



Billion SG6200NXL

Smart Energy Gateway

User Manual

Version release: 1.04.ha.dc24

Last revised: March 17, 2014

Table of Contents

| | |
|--|----|
| <i>Chapter 1: Introduction</i> | 1 |
| Introduction to your Router | 1 |
| Features | 2 |
| <i>Chapter 2: Product Overview</i> | 6 |
| Important note for using this router | 8 |
| Package Contents | 8 |
| Device Description | 9 |
| The Front LEDs | 9 |
| The Rear Ports | 10 |
| Cabling | 11 |
| <i>Chapter 3: Basic Installation</i> | 12 |
| Connecting your router | 13 |
| Network Configuration | 14 |
| Factory Default Settings | 22 |
| Information from your ISP | 23 |
| Configuring with your Web Browser | 24 |
| <i>Chapter 4: Basic Configuration</i> | 25 |
| Status | 26 |
| Quick Start | 27 |
| WAN..... | 29 |
| WLAN | 32 |
| <i>Chapter 5: Advanced Configuration</i> | 35 |
| Status | 36 |
| BEsmart Status..... | 37 |
| ZigBee Status | 38 |
| Power Status..... | 39 |
| Sensor Status | 40 |
| RS485 Status | 41 |
| Wireless Status | 42 |

| | |
|------------------------------------|-----|
| 3G Status..... | 43 |
| ARP Table..... | 44 |
| DHCP Table..... | 44 |
| System Log..... | 45 |
| Firewall Log..... | 45 |
| UPnP Portmap..... | 46 |
| Quick Start..... | 47 |
| Power Management..... | 56 |
| Meter Config..... | 57 |
| Power Control..... | 59 |
| RS485 Config..... | 63 |
| Control Rules..... | 64 |
| Mail Alert..... | 65 |
| Configuration..... | 66 |
| LAN (Local Area Network)..... | 66 |
| Ethernet..... | 67 |
| IP Alias..... | 67 |
| Wireless..... | 68 |
| Wireless Security..... | 70 |
| WPS..... | 73 |
| DHCP Server..... | 85 |
| WAN (Wide Area Network)..... | 88 |
| WAN Interface(EWAN)..... | 88 |
| WAN Interface(3G)..... | 88 |
| WAN Interface(WirelessClient)..... | 89 |
| WAN Interface(Dual WAN)..... | 90 |
| WAN Profile..... | 91 |
| BEsmart..... | 100 |
| Register..... | 100 |
| Forget Password..... | 101 |
| System..... | 102 |
| Time Zone..... | 102 |
| Gateway FW Upgrade..... | 103 |
| ZigBee FW Upgrade..... | 104 |
| Backup / Restore..... | 105 |
| Restart Router..... | 106 |
| User Management..... | 107 |

| | |
|---|------------|
| Mail Alert | 108 |
| Firewall and Access Control..... | 109 |
| Packet Filter | 111 |
| MAC Filter | 113 |
| Intrusion Detection..... | 114 |
| QoS (Quality of Service)..... | 118 |
| Quality of Service Introduction..... | 118 |
| QoS Setup | 118 |
| Virtual Server | 122 |
| Port Mapping | 124 |
| DMZ | 126 |
| Wake on LAN | 128 |
| Time Schedule..... | 129 |
| Advanced | 130 |
| Static Route..... | 131 |
| Static ARP..... | 131 |
| Dynamic DNS | 132 |
| Device Management..... | 133 |
| IGMP | 140 |
| SNMP Access Control..... | 141 |
| Remote Access..... | 143 |
| Save Configuration to Flash | 144 |
| Restart | 145 |
| Logout..... | 146 |
| <i>Chapter 6: Troubleshooting</i> | <i>147</i> |
| <i>Appendix: Product Support & Contact.....</i> | <i>149</i> |

Chapter 1: Introduction

Introduction to your Router

Thank you for purchasing the Billion SG6200NXL **Smart Energy Gateway**. Your new router is an all-in-one unit that combines a Broadband modem, Ethernet network switch and two USB ports to provide everything you need to get the machines on your network connected to the Internet over a 3G broadband connection. With built-in ZigBee function, the Billion SG6200NXL can communicate with ZigBee embedded devices such as smart meter, load control, and PCT (Programmable Communicating Thermostat) for monitoring and managing the energy usage or event control.

The Billion SG6200NXL supports 3G, EWAN and WirelessClient (to connect to an AP to access the internet) to establish a connection with your ISP.

The perfect solution for connecting a small group of PCs to a high-speed broadband Internet connection, the Billion SG6200NXL allows multiple users to have high-speed Internet access simultaneously.

Your new router also serves as an Internet firewall, protecting your network from access by outside users. Not only does it provide a natural firewall function with Network Address Translation (NAT), it also provides rich firewall features to secure your network. All incoming data packets are monitored and filtered. You can also configure your new router to block internal users from accessing the Internet.

The Billion SG6200NXL provides two levels of security support. First, it masks LAN IP addresses making them invisible to outside users on the Internet, so it is much more difficult for a hacker to target a machine on your network. Second, it can block and redirect certain ports to limit the services that outside users can access. To ensure that games and other Internet applications run properly, you can open specific ports for outside users to access internal services on your network.

The Integrated DHCP (Dynamic Host Control Protocol) client and server services allow multiple users to get IP addresses automatically when the router boots up. Simply set local machines as a DHCP client to accept a dynamically assigned IP address from the DHCP server and reboot. Each time a local machine is powered up; the router recognizes it and assigns an IP address to instantly connect it to the LAN.

For advanced users, Virtual Service (port mapping) functions allow the product to provide limited visibility to local machines with specific services for outside users. For instance, a dedicated web

server can be connected to the Internet via the router and then incoming requests for web pages that are received by the router can be rerouted to your dedicated local web server, even though the server now has a different IP address.

Virtual Server can also be used to re-task services to multiple servers. For instance, you can set the router to allow separated FTP, Web, and Multiplayer game servers to share the same Internet-visible IP address while still protecting the servers and LAN users from hackers.

Features

ZigBee

The Billion SG6200NXL provides a full featured connectivity and allows a greater diversity of devices and applications to connect to the ZigBee network. The Billion SG6200NXL can convert the wireless protocols and sensor data into various kinds of formats which are necessary for industrial, commercial, and residential systems, allowing wireless sensor networks to use wireless protocols such as ZigBee that are well suited for a harsh RF environment as well as battery powered applications.

BEsmart

Billion BEsmart offers controlling and monitoring of the power energy consumption using the latest energy monitoring technologies. With the implementation of the BEsmart service, energy usage can be clearly examined and analyzed anytime and anywhere simply through a smart phone. It helps reduce energy waste, provide a green environment, and further increase the benefit for the mutual investment for both investors and customers, which is an optimal choice for Telco/ISP/SI service providers.

3G

3 G-based Internet connections (requires an additional 3G USB modem), with automatic fail-over to ensure an always-on Internet connection in the event that one of your Internet services fails. The setup of 3G is simplified by the web browser-based configuration. It is easy for you to access to the Internet wherever a 3G connection is available, you can even share your Internet connection with others, no matter whether you're in a meeting, or taking a cross-country train trip.

802.11n Wireless AP with WPA Support

With integrated 802.11n Wireless Access Point in the router, the device offers a quick and easy access among wired network, wireless network and broadband connection with single device simplicity, and as a result, mobility to the users. In addition to 300 Mbps 802.11n data rate, it also interoperates backward with existing 802.11g and 802.11b equipment. The Wi-Fi Protected Access (WPA) and

Wired Equivalent Privacy (WEP) supported features enhance the security level of data protection and access control via Wireless LAN.

Fast Ethernet Switch

A 3-port 10/100Mbps fast Ethernet switch is built-in with automatic switching between MDI and MDI-X for 10Base-T and 100Base-TX ports, with auto detection allowing you to use either straight or cross-over Ethernet cables.

EWAN

Billion SG6200NXL Smart Energy Gateway offers a WAN port to connect to Cable Modems and fibre optic lines. This alternative, yet faster method to connect to the internet will provide users more flexibility to get online.

3G Management Center

Monitoring your 3G connection status is easy with the Billion SG6200NXL smart gateway. The unique Billion 3G Management Center is a web-based utility tool, displaying visually its current 3G-signal status for users to maximize their connection. Users can monitor their bandwidth with current upload and download speed. This tool also calculates the total amount of hours or data traffic used per month, allowing users to manage their 3G monthly subscriptions. The web-based user interface of the Billion SG6200NXL makes it extremely easy for users to install and manage their network. Supporting DHCP client and server, the router enables system administrators to easily integrate this router into existing network environments and manage IP assignment without the need to reconfigure other stations.

Multi-Protocol to Establish a Connection

The router supports PPP over Ethernet, DHCP Client and Fixed IP address to establish a connection with an ISP.

Universal Plug and Play (UPnP) and UPnP NAT Traversal

This protocol is used to enable simple and robust connectivity among stand-alone devices and PCs from many different vendors, and it makes setting up a network simple and affordable. UPnP architecture leverages TCP/IP and the Web to enable proximity networking in addition to control and data transfer among networked devices. With this feature enabled, you can seamlessly connect to Net Meeting or MSN Messenger.

Network Address Translation

Network Address Translation (NAT) allows multiple users to access outside resources such as the Internet simultaneously with one IP address/one Internet access account. Many application layer gateways (ALG) are supported such as web browser, ICQ, FTP, Telnet, E-mail, News, Net2phone, Ping, NetMeeting, IP phone and others.

Firewall

NAT technology supports simple firewalls and provides options for blocking access from the Internet, like Telnet, FTP, TFTP, WEB, SNMP and IGMP.

Domain Name System Relay

Domain Name System (DNS) relay provides an easy way to map a domain name with a user-friendly name such as www.google.com with an IP address. When a local machine sets its DNS server to the router's IP address, every DNS conversion request packet from the PC to this router is forwarded to the real DNS on the outside network.

Dynamic Domain Name System (DDNS)

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname. This dynamic IP address is the WAN IP address. To use the service, you must first apply for an account from a DDNS service such as <http://www.dyndns.org/>.

PPP over Ethernet (PPPoE)

The Billion SG6200NXL provides an embedded PPPoE client function to establish a connection. You get greater access speed without changing the operation concept, while sharing the same ISP account and paying for one access account. No PPPoE client software is required for the local computer. Automatic Reconnect and Disconnect Timeout (Idle Timer) functions are also provided.

Quality of Service (QoS)

QoS gives you full control over which types of outgoing data traffic should be given priority by the router, ensuring important data like gaming packets, customer information, or management information move through the router at lightning speed, even under heavy load. The QoS features are configurable by Internal IP address, External IP address, protocol, and port. You can throttle the speed at which different types of outgoing data pass through the router, to ensure P2P users don't saturate upload bandwidth, or office browsing doesn't bring client web serving to a halt. In addition, or alternatively, you can simply change the priority of different types of upload data and let the router sort

out the actual speeds.

Virtual Server

You can specify which services are visible to outside users. The router detects an incoming service request and forwards it to the specific local computer for handling. For example, you can assign a PC in a LAN to act as a Web server inside and expose it to the outside network. Outside users can browse inside the web server directly while it is protected by NAT. A DMZ host setting is also provided for local computers exposed to the outside Internet network.

Dynamic Host Configuration Protocol (DHCP) Client and Server

On a WAN site, the DHCP client obtains an IP address from the Internet Service Provider (ISP) automatically. On a LAN site, the DHCP server allocates a range of client IP addresses, including subnet masks and DNS IP addresses and distributes them to local computers. This provides an easy way to manage the local IP network.

Rich Packet Filtering

This feature filters the packet based on IP addresses as well as Port numbers. Filtering packets to and from the Internet provides a higher level of security control.

Web-based GUI

A web-based GUI offers easy configuration and management. It also supports remote management capability for remote users to configure and manage this product.

Firmware Upgradeable

You can upgrade the router with the latest firmware through its web-based GUI.

Chapter 2: Product Overview

Billion SG6200NXL **Smart Energy Gateway** is an all-in-one network device enabling SOHO and office users to enjoy the freedom of secure and high-speed Internet connectivity at the home, office, or mobile. Using the integrated USB 2.0 ports, the device offers users to share a blistering wired or 3G-based wireless Internet connection over 3G networks. With built-in ZigBee function, the Billion SG6200NXL can communicate with ZigBee embedded devices such as smart meter, load control, and PCT (Programmable Communicating Thermostat) for monitoring and managing the energy usage or event control. With a supported Ethernet WAN port, the Billion SG6200NXL can be wired to an ADSL/Cable modem. An optional 12V car power allows you to power the device using your car's cigarette lighter for ultimate on the road mobility. The 3G-connection statuses can be monitored at any time using Billion's value added application utility, the 3G Management Centre.

With Billion's SG6200NXL, you can connect a 3G / HSDPA USB modem to the built-in USB port, enabling you to access to the Internet over a 3.5G / HSDPA, 3.75G / HSUPA, HSPA+, UMTS, EDGE, GPRS, or GSM networks, making downstream rates of up to 14.4 Mbps*1 possible. With the increasing popularity of the 3G standard, communication via the Billion SG6200NXL is becoming more convenient and widely available - allowing you to watch movies, download music on the road, or access e-mail no matter where you are - in a meeting, or speeding across the country on a train. The built-in auto fail-over ensures maximum connectivity and minimum interruption by quickly and smoothly connecting to a 3G network in the event that current wired connection fails. The Billion SG6200NXL will automatically reconnect to the wired connection when it's restored, minimizing connection costs. These features are perfect for office situations where constant connection is paramount.

Also the Billion's SG6200NXL can flexibly act as a wireless client to connect to an wireless AP for accessing the internet, adding another way of connecting to the internet.

The Billion SG6200NXL can also serve as multi-function servers with its USB port to help you set up your own network. You can share the printer in your office network, monitor your house with a Webcam and share files with your colleagues or friends. If you need to handle office business, home security and personal entertainment, the Billion SG6200NXL can connect with your network devices using the built-in USB port.

With an integrated 802.11n Wireless Access Point, the router delivers up to 6 times the speeds and 3 times the wireless coverage of a 802.11b/g network device and supports a data rate of up to 300 Mbps, so that wireless access is available everywhere in the house or at work. The Wi-Fi Protected Access

(WPA-PSK / WPA2-PSK) and Wired Equivalent Privacy (WEP) features enhance the level of transmission security and access control over the Wireless network. The router also supports the Wi-Fi Protected Setup (WPS) standard, allowing users to establish a secure wireless network by simply pushing a button. If your network requires wider coverage, the built-in Wireless Distribution System (WDS) repeater function allows you to expand your wireless network without the need for any further wires or cables. Multiple SSIDs allow users to access different networks through a single access point. Network managers can assign different policies and functions for each SSID, increasing the flexibility and efficiency of the network infrastructure. Keep in mind, however, that the number, thickness and location of walls, ceilings, or other objects that the wireless signals must pass.

Keep the number of walls and ceilings between the Billion SG6200NXL and other network devices to a minimum - each wall or ceiling can reduce your Billion SG6200NXL wireless product's range from 3-90 feet (1-30 meters.)

Position your devices so that the number of walls or ceilings is minimized. Be aware of the direct line between network devices. Position the devices so that the signal will travel straight through a wall or ceiling (instead of at an angle) for better reception. Building Materials can impede the wireless signal - a solid metal door or aluminium studs may have a negative effect on range.

Try to position wireless devices and computers with wireless adapters so that the signal passes through drywall or open doorways and not other materials. Keep your product away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate extreme RF (radio frequency) noise.

Important note for using this router



Warning

- Do not use the router in high humidity or high temperatures.
- Do not use the same power source for the router as other equipment.
- Do not open or repair the case yourself. If the router is too hot, turn off the power immediately and have it repaired at a qualified service center.
- Avoid using this product and all accessories outdoors.



Attention

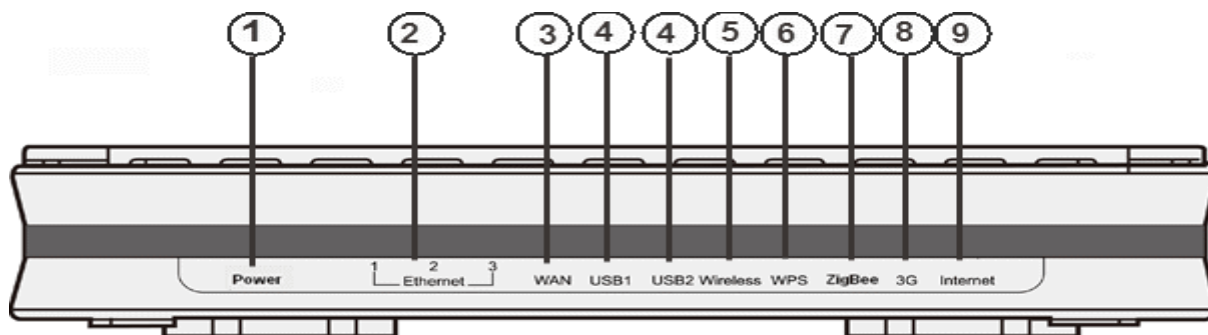
- Place the router on a stable surface.
- Only use the power adapter that comes with the package. Using a different voltage rating power adaptor may damage the router.

Package Contents

- Billion SG6200NXL Smart Energy Gateway
- CD containing the online manual
- Ethernet Cable
- AC-DC power adapter
- Antennas (2 pcs)

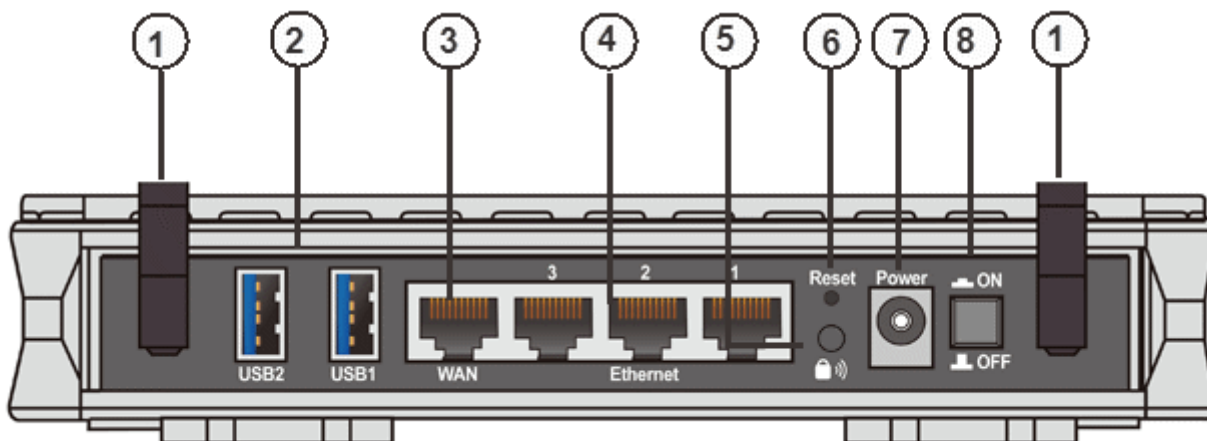
Device Description

The Front LEDs



| LED | | Meaning |
|-----|----------------------|---|
| 1 | Power | Lit red when power is ON. Lit green when the device is ready. Lit red means system failure. Restart the device or contact Billion for support. |
| 2 | Ethernet Port | Lit when one of LAN ports is connected to an Ethernet device. Lit green when the speed of transmission hits 100Mbps; Lit orange when the speed of transmission hits 10Mbps. Blink when data is being Transmitted / Received. |
| 3 | WAN | Lit green when connected to a modem or Cable modem's Ethernet port well. |
| 4 | USB | Lit green when the router is connected to a USB device. Flash when data is received / transmitted. (The function of USB1 is the same with USB2) |
| 5 | Wireless | Lit green when the wireless connection is established. Flashes when sending/receiving data. |
| 6 | WPS | Lit green when WPS is being in progress. Unlit when WPS is connected. |
| 7 | ZigBee | Flashes about once every 3 seconds when the wireless connection is established. Flashes about 3 times per second when the device is set to the state waiting for being joined by other smartmeters. |
| 8 | 3G | Lit orange when the device receive 3G signal. Lit green if the router supports this 3G card. The Internet LED will lit when the device obtain IP address successfully. |
| 9 | Internet | Lit green when IP connected. Flashes green when IP connected and IP traffic is passing thru the device. Lit red when device attempted to become IP connected and failed. Lit off when device in bridged mode connection not present. |

The Rear Ports



| | | |
|---|-------------------|---|
| 1 | Antenna | Connect the detachable antenna to this port. |
| 2 | USB | Connect the USB cable to this port. 3G/ HSDPA USB modem backup for Internet access, can also connect with printer, serve as multi-function servers with to help set up your own network. (The function of USB1 is the same with USB2) |
| 3 | WAN | WAN 10/100M Ethernet port (with auto crossover support); connect Cable modem here. |
| 4 | Ethernet | Connect a UTP Ethernet cable (Cat-5 or Cat-5e) to one of the LAN ports when connecting to a PC or an office/home network of 10Mbps or 100Mbps. |
| 5 | WPS | Push WPS button to trigger ZigBee function, thus smartmeter allowing join in is starting. See Meter Config section. Push WPS button more than 5 seconds to trigger Wi-Fi Protected Setup function. See WPS section. |
| 6 | RESET | To be sure the device is being turned on press RESET button for 6 seconds and above: restore to factory default settings. (Cannot login to the router or forgot your Username/Password. Press the button for more than 6 seconds). Caution: After pressing the RESET button for more than 6 seconds, to be sure you power cycle the device again. |
| 7 | Power | Connect it with the supplied power adapter. |
| 8 | Power Jack | Device is power on/off. |

Cabling

The most common problem associated with Ethernet is bad cabling. Make sure that all connected devices are turned on. On the front of the product is a bank of LEDs. Verify that the LAN Link and WAN Link LEDs are lit. If they are not, verify that you are using the proper cables.

Chapter 3: Basic Installation

You can configure the Billion SG6200NXL router through the convenient and user-friendly interface of a web browser. Most popular operating systems such as Linux and Windows 98/NT/2000/XP/Me include a web browser as a standard application.

PCs must have a properly installed Ethernet interface which connects to the router directly or through an external repeater hub. In addition, PCs must have TCP/IP installed and configured to obtain an IP address through a DHCP server or a fixed IP address that must be in the same subnet as the router. The default IP address of the router is **192.168.1.254** and the subnet mask is **255.255.255.0** (i.e. any attached PC must be in the same subnet, and have an IP address in the range between 192.168.1.1 and 192.168.1.253). The easiest way is to configure the PC is to obtain an IP address automatically from the router using DHCP. If you encounter any problems accessing the router's web interface you are advised to **uninstall** any kind of software firewall on your PCs, as they can cause problems when trying to access the 192.168.1.254 IP address of the router.

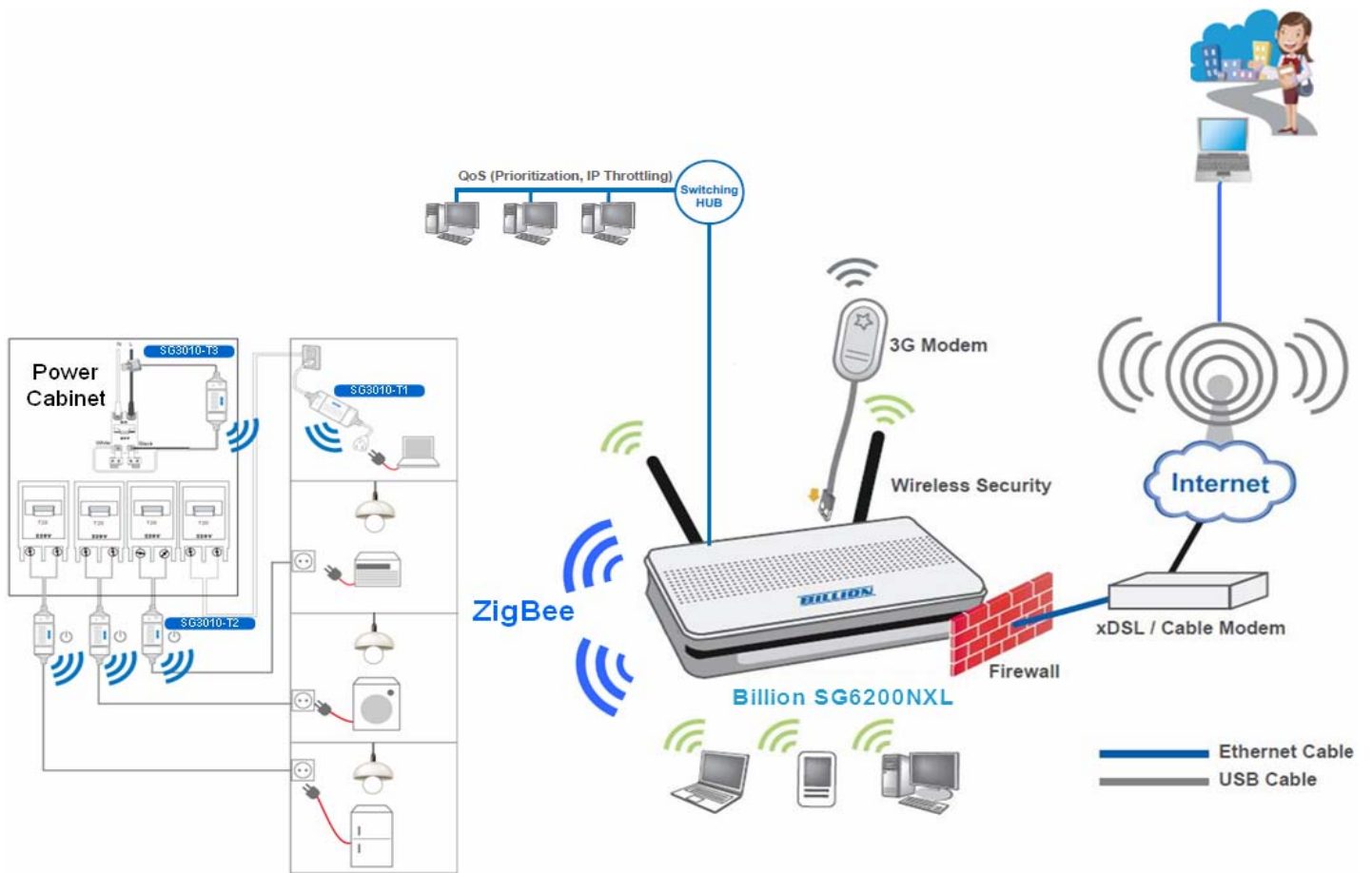
Please follow the steps below for installation on your PC's network environment. First of all, check your PC's network components. The TCP/IP protocol stack and Ethernet network adapter must be installed. If not, please refer to your Windows-related or other operating system manuals.



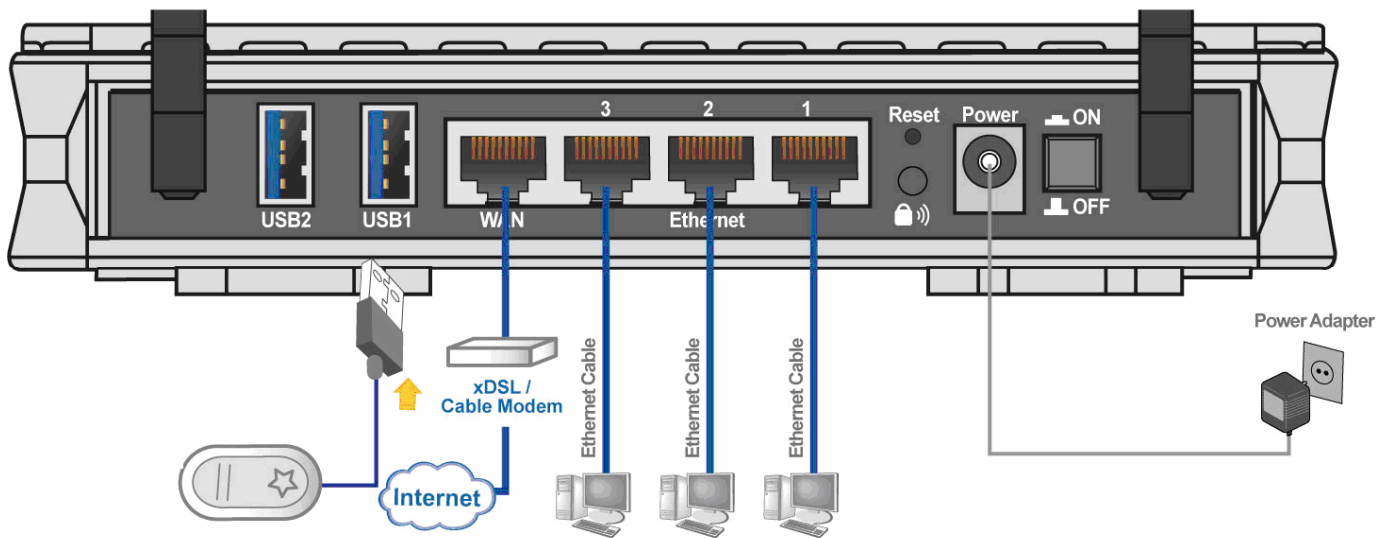
Any TCP/IP capable workstation can be used to communicate with or through the Billion SG6200NXL. To configure other types of workstations, please consult the manufacturer's documentation.

Connecting your router

Overview:



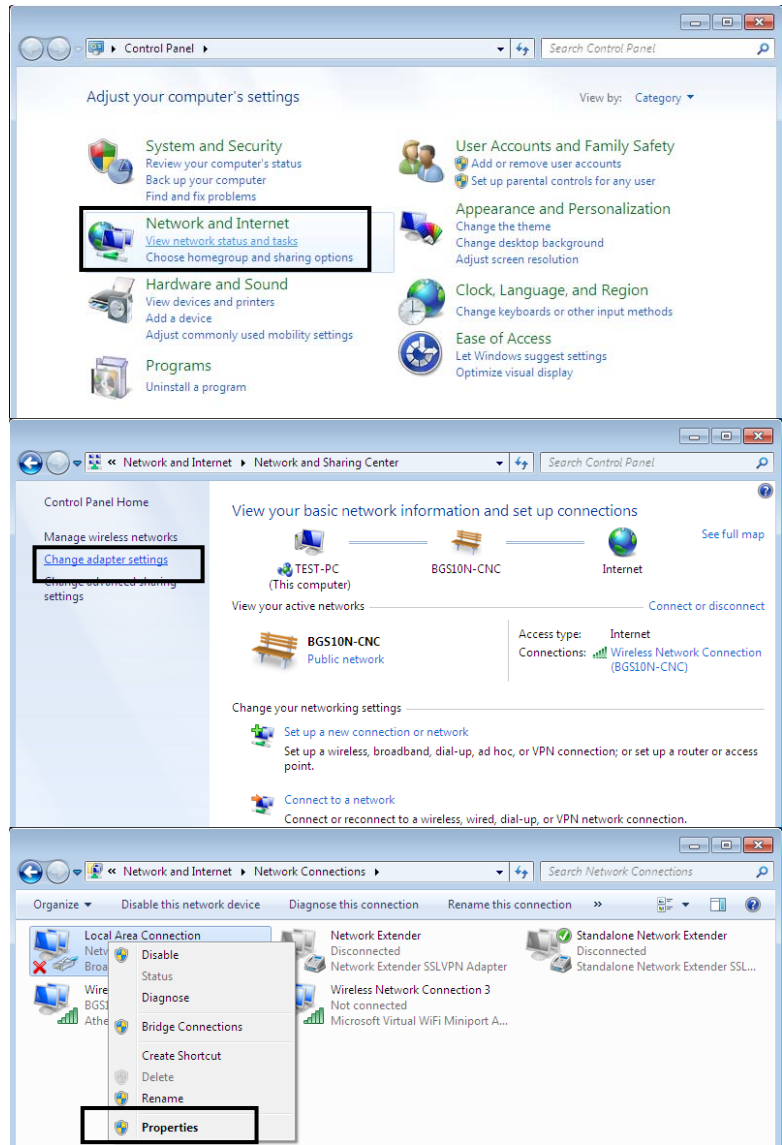
Detailed:



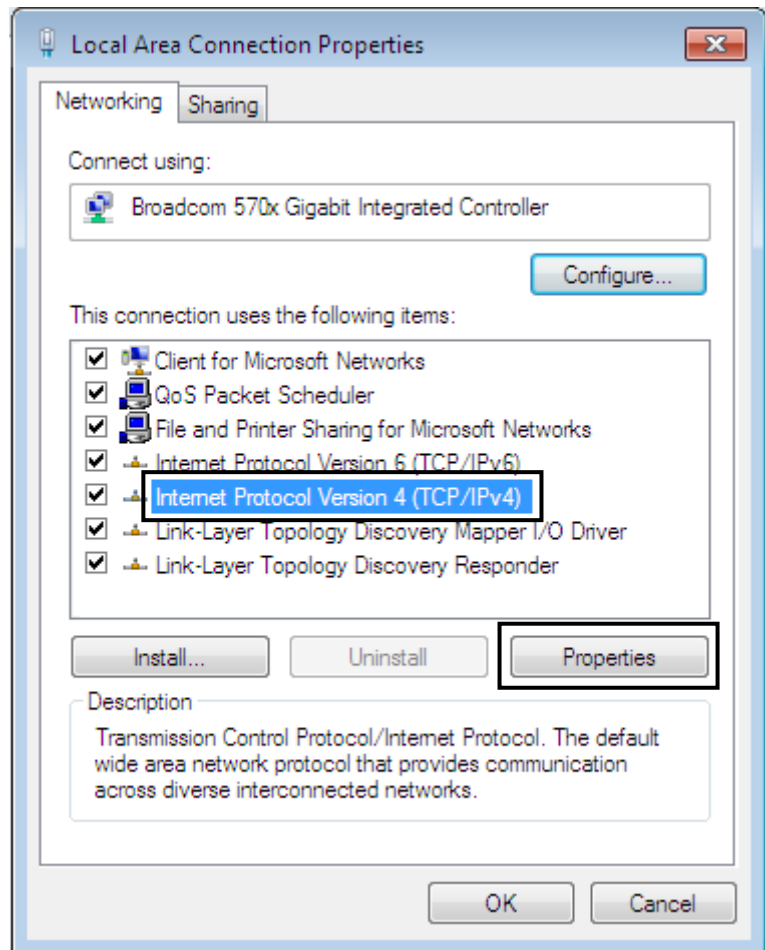
Network Configuration

Configuring a PC in Windows 7

1. Go to **Start**. Click on **Control Panel**.
2. Then click on **Network and Internet**.
3. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.
4. Select the **Local Area Connection**, and right click the icon to select **Properties**.

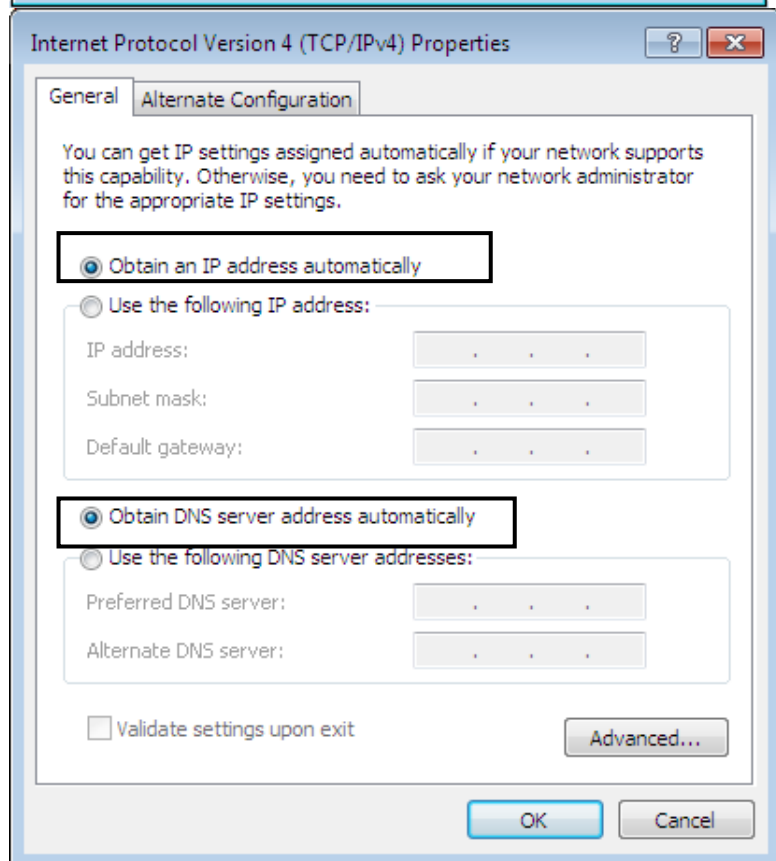


5. Select **Internet Protocol Version 4 (TCP/IPv4)** then click **Properties**.



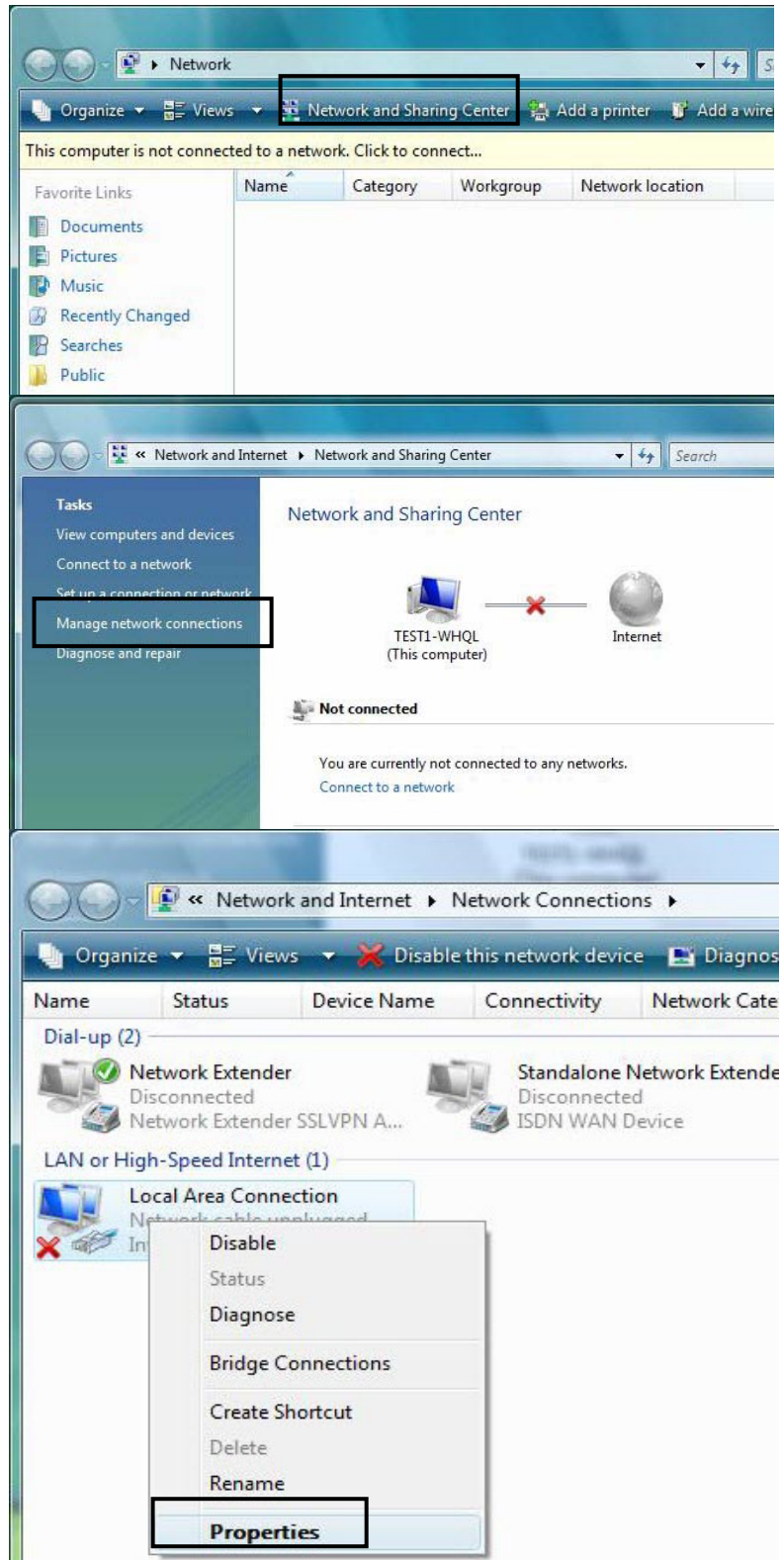
6. In the **TCP/IPv4 properties** window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.

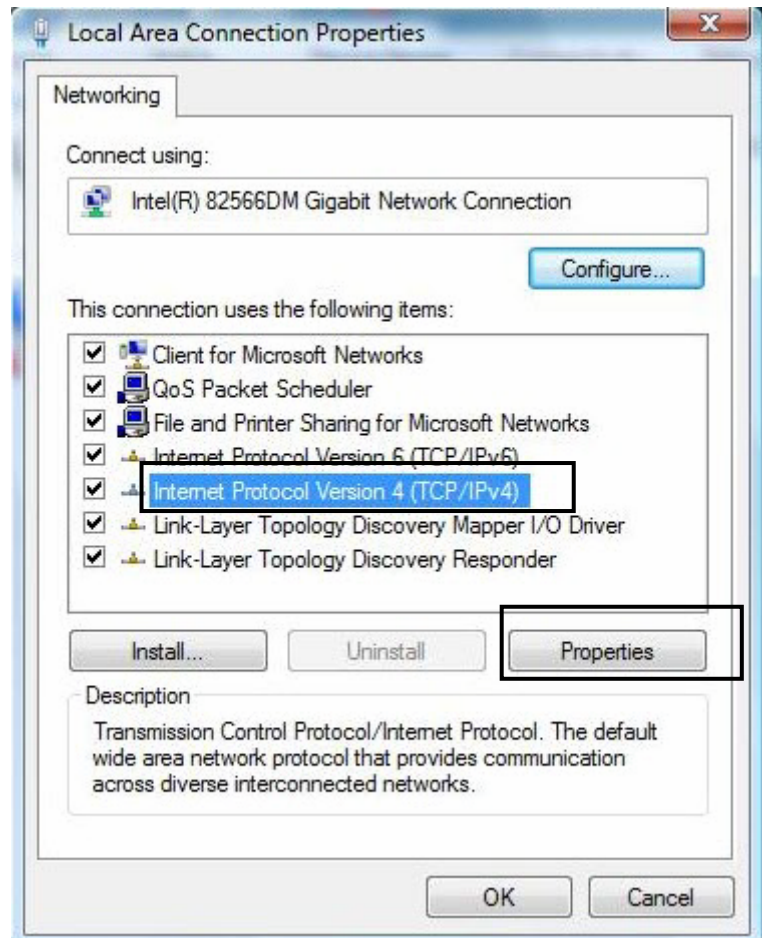


Configuring a PC in Windows Vista

1. Go to **Start**. Click on **Network**.
2. Then click on **Network and Sharing Center** at the top bar.
3. When the **Network and Sharing Center** window pops up, select and click on **Manage network connections** on the left window pane.
4. Select the **Local Area Connection**, and right click the icon to select **Properties**.

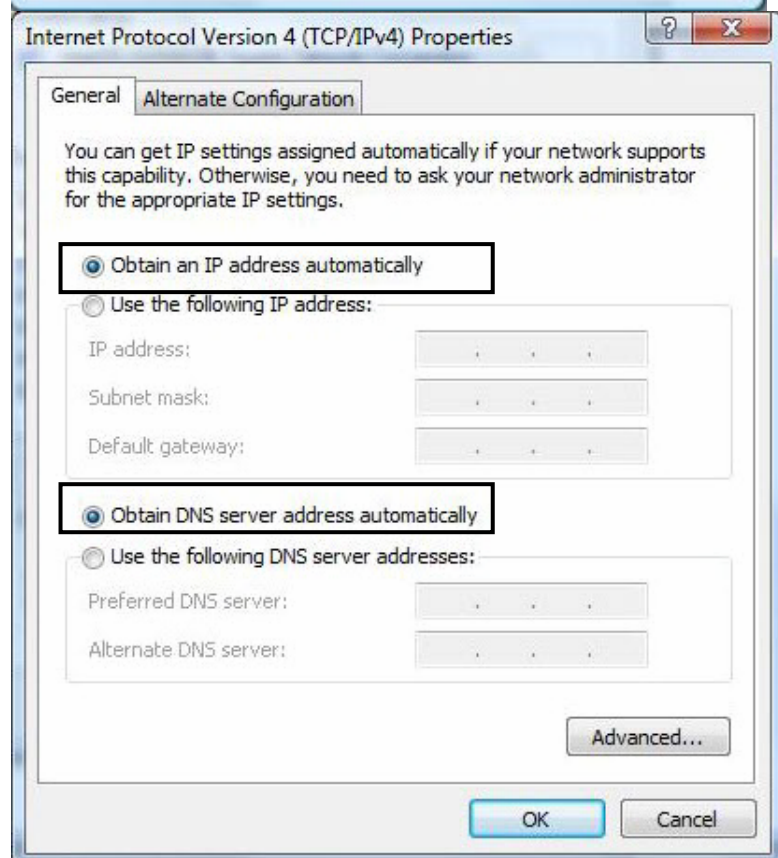


5. Select **Internet Protocol Version 4 (TCP/IPv4)** then click **Properties**.



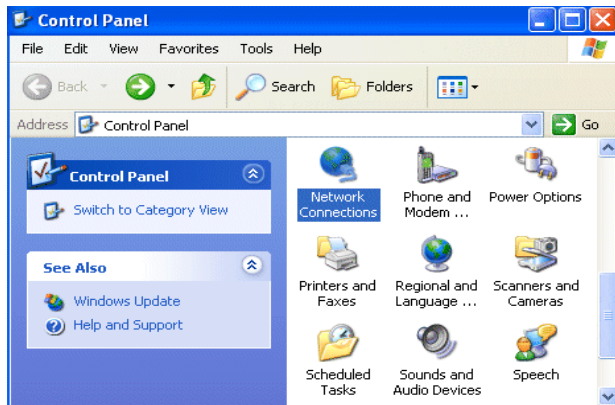
6. In the **TCP/IPv4 properties** window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.

