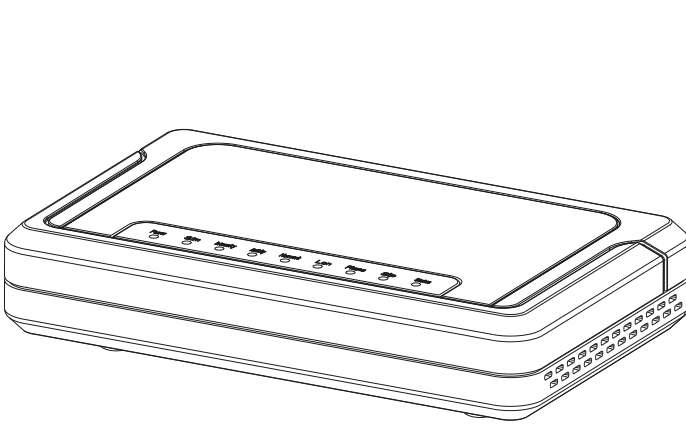


ENGLISH

WiMAX VoIP Indoor Gateway

User Manual



Copyright © 2008 All Rights Reserved.

<the company> designs are trademarks of <the company>. All <the company> product names are trademarks of <the company>. Other product and company names mentioned in this document may be the trademarks or registered trademarks of their respective holders.

<the company> reserves the right to make changes to its products, manufacturing methods or circumstances without notice.

Important Safety Notices

Safety Information

1. Read this user manual and follow all operating and safety instructions.
2. Keep all product information for future reference.
3. The power requirements are indicated on the product-marking label. Do not exceed the described limits.
4. Use only a damp cloth for cleaning. Do not use liquid or aerosol cleaners. Disconnect the power before cleaning.
5. Disconnect power when unit is stored for long periods.


Important Warning Symbols

The following symbols may be encountered during installation or troubleshooting.


These warning symbols mean danger. Bodily injury may result if users are not aware of the safety hazards involved in working with electrical equipment and radio transmitters. Users should be familiar with standard safety practices before continuing.

Note:

The following NOTE symbol is placed after material to offer suggestions or comments for ease of use. See the Note as follows.


	NOTE: Useful information and tips on the Gateway and networking.
---	---

Warning:

	WARNING: Important information appears before the text it references and should not be ignored as the content may prevent damage to the machine.
---	---

The preceding WARNING is placed before an item of importance that requires attention to prevent damage to equipment or loss of data.

Caution:

	CAUTION: TO REDUCE THE RISK OF ELECTRIC SHOCK, ONLY QUALIFIED SERVICE PERSONNEL SHOULD SERVICE THIS EQUIPMENT.
---	---

The preceding CAUTION symbol is placed before material that requires attention to prevent personal injury or even death.

Conformance Documents

R&TTE Directive 1999/5/EC - Declarations of conformity are available at the following web site address: <http://www.rtte.net/Directive.htm>

Federal Communication Commission Interference Statement

FCC Part 15 Description

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.

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.

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.

RF Exposure statement for mobile device without SAR measurement

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 20cm between the radiator & your body.

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

R&TTE Directive 1999/5/EC Statements

Installation

The transceiver and antenna equipment must be installed by a qualified professional installer and must be installed in compliance with regional, national, and local regulations. It is the responsibility of the system installer and/or system operator to ensure the installed system does not exceed any operational constraints identified by local regulations. Refer to the sections in this product User Guide for detailed information about the correct installation steps to ensure power and frequency settings are set correctly before connecting the antenna.

National Interface documents may identify, among other parameters, a maximum output power for the system, expressed in terms of an EIRP level that must not be exceeded. Any use of a combination of output power and antenna resulting in an EIRP level above the national limit may be considered illegal and is outside the scope of the R&TTE Directive 1999/5/EC compliance declaration.

WEEE Product Return Process



In accordance with the WEEE (Waste from Electrical and Electronic Equipment) directive, 2002/96/EC, this equipment is marked with the logo shown. The WEEE directive seeks to increase recycling and re-use of electrical and electronic equipment. This symbol indicates that this product should not be disposed of as part of the local municipal waste program.

Important Service Information

1. Refer all repairs to qualified service personnel. Do not remove the covers or modify any part of this device, as this voids the warranty.
2. Disconnect the power to this product and return it for service if the following conditions apply:
 - The unit does not function after following the operating instructions outlined in this manual.
 - The product has been dropped or the housing is damaged.
3. Record the Gateway serial numbers for future reference.

Version 0.0.0, October 2008

This page left blank intentionally.

Table of Contents

Important Safety Notices	i
Safety Information	i
Important Warning Symbols	ii
Conformance Documents	ii
Federal Communication Commission Interference Statement	iii
R&TTE Directive 1999/5/EC Statements	iv
WEEE Product Return Process	iv
Important Service Information	v
1 Product Overview	1
1.1 Introduction	1
1.2 Main Features	2
1.3 Front View	3
1.3.1 LED Status Activity	4
1.4 Rear View	5
2 Basic Installation	7
2.1 Safety Measures	7
2.2 System Requirements	7
2.3 Unpacking the Gateway	8
2.4 Hardware Installation	9
2.4.1 Choose a Location	10
2.4.2 Attaching the Antennas	11
2.4.3 Connecting the Ethernet Cable	12
2.4.4 Connecting the Phone Cable	13
2.4.5 Powering on the Unit	14
2.4.6 Locating the Strongest WiMAX Signal	15

3 Features and Web GUI Configuration	17
3.1 Logging In	18
3.2 Using the System Page	20
3.2.1 LAN Settings	20
3.2.2 NTP Settings	22
3.2.3 VLAN Tagging	23
3.2.4 Corrigenda	24
3.3 Using the Band Page	25
3.3.1 Band Settings	25
3.3.2 FFT Settings	26
3.4 Using the Security Page	27
3.4.1 Changing Login Details	27
3.4.2 PKM Settings	28
3.4.3 SNMP Settings	29
3.5 Using the VoIP Page	30
3.5.1 Network Settings	30
3.5.2 SIP Settings	31
3.5.3 Call Control	33
3.6 Using the Status Page	35
3.6.1 System Status	35
3.6.2 LAN Status	36
3.6.3 Forwarding Status	37
3.6.4 Connection Status	38
3.6.5 VoIP Status	39
3.7 Using the Tools Page	40
3.7.1 Upgrading the Firmware	40
3.7.2 Restoring Factory Defaults	42
3.7.3 Rebooting the Gateway	43
4 Troubleshooting	45
4.1 Common Issues	46
Glossary	49
Index	53

Product Overview

1.1 Introduction

This series of Indoor desktop WiMAX VoIP Gateways feature a compact design easy to install by end users, without any professional techniques or previous networking deployment experience, and voice capability providing an RJ-11 port for existing land line connections offering global users a cost efficient platform for concurrent high speed data connectivity and VoIP calls.

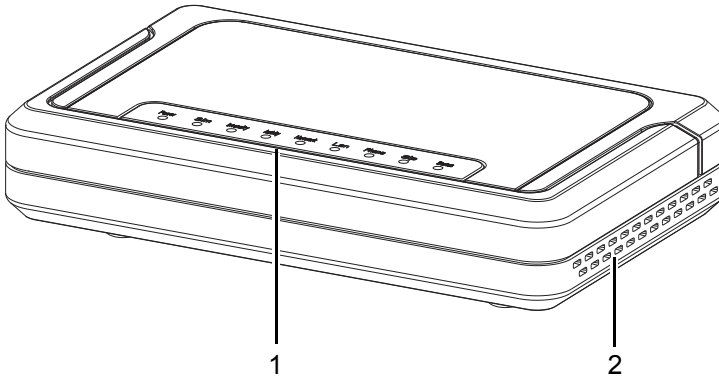
Featuring IEEE 802.16-2005 (802.16e) WiMAX compliant technology, this Gateway supports MIMO (1X2) technology delivering optimized throughput and a least cost solution for WiMAX network connectivity. Advanced security and authentication protocols, such as PKMv2, X.509, EAP-TLS/TTLS and AES are integrated to provide the utmost security while enjoying high-speed internet connectivity.

