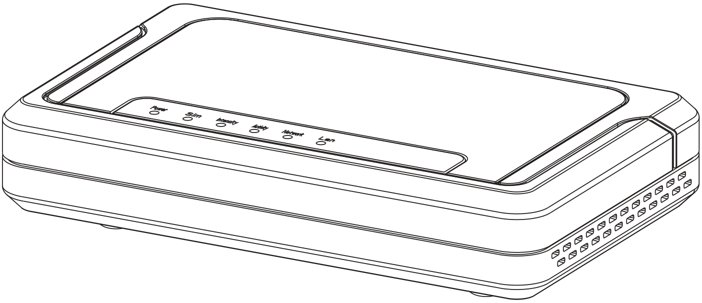
ENGLISH

WiMAX Indoor Gateway

User Manual



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.

Note:

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

Note	**NOTE:** Useful information and tips on the Gateway and networking.

Warning:

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.

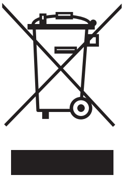
R&TTE Directive 1999/5/EC Statements

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

1

Product Overview

1.1 Introduction

This Gateway provides high-speed, "always-on" Internet access. The Gateway works like a cell phone, in that it communicates with your service provider's WiMAX network and does not require a special wired connection or outdoor antenna.

Installation is easy: simply plug in the Gateway and connect it to your computer's Ethernet port. The Gateway automatically connects to the network and you can then set up your Internet account using a Web browser.

1.1.1 IEEE 802.16e WiMAX Compliance

The IEEE 802.16e-2005 specifications describe a point-to-multipoint (PMP) broadband wireless access standard for devices that operate between the frequencies 2-11 GHz and 10-66 GHz. Both the Media Access Control (MAC) and the physical (PHY) layers descriptions are regulated by IEEE 802.16e-2005 certification.

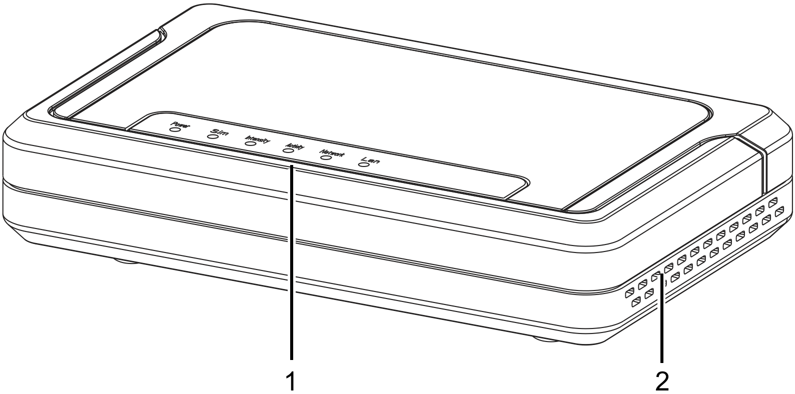
NOTE: This Gateway device compliance applies to a specific revision of the 802.16 standard which is subject to amendment.

This Gateway device does not support mesh communication (direct subscriber-to-subscriber).

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
- Output power: 25.5dBm typical
- LED signal indicators
- MIMO 1Tx/2Rx support
- Ease of use web interface for management and configuration

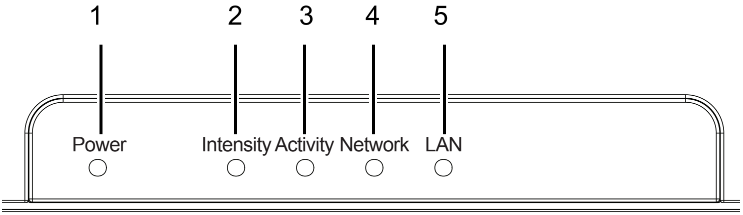
1.3 Front View



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

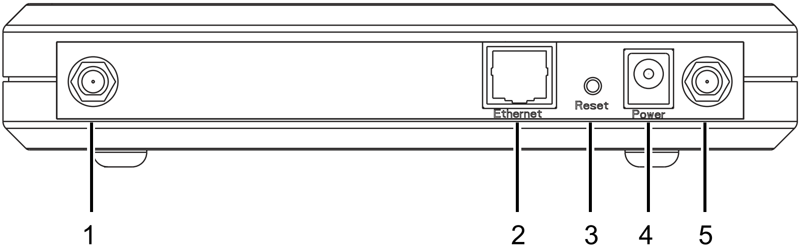
1.3.1 LED Status Activity

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



Label	Function	Status	
1.	Power	Lights when Gateway is powered on	
2.	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
3.	Activity	Lights when WiMAX activity is detected	
4.	Network	Lights when network activity is detected	
5.	LAN	Lights when ethernet port is connected	

