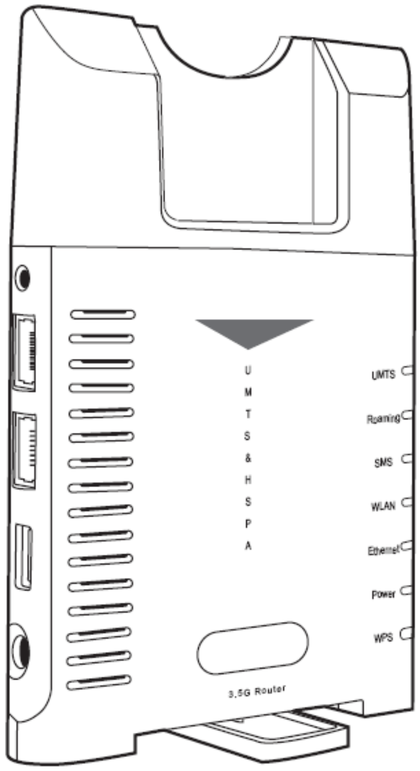
BandLuxe R100 3.5G WiFi Router

User Manual



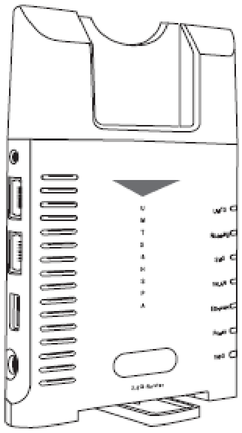
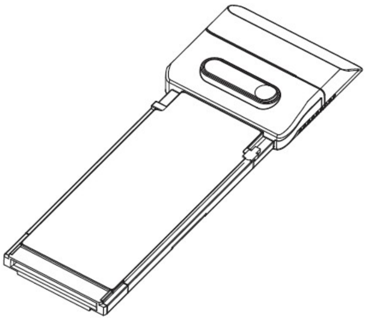
BandLuxe™

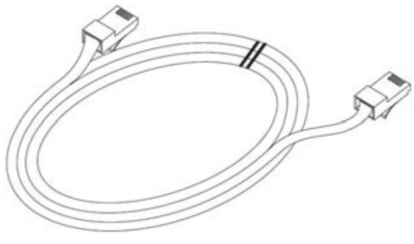
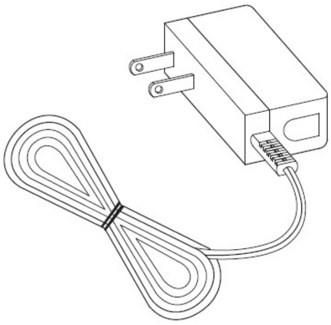
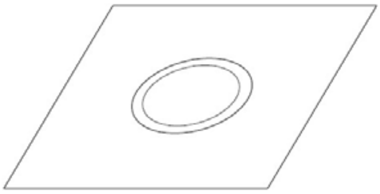
Table of Contents

Package Contents

Thank you for your purchase of this 3.5G WiFi Router. This product is designed to access the Internet via 3.5G technology and share the bandwidth through a WiFi network. It is easy to configure and operate even for non-technical users. This manual contains instructions for installing and configuring the product. Read the manual carefully before you use the product, so that you can fully exploit the product functions.

Package Contents

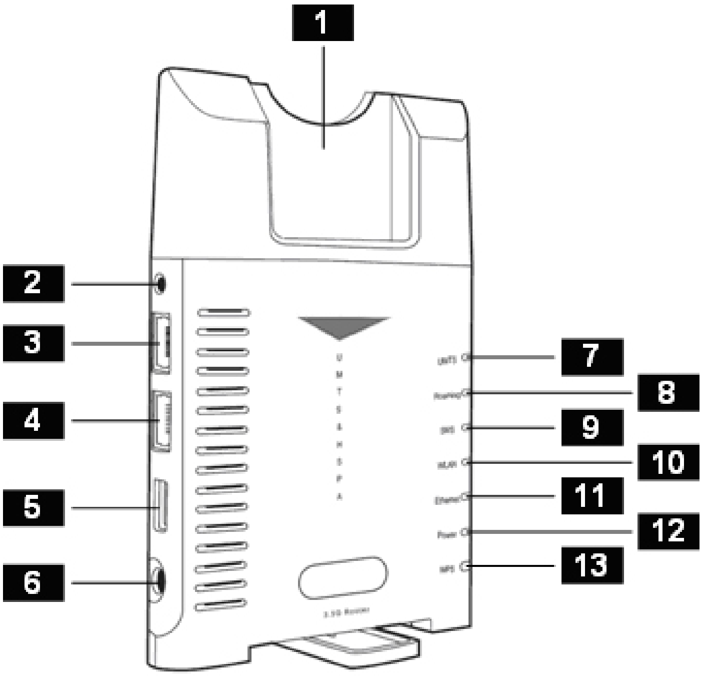
	
BandLuxe R100 3.5G WiFi Router	*BandLuxe C100/C100S HSDPA ExpressCard. (Optional)*

		
Ethernet Cable	*Power Adaptor*	*Setup CD*

Features

- Share mobile broadband access for multiple users.
- Router on the road, data card on the move.
- 3.5G ExpressCard for WAN access supported.
- Compatible with 802.11b and 802.11g clients.
- Compact & Stylish Design.

Hardware Overview



1	**ExpressCard Slot**	Connect a BandLuxe C100/C100S HSDPA ExpressCard or a compatible data card.
2	**Factory Reset button**	To reset the Router, press the reset button briefly. To restore the Router's factory settings, press the reset button for longer than 10 seconds.
3	**WAN Port**	Connect a DSL or Cable modem.
4	**LAN Port**	Connect Ethernet devices such as computers, switches, and hubs.

5 USB Port

6 Receptor Receptor for the Power Adaptor.

7 UMTS LED A solid light shows the Router is connected to a mobile network and ready. When green, the mobile network is in 3G mode. When blue, the mobile network is in 3.5G mode. When purple, the mobile network is in GPRS mode. A blinking light indicates that the Router is not connected to a mobile network or not ready. If the LED light is not lit, there is no link between the data card and the Router. Check the switch on the back of the Router and make sure the setting is correct.

8 Roaming LED A solid light shows that the Roaming connection is on.

9 SMS LED A solid light indicates that a message has been sent to your SIM card.

10 WLAN LED A solid light indicates that the wireless segment is ready. A flashing light shows that data is being transmitted via WLAN.

11 Ethernet LED A solid light shows that an Ethernet-enabled computer is connected via the LAN port but no data is being transmitted. A flashing light shows that data is being transmitted via LAN.

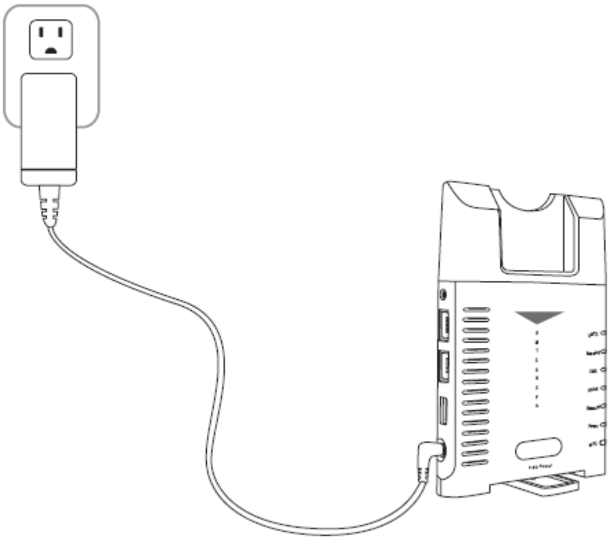
12 Power LED A solid light indicates that the power supply is connected properly.

13 WPS Button

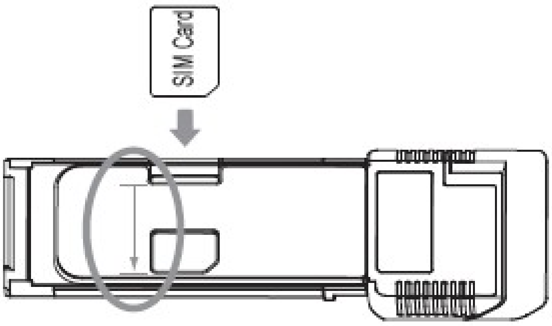
14 ExpressCard/ USB switch Only one of the interfaces (ExpressCard or USB) can be used at a time.

***on the back of Router**

Installation



1. Connect the power adaptor to the Router and connect it to an outlet.

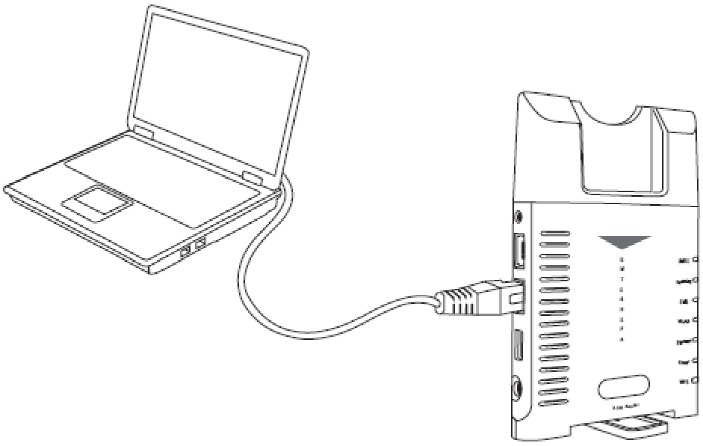


2. Insert your SIM card into the slot on the BandLuxe C100/C100S data card, making sure the SIM card orientation matches the SIM card slot, as shown in the picture. Then insert the BandLuxe data card into the Router.

> **Note:** Please use the ExpressCard/USB switch in the back of the Router to select the interface. Only one of the interfaces can be used at a time.

3. One of the following two methods can be chosen to link your Router with PC.

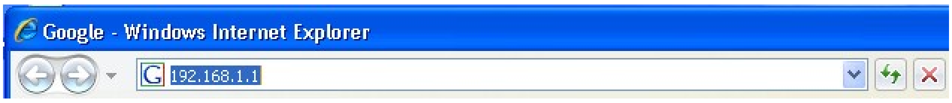
A. To link the Router with your PC via WiFi, in Microsoft Windows, go to *Control Panel* > ***Network Connections***, right-click on **Wireless Network Connection,**.and choose **View Available Wireless Networks**. Select the **HSPA_ROUTER** wireless network, and click **Connect**.



B. To link the Router with your PC via Ethernet cable, connect one end of the cable to the LAN port on the Router, and the other end of the cable to the Ethernet port on your computer.

> **Note:** If you choose to access the Internet via Ethernet, connect one end of the cable to the WAN port of R100, and the other end to your xDSL/Cable Modem.

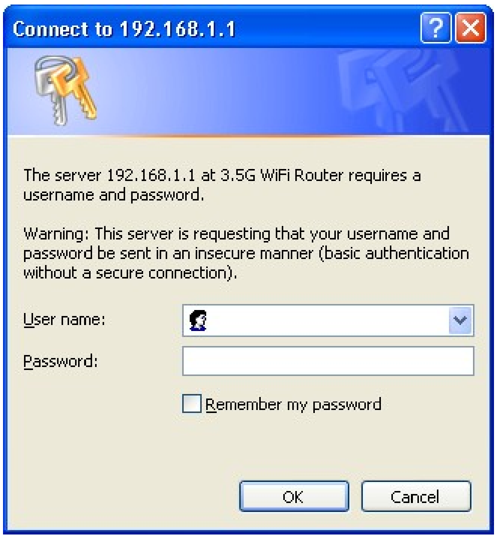
The 3.5G WiFi Router uses a web-based configuration utility. To access the configuration utility, open a browser (for example Internet Explorer) and enter the IP address (**192.168.1.1**) or the URL (**http://R100.ROUTER**) for the Router in your browser's address bar.



Google - Windows Internet Explorer

192.168.1.1

Enter the Router user name **(admin)** and password **(hsparouter)**.



The server 192.168.1.1 at 3.5G WiFi Router requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

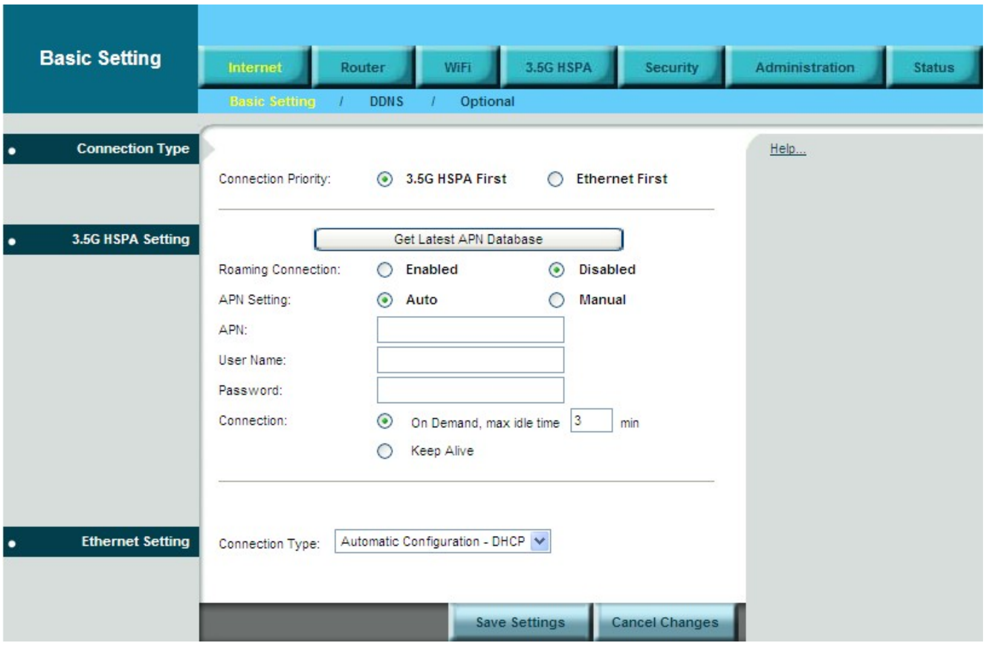
User name:

Password:

□ Remember my password

Internet Setup

Basic Setting



Connection Priority: ● 3.5G HSPA First ○ Ethernet First

Roaming Connection: ○ Enabled ● Disabled

APN Setting: ● Auto ○ Manual

APN:

User Name:

Password:

Connection: ● On Demand, max idle time 3 min

○ Keep Alive

Connection Type: Automatic Configuration - DHCP

Connection Type

The 3.5G HSPA Router can link to the internet via 3.5G HSPA or Ethernet. Select the connection type you prefer.

3.5G HSPA Setting

Get Latest APN Database

Get the latest Profile Name, Number, User Name, Password, and APN from the web site automatically.

Roaming Connection

To allow roaming network connection, select **Enabled**. To block roaming connection, select **Disabled**.

> **Note:** Charges for roaming connection may be high. Contact your mobile network operator for more information.

APN Setting

The APN (Access Point Name) is provided by your mobile network operator. You can choose to set the APN automatically or manually. In most cases, the 3.5G Router works properly when the APN is set to Auto.

To set the APN manually, contact your mobile network operator for the APN, User Name and Password of the data service.

Connection

On Demand: You can set the idle time for the 3.5G HSPA connection. When the Router is idle, the connection will be disconnected automatically after the idle time expires.

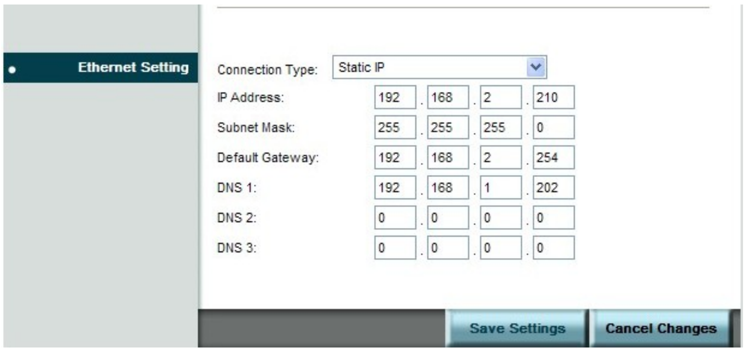
Keep Alive: The connection is always kept on. If the HSPA connection is disconnected, the Router tries to reconnect.

