



## Smart Energy Gateway

# User Manual

Version release: 1.03.ha.ds13  
Last revised: 2012-08-25

# 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 .....	28
WLAN .....	30
<i>Chapter 5: Advanced Configuration</i> .....	33
Status.....	34
ZigBee Status.....	35
Power Status .....	36
3G Status .....	37
USB Status.....	38
ARP Table .....	39
DHCP Table .....	39
System Log .....	40
Firewall Log.....	40
UPnP Portmap .....	41
Quick Start .....	42
Power Management.....	47
ZigBee Config.....	48
Power Control.....	50

ZigBee Firmware .....	53
ZigBee API Settings .....	54
Configuration.....	55
LAN (Local Area Network).....	55
Ethernet .....	56
IP Alias.....	56
Wireless .....	57
Wireless Security .....	59
WPS .....	62
DHCP Server .....	74
WAN (Wide Area Network).....	77
WAN Interface(EWAN).....	77
WAN Interface(3G) .....	77
WAN Interface(APCLIENT).....	78
WAN Interface(Dual WAN).....	79
WAN Profile .....	80
System .....	89
Time Zone.....	89
Firmware Upgrade .....	90
Backup / Restore .....	91
Restart Router .....	92
User Management .....	93
Mail Alert.....	94
USB.....	95
User Management .....	95
Storage .....	99
Samba Server.....	102
FTP Server .....	105
Printer Server.....	106
Webcam.....	111
Firewall and Access Control .....	112
Packet Filter.....	114
MAC Filter.....	116
Intrusion Detection.....	117
Download Tool .....	121
FTP Client.....	121
QoS (Quality of Service).....	126
Quality of Service Introduction .....	126

QoS Setup .....	126
Virtual Server.....	130
Port Mapping .....	132
DMZ.....	134
Wake on LAN .....	136
Time Schedule .....	137
Advanced .....	138
Static Route .....	139
Static ARP.....	139
Dynamic DNS .....	140
Device Management.....	141
IGMP .....	148
SNMP Access Control.....	149
Remote Access.....	151
Save Configuration to Flash .....	152
Restart.....	153
Logout .....	154
<i>Chapter 6: Troubleshooting .....</i>	<i>155</i>
<i>Appendix: Product Support &amp; Contact.....</i>	<i>157</i>

# Chapter 1: Introduction

## Introduction to your Router

Thank you for purchasing the PowerTracker/Billion 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 PowerTracker/Billion SMART ENERGY GATEWAY 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 PowerTracker/Billion SMART ENERGY GATEWAY supports 3G, PPP over Ethernet, DHCP Client and Fixed IP address 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 PowerTracker/Billion SMART ENERGY GATEWAY 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 PowerTracker/Billion SMART ENERGY GATEWAY 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 PowerTracker/Billion SMART ENERGY GATEWAY provides a full featured connectivity and allows a greater diversity of devices and applications to connect to the ZigBee network. The PowerTracker/Billion SMART ENERGY GATEWAY 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.

### **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**

PowerTracker/Billion SMART ENERGY GATEWAY 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.

### **USB Server**

PowerTracker/Billion SMART ENERGY GATEWAY supports two USB 2.0 ports, 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. Printer, Webcam and HDD can also connect to USB port, The PowerTracker/Billion SMART ENERGY GATEWAY 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, share files with your colleagues or friends with FTP server. If you need to handle office business, home security and personal entertainment, the PowerTracker/Billion SMART ENERGY GATEWAY can connect with your network devices using the built-in USB port.

### **3G Management Center**

Monitoring your 3G connection status is easy with the PowerTracker/Billion SMART ENERGY GATEWAY smart gateway. The unique PowerTracker/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 PowerTracker/Billion SMART ENERGY GATEWAY 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](http://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 PowerTracker/Billion SMART ENERGY GATEWAY 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

PowerTracker/Billion 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 PowerTracker/Billion SMART ENERGY GATEWAY 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 router can also function as a printer server, Webcam server and FTP server for network device sharing. With a supported Ethernet WAN port, the PowerTracker/Billion SMART ENERGY GATEWAY 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 PowerTracker/Billion's value added application utility, the 3G Management Centre.

With PowerTracker/Billion's SMART ENERGY GATEWAY, 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 PowerTracker/Billion SMART ENERGY GATEWAY 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 PowerTracker/Billion SMART ENERGY GATEWAY 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.

The PowerTracker/Billion SMART ENERGY GATEWAY 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 PowerTracker/Billion SMART ENERGY GATEWAY 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 PowerTracker/Billion SMART ENERGY GATEWAY and other network devices to a minimum - each wall or ceiling can reduce your PowerTracker/Billion SMART ENERGY GATEWAY 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

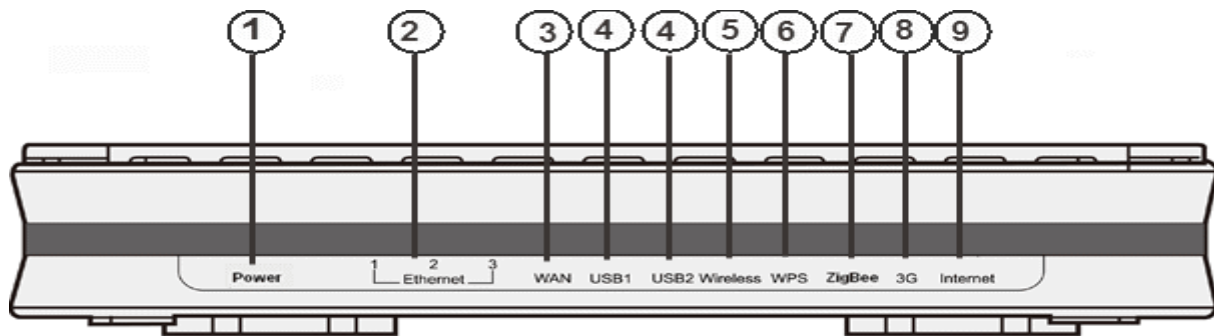
- Place the router on a stable surface.
- Only use the power adapter that comes with the package. Using a different voltage rating power adaptor may damage the router.

## Package Contents

- PowerTracker/Billion SMART ENERGY GATEWAY
- Quick Start Guide
- CD containing the online manual
- Ethernet Cable
- AC-DC power adapter
- Antennas (2 pcs)

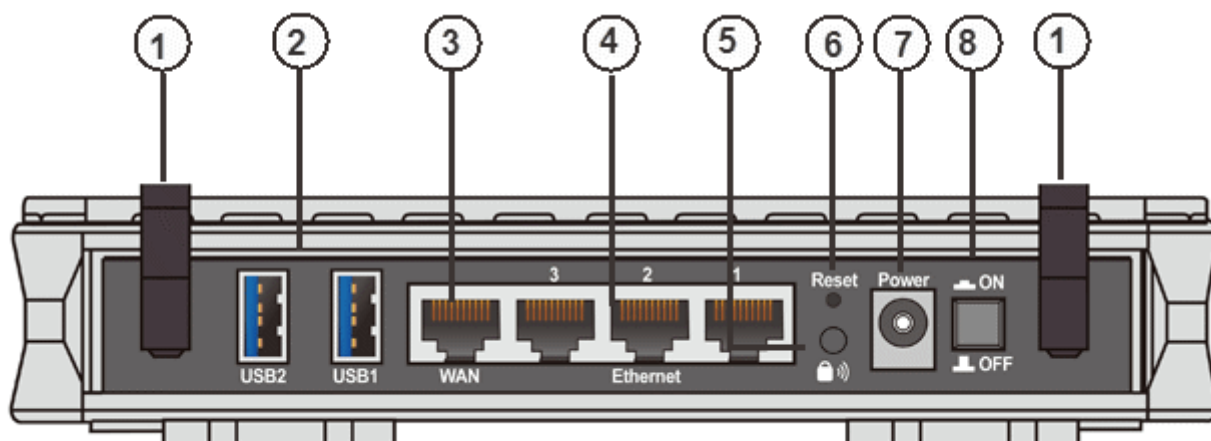
# Device Description

## The Front LEDs



LED		Meaning
1	<b>Power</b>	Lit red when power is ON. Lit green when the device is ready. Lit red means system failure. Restart the device or contact PowerTracker/Billion for support.
2	<b>Ethernet Port</b>	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	<b>WAN</b>	Lit green when connected to a modem or Cable modem's Ethernet port well.
4	<b>USB</b>	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	<b>Wireless</b>	Lit green when the wireless connection is established. Flashes when sending/receiving data.
6	<b>WPS</b>	Lit green when WPS is being in progress. Unlit when WPS is connected.
7	<b>ZigBee</b>	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	<b>3G</b>	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	<b>Internet</b>	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	<b>Antenna</b>	Connect the detachable antenna to this port.
2	<b>USB</b>	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	<b>WAN</b>	WAN 10/100M Ethernet port (with auto crossover support); connect Cable modem here.
4	<b>Ethernet</b>	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	<b>WPS</b>	Push WPS button to trigger ZigBee function, thus smartmeter allowing join in is starting. See <a href="#">ZigBee Config</a> section. Push WPS button more than 5 seconds to trigger Wi-Fi Protected Setup function. See <a href="#">WPS</a> section.
6	<b>RESET</b>	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). <b>Caution: After pressing the RESET button for more than 6 seconds, to be sure you power cycle the device again.</b>
7	<b>Power</b>	Connect it with the supplied power adapter.
8	<b>Power Jack</b>	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 PowerTracker/Billion SMART ENERGY GATEWAY 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 **192.168.100.254** 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 192.168.100.1 and 192.168.100.253). 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 192.168.100.254 IP address of the router.

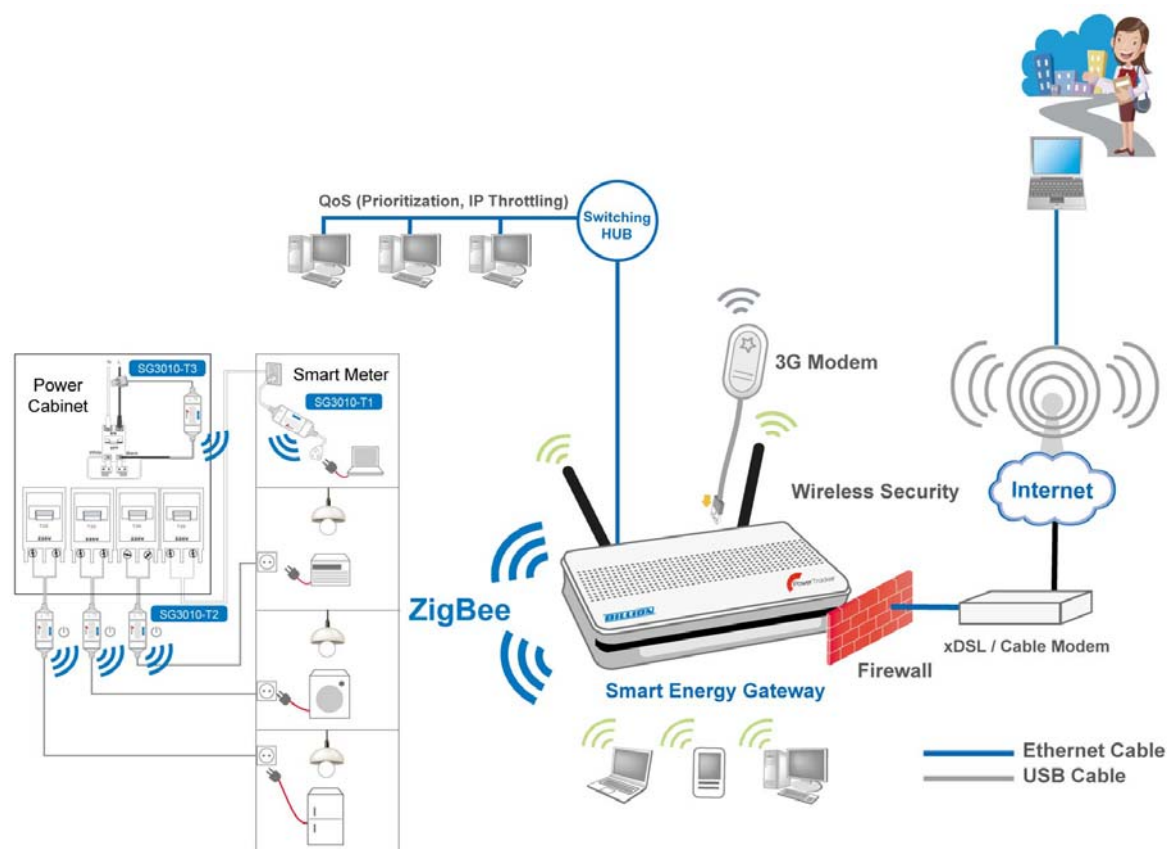
Please follow the steps below for installation on your PC's network environment. First of all, check your PC's network components. The TCP/IP protocol stack and Ethernet network adapter must be installed. If not, please refer to your Windows-related or other operating system manuals.



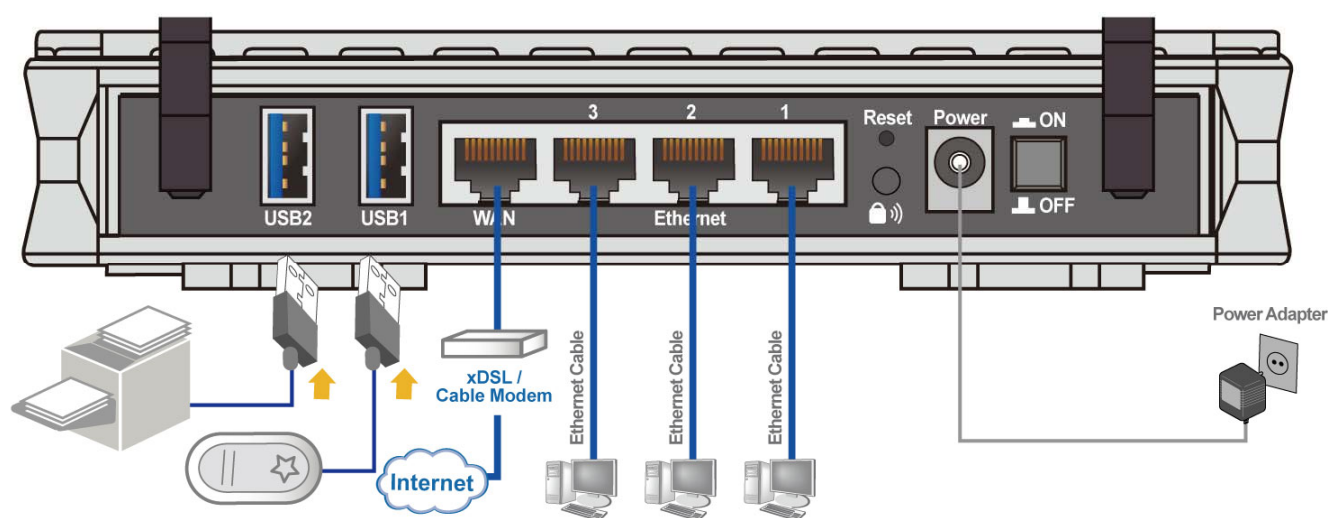
Any TCP/IP capable workstation can be used to communicate with or through the PowerTracker/Billion SG6200NXL. To configure other types of workstations, please consult the manufacturer's documentation.

# Connecting your router

Overview:



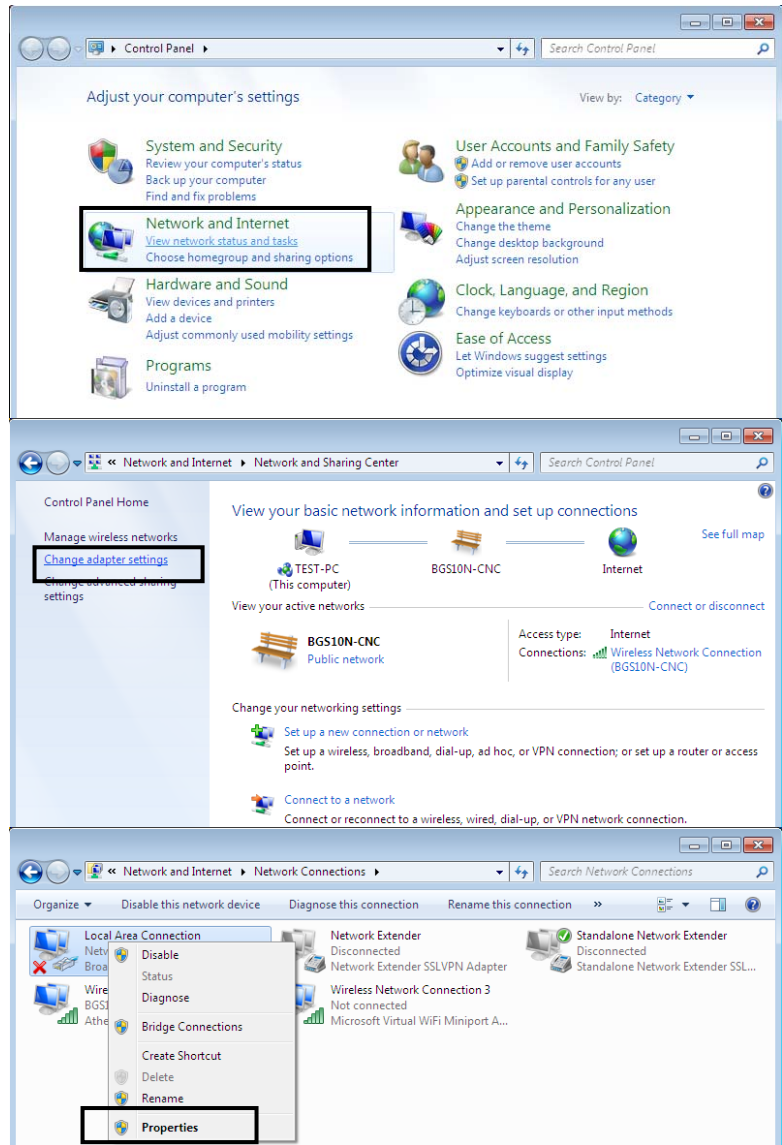
Detailed:



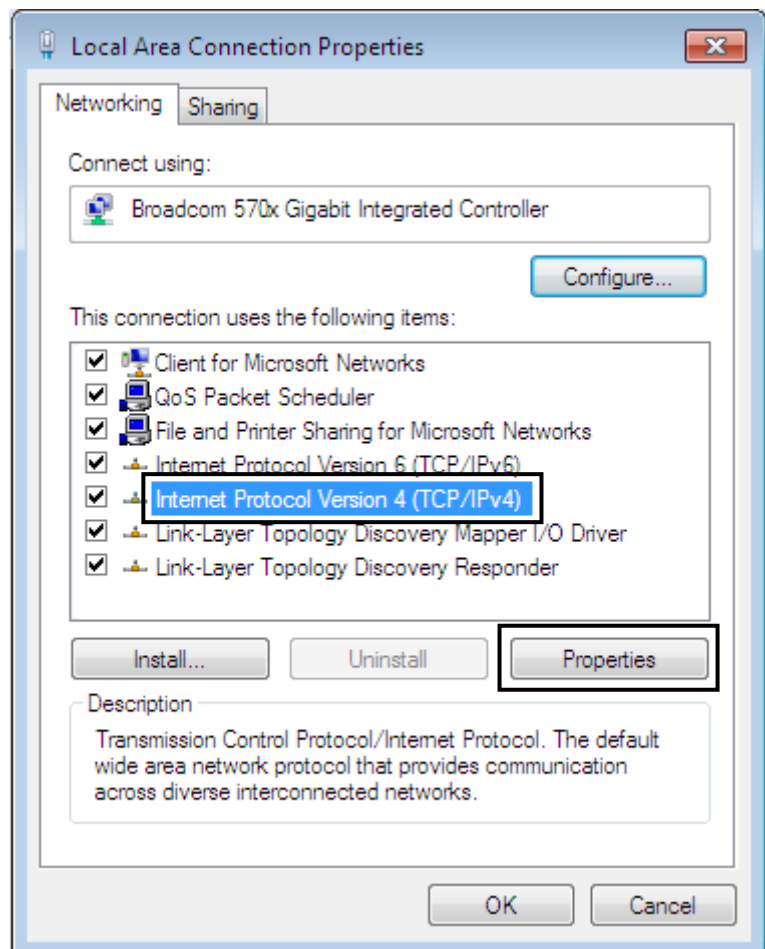
# Network Configuration

## 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**.

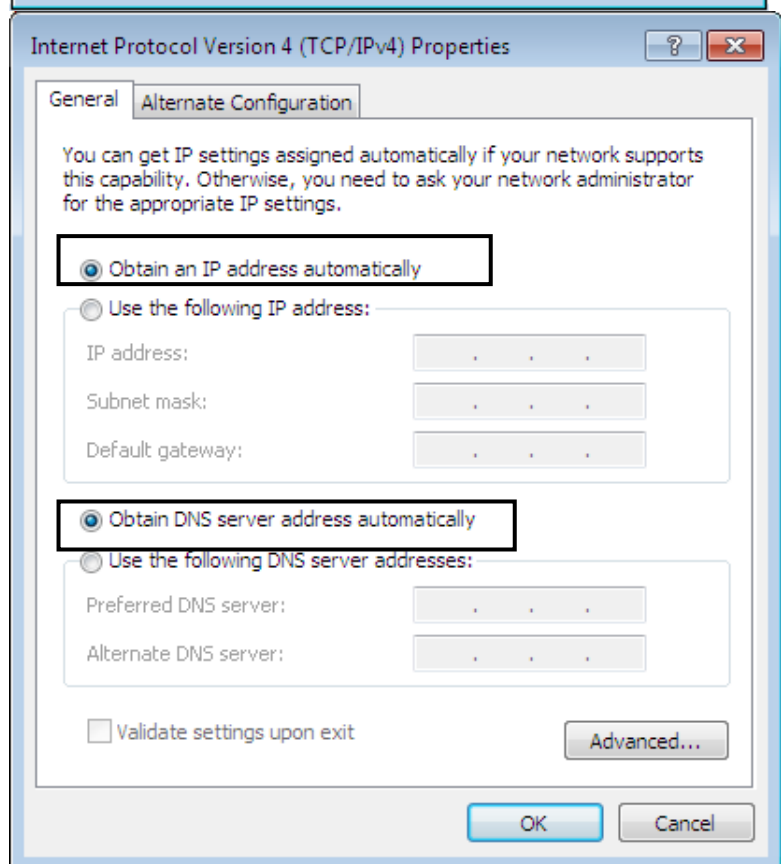


5. Select **Internet Protocol Version 4 (TCP/IPv4)** then click **Properties**.



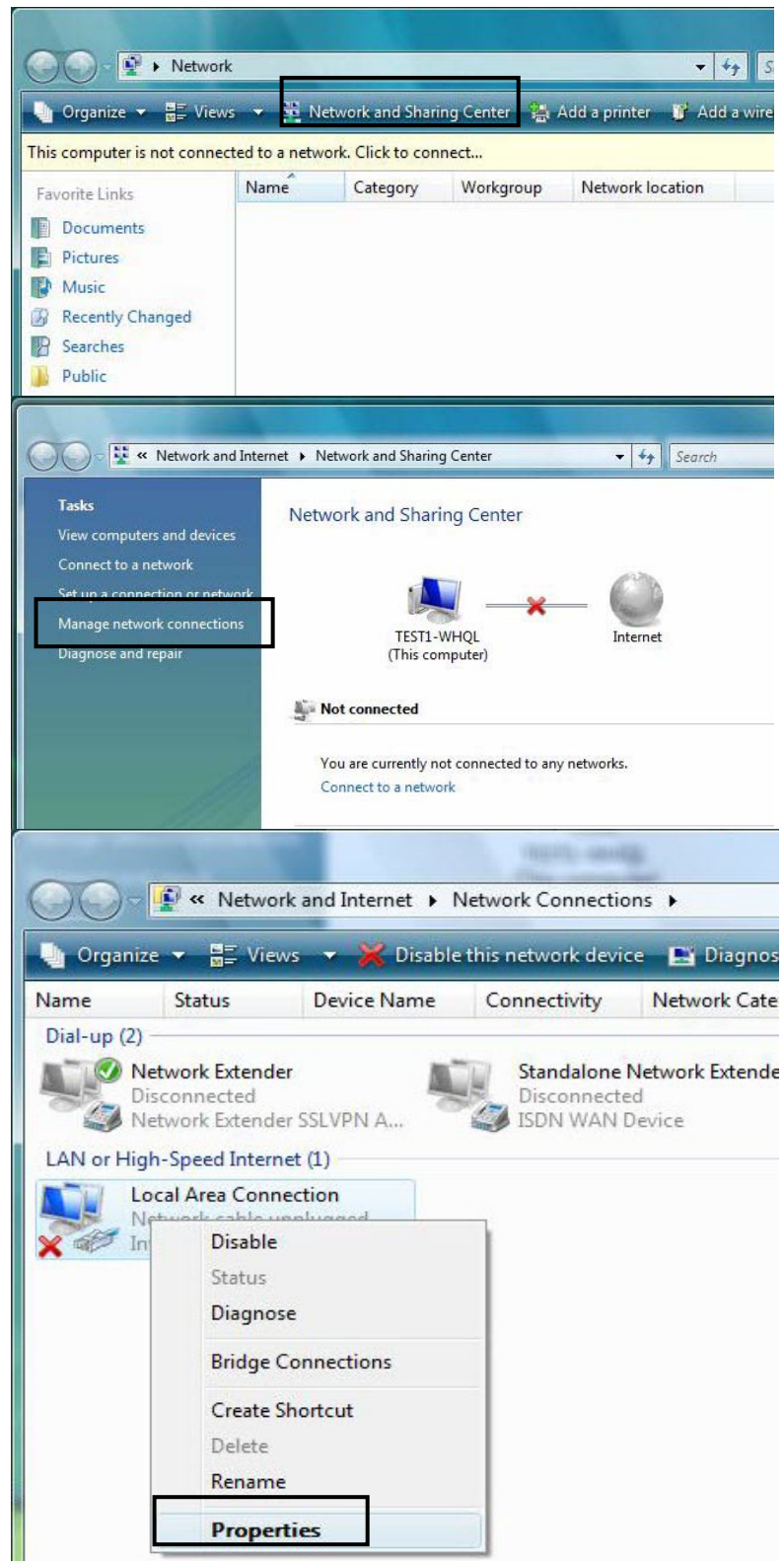
6. In the **TCP/IPv4 properties** window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

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

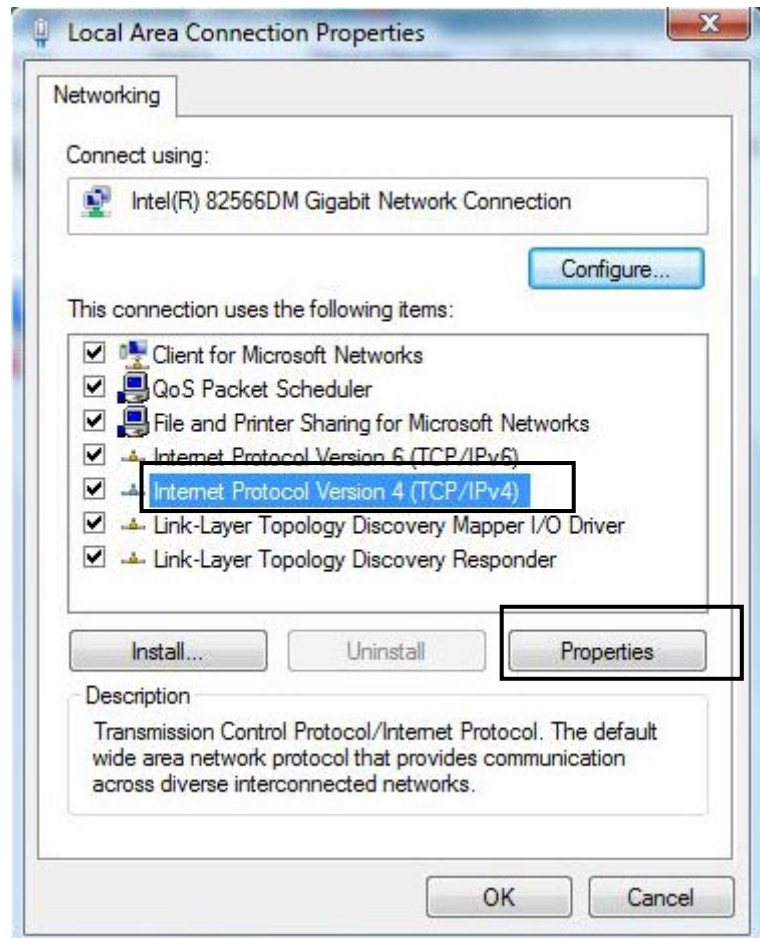


## Configuring a PC in Windows Vista

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**.

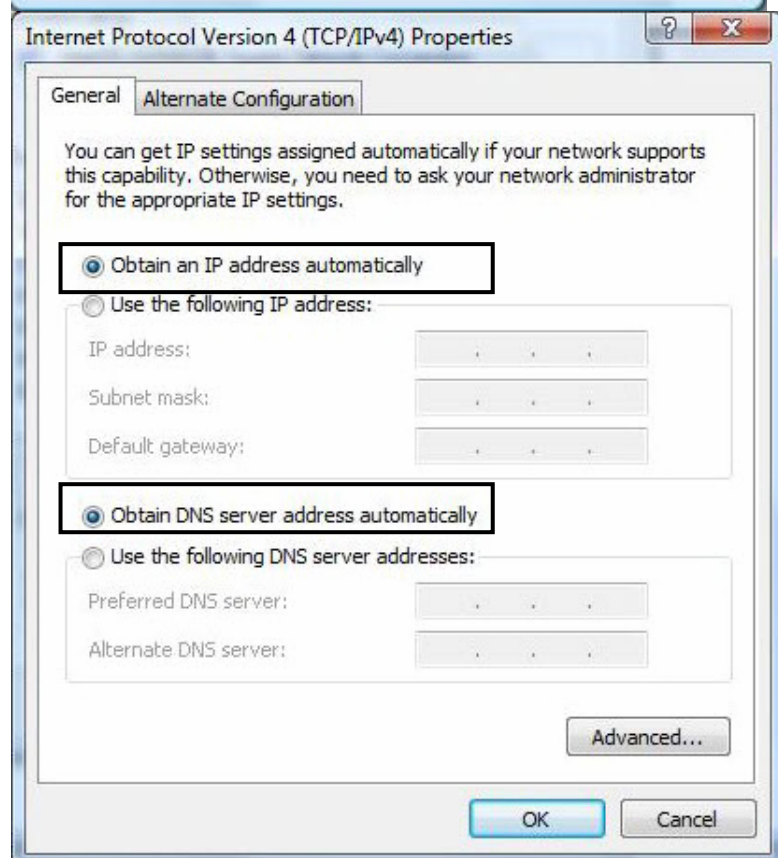


5. Select **Internet Protocol Version 4 (TCP/IPv4)** then click **Properties**.



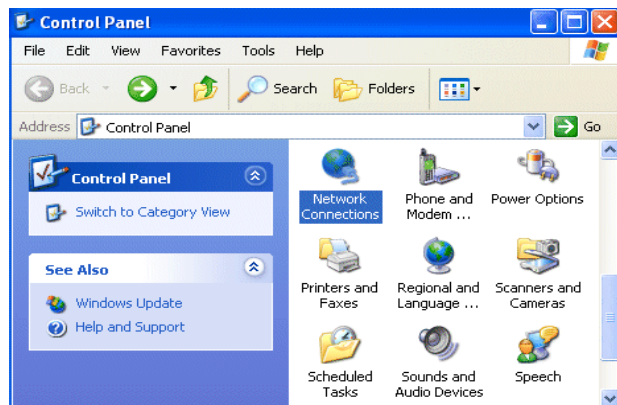
6. In the **TCP/IPv4 properties** window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

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

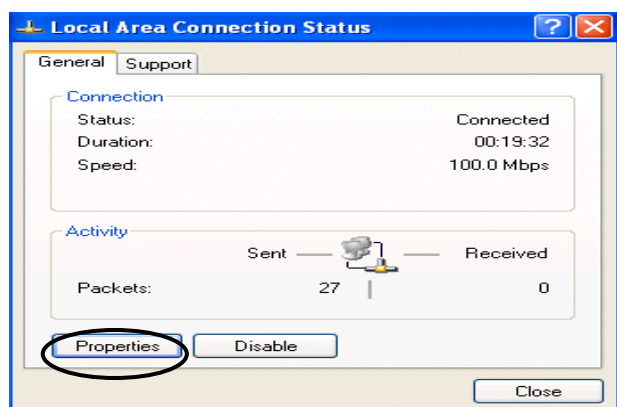


# Configuring a PC in Windows XP

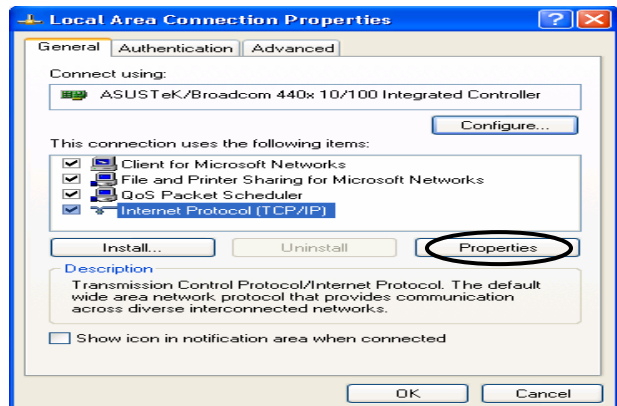
1. Go to **Start**. Click on **Control Panel**.
2. Then click on **Network and Internet**.