1.4 Rear View



Label	Item	Description
1.	Antenna	Connect the supplied antenna to this port
2.	RJ-45 Port	Connect to a standard ethernet port
3.	Reset Button	Press to reset the Gateway to factory defaults
4.	Power Jack	Connect the supplied power supply to this port
5.	Antenna	Connect the supplied antenna to this port

This page left blank intentionally.

2

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 with the Gateway
- 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:

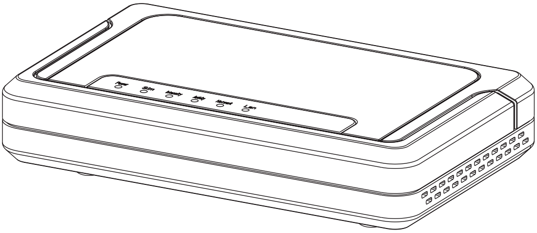
- A PC with an Ethernet (10/100Base-TX) port
- A Web browser installed such as Microsoft Internet Explorer® version 6.0, Firefox®version 2.0, or Safari® version 3.0.3.

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

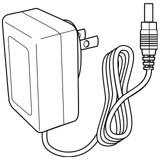
2.3 Unpacking the Gateway

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

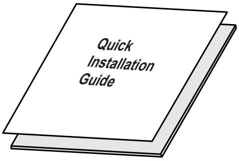
Materials List



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

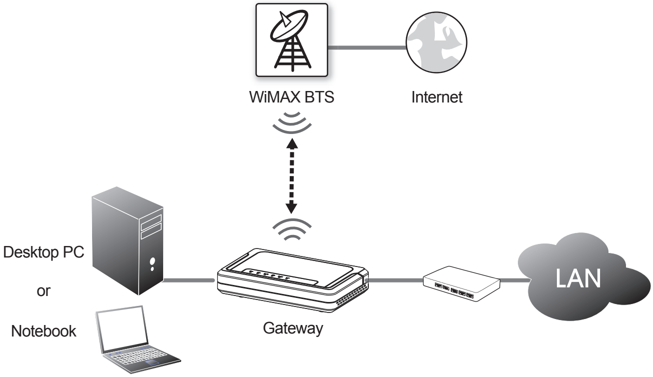
The proper installation procedure for the Gateway is as follows:

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	**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 *14*
- 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

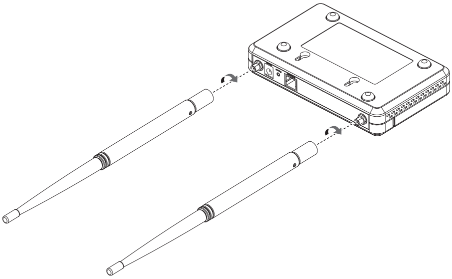
2.4.2 Attaching the Antennas

To attach the two antennas:

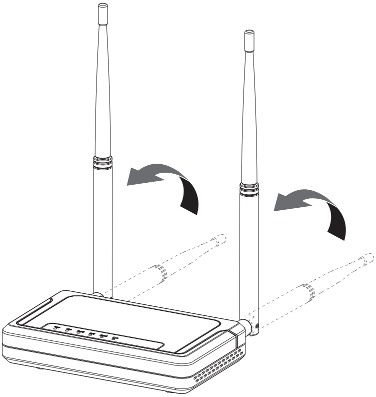
1. Turn off your computer and turn off or unplug any attached network devices.
2. Write down the Ethernet and MAC addresses of the Gateway, as well as the serial number; the information is used for configuring the unit.

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.

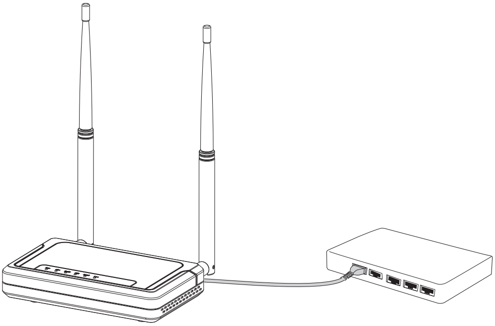


2.4.3 Connecting the Ethernet Cable

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.