Ethernet Setting

Automatic Configuration - DHCP

Choose **Dynamic IP Address** to obtain IP Address information automatically from your ISP. Select this option if your ISP does not give you any IP numbers to use. This option is commonly used for cable modem services.

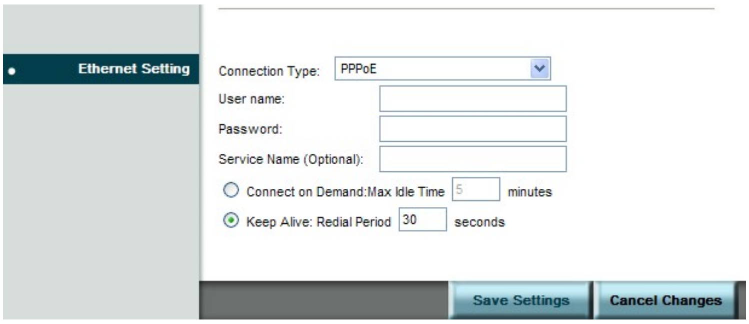
Static IP



Connection Type: Static IP
IP Address: 192 . 168 . 2 . 210
Subnet Mask: 255 . 255 . 255 . 0
Default Gateway: 192 . 168 . 2 . 254
DNS 1: 192 . 168 . 1 . 202
DNS 2: 0 . 0 . 0 . 0
DNS 3: 0 . 0 . 0 . 0

Select **Static IP** if all WAN IP information is provided to you by your ISP. You will need to enter the IP address, subnet mask, gateway address, and DNS address(es) provided to you by your ISP.

PPPoE



Connection Type: PPPoE
User name:
Password:
Service Name (Optional):
○ Connect on Demand:Max Idle Time 5 minutes
● Keep Alive: Redial Period 30 seconds

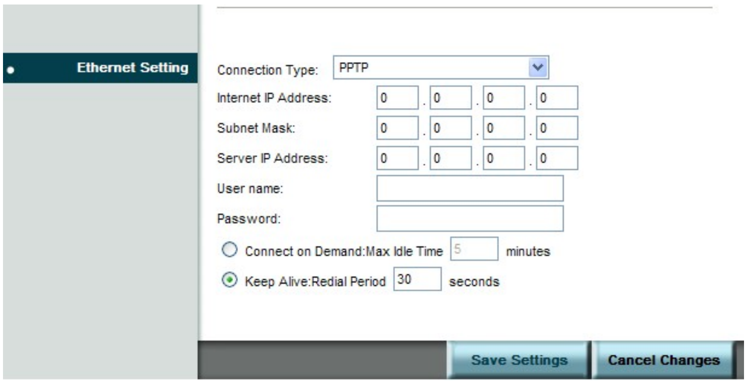
Choose **PPPoE** (Point to Point Protocol over Ethernet) if your ISP uses a PPPoE connection. Your ISP will provide you with a username and password. This option is typically used for DSL services.

Service Name: Enter the ISP Service Name (optional).

Connect on Demand: Enter a maximum idle time during which the Internet connection is maintained during inactivity.

Keep Alive: If you select this option, the Router will periodically check your Internet connection. If you are disconnected, then the Router automatically tries to re-establish your connection. To use this option, select Keep Alive. In the Redial Period field, specify how often you want the Router to check the Internet connection.

PPTP



Connection Type: PPTP
Internet IP Address: 0 . 0 . 0 . 0
Subnet Mask: 0 . 0 . 0 . 0
Server IP Address: 0 . 0 . 0 . 0
User name:
Password:
○ Connect on Demand:Max Idle Time 5 minutes
● Keep Alive:Redial Period 30 seconds

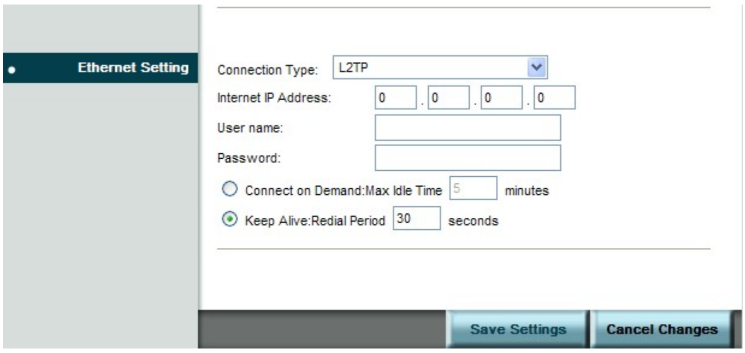
Choose **PPTP** (Point-to-Point-Tunneling Protocol) if your ISP uses a PPTP connection. Your ISP will provide you with a username and password.

Internet IP Address: Enter the IP address

Subnet Mask: This is the Router's Subnet Mask, as seen by users on the Internet (including your ISP). Your ISP will provide you with the Subnet Mask.

Server IP Address: Enter the Server IP provided by your ISP (optional).

L2TP



Connection Type: L2TP

Internet IP Address: 0 . 0 . 0 . 0

User name:

Password:

○ Connect on Demand:Max Idle Time 5 minutes

● Keep Alive:Redial Period 30 seconds

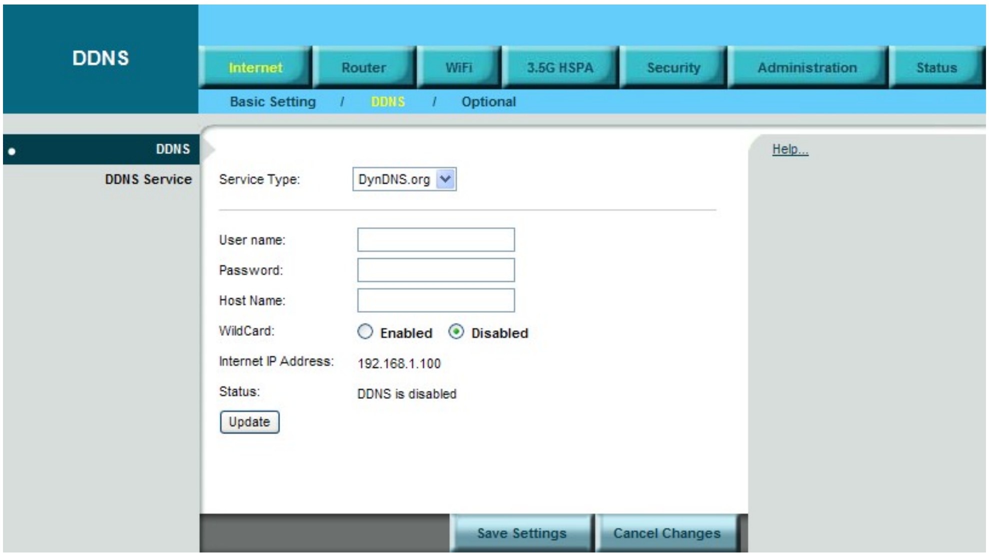
Choose **L2TP** (Layer 2 Tunneling Protocol) if your ISP uses a L2TP connection. Your ISP will provide you with a username and password.

Internet IP Address: Enter the IP address provided by your ISP.

Connect on Demand: Enter a maximum idle time during which the Internet connection is maintained during inactivity.

Keep Alive: Redial Period If you select this option, the Router will periodically check your Internet connection. If you are disconnected, the Router automatically tries to re-establish your connection. To use this option, select **Keep Alive**. In the **Redial Period** field, you specify how often you want the Router to check the Internet connection.

DDNS



Service Type: DynDNS.org

User name:

Password:

Host Name:

WildCard: ○ Enabled ● Disabled

Internet IP Address: 192.168.1.100

Status: DDNS is disabled

DDNS (Dynamic DNS Service) is a system which allows the domain name data held in a name server to be updated in real time. It allows an Internet domain name to be assigned to a computer with a varying (dynamic) IP address. Before you can use this feature, you need to sign up for DDNS service with a DDNS service provider, www.dyndns.org or www.TZO.com.

Service Type: From the drop-down list, select your DDNS service type.

User name: Enter the user name for your DDNS account.

Password: Enter the password for your DDNS account.

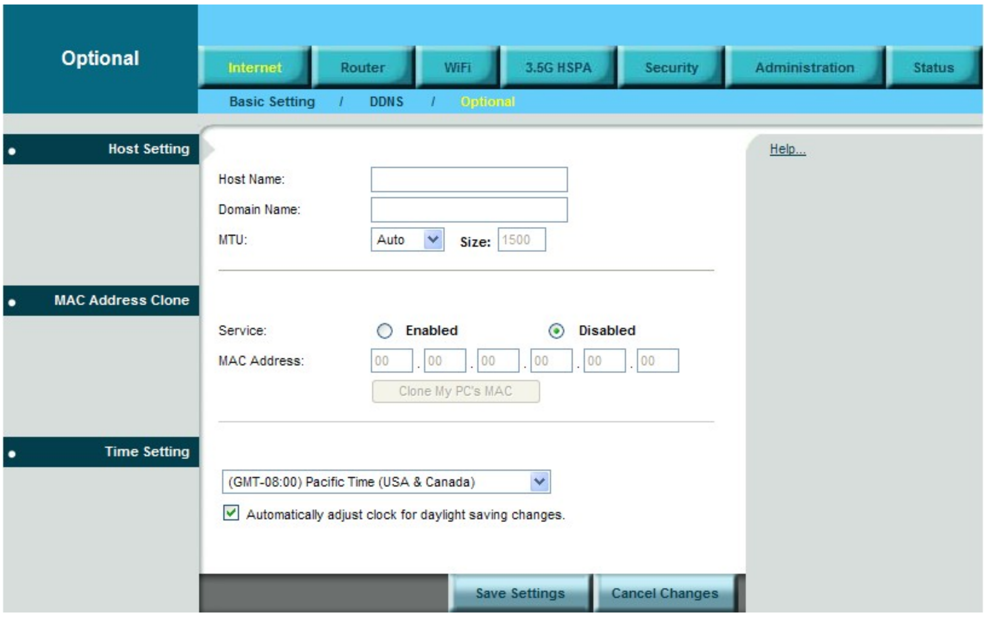
Host name: The Host Name is optional but may be required by some ISPs.

WildCard: Some DDNS servers support the wildcard alias feature which points *.yourhost.dyndns.org to your computers automatically. All aliases for your domain such as www.yourhost.dyndns.org will point to your computer by default due to Wildcard Alias. This allows users to access your computer using all types of derivatives of your domain name.

Internet IP Address: The Router’s Internet IP address is displayed here. Because it is dynamic, it changes.

Status: This shows whether the DDNS service is enabled or disabled.

Optional



Host Name:

Domain Name:

MTU: Auto Size: 1500

Service: ○ Enabled ● Disabled

MAC Address: 00 . 00 . 00 . 00 . 00 . 00

(GMT-08:00) Pacific Time (USA & Canada)

☑ Automatically adjust clock for daylight saving changes.

Host Setting

Host Name and Domain Name

These fields allow you to assign a host and domain name for the Router. Some ISPs require these names as identification. In most cases, leaving the fields blank will work.

MTU

MTU (Maximum Transmission Unit) specifics the largest packet size permitted for Internet transmission. To have the Router select the best MTU for your Internet connection, keep the default setting, Auto.

MAC Address Clone

Some ISPs will require you to register a MAC address in order to access the Internet. If you do not want to re-register the MAC address with your ISP, you can assign the MAC address you have currently registered with your ISP to the Router by clicking the **Clone My PCs MAC** button.

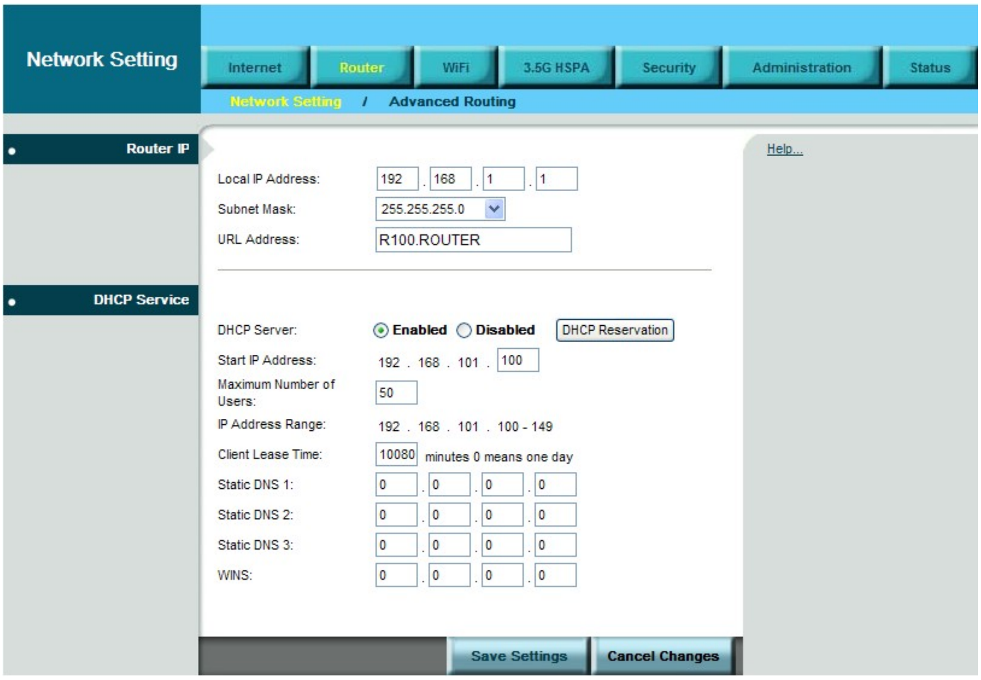
Time Setting

Select the Time Zone from the drop-down menu according to your current location.

Automatically adjust clock for daylight saving changes: Select the checkbox to enable Daylight Saving time.

Router Setup

Network Setting



Local IP Address: 192 . 168 . 1 . 1

Subnet Mask: 255.255.255.0

URL Address: R100.ROUTER

DHCP Server: ● Enabled ○ Disabled

Start IP Address: 192 . 168 . 101 . 100

Maximum Number of Users: 50

IP Address Range: 192 . 168 . 101 . 100 - 149

Client Lease Time: 10080 minutes 0 means one day

Static DNS 1: 0 . 0 . 0 . 0

Static DNS 2: 0 . 0 . 0 . 0

Static DNS 3: 0 . 0 . 0 . 0

WINS: 0 . 0 . 0 . 0

Router IP

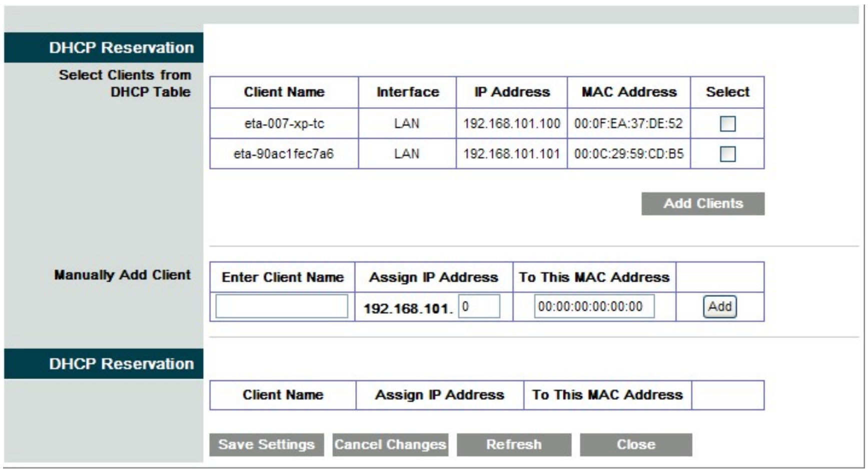
This is the Router’s IP address and subnet mask which is seen in your local network. The default IP address is 192.168.1.1, and the default Subnet Mask is 255.255.255.0. Keeping the default values will work.

