



Accton Wireless Broadband Corp.

RG230
WiMAX 802.16e
Self-Install Residential Gateway

User Guide

RG230

*Indoor IEEE 802.16e-2005 Mobile WiMAX Gateway,
with 2.3/2.5/3.5 GHz Frequency Band Support,
Four LAN (RJ-45) Ports,
Two Optional VoIP (RJ-11) Ports,
and Optional 802.11g Wi-Fi*

RG230
E072009-CS-R02
149100001700W

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.

IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.

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.

Note to US Model Owner: To comply with US FCC regulation, the country selection function has been completely removed from all US models. The above function is for non-US models only.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

Due to the essential high output power nature of WiMAX devices, use of this device with other transmitters at the same time may exceed the FCC RF exposure limit and such usage must be prohibited (unless such co-transmission has been approved by FCC in the future).

This device is for ATC of Open Range Communications and follows Part 25 regulation.

EC Conformance Declaration 0682

Marking by the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). This equipment meets the following conformance standards:

- EN 60950-1 (IEC 60950-1) - Product Safety
- EN 301 489-1, EN 301 489-4, EN 302 326-2 (V1.2.2), EN 302 326-3 (V1.2.2) - EMC requirements for radio equipment

This device is intended for use in all European Community countries.

NCC CCAA08W20050T4

本設備已取得國家通訊傳播委員會低功率射頻認證。依國家通訊傳播委員會低功率射頻電機技術規範(LP0002)及低功率電波輻射性電機管理辦法之第十二條規定，經型式認證合格之低功率射頻電機之設備使用者，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

About This Guide

Purpose

This guide details the hardware features of the WiMAX 802.16e Self-Install 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 802.16e Self-Install Residential Gateway.

Quick Installation Guide

As part of the WiMAX 802.16e Self-Install 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.

July 2009 Revision

This is the second revision of this guide. This guide is valid for software release v0.2.0.3. It includes the following changes:

- Updated for regulatory standards compliance.

December 2008 Revision

This is the first revision of this guide. This guide is valid for software release v0.2.0.3.

Table of Contents

Chapter 1: Introduction	1-1
RG230 Hardware Description	1-2
Scan Button	1-3
WiMAX Antennas	1-3
Wi-Fi Option	1-3
Power Status Indicator LED	1-3
Wi-Fi Status Indicator LED	1-4
WiMAX Signal Indicator LEDs	1-4
10BASE-T/100BASE-TX LAN Ports	1-5
VoIP Phone Ports	1-5
Power Adapter Socket	1-5
Reset Button	1-5

Chapter 2: Installing the RG230	2-1
Package Checklist	2-1
Installation Overview	2-1
Select a Location	2-1
Cable Connections	2-2

Chapter 3: Initial Configuration	3-1
Accessing the Web Management Interface	3-1
Home Page	3-2
Using the Setup Wizard	3-3
The Advanced Setup Menu	3-5

Chapter 4: System Settings	4-1
System Status	4-2
Administrator Settings	4-4
Firmware Update	4-4
Configuration Tools	4-5
System Time	4-5
Reset	4-7

Chapter 5: Gateway Configuration	5-1
LAN	5-2
LAN Settings	5-2

DHCP Client List	5-3
NAT	5-3
Virtual Server	5-3
Port Mapping	5-5
DMZ	5-6
Firewall	5-6
Firewall Options	5-7
Client Filtering	5-8
MAC Control	5-9
Route	5-10
UPnP	5-11
<hr/>	
Chapter 6: WiMAX Settings	6-1
User Account Settings	6-1
Subscriber Station Information	6-2
Antenna Setting	6-3
<hr/>	
Chapter 7: VoIP Settings	7-1
SIP Account	7-2
Dial Plan	7-3
Call Feature	7-5
<hr/>	
Appendix A: Troubleshooting	A-1
Diagnosing LED Indicators	A-1
Cannot Connect to the Internet	A-1
Cannot Access Web Management	A-1
Forgot or Lost the Password	A-2
Resetting the Unit	A-2
<hr/>	
Appendix B: Specifications	B-1
Physical Specifications	B-1
WiMAX Specifications	B-2
VoIP Specifications	B-3
Compliances	B-3
<hr/>	
Appendix C: Cables and Pinouts	C-1
Twisted-Pair Cable Assignments	C-1
10/100BASE-TX Pin Assignments	C-1
Straight-Through Wiring	C-2
Crossover Wiring	C-2

RJ-11 Ports	C-3
-------------	-----

Appendix D: License Information **D-1**

The GNU General Public License	D-1
--------------------------------	-----

Glossary**Index**

Tables

Table 1-1	RG230 Models	1-1
Table 1-2	Power Status LED	1-3
Table 1-3	Wi-Fi Status LED	1-4
Table 1-4	WiMAX Signal Status LEDs	1-4
Table 1-5	LAN Port Status LEDs	1-5
Table 4-1	System Settings	4-1
Table 5-1	Gateway Configuration	5-1
Table 6-1	WiMAX Settings	6-1
Table A-1	Troubleshooting Chart	A-1
Table C-1.	10/100BASE-TX MDI and MDI-X Port Pinouts	C-2
Table C-2.	RJ-11 Port Pinout	C-3

Figures

Figure 1-1	Front of the RG230	1-2
Figure 1-2	RG230 LED Indicators	1-3
Figure 1-3	Back of the RG230	1-4
Figure 1-4	Base of the RG230	1-6
Figure 2-1	RG230 Connections	2-2
Figure 3-1	Login Page	3-1
Figure 3-2	Home Page	3-2
Figure 3-3	WiMAX Login	3-3
Figure 3-4	Apply Settings	3-4
Figure 3-5	Setup Wizard Finished	3-4
Figure 3-6	Advanced Setup	3-5
Figure 4-1	System Status – Internet	4-2
Figure 4-2	System Status – Gateway	4-2
Figure 4-3	System Status – VoIP	4-3
Figure 4-4	System Status – Information	4-3
Figure 4-5	Setting a Password	4-4
Figure 4-6	Firmware Update	4-4
Figure 4-7	Configuration Tools	4-5
Figure 4-8	Restore Factory Default Configuration	4-5
Figure 4-9	System Time	4-6
Figure 4-10	Reset Unit	4-7
Figure 5-1	LAN Settings	5-2
Figure 5-2	DHCP Client List	5-3
Figure 5-3	Virtual Server	5-4
Figure 5-4	Port Mapping	5-5
Figure 5-5	DMZ Settings	5-6
Figure 5-6	Firewall Setting	5-6
Figure 5-7	Firewall Options	5-7
Figure 5-8	Client Filtering Settings	5-8
Figure 5-9	MAC Control	5-9
Figure 5-10	Routing Table	5-10
Figure 5-11	UPnP Setting	5-11
Figure 6-1	WiMAX Account Settings	6-1
Figure 6-2	Subscriber Station Information	6-2
Figure 6-3	WiMAX Antenna Setting	6-3
Figure 7-1	SIP Account Settings	7-2
Figure 7-2	Dial Plan Settings	7-3
Figure 7-3	Call Features	7-6
Figure C-1	RJ-45 Connector	C-1
Figure C-2	Straight-Through Wiring	C-2
Figure C-3	Crossover Wiring	C-2
Figure C-4	RJ-11 Port Pinout	C-3

Chapter 1: Introduction

The RG230 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 is a plug-and-play device. There are two available models for each of the 2.3, 2.5, and 3.5 GHz WiMAX frequency bands. Which model you use will depend on the frequency band of your service provider's WiMAX service.

The RG230 includes four RJ-45 Ethernet switch ports for LAN connections and two optional RJ-11 Voice over IP (VoIP) phone ports. An 802.11b/g Wi-Fi module is available for the 3.5 GHz models that provides a local Wi-Fi access point service.

For the 2.5 GHz SKUs, the RG230 covers the ATC frequency band from 2483.5 MHz up to 2690 MHz.

The following table lists the available RG230 models.