In addition, the LED signal strength indicator allows users to identify the location with the best signal quality suitable for installation.

1.2 Main Features

- IEEE 802.16e-2005 compliance
- Operating Frequency 2.5GHz
- OFDMA modulation, 512 1024 FFT points QPSK, 16QAM, 64QAM
- Security support for 3DES, AES(CCMP), EAP-TLS/EAP-TTLS, PKMv2 and X.509
- One Ethernet port/RJ-45
- One VoIP/RJ-11 port
- Output power: 25.5dBm typical
- LED signal indicators
- MIMO 1Tx/2Rx support
- Ease of use web interface for management and configuration

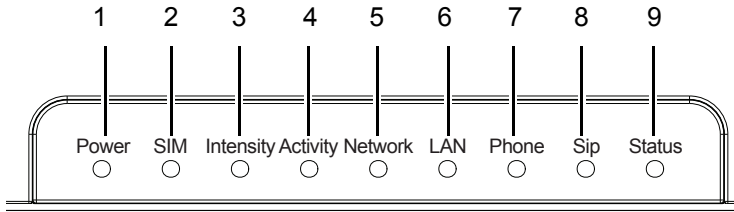
1.3 Front View



Label	Item	Description
1.	LED Panel	Nine LED describe system status. See <i>LED Status Activity</i> on page 4.
2.	Vent	Air vents keep the device cool even after prolonged use

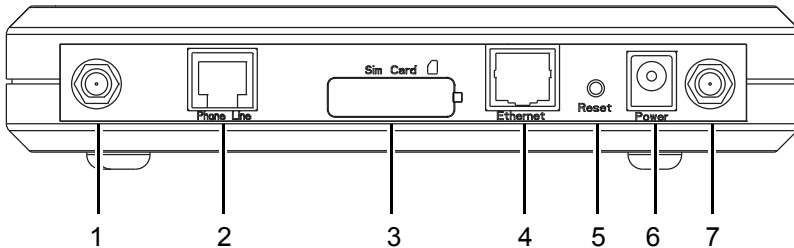
1.3.1 LED Status Activity

There are a total of 9 LEDs. A description of their function is listed as follows:



Label	Function	Status
1.	Power	Lights when Gateway is powered on
2.	SIM	Lights when a SIM card is inserted
3.	Intensity	Indicates signal strength by color:
	Green	Excellent Signal
	Green/Orange flashing	Good Signal
	Orange	Average Signal
	Orange/Red flashing	Poor Signal
	Red	No Signal
4.	Activity	Lights when WiMAX activity is detected
5.	Network	Lights when network activity is detected
6.	LAN	Lights when ethernet port is connected
7.	Phone	Lights when the phone line is in use
8.	SIP	Lights when SIP is registered
9.	Status	Shows phone line status

1.4 Rear View



Label	Item	Description
1.	Antenna	Connect the supplied antenna to this port
2.	RJ-11 Port	Connect to a standard telephony port for VoIP
3.	SIM Card	Connect a SIM card to this card reader
4.	RJ-45 Port	Connect to a standard ethernet port
5.	Reset Button	Press to reset the Gateway to factory defaults
6.	Power Jack	Connect the supplied power supply to this port
7.	Antenna	Connect the supplied antenna to this port

This page left blank intentionally.

Basic Installation

This chapter contains information on safety and installation procedures for the Gateway. Follow the recommendations outlined in this chapter to ensure the correct operation of the Gateway and reduce the risk of damage to the device or personal injury.

2.1 Safety Measures

Before installing and using the Gateway, take note of the following precautions:

- Read all instructions carefully
- Use only the power adapter supplied
- Follow all warnings and cautions in this manual and on the unit case

2.2 System Requirements

Proper installation of the Gateway requires the following minimal configuration:

- A PC with an Ethernet (10/100Base-TX) port
- A Web browser installed such as Microsoft Internet Explorer® version 6.0, Firefox® version 2.0, or Safari® version 3.0.3.

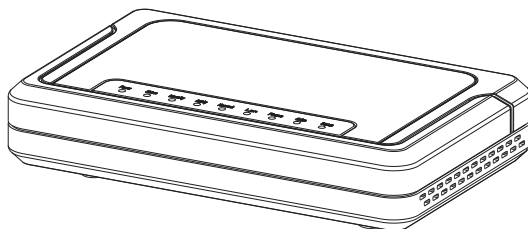


NOTE: The browser versions listed are the minimum requirement. Later versions of the software are also acceptable.

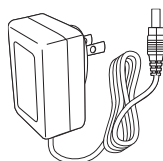
2.3 Unpacking the Gateway

1. Unpack the Gateway and make sure you have all the pieces shown below.

Materials List



Gateway



Power Adapter



Quick Installation Guide



CD Containing User Manual



NOTE: Please check that all the listed items are present and in good condition. If there is anything missing or damaged, contact the dealer immediately.

2. Write down the MAC address and serial number of the Gateway—this information is used during Gateway configuration.

2.4 Hardware Installation

This section describes the proper steps required to install the Gateway, and to align the antenna.



WARNING: Before installing and using this product, see *Important Safety Notices* on page *i* of this manual.

The proper installation procedure for the Gateway is as follows:

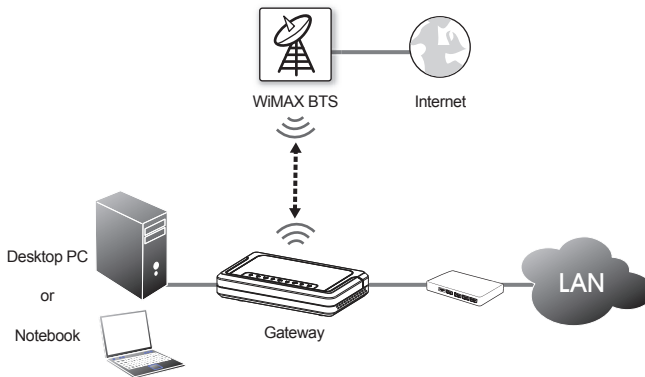
1. Choose a Location
2. Attach the Antennas
3. Connect the Ethernet Cable
4. Connect the Power Adapter
5. Check the Intensity LED lights green, indicating good signal quality



NOTE: If the Intensity LED does not light green, choose a different location and repeat the process.

2.4.1 Choose a Location

To achieve the best results when connecting the Gateway to the LAN or a single computer it is recommended that you follow these guidelines when choosing a location:



- Place the Gateway where the signal is strongest, usually close to an external window. *Locating the Strongest WiMAX Signal* on page 15
- Do not place the Gateway on the floor or near metal objects (such as file cabinets)
- Make sure you can easily disconnect power to the Gateway if necessary
- Make sure there is airflow around the Gateway
- Do not expose the Gateway to vibration or excessive heat
- The Gateway installation must obey local regulations at all times

2.4.2 Attaching the Antennas

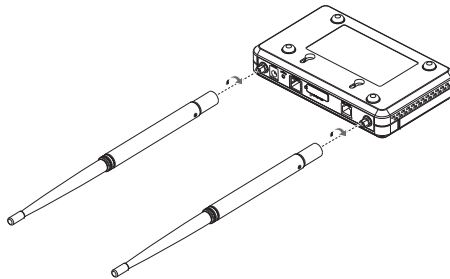
To attach the two antennas:

1. Turn off your computer and turn off or unplug any attached network devices.
2. Write down the Ethernet and MAC addresses of the Gateway, as well as the serial number; the information is used for configuring the unit.