DHCP Service

DHCP stands for Dynamic Host Control Protocol. The DHCP Server will automatically assign an IP address to the computers on the LAN/private network. If the Router’s DHCP server option is enabled, make sure there is no other DHCP server on your network.

DHCP Reservation

To assign the same IP address to a PC every time it reboots, click the **DHCP Reservation** button.



Select Clients from DHCP Table

Client Name	Interface	IP Address	MAC Address	Select
eta-007-xp-tc	LAN	192.168.101.100	00:0F:EA:37:DE:52	□
eta-90ac1fec7a6	LAN	192.168.101.101	00:0C:29:59:CD:B5	□

Manually Add Client

Enter Client Name	Assign IP Address	To This MAC Address	
	192.168.101. 0	00:00:00:00:00:00	Add

Client Name	Assign IP Address	To This MAC Address	

A list of DHCP clients is displayed with the following information: Client Name, Interface, IP Address, and MAC Address. Select a checkbox to reserve a client’s IP address. To add clients, click **Add Clients**. To manually assign an IP address, enter the client’s name in the **Enter Client Name** field. Enter an IP address in the **Assign IP Address** field. Enter a MAC Address in the **To This MAC Address** field. Click **Add**. A list of DHCP clients and their fixed local IP addresses is displayed at the bottom of the screen. If you want to remove a client from this list, click **Remove**. To view the most up-to-date information, click **Refresh**.

Start IP Address: Enter a starting IP address for the DHCP server’s IP assignment.

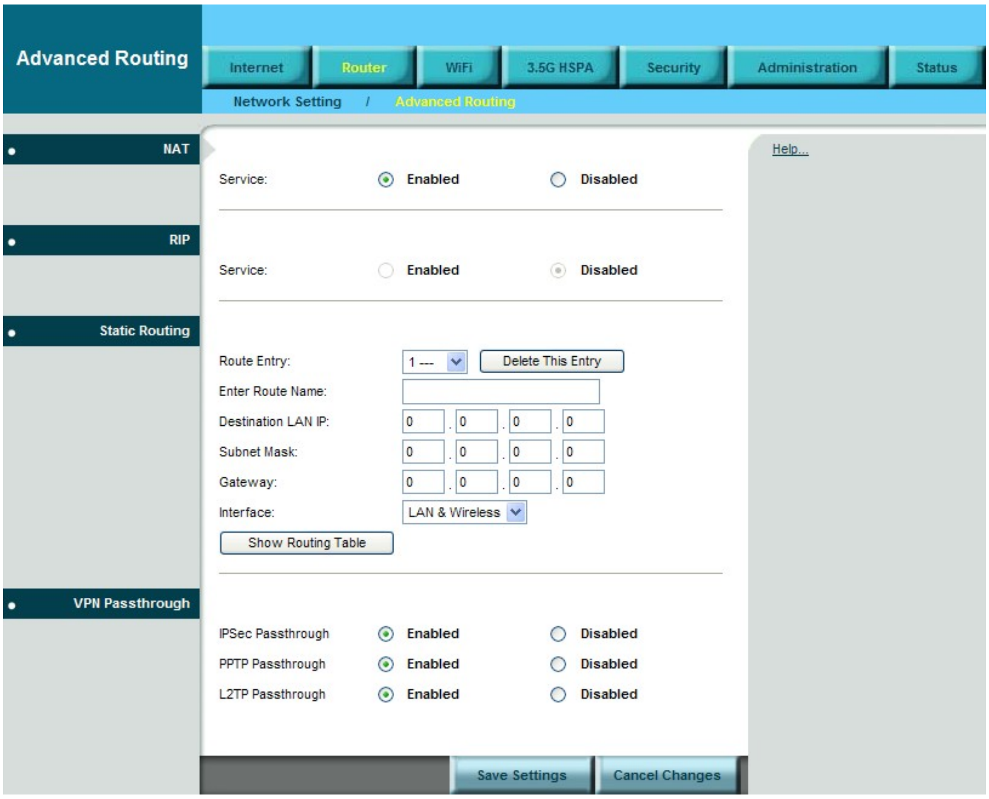
Maximum Number of Users: Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to.

DHCP Lease Time: The length of time for the IP address lease. Enter the lease time in minutes.

Static DNS (1-3): The Domain Name System (DNS) is how the Internet translates domain or website names into Internet addresses or URLs. Your ISP will provide you with at least one DNS Server IP Address. You can enter up to three DNS Server IP Addresses here. The Router will use these for quicker access to functioning DNS servers.

WINS: The Windows Internet Naming Service (WINS) manages each PC's interaction with the Internet. If you use a WINS server, enter that server’s IP Address here. Otherwise, leave this blank.

Advanced Routing



NAT

Service: ● Enabled ○ Disabled

RIP

Service: ○ Enabled ● Disabled

Static Routing

Route Entry: 1 ---

Enter Route Name:

Destination LAN IP: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

Gateway: 0 . 0 . 0 . 0

Interface: LAN & Wireless

VPN Passthrough

IPSec Passthrough ● Enabled ○ Disabled

PPTP Passthrough ● Enabled ○ Disabled

L2TP Passthrough ● Enabled ○ Disabled

NAT Setup

The Network Address Translation (NAT) service is a standard that allows multiple computers on a private network to share a single IP address.

RIP

The **Routing Information Protocol (RIP)** helps the Router dynamically adapt to changes of network connections by communicating information about which networks each Router can reach and how far away those networks are.

Static Routing

This section allows you to define fixed routes to defined destinations.

Route Entry: To set up a static route, select a number from the drop-down list.

Enter Route Name: Enter a name for the route here.

Destination LAN IP: Enter the Destination IP address that will be assigned to a specific network or host.

Subnet Mask: Enter the subnet mask associated with the Destination IP.

Gateway: This is the IP address of the gateway device that allows for contact between the Router and the remote network or host.

Interface: This interface tells you whether the Destination IP Address is on the LAN & Wireless (Ethernet and wireless networks) or the WAN (Internet).

Show Routing Table: Click **Show Routing Table** to open a screen displaying how data is routed through your local network. Click **Refresh** to update the information.

VPN Passthrough

A **Virtual Private Network (VPN)** is a type of secured private network connection, built upon publicly-accessible infrastructure such as the Internet. They usually provide connectivity to various devices behind a gateway or firewall.

IPSec Passthrough

IP Security (IPSec) provides authentication and encryption. Since it is mainly a Layer 3 technology, it can secure all data on the network. To allow IPSec tunnels to pass through the Router, click **Enabled**.

PPTP Passthrough

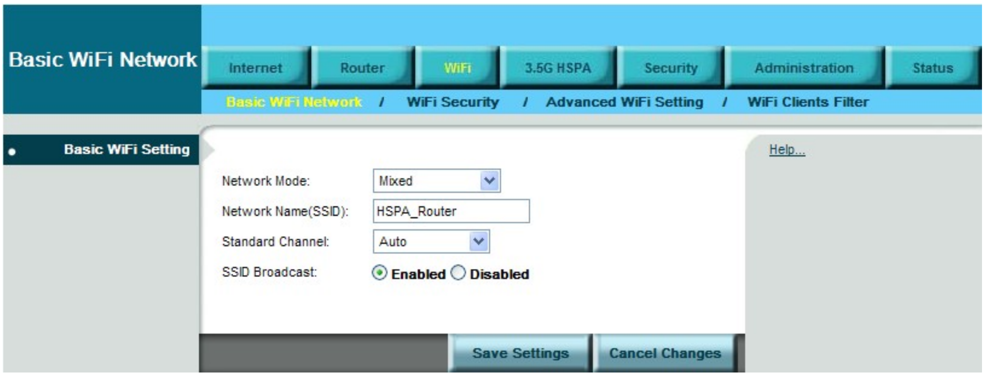
Point-to-Point Tunneling Protocol (PPTP) allows you to establish a connection to an enterprise network. To allow PPTP tunnels to pass through the Router, click **Enabled**.

L2TP Passthrough

Layer 2 Tunneling Protocol (L2TP) is an extension of the Point-to-Point Tunneling Protocol and is also used to establish virtual private networks. To allow L2TP tunnels to pass through the Router, click **Enabled**.

WiFi Setup

Basic WiFi Network



Network Mode: Mixed

Network Name(SSID): HSPA_Router

Standard Channel: Auto

SSID Broadcast: ● Enabled ○ Disabled

Basic WiFi Setting

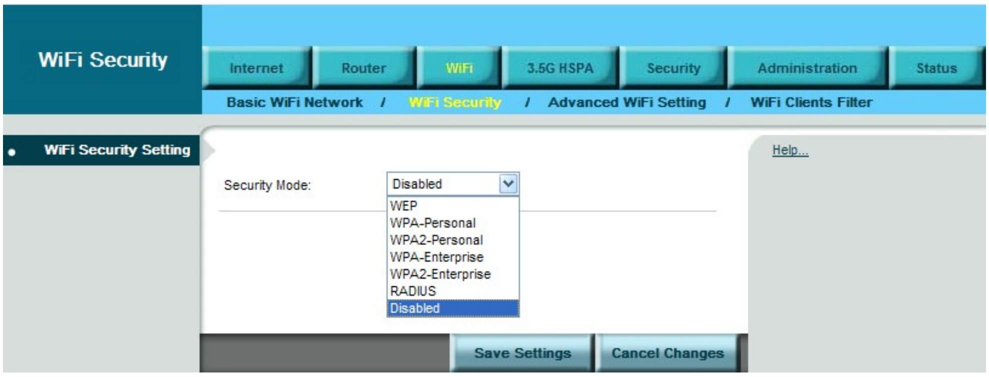
Network Mode: From this drop-down menu, you can select the wireless standards running on your network. If you have both 802.11g and 802.11b devices in your network, keep the default setting, Mixed. If you have only 802.11g devices, select **Wireless-G Only**. If you have only 802.11b devices, select **Wireless-B Only**. If you do not want to use any WiFi network, select **Disabled**.

Network Name (SSID): Network Name is used for identifying the Wireless LAN (WLAN). The default SSID is HSPA_ROUTER.

Standard Channel: The radio channel number. The permissible channels depend on the Regulatory Domain. Keeping the default value.

SSID Broadcast: Disable this function will let your SSID setting not be exposed to view in the air. For security purposes, you may choose to hide your network's SSID by selecting enable from the drop-down list. This will prevent computers scanning for the presence of wireless networks to detect your network name. The default setting is **Enabled**.

WiFi Security

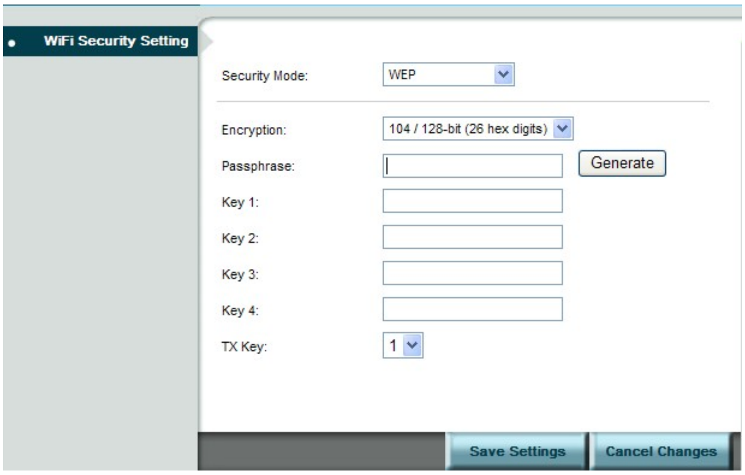


Security Mode: Disabled

WiFi Security Setting

R100 provides several different levels of security to protect your WiFi network. Select a level in the Security Mode drop-down menu.

WEP



Security Mode: WEP

Encryption: 104 / 128-bit (26 hex digits)

Passphrase:

Key 1:

Key 2:

Key 3:

Key 4:

TX Key: 1

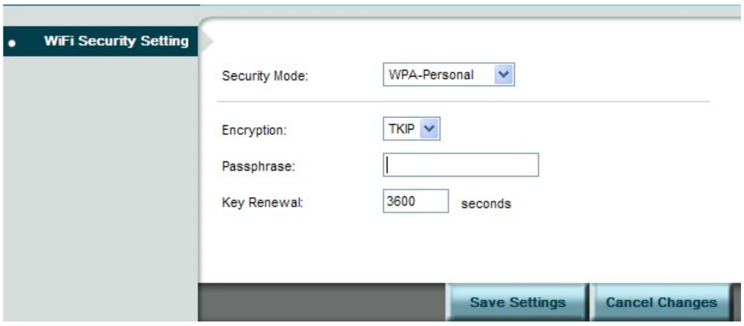
The Router supports two WEP (Wired Equivalent Privacy) standards: 64-bit and 128-bit. Select a standard from the drop-down list. The 64-bits encryption requires 10 hexadecimal digits (letters a-f and numbers 0-9 are valid). The 128-bits encryption requires 26 hexadecimal digits (letters a-f and numbers 0-9 are valid).You can set up to four different keys.

Passphrase: Strings of hexadecimal characters are not easy to remember. This conversion utility converts a simple word or phrase into hex, so that you can easily remember and regenerate the pass-phrase.

TX Key: You can specify which key you want to use for the WiFi network.

WPA, or WiFi Protected Access, is a WiFi standard that was designed to improve the security features of WEP. WPA uses two encryption methods, TKIP and AES, with dynamic keys.

WPA-Personal



WiFi Security Setting

Security Mode: WPA-Personal

Encryption: TKIP

Passphrase:

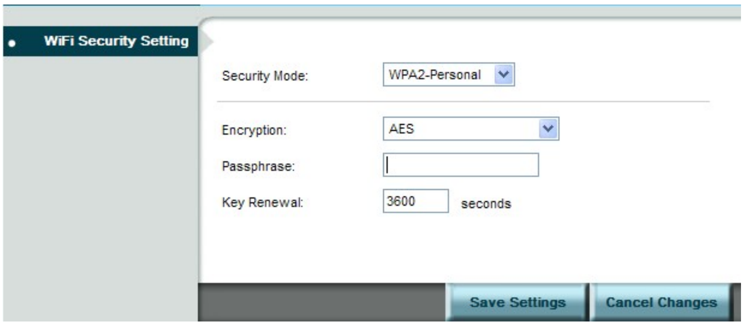
Key Renewal: 3600 seconds

Encryption: Choose **TKIP** or **AES** from the drop down list. (AES is a stronger encryption method than TKIP.)

Passphrase: Enter a passphrase between 8-63 characters.

Key Renewal: Enter a key renewal value to tell the Router how often it should change the encryption keys. The value must be between 60-99999.

WPA2-Personal



WiFi Security Setting

Security Mode: WPA2-Personal

Encryption: AES

Passphrase:

Key Renewal: 3600 seconds

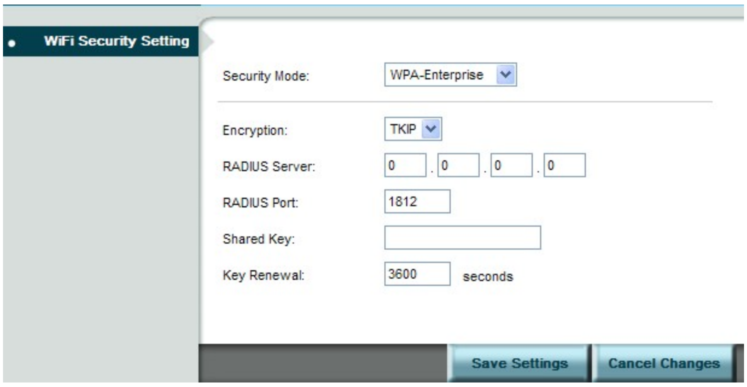
WPA2 is a more advanced, more secure version of WPA.