Table 1-1 RG230 Models

Frequency Band	Model Number	Description
2.3 GHz	RG230-2.3-1D	Unit with 1 data port.
	RG230-2.3-1D2V	Unit with 1 data port and 2 VoIP ports.
	RG230-2.3-4D	Unit with 4 data ports.
	RG230-2.3-4D2V	Unit with 4 data ports and 2 VoIP ports.
2.5 GHz	RG230-2.5-1D	Unit with 1 data port.
	RG230-2.5-1D2V	Unit with 1 data port and 2 VoIP ports.
	RG230-2.5-4D	Unit with 4 data ports.
	RG230-2.5-4D2V	Unit with 4 data ports and 2 VoIP ports.
3.5 GHz	RG230-3.5-1D	Unit with 1 data port.
	RG230-3.5-1D2V	Unit with 1 data port and 2 VoIP ports.
	RG230-3.5-4D	Unit with 4 data ports.
	RG230-3.5-4D2V	Unit with 4 data ports and 2 VoIP ports.
	RG230-3.5-4D1W	Unit with 4 data ports and Wi-Fi.
	RG230-3.5-4D2V1W	Unit with 4 data ports, 2 VoIP ports, and Wi-Fi.

The RG230 offers a user-friendly web-based management interface for the configuration of all the unit's features. Any PC directly attached to the unit can access the management interface using a web browser, such as Internet Explorer (version 6.0 or above) or Firefox (version 1.5 or above).

1 Introduction

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.

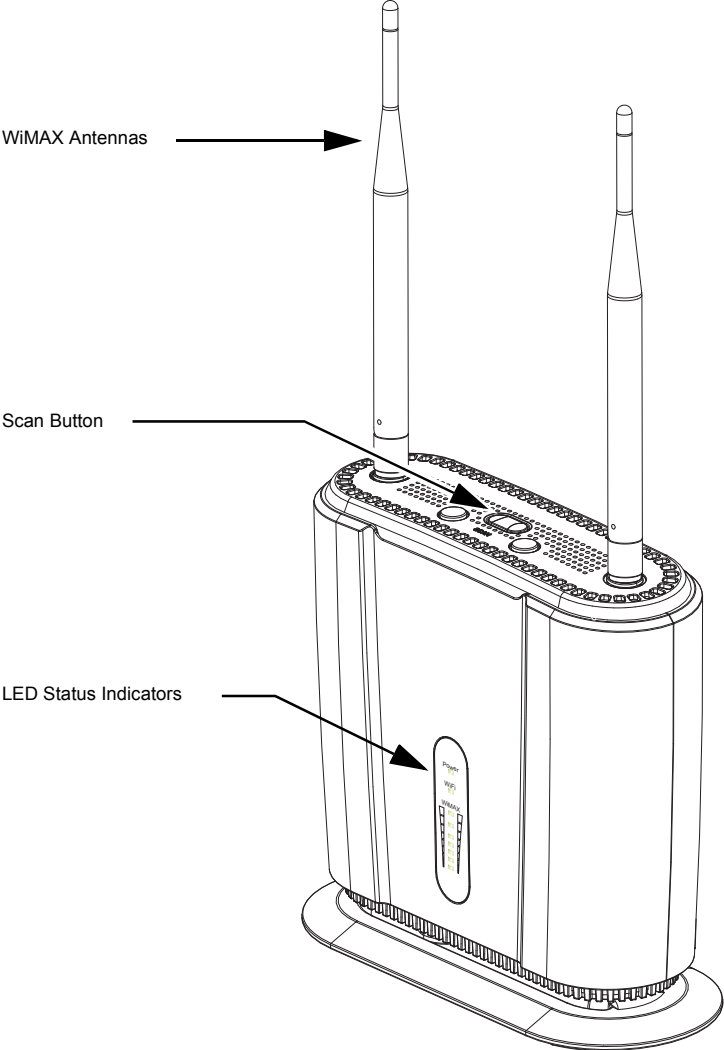


Figure 1-1 Front of the RG230

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.

Wi-Fi Option

The RG230 3.5 GHz model includes the 802.11b/g Wi-Fi option. This unit includes internal antennas for local wireless connections to PCs.

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.

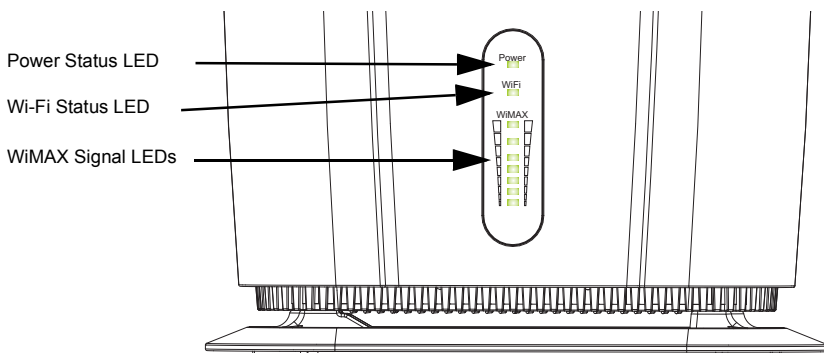


Figure 1-2 RG230 LED Indicators

Table 1-2 Power Status LED

Status	Description
On Green	The unit has completed entry to a WiMAX network.
Blinking Green	When blinking with three of the WiMAX signal LEDs turned on, indicates authentication has failed.
On Orange	Indicates one of the following conditions: <ul style="list-style-type: none"> • After power on, indicates the unit is running its self test. • Indicates the network entry process has restarted.
On Red	A system failure has occurred.
Off	No power is being supplied to the unit.

Wi-Fi Status Indicator LED

The 3.5 GHz RG230 model, which supports Wi-Fi operation, includes a Wi-Fi LED indicator that displays the Wi-Fi network status. The LED, which is located on the front panel, is described in the following table.

Table 1-3 Wi-Fi Status LED

Status	Description
On Green	The Wi-Fi radio is enabled and operating normally.
Flashing Green	Indicates data traffic in the Wi-Fi network.
Off	There is no Wi-Fi connection or the radio is disabled.

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.
All 7 LEDs	Off	No power is being supplied to the unit.

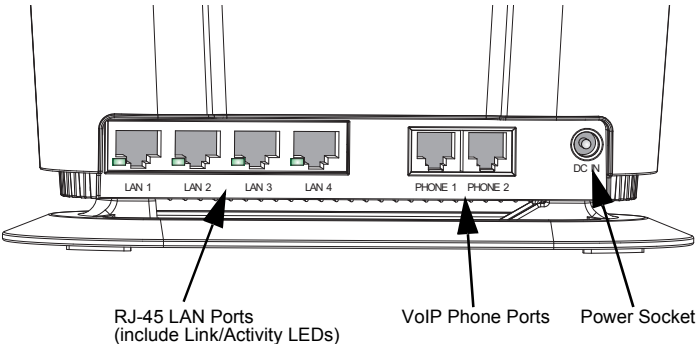


Figure 1-3 Back of the RG230

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

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.

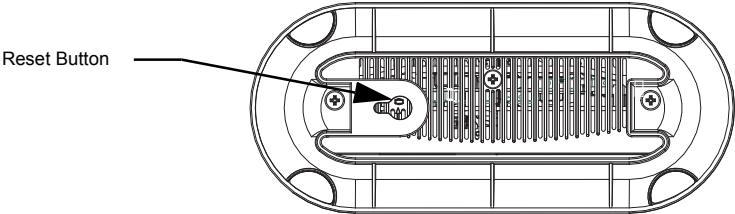


Figure 1-4 Base of the RG230

Chapter 2: Installing the RG230

This section describes how to install and connect the RG230 WiMAX 802.16e Self-Install Residential Gateway.

Package Checklist

The RG230 package includes:

- RG230 unit (RG230-2.3, RG230-2.5, or RG230-3.5)
- 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.

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.

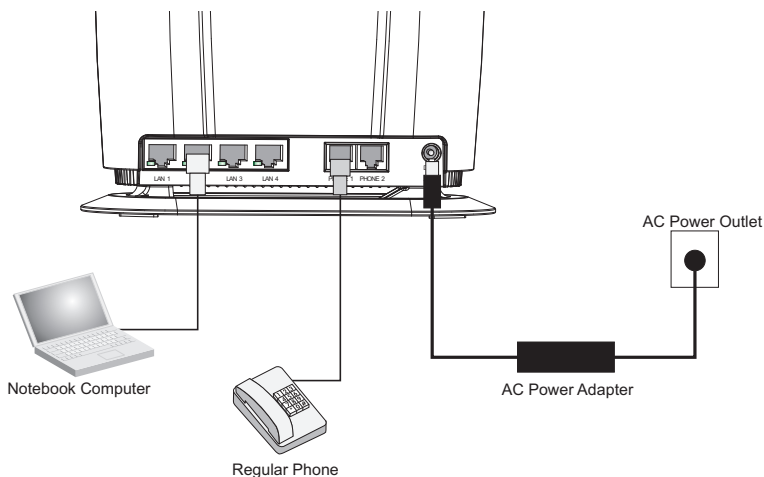


Figure 2-1 RG230 Connections

To connect the RG230, follow these steps:

1. Power on the RG230 by 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."

2 Installing the RG230

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.