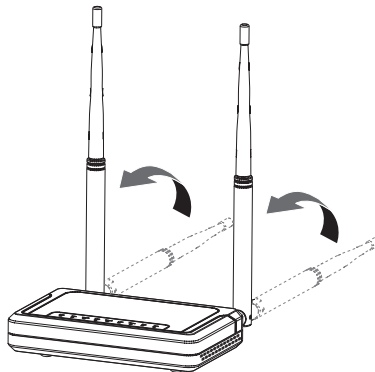


NOTE: The serial number is required to obtain support from the vendor. Maintain this information in a safe place for future reference. You can find your serial number on the bottom label of the Gateway and on the side of the package. If you ever need to technical assistance, you will need this number.

3. Connect the two antennas as shown in the following image. Hand-tighten the antennas until they are secure.



4. Once connected, adjust the antennas to the upright position as shown.

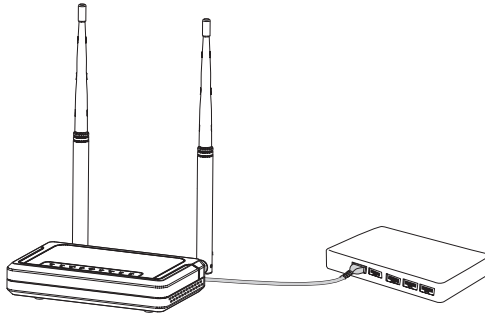


2.4.3 Connecting the Ethernet Cable

Connect to the LAN by attaching an Ethernet cable (RJ-45) from the Gateway to a network switch or from the Gateway directly to the destination computer.

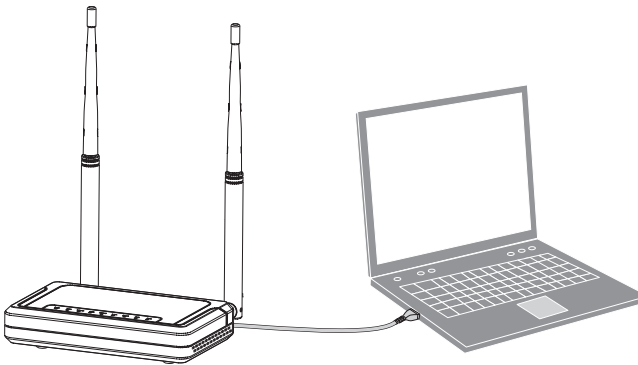
To connect the Gateway to a router or switch:

Connect an Ethernet cable from the Gateway to the router or switch, as shown below.



To connect the Gateway directly to a computer:

Connect an Ethernet cable from the Gateway to the computer as shown below.

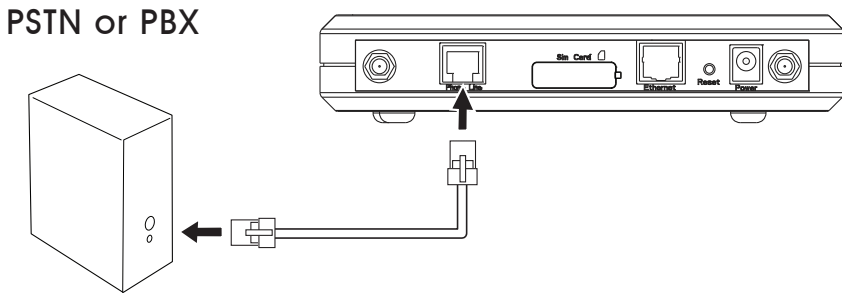


2.4.4 Connecting the Phone Cable

Connect to a PSTN by attaching a standard telephony cable (RJ-11) from the Gateway to a PSTN or PBX.

To connect the phone port:

Connect an RJ-11 cable from the Gateway to the PSTN switch as shown below.



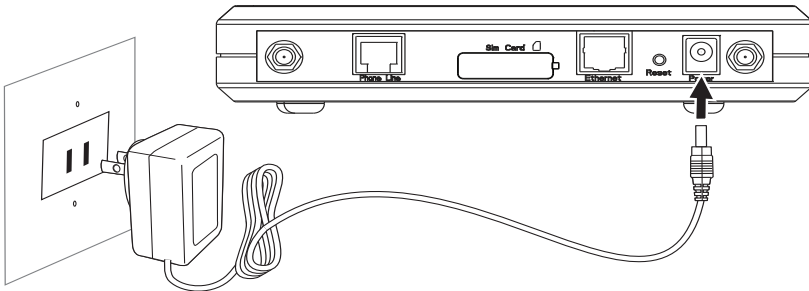
2.4.5 Powering on the Unit

After making the necessary cable connections, attach the power cable as follows:



CAUTION: ONLY USE THE SUPPLIED DC ADAPTER TO PREVENT DAMAGE OR PERSONAL INJURY.

1. Plug the power adaptor in to the rear DC port of the Gateway.
2. Connect the power cable on the adaptor to a standard electrical outlet.



3. Turn on your network devices and PC.

There is no on/off switch on the Gateway. Once the power adapter is connected, the Gateway is operational.

A diagnostic sequence occurs in which the Gateway LEDs blink for a few seconds. The Gateway is ready for use when the LEDs stop flashing.

2.4.6 Locating the Strongest WiMAX Signal

Positioning the Gateway correctly is essential for establishing the best possible link. The antenna locating process is usually performed during installation and prior to affixing the Gateway to a permanent location.

The Intensity LED displays the strength of the WiMAX signal. The following table provides a description of the color indication:

Color	Status
Red	No signal
Orange + Red	Bad
Orange	Normal
Green + Orange	Good
Green	Excellent

To achieve the strongest possible signal reception, perform the following steps:

1. Using the Intensity LED to find the optimal signal strength, locate the Gateway as described in *Choose a Location* on page 10.
2. Physically move the Gateway around in the area chosen to locate the greatest signal strength.



NOTE: Before positioning the Gateway, ensure that the Intensity LED shows normal signal strength (orange) or better.

Installation of the Gateway is now complete. Read the following chapters to begin configuration through the web based interface.

This page left blank intentionally.

Features and Web GUI Configuration

This chapter contains information on the Web-based Graphical User Interface (GUI). The Gateway's GUI enables quick and simple setup, and the configuration of the following options:

- Connection of the Gateway to WiMAX base transceiver stations (BTS)
- Network setting changes, such as internal IP address, IP address pool, DHCP settings, and more
- Configure VoIP settings
- Internal password change
- Default settings reset
- Firmware updates

3.1 Logging In

To log in to the GUI, perform the following steps:

1. Ensure the installation described in Chapter 2 is complete. Check that the Gateway has power and that the signal strength is good.
2. Launch an Internet browser on the administrator's PC.



NOTE: Ensure that an up-to-date browser is installed to correctly display the GUI. Safari® users must install v3.0.3 or later to guarantee functionality.

3. Enter the default IP address **192.168.0.10** in the browser address field and press **Enter**.

The login screen appears.



4. Input the default user name and password and press **Enter**.

Username: **admin**

Password: **admin**

The Gateway configuration homepage appears.

The screenshot shows the Gateway configuration homepage. It features a navigation bar at the top with links for System, Band, Security, VoIP, Status, Tools, and Logout. A 'Sections' sidebar on the left lists LAN, NTP, VLAN Tagging, and Corrigenda. The main content area is divided into two sections: 'LAN' and 'DHCP Server'. The LAN section includes fields for IP Address (192.168.0.10), Subnet Mask (255.255.255.0), and Default Gateway (192.168.0.1). The DHCP Server section includes options for enabling/disabling the server, starting IP address (192.168.0.100), number of users (100), and client lease period (0 minutes). At the bottom, there are 'Save Settings' and 'Cancel Changes' buttons. Numbered callouts 1 through 5 point to the Sections sidebar, the LAN description, the IP address field, the Default Gateway field, and the Save/Cancel buttons respectively.

The Web configuration homepage shows:

No.	Item	Description
1.	Navigation Bar	Select the desired submenu.
2.	Menu Bar	Select the desired main menu.
3.	Description Panel	A brief description of the current menu and settings.
4.	Settings Panel	Enter or modify configuration settings.
5.	Action Buttons	Perform context sensitive actions.