Encryption: Choose **AES**, or **WPA-TKIP**, or **WPA2-AES** from the drop down list.

Passphrase: Enter a passphrase between 8-63 characters.

Key Renewal: Enter a key renewal value to tell the Router how often it should change the encryption keys. The value must be between 60-99999.

WPA-Enterprise



WiFi Security Setting

Security Mode: WPA-Enterprise

Encryption: TKIP

RADIUS Server: 0 . 0 . 0 . 0

RADIUS Port: 1812

Shared Key:

Key Renewal: 3600 seconds

This option features WPA used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.)

Encryption: Choose **TKIP** or **AES** from the drop down list. (AES is a stronger encryption method than TKIP.)

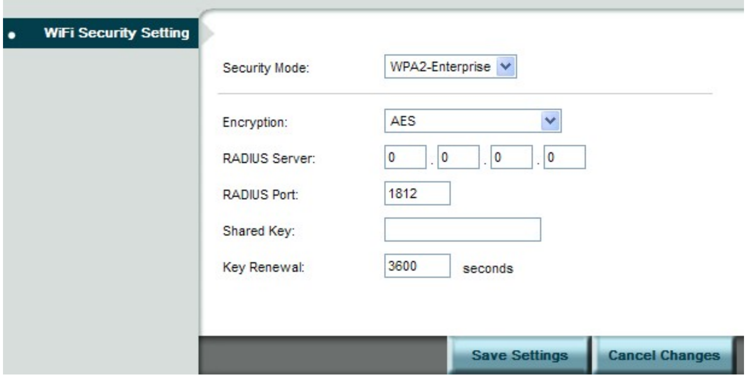
RADIUS Server: Enter the IP Address of the RADIUS server.

RADIUS Port: Enter the port number of the RADIUS server. The default value is 1812.

Shared Key: Enter the key shared between the Router and the server.

Key Renewal: Enter a key renewal value to tell the Router how often it should change the encryption keys. The value must be between 60-99999.

WPA2-Enterprise



WiFi Security Setting

Security Mode: WPA2-Enterprise

Encryption: AES

RADIUS Server: 0 . 0 . 0 . 0

RADIUS Port: 1812

Shared Key:

Key Renewal: 3600 seconds

This option features WPA2 used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.)

Encryption: Choose **AES** or **WPA-TKIP** or **WPA2-AES** from the drop down list.

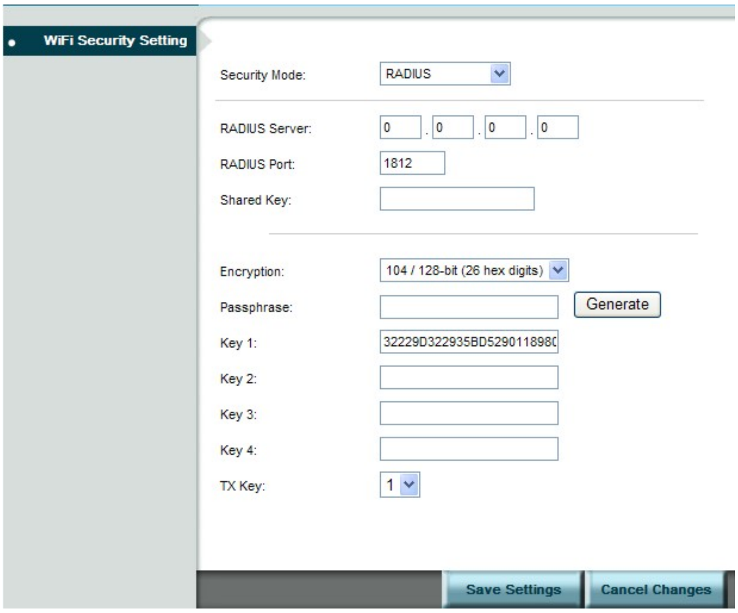
RADIUS Server: Enter the IP Address of the RADIUS server.

RADIUS Port: Enter the port number of the RADIUS server. The default value is 1812.

Shared Key: Enter the key shared between the Router and the server.

Key Renewal: Enter a key renewal value to tell the Router how often it should change the encryption keys. The value must be between 60-99999.

RADIUS



Security Mode: RADIUS

RADIUS Server: 0 . 0 . 0 . 0

RADIUS Port: 1812

Shared Key:

Encryption: 104 / 128-bit (26 hex digits)

Passphrase:

Key 1: 32229D322935BD529011898

Key 2:

Key 3:

Key 4:

TX Key: 1

RADIUS stands for Remote Authentication Dial-In User Service. It is a networking protocol that uses access servers to provide centralized management of access to large networks.

RADIUS Server: Enter the IP Address of the RADIUS server.

RADIUS Port: Enter the port number of the RADIUS server. The default value is 1812.

Shared Key: Enter the key shared between the Router and the server.

Encryption: Select either 64-bits or 128-bits from the drop-down list The 64-bits encryption requires 10 hexadecimal digits. The 128-bits encryption requires 26 hexadecimal digits .You can set up to four different keys.

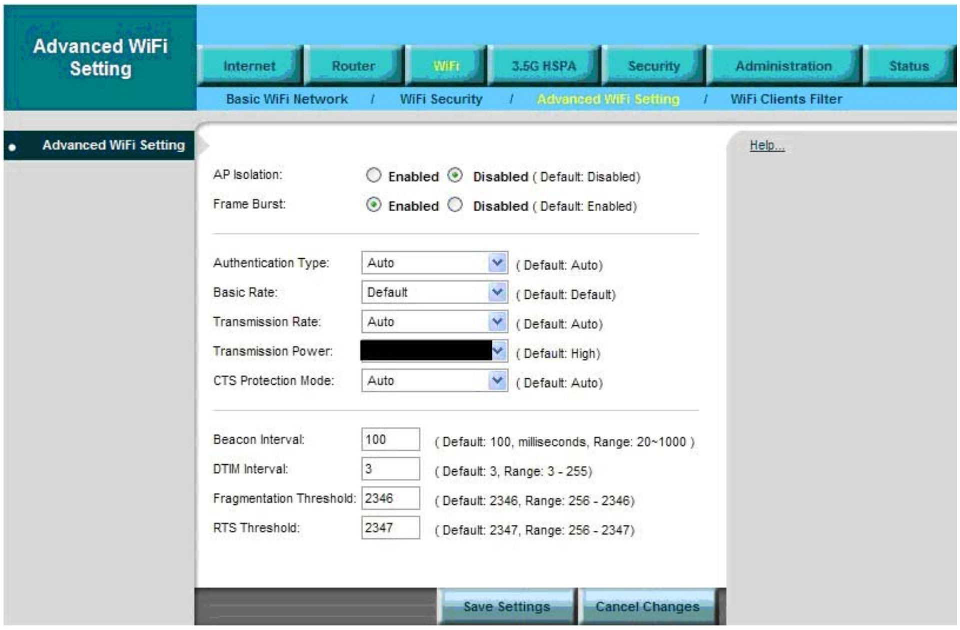
Passphrase: Strings of hexadecimal characters are not easy to remember. This conversion utility converts a simple word or phrase into hex, so that you can easily remember and regenerate the pass-phrase.

TX Key: You can specify which key you want to use for the WiFi network.

Disabled

If you do not want to use any security method for your wireless network, choose **Disabled**.

Advanced WiFi Setting



AP Isolation: ○ Enabled ● Disabled (Default: Disabled)

Frame Burst: ● Enabled ○ Disabled (Default: Enabled)

Authentication Type: Auto (Default: Auto)

Basic Rate: Default (Default: Default)

Transmission Rate: Auto (Default: Auto)

Transmission Power: [redacted] (Default: High)

CTS Protection Mode: Auto (Default: Auto)

Beacon Interval: 100 (Default: 100, milliseconds, Range: 20~1000)

DTIM Interval: 3 (Default: 3, Range: 3 - 255)

Fragmentation Threshold: 2346 (Default: 2346, Range: 256 - 2346)

RTS Threshold: 2347 (Default: 2347, Range: 256 - 2347)

AP Isolation: This isolates all wireless clients and wireless devices on your network from each other. Wireless devices will be able to communicate with the Router but not with each other.

Frame Burst: Enabling this option may provide your network with greater performance.

Authentication Type: The default is Open System authentication, where the sender and the recipient do not use a WEP key for authentication. To use a WEP key for authentication, select Shared Key.

Basic Rate: The Basic Rate setting is not actually one rate of transmission but a series of rates at which the Router can transmit. The Router advertises its Basic Rate to the other wireless devices in your network, so they know which rates are used. The Router also advertises that automatically selects the best rate for transmission. The default setting is **Auto**, where the Router can transmit at all standard wireless rates. The Basic Rate is not the actual rate of data transmission. If you want to specify the Router’s rate of data transmission, configure the **Transmission Rate** setting.

Transmission Rate: The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds.

CTS Protection Mode: CTS (Clear To Send) is a function used to minimize collisions among wireless devices on a wireless local area network (LAN). The default setting is **Auto** and the Router automatically uses CTS Protection Mode when your Wireless-G products are experiencing severe problems and are not able to transmit to the Router in an environment with heavy traffic. This function boosts the Router's ability to catch all Wireless-B and Wireless-G transmissions, but it severely decreases performance.

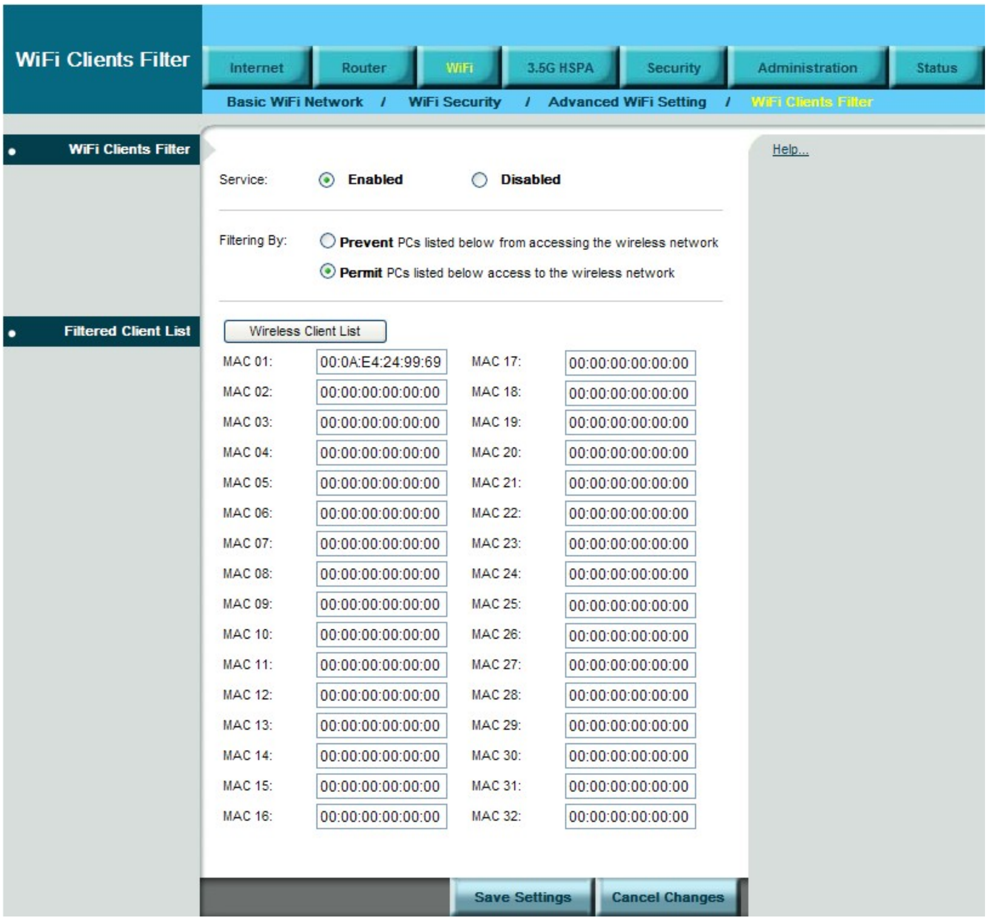
Beacon interval: Beacons are packets sent by an Access Point to synchronize a wireless network. Specify a value. 100 is the default setting.

DTIM Interval: The default setting for DTIM (Delivery Traffic Indication Message) is 3. A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.

Fragmentation Threshold: The fragmentation threshold, which is specified in bytes, determines whether packets will be fragmented. Packets exceeding the setting value will be fragmented before transmission. 2346 is the default setting.

RTS Threshold: This value should remain at its default setting of 2347. If inconsistent data flow is a problem, only a minor modification should be made.

WiFi Clients Filter



Service: ● **Enabled** ○ **Disabled**

Filtering By: ○ **Prevent** PCs listed below from accessing the wireless network
● **Permit** PCs listed below access to the wireless network

MAC 01:	00:0A:E4:24:99:69	MAC 17:	00:00:00:00:00:00
MAC 02:	00:00:00:00:00:00	MAC 18:	00:00:00:00:00:00
MAC 03:	00:00:00:00:00:00	MAC 19:	00:00:00:00:00:00
MAC 04:	00:00:00:00:00:00	MAC 20:	00:00:00:00:00:00
MAC 05:	00:00:00:00:00:00	MAC 21:	00:00:00:00:00:00
MAC 06:	00:00:00:00:00:00	MAC 22:	00:00:00:00:00:00
MAC 07:	00:00:00:00:00:00	MAC 23:	00:00:00:00:00:00
MAC 08:	00:00:00:00:00:00	MAC 24:	00:00:00:00:00:00
MAC 09:	00:00:00:00:00:00	MAC 25:	00:00:00:00:00:00
MAC 10:	00:00:00:00:00:00	MAC 26:	00:00:00:00:00:00
MAC 11:	00:00:00:00:00:00	MAC 27:	00:00:00:00:00:00
MAC 12:	00:00:00:00:00:00	MAC 28:	00:00:00:00:00:00
MAC 13:	00:00:00:00:00:00	MAC 29:	00:00:00:00:00:00
MAC 14:	00:00:00:00:00:00	MAC 30:	00:00:00:00:00:00
MAC 15:	00:00:00:00:00:00	MAC 31:	00:00:00:00:00:00
MAC 16:	00:00:00:00:00:00	MAC 32:	00:00:00:00:00:00

WiFi Clients Filter

You can allow or deny specific users to access your wireless network by using the WiFi Clients Filter.

Service: To use the WiFi Clients Filter, select Enabled. To disable it, select **Disabled**.

Filtering By: You can filter users by two methods: **Prevent** the listed PCs from accessing the wireless network, or **Permit** the listed PCs to access the wireless network. Select the method you want.

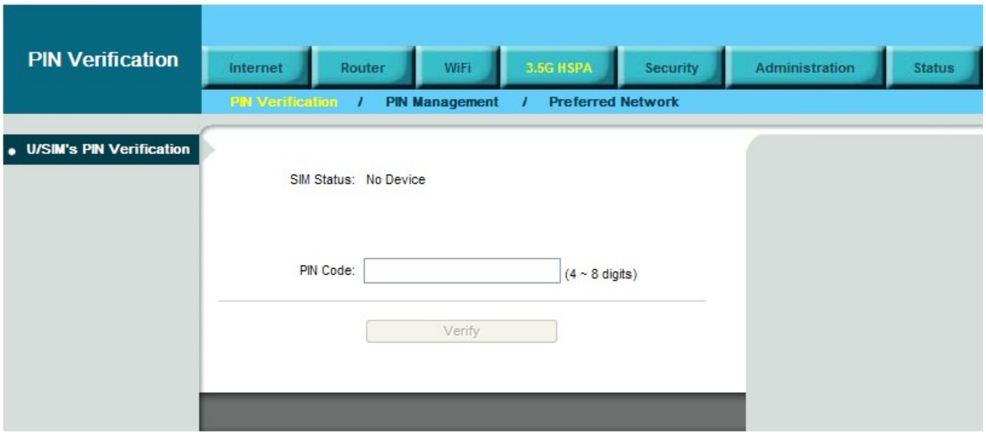
Filtered Client List

Enter MAC addresses in the Filtered Client List section, and click **Save Settings**.

