

BiPAC 7300GX

3G/ ADSL2+ Wireless Router

User's Manual

Table of Contents

Chapter 1	3
1.1 Introducing the BiPAC 7300GX	3
1.2 Features.....	5
1.3 Applications of the BiPAC 7300GX	8
Chapter 2	9
2.1 Important Notes	10
2.2 Package Contents	10
2.3 The Front LEDs	11
2.4 The Rear Ports	12
2.5 Cabling	14
Chapter 3	15
3.1 Before Configuration.....	15
3.2 Factory Default Settings	20
3.3 LAN and WAN Port Addresses	21
3.4 Information from your ISP	22
3.5 Configuring with your BiPAC 7300GX	23
Chapter 4	27
4.1 Status.....	28
4.2 Quick Start	29
4.3 WAN	31
4.4 WLAN	35
Chapter 5	38
5.1 Status.....	39
5.1.1 ADSL Status.....	41
5.1.2 3G Status.....	42
5.1.2 ARP Table	43
5.1.3 DHCP Table	44
5.1.4 System Log.....	45
5.1.5 Firewall Log	46
5.2 Quick Start	47
5.3 Configuration	50
5.3.1 LAN (Local Area Network)	51
5.3.2 WAN (Wide Area Network)	70
5.3.3 System.....	81
5.3.4 Firewall	86
5.3.5 QoS (Quality of Service)	95
5.3.6 Virtual Server	100
5.3.7 Time Schedule	105
5.3.8 Advanced.....	107
5.4 Save Configuration to Flash	121

5.5 Restart	122
5.6 Logout.....	123
Chapter 6	124

Chapter 1

Introduction

1.1 Introducing the BiPAC 7300GX

Thank you for purchasing the BiPAC 7300GX ADSL2+ Router by Billion. Your new router is an all-in-one unit that combines an ADSL modem, ADSL2/2+ router, PC card slot for 3G/HSDPA data card and Ethernet network switch to provide everything you need to get the machines on your network connected to the Internet over an ADSL broadband connection.

The BiPAC 7300GX router complies with ADSL2+ standards for deployment worldwide and supports downstream rates of up to 24 Mbps and upstream rates of up to 1 Mbps. Designed for small office, home office and residential users, the router enables even faster Internet connections. You can enjoy ADSL services and broadband multimedia applications such as interactive gaming, video streaming and real-time audio much easier and faster than ever before. Otherwise, the PC card slot in BiPAC 7300GX is ready for 3rd generation (3G) data service. You can insert the 3G/HSDPA data card into PC card slot to instead ADSL to enjoy your internet connection.

The BiPAC 7300GX supports PPPoA (RFC 2364 – PPP (Point-to-Point Protocol) over ATM Adaptation Layer 5), RFC 1483 encapsulation over ATM (bridged or routed), PPP over Ethernet (RFC 2516) to establish a connection with your ISP. Your new router also supports VC-based and LLC-based multiplexing.

The perfect solution for connecting a small group of PCs to a high-speed broadband Internet connection, the BiPAC 7300GX 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 BiPAC 7300GX 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.

1.2 Features

● Express Internet Access – ADSL2/2+ capable

The BiPAC 7300GX complies with ADSL worldwide standards. Supporting downstream rates of 8Mbps with ADSL, the router is capable of up to 12/24 Mbps with ADSL2/2+, and upstream rates of up to 1 Mbps. Users enjoy not only high-speed ADSL services but also broadband multimedia applications such as interactive gaming, video streaming and real-time audio which are easier and faster than ever. The router is compliant with Multi-Mode standard (ANSI T1.413, Issue 2; G.dmt (ITU G.992.1); G.hs (ITU G994.1); G.dmt.bis (ITU G.992.3); and G.dmt.bisplus (ITU G.992.5)

● Communication Diversity with HSDPA/UMTS

Including one PC card slot, the BiPAC 7300GX router allows the users to insert a 3G/HSDPA PC card to share 3G/HSDPA, UMTS, EDGE, GPRS, or GSM Internet connection.

● 802.11g Wireless AP with WPA Support

With integrated 802.11g Wireless Access Point in the router, the device offers a quick and easy access among wired network, wireless network and broadband connection (ADSL) with single device simplicity, and as a result, mobility to the users. In addition to 54 Mbps 802.11g data rate, it also interoperates backward with existing 802.11b equipment. The Wireless Protected Access (WPA) and Wireless Encryption Protocol (WEP) supported features enhance the security level of data protection and access control via Wireless LAN.