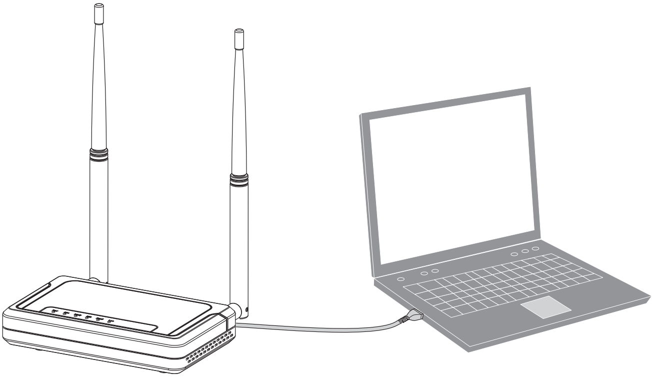
To connect the Gateway to a router or switch:

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.

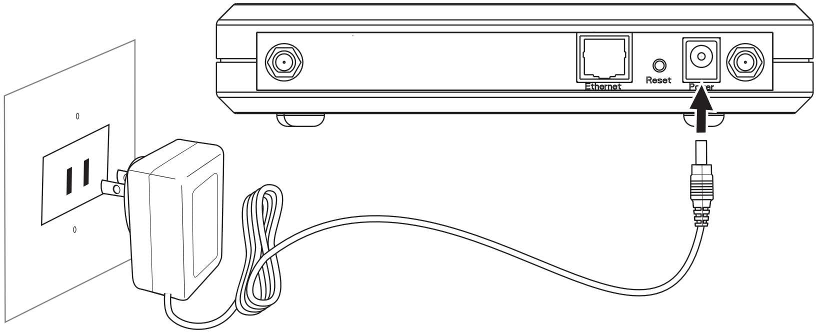


2.4.4 Powering on the Unit

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.

2.4.5 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.

3

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
- Internal password change
- Default settings reset
- Firmware updates

3.1 Logging In

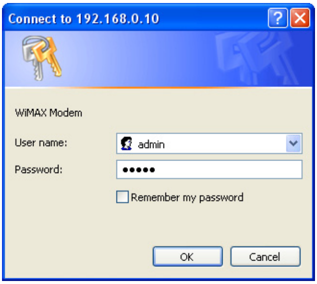
To log in to the GUI, perform the following steps:

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

N te	**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.



Connect to 192.168.0.10

WiMAX Modem

User name: admin

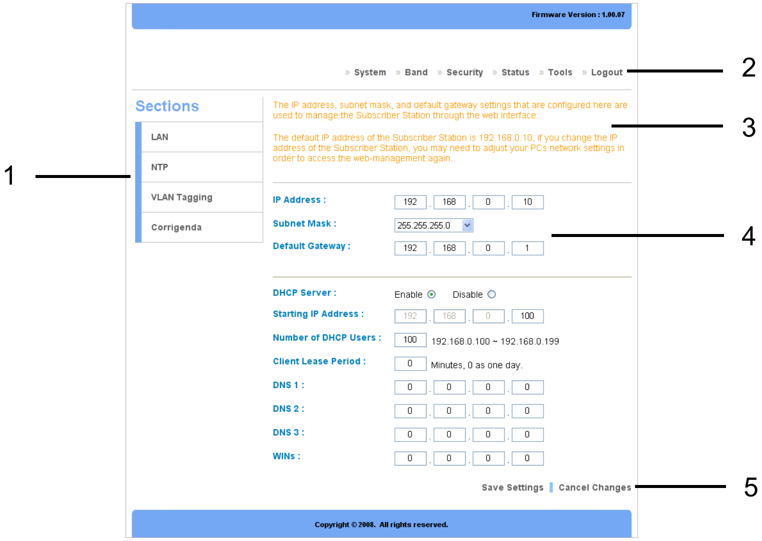
Password: •••••

□ Remember my password

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

   Username: **admin**
   Password: **admin**

The Gateway configuration homepage appears.