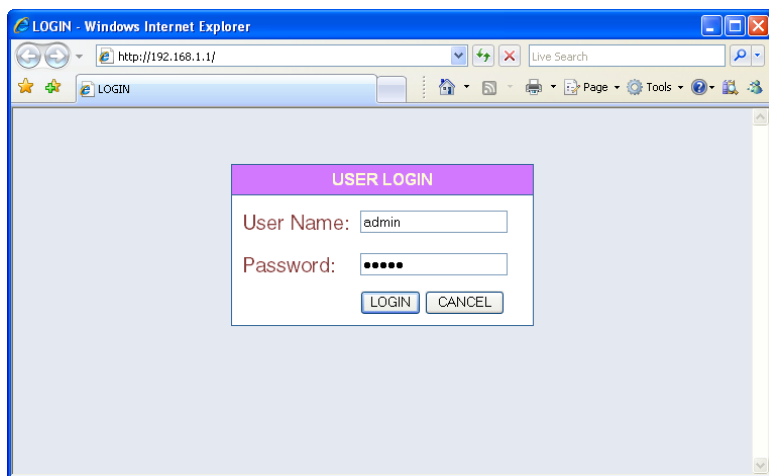


Figure 3-1 Login Page

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

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

Home Page

The home page displays the current status of the WiMAX connection.

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 3-5.

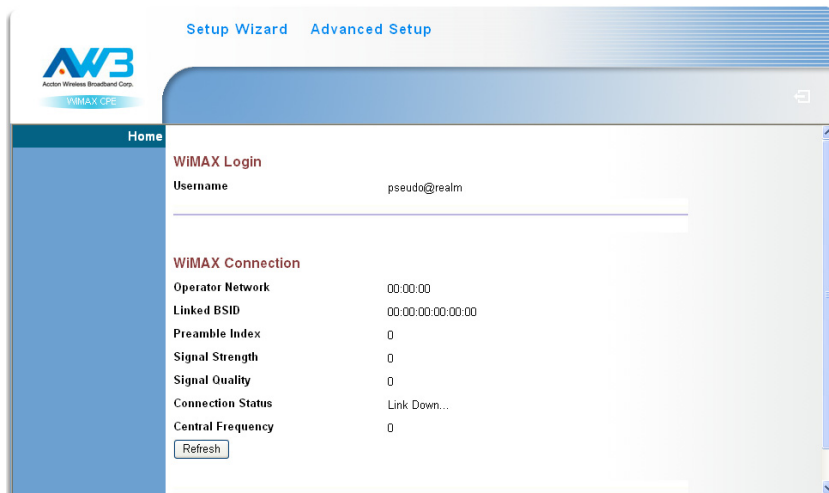


Figure 3-2 Home Page

The following parameters are displayed on the home page:

- **Username** – Describes the WiMAX network login name.
- **Operator Network** – The identity of the operator network.
- **Linked BSID** – The identifier of the connected base station.
- **Preamble Index** – A number that identifies the sector on the connected base station.
- **Signal Strength** – The current signal strength value of the received WiMAX radio signal.
- **Signal Quality** – An indication of the carrier-to-interference-plus-noise-ratio (CINR), which measures the strength of the receive signal compared to other interference and noise.
- **Connection Status** – The current status of the WiMAX connection.
- **Central Frequency** – The center frequency of the WiMAX signal.

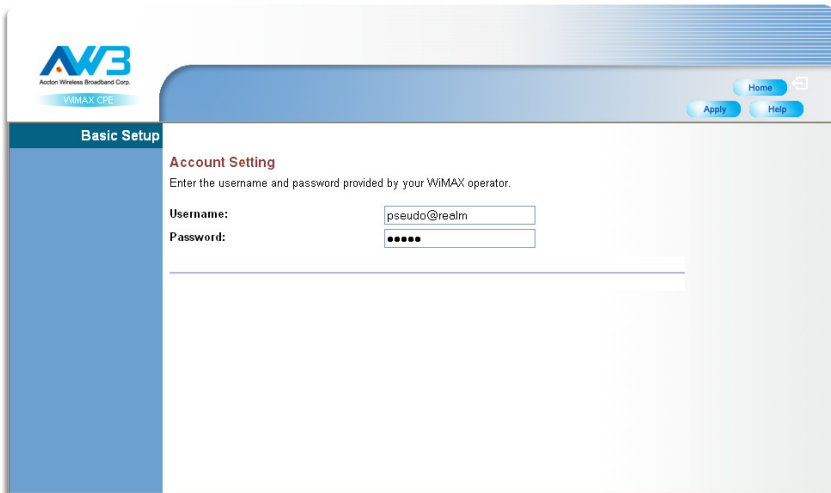
Using the Setup Wizard

The Setup Wizard takes you through the basic configuration steps for the RG230.

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. **WiMAX Login** – Configures user authentication settings for connection to the WiMAX network.



The screenshot shows a web interface for the 'Basic Setup' section. On the left is a blue sidebar with the 'Basic Setup' label. The main content area is titled 'Account Setting' and includes the instruction: 'Enter the username and password provided by your WiMAX operator.' Below this are two input fields: 'Username:' with the value 'pseudo@realm' and 'Password:' with masked characters '*****'. In the top right corner, there are 'Home', 'Apply', and 'Help' buttons. The top left corner features the 'AVB' logo (Action Video Broadband Corp.) and 'WiMAX CPE' text.

Figure 3-3 WiMAX Login

User Name – The user name required for authentication as provided by the WiMAX operator. (Default: pseudo@realm)

Password – The user password required for authentication as provided by the WiMAX operator. (Default: hello)

3 Initial Configuration

2. **Apply Settings** – Click “Apply” to confirm the basic settings.

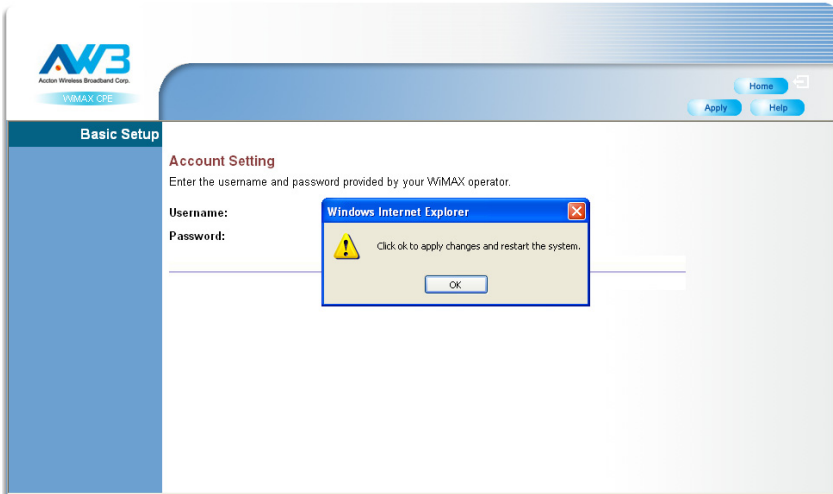


Figure 3-4 Apply Settings

3. **Basic Setup Finished** – When the Setup Wizard steps are completed the unit reboots and attempts to connect to the specified WiMAX network. Click on the Home button to return to the Home page.