To display a list of network users, click **Wireless Client List**.

3.5G HSPA Setup

PIN Verification

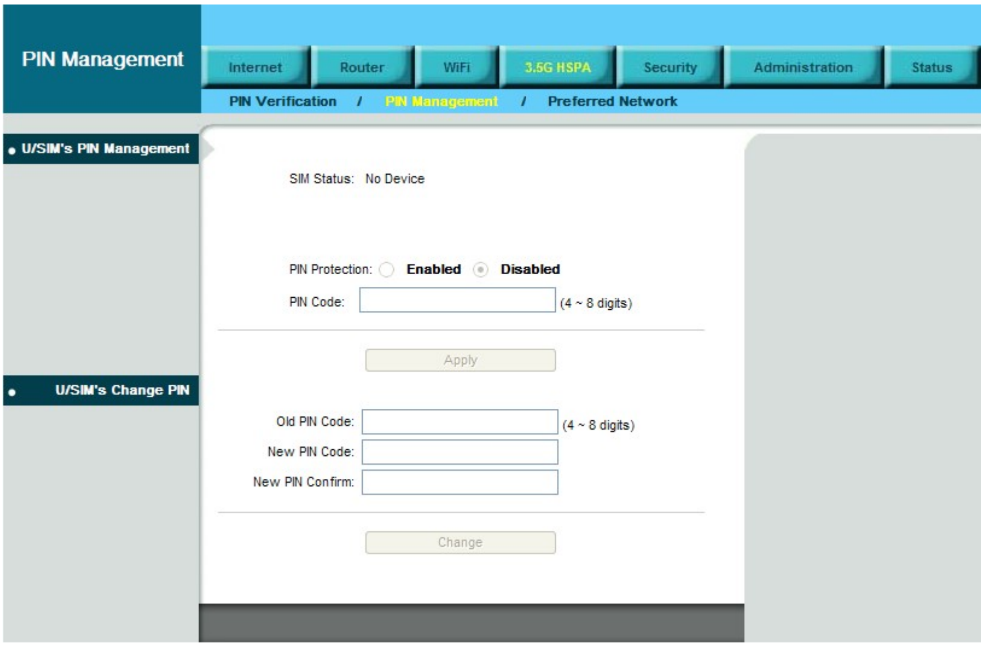


SIM Status: No Device

PIN Code: (4 ~ 8 digits)

After the Router is connected to the HSDPA ExpressCard, if your SIM card PIN protection is enabled, you must enter the PIN code for verification. Enter the code in the PIN Code field, and click **Verify**.

PIN Management



SIM Status: No Device

PIN Protection: ○ Enabled ● Disabled

PIN Code: (4 ~ 8 digits)

Old PIN Code: (4 ~ 8 digits)

New PIN Code:

New PIN Confirm:

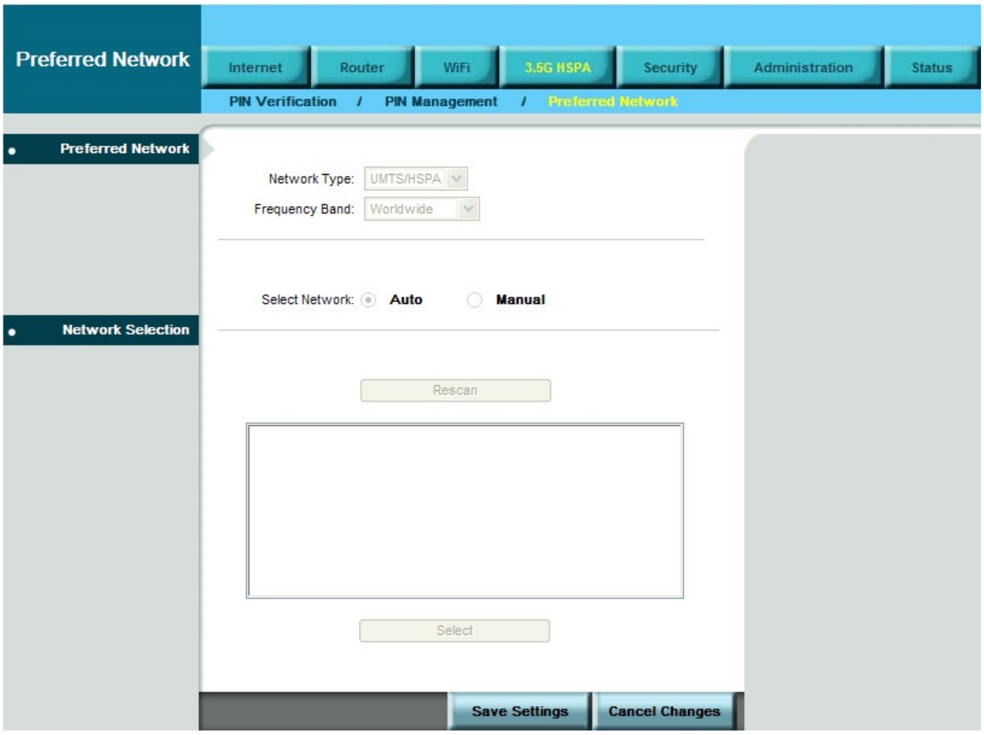
U/SIM's PIN Management

After your SIM card is verified, you can enable or disable the PIN protection on your SIM card. Select **Enabled** or **Disabled**, and click **Apply**.

U/SIM's Change PIN

You can change the PIN code on the SIM card. Enter your original PIN code in the **Old PIN Code** field, enter the new PIN code in the **New PIN Code** field and the **New PIN Confirm** field, and click **Change**.

Preferred Network



Network Type: UMTS/HSPA

Frequency Band: Worldwide

Select Network: ● Auto ○ Manual

Preferred Network

Network Type: In the drop-down menu, select the network type your SIM card supports. If you do not know the network type, select **Auto**.

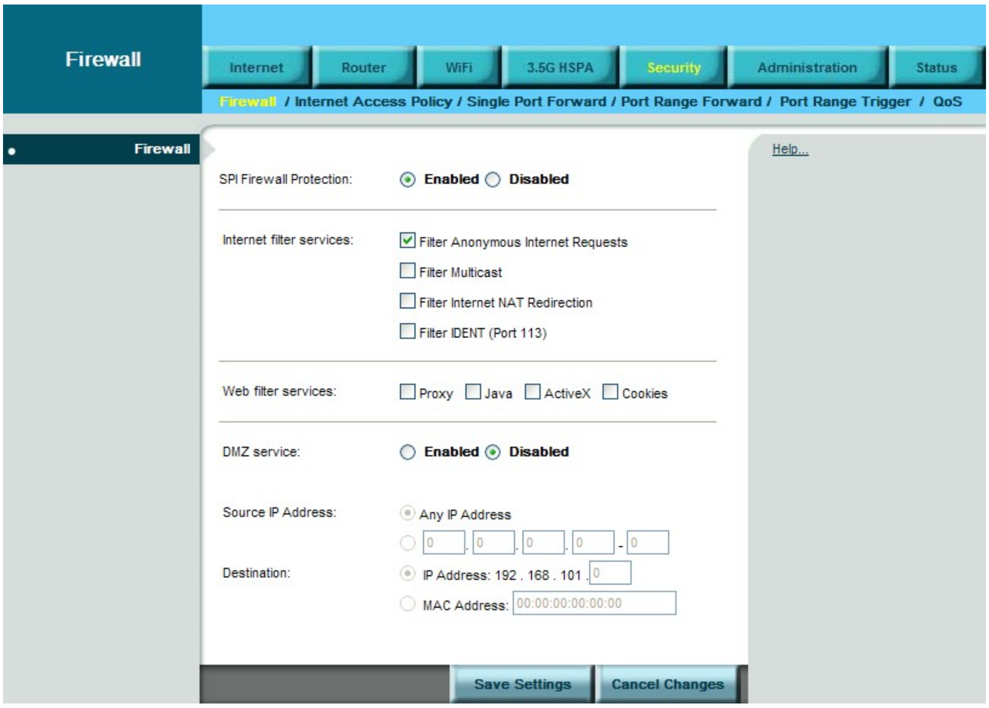
Frequency Band: Frequency band is the radio spectrum frequency designated by the ITU for the operation of the GSM for mobile phones. To accelerate the band search, choose one of the options from the drop-down list according to your location (worldwide, Europe/Asia, or North America). If you do not know the frequency band, select the **Worldwide**.

Network Selection

To select the mobile network operator automatically, in the **Select Network** field, select **Auto**. To select the operator from a list, select **Manual** and click **Rescan**. The list is displayed below. Select the mobile network operator you are currently using on your SIM card.

Security Setup

Firewall



SPI Firewall Protection: ● Enabled ○ Disabled

Internet filter services: ☑ Filter Anonymous Internet Requests
□ Filter Multicast
□ Filter Internet NAT Redirection
□ Filter IDENT (Port 113)

Web filter services: □ Proxy □ Java □ ActiveX □ Cookies

DMZ service: ○ Enabled ● Disabled

Source IP Address: ● Any IP Address
○ 0 . 0 . 0 . 0 - 0

Destination: ● IP Address: 192 . 168 . 101 . 0
○ MAC Address: 00:00:00:00:00:00

Firewall

This tab is used to configure a firewall that filters out various types of unwanted traffic on the Router's local network.

SPI Firewall Protection

The SPI (stateful packet inspection) firewall is programmed to recognize legitimate packets for different types of connections. Only packets matching a known connection state will be allowed by the firewall; others will be rejected.

Internet filter services

Filter Anonymous Internet Requests: This feature makes it more difficult for outside users to work their way into your network.

Filter Multicast: Multicasting allows for multiple transmissions to specific recipients at the same time. If multicasting is permitted, the Router allows IP multicast packets to be forwarded to the appropriate computers.

Filter Internet NAT Redirection: To use port forwarding to block access to local servers from local networked computers, select **Filter Internet NAT Redirection**.

Filter IDENT (Port 113): This feature keeps port 113 from being scanned by devices outside of your local network.

Web filter services

Using the Web Filters feature, you may enable up to four specific filtering methods.

Proxy: Use of WAN proxy servers may compromise the Router's security. Select this option to disable access to any WAN proxy servers.

Java: Java is a programming language for websites. Select this option to disable Java. If you disable Java, you run the risk of not having access to Internet sites created using this programming language.

ActiveX: ActiveX is a programming language for websites. Select this option to disable ActiveX. If you disable ActiveX, you run the risk of not having access to Internet sites created using this programming language.

Cookies: A cookie is data stored on your PC and used by Internet sites when you interact with them. Select this option to disable cookies.

DMZ service

When a firewall is used, it is sometimes necessary to place some clients (for example Internet games, video conferencing, or VPN connections) outside of the firewall while leaving the others protected. You can do this using a Demilitarized Zone. This feature allows you to specify the IP address of the computers that are placed outside the firewall of your network.

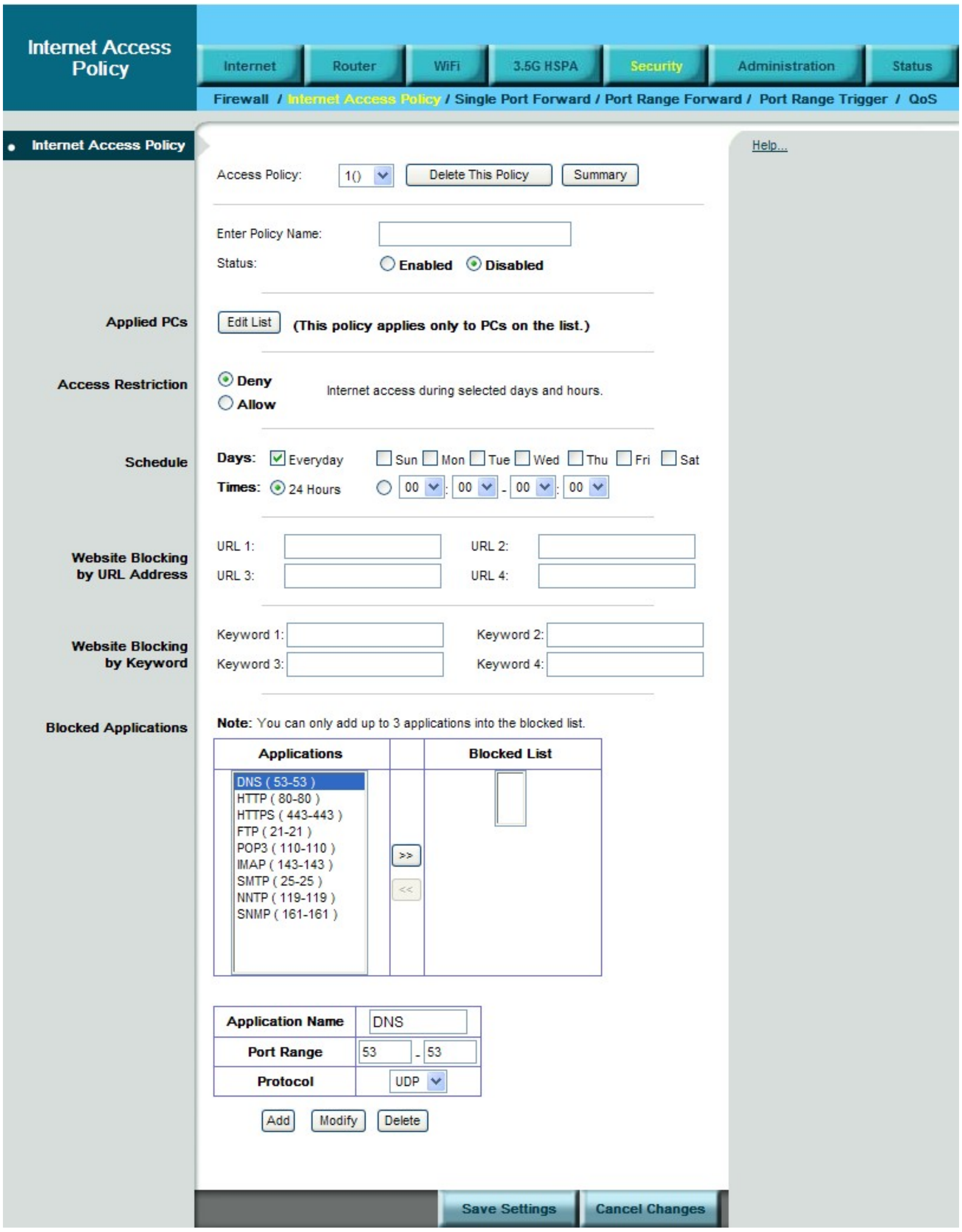
Source IP Address

If you want to allow any Internet IP address to access the exposed computer, select **Any IP Address**. If you want to allow a specific IP address or range of IP addresses to access the exposed computer, select the second option and enter the IP address or range of IP addresses in the fields provided.

Destination

Enter the IP address or MAC address of the computer you want to expose.

Internet Access Policy



Access Policy: 1() [Delete This Policy] [Summary]

Enter Policy Name:

Status: ○ Enabled ● Disabled

Applied PCs [Edit List] (This policy applies only to PCs on the list.)

Access Restriction ● Deny ○ Allow Internet access during selected days and hours.

Schedule
Days: ☑ Everyday □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat
Times: ● 24 Hours ○ 00 : 00 - 00 : 00

Website Blocking by URL Address
URL 1: URL 2:
URL 3: URL 4:

Website Blocking by Keyword
Keyword 1: Keyword 2:
Keyword 3: Keyword 4:

Blocked Applications
Note: You can only add up to 3 applications into the blocked list.

