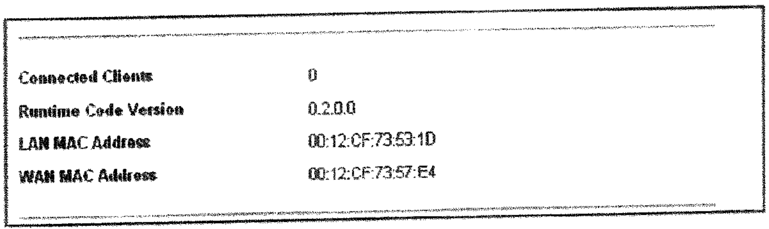


IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Server	Enable
Firewall	Disable

Figure 4-9 System Status – Gateway

GATEWAY – Display system IP settings, as well as DHCP, NAT and firewall status:

- **IP Address** – Displays the unit's IP address.
- **Subnet Mask** – Displays the subnet mask.
- **DHCP Server** – Displays the DHCP server status.
- **Firewall** – Displays the firewall status.



Connected Clients	0
Runtime Code Version	0.2.0.0
LAN MAC Address	00:12:CF:73:53:1D
WAN MAC Address	00:12:CF:73:57:E4

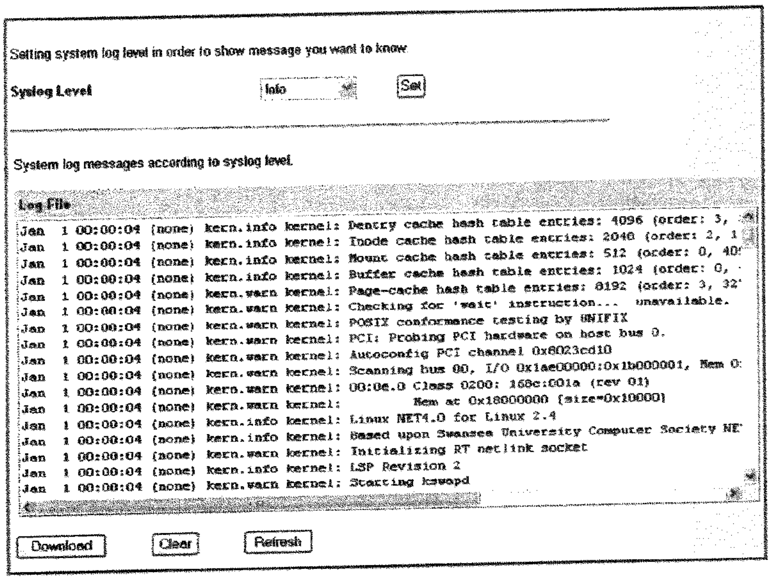
Figure 4-10 System Status – Information

INFORMATION – Displays the number of connected clients, as well as the unit's LAN and WAN MAC addresses:

- **Connected Clients** – Displays the number of connected clients, if any.
- **Runtime Code Version** – Displays the runtime code version.
- **LAN MAC Address** – Displays the LAN MAC address.
- **WAN MAC Address** – Displays WAN MAC address.

System Log

The System Log page allows you to display system event messages. The logged messages can serve as a valuable tool for isolating device and network problems, and also indicate if any unauthorized attempts have been made to gain access to your network.



Setting system log level in order to show message you want to know

Syslog Level: Info

System log messages according to syslog level.

Log File

```
Jan  1 00:00:04 (none) kern.info kernel: Dentry cache hash table entries: 4096 (order: 3,
Jan  1 00:00:04 (none) kern.info kernel: Inode cache hash table entries: 2048 (order: 2, 1
Jan  1 00:00:04 (none) kern.info kernel: Mount cache hash table entries: 512 (order: 0, 40
Jan  1 00:00:04 (none) kern.info kernel: Buffer cache hash table entries: 1024 (order: 0,
Jan  1 00:00:04 (none) kern.warn kernel: Page-cache hash table entries: 8192 (order: 3, 32
Jan  1 00:00:04 (none) kern.warn kernel: Checking for 'wait' instruction...  unavailable.
Jan  1 00:00:04 (none) kern.warn kernel: POSIX conformance testing by UNIFIX
Jan  1 00:00:04 (none) kern.warn kernel: PCI: Probing PCI hardware on host bus 0.
Jan  1 00:00:04 (none) kern.warn kernel: Autoconfig PCI channel 0x8023cd10
Jan  1 00:00:04 (none) kern.warn kernel: Scanning bus 00, I/O 0x1ae00000:0x1b000001, Mem 0:
Jan  1 00:00:04 (none) kern.warn kernel: 00:0e.0 Class 0200: 168c:001a (rev 01)
Jan  1 00:00:04 (none) kern.warn kernel:         Mem at 0x18000000 (size=0x10000)
Jan  1 00:00:04 (none) kern.info kernel: Linux NET4.0 for Linux 2.4
Jan  1 00:00:04 (none) kern.info kernel: Based upon Swansea University Computer Society NE
Jan  1 00:00:04 (none) kern.warn kernel: Initializing RT netlink socket
Jan  1 00:00:04 (none) kern.info kernel: LSP Revision 2
Jan  1 00:00:04 (none) kern.warn kernel: Starting kswapd
```

Figure 4-11 System Log

Syslog Level – Sets the minimum severity level for event logging. The system allows you to limit the messages that are logged by specifying a minimum severity level. Error message levels range from the most severe (Emergency) to least severe (Debug). The message levels that are logged include the specified minimum level up to the Emergency level. (Default: Info)

Download – Downloads the current log file to the web management station.

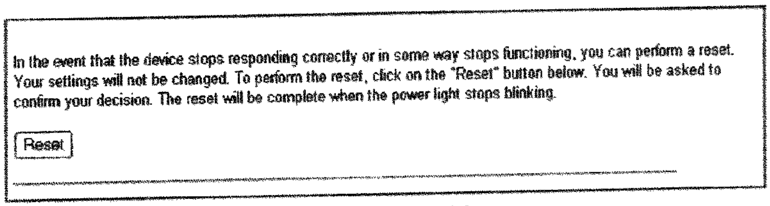
Clear – Deletes all entries in the current log file.