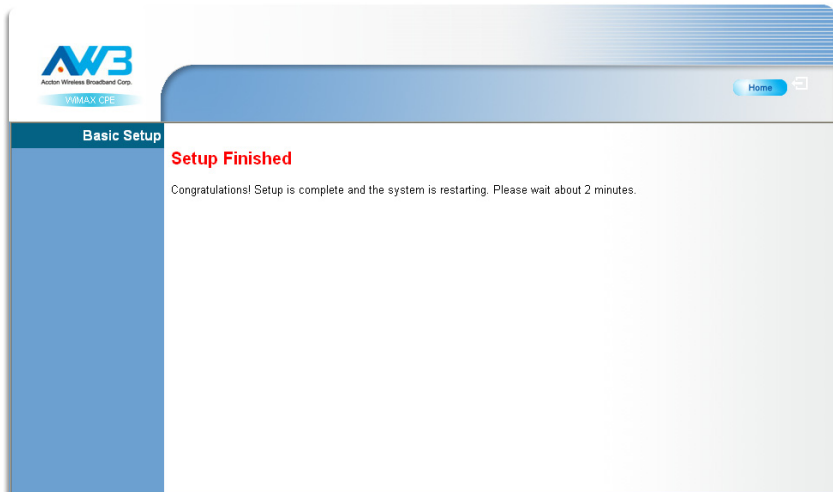


Figure 3-5 Setup Wizard Finished

The Advanced Setup Menu

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

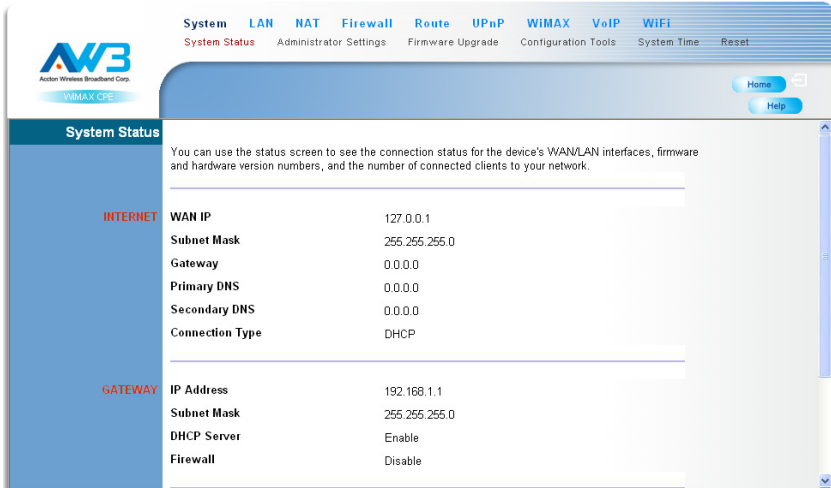


Figure 3-6 Advanced Setup

Each primary menu item is summarized 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
- **LAN** – Configures LAN settings. see page 5-2
- **NAT** – Configures Network Address Translation settings. see page 5-3
- **Firewall** – Configures firewall settings. see page 5-6
- **Route** – Configures static routing settings. see page 5-10
- **UPnP** – Enables UPnP. see page 5-11
- **WiMAX** – Views the wireless connection status. see page 6-1
- **VoIP** – Configures VoIP SIP settings. see page 7-1
- **WiFi** – Configures 802.11 access point settings. see page 8-1

3 Initial Configuration

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
System Status	Displays WAN and LAN interface information and other system details	4-2
Administrator Settings	Configures user password for management access	4-4
Firmware Upgrade	Updates the current firmware	4-4
Configuration Tools	Restores the factory default settings, or save the unit's current settings	4-5
System Time	Configures the system time settings for updates from a time server	4-5
Reset	Resets the device	4-7

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 4-1 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 DHCP for dynamic IP assignment.

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Server	Enable
Firewall	Disable

Figure 4-2 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.

Phone 1 Status	Registration not active
Phone 2 Status	Registration not active

Figure 4-3 System Status – VoIP

VoIP STATUS – Displays the VoIP phone status:

- **Phone 1 Status** – Displays the SIP status of phone line 1.
- **Phone 2 Status** – Displays the SIP status of phone line 2.

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

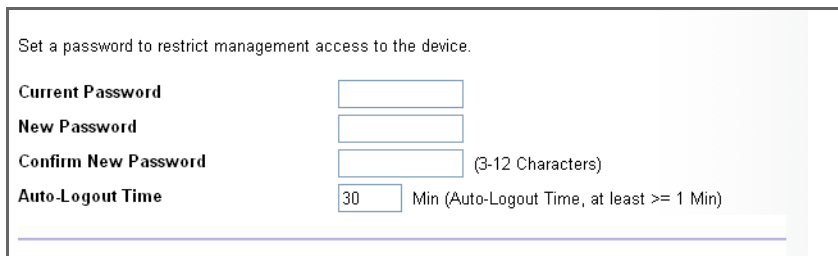
Figure 4-4 System Status – Information

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.

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

Figure 4-5 Setting a Password

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

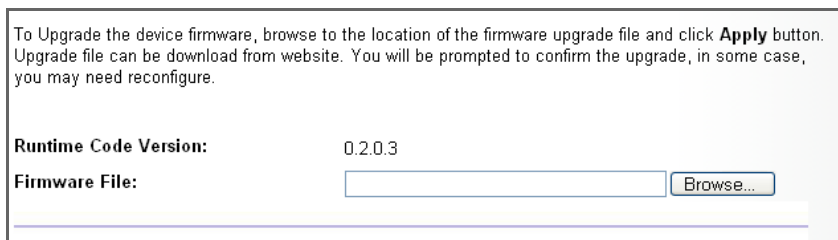
New Password – Enter a new administrator password. (Range: 3~12 characters)

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.



To Upgrade the device firmware, browse to the location of the firmware upgrade file and click **Apply** button. Upgrade file can be download from website. You will be prompted to confirm the upgrade, in some case, you may need reconfigure.

Runtime Code Version: 0.2.0.3

Firmware File:

Figure 4-6 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.

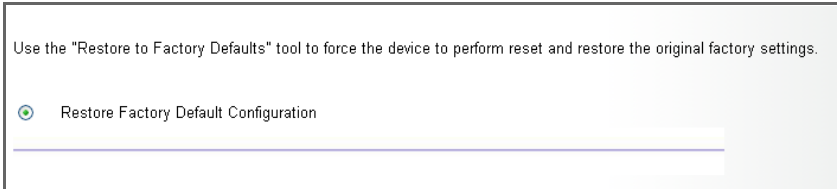


Figure 4-7 Configuration Tools

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

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



Figure 4-8 Restore Factory Default Configuration

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 device to synchronize the system clock to the global Internet. The synchronized clock in the device is used to record the security log and control client filtering.

Time Protocol	SNTP ▾
Time Server Address	192.43.244.18
Current Time (hh:mm:ss)	13:51:21
New Time (hh:mm:ss)	<input type="text"/>
Current Date (yyyy/mm/dd)	2008/02/01
New Date (yyyy/mm/dd)	<input type="text"/>
Set Time Zone	(GMT+08:00) Taipei ▾

Figure 4-9 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)

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.

Reset

Figure 4-10 Reset Unit

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

4

System Settings

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
<i>LAN</i>		5-2
LAN Settings	Sets the unit's IP address and configures the DHCP server for the local network	5-2
DHCP Client List	Displays connected DHCP clients that have been assigned IP addresses by the DHCP server	5-3
<i>NAT</i>		5-3
Virtual Server	Allows the unit to be configured as a virtual server	5-3
Port Mapping	Enables IP port mapping for special applications	5-5
DMZ	Allows clients to connect to the unit directly bypassing the firewall	5-6
<i>Firewall</i>		5-6
Firewall Setting	Controls access to and from the local network	5-6
Firewall Options	Blocks scans of the network services from an outside hacker	5-6
Client Filtering	Blocks Internet access based on IP addresses	5-8
MAC Control	Blocks internet access based on MAC addresses	5-9
<i>Route</i>		5-10
Routing Table List	Displays the routing table	5-10
<i>UPnP</i>		5-11
Settings	Provides support for Universal Plug and Play devices	5-11

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	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="1"/> . <input type="text" value="1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
The Gateway acts as DHCP Server	<input checked="" type="checkbox"/> Enable
IP Pool Starting Address	192.168.1. <input type="text" value="2"/>
IP Pool Ending Address	192.168.1. <input type="text" value="254"/>
Lease Time	<input type="text" value="Half hour"/> ▾
Local Domain Name	<input type="text" value="awbnetworks.com"/> (optional)

Figure 5-1 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 from 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 5-2 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 through 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	4567	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	80	<input checked="" type="checkbox"/>
2	192.168.1. 35	4321	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	21	<input checked="" type="checkbox"/>
3	192.168.1. <input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input type="checkbox"/>
4	192.168.1. <input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input type="checkbox"/>
5	192.168.1. <input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input type="checkbox"/>

Figure 5-3 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: 1-65535)

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: 1-65535)

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	<input checked="" type="checkbox"/>
2	192.168.1. <input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	192.168.1. <input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	192.168.1. <input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	192.168.1. <input type="text"/>	<input type="text"/>	<input type="checkbox"/>