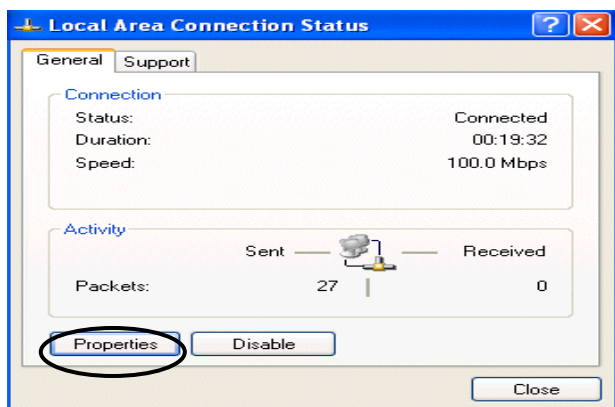


Configuring a PC in Windows XP

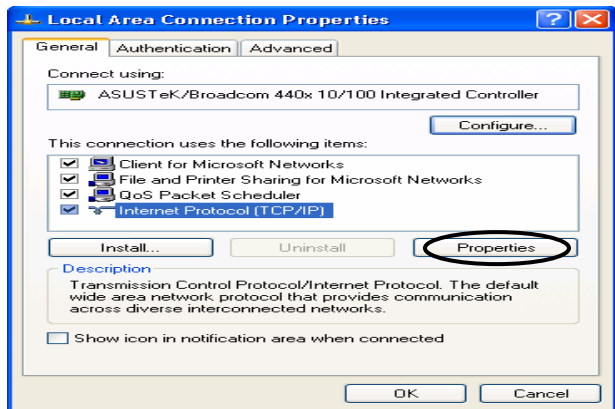
1. Go to **Start**. Click on **Control Panel**.
2. Then click on **Network and Internet**.



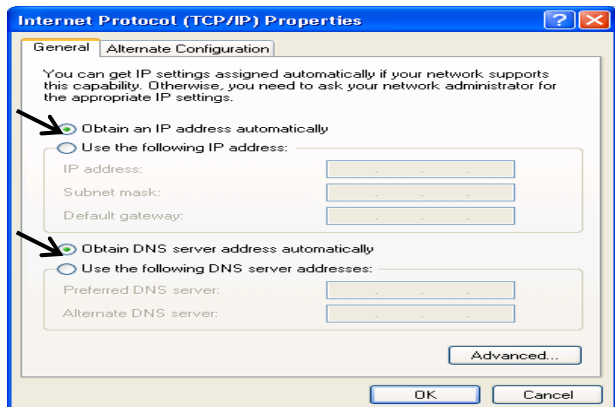
3. In the **Local Area Connection Status** window, click **Properties**.



4. Select **Internet Protocol (TCP/IP)** and click **Properties**.



5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.

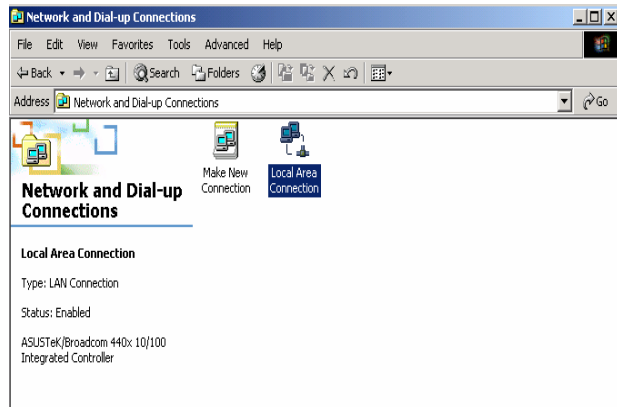


6. Click **OK** to finish the configuration.

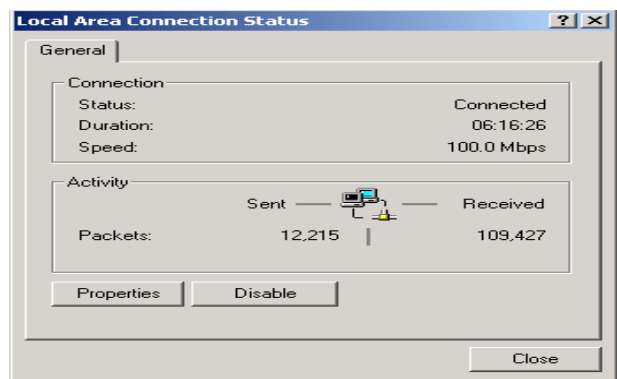
Configuring a PC in Windows 2000

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network and Dial-up Connections**.

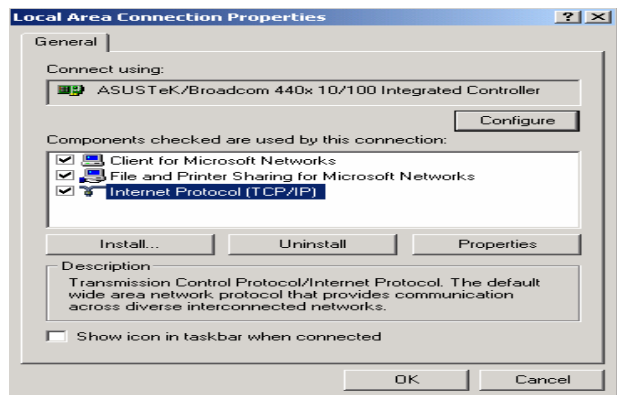
2. Double-click **Local Area Connection**.



3. In the **Local Area Connection Status** window click **Properties**.

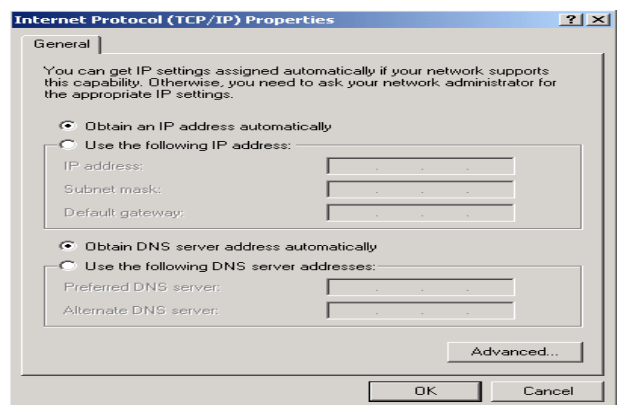


4. Select **Internet Protocol (TCP/IP)** and click **Properties**.



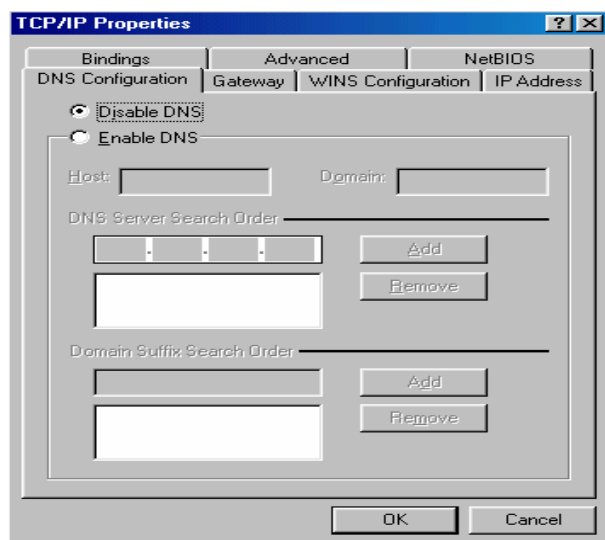
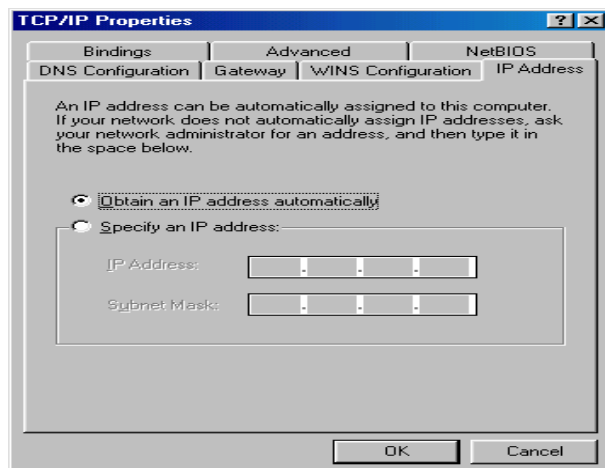
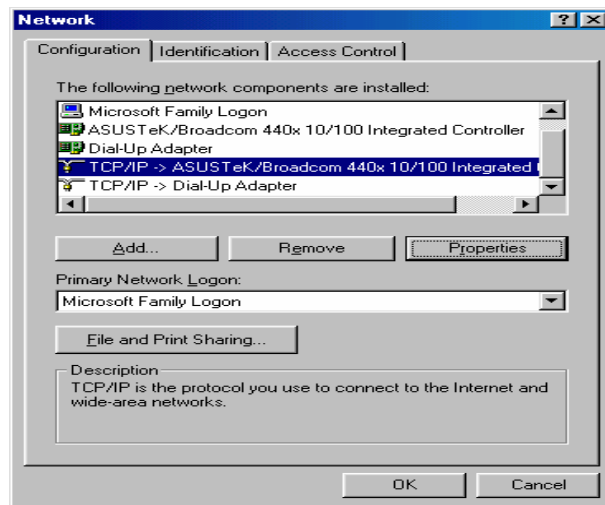
5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.

6. Click **OK** to finish the configuration.



Configuring PC in Windows 98/Me

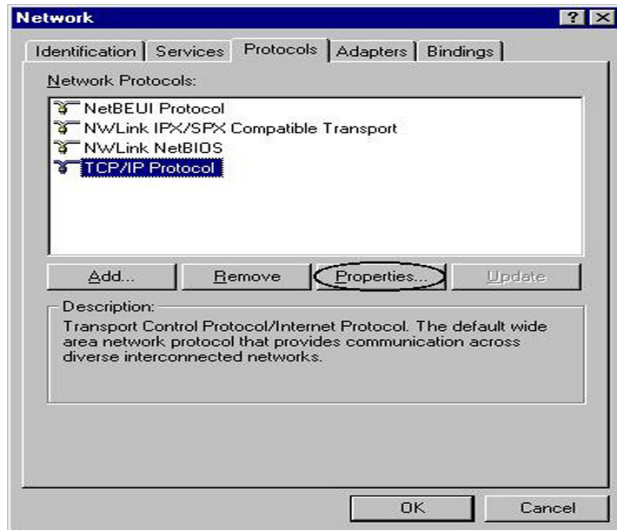
1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network** and choose the **Configuration** tab.
2. Select **TCP/IP ->NE2000 Compatible**, or the name of your Network Interface Card (NIC) in your PC.
3. Select the **Obtain an IP address automatically** radio button.
4. Then select the **DNS Configuration** tab.
5. Select the **Disable DNS** radio button and click **OK** to finish the configuration.



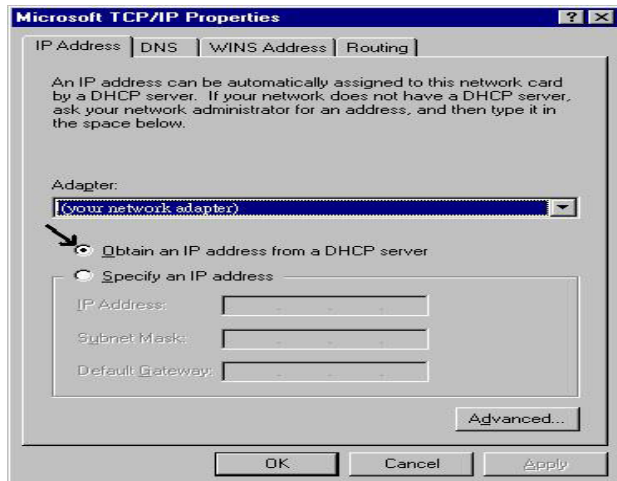
Configuring PC in Windows NT4.0

1. Go to **Start / Settings / Control Panel**.
In the Control Panel, double-click on **Network** and choose the **Protocols** tab.

2. Select **TCP/IP Protocol** and click **Properties**.



3. Select the **Obtain an IP address from a DHCP server** radio button and click **OK**.



Factory Default Settings

Before configuring the Billion SG6200NXL router, you need to know the following default settings.

Web Interface: (Username and Password)

- ▶ Username: admin
- ▶ Password: admin

The default username and password are “**admin**” and “**admin**” respectively.



Attention

If you ever forget the username/password to login to the router, you may press the RESET button up to 6 seconds then release it to restore the factory default settings.

Caution: After pressing the RESET button for more than 6 seconds then release it, to be sure you power cycle the device again.

Device LAN IP settings

- ▶ IP Address: 192.168.1.254
- ▶ Subnet Mask: 255.255.255.0

ISP setting in WAN site

- ▶ Obtain an IP Address Automatically

DHCP server

- ▶ DHCP server is enabled.
- ▶ Start IP Address: 192.168.1.100
- ▶ IP pool counts: 100

LAN and WAN Port Addresses

The parameters of LAN and WAN ports are preset at the factory. The default values are shown below.

| LAN Port | | WAN Port |
|--------------------------------------|--|---|
| IP address | 192.168.1.254 | The DHCP function is <i>enabled</i> to automatically get the WAN port configuration from the ISP. |
| Subnet Mask | 255.255.255.0 | |
| DHCP server function | Enabled in ports 1, 2 and 3 | |
| IP addresses for distribution to PCs | 100 IP addresses continuing from 192.168.1.100 through 192.168.1.199 | |

Information from your ISP

Before configuring this device, you have to check with your ISP (Internet Service Provider) what kind of services are provided, such as PPPoE, Obtain an IP Address Automatically, Fixed IP address.

Gather the information as illustrated in the following table and keep it for reference.

| | |
|---|---|
| PPPoE | Username, Password, Service Name, and Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually). |
| Obtain an IP Address Automatically | DHCP Client (it can be automatically assigned by your ISP when you connect or be set manually). |
| Fixed IP Address | IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is fixed IP address). |

Configuring with your Web Browser

Open your web browser, enter the IP address of your router, which by default is **192.168.1.254**, and click **Go**, a user name and password window prompt appears. Enter the user name and password that your **Administrator** has set for you and select the **Account Type**, then click **Login**. When you are authorised, you will access to the router. The default username and password are **“admin”** and **“admin”** respectively for the Administrator account type.



BILLION

Smart Energy Gateway

Username

Password







Account Administrator ▾

Login

Congratulations! You have successfully logged on to your Billion SG6200NXL Smart Energy Gateway!

Chapter 4: Basic Configuration

Once you have logged on to your Billion SG6200NXL Smart Energy Gateway via your web browser, you can begin to set it up according to your requirements. On the configuration homepage, the left navigation pane links you directly to the setup pages, which includes:

-  **Advanced** (Switch to Advanced Configuration mode)
-  **Status**
-  **Quick Start**
-  **WAN**
-  **WLAN**
-  **Language**

Status

Device Information

| | |
|------------------|------------------|
| Model Name | SG6200NXL |
| System Up-Time | 9 min(s) |
| Software Version | 1.04.ha.dc24 |
| ZigBee Firmware | rsp-hazc-1.0.8 |
| ZigBee EUI64 | 000D6F00007588C2 |

Port Status

| | |
|----------------|---|
| Ethernet | ✓ |
| EWAN | ✓ |
| 3G | ✗ |
| WirelessClient | ✗ |
| Wireless | ✓ |

WAN

| Port | Protocol | Operation | Connection | IP Address | Netmask | Gateway | Primary DNS |
|------|----------|---|------------|--------------|---------------|--------------|--------------|
| EWAN | Dynamic | <input type="button" value="Renew"/> <input type="button" value="Release"/> | | 172.16.1.194 | 255.255.255.0 | 172.16.1.254 | 172.16.1.254 |

Device Information

Model Name: Provide a name for the router for identification purposes.

System Up-Time: Record system up-time.

Software Version: Firmware version.

ZigBee Firmware: the ZigeBee firmware version.

ZigBee EUI64: 64-bit Global Identifier for ZigBee, can be viewed as MAC of ZigBee.

Port Status

Port Status : User can look up to see if they are connected to Ethernet, EWAN, 3G, WirelessClient and Wireless.

WAN

Port: Name of the WAN connection.

Protocol: PPPoE, Dynamic or Fixed.

Operation: Current available operation.

Connection: The current connection status.

Netmask: WAN port IP subnet mask.

Gateway: The IP address of the default gateway.

IP Address: WAN port IP address.

Primary DNS: The IP address of the primary DNS server.

Quick Start

Quick Start

Time Zone

Parameters

| | |
|------------------------------|---|
| Time Zone | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Local Time Zone (+-GMT Time) | (GMT) Greenwich Mean Time |

Continue

Quick Start

WAN Port (WAN > Wireless > BEsmart Register)

Select WAN Port

| | |
|--------------|------------------------------------|
| Connect Mode | EWAN (Recommended) |
| Protocol | Obtain an IP Address Automatically |

Continue Jump to Wireless setting Jump to BEsmart Register

Set Wireless configuration

Quick Start

Wireless (WAN > Wireless > BEsmart Register)

Set Wireless configuration.

| | |
|-------------------|---|
| WLAN Service | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| ESSID | wlan-ap |
| Channel ID | Channel 1 (2.412 GHz) |
| Security Mode | Disable |
| Regulation Domain | N.America |

Continue

WLAN Service: Default setting is set to **Enable**.

ESSID: The ESSID is the unique name of a wireless access point (AP) to be distinguished from another. For security purpose, change to a unique ID name to the AP which is already built-in to the router's wireless interface. It is case sensitive and must not exceed 32 characters. Make sure your wireless clients have exactly the ESSID as the device, in order to get connected to your network.

Channel ID: Select the ID channel that you would like to use.

Security Mode: You can disable or enable with WPA or WEP for protecting wireless network. The default mode of wireless security is **Disable**.

BEsmart Register

Billion BEsmart offers controlling and monitoring of the power energy consumption using the latest energy monitoring technologies. With the implementation of the BEsmart service, energy usage can be clearly examined and analyzed anytime and anywhere simply through a smart phone. It helps reduce energy waste, provide a green environment, and further increase the benefit for the mutual investment for both investors and customers, which is an optimal choice for Telco/ISP/SI service providers.

Quick Start

BEsmart Register (WAN > Wireless > BEsmart Register)

Parameters

Username

Password

Re-type Password

Email

Terms of Service:

Please read the Terms of Service below:
Billion "BEsmart" Terms of Use

The BEsmart (the "Service") belongs to a product/service of Billion (Billion Electric Co., Ltd.). The Service includes App and any or all of its components. By using the Service, it also indicates that you (the "User") accept to be bound by the following terms and conditions and that you agree to abide by them. These terms and policies are in effect throughout the full duration of your use of the Site and Service, so if you do not agree with these Terms of Use, we suggest you should stop downloading, installing or using the service right away.

1. Account and Password
Upon registration, we will provide you with a login identifier and a password in order to access the site and use the service. Please be responsible for safeguarding such information from disclosure and for unauthorized use for your own rights and interests. You are fully and solely responsible for all people, including yourself or the third

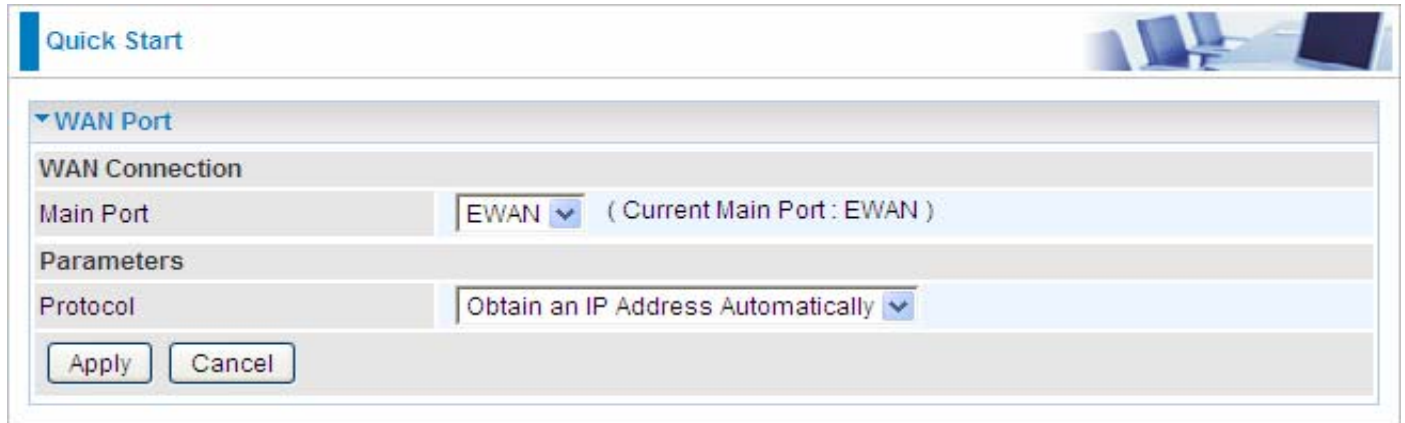
I accept the Terms of Service.

Apply

See [BEsmart registration](#).

WAN

EWAN



Quick Start

▼ WAN Port

WAN Connection

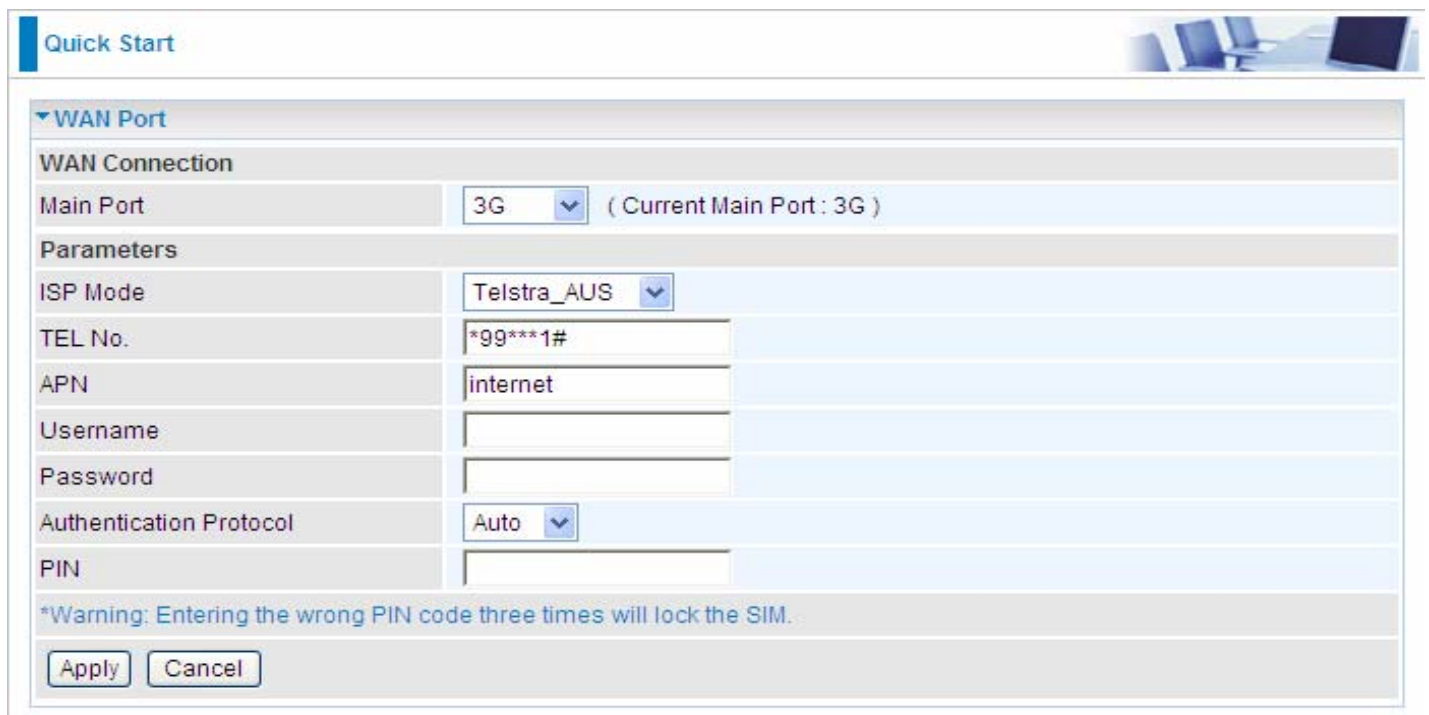
Main Port: EWAN (Current Main Port : EWAN)

Parameters

Protocol: Obtain an IP Address Automatically

Apply Cancel

3G



Quick Start

▼ WAN Port

WAN Connection

Main Port: 3G (Current Main Port : 3G)

Parameters

ISP Mode: Telstra_AUS

TEL No.: *99***1#

APN: internet

Username:

Password:

Authentication Protocol: Auto

PIN:

*Warning: Entering the wrong PIN code three times will lock the SIM.

Apply Cancel

APN: An APN is similar to a URL on the WWW, it is what the unit makes a GPRS / UMTS call. The service provider is able to attach anything to an APN to create a data connection. Requirements for APN assignment varies between different service providers. Most service providers have an internet portal which they connect a DHCP Server to, giving you access to the internet i.e. Some 3G operators use the APN 'internet' for their portal. The default value of APN is "internet".

Username: Enter the username provided by your service provider.

Password: Enter the password provided by your service provider.

Auth. Protocol: Manually specify CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol) if you know which authentication type the server is using (when acting as a client), or the authentication type you want the clients to use when they are connecting to you (when acting as a server). When using PAP, the password is sent unencrypted, while CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that an intruder has not replaced the client.

PIN: PIN stands for Personal Identification Number. A PIN code is a numeric value used in certain systems as a password to gain access, and authentication. In mobile phones a PIN code locks the SIM card until you enter the correct code. If you enter the PIN code incorrectly into the phone 3 times in a row, then the SIM card will be blocked and a PUK code will be required from your network / service provider to unlock it.



When insert 3G card, you should wait 30 seconds then dial up; or you can dial up first then insert 3G card after 30 seconds.
If there is an error occurs while you don't operate according to the above, pull out the 3G card or restart the router will solve this problem.

WirelessClient

When WirelessClient is select, the router will act as an ordinary wireless client to connect to an AP to connect to the Internet.

Quick Start

WAN Port

WAN Connection

Main Port: WirelessClient (Current Main Port : APCLIENT)

Parameters

Protocol: Obtain an IP Address Automatically

NAT: Enable

Obtain DNS: Automatic Primary Secondary

SSID: billion-ap

Security Mode: WPA2PSK

Encryption Type: AES

Pass Phrase:

Continue Cancel SCAN

Site Survey

| Ch | SSID | BSSID | Security | Signal(%) | W-Moe | ExtCh | NT | |
|----------------------------------|------|------------|-------------------|----------------|-------|---------|-------|----|
| <input type="radio"/> | 7 | Altratek | 00:04:ed:11:22:68 | WPAPSK/TKIPAES | 20 | 11b/g/n | ABOVE | In |
| <input type="radio"/> | 7 | CMCC | 00:04:ed:11:22:69 | NONE | 15 | 11b/g/n | ABOVE | In |
| <input checked="" type="radio"/> | 7 | billion-ap | 02:10:18:01:00:02 | WPA2PSK/AES | 24 | 11b/g/n | NONE | In |
| <input type="radio"/> | 10 | SSID1 | d8:42:ac:a7:41:34 | NONE | 10 | 11b/g/n | BELOW | In |
| <input type="radio"/> | 10 | SSID2 | d8:42:ac:a7:41:35 | NONE | 20 | 11b/g/n | BELOW | In |

Protocol: Select to obtain an IP address automatically or choose to set a fixed IP for your gateway.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single ISP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

Obtain DNS: Choose Automatic or set the exact values yourself.

SSID: The target wireless AP. User can alternatively input the SSID manually or also use the Scan button to scan and select.

Security Mode: Set the wireless security mode, namely, OPEN, SHARED, WPAPSK and WPA2PSK. User can set the mode yourself if well knowing the mode, or user can choose to scan button and select the target SSID.

Encryption Type: TKIP (Temporal Key Integrity Protocol) / AES (Advanced Encryption Standard).

Pass Phrase: The pre-set phrase key for authentication.

Continue: Move on to connect to the SSID.

Cancel: undo the current step.

SCAN: Press this button to scan the SSIDs in the air.

WLAN

The screenshot shows the 'Configuration' page for WLAN. Under the 'WLAN' section, there are two main areas: 'Wireless Parameters' and 'Security Parameters'. In 'Wireless Parameters', 'WLAN Service' is set to 'Enable' (radio button selected), 'ESSID' is 'wlan-ap', 'Hide ESSID' is 'Disable' (radio button selected), 'Regulation Domain' is 'N.America', and 'Channel ID' is 'Channel 1 (2.412 GHz)'. In 'Security Parameters', 'Security Mode' is 'Disable'. At the bottom, there are 'Apply' and 'Cancel' buttons.

WLAN Service: Default setting is set to **Enable**.

ESSID: The ESSID is the unique name of a wireless access point (AP) to be distinguished from another. For security propose, change to a unique ID name to the AP which is already built-in to the router's wireless interface. It is case sensitive and must not excess 32 characters. Make sure your wireless clients have exactly the ESSID as the device, in order to get connected to your network.

Note: ESSID is case sensitive and must not excess 32 characters.

Hide ESSID: It is function in which transmits its ESSID to the air so that when wireless client searches for a network, router can then be discovered and recognized. Default setting is **Disable**.

Ⓐ **Enable:** Select Enable if you do not want broadcast your ESSID. When select Enable, no one will be able to locate the Access Point (AP) of your router.

Ⓑ **Disable:** When Disable is selected, you can allow anybody with a wireless client to be able to locate the Access Point (AP) of your router.

Regulation Domain: There are seven Regulation Domains for you to choose from, including **North America (N.America)**, **Europe**, **France**, etc. The Channel ID will be different based on this setting.

Channel ID: Select the ID channel that you would like to use.

Security Mode: You can disable or enable with WPA or WEP for protecting wireless network. The default mode of wireless security is **Disable**.

Security Parameters

● WPA Pre-Shared Key

The screenshot shows the 'Security Parameters' configuration page. 'Security Mode' is set to 'WPA Pre-Shared Key'. The 'WPA Shared Key' field is empty. 'Group Key Renewal' is set to '3600 seconds'. At the bottom, there are 'Apply' and 'Cancel' buttons.

WPA Shared Key: The key for network authentication. The input format is in character style and the

key size should be in the range between 8 and 63 characters.

Group Key Renewal: The period of renewal time for changing the security key between wireless client and Access Point (AP). This process is done automatically.

● WPA2 Pre-Shared Key

| Security Parameters | |
|--|-----------------------|
| Security Mode | WPA2 Pre-Shared Key ▾ |
| WPA Shared Key | <input type="text"/> |
| Group Key Renewal | 3600 seconds |
| <input type="button" value="Apply"/> <input type="button" value="Cancel"/> | |

WPA Shared Key: The key for network authentication. The input format is in character style and key size should be in the range between 8 and 63 characters.

Group Key Renewal: The period of renewal time for changing the security key between wireless client and Access Point (AP). This process is done automatically.

● WPA/WPA2 Pre-Shared Key

| Security Parameters | |
|--|---------------------------|
| Security Mode | WPA/WPA2 Pre-Shared Key ▾ |
| WPA Shared Key | <input type="text"/> |
| Group Key Renewal | 3600 seconds |
| <input type="button" value="Apply"/> <input type="button" value="Cancel"/> | |

WAP Shared Key: The key for network authentication. The input format is in character style and key size should be in the range between 8 and 63 characters.

Group Key Renewal: The period of renewal time for changing the security key between wireless client and Access Point (AP). This process is done automatically.

WEP

| Security Parameters | |
|---|--|
| Security Mode | WEP |
| WEP Authentication | Open System |
| Default Used WEP Key | <input checked="" type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4 |
| Passphrase (Generate Key) | <input type="text"/> <input type="button" value="WEP64"/> <input type="button" value="WEP128"/> |
| Key 1 | Hex <input type="text"/> |
| Key 2 | Hex <input type="text"/> |
| Key 3 | Hex <input type="text"/> |
| Key 4 | Hex <input type="text"/> |
| <small>WEP 64 - Hex: 10 Hex codes, (1~9, a~f, A~F). EX: 11aa22cc33. WEP 64 - ASCII: 5 ASCII characters are required. Insert your WEP key manually. EX: 1a3eb. WEP 128 - Hex: 26 Hex codes, (1~9, a~f, A~F). EX: 11aa22cc33dd44ee55efffe35f. WEP 128 - ASCII: 13 ASCII characters are required. Insert your WEP key manually. EX: 1a3e?!dbd3ert.</small> | |
| <input type="button" value="Apply"/> <input type="button" value="Cancel"/> | |

WEP Authentication: To prevent unauthorized wireless stations from accessing data transmitted over the network, the router offers secure data encryption, known as WEP. If you require high security for transmissions, there are three options to select from: **Open System**, **Share key** or **Both**.







Default Used WEP Key: Select the encryption key ID; please refer to **Key (1~4)** below.

Passphrase: This is used to generate WEP keys automatically based upon the input string and a pre-defined algorithm in WEP64 or WEP128. You can input the same string in both the AP and Client card settings to generate the same WEP keys. Please note that you do not have to enter **Key (1-4)** as below when the **Passphrase** is enabled.

Key (1-4): Enter the key to encrypt wireless data. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as the router. There are four keys for your selection. The input format is in HEX or ASCII style, 5 and 13 ASCII codes are required for WEP64 and WEP128 respectively-no any separator is included.

Chapter 5: Advanced Configuration

Once you have logged on to your Billion SG6200NXL Router via your web browser, you can begin to set it up according to your requirements. On the configuration homepage, the left navigation pane links you directly to the setup pages, which include:

-  **Basic** (Switch to Basic Configuration Mode)
-  **Status** (BEsmart Status, ZigBee Status, Power Status, Sensor Status, RS485 Status, Wireless Status, 3G Status, ARP Table, DHCP Table, System Log, Firewall Log, UPnP Portmap)
-  **Quick Start**
-  **Power Management** (Meter Config, Power Control, RS485 Config, Control Rules, Mail Alert)
-  **Configuration** (LAN, WAN, System, Firewall, QoS, Virtual Server, Wake on LAN, Time Schedule and Advanced)
-  **Language**

The following sections provide an overview of the settings available for configuring your router.

Status

Device Information

| | |
|------------------|--------------------------|
| Model Name | SG6200NXL |
| Host Name ▶ | home.gateway |
| System Up-Time | 10 min(s) |
| Current Time ▶ | Thu Mar 13 05:45:11 2014 |
| Software Version | 1.04.ha.dc24 |
| MAC Address | 00:04:ed:30:52:62 |
| ZigBee Firmware | rsp-hazc-1.0.8 |
| ZigBee EUI64 | 000D6F00007588C2 |

Port Status

| | |
|----------------|---|
| Ethernet | ✓ |
| EWAN | ✓ |
| 3G ▶ | ✗ |
| WirelessClient | ✗ |
| Wireless ▶ | ✓ |

WAN

| Port▶ | Protocol | Operation | Connection | IP Address | Netmask | Gateway | Primary DNS |
|-------|----------|---|------------|--------------|---------------|--------------|--------------|
| EWAN▶ | Dynamic | <input type="button" value="Renew"/> <input type="button" value="Release"/> | | 172.16.1.194 | 255.255.255.0 | 172.16.1.254 | 172.16.1.254 |

Device Information

Model Name: Display the model name.

Host Name: Provide a name for the router for identification purposes. Host Name lets you change the router name.

System Up-Time: Record system up-time.

Current time: Set the current time. See the Time Zone section for more information.

Software Version: Firmware version.

MAC Address: The LAN MAC address.

ZigBee Firmware: the ZigeBee firmware version.

ZigBee EUI64: 64-bit Global Identifier for ZigBee, can be viewed as MAC of ZigBee.

Port Status

Port Status : User can look up to see if they are connected to Ethernet, EWAN, 3G, WirelessClient and Wireless.

WAN

Port: Name of the WAN connection.

Operation: Current available operation.

Connection: The current connection status.


IP Address: WAN port IP address.

Net mask: WAN port IP subnet mask.

Gateway: The IP address of the default gateway.

Primary DNS: The IP address of the primary DNS server.

BEsmart Status

Status 

▼ BEsmart Status

Parameters

| | |
|-----------|-----------------------|
| Device ID | 0004EDFFFE305262 |
| Status | Gateway Login Success |

Device ID: Show the unique ID of the device.

Status: Show whether the device is registered.

ZigBee Status



The screenshot shows a web interface with a 'Status' tab. Underneath, there is a section titled 'Zigbee Status' which contains a table of parameters. The parameters listed are Status (Joined Network), Channel (14), PAN ID (aefb), EUI address (000D6F00007588C2), and Version (rsp-hazc-1.0.8). A 'Refresh' button is located at the bottom of the table.

| Parameters | |
|-------------|------------------|
| Status | Joined Network |
| Channel | 14 |
| PAN ID | aefb |
| EUI address | 000D6F00007588C2 |
| Version | rsp-hazc-1.0.8 |

Status: The ZigBee status.

Channel: The using ZigBee Channel. 16 channels are designed in the 2.4GHz radio band.

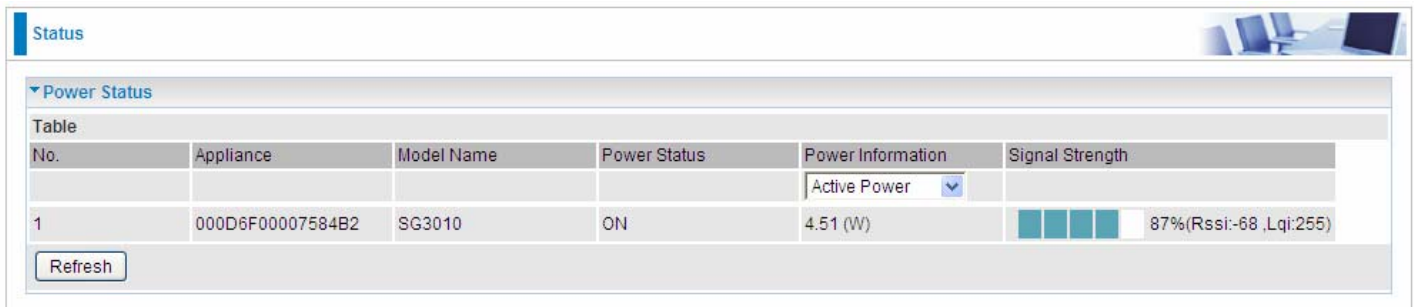
PAN ID: The PAN ID is a 14 bit string that identifies the unique ZigBee network.

EUI address: 64-bit Global Identifier for ZigBee, can be viewed as MAC of ZigBee.


Version: ZigBee firmware version.

Power Status

You can view the status information for each device through ZigBee status.



The screenshot shows a web interface with a 'Status' tab. Underneath, there is a 'Power Status' section containing a table. The table has columns for 'No.', 'Appliance', 'Model Name', 'Power Status', 'Power Information', and 'Signal Strength'. A single row is visible with the following data: No. 1, Appliance 000D6F00007584B2, Model Name SG3010, Power Status ON, Power Information 4.51 (W) (with a dropdown menu set to 'Active Power'), and Signal Strength 87%(Rssi:-68 ,Lqi:255). A 'Refresh' button is located below the table.

| No. | Appliance | Model Name | Power Status | Power Information | Signal Strength |
|-----|------------------|------------|--------------|-------------------|--|
| 1 | 000D6F00007584B2 | SG3010 | ON | 4.51 (W) |  87%(Rssi:-68 ,Lqi:255) |

No.: The sequence number.

Appliance: Display the EUI 64 or the specified alias (if set) of the corresponding SmartMeter.

Model Name: Show the model name of the meter.


Power Status: Indicate the current status of the devices, ON or OFF.

Power Information: Display the current power information of the specific selected item. Select the item you want to check. Here 7 aspects are provided for users to check the power usage information: Voltage, Current, Frequency, Active power, Apparent Power and Main Energy.

Signal Strength: Display the Signal of the Smart Meter


Refresh: Press **Refresh** to check the latest power status.

Sensor Status

Status 

▼ Sensor Status

Table

| No. | Device ID | Appliance | Model Name | Temperature | Humidity | Signal Strength |
|-----|------------------|------------|------------|-------------|----------|---|
| 1 | 00158D00001C066E | SG100TH-RT | SG100TH-RT | 23.75 | 47.81 |  100%(Rssi:-42 ,Lqi:255) |

No.: Number marked for connected sensor devices.

Device ID: The device id of each connected sensor device.

Appliance Name: User-defined name for connected device.


Temperature: The current temperature detects by sensor.

Humidity: The current humidity detects by sensor.

Signal Strength: Show the current Zigbee wireless signal strength.

RS485 Status

RS485 Status lists the status of connected RS 485 smart instruments.

Status 


▼ RS485 Status

Address

| Attribute | Value | Attribute | Value |
|-----------|-------|-----------|-------|
|-----------|-------|-----------|-------|

Wireless Status

Wireless status shows users wireless connecting information including “WirelessClient Status”, “STAINfo” and “WDSInfo”.

Status 

▼ Wireless Status

| | |
|-----------------------|------------|
| WirelessClient Status | Disconnect |
|-----------------------|------------|

▼ STAINfo

| MAC | Physical mode | Idle | Rate | RSSI0 | RSSI1 |
|-------------------|---------------|------|--------|------------|-----------|
| 00:18:DE:CE:8F:5B | CCK | 300 | 5 Mbps | -82 (20 %) | -92 (0 %) |

▼ WDSInfo

| MAC | Physical mode | RSSI0 | RSSI1 |
|-----|---------------|-------|-------|
|-----|---------------|-------|-------|

3G Status

This section displays the 3G Card overall status with information such as the current signal strength, statistics of current data transmission and total data transmission.

Status 

▼ 3G Status

Parameters

| | |
|----------------------------|---|
| Status ▶ | Up |
| Signal Strength |  |
| Network Name | N/A |
| Card Name | 119 |
| Card Firmware | +CGMR:AC8710_V3_LU9A7690_CTAT |
| Card IMEI | 0x90472CCB |
| Current TX Bytes / Packets | 29K / 0.3K |
| Current RX Bytes / Packets | 67.2K / 0.2K |
| Total TX Bytes / Packets | 29K / 0.3K |
| Total RX Bytes / Packets | 67.2K / 0.2K |

3G usage allowance

| | |
|----------------|--|
| Amount used |  NaNHours of Hours |
| Billing period |  Day:NaN |

Status: The current status of the 3G card. Click this link to configure 3G. For detail, turn to [Main Port 3G](#) section for help.

Signal Strength: The signal strength bar indicates the current 3G signal strength.

Network Name: The network name that the device is connected to.

Card Name: The name of the 3G card.

Card Firmware: The current firmware of the 3G card.

Card IMEI: The unique identification number that is used to identify the 3G card.

Current TX Bytes / Packets: The statistics of data transmission in bytes / packets during a call.

Current RX Bytes / Packets: The statistics of data received in bytes / packets during a call.

Total TX Bytes / Packets: The statistics of total data transmission in bytes / packets since system ready.

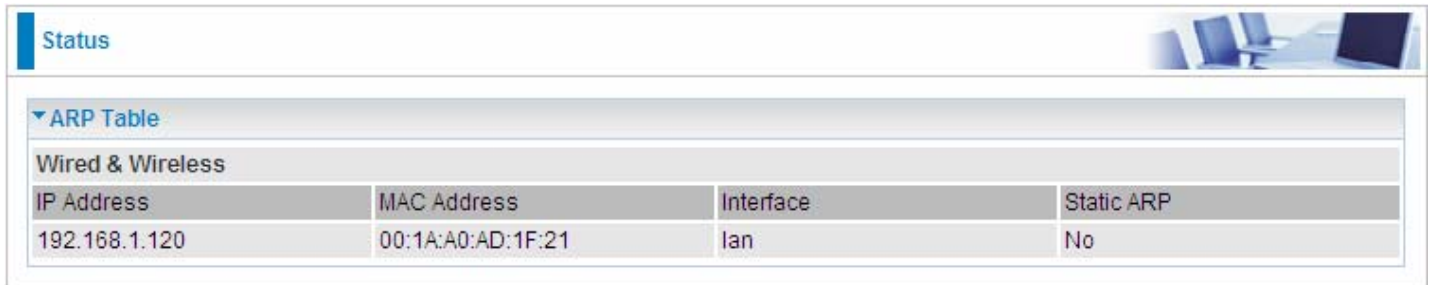
Total RX Bytes / Packets: The statistics of total data received in bytes / packets since system ready.