Refresh – Updates the displayed log entries on the web page.

Note: Log messages saved in the unit's memory are erased when the device is rebooted.

Reset

The Reset page allows you to restart the device's software. If the unit stops responding correctly or in some way stops functioning, performing a reset can clear the condition.



In the event that the device stops responding correctly or in some way stops functioning, you can perform a reset. Your settings will not be changed. To perform the reset, click on the "Reset" button below. You will be asked to confirm your decision. The reset will be complete when the power light stops blinking.

Figure 4-12 Reset Unit

Reset – Resets the unit. All current settings are retained.

Chapter 5: Gateway Configuration

The information in this chapter covers the configuration options for the RG230's Internet gateway functions.

The RG230 provides comprehensive firewall features and NAT isolation for Internet traffic passing from the WiMAX service provider to the local network connected to the LAN ports. The DHCP server feature can assign IP addresses for up to 32 local network PCs and wireless clients.

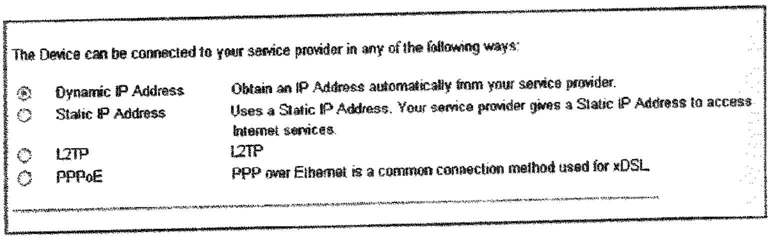
The Advanced Setup menu includes the following items for Internet gateway configuration.

Table 5-1 Gateway Configuration

Menu	**Description**	**Page**
WAN		5-2
WAN Settings	Sets the connection method of your Internet service provider	5-2
DNS	Specifies DNS servers that you want to access	5-6
LAN		5-7
LAN Settings	Sets the unit's IP address and configures the DHCP server for the local network	5-7
DHCP Client List	Displays connected DHCP clients that have been assigned IP addresses by the DHCP server	5-8
NAT		5-8
Virtual Server	Allows the unit to be configured as a virtual server	5-8
Port Mapping	Enables IP port mapping for special applications	5-10
DMZ	Allows clients to connect to the unit directly bypassing the firewall	5-11
Firewall		5-11
Firewall Setting	Controls access to and from the local network	5-11
Firewall Options	Blocks scans of the network services from an outside hacker	5-11
Client Filtering	Blocks Internet access based on IP addresses	5-13
MAC Control	Blocks internet access based on MAC addresses	5-14
Route		5-15
Routing Table List	Displays the routing table	5-15
UPnP		5-16
Settings	Provides support for Universal Plug and Play devices	5-16

WAN Settings

Select the WAN connection type used by your service provider and specify DNS (Domain Name System) servers.



The Device can be connected to your service provider in any of the following ways:

●	Dynamic IP Address	Obtain an IP Address automatically from your service provider.
○	Static IP Address	Uses a Static IP Address. Your service provider gives a Static IP Address to access Internet services.
○	L2TP	L2TP
○	PPPoE	PPP over Ethernet is a common connection method used for xDSL

Figure 5-1 WAN Settings

The unit can be connected to your ISP in one of the following ways:

Dynamic IP Address – Selects configuration for an Internet connection using DHCP for IP address assignment. This is the default setting.

Static IP Address – Selects configuration for an Internet connection using a fixed IP assignment.

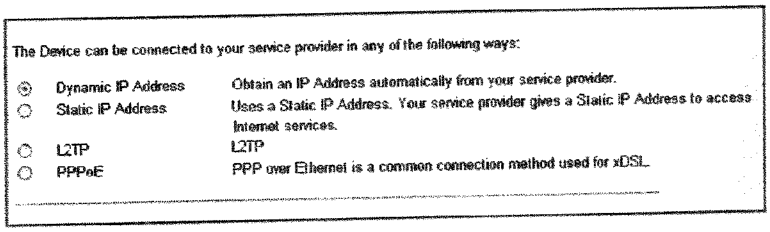
L2TP – Selects configuration for an Internet connection using the Layer 2 Tunneling Protocol, an access protocol often used for virtual private networks.

PPPoE – Selects configuration for an Internet connection using the Point-to-Point Protocol over Ethernet (PPPoE), a common connection method used for DSL access.

Note: For the Dynamic IP Address (DHCP) option, the unit requires no further configuration. Selecting other WAN types displays the parameters that are required for configuring the connection.

Dynamic IP Address

For dynamic IP assignment from the service provider, the unit functions as a Dynamic Host Configuration Protocol (DHCP) client. When enabled, no other settings are required.



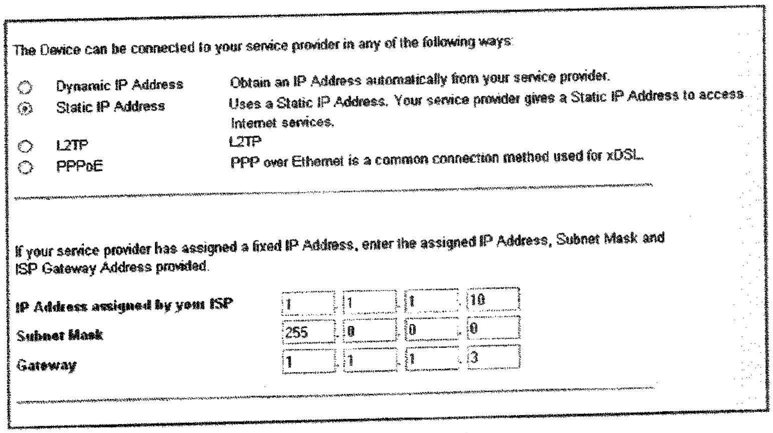
The Device can be connected to your service provider in any of the following ways:

●	Dynamic IP Address	Obtain an IP Address automatically from your service provider.
○	Static IP Address	Uses a Static IP Address. Your service provider gives a Static IP Address to access Internet services.
○	L2TP	L2TP
○	PPPoE	PPP over Ethernet is a common connection method used for xDSL.