Firmware Version : 1.00.07

» System » Band » Security » 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 : 192 . 168 . 0 . 10

Subnet Mask : 255.255.255.0

Default Gateway : 192 . 168 . 0 . 1

DHCP Server : Enable ● Disable ○

Starting IP Address : 192 . 168 . 0 . 100

Number of DHCP Users : 100 192.168.0.100 ~ 192.168.0.199

Client Lease Period : 0 Minutes, 0 as one day.

DNS 1 : 0 . 0 . 0 . 0

DNS 2 : 0 . 0 . 0 . 0

DNS 3 : 0 . 0 . 0 . 0

WINs : 0 . 0 . 0 . 0

Save Settings | Cancel Changes

Copyright © 2008. All rights reserved.

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.

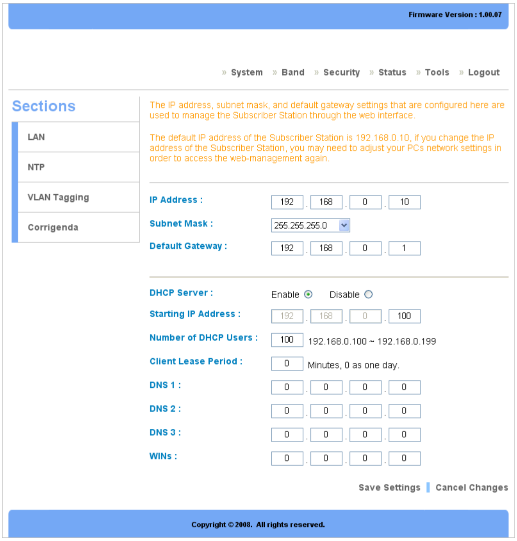
3.2 Using the System Page

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 : 1.00.07
» System » Band » Security » Status » Tools » Logout
Sections
LAN
NTP
VLAN Tagging
Corrigenda
Save Settings
Cancel Changes
Copyright © 2008. All rights reserved.

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 : 192 . 168 . 0 . 10

Subnet Mask : 255.255.255.0

Default Gateway : 192 . 168 . 0 . 1

DHCP Server : Enable ● Disable ○

Starting IP Address : 192 . 168 . 0 . 100

Number of DHCP Users : 100 192.168.0.100 ~ 192.168.0.199

Client Lease Period : 0 Minutes, 0 as one day.

DNS 1 : 0 . 0 . 0 . 0

DNS 2 : 0 . 0 . 0 . 0

DNS 3 : 0 . 0 . 0 . 0

WINs : 0 . 0 . 0 . 0

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:

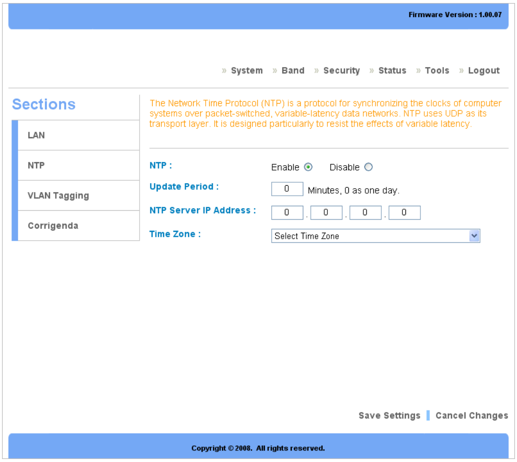
1. Starting IP Address—enter the starting range of IP addresses available for distribution. The default value is 192.168.9.100.
2. Number of DHCP Users—enter the maximum number of available IP addresses for distribution. The default value is 100.

> **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 : 1.00.07
» System » Band » Security » Status » Tools » Logout
Sections
LAN
NTP
VLAN Tagging
Corrigenda
Save Settings | Cancel Changes

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 : 0 Minutes, 0 as one day.

NTP Server IP Address : 0 . 0 . 0 . 0

Time Zone : Select Time Zone

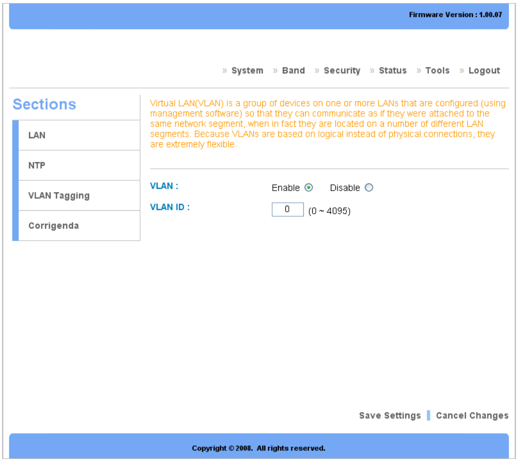
Copyright © 2008. All rights reserved.