● Fast Ethernet Switch

A 4-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.

● Multi-Protocol to Establish a Connection

The router supports PPPoA (RFC 2364 - PPP over ATM Adaptation Layer 5), RFC 1483 encapsulation over ATM (bridged or routed), PPP over Ethernet (RFC 2516) to establish a connection with an ISP. The router also supports VC-based and LLC-based multiplexing.

● **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.billion.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 BiPAC 7300GX 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.

1.3 Applications of the BiPAC 7300GX



Chapter 2

Product Overview

Standards-Based Technology

The BiPAC 7300GX Wireless Router utilizes the **802.11g** standard. The IEEE **802.11g** standard is an extension of the 802.11b standard. It increases the data rate up to 54Mbps* within the 2.4GHz band, utilizing **OFDM technology**. This means that in most environments, within the specified range of this device, you will be able to transfer large files quickly or even watch a movie in MPEG format over your network without noticeable delays. This technology works by transmitting high-speed digital data over a radio wave utilizing **OFDM (Orthogonal Frequency Division Multiplexing)** technology. **OFDM** works by splitting the radio signal into multiple smaller sub-signals that are then transmitted simultaneously at different frequencies to the receiver. **OFDM** reduces the amount of **crosstalk** (interference) in signal transmissions.

The BiPAC 7300GX is backwards compatible with 802.11b devices. This means that if you have an existing 802.11b network, the devices in that network will be compatible with 802.11g devices at speeds of up to 11Mbps in the 2.4GHz range.

Installation Considerations

The BiPAC 7300GX Wireless Router lets you access your network, using a wireless connection, from virtually anywhere within its operating range. 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 BiPAC 7300GX and other network devices to a minimum - each wall or ceiling can reduce your BiPAC 7300GX 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 aluminum 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.

2.1 Important Notes



Warning

- ✓ Do not use the BiPAC 7300GX in high humidity or high temperatures.
- ✓ Do not use the same power source for the BiPAC 7300GX as other equipment.
- ✓ Do not open or repair the case yourself. If the BiPAC 7300GX 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.



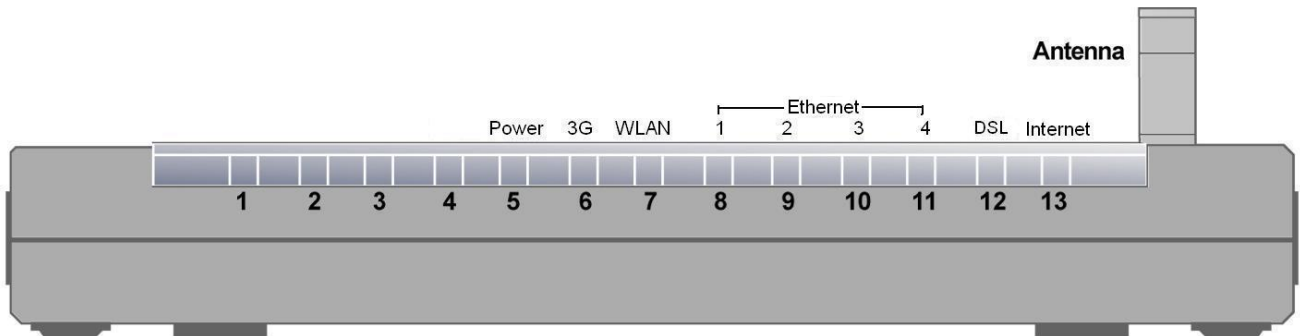
Attention

- ✓ Place the BiPAC 7300GX 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.
- ✓ Have better use the 3G/ HSDPA data card that offered by ISP or recommend on the color box.