Figure 5-2 Dynamic IP Address

Static IP Settings

Selecting Static IP Address for the WAN type enables you to enter static IP settings as assigned by the service provider.



The Device can be connected to your service provider in any of the following ways:

○	Dynamic IP Address	Obtain an IP Address automatically from your service provider.
●	Static IP Address	Uses a Static IP Address. Your service provider gives a Static IP Address to access Internet services.
○	L2TP	L2TP
○	PPPoE	PPP over Ethernet is a common connection method used for xDSL.

If your service provider has assigned a fixed IP Address, enter the assigned IP Address, Subnet Mask and ISP Gateway Address provided.

IP Address assigned by your ISP	1 . 1 . 1 . 10
Subnet Mask	255 . 0 . 0 . 0
Gateway	1 . 1 . 1 . 3

Figure 5-3 Static IP Settings

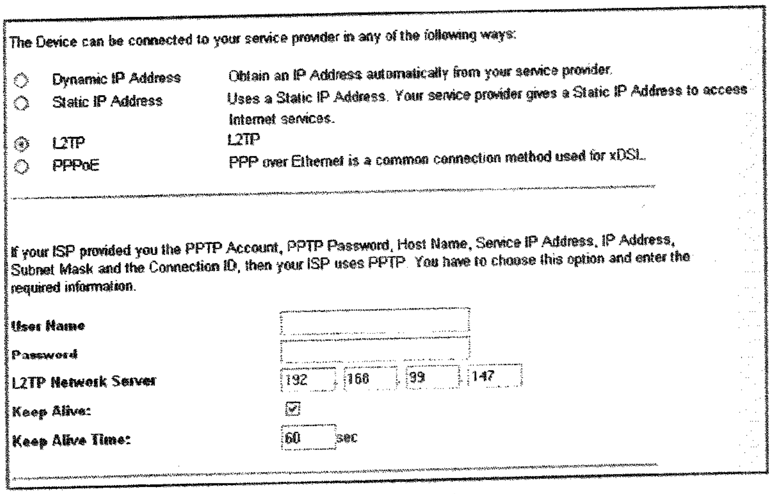
IP Address assigned by your ISP – The IP address provided by your service provider. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods.

Subnet Mask – Indicates the subnet mask, such as 255.255.255.0.

Gateway – The gateway IP address provided by your service provider.

L2TP Settings

If your service provider supports Layer 2 Tunneling Protocol (L2TP) for your Internet connection, configure the settings described below.



The Device can be connected to your service provider in any of the following ways:

○	Dynamic IP Address	Obtain an IP Address automatically from your service provider.
○	Static IP Address	Uses a Static IP Address. Your service provider gives a Static IP Address to access Internet services.
●	L2TP	L2TP
○	PPPoE	PPP over Ethernet is a common connection method used for xDSL.

If your ISP provided you the PPTP Account, PPTP Password, Host Name, Service IP Address, IP Address, Subnet Mask and the Connection ID, then your ISP uses PPTP. You have to choose this option and enter the required information.

User Name	
Password	
L2TP Network Server	192 . 168 . 99 . 147
Keep Alive:	☑
Keep Alive Time:	60 sec

Figure 5-4 L2TP Settings

User Name – Enter your user name for connecting to the L2TP service, as supplied by the service provider. (Range: 1-32 characters)

Password – Specify the password for your connection, as supplied by the service provider. (Default: No password)

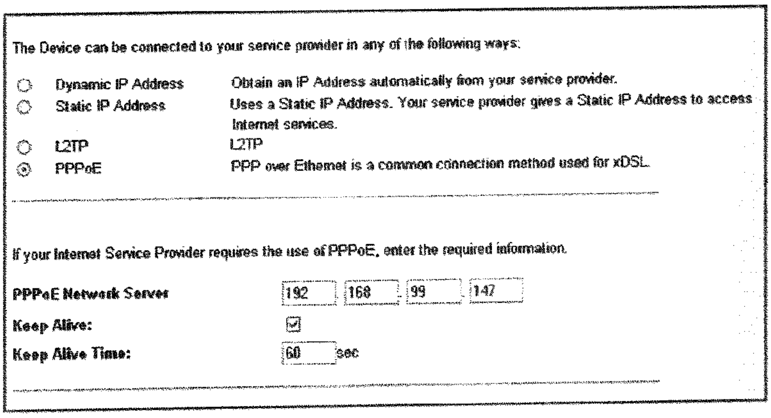
L2TP Network Server – The IP address of the L2TP server, as specified by the service provider.

Keep Alive – This option enables the unit to check periodically that the L2TP connection is still operating. If the connection is found to be lost, the unit automatically attempts to reconnect to the service provider. (Default: Enabled)

Keep Alive Time – The time period the unit waits before checking that the L2TP connection is still operating. This parameter only applies when Keep Alive is enabled. (Default: 60 seconds; Range: 10-180 seconds)

PPPoE Settings

If your service provider supports Point-to-Point Protocol over Ethernet (PPPoE) for your Internet connection, configure the settings described below.



The Device can be connected to your service provider in any of the following ways:

○	Dynamic IP Address	Obtain an IP Address automatically from your service provider.
○	Static IP Address	Uses a Static IP Address. Your service provider gives a Static IP Address to access Internet services.
○	L2TP	L2TP
●	PPPoE	PPP over Ethernet is a common connection method used for xDSL.

If your Internet Service Provider requires the use of PPPoE, enter the required information.