Figure 5-4 Port Mapping

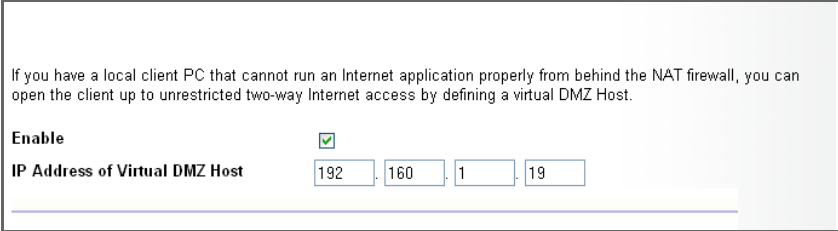
Server IP – The IP address of the local server. (Range: 192.168.1.1 to 192.168.1.254)

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: 1-65535)

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

Figure 5-5 DMZ Settings

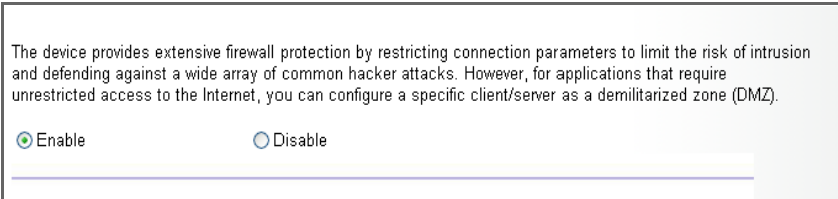
Enable – Enables the feature. (Default: Disabled)

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 5-6 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	<input type="checkbox"/>
Discard PING from WAN side	<input type="checkbox"/>
Discard to PING the Gateway	<input type="checkbox"/>
Drop Port Scan	<input type="checkbox"/>

Figure 5-7 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 from 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. <input type="text" value="50"/> ~ <input type="text" value="60"/>	<input type="text" value="20"/> ~ <input type="text" value="30"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input checked="" type="checkbox"/>
2	192.168.1. <input type="text"/> ~ <input type="text"/>	<input type="text"/> ~ <input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
3	192.168.1. <input type="text"/> ~ <input type="text"/>	<input type="text"/> ~ <input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
4	192.168.1. <input type="text"/> ~ <input type="text"/>	<input type="text"/> ~ <input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
5	192.168.1. <input type="text"/> ~ <input type="text"/>	<input type="text"/> ~ <input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>

Figure 5-8 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: 1-65535)

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 20 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	
<input type="checkbox"/>	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	<input type="button" value=" << Add"/>
<input checked="" type="checkbox"/>	00:12:34:56:78:9a	<input type="button" value=" Delete"/>
<input checked="" type="checkbox"/>	00:11:22:33:44:55	<input type="button" value=" Delete"/>

Figure 5-9 MAC Control

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

Block Connect to Internet – Blocks Internet access for the specified 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 5-10 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 form 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 5-11 UPnP Setting

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

Chapter 6: WiMAX Settings

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

The WiMAX pages include the following options.

Table 6-1 WiMAX Settings		
Menu	Description	Page
Account	Configures WiMAX network user authentication	6-2
SSinfo	Displays subscriber station information for the unit	6-2
Antenna Setting	Configures use of internal or external antennas	6-3

User Account Settings

Configures user account authentication settings for connection to the WiMAX network.

Enter the username and password provided by your WiMAX operator.

Username:

Password:

Figure 6-1 WiMAX Account Settings

User Name – The user name required for authentication as provided by the WiMAX operator. (Default: pseudo@realm)

Password – The user password required for authentication as provided by the WiMAX operator. (Default: hello)

Subscriber Station Information

The SSInfo page displays information about the software versions on the RG230 unit.

Note: The current WiMAX connection status is described under the section “Home Page” on page 3-2.

Show the subscriber station information.

Firmware Version	0.0.0
Driver Version	
Library Version	04.01.121
Baseband Chip Version	0
RF Chip Version	0

Figure 6-2 Subscriber Station Information

Firmware Version – The version of software code running on the unit.

Driver Version – The version of the WiMAX chip driver software.

Library Version – The version of WiMAX library software.

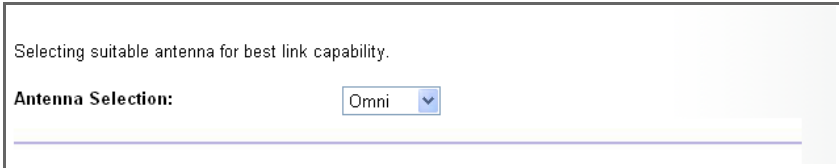
Baseband Chip Version – The version of the WiMAX baseband chip.

RF Chip Version – The version of the WiMAX radio chip.

Antenna Setting

The RG230 provides the option of using an external antenna instead of the omnidirectional antennas supplied with the unit.

Note: External antennas are not currently supported on the RG230. The only valid setting is “Omni.”



Selecting suitable antenna for best link capability.

Antenna Selection:

Figure 6-3 WiMAX Antenna Setting

Chapter 7: VoIP Settings

Voice over Internet Protocol (VoIP) technology is a way of using the Internet to make phone calls. Phone calls can be transmitted over the Internet by encoding a voice call into data packets at one end and then decoding it back into voice calls at the other end. This encoding and decoding is from an analog signal (your voice) into a digital signal (data packets) and then back into an analog signal.

The RG230 uses Session Initiation Protocol (SIP) as the control mechanism that sets up, initiates, and terminates calls between a caller and a called party. The SIP messaging makes use of “Proxy,” “Redirect,” and “Registration” servers to process call requests and find the location of called parties across the Internet. When SIP has set up a call between two parties, the actual voice communication is a direct peer-to-peer connection using the standard Real-Time Protocol (RTP), which streams the encoded voice data across the network.

You can make VoIP calls by connecting a regular phone to one of the RG230’s RJ-11 Phone ports. You can also make VoIP calls from your computer using a VoIP application with a simple microphone and computer speakers. Using either method, VoIP provides an experience identical to normal telephoning.

The RG230 allows the two RJ-11 Phone ports to be configured separately with different settings.

The VoIP configuration pages include the following options.

Menu	Description	Page
SIP Account	Shows the basic SIP account details for Phone 1 and Phone 2	7-3
Dial Plan	Sets control strings for dialed phone numbers	7-3
Call Feature	Configures call forwarding options	

SIP Account

From the VoIP SIP Account page, you can view the SIP account numbers that have been provided by the service operator.

Below data is the phone number on your device.

Phone 1 Number	1111
Phone 2 Number	2222

Figure 7-1 SIP Account Settings

Phone 1 Number – The first SIP account user number provided by the service operator.

Phone 2 Number – The second SIP account user number provided by the service operator.

Dial Plan

Dial-plan strings specify key sequences used for specific calling features (Transfer, New Call, 3-way conference), as well as defining call restriction filters.

A dial plan can filter the number and pattern of digits that a user dials to reach a particular telephone number. Access codes, area codes, specialized codes, and combinations of the number of digits dialed can all be part of a dial plan. This enables a user to predefine dialling sequences that are permitted.

The dial-plan string consists of a single digit rule. A typical example of a dial-plan string is: [0123]xxxxxx.t

Three standard dial plans are defined; Call Transfer Key, New Call Key, and 3-way Conference. Up to 10 other dial plans can be defined by the user.

A dial-plan string can be specified to control phone numbers dialed out through the gateway. A dial plan describes the number and pattern of digits that a user dials to reach a particular telephone number. Access codes, area codes, specialized codes, and combinations of the number of digits dialed can all be part of a dial plan. This enables a user to predefine dialling sequences that are permitted. It can help transfer, check, limit phone numbers, and handle prefixes to certain numbers. For more detailed description, please refer to the online help.

SNo	Action	Plan
1	Call Transfer Key	*#
2	New Call Key	##
3	3-way Conference	*3
4	Dial Plan 1	x.t
5	Dial Plan 2	
6	Dial Plan 3	
7	Dial Plan 4	
8	Dial Plan 5	

Figure 7-2 Dial Plan Settings

The function of elements allowed in a dial plan are described in the table below:

Table 7-1. Dial Plan Elements		
Element	Example	Description
x	xxxx	Represents a digit of any value (0 to 9) that can be dialed on a phone. This example has a rule with four digits of any number.
.	xx.	Indicates zero or more occurrences of the previous symbol. The example acts like a wildcard, meaning any dialed phone number of two or more digits is allowed.
0-9	01xx	Indicates dialed digits that must be matched. This example only allows four-digit numbers starting "01."