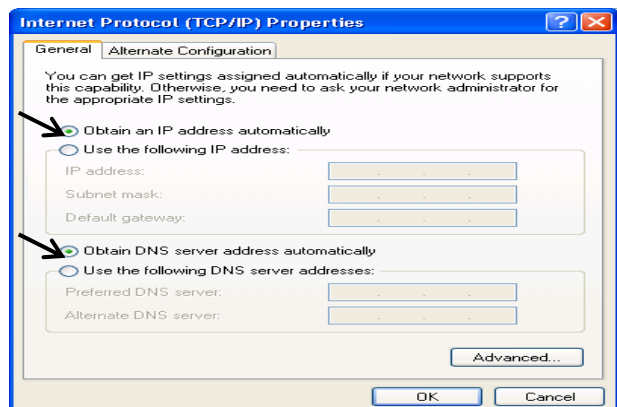
3. In the **Local Area Connection Status** window, click **Properties**.



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.

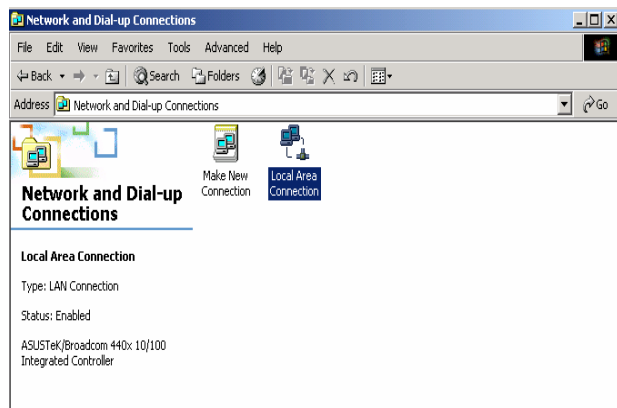


6. Click **OK** to finish the configuration.

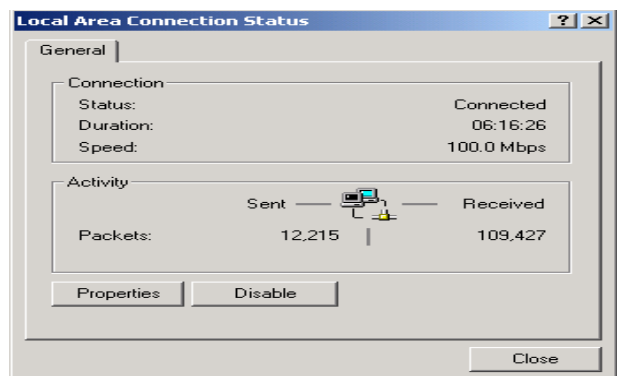
# Configuring a PC in Windows 2000

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

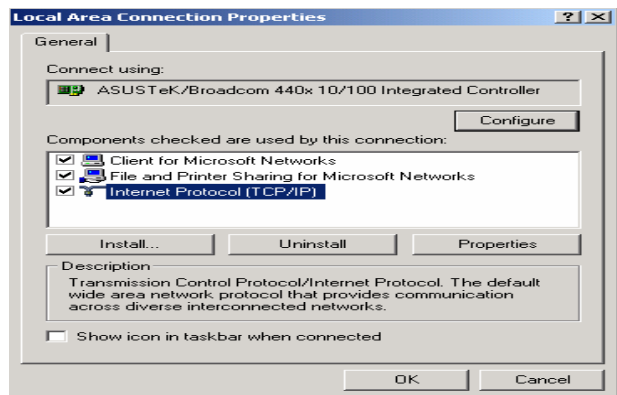
2. Double-click **Local Area Connection**.



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

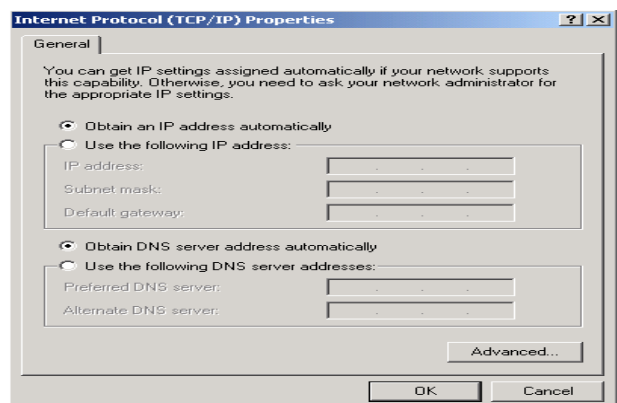


4. Select **Internet Protocol (TCP/IP)** and click **Properties**.



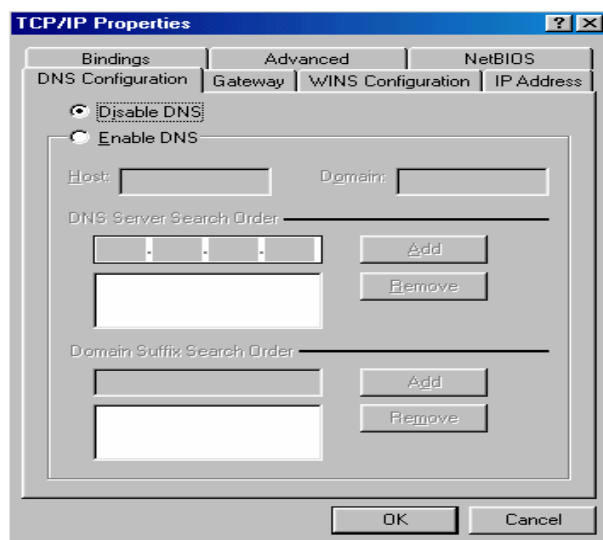
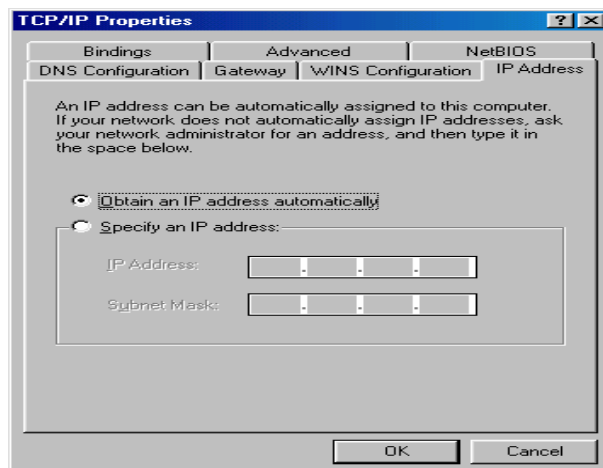
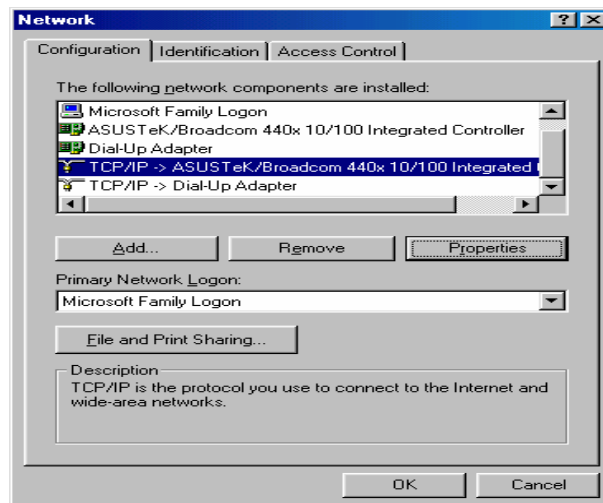
5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.

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



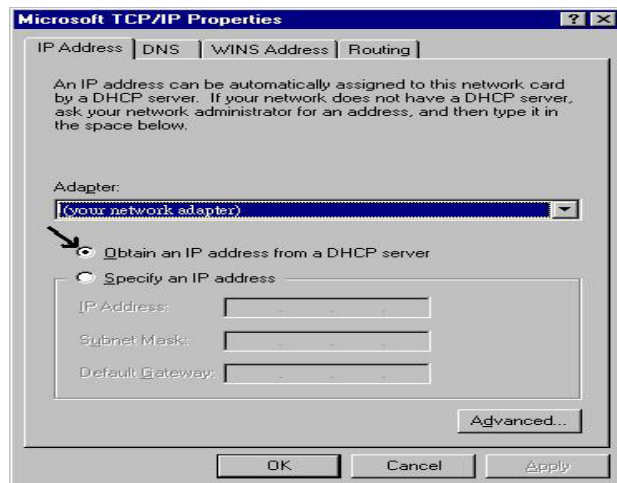
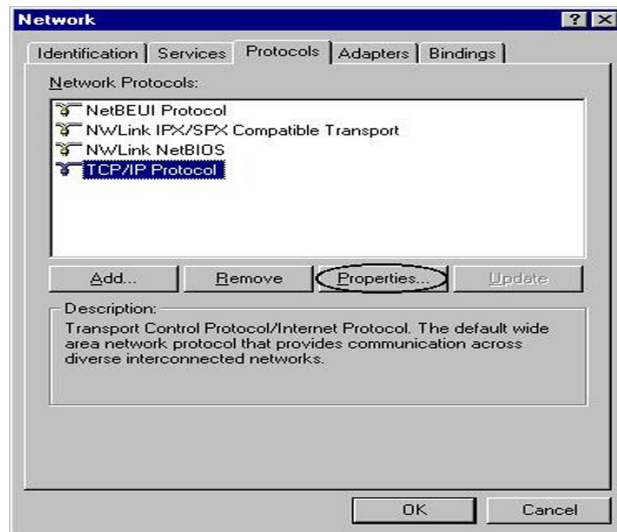
# Configuring PC in Windows 98/Me

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 PowerTracker/Billion SMART ENERGY GATEWAY 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: 192.168.100.254
- ▶ 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: 192.168.100.100
- ▶ 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	192.168.100.254	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 192.168.100.100 through 192.168.100.199	

## 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.

<b>PPPoE</b>	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).
<b>Obtain an IP Address Automatically</b>	DHCP Client (it can be automatically assigned by your ISP when you connect or be set manually).
<b>Fixed IP Address</b>	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 **192.168.100.254**, 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.









The image shows the login interface for a Billion PowerTracker Smart Energy Gateway. At the top, there is a header with the "BILLION" logo on the left and the "PowerTracker" logo on the right. Below the header, there is a central area featuring a photograph of the white gateway device with two antennas. To the right of the device, the text "Smart Energy Gateway" is displayed in a blue, italicized font. Below this image and text, there is a login form with three input fields: "Username" with a text box, "Password" with a text box, and "Account" with a dropdown menu currently showing "Administrator". A blue "Submit" button is located below the "Account" dropdown.

Congratulations! You have successfully logged on to your PowerTracker/Billion SMART ENERGY GATEWAY!

# Chapter 4: Basic Configuration

Once you have logged on to your PowerTracker/Billion SMART ENERGY GATEWAY 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

Status

▼Device Information

Model NameSG6200NXL

System Up-Time28 min(s)

Software Version1.03.ha.ds13

ZigBee Firmwarersp-hazc-1.1.9

ZigBee EUI640000000000000002

▼Port Status

Ethernet✓

EWAN✗

3G✗

APCLIENT✗

Wireless ▶✓

▼WAN

Port ▶	Protocol	Operation	Connection	IP Address	Netmask	Gateway	Primary DNS
EWAN	Fixed			192.168.1.100	255.255.255.0	192.168.1.254	8.8.8.8

## 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, APCLIENT 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



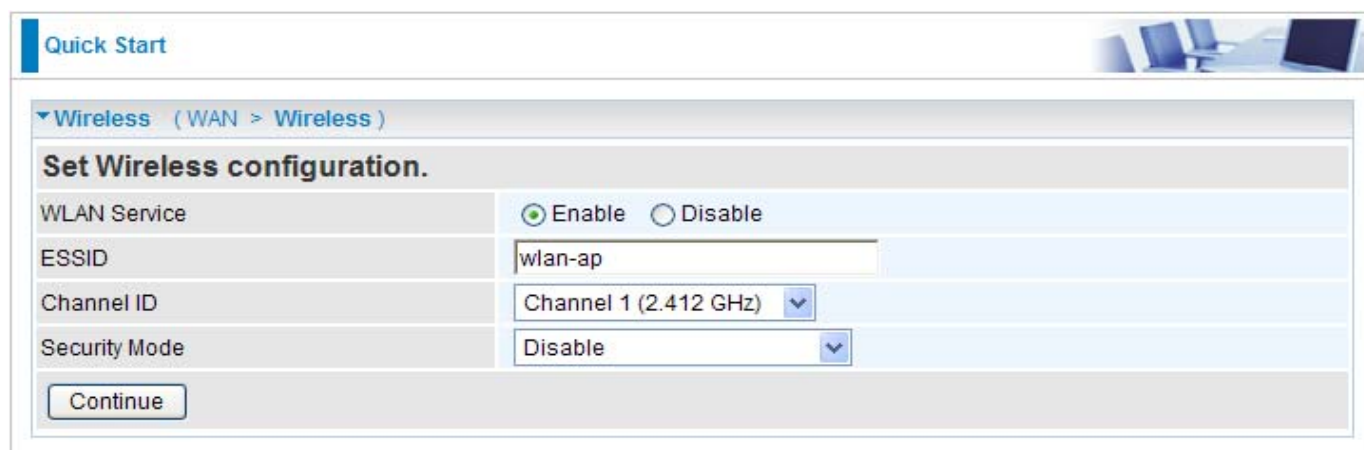
Quick Start

▼ WAN Port ( WAN > Wireless )

**Select WAN Port**

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

## Set Wireless configuration



Quick Start

▼ Wireless ( WAN > Wireless )

**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 ▼

**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 excess 32 characters. Make sure your wireless clients have exactly the ESSID as the device, in order to get connected to your network.

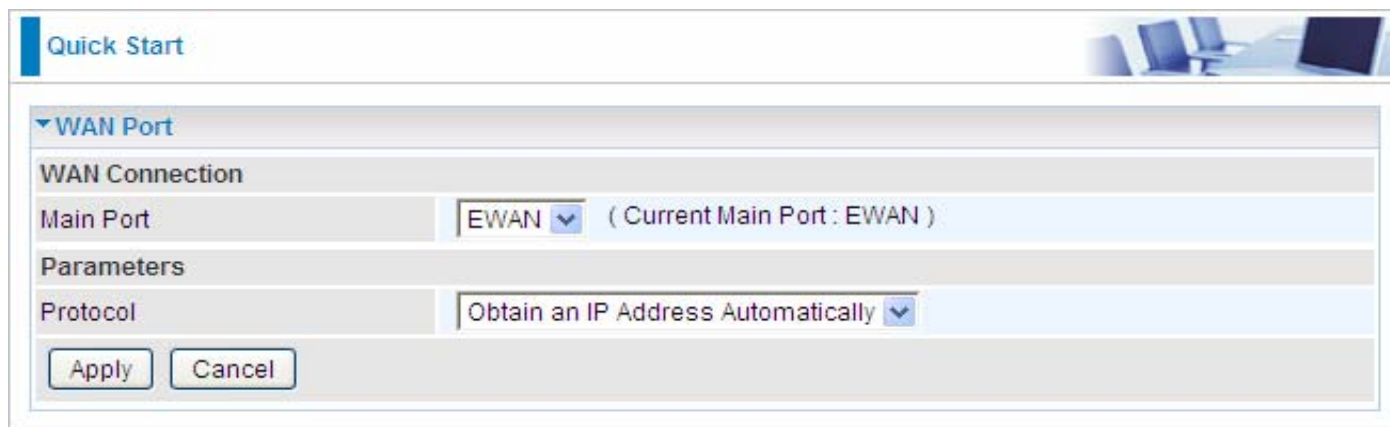
**Channel ID:** Select the ID channel that you would like to use.

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

For detailed Quick Start configuration, turn to Page 41-45 for help.

# WAN

## EWAN



Quick Start

▼ WAN Port

WAN Connection

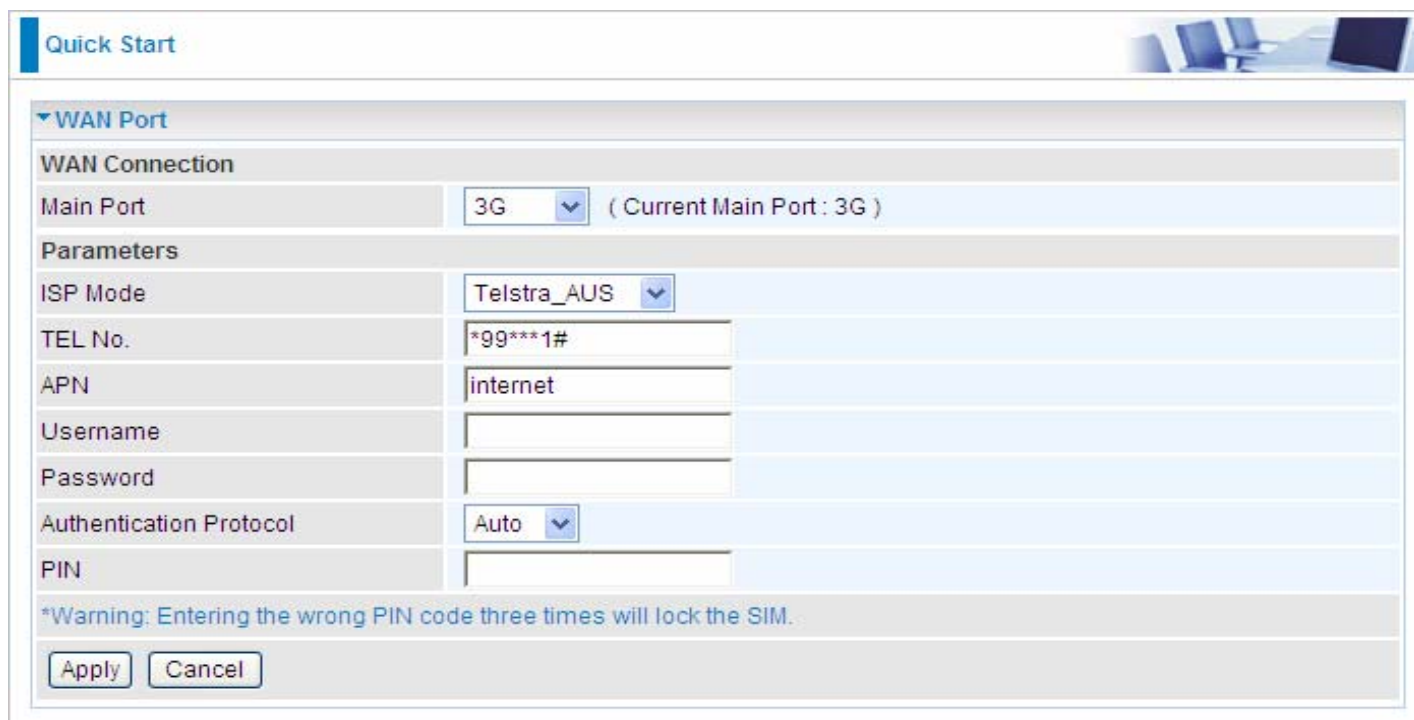
Main Port: EWAN (Current Main Port : EWAN)

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.

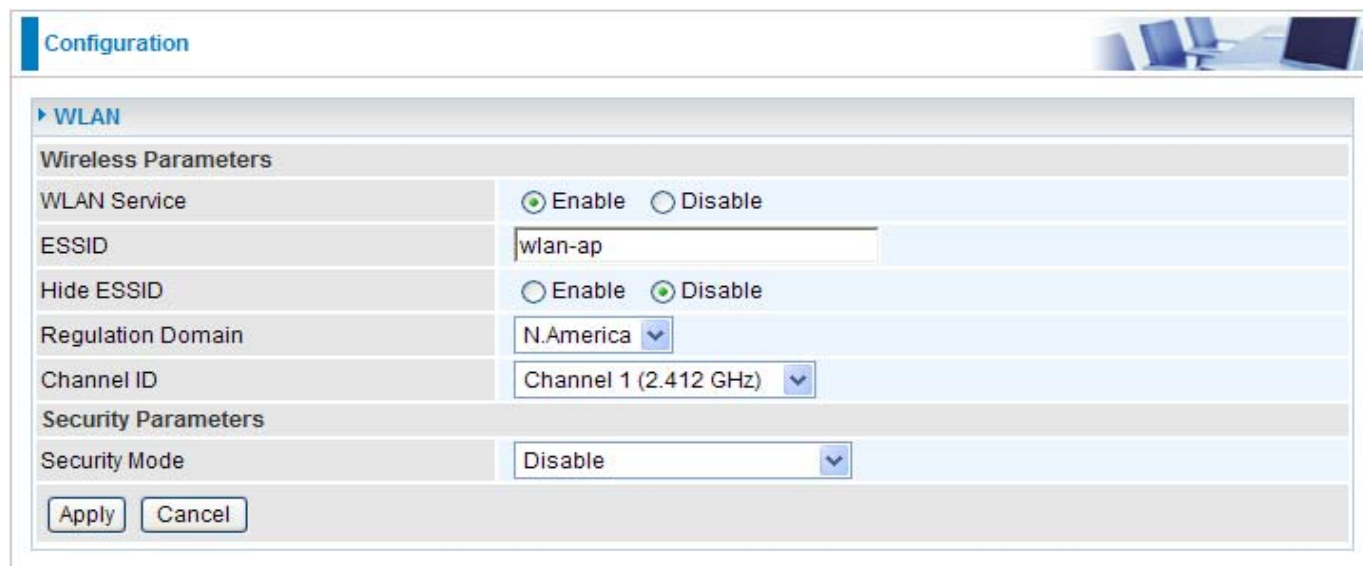
**Auth. Protocol:** Manually specify CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol) if you know which authentication type the server is using (when acting as a client), or the authentication type you want the clients to use when they are connecting to you (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.

# WLAN



Configuration

WLAN

Wireless Parameters

WLAN Service ☒ Enable ☐ Disable

ESSID wlan-ap

Hide ESSID ☐ Enable ☒ Disable

Regulation Domain N.America

Channel ID Channel 1 (2.412 GHz)

Security Parameters

Security Mode Disable

Apply Cancel

**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.

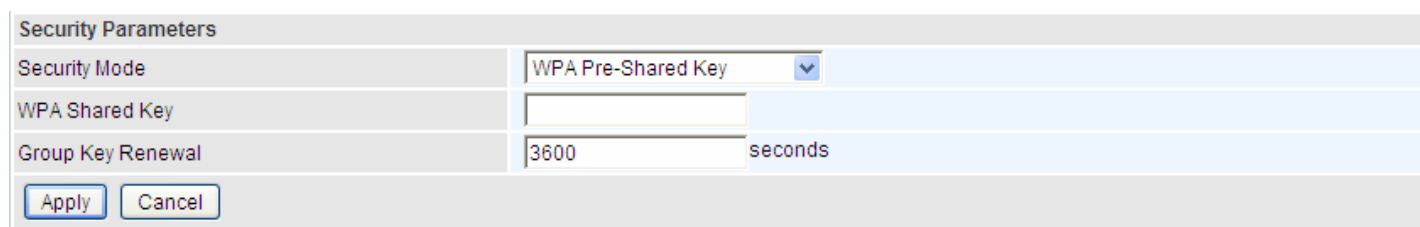
**Regulation Domain:** There are seven Regulation Domains for you to choose from, including **North America (N.America)**, **Europe**, **France**, etc. The Channel ID will be different based on this setting.

**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



Security Parameters

Security Mode WPA Pre-Shared Key

WPA Shared Key

Group Key Renewal 3600 seconds

Apply Cancel

**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	
Group Key Renewal	3600 seconds
<div>Apply Cancel</div>	

**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	
Group Key Renewal	3600 seconds
<div>Apply Cancel</div>	

**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 <span>▼</span>
WEP Authentication	Open System <span>▼</span>
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"/> <span>WEP64</span> <span>WEP128</span>
Key 1	Hex <span>▼</span> <input type="text"/>
Key 2	Hex <span>▼</span> <input type="text"/>
Key 3	Hex <span>▼</span> <input type="text"/>
Key 4	Hex <span>▼</span> <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>	
<span>Apply</span> <span>Cancel</span>	

**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 SMART ENERGY GATEWAY 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** (ZigBee Status, Power Status, 3G Status, USB Status, ARP Table, DHCP Table, System Log, Firewall Log, UPnP Portmap)
-  **Quick Start**
-  **Power Management** (ZigBee Config, Power Control, ZigBee Firmware, ZigBee API Settings)
-  **Configuration** (LAN, WAN, System, USB, 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

Status

▼ Device Information

Model NameSG6200NXL

Host Name ▶home.gateway

System Up-Time34 min(s)

Current Time ▶Sat Jan 1 00:34:36 2000

Software Version1.03.ha.ds13

MAC Address00:04:ed:d7:8a:24

ZigBee Firmwarersp-hazc-1.1.9

ZigBee EUI640000000000000002

▼ Port Status

Ethernet✓

EWAN✗

3G ▶✗

APCLIENT✗

Wireless ▶✓

▼ WAN

Port ▶	Protocol	Operation	Connection	IP Address	Netmask	Gateway	Primary DNS
EWAN ▶	Fixed			192.168.1.100	255.255.255.0	192.168.1.254	8.8.8.8

## 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, APCLIENT 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.

# ZigBee Status

Status



**▼ Zigbee Status**

Parameters	
Status	Joined Network
Channel	13
PAN ID	66c4
EUI address	0000000000000002
Version	rsp-hazc-1.1.9

Refresh

**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.

Status

SmartMeter status

Table

No.	Appliance	Power Status	Power Information	Signal Strength
			Active Power	
1	PC	ON	11.52 (W)	<div><div></div><div></div><div></div><div></div><div></div></div> 88%(Rssi:-67 ,Lqi:255)

Refresh

**No.:** The sequence number.

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

**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

**RSSI:**Namely “Received Signal Strength Indicator” (RSSI) is a measurement of the power present in a received radio signal.

**LQI:** Namely “Link Quality Indicator” indicates the strength and quality of the received radio frame.

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

## 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	<div><div></div></div>
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	<div><div></div></div> <div>NaNHours of Hours</div>
Billing period	<div><div></div></div> <div>Day:NaN</div>

Clear

**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.

# USB Status

This section displays the status of USB such as the USB device Status, the USB Storage Status and the USB Server Status which give users a overall view of the USB configuration.

Status

▼ USB Server Status

Parameters

Samba Server ▶	Disable
FTP Server ▶	Enable
Printer Server ▶	Disable
Web Camera Server ▶	Disable

▼ USB Device Status

USB Port	Device Type	Device Model	Device Manufacturer	Support
USB Port00	Storage	USB2.0	N/A	✓

Refresh

▼ USB Storage Status

Disk	Type	Capacity	Used	Free Space	%Used	Mount On
Disk1	vfat	3.8G	1.5G	2.3G	39%	/media/sda1

Refresh

## USB Server Status

**Samba Server:** Display the current status of the Samba, enable or disable.

**FTP Server:** Display the current status of the FTP Server, enable or disable.

**Printer Server:** Display the current status of the Printer Server, enable or disable.

**Web Camera Server:** Display the current status of the Web Camera Server, enable or disable.

Click the of the above four links to enter the corresponding page to configure furter. For more information , please turn to **Samba Server**, **FTP Server**, **Printer Server**, **Webcam** in **USB Server** section for detail.

## USB Device Status

**USB Port:** Display which USB port the device are connected to.

**Device Type:** Display the type of the device.

**Device Model:** Display the model of the device.

**Device manufacture:** Display the manufacture of the device.

**Support:** Indicate whether the device is supported.

**Refresh:** To get the latest statistics.

## USB Storage Status

**Disk:** Display the storage partition.

**Type:** Display the file storage type.

**Capacity:** Display the capacity of the disk.

**Used:** Display how much has been used.

**Free Space:** Display the remaining space available.


**%Used:** Display the percentage of used space to the all space.

**Mount on:** Display which partition path the device is mounted on.

**Refresh:** To refresh to show the latest statistics.

## 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.

Status 			
▼ ARP Table			
Wired & Wireless			
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

Status 			
▼ DHCP Table			
Leased 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.

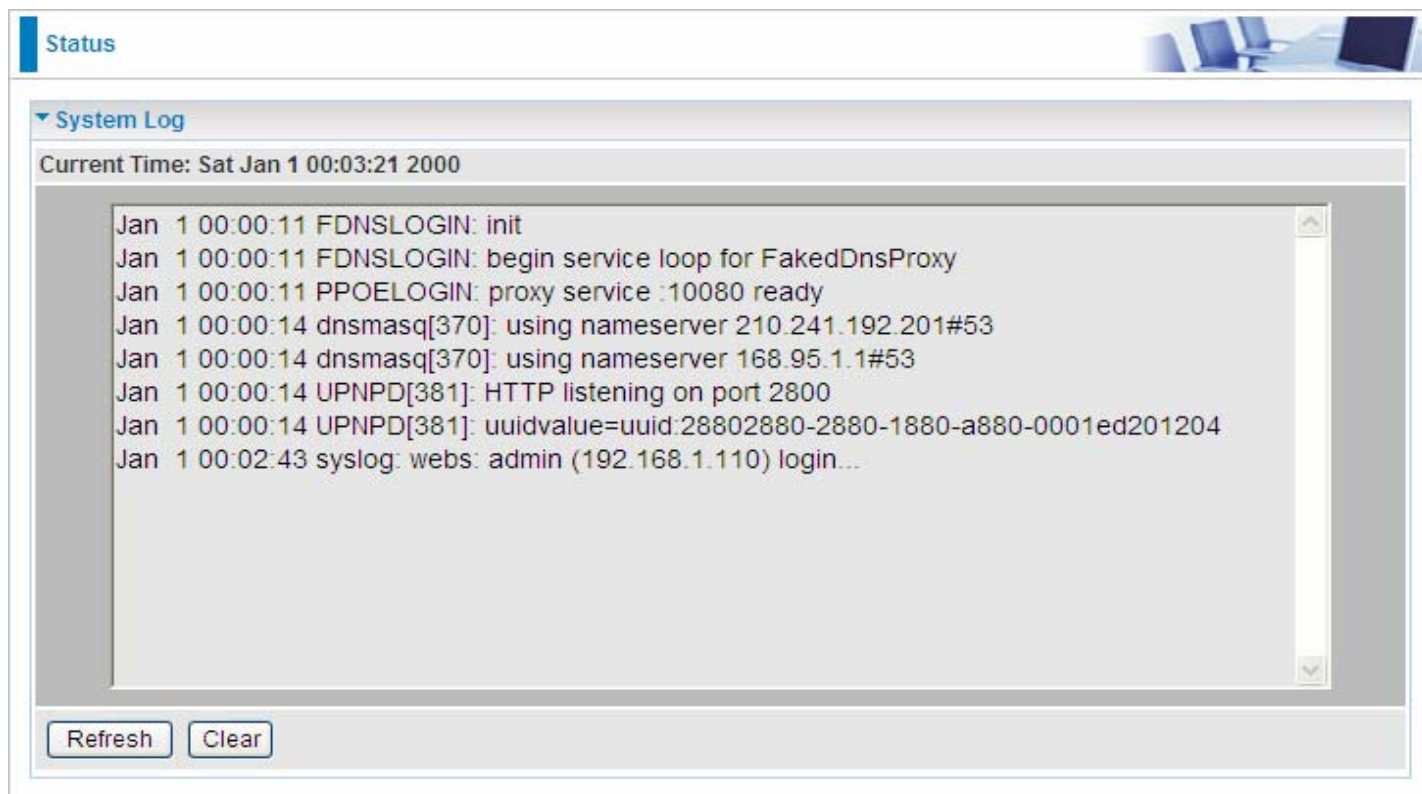
**MAC Address:** The MAC Address of internal DHCP client host.

**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.



## 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.



# 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.

Status

UPnP Portmap

Table

Name	Protocol	External Port	Internal Port	IP Address
------	----------	---------------	---------------	------------

**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

## 3G

Quick Start

▼ WAN Port ( WAN > Wireless )

Select WAN Port

Connect Mode

3G (Recommended) ▼

TEL No.