PPPoE Network Server 192 . 168 . 99 . 147

Keep Alive: ☑

Keep Alive Time: 60 sec

Figure 5-5 PPPoE Settings

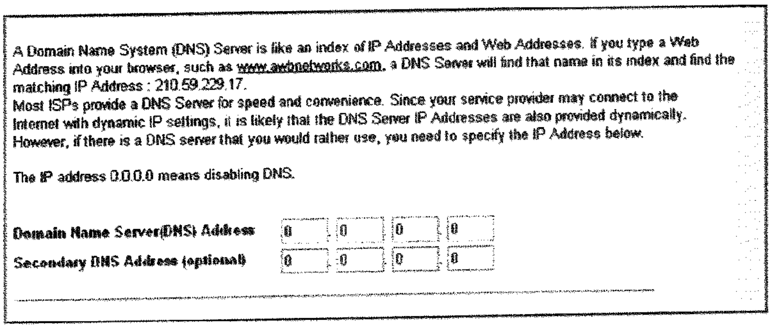
PPPoE Network Server – The IP address of the PPPoE server, as specified by the service provider.

Keep Alive – This option enables the unit to check periodically that the PPPoE connection is still operating. If the connection is found to be lost, the unit automatically attempts to reconnect to the service provider. (Default: Enabled)

Keep Alive Time – The time period the unit waits before checking that the PPPoE connection is still operating. This parameter only applies when Keep Alive is enabled. (Default: 60 seconds; Range: 10-180 seconds)

DNS

DNS (Domain Name System) server addresses are usually provided by service providers, however if you want to specify certain servers, the DNS page enables you to enter primary and secodary DNS addresses.



A Domain Name System (DNS) Server is like an index of IP Addresses and Web Addresses. If you type a Web Address into your browser, such as www.awbnetworks.com, a DNS Server will find that name in its index and find the matching IP Address : 210.59.229.17.
Most ISPs provide a DNS Server for speed and convenience. Since your service provider may connect to the Internet with dynamic IP settings, it is likely that the DNS Server IP Addresses are also provided dynamically. However, if there is a DNS server that you would rather use, you need to specify the IP Address below.

The IP address 0.0.0.0 means disabling DNS.

Domain Name Server(DNS) Address 0 . 0 . 0 . 0

Secondary DNS Address (optional) 0 . 0 . 0 . 0

Figure 5-6 DNS Settings

Domain Name Server (DNS) Address – Address of the primary DNS server, specified in the form of 0.0.0.0. (The default address 0.0.0.0 disables the manual DNS setting.)

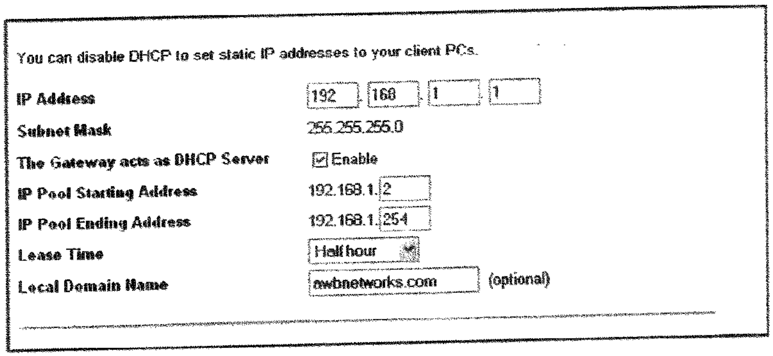
Secondary DNS Address (optional) – Optional address of a secondary DNS server, specified in the form of 0.0.0.0.

LAN

The RG230 must have a valid IP address for management using a web browser and to support other features. The unit has a default IP address of 192.168.1.1. You can use this IP address or assign another address that is compatible with your existing local network. The unit can also be enabled as a Dynamic Host Configuration Protocol (DHCP) server to allocate IP addresses to local PCs.

LAN Settings

The RG230 includes a DHCP server that can assign temporary IP addresses to any attached host requesting the service. Addresses are assigned to clients from a common address pool configured on the unit. Configure an address pool by specifying start and end IP addresses. Be sure not to include the unit's IP address in the address pool range.



You can disable DHCP to set static IP addresses to your client PCs.

IP Address	192 . 168 . 1 . 1
Subnet Mask	255.255.255.0
The Gateway acts as DHCP Server	☑ Enable
IP Pool Starting Address	192.168.1. 2
IP Pool Ending Address	192.168.1. 254
Lease Time	Half hour
Local Domain Name	awbnetworks.com (optional)

Figure 5-7 LAN Settings

IP Address – The IP address of the unit. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods.The default setting is 192.168.1.1.

Subnet Mask – Indicates the local subnet mask is fixed as 255.255.255.0.

The Gateway acts as DHCP Server – Check this box to enable the DHCP server.

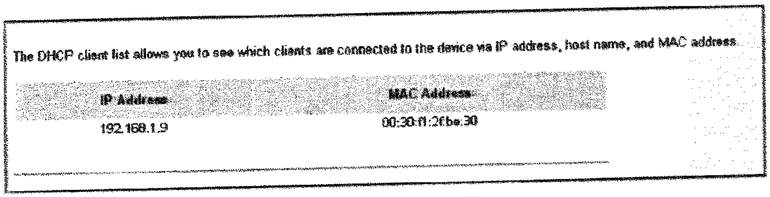
IP Pool Starting/Ending Address – Specifies the start and end IP address of a range that the DHCP server can allocate to DHCP clients. You can specify a single address or an address range. Note that the address pool range is always in the same subnet as the unit's IP setting. (Default: 192.168.1.2 to 192.168.1.254)

Lease Time – Selects a time limit for the use of an IP address form the IP pool. When the time limit expires, the client has to request a new IP address. (Default: Half hour; Options: Half hour, one hour, two hours, half day, one day, two days, one week, two weeks)

Local Domain Name – This optional parameter specifies the name of the domain the unit is attached to.

DHCP Client List

The DHCP Client List page enables you to see the MAC address of devices that are currently connected to the unit and have been assigned an IP address by the DHCP server.



The DHCP client list allows you to see which clients are connected to the device via IP address, host name, and MAC address.