Table 7-1. Dial Plan Elements

Element	Example	Description
[]	[125-8]	Limits a dialed digit to specified values or a range of values. The example specifies that only digits 1, 2, 5, 6, 7, and 8 are permitted.
t	xx.t	The timeout indicator that can be placed after dialed digits or at the end of the dial-plan string.

When a user dials a series of digits, the dial-plan rule is tested for a possible match. If a match is made, the dialed sequence is transmitted. If no match is made, the dialed number is blocked and the user will hear an error tone.

A dial-plan string cannot include spaces between elements. Dialed sequences that are longer than specified in a dial-plan rule are truncated after the number of specified digits. For example, if the dial-plan rule is "011x" and "0115678" is dialed, only the digit sequence "0115" is transmitted.

Call Feature

The RG230 allows you to configure several call features, such as call waiting and call-forwarding. Other call features can be implemented by pressing specific phone buttons or entering dial patterns.

The table below describes the various call features available.

Note: Some call features may be dependent on support at the SIP server. Check with the SIP service provider.

Table 7-1. VoIP Call Features		
Call Feature	Description	Activation
Call Hold	Places an active call on hold for an unlimited period of time.	Press the "Flash," "Flash Hook," or "Hold" button on the phone.
Call Waiting	If during a call there is another incoming call, an alert tone is heard.	This feature must first be enabled using the web interface. You can place the active call on hold and switch to the incoming call. You can switch between the two calls by placing the active call on hold.
Call Switching	Calls two numbers, then switches between them.	Dial the first number, then place it on hold. Dial the key sequence "***" and wait until you hear the dial tone, then dial the second number. Placing the active call on hold switches to the other call. If the active call is hung up, the phone rings again to activate the other call.
Call Transfer	Transfers any received call to another number you specify.	First place the received call on hold, then dial the transfer key sequence "**#". When you hear a dial tone, enter the transfer phone number, then hang up.
Call Forward	Forwards an incoming call to another number.	This feature can be configured using the web interface. You can specify forwarding numbers for all calls, when busy, or for no answer.
3-Way Conference	Calls two numbers, then allows all to talk together.	Dial the first number, then place it on hold. Dial the key sequence "***" and wait until you hear the dial tone, then dial the second number. When the second call is active, dial "**3" to establish the three-way conference.

Call Waiting Enable Disable

Call Waiting Timeout secs

	Phone 1	Phone 2
Always Forward Phone Number	<input type="text"/>	<input type="text"/>
On Busy Forward Phone Number	<input type="text"/>	<input type="text"/>
No Answer Forward Phone Number	<input type="text"/>	<input type="text"/>
No Answer Call Forward Timeout	<input type="text" value="10"/>	<input type="text" value="10"/>

Figure 7-3 Call Features

Call Waiting – Enables a call waiting alert. If during a call there is another incoming call, an alert tone is heard. You can place the active call on hold (press the “Flash,” “Flash Hook,” or “Hold” button on the phone) and switch to the incoming call. (Default: Disabled)

Call Waiting Timeout – The time a second incoming call waits before a “no answer” message is sent. (Range: Must be less than or equal to the value of Answer Timeout; Default: 30 seconds)

Always Forward Phone Number – Another phone number to which all incoming calls are forwarded.

On Busy Forward Phone Number – Another phone number to which incoming calls are forwarded when the phone is busy.

No Answer Forward Phone Number – Another phone number to which incoming calls are forwarded when there is no answer.

Call Forward No Answer Timeout – The time a call waits for an answer before being forwarded to the No Answer Forward Phone Number. (Range: Must be less than or equal to the value of Answer Timeout; Default: 10 seconds)

Appendix A: Troubleshooting

Diagnosing LED Indicators

Symptom	Action
Power LED is Off	<ul style="list-style-type: none">• AC power adapter may be disconnected. Check connections between the unit, the AC power adapter, and the wall outlet.
Power LED is Red	<ul style="list-style-type: none">• The unit has detected a system error. Reboot the unit to try and clear the condition.• If the condition does not clear, contact your local dealer for assistance.
WiMAX Signal LEDs are Off	<ul style="list-style-type: none">• Move the location of the unit.• Check with the WiMAX service provider for service coverage information.
LAN link LED is Off	<ul style="list-style-type: none">• Verify that the unit and attached device are powered on.• Be sure the cable is plugged into both the unit and corresponding device.• Verify that the proper cable type is used and its length does not exceed specified limits.• Check the cable connections for possible defects. Replace the defective cable if necessary.

Cannot Connect to the Internet

If you cannot access the Internet from the PC, check the following:

- If you cannot access the Internet, be sure your Windows system is correctly configured for TCP/IP. The IP settings should be set to “obtain an IP address automatically.”
- You may be out of the service area of the WiMAX network. Check with the WiMAX service provider for service coverage information.
- If you cannot resolve the problem, check the System Status page of the web interface and contact your WiMAX service provider.

Cannot Access Web Management

If the management interface cannot be accessed using a web browser:

- Be sure the management station is correctly configured for TCP/IP. The IP settings should be set to “obtain an IP address automatically.”
- Try a Ping command from the management station to the unit’s IP address to verify that the entire network path between the two devices is functioning correctly.



- Check that the management station has a valid network connection and that the Ethernet port that you are using has not been disabled.
- Check the network cabling between the management station and the unit. If the problem is not resolved, try using a different port or a different cable.

Forgot or Lost the Password

Set the unit to its default configuration by pressing the reset button on the back panel for 5 seconds or more. Then use the default password “admin” to access the management interface.

Resetting the Unit

If all other recovery measures fail and the unit is still not functioning properly, take either of these steps:

- Reset the unit using the web interface, or through a power reset.
- Reset the unit to its factory default configuration by pressing the reset button on the back panel for 5 seconds or more. Then use the default password “admin” to access the management interface.

Appendix B: Specifications

Physical Specifications

Ports

4 LAN ports, 10/100BASE-TX with auto-negotiation, RJ-45 connector
(Optional) 2 FXS ports (PHONE1, PHONE2), RJ-11 connector

Network Interface

RJ-45 connector, auto MDI/X:

10BASE-T: RJ-45 (100-ohm, UTP cable; Category 3 or better)

100BASE-TX: RJ-45 (100-ohm, UTP cable; Category 5 or better)

LED Indicators

System: Power, WiMAX signal strength, WiFi

Ports: Link/Activity

AC Power Adapter

Input: 100-240 VAC, 50-60 Hz, 1.6 A

Output: 19 VDC, 3.42 A

Unit Power Supply

DC Input: 19 VDC, 1 A maximum

Power Consumption: 11 W maximum

Physical Size

169 x 184 x 80 mm (6.65 x 7.24 x 3.15 in)

Weight

1.2 kg (2.65 lbs)

Temperature

Operating: -5 to 40 °C (23 to 104 °F)

Storage: -40 to 75 °C (-40 to 167 °F)

Humidity

5% to 95% (non-condensing)

WiMAX Specifications

Antennas

Omnidirectional:

Included dual dipole antennas

Transmit: Single antenna

Receive: Two antennas using Maximal-Ratio Combining (MRC)

Gain: 5 dBi at 2.5 GHz, 4 dBi at 3.5 GHz

Impedance: 50 Ohm

Operating Frequency

ETSI: 3.4–3.6 GHz

FCC-2.3: 2305-2320 MHz, 2345-2360 MHz

FCC-2.5: 2483.5-2690 MHz

The operation methods and device behavior from 2483.5 MHz to 2500 MHz, which has only one channel at 2490 MHz and a channel bandwidth of 10 MHz for Globalstar/Open Range with Part 25 application are the same with Part 27.

No specific function or behavior is enabled while setting operating frequency to 2490 MHz.