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 (0 ~ 4095)

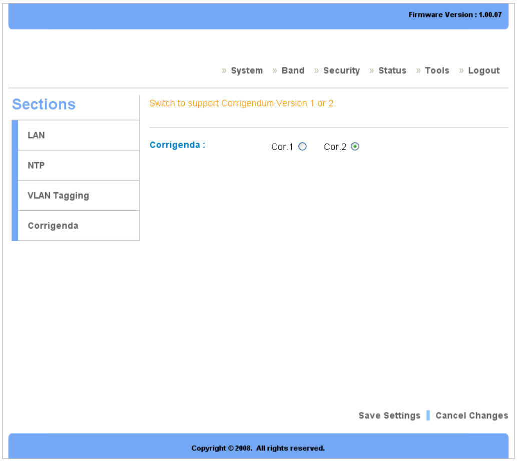
To configure VLAN, perform the following steps:

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.



Firmware Version : 1.00.07
» System » Band » Security » Status » Tools » Logout
Sections
LAN
NTP
VLAN Tagging
Corrigenda
Save Settings
Cancel Changes
Copyright © 2008. All rights reserved.

Switch to support Corrigendum Version 1 or 2.

Corrigenda : Cor.1 ○ Cor.2 ●

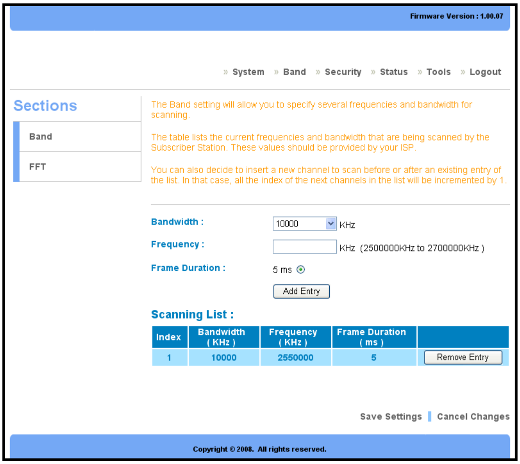
Select the required Corrigenda version and click **Save Settings** to apply the change.

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.



Firmware Version : 1.00.07
» System » Band » Security » Status » Tools » Logout
Sections
Band
FFT

The Band setting will allow you to specify several frequencies and bandwidth for scanning.

The table lists the current frequencies and bandwidth that are being scanned by the Subscriber Station. These values should be provided by your ISP.

You can also decide to insert a new channel to scan before or after an existing entry of the list. In that case, all the index of the next channels in the list will be incremented by 1.

Bandwidth : 10000 KHz

Frequency : KHz (2500000KHz to 2700000KHz)

Frame Duration : 5 ms ●

Scanning List :

Index	Bandwidth (KHz)	Frequency (KHz)	Frame Duration (ms)	
1	10000	2550000	5	Remove Entry

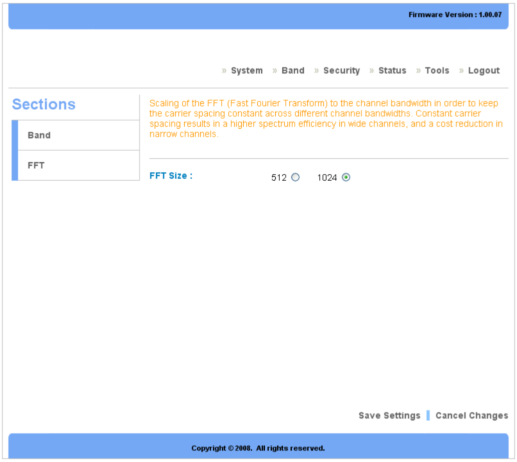
Save Settings | Cancel Changes
Copyright © 2008. All rights reserved.

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.


Firmware Version : 1.00.07
» System » Band » Security » Status » Tools » Logout
Sections
Band
FFT
Save Settings
Cancel Changes
Copyright © 2008. All rights reserved.

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.