IP Address	MAC Address
192.168.1.9	00:30:f1:2f:be:30

Figure 5-8 DHCP Client List

NAT

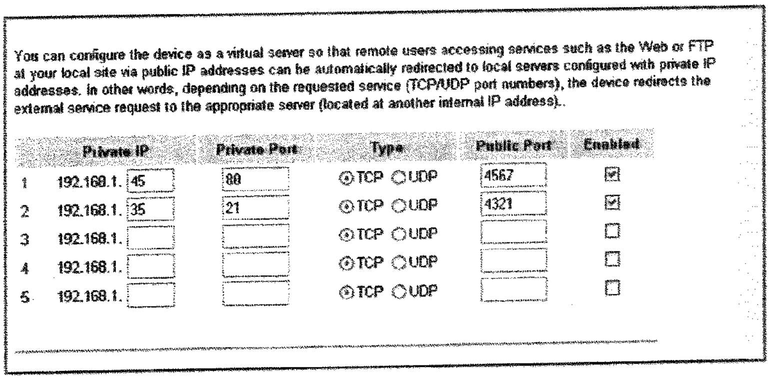
Network Address Translation (NAT) is a standard method of mapping multiple "internal" IP addresses to one "external" IP address on devices at the edge of a network. For the RG230, the internal (local) IP addresses are the IP addresses assigned to local PCs by the DHCP server, and the external IP address is the IP address assigned to the WiMAX interface.

Virtual Server

Using the NAT Virtual Server feature, remote users can access different servers on your local network using your single public IP address.

Remote users accessing services such as web or FTP at your local site thorugh your public IP address, are redirected (mapped) to other local server IP addresses and TCP/UDP port numbers. For example, if you set Type/Public Port to TCP/80 (HTTP or web) and the Private IP/Port to 192.168.7.9/80, then all HTTP requests from outside users forwarded to 192.168.7.9 on port 80. Therefore, by just using your external IP address provided by your ISP, Internet users can access the services they need at the local addresses to which you redirect them.

The more common TCP service port numbers include: HTTP: 80, FTP: 21, Telnet: 23, and POP3: 110.



You can configure the device as a virtual server so that remote users accessing services such as the Web or FTP at your local site via public IP addresses can be automatically redirected to local servers configured with private IP addresses. In other words, depending on the requested service (TCP/UDP port numbers), the device redirects the external service request to the appropriate server (located at another internal IP address)..

	Private IP	Private Port	Type	Public Port	Enabled
1	192.168.1. 45	80	● TCP ○ UDP	4567	☑
2	192.168.1. 35	21	● TCP ○ UDP	4321	☑
3	192.168.1.		● TCP ○ UDP		□
4	192.168.1.		● TCP ○ UDP		□
5	192.168.1.		● TCP ○ UDP		□

Figure 5-9 Virtual Server

Private IP – The IP address of the server on the local Ethernet network. The specified address must be in the same subnet as the RG230 and its DHCP server address pool. (Range: 192.168.1.1 to 192.168.1.254)

Private Port – Specifies the TCP/UDP port number used on the local server for the service. (Range: 0-65535)

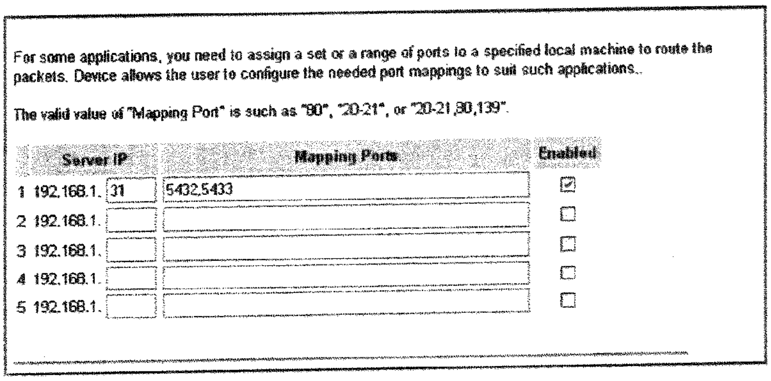
Type – Specifies the port type. (Options: TCP or UDP; Default: TCP)

Public Port – Specifies the public TCP/UDP port used for the service on the WAN interface. (Range: 0-65535)

Enabled – Enables the virtual server mapping on the specified ports. (Default: Disabled)

Port Mapping

Some applications, such as Internet gaming, videoconferencing, Internet telephony and others, require multiple connections. These applications cannot work with Network Address Translation (NAT) enabled. If you need to run applications that require multiple connections, use port mapping to specify the additional public ports to be opened for each application.



For some applications, you need to assign a set or a range of ports to a specified local machine to route the packets. Device allows the user to configure the needed port mappings to suit such applications..

The valid value of "Mapping Port" is such as "80", "20-21", or "20-21,80,139".

	Server IP	Mapping Ports	Enabled
1	192.168.1. 31	5432,5433	☑
2	192.168.1.		□
3	192.168.1.		□
4	192.168.1.		□
5	192.168.1.		□

Figure 5-10 Port Mapping

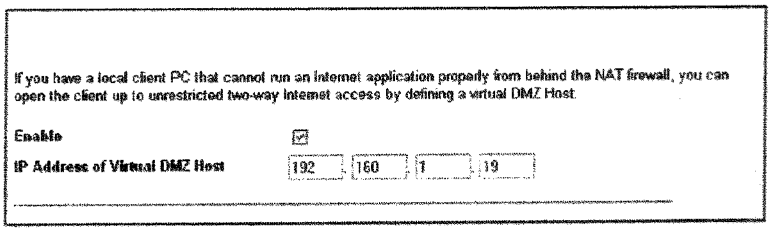
Server IP – The IP address of the local server. (Range: 192.168.1.1 to 192.168.1.254)

Mapping Ports – Specifies the TCP/UDP ports that the application requires. The ports may be specified individually, in a range, or a combination of both. For example, 7, 11, 57, 72-96. (Range: 0-65535)

Enabled – Enables port mapping for the specified IP address. (Default: Disabled)

DMZ

If you have a client PC that cannot run an Internet application properly from behind the NAT firewall, you can open the client up to unrestricted two-way internet access by defining a virtual-DMZ (virtual-demilitarized-zone) host.



If you have a local client PC that cannot run an Internet application properly from behind the NAT firewall, you can open the client up to unrestricted two-way Internet access by defining a virtual DMZ Host.