Amount used: Show the traffic or hours has been used.

Billing preiod: The day from which the fee is charged.

ARP Table

This section displays the router's ARP (Address Resolution Protocol) Table, which shows the mapping of Internet (IP) addresses to Ethernet (MAC) addresses. This is useful as a quick way of determining the MAC address of the network interface of your PCs to use with the router's **Firewall - MAC Address Filter** function. See the Firewall section of this manual for more information on this feature.



| IP Address | MAC Address | Interface | Static ARP |
|---------------|-------------------|-----------|------------|
| 192.168.1.120 | 00:1A:A0:AD:1F:21 | lan | No |

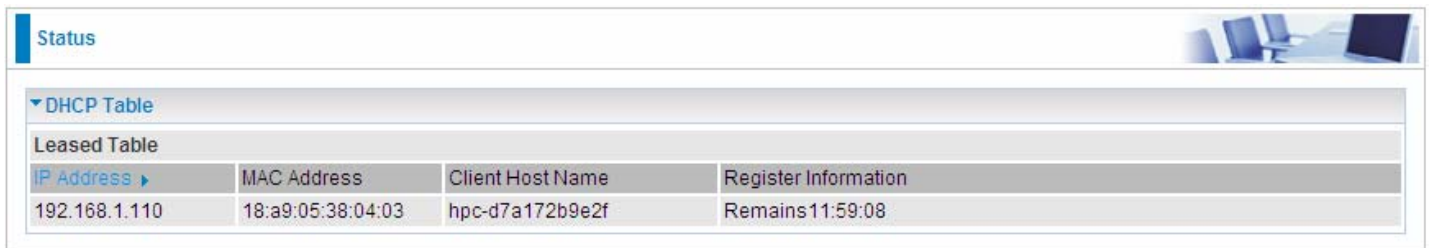
IP Address: It is IP Address of internal host that join this network.

MAC Address: The MAC address of internal host.

Interface: The ARP interface.

Static ARP: The state for ARP.

DHCP Table



| IP Address | MAC Address | Client Host Name | Register Information |
|---------------|-------------------|------------------|----------------------|
| 192.168.1.110 | 18:a9:05:38:04:03 | hpc-d7a172b9e2f | Remains 11:59:08 |

IP Address: The current corresponding DHCP-assigned dynamic IP address of the device. Click this link to configure DHCP Server, for more information, See [DHCP Server](#) section.

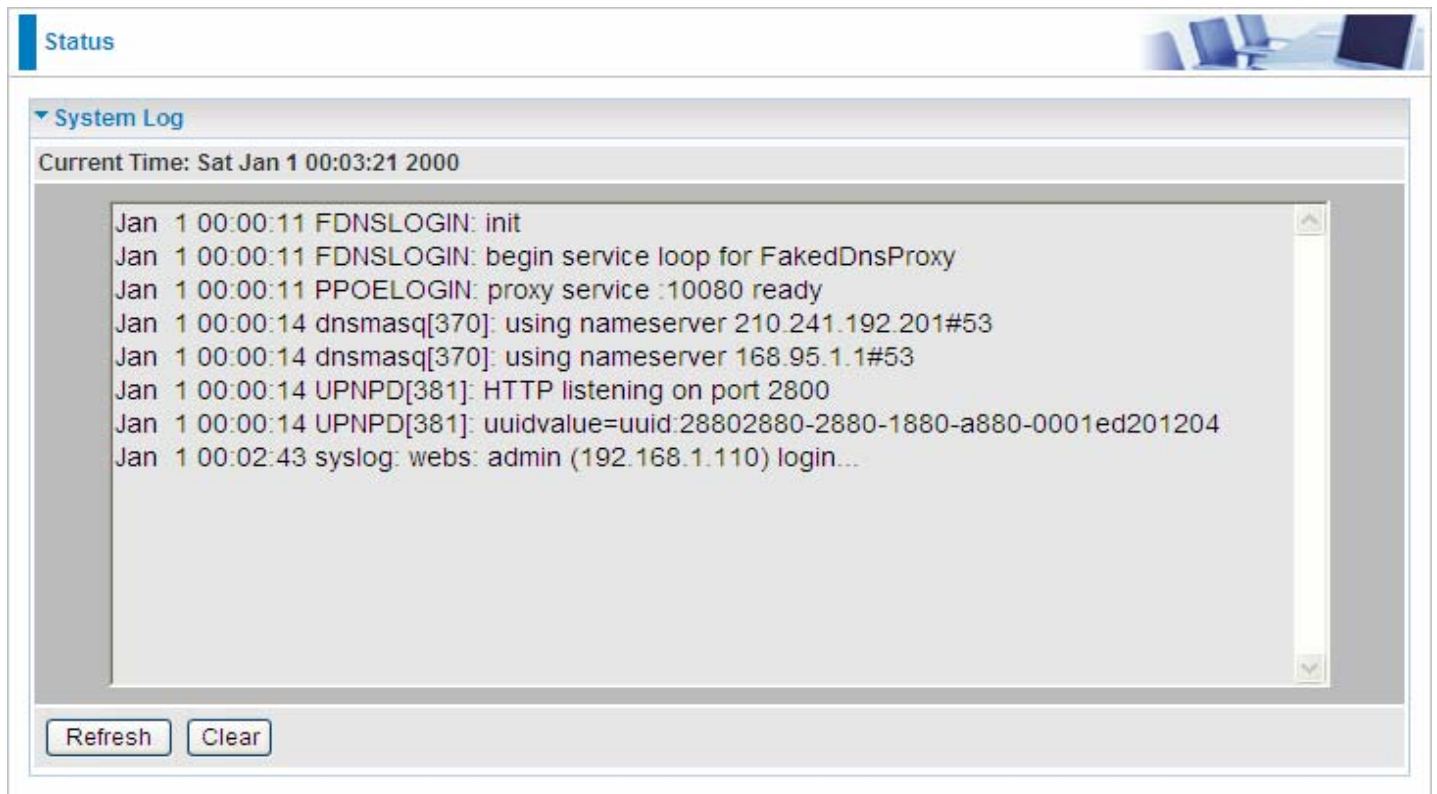
MAC Address: The MAC Address of internal DHCP client host.

Client Host Name: The Host Name of internal DHCP client.

Register Information: Register time information.

System Log

Display system logs accumulated up to the present time. You can trace historical information with this function.



The screenshot shows a web interface with a 'Status' header and a 'System Log' section. The current time is 'Sat Jan 1 00:03:21 2000'. The log contains the following entries:

```
Jan 1 00:00:11 FDNSLOGIN: init
Jan 1 00:00:11 FDNSLOGIN: begin service loop for FakedDnsProxy
Jan 1 00:00:11 PPOELOGIN: proxy service :10080 ready
Jan 1 00:00:14 dnsmasq[370]: using nameserver 210.241.192.201#53
Jan 1 00:00:14 dnsmasq[370]: using nameserver 168.95.1.1#53
Jan 1 00:00:14 UPNPD[381]: HTTP listening on port 2800
Jan 1 00:00:14 UPNPD[381]: uuidvalue=uuid:28802880-2880-1880-a880-0001ed201204
Jan 1 00:02:43 syslog: webs: admin (192.168.1.110) login...
```

At the bottom of the log area are 'Refresh' and 'Clear' buttons.

Firewall Log

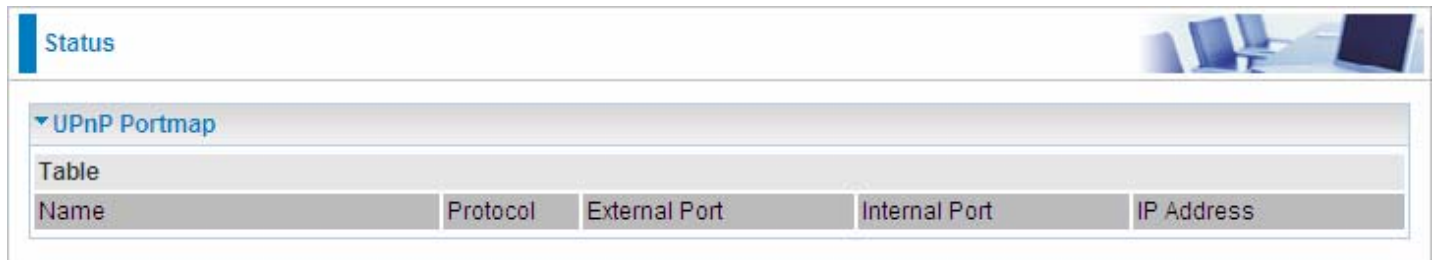
Firewall Log displays log information of any unexpected action with your firewall settings. This page displays the router's Firewall Log entries. The log shows log entries when you have enabled Intrusion Detection or Block WAN PING in the **Configuration - Firewall** section of the interface. Please see the **Firewall** section of this manual for more details on how to enable Firewall logging.



The screenshot shows a web interface with a 'Status' header and a 'Firewall Log' section. The current time is 'Sat Jan 1 03:37:31 2000'. The log area is currently empty. At the bottom of the log area are 'Refresh' and 'Clear' buttons.

UPnP Portmap

The section lists all port-mapping established using UPnP (Universal Plug and Play). Please see the Advanced section of this manual for more details on UPnP and the router's UPnP configuration options.



The screenshot shows a web interface with a 'Status' tab selected. Below it, there is a section titled 'UPnP Portmap' which contains a table. The table has five columns: Name, Protocol, External Port, Internal Port, and IP Address. The table is currently empty.

Name: The name of this UPnP mapping.

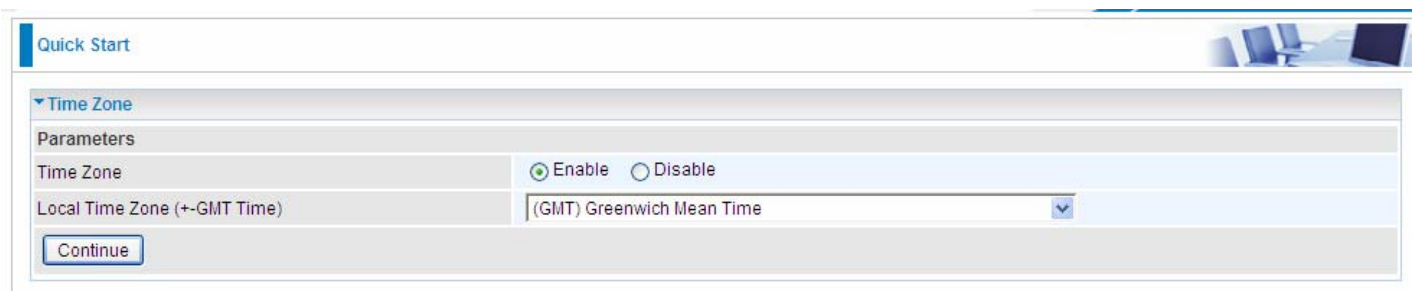
Protocol: The protocol used by this mapping.

External Port: The external service port the internal port mapped to.

Internal Port: The internal service port.

IP Address: The IP Address of the host in LAN.

Quick Start



Quick Start

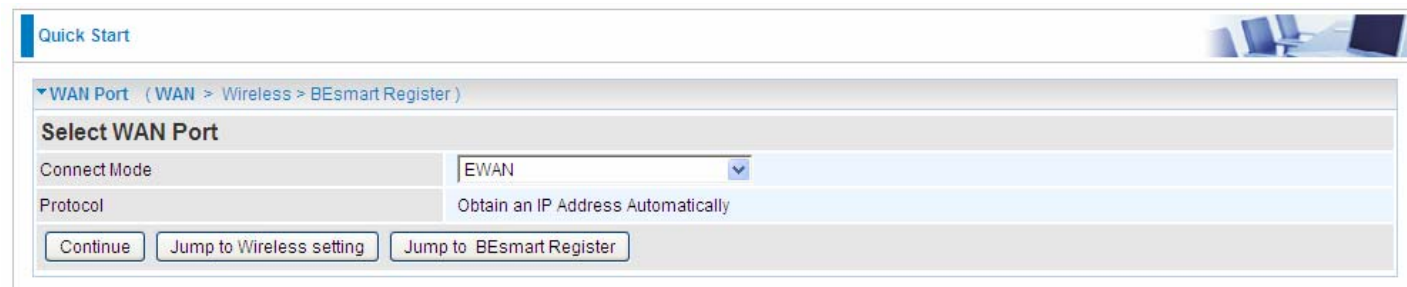
Time Zone

Parameters

Time Zone Enable Disable

Local Time Zone (+-GMT Time) (GMT) Greenwich Mean Time

Continue



Quick Start

WAN Port (WAN > Wireless > BEsmart Register)

Select WAN Port

Connect Mode EWAN

Protocol Obtain an IP Address Automatically

Continue Jump to Wireless setting Jump to BEsmart Register

Select connection mode to continue, or click **Jump to Wireless Setting** or **Jump to BEsmart Register to Register** BEsmart service account.

3G



Quick Start

WAN Port (WAN > Wireless > BEsmart Register)

Select WAN Port

Connect Mode 3G

TEL No. *99***1#

Username

APN internet

Continue Jump to Wireless setting Jump to BEsmart Register

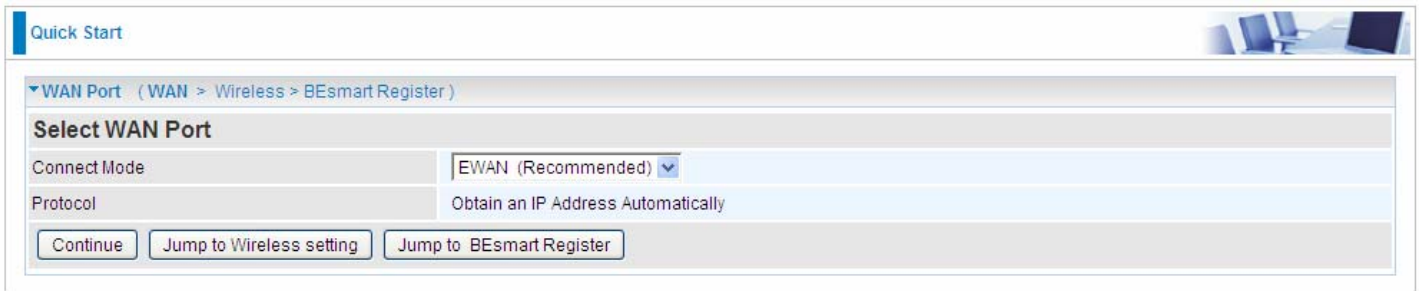
Connect mode: 3G

TEL No.: The dial string to make a GPRS / 3G user internetworking call. It may be provided by your mobile service provider.

Username: Enter the username provided by your service provider.

APN: An APN is similar to a URL on the WWW, it is what the unit makes a GPRS / UMTS call. The service provider is able to attach anything to an APN to create a data connection. Requirements for APN assignment varies between different service providers. Most service providers have an internet portal which they connect a DHCP Server to, giving you access to the internet i.e. Some 3G operators use the APN 'internet' for their portal. The default value of APN is "internet".

EWAN



The screenshot shows a web-based configuration interface. At the top left, there is a 'Quick Start' link. Below it, a breadcrumb trail reads 'WAN Port (WAN > Wireless > BEsmart Register)'. The main section is titled 'Select WAN Port'. It contains two rows of settings: 'Connect Mode' is set to 'EWAN (Recommended)' with a dropdown arrow, and 'Protocol' is set to 'Obtain an IP Address Automatically'. At the bottom of this section, there are three buttons: 'Continue', 'Jump to Wireless setting', and 'Jump to BEsmart Register'.

Connect mode: EWAN

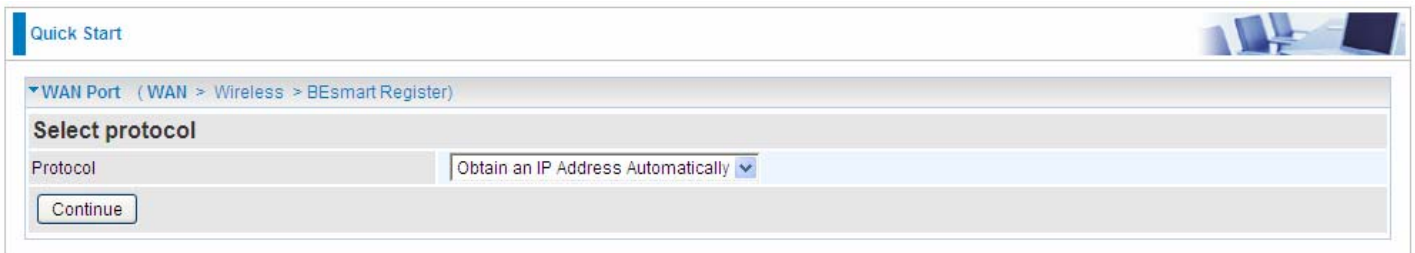
Protocol: The current protocol in the device.

Click on **Continue** to choose the Protocol to connect with EWAN.

Protocol: Obtain an IP Address Automatically to connect and setup wireless settings at the same time.

● Obtain an IP Address Automatically


When connecting to the ISP, Billion SG6200NXL also functions as a DHCP client. Billion SG6200NXL can automatically obtain an IP address, subnet mask, gateway address, and DNS server addresses if the ISP assigns this information via DHCP.



The screenshot shows the 'Quick Start' section of the router's web interface. The breadcrumb trail is 'WAN Port > (WAN > Wireless > BEsmart Register)'. The main heading is 'Select protocol'. Below this, there is a 'Protocol' dropdown menu with 'Obtain an IP Address Automatically' selected. A 'Continue' button is located at the bottom left of the configuration area.

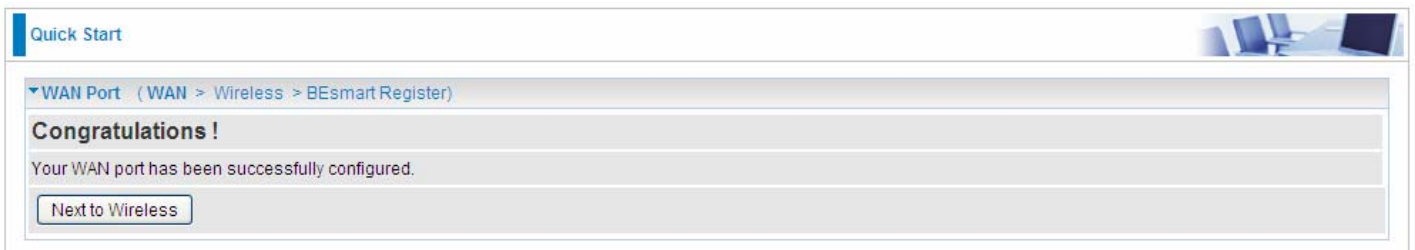
Protocol: The current protocol in the device

Click on the **Continue** button and wait for your connection to be connected.



The screenshot shows the 'Quick Start' section of the router's web interface. The breadcrumb trail is 'WAN Port > (WAN > Wireless > BEsmart Register)'. The main heading is 'Please wait while the device is configured...'. This is a status message indicating that the configuration process is in progress.

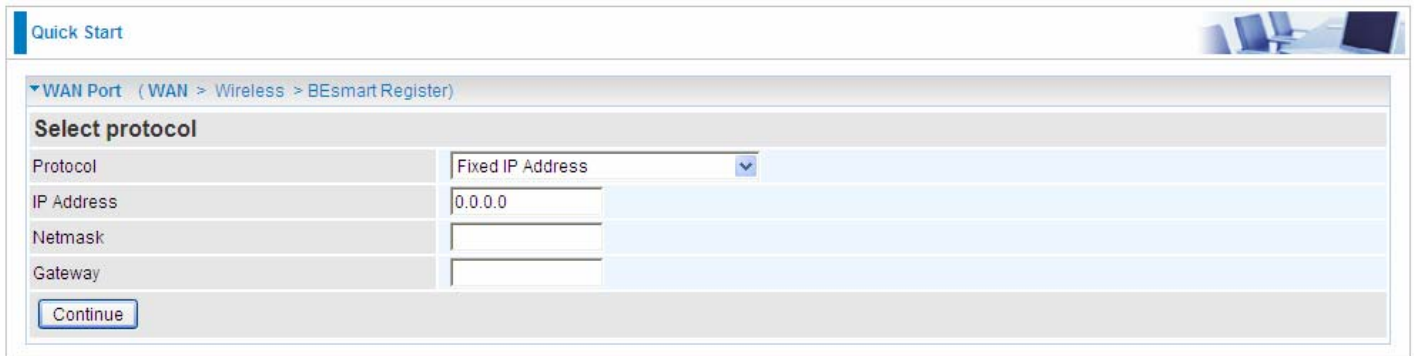
If connection is successful the following image will be shown.



The screenshot shows the 'Quick Start' section of the router's web interface. The breadcrumb trail is 'WAN Port > (WAN > Wireless > BEsmart Register)'. The main heading is 'Congratulations !'. Below this, the text reads 'Your WAN port has been successfully configured.' A 'Next to Wireless' button is located at the bottom left of the configuration area.

Fixed IP Address

Select this option to set static IP information. You will need to enter in the Connection type, IP address, Netmask, and gateway address, provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which are four IP octets separated by a dot (x.x.x.x). The Router will not accept the IP address if it is not in this format.



The screenshot shows the 'Quick Start' configuration page for the WAN Port. The breadcrumb trail is 'WAN > Wireless > BEsmart Register'. Under the heading 'Select protocol', there is a table with the following fields:

| | |
|------------|------------------|
| Protocol | Fixed IP Address |
| IP Address | 0.0.0.0 |
| Netmask | |
| Gateway | |

At the bottom of the form is a 'Continue' button.

Protocol: The current ATM protocol in the device

IP Address: Your WAN IP address. Leave this at 0.0.0.0 to automatically obtain an IP address from your ISP.

Netmask: The default is 0.0.0.0. User can change it to other such as 255.255.255.0. Type the subnet mask assigned to you by your ISP (if given).

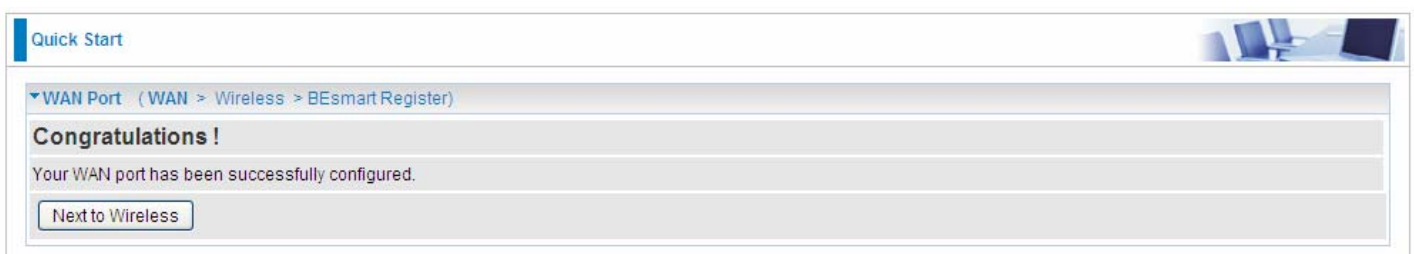
Gateway: You must specify a gateway IP address (supplied by your ISP)

Click on the **Continue** button and wait for your connection to be connected.



The screenshot shows the 'Quick Start' configuration page for the WAN Port. The breadcrumb trail is 'WAN > Wireless > BEsmart Register'. The main content area displays the message: 'Please wait while the device is configured...'

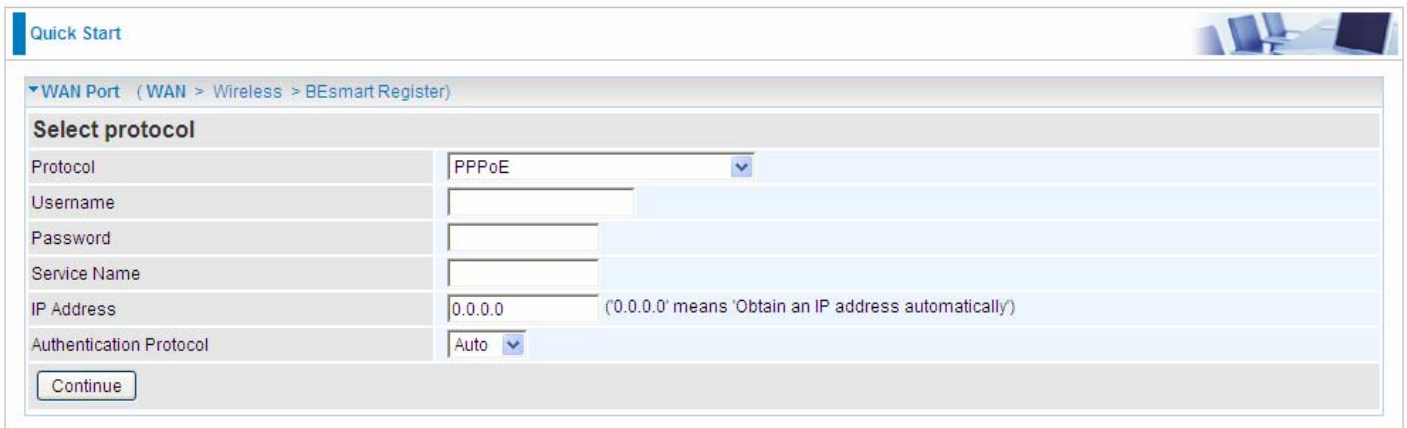
If connection is successful the following image will be shown.



The screenshot shows the 'Quick Start' configuration page for the WAN Port. The breadcrumb trail is 'WAN > Wireless > BEsmart Register'. The main content area displays the message: 'Congratulations ! Your WAN port has been successfully configured.' At the bottom of the form is a 'Next to Wireless' button.

PPPoE

PPPoE (PPP over Ethernet) provides access control in a manner similar to dial-up services using PPP.



Quick Start

WAN Port (WAN > Wireless > BEsmart Register)

Select protocol

| | |
|-------------------------|--|
| Protocol | PPPoE |
| Username | |
| Password | |
| Service Name | |
| IP Address | 0.0.0.0 (0.0.0.0 means 'Obtain an IP address automatically') |
| Authentication Protocol | Auto |

Continue

Protocol: The current ATM protocol in the device

Username: Enter the username provided by your ISP. You can input up to 128 alphanumeric characters (case sensitive). This is in the format of “username@ispname” instead of simply “username”.

Password: Enter the password provided by your ISP. You can input up to 128 alphanumeric characters (case sensitive).

Service Name: Enter a name for this connection.

IP Address: Your WAN IP address. Leave this at 0.0.0.0 to automatically obtain an IP address from your ISP.

Auth. Protocol: Default is Auto. Your ISP advises on using Chap or Pap.

Click on the **Continue** button and wait for your connection to be connected.



Quick Start

WAN Port (WAN > Wireless > BEsmart Register)

Please wait while the device is configured...

If connection is successful the following image will be shown.



Quick Start

WAN Port (WAN > Wireless > BEsmart Register)

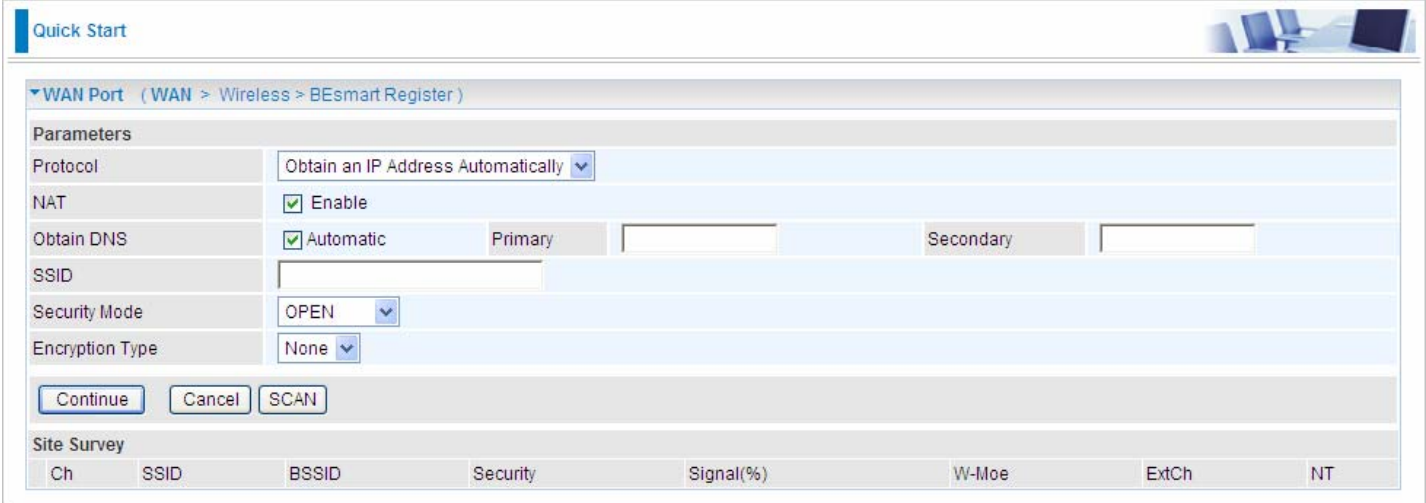
Congratulations !

Your WAN port has been successfully configured.

Next to Wireless

WirelessClient

When WirelessClient is selected, the router will act as an ordinary wireless client to connect to an AP to connect to the Internet.



Quick Start

WAN Port (WAN > Wireless > BEsmart Register)

Parameters

Protocol: Obtain an IP Address Automatically

NAT: Enable

Obtain DNS: Automatic Primary Secondary

SSID:

Security Mode: OPEN

Encryption Type: None

Continue Cancel SCAN

Site Survey

| Ch | SSID | BSSID | Security | Signal(%) | W-Moe | ExtCh | NT |
|----|------|-------|----------|-----------|-------|-------|----|
|----|------|-------|----------|-----------|-------|-------|----|

Protocol: Select to obtain an IP address automatically or choose to set a fixed IP for your gateway.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single ISP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

Obtain DNS: Choose Automatic or set the exact values yourself.

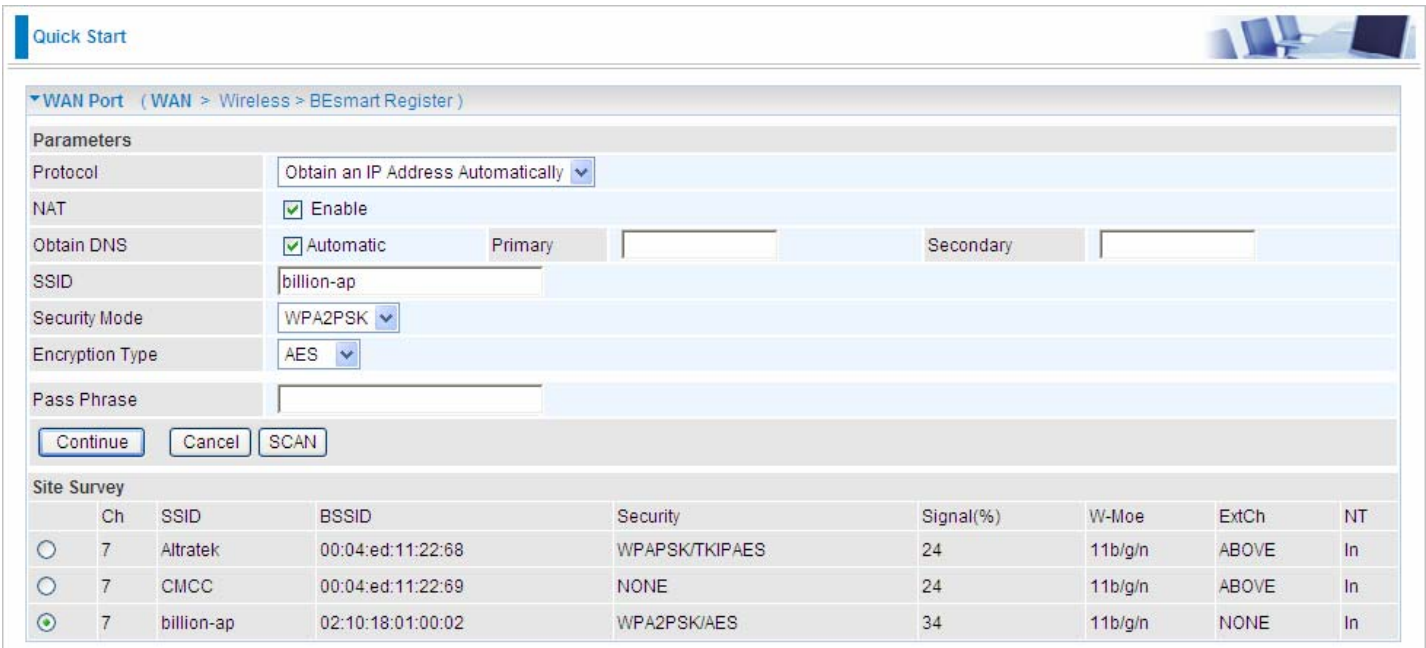
SSID: The target wireless AP. User can alternatively input the SSID manually or also use the Scan button to scan and select.

Security Mode: Set the wireless security mode, namely, OPEN, SHARED, WPAPSK and WPA2PSK. User can set the mode yourself if well knowing the mode, or user can choose to scan button and select the target SSID.

Continue: Move on to connect to the SSID.

Cancel: undo the current step.

SCAN: Press this button to scan the SSIDs in the air.



Quick Start

WAN Port (WAN > Wireless > BEsmart Register)

Parameters

Protocol: Obtain an IP Address Automatically

NAT: Enable

Obtain DNS: Automatic Primary Secondary

SSID: billion-ap

Security Mode: WPA2PSK

Encryption Type: AES

Pass Phrase:

Continue Cancel SCAN

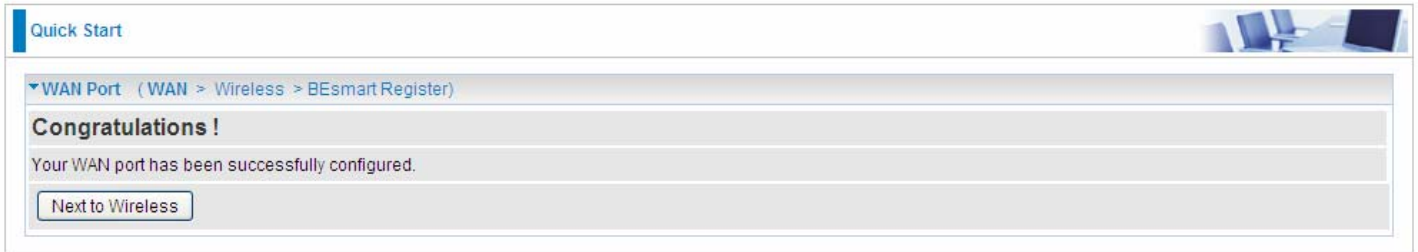
Site Survey

| Ch | SSID | BSSID | Security | Signal(%) | W-Moe | ExtCh | NT | |
|----------------------------------|------|------------|-------------------|----------------|-------|---------|-------|----|
| <input type="radio"/> | 7 | Altratek | 00:04:ed:11:22:68 | WPAPSK/TKIPAES | 24 | 11b/g/n | ABOVE | In |
| <input type="radio"/> | 7 | CMCC | 00:04:ed:11:22:69 | NONE | 24 | 11b/g/n | ABOVE | In |
| <input checked="" type="radio"/> | 7 | billion-ap | 02:10:18:01:00:02 | WPA2PSK/AES | 34 | 11b/g/n | NONE | In |

Click on the **Continue** button and wait for your connection to be connected.



If connection is successful the following image will be shown.



Set Wireless configuration

Quick Start

Wireless (WAN > Wireless > BEsmart Register)

Set Wireless configuration.

WLAN Service Enable Disable

ESSID

Channel ID

Security Mode

Regulation Domain

WLAN Service: Default setting is set to **Enable**.

ESSID: The ESSID is the unique name of a wireless access point (AP) to be distinguished from another. For security propose, change to a unique ID name to the AP which is already built-in to the router's wireless interface. It is case sensitive and must not excess 32 characters. Make sure your wireless clients have exactly the ESSID as the device, in order to get connected to your network.

Channel ID: Select the ID channel that you would like to use.

Security Mode: You can disable or enable with WPA or WEP for protecting wireless network. The default mode of wireless security is **Disable**. For more information, turn to [Security Parameters](#) section for help.

Click **Next to BEsmart Register** move on to register a BEsmart service account.

Quick Start

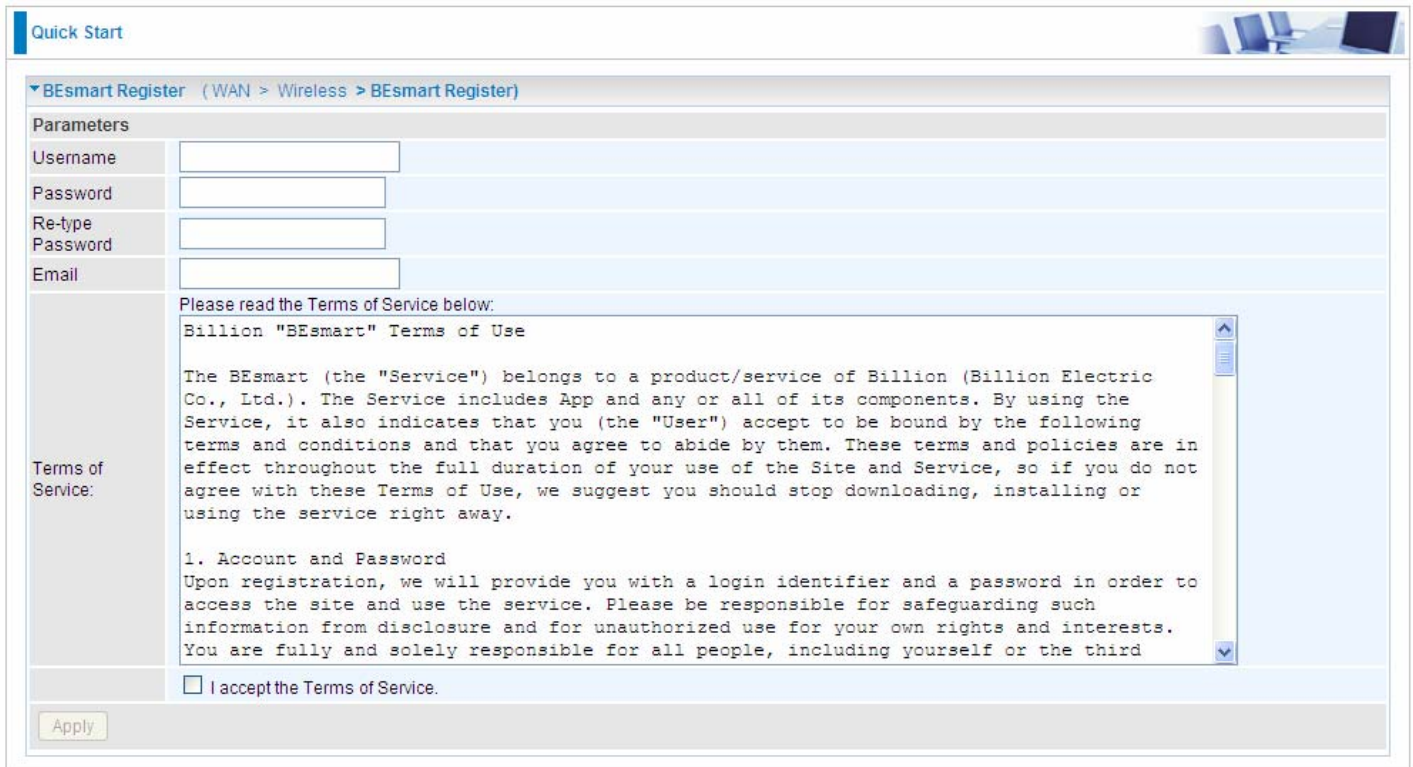
Wireless (WAN > Wireless > BEsmart Register)

Configuration!

Your Wirless has been succesfully configured.

Register a new BEsmart service account

To use the service, please register an account.



Quick Start

BEsmart Register (WAN > Wireless > BEsmart Register)

Parameters

Username:

Password:

Re-type Password:

Email:

Terms of Service:

Please read the Terms of Service below:
Billion "BEsmart" Terms of Use

The BEsmart (the "Service") belongs to a product/service of Billion (Billion Electric Co., Ltd.). The Service includes App and any or all of its components. By using the Service, it also indicates that you (the "User") accept to be bound by the following terms and conditions and that you agree to abide by them. These terms and policies are in effect throughout the full duration of your use of the Site and Service, so if you do not agree with these Terms of Use, we suggest you should stop downloading, installing or using the service right away.

1. Account and Password
Upon registration, we will provide you with a login identifier and a password in order to access the site and use the service. Please be responsible for safeguarding such information from disclosure and for unauthorized use for your own rights and interests. You are fully and solely responsible for all people, including yourself or the third

I accept the Terms of Service.

Apply

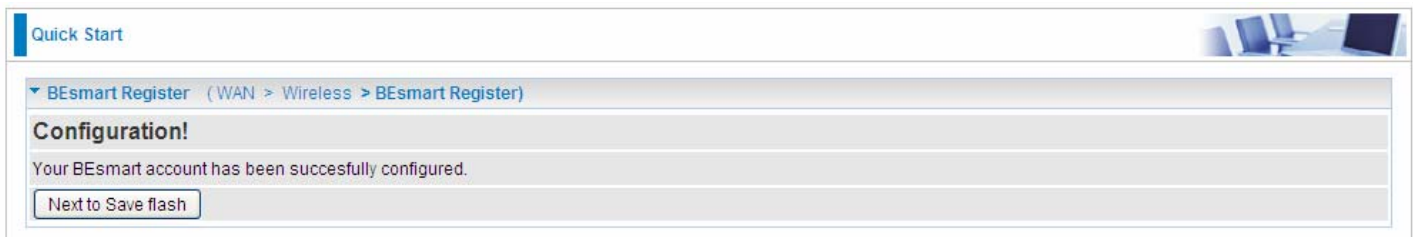
Username: Enter the username.

Password: Enter the password for the account.

Re-type Password: Confirm the password.

Email: Enter an email address to receive the messages like account information when user forgets the account and wants to retrieve the account, from the router.

Click **Next to Save flash** to save the settings to the flash.



Quick Start

BEsmart Register (WAN > Wireless > BEsmart Register)

Configuration!

Your BEsmart account has been successfully configured.