FFT Size : 512 ○ 1024 ●

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

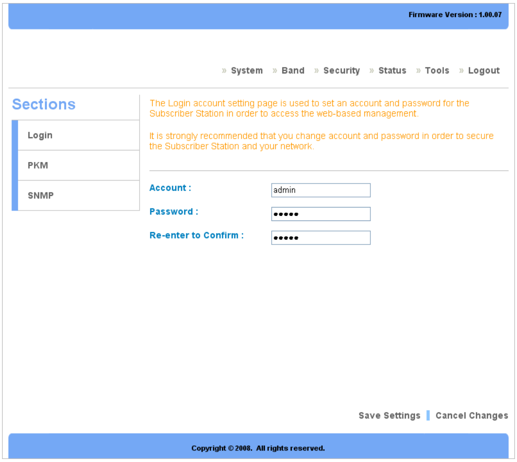
3.4 Using the Security Page

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	**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 : 1.00.07
» System » Band » Security » Status » Tools » Logout
Sections
Login
PKM
SNMP
Save Settings
Cancel Changes
Copyright © 2008. All rights reserved.

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 : admin

Password : •••••

Re-enter to Confirm : •••••

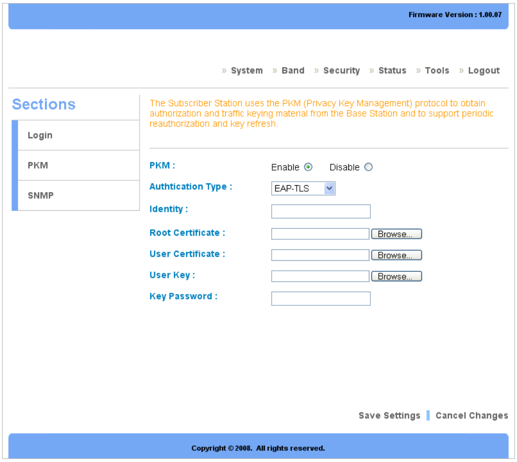
To change the login details, perform the following steps:

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 : 1.00.07
» System » Band » Security » Status » Tools » Logout
Sections
Login
PKM
SNMP
Browse...
Save Settings | Cancel Changes
Copyright © 2008. All rights reserved.

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 ○

Authtication Type : EAP-TLS

Identity :

Root Certificate :

User Certificate :

User Key :

Key Password :

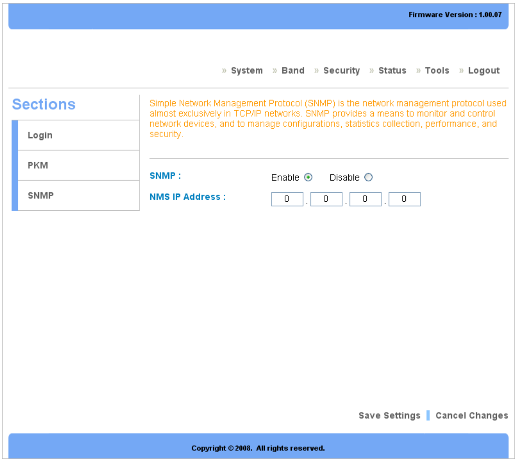
To configure PKM, perform the following steps:

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.


Firmware Version : 1.00.07
» System » Band » Security » Status » Tools » Logout
Sections
Login
PKM
SNMP
Save Settings
Cancel Changes
Copyright © 2008. All rights reserved.

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 ○

NMS IP Address : 0 . 0 . 0 . 0

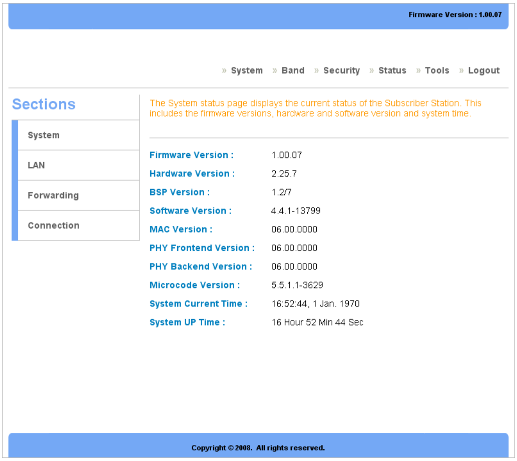
SNMP management tool requires no configuration. Select **Enable** or **Disable** and click **Save Settings** to turn SNMP on or off.