\*99\*\*\*1#

Username

APN

internet

Continue

Jump to Wireless setting

### 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

Quick Start

▼ WAN Port ( WAN > Wireless )

Select WAN Port

Connect Mode

EWAN (Recommended) ▼

Protocol

Obtain an IP Address Automatically

Continue

Jump to Wireless setting

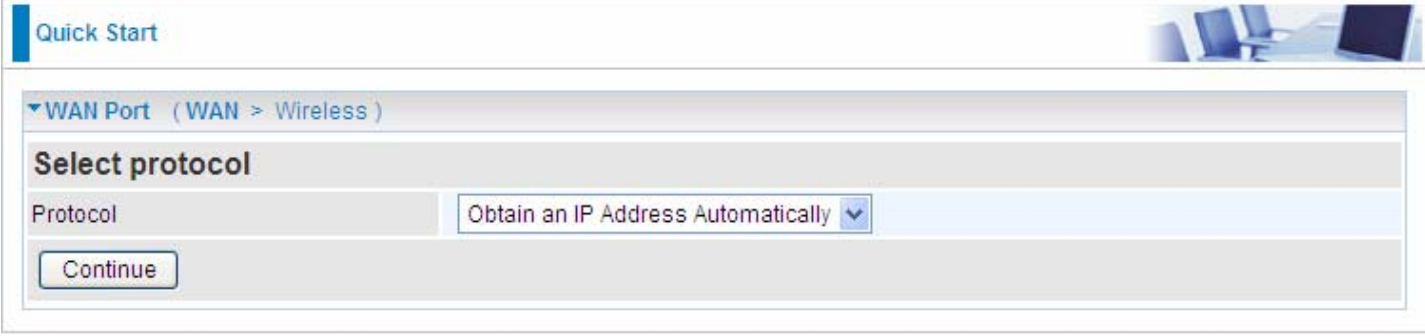
### Connect mode: EWAN

**Protocol:** The current protocol in the device.

Click on **Continue** to choose the Protocol to connect with EWAN or click **Jump to Wireless Setting** to use 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, PowerTracker/Billion SMART ENERGY GATEWAY also functions as a DHCP client. PowerTracker/Billion SMART ENERGY GATEWAY can automatically obtain an IP address, subnet mask, gateway address, and DNS server addresses if the ISP assigns this information via DHCP.



Quick Start

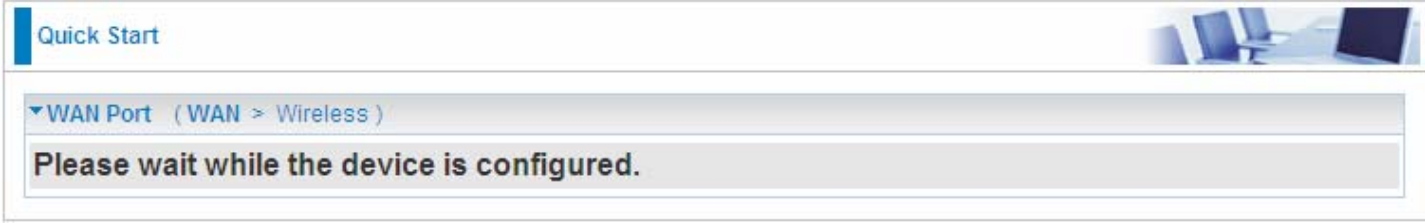
▼ WAN Port ( WAN > Wireless )

**Select protocol**

Protocol

**Protocol:** The current protocol in the device

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




Quick Start

▼ WAN Port ( WAN > Wireless )

**Please wait while the device is configured.**

If connection is successful the following image will be shown.



Quick Start

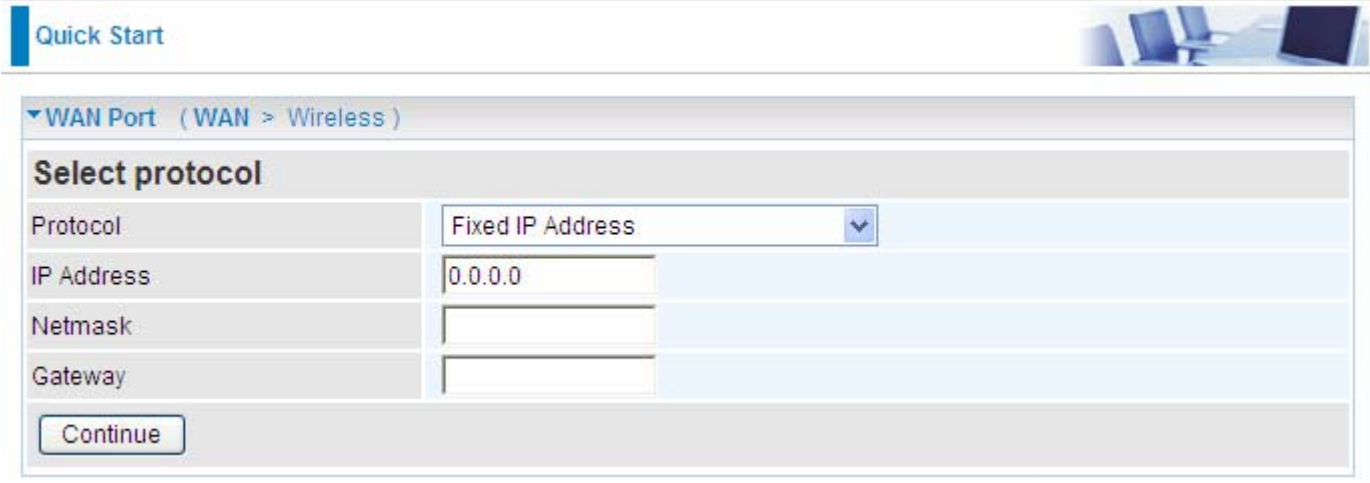
▼ WAN Port ( WAN > Wireless )

**Congratulations !**

Your WAN port has been successfully configured.

## 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.



Quick Start

▼ WAN Port ( WAN > Wireless )

**Select protocol**

Protocol	Fixed IP Address
IP Address	0.0.0.0
Netmask	
Gateway	

Continue

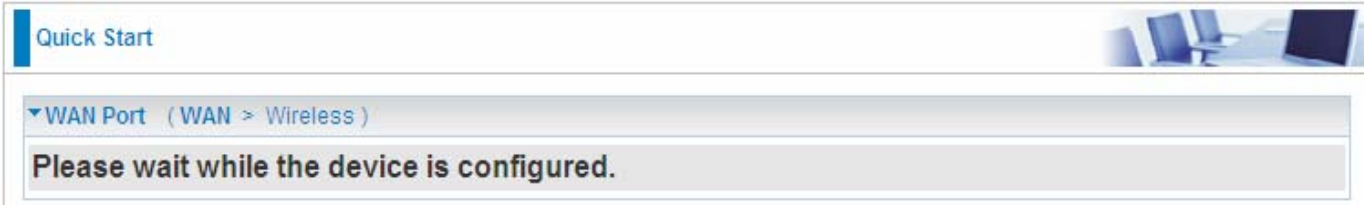
**Protocol:** The current ATM protocol in the device

**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.




Quick Start

▼ WAN Port ( WAN > Wireless )

**Please wait while the device is configured.**

If connection is successful the following image will be shown.



Quick Start

▼ WAN Port ( WAN > Wireless )

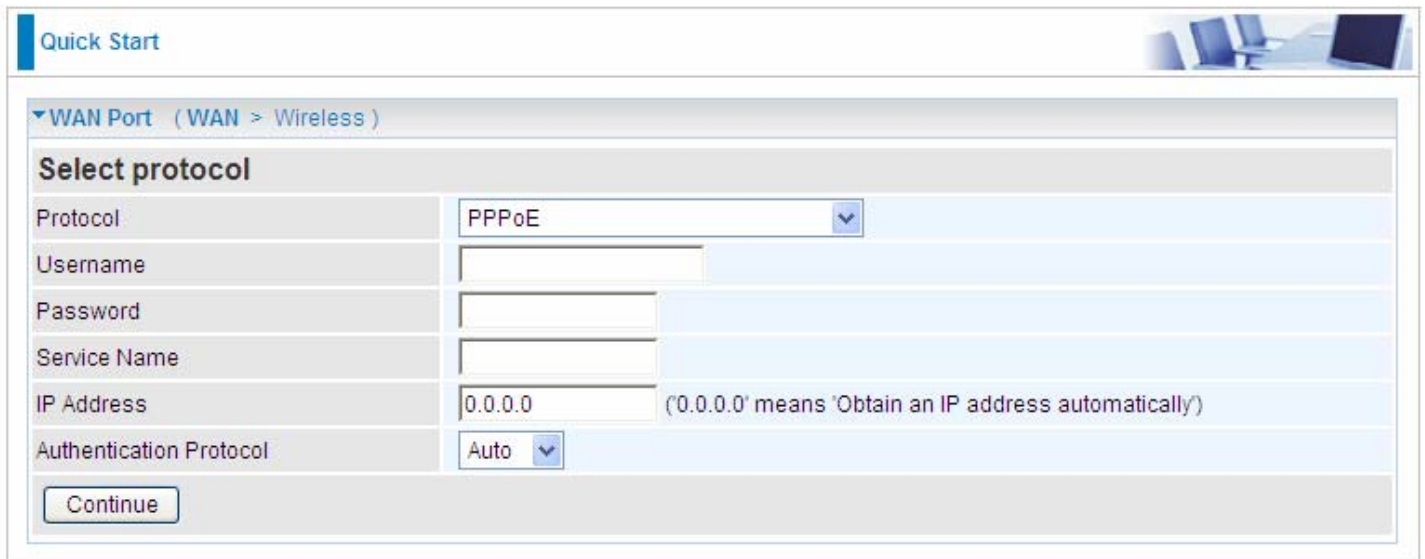
**Congratulations !**

Your WAN port has been successfully configured.

Next to Wireless

## PPPoE

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



Quick Start

▼ WAN Port ( WAN > Wireless )

**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”.

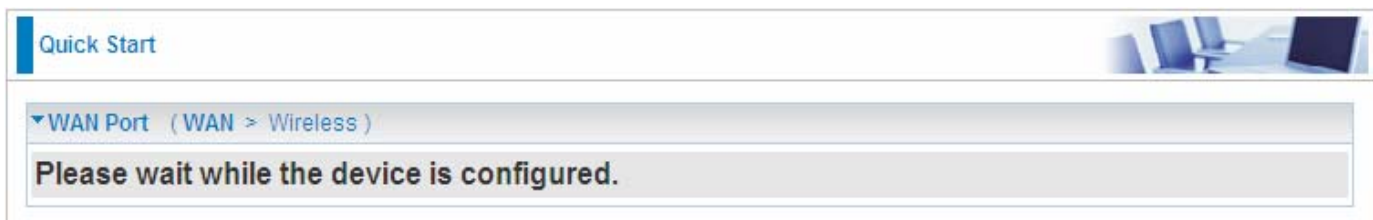
**Password:** Enter the password provided by your ISP. You can input up to 128 alphanumeric characters (case sensitive).

**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 )

**Please wait while the device is configured.**

If connection is successful the following image will be shown.



Quick Start

▼ WAN Port ( WAN > Wireless )

**Congratulations !**

Your WAN port has been successfully configured.

Next to Wireless

## Set Wireless configuration

Quick Start

▼ Wireless ( WAN > Wireless )

Set Wireless configuration.

WLAN Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
ESSID	<input type="text" value="wlan-ap"/>
Channel ID	<input type="button" value="Channel 1 (2.412 GHz)"/> ▼
Security Mode	<input type="button" value="Disable"/> ▼

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 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.

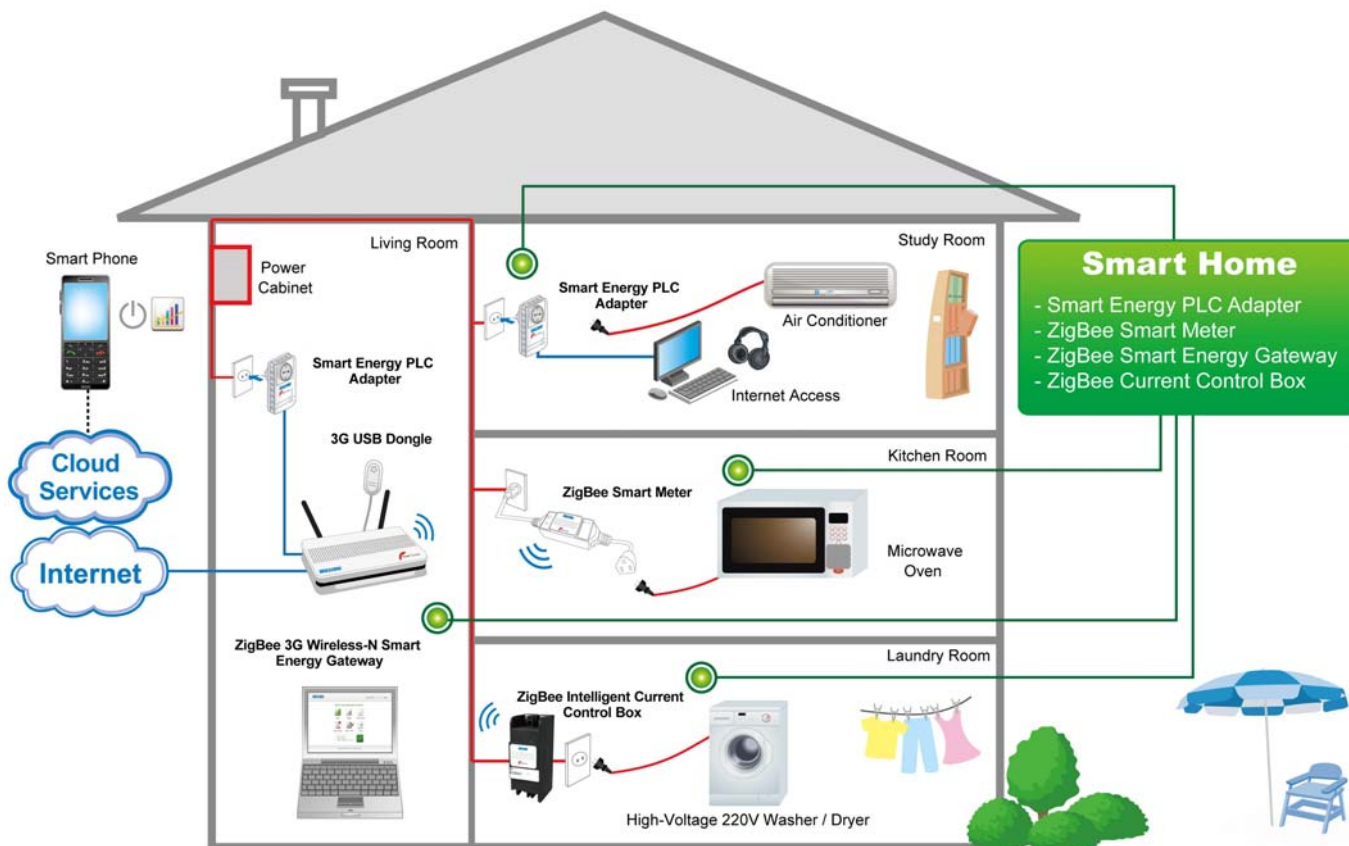
**Channel ID:** Select the ID channel that you would like to use.

**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.

# Power Management

In Smart Meter Serial products, PowerTracker/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.

See [User Management](#).

## ZigBee 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.)

PowerTracker/Billion SG2097 Smart Energy PLC Adapter

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

Power Management

**ZigBee Config**

Parameters

Allow Join

Scan Meter  (☐ show non-meter device)

Meter List	Alias	Display Order	Remove
000D6F00007343E1	N/A	<input type="button" value="v"/>	<input type="button" value="Identify"/> <input type="button" value="Remove"/>
000D6F00008E3129	N/A	<input type="button" value="v"/>	<input type="button" value="Identify"/> <input type="button" value="Remove"/>

[(SG2097 connected)]

**ZigBee Config**

Parameters

Allow Join

Scan Meter  (☐ show non-meter device)

Meter List	Alias	Display Order	Remove
000D6F00004DC114	FAN	1 <input type="button" value="v"/>	<input type="button" value="Identify"/> <input type="button" value="Remove"/>
192.168.1.250	Laptop	2 <input type="button" value="v"/>	<input type="button" value="Identify"/> <input type="button" value="Remove"/>
192.168.1.251	Lamp	3 <input type="button" value="v"/>	<input type="button" value="Identify"/> <input type="button" value="Remove"/>

ZigBee Meter is MAC base. (000D6F00004DC114)

SG2097 is IP base. (192.168.1.250 and 192.168.1.251), if user use SG2097, you can see the figure shown above, here we just take the common meter ZigBee Meter for example]

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

**Scan:** Show all alive smart Meters.

**SmartMeter:** Display the unique identification of each PowerTracker/Billion SmartMeter.

**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 SMART ENERGY GATEWAY gateway, set the parameters as follows. Then click **Apply** to save. Now you have finished **ZigBee Config**.

Power Management

ZigBee Config

Parameters

Allow Join

Start

Scan Meter

Scan

(☐ show non-meter device )

Meter List

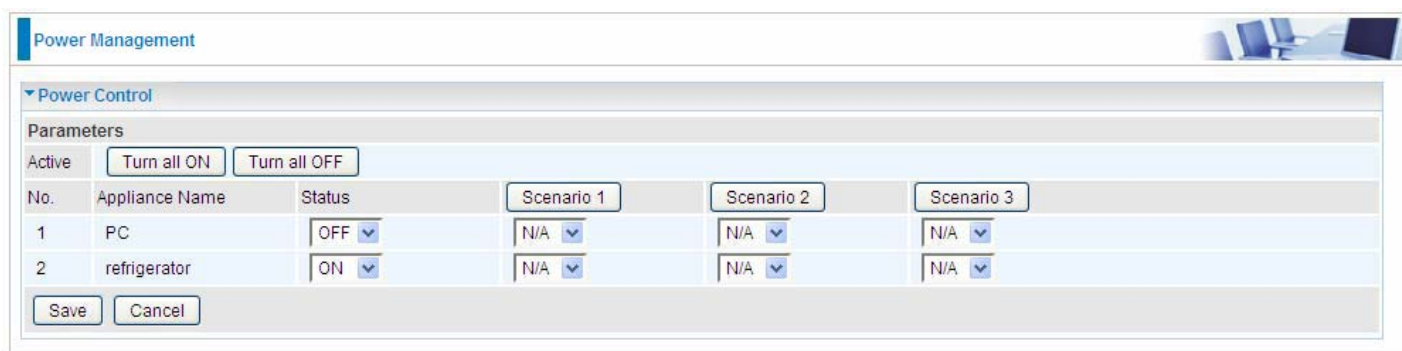
Alias	Display Order	Remove
000D6F00007343E1 refrigerator	2	Identify Remove
000D6F00008E3129 PC	1	Identify Remove

Apply

Cancel

## Power Control

In this section, you can control your home devices' on or off via SG6200NXL gateway remotely to achieve home automation.



Power Management

Power Control

Parameters

Active:

No.	Appliance Name	Status	Scenario 1	Scenario 2	Scenario 3
1	PC	OFF	N/A	N/A	N/A
2	refrigerator	ON	N/A	N/A	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 **ZigBee 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	PC	ON	OFF
2	refrigerator	OFF	ON

## ZigBee step by step configuration

1. Connect the SmartMeter and the end device.



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

The screenshot shows a web interface titled "Power Management" with a sub-tab "ZigBee Config". Under "Parameters", there are buttons for "Allow Join" (labeled "Start") and "Scan Meter" (labeled "Scan"). Next to "Scan Meter" is a checkbox labeled "show non-meter device". Below this is a "Meter List" table with columns for "Meter List", "Alias", "Display Order", and "Remove".

Meter List	Alias	Display Order	Remove
000D6F00007343E1	N/A	▼	Identify Remove
000D6F00008E3129	N/A	▼	Identify Remove

At the bottom of the table are "Apply" and "Cancel" buttons.

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.

Click allow Join **Start**, when Status LED lights, press  for 3~5 seconds until the **Status** LED blinks, which indicates that the device is connected to ZigBee network and When connected, the above screenshot will appear.



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

**Power Management**

**ZigBee Config**

Parameters

Allow Join:

Scan Meter:  (☐ show non-meter device)

Meter List	Alias	Display Order	Remove
000D6F00007343E1	refrigerator	2	<input type="button" value="Identify"/> <input type="button" value="Remove"/>
000D6F00008E3129	PC	1	<input type="button" value="Identify"/> <input type="button" value="Remove"/>

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

**Power Management**

**Power Control**

Parameters

Active:

No.	Appliance Name	Status	Scenario 1	Scenario 2	Scenario 3
1	PC	OFF	N/A	N/A	N/A
2	refrigerator	ON	N/A	N/A	N/A

- 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.

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

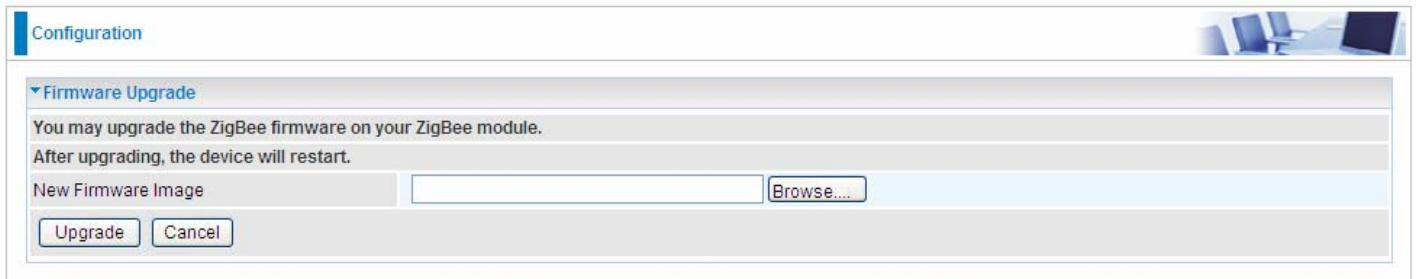
- If you want to turn on the PC and turn off the refrigerator sometime, you can make a scenario, such as scenario1, set as follows.

No.	Appliance Name	Status	Scenario 1
1	PC	ON	ON
2	refrigerator	ON	OFF

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

## ZigBee Firmware

“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, the 'Firmware Upgrade' section is expanded, showing instructions: 'You may upgrade the ZigBee firmware on your ZigBee module. After upgrading, the device will restart.' There is a text input field labeled 'New Firmware Image' and a 'Browse....' button next to it. At the bottom of the section are 'Upgrade' and 'Cancel' buttons.

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.

## ZigBee API Settings

In this part, users can set to deliver all the meter status information (Power, Voltage, Current, etc) to a specified server for easy view.

Configuration

▼ ZigBee API Configuration

Parameters

Enable	<input checked="" type="checkbox"/> Enable
Server Name	api.powertracker.com.a
Port	80
HTTP POST Interval(mins)	1
Index Page	index.php
Historical Interval(mins)	1

Apply

**Server Name:** The server URL or address.

**Port:** The access port.

**HTTP POST Interval:** unit: min. if set to 1, the information of the meters will be sent to the server every 1 min.

**Index Page:** The default index page.

**Historical Interval:** The frequency of the upgrade of the meters' information, when set to 1, the upgrade will be done every 1 min.

# Configuration

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

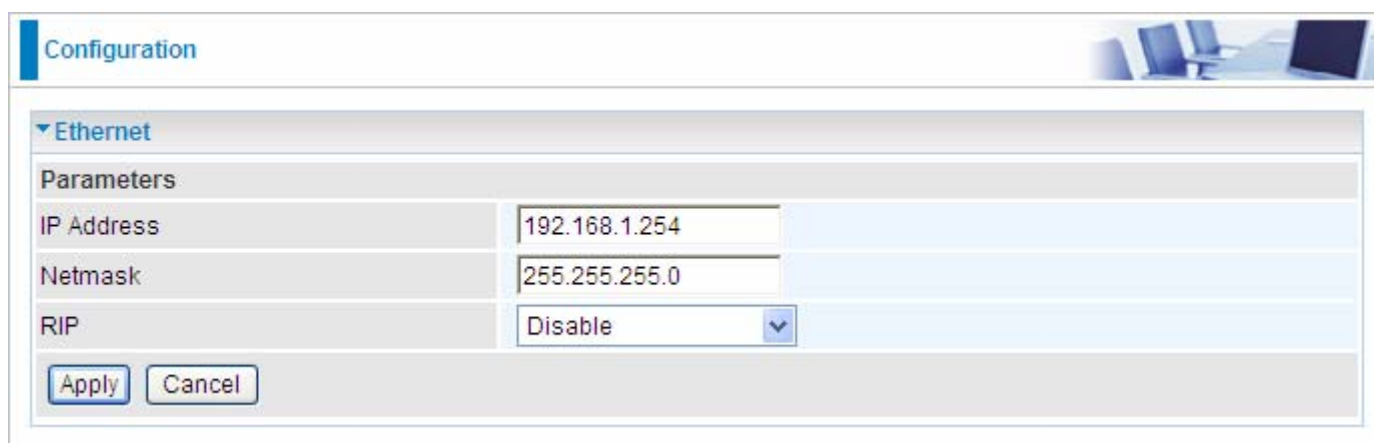
These functions are described in the following sections.

## 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



The screenshot shows a web-based configuration interface for a router. At the top, there is a 'Configuration' tab. Below it, the 'Ethernet' section is expanded. Under 'Parameters', there are three fields: 'IP Address' with the value '192.168.1.254', 'Netmask' with the value '255.255.255.0', and 'RIP' with a dropdown menu set to 'Disable'. At the bottom of the form are 'Apply' and 'Cancel' buttons.

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 192.168.100.254.

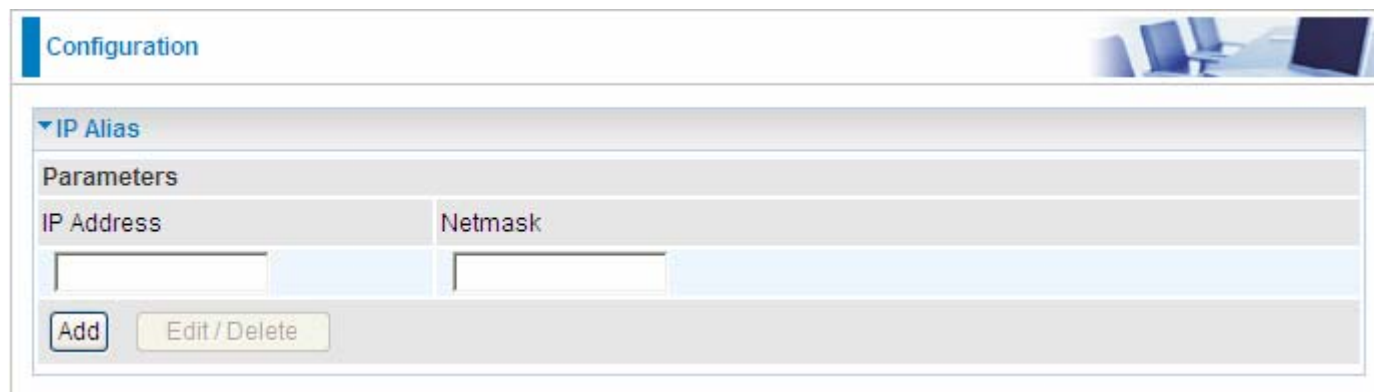
**IP Address:** The default IP on this router.

**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.



The screenshot shows a web-based configuration interface for a router. At the top, there is a 'Configuration' tab. Below it, the 'IP Alias' section is expanded. Under 'Parameters', there are two columns: 'IP Address' and 'Netmask'. Below these columns are two empty input fields. At the bottom of the form are 'Add' and 'Edit / Delete' buttons.

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

**Netmask:** Specify a subnet mask on this virtual interface.

## Wireless

Configuration

Wireless

Parameters

WLAN Service

☒ Enable ☐ Disable

Mode

802.11g + n

Number of Active SSID

1

SSID No.

☒ SSID1

ESSID

wlan-ap

Hide ESSID

☐ Enable ☒ 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

☐ Enable ☒ Disable

WPS State

☐ Configured ☒ Unconfigured

WMM

☐ Enable ☒ Disable

Wireless Distribution System (WDS)

WDS Service

☐ Enable ☒ Disable

Peer WDS MAC address

1.

2.

3.

4.

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

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

57

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**.

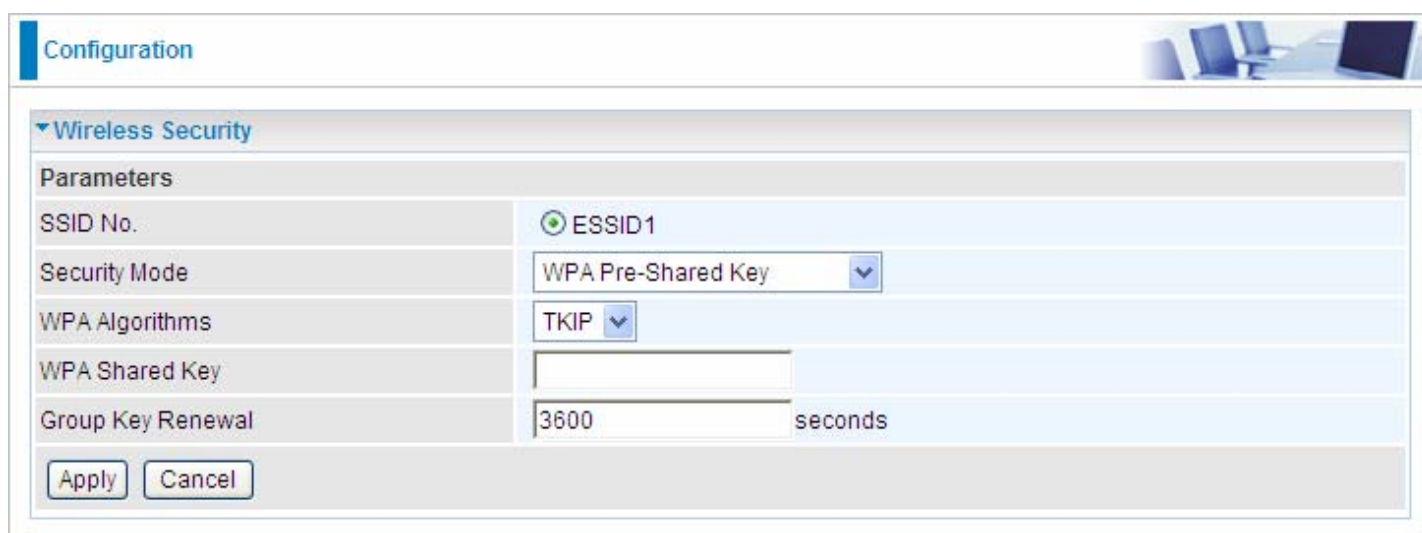


The screenshot shows a web interface for configuring wireless security. At the top, there's a 'Configuration' tab. Below it, the 'Wireless Security' section is expanded. Under 'Parameters', the 'SSID No.' is set to 'ESSID1' with a radio button. The 'Security Mode' is set to 'Disable' in a dropdown menu. At the bottom, there are 'Apply' and 'Cancel' buttons.

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

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

### WPA Pre-Shared Key



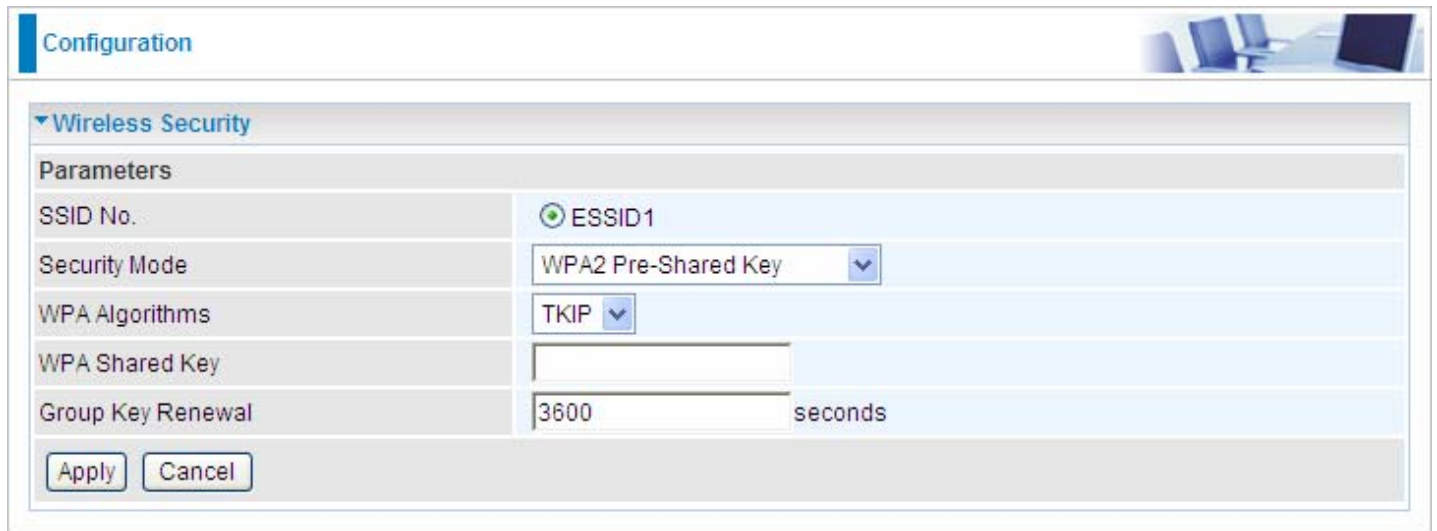
This screenshot shows the 'Wireless Security' configuration page with 'WPA Pre-Shared Key' selected in the 'Security Mode' dropdown. The 'WPA Algorithms' dropdown is set to 'TKIP'. The 'WPA Shared Key' is an empty text field. The 'Group Key Renewal' is set to '3600 seconds'. 'Apply' and 'Cancel' buttons are 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 web-based configuration interface for wireless security. The 'Configuration' tab is active. Under the 'Wireless Security' section, the 'Parameters' table is displayed. The 'SSID No.' is set to 'ESSID1'. The 'Security Mode' is set to 'WPA2 Pre-Shared Key'. The 'WPA Algorithms' are set to 'TKIP'. The 'WPA Shared Key' field is empty. The 'Group Key Renewal' is set to '3600 seconds'. At the bottom, there are 'Apply' and 'Cancel' buttons.