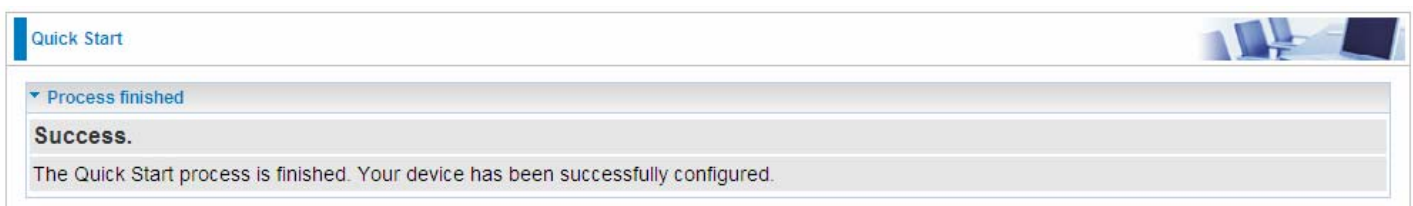
Next to Save flash



Quick Start

Save configuration

Saving configuration to FLASH. Please wait for 10 seconds



Quick Start

Process finished

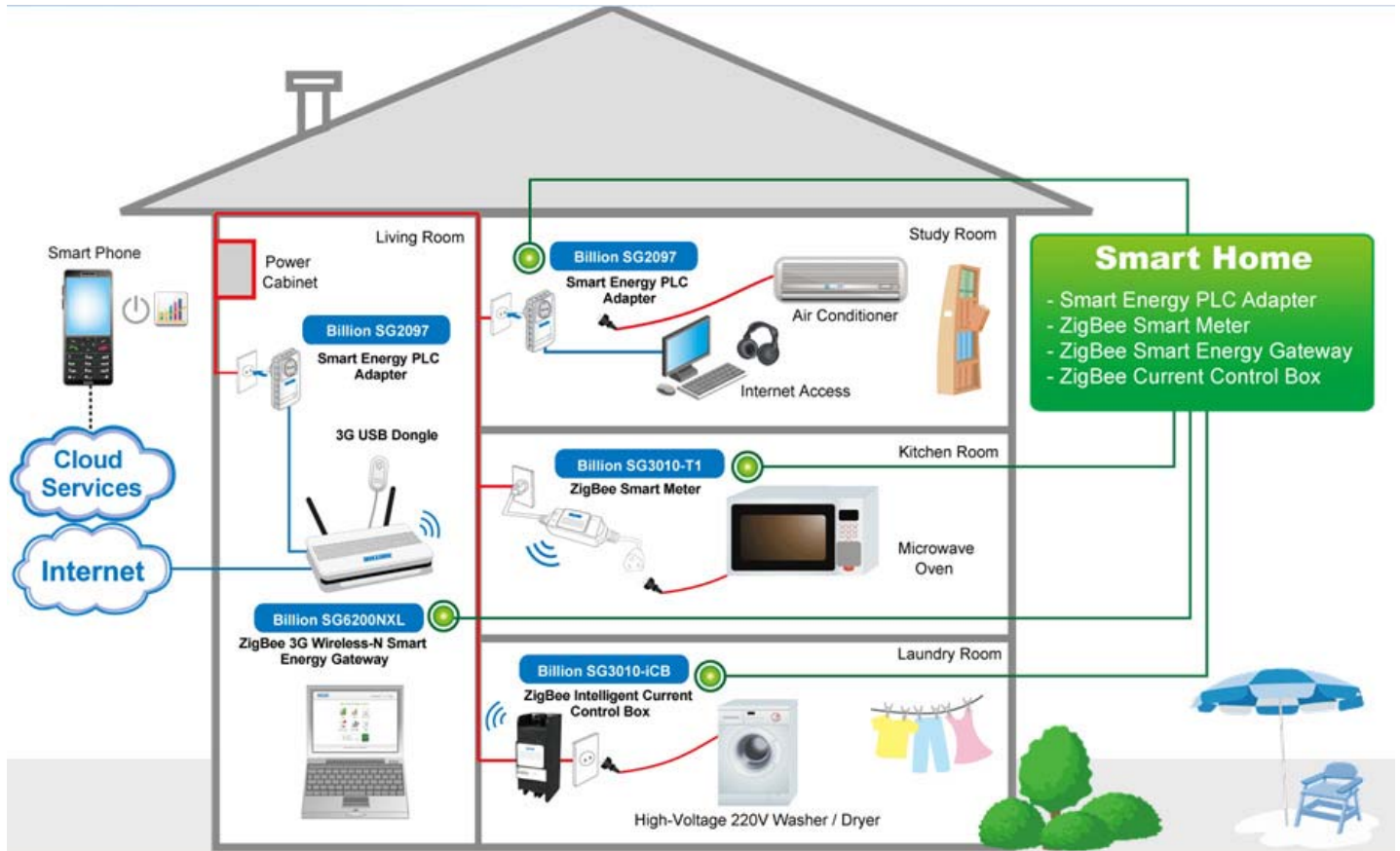
Success.

The Quick Start process is finished. Your device has been successfully configured.

Power Management

In Smart Meter Serial products, Billion provide Smart Gateway and Smart meter to build Energy Management Solutions give consumers insight and control of home energy usage by intuitive online interface. Access energy data through ZigBee and Poweline Interface, it enables customers to reduce the amount of energy consumer's waste.

A simple diagram



Remote Control

Via Smart Gateway, users on-the-go can remotely control in-home electric appliances that connect to Smart meter by user Internet based device even a smart phone.

Remote Monitor

Via Smart Gateway, users on-the-go can remotely monitor in-home electric appliances that connect to Smart meter by user Internet based device even a smart phone.

Meter Config

Before configuring, first connect one end of your SmartMeter to the power source or power outlet, one end to the device as follows.



(This is a kind of SmartMeter for example, for more information please refer to the SmartMeter usage document.)

Then click **Power Management > Meter Config**. (Meter connected)

Power Management

Meter Config

Parameters

Allow Join

Scan Meter

PLC IP Range ~

| Meter List | Model Name | Alias | Display Order | Identify | Remove |
|------------------|------------|----------------------------------|--------------------------------|---|---------------------------------------|
| 000D6F00007584B2 | SG3010 | <input type="text" value="N/A"/> | <input type="text" value="1"/> | <input type="button" value="Identify"/> | <input type="button" value="Remove"/> |
| 000D6F00008E2FF0 | SG3010 | <input type="text" value="N/A"/> | <input type="text" value="1"/> | <input type="button" value="Identify"/> | <input type="button" value="Remove"/> |

Power Management

Meter Config

Parameters

Allow Join

Scan Meter

PLC IP Range ~

| Meter List | Model Name | Alias | Display Order | Identify | Remove |
|------------------|------------|---|--------------------------------|---|---------------------------------------|
| 000D6F00007584B2 | SG3010 | <input type="text" value="refrigerator"/> | <input type="text" value="1"/> | <input type="button" value="Identify"/> | <input type="button" value="Remove"/> |
| 000D6F00008E2FF0 | SG3010 | <input type="text" value="PC"/> | <input type="text" value="2"/> | <input type="button" value="Identify"/> | <input type="button" value="Remove"/> |

Allow Join: Click **Start** to join SmartMeters in.

Scan Meter: Show all alive smart Meters.

PLC IP Range: Set the IP Range. Only IP within this range can be controlled on/off by your SG6200NXL gateway.

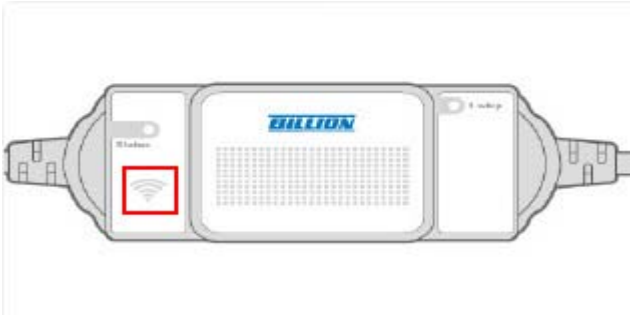
Meter List: Display the unique identification of each Billion SmartMeter.

Model Name: Display the model of the meter.

Alias: Enter a given name for each SmartMeter, usually for identification for each SmartMeter usage, or the device connected to the SmartMeter, for example, if a SmartMeter is connected to a refrigerator, you can alias this alias name as refrigerator for identification.

Display Order: select the display order for each SmartMeter (device) connected as needed. And in Power Control page, the devices will be displayed according to this order.

Identify: Click **Identify** to distinguish the connected SmartMeter; When clicked, the light of the SmartMeter will flash orange and last for about 20 seconds for customers to tell from the many connected devices.



Remove: Click **Remove** to remove the connected SmartMeter.

Click **Apply** to save your settings.

Here two SmartMeters are connected to SG6200NXL gateway, set the parameters as follows. Then click **Apply** to save. Now you have finished **Meter Config**.

Power Management

Meter Config

Parameters

Allow Join

Scan Meter

PLC IP Range ~

| Meter List | Model Name | Alias | Display Order | Identify | Remove |
|------------------|------------|---|---------------|---|---------------------------------------|
| 000D6F00007584B2 | SG3010 | <input type="text" value="refrigerator"/> | 1 ▼ | <input type="button" value="Identify"/> | <input type="button" value="Remove"/> |
| 000D6F00008E2FF0 | SG3010 | <input type="text" value="PC"/> | 2 ▼ | <input type="button" value="Identify"/> | <input type="button" value="Remove"/> |

Power Control

In this section, you can control your home devices' on or off via SG6200NX gateway remotely to achieve home automation.

The screenshot shows a web interface for Power Management. Under the 'Power Control' section, there are buttons for 'Turn all ON' and 'Turn all OFF'. Below this is a table with columns for 'No.', 'Device ID', 'Appliance Name', 'Status', 'Scenario 1', 'Scenario 2', and 'Scenario 3'. Two devices are listed: a refrigerator (No. 1) and a PC (No. 2). The refrigerator is currently ON, and the PC is currently OFF. Scenario 1 has the refrigerator ON and PC OFF. Scenario 2 has the refrigerator OFF and PC ON. Scenario 3 is N/A for both. There are 'Save' and 'Cancel' buttons at the bottom.

| No. | Device ID | Appliance Name | Status | Scenario 1 | Scenario 2 | Scenario 3 |
|-----|------------------|----------------|--------|------------|------------|------------|
| 1 | 000D6F00007584B2 | refrigerator | ON | ON | OFF | N/A |
| 2 | 000D6F00008E2FF0 | PC | OFF | OFF | ON | N/A |

Active: click one of the following buttons to turn on or off the devices through one-time operation to simplify the repetitive operations. Besides Turn all on and Turn all off, three scenarios are provided to allow users to specify the on or off of the devices as required.

- Turn all ON: Turn all the connected devices on.
- Turn all OFF: Turn all connected devices off.
- Scenario1/2/3: specify which device is on and which one is off to form a Scenario for one-time operation to meet your needs.

No.: The sequence number.

Appliance Name: Display the corresponding device you set at **Meter Config** page to the order number.

Status: Select ON or OFF to let the device be on or off. It is a real-time operation, if you select ON for PC, you will turn on PC immediately.

Scenario1/2/3: Set ON or OFF for each device.

Click **Save** to apply your settings.

Example for scenario application: see the following diagram, sometime you want to turn on PC and turn off refrigerator, you can press Scenario1 button to meet your needs through one time operation, and when some time, you want to turn on refrigerator and turn off PC, you can press Scenario 2 to meet your needs. You see, here scenario servers as a one-time operation sheet used for simplifying the repetitive operations. You can specify the wanted on or off operation of each device in a scenario, then instead of turning on or off one by one, you only press the scenario button, it will be OK.

| No. | Appliance Name | Scenario1 | Scenario 2 |
|-----|----------------|-----------|------------|
| 1 | refrigerator | ON | OFF |
| 2 | PC | OFF | ON |

ZigBee step by step configuration (meter of SG30XX series for example)

1. Connect the SmartMeter and the end device.



2. Enter the router, Click **Power Management > Meter Config**. You will see the following page.

Power Management

Meter Config

Parameters

Allow Join

Scan Meter

PLC IP Range ~


| Meter List | Model Name | Alias | Display Order | Identify | Remove |
|------------------|------------|----------------------------------|----------------------------------|---|---------------------------------------|
| 000D6F00007584B2 | SG3010 | <input type="text" value="N/A"/> | <input type="button" value="v"/> | <input type="button" value="Identify"/> | <input type="button" value="Remove"/> |
| 000D6F00008E2FF0 | SG3010 | <input type="text" value="N/A"/> | <input type="button" value="v"/> | <input type="button" value="Identify"/> | <input type="button" value="Remove"/> |

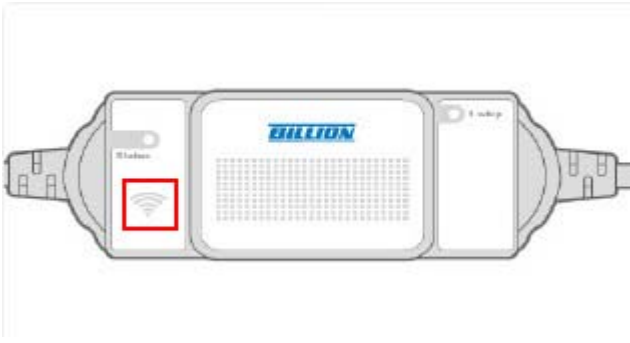
Commonly, you will see the connected SmartMeters, but if not, or you want to join other SmartMeters in, you should Allow Join the SmartMeters as needed.

① How to join the ZigBee network:

- 1) Power on the meter.
- 2) Click Allow Join **Start** when Status LED lights. If you witness the blinking Status LED, the meter has successfully connected to the ZigBee network. And now, you can see the above shown screenshot (if not, please refresh the page).

① How to leave the ZigBee network

- 1) Power off the meter and power on again.
- 2) Press  till the Status LED blinks within 30 seconds starting from 5 seconds after re-powering on the meter. When the Status LED starts blinking, you have 6 seconds to power off the meter to get this meter removed from the ZigBee network.
- 3) Power on again, you will see Status LED lights for joining a new ZigBee network.



3. Set the parameters, such as the alias, the display order. Remember to click **Apply** to save your settings.

Power Management

Meter Config

Parameters

Allow Join

Scan Meter

PLC IP Range ~

| Meter List | Model Name | Alias | Display Order | Identify | Remove |
|------------------|------------|--------------|---------------|---|---------------------------------------|
| 000D6F00007584B2 | SG3010 | refrigerator | 1 | <input type="button" value="Identify"/> | <input type="button" value="Remove"/> |
| 000D6F00008E2FF0 | SG3010 | PC | 2 | <input type="button" value="Identify"/> | <input type="button" value="Remove"/> |

4. **Power Management > Power Control** to remotely control your devices' on or off. .

Power Management

Power Control

Parameters

Active

| No. | Device ID | Appliance Name | Status | Scenario 1 | Scenario 2 | Scenario 3 |
|-----|------------------|----------------|--------|------------|------------|------------|
| 1 | 000D6F00007584B2 | refrigerator | ON | ON | OFF | N/A |
| 2 | 000D6F00008E2FF0 | PC | OFF | OFF | ON | N/A |

1). You can directly go to **status** field, select the ON or OFF for the device you want it to be. Then it will be on or off immediately.

2). If you want to turn all the devices on or off, press or .

3) If you want to turn on the refrigerator and turn off the PC sometime, you can make a scenario, such as scenario1, set as follows.

| No. | Device ID | Appliance Name | Status | Scenario 1 |
|-----|------------------|----------------|--------|------------|
| 1 | 000D6F00007584B2 | refrigerator | ON ▼ | ON ▼ |
| 2 | 000D6F00008E2FF0 | PC | ON ▼ | OFF ▼ |

Click **Save** to apply your settings. And now you can press **Scenario1** button to make it.

RS485 Config

RS485 Cnfig offers to configure the RS485 smart instruments.

Configuration

RS485 Config

Parameters

Auto Detect: Enable

Baud Rate: 19200

Address Table

| Address | Model | Address | Model |
|---------|-------|---------|-------|
| 1 | N/A | 2 | N/A |
| 3 | N/A | 4 | N/A |
| 5 | N/A | 6 | N/A |
| 7 | N/A | 8 | N/A |
| 9 | N/A | 10 | N/A |
| 11 | N/A | 12 | N/A |
| 13 | N/A | 14 | N/A |
| 15 | N/A | 16 | N/A |
| 17 | N/A | 18 | N/A |
| 19 | N/A | 20 | N/A |
| 21 | N/A | 22 | N/A |
| 23 | N/A | 24 | N/A |
| 25 | N/A | 26 | N/A |
| 27 | N/A | 28 | N/A |
| 29 | N/A | 30 | N/A |

Apply Reset

Auto Detect: Select to Enable or Disable RS485 Config feature. If enabled, our SG6200NXL gateway will automatically detect the RS485 devcies connected when pressing the WPS/ZigBee button.

Baud Rate: Select the working baud rate.

Address Table

Address: The address of the connected RS485 device.

Model: The list-box lists the current supported RS485 models. User can select the RS485 device to be connected.

Control Rules

Control Rules equips users to set up to 30 different controlling rules to automatically control how a connected device acts under certain circumstances, currently by temperature or humidity.

Configuration

▼ Control Rules

Parameters

Rule ID: 1

Name:

Device ID:

Condition: Temperature | Upper |

Action: Mail Alert

| Edit | Rule ID | Name | Device ID | Condition | Action | Controlled Device ID | Delete |
|------|---------|------|-----------|-----------|--------|----------------------|--------|
| | 1 | | | | | | |

Rule ID: Integer rule index, automatically climbing after a rule is successfully added.

Name: The user-defined rule name.

Device ID: Select the device which detects the temperature or humidity.

Condition: Set the condition by temperature or humidity detected by device set above.

Action: The action to be executed under the set circumstance.

① **Mail Alert:** Use Mail alert to inform the condition now. See [Mail Alert](#).

① **Turn on/off:** Turn on/off the controlled device set below.

Controlled Device ID: Select the controlled device id from the list-box. The device can be turned on/off.

Configuration

▼ Control Rules

Parameters

Rule ID: 1

Name:

Device ID:

Condition: Temperature | Upper |

Action: Turn On

Controlled Device ID:

| Edit | Rule ID | Name | Device ID | Condition | Action | Controlled Device ID | Delete |
|------|---------|------|-----------|-----------|--------|----------------------|--------|
| | 1 | | | | | | |

Configuration

▼ Control Rules

Parameters

Rule ID: 1

Name: 11

Device ID: 00158D00001C066E

Condition: Temperature | Upper | 30

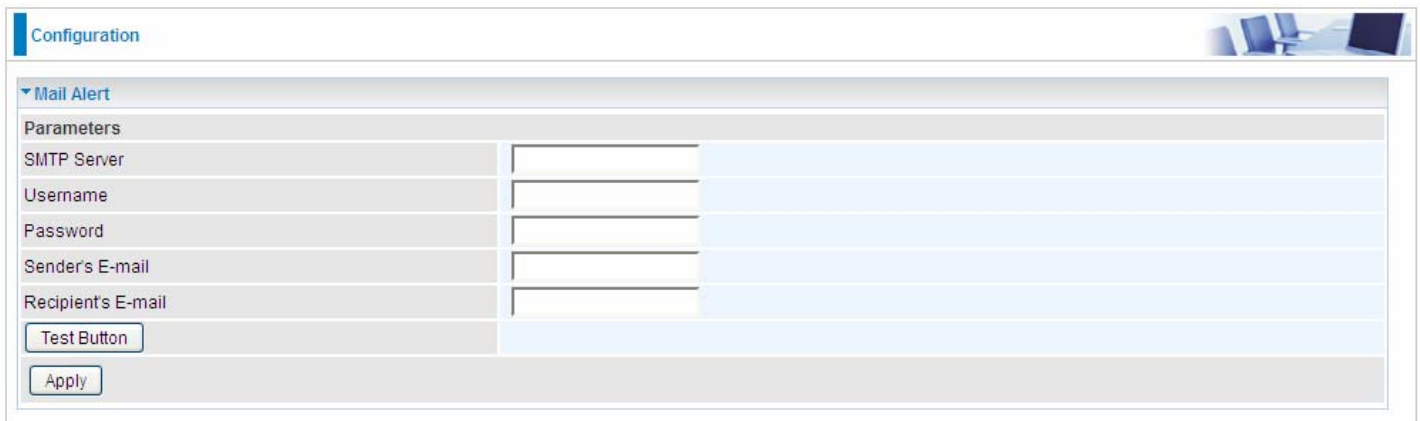
Action: Turn On

Controlled Device ID: 0000000000000002

| Edit | Rule ID | Name | Device ID | Condition | Action | Controlled Device ID | Delete |
|--------------------------|---------|------|------------------|----------------------|---------|----------------------|--------------------------|
| <input type="checkbox"/> | 1 | 11 | 00158D00001C066E | temperature upper 30 | turn_on | 0000000000000002 | <input type="checkbox"/> |

Mail Alert

Mail alert is designed to keep administrator alert of any unexpected events (temperature/humidity abnormality) that might have occurred to the connected ZigBee or PLC devices for monitoring efficiency. Set in [Control Rules](#).



The screenshot shows a web-based configuration interface. At the top left, there is a 'Configuration' tab. Below it, a 'Mail Alert' section is expanded, showing a 'Parameters' table with the following fields: SMTP Server, Username, Password, Sender's E-mail, and Recipient's E-mail. Each field has a corresponding text input box. Below the table, there are two buttons: 'Test Button' and 'Apply'.

| Parameters | |
|--------------------|----------------------|
| SMTP Server | <input type="text"/> |
| Username | <input type="text"/> |
| Password | <input type="text"/> |
| Sender's E-mail | <input type="text"/> |
| Recipient's E-mail | <input type="text"/> |

SMTP Server: Enter the SMTP server that you would like to use for sending emails.

Username: Enter the username of your email account registered at the SMTP server.

Password: Enter the password of your email account.

Sender's Email: Enter your email address registered at your SMTP server.

Recipient's Email: Enter the email address that will receive the alert message.

Configuration

Click this item to access the following sub-items that configure the 3G router: **LAN, WAN, BEsmart, System, USB, Firewall, QoS, Virtual Server, Wake on LAN, Time Schedule** and **Advanced**.

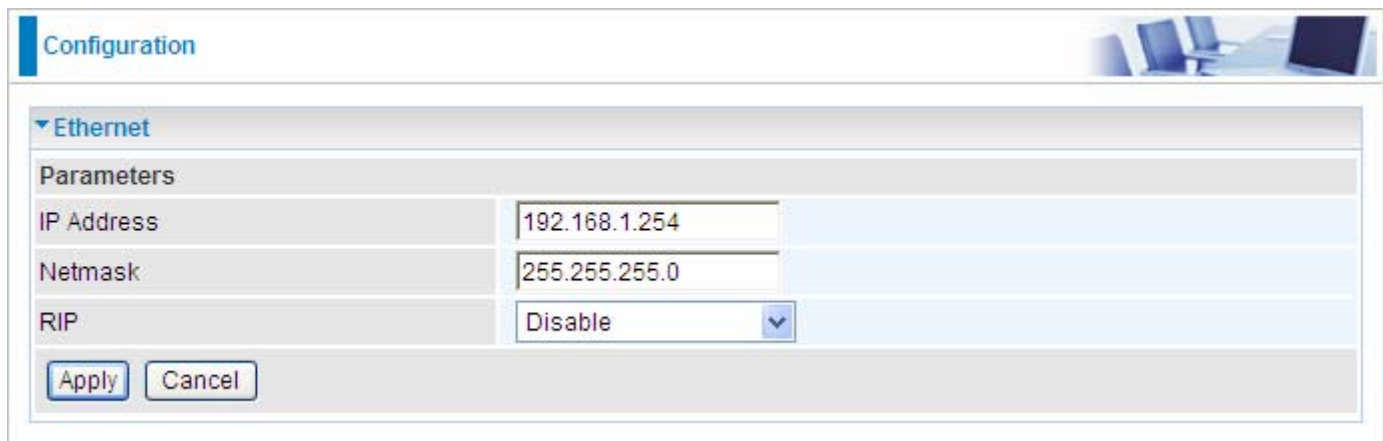
These functions are described in the following sections.

LAN (Local Area Network)

A Local Area Network (LAN) is a shared communication system to which many computers are attached and is limited to the immediate area, usually the same building or floor of a building.

There are six items within the LAN section: **Ethernet, IP Alias, Wireless, Wireless Security, WPS** and **DHCP Server**.

Ethernet



| Parameters | |
|------------|---------------|
| IP Address | 192.168.1.254 |
| Netmask | 255.255.255.0 |
| RIP | Disable |

Apply Cancel

The router supports more than one Ethernet IP addresses in the LAN, and with distinct LAN subnets through which you can access the Internet at the same time. Users usually only have one subnet in their LAN. The default IP address for the router is 192.168.1.254.

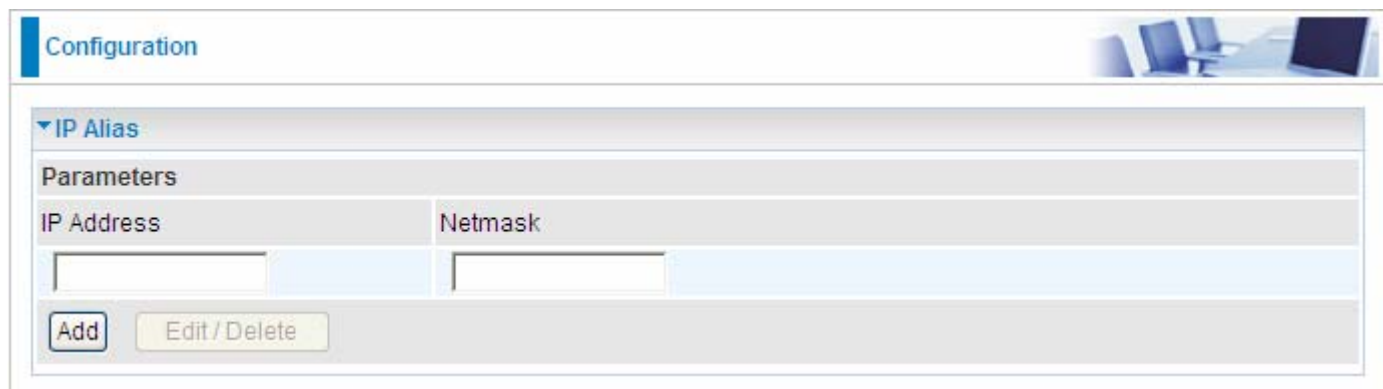
IP Address: The default IP on this router.

Netmask: The default subnet mask on this router.

RIP: RIP v1, RIP v2 Broadcast, RIP v1+v2 Broadcast and RIP v2 Multicast.

IP Alias

This function allows the creation of multiple virtual IP interfaces on this router. It helps to connect two or more local networks to the ISP or remote node. In this case, an internal router is not required.



| Parameters | |
|----------------------|----------------------|
| IP Address | Netmask |
| <input type="text"/> | <input type="text"/> |

Add Edit/Delete

IP Address: Specify an IP address on this virtual interface.

Netmask: Specify a subnet mask on this virtual interface.

Wireless

The screenshot shows the 'Configuration' page for wireless settings. The 'Wireless' section is expanded, showing a 'Parameters' table. The settings are as follows:

| | |
|---|--|
| WLAN Service | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Mode | 802.11g + n |
| Number of Active SSID | 1 |
| SSID No. | SSID1 |
| ESSID | wlan-ap |
| Hide ESSID | <input type="radio"/> Enable <input checked="" type="radio"/> Disable |
| Regulation Domain | N.America |
| Channel ID | Channel 1 (2.412 GHz) |
| Channel Width | 20/40MHZ |
| Tx PowerLevel | 100 (0 ~ 100) |
| AP MAC Address | 00:1D:92:C0:13:CD |
| AP Firmware Version | 2.3.0.0 |
| WPS Service | <input type="radio"/> Enable <input checked="" type="radio"/> Disable |
| WPS State | <input type="radio"/> Configured <input checked="" type="radio"/> Unconfigured |
| WMM | <input type="radio"/> Enable <input checked="" type="radio"/> Disable |
| Wireless Distribution System (WDS) | |
| WDS Service | <input type="radio"/> Enable <input checked="" type="radio"/> Disable |
| Peer WDS MAC address | 1. <input type="text"/> 2. <input type="text"/> 3. <input type="text"/> 4. <input type="text"/> |

** WDS depends on the settings of main security encryption type. **

Buttons: Apply, Cancel, Security settings >

Parameters

WLAN Service: Default setting is set to **Enable**.

Mode: The default setting is **802.11g+n** (Mixed mode). If you do not know or have both 11g and 11n devices in your network, then keep the default in **mixed mode**. From the drop-down manual, you can select **802.11g** if you have only 11g card. If you have only 11b card, then select **802.11b**. If you have only 11n card, then select **802.11n**.

Number of Active SSID: Number of SSID you can choose.

SSID No.: The SSID you choose.

ESSID: The ESSID is the unique name of a wireless access point (AP) to be distinguished from another. For security propose, change to a unique ID name to the AP which is already built-in to the router's wireless interface. It is case sensitive and must not excess 32 characters. Make sure your wireless clients have exactly the ESSID as the device, in order to get connected to your network.

Note: ESSID is case sensitive and must not excess 32 characters.

Hide ESSID: It is function in which transmits its ESSID to the air so that when wireless client searches for a network, router can then be discovered and recognized. Default setting is **Disable**.

Enable: Select Enable if you do not want broadcast your ESSID. When select Enable, no one

will be able to locate the Access Point (AP) of your router.

Ⓒ **Disable:** When Disable is selected, you can allow anybody with a wireless client to be able to locate the Access Point (AP) of your router.

Regulation Domain: There are seven Regulation Domains for you to choose from, including **North America (N.America)**, **Europe**, **France**, etc. The Channel ID will be different based on this setting.

Channel ID: Select the ID channel that you would like to use.

Channel Width: Select either **20 MHz** or **20/40 MHz** for the channel bandwidth. The higher the bandwidth the better the performance will be.

Tx Power Level: It is function that enhances the wireless transmitting signal strength. User may adjust this power level from minimum 0 up to maximum 100.

Note: The Power Level maybe different in each access network user premises environment and choose the most suitable level for your network.

AP MAC Address: It is a unique hardware address of the Access Point.

AP Firmware Version: The Access Point firmware version.

WPS service: Enable / disable

WPS State: Current WPS state in AP. It is be used for WCN (Windows Connect Now).

Ⓒ **Configured:** This AP is be configured via WPS. It is not allow to configure via WCN.

Ⓒ **Unconfigured:** This AP is un-configured via WPS. It can be configure via WCN.

WMM: This feature works concurrently with QoS that enables the system to prioritize the flow of data packets according to 4 categories: Voice, Video, Best Efforts and Background.

Ⓒ **Enable:** Click to activate WMM feature.

Ⓒ **Disable:** Click to deactivate WMM feature.

Wireless Distribution System (WDS)

It is a wireless access point mode that enables wireless link and communication with other access point. It is easy to be installed, simply define the peer's MAC address of the connected AP. WDS takes advantages of cost saving and flexibility which no extra wireless client device is required to bridge between two access points and extending an existing wired or wireless infrastructure network to create a larger network.

WDS Service: The default setting is **Disable**. Check **Enable** radio button to activate this function.

1. Peer WDS MAC Address: It is the associated AP's MAC Address. It is important that your peer's AP must include your MAC address in order to acknowledge and communicate with each other.

2. Peer WDS MAC Address: It is the second associated AP's MAC Address.

3. Peer WDS MAC Address: It is the third associated AP's MAC Address.

4. Peer WDS MAC Address: It is the fourth associated AP's MAC Address.

Note: For MAC Address, Semicolon (;) or Dash (-) must be included.

Wireless Security

You can disable or enable with WPA or WEP for protecting wireless network. The default mode of wireless security is **Disable**.

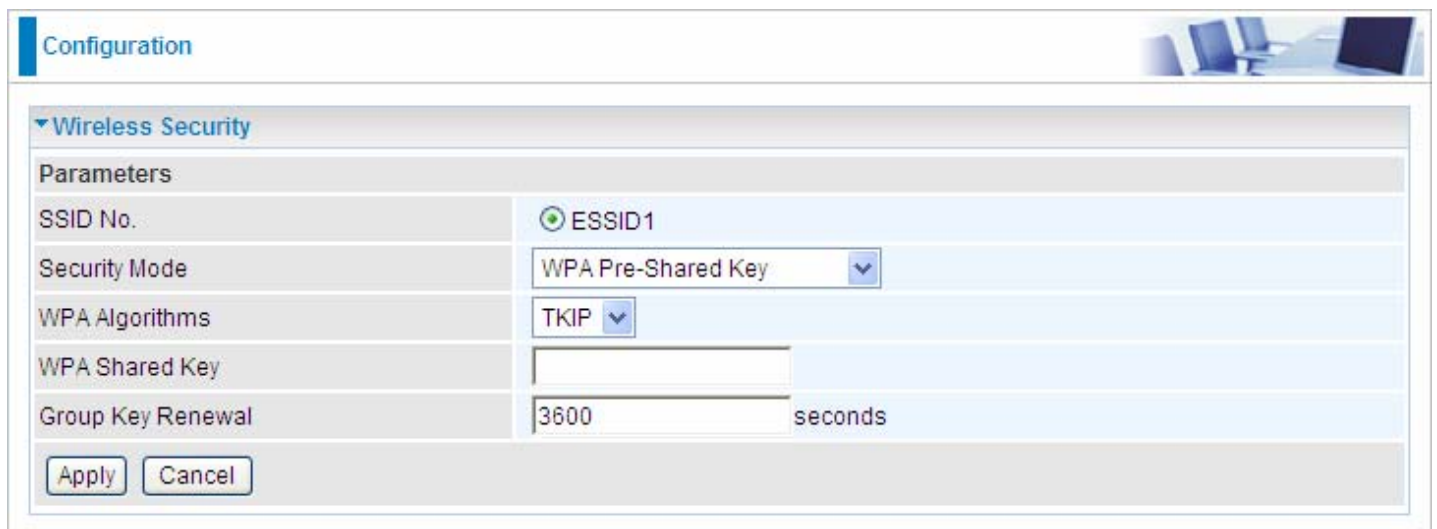


The screenshot shows a web-based configuration interface for wireless security. At the top, there is a 'Configuration' header and a small image of a meeting room. Below this, a section titled 'Wireless Security' is expanded. Underneath, a 'Parameters' section contains two rows: 'SSID No.' with a radio button selected next to 'ESSID1', and 'Security Mode' with a dropdown menu set to 'Disable'. At the bottom of the parameters section are two buttons: 'Apply' and 'Cancel'.

SSID No.: Choose the SSID you want to set.

Security Mode: There are five security modes for you to choose.

● WPA Pre-Shared Key



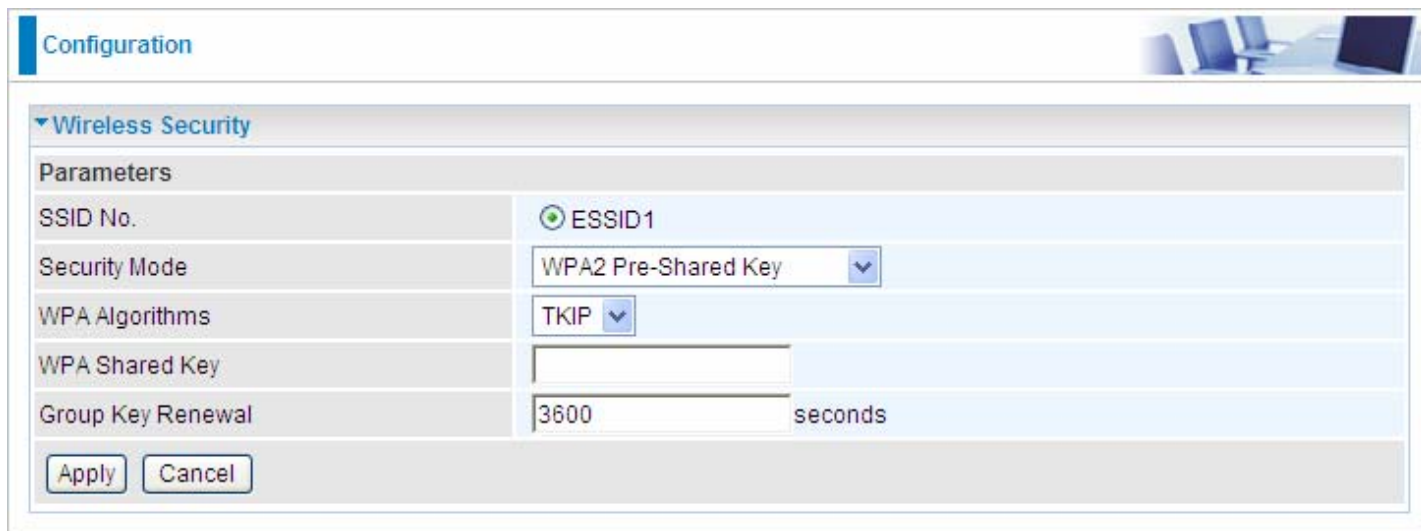
The screenshot shows the same web-based configuration interface, but now the 'Security Mode' dropdown is set to 'WPA Pre-Shared Key'. Below this, there are three more rows: 'WPA Algorithms' with a dropdown set to 'TKIP', 'WPA Shared Key' with an empty text input field, and 'Group Key Renewal' with a text input field containing '3600' and the unit 'seconds' to its right. The 'Apply' and 'Cancel' buttons are still present at the bottom.

WPA Algorithms: TKIP (Temporal Key Integrity Protocol) / AES (Advanced Encryption Standard) utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers.

WPA Shared Key: The key for network authentication. The input format is in character style and key size should be in the range between 8 and 63 characters.

Group Key Renewal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP).

● WPA2 Pre-Shared Key



The screenshot shows a configuration window titled "Configuration" with a "Wireless Security" section. The "Parameters" table is as follows:

| Parameters | |
|-------------------|----------------------|
| SSID No. | ESSID1 |
| Security Mode | WPA2 Pre-Shared Key |
| WPA Algorithms | TKIP |
| WPA Shared Key | <input type="text"/> |
| Group Key Renewal | 3600 seconds |

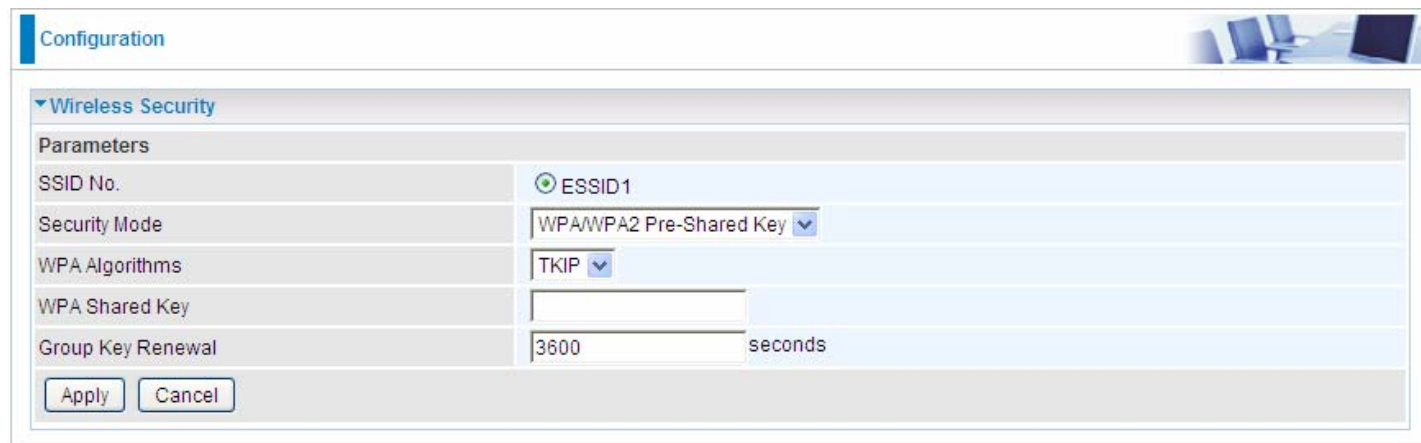
Buttons: Apply, Cancel

WPA Algorithms: TKIP (Temporal Key Integrity Protocol) / AES (Advanced Encryption Standard) utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers.

WPA Shared Key: The key for network authentication. The input format is in character style and key size should be in the range between 8 and 63 characters.

Group Key Renewal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP).

● WPA/WPA2 Pre-Shared Key



The screenshot shows a configuration window titled "Configuration" with a "Wireless Security" section. The "Parameters" table is as follows:

| Parameters | |
|-------------------|-------------------------|
| SSID No. | ESSID1 |
| Security Mode | WPA/WPA2 Pre-Shared Key |
| WPA Algorithms | TKIP |
| WPA Shared Key | <input type="text"/> |
| Group Key Renewal | 3600 seconds |

Buttons: Apply, Cancel

WPA Algorithms: TKIP (Temporal Key Integrity Protocol) / AES (Advanced Encryption Standard) utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers.

WPA Shared Key: The key for network authentication. The input format is in character style and key size should be in the range between 8 and 63 characters.

Group Key Renewal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP).

WEP

Configuration

▼ Wireless Security

Parameters

| | |
|---------------------------|---|
| SSID No. | <input checked="" type="radio"/> ESSID1 |
| Security Mode | WEP |
| WEP Authentication | Open System |
| Default Used WEP Key | <input type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4 |
| Passphrase (Generate Key) | <input type="text"/> <input type="button" value="WEP64"/> <input type="button" value="WEP128"/> |
| Key 1 | Hex <input type="text"/> |
| Key 2 | Hex <input type="text"/> |
| Key 3 | Hex <input type="text"/> |
| Key 4 | Hex <input type="text"/> |

WEP 64 - Hex: 10 Hex codes, (1~9, a~f, A~F). EX: 11aa22cc33.
WEP 64 - ASCII: 5 ASCII characters are required. Insert your WEP key manually. EX: 1a3eb.
WEP 128 - Hex: 26 Hex codes, (1~9, a~f, A~F). EX: 11aa22cc33dd44ee55efffe35f.
WEP 128 - ASCII: 13 ASCII characters are required. Insert your WEP key manually. EX: 1a3e?l!dbd3ert.

WEP Authentication: To prevent unauthorized wireless stations from accessing data transmitted over the network, the router offers secure data encryption, known as WEP. If you require high security for transmissions, there are three options to select from: **Open System**, **Share key** or **Both**.


Default Used WEP Key: Select the encryption key ID; please refer to **Key (1~4)** below.

Passphrase: This is used to generate WEP keys automatically based upon the input string and a pre-defined algorithm in WEP64 or WEP128. You can input the same string in both the AP and Client card settings to generate the same WEP keys. Please note that you do not have to enter **Key (1-4)** as below when the **Passphrase** is enabled.

Key (1-4): Enter the key to encrypt wireless data. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as the router. There are four keys for your selection. The input format is in HEX or ASCII style, 5 and 13 ASCII codes are required for WEP64 and WEP128 respectively-no any separator is included.

WPS

WPS (WiFi Protected Setup) feature is a standard protocol created by Wi-Fi Alliance. This feature greatly simplifies the steps needed to create a Wi-Fi network for a residential or an office setting. WPS supports 2 types of configuration methods which are commonly known among consumers: **PIN Method & PBC Method**.

Configuration 

▼ WPS

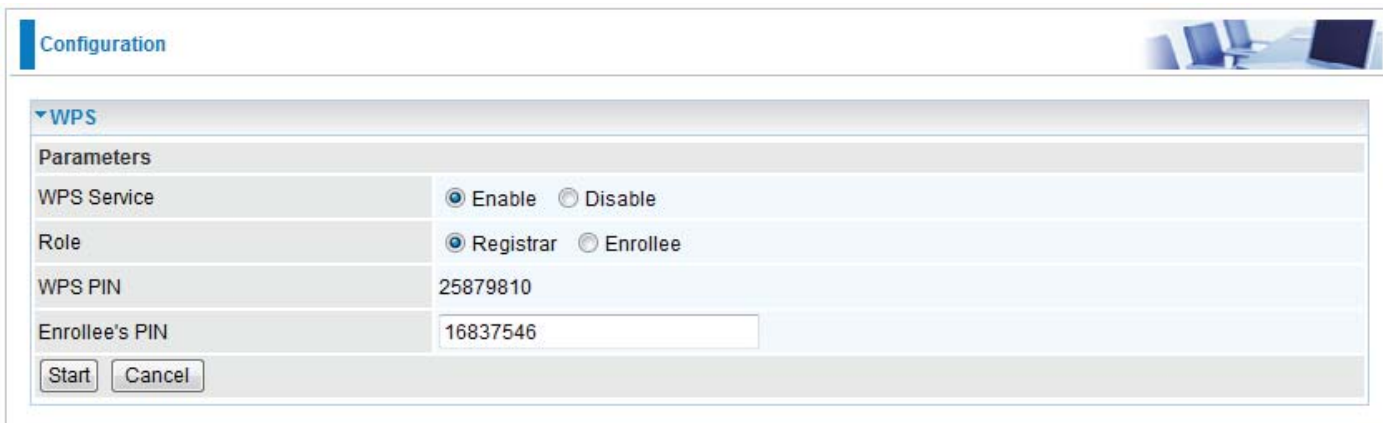
Parameters

| | |
|----------------|---|
| WPS Service | <input type="radio"/> Enable <input checked="" type="radio"/> Disable |
| Role | <input checked="" type="radio"/> Registrar <input type="radio"/> Enrollee |
| WPS PIN | 25879810 |
| Enrollee's PIN | <input type="text"/> |

Wi-Fi Network Setup

PIN Method: Configure AP as Registrar

1. Jot down the client's Pin (e.g. 16837546).



Configuration

WPS

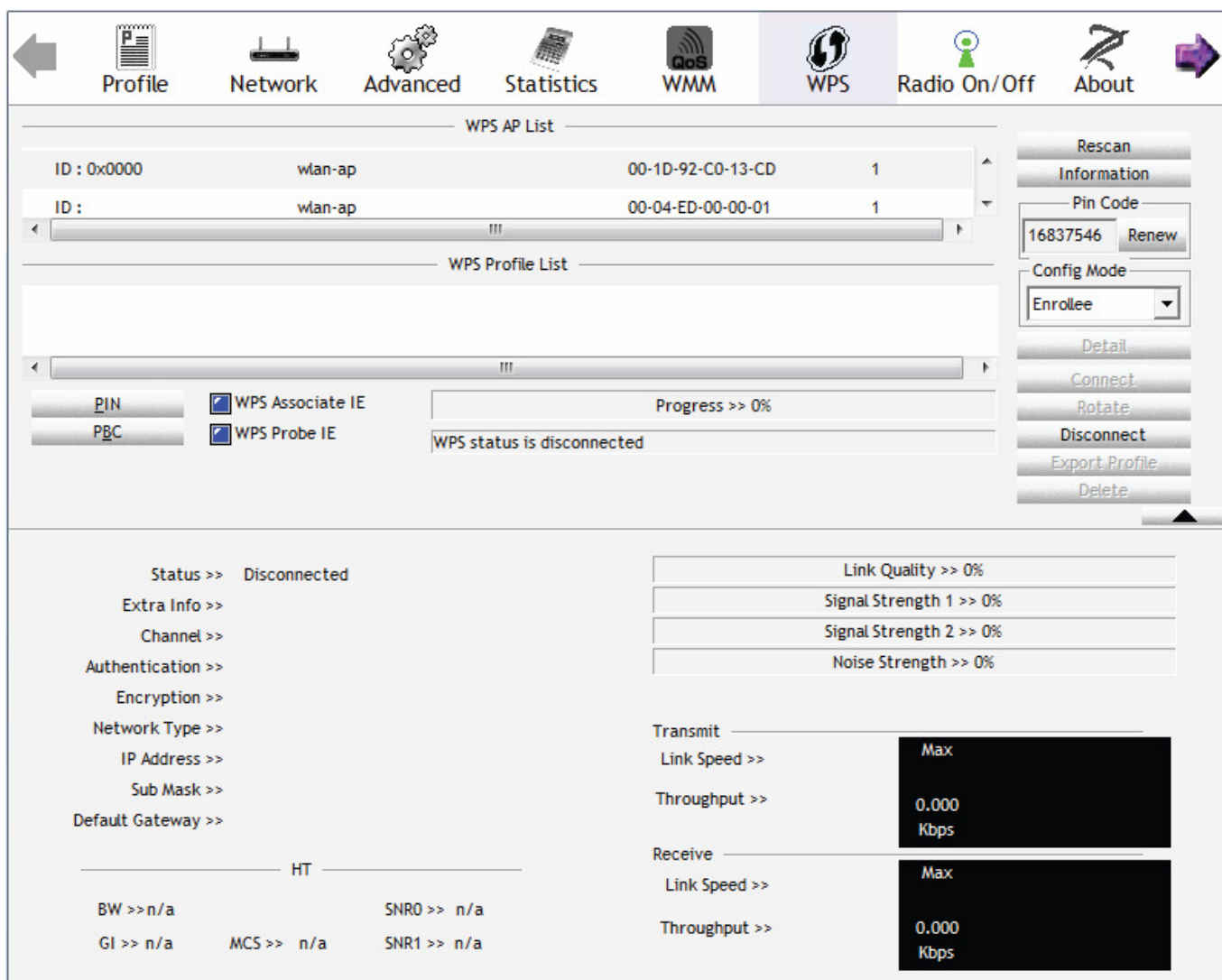
Parameters

| | |
|----------------|---|
| WPS Service | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Role | <input checked="" type="radio"/> Registrar <input type="radio"/> Enrollee |
| WPS PIN | 25879810 |
| Enrollee's PIN | 16837546 |

Start Cancel

2. Enter the Enrollee's PIN number and then press Start.

3. Launch the wireless client's WPS utility (eg. Ralink Utility). Set the Configure Mode as Enrollee, press the WPS button on the top bar, select the AP (eg. wlan-ap) from the WPS AP List column. Then press the PIN button located on the middle left of the page to run the scan.