Applications		Blocked List
DNS (53-53) HTTP (80-80) HTTPS (443-443) FTP (21-21) POP3 (110-110) IMAP (143-143) SMTP (25-25) NNTP (119-119) SNMP (161-161)	>> <<	

Application Name	DNS
Port Range	53 - 53
Protocol	UDP

[Add] [Modify] [Delete]

[Save Settings] [Cancel Changes]

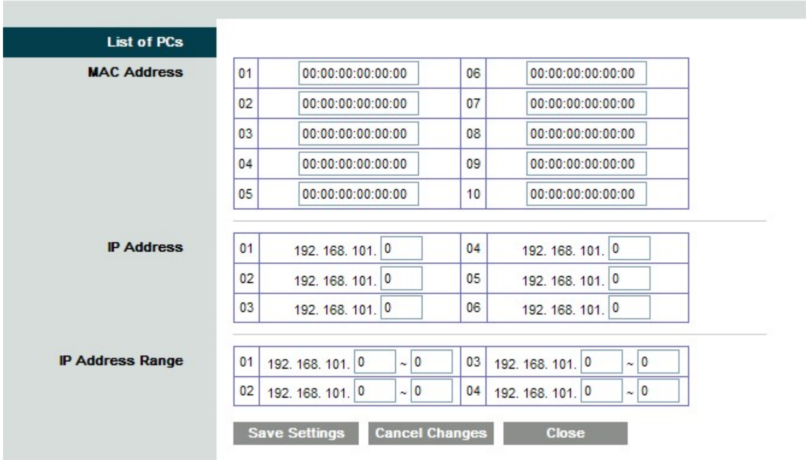
Access can be managed by a policy. Use the settings on this screen to establish and access policies. To display a policy’s settings, select the policy from the drop-down menu. To delete a policy, select the policy’s number and click **Delete This Policy**. To view all the policies, click **Summary**. To delete multiple policies, in the Summary screen, selecting the policies and click **Delete**).

To create an Internet access policy:

1. Select a number from the **Access Policy** dropdown menu.

2. Enter a policy name in the field provided.

3. To enable the policy, select **Enabled**.



List of PCs

MAC Address

01	00:00:00:00:00:00	06	00:00:00:00:00:00
02	00:00:00:00:00:00	07	00:00:00:00:00:00
03	00:00:00:00:00:00	08	00:00:00:00:00:00
04	00:00:00:00:00:00	09	00:00:00:00:00:00
05	00:00:00:00:00:00	10	00:00:00:00:00:00

IP Address

01	192. 168. 101. 0	04	192. 168. 101. 0
02	192. 168. 101. 0	05	192. 168. 101. 0
03	192. 168. 101. 0	06	192. 168. 101. 0

IP Address Range

01	192. 168. 101. 0 ~ 0	03	192. 168. 101. 0 ~ 0
02	192. 168. 101. 0 ~ 0	04	192. 168. 101. 0 ~ 0

4. To select which PCs are affected by the policy, click **Edit List**. The List of PCs screen appears. You can select a PC by MAC Address or IP Address. You can also enter a range of IP Addresses if you want the policy to affect a group of PCs. After making your changes, click **Save Settings** to apply your changes or **Cancel Changes** to cancel your changes. Then click **Close**.

5. Select the appropriate option, Deny or Allow, depending on whether you want to block or allow Internet access for the PCs you listed on the List of PCs screen.

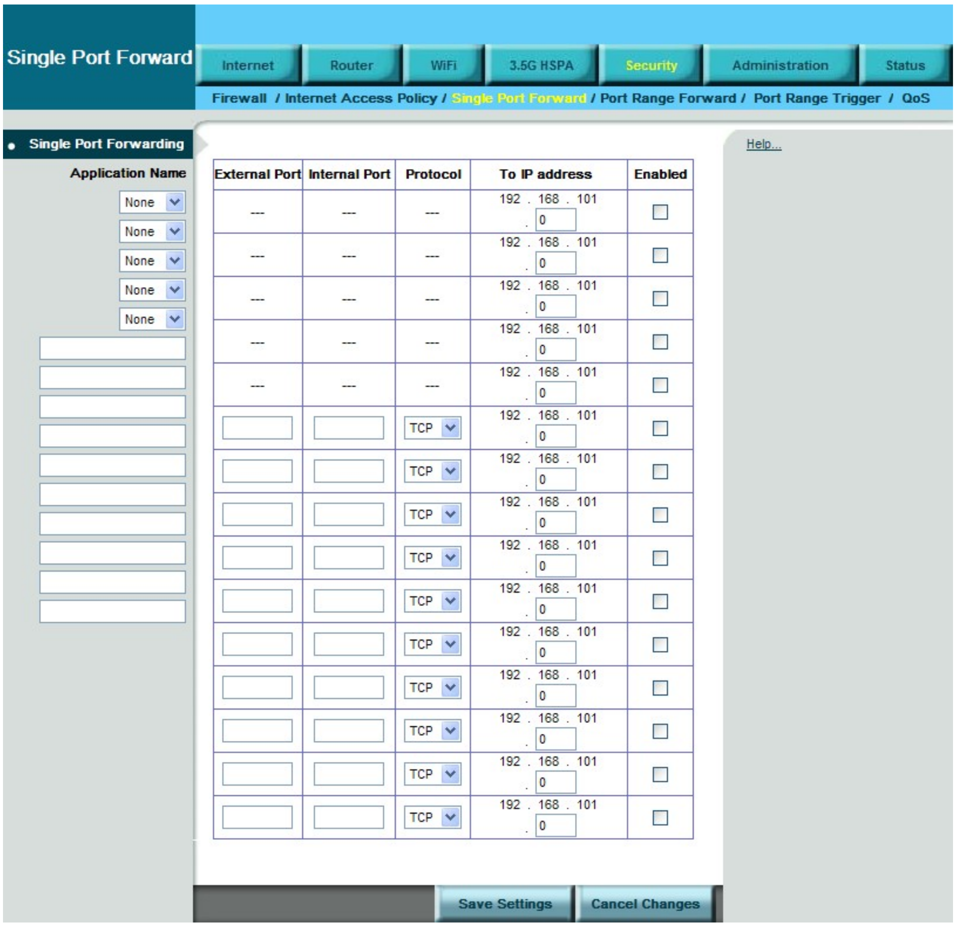
6. Decide which days and what times you want this policy to be enforced. Select the individual days during which the policy will be in effect, or select **Everyday**. To set times for the policy, select **24 Hours**, and enter the times you want.

7. To filter websites by URL, enter URLs in the **Website Blocking by URL Address** fields. To filter websites by keywords, enter keywords in the **Website Blocking by Keyword** fields.

8. To filter access to various services accessed over the Internet, such as FTP or telnet, select services in the **Applications** column, and click **Add** to add them to the Blocked List. (You can only add up to 3 applications.) You can also add an application into the **Applications** column. Enter the information in the **Application Name**, **Port Range**

and **Protocol** fileds, and click **Add**.

Single Port Forward



Application Name	External Port	Internal Port	Protocol	To IP address	Enabled
None	---	---	---	192 . 168 . 101 . 0	□
None	---	---	---	192 . 168 . 101 . 0	□
None	---	---	---	192 . 168 . 101 . 0	□
None	---	---	---	192 . 168 . 101 . 0	□
None	---	---	---	192 . 168 . 101 . 0	□
			TCP	192 . 168 . 101 . 0	□
			TCP	192 . 168 . 101 . 0	□
			TCP	192 . 168 . 101 . 0	□
			TCP	192 . 168 . 101 . 0	□
			TCP	192 . 168 . 101 . 0	□
			TCP	192 . 168 . 101 . 0	□
			TCP	192 . 168 . 101 . 0	□
			TCP	192 . 168 . 101 . 0	□
			TCP	192 . 168 . 101 . 0	□
			TCP	192 . 168 . 101 . 0	□

Single Port Forwarding

Port Forwarding allows you to set up public services on your network, such as web servers, ftp servers, e-mail servers, and other specialized Internet applications. To forward a port, enter the information in each field.

Application Name: You can select an application from the 10 preset applications in the drop-down menu. For custom applications, enter the name of your application in one of the available fields.

External Port: Enter the port number of external ports used by the server or Internet application.

Internal Port: Enter the port number of internal ports used by the server or Internet application.

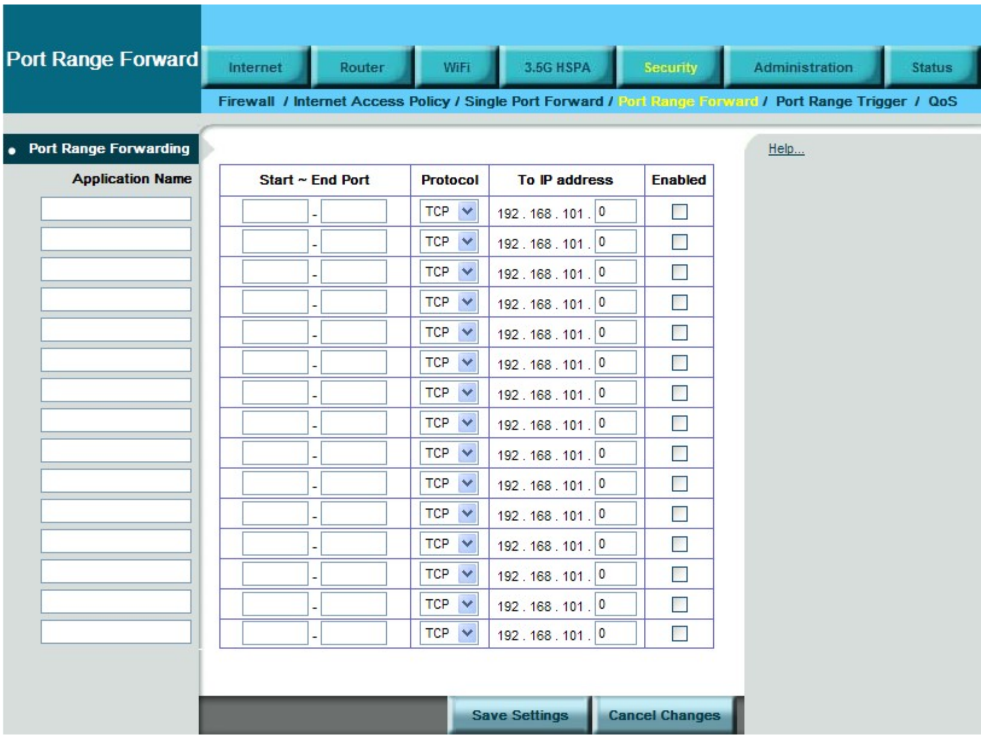
Protocol: Select the protocol used for this application: TCP, UDP, or Both.

To IP address: For each application, enter the IP address of the PC running the specific application.

Enabled: To enable port forwarding for the application, select **Enabled**.

To apply the changes, click **Save Settings**.

Port Range Forward



Application Name	Start ~ End Port	Protocol	To IP address	Enabled
	-	TCP	192 . 168 . 101 . 0	□
	-	TCP	192 . 168 . 101 . 0	□
	-	TCP	192 . 168 . 101 . 0	□
	-	TCP	192 . 168 . 101 . 0	□
	-	TCP	192 . 168 . 101 . 0	□
	-	TCP	192 . 168 . 101 . 0	□
	-	TCP	192 . 168 . 101 . 0	□
	-	TCP	192 . 168 . 101 . 0	□
	-	TCP	192 . 168 . 101 . 0	□
	-	TCP	192 . 168 . 101 . 0	□
	-	TCP	192 . 168 . 101 . 0	□
	-	TCP	192 . 168 . 101 . 0	□
	-	TCP	192 . 168 . 101 . 0	□
	-	TCP	192 . 168 . 101 . 0	□
	-	TCP	192 . 168 . 101 . 0	□

Port Range Forwarding

Port Range Forwarding allows you to set up public services on your network, such as web servers, ftp servers, e-mail servers, and other specialized Internet applications.

Application Name: Enter the name of your application.

Start - End Port: Enter the number that starts the port range in the left field and the number that ends the range in the right field.

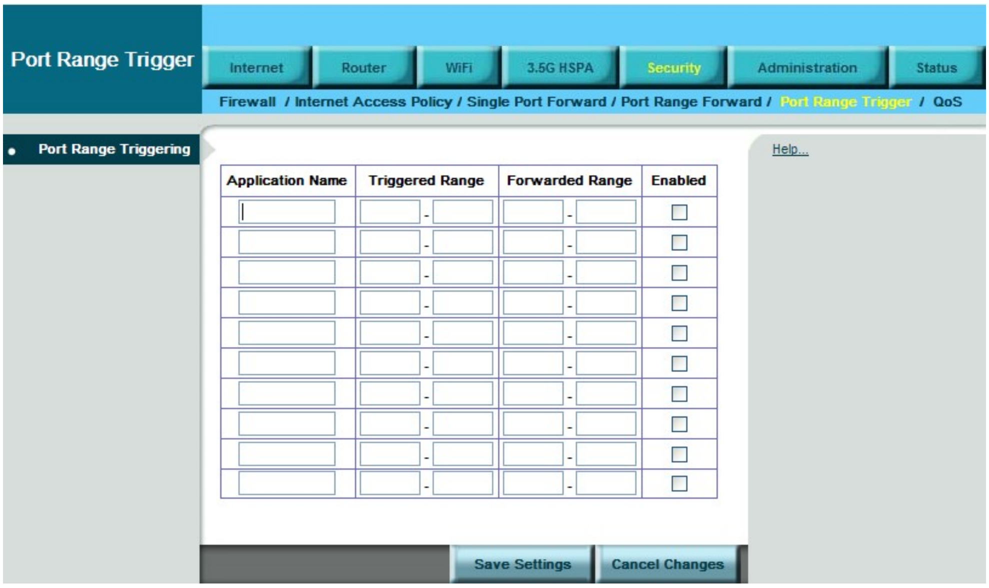
Protocol: Select the protocol used for this application: **TCP**, **UDP**, or **Both**.

To IP address: For each application, enter the IP address of the PC running the specific application.

Enabled: To enable port forwarding for the application, click the **Enabled** checkbox to enable port forwarding for the relevant application.

To apply the changes, click **Save Settings**.

Port Range Trigger



Application Name	Triggered Range	Forwarded Range	Enabled
	-	-	□
	-	-	□
	-	-	□
	-	-	□
	-	-	□
	-	-	□
	-	-	□
	-	-	□
	-	-	□
	-	-	□

Port Range Triggering

This feature allows the Router to watch outgoing data for specific port numbers. The Router remembers the IP address of the computer that sends the matching data, so that when the requested data returns through the Router, the data is pulled back to the proper computer by way of IP address and port mapping rules.

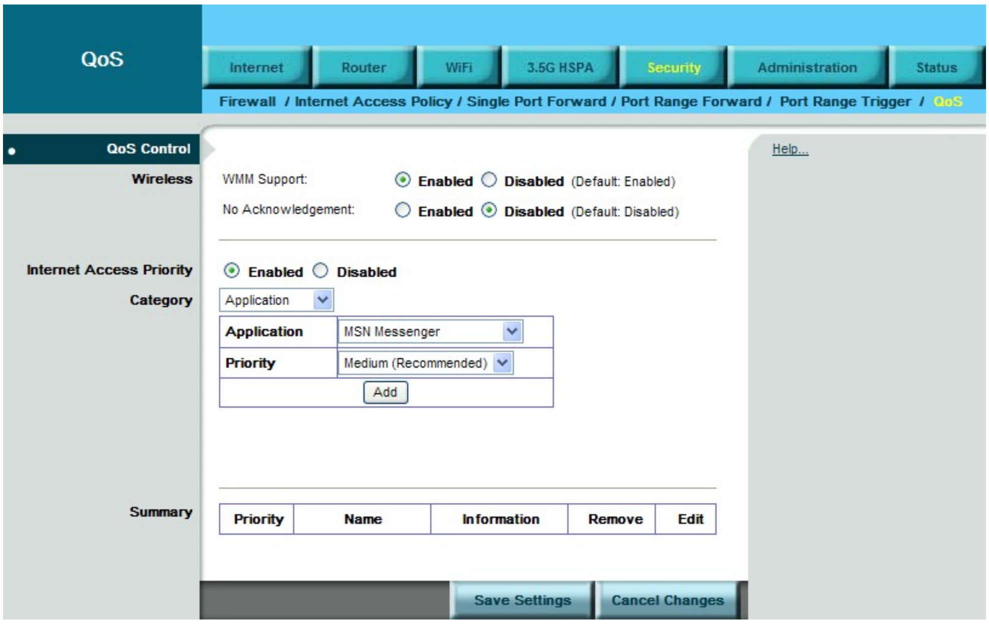
Application Name: Enter the application name of the trigger.