Parameters	
SSID No.	ESSID1
Security Mode	WPA2 Pre-Shared Key
WPA Algorithms	TKIP
WPA Shared Key	
Group Key Renewal	3600 seconds

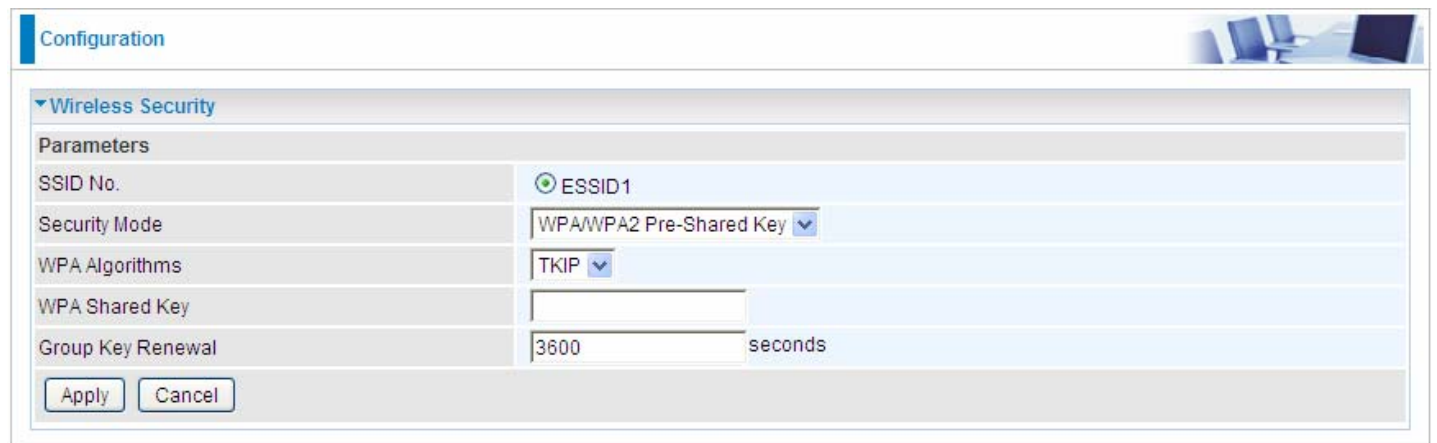
Apply Cancel

**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 web-based configuration interface for wireless security. The 'Configuration' tab is active. Under the 'Wireless Security' section, the 'Parameters' table is displayed. The 'SSID No.' is set to 'ESSID1'. The 'Security Mode' is set to 'WPA/WPA2 Pre-Shared Key'. The 'WPA Algorithms' are set to 'TKIP'. The 'WPA Shared Key' field is empty. The 'Group Key Renewal' is set to '3600 seconds'. At the bottom, there are 'Apply' and 'Cancel' buttons.

Parameters	
SSID No.	ESSID1
Security Mode	WPA/WPA2 Pre-Shared Key
WPA Algorithms	TKIP
WPA Shared Key	
Group Key Renewal	3600 seconds

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).

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?lbd3ert.

**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"/>

Start

Cancel

## 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

☒ Enable

☐ Disable

Role

☒ Registrar

☐ 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

PIN

PBC

☒ 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

Extra Info >>

Channel >>

Authentication >>

Encryption >>

Network Type >>

IP Address >>

Sub Mask >>

Default Gateway >>

HT

BW >> n/a

GI >> n/a

MCS >> n/a

SNRO >> n/a

SNR1 >> n/a

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

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

**WPS AP List**

ID	SSID	MAC	Count
wlan-ap	00-1D-92-C0-13-CD	1	
wlan-ap	00-04-ED-38-F7-2E	1	

**WPS Profile List**

Profile
wlan-ap

**WPS Configuration**

PIN: ☐ WPS Associate IE ☒ WPS Probe IE

Progress >> 100%

PIN - Get WPS profile successfully.

**WPS AP Details**

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 Parameters**

Parameter	Value
BW	>> 40
GI	>> long
MCS	>> 15
SNR0	>> 19
SNR1	>> n/a

**Signal Strength Indicators**

Link Quality >> 100%

Signal Strength 1 >> 64%

Signal Strength 2 >> 34%

Noise Strength >> 26%

**Transmit Statistics**

Link Speed >> 270.0 Mbps

Throughput >> 5.600 Kbps

**Receive Statistics**

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

☒ Enable

☐ Disable

Role

☐ Registrar

☒ 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

PBC

☒ WPS Associate IE

☒ WPS Probe IE

Progress >> 0%

Rescan

Information

Pin Code

25879810

Renew

Config Mode

Registrar

Detail

Connect

Rotate

Disconnect

Export Profile

Status >> Disconnected

Extra Info >>

Channel >>

Authentication >>

Encryption >>

Network Type >>

IP Address >>

Sub Mask >>

Default Gateway >>

HT

BW >> n/a

GI >> n/a

MCS >> n/a

SNR0 >> n/a

SNR1 >> n/a

Link Quality >> 0%

Signal Strength 1 >> 0%

Signal Strength 2 >> 0%

Noise Strength >> 0%

Transmit

Link Speed >>

Throughput >>

Receive

Link Speed >>

Throughput >>

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

←

Profile

Network

Advanced

Statistics

WMM

WPS

Radio On/Off

About

→

WPS AP List

ID :	ExRegNWEA4036	00-1D-92-C0-13-CD	1	🔑
ID :	wlan-ap	00-04-ED-38-F7-2E	1	

WPS Profile List

ExRegNWEA4036

PIN

PBC

☒ WPS Associate IE

☒ WPS Probe IE

Progress >> 100%

PIN - Get WPS profile successfully.

Rescan

Information

Pin Code

25879810

Renew

Config Mode

Registrar

Detail

Connect

Rotate

Disconnect

Export Profile

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

BW >> 40

GI >> long

MCS >> 14

SNRO >> 20

SNR1 >> n/a

Link Quality >> 100%

Signal Strength 1 >> 65%

Signal Strength 2 >> 39%

Noise Strength >> 26%

Transmit

Link Speed >> 243.0 Mbps

Throughput >> 0.000 Kbps

Receive

Link Speed >> 40.5 Mbps

Throughput >> 98.612 Kbps

Max

5,392 Kbps

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.

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-22-22-23	1

WPS Profile List

ExRegNWEA4036

PIN

PBC

☒ WPS Associate IE

☒ WPS Probe IE

Progress >> 0%

WPS status is disconnected

Rescan

Information

Pin Code

25879810

Renew

Config Mode

Registrar

Detail

Connect

Rotate

Disconnect

Export Profile

SSID >>

ExRegNWEA4036

BSSID >>

00-00-00-00-00-00

Authentication Type >>

WPA2-PSK

Encryption Type >>

AES

Key Length >>

5

Key Index >>

1

Key Material >>

811B5B9F3403DCB08BA73BF3E4787581C37DC4BDD147C4E62526D4E8C39D8F78

☒ Show Password

OK

Cancel

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

Configuration

▼ Wireless

Parameters

WLAN Service

☒ Enable ☐ Disable

Mode

802.11g + n

Number of Active SSID

1

SSID No.

☒ SSID1

ESSID

wlan-ap

Hide ESSID

☐ Enable ☒ 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

☒ Enable ☐ Disable

WPS State

☒ Configured ☐ Unconfigured

WMM

☐ Enable ☒ Disable

Wireless Distribution System (WDS)

WDS Service

☐ Enable ☒ Disable

Peer WDS MAC address

1.

2.

3.

4.

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

Apply

Cancel

Security settings ▶

Configuration

▼ Wireless Security

Parameters

SSID No.

☒ ESSID1

Security Mode

WPA2 Pre-Shared Key

WPA Algorithms

AES

WPA Shared Key

811B5B9F3403DCB08I

Group Key Renewal

3600

seconds

Apply

Cancel

68

**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.

←

Profile

Network

Advanced

Statistics

WMM

**WPS**

Radio On/Off

About

→

WPS AP List

ID :	wlan-ap	00-04-ED-00-00-01	1
ID : 0x0004	wlan-ap	00-1D-92-C0-13-CD	1

WPS Profile List

PIN

PBC

☒ 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

Extra Info >>

Channel >>

Authentication >>

Encryption >>

Network Type >>

IP Address >>

Sub Mask >>

Default Gateway >>

HT

BW >> n/a

GI >> n/a

MCS >> n/a

SNR0 >> n/a

SNR1 >> n/a

Link Quality >> 0%

Signal Strength 1 >> 0%

Signal Strength 2 >> 0%

Noise Strength >> 0%

Transmit

Link Speed >>

Throughput >>

8.800 Kbps

Receive

Link Speed >>

Throughput >>

147.408 Kbps

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.

←

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

PIN

PBC

☒ WPS Associate IE

☒ WPS Probe IE

Progress >> 100%

PBC - Get WPS profile successfully.

Rescan

Information

Pin Code

16837546

Renew

Config Mode

Enrollee

Detail

Connect

Rotate

Disconnect

Export Profile

Delete

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

BW >> 40

GI >> long

MCS >> 14

SNRU >> 20

SNR1 >> n/a

Link Quality >> 100%

Signal Strength 1 >> 60%

Signal Strength 2 >> 44%

Noise Strength >> 26%

Transmit

Link Speed >> 243.0 Mbps

Throughput >> 0.192 Kbps

Receive

Link Speed >> 81.0 Mbps

Throughput >> 93.732 Kbps

## 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"/>

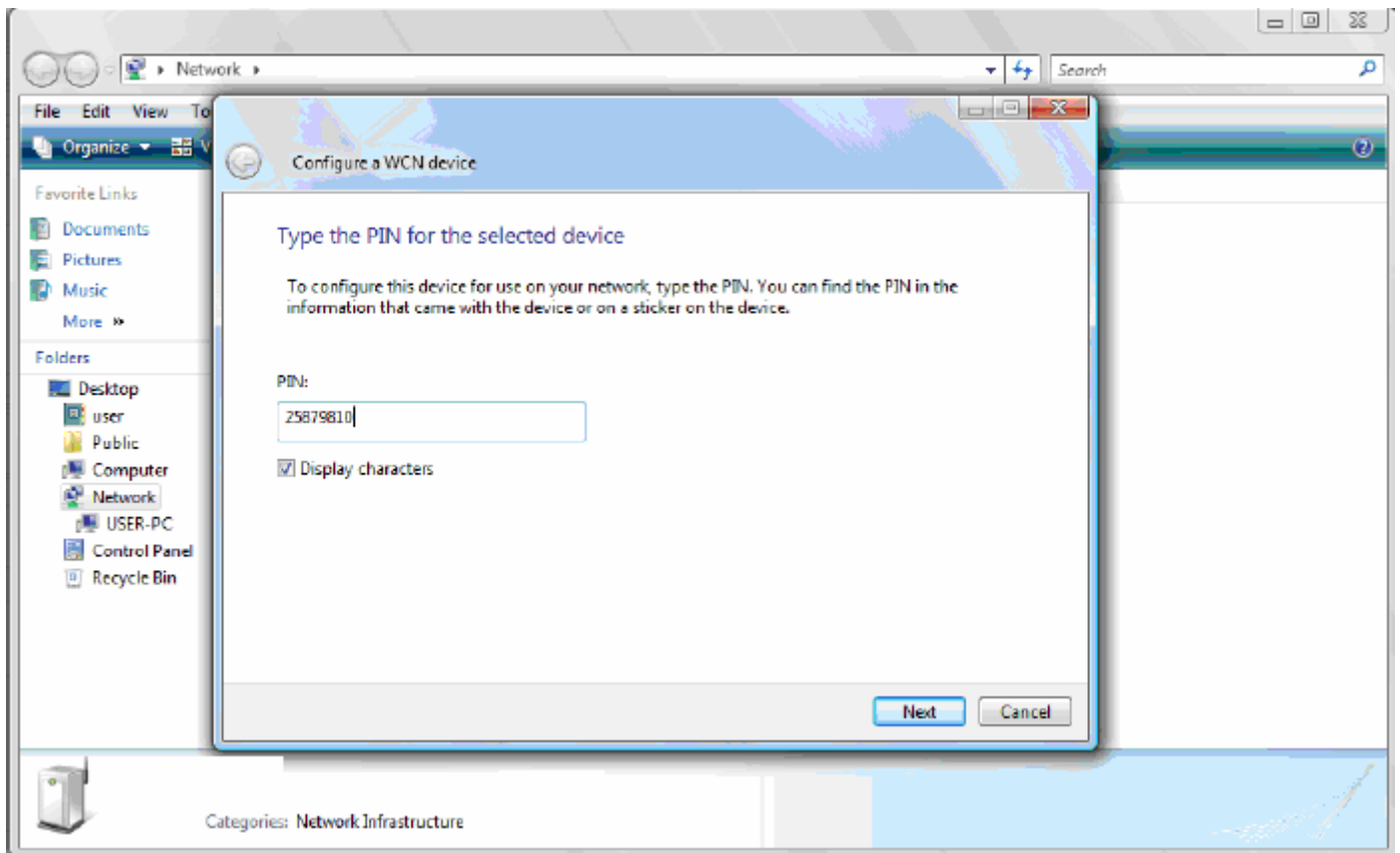
\*\* WDS depends on the settings of main security encryption type. \*\*

Apply

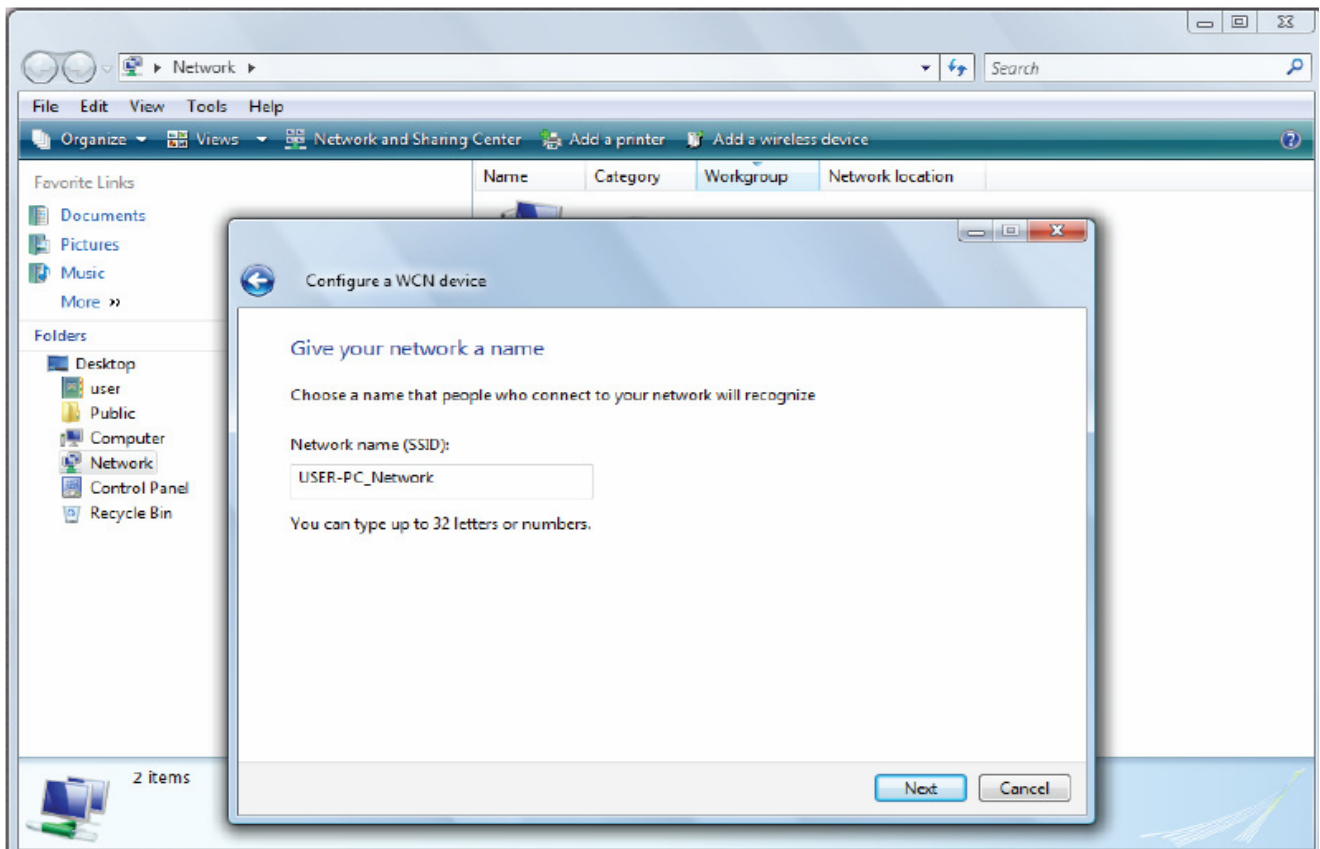
Cancel

Security settings ▶

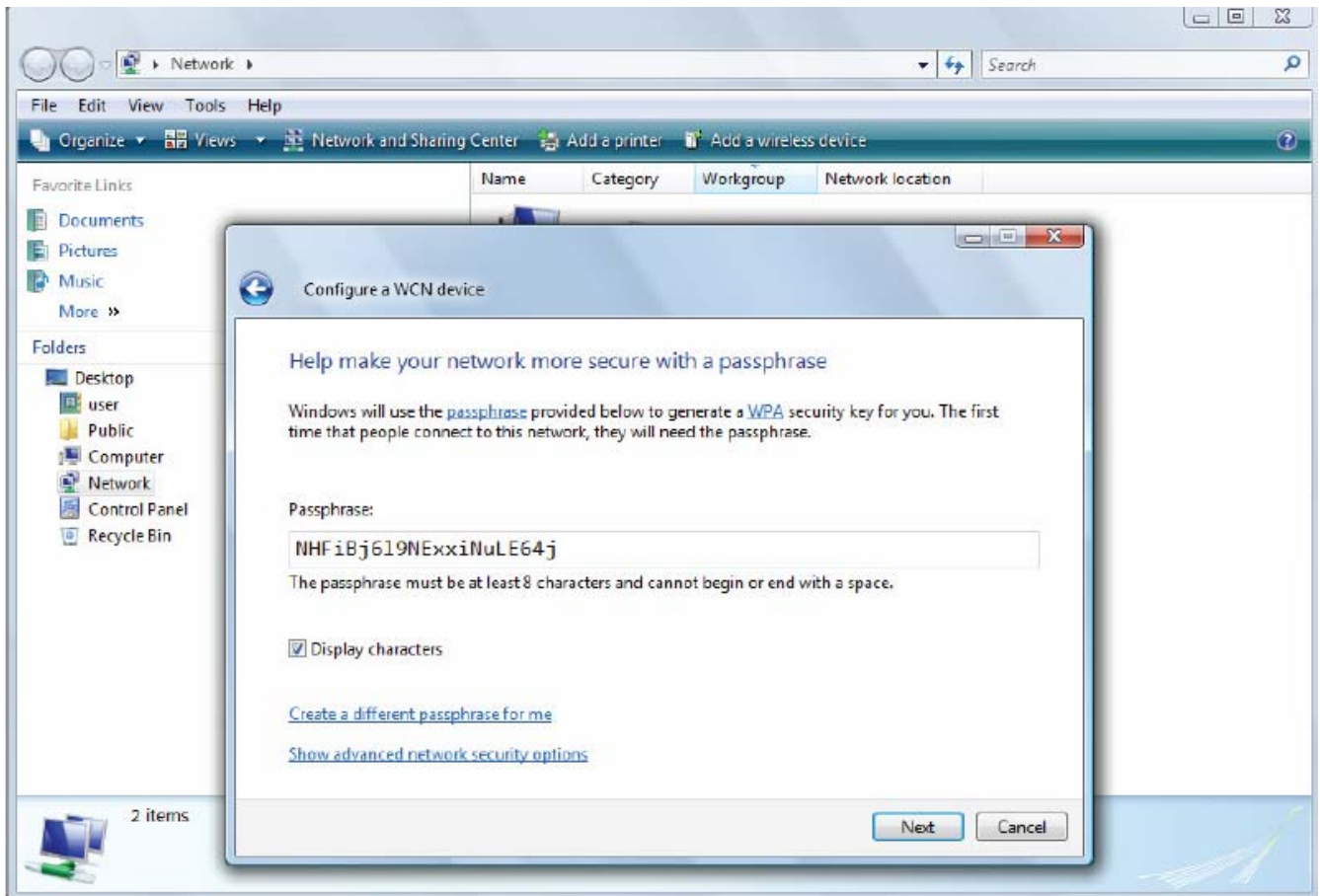
3. In your Vista operating system, access the Control Panel page, then select Network and Internet > View Network Computers and Devices. Double click on the router icon and enter the AP PIN in the column provided then press Next.



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 192.168.100.254).

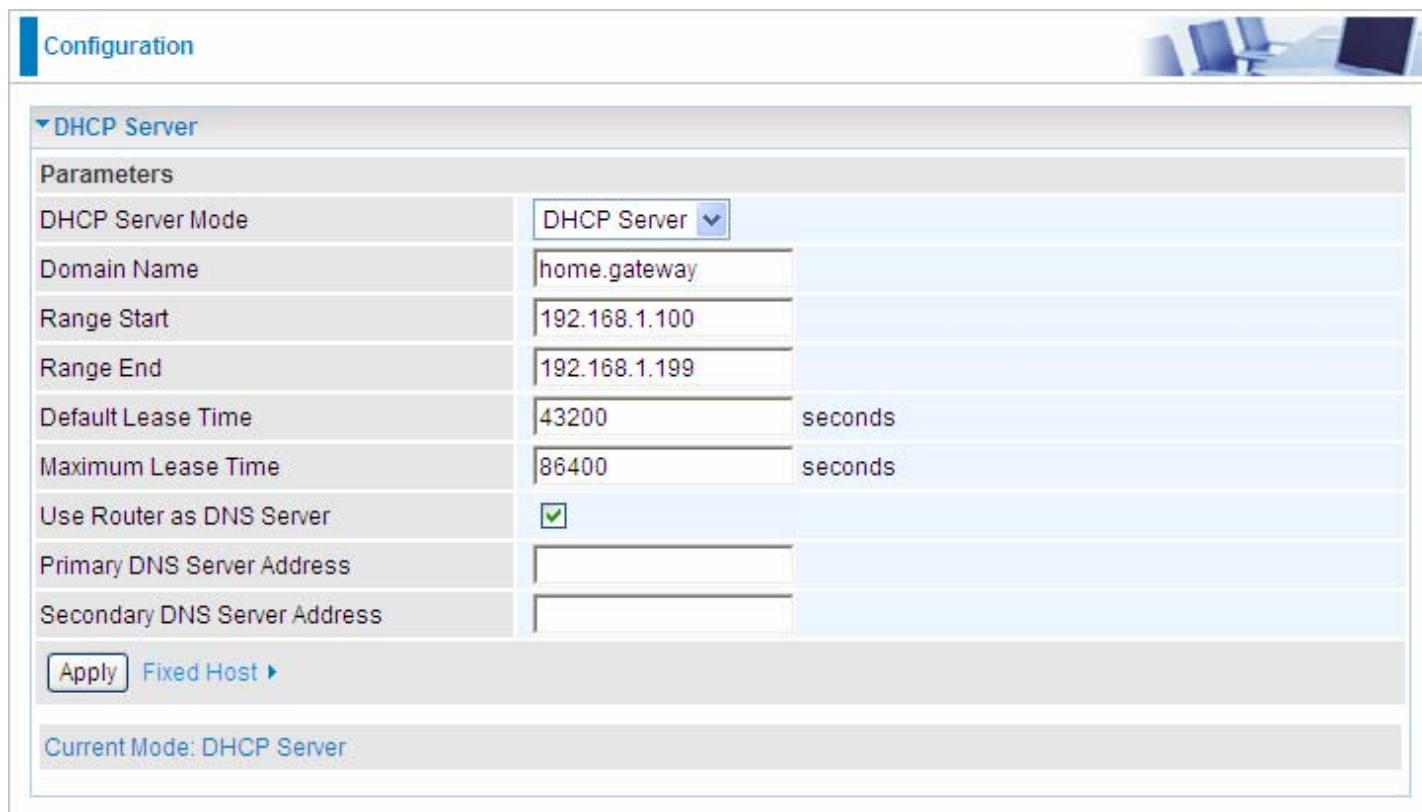


The screenshot shows a web-based configuration interface for a DHCP Server. At the top, there is a 'Configuration' tab. Below it, the 'DHCP Server' section is expanded, showing a 'Parameters' subsection. The 'DHCP Server Mode' is set to 'Disable' in a dropdown menu. An 'Apply' button is visible below the dropdown. At the bottom of the section, it says 'Current Mode: DHCP Server'.

Configuration	
▼ DHCP Server	
Parameters	
DHCP Server Mode	Disable ▼
<input type="button" value="Apply"/>	
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).



Configuration

▼ DHCP Server

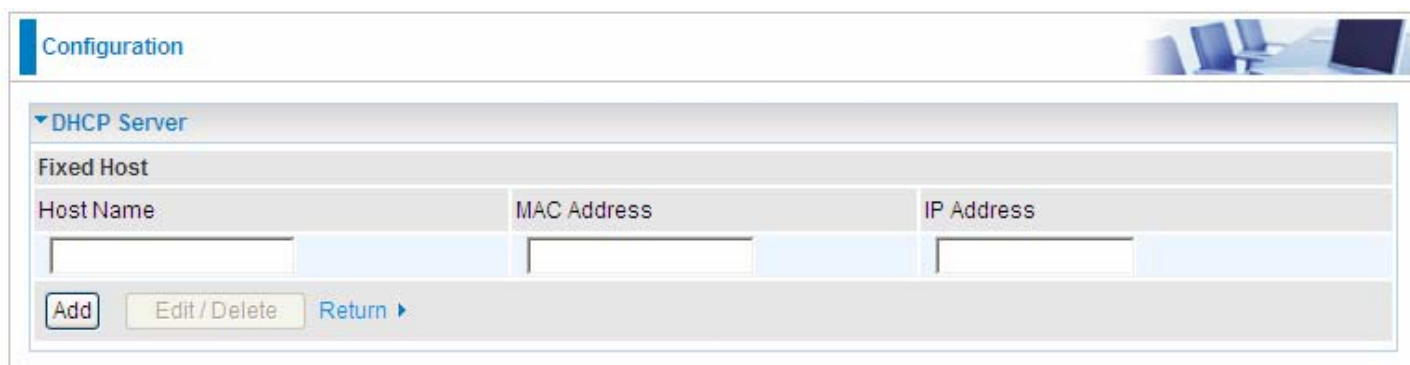
Parameters

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.



Configuration

▼ DHCP Server

Fixed Host

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

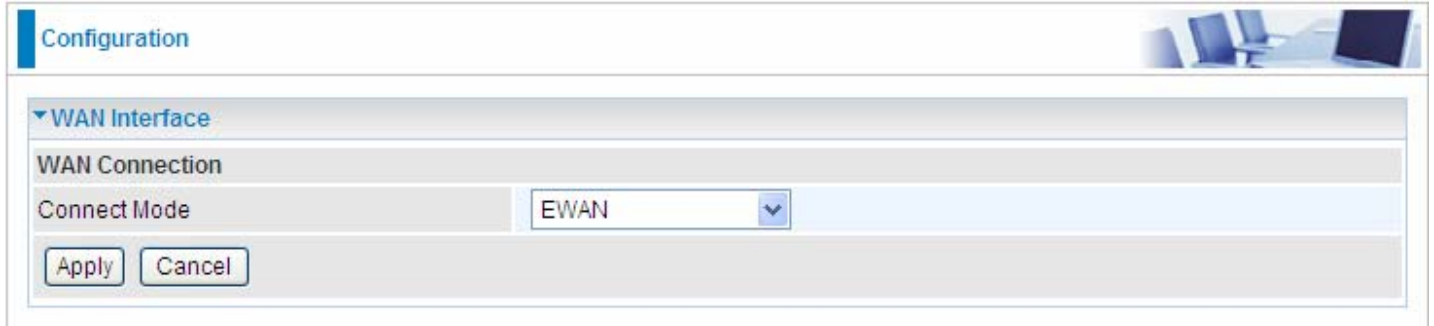
Apply

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)

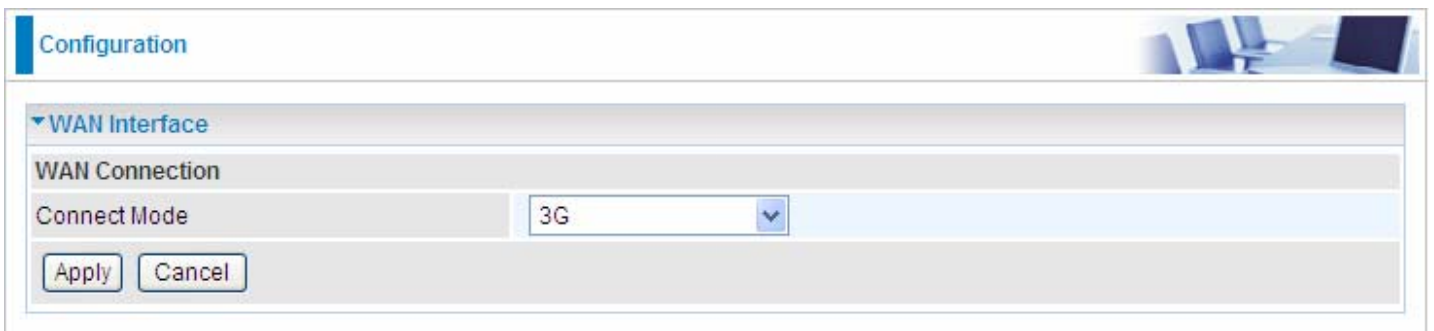


The screenshot shows a configuration window titled "Configuration" with a sub-section "WAN Interface". Under "WAN Connection", the "Connect Mode" is set to "EWAN" in a drop-down menu. At the bottom, there are "Apply" and "Cancel" buttons.

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

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" in a drop-down menu. At the bottom, there are "Apply" and "Cancel" buttons.

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

Click Apply to confirm the change.

# WAN Interface(APCLIENT)

In this mode, WAN interface serves as an AP client used to connect to other APs for Internet Access like commonly used wireless devices.

Configuration

▼ WAN Interface

WAN Connection

Connect Mode

APCLIENT

Apply

Cancel

## WAN Interface(Dual WAN)



The screenshot shows a web-based configuration interface for a WAN interface. The page is titled 'Configuration' and has a sub-section 'WAN Interface'. Under 'WAN Interface', there is a 'WAN Connection' section with a 'Connect Mode' dropdown set to 'Dual WAN(Failover)'. Below this is a 'Failover Parameters' section. It includes 'Main WAN' (EWAN) and 'Backup WAN' (3G), each with a link to its profile. The 'Probe' checkbox is checked. 'Connectivity Decision' is set to 'Not in service when probing failed after 3 consecutive times.' 'Failover Probe Cycle' is set to 'Every 12 seconds.' 'Failback Probe Cycle' is set to 'Every 4 seconds.' 'Detect Rule' has two options: 'Ping Gateway' (selected) and 'Ping Host' (unselected). At the bottom are 'Apply' and 'Cancel' buttons.