Taiwan NCC: 2500-2690 MHz

Support for Full Scan and Partial Scan

Channel Bandwidth

5, 7, 8.75, or 10 MHz depending on model (software configurable)

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

Modulation Scheme

Scaleable OFDMA employing Time-Division Duplex (TDD) mechanism

PRBS subcarrier randomization

Contains pilot, preamble, and ranging modulation

Modulation and Coding Types

Down Link: QPSK, 16 QAM, 64 QAM

Up Link: QPSK, 16 QAM

Receive Sensitivity

-94 dBm maximum

VoIP Specifications

Voice Signaling Protocol

SIP v2 (RFC 3261)

Voice Codec

G.711 (a-law and u-law)

G.726

G.729ab

G.723.1

Voice Quality

VAD (Voice Activity Detection)

CNG (Comfortable Noise Generation)

Echo cancellation (G.165/G.168)

Adaptive jitter buffer, up to 200 milliseconds

DTMF tone detection and generation

Call Features

Call transfer

Call waiting/hold/retrieve

3-way conference call

Call blocking

T.38 fax relay

Dial plan (E.164 dialing plan)

Call forwarding: No Answer/Busy/All

REN (Ring Equivalent Number)

3 REN total in system

Compliances

Emissions

FCC CFR 47 Part 15 Class B

EN 55022 class B

EN 301 489-1/4/17

Immunity

EN 61000-4-2/3/4/5/6/8/11

WiMAX Radio Signal Certification

US: 2.3 GHz - FCC CFR 47 Part 27D; 2.5 GHz - CFR 47 Part 27M

US: 2.5 GHz - CFR 47 Part 25.254 for ATC frequency band

Europe (3.5 GHz): EN 302 326-2 (V1.2.2), EN 302 326-3 (V1.2.2)

Wi-Fi Radio Signal Certification

FCC CFR 47 Part 15 Subpart C

EN 300 328

Safety

cTUVus + TUV/SUD

Standards

IEEE 802.16e-2005 WAVE 1 and WAVE 2

IEEE 802.3-2005 10BASE-T and 100BASE-TX

IEEE 802.11b and 802.11g

UPnP

Appendix C: Cables and Pinouts

Twisted-Pair Cable Assignments

For 10/100BASE-TX connections, a twisted-pair cable must have two pairs of wires. Each wire pair is identified by two different colors. For example, one wire might be green and the other, green with white stripes. Also, an RJ-45 connector must be attached to both ends of the cable.

Caution: Each wire pair must be attached to the RJ-45 connectors in a specific orientation. (See “Straight-Through Wiring” on page C-2 and “Crossover Wiring” on page C-2 for an explanation.)

Caution: DO NOT plug a phone jack connector into the RJ-45 port. Use only twisted-pair cables with RJ-45 connectors that conform with FCC standards.

The following figure illustrates how the pins on the RJ-45 connector are numbered. Be sure to hold the connectors in the same orientation when attaching the wires to the pins.

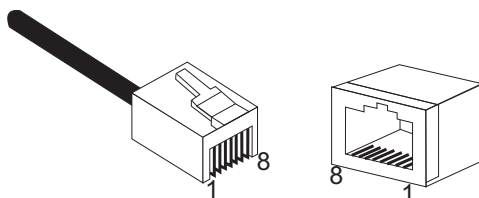


Figure C-1 RJ-45 Connector

10/100BASE-TX Pin Assignments

Use unshielded twisted-pair (UTP) or shielded twisted-pair (STP) cable for RJ-45 connections: 100-ohm Category 3 or better cable for 10 Mbps connections, or 100-ohm Category 5 or better cable for 100 Mbps connections. Also be sure that the length of any twisted-pair connection does not exceed 100 meters (328 feet).

The RJ-45 ports on the unit supports automatic MDI/MDI-X operation, so you can use straight-through or crossover cables for all network connections to PCs, switches, or hubs. In straight-through cable, pins 1, 2, 3, and 6, at one end of the cable, are connected straight through to pins 1, 2, 3, and 6 at the other end of the cable.

Table C-1. 10/100BASE-TX MDI and MDI-X Port Pinouts		
Pin	MDI-X Signal Name	MDI Signal Name
1	Receive Data plus (RD+)	Transmit Data plus (TD+)
2	Receive Data minus (RD-)	Transmit Data minus (TD-)
3	Transmit Data plus (TD+)	Receive Data plus (RD+)
6	Transmit Data minus (TD-)	Receive Data minus (RD-)
4,5,7,8	Not used	Not used

Note: The "+" and "-" signs represent the polarity of the wires that make up each wire pair.

Straight-Through Wiring

If the twisted-pair cable is to join two ports and only one of the ports has an internal crossover (MDI-X), the two pairs of wires must be straight-through.

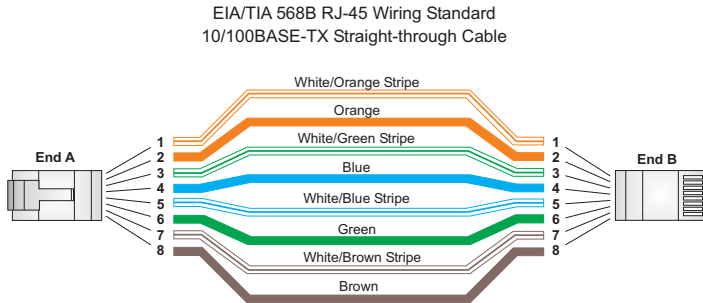


Figure C-2 Straight-Through Wiring

Crossover Wiring

If the twisted-pair cable is to join two ports and either both ports are labeled with an "X" (MDI-X) or neither port is labeled with an "X" (MDI), a crossover must be implemented in the wiring.

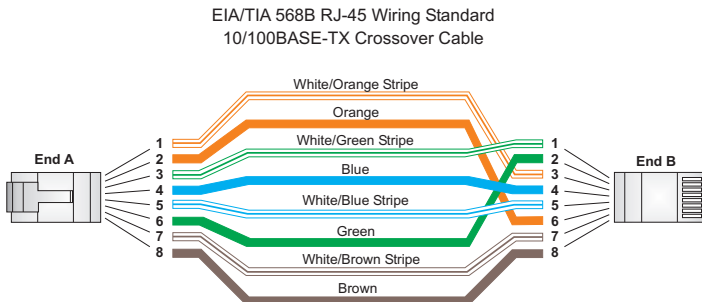


Figure C-3 Crossover Wiring

RJ-11 Ports

Standard telephone RJ-11 connectors and cabling can be found in several common wiring patterns. These six-pin connectors can accommodate up to three wire pairs (three telephone lines), but usually only one or two pairs of conductor pins and wires are implemented.

The RJ-11 ports on this device contain only one wire pair on the inner pins (3 and 4).

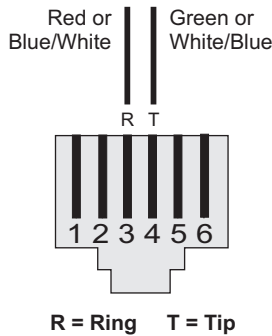


Figure C-4 RJ-11 Port Pinout

Pin	Signal Name	Wire Color
1	<i>Not used</i>	
2	<i>Not used</i>	
3	Line 1 Ring	Red or Blue/White
4	Line 1 Tip	Green or White/Blue
5	<i>Not used</i>	
6	<i>Not used</i>	

Appendix D: License Information

This product includes copyrighted third-party software subject to the terms of the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other related free software licences. The GPL code used in this product is distributed WITHOUT ANY WARRANTY and is subject to the copyrights of one or more authors. For details, refer to the section “The GNU General Public License” below, or refer to the applicable licence as included in the source-code archive.

The GNU General Public License

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

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

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software—to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation’s software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

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

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

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

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

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

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

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

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

- a). You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
- b). You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
- c). If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:
 - a). Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
 - b). Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

- c). Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.
6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.
7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a

consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

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

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Glossary

10BASE-T

IEEE 802.3-2005 specification for 10 Mbps Ethernet over two pairs of Category 3 or better UTP cable.

100BASE-TX

IEEE 802.3-2005 specification for 100 Mbps Fast Ethernet over two pairs of Category 5 or better UTP cable.

Access Point

An Wi-Fi internetworking device that seamlessly connects wired and wireless networks.

Authentication

The process to verify the identity of a client requesting network access.

Auto-Negotiation

Signalling method allowing each node to select its optimum operational mode (speed and duplex mode) based on the capabilities of the node to which it is connected.

Base Station

A WiMAX service provider's equipment that is installed at a fixed location to provide network connectivity for subscriber stations within a defined service area.

Beacon

A signal periodically transmitted from a Wi-Fi access point that is used to identify the network and maintain contact with wireless clients.

Carrier-to-Interference-Plus-Noise Ratio (CINR)

A measurement of the channel quality in a WiMAX link. Subscriber stations measure the received CINR and send the information back to the base station. The base station can then adjust modulation and coding for the link to optimize throughput.