NOTE: Only one administrator at a time can log into the Gateway to make changes to settings.

3.2 Using the System Page

The System page is used to configure Gateway basic settings such as the Gateway's LAN address, DHCP settings, Gateway time and date synchronization, and available managed VLAN devices.

3.2.1 LAN Settings

LAN Settings is the default GUI page after logon. The default IP address, subnet mask, default gateway, and DHCP/DNS settings are displayed in the LAN Settings page.



NOTE: Making changes to the default IP address may cause GUI connection problems.

Firmware Version : 1.08.06

[System](#) » [Band](#) » [Security](#) » [VoIP](#) » [Status](#) » [Tools](#) » [Logout](#)

Sections

- LAN
- NTP
- VLAN Tagging
- Corrigenda

The IP address, subnet mask, and default gateway settings that are configured here are used to manage the Subscriber Station through the web interface.

The default IP address of the Subscriber Station is 192.168.0.10, if you change the IP address of the Subscriber Station, you may need to adjust your PCs network settings in order to access the web-management again.

IP Address : . . .

Subnet Mask : . . .

Default Gateway : . . .

DHCP Server : Enable Disable

Starting IP Address : . . .

Number of DHCP Users : 192.168.0.100 – 192.168.0.199

Client Lease Period : Minutes, 0 as one day.

DNS 1 : . . .

DNS 2 : . . .

DNS 3 : . . .

WINS : . . .

Save Settings | Cancel Changes

Copyright © 2006. All rights reserved.

To make changes to the default settings, perform the following steps:

1. Make any desired modifications to the IP, subnet mask, and default gateway fields.
2. Click **Save Settings**.

DHCP SERVER SETTINGS

Disabled by default, Dynamic Host Configuration Protocol (DHCP) assigns reusable IP addresses to DHCP client devices connected to the LAN. Enable or Disable DHCP by selecting the appropriate button.



NOTE: If the Gateway DHCP function is enabled and a DHCP server is already present on the LAN, either disable the DHCP function on the Gateway or DHCP server, or ensure that the available IP Pools do not overlap. If both the Gateway and the existing DHCP server are active, both devices may fail to provide services to the network.

To configure DHCP, enter the following information:

1. Starting IP Address—enter the starting range of IP addresses available for distribution. The default value is 192.168.9.100.
2. Number of DHCP Users—enter the maximum number of available IP addresses for distribution. The default value is 100.

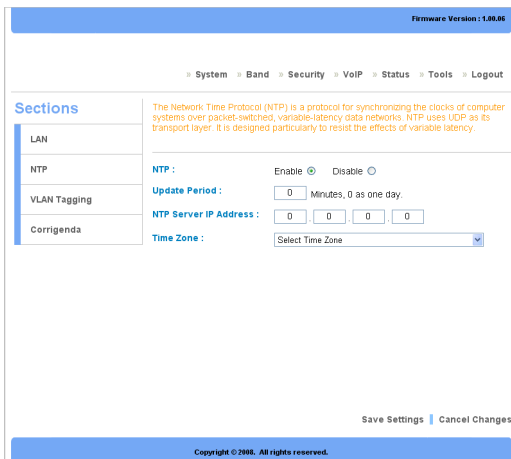


NOTE: The full range displays to the right of the field, 192.168.0.100 - 192.168.0.199 in the example.

3. Client Lease Period—enter the length of time (minutes) that the DHCP server reserves IP addresses before recycling them. The default period is one day, represented by 0.
4. DNS 1 to 3—enter Domain Name System (DNS) information in the supplied fields. The ISP may supply this information.
5. WINS—enter Windows Internet Name Service (WINS) information in the supplied field. The ISP may supply this information.
6. Click **Save Settings**.

3.2.2 NTP Settings

Network Time Protocol (NTP) is used to synchronize the Gateway date and time with a third party NTP server. Synchronization is automatic, updating at specific time intervals. NTP is disabled by default.



Firmware Version : 1.00.06

System » Band » Security » VoIP » Status » Tools » Logout

Sections

- LAN
- NTP**
- VLAN Tagging
- Corrigenda

The Network Time Protocol (NTP) is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. NTP uses UDP as its transport layer. It is designed particularly to resist the effects of variable latency.

NTP : Enable Disable

Update Period : Minutes, 0 as one day

NTP Server IP Address :

Time Zone :

Save Settings | Cancel Changes

Copyright © 2008. All rights reserved.

To configure NTP, perform the following steps:

1. Select **Enable** to access the configuration fields.
2. Enter a synchronization update period in minutes, or enter 0 to synchronize once every 24 hours.
3. Enter an NTP Server IP Address in the fields provided. Many third party NTP service providers are available. Contact the ISP for more details.
4. Select the current time zone from the drop down menu.
5. Click **Save Settings**.

3.2.3 VLAN Tagging

Virtual LAN (VLAN) describes a group of devices on one or more LANs that are configured (using management software) to communicate as if they were located on the same network segment, regardless of their actual network location. VLAN Tagging is disabled by default.

Virtual LAN (VLAN) is a group of devices on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same network segment, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

VLAN : Enable Disable

VLAN ID : (0 ~ 4095)

Save Settings | Cancel Changes

Copyright © 2006. All rights reserved.

To configure VLAN, perform the following steps:

1. Select **Enable** to access the configuration fields.
2. Enter a unique **VLAN ID** in the field provided.
3. Click **Save Settings**.

3.2.4 Corrigenda

The Corrigenda page is used to specify which version of gateway control protocol Corrigenda to use. Currently, only Corrigenda versions Cor.1 and Cor.2 are supported—this Gateway is set to Cor.2 as default.

Contact the ISP for more information.

The screenshot shows a web GUI configuration page for Corrigenda. At the top right, it displays "Firmware Version: 1.00.06". Below this is a breadcrumb navigation menu: "System > Band > Security > VoIP > Status > Tools > Logout". On the left side, there is a "Sections" menu with options: LAN, NTP, VLAN Tagging, and Corrigenda. The main content area shows a warning message: "Switch to support Corrigendum Version 1 or 2." Below the warning, the "Corrigenda:" label is followed by two radio buttons: "Cor.1" (unselected) and "Cor.2" (selected). At the bottom right of the main area, there are two buttons: "Save Settings" and "Cancel Changes". The footer of the page contains the text "Copyright © 2008. All rights reserved."

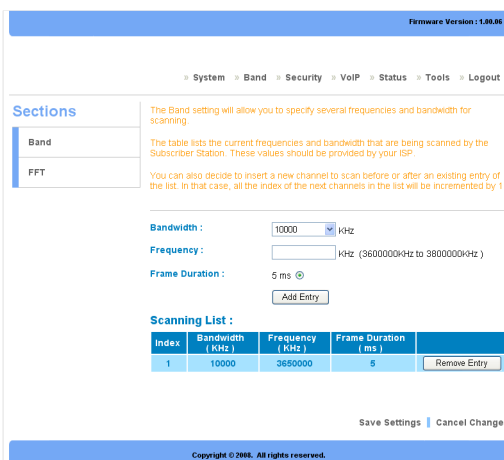
Select the required Corrigenda version and click **Save Settings** to apply the change.

3.3 Using the Band Page

The Band page is used to set WiMAX scan frequencies as provided by the ISP, and to set the Fast Fourier Transform rate.

3.3.1 Band Settings

Band Settings are used to enter the frequencies and bandwidths supplied by the ISP, allowing the Gateway to connect successfully to the BTS. The Scanning List describes the bandwidths and frequencies currently scanned for connection.



Bandwidth : kHz

Frequency : kHz (3600000kHz to 3800000kHz)

Frame Duration : ms

Index	Bandwidth (KHz)	Frequency (KHz)	Frame Duration (ms)	
1	10000	3600000	5	<input type="button" value="Remove Entry"/>

Copyright © 2008. All rights reserved.