Profile Network Advanced Statistics WMM WPS Radio On/Off About

WPS AP List

| | | | |
|-------------|---------|-------------------|---|
| ID : 0x0000 | wlan-ap | 00-1D-92-C0-13-CD | 1 |
| ID : | wlan-ap | 00-04-ED-00-00-01 | 1 |

WPS Profile List

WPS Associate IE WPS Probe IE

Progress >> 0%

WPS status is disconnected

Rescan Information Pin Code 16837546 Renew Config Mode Enrollee Detail Connect Rotate Disconnect Export Profile Delete

Status >> Disconnected

Link Quality >> 0%

Signal Strength 1 >> 0%

Signal Strength 2 >> 0%

Noise Strength >> 0%

Transmit Link Speed >> Max

Throughput >> 0.000 Kbps

Receive Link Speed >> Max

Throughput >> 0.000 Kbps

HT

BW >> n/a SNRO >> n/a

GI >> n/a MCS >> n/a SNR1 >> n/a

4. The client's SSID and security setting will now be configured to match the SSID and security setting of the registrar.

The screenshot displays a network configuration interface with the following sections:

- Navigation Bar:** Profile, Network, Advanced, Statistics, WMM, **WPS**, Radio On/Off, About.
- WPS AP List:**

| | | | |
|------|---------|-------------------|---|
| ID : | wlan-ap | 00-1D-92-C0-13-CD | 1 |
| ID : | wlan-ap | 00-04-ED-38-F7-2E | 1 |
- WPS Profile List:** wlan-ap
- WPS Configuration:**
 - PIN
 - WPS Associate IE
 - PBC
 - WPS Probe IE

Progress >> 100%

PIN - Get WPS profile successfully.
- WPS Action Panel:** Rescan, Information, Pin Code (16837546, Renew), Config Mode (Enrollee), Detail, Connect, Rotate, Disconnect, Export Profile, Delete.
- Status & Performance:**
 - Status >> wlan-ap <-> 00-1D-92-C0-13-CD
 - Extra Info >> Link is Up [TxPower:100%]
 - Channel >> 1 <-> 2412 MHz; central channel : 3
 - Authentication >> Open
 - Encryption >> NONE
 - Network Type >> Infrastructure
 - IP Address >> 192.168.1.100
 - Sub Mask >> 255.255.255.0
 - Default Gateway >> 192.168.1.254
- HT (High Throughput) Parameters:**
 - BW >> 40
 - GI >> long
 - MCS >> 15
 - SNR0 >> 19
 - SNR1 >> n/a
- Link Quality & Signal Strength:**
 - Link Quality >> 100%
 - Signal Strength 1 >> 64%
 - Signal Strength 2 >> 34%
 - Noise Strength >> 26%
- Transmit Performance:**
 - Link Speed >> 270.0 Mbps
 - Throughput >> 5.600 Kbps
- Receive Performance:**
 - Link Speed >> 54.0 Mbps
 - Throughput >> 81.608 Kbps

PIN Method: Configure AP as Enrollee

1. In the WPS configuration page, change the Role to Enrollee. Then press Start.
2. Jot down the WPS PIN (e.g. 25879810).

Configuration

▼ WPS

Parameters

| | |
|-------------|---|
| WPS Service | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Role | <input type="radio"/> Registrar <input checked="" type="radio"/> Enrollee |
| WPS PIN | 25879810 |
| Mode | PIN |

Start Cancel

3. Launch the wireless client's WPS utility (e.g. Ralink Utility). Set the Config Mode as Registrar. Enter the PIN number in the PIN Code column then choose the correct AP (eg. wlan-ap) from the WPS AP List section before pressing the PIN button to run the scan.

← Profile
Network
Advanced
Statistics
WMM
WPS
Radio On/Off
About →

WPS AP List

| | | | |
|-------------|---------|-------------------|---|
| ID : 0x0000 | wlan-ap | 00-1D-92-C0-13-CD | 1 |
| ID : | D2-VPN | 00-1B-11-E4-DA-D5 | 7 |

WPS Profile List

ExRegNWEA4036

| | | |
|-----|--|----------------|
| PIN | <input checked="" type="checkbox"/> WPS Associate IE | Progress >> 0% |
| PBC | <input checked="" type="checkbox"/> WPS Probe IE | |

Rescan

Information

Pin Code

25879810

Config Mode

Registrar

Detail

Connect

Rotate

Disconnect

Export Profile

| | |
|------------------------|--------------------------|
| Status >> Disconnected | Link Quality >> 0% |
| Extra Info >> | Signal Strength 1 >> 0% |
| Channel >> | Signal Strength 2 >> 0% |
| Authentication >> | Noise Strength >> 0% |
| Encryption >> | |
| Network Type >> | |
| IP Address >> | Transmit |
| Sub Mask >> | Link Speed >> Max |
| Default Gateway >> | Throughput >> 0.000 Kbps |
| | Receive |
| HT | Link Speed >> Max |
| BW >> n/a | Throughput >> 0.000 Kbps |
| GI >> n/a | |
| MCS >> n/a | |
| SNR0 >> n/a | |
| SNR1 >> n/a | |

4. The router's (AP's) SSID and security setting will now be configured to match the SSID and security setting of the registrar.

The screenshot displays the WPS configuration interface on a router. At the top, navigation tabs include Profile, Network, Advanced, Statistics, WMM, WPS (selected), Radio On/Off, and About. The main content area is divided into several sections:

- WPS AP List:** A table listing available WPS APs.

| ID | SSID | MAC | Priority |
|---------------|-------------------|-----|----------|
| ExRegNWEA4036 | 00-1D-92-C0-13-CD | 1 | |
| wlan-ap | 00-04-ED-38-F7-2E | 1 | |
- WPS Profile List:** Shows the selected profile 'ExRegNWEA4036' with a key icon.
- Configuration Options:** Includes checkboxes for 'WPS Associate IE' and 'WPS Probe IE', both of which are checked. A progress bar indicates 'Progress >> 100%'. A message below reads 'PIN - Get WPS profile successfully.' Buttons for PIN and PBC are also visible.
- Control Panel:** A vertical stack of buttons on the right side: Rescan, Information, Pin Code (with input field '25879810' and a Renew button), Config Mode (with a dropdown menu set to 'Registrar'), Detail, Connect, Rotate, Disconnect, and Export Profile.
- Connection Statistics:**
 - Status >> ExRegNWEA4036 <-> 00-1D-92-C0-13-CD
 - Extra Info >> Link is Up [TxPower:100%]
 - Channel >> 1 <-> 2412 MHz; central channel : 3
 - Authentication >> WPA2-PSK
 - Encryption >> AES
 - Network Type >> Infrastructure
 - IP Address >> 192.168.1.100
 - Sub Mask >> 255.255.255.0
 - Default Gateway >> 192.168.1.254
- HT (High Throughput) Parameters:**
 - BW >> 40
 - GI >> long
 - MCS >> 14
 - SNRO >> 20
 - SNR1 >> n/a
- Link Quality and Signal Metrics:**
 - Link Quality >> 100%
 - Signal Strength 1 >> 65%
 - Signal Strength 2 >> 39%
 - Noise Strength >> 26%
- Transmit Statistics:**
 - Link Speed >> 243.0 Mbps
 - Throughput >> 0.000 Kbps
 - Graph: Max 5,392 Kbps
- Receive Statistics:**
 - Link Speed >> 40.5 Mbps
 - Throughput >> 98.612 Kbps
 - Graph: Max 118.432 Kbps

5. Now to make sure that the setup is correctly done, cross check to see if the SSID and the security setting of the registrar setting match with the parameters found on both Wireless Configuration and Wireless Security Configuration page.

The screenshot displays the WPS configuration interface. The top navigation bar includes Profile, Network, Advanced, Statistics, WMM, WPS, Radio On/Off, and About. The main area is divided into 'WPS AP List' and 'WPS Profile List'. The 'WPS AP List' shows two entries with IDs 'wlan-ap' and MAC addresses '00-1D-92-C0-13-CD' and '00-04-ED-22-22-23'. The 'WPS Profile List' shows a profile named 'ExRegNWEA4036'. Below this, there are checkboxes for 'WPS Associate IE' and 'WPS Probe IE', both of which are checked. A progress bar shows 'Progress >> 0%' and the status 'WPS status is disconnected'. On the right side, there are buttons for 'Rescan', 'Information', 'Pin Code' (with a field containing '25879810' and a 'Renew' button), 'Config Mode' (set to 'Registrar'), 'Detail', 'Connect', 'Rotate', 'Disconnect', and 'Export Profile'. At the bottom, there is a configuration form for the registrar with fields for SSID, BSSID, Authentication Type, Encryption Type, Key Length, Key Index, and Key Material, along with a 'Show Password' checkbox and 'OK'/'Cancel' buttons.

the parameters on both Wireless Configuration and Wireless Security Configuration page are as follows:

Configuration

▼ **Wireless**

Parameters

| | | |
|-----------------------|--|-----------|
| WLAN Service | <input checked="" type="radio"/> Enable <input type="radio"/> Disable | |
| Mode | 802.11g + n ▼ | |
| Number of Active SSID | 1 ▼ | |
| SSID No. | <input checked="" type="radio"/> SSID1 | |
| ESSID | <input type="text" value="wlan-ap"/> | |
| Hide ESSID | <input type="radio"/> Enable <input checked="" type="radio"/> Disable | |
| Regulation Domain | N.America ▼ | |
| Channel ID | Channel 1 (2.412 GHz) ▼ | |
| Channel Width | 20/40MHZ ▼ | |
| Tx PowerLevel | <input type="text" value="100"/> | (0 ~ 100) |
| AP MAC Address | 00:1D:92:C0:13:CD | |
| AP Firmware Version | 2.3.0.0 | |
| WPS Service | <input checked="" type="radio"/> Enable <input type="radio"/> Disable | |
| WPS State | <input checked="" type="radio"/> Configured <input type="radio"/> Unconfigured | |
| WMM | <input type="radio"/> Enable <input checked="" type="radio"/> Disable | |

Wireless Distribution System (WDS)

| | | |
|----------------------|---|-------------------------|
| WDS Service | <input type="radio"/> Enable <input checked="" type="radio"/> Disable | |
| Peer WDS MAC address | 1. <input type="text"/> | 2. <input type="text"/> |
| | 3. <input type="text"/> | 4. <input type="text"/> |

** WDS depends on the settings of main security encryption type. **

Apply
Cancel
Security settings ▶

Configuration

▼ **Wireless Security**

Parameters

| | | |
|-------------------|---|---------|
| SSID No. | <input checked="" type="radio"/> ESSID1 | |
| Security Mode | WPA2 Pre-Shared Key ▼ | |
| WPA Algorithms | AES ▼ | |
| WPA Shared Key | <input type="text" value="811B5B9F3403DCB08I"/> | |
| Group Key Renewal | <input type="text" value="3600"/> | seconds |

Apply
Cancel

PBC Method:

1. Press the PBC button of the AP.
2. Launch the wireless client's WPS Utility (eg. Ralink Utility). Set the Config Mode as Enrollee. Then press the WPS button and choose the correct AP (eg. wlan-ap) from the WPS AP List section before pressing the PBC button to run the scan.

The screenshot displays the WPS Utility interface with the following components:

- Navigation Bar:** Profile, Network, Advanced, Statistics, WMM, **WPS**, Radio On/Off, About.
- WPS AP List:**

| ID | WPS AP Name | MAC Address | Priority |
|-------------|-------------|-------------------|----------|
| ID : | wlan-ap | 00-04-ED-00-00-01 | 1 |
| ID : 0x0004 | wlan-ap | 00-1D-92-C0-13-CD | 1 |
- WPS Profile List:** (Empty list)
- WPS Configuration:**
 - PIN
 - WPS Associate IE
 - PBC
 - WPS Probe IE
 - Progress >> 0%
 - WPS status is disconnected
- Right Panel:** Rescan, Information, Pin Code (16837546, Renew), Config Mode (Enrollee), Detail, Connect, Rotate, Disconnect, Export Profile, Delete.
- Status & Performance:**
 - Status >> Disconnected
 - Link Quality >> 0%
 - Signal Strength 1 >> 0%
 - Signal Strength 2 >> 0%
 - Noise Strength >> 0%
 - Transmit: Link Speed >> 8.800 Kbps, Throughput >> [Graph]
 - Receive: Link Speed >> 147.408 Kbps, Throughput >> [Graph]
 - HT: BW >> n/a, SNR0 >> n/a, GI >> n/a, MCS >> n/a, SNR1 >> n/a

3. When the PBC button is pushed, a wireless communication will be established between your router and the PC. The client's SSID and security setting will now be configured to match the SSID and security setting of the router.

The screenshot displays the WPS configuration interface on a router. At the top, navigation tabs include Profile, Network, Advanced, Statistics, WMM, WPS (selected), Radio On/Off, and About. The main area is divided into two sections: WPS AP List and WPS Profile List.

WPS AP List:

| | | | |
|------|---------|-------------------|---|
| ID : | wlan-ap | 00-1D-92-C0-13-CD | 1 |
| ID : | wlan-ap | 00-04-ED-38-F7-2E | 1 |

WPS Profile List:

- wlan-ap

Below the profile list, there are checkboxes for **WPS Associate IE** and **WPS Probe IE**, both of which are checked. A progress bar indicates **Progress >> 100%**. A message at the bottom of this section reads: **PBC - Get WPS profile successfully.**

On the right side, there are several control buttons: Rescan, Information, Pin Code (with input field 16837546 and Renew button), Config Mode (dropdown menu set to Enrollee), Detail, Connect, Rotate, Disconnect, Export Profile, and Delete.

The bottom section provides detailed connection information:

- Status >>** wlan-ap <-> 00-1D-92-C0-13-CD
- Extra Info >>** Link is Up [TxPower:100%]
- Channel >>** 1 <-> 2412 MHz; central channel : 3
- Authentication >>** Open
- Encryption >>** NONE
- Network Type >>** Infrastructure
- IP Address >>** 192.168.1.100
- Sub Mask >>** 255.255.255.0
- Default Gateway >>** 192.168.1.254

Performance metrics are shown on the right:

- Link Quality >>** 100%
- Signal Strength 1 >>** 60%
- Signal Strength 2 >>** 44%
- Noise Strength >>** 26%

Transmit and Receive statistics are also provided:

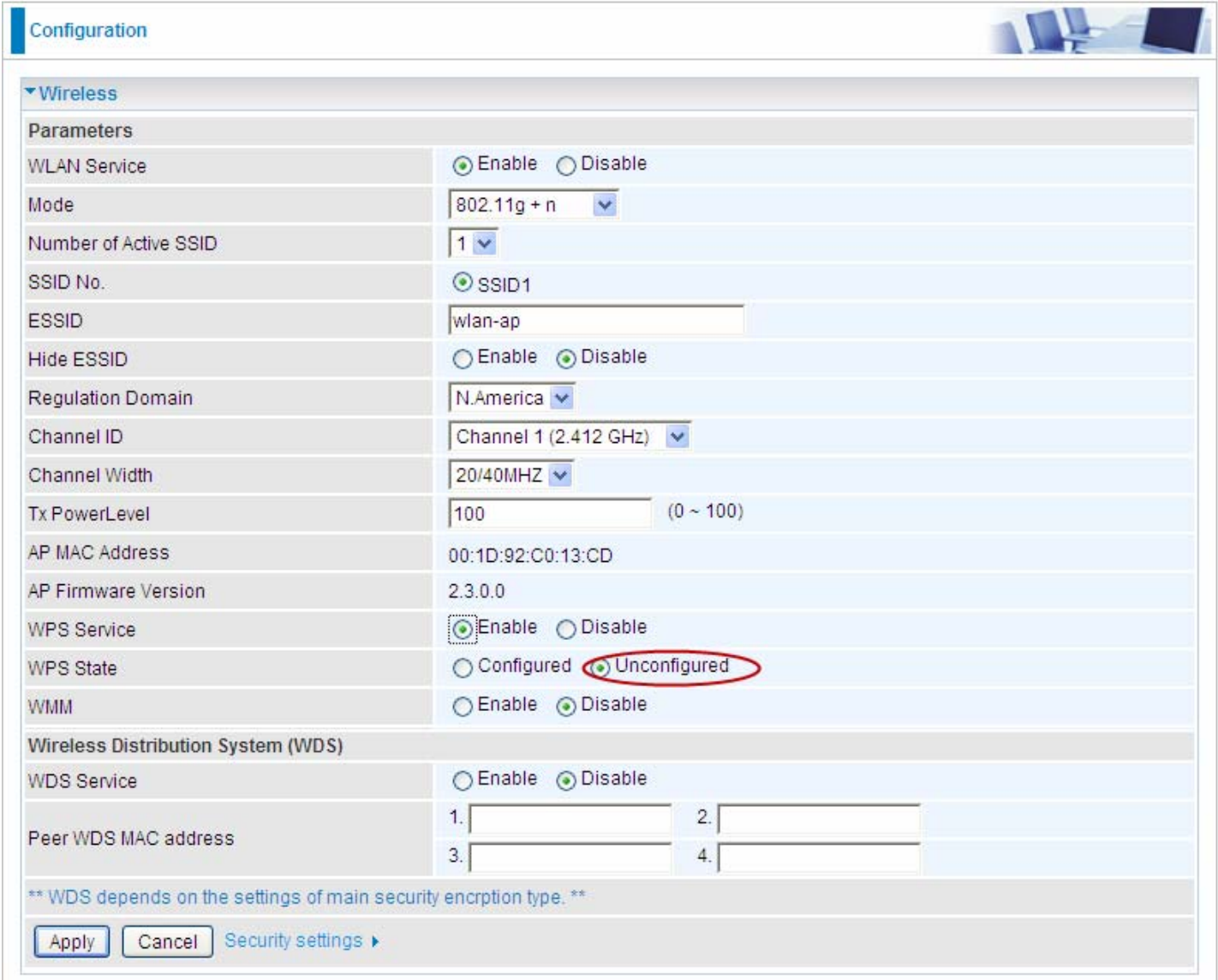
- Transmit:** Link Speed >> 243.0 Mbps, Throughput >> 0.192 Kbps. A graph shows a peak of 37.696 Kbps.
- Receive:** Link Speed >> 81.0 Mbps, Throughput >> 93.732 Kbps. A graph shows a peak of 1.798 Mbps.

At the bottom, HT (High Throughput) settings are listed:

- BW >>** 40
- GI >>** long
- MCS >>** 14
- SNRU >>** 20
- SNR1 >>** n/a

Wi-Fi Network Setup with Windows Vista WCN:

1. Jot down the AP PIN from the Web (eg. 25879810).
2. Access the Wireless configuration of the web GUI. Set the WPS State to **Unconfigured** then click Apply.



Configuration

▼ Wireless

Parameters

| | |
|-----------------------|--|
| WLAN Service | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Mode | 802.11g + n |
| Number of Active SSID | 1 |
| SSID No. | <input checked="" type="radio"/> SSID1 |
| ESSID | wlan-ap |
| Hide ESSID | <input type="radio"/> Enable <input checked="" type="radio"/> Disable |
| Regulation Domain | N.America |
| Channel ID | Channel 1 (2.412 GHz) |
| Channel Width | 20/40MHZ |
| Tx PowerLevel | 100 (0 ~ 100) |
| AP MAC Address | 00:1D:92:C0:13:CD |
| AP Firmware Version | 2.3.0.0 |
| WPS Service | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| WPS State | <input type="radio"/> Configured <input checked="" type="radio"/> Unconfigured |
| WMM | <input type="radio"/> Enable <input checked="" type="radio"/> Disable |

Wireless Distribution System (WDS)

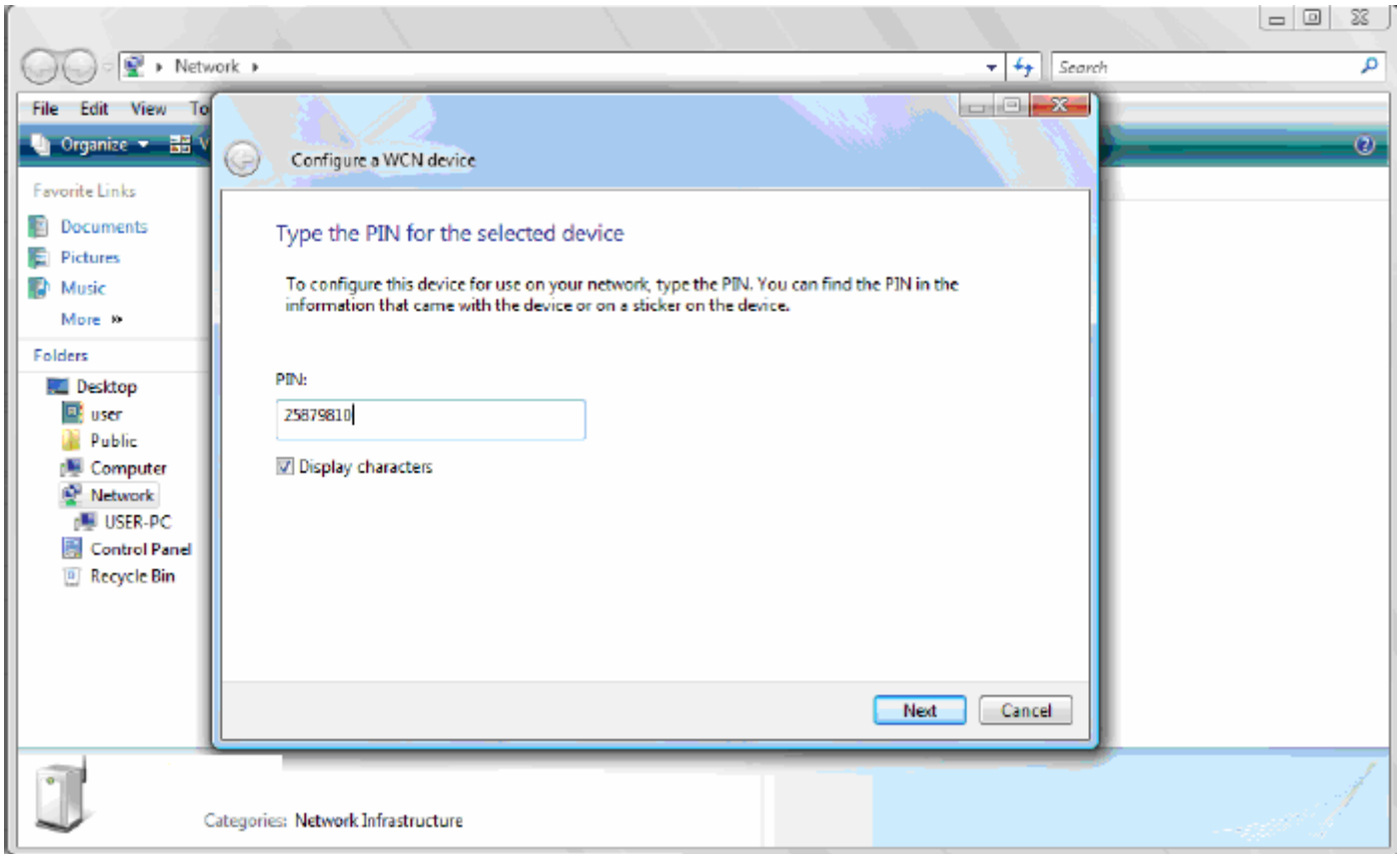
| | |
|----------------------|--|
| WDS Service | <input type="radio"/> Enable <input checked="" type="radio"/> Disable |
| Peer WDS MAC address | 1. <input type="text"/> 2. <input type="text"/> 3. <input type="text"/> 4. <input type="text"/> |

** WDS depends on the settings of main security encryption type. **

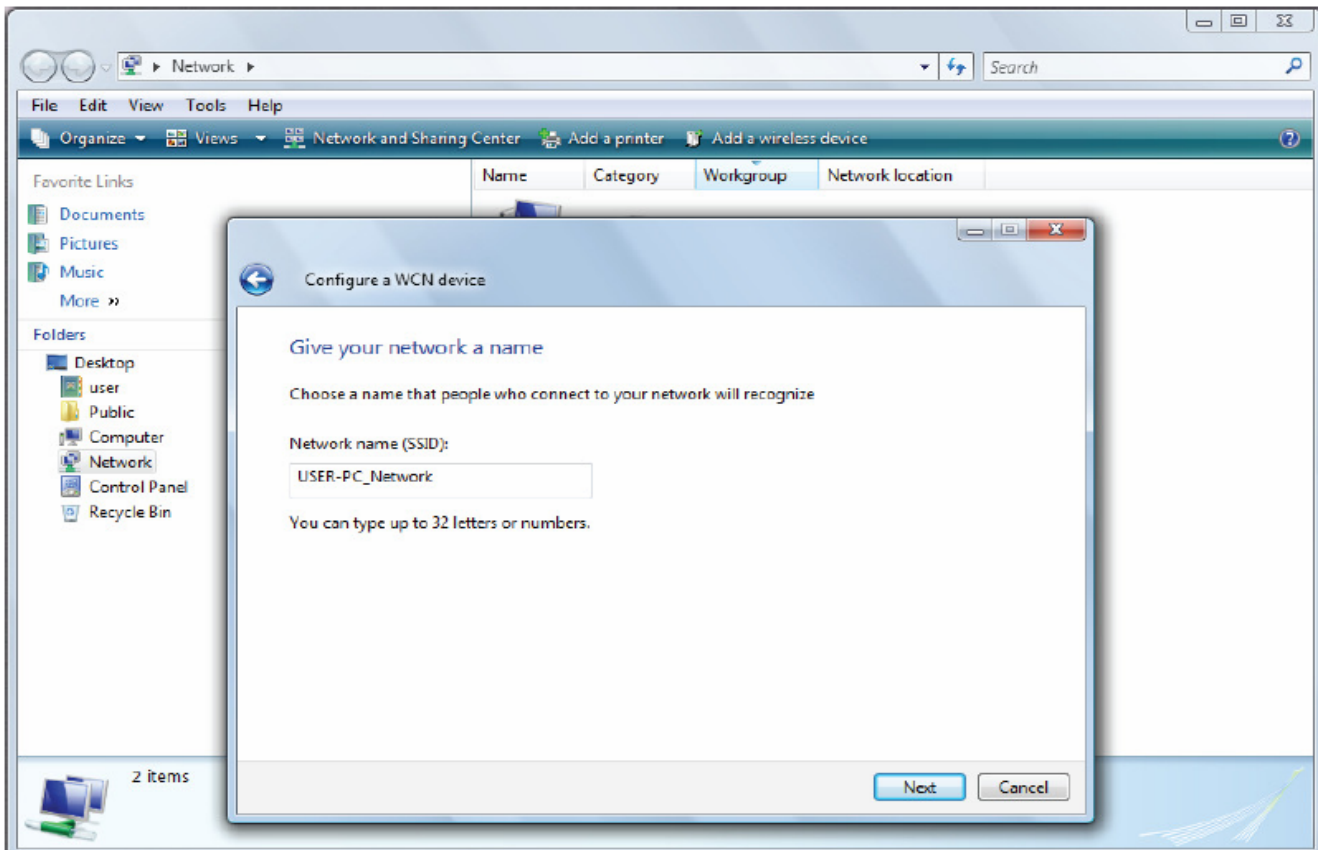
Apply Cancel [Security settings ▶](#)

3. In your Vista operating system, access the Control Panel page, then select Network and Internet >

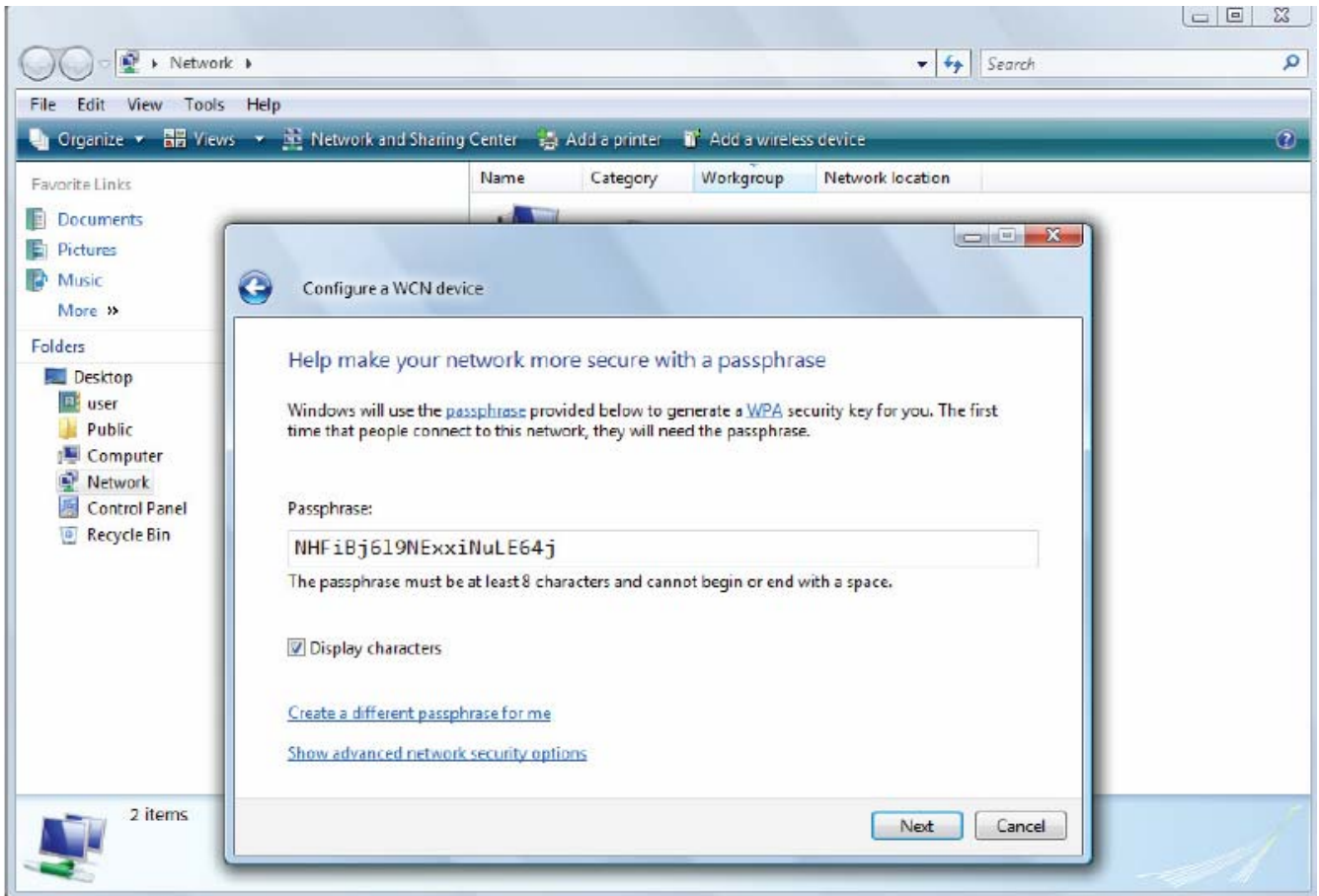
View Network Computers and Devices. Double click on the router icon and enter the AP PIN in the column provided then press Next.



4. Enter the AP SSID then click Next.



5. Enter the passphrase then click Next.



6. When you have come to this step, you will have completed the Wi-Fi network setup using the built-in WCN feature in Windows Vista.



DHCP Server

You can disable or enable the DHCP (Dynamic Host Configuration Protocol) server or enable the router's DHCP relay functions. The DHCP protocol allows your router to dynamically assign IP addresses to PCs on your network if they are configured to obtain IP addresses automatically.

DHCP Server Mode: Disable

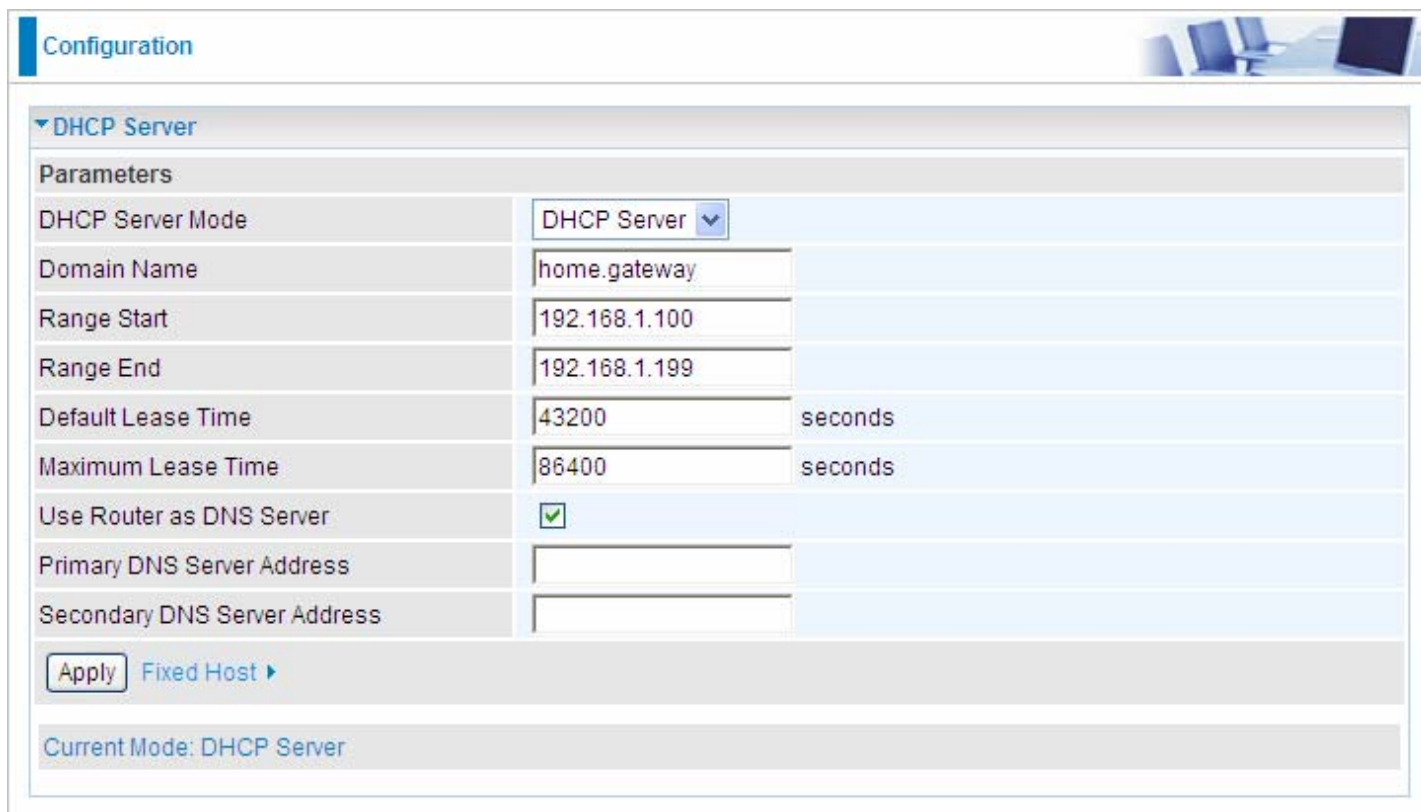
To disable the router's DHCP Server, check **Disabled** and then click **Apply**. When the DHCP Server is disabled, you will need to manually assign a fixed IP address to each PC on your network, and set the default gateway for each PC to the IP address of the router (the default is 192.168.1.254).



The screenshot shows a configuration page for the DHCP Server. At the top left, there is a 'Configuration' tab. Below it, the 'DHCP Server' section is expanded. Under the 'Parameters' heading, the 'DHCP Server Mode' is set to 'Disable' in a dropdown menu. An 'Apply' button is visible below the dropdown. At the bottom of the configuration area, it displays 'Current Mode: DHCP Server'.

DHCP Server Mode: DHCP Server

To configure the router's DHCP Server, check **DHCP Server**. You can then configure parameters of the DHCP Server including the IP pool (starting IP address and ending IP address to be allocated to PCs on your network), lease time for each assigned IP address (the period of time the IP address assigned will be valid), DNS IP address and the gateway IP address. These details are sent to the DHCP client (i.e. your PC) when it requests an IP address from the DHCP server. Click **Apply** to enable this function. If you check "**Use Router as a DNS Server**", the 3G Router performs the domain name lookup, finds the IP address from the outside network automatically and forwards it back to the requesting PC in the LAN (your Local Area Network).



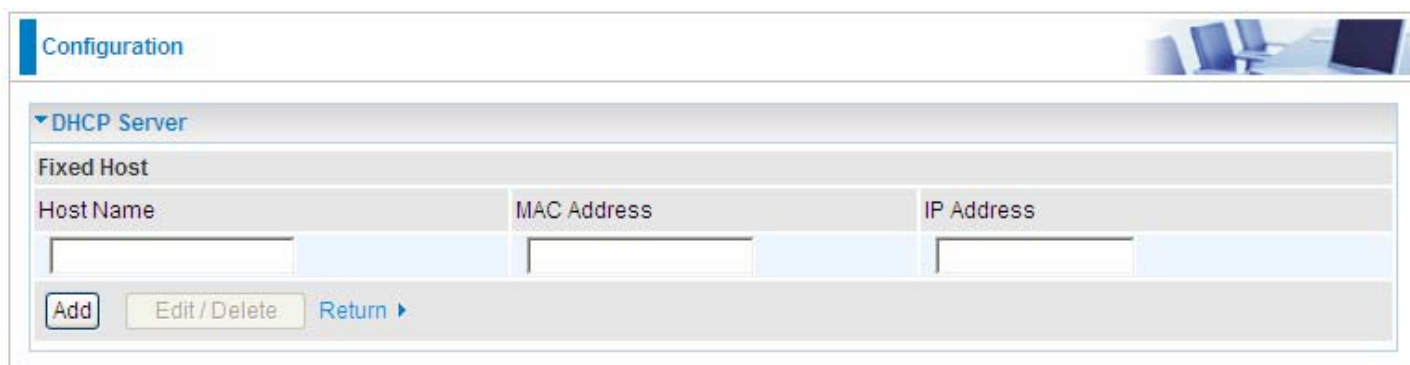
The screenshot shows the 'Configuration' page for the DHCP Server. The 'DHCP Server' section is expanded, showing a 'Parameters' table. The 'DHCP Server Mode' is set to 'DHCP Server'. The 'Domain Name' is 'home.gateway'. The 'Range Start' is '192.168.1.100' and the 'Range End' is '192.168.1.199'. The 'Default Lease Time' is '43200' seconds and the 'Maximum Lease Time' is '86400' seconds. The 'Use Router as DNS Server' checkbox is checked. There are empty input fields for 'Primary DNS Server Address' and 'Secondary DNS Server Address'. At the bottom, there is an 'Apply' button and a 'Fixed Host' link with a right-pointing arrow. Below the form, it says 'Current Mode: DHCP Server'.

| Parameters | |
|------------------------------|-------------------------------------|
| DHCP Server Mode | DHCP Server |
| Domain Name | home.gateway |
| Range Start | 192.168.1.100 |
| Range End | 192.168.1.199 |
| Default Lease Time | 43200 seconds |
| Maximum Lease Time | 86400 seconds |
| Use Router as DNS Server | <input checked="" type="checkbox"/> |
| Primary DNS Server Address | |
| Secondary DNS Server Address | |

Apply Fixed Host ▶

Current Mode: DHCP Server

Click [Fixed Host ▶](#) to set to assign a certain IP to a specific MAC if you want.



The screenshot shows the 'Configuration' page for the Fixed Host. The 'Fixed Host' section is expanded, showing a table with three columns: 'Host Name', 'MAC Address', and 'IP Address'. There are three empty input fields corresponding to these columns. At the bottom, there are buttons for 'Add', 'Edit / Delete', and 'Return ▶'.


| Host Name | MAC Address | IP Address |
|-----------|-------------|------------|
| | | |

Add Edit / Delete Return ▶

Enter the Host Name, MAC Address, the IP Address, the IP Address should in the DHCP server IP range. Click **Add**. It will be OK.

DHCP Server Mode: DHCP Relay

If you check **DHCP Relay** and then you must enter the IP address of the DHCP server which assigns an IP address back to the DHCP client in the LAN. Use this function only if advised to do so by your network administrator or ISP. Click **Apply** to enable this function.

Configuration 

▼ DHCP Server

Parameters

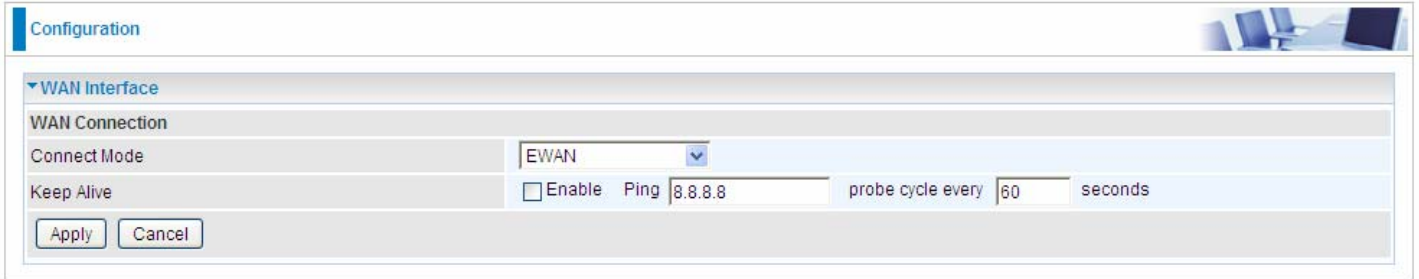
| | |
|-------------------|----------------------|
| DHCP Server Mode | DHCP Relay ▼ |
| DHCP Relay Server | <input type="text"/> |

Current Mode: DHCP Server

WAN (Wide Area Network)

A WAN (Wide Area Network) is an outside connection to another network or the Internet. There are two items within the **WAN** section: **WAN interface and WAN Profile.**

WAN Interface(EWAN)



The screenshot shows a configuration window titled "Configuration" with a sub-section "WAN Interface". Under "WAN Connection", the "Connect Mode" is set to "EWAN" via a dropdown menu. The "Keep Alive" section has an unchecked "Enable" checkbox, a "Ping" field with the value "8.8.8.8", and a "probe cycle every" field with the value "60" followed by the unit "seconds". At the bottom left, there are "Apply" and "Cancel" buttons.

Connect Mode: Select the main port from the drop-down menu.

Keep Alive: Enable to ping the IP (can be changed as required) every 60 seconds (can be changed based as required) to keep your EWAN connection always-on.

Click **Apply** to confirm the change.