Center Frequency

The radio frequency at the center of a WiMAX channel. WiMAX channels can be of different widths (the channel bandwidth) and the transmitted radio signal is spread across the full width of the channel.

Channel Bandwidth

The range of frequencies occupied by a WiMAX radio signal. The amount of information that can be transmitted in a radio signal is related to the channel

bandwidth, which is measured in Megahertz (MHz). WiMAX supports a range of channel bandwidths that can be defined by the service operator depending on performance requirements, operating preferences, and regulatory constraints.

CPE (Customer-Premises Equipment)

Terminal equipment provided by a service provider that is located at a subscriber's premises and supports a communication channel between a customer and the service provider.

Domain Name System (DNS)

A system used for translating host names for network nodes into IP addresses.

Dynamic Host Configuration Protocol (DHCP)

Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

Encryption

Data passing between a base station and subscribers uses encryption to protect from interception and eavesdropping.

Ethernet

A popular local area data communications network, which accepts transmission from computers and terminals.

Extensible Authentication Protocol (EAP)

An authentication protocol used to authenticate subscribers. EAP is used with TLS or TTLS authentication to provide "mutual authentication" between a subscriber and a WiMAX network.

Hypertext Transfer Protocol (HTTP)

HTTP is a standard used to transmit and receive all data over the World Wide Web.

IEEE 802.11b

The Wi-Fi wireless standard that supports communications in the 2.4 GHz band using Direct Sequence Spread Spectrum (DSSS). The standard provides for data rates of 1, 2, 5.5, and 11 Mbps.

IEEE 802.11g

The Wi-Fi wireless standard that supports communications in the 2.4 GHz band using Orthogonal Frequency Division Multiplexing (OFDM). The standard provides for data rates of 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps. IEEE 802.11g is also backward compatible with IEEE 802.11b.

IEEE 802.16e

The WiMAX standard that provides mobile broadband wireless access using Scalable Orthogonal Frequency Division Multiple Access (SOFDMA).

IEEE 802.1X

Port Authentication controls access to the switch ports by requiring users to first enter a user ID and password for authentication.

Internet Service Provider

A company that offers an access service that connects customers to the Internet.

IP Address

The Internet Protocol (IP) address is a numerical identification assigned to a device that communicates in a network using the Internet Protocol.

LED

Light emitting diode, used for indicating a device or network condition.

Local Area Network (LAN)

A group of interconnected computer and support devices.

MAC Address

The physical layer address used to uniquely identify network nodes.

MS-CHAPV2

Microsoft's version 2 of the Challenge-Handshake Authentication Protocol. Introduced by Microsoft with Windows 2000, MS-CHAPV2 (defined in RFC 2759) provides mutual authentication between peers using user names and passwords.

Orthogonal Frequency Division Multiplexing (OFDM)

The air interface defined for IEEE 802.11g Wi-Fi. OFDM allows multiple users to transmit in an allocated band by dividing the bandwidth into many narrow bandwidth carriers.

RADIUS

Remote Authentication Dial-in User Service. A logon authentication protocol that uses software running on a central server to control access to a network.

RJ-45 Connector

A connector for twisted-pair wiring.

Receive Signal Strength Indicator (RSSI)

A measurement of the strength of a received wireless signal. The higher the RSSI value, the stronger the received signal from the antenna.

Roaming

The process where a WiMAX subscriber can move onto another operator's network while maintaining a continuous connection.

Scalable Orthogonal Frequency Division Multiple Access (SOFDMA)

The air interface defined for mobile WiMAX. SOFDMA is a multiple access method that allows simultaneous transmissions to and from several users, employing a subchannel structure that scales with bandwidth.

Service Provider

See *Internet Service Provider*.

Service Set Identifier (SSID)

A name that is sent in packets over a Wi-Fi network, which functions as a password for clients connecting to the network. The SSID differentiates one Wi-Fi network from another.

Simple Network Time Protocol (SNTP)

SNTP allows a device to set its internal clock based on periodic updates from a Network Time Protocol (NTP) server. Updates can be requested from a specific NTP server, or can be received via broadcasts sent by NTP servers.

Subscriber Identity Module (SIM)

A standard for a small removable integrated circuit card that securely stores information used to identify a mobile wireless subscriber.

Subscriber Station

A general term for a customer's WiMAX terminal equipment that provides connectivity with a base station.

Transmission Control Protocol/Internet Protocol (TCP/IP)

Protocol suite that includes TCP as the primary transport protocol, and IP as the network layer protocol.

Transport Layer Security (TLS)

An standard defined in RFC 5216, EAP-TLS is an authentication protocol that provides strong security through the use of client-side certificates.

Tunneled Transport Layer Security (TTLS)

EAP-TTLS is a protocol extension of EAP-TLS. The authentication server is authenticated to the client using its Certification Authority certificate, this establishes a secure “tunnel” through which the client is then authenticated.

URL (Uniform Resource Locator)

An easy-to-read character string that is used to represent a resource available on the Internet. For example, “http://www.url-example.com/.”

UTP

Unshielded twisted-pair cable.

Wi-Fi Protected Access

WPA employs IEEE 802.1X as its basic framework for user authentication and dynamic key management to provide an enhanced security solution for 802.11 Wi-Fi networks.

Wired Equivalent Privacy (WEP)

WEP is the Wi-Fi security based on the use of RC4 encryption keys. Wi-Fi devices without a valid WEP key are excluded from the network.

WPA Pre-shared Key (PSK)

PSK security can be used for small Wi-Fi networks that may not have the resources to configure and maintain a RADIUS server. WPA provides a simple operating mode that uses just a pre-shared password for network access.

WiMAX

The IEEE 802.16 standard for Worldwide Interoperability for Microwave Access. The IEEE 802.16-2004 standard, known as “fixed WiMAX,” supports only point-to-point links and has no support for mobility. The IEEE 802.16e-2005 standard, known as “mobile WiMAX,” is an amendment to IEEE 802.16-2004 and supports mobility. Note that mobile WiMAX standard is not backward compatible with the fixed WiMAX standard.

Index

A

AC power adapter 1-5
administrator password, setting 4-4
administrator settings 4-4
Advanced Setup menu 3-5
antennas 1-3
auto-logout time 4-4

B

button, Reset 1-5

C

cable assignments C-1
cable connections 2-2
checklist 2-1
client filter, enable 5-8
configuration, basic 3-3
contents, package 2-1

D

default settings, restore 4-5
defaults, factory 4-5
DHCP server 5-2
discard ping 5-7
DMZ host 5-5
downloading software 4-4

E

Ethernet ports 1-5

F

factory defaults, restoring 4-5
firewall protection 5-6
firmware update 4-4

G

Gateway address 5-10
gateway function 2-2

GPL information D-1

H

hacker attack, prevention 5-6, 5-7
hardware, description 1-2

I

installation, connecting cables 2-2
Internet connection, block 5-9
Internet gateway settings 5-1
IP address 5-2
IP filters 5-8

L

LAN status information 4-2
LEDs 1-3, 1-4, 1-5
license information D-1
login, web 3-1
lost password, recovery A-2

M

MAC address filters 5-9
mapping ports, NAT 5-5
MDI/MDI-X, automatic 1-5

O

operating frequency B-2

P

package checklist 2-1
panels, front and rear 1-2
password, setting 4-4
ping discard 5-7
pinouts C-1
port indicators 1-3, 1-4, 1-5
port mapping, NAT 5-5
port scan prevention 5-7
power socket 1-5
power supply, specifications B-1

private IP 5-4
private port 5-4
public port 5-4

R

rear panel sockets 1-5
reboot unit 4-7, A-2
Reset button 1-5
resetting the unit 4-7, A-2
RJ-45 ports 1-5
runtime code version 4-3

S

Setup Wizard
 launching 3-3
Simple Network Time Protocol *See*
 SNTP
SNTP 4-5
 enabling client 4-6
software update 4-4
status information 4-2
subnet mask 5-2, 5-10
subscriber station 1-1

system clock, setting 4-6
system indicators 1-3, 1-4
system information 4-3
system status 4-2
system time 4-5

T

time updates 4-5
troubleshooting A-1

U

upgrading software 4-4
UPnP 5-11

W

WAN connection type 4-2
web management interface
 access 3-1
 login 3-1
 troubleshooting A-1
WiMAX connection status 6-1
Wizard, setup 3-3

RG230
E072009-CS-R02
149100001700W