To enter band settings manually, perform the following steps:

1. Select a bandwidth from the drop down menu as supplied by the ISP.
2. Enter a frequency between 2500000 and 2700000 KHz as supplied by the ISP.
3. Select the Frame Duration in milliseconds as supplied by the ISP.
4. Click **Add Entry** to refresh the Scanning List.
5. Click **Save Settings**.

3.3.2 FFT Settings

Fast Fourier Transform (FFT) scaling to the current channel bandwidth helps keep the carrier spacing constant across different channel bandwidths, resulting in higher spectrum efficiency in wide channels and cost reductions in narrow channels. The default FFT size is 1024.

The screenshot shows the 'FFT Settings' page in a web GUI. At the top right, it says 'Firmware Version: 1.00.06'. Below that is a navigation menu with 'System', 'Band', 'Security', 'VoIP', 'Status', 'Tools', and 'Logout'. The main content area is titled 'Sections' and has a table with two rows: 'Band' and 'FFT'. The 'FFT' row is selected. To the right of the table, there is a text box explaining the FFT scaling: 'Scaling of the FFT (Fast Fourier Transform) to the channel bandwidth in order to keep the carrier spacing constant across different channel bandwidths. Constant carrier spacing results in a higher spectrum efficiency in wide channels, and a cost reduction in narrow channels.' Below this text box, there is a label 'FFT Size:' followed by two radio buttons: '512' and '1024'. The '1024' radio button is selected. At the bottom right of the main content area, there are two buttons: 'Save Settings' and 'Cancel Changes'. At the very bottom of the page, there is a footer that says 'Copyright © 2008. All rights reserved.'

Select **512** or **1024** as instructed by the ISP and click **Save Settings**.

3.4 Using the Security Page

The Security page is used to manage all aspects of Gateway access security, including login details, Privacy Key Management (PKM), and Simple Network Management Protocol (SNMP).

3.4.1 Changing Login Details

The Gateway GUI management login details are modified using the Login page.



WARNING: It is strongly recommended that the login user name and password are changed after the first instance of login in order to secure the Gateway and network.

Firmware Version: 1.00.06

» System » Band » Security » VoIP » Status » Tools » Logout

Sections

- Login
- PKM
- SNMP

The Login account setting page is used to set an account and password for the Subscriber Station in order to access the web-based management.

It is strongly recommended that you change account and password in order to secure the Subscriber Station and your network.

Account:

Password:

Re-enter to Confirm:

Save Settings | Cancel Changes

Copyright © 2008. All rights reserved.

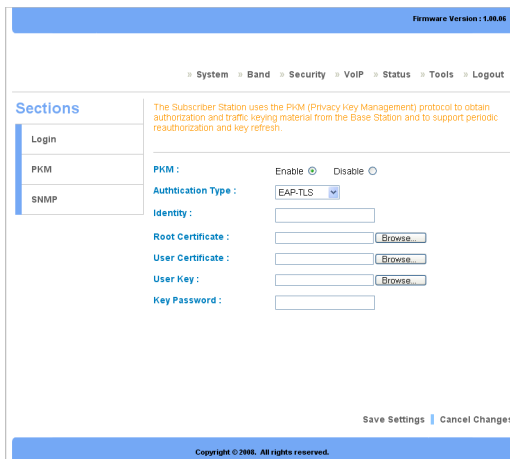
To change the login details, perform the following steps:

1. Enter an account name or use the default **admin**.
2. Enter a new password and re-enter it in the confirm field.
3. Click **Save Settings**.

3.4.2 PKM Settings

The Gateway uses Privacy Key Management (PKM) to obtain authorization and traffic key material from the BTS and to periodically reauthorize and refresh the user key and certificates. PKM is disabled by default.

The ISP provides all the necessary PKM information as well as the required certificates.



Firmware Version : 1.00.06

System > Band > Security > VoIP > Status > Tools > Logout

Sections

- Login
- PKM
- SNMP

The Subscriber Station uses the PKM (Privacy Key Management) protocol to obtain authorization and traffic keying material from the Base Station and to support periodic reauthorization and key refresh.

PKM : Enable Disable

Authentication Type : EAP-TLS

Identity :

Root Certificate :

User Certificate :

User Key :

Key Password :

Save Settings | Cancel Changes

Copyright © 2008. All rights reserved.

To configure PKM, perform the following steps:

1. Select **Enable** to access the configuration fields.
2. Select the **Authentication Type** from the drop down menu.
3. Enter the **Identity** as supplied by the ISP.
4. Click **Browse** to locate the **Root Certificate**, **User Certificate**, **User Key**, and **Key Password** supplied by the ISP.
5. Click **Save Settings**.

Contact the ISP for more information.

3.4.3 SNMP Settings

Simple Network Management Protocol (SNMP) is the most commonly used management protocol on TCP/IP networks. SNMP monitors and controls network device configurations and collects statistics on performance and security. SNMP is disabled by default.

FW Version: 1.00.00

» System » Band » Security » VoIP » Status » Tools » Logout

Sections

- Login
- PKM
- SNMP

Simple Network Management Protocol (SNMP) is the network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

SNMP : Enable Disable

SNMP IP Address :

Save Settings | Cancel Changes

Copyright © 2006. All rights reserved.

SNMP management tool requires no configuration. Select **Enable** or **Disable** and click **Save Settings** to turn SNMP on or off.

3.5 Using the VoIP Page

The Voice over Internet Protocol (VoIP) page is used to manage your VoIP connection through the Network, SIP, and Call Control settings pages.

3.5.1 Network Settings

VoIP is an IP-based service that enables you to make calls over a broadband Internet connection instead of a standard (analog) phone line.

Firmware Version : 1.00.05

System » Band » Security » VoIP » Status » Tools » Logout

Sections

Network
SIP
Call Control

Voice over internet Protocol (VoIP) is IP-Based service that allows you to make voice calls using a broadband internet connection instead of a regular (or analog) phone line. Please choose proper internet connection type and fill in the necessary information request.

Connection Type : Static IP DHCP

IP Address :	192	168	0	254
Subnet Mask :	255	255	255	0
Default Gateway :	0	0	0	0
DNS :	0	0	0	0

Save Settings | Cancel Changes

Copyright © 2008. All rights reserved.

To configure VoIP Network settings, perform the following steps:

STATIC CONNECTION (DEFAULT)

1. Select **Static IP** to assign a static IP address to the VoIP connection.
2. Enter the required information in the IP, Subnet Mask, Gateway, and DNS fields.
3. Click **Save Settings**.

DHCP CONNECTION

1. Select **DHCP** to automatically assign network information.
2. Click **Save Settings**.

3.5.2 SIP Settings

Session Initiation Protocol (SIP) is an application layer protocol that handles call signalling for VoIP. SIP also enables the Gateway to provide other regular services such as call waiting and voicemail.

FW Version: 1.00.06

System > Band > Security > VoIP > Status > Tools > Logout

Sections

- Network
- SIP**
- Call Control

Session Initiation Protocol (SIP) is an application layer control protocol for call signaling for VoIP. It also implements the necessary mechanisms so that different services can be provided.

VOIP : Enable Disable

Registrar :

Registrar Port : 5060 (1 ~ 65535)

Proxy Domain :

Outbound Proxy : 192.168.0.168

Outbound Proxy Port : 5060 (1 ~ 65535)

SIP Port : 5060 (1 ~ 65535)

Proxy :

Proxy Port : 5060 (1 ~ 65535)

SIP Display Name : 1

SIP Phone Number : 1

Username : 1

Password :

Register Expires : 3600

User Agent : Enable Disable

STUN : Enable Disable

Session : Enable Disable

Session Timer : 1800

Min-SE : 180

Proxy-Require : Enable Disable

SIP Update Send : Enable Disable

SIP Prack Send : Enable Disable

Call Waiting : Enable Disable

Anonymous : Enable Disable

Voice Mail : Enable Disable

Phone : Enable Disable

Save Settings | Cancel Changes

Copyright © 2008. All rights reserved.