WAN Connection	
Connect Mode	Dual WAN(Failover)

Failover Parameters	
Main WAN	EWAN <a href="#">EWAN</a>
Backup WAN	3G <a href="#">3G</a>
Probe	<input checked="" type="checkbox"/> Enable
Connectivity Decision	Not in service when probing failed after 3 consecutive times.
Failover Probe Cycle	Every 12 seconds.
Failback Probe Cycle	Every 4 seconds.
Detect Rule	<input checked="" type="radio"/> Ping Gateway <input type="radio"/> Ping Host

Apply Cancel

**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.

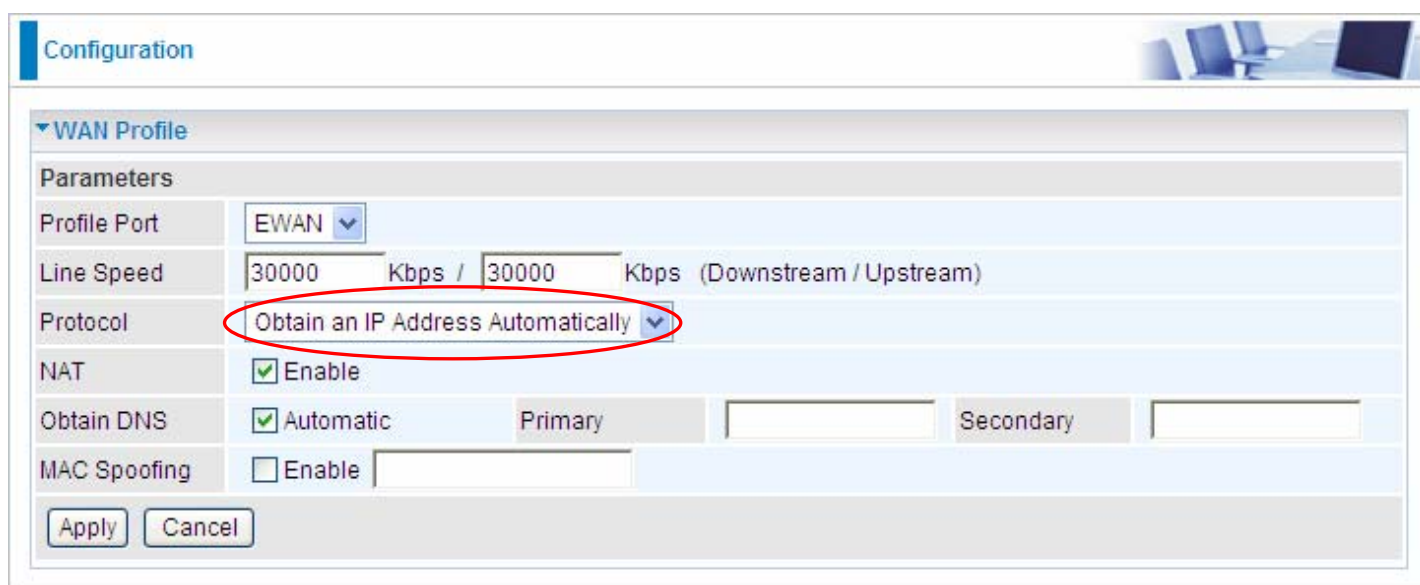
## WAN Profile

### Main Port – EWAN

PowerTracker/Billion SMART ENERGY GATEWAY 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, PowerTracker/Billion SMART ENERGY GATEWAY also functions as a DHCP client. PowerTracker/Billion SMART ENERGY GATEWAY can automatically obtain an IP address, Netmask, gateway address, and DNS server addresses if the ISP assigns this information via DHCP.



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

- Profile Port:** EWAN (selected from a dropdown)
- Line Speed:** 30000 Kbps / 30000 Kbps (Downstream / Upstream)
- Protocol:** Obtain an IP Address Automatically (selected from a dropdown and circled in red)
- NAT:** ☒ Enable
- Obtain DNS:** ☒ Automatic. Primary and Secondary fields are empty.
- MAC Spoofing:** ☐ Enable. The field is empty.

At the bottom are 'Apply' and 'Cancel' buttons.

**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.

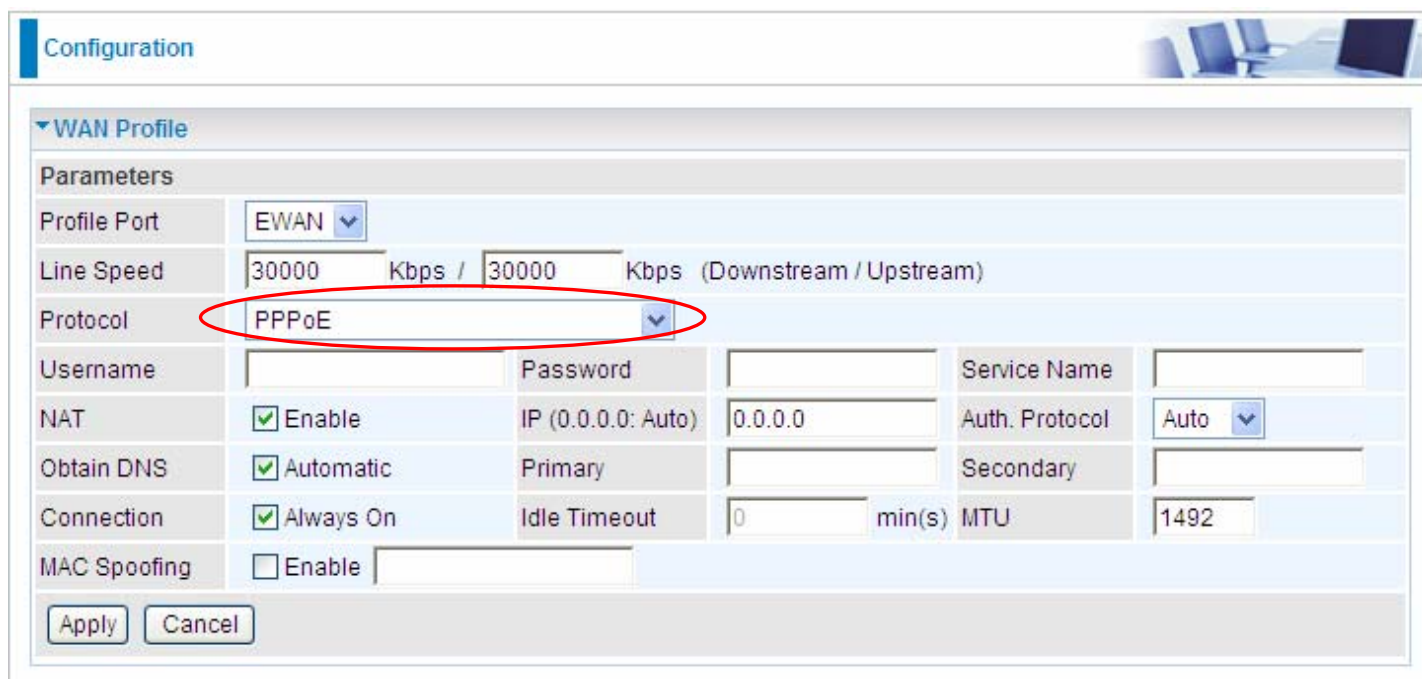
**Obtain DNS Automatically:** Select this check box to use DNS.

**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 a 'Configuration' window with a 'WAN Profile' section. Under 'Parameters', the 'Protocol' dropdown is highlighted with a red circle and set to 'PPPoE'. Other fields include 'Profile Port' (EWAN), 'Line Speed' (30000 Kbps / 30000 Kbps), 'Username', 'Password', 'Service Name', 'NAT' (checked), 'Obtain DNS' (checked), 'Connection' (checked), 'MAC Spoofing' (unchecked), 'IP (0.0.0.0: Auto)' (0.0.0.0), 'Auth. Protocol' (Auto), 'Primary' and 'Secondary' DNS fields, 'Idle Timeout' (0 min(s)), and 'MTU' (1492). 'Apply' and 'Cancel' buttons are at the bottom.

**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.

Configuration

▼ WAN Profile

Parameters

Profile Port: EWAN

Line Speed: 30000 Kbps / 30000 Kbps (Downstream / Upstream)

Protocol: Fixed IP Address

NAT: ☒ Enable

IP Address: 172.16.1.102 Netmask: 255.255.255.0 Gateway: 172.16.1.254

Obtain DNS: ☐ Automatic Primary: 172.16.1.254 Secondary: 172.16.1.240

MAC Spoofing: ☐ Enable

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)

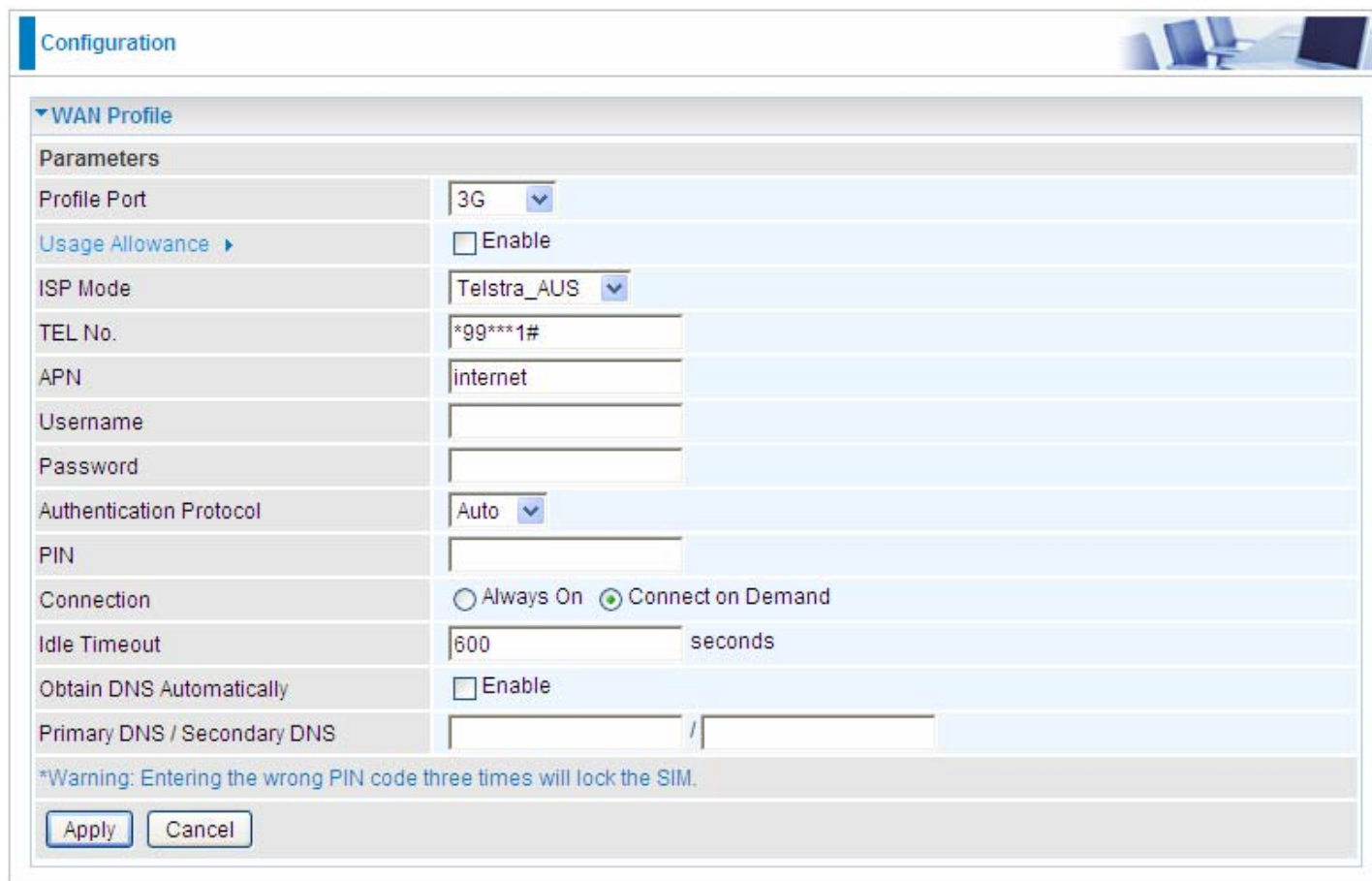
**Obtain DNS Automatically:** Select this check box to use DNS.

**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\*.



Configuration

▼ WAN Profile

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 ▶

☐ Enable

Configuration

▼ 3G Usage Allowance

Parameters

Mode

☒ Volume-based

Only Download

50

MB data volume per month included

☐ 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

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

☒ Volume-based

Only Download

50

MB data volume per month included

☐ Time-based

212

hours per month 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.

▼ 3G Usage Allowance

Parameters

Mode

☐

Volume-based

Only Download

▼

50

MB data volume per month included

☒

Time-based

212

hours per month included

The billing period always begins on day

12

of a month.

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.

E-mail Alert and Disconnect ▼

E-mail Alert

E-mail Alert and Disconnect

Disconnect

**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.

Every one hour ▼

Every one hour

Disable

## Main Port – APCLIENT

### Obtain an IP Address Automatically (APCLIENT)

Configuration

WAN Profile

Parameters

Main Port

APCLIENT

Protocol

Obtain an IP Address Automatically

NAT

☒ Enable

Obtain DNS

☒ Automatic

Primary

Secondary

SSID

Channel

1

Security Mode

OPEN

Encryption Type

None

Apply

Cancel

SCAN

Site Survey

Ch	SSID	BSSID	Security	Signal(%)	W-Moe	ExtCh	NT
6	wlan-ap4444	00:04:ed:01:23:45	NONE	24	11b/g/n	NONE	In
6	6300NXL5	00:04:ed:12:08:22	NONE	20	11b/g/n	NONE	In
9		00:04:ed:60:52:00	NONE	0	11b/g/n	ABOVE	In
9	billion-ap	00:04:ed:1e:37:7f	WPA2PSK/AES	55	11b/g	NONE	In

**NAT:** The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing a single IP address.

**Obtain DNS:** Automatically obtain the IP or enter the fixed DNS addresses.

**SSID:** User can specify the exact SSID you are already sure, or you can scan the APs active on the air and type the exact one in this field.

**Channel:** Select the channel, which should be consistent with your wireless AP.

**Security Mode:** Select the security mode according to the settings in your wireless AP.

**Encryption Type:** The encryption information should be consistent with the settings in your wireless AP.

## Fixed IP Address (APCLIENT)

Configuration

WAN Profile

Parameters

Main Port

APCLIENT

Protocol

Fixed IP Address

NAT

☒ Enable

IP Address

0.0.0.0

Netmask

Gateway

Obtain DNS

☐ Automatic

Primary

Secondary

SSID

Channel

1

Security Mode

OPEN

Encryption Type

None

Apply

Cancel

SCAN

Site Survey

Ch	SSID	BSSID	Security	Signal(%)	W-Moe	ExtCh	NT
6	wlan-ap4444	00:04:ed:01:23:45	NONE	29	11b/g/n	NONE	In
7	RT5390	00:1f:a4:91:87:6c	NONE	0	11b/g/n	BELOW	In
7	RT5390_4	00:1f:a4:91:87:6f	NONE	0	11b/g/n	BELOW	In
9	billion-ap	00:04:ed:1e:37:7f	WPA2PSK/AES	55	11b/g	NONE	In

**NAT:** The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing a single IP address.

**IP Address:** Enter the IP/ Netmask/ Gateway / Primary addresses.

**SSID:** User can specify the exact SSID you are already sure, or you can scan the APs active on the air and type the exact one in this field.

**Channel:** Select the channel, which should be consistent with your wireless AP.

**Security Mode:** Select the security mode according to the settings in your wireless AP.

**Encryption Type:** The encryption information should be consistent with the settings in your wireless AP.

# System

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

## Time Zone

Configuration

Time Zone

Parameters

Time Zone

☒ Enable

☐ Disable

Local Time Zone (+-GMT Time)

(GMT) Greenwich Mean Time

SNTP Server IP Address

192.43.244.18

128.138.140.44

129.6.15.29

131.107.1.10


Daylight Saving

☒ Automatic

Resync Period

1440

minutes



Apply

Cancel

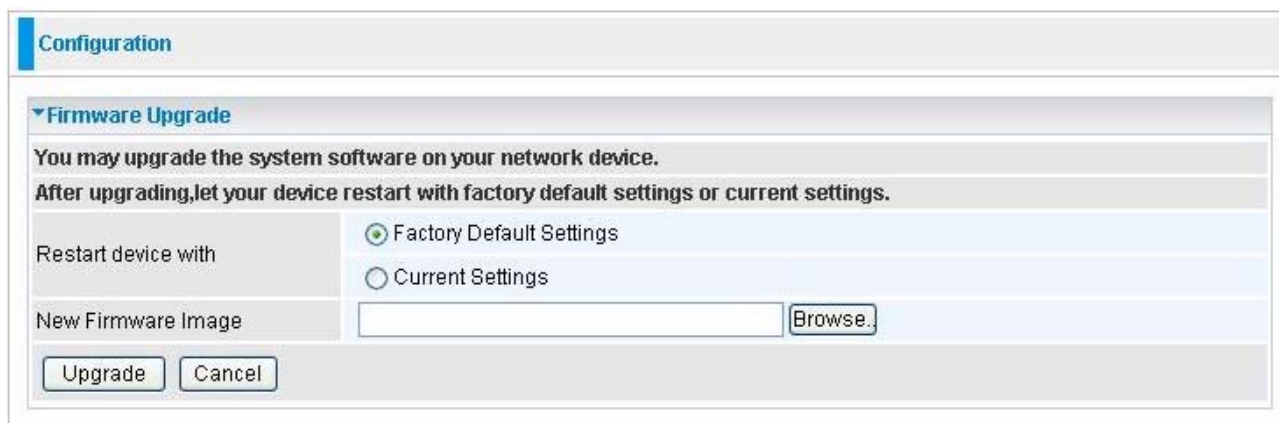
The router does not have a real time clock on board; instead, it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server outside your network. Choose your local time zone, click **Enable** and click the **Apply** button. After a successful connection to the Internet, 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.

## Firmware 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.



The screenshot shows a web interface for router configuration. At the top is a blue header bar with the word "Configuration". Below it is a section titled "Firmware Upgrade" with a dropdown arrow. The section contains the following text: "You may upgrade the system software on your network device." and "After upgrading, let your device restart with factory default settings or current settings." Below this text are two radio button options: "Factory Default Settings" (which is selected) and "Current Settings". Below the radio buttons is a text input field labeled "New Firmware Image" and a "Browse..." button. At the bottom of the section are two buttons: "Upgrade" and "Cancel".

**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.

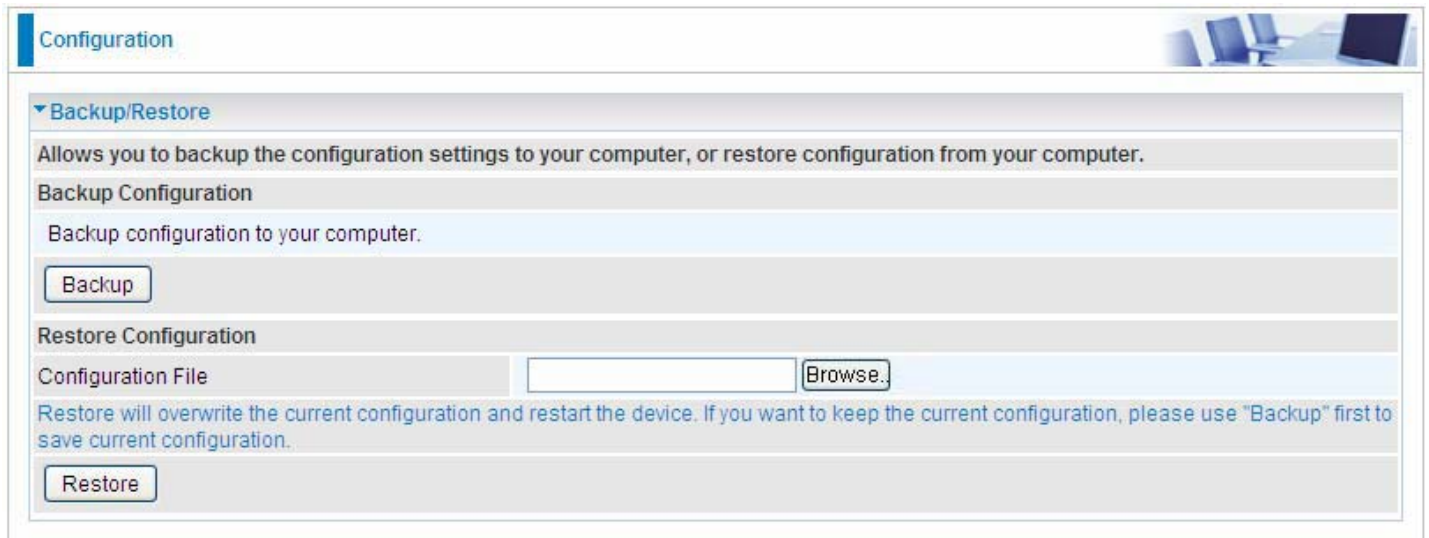
**Upgrade:** Click **upgrade** to begin the upload process. This process may take up to three minutes.



### 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.

## 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' is expanded. This section contains two main areas: 'Backup Configuration' and 'Restore Configuration'. The 'Backup Configuration' area has a description 'Allows you to backup the configuration settings to your computer, or restore configuration from your computer.' and a sub-section 'Backup Configuration' with the text 'Backup configuration to your computer.' and a 'Backup' button. The 'Restore Configuration' area has a sub-section 'Restore Configuration' with a 'Configuration File' label, an empty text input field, and a 'Browse...' button. Below the input field, there is a warning message: '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.' and a 'Restore' button.

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.

Configuration

Restart

After restarting. Please wait for several seconds to let the system come up.

Restart device with

☐ Factory Default Settings

☒ Current Settings

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

Configuration

▼ User Priority Setup

Parameters

High Priority User

Guest

ApplyCancel

▼ User Management

Parameters

Valid

User

Password

Confirm

Login Mode

Level

☐

Basic

Super

AddEdit / 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.

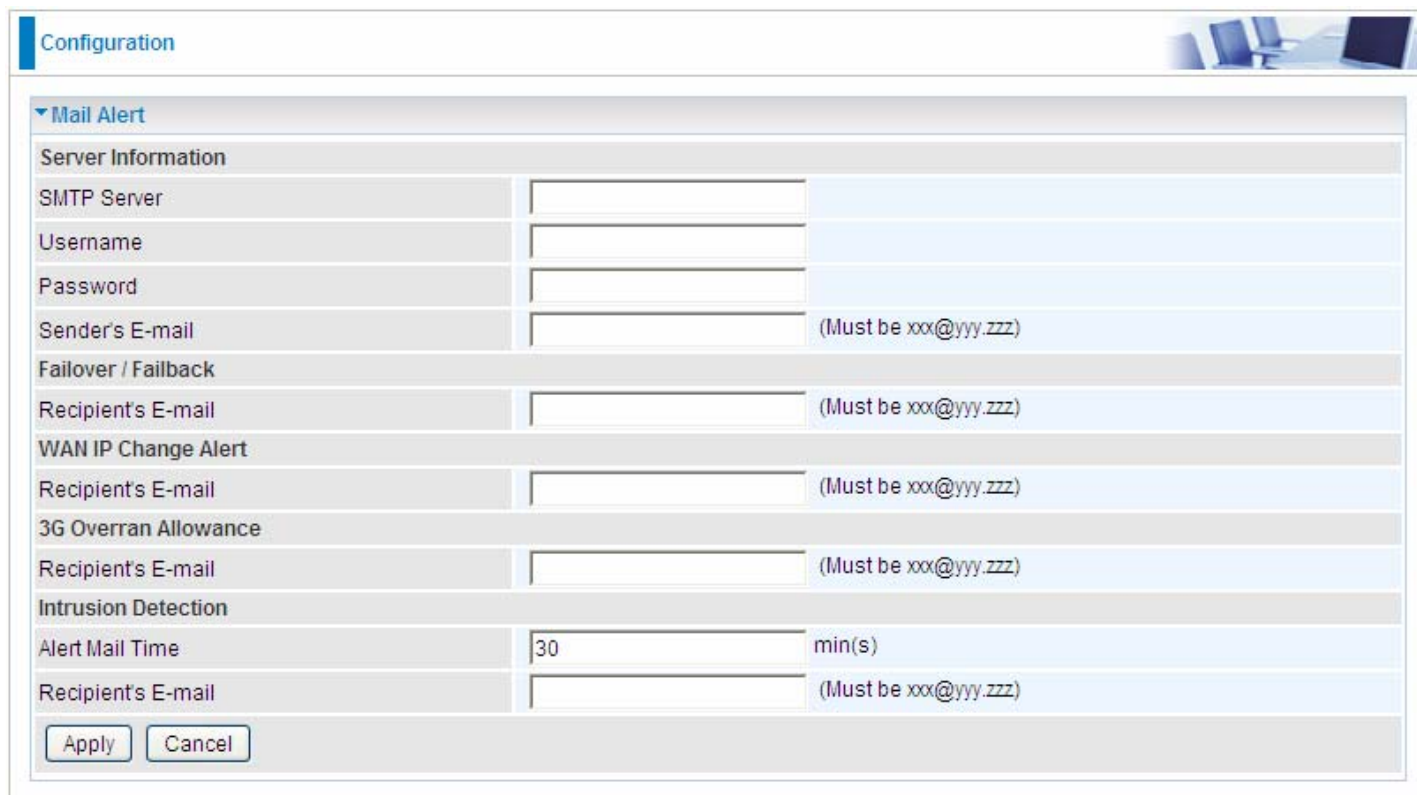
You are able to **Edit** existing users and **Add** new users who are able to access the device’s configuration interface. Once you have clicked **Edit** on the account you want to edit, the information of the account will be displayed above. Just go ahead and change the password.

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)

**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.

# USB

Besides connecting to 3G modem, USB 2.0 port can also be connected to Printer, Webcam or HDD. USB Server has integrated FTP Server, Printer Server and WebCam supervisory functions. Through FTP Server, Samba Server user can management the account, set the authority of download and upload. Printer server supports Internet Print Protocol, user can remote print.

There are six items within the USB section: **User Management**, **Storage**, **Samba Server**, **FTP Server**, **Printer Server** and **Webcam**.

## User Management

Configuration

▼ User Management

Parameters

User Setup	FTP Authority Setup	Samba Authority Setup	Webcam Authority Setup
Username <input type="text"/>	FTP Access <input checked="" type="radio"/> Enable <input type="radio"/> Disable Max. Login <input type="text" value="3"/> (0:No Limit)	Samba Access <input checked="" type="radio"/> Enable <input type="radio"/> Disable	Webcam Access <input checked="" type="radio"/> Enable <input type="radio"/> Disable
Password <input type="password"/>			

\*\*Please reset the Samba server after config changed.\*\*

Edit	Username	FTP Used	Samba Used	Webcam Used	Delete
------	----------	----------	------------	-------------	--------

Here user can set up account(s) and grant it or them authority (ies) for accessing the FTP, Samba and Webcam.

### User Setup

**Username:** Enter the name for the account.

**Password:** Set the password for the account.

### FTP Authority Setup

**FTP Access:** If you enable this function, this account has the access authority to FTP Server.

**Max. Login:** This option specifies the maximum number of users (both anonymous and non-anonymous) that are allowed to be using the FTP server simultaneously.

### Samba Authority Setup

**Samba Access:** If you enable this function, this account has the access authority to Samba Server.

### Webcam Authority Setup

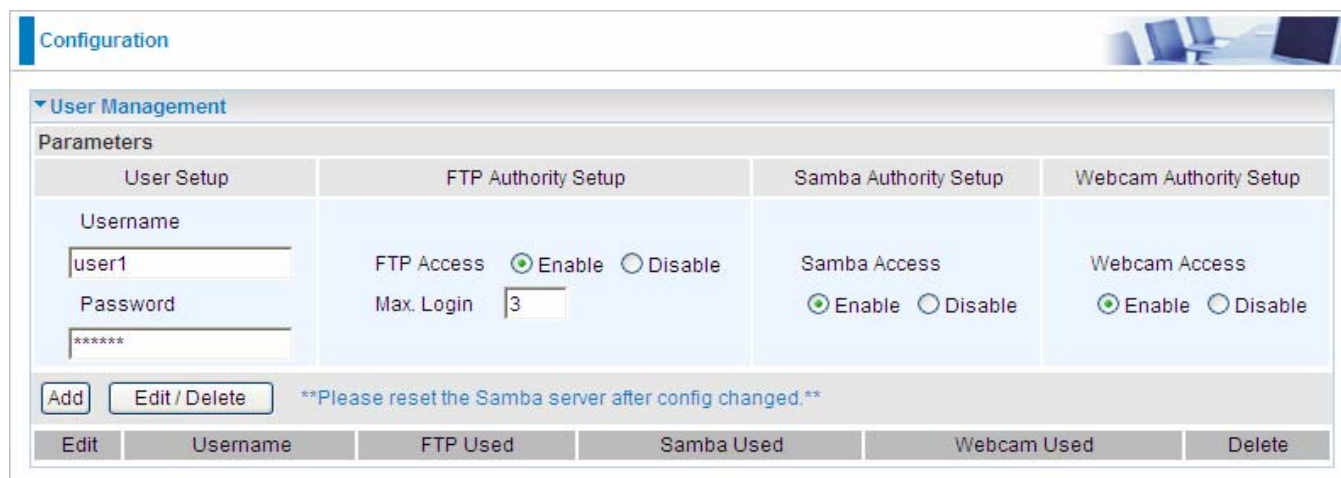
**Webcam Access:** If you enable this function, this account has the access authority to Webcam Server.

**Add:** Click this button to add a new account and it will appear at the bottom table.

**Edit/Delete:** Choose one account which you wish to Edit/Delete, and then click "Edit/Delete".

## Add/Delete User

1. Enter username and password



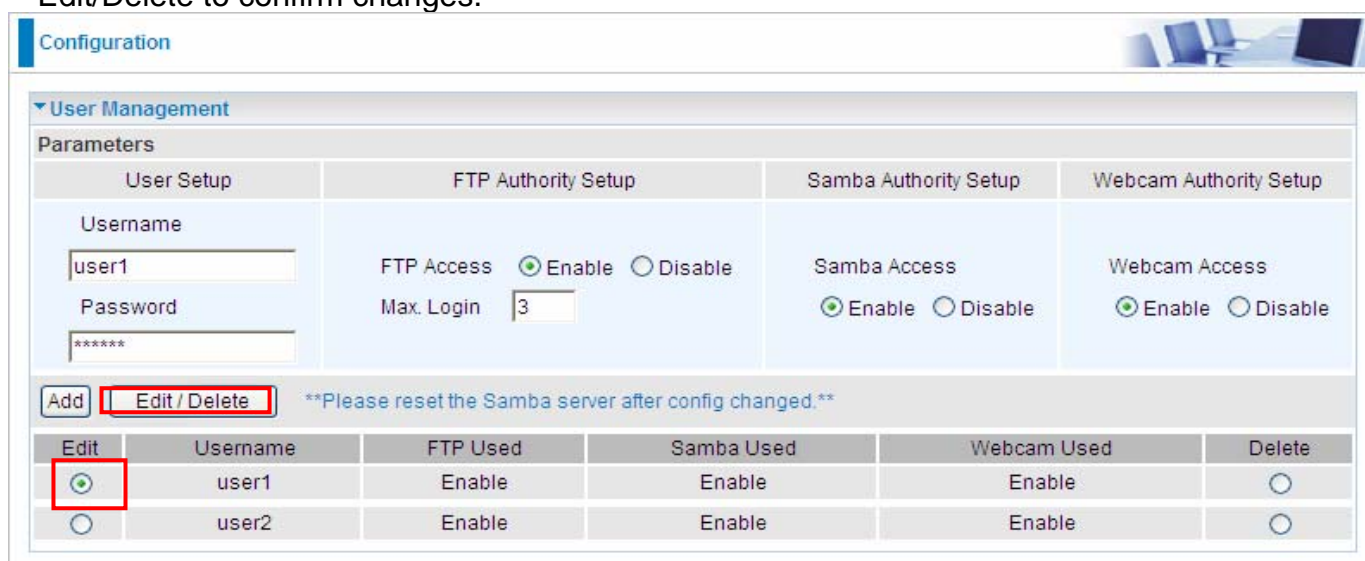
The screenshot shows the 'Configuration' page with a 'User Management' section. Under 'Parameters', there are four columns: 'User Setup', 'FTP Authority Setup', 'Samba Authority Setup', and 'Webcam Authority Setup'. The 'User Setup' column has input fields for 'Username' (containing 'user1') and 'Password' (containing '\*\*\*\*\*'). The 'FTP Authority Setup' column has 'FTP Access' (radio buttons for 'Enable' and 'Disable', with 'Enable' selected) and 'Max. Login' (a text box containing '3'). The 'Samba Authority Setup' column has 'Samba Access' (radio buttons for 'Enable' and 'Disable', with 'Enable' selected). The 'Webcam Authority Setup' column has 'Webcam Access' (radio buttons for 'Enable' and 'Disable', with 'Enable' selected). Below these fields are 'Add' and 'Edit / Delete' buttons. A note below the buttons says '\*\*Please reset the Samba server after config changed.\*\*'. At the bottom, there is a table with columns: Edit, Username, FTP Used, Samba Used, Webcam Used, and Delete.

Edit	Username	FTP Used	Samba Used	Webcam Used	Delete
<input type="radio"/>	user1	Enable	Enable	Enable	<input type="radio"/>

2. Click **Add**. The new user account will display below.

Edit	Username	FTP Used	Samba Used	Webcam Used	Delete
<input type="radio"/>	user1	Enable	Enable	Enable	<input type="radio"/>

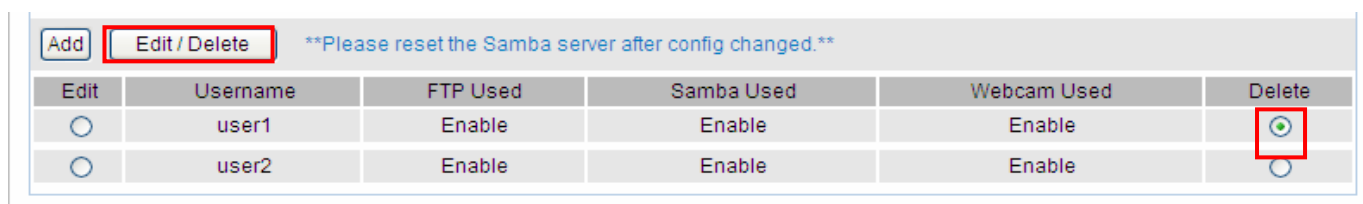
3. Choose the account which you want to edit then you can change the account's parameters, click Edit/Delete to confirm changes.