Enable ☑

IP Address of Virtual DMZ Host 192 . 160 . 1 . 19

Figure 5-11 DMZ Settings

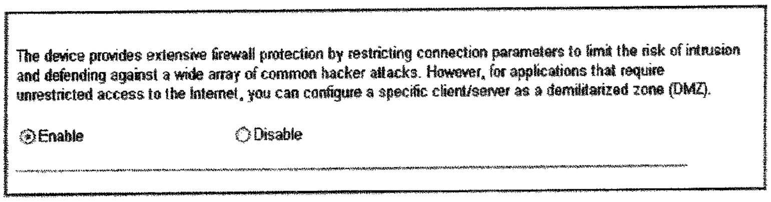
Enable – Enables the feature. (Default: Disabled)

IP Address of Virtual DMZ Host – Specifies the IP address of the virtual DMZ host. (Range: 192.168.1.1 to 192.168.1.254; Default: 0.0.0.0)

Note: Adding a host to the DMZ may expose your local network to a variety of security risks, so only use this option as a last resort.

Firewall

The RG230 provides extensive firewall protection by restricting connection parameters to limit the risk of intrusion and defending against a wide array of common hacker attacks. You can also block access to the Internet from clients on the local network based on IP addresses and TCP/UDP port numbers, or specific MAC addresses.



The device provides extensive firewall protection by restricting connection parameters to limit the risk of intrusion and defending against a wide array of common hacker attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server as a demilitarized zone (DMZ).

● Enable ○ Disable

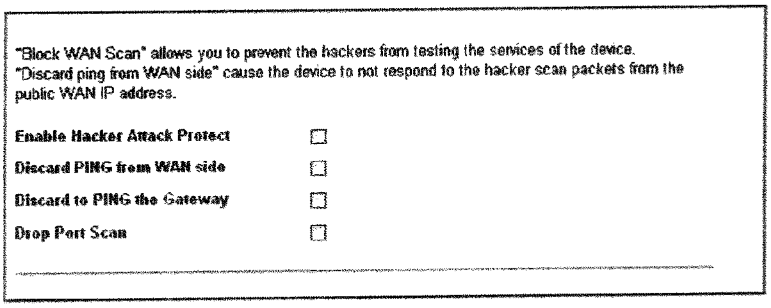
Figure 5-12 Firewall Setting

Enable – Enables the feature.

Disable – Disables the feature. (This is the default.)

Firewall Options

The RG230's firewall enables access control of client PCs, blocks common hacker attacks, including IP Spoofing, Land Attack, Ping of Death, Smurf Attack, TCP null scan, ICMP defect, and TCP SYN flooding. The firewall does not significantly affect system performance and it is best to leave it enabled to protect your network.



"Block WAN Scan" allows you to prevent the hackers from testing the services of the device.
"Discard ping from WAN side" cause the device to not respond to the hacker scan packets from the public WAN IP address.

Enable Hacker Attack Protect □

Discard PING from WAN side □

Discard to PING the Gateway □

Drop Port Scan □

Figure 5-13 Firewall Options

Enable Hacker Attack Protect – Network attacks that deny access to a network device are called DoS attacks. DoS attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources. The Router protects against the following DoS attacks: IP Spoofing, Land Attack, Ping of Death, Smurf Attack, TCP null scan, ICMP defect, and TCP SYN flooding.

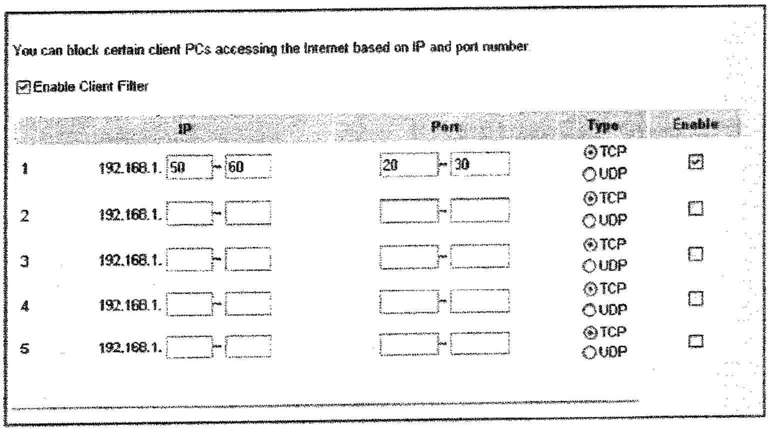
Discard PING from WAN side – Prevents pings on the unit's WiMAX interface from being routed to the network.

Discard to PING the Gateway – Prevents any response to a ping to the unit's IP address.

Drop Port Scan – Prevents outside hackers form testing the TCP/UDP port numbers on the unit for any services.

Client Filtering

You can block access to the Internet from clients on the local network by specifying IP addresses and TCP/UDP port numbers. You can configure up to five IP filters on the unit.



You can block certain client PCs accessing the Internet based on IP and port number

☑ Enable Client Filter

	IP	Port	Type	Enable
1	192.168.1. 50 ~ 60	20 ~ 30	● TCP ○ UDP	☑
2	192.168.1. ~	~	● TCP ○ UDP	□
3	192.168.1. ~	~	● TCP ○ UDP	□
4	192.168.1. ~	~	● TCP ○ UDP	□
5	192.168.1. ~	~	● TCP ○ UDP	□

Figure 5-14 Client Filtering Settings

Enable Client Filter – Enables client filtering for entries in the table. (Default: Disabled)

IP – Specifies an IP address or range on the local network. (Range: 192.168.1.1 to 192.168.1.254)

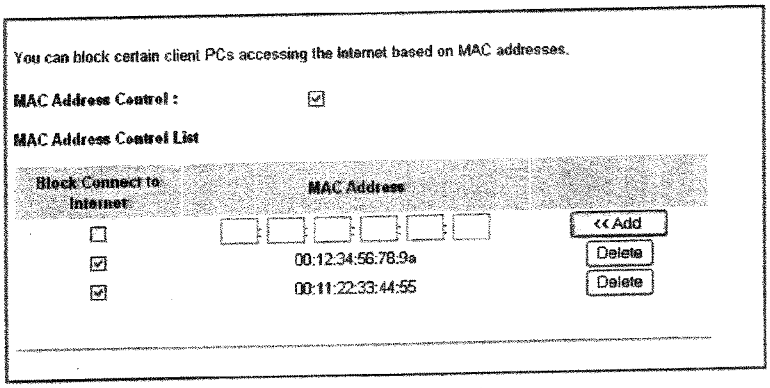
Port – Specifies a TCP/UDP port number range to filter. (Range: 0-65535)

Type – Specifies the the port type. (Options: TCP or UDP; Default: TCP)

Enable – Enables filtering for the table entry. (Default: Disabled)

MAC Control

You can block access to the Internet from clients on the local network by MAC addresses. You can configure up to 32 MAC address filters on the unit.