Refer to the following information for a brief description of the available options. For more information, contact your VoIP service provider.

- Registrar—the Registrar should be the same as the Outbound Proxy.
- Registrar Port—this is the port number of the SIP proxy. The default port is **5060**.
- Outbound Proxy Domain, IP, and Port—the domain, IP address and port number of the SIP proxy server, assigned by the SIP service provider. The default port is **5060**.

- SIP Port, Proxy IP and Port—the SIP Port, IP address and port number of the SIP server, assigned by the SIP service provider. The default port is **5060**.
- SIP Display Name—the name displayed during SIP calls.
- SIP Phone Number—the phone number associated with the SIP user.
- Username and Password—the SIP username and password used to access the connection.
- Register Expires—the time (sec) interval after which the phone refreshes SIP sessions. The default value is **3600**.
- User Agent—enable or disable a User Agent as specified by the service provider. The default value is **Disable**.
- STUN—enable or disable a STUN server as specified by the service provider. The default value is **Disable**.
- Session—enable or disable session timer and minimum seconds timer. The default value is **Enable**.



NOTE: The Session Timer value cannot be lower than the Min-SE value.

- Proxy-Require—enable or disable the proxy requirement during connection. The default value is **Disable**.
- SIP Update Send—enable or disable the Update Request feature. The default is **Disable**.
- SIP Prack Send—Provisional Acknowledgment (PRACK) ensures correct signal transmission by requesting acknowledgement of receipt of signal during transmission. The default is **Disable**.
- Call Waiting—when the line is in use, the user is informed of incoming calls as they are connected. The default value is **Enable**.
- Anonymous—prevent the sender phone number from being visible to the receiver. The default is **Disable**.
- Voicemail—enable or disable the voicemail feature. The default is **Disable**.
- Phone—enable or disable the phone connection. The default is **Enable**.

3.5.3 Call Control

The Call Control page provides advanced VoIP implementation settings such as Real-time Protocol (RTP) for voice media.

Call Control provides the advanced setting for the implementations of VoIP, for example, Real-time Protocol (RTP) for voice media.

RTP Port :	<input type="text" value="41000"/>	(1 ~ 65535)
RTP TOS :	<input type="text" value="184"/>	(0 ~ 255)
Default Codec :	<input type="text" value="G.729A"/>	
Packet Size :	<input type="text" value="20ms"/>	
Jitter Buffer :	<input type="text" value="60ms"/>	
VAD :	Enable <input type="radio"/> Disable <input checked="" type="radio"/>	
LEC :	Enable <input checked="" type="radio"/> Disable <input type="radio"/>	
Flash Timer Min :	<input type="text" value="28"/>	(Ms)
Flash Timer Max :	<input type="text" value="110"/>	(Ms)
Inter-digit Timeout :	<input type="text" value="5"/>	(Sec)
DTMF Command :	<input type="text" value="INBAND"/>	
DTMF MIME Type :	<input type="text" value="DTMF-relay"/>	
DTMF Payload Type :	<input type="text" value="101"/>	(96 ~ 127)
Speaker Volume :	<input type="text" value="-8"/>	
Mic. Gain :	<input type="text" value="-8"/>	
Tone Volume :	<input type="text" value="-5"/>	
Tone Country :	<input type="text" value="USA"/>	

Save Settings | Cancel Changes

Copyright © 2008. All rights reserved.

Refer to the following information for a brief description of the available options. For more information, contact your VoIP service provider.

- RTP Port—enter the port to use for RTP. The default is **41000**.
- RTP TOS—enter the RTP Type of Service (ToS). The default is **184**.
- Default Codec—select the default codec from the drop down menu. The default is **G.729A**.
- Packet Size—select the packet size from the drop down menu. The default is **20 ms**.
- Jitter Buffer—select the jitter buffer size from the drop down menu. The default is **60 ms**.

- VAD—enable or disable the Voice Activity Detection (VAD) feature. The default is **Disable**.
- LEC—enable or disable the Line Echo Canceller (LEC) feature. The default is **Enable**.
- Flash Timer Min/Max—set the flash timer minimum and maximum in milliseconds. The default values are **28** and **110** ms respectively.
- Inter-digit Timeout—set the interdigit timeout in seconds. The default value is **5** seconds.
- DTMF Command—select the Dual-tone multi-frequency (DTMF) from the drop down menu. The default is **INBAND**.
- DTMF Mime Type—select the DTMF mime type from the drop down menu. The default is **DTMF-relay**.
- DTMF Payload Type—set the DTMF payload type. The default value is **101**.
- Speaker Volume—set the speaker output volume. The default value is **-8**.
- Mic. Gain—set the Microphone gain level. The default value is **-8**.
- Tone Volume—set the ring tone volume. The default value is **-5**.
- Tone Country—select the country of residence from the drop down menu. The default value is **USA**.

3.6 Using the Status Page

The Status page displays useful information in the form of easy to read tables including System, LAN, Forwarding, and Connection Status pages.

3.6.1 System Status

The System Status page displays the current status of the Gateway including firmware version, software version, date and time, and total running time.

The screenshot shows the System Status page with the following details:

- Firmware Version:** 1.00.06
- Hardware Version:** 2.37.7
- BSP Version:** 1.27
- Software Version:** 4.4.1-13799
- MAC Version:** 06.00.0000
- PHY Frontend Version:** 06.00.0000
- PHY Backend Version:** 06.00.0000
- Microcode Version:** 5.5.1.1-3629
- System Current Time:** 00:02:13, 1 Jan, 1970
- System UP Time:** 02 Min 13 Sec

The page also includes a navigation menu with options: System, Band, Security, VoIP, Status, Tools, and Logout. A 'Sections' sidebar on the left lists System, LAN, Forwarding, Connection, and VoIP. A note states: 'The System status page displays the current status of the Subscriber Station. This includes the firmware versions, hardware and software version and system time.' The footer contains the text: 'Copyright © 2006. All rights reserved.'

Information on the System Status page is read only, it is not possible to modify the display.

3.6.2 LAN Status

The LAN Status page displays the current LAN information including IP address, Host Name (if applicable), and MAC address.

Firmware Version : 1.00.05

» System » Band » Security » VoIP » Status » Tools » Logout

Sections

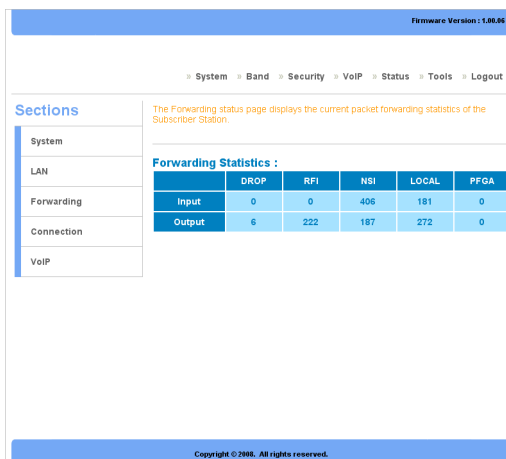
System	
LAN	LAN IP Address : 192.168.0.10 Subnet Mask : 255.255.255.0
Forwarding	Default Gateway : 192.168.0.1
Connection	Host Name : host MAC Address : 00:1E:37:81:DD:EF
VoIP	

Copyright © 2008. All rights reserved.

Information on the LAN Status page is read only, it is not possible to modify the display.

3.6.3 Forwarding Status

The Forwarding Status page displays the current packet forwarding statistics of the Gateway. Both incoming and outgoing statistics are displayed.



Firmware Version: 1.00.06

» System » Band » Security » VoIP » Status » Tools » Logout

Sections

- System
- LAN
- Forwarding
- Connection
- VoIP

The Forwarding status page displays the current packet forwarding statistics of the Subscriber Station.