Triggered Range: For each application, enter the triggered port number range. Check with the Internet application documentation for the port number needed. Enter the starting port number of the Triggered Range in the left field. Enter the ending port number of the Triggered Range in the right field.

Forwarded Range: For each application, enter the forwarded port number range. Check with the Internet application documentation for the port number needed. Enter the ending port number of the Triggered Range in the right field.

Enabled: To enable port triggering for the application, select **Enabled**.

QoS



Wireless

WMM Support: ● Enabled ○ Disabled (Default: Enabled)

No Acknowledgement: ○ Enabled ● Disabled (Default: Disabled)

Internet Access Priority: ● Enabled ○ Disabled

Category: Application

Application	MSN Messenger
Priority	Medium (Recommended)

Summary

Priority	Name	Information	Remove	Edit

QoS Control

Quality of service is the ability to provide different priorities to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow.

Wireless

WMM Support: If no devices on your network support WMM, select **Disabled**. Otherwise, keep the default, **Enabled**.

No Acknowledgement: If the Router's Acknowledgement feature is disabled, the Router will not re-send data if an error occurs, then keep the default, **Disabled**. Otherwise, select **Enabled**.

Internet Access Priority

You can set the Internet bandwidth priority for a variety of applications and devices. There are four levels priority: **High**, **Medium**, **Normal**, and **Low**. To use the Internet Access policies you set, select **Enabled**.

Category

There are four categories available. Select one of the categories and proceed to the instructions for your selection.

To add an online games or applications:

1. Select the appropriate online games or applications.

2. Select the appropriate priority: **High**, **Medium**, **Normal**, or **Low**.

3. Click **Add** to save your changes.

To add a new online games or applications:

1. Select **Add a New Game/Application**.

2. Enter any name to indicate the name of the entry.

3. Enter the port range that the application will be using. You can have up to three ranges to define for this bandwidth allocation. Port numbers can range from 1 to 65535.

4. Select the protocol **TCP** or **UDP**, or select **Both**.

5. Select the appropriate priority: **High**, **Medium**, **Normal**, or **Low**.

6. Click **Add** to save your changes.

To add an MAC address:

1. Enter a name for your device.

2. Enter the MAC address of your device.

3. Select the appropriate priority: **High**, **Medium**, **Normal**, or **Low**.

4. Click **Add** to save your changes.

To add a Voice Device:

1. Enter a name for your voice device.

2. Enter the MAC address of your voice device.

3. Select the appropriate priority: **High**, **Medium**, **Normal**, or **Low**.

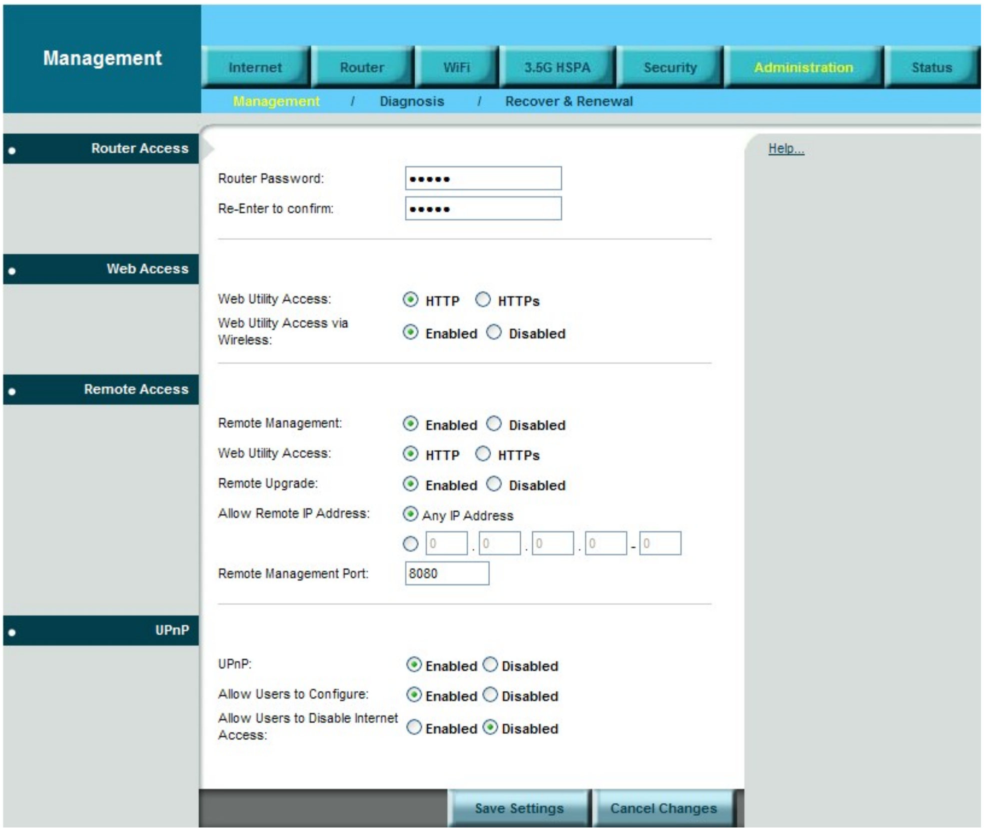
4. Click **Add** to save your changes.

Summary

This lists the QoS entries you have created for your applications and devices. Select **Edit** to edit an item or **Remove** to remove the item. Preset items cannot be edited.

Administration Setup

Management



Router Password: •••••

Re-Enter to confirm: •••••

Web Utility Access: ● HTTP ○ HTTPs

Web Utility Access via Wireless: ● Enabled ○ Disabled

Remote Management: ● Enabled ○ Disabled

Web Utility Access: ● HTTP ○ HTTPs

Remote Upgrade: ● Enabled ○ Disabled

Allow Remote IP Address: ● Any IP Address

○ 0 . 0 . 0 . 0 - 0

Remote Management Port: 8080

UPnP: ● Enabled ○ Disabled

Allow Users to Configure: ● Enabled ○ Disabled

Allow Users to Disable Internet Access: ○ Enabled ● Disabled

Router Access

You can change the Router's password here. Enter the password you want to set in the **Router Password** field, and re-enter it in the **Re-Enter to confirm** field. Then click **Save Settings**.

Web Access

Web Utility Access: HTTP (HyperText Transport Protocol) is the communications protocol used to connect to servers on the World Wide Web. **HTTPs** uses SSL (Secured Socket Layer) to encrypt data transmitted for higher security.

Web Utility Access via Wireless: If you are using the Router in a public domain where you are giving wireless access to your guests, you can disable wireless access to the Router's web-based utility. The wireless access to the Router web-based utility can be disabled. If you disable the setting, you are only able to access the web-based utility via a wired connection.

Remote Access

Remote Management: To access the Router remotely, from outside the network, select **Enabled**.

Web Utility Access: Choose to access the Router via **HTTP** or **HTTPs**.

Remote Upgrade: To enable remote upgrade of the Router, select **Enabled**.

Allow Remote IP Address: To allow any IP address to access to access the Router, select Any IP Address. To allow a specific range of IP addresses to access the Router, enter IP addresses.

Remote Management Port: Enter the port number that will be open to outside access.

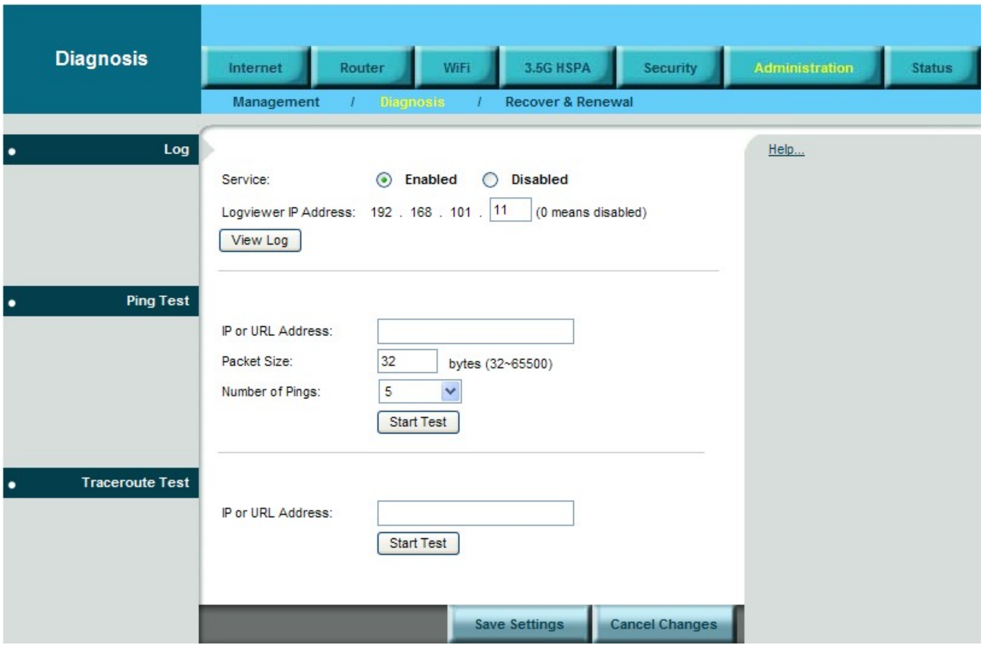
UPnP

UPnP: Universal Plug and Play (UPnP) is a set of computer network protocols that allows compatible devices to be ready to work without any configuration once they are connected to the network.

Allow Users to Configure: To enable manual changes to the Router while using the UPnP feature, keep the default setting, **Enabled**. To disable manual changes, select **Disabled**.

Allow Users to Disable Internet Access: To prohibit users from accessing the Router web-based utilities, keep the default setting, **Disabled**. Otherwise, select **Enabled**.

Diagnosis



Service: ● Enabled ○ Disabled

Logviewer IP Address: 192 . 168 . 101 . 11 (0 means disabled)

IP or URL Address:

Packet Size: 32 bytes (32~65500)

Number of Pings: 5

IP or URL Address:

Log

The Router can keep logs of all traffic for your Internet connection. To monitor the network, select **Enabled**.

You can view logs by clicking **View Log**. If you want to view logs in a browser, enter an IP address in the **Logviewer IP Address** field. You can enter this IP in a browser to view logs.

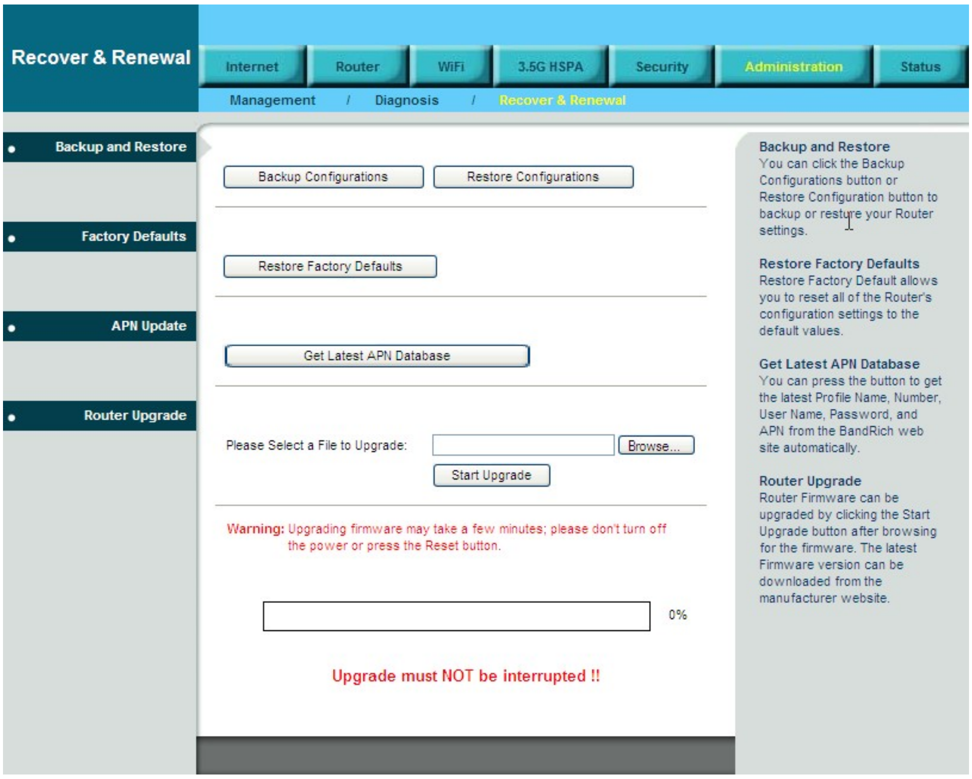
Ping Test

To check the status of a connection, enter the IP address or URL that you want to ping in the **IP or URL Address** field, define the packet size you want to use in the **Packet Size** field, And select the number of times you wish to ping: **5**, **10**, **15**, or **Unlimited**. Click **Start Test** to begin the ping test. A new screen displays the test results.

Traceroute Test

To test the performance of a connection, enter a URL or IP address in the **IP or URL Address** field, and click **Start Test**. A new screen displays the test results.

Recover & Renewal



Please Select a File to Upgrade:

Warning: Upgrading firmware may take a few minutes; please don't turn off the power or press the Reset button.

Upgrade must NOT be interrupted !!

Backup and Restore
You can click the Backup Configurations button or Restore Configuration button to backup or restore your Router settings.

Restore Factory Defaults
Restore Factory Default allows you to reset all of the Router's configuration settings to the default values.

Get Latest APN Database
You can press the button to get the latest Profile Name, Number, User Name, Password, and APN from the BandRich web site automatically.

Router Upgrade
Router Firmware can be upgraded by clicking the Start Upgrade button after browsing for the firmware. The latest Firmware version can be downloaded from the manufacturer website.

Backup and Restore

Backup Configurations

Click **Backup Configurations** to back up your Router's current configuration. In the file dialog box, select a location and file name for the configuration file.

Restore Configurations

Click the **Restore Configurations**. In the file dialog box, click Browse to locate the configuration file, and click **Restore**.

Factory Defaults

To reset the Router's configuration settings to the default values, click **Restore Factory Default**.

APN Update

To update the APN database, click **Get Latest APN Database**. In the dialog box, click **Start**.