WAN Interface(3G)



The screenshot shows a configuration window titled "Configuration" with a sub-section "WAN Interface". Under "WAN Connection", the "Connect Mode" is set to "3G" via a dropdown menu. The "Keep Alive" section has an unchecked "Enable" checkbox, a "Ping" field with the value "8.8.8.8", and a "probe cycle every" field with the value "60" followed by the unit "seconds". At the bottom left, there are "Apply" and "Cancel" buttons.

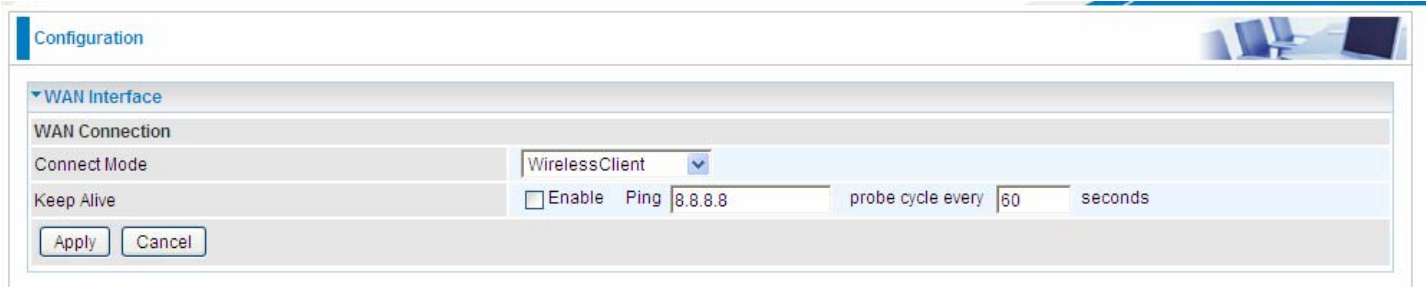
Connect Mode: Select the main port from the drop-down menu.

Keep Alive: Enable to ping the IP (can be changed as required) every 60 seconds (can be changed based as required) to keep your 3G WAN connection always-on.

Click **Apply** to confirm the change.

WAN Interface(WirelessClient)

When WirelessClient is selected, the router will act as an ordinary wireless client to connect to an AP to connect to the Internet. Move on to WAN Profile to configure exact parameters.



Configuration

WAN Interface

WAN Connection

Connect Mode: WirelessClient

Keep Alive: Enable Ping: 8.8.8.8 probe cycle every: 60 seconds

Apply Cancel

Keep Alive: Enable to ping the IP (can be changed as required) every 60 seconds (can be changed based as required) to keep your WAN connection always-on.

Click **Apply** to confirm the change.

WAN Interface(Dual WAN)



The screenshot shows a configuration window titled "Configuration" with a sub-section "WAN Interface". The "WAN Connection" section is expanded to show "Dual WAN(Failover)". Under "Failover Parameters", the "Main WAN" is set to "EWAN" and the "Backup WAN" is set to "3G". The "Probe" checkbox is checked and labeled "Enable". The "Connectivity Decision" is set to "Not in service when probing failed after 3 consecutive times." The "Failover Probe Cycle" is set to "Every 12 seconds." and the "Failback Probe Cycle" is set to "Every 4 seconds." The "Detect Rule" section has two radio buttons: "Ping Gateway" (selected) and "Ping Host" (unselected). At the bottom, there are "Apply" and "Cancel" buttons.

Connect Mode: Select the Dual WAN from the drop-down menu.

Main WAN: Choose EWAN or 3G as main WAN. Click the link to go to WAN Profile page to configure its parameters.

Backup WAN: Choose the left as backup WAN. Click the link to go to WAN Profile page to configure its parameters.

Connectivity Decision: Enter the value for the times when probing failed to switch backup port.

Failover Probe Cycle: Set the time duration for the Failover Probe Cycle to determine when the router will switch to the backup connection (backup port) once the main connection (main port) fails.

Note: *The time values entered in Failover Probe Cycle field is set for each probe cycle and decided by Probe Cycle duration multiplied by Connection Decision value (e.g. 60 seconds are multiplied by 12 seconds and 5 consecutive fails).*

Faiback Probe Cycle: Set the time for the Faiback Probe Cycle.

Detect Rule (either one):

- **Ping Gateway:** It will send ping packet to gateway and wait response from gateway in every "Probe Cycle".
- **Ping Host:** It will send ping packet to specific host and wait response in every "Probe Cycle". The host must be an IP address.

Click **Apply** to confirm the change.

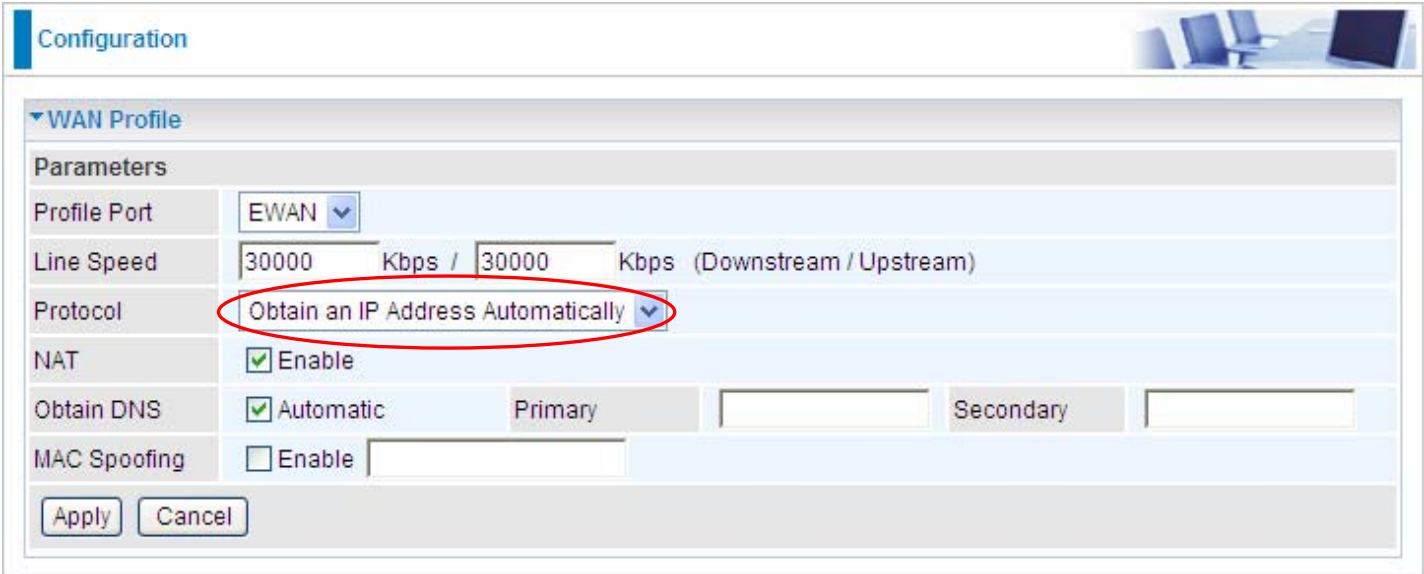
WAN Profile

Main Port – EWAN

Billion SG6200NXL offers a WAN port to connect to Cable Modems and fiber optic lines. This alternative, yet faster method to connect to the internet will provide users with more flexibility to get online.

Obtain an IP Address Automatically (EWAN)

When connecting to the ISP, Billion SG6200NXL also functions as a DHCP client. Billion SG6200NXL can automatically obtain an IP address, Netmask, gateway address, and DNS server addresses if the ISP assigns this information via DHCP.



The screenshot shows a web-based configuration interface for a WAN profile. The page title is 'Configuration'. Under the 'WAN Profile' section, there are several parameters to be configured:

- Profile Port:** A dropdown menu set to 'EWAN'.
- Line Speed:** Two input fields, both containing '30000', followed by 'Kbps / Kbps (Downstream / Upstream)'.
- Protocol:** A dropdown menu with 'Obtain an IP Address Automatically' selected. This dropdown is circled in red in the image.
- NAT:** A checkbox labeled 'Enable' which is checked.
- Obtain DNS:** A checkbox labeled 'Automatic' which is checked. To its right are two input fields labeled 'Primary' and 'Secondary', both currently empty.
- MAC Spoofing:** A checkbox labeled 'Enable' which is unchecked. To its right is an empty input field.

At the bottom of the configuration area, there are two buttons: 'Apply' and 'Cancel'.

Line Speed: Set the downstream and upstream of your connection in kilobytes per second. The connection speed is used by QoS settings.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single ISP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

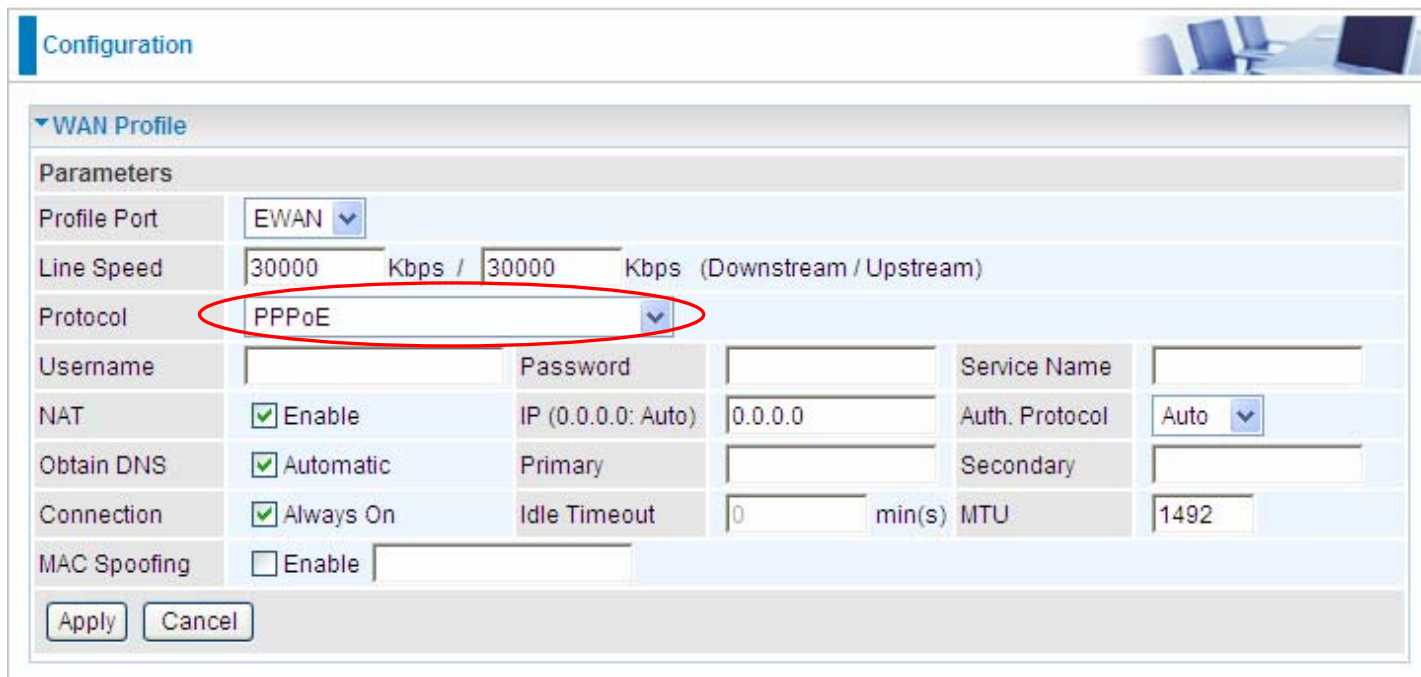
Obtain DNS Automatically: Select this check box to use DNS.

Primary DNS/ Secondary DNS: Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the netmask.

MAC Spoofing: Select Enable and enter a MAC address that will temporarily change your router's MAC address to the one you have specified in this field. Leave it as Disabled if you do not wish to change the MAC address of your router.

PPPoE (EWAN)

PPPoE (PPP over Ethernet) provides access control in a manner similar to dial-up services using PPP.



The screenshot shows the 'WAN Profile' configuration page. The 'Protocol' dropdown menu is highlighted with a red circle and set to 'PPPoE'. Other fields include Profile Port (EWAN), Line Speed (30000 Kbps), Username, Password, Service Name, NAT (checked), Obtain DNS (checked), Connection (checked), and MTU (1492).

Username: Enter the username provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive). This is in the format of “username@ispname” instead of simply “username”.

Password: Enter the password provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive)

Service Name: This item is for identification purposes. If it is required, your ISP provides you the information. Maximum input is **15** alphanumeric characters.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single ISP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

IP Address: Your WAN IP address. Leave this at 0.0.0.0 to automatically obtain an IP address from your ISP.

Auth. Protocol: Default is **Auto**. Your ISP advises on using **Chap** or **Pap**.

Obtain DNS Automatically: Select this check box to use DNS.

Primary DNS/ Secondary DNS: Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the Netmask.

Connection:

Ⓞ **Always on:** If you want the router to establish a PPPoE session when starting up and to automatically re-establish the PPPoE session when disconnected by the ISP.

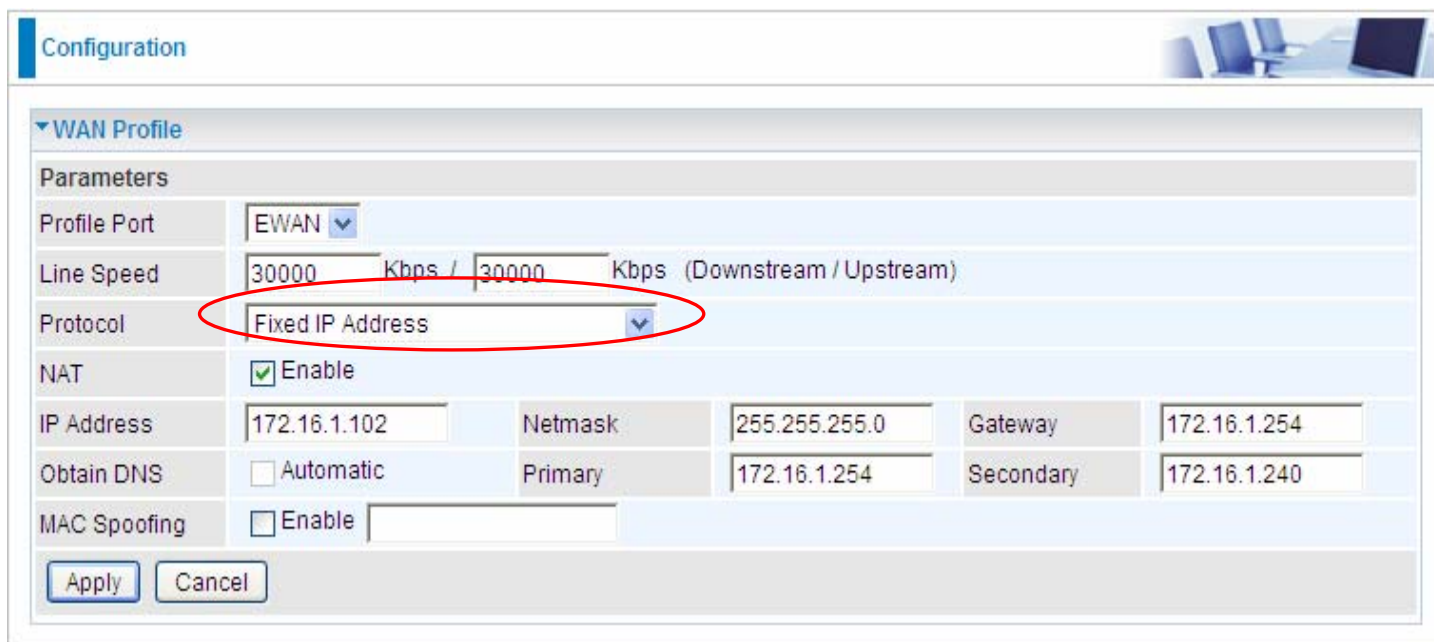
Ⓞ **Connect to Demand (un-select Always On):** If you want to establish a PPPoE session only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet). In this mode, you must set Idle Timeout value at same time.

Idle Timeout: Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time. The minimum value is 10 minutes.

MTU: Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) an IP attempts to send through the interface.

Fixed IP Address (EWAN)

Select this option to set static IP information. You will need to enter in the Connection type, IP address, netmask, and gateway address, provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which is four IP octets separated by a dot (x.x.x.x). The Router will not accept the IP address if it is not in this format.



The screenshot shows the 'Configuration' page for the WAN Profile. The 'Parameters' section includes the following fields:

| | | | | | |
|--------------|--|---------|---------------|-----------|-------------------------|
| Profile Port | EWAN | | | | |
| Line Speed | 30000 | Kbps / | 30000 | Kbps | (Downstream / Upstream) |
| Protocol | Fixed IP Address | | | | |
| NAT | <input checked="" type="checkbox"/> Enable | | | | |
| IP Address | 172.16.1.102 | Netmask | 255.255.255.0 | Gateway | 172.16.1.254 |
| Obtain DNS | <input type="checkbox"/> Automatic | Primary | 172.16.1.254 | Secondary | 172.16.1.240 |
| MAC Spoofing | <input type="checkbox"/> Enable | | | | |

Buttons: Apply, Cancel

Line Speed: Set the downstream and upstream of your connection in kilobytes per second. The connection speed is used by QoS settings.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

IP Address: Your WAN IP address. Leave this at 0.0.0.0 to automatically obtain an IP address from your ISP.

IP Netmask: The default is 0.0.0.0. User can change it to other such as 255.255.255.0. Type the netmask assigned to you by your ISP (if given).

Gateway: You must specify a gateway IP address (supplied by your ISP)

Obtain DNS Automatically: Select this check box to use DNS.

Primary DNS/ Secondary DNS: Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the netmask.

MAC Spoofing: Select Enable and enter a MAC address that will temporarily change your router's MAC address to the one you have specified in this field. Leave it as Disabled if you do not wish to change the MAC address of your router.

Main Port - 3G

The router allows you to insert a 3G/HSDPA card to its USB slot, enabling you to use a 3G/ HSDPA, UMTS, EDGE, GPRS, or GSM Internet connection, makes downstream rates of to 14.4 Mbps*.

| Parameters | |
|-----------------------------|--|
| Profile Port | 3G |
| Usage Allowance | <input type="checkbox"/> Enable |
| ISP Mode | Telstra_AUS |
| TEL No. | *99***1# |
| APN | internet |
| Username | |
| Password | |
| Authentication Protocol | Auto |
| PIN | |
| Connection | <input type="radio"/> Always On <input checked="" type="radio"/> Connect on Demand |
| Idle Timeout | 600 seconds |
| Obtain DNS Automatically | <input type="checkbox"/> Enable |
| Primary DNS / Secondary DNS | |

*Warning: Entering the wrong PIN code three times will lock the SIM.

Apply Cancel

ISP Mode: Choose 3G service provider.

TEL No.: The dial string to make a GPRS / 3G user internetworking call. It may be provided by your mobile service provider.

APN: An APN is similar to a URL on the WWW, it is what the unit makes a GPRS / UMTS call. The service provider is able to attach anything to an APN to create a data connection. Requirements for APN assignment varies between different service providers. Most service providers have an internet portal which they connect a DHCP Server to, giving you access to the internet i.e. Some 3G operators use the APN 'internet' for their portal. The default value of APN is "internet".

Username: Enter the username provided by your service provider.

Password: Enter the password provided by your service provider.

Auth. Protocol: Manually specify CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol) if you know which authentication type the server is using (when acting as a client), or the authentication type you want the clients to use when they are connecting to you (when acting as a server). When using PAP, the password is sent unencrypted, while CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that an intruder has not replaced the client.

MTU: Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

PIN: PIN stands for Personal Identification Number. A PIN code is a numeric value used in certain systems as a password to gain access, and authentication. In mobile phones a PIN code locks the SIM card until you enter the correct code. If you enter the PIN code incorrectly into the phone 3 times in a row, then the SIM card will be blocked and a PUK code will be required from your network / service provider to unlock it.

Note: If you enter an incorrect PIN code three times in a row, your SIM card will be blocked. In this case, please enter your PUK code (it can be supplied by your service provider) and then re-enter your PIN.

Connection:

- **Always On:** The router will make UMTS/GPRS call when starting up. Enabling Always On, will give you an option of Keep Alive.
- **Connect on Demand:** If you want to make UMTS/GPRS call only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet). In this mode, you must set Idle Timeout value at same time. Enabling Connect on Demand will give you an option of Idle Timeout.

Idle Timeout: Auto-disconnect the connection when there is no activity on this call for a predetermined period of time. The default value is 10 seconds.

Obtain DNS Automatically: Select this checkbox to use DNS.

Primary DNS/ Secondary DNS: Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.

Note: If you don't know how to set these values and please keep them untouched.



When insert 3G card, you should wait 30 seconds then dial up; or you can dial up first then insert 3G card after 30 seconds. If there is an error occurs while you don't operate according to the above, pull out the 3G card or restart the router will solve this problem.

Click **Usage Allowance** to go to the Usage Allowance configuration page.

| | |
|-------------------|---------------------------------|
| ▼ WAN Profile | |
| Parameters | |
| Profile Port | 3G ▼ |
| Usage Allowance ▶ | <input type="checkbox"/> Enable |

| | |
|--------------------------------------|--|
| Configuration | |
| ▼ 3G Usage Allowance | |
| Parameters | |
| Mode | <input checked="" type="radio"/> Volume-based |
| | Only Download ▼ 50 MB data volume per month included |
| | <input type="radio"/> Time-based |
| | 212 hours per month included |
| | The billing period always begins on day 12 of a month. |
| Over usage allowance action | E-mail Alert and Disconnect ▼ |
| Save the statistics to ROM | Every one hour ▼ |
| <input type="button" value="Apply"/> | |

In order to query online time or volume used, you can set the following options.

Mode: Two methods are provided, that is, **Volume-based** and **Time-based**.

Volume-based: If choosing **Volume-based**, you can view the volume you have used.

| | |
|------------|--|
| Parameters | |
| Mode | <input checked="" type="radio"/> Volume-based |
| | Only Download ▼ 50 MB data volume per month included |
| | Only Download Only Upload Download and Upload |
| | th included |
| | The billing period always begins on day 12 of a month. |

Only Download: Only make statistics of Download Traffic.

Only Upload: Only make statistics of Upload Traffic.

Download and Upload: Make statistics of both Download and Upload Traffic.

Time-based: If choosing **Time-based**, you can view the online hours you have used.

The screenshot shows a configuration window titled "3G Usage Allowance". Under the "Parameters" section, there are two radio button options: "Volume-based" and "Time-based". The "Time-based" option is selected. Below the "Volume-based" option, there is a dropdown menu set to "Only Download" and a text input field containing "50", followed by the text "MB data volume per month included". Below the "Time-based" option, there is a text input field containing "212", followed by the text "hours per month included". At the bottom, there is a text input field containing "12", followed by the text "The billing period always begins on day 12 of a month." On the left side of the form, there is a label "Mode" next to a greyed-out area.

You can also assign the billing period.

Over usage allowance action: If the online time or traffic you have used exceeds the usage allowance you set. The system will do the followings operations.

A dropdown menu with the following options: "E-mail Alert and Disconnect", "E-mail Alert", "E-mail Alert and Disconnect", and "Disconnect". The "E-mail Alert and Disconnect" option is currently selected and highlighted in blue.

Save the statistics to ROM: Choose the time interval for saving statistics. You can choose to save for **Every one hour** or **Disable** the function.

A dropdown menu with the following options: "Every one hour", "Every one hour", and "Disable". The "Every one hour" option is currently selected and highlighted in blue.

Main Port – WirelessClient

Configuration

WAN Profile

Parameters

Main Port: WirelessClient

Protocol: Obtain an IP Address Automatically

NAT: Enable

Obtain DNS: Automatic Primary: [] Secondary: []

SSID: []

Security Mode: OPEN

Encryption Type: None

Apply Cancel SCAN

Site Survey

| Ch | SSID | BSSID | Security | Signal(%) | W-Moe | ExtCh | NT |
|----|------|-------|----------|-----------|-------|-------|----|
|----|------|-------|----------|-----------|-------|-------|----|

Protocol: Select to obtain an IP address automatically or choose to set a fixed IP for your gateway.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single ISP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

Obtain DNS: Choose Automatic or set the exact values yourself.

SSID: The target wireless AP. User can alternatively input the SSID manually or also use the Scan button to scan and select.

Security Mode: Set the wireless security mode, namely, OPEN, SHARED, WPAPSK and WPA2PSK. User can set the mode yourself if user himself (herself) knows the mode well, or user can choose to scan button and select the target SSID.

Continue: Move on to connect to the SSID.

Cancel: Undo the current step.

SCAN: Press this button to scan the SSIDs in the air.



WAN Profile

Parameters

| | | | |
|-----------------|---|-----------|----------------------|
| Main Port | WirelessClient | | |
| Protocol | Obtain an IP Address Automatically | | |
| NAT | <input checked="" type="checkbox"/> Enable | | |
| Obtain DNS | <input checked="" type="checkbox"/> Automatic | Primary | <input type="text"/> |
| | | Secondary | <input type="text"/> |
| SSID | <input type="text"/> | | |
| Security Mode | OPEN | | |
| Encryption Type | None | | |

Site Survey

| | Ch | SSID | BSSID | Security | Signal(%) | W-Moe | ExtCh | NT |
|-----------------------|----|------------|-------------------|-----------------|-----------|---------|-------|----|
| <input type="radio"/> | 7 | billion-ap | 02:10:18:01:00:02 | WPA2PSK/AES | 34 | 11b/g/n | NONE | In |
| <input type="radio"/> | 7 | Altratek | 00:04:ed:11:22:68 | WPAPSK/TKIP/AES | 24 | 11b/g/n | ABOVE | In |
| <input type="radio"/> | 7 | CMCC | 00:04:ed:11:22:69 | NONE | 24 | 11b/g/n | ABOVE | In |

BEsmart

Register

The issue of environmental protection and energy conservation has been received great attentions since the global warming and energy shortage have become a serious worldwide crisis.

Billion BEsmart highlights the importance of energy preservations and managements, and contributes smart solutions for Telco/ISP/SI service providers who dedicate to strengthening customer satisfactions. With the implement of the smart control, track, and monitor power consumption technologies, energy usage could be clearly examined and analyzed anytime and anywhere simply through a smart phone. It helps reduce energy waste, provide a green environment, and further increase the benefit of the mutual investment, that is, the investors and customers.

User need to register an account to access the site and use the BEsmart service.

Configuration

Register

Parameters

Username

Password

Re-type Password

Email

Terms of Service:

Please read the Terms of Service below:
Billion "BEsmart" Terms of Use

The BEsmart (the "Service") belongs to a product/service of Billion (Billion Electric Co., Ltd.). The Service includes App and any or all of its components. By using the Service, it also indicates that you (the "User") accept to be bound by the following terms and conditions and that you agree to abide by them. These terms and policies are in effect throughout the full duration of your use of the Site and Service, so if you do not agree with these Terms of Use, we suggest you should stop downloading, installing or using the service right away.

1. Account and Password
Upon registration, we will provide you with a login identifier and a password in order to access the site and use the service. Please be responsible for safeguarding such information from disclosure and for unauthorized use for your own rights and interests. You are fully and solely responsible for all people, including yourself or the third

I accept the Terms of Service.

Apply

Username: Enter the username.

Password: Enter the password for the account.

Re-type Password: Confirm the password.

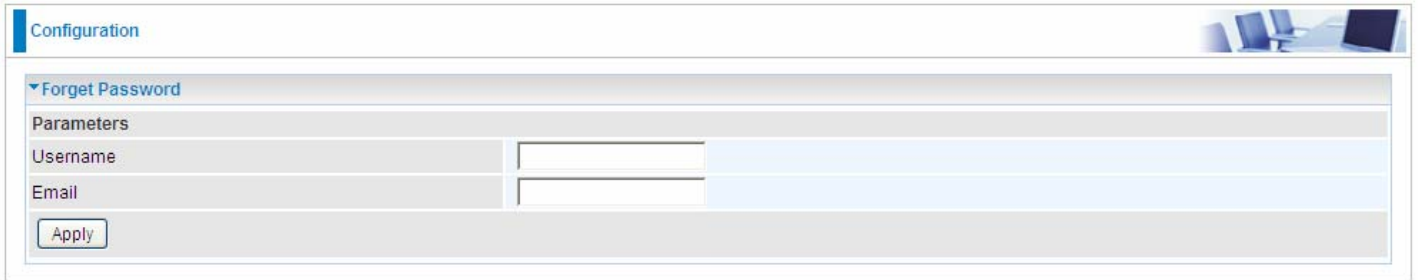
Email: Enter an email address to receive the messages like account information when user forgets the account and wants to retrieve the account, from the router.

Please first read the terms of service and accept the terms of service if user wants to register the account.

Press **Apply** to submit.

Forget Password

This section is for user to retrieve your password when forgotten.



The screenshot shows a web interface with a 'Configuration' header. Below it is a section titled 'Forget Password' with a dropdown arrow. Underneath, there is a 'Parameters' section containing two input fields: 'Username' and 'Email'. An 'Apply' button is located at the bottom left of the form area.

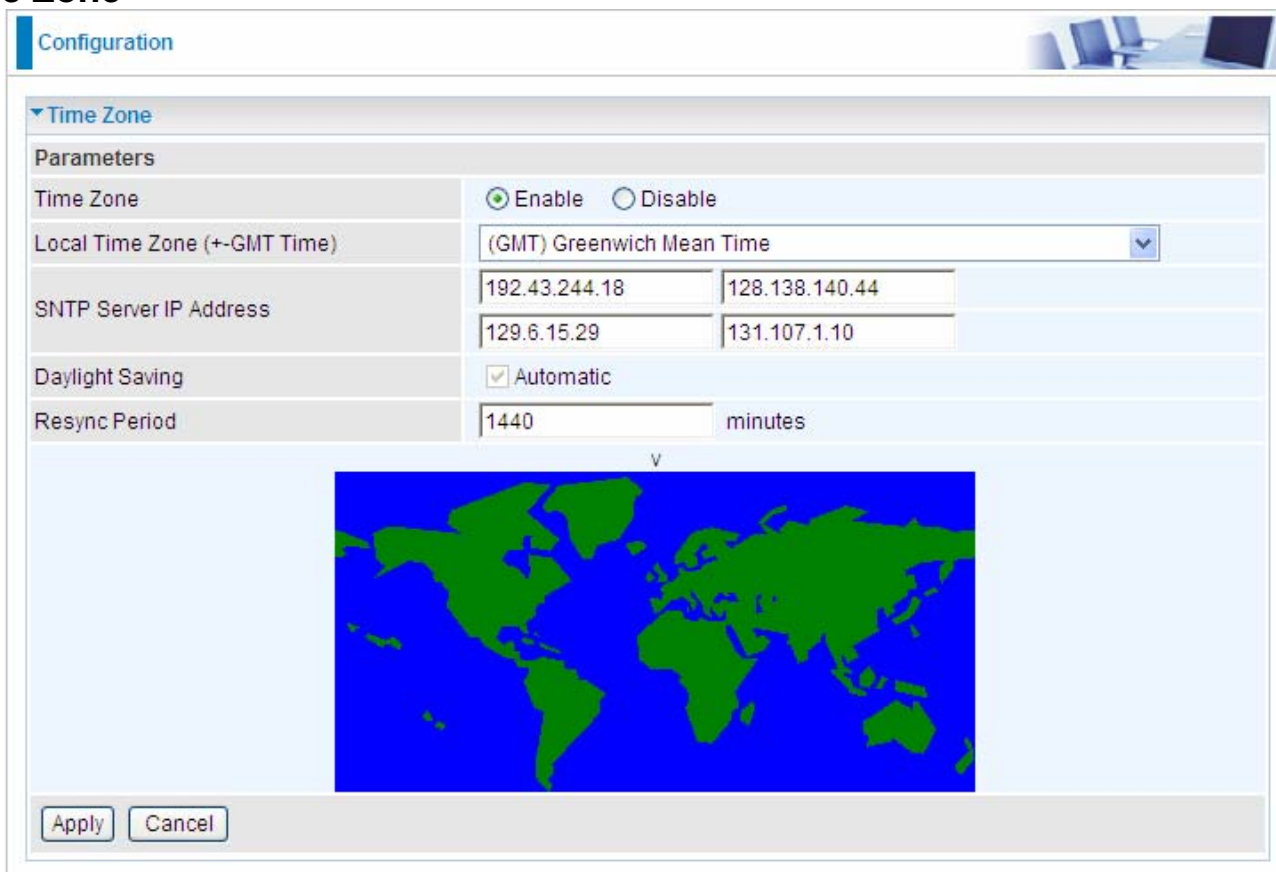
Username: Enter your username of your BEsmart service account registered.

Email: Enter the email address you previously registered to receive the message concerning your password.

System

There are six items within the **System** section: **Time Zone**, **Firmware Upgrade**, **Backup/Restore**, **Restart**, **User Management** and **Mail Alert**.

Time Zone



The screenshot shows a web-based configuration interface for a router. The main heading is 'Configuration'. Below it, there is a section for 'Time Zone'. The 'Parameters' section includes:

- Time Zone:** A radio button for 'Enable' (selected) and a radio button for 'Disable'.
- Local Time Zone (+-GMT Time):** A dropdown menu currently set to '(GMT) Greenwich Mean Time'.
- SNTP Server IP Address:** A list of four IP addresses: 192.43.244.18, 128.138.140.44, 129.6.15.29, and 131.107.1.10.
- Daylight Saving:** A checkbox for 'Automatic' which is checked.
- Resync Period:** A text input field containing '1440' followed by the unit 'minutes'.

Below the parameters is a world map showing the continents in green against a blue background. At the bottom of the configuration area are two buttons: 'Apply' and 'Cancel'.

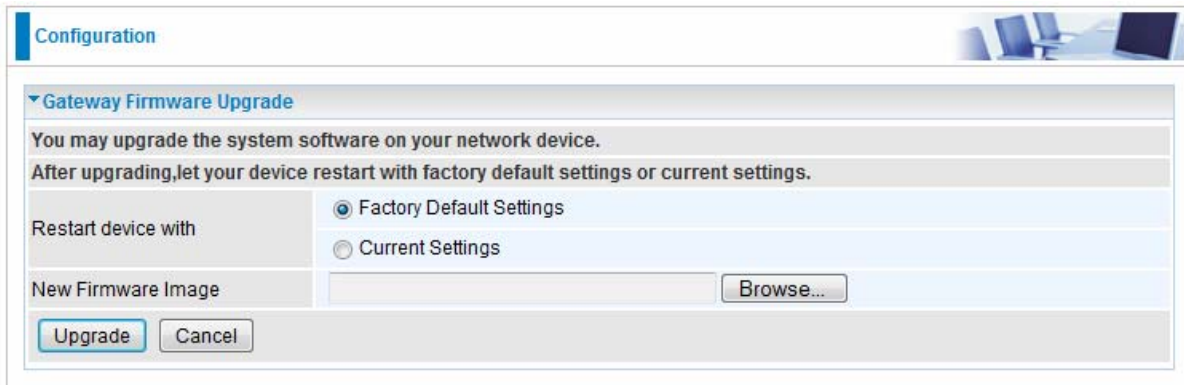
The router does not have a real time clock on board; instead, it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server outside your network. Choose your local time zone, click **Enable** and click the **Apply** button. After a successful connection to the Internet, the router retrieves the correct local time from the SNTP server you have specified. If you prefer to specify an SNTP server other than those in the drop-down list, simply enter its IP address as shown above. Your ISP may provide an SNTP server for you to use.

Resync Period (in minutes) is the periodic interval the router waits before it resynchronizes the router's time with that of the specified SNTP server. To avoid unnecessarily increasing the load on your specified SNTP server you should keep the poll interval as high as possible – at the absolute minimum every few hours or even days.

Gateway FW Upgrade

Your router's "firmware" is the software that allows it to operate and provides all its functionality. Think of your router as a dedicated computer, and the firmware as the software it runs. Over time this software may be improved and modified. Your router allows you to upgrade the software it runs to take advantage of these changes.

Clicking on **Browse** allows you to select the new firmware image file you have downloaded to your PC. Once the correct file is selected, click Upgrade to update the firmware in your router.



Configuration

Gateway Firmware Upgrade

You may upgrade the system software on your network device.
After upgrading, let your device restart with factory default settings or current settings.

Restart device with

Factory Default Settings
 Current Settings

New Firmware Image

Restart Device with: To choose "Factory Default Settings" or "Current Settings" which uses your current setting on the new firmware (it is highly advised to use Factory Default Settings over Current Settings for a clean firmware upgrade).

New Firmware Image: Type in the location of the file you wish to upload in this field or click **Browse...** to locate it.

Browse...: Click **Browse...** to find the file with the **.afw** file extension that you wish to upload. Remember that you must decompress compressed (.zip) files before you can upgrade from the file.

Upgrade: Click **upgrade** to begin the upload process. This process may take up to three minutes.

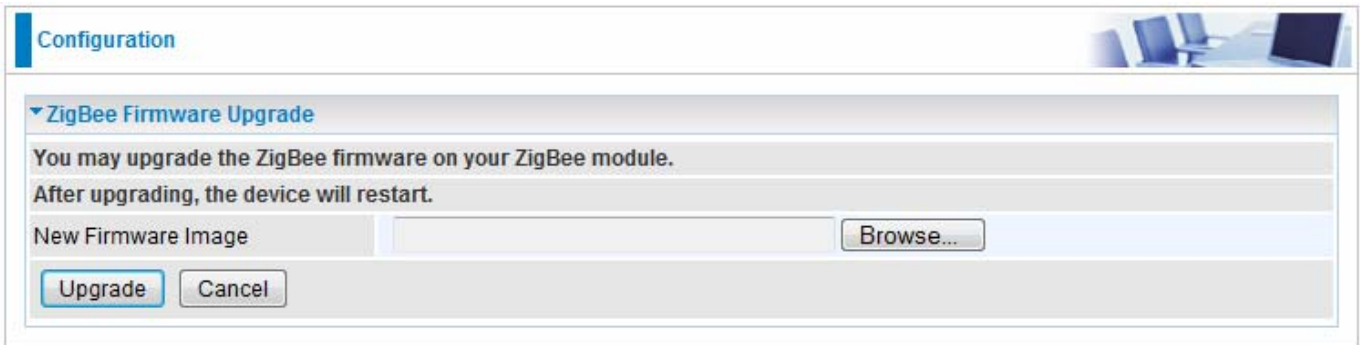


Warning

Do not power down the router or interrupt the firmware upgrade while it is still in process. Improper operation may damage the router. Please see section 2.4 for emergency recovery procedures.

ZigBee FW Upgrade

“ZigBee firmware” is the software that allows it to operate and provides all its functionality. Over time this software may be improved and modified. Your ZigBee model allows you to upgrade the software it runs to take advantage of these changes.

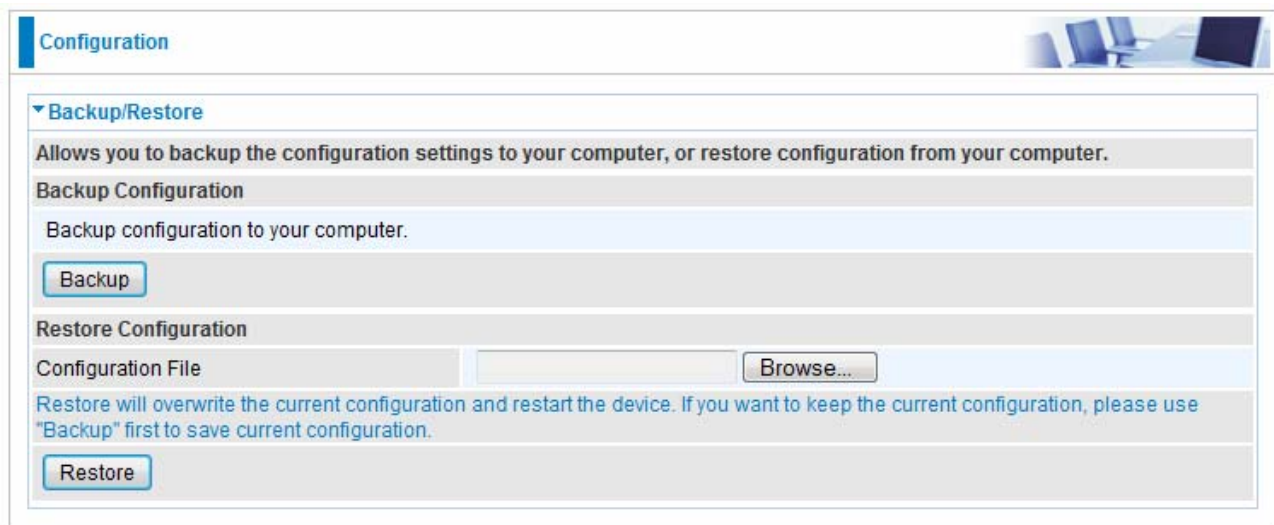


The screenshot shows a web interface for configuring a ZigBee device. At the top, there is a 'Configuration' tab. Below it, a section titled 'ZigBee Firmware Upgrade' contains the following text: 'You may upgrade the ZigBee firmware on your ZigBee module. After upgrading, the device will restart.' Below this text is a text input field labeled 'New Firmware Image' with a 'Browse...' button to its right. At the bottom of the section are two buttons: 'Upgrade' and 'Cancel'.

Clicking on **Browse** allows you to select the new firmware image file (.edl) you have downloaded to your PC.

Once the correct file is selected, click Upgrade to update the firmware in your router.

Backup / Restore



The screenshot shows a web interface for router configuration. At the top, there is a 'Configuration' tab. Below it, a section titled 'Backup/Restore' contains the following elements:

- A header: 'Backup/Restore' with a dropdown arrow.
- A description: 'Allows you to backup the configuration settings to your computer, or restore configuration from your computer.'
- A sub-section 'Backup Configuration' with the text 'Backup configuration to your computer.' and a 'Backup' button.
- A sub-section 'Restore Configuration' with a 'Configuration File' input field, a 'Browse...' button, and a 'Restore' button.
- A warning note: 'Restore will overwrite the current configuration and restart the device. If you want to keep the current configuration, please use "Backup" first to save current configuration.'

These functions allow you to save and backup your router's current settings to a file on your PC, or to restore a previously saved backup. This is useful if you wish to experiment with different settings, knowing that you have a backup handy in the case of any mistakes. It is advisable to backup your router's settings before making any significant changes to your router's configuration.

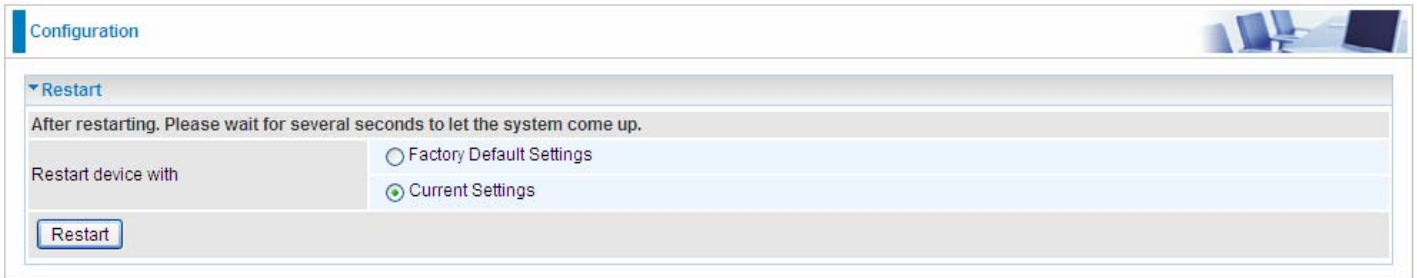
Press **Backup** to select where on your local PC to save the settings file. You may also change the name of the file when saving if you wish to keep multiple backups.

Press **Browse...** to select a file from your PC to restore. You should only restore settings files that have been generated by the Backup function, and that were created when using the **current version** of the router's firmware. **Settings files saved to your PC should not be manually edited in any way.**

Select the settings files you wish to use, and press **Restore** to load those settings into the router.