3.5 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.

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

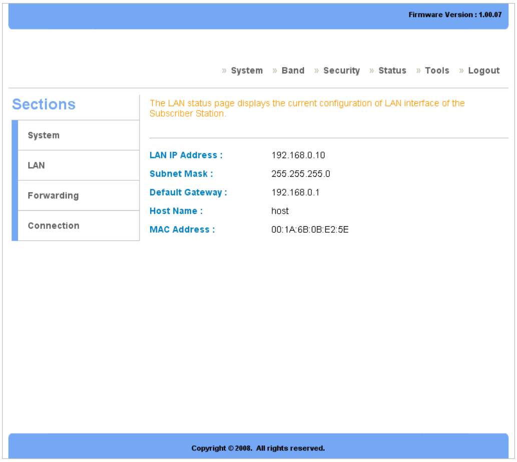
Firmware Version :	1.00.07
Hardware Version :	2.25.7
BSP Version :	1.2/7
Software Version :	4.4.1-13799
MAC Version :	06.00.0000
PHY Frontend Version :	06.00.0000
PHY Backend Version :	06.00.0000
Microcode Version :	5.5.1.1-3629
System Current Time :	16:52:44, 1 Jan. 1970
System UP Time :	16 Hour 52 Min 44 Sec

Copyright © 2008. All rights reserved.

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

3.5.2 LAN Status

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


Firmware Version : 1.00.07
» System » Band » Security » Status » Tools » Logout
Sections
System
LAN
Forwarding
Connection

The LAN status page displays the current configuration of LAN interface of the Subscriber Station.

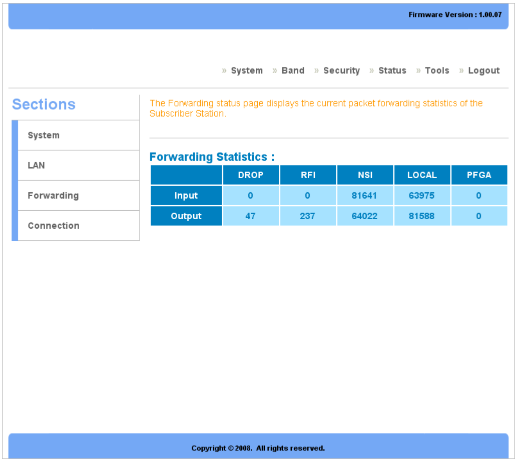
LAN IP Address :	192.168.0.10
Subnet Mask :	255.255.255.0
Default Gateway :	192.168.0.1
Host Name :	host
MAC Address :	00:1A:6B:0B:E2:5E

Copyright © 2008. All rights reserved.

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

3.5.3 Forwarding Status

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


Firmware Version : 1.00.07
» System » Band » Security » Status » Tools » Logout
Sections
System
LAN
Forwarding
Connection

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

Forwarding Statistics :

	DROP	RFI	NSI	LOCAL	PFGA
Input	0	0	81641	63975	0
Output	47	237	64022	81588	0

Copyright © 2008. All rights reserved.

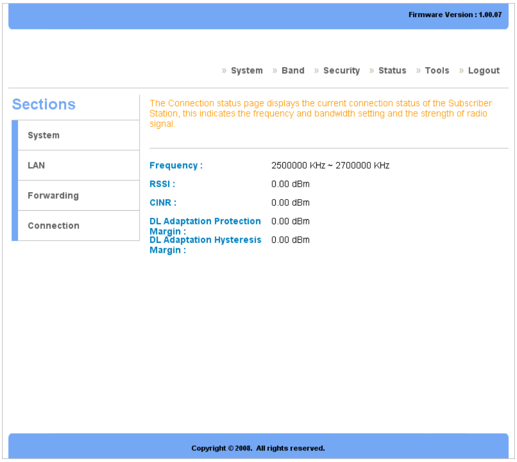
The column headings are described as follows:

- 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.

3.5.4 Connection Status

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



Firmware Version : 1.00.07
» System » Band » Security » Status » Tools » Logout
Sections
System
LAN
Forwarding
Connection

The Connection status page displays the current connection status of the Subscriber Station, this indicates the frequency and bandwidth setting and the strength of radio signal.