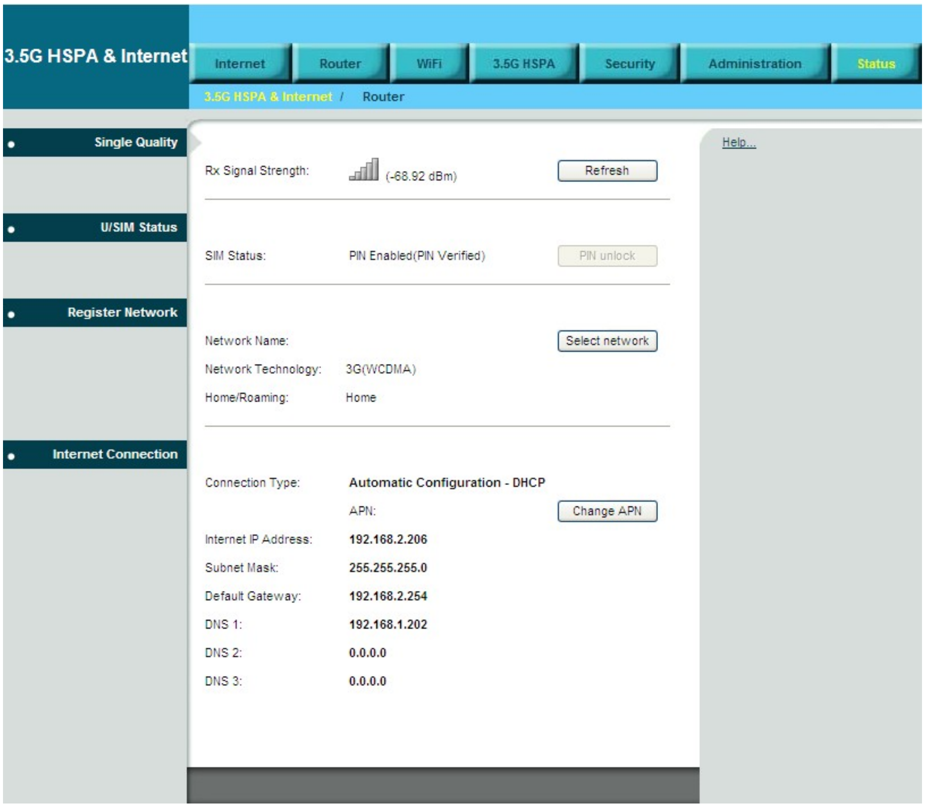
Router Upgrade

To upgrade the Router's firmware, click **Browse** and locate the latest firmware upgrade file. After the file is located, click **Start Upgrade**. The upgrade progress is displayed. You can download the latest firmware from www.bandluxe.com.

🚫	**Warning:** Upgrading firmware may take a few minutes; do not turn off the power or press the Reset button during upgrade.

Status

3.5G HSPA & Internet



Rx Signal Strength: (-68.92 dBm)

SIM Status: PIN Enabled(PIN Verified)

Network Name:

Network Technology: 3G(WCDMA)

Home/Roaming: Home

Connection Type: Automatic Configuration - DHCP

APN:

Internet IP Address: 192.168.2.206

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.2.254

DNS 1: 192.168.1.202

DNS 2: 0.0.0.0

DNS 3: 0.0.0.0

Signal Quality

When you access the Internet via 3G or 3.5G, click **Refresh** to show the signal strength.

U/SIM Status

Your SIM card verification status is shown in this area. Clicking **Pin unlock** displays the **PIN Verification** tab.

Register Network

Network Name: This shows the name of your network operator.

Network Technology: This shows the network technology you are currently using.

Home/Roaming: This indicates whether the Router is in Home or

Roaming status.

Internet Connection

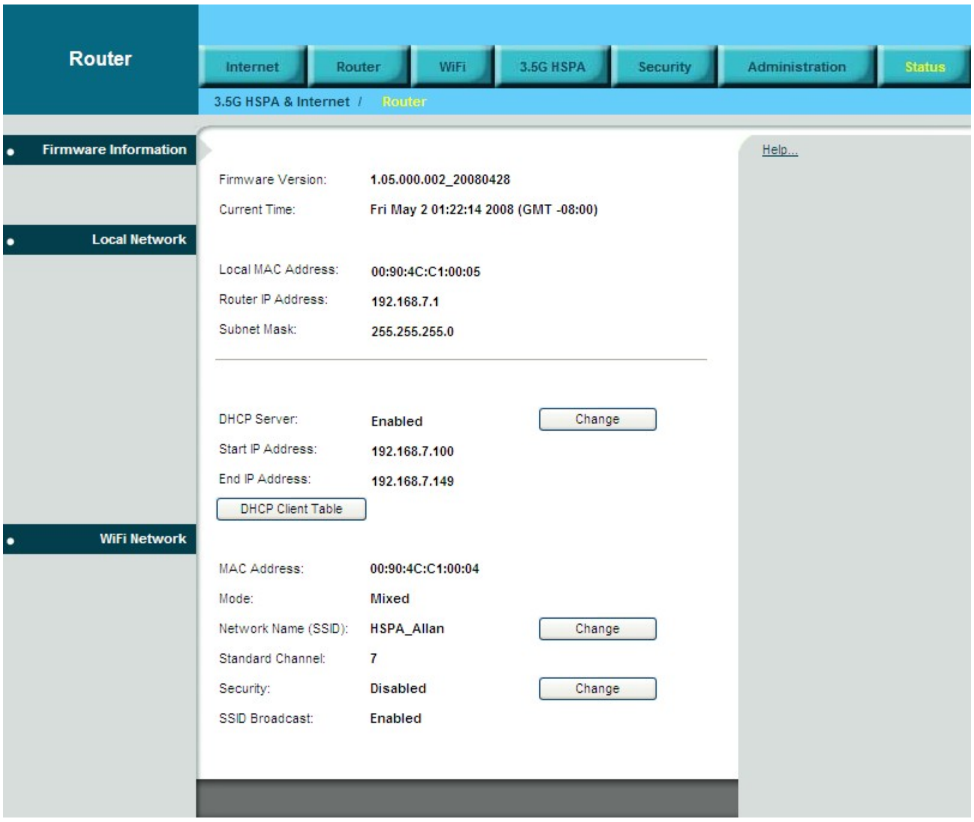
Connection Type: This indicates the type of Internet connection you are using.

Internet IP Address: This is the Router's IP Address, as seen on your local network.

Subnet Mask and **Default Gateway:** The Router’s Subnet Mask and Default Gateway address are displayed here for DHCP and static IP connections.

DNS1-3: The DNS (Domain Name System) IP addresses currently used by the Router are shown here.

Router



Firmware Information

Firmware Version: 1.05.000.002_20080428

Current Time: Fri May 2 01:22:14 2008 (GMT -08:00)

Local Network

Local MAC Address: 00:90:4C:C1:00:05

Router IP Address: 192.168.7.1

Subnet Mask: 255.255.255.0

DHCP Server: Enabled

Start IP Address: 192.168.7.100

End IP Address: 192.168.7.149

WiFi Network

MAC Address: 00:90:4C:C1:00:04

Mode: Mixed

Network Name (SSID): HSPA_Allan

Standard Channel: 7

Security: Disabled

SSID Broadcast: Enabled

Firmware Information

Firmware Version: This is the Router’s current firmware.

Current Time: This shows the time, as you set on the Optional tab.

Local Network

Local MAC Address: This is the Router’s MAC Address, as seen by your ISP

Router IP Address: The Router’s IP Address that appears on your local network.

Subnet Mask: This shows the current subnet mask being configured for your local network.

DHCP Server: The status of the DHCP server function is displayed here.

Start IP Address: This shows the beginning of the range of IP Addresses used by devices on your local Ethernet network.

End IP Address: The end of the range of IP Addresses used by devices on your local Ethernet network is shown here.

DHCP Client Table: Click this button to open a screen showing you which PCs are utilizing the Router as a DHCP server.

WiFi Network

MAC Address: This is the Router’s MAC Address, as seen on your local wireless network.

Mode: This displays the wireless mode (Mixed, Wireless-G Only, Wireless-B Only, or Disabled) used by the network.

Network Name (SSID): This displays the wireless network name or SSID.

Standard Channel: This displays the channel on which your wireless network is broadcasting.

Security: This shows the security method you are using.

SSID Broadcast: This shows whether the Router's SSID Broadcast function is on or off.

Appendix A: Specification

Form Factor	
Dimension (L x W x H, mm)	153 x 103 x 24 mm
Weight (g)	160g typical
Interface	
ExpressCard/34 interface for HSPA data modem	Supported
ExpressCard / USB interface switch	Manual switch
Wireless SecureEasySetup Button	Yes
LAN port	RJ45, 1 port
WAN port	RJ45, 1 port
Power plug	Yes
Reset button	Yes
Connectivity and Data Speed	
WLAN	802.11b/g
LAN	Ethernet
Antenna	
WiFi Antenna	2 embedded antenna @ 2.4-2.5GHz 1 Dipole Antenna and 1 Monopole Antenna Peak Gain 4dBi

Protocol

Default connection	"3.5G HSPA First" or "Ethernet First" customizable
Automatic WAN connection fail-over	Supported
Fixed WAN connection	DHCP, Static IP, PPPoE, PPTP, L2TP
UMTS/HSPA connection	Connection On Demand, Connection when available, Auto APN matching with USIM
Security	Multiple VPN passthrough (IPsec, PPTP, L2TP), Internet access restriction, Firewall, DoS Prevention, Traffic and Event Logging
NAT-NAPT	Port forwarding, Port triggering, DMZ,Multicast Pass-Through, Static Routing, Dynamic Routing (RIP 1, RIP2), QoS
DNS	DNS Agent, DDNS
ALG Support	Yahoo messenger, AOL messenger, MSN messenger, ICQ, RealAudio, NetMeeting, Telnet, FTP, Microsoft Traceroute, Quake, IRC, Microsoft PPTP Client
Other Features	IPv4, TCP, UDP, ICMPv4, ARP, DHCP Server/Client, HTTPs, NTP, TFTP server, MAC Clone

Wireless LAN

802.11b data rate	1/2/5.5/11 Mbps, Auto or Fixed Rate
802.11g data rate	6/9/12/18/24/36/48/54 Mbps, Auto or Fixed Rate
Transmit Power	IEEE 802.11g: 15 dBm IEEE 802.11b: 18 dBm
Receive Sensitivity	IEEE 802.11 g: -65dBm @ 54Mbps PER=g 10% IEEE 802.11 b: -79+/-2dBm @ 11 Mbps PER^8%
Security	WPA2/WPA/AES/TKIP, WPA/WPA2 PSK mode, 802.1x (identify all EAP types supported), 64/128 bits WEP Encryption, MAC address filtering, open system and shared key authentication, SSID Broadcast Disable
Other Features	Support up to 32 simultaneous wireless users, Broadcom Wireless SES security implementation , WME, WDS bridge/repeater modes

Status Indication

LED	UMTS, Roaming, SMS, WLAN, Ethernet, Power

Accessories	
Power adaptor	Supported
Power Consumption	
Voltage	12V DC
Current	1A max.
Environment	
Operation Temperature	0°C~45°C (32°F-113°F)
Storage Temperature	-20°C~70°C (-4°F-158°F)
Operating Humidity	10%~90% non-condensing
Storage Humidity	5%~90% non-condensing
Conformance of Environmental Regulation	
	RoHS

Appendix B: Important Safety Information and Glossary

Europe – EU Declaration of Conformity

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC:

- EN60950-1:2001 A11:2004
  Safety of Information Technology Equipment

- EN50385 : (2002-08)
- Product standard to demonstrate the compliance of radio base stations and fixed terminal stations for wireless telecommunication systems with the basic restrictions or the reference levels related to human exposure to radio frequency electromagnetic fields (110MHz - 40 GHz) - General public

- EN 300 328 V1.7.1: (2006-10)
- Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive

- EN 301 489-1 V1.6.1: (2005-09)
  Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements

- EN 301 489-17 V1.2.1 (2002-08)
- Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2,4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment

This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of

2454 – 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

CE 0560 ❗

Česky [Czech]	*[Jméno výrobce]* tímto prohlašuje, že tento *[typ zařízení]* je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
Dansk [Danish]	Undertegnede *[fabrikantens navn]* erklærer herved, at følgende udstyr *[udstyrets typebetegnelse]* overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt *[Name des Herstellers]*, dass sich das Gerät *[Gerätetyp]* in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab *[tootja nimi = name of manufacturer]* seadme *[seadme tüüp = type of equipment]* vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, *[name of manufacturer]*, declares that this *[type of equipment]* is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]	Por medio de la presente *[nombre del fabricante]* declara que el *[clase de equipo]* cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ *[name of manufacturer]* ΔΗΛΩΝΕΙ ΟΤΙ *[type of equipment]* ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Français [French]	Par la présente *[nom du fabricant]* déclare que l'appareil *[type d'appareil]* est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italian]	Con la presente *[nome del costruttore]* dichiara che questo *[tipo di apparecchio]* è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo *[name of manufacturer / izgatavotāja nosaukums]* deklarē, ka *[type of equipment / iekārtas tips]* atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo *[manufacturer name]* deklaruoja, kad šis *[equipment type]* atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart *[naam van de fabrikant]* dat het toestel *[type van toestel]* in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.

mt Malti [Maltese]	Hawnhekk, *[isem tal-manifattur]*, jiddikjara li dan *[il-mudel tal-prodott]* jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
hu Magyar [Hungarian]	Alulírott, *[gyártó neve]* nyilatkozom, hogy a *[... típus]* megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
pl Polski [Polish]	Niniejszym *[nazwa producenta]* oświadcza, że *[nazwa wyrobu]* jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
pt Português [Portuguese]	*[Nome do fabricante]* declara que este *[tipo de equipamento]* está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
sl Slovensko [Slovenian]	*[Ime proizvajalca]* izjavlja, da je ta *[tip opreme]* v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	*[Meno výrobcu]* týmto vyhlasuje, že *[typ zariadenia]* spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
fi Suomi [Finnish]	*[Valmistaja = manufacturer]* vakuuttaa täten että *[type of equipment = laitteen tyyppimerkintä]* tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
sv Svenska [Swedish]	Härmed intygar *[företag]* att denna *[utrustningstyp]* står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

Federal Communication Commission Interference Statement

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

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

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.

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, except the tested 3.5G HSDPA ExpressCard (FCC ID: UZI-100). Other 3.5G ExpressCard have not been verified and may not comply with FCC RF exposure limit and shall not be use with this product.

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

Glossary

2G: Second-generation mobile networking technology. Represents a switchover from analog to digital; most 2G networks use GSM.

3G: Third-generation mobile networking technology that enables simultaneous transfer of voice and non-voice data; most 3G networks use WCDMA.

3.5G: A more recent standard of mobile networking technology; generally uses HSDPA.

APN (Access Point Name/Network): Provides GPRS routing information. Consists of:

Network ID: Identifies the external service requested by a GPRS user.

Mobile network operator ID: Specifies routing information.

ARFCN (Absolute Radio Frequency Channel Number): The specific ID numbers for all radio channels used in cellular mobile communications.

bps (bits per second): How data flow is measured.

DNS (Domain Name System): Helps route network traffic by making the addressing process more user-friendly.

DHCP (Dynamic Host Configuration Protocol): How devices obtain IP addresses from a server.

DUN (Dial-Up Network): Windows component that enables online access via a modem.

EDGE (Enhanced Data GSM Environment/Enhanced Data for Global Evolution): Advanced GPRS that delivers multimedia and other data needing greater bandwidth at up to 237 kbps.

GPRS (General Packet Radio Service): Delivers data in packets at up to 86 kbps.

GSM (Global System for Mobile Communications): The most popular cellular network, mostly operates in 850-900 or 1800-1900 MHz; the primary 2G system.

IMEI (International Mobile Equipment Identity): A number unique to each GSM/UMTS device that can be used block network access by a stolen mobile device.

IP (Internet Protocol): Routes packets over a network.

HSDPA (High Speed Downlink Packet Access): Advanced WCDMA that delivers bandwidth intensive data at up to 7.2Mbps; typically associated with 3.5G.

Kbps (Kilobits per second): A data flow measure; 1024 bits/second.

LAN (Local Area Network): A data network with limited range but good bandwidth.

Mbps (Megabits per second): A data flow measure; 1,048,576 bits/second.

PPP (Point-to-Point Protocol): An internet connection method.

PIN (Personal Identity Number): Four to eight digital numbers SIM card security code; allows access to the carrier's network.

Rx: Shorthand for Reception.

SIM (Subscriber Identity Module): A small card that contains key mobile device identification, subscription and contact information.

SMS (Short Messaging Service): Allows text messages of up to 160 characters.

Tx: Shorthand for Transmission.

WCDMA (Wideband Code Division Multiple Access): Advanced EDGE that supports 384kbps data flow. Most 3G networks use this standard; aka UMTS.