Forwarding Statistics :

	DROP	RFI	NSI	LOCAL	PFGA
Input	0	0	406	181	0
Output	6	222	187	272	0

Copyright © 2006. All rights reserved.

The column headings are described as follows:

- DROP—the total number of packets discarded.
- RFI—the total number of requests for information (RFI).
- NSI—the total number of network side interface (NSI) packets.
- LOCAL—the total number of local packets forwarded.
- PFGA—the total number of PFGA packets forwarded.

Information on the Forwarding Status page is read only, it is not possible to modify the display.

3.6.4 Connection Status

The Connection Status page displays the current connection status of the Gateway including the frequency, bandwidth, and signal strength (RSSI).

Firmware Version : 1.00.06

[System](#) » [Band](#) » [Security](#) » [VoIP](#) » [Status](#) » [Tools](#) » [Logout](#)

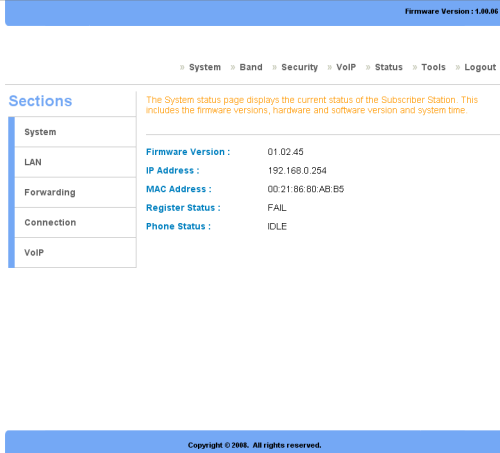
Sections	
System	
LAN	Frequency : 3600000 KHz ~ 3800000 KHz RSSI : 0.00 dBm
Forwarding	CINR : 0.00 dBm
Connection	DL Adaptation Protection Margin : 0.00 dBm DL Adaptation Hysteresis Margin : 0.00 dBm
VoIP	

Copyright © 2008. All rights reserved.

Information on the Connection Status page is read only, it is not possible to modify the display.

3.6.5 VoIP Status

The VoIP Status page displays information about the VoIP connection including the current firmware, IP address, and phone status.



Firmware Version: 1.06.06

» System » Band » Security » VoIP » Status » Tools » Logout

Sections

- System
- LAN
- Forwarding
- Connection
- VoIP

The System status page displays the current status of the Subscriber Station. This includes the firmware versions, hardware and software version and system time.

Firmware Version :	01.02.45
IP Address :	192.168.0.254
MAC Address :	00 21 86 80 AB B5
Register Status :	FAIL
Phone Status :	IDLE

Copyright © 2006. All rights reserved.


Information on the VoIP Status page is read only, it is not possible to modify the display.

3.7 Using the Tools Page

The Tools page is used to perform maintenance tasks and upgrades including rebooting the Gateway and resetting the Gateway to the factory supplied defaults.

3.7.1 Upgrading the Firmware

The Firmware Upgrade page is used to upload newer versions of the firmware to the Gateway. Firmware upgrades are released from time-to-time to correct bugs or add functionality to devices.

	<p>WARNING: To avoid major system malfunction, ensure the selected firmware version is newer than the currently installed version.</p>
---	---

Firmware Version : 1.00.05

[System](#) » [Band](#) » [Security](#) » [VoIP](#) » [Status](#) » [Tools](#) » [Logout](#)


<p>Sections</p> <ul style="list-style-type: none"> <li style="border-bottom: 1px solid #ccc; padding: 2px 5px;">Firmware Upgrade <li style="border-bottom: 1px solid #ccc; padding: 2px 5px;">Reset to Default <li style="border-bottom: 1px solid #ccc; padding: 2px 5px;">Reboot 	<p>The Firmware Upgrade page is used to upgrade the firmware of the Subscriber Station to the latest version in order to add features, and improve the functionality and performance.</p> <p>Ensure that you have obtained the appropriate firmware for upgrading.</p> <p style="color: red; font-weight: bold;">Upgrading firmware may take a few minutes, please don't turn off the power or press the reset button while upgrading.</p> <p>Firmware File : <input type="text"/> <input type="button" value="Browse..."/></p>
--	---

Copyright © 2000. All rights reserved.

To upgrade the Gateway firmware, perform the following steps:

1. Enter the file path of the firmware upgrade or click **Browse** to locate the file.

2. Click **Upgrade** to start the firmware upload.

	WARNING: The upgrade may take a few minutes: Do not power off or reset the Gateway during the upgrade procedure.
---	---


A progress page displays the upgrade status.

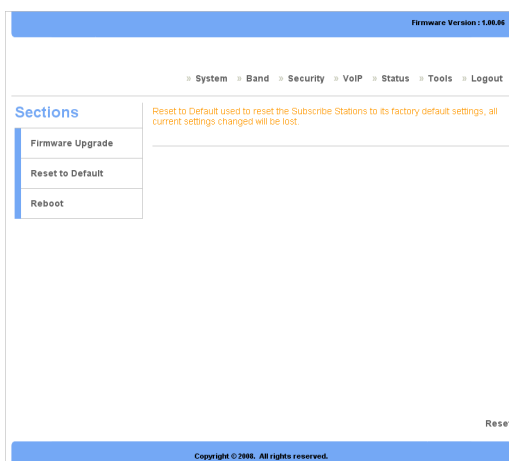


3. Follow the onscreen prompts to complete the upgrade.

3.7.2 Restoring Factory Defaults

The Restore Factory Defaults screen is used to restore the Gateway to the factory supplied defaults.

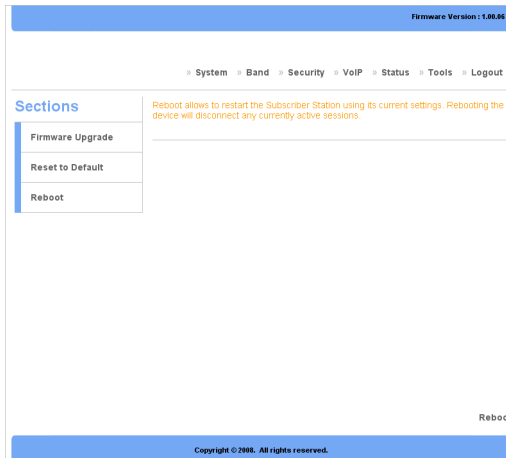
	WARNING: All settings changes are lost when factory defaults are restored.
---	---



To reset the Gateway to the factory defaults, click **Reset** and follow the onscreen prompts.

3.7.3 Rebooting the Gateway

The Reboot screen is used to reboot the Gateway from a desktop computer without disconnecting the power or pressing reset. Restarting the Gateway does not affect any configuration changes.



To reboot the Gateway, click **Reboot** and follow the onscreen prompts.

This page left blank intentionally.

Troubleshooting

This appendix contains troubleshooting and fault finding information for the Gateway in the form of common questions and answers.

Before beginning, perform the following basic troubleshooting sequence to confirm all the hardware is functioning correctly:

1. Make sure that the Gateway is powered on. The Power LED should be green and not flashing.
2. If the Power LED is flashing, then power off all network devices, including the modem, router, and computers.
3. Power on each device in the following order:
 - Router or switch (if present)
 - Gateway
 - Computer(s)
4. Check all cable connections.

4.1 Common Issues

Why can't I connect to the Gateway to perform web configuration?

1. Check if the device is properly connected to the power adapter.
2. Ensure the PC IP address is in the same network segment as the device address. For example, the PC IP address is 192.168.0.x while the default device's IP address is 192.168.0.10.
3. Restore the factory default settings and re-log onto the Gateway's web-based configuration page.

How do I reset my password if I've forgotten it?

- Call the Internet service provider (ISP).

How do I restore my Gateway to the factory default settings?

1. Launch an Internet browser and access the Gateway configuration webpage at the default address: <http://192.168.0.10>
2. Go to **Tools**→ **Reset to Default** and follow the on screen prompts.