Restart Router

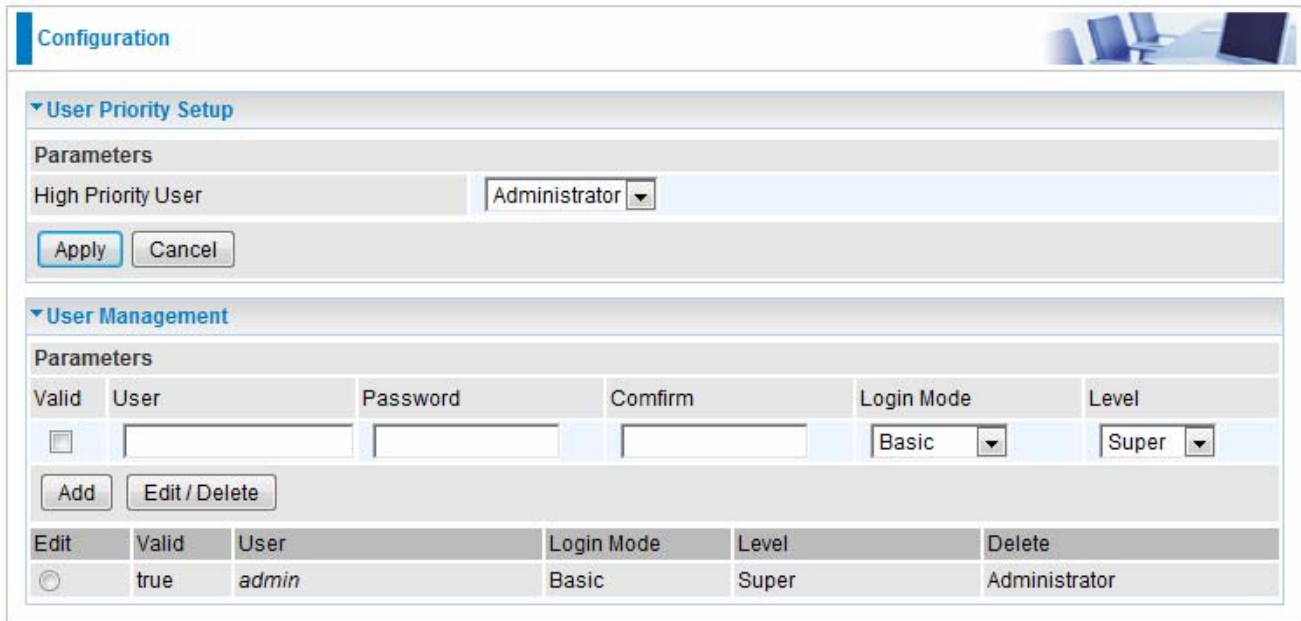
Click **Restart** with option **Current Settings** to reboot your router and save the current configuration to device.



The screenshot shows a web interface for router configuration. At the top left, there is a blue header with the word "Configuration". To the right of the header is a small image of a desk with a laptop and a chair. Below the header, there is a section titled "Restart" with a downward-pointing arrow. Underneath this section, there is a grey bar with the text "After restarting. Please wait for several seconds to let the system come up." Below this bar, there is a label "Restart device with" followed by two radio button options: "Factory Default Settings" and "Current Settings". The "Current Settings" option is selected, indicated by a green dot. At the bottom left of the section, there is a blue button labeled "Restart".

If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select **Factory Default Settings** to reset to factory default settings.

User Management



The screenshot shows a web-based configuration interface for a router. It is divided into two main sections: "User Priority Setup" and "User Management".

User Priority Setup

Parameters

High Priority User: Administrator

Buttons: Apply, Cancel

User Management

Parameters

| Valid | User | Password | Confirm | Login Mode | Level |
|--------------------------|------|----------|---------|------------|-------|
| <input type="checkbox"/> | | | | Basic | Super |

Buttons: Add, Edit / Delete

| Edit | Valid | User | Login Mode | Level | Delete |
|-----------------------|-------|-------|------------|-------|---------------|
| <input type="radio"/> | true | admin | Basic | Super | Administrator |

In order to prevent unauthorized access to your router's configuration interface, it requires all users to login with a password. You can set up multiple user accounts, each with their own password.

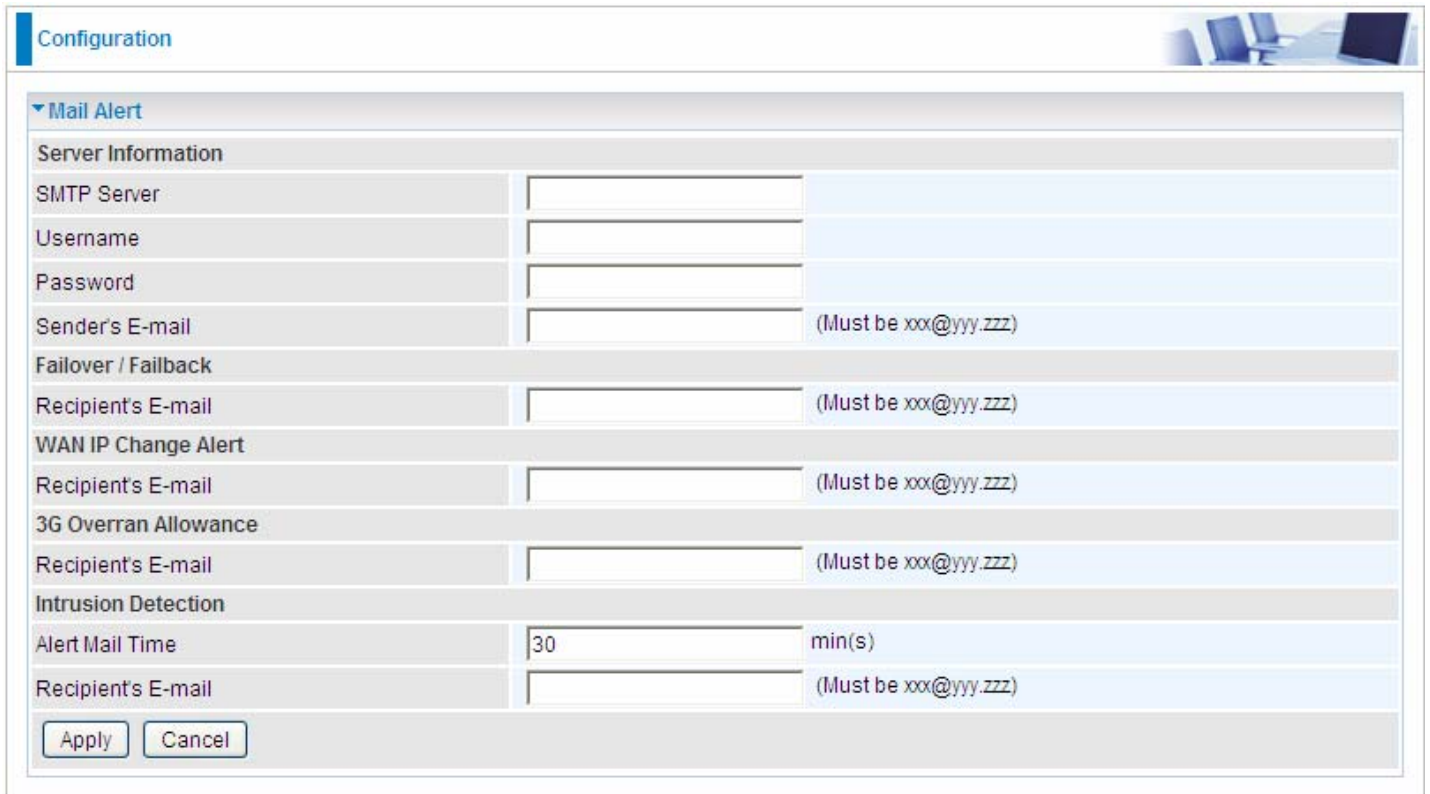
You are able to **Edit** existing users and **Add** new users who are able to access the device's configuration interface. Once you have clicked Edit on the account you want to edit, the information of the account will be displayed above. Just go ahead and change the password.

You can change the user's password, whether their account is active and **Valid**. These options are the same when creating a user account, with the exception that once created you cannot change the username. You cannot delete the default admin account; however you can delete any other created accounts by clicking ticking the box under Delete and then press the **Edit/Delete** button.

You are strongly advised to change the password on the default "**admin**" account when you receive your router, and any time you reset your configuration to Factory Defaults.

Mail Alert

Mail alert is designed to keep system administrator or other relevant personnel alerted of any unexpected events that might have occurred to the network computers or server for monitoring efficiency. With this alert system, appropriate solutions may be tackled to fix problems that may have arisen so that the server can be properly maintained.



Configuration

Mail Alert

Server Information

SMTP Server

Username

Password

Sender's E-mail (Must be xxx@yyy.zzz)

Failover / Failback

Recipient's E-mail (Must be xxx@yyy.zzz)

WAN IP Change Alert

Recipient's E-mail (Must be xxx@yyy.zzz)

3G Overran Allowance

Recipient's E-mail (Must be xxx@yyy.zzz)

Intrusion Detection

Alert Mail Time min(s)

Recipient's E-mail (Must be xxx@yyy.zzz)

Apply Cancel

SMTP Server: Enter the SMTP server that you would like to use for sending emails.

Username: Enter the username of your email account to be used by the SMTP server.

Password: Enter the password of your email account.

Sender's Email: Enter your email address.

Recipient's Email (Failover / Failback): Enter the email address that will receive the alert message once a computer / network server failover occurs.

Recipient's Email (WAN IP Change Alert): Enter the email address that will receive the alert message once a WAN IP change has been detected.

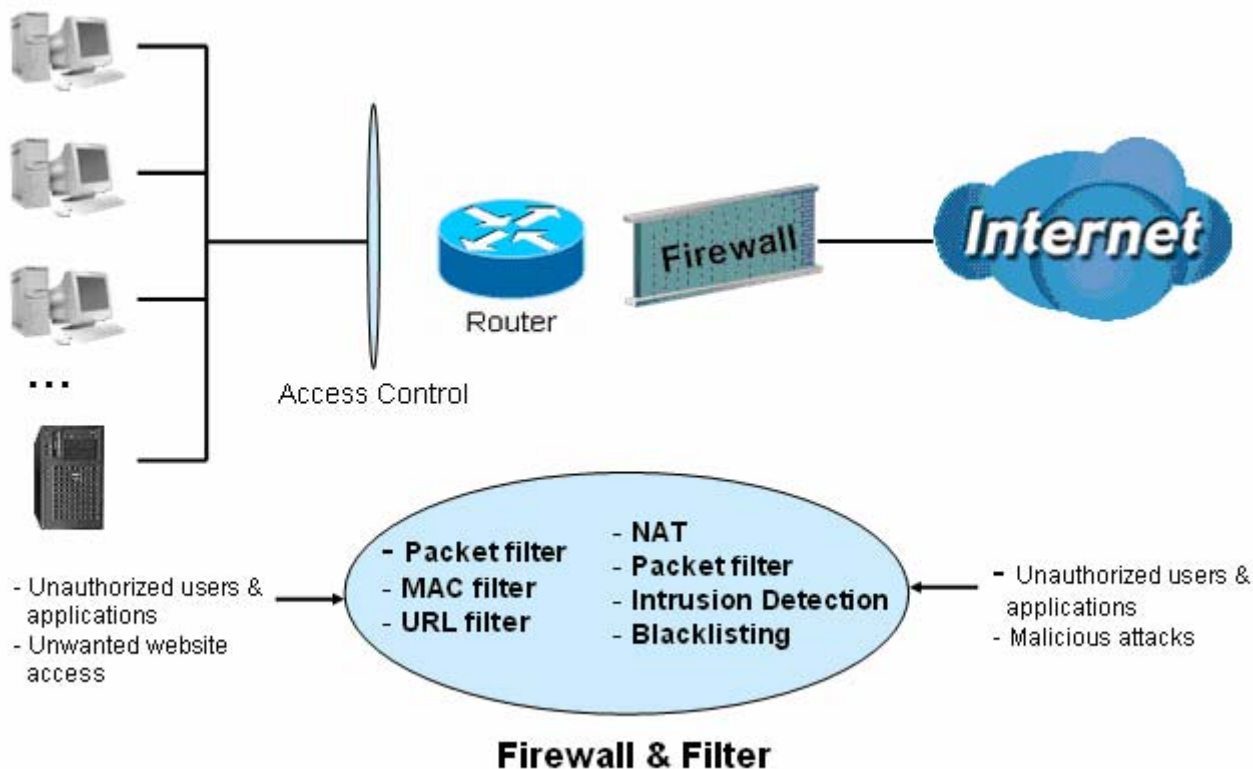
Recipient's Email (3G Overran Allowance): Enter the email address that will receive the alert message once 3G overran allowance was detected.

Alert Mail Time (Intrusion Detection): The time interval of sending Email.

Recipient's Email (Intrusion Detection): Enter the email address that will receive the alert message once intrusion has been detected.

Firewall and Access Control

Your router includes a full SPI (Stateful Packet Inspection) firewall for controlling Internet access from your LAN, as well as helping to prevent attacks from hackers. In addition to this, when using NAT (Network Address Translation) the router acts as a “natural” Internet firewall, since all PCs on your LAN use private IP addresses that cannot be directly accessed from the Internet. See the **WAN** configuration section for more details on NAT.



Firewall: Prevents access from outside your network.

NAT natural firewall: This masks LAN users' IP addresses, which are invisible to outside users on the Internet, making it much more difficult for a hacker to target a machine on your network. This natural firewall is on when the NAT function is enabled.

NOTE:

When using Virtual Servers (port mapping) your PCs are exposed to the ports specified opened in your firewall packet filter settings.

Firewall Security and Policy (General Settings): Inbound direction of Packet Filter rules prevent unauthorized computers or applications accessing your local network from the Internet.

Intrusion Detection: Enable Intrusion Detection to detect, prevent, and log malicious attacks.

MAC Filter rules: Prevents unauthorized computers accessing the Internet.

URL Filter: Blocks PCs on your local network from unwanted websites.

A detailed explanation of each of the following five items appears in the **Firewall** section below: **Packet Filter, MAC Filter, Intrusion detection, Block WAN PING** and **URL Filter**.

Packet Filter

Packet filtering enables you to configure your router to block specified internal/external users (**IP address**) from Internet access, or you can disable specific service requests (**Port number**) to /from Internet. This configuration program allows you to set up to 6 different filter rules for different users based on their IP addresses or their network Port number. The relationship among all filters is “**or**” operation, which means that the router checks these different filter rules one by one, starting from the first rule. As long as one of the rules is satisfied, the specified action will be taken.

| Edit | Order | Rule Name | Internal IP Address External IP Address | Protocol | Internal Port External Port | Direction | Action | Time Schedule | Delete |
|------|-------|-----------|--|----------|--------------------------------|-----------|---------|---------------|--------|
| | | Default | Any Any | Any | Any Any | outgoing | forward | Always On | |

Rule Name: Users-define description to identify this entry. The maximum name length is 32 characters, and then can choose application that they want from list box.

Internal IP Address / External IP Address: This is the Address-Filter used to allow or block traffic to/from particular IP address (es). Input the range you want to filter out. If you leave empty or 0.0.0.0, it means any IP address.

Protocol: Specify the packet type (TCP, UDP, ICMP, etc.) that the rule applies to.

Select **TCP** if you wish to search for the connection-based application service on the remote server using the port number. Or select **UDP** if you want to search for the connectionless application service on the remote server using the port number.

Action: If a packet matches this filter rule, **Forward (allows the packets to pass)** or **Drop (disallow the packets to pass)** this packet.

Internal Port: This Port or Port Range defines the ports allowed to be used by the Remote/WAN to connect to the application. Default is set from range **0 ~ 65535**. It is recommended that this option be configured by an advanced user.

External Port: This is the Port or Port Range that defines the application.

Direction: Determine whether the rule is for outgoing packets or for incoming packets.

Time Schedule: It is self-defined time period. You may specify a time schedule for your prioritization policy. For setup and detail, refer to **Time Schedule** section.

Log: Choose “log” if you wish to generate logs when the filter rule is applied to a packet.

Add: Click this button to add a new packet filter rule and the added rule will appear at the bottom table.

Edit: Check the Rule No. you wish to edit, and then click “Edit”.

Delete: Check the Rule No. you wish to delete, and then click “Delete”.

| Edit | Rule Name | Internal IP Address | Protocol | Internal Port | Direction | Action | Time Schedule | Delete |
|-----------------------|-----------|------------------------------------|----------|---------------|-----------|---------|---------------|--------------------------|
| | | External IP Address | | External Port | | | | |
| <input type="radio"/> | FTP | 0.0.0.0~0.0.0.0 0.0.0.0~0.0.0.0 | TCP | 0~0 21~21 | outgoing | forward | Always On | <input type="checkbox"/> |
| <input type="radio"/> | HTTP | 0.0.0.0~0.0.0.0 0.0.0.0~0.0.0.0 | TCP | 0~0 80~80 | outgoing | forward | Always On | <input type="checkbox"/> |



Attention

If the DHCP server option is enabled, you must be very careful in assigning IP addresses of a filtered private IP range to avoid conflicts because you do not know which PC in the LAN is assigned which IP address. The easiest and safest way is that the filtered IP address is assigned to a specific PC that is not allowed to access an outside resource such as the Internet. You configure the filtered IP address manually for this PC, but it stays in the same subnet with the router.

MAC Filter

A MAC (Media Access Control) address is the unique network hardware identifier for each PC on your network's interface (i.e. its Network Interface Card or Ethernet card). Using your router's MAC Address Filter function, you can configure to block specific machines from accessing your LAN.

There are no pre-defined MAC address filter rules; you can add the filter rules to meet your requirements.



The screenshot shows a web-based configuration page for a MAC Filter. At the top left, there is a 'Configuration' tab. The main section is titled 'MAC Filter'. Under 'Filter Action', there are three radio buttons: 'Disable', 'Allow', and 'Block', with 'Block' selected. An 'Apply' button is located below the radio buttons. The 'Parameters' section contains a 'MAC Address' field with a dropdown menu showing '<< --select--' and a note '(type or select from listbox)'. Below that is a 'Time Schedule' dropdown menu set to 'Always On'. At the bottom of the parameters section, there are 'Add' and 'Edit/Delete' buttons.

Action: select to determine how to do with the filter.

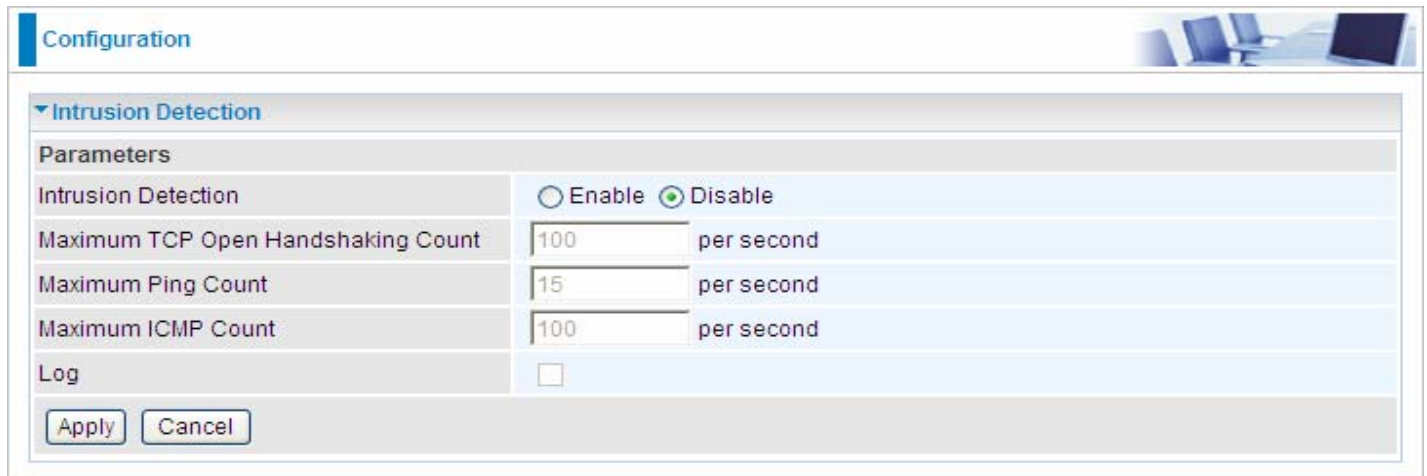
- **Disable:** to disable the MAC filter function.
- **Allow:** to enable the MAC filter function and allow the host of the following set MAC addresses to access.
- **Block:** to enable the MAC filter function and block the host of the following set MAC addresses to access.

MAC Address: Enter the MAC addresses you wish to manage.

Time Schedule: It is self-defined time period. You may specify a time schedule for your prioritization policy. For setup and detail, refer to **Time Schedule** section.

Intrusion Detection

Check Enable if you wish to detect intruders accessing your computer without permission. The router automatically detects and blocks a DoS (Denial of Service) attack if a user enables this function. This kind of attack is not to access confidential data on the network; instead, it aims to disrupt specific equipment or the entire network. If this happens, users will have trouble accessing the network resources.



| Parameters | |
|------------------------------------|---|
| Intrusion Detection | <input type="radio"/> Enable <input checked="" type="radio"/> Disable |
| Maximum TCP Open Handshaking Count | <input type="text" value="100"/> per second |
| Maximum Ping Count | <input type="text" value="15"/> per second |
| Maximum ICMP Count | <input type="text" value="100"/> per second |
| Log | <input type="checkbox"/> |

Intrusion Detection: Check Enable if you wish to detect intruders accessing your computer without permission.

Maximum TCP Open Handshaking Count: This is a threshold value to decide whether a SYN Flood attempt is occurring or not. Default value is 100 TCP SYN per seconds.

Maximum Ping Count: This is a threshold value to decide whether an ICMP Echo Storm is occurring or not. Default value is 15 ICMP Echo Requests (PING) per second.

Maximum ICMP Count: This is a threshold to decide whether an ICMP flood is occurring or not. Default value is 100 ICMP packets per seconds except ICMP Echo Requests (PING).

Log: Check Log if you wish to generate logs when the filter rule is applied to the Intrusion Detection.

For SYN Flood, ICMP Echo Storm and ICMP flood, IDS will just warn the user in the Event Log but it will not be able to protect against such attacks.
Hacker attack types recognized by the IDS

| Intrusion Name | Detect Parameter | Blacklist | Type of Block Duration | Drop Packet | Show Log |
|-----------------------------|--|-----------|------------------------|-------------|----------|
| Ascend Kill | Ascend Kill data | Src IP | DoS | Yes | Yes |
| WinNuke | TCP Port 135, 137~139, Flag: URG | Src IP | DoS | Yes | Yes |
| Smurf | ICMP type 8 Des IP is broadcast | Dst IP | Victim Protection | Yes | Yes |
| Land attack | SrcIP = DstIP | | | Yes | Yes |
| Echo/CharGen Scan | UDP Echo Port and CharGen Port | | | Yes | Yes |
| Echo Scan | UDP Dst Port = Echo(7) | Src IP | Scan | Yes | Yes |
| CharGen Scan | UDP Dst Port = CharGen(19) | Src IP | Scan | Yes | Yes |
| X'mas Tree Scan | TCP Flag: X'mas | Src IP | Scan | Yes | Yes |
| IMAP SYN/FIN Scan | TCP Flag: SYN/FIN DstPort: IMAP(143) SrcPort: 0 or 65535 | Src IP | Scan | Yes | Yes |
| SYN/FIN/RST/ACK Scan | TCP, No Existing session And Scan Hosts more than five. | Src IP | Scan | Yes | Yes |
| Net Bus Scan | TCP No Existing session DstPort = Net Bus 12345,12346, 3456 | SrcIP | Scan | Yes | Yes |
| Back Orifice Scan | UDP, DstPort = Orifice Port (31337) | SrcIP | Scan | Yes | Yes |
| SYN Flood | Max TCP Open Handshaking Count (Default 100 c/sec) | | | | Yes |
| ICMP Flood | Max ICMP Count (Default 100 c/sec) | | | | Yes |
| ICMP Echo | Max PING Count (Default 15 c/sec) | | | | Yes |

Src IP: Source IP **Src Port:** Source Port
Dst Port: Destination Port **Dst IP:** Destination IP

Block WAN PING

Check Enable if you wish to exclude outside PING requests from reaching this router.



Configuration

Block WAN PING

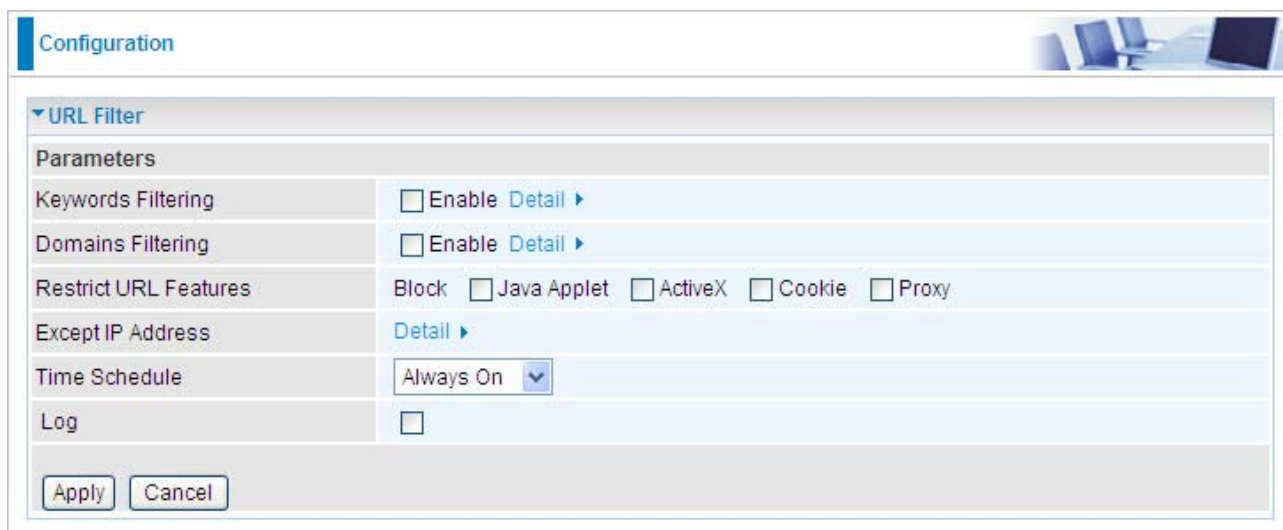
Parameters

Block WAN PING Enable Disable

Apply Cancel

URL Filter

URL (Uniform Resource Locator – e.g. an address in the form of <http://www.example.com>) filter rules allow you to prevent users on your network from accessing particular websites from their URL. There are no pre-defined URL filter rules; you can add filter rules to meet your requirements.



Configuration

URL Filter

Parameters

Keywords Filtering Enable [Detail](#) ▶

Domains Filtering Enable [Detail](#) ▶

Restrict URL Features Block Java Applet ActiveX Cookie Proxy

Except IP Address [Detail](#) ▶

Time Schedule Always On ▼

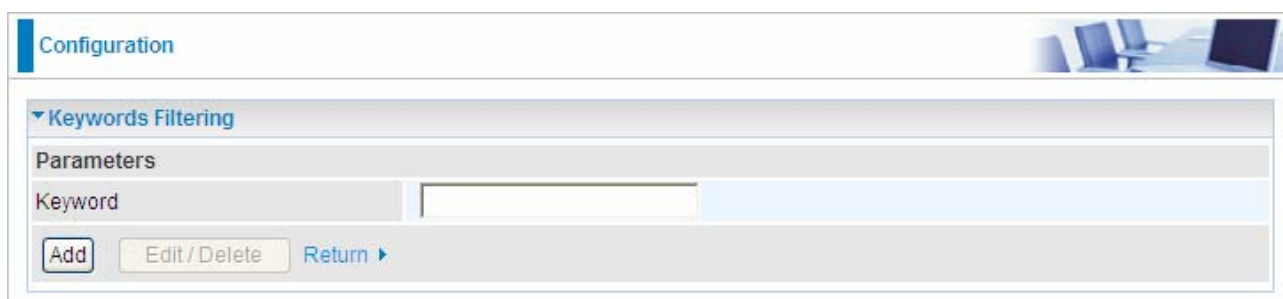
Log

Apply Cancel

Keywords Filtering

Allows blocking by specific keywords within a particular URL rather than having to specify a complete URL (e.g. to block any image called “advertisement.gif”). When enabled, your specified keywords list is checked to see if any keywords are present in URLs accessed to determine if the connection attempt should be blocked. Note that the URL filter blocks web browser (HTTP) connection attempts using port 80 only.

For example, the URL <http://www.abc.com/abcde.html> would be dropped since the keyword “abcde” occurs in the URL.



Configuration

Keywords Filtering

Parameters

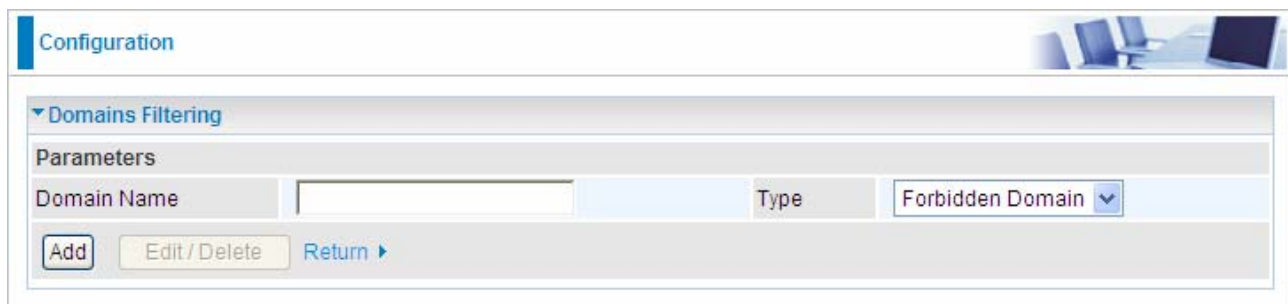
Keyword

Add Edit/Delete Return ▶

Domains Filtering

Checks the domain name in URLs accessed against your list of domains to block or allow. If it matches, the URL request is sent (Trusted) or dropped (Forbidden). The checking procedure is:

1. Check the domain in the URL to determine if it is in the trusted list. If yes, the connection attempt is sent to the remote web server.
2. If not, it is checked with the forbidden list. If present, the connection attempt is dropped.
3. If the packet matches neither of the above, it is sent to the remote web server.
4. Please be note that the completed URL, “www” + domain name shall be specified. For example to block traffic to www.google.com.au, enter “www.google” or “www.google.com”



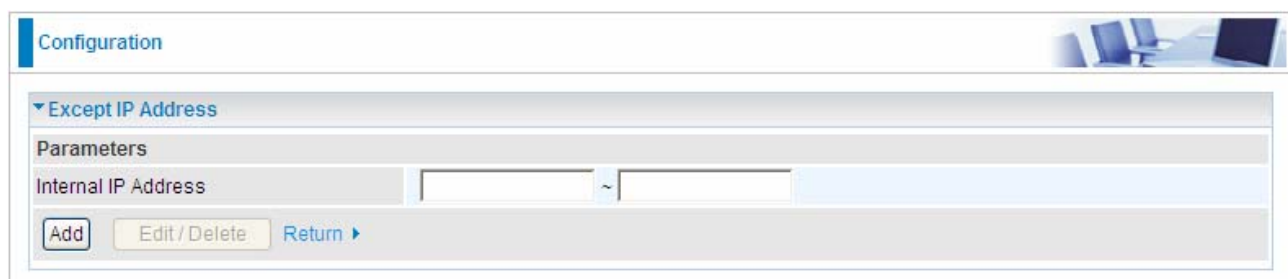
The screenshot shows a configuration window titled "Configuration" with a sub-section "Domains Filtering". Under "Parameters", there is a "Domain Name" input field, a "Type" dropdown menu set to "Forbidden Domain", and three buttons: "Add", "Edit/Delete", and "Return".

Restrict URL Features

This function enhances the restriction to your URL rules.

- ⊙ **Block Java Applet:** Blocks Web content which includes the Java Applet to prevent someone who wants to damage your system via the standard HTTP protocol.
- ⊙ **Block ActiveX:** Blocks ActiveX
- ⊙ **Block Cookies:** Blocks Cookies
- ⊙ **Block Proxy:** Blocks Proxy

Except IP Address



The screenshot shows a configuration window titled "Configuration" with a sub-section "Except IP Address". Under "Parameters", there is an "Internal IP Address" input field with a tilde (~) separator between two boxes, and three buttons: "Add", "Edit/Delete", and "Return".

Time Schedule: It is self-defined time period. You may specify a time schedule for your prioritization policy. For setup and detail, refer to Time Schedule section.

Log: Click “Log” if you wish to generate logs when the filter rule is applied to the URL Filter.

QoS (Quality of Service)

Quality of Service Introduction

If you've ever found your 'net' speed has slowed to a crawl because another family member is using a P2P file sharing program, you'll understand why the Quality of Service features in the routers is such a breakthrough for home users and office users.

QoS: Keeping Your Net Connection Fast and Responsive

Configurable by internal IP address, external IP address, protocol, and port, the Quality of Service (QoS) gives you full control over which types of outgoing data traffic should be given priority by the router, ensuring bandwidth-consumption data like gaming packets, latency-sensitive application like voice, or even mission critical files, move through the router at lightning speed, even under heavy load. You can throttle the speed at which different types of outgoing data pass through the router. In addition, you can simply change the priority of different types of upload data and let the router sort out the actual speeds.

QoS Setup

Please choose the **QoS** in the **Configuration** item of the left window as depicted below.

Configuration

QoS

Non-Assigned Bandwidth Ratio => Upstream (LAN to WAN) : 100% Downstream (WAN to LAN) : 100%

Parameters

| | | | |
|---------------------|---|---------------|---|
| Application | <input type="text"/> | Direction | LAN to WAN |
| Protocol | Any | DSCP Marking | Disable |
| Rate Type | Guaranteed (Minimum) | Ratio | <input type="text"/> % |
| | | Priority | Normal |
| Internal IP Address | <input type="text"/> ~ <input type="text"/> | Internal Port | <input type="text"/> ~ <input type="text"/> |
| External IP Address | <input type="text"/> ~ <input type="text"/> | External Port | <input type="text"/> ~ <input type="text"/> |
| Time Schedule | Always On | | |

Add Edit/Delete

After clicking the QoS item, you can Add/Edit/Delete a QoS policy. This page will show the brief information for policies you have added or edited. This page will also display the total available (Non-assigned) bandwidth, in percentage, can be assigned.

Application: A name that identifies an existing policy.

Direction: The traffic flow direction to be controlled by the QoS policy.

There are two settings to be provided in the Router:

© **LAN to WAN:** You want to control the traffic flow from the local network to the outside world. e.g., you have a FTP server inside the local network and you want to have a limited traffic rate controlled by the QoS policy. So, you need to add a policy with LAN to WAN direction setting.

© **WAN to LAN:** Control Traffic flow from the WAN to LAN. The connection maybe either issued from

LAN to WAN or WAN to LAN.)

Protocol: The Protocol will be controlled. For GRE protocol, there is no need to specify the IP addresses or Application ports in this page. For other protocols, at least one value shall be given.

Ⓒ **ANY:** No protocol type is specified.

Ⓒ **TCP**

Ⓒ **UDP**

Ⓒ **ICMP**

Ⓒ **GRE**

DSCP Marking: Differentiated Services Code Point (DSCP), it is the first 6 bits in the ToS byte. DSCP Marking allows users to classify traffic based on DSCP value and send packets to next Router.

Note: To be sure the router(s) in the backbones network have the capability in executing and checking the DSCP through-out the QoS network.

The DSCP Mapping Table

| DSCP Mapping Table | |
|---------------------------|-----------------------------|
| 3G Router | Standard DSCP |
| Disabled | None |
| Best Effort | Best Effort (000000) |
| Premium | Express Forwarding (101110) |
| Gold service (L) | Class 1, Gold (001010) |
| Gold service (M) | Class 1, Silver (001100) |
| Gold service (H) | Class 1, Bronze (001110) |
| Silver service (L) | Class 2, Gold (010010) |
| Silver service (M) | Class 2, Silver (010100) |
| Silver service (H) | Class 2, Bronze (010110) |
| Bronze service (L) | Class 3, Gold (011010) |
| Bronze service (M) | Class 3, Silver (011100) |
| Bronze service (H) | Class 3, Bronze (011110) |

Rate Type: 2 types are provided:

⊙ **Limited (Maximum):** Specify a limited data rate for this policy. It also is the maximal rate for this policy. As above FTP server example, you may want to “throttle” the outgoing FTP speed to 20% of 256K and limit to it, you may use this type.

⊙ **Guaranteed (Minimum):** Specify a minimal data rate for this policy. For example, you want to provide a guaranteed data rate for your outside customers to access your internal FTP server with, say at least, 20% of your total bandwidth. You can use this type. Then, if there is available bandwidth that is not used, it will be given to this policy by following priority assignment.

Ratio: Assign the data ratio for this policy to be controlled. For examples, we want to only allow 20% of the total data transfer rate for the LAN-to-WAN direction to be used for FTP server. Then we can specify here with data ratio = 20.

Priority: Specify the priority for the bandwidth that is not used. For examples, you may specify two different QoS policies for different applications. Both applications need a minimal bandwidth and need more bandwidth, beside the assigned one, if there is any available/non-used one available. So, you may specify which application can have higher priority to acquire the non-used bandwidth.

⊙ **High**

⊙ **Normal:** The default is normal priority.

⊙ **Low**

For the sample priority assignment for different policies, it is served in a First-In-First-Out way.

Internal IP Address: The IP address values for Local LAN machines you want to control. (For IP packets from LAN to WAN, it is the source IP address. For IP packages from WAN to LAN, it is the destination IP address.)

Internal Port: The Application port values for local LAN machines you want to control. (For TCP/UDP packets from LAN to WAN, it is the source port value. For TCP/UDP packets from WAN to LAN, it is the destination port value.)

External IP Address: The IP address values for Remote WAN machines you want to control. (For IP packets from LAN to WAN, it is the destination IP address. For IP packages from WAN to LAN, it is the source IP address.)

External Ports: The Application port values for remote machines you want to control. (For TCP/UDP packets from LAN to WAN, it is the destination port value. For TCP/UDP packets from WAN to LAN, it is the source port value.)

Time Schedule: Scheduling your prioritization policy.

Virtual Server

In TCP and UDP networks a port is a 16-bit number used to identify which application program (usually a server) incoming connections should be delivered to. Some ports have numbers that are pre-assigned to them by the IANA (the Internet Assigned Numbers Authority), and these are referred to as “well-known ports”. Servers follow the well-known port assignments so clients can locate them.

If you wish to run a server on your network that can be accessed from the WAN (i.e. from other machines on the Internet that are outside your local network), or any application that can accept incoming connections (e.g. Peer-to-peer/P2P software such as instant messaging applications and P2P file-sharing applications) and are using NAT (Network Address Translation), then you need to configure your router to forward these incoming connection attempts using specific ports to the PC on your network running the application. You also need to use port forwarding if you wish to host an online game server.

The reason is that when using NAT, your publicly accessible IP address is used by and points to your router, which needs to deliver all traffic to the private IP addresses used by your PCs. Please see the **WAN** configuration section of this manual for information on NAT.

The Internet Assigned Numbers Authority (IANA) is the central coordinator for the assignment of unique parameter values for Internet protocols. Port numbers range from 0 to 65535, but only port numbers 0 to 1023 are reserved for privileged services and are designated as “well-known ports”. The registered ports are numbered from 1024 through 49151. The remaining ports, referred to as dynamic ports, or private ports, are numbered from 49152 through 65535.

Examples of well-known and registered port numbers are shown below, for further information, please see IANA's website at: <http://www.iana.org/assignments/port-numbers>

Well-known and Registered Ports

| Port Number | Protocol | Description |
|-------------|-----------|---------------------------------------|
| 20 | TCP | FTP Data |
| 21 | TCP | FTP Control |
| 22 | TCP & UDP | SSH Remote Login Protocol |
| 23 | TCP | Telnet |
| 25 | TCP | SMTP (Simple Mail Transfer Protocol) |
| 53 | TCP & UDP | DNS (Domain Name Server) |
| 69 | UDP | TFTP (Trivial File Transfer Protocol) |
| 80 | TCP | World Wide Web HTTP |
| 110 | TCP | POP3 (Post Office Protocol Version 3) |
| 119 | TCP | NEWS (Network News Transfer Protocol) |
| 123 | UDP | NTP (Network Time Protocol) |
| 161 | TCP | SNMP |
| 443 | TCP & UDP | HTTPS |
| 1503 | TCP | T.120 |
| 1720 | TCP | H.323 |
| 4000 | TCP | ICQ |
| 7070 | UDP | RealAudio |

Port Mapping

Configuration

Port Mapping

Parameters

| | | | | |
|---------------------|----------------------|----------------------------------|----------------------------------|---|
| Application | <input type="text"/> | << --select-- | <input type="button" value="v"/> | (type or select from listbox) |
| Protocol | TCP | <input type="button" value="v"/> | External Port | <input type="text"/> ~ <input type="text"/> |
| Internal IP Address | <input type="text"/> | << --select-- | <input type="button" value="v"/> | (type or select from listbox) |
| Internal Port | <input type="text"/> | Time Schedule | Always On | <input type="button" value="v"/> |

Application: Select the service you wish to configure.

Protocol: Automatic when you choose Application from list-box or select a protocol type which you want.

External Port & Internal Port: Enter the public port number & range you wish to configure.

Internal IP Address: Enter the IP address of a specific internal server to which requests from the specified port is forwarded.

Add: Click to add a new virtual server rule. Click again and the next figure appears.

Edit: Check the Rule No. you wish to edit and then click “Edit/Delete”.

Delete: Check the Rule No. you wish to delete then click “Edit/Delete”.

Since NAT acts as a “natural” Internet firewall, your router protects your network from access by outside users, as all incoming connection attempts point to your router unless you specifically create Virtual Server entries to forward those ports to a PC on your network. When your router needs to allow outside users to access internal servers, e.g. a web server, FTP server, Email server or game server, the router can act as a “virtual server”. You can set up a local server with a specific port number for the service to use, e.g. web/HTTP (port 80), FTP (port 21), Telnet (port 23), SMTP (port 25), or POP3 (port 110). When an incoming access request to the router for a specified port is received, it is forwarded to the corresponding internal server.

For example, if you set the port number 80 (Web/HTTP) to be mapped to the IP Address 192.168.1.2, then all incoming HTTP requests from outside users are forwarded to the local server (PC) with the IP address of 192.168.1.2. If the port is not listed as a predefined application, you need to add it manually.

Configuration

▼ Port Mapping

Parameters

| | | | | |
|---------------------|--------------------------------------|---------------|---|-------------------------------|
| Application | <input type="text"/> | << --select-- | <input type="button" value="v"/> | (type or select from listbox) |
| Protocol | <input type="button" value="v"/> TCP | External Port | <input type="text"/> ~ <input type="text"/> | |
| Internal IP Address | <input type="text"/> | << --select-- | <input type="button" value="v"/> | (type or select from listbox) |
| Internal Port | <input type="text"/> | Time Schedule | <input type="button" value="v"/> Always On | |

| Edit | Application | Protocol | External Port | Internal IP Address | Internal Port | Time Schedule | Delete |
|-----------------------|-------------|----------|---------------|---------------------|---------------|---------------|--------------------------|
| <input type="radio"/> | FTP | TCP | 21~21 | 192.168.1.25 | Any | Always On | <input type="checkbox"/> |
| <input type="radio"/> | HTTP | TCP | 80~80 | 192.168.1.2 | Any | Always On | <input type="checkbox"/> |

In addition to specifying the port number used, you also need to specify the protocol used. The protocol is determined by the particular application. Most applications use TCP or UDP, however you can specify other protocols using the drop-down **Protocol** menu. Setting the protocol to “all” causes all incoming connection attempts using all protocols on all port numbers to be forwarded to the specified IP address.

DMZ

The DMZ Host is a local computer exposed to the Internet. When setting a particular internal IP address as the DMZ Host, all incoming packets are checked by the Firewall and NAT algorithms, it is then passed to the DMZ host when a packet received does not use a port number in use by any other Virtual Server entries.

Configuration

DMZ

Parameters

Internal IP Address: << --select-- (type or select from listbox)

Time Schedule: Always On

Except Ports

Port: << --select--

Protocol: TCP

Description:

Except List

| ID | Description | Protocol | Port | Operation |
|----|-------------|----------|------|-----------|
|----|-------------|----------|------|-----------|

Internal IP Address: Enter the IP address of a specific internal server to which will be the DMZ Host.

Time Schedule: A self defined time period. You may specify a time schedule. For setup and detail, refer to Time Schedule section.

Port: The except port number. Default is set from range 1 ~ 65535. You can select from the drop down list and also can enter manually.

Protocol: Select the TCP or UDP protocol from the drop down list.

Description: The description of the port's function.

Add/Delete Except Ports

1. Enter except port number in the port field or choose from the drop down list. Select the port and describe the port.

Except Ports

Port: 80 << Remote Access (TCP 80)

Protocol: TCP

Description: Remote Access

2. Click **Add**. The new except port will display below.

| Except List | | | | |
|-------------|---------------|----------|------|------------------------|
| ID | Description | Protocol | Port | Operation |
| 1 | Remote Access | tcp | 80 | Delete |

3. Click **Delete** to delete the one which you want to remove from the except list.

| Except List | | | | |
|-------------|----------------|----------|------|------------------------|
| ID | Description | Protocol | Port | Operation |
| 1 | Remote Access | tcp | 80 | Delete |
| 2 | Printer Server | tcp | 631 | Delete |
| 3 | Web Cam | tcp | 8081 | Delete |



Using port mapping does have security implications, since outside users are able to connect to PCs on your network. For this reason you are advised to use specific Virtual Server entries just for the ports your application requires instead of simply using DMZ or creating a Virtual Server entry for "All" protocols, as doing so results in all connection attempts to your public IP address accessing the specified PC.



Attention

If you have disabled the NAT option in the WAN-ISP section, the Virtual Server will hence become invalid. If the DHCP option is enabled, you have to be very careful in assigning the IP addresses of the virtual servers in order to avoid conflicts. The easiest way of configuring Virtual Servers is to manually assign static IP address to each virtual server PC, with an address that does not fall into the range of IP addresses that are to be issued by the DHCP server. You can configure the virtual server IP address manually, but it must still be in the same subnet as the router.