Frequency :	2500000 KHz ~ 2700000 KHz
RSSI :	0.00 dBm
CINR :	0.00 dBm
DL Adaptation Protection Margin :	0.00 dBm
DL Adaptation Hysteresis Margin :	0.00 dBm

Copyright © 2008. All rights reserved.

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

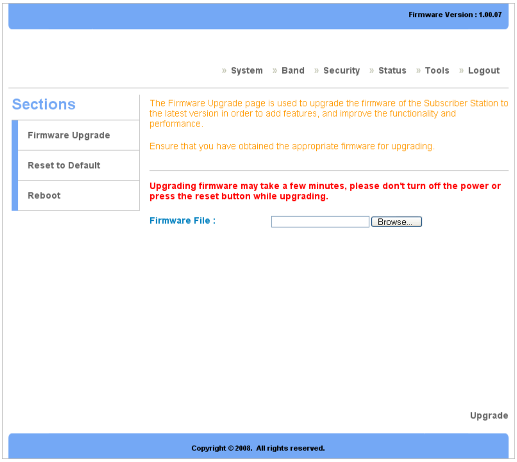
3.6 Using the Tools Page

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

3.6.1 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.

WARNING: To avoid major system malfunction, ensure the selected firmware version is newer than the currently installed version.



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.

Ensure that you have obtained the appropriate firmware for upgrading.

Upgrading firmware may take a few minutes, please don't turn off the power or press the reset button while upgrading.

Firmware File :

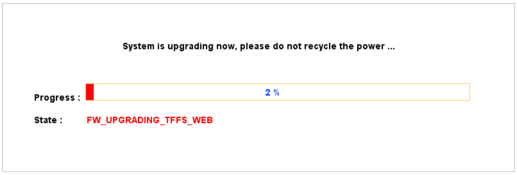
To upgrade the Gateway firmware, perform the following steps:

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	**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.



System is upgrading now, please do not recycle the power ...

Progress : 2 %

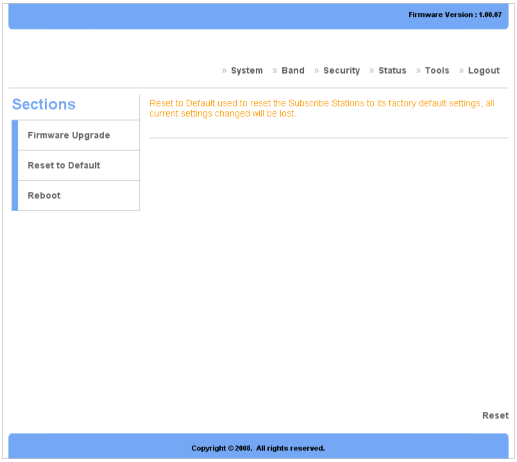
State : FW_UPGRADING_TFFS_WEB

3. Follow the onscreen prompts to complete the upgrade.

3.6.2 Restoring Factory Defaults

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

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



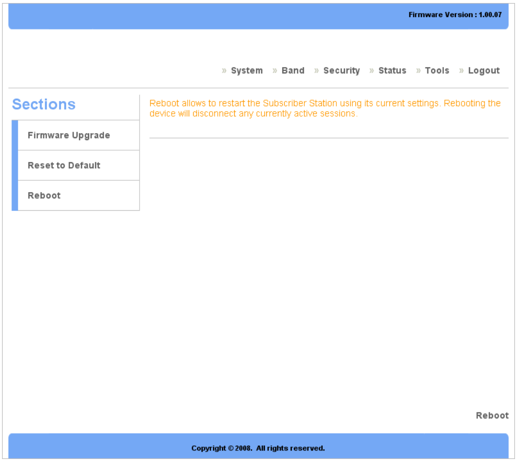
Firmware Version : 1.00.07
» System » Band » Security » Status » Tools » Logout
Sections
Firmware Upgrade
Reset to Default
Reboot
Reset
Copyright © 2008. All rights reserved.

Reset to Default used to reset the Subscribe Stations to its factory default settings, all current settings changed will be lost.

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

3.6.3 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.



Firmware Version : 1.00.07

Reboot allows to restart the Subscriber Station using its current settings. Rebooting the device will disconnect any currently active sessions.

Copyright © 2008. All rights reserved.

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

This page left blank intentionally.

4

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 Gateway, 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 Gateway, 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 Home-Connect 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 Inter-NIC).

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