The screenshot shows the 'Configuration' page with the 'User Management' section. The 'Add' button is now disabled, and the 'Edit / Delete' button is highlighted with a red box. The table below now has two rows: 'user1' and 'user2'. The 'Edit' column for 'user1' has a radio button that is selected (highlighted with a red box), while the 'Delete' column for 'user1' has an unselected radio button. The 'Edit' column for 'user2' has an unselected radio button, and the 'Delete' column for 'user2' has an unselected radio button.

Edit	Username	FTP Used	Samba Used	Webcam Used	Delete
<input checked="" type="radio"/>	user1	Enable	Enable	Enable	<input type="radio"/>
<input type="radio"/>	user2	Enable	Enable	Enable	<input type="radio"/>

4. Choose the account which you want to delete, click Edit/Delete to remove it.



The screenshot shows the 'Configuration' page with the 'Edit / Delete' button highlighted with a red box. The table below now has two rows: 'user1' and 'user2'. The 'Delete' column for 'user1' has a radio button that is selected (highlighted with a red box), while the 'Edit' column for 'user1' has an unselected radio button. The 'Delete' column for 'user2' has an unselected radio button, and the 'Edit' column for 'user2' has an unselected radio button.

Edit	Username	FTP Used	Samba Used	Webcam Used	Delete
<input type="radio"/>	user1	Enable	Enable	Enable	<input checked="" type="radio"/>
<input type="radio"/>	user2	Enable	Enable	Enable	<input type="radio"/>

5. Access from web browser. Open your web browser, enter the IP address of your router, Enter the user name and password that your administrator has set for you and select **Guest** from the **Account Type** list, and then click **Login**.





Username:

Password:

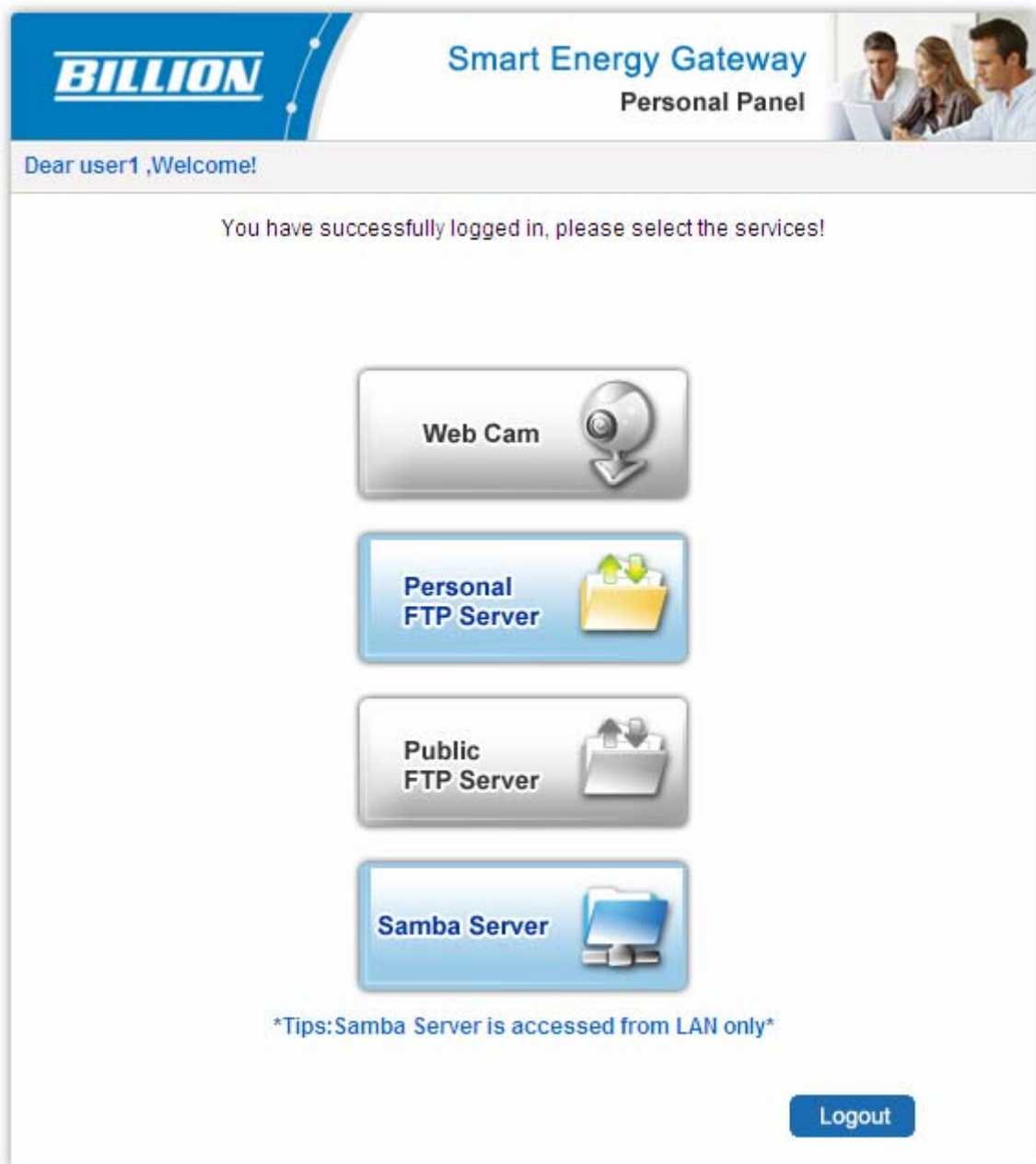
Account Type:

Guest

▼

Submit

When user1 is authorized, you will access to the router.



**Note:** To enable the servers, please go to [Samba Server](#), [FTP Server](#), [Web Cam](#) to enable the services.

# Storage

Storage page display the information of storage device which plugged in USB port, such as directory, partition and so on. You can also setup the storage.

Configuration

▼ Disk Management

Parameters

Directory Setup

Partition Setup

Directory Name

Partition

Path

/dev/sda6

/media/sda6

/dev/sda5

/media/sda5

Add

Delete

Delete	Directory Path	Partition
<div></div>	/media/sda6/sdgs	/dev/sda6
<div></div>	/media/sda6/eee	/dev/sda6
<div></div>	/media/sda6/public	/dev/sda6
<div></div>	/media/sda5/2003	/dev/sda5
<div></div>	/media/sda5/public	/dev/sda5
<div></div>	/media/sda5/System Volume Information	/dev/sda5
<div></div>	/media/sda5/Vista_Business_VL	/dev/sda5
<div></div>	/media/sda5/Win XP En	/dev/sda5
<div></div>	/media/sda5/win2000	/dev/sda5

Remove Disk

**Directory Setup:** Enter the directory name which you wish to create in the Directory Name field.

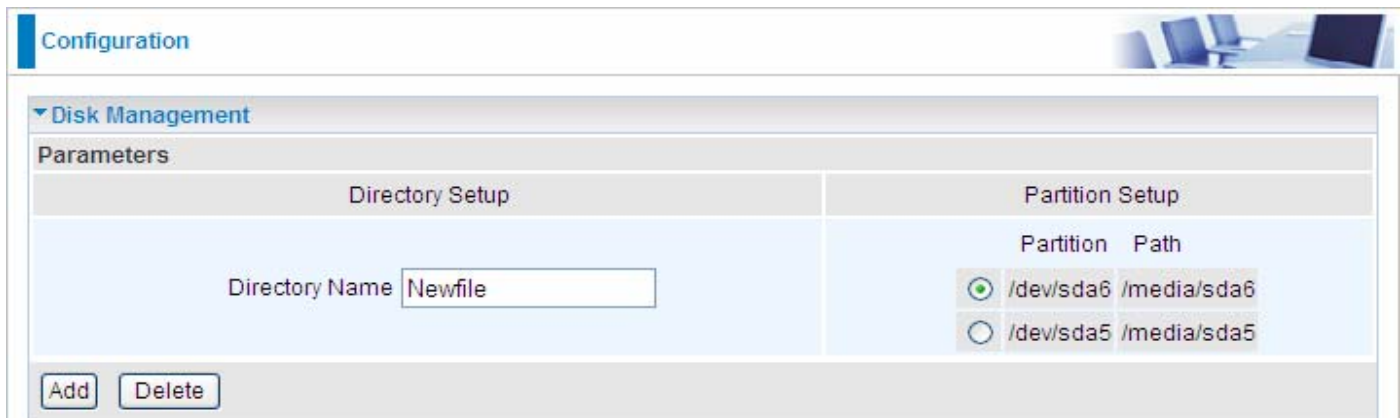
**Partition Setup:** Choose the partition of disk which you want to edit.

**Remove Disk:** Click this button to remove the disk which you choose in **Partition Path**.

99

## Add/Delete directory

1. Enter directory name in the directory name field and choose partition path which the directory will located.



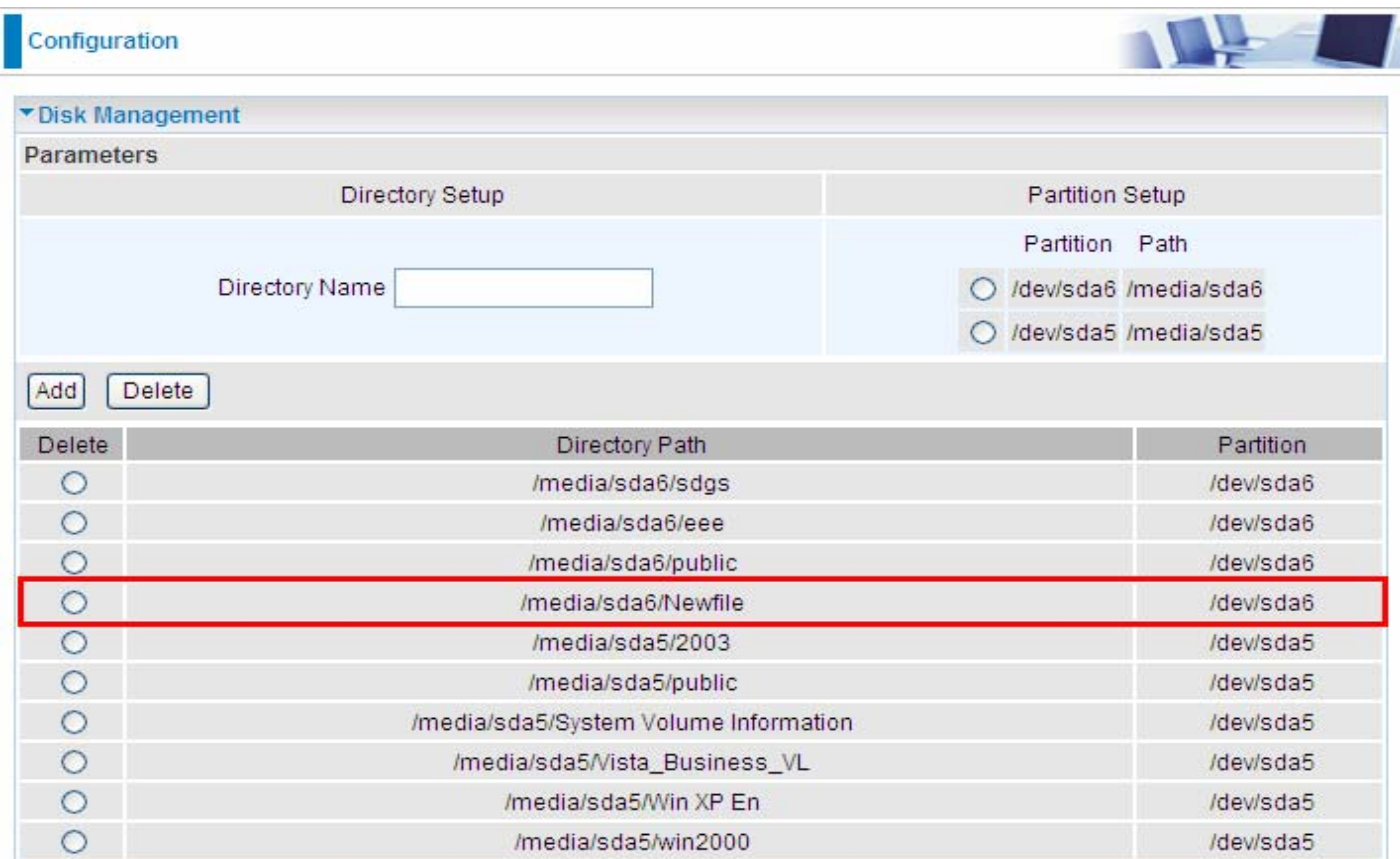
Configuration

▼ Disk Management

Parameters

Directory Setup	Partition Setup						
Directory Name <input type="text" value="Newfile"/>	<table><thead><tr><th>Partition</th><th>Path</th></tr></thead><tbody><tr><td><input checked="" type="radio"/> /dev/sda6</td><td>/media/sda6</td></tr><tr><td><input type="radio"/> /dev/sda5</td><td>/media/sda5</td></tr></tbody></table>	Partition	Path	<input checked="" type="radio"/> /dev/sda6	/media/sda6	<input type="radio"/> /dev/sda5	/media/sda5
Partition	Path						
<input checked="" type="radio"/> /dev/sda6	/media/sda6						
<input type="radio"/> /dev/sda5	/media/sda5						

2. Click **Add**. The New directory will display below.



Configuration

▼ Disk Management

Parameters

Directory Setup	Partition Setup						
Directory Name <input type="text"/>	<table><thead><tr><th>Partition</th><th>Path</th></tr></thead><tbody><tr><td><input checked="" type="radio"/> /dev/sda6</td><td>/media/sda6</td></tr><tr><td><input type="radio"/> /dev/sda5</td><td>/media/sda5</td></tr></tbody></table>	Partition	Path	<input checked="" type="radio"/> /dev/sda6	/media/sda6	<input type="radio"/> /dev/sda5	/media/sda5
Partition	Path						
<input checked="" type="radio"/> /dev/sda6	/media/sda6						
<input type="radio"/> /dev/sda5	/media/sda5						

Delete	Directory Path	Partition
<input type="radio"/>	/media/sda6/sdgs	/dev/sda6
<input type="radio"/>	/media/sda6/eee	/dev/sda6
<input type="radio"/>	/media/sda6/public	/dev/sda6
<input type="radio"/>	/media/sda6/Newfile	/dev/sda6
<input type="radio"/>	/media/sda5/2003	/dev/sda5
<input type="radio"/>	/media/sda5/public	/dev/sda5
<input type="radio"/>	/media/sda5/System Volume Information	/dev/sda5
<input type="radio"/>	/media/sda5/Vista_Business_VL	/dev/sda5
<input type="radio"/>	/media/sda5/Win XP En	/dev/sda5
<input type="radio"/>	/media/sda5/win2000	/dev/sda5

3. Choose the directory which you want to delete then click **Delete** to remove this directory.

Configuration

▼ Disk Management

Parameters

Directory Setup

Partition Setup

Directory Name

☐

/dev/sda6

/media/sda6

☐

/dev/sda5

/media/sda5


Add

Delete

Delete	Directory Path	Partition
<input type="radio"/>	/media/sda6/sdgs	/dev/sda6
<input type="radio"/>	/media/sda6/eee	/dev/sda6
<input type="radio"/>	/media/sda6/public	/dev/sda6
<input checked="" type="radio"/>	/media/sda6/Newfile	/dev/sda6
<input type="radio"/>	/media/sda5/2003	/dev/sda5
<input type="radio"/>	/media/sda5/public	/dev/sda5
<input type="radio"/>	/media/sda5/System Volume Information	/dev/sda5
<input type="radio"/>	/media/sda5/Vista_Business_VL	/dev/sda5
<input type="radio"/>	/media/sda5/Win XP En	/dev/sda5
<input type="radio"/>	/media/sda5/win2000	/dev/sda5

# Samba Server

Configuration



▼ Samba Server Setup

Parameters

SAMBA Server

☒ Enable ☐ Disable

Workgroup

Workgroup

NetBIOS Name

NetBIOS

Apply

Cancel

▼ Sharing Directory List Setup

Parameters

Access Directory Setup

Directory Name

Access User Setup

Access User

☐ user1  
☐ uesr2

Access Path Setup

	Path	Partition
<input type="radio"/>	/media/sda6/sdgs	/dev/sda6
<input type="radio"/>	/media/sda6/eee	/dev/sda6
<input type="radio"/>	/media/sda6/public	/dev/sda6
<input type="radio"/>	/media/sda6/Newfile	/dev/sda6
<input type="radio"/>	/media/sda5/2003	/dev/sda5
<input type="radio"/>	/media/sda5/public	/dev/sda5
<input type="radio"/>	/media/sda5/System Volume Information	/dev/sda5
<input type="radio"/>	/media/sda5/Ista_Business_VL	/dev/sda5
<input type="radio"/>	/media/sda5/Win XP En	/dev/sda5
<input type="radio"/>	/media/sda5/win2000	/dev/sda5

Add

Delete

Delete	Directory Name	Directory Path	Allowes Users
--	public	/media/sda5/public	All Users

102

## Samba Server Setup

Configuration

▼ Samba Server Setup

Parameters

SAMBA Server	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Workgroup	<input type="text" value="Workgroup"/>
NetBIOS Name	<input type="text" value="NetBIOS"/>

**SAMBA Service:** Enable or Disable SAMBA Server function. Default setting is set to **Disable**.

**Workgroup:** Enter the workgroup name in this field and default name is workgroup.

**NetBIOS Name:** Enter NetBIOS name in this field and default name is NetBIOS.

Click **Apply** to confirm the configuration.

## Sharing Directory List Setup

▼ Sharing Directory List Setup

Parameters

Access Directory Setup	Access User Setup	Access Path Setup																																	
Directory Name <input type="text" value="file"/>	Access User <input checked="" type="checkbox"/> user1 <input type="checkbox"/> user2	<table><thead><tr><th></th><th>Path</th><th>Partition</th></tr></thead><tbody><tr><td><input type="radio"/></td><td>/media/sda6/sdgs</td><td>/dev/sda6</td></tr><tr><td><input type="radio"/></td><td>/media/sda6/eee</td><td>/dev/sda6</td></tr><tr><td><input type="radio"/></td><td>/media/sda6/public</td><td>/dev/sda6</td></tr><tr><td><input checked="" type="radio"/></td><td>/media/sda6/Newfile</td><td>/dev/sda6</td></tr><tr><td><input type="radio"/></td><td>/media/sda5/2003</td><td>/dev/sda5</td></tr><tr><td><input type="radio"/></td><td>/media/sda5/public</td><td>/dev/sda5</td></tr><tr><td><input type="radio"/></td><td>/media/sda5/System Volume Information</td><td>/dev/sda5</td></tr><tr><td><input type="radio"/></td><td>/media/sda5/Vista_Business_VL</td><td>/dev/sda5</td></tr><tr><td><input type="radio"/></td><td>/media/sda5/Win XP En</td><td>/dev/sda5</td></tr><tr><td><input type="radio"/></td><td>/media/sda5/win2000</td><td>/dev/sda5</td></tr></tbody></table>		Path	Partition	<input type="radio"/>	/media/sda6/sdgs	/dev/sda6	<input type="radio"/>	/media/sda6/eee	/dev/sda6	<input type="radio"/>	/media/sda6/public	/dev/sda6	<input checked="" type="radio"/>	/media/sda6/Newfile	/dev/sda6	<input type="radio"/>	/media/sda5/2003	/dev/sda5	<input type="radio"/>	/media/sda5/public	/dev/sda5	<input type="radio"/>	/media/sda5/System Volume Information	/dev/sda5	<input type="radio"/>	/media/sda5/Vista_Business_VL	/dev/sda5	<input type="radio"/>	/media/sda5/Win XP En	/dev/sda5	<input type="radio"/>	/media/sda5/win2000	/dev/sda5
			Path	Partition																															
		<input type="radio"/>	/media/sda6/sdgs	/dev/sda6																															
		<input type="radio"/>	/media/sda6/eee	/dev/sda6																															
		<input type="radio"/>	/media/sda6/public	/dev/sda6																															
		<input checked="" type="radio"/>	/media/sda6/Newfile	/dev/sda6																															
		<input type="radio"/>	/media/sda5/2003	/dev/sda5																															
		<input type="radio"/>	/media/sda5/public	/dev/sda5																															
		<input type="radio"/>	/media/sda5/System Volume Information	/dev/sda5																															
		<input type="radio"/>	/media/sda5/Vista_Business_VL	/dev/sda5																															
<input type="radio"/>	/media/sda5/Win XP En	/dev/sda5																																	
<input type="radio"/>	/media/sda5/win2000	/dev/sda5																																	

**Directory Name:** Enter the mapping directory name which will be seen in server.

**Access User:** Choose User which is allowed to access the directory.

**Path Partition:** Choose partition path which user can access.

**Add:** Click this button to add a new setup and the added setup will appear at the bottom table.

**Add/Delete directory**

1. Enter mapping directory name in the directory name field, choose access user and partition path.

▼ Sharing Directory List Setup

Parameters

Access Directory Setup

Access User Setup

Access Path Setup

Directory Name

file

Access User

☒ user1

☐ user2

Path

Partition

☐ /media/sda6/sdgs

/dev/sda6

☐ /media/sda6/eee

/dev/sda6

☐ /media/sda6/public

/dev/sda6

☒ /media/sda6/Newfile

/dev/sda6

☐ /media/sda5/2003

/dev/sda5

☐ /media/sda5/public

/dev/sda5

☐ /media/sda5/System Volume Information

/dev/sda5

☐ /media/sda5/Vista\_Business\_VL

/dev/sda5

☐ /media/sda5/Win XP En

/dev/sda5

☐ /media/sda5/win2000

/dev/sda5

Add

Delete

2. Click Add. The New directory will display below.

Delete	Directory Name	Directory Path	Allowes Users
--	public	/media/sda5/public	All Users
<input type="radio"/>	file	/media/sda6/Newfile	user1

Click **Apply** to confirm configuration.

3. Choose the directory which you want to delete then click Delete to romove this directory.

## FTP Server

Configuration

FTP Server Setup

Parameters

FTP Server	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Enable Ftp Access From WAN:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Anonymous Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Anonymous Permit	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
FTP Port	<input type="text" value="21"/>
Max. Users	<input type="text" value="10"/>
Stay Timeout	<input type="text" value="240"/> Second

**FTP Server:** Enable or Disable FTP Server function. Default setting is set to disable.

**Enable Ftp Access From WAN:** Enable or Disable access FTP Server from WAN. Default setting is set to disable. Enable this function, both WAN and LAN can use FTP server.

**Anonymous Login:** Enable or disable Anonymous Login. Default setting is set to disable.

**Anonymous Permit:** Enable or disable Anonymous Permit. Default setting is set to disable. If you enable this function, this will permit the anonymous user to edit directory.

**FTP Port:** Enter FTP port in this field; please avoid conflicts with other port.

**Max. Users:** This option specifies the maximum number of user accounts.

**Stay Timeout:** Enter the Stay timeout value. Auto-disconnect when there is no activity for a predetermined period of time. The default value is 240 seconds.

Click **Apply** to save the configuration.

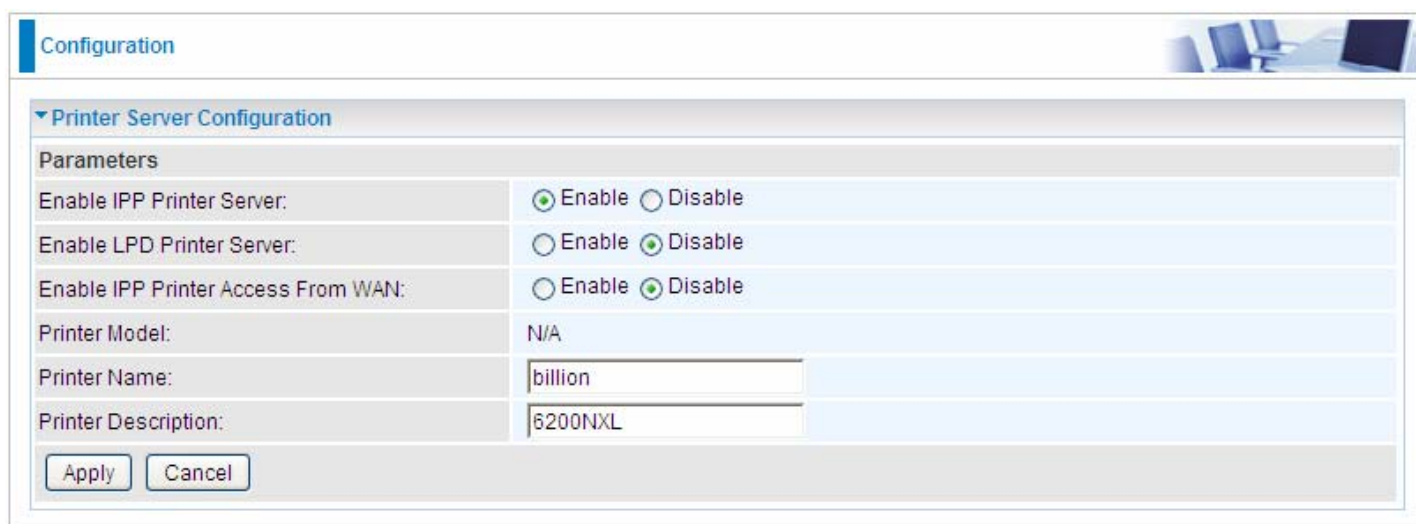
## Printer Server

Printer Server provides a simple and efficient network printing solution. Connect one end of the printer server to the printer and one end to the network, then anywhere the printer is in the network, users can print easily.

**IPP**, short for Internet Printing Protocol, provides a set of network printing services which give printing a more efficient and secure environment.

**LPD**, stands for Line Printer Daemon. Its function is to wait for the printing tasks transmitted by the LPR(line printer remote). When the LPD receives a print job, it first gets the print jobs temporarily stored in the print queue. The print queue is a file directory and many of the LPD print job are waiting here for processing. When the printing device is idle, LPD remove the print job from the print queue and pass it to the printer task to print.

Here enable IPP Printer Server if you want to use IPP Printer or enable LPD Printer Server if you want to use LPD Printer. Also you can enable the two. But LPD printer can only be used in LAN, if you want to printe from WAN, please enable IPP Printer Access From WAN.



The screenshot shows a web-based configuration interface. At the top, there's a 'Configuration' tab. Below it, the 'Printer Server Configuration' section is expanded. It contains several settings:

- Enable IPP Printer Server:** Radio buttons for 'Enable' (selected) and 'Disable'.
- Enable LPD Printer Server:** Radio buttons for 'Enable' and 'Disable' (selected).
- Enable IPP Printer Access From WAN:** Radio buttons for 'Enable' and 'Disable' (selected).
- Printer Model:** A text box containing 'N/A'.
- Printer Name:** A text box containing 'billion'.
- Printer Description:** A text box containing '6200NXL'.

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

**Enable IPP Printer Server:** Enable or Disable IPP Printer Server function. Default setting is set to disable.

**Enable LPD Printer Server:** Enable or Disable LPD Printer Server function. Default setting is set to disable.

**Enable Printer Access From WAN:** Enable or disable printer access from WAN. Default setting is set to disable. Enable this function, both WAN and LAN can use the printer.

**Printer Model:** Display the model of printer.

**Printer Name:** Set printer's alias.

**Printer Description:** Enter the information of the printer.

Click **Apply** to confirm the configuration.



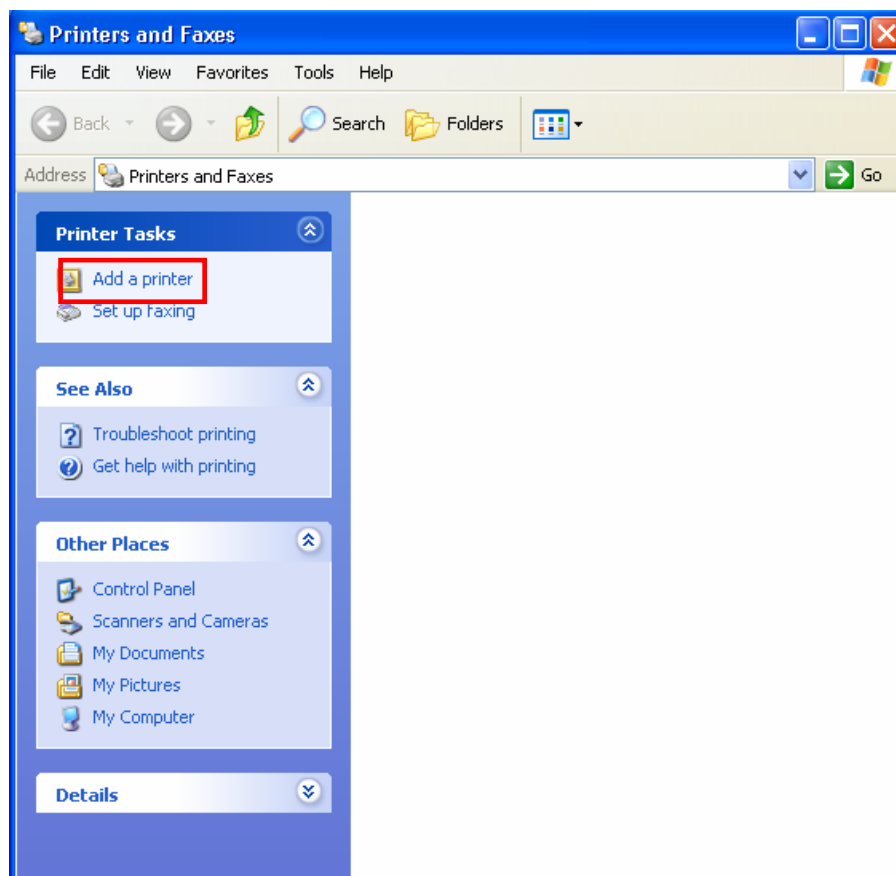
If both the USB ports connect to printer, only the one which connected first will be work.

## Set up of Printer client

**Step 1:** Click **Start** and select "Printer and Faxes".



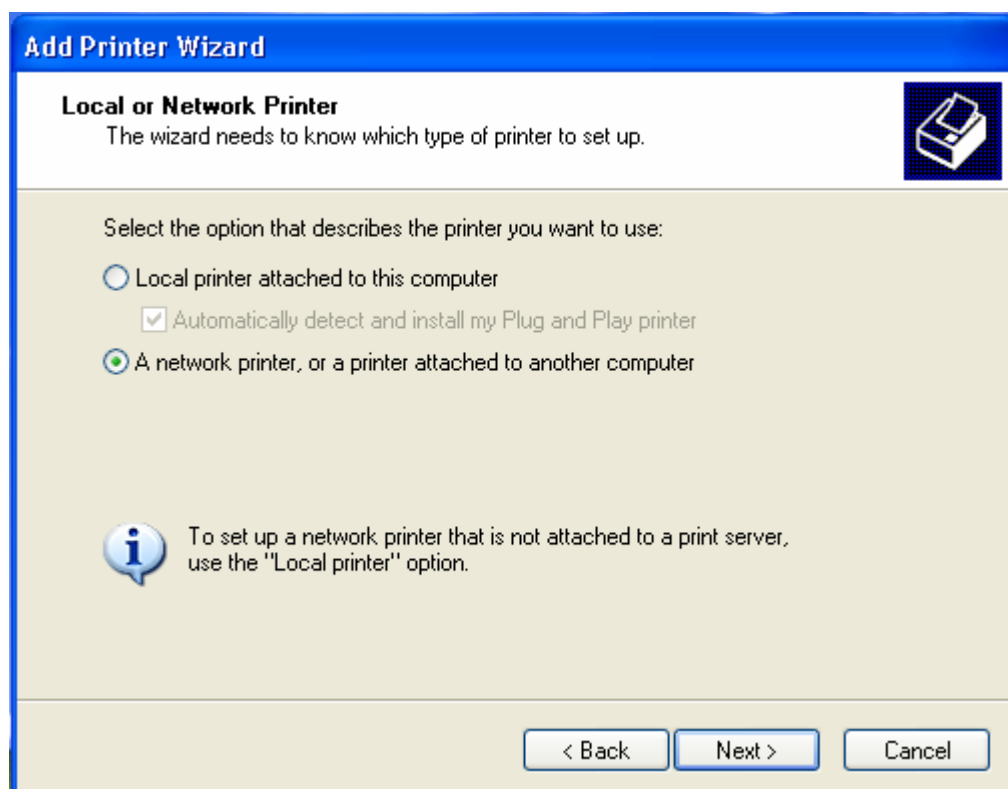
**Step 2:** Click "Add a Printer".