Wake on LAN

Wake on LAN (WOL, sometimes WoL) is an Ethernet computer networking standard that allows a computer to be turned on or woken up remotely by a network message.

The screenshot shows a web-based configuration interface. At the top left is a 'Configuration' tab. Below it is a section titled 'Wake on LAN'. Under 'Parameters', there is a 'MAC Address' input field, a dropdown menu with '--select--' and a '(type or select from listbox)' hint, and two buttons: 'Add' and 'Edit / Delete'. Below this is a table with the following structure:

| Edit | Action | MAC Address | Ready | Delete |
|-----------------------|---------|-------------------|-------|--------------------------|
| <input type="radio"/> | Wake Up | 00:1A:A0:AD:1F:21 | Yes | <input type="checkbox"/> |

Select: Select MAC address of the computer that you want to wake up or turn on remotely.

Add: After selecting, click **Add** then you can perform the Wake-up action.

Edit/Delete: Click to edit or delete the selected MAC address.

Ready: “Yes“ indicating the remote computer is ready for your waking up.

“No“ indicating the machine is not ready for your waking up.

Delete: Delete the selected MAC address.

Time Schedule

The Time Schedule supports up to 16 time slots which helps you to manage your Internet connection. In each time profile, you may schedule specific day(s) i.e. Monday through Sunday to restrict or allowing the usage of the Internet by users or applications.

This Time Schedule correlates closely with router's time, since router does not have a real time clock on board; it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server from the Internet. Refer to **Time Zone** for details. You router time should correspond with your local time. If the time is not set correctly, your Time Schedule will not function properly.

Configuration

Time Schedule
▼

Parameters

Name

Day in a week Sun Mon Tue Wed Thu Fri Sat

Start Time :

End Time :

| Edit | Name | Day in a week | Start Time | End Time | Clear |
|-----------------------|------------|--|------------|----------|--------------------------|
| <input type="radio"/> | TimeSlot1 | <input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat | 08:00 | 18:00 | <input type="checkbox"/> |
| <input type="radio"/> | TimeSlot2 | <input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat | 08:00 | 18:00 | <input type="checkbox"/> |
| <input type="radio"/> | TimeSlot3 | <input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat | 08:00 | 18:00 | <input type="checkbox"/> |
| <input type="radio"/> | TimeSlot4 | <input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat | 08:00 | 18:00 | <input type="checkbox"/> |
| <input type="radio"/> | TimeSlot5 | <input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat | 08:00 | 18:00 | <input type="checkbox"/> |
| <input type="radio"/> | TimeSlot6 | <input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat | 08:00 | 18:00 | <input type="checkbox"/> |
| <input type="radio"/> | TimeSlot7 | <input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat | 08:00 | 18:00 | <input type="checkbox"/> |
| <input type="radio"/> | TimeSlot8 | <input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat | 08:00 | 18:00 | <input type="checkbox"/> |
| <input type="radio"/> | TimeSlot9 | <input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat | 08:00 | 18:00 | <input type="checkbox"/> |
| <input type="radio"/> | TimeSlot10 | <input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat | 08:00 | 18:00 | <input type="checkbox"/> |
| <input type="radio"/> | TimeSlot11 | <input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat | 08:00 | 18:00 | <input type="checkbox"/> |
| <input type="radio"/> | TimeSlot12 | <input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat | 08:00 | 18:00 | <input type="checkbox"/> |
| <input type="radio"/> | TimeSlot13 | <input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat | 08:00 | 18:00 | <input type="checkbox"/> |
| <input type="radio"/> | TimeSlot14 | <input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat | 08:00 | 18:00 | <input type="checkbox"/> |
| <input type="radio"/> | TimeSlot15 | <input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat | 08:00 | 18:00 | <input type="checkbox"/> |
| <input type="radio"/> | TimeSlot16 | <input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat | 08:00 | 18:00 | <input type="checkbox"/> |

Name: A user-define description to identify this time portfolio.

Day in a week: The default is set from Sunday through Saturday. You may specify the days for the schedule to be applied.

Start Time: The default is set at 8:00 AM. You may specify the start time of the schedule.

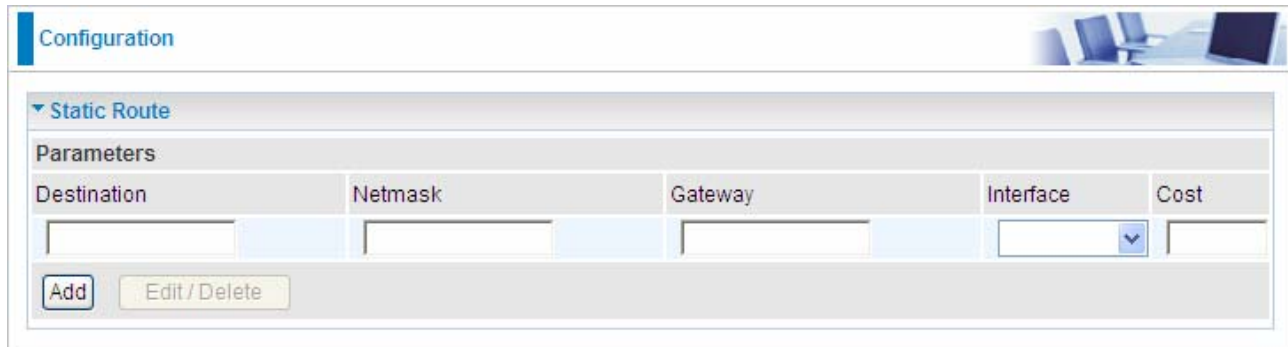
End Time: The default is set at 18:00 (6:00PM). You may specify the end time of the schedule. Select the Apply button to apply your changes.

Advanced

Configuration options within the **Advanced** section are for users who wish to take advantage of the more advanced features of the router. Users who do not understand the features should not attempt to reconfigure their router, unless advised to do so by support staff.

There are seven items within the **Advanced** section: **Static Route, Static ARP, Dynamic DNS, Device Management, IGMP, SNMP Access Control** and **Remote Access**.

Static Route



The screenshot shows a web-based configuration interface for a network device. At the top, there is a 'Configuration' tab. Below it, a section titled 'Static Route' is expanded. Underneath, there is a 'Parameters' section with five input fields: 'Destination', 'Netmask', 'Gateway', 'Interface', and 'Cost'. The 'Destination', 'Netmask', and 'Gateway' fields are empty text boxes. The 'Interface' field is a dropdown menu with a blue arrow pointing down. The 'Cost' field is an empty text box. Below the input fields, there are two buttons: 'Add' and 'Edit/Delete'.

Destination: The destination subnet IP address.

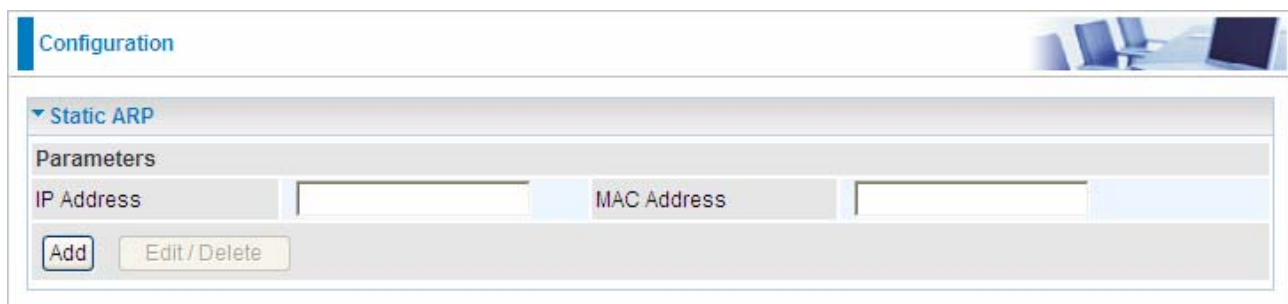
Netmask: Subnet mask of the destination IP addresses based on above destination.

Gateway: The gateway IP address to which packets are forwarded.

Interface: Select the interface through which packets are forwarded.

Cost: Represents the cost of transmission for routing purposes. The number need not be precise, but it must be between 0 and 65535.

Static ARP



The screenshot shows a web-based configuration interface for a network device. At the top, there is a 'Configuration' tab. Below it, a section titled 'Static ARP' is expanded. Underneath, there is a 'Parameters' section with two input fields: 'IP Address' and 'MAC Address'. Both fields are empty text boxes. Below the input fields, there are two buttons: 'Add' and 'Edit/Delete'.

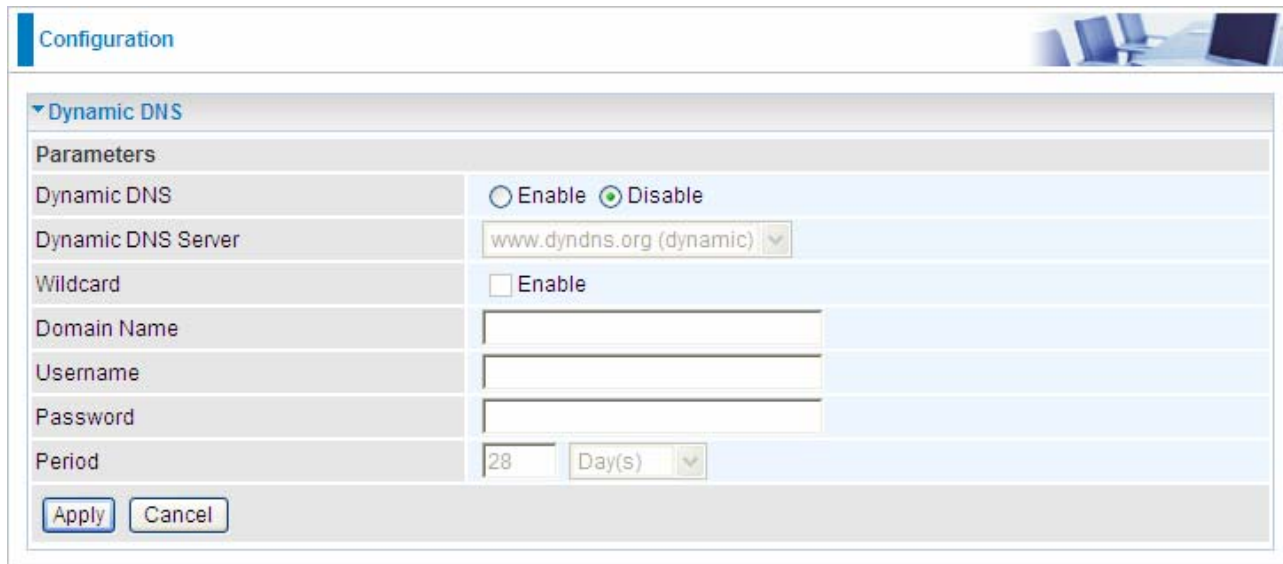
IP Address: Fill in the IP address of the host computer that is sending the data packet.

MAC Address: Fill in the MAC address of the computer that the incoming data packets are to be forwarded.

Dynamic DNS

The Dynamic DNS function lets you alias a dynamic IP address to a static hostname, so if your ISP does not assign you a static IP address you can still use a domain name. This is especially useful for hosting servers via your 3G connection, so that anyone wishing to connect to you may use your domain name, rather than having to use your dynamic IP address, which changes from time to time. This dynamic IP address is the WAN IP address of the router, which is assigned to you by your ISP.

You first need to register and establish an account with the Dynamic DNS provider using their website, for example <http://www.dyndns.org/>.



The screenshot shows a web-based configuration page for Dynamic DNS. At the top left, there is a 'Configuration' tab. Below it, a section titled 'Dynamic DNS' is expanded. Underneath, a 'Parameters' section contains the following fields:

| | |
|--------------------|---|
| Dynamic DNS | <input type="radio"/> Enable <input checked="" type="radio"/> Disable |
| Dynamic DNS Server | www.dyndns.org (dynamic) ▼ |
| Wildcard | <input type="checkbox"/> Enable |
| Domain Name | <input type="text"/> |
| Username | <input type="text"/> |
| Password | <input type="text"/> |
| Period | 28 Day(s) ▼ |

At the bottom of the configuration area, there are two buttons: 'Apply' and 'Cancel'.

Disable: Check to disable the Dynamic DNS function.

Enable: Check to enable the Dynamic DNS function. The fields following are activated and required.

Dynamic DNS Server: Select the DDNS service you have established an account with.

Wildcard: Select this check box to enable the DYNDNS Wildcard.

Domain Name, Username and Password: Enter your registered domain name and your username and password for this service.

Period: Set the time period between updates, for the Router to exchange information with the DDNS server. In addition to updating periodically as per your settings, the router will perform an update when your dynamic IP address changes.

Device Management

The Device Management advanced configuration settings allow you to control your router's security options and device monitoring features.



The screenshot shows the 'Configuration' page of a router, specifically the 'Device Management' section. The page has a blue header with the word 'Configuration' and a small image of a desk with a laptop and monitor. Below the header, there is a 'Device Management' section with a dropdown arrow. The settings are as follows:

| Device Management | | |
|--|---|---------------------------------------|
| Device Host Name | | |
| Host Name | <input type="text" value="home_gateway"/> | |
| Embedded Web Server | | |
| HTTP Port | <input type="text" value="80"/> | (The default HTTP port number is 80.) |
| Expire to auto-logout | <input type="text" value="3"/> | min(s) |
| Universal Plug and Play (UPnP) | | |
| UPnP | <input checked="" type="radio"/> Enable <input type="radio"/> Disable | |
| UPnP Port | <input type="text" value="2800"/> | |
| <input type="button" value="Apply"/> <input type="button" value="Cancel"/> | | |

Embedded Web Server

HTTP Port: The port number of the router's embedded web server (for web-based configuration uses). The default value is the standard HTTP port, 80. You may specify an alternative if, for example, you are running a web server on a PC within your LAN.

For Example: User A changes HTTP port number to **100**, specifies their own IP address of **192.168.1.55**, and sets the logout time to be **100** minutes. The router only allows User A access from the IP address **192.168.1.55** to logon to the Web GUI by typing: <http://192.168.1.254:100> in their web browser. After 100 minutes, the device automatically logs out User A.

Universal Plug and Play (UPnP)

UPnP offers peer-to-peer network connectivity for PCs and other network devices, along with control and data transfer between devices. UPnP offers many advantages for users running NAT routers through UPnP NAT Traversal, and on supported systems makes tasks such as port forwarding much easier by letting the application control the required settings, removing the need for the user to control advanced configuration of their device.

Both the user's Operating System and the relevant application must support UPnP in addition to the router. Windows XP and Windows Me natively support UPnP (when the component is installed), and Windows 98 users may install the Internet Connection Sharing client from Windows XP in order to support UPnP. Windows 2000 does not support UPnP.

Disable: Check to disable the router's UPnP functionality.

Enable: Check to enable the router's UPnP functionality.

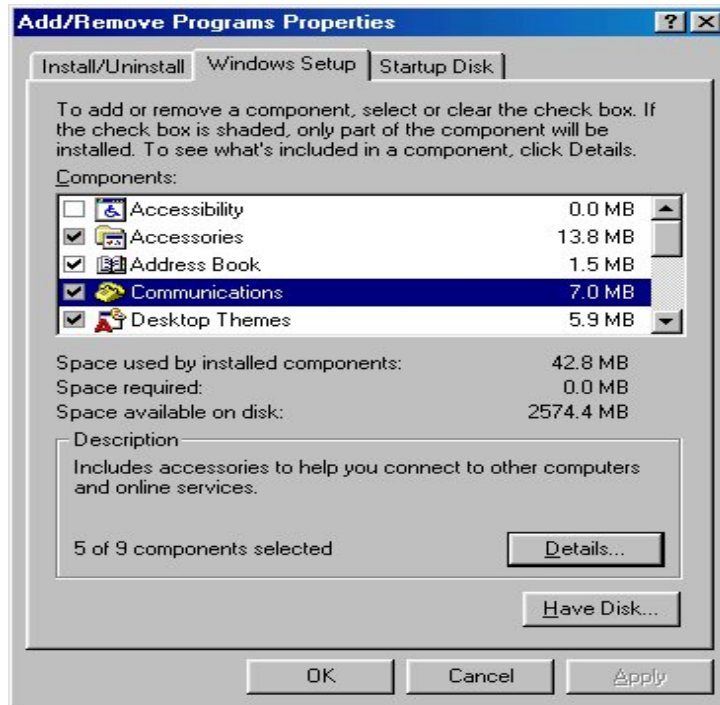
UPnP Port: The Default setting is 2800. It is highly recommended you use this port value. If this value conflicts with other ports already in use you may wish to change the port.

Installing UPnP in Windows Example

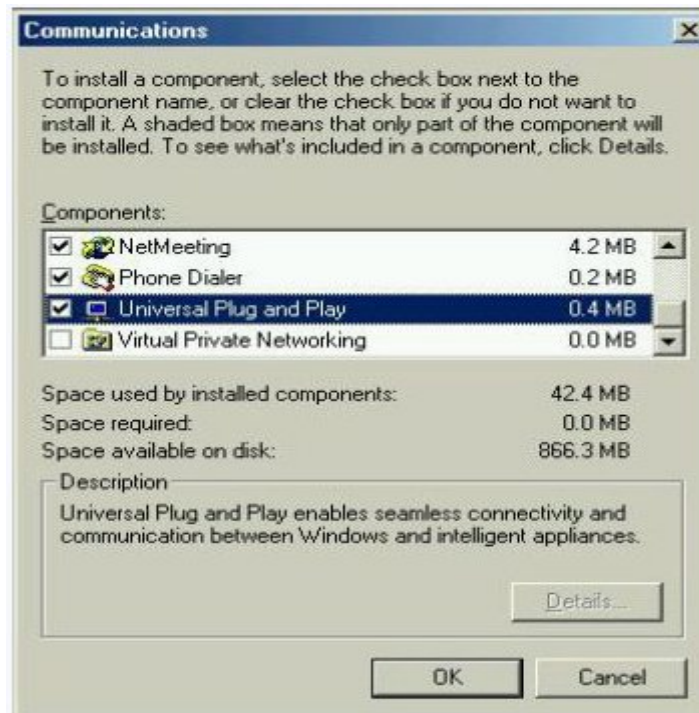
Follow the steps below to install the UPnP in Windows Me.

Step 1: Click Start and Control Panel. Double-click Add/Remove Programs.

Step 2: Click on the Windows Setup tab and select Communication in the Components selection box. Click Details.



Step 3: In the Communications window, select the Universal Plug and Play check box in the Components selection box.



Step 4: Click OK to go back to the Add/Remove Programs Properties window. Click Next.

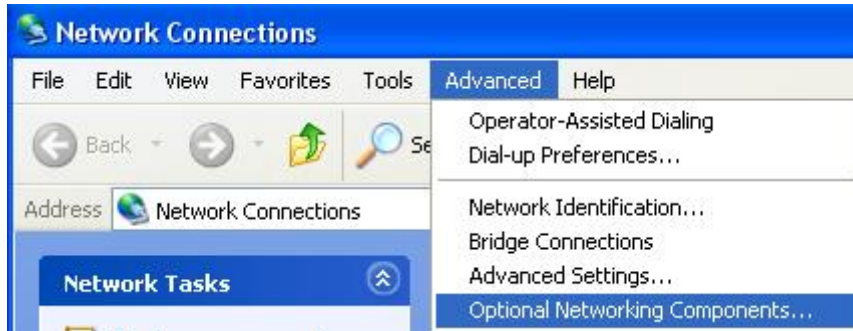
Step 5: Restart the computer when prompted.

Follow the steps below to install the UPnP in Windows XP.

Step 1: Click Start and Control Panel.

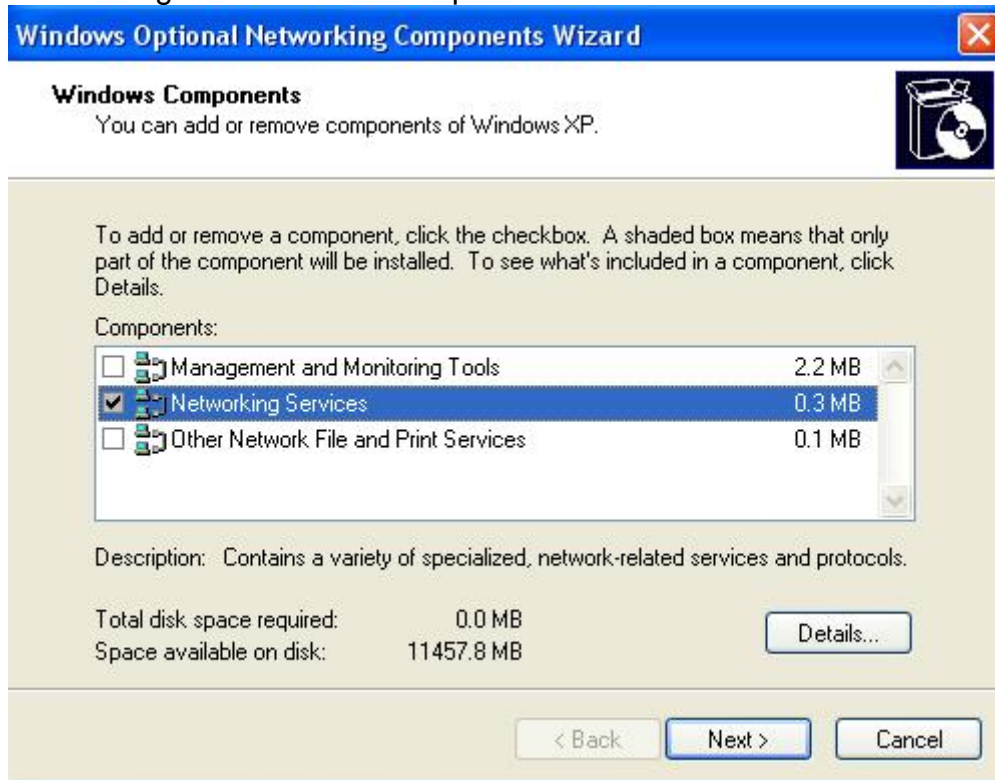
Step 2: Double-click Network Connections.

Step 3: In the Network Connections window, click Advanced in the main menu and select Optional Networking Components



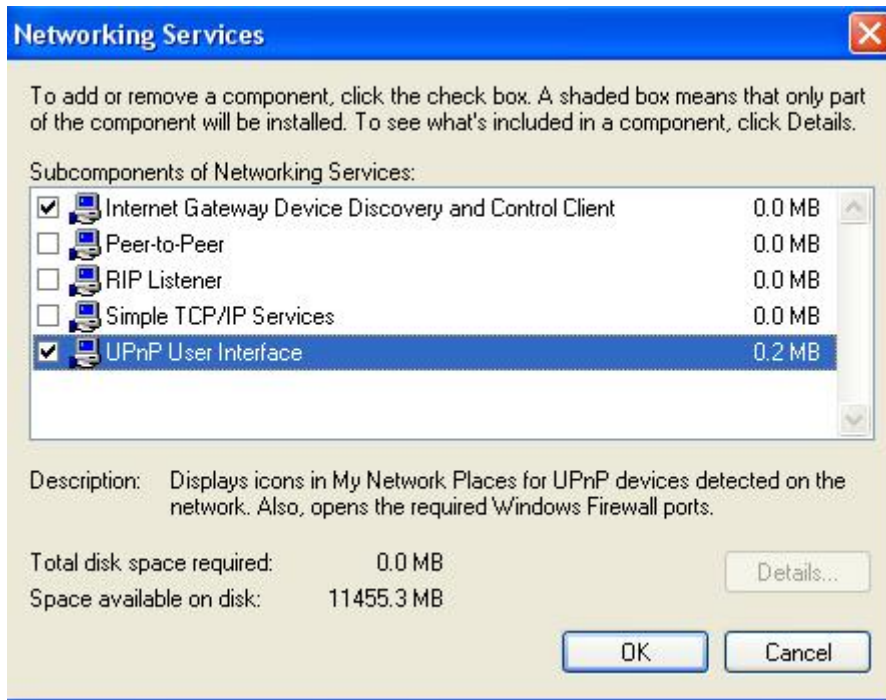
The Windows Optional Networking Components Wizard window displays.

Step 4: Select Networking Service in the Components selection box and click Details.



Step 5: In the Networking Services window, select the Universal Plug and Play check box.

Step 6: Click **OK** to go back to the Windows Optional Networking Component Wizard window and click **Next**.



Auto-discover Your UPnP-enabled Network Device

Step 1: Click start and Control Panel. Double-click Network Connections. An icon displays under Internet Gateway.

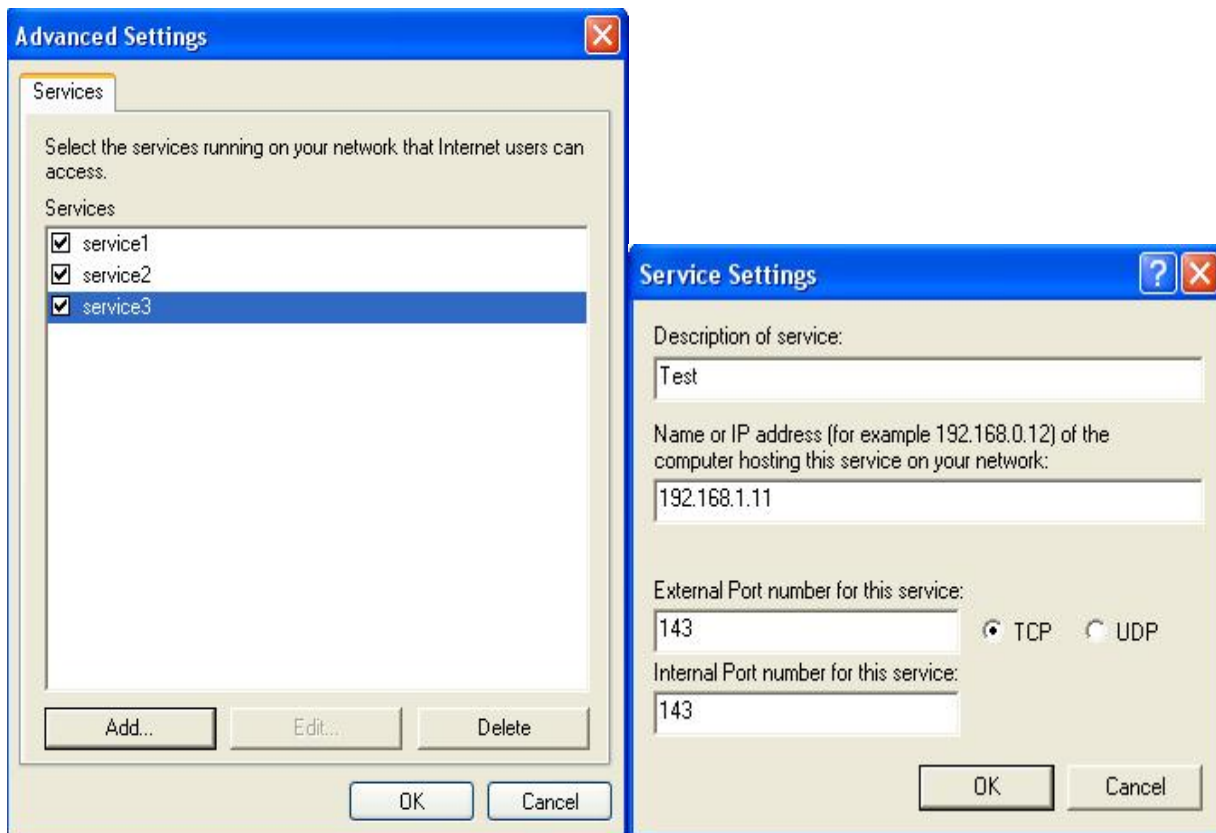
Step 2: Right-click the icon and select Properties.



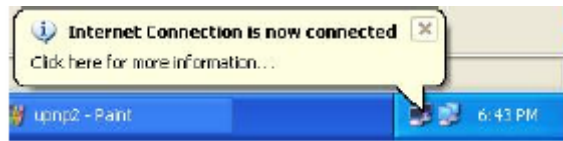
Step 3: In the Internet Connection Properties window, click Settings to see the port mappings that were automatically created.



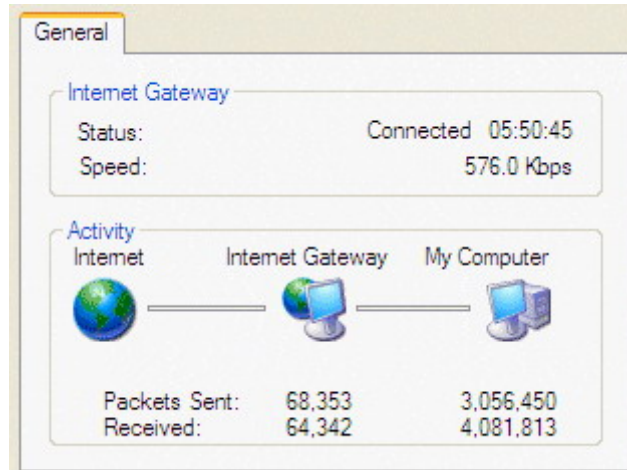
Step 4: You may edit or delete the port mappings or click Add to manually add port mappings.



Step 5: Select Show icon in notification area when connected option and click OK. An icon displays in the system tray



Step 6: Double-click on the icon to display your current Internet connection status.



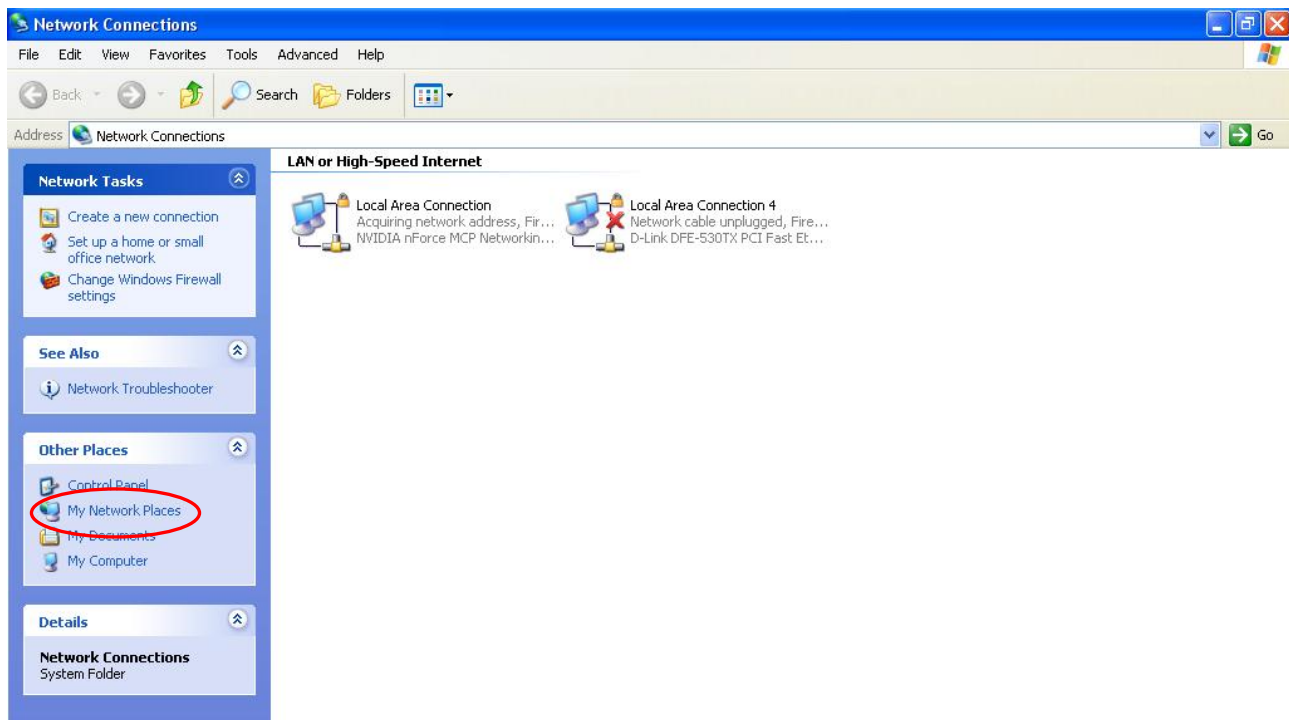
Web Configurator Easy Access

With UPnP, you can access web-based configuration for the Billion SG6200NXL without first finding out the IP address of the router. This helps if you do not know the router's IP address. Follow the steps below to access web configuration.

Step 1: Click Start and then Control Panel.

Step 2: Double-click Network Connections.

Step 3: Select My Network Places under Other Places.



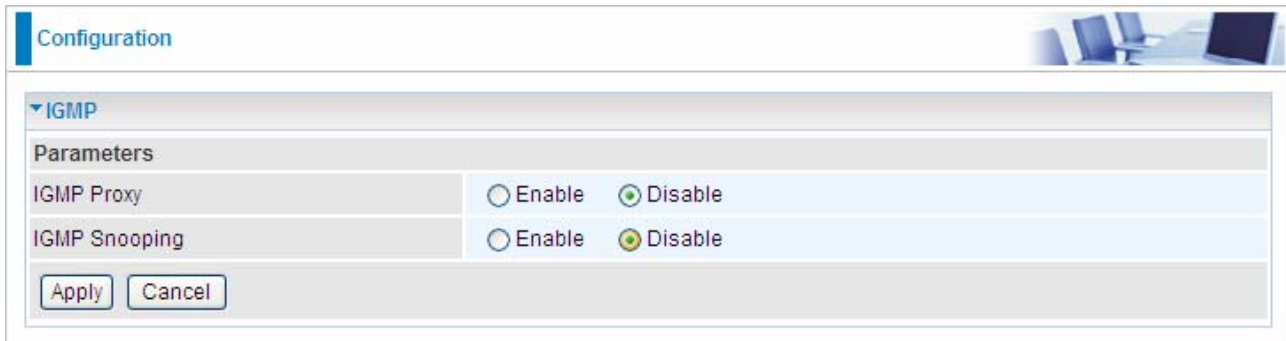
Step 4: An icon describing each UPnP-enabled device shows under Local Network.

Step 5: Right-click on the icon of your Billion SG6200NXL and select Invoke. The web configuration login screen displays.

Step 6: Right-click on the icon of your Billion SG6200NXL and select Properties. A properties window displays basic information about the Billion SG6200NXL.

IGMP

IGMP, known as Internet Group Management Protocol, is used to management hosts from multicast group.



The image shows a network configuration interface. At the top, there is a blue header with the word "Configuration" on the left and a small graphic of a meeting room on the right. Below the header, there is a section titled "IGMP" with a dropdown arrow. Underneath, there is a "Parameters" section. It contains two rows of configuration options. The first row is "IGMP Proxy" with two radio buttons: "Enable" (unselected) and "Disable" (selected). The second row is "IGMP Snooping" with two radio buttons: "Enable" (unselected) and "Disable" (selected). At the bottom of the configuration area, there are two buttons: "Apply" and "Cancel".

| Parameters | |
|---------------|---|
| IGMP Proxy | <input type="radio"/> Enable <input checked="" type="radio"/> Disable |
| IGMP Snooping | <input type="radio"/> Enable <input checked="" type="radio"/> Disable |

Apply Cancel

IGMP Proxy: Accepting multicast packet. Default is set to **Disable**.

IGMP Snooping: Allowing switched Ethernet / Wireless to check and make correct forwarding decisions. Default is set to **Disable**.

SNMP Access Control

Software on a PC within the LAN is required in order to utilize this function - Simple Network Management Protocol.

Configuration

SNMP Access Control

Parameters

SNMP Enable Disable

SNMP V1 and V2

| | | | |
|-----------------|----------------------|------------|----------------------|
| Read Community | <input type="text"/> | IP Address | <input type="text"/> |
| Write Community | <input type="text"/> | IP Address | <input type="text"/> |

SNMP V3

| | | | |
|----------|----------------------|----------|----------------------|
| Username | <input type="text"/> | Password | <input type="text"/> |
|----------|----------------------|----------|----------------------|

SNMP V1 and V2

Read Community: Specify a name to be identified as the Read Community, and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, user obtains this IP address will be able to view the data.

Write Community: Specify a name to be identified as the Write Community, and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, users from this IP address will be able to view and modify the data.

Trap Community: Specify a name to be identified as the Trap Community, and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, users from this IP address will be sent SNMP Traps.

SNMP V3

Specify a name and password for authentication. And define the access right from identified IP address. Once the authentication has succeeded, users from this IP address will be able to view and modify the data.

SNMP Version: SNMPV2c and SNMPv3

SNMPv2c is the combination of the enhanced protocol features of SNMPv2 without the SNMPv2 security. The "c" comes from the fact that SNMPv2c uses the SNMPv1 community string paradigm for "security", but is widely accepted as the SNMPv2 standard.

SNMPv3 is a strong authentication mechanism, authorization with fine granularity for remote monitoring.

Traps supported: Cold Start, Authentication Failure.

The following MIBs are supported:

From RFC 1213 (MIB-II):

- System group
- Interfaces group
- Address Translation group
- IP group
- ICMP group
- TCP group
- UDP group
- EGP (not applicable)
- Transmission
- SNMP group

From RFC1650 (EtherLike-MIB):

- dot3Stats

From RFC 1493 (Bridge MIB):

- dot1dBase group
- dot1dTp group
- dot1dStp group (if configured as spanning tree)

From RFC 1471 (PPP/LCP MIB):

- pppLink group
- pppLqr group

From RFC 1472 (PPP/Security MIB):

- PPP Security Group)

From RFC 1473 (PPP/IP MIB):

- PPP IP Group

From RFC 1474 (PPP/Bridge MIB):

- PPP Bridge Group

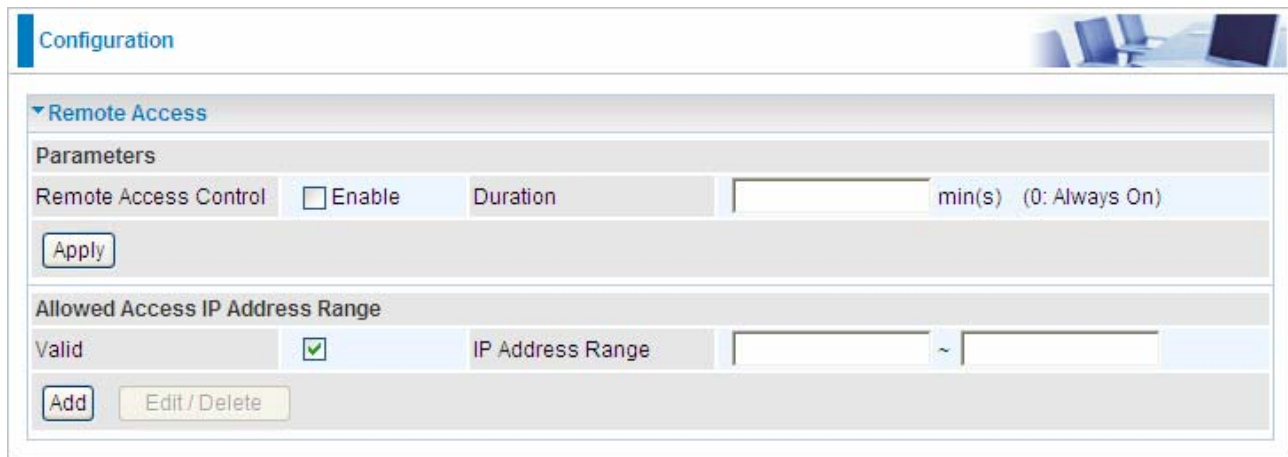
From RFC1573 (IfMIB):

- ifMIBObjects Group

From RFC 1907 (SNMPv2):

only snmpSetSerialNo OID

Remote Access



The screenshot shows a configuration window titled "Configuration" with a sub-section for "Remote Access". Under "Parameters", there is a checkbox for "Enable" (currently unchecked), a "Duration" input field, and a label "min(s) (0: Always On)". Below this is an "Apply" button. The "Allowed Access IP Address Range" section has a "Valid" checkbox (checked) and an "IP Address Range" input field with a tilde (~) separator. At the bottom of this section are "Add" and "Edit / Delete" buttons.

Remote Access Control

Enable: Select Enable to allow management access from remote side (mostly from internet).

Duration: Set how many minutes to allow management access from remote side. Zero means always on.

Allowed Access IP Address Range

Valid: Select Valid to allow remote management from these IP ranges.

IP Address Range: Specify what IP address to be allowed to access device from remote side. Click Add to insert management IP address list.

Save Configuration to Flash

After changing the router's configuration settings, you must save all of the configuration parameters to FLASH to avoid losing them after turning off or resetting your router. Click "**Save Config**" and click "**Apply**" to write your new configuration to FLASH.

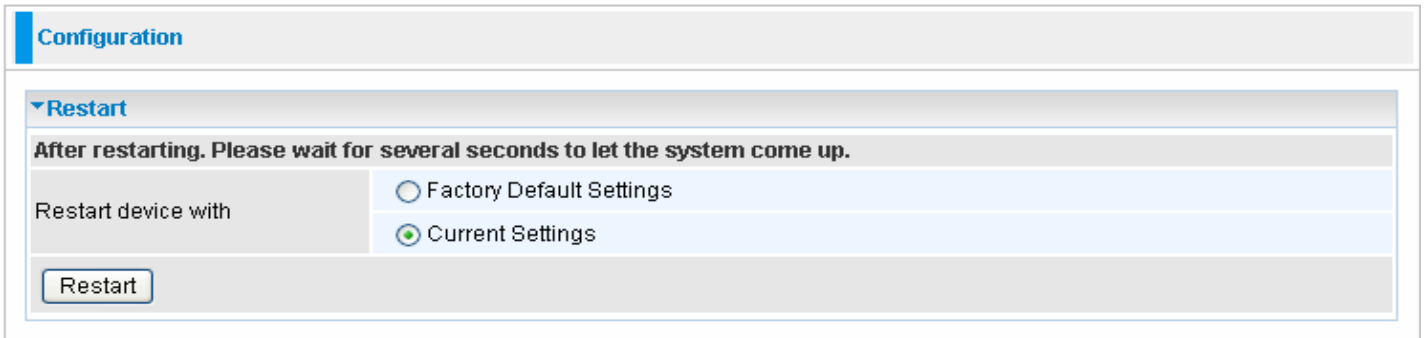
Configuration

▼ **Save Config to FLASH**

Write settings to FLASH

Restart

Click **Restart** with option **Current Settings** to reboot your router (and restore your last saved configuration).



The screenshot shows a web interface for router configuration. At the top, there is a 'Configuration' tab. Below it, a 'Restart' section is expanded, showing a warning: 'After restarting. Please wait for several seconds to let the system come up.' Underneath, there are two radio button options: 'Factory Default Settings' and 'Current Settings'. The 'Current Settings' option is selected. A 'Restart' button is located at the bottom of the section.

If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select **Factory Default Settings** to reset to factory default settings.

Logout

To exit the router's web interface, choose **Logout**. Please ensure that you have saved the configuration settings before you logout.

Be aware that the router is restricted to only one PC accessing the configuration web pages at a time. Once a PC has logged into the web interface, other PCs cannot get access until the current PC has logged out of the web interface. If the previous PC forgets to logout, the second PC can access the page after a user-defined period, by default 3 minutes. You can modify this value using the **Advanced - Device Management** section of the web interface. Please see the **Advanced** section of this manual for more information.

Chapter 6: Troubleshooting

If your 3G Router is not functioning properly, you can refer first to this chapter for simple troubleshooting before contacting your service provider support. This can save you time and effort but if symptoms persist, consult your service provider.

Problems starting up the router

| Problem | Corrective Action |
|---|---|
| None of the LEDs are on when you turn on the router. | Check the connection between the adapter and the router. If the error persists, you may have a hardware problem. In this case you should contact technical support. |

Problems with the LAN Interface

| Problem | Corrective Action |
|---------------------------------------|---|
| Can't ping any PCs on the LAN. | Check the Ethernet LEDs on the front panel. The LED should be on for a port that has a PC connected. If it is off, check the cables between your router and the PC. Make sure you have uninstalled any software firewall for troubleshooting. Verify that the IP address and the subnet mask are consistent between the router and the workstations. |

Problems with the FTP Server

| Problem | Corrective Action |
|---|--|
| FTP client which behind firewall remote access the router fail | Because the firewall has NAT function, this make can't access the router successful. There are two suggestions to solve the problem. <ol style="list-style-type: none">1. Set the FTP port as 21, you can access the router successful2. Use FTP client software (such as flashfxp V3.6), set the connect behaviour to be "active mode" you can also access the router successful. |

Problems with the Printer

| Problem | Corrective Action |
|---|---|
| Can't access the printer | Make sure you have added printer correctly, please reference Set up of Printer client. |
| The printer can't print though the printer have been added correctly | The router can support Ink-jet Printer well. For laser printer, because of its operation ways, maybe can't normal printing. |

Appendix: Product Support & Contact

If you come across any problems please contact the dealer from where you purchased your product.

Contact Billion

Worldwide:

<http://www.billion.com>

MAC OS is a registered Trademark of Apple Computer, Inc.

Windows 7/98, Windows NT, Windows 2000, Windows Me, Windows XP and Windows Vista are registered Trademarks of Microsoft Corporation.