You can block certain client PCs accessing the Internet based on MAC addresses.

MAC Address Control : ☑

MAC Address Control List

Block Connect to Internet	MAC Address	
□	__ : __ : __ : __ : __ : __	<<Add
☑	00:12:34:56:78:9a	Delete
☑	00:11:22:33:44:55	Delete

Figure 5-15 MAC Control

MAC Address Control – Enables the feature. (Default: Enabled)

Block Connect to Internet – Blocks Internet access for the scpecified MAC address. (Default: Enabled)

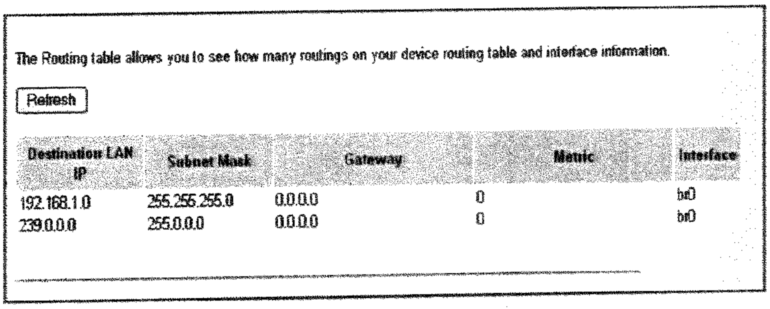
MAC Address – Specifies a local PC MAC address.

Add – Adds a new MAC address to the filter table.

Delete – Removes a MAC address from the filter table.

Route

The Routing Table displays the list of static routes on the unit.



The Routing table allows you to see how many routings on your device routing table and interface information.

Destination LAN IP	Subnet Mask	Gateway	Metric	Interface
192.168.1.0	255.255.255.0	0.0.0.0	0	br0
239.0.0.0	255.0.0.0	0.0.0.0	0	br0

Figure 5-16 Routing Table

Destination LAN IP – The IP address that identifies the IP subnet of the remote network.

Subnet Mask – The mask that identifies the IP subnet of the remote network.

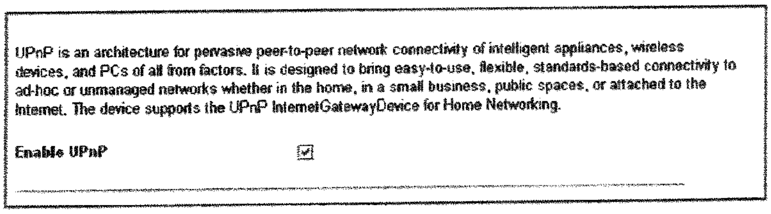
Gateway – The IP address of the router within the local IP subnet that forwards traffic to the remote IP subnet.

Metric – Cost for the local interface. This cost is only used when routes are imported by a dynamic routing protocol.

Interface – Indicates the local network interface on the unit.

UPnP

UPnP (Universal Plug and Play Forum) provides inter-connectivity between devices supported by the same standard.



UPnP is an architecture for pervasive peer-to-peer network connectivity of intelligent appliances, wireless devices, and PCs of all from factors. It is designed to bring easy-to-use, flexible, standards-based connectivity to ad-hoc or unmanaged networks whether in the home, in a small business, public spaces, or attached to the Internet. The device supports the UPnP InternetGatewayDevice for Home Networking.

Enable UPnP ☑

Figure 5-17 UPnP Setting

UPnP – Enables UpnP support on the unit. (Default: Enabled)

Chapter 6: WiMAX Settings

The RG230's WiMAX menu enables you to configure WiMAX connection profiles, view subscriber station information, and select an operating antenna.

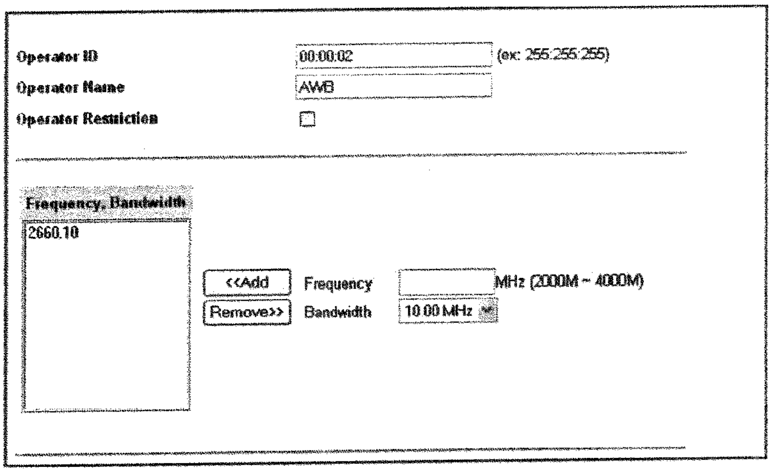
The WiMAX pages include the following options.

Table 6-1 WiMAX Settings

Menu	Description	Page
Profile	Configures WiMAX connection profiles	6-1
SSinfo	Displays subscriber station information for the unit	6-4
Antenna Setting	Configures use of internal or external antennas	6-5

Profile Configuration

A profile allows a user to set specific details for connecting to various WiMAX service providers. The RG230 must have at least one profile configured to be able to connect to a WiMAX service.