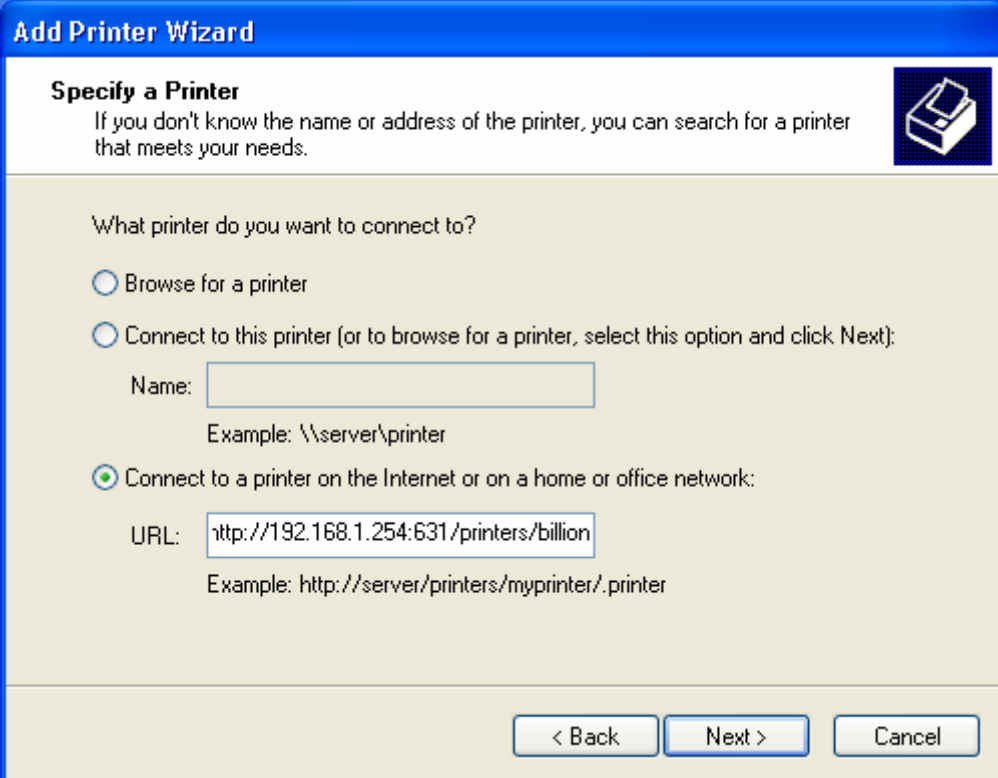
**Step 3:** To continue, click “Next”



**Step 4:** Select network printer and apply “Next” button.



**Step 5:** Select "Connect to a printer on the Internet or on a home or office network" then enter the printer's URL: http://LAN IP/printers/ printername or http://WAN IP:631/printers/ printername. Make sure printer's name is the same with you set in web page.



**Add Printer Wizard**

**Specify a Printer**  
If you don't know the name or address of the printer, you can search for a printer that meets your needs.

What printer do you want to connect to?

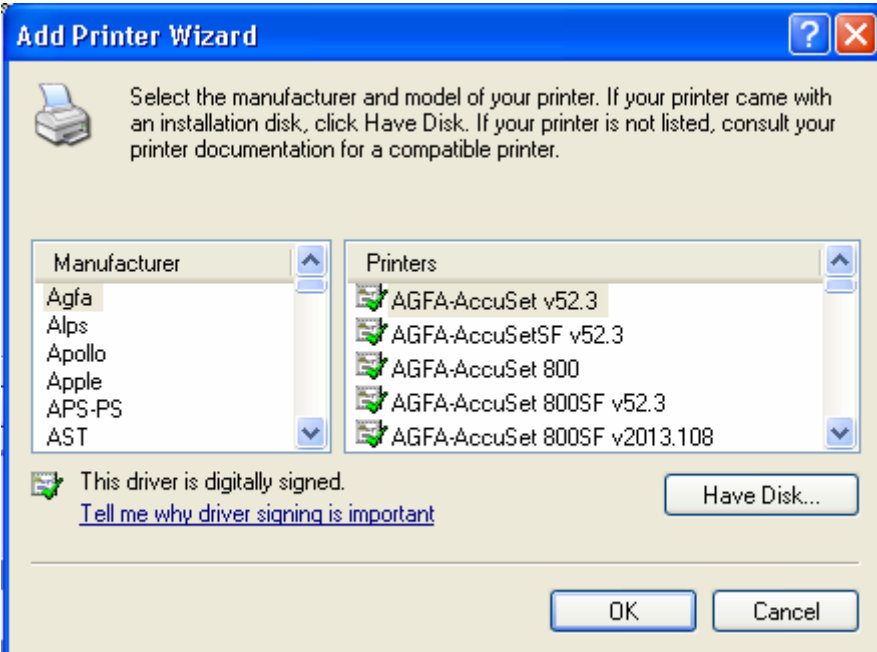
☐ Browse for a printer

☐ Connect to this printer (or to browse for a printer, select this option and click Next):  
Name:   
Example: \\server\printer

☒ Connect to a printer on the Internet or on a home or office network:  
URL:   
Example: http://server/printers/myprinter/.printer

< Back   Next >   Cancel

**Step 6:** Click "Next" to add the printer driver. If your printer is not listed and your printer came with an installation disk, click "Have Disk" find it and install the driver.



**Add Printer Wizard**

Select the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for a compatible printer.

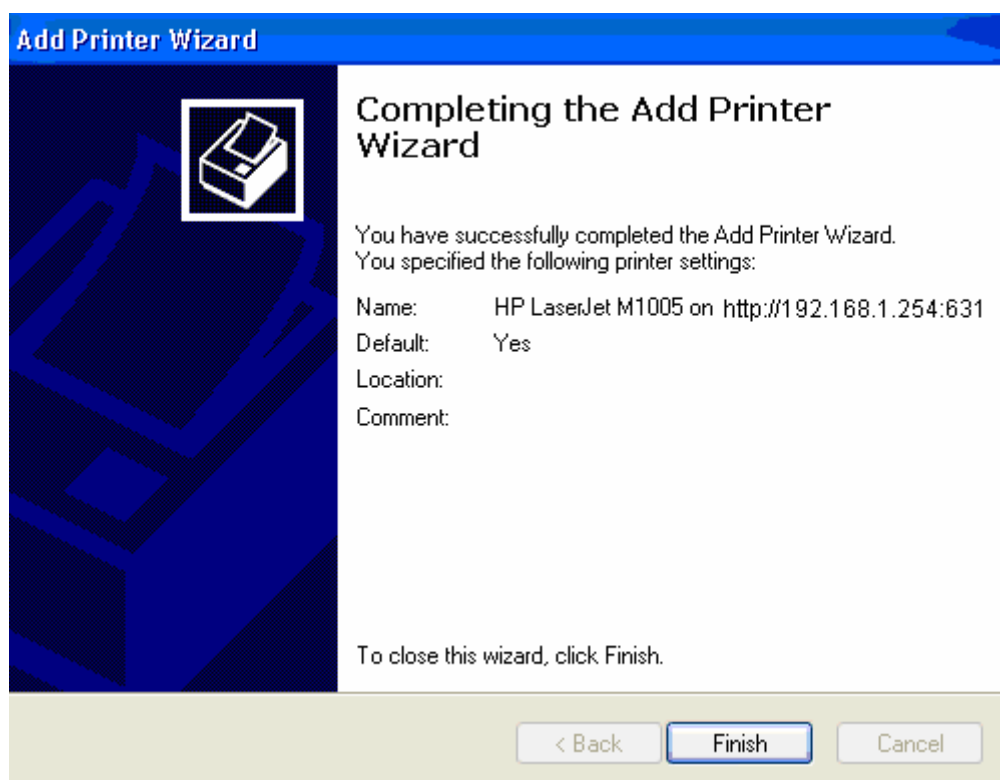
Manufacturer	Printers
Agfa	AGFA-AccuSet v52.3
Alps	AGFA-AccuSetSF v52.3
Apollo	AGFA-AccuSet 800
Apple	AGFA-AccuSet 800SF v52.3
APS-PS	AGFA-AccuSet 800SF v2013.108
AST	

This driver is digitally signed.  
[Tell me why driver signing is important](#)

Have Disk...

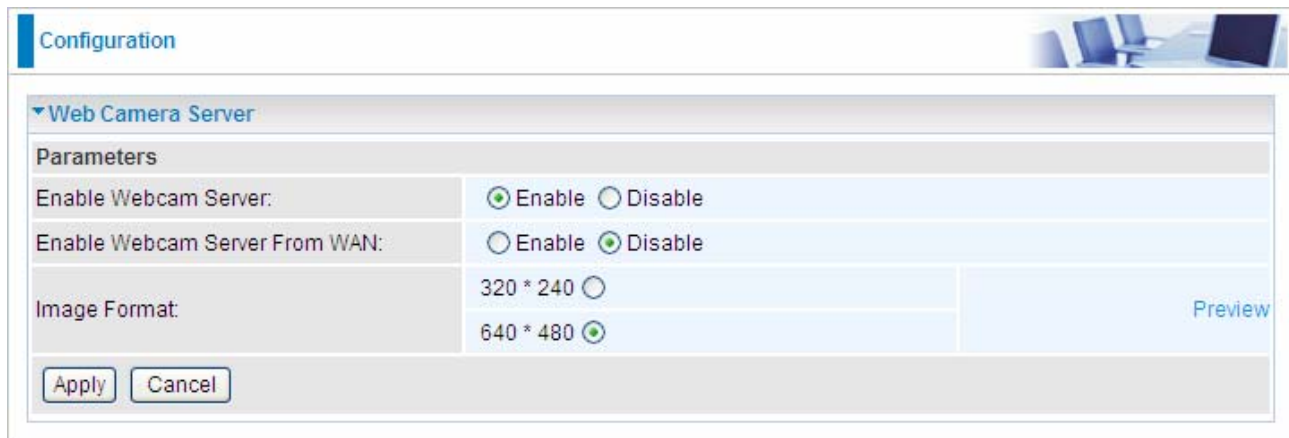
OK   Cancel

**Step 7:** Click “Finish” to complete the add printer.



## Webcam

Plug in the webca to your router.



Parameters	
Enable Webcam Server:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Enable Webcam Server From WAN:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Image Format:	320 * 240 <input type="radio"/> 640 * 480 <input checked="" type="radio"/>

[Preview](#)

**Enable Webcam Server:** Enable or Disable Webcam Server function. Default setting is set to disable.

**Enable Webcam Server From WAN:** Enable or disable this function. Default setting is set to disable.

Enable this function, both WAN and LAN can see the image.

**Image Format:** Choose the size of the image you will see.

**Preview:** Click the link, you can preview the image which transmitted by the webcam.

Click **Apply** to confirm the configuration.

Examples:

### ① Preview mode

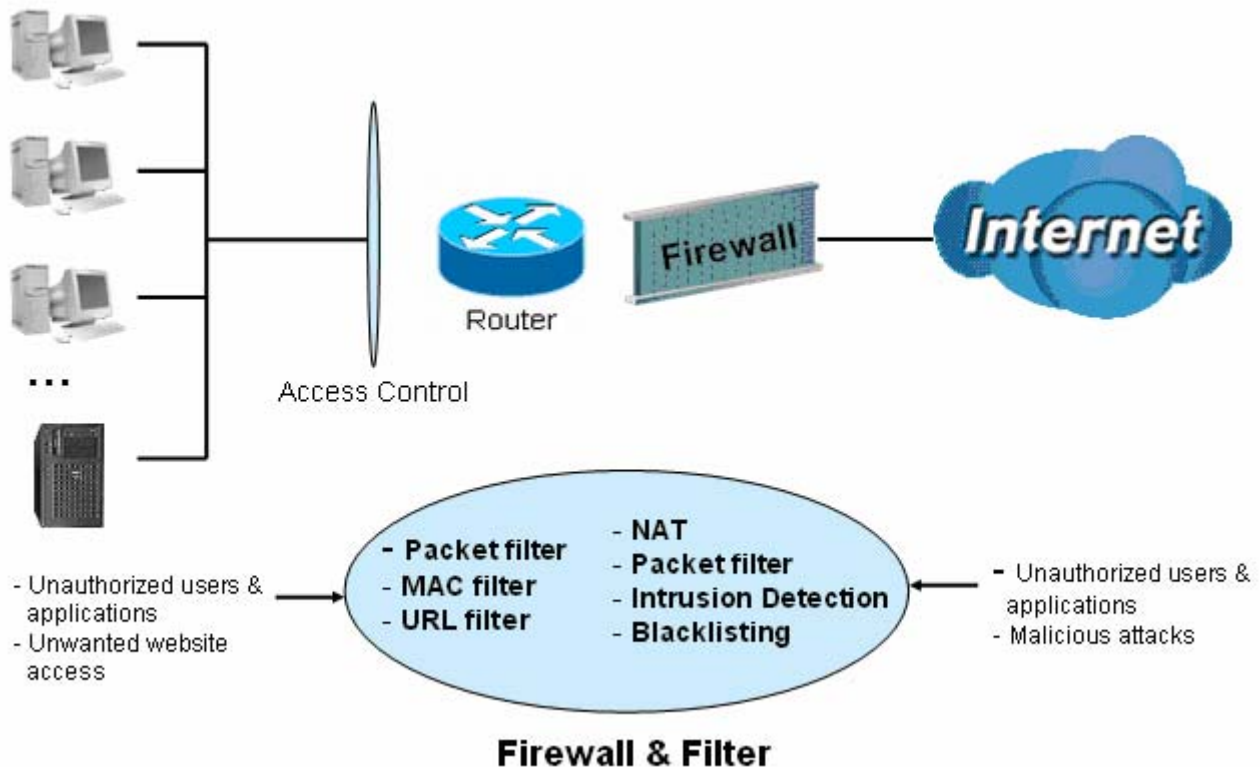
After configuration as above, click **Preview**, you will see the figure.



You can click Return to return back and select another image format.

## 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.

Configuration

▼ Packet Filter

Parameters

Rule Name

<< --select--

(type or select from listbox)

Internal IP Address

~

External IP Address

~

Protocol

TCP

Action

forward

Internal Port

~

External Port

~

Direction

outgoing

Time Schedule

Always On

Log

☐

Add

Edit / Delete

Reorder

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.

114

**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	TCP	0~0	outgoing	forward	Always On	<input type="checkbox"/>
		0.0.0.0~0.0.0.0		21~21				
<input type="radio"/>	HTTP	0.0.0.0~0.0.0.0	TCP	0~0	outgoing	forward	Always On	<input type="checkbox"/>
		0.0.0.0~0.0.0.0		80~80				



### 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 interface for a router. At the top, there is a 'Configuration' tab. Below it, the 'MAC Filter' section is expanded. Under 'Filter Action', there are three radio buttons: 'Disable', 'Allow', and 'Block'. The 'Block' option is selected. An 'Apply' button is located below these options. Under the 'Parameters' section, there is a 'MAC Address' field with a text input and a dropdown menu showing '--select--' with a hint '(type or select from listbox)'. Below this is a 'Time Schedule' dropdown menu set to 'Always On'. At the bottom of the parameters section, there are two buttons: 'Add' and 'Edit / Delete'.

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

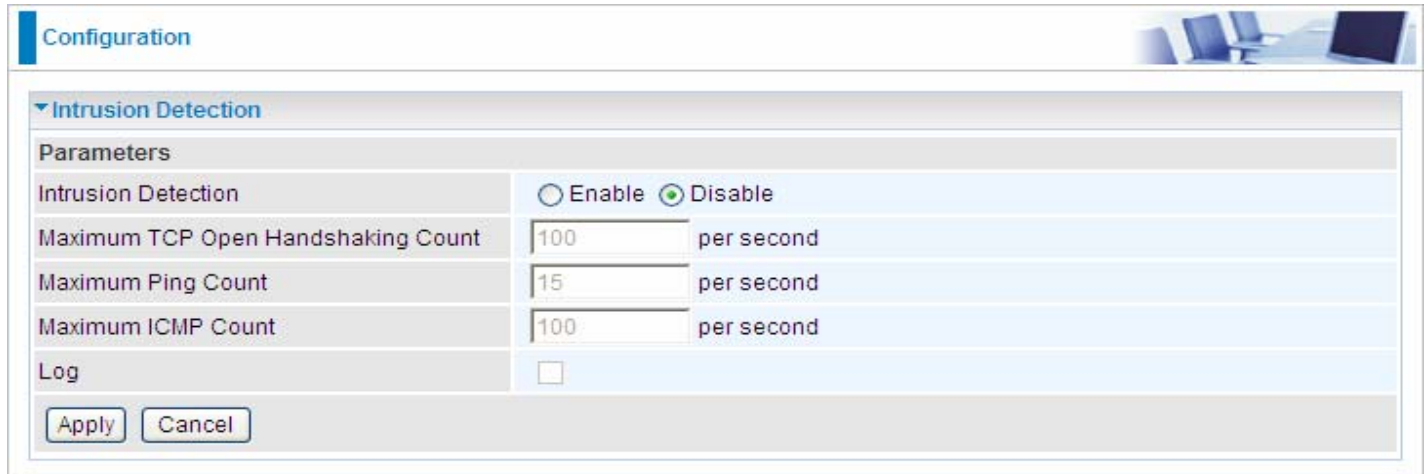
- **Disable:** to disable the MAC filter function.
- **Allow:** to enable the MAC filter function and allow the host of the following set MAC addresses to access.
- **Block:** to enable the MAC filter function and block the host of the following set MAC addresses to access.

**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"/>

Apply Cancel

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

**Src IP:** Source IP

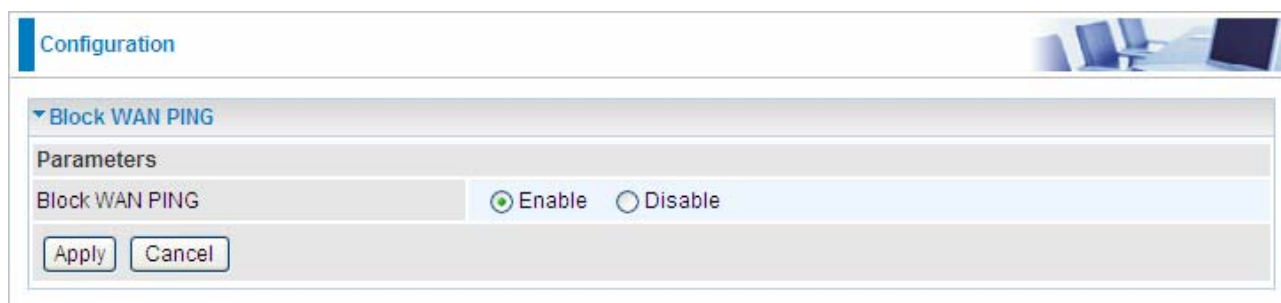
**Src Port:** Source Port

**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

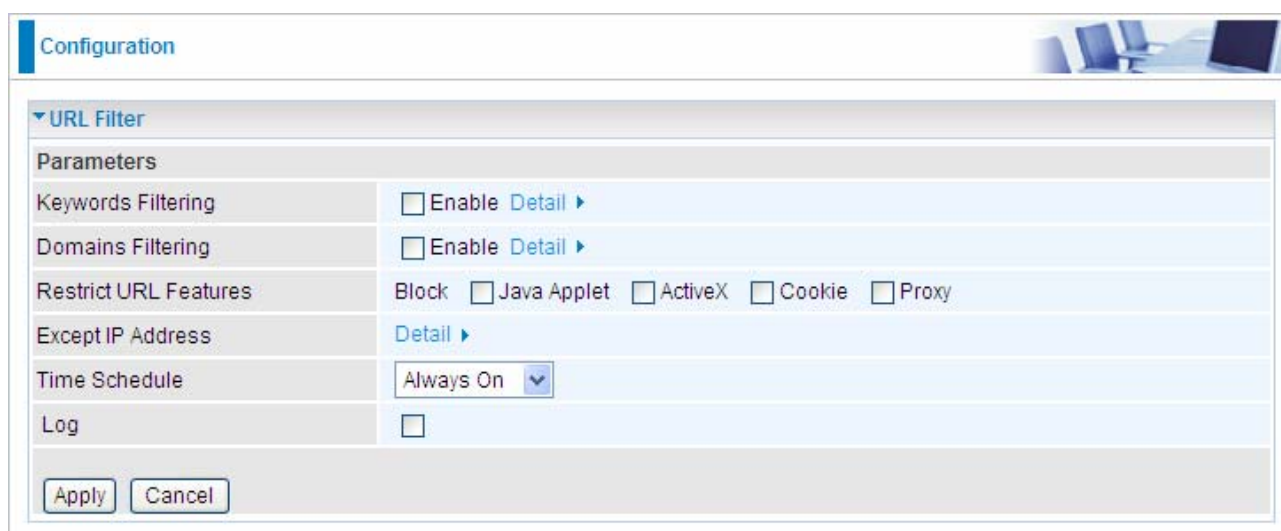
Parameters

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 ▼

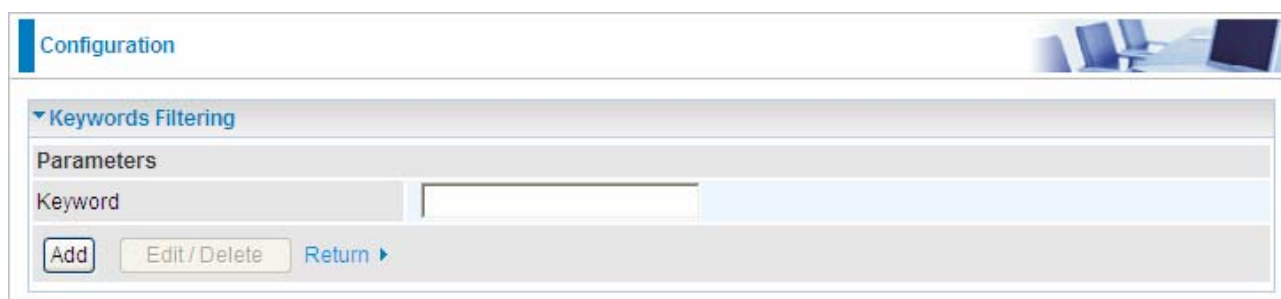
Log ☐

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

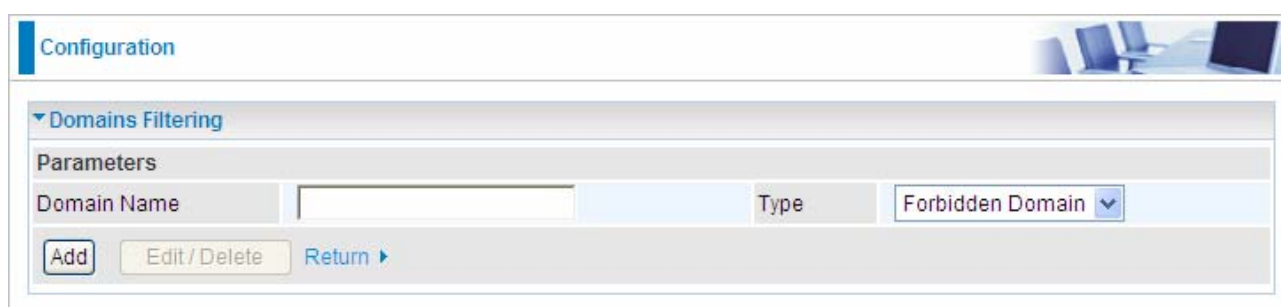
Keyword

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](http://www.google.com.au), enter “[www.google](http://www.google)” or “[www.google.com](http://www.google.com)”



The screenshot shows the 'Configuration' window with the 'Domains Filtering' section expanded. Under 'Parameters', there is a 'Domain Name' text 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 the 'Configuration' window with the 'Except IP Address' section expanded. Under 'Parameters', there is an 'Internal IP Address' field with two input boxes separated by a tilde (~), 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.

# Download Tool

## FTP Client

Configuration

FTP/HTTP Client

Parameters

FTP/HTTP Client

☒ Enable ☐ Disable

URL

Save Directory

☒ /media/sda0

Save Name

Repeated attempts

1

Timeout

Seconds

Rate limit

K

Login to the server

☐

Username

Password

Start Download

Reload / Delete

Refresh

Downloading task list

Edit	Active	Status	File Name	File Size	Download Progress	Remaining time	Delete
------	--------	--------	-----------	-----------	-------------------	----------------	--------

Downloaded task list

Status	File Name	File Size	Save Directory	Delete
--------	-----------	-----------	----------------	--------

Unable download list

Edit	Status	File Name	File Size	Delete
------	--------	-----------	-----------	--------

### Parameters

**FTP/HTTP Client:** select whether to enable or disable the FTP/ Http Client.

**URL:** Enter the URL of the file you want to download, it must be a complete one.

**Save Directory:** Enter the Directory you want to save to. The directory is one of the USB directories. If not existed, a new one with the name will be created.

**Save Name:** Enter the name you want to save as the file name.

**Repeated attempts:** select the repeated attempts you want form the drop-down box. When connection is failed, it will again connect according to the value you set.

**Timeout:** Enter the timeout time. Auto-disconnect the connection when the task doesn't connect to the server for a predetermined period of time (timeout time).

**Rate limit:** The limit rate. Specify as you want or leave it there.

**Login to the server:** check the checkbox to enable login to the server then enter the username and password of the server if username and password are required.

### Downloading task list:

**Edit:** Press the radio button, the message of the corresponding task will be listed above, you can just view.

**Active:** Check the checkbox to active the downloading task.

**Status:** Display the status of the downloading task.

**File Name:** Display the File Name you set to the downloading file.

**File Size:** Display the size of the file.

**Download Progress:** Display the download progress of the task.

**Remaining time:** Display the remaining time of the task.

**Delete:** Press the radio button, then press **Reload/Delete** to delete the task.

#### Downloaded task list:

**Status:** Display the task status.

**File Name:** Display the user-set Name of the file downloaded.

**File Size:** Display the size of the file downloaded.

**Save Directory:** Display the directory in the USB device.

**Delete:** Press the radio button, then press **Reload/Delete** to delete the record.

#### Unable Download List:

**Edit:** Press the radio button, then press **Reload/Delete** to edit and reload.

**Status:** Display the status of the task.

**File Name:** Display the user-set file name.

**File Size:** Display the file size

**Delete:** Press the radio button, then press **Reload/Delete** to delete the record.

Set up a download task:

You can set a http or ftp connection, here take http client for example. Enter the necessary information of the task, leave the others as default as you like, then press **Start Download**.

Configuration

FTP/HTTP Client

Parameters

FTP/HTTP Client

☒ Enable ☐ Disable

URL

/0170/bef20bb3611045238f7a7dcb70357b4a.mp3

Save Directory

music

☒ /media/sda0

Save Name

123.mp3

Repeated attempts

1

Timeout

Seconds

Rate limit

K

Login to the server

☐

Username

Password

Start Download

Reload / Delete

Refresh

Downloading task list

Edit	Active	Status	File Name	File Size	Download Progress	Remaining time	Delete
------	--------	--------	-----------	-----------	-------------------	----------------	--------

Downloaded task list

Status	File Name	File Size	Save Directory	Delete
--------	-----------	-----------	----------------	--------

Unable download list

Edit	Status	File Name	File Size	Delete
------	--------	-----------	-----------	--------

Then the task will be listed in the **Downloading task list** table. Check the **Active** checkbox to temporarily stop the downloading task and recheck the Active box to active the downloading task.

Configuration

FTP/HTTP Client

Parameters

FTP/HTTP Client

☒ Enable ☐ Disable

URL

Save Directory

☒ /media/sda0

Save Name

Repeated attempts

1

Timeout

Seconds

Rate limit

K

Login to the server

☐

Username

Password

Start Download

Reload / Delete

Refresh

Downloading task list

Edit	Active	Status	File Name	File Size	Download Progress	Remaining time	Delete
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Downloading	123.mp3	6.2M	2%	3m 22s	<input type="radio"/>

Downloaded task list

Status	File Name	File Size	Save Directory	Delete
--------	-----------	-----------	----------------	--------

Unable download list

Edit	Status	File Name	File Size	Delete
------	--------	-----------	-----------	--------

You can press Refresh to view the latest information especially the download progress. And when the task is finished, it will be listed in the **Downloaded task** list.

Configuration

FTP/HTTP Client

Parameters

FTP/HTTP Client

☒ Enable
 ☐ Disable

URL

Save Directory

☒ /media/sda0

Save Name

Repeated attempts

1

Timeout

Seconds

Rate limit

K

Login to the server

☐

Username

Password

Start Download

Reload / Delete

Refresh

Downloading task list

Edit	Active	Status	File Name	File Size	Download Progress	Remaining time	Delete
------	--------	--------	-----------	-----------	-------------------	----------------	--------

Downloaded task list

Status	File Name	File Size	Save Directory	Delete
✓	123.mp3	6.2M	/media/sda0/home/tmp/music/123.mp3	<input type="radio"/>

Unable download list

Edit	Status	File Name	File Size	Delete
------	--------	-----------	-----------	--------

Here you have finished the downloading task.

**Delete the task:** press the **Delete** radio button beside the item you want to delete, then press the **Reload/Delete** button to delete it. The delete action is the same in the other two lists.

Configuration

▼ FTP/HTTP Client

Parameters

FTP/HTTP Client

☒ Enable ☐ Disable

URL

Save Directory

☒ /media/sda0

Save Name

Repeated attempts

▼

Timeout

Seconds

Rate limit

K

Login to the server

☐

Username

Password

Start Download

Reload / Delete

Refresh

Downloading task list

Edit	Active	Status	File Name	File Size	Download Progress	Remaining time	Delete
Downloaded task list							
Status	File Name	File Size	Save Directory	Delete			
✓	123.mp3	6.2M	/media/sda0/home/tmp/music/123.mp3	<input checked="" type="radio"/>			
Unable download list							
Edit	Status	File Name	File Size	Delete			

**Edit and Reload the task:**

If there task unable to download, you can reedit for reloading.

Configuration

FTP/HTTP Client

Parameters

FTP/HTTP Client

☒ Enable ☐ Disable

URL

Save Directory

☒ /media/sda0

Save Name

12

Repeated attempts

1

Timeout

Seconds

Rate limit

K

Login to the server

☐

Username

Password

Start Download

Reload / Delete

Refresh

Downloading task list

Edit	Active	Status	File Name	File Size	Download Progress	Remaining time	Delete

Downloaded task list

Status	File Name	File Size	Save Directory	Delete
✓	123.mp3	6.2M	/media/sda0/home/tmp/music/123.mp3	<input type="radio"/>

Unable download list

Edit	Status	File Name	File Size	Delete
<input checked="" type="radio"/>	✗	12	---	<input type="radio"/>

Enter the necessary message and press **Reload/Delete**.

Configuration

FTP/HTTP Client

Parameters

FTP/HTTP Client

☒ Enable ☐ Disable

URL

Save Directory

☒ /media/sda0

Save Name

Repeated attempts

1

Timeout

Seconds

Rate limit

K

Login to the server

☐

Username

Password

Start Download

Reload / Delete

Refresh

Downloading task list

Edit	Active	Status	File Name	File Size	Download Progress	Remaining time	Delete
<input type="radio"/>	<input checked="" type="checkbox"/>	Downloading	12	6.2M	1%	---	<input type="radio"/>

Downloaded task list

Status	File Name	File Size	Save Directory	Delete
✓	123.mp3	6.2M	/media/sda0/home/tmp/music/123.mp3	<input type="radio"/>

Unable download list

Edit	Status	File Name	File Size	Delete

# QoS (Quality of Service)

## Quality of Service Introduction

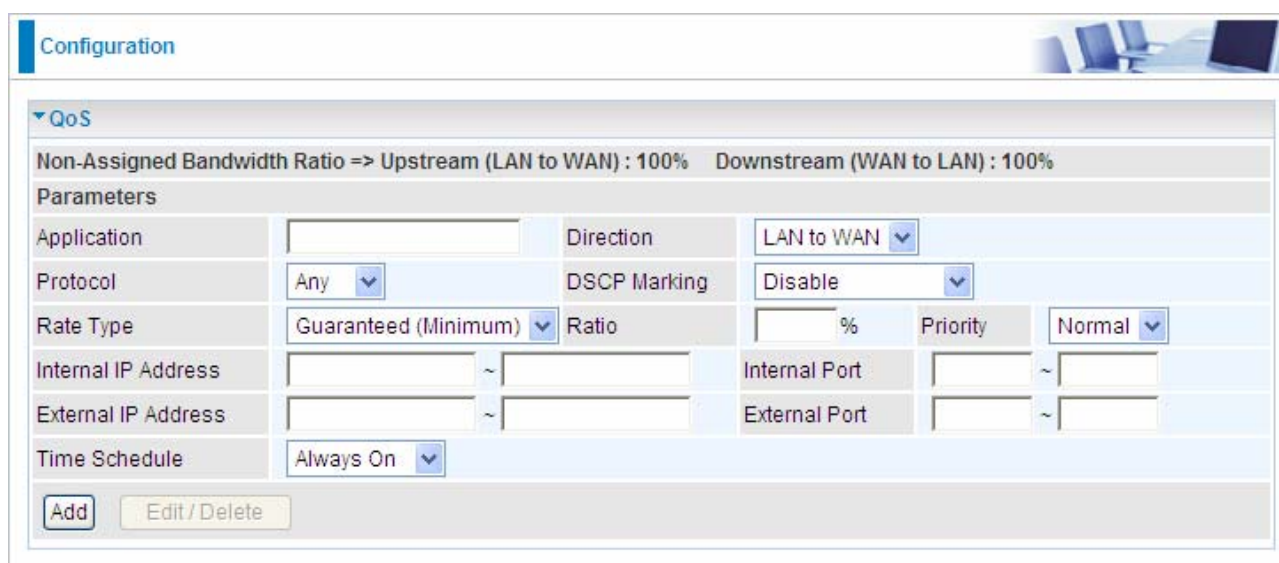
If you've ever found your 'net' speed has slowed to a crawl because another family member is using a P2P file sharing program, you'll understand why the Quality of Service features in the routers is such a breakthrough for home users and office users.