How can I find out the Gateway's MAC address?

1. Launch an Internet browser and access the Gateway configuration webpage at the default address: <http://192.168.0.10>
2. The MAC address is displayed under **Status**→ **LAN** on the status page.

How do I set up an IP Address for my PC with Windows XP/2000 installed?

1. The Gateway is set to DHCP server enabled by default.



NOTE: If a DHCP server is already present on the LAN, disable the DHCP function on the Gateway or DHCP server. If there is more than one device supplying IP addresses to network devices, the resulting conflict prevents the network from functioning.

2. Ensure that the target PC is set to obtain an IP address automatically by going to **Start**→ **Control Panel**→ **Network Connections**→ **Local Area Connection**→ **Properties**→ **Internet Protocol (TCP/IP)**→ **Properties** and select Obtain an IP address automatically,

OR

1. Go to **Properties** as described in step 2 above and select **Use the following IP address**.
2. Enter a static IP address in the same segment of the device's address. For example, the PC IP address is 192.168.0.x while the default device's IP address is 192.168.0.10.

How can I login to the GUI if DHCP cannot assign my computer an IP address?

- If the default log in IP address doesn't respond, use 169.254.1.1 as an alternative.

Why can't I use LAN ports to connect to the Internet?

1. Check if the device is properly connected to the power adapter.
2. Check the Gateway RSSI LED and make sure the WiMAX signal strength is good.
3. Configure the PC with a static IP address within the same segment of the device's address. For example, the PC IP address is 192.168.0.x while the default device's IP address is 192.168.0.10.
4. Log in to the web configuration page and go to **Status** → **Connection**. Check that Connection Status is good between the device and the WiMAX base station. If the connection is not OK, contact the ISP.
5. If the WiMAX connection is OK in the above step, but devices still can not connect to the Internet, ensure DHCP service is enabled and correctly configured in **System Setting** → **DHCP Server**.

Why can't my computer connect wirelessly to the network?

- Check the computer wireless security method and key is the same as the Gateway.

This page left blank intentionally.

Glossary

This section defines or identifies technical terms, abbreviations, and acronyms used through out this document.

Administrator

An administrator performs the service of maintaining a network. In the case of this CPE, the person who sets up the network connections and makes changes to the settings.

BTS

Base Transceiver Station. The WiMAX service provider base transmitter providing the WiMAX signal.

Client

A device on the network that uses the services of the CPE, for example a computer accessing the internet.

DHCP

Dynamic Host Configuration Protocol. When enabled, this protocol automatically configures the TCP/IP settings of every computer on the network.

Dial-Up

A connection which uses the public telephone network.

DNS Server Address

DNS stands for Domain Name System, which allows Internet host computers to have a domain name and one or more IP addresses (such as 192.168.0.20). A DNS server keeps a database of host computers and their respective domain names and IP addresses, so that when a domain name is requested (as in typing easyDNS.com into an Internet browser), the user is sent to the proper IP

address. The DNS server address used by the computers on the home network is the location of the DNS server the ISP has assigned.

DSL Modem

DSL stands for Digital Subscriber Line. A DSL modem uses an existing phone lines to transmit data at high speeds.

Ethernet

A standard for computer networks. Ethernet networks are connected by special cables and hubs, and move data around at up to 10 million bits per second (Mbps).

Firewall

An electronic boundary that prevents unauthorized users from accessing certain files or computers on a network.

Firmware

Software stored in memory. Essential programs that remain even when the system is turned off. Firmware is easier to change than hardware but more permanent than software stored on a disk.

IP Address

IP stands for Internet Protocol. An IP address consists of a series of four numbers separated by periods, that identifies a single, unique Internet computer host. Example: 192.34.45.8

ISP

Internet Service Provider. An ISP is a business that provides connectivity to the Internet for individuals and other businesses or organizations.

LAN

Local Area Network. A LAN is a group of computers and devices connected together in a relatively small area (such as a house or an office). A home network is considered a LAN.

MAC Address

MAC stands for Media Access Control. A MAC address is the hardware address of a device connected to a network.

MTU

Maximum Transmission Unit. The largest unit of data that can be transmitted on any particular physical medium.

NAT

Network Address Translation. This process allows all of the computers on the home network to use one IP address. Using the NAT capability of the HomeConnect home network gateway, access is available to the Internet from any computer on the home network without having to purchase more IP addresses from the ISP.

Port

A logical channel that is identified by its unique port number. Applications listen on specific ports for information that may be related to it.

SNTP

Simple Network Time Protocol. A communication standard that allows for the transmission of real time information over a network or the Internet.

SPI

Stateful Packet Inspection. SPI is the type of corporate-grade Internet security provided by a HomeConnect home network gateway. Using SPI, the gateway acts as a firewall, protecting the network from computer hackers.

Subnet Mask

A subnet mask, which may be a part of the TCP/IP information provided by the ISP, is a set of four numbers configured like an IP address. It is used to create IP address numbers used only within a particular network (as opposed to valid IP address numbers recognized by the Internet, which must assigned by InterNIC).

TCP

Transmission Control Protocol. The most common Internet transport layer protocol. TCP is connection-oriented and stream-oriented, and provides for reliable communication over packet-switched networks.

TCP / IP

Transmission Control Protocol over Internet Protocol. This is the standard protocol for data transmission over the Internet.

UDP

User Datagram Protocol. Communications protocol for the Internet network layer, transport layer, and session layer, which makes it possible to send a datagram message from one computer to an application running in another computer. Unlike TCP, UDP is connectionless and does not guarantee reliable communication; the application itself must process any errors and check for reliable delivery.

Index

A

Antennas
Attaching 11

B

Band
Changing 25
Band Settings 25

C

Call Control 33
Changing 27
Channel and Frequency
Band Settings 25
FFT Settings 26
Choosing a Location 10
Conformance
R&TTE iv
WEEE iv
Conformance Documents ii
Connection
LAN 12
Stand Alone PC 12
Connection Status 38
Corrigenda 24

D

DHCP 21

F

Factory Defaults 42
Fast Fourier Transform 26
FFT Settings 26
Firmware 40
Forwarding Status 37

G

GUI Password 27

I

Installation
Hardware 9
LAN 12
Location 10
Powering On 14
Safety 7
Safety Measures 7
Stand Alone PC Connection 12
System Requirements 7

L

LAN Settings 20
LAN Status 36
Login Details 27

N

Network Time Protocol 22
NTP 22

P

- Package Contents 8
- Password 27
- Privacy Key Management
 - Using 28

R

- Rebooting 43

S

- Safety
 - Information i
 - Notices i
- Security Settings
 - Login Details 27
 - PKM Settings 28
 - SNMP Settings 29
 - Using 27
- Session Initiation Protocol 31
- Simple Network Management Protocol 29
- SIP Settings 31
- Status LEDs
 - Functions 4
- Status Pages
 - Connection Status 38
 - Displaying 35
 - Forwarding Status 37
 - LAN Status 36
 - System Status 35
 - VoIP Status 39
- System Settings
 - Changing 20
 - Corrigenda 24
 - DHCP Server Settings 21
 - LAN Settings 20

- NTP Settings 22

- VLAN Tagging 23

- System Status 35

- System Tools

- Rebooting the Gateway 43

- Restoring Factory Defaults 42

- Upgrading 40

- Using 40

- System Tour

- Front View 3

- Main Features 2

- Rear View 5

T

- Tools 40

- Troubleshooting

- Basics 45

- Common Issues 46

U

- Unpacking the Gateway 8

- Upgrading Firmware 40

V

- VLAN 23

- VoIP Settings

- Call Control 33

- Network Settings 30

- SIP Settings 31

- Using 30

- VoIP Status 39

W

- Warning Symbols

- Caution ii

- Note ii

- Warning ii

- Web Configuration

Homepage	19
Logging In	18
Navigating	19
Web GUI Configuration	
Introduction	17

This page left blank intentionally.