Operator ID	00:00:02 (ex: 255:255:255)
Operator Name	AWB
Operator Restriction	□

Frequency, Bandwidth: 2660.10

Frequency: MHz (2000M ~ 4000M)

Bandwidth: 10.00 MHz

Figure 6-1 WiMAX Profile Configuration

Operator ID – The ID number that identifies the WiMAX operator for this profile. (Default: 00:00:02)

Operator name – The WiMAX operator name. (Default: AWB)

Operator Restriction – When enabled, the user can only connect to the service provider specified in the profile. The user cannot roam to other networks. When disabled, the operator specified in the profile will be used when base stations are detected, otherwise the user can roam to other networks. (Default: Disabled)

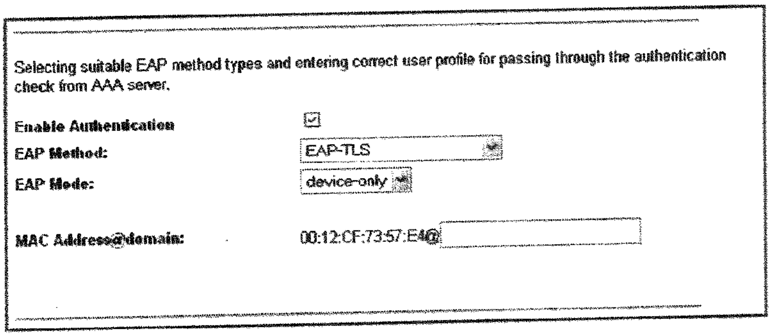
Scan Frequency – Specifies a center frequency to scan.
Range: FCC_2.3: 2305 – 2320 MHz, 2345 – 2360 MHz
FCC_2.5: 2496 – 2690 MHz
Taiwan NCC: 2500 – 2690 MHz
Support for Full Scan and Partial Scan

Scan Bandwidth – Either 5, 7, 8.75, or 10 MHz, depending on model (software configurable). (Options: 5.00, 7.00, 8.75, 10.00 MHz)
2.3 GHz model: 5, 8.75, and 10 MHz
2.5 GHz model: 5, and 10 MHz
3.5 GHz model: 5, 7, and 10 MHz

Add/Remove – Use the Add button to add a new center frequency and channel bandwidth to scan. Use the Remove button to delete a frequency from the scan list.

Authentication

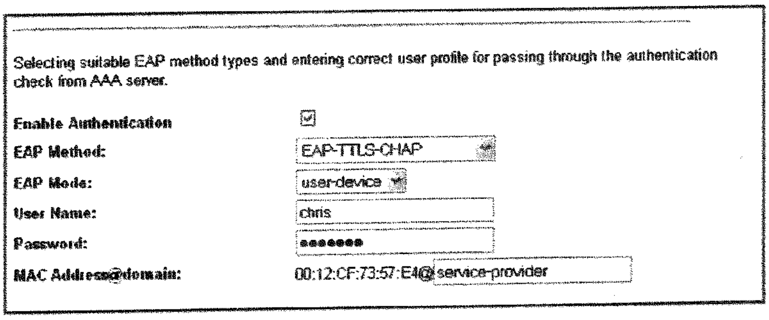
Set user authentication for the WiMAX connection profile, as specified by the service provider. Selecting EAP-TLS, EAP-TTLS-CHAP, or EAP-TTLS-MSCHAPV2 displays the parameters that are required for configuring the authentication method.



Selecting suitable EAP method types and entering correct user profile for passing through the authentication check from AAA server.

Enable Authentication ☑
EAP Method: EAP-TLS
EAP Mode: device-only
MAC Address@domain: 00:12:CF:73:57:E4@

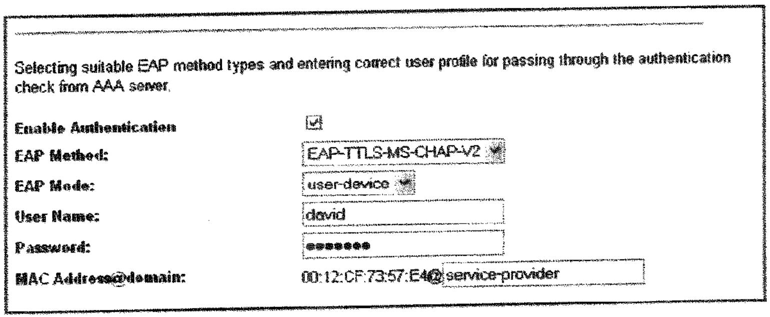
Figure 6-2 WiMAX Profile Authentication - EAP-TLS



Selecting suitable EAP method types and entering correct user profile for passing through the authentication check from AAA server.

Enable Authentication	☑
EAP Method:	EAP-TTLS-CHAP
EAP Mode:	user-device
User Name:	chris
Password:	●●●●●●●
MAC Address@domain:	00:12:CF:73:57:E4@ service-provider

Figure 6-3 WiMAX Profile Authentication - EAP-TTLS-CHAP



Selecting suitable EAP method types and entering correct user profile for passing through the authentication check from AAA server.

Enable Authentication	☑
EAP Method:	EAP-TTLS-MS-CHAP-V2
EAP Mode:	user-device
User Name:	david
Password:	●●●●●●●
MAC Address@domain:	00:12:CF:73:57:E4@ service-provider

Figure 6-4 WiMAX Profile Authentication - EAP-TTLS-MSCHAPV2

Enable Authentication – Enables user authentication for connection to the network. (Default: Disabled)

EAP Method – Selects the Extensible Authentication Protocol (EAP) method to use for authentication. (Default: EAP-TTLS-MSCHAPV2)

- **EAP-TLS** – Transport Layer Security. Provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based encryption keys to secure subsequent communications between the user and the network.
- **EAP-TTLS-CHAP** – Tunneled Transport Layer Security with Challenge-Handshake Authentication Protocol (CHAP). This security method provides for certificate-based, mutual authentication of the client and network through an encrypted channel. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates.
- **EAP-TTLS-MSCHAPV2** – Tunneled Transport Layer Security with Microsoft's version 2 of CHAP.