## 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.



The screenshot shows the 'Configuration' tab with the 'QoS' section expanded. At the top, it displays 'Non-Assigned Bandwidth Ratio => Upstream (LAN to WAN) : 100% Downstream (WAN to LAN) : 100%'. Below this is a 'Parameters' table with the following fields:

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			

At the bottom of the form are two buttons: 'Add' and '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.

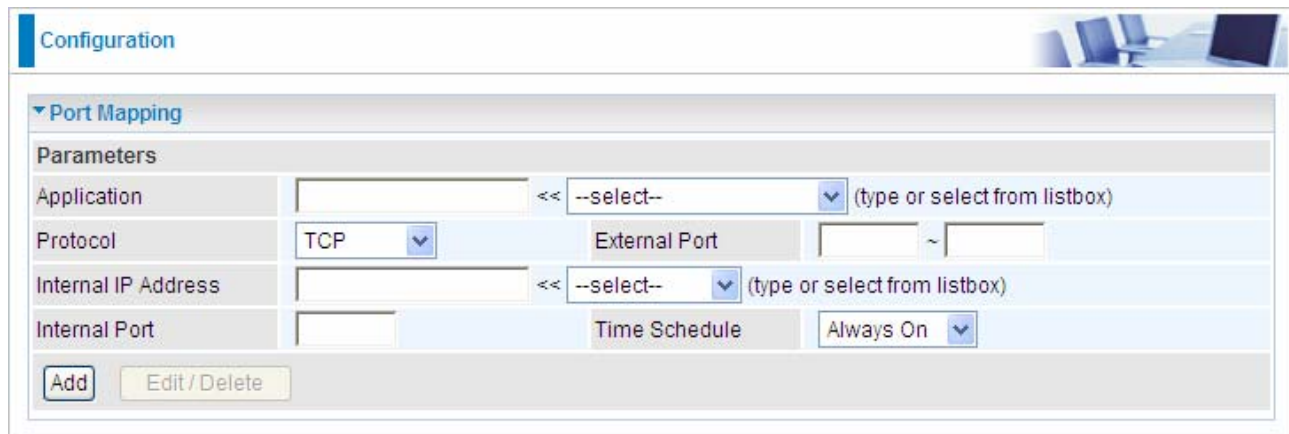
The Internet Assigned Numbers Authority (IANA) is the central coordinator for the assignment of unique parameter values for Internet protocols. Port numbers range from 0 to 65535, but only port numbers 0 to 1023 are reserved for privileged services and are designated as “well-known ports”. The registered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



The screenshot shows a 'Configuration' window with a 'Port Mapping' section. The 'Parameters' table includes fields for Application, Protocol, Internal IP Address, Internal Port, External Port, and Time Schedule. The 'Add' button is highlighted.

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

--select-- (type or select from listbox)

Protocol

TCP

External Port

~

Internal IP Address

--select-- (type or select from listbox)

Internal Port

Time Schedule

Always On

Add

Edit / Delete

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.

133

# 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

Add

Except List

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

Apply

Cancel

**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

Add

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

Except List				
ID	Description	Protocol	Port	Operation
1	Remote Access	tcp	80	<a href="#">Delete</a>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>				

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	<a href="#">Delete</a>
2	Printer Server	tcp	631	<a href="#">Delete</a>
3	Web Cam	tcp	8081	<a href="#">Delete</a>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>				



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.

Configuration

Wake on LAN

Parameters

MAC Address

<< --select--

(type or select from listbox)

Add

Edit / Delete

Edit	Action	MAC Address	Ready	Delete
<input type="radio"/>	<div>Wake Up</div>	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. Your 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

08 : 00

End Time

18 : 00

Edit / Clear

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-defined 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.

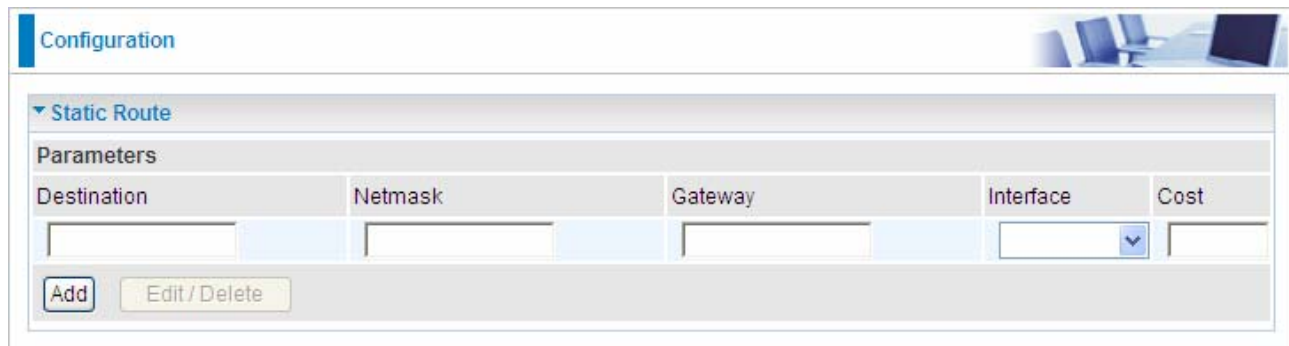
**End Time:** The default is set at 18:00 (6:00PM). You may specify the end time of the schedule. Select the Apply button to apply your changes.

## 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. Under this section, there is a 'Parameters' table with five columns: 'Destination', 'Netmask', 'Gateway', 'Interface', and 'Cost'. Each column has a corresponding input field. The 'Destination' field is currently empty. The 'Netmask' field is also empty. The 'Gateway' field is empty. The 'Interface' field is a dropdown menu with a blue arrow pointing down. The 'Cost' field is empty. Below the table, there are two buttons: 'Add' and 'Edit / Delete'.

Destination	Netmask	Gateway	Interface	Cost
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="v"/>	<input type="text"/>

**Destination:** The destination subnet IP address.

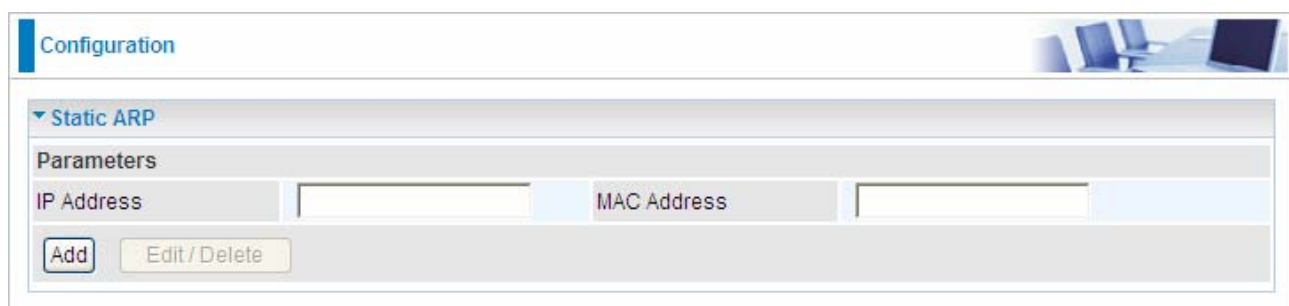
**Netmask:** Subnet mask of the destination IP addresses based on above destination.

**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. Under this section, there is a 'Parameters' table with two columns: 'IP Address' and 'MAC Address'. Each column has a corresponding input field. The 'IP Address' field is currently empty. The 'MAC Address' field is also empty. Below the table, there are two buttons: 'Add' and 'Edit / Delete'.

IP Address	MAC Address
<input type="text"/>	<input type="text"/>

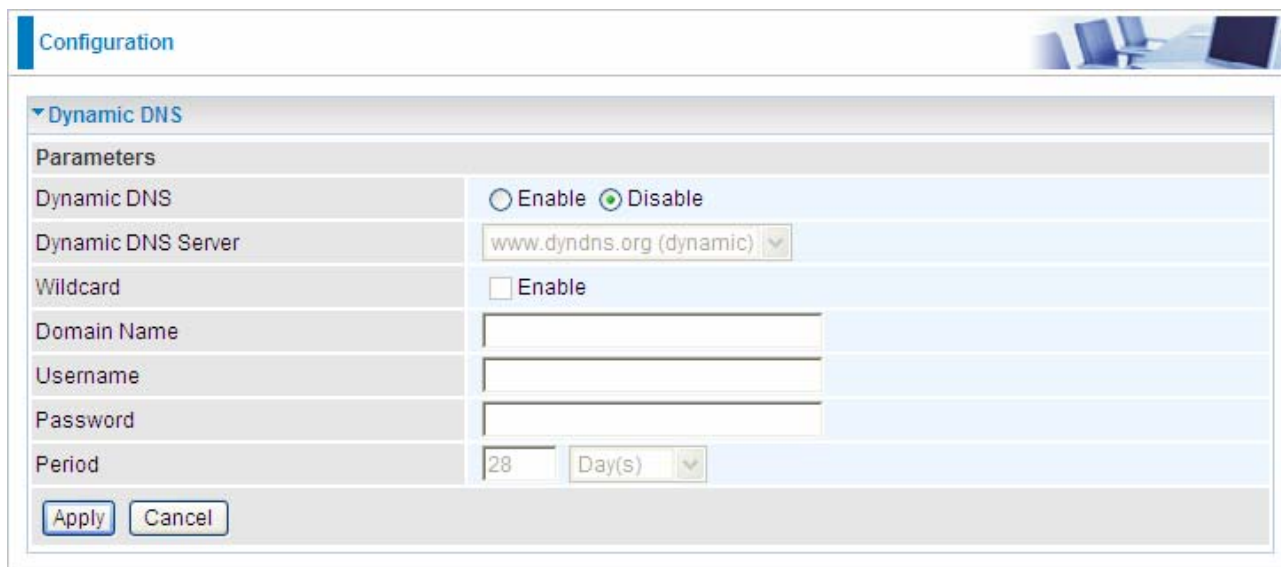
**IP Address:** Fill in the IP address of the host computer that is sending the data packet.

**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 interface titled "Configuration" with a sub-section "Dynamic DNS". Under "Parameters", there are several settings:

- Dynamic DNS:** Radio buttons for "Enable" and "Disable". The "Disable" option is selected.
- Dynamic DNS Server:** A dropdown menu showing "www.dyndns.org (dynamic)".
- Wildcard:** A checkbox labeled "Enable" which is currently unchecked.
- Domain Name:** An empty text input field.
- Username:** An empty text input field.
- Password:** An empty text input field.
- Period:** A text input field containing "28" and a dropdown menu set to "Day(s)".

At the bottom of the configuration area are "Apply" and "Cancel" buttons.

**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 a web interface for router configuration. At the top, there is a 'Configuration' tab. Below it, a 'Device Management' section is expanded. This section contains several fields: 'Device Host Name' with a sub-field 'Host Name' set to 'home.gateway'; 'Embedded Web Server' with 'HTTP Port' set to '80' (with a note: '(The default HTTP port number is 80.)') and 'Expire to auto-logout' set to '3 min(s)'; and 'Universal Plug and Play (UPnP)' with 'UPnP' set to 'Enable' (radio button selected) and 'UPnP Port' set to '2800'. At the bottom of the section are 'Apply' and 'Cancel' buttons.

### 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 **192.168.100.55**, and sets the logout time to be **100** minutes. The router only allows User A access from the IP address **192.168.100.55** to logon to the Web GUI by typing: <http://192.168.100.254:100> 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.

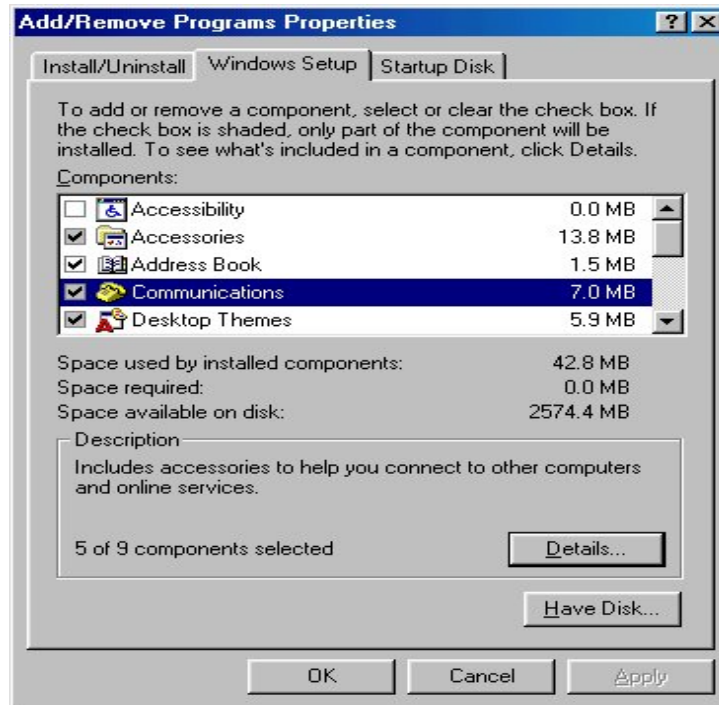
**UPnP Port:** The Default setting is 2800. It is highly recommended you use this port value. If this value conflicts with other ports already in use you may wish to change the port.

## Installing UPnP in Windows Example

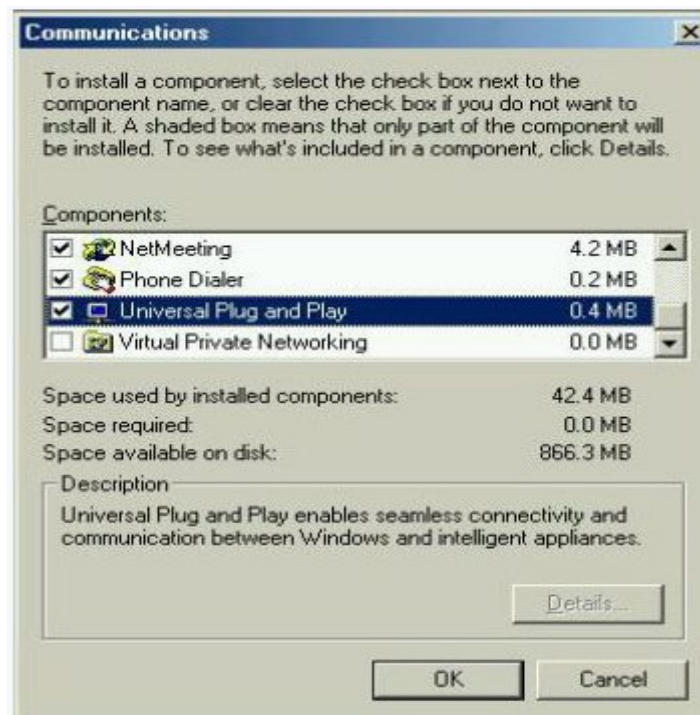
Follow the steps below to install the UPnP in Windows Me.

**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.

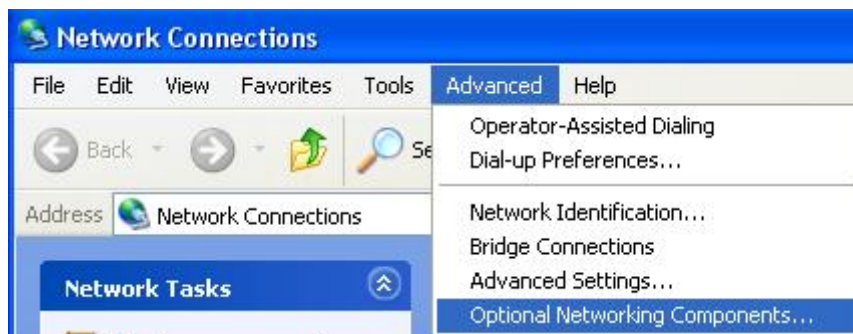
**Step 5:** Restart the computer when prompted.

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

**Step 1:** Click Start and Control Panel.

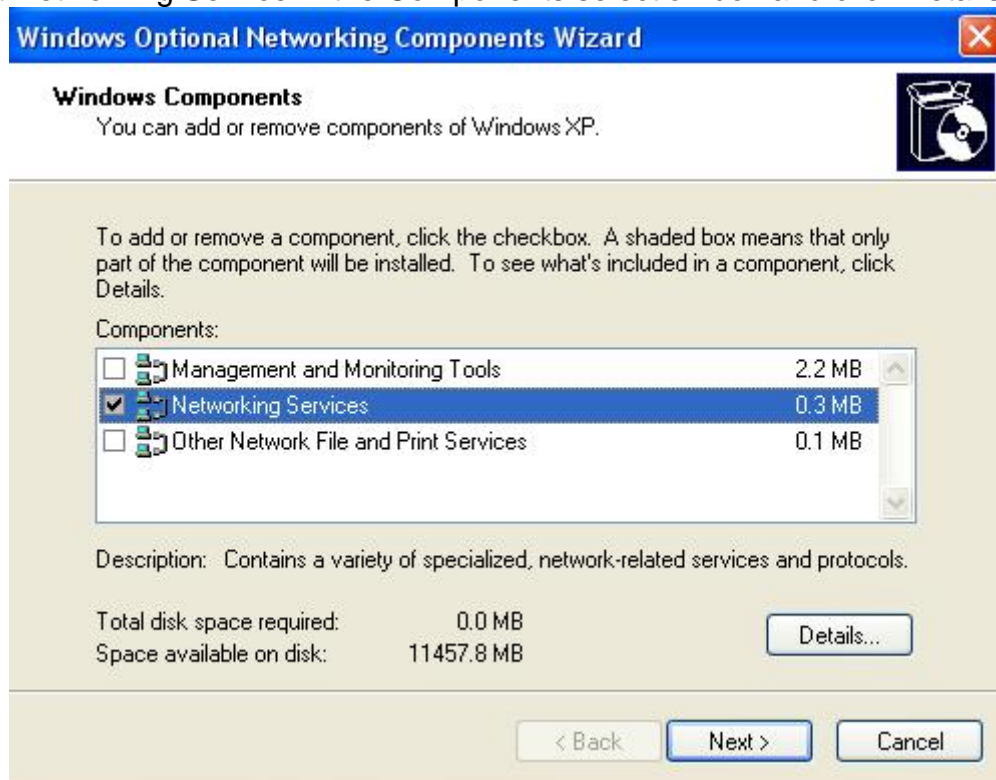
**Step 2:** Double-click Network Connections.

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



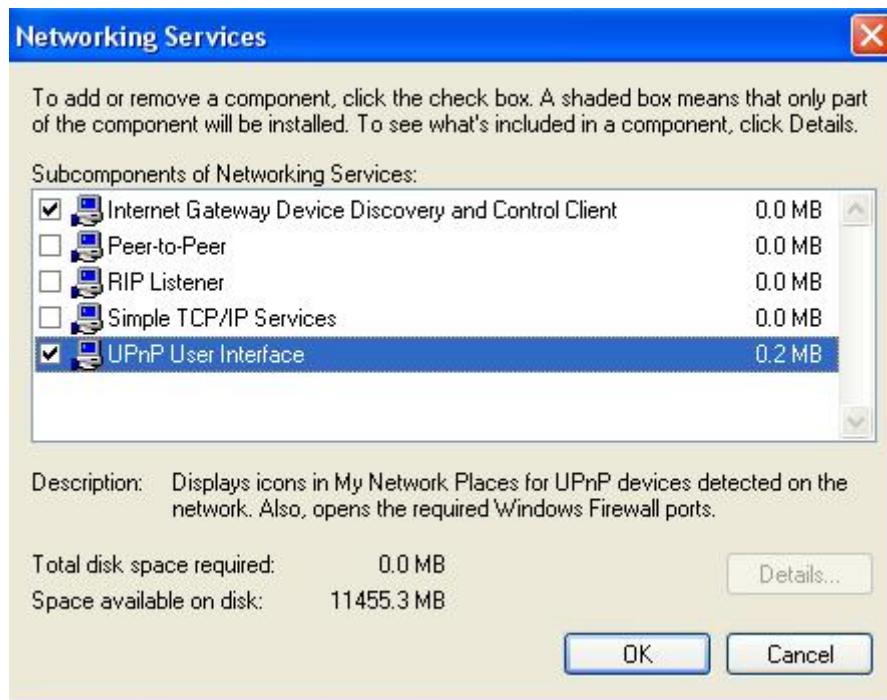
The Windows Optional Networking Components Wizard window displays.

**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.

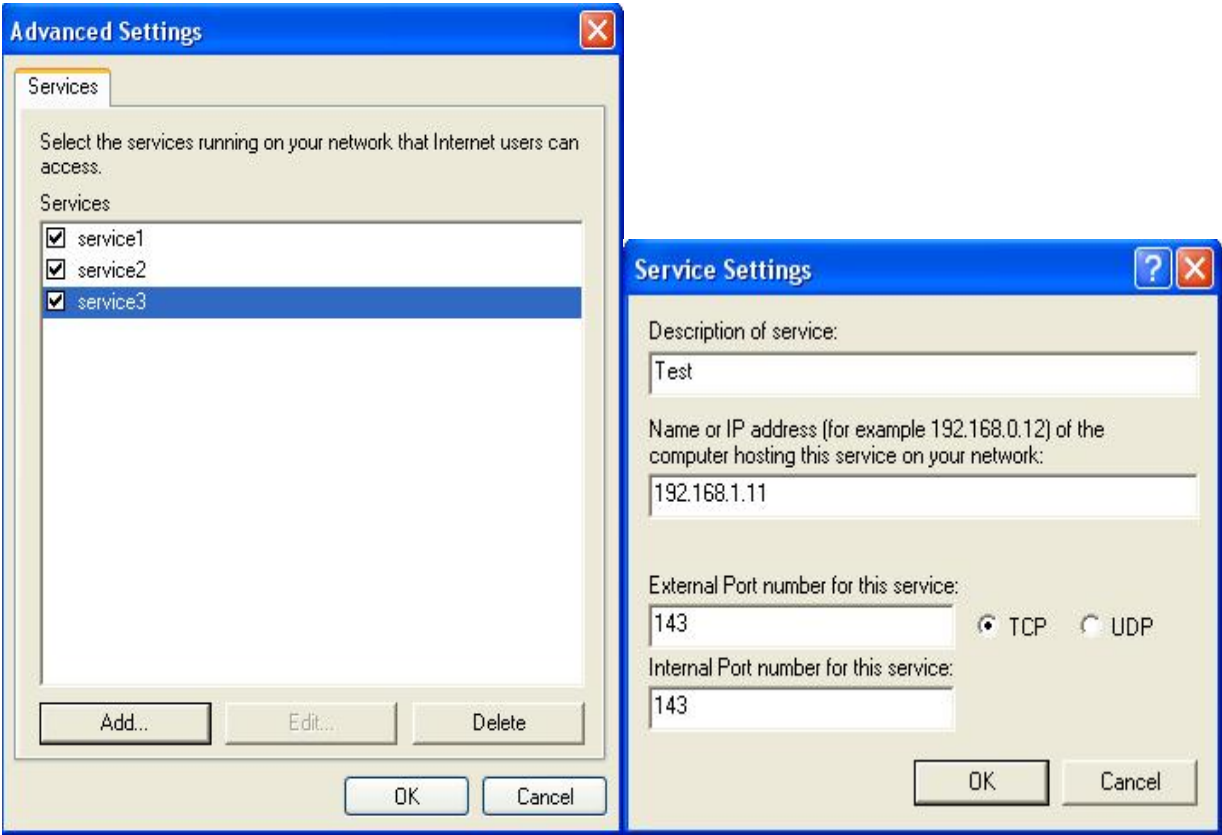
**Step 2:** Right-click the icon and select Properties.



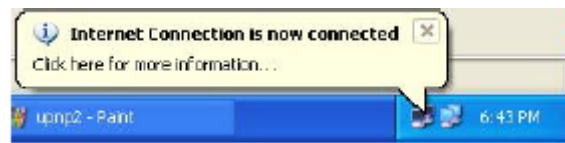
**Step 3:** In the Internet Connection Properties window, click Settings to see the port mappings that were automatically created.



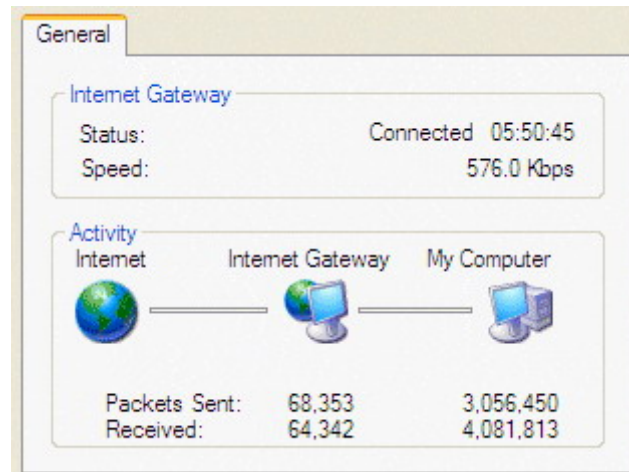
**Step 4:** You may edit or delete the port mappings or click Add to manually add port mappings.



**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

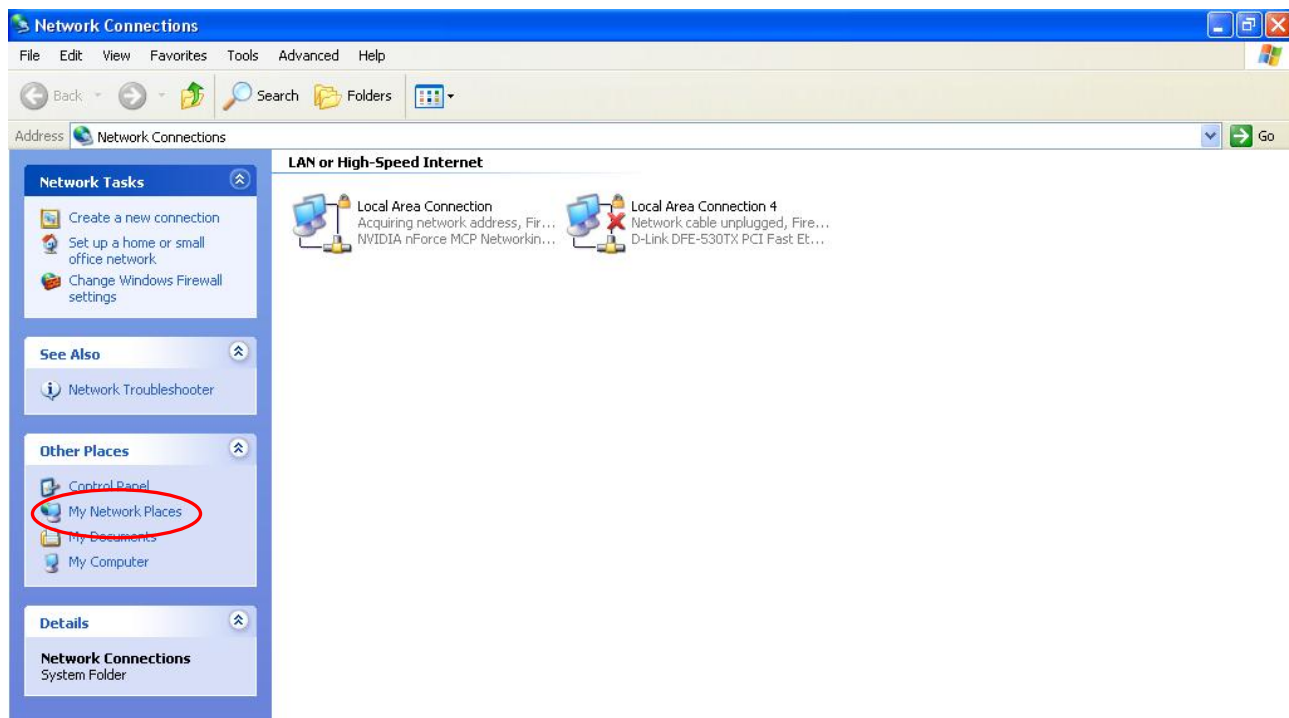
With UPnP, you can access web-based configuration for the PowerTracker/Billion SMART ENERGY GATEWAY without first finding out the IP address of the router. This helps if you do not know the router's IP address.

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.



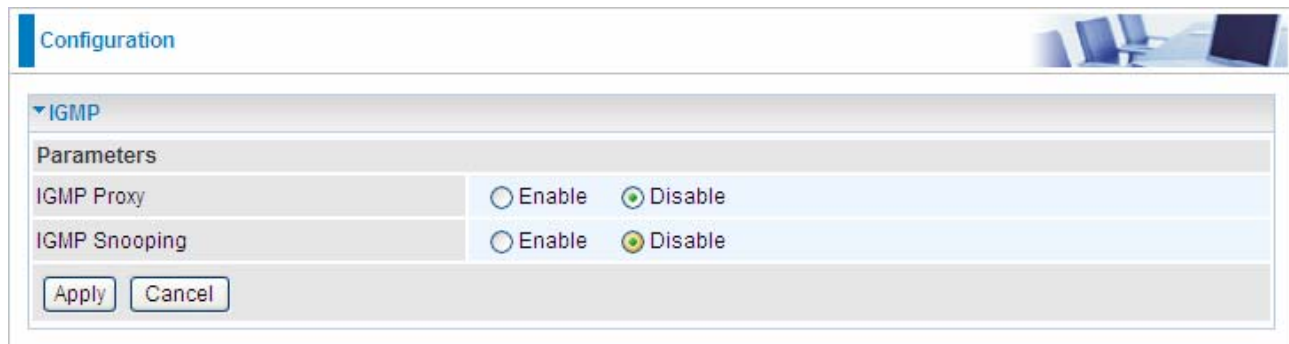
**Step 4:** An icon describing each UPnP-enabled device shows under Local Network.

**Step 5:** Right-click on the icon of your PowerTracker/Billion SMART ENERGY GATEWAY and select Invoke. The web configuration login screen displays.

**Step 6:** Right-click on the icon of your PowerTracker/Billion SMART ENERGY GATEWAY and select Properties. A properties window displays basic information about the PowerTracker/Billion SMART ENERGY GATEWAY.

## IGMP

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



The screenshot shows a web-based configuration interface for IGMP. At the top, there is a 'Configuration' tab. Below it, the 'IGMP' section is expanded, showing a 'Parameters' table. The table has two rows: 'IGMP Proxy' and 'IGMP Snooping'. Each row has two radio buttons: 'Enable' and 'Disable'. For 'IGMP Proxy', the 'Disable' button is selected. For 'IGMP Snooping', the 'Disable' button is also selected. At the bottom of the configuration area, there are 'Apply' and 'Cancel' buttons.

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  IP Address

Write Community  IP Address

**SNMP V3**

Username  Password

### 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

Configuration

Remote Access

Parameters

Remote Access Control

☐ Enable

Duration

min(s) (0: Always On)

Apply

Allowed Access IP Address Range

Valid

☒

IP Address Range

~

Add

Edit / Delete

## 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

Apply

# Restart

Click **Restart** with option **Current Settings** to reboot your router (and restore your last saved configuration).

Configuration

Restart

After restarting. Please wait for several seconds to let the system come up.

Restart device with

☐ Factory Default Settings

☒ Current Settings

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.

## 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
<b>None of the LEDs are on when you turn on the router.</b>	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
<b>Can't ping any PCs on the LAN.</b>	<p>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.</p> <p>Verify that the IP address and the subnet mask are consistent between the router and the workstations.</p>

## Problems with the FTP Server

Problem	Corrective Action
<b>FTP client which behind firewall remote access the router fail</b>	<p>Because the firewall has NAT function, this make can't access the router successful. There are two suggestions to solve the problem.</p> <ol style="list-style-type: none"><li>1. Set the FTP port as 21, you can access the router successful</li><li>2. Use FTP client software (such as flashfxp V3.6), set the connect behaviour to be "active mode" you can also access the router successful.</li></ol>

## Problems with the Printer

Problem	Corrective Action
<b>Can't access the printer</b>	Make sure you have added printer correctly, please reference <b>Set up of Printer client</b> .
<b>The printer can't print though the printer have been added correctly</b>	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 PowerTracker/Billion

### Worldwide:

<http://www.powertracker.com.au> ; <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.