2.2 Package Contents

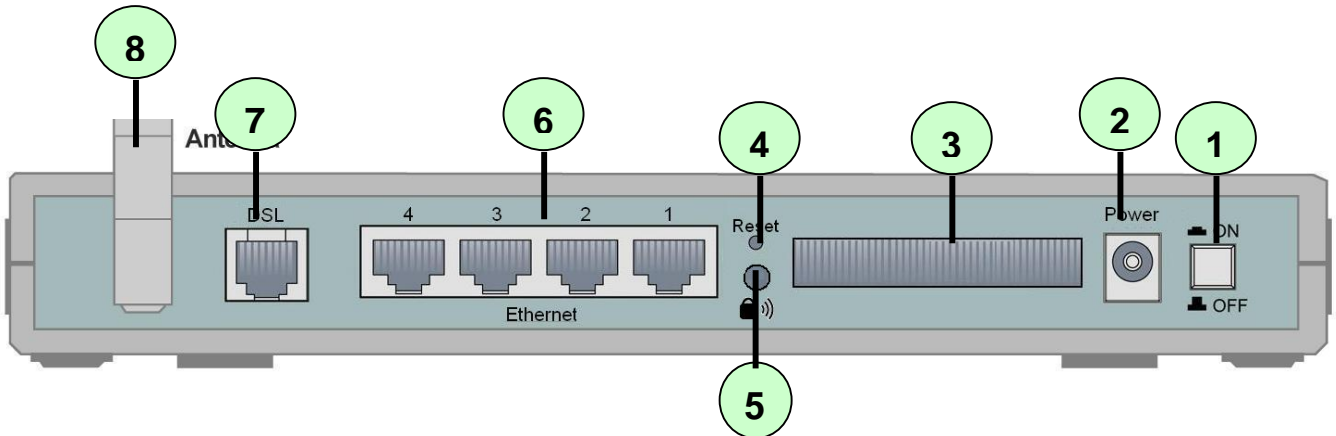
- BiPAC 7300GX ADSL2+ Router
- CD-ROM containing the online manual
- RJ-11 ADSL/telephone Cable (1.8M)
- Ethernet (CAT-5 LAN) Cable (1.8M Straight)
- AC-DC power adapter (12V DC, 1A)
- Quick Start Guide (130*185mm)

2.3 The Front LEDs



LED		Description
5	Power	<ul style="list-style-type: none"> ● Lights Green when the power and router system are ready. ● Flickering Green when system is booting or system upgrade. ● Lights Red when device can not boot successfully. ● Lights off means power off.
6	3G	<ul style="list-style-type: none"> ● Lights when 3G service is ready.
7	WLAN	<ul style="list-style-type: none"> ● Lights Green when the wireless connection is established. ● Flashes when sending/receiving data.
8-11	Ethernet Port 1-4	<ul style="list-style-type: none"> ● Steady glow when connected to an Ethernet device. ● Glows green for 100Mbps; Orange for 10Mbps. ● Blinking light when data is Transmitted / Received.
12	DSL	<ul style="list-style-type: none"> ● Lights Green when successfully connected to an ADSL DSLAM (linesync). ● Flashing Green when DSL attempting sync.
13	Internet	<ul style="list-style-type: none"> ● Lights Green when the device has a WAN IP address. ● Lights RED when device attempted to become IP connected and failed. ● Lights off when modem power off, modem in bridged mode or internet connection not present.

2.4 The Rear Ports



Port		Description
1	Power Switch	Power ON/OFF switch.
2	Power	Connect the supplied power adapter to this jack.
3	3G card slot	Connect the 3G card bus data card to this slot
4	Reset	<p>After the router is powered on, press this reset button using the end of paper clip or other small pointed object to reset the router and to restore it to factory default settings.</p> <ol style="list-style-type: none"> 1. Recovery procedures for non-working routers (e.g. after a failed firmware upgrade flash). 2. Recovery procedures for a lost web interface password:
5	WPS	Push WPS button to trigger Wi-Fi Protected Setup function.
6	Ethernet	Connect a UTP Ethernet cable (Cat-5 or Cat-5e) to one of the four LAN ports when connecting to a PC or an office/home network of 10Mbps or 100Mbps.
7	DSL	Connect the supplied RJ-11 ("telephone") cable to this port when connecting to the ADSL/telephone network.
8	Antenna	Connect the detachable antenna to this port.



The 3G card slot does not support hot swap (swapping whilst the device is still turned on). If you need to change the 3G card, please turn the power off before replacing the 3G card.

Attention

● The detail instruction in Reset Button

1. Recovery procedures for non-working routers (e.g. after a failed firmware upgrade flash):

Hold the *Reset Button* on the back of the modem in. Keep this button held in and turn on the modem. Once the lights on the modem have stopped flashing, release the *Reset Button*. The modem's emergency-reflash web interface will then be accessible via <http://192.168.0.254> where you can upload a firmware image to restore the modem to a functional state. Please note that the modem will only respond via its web interface at this address, and will not respond to ping requests from your PC or to telnet connections.

2. Recovery procedures for a lost web interface password:

After turning the router on, please press the *Reset Button* on the back of the modem, and hold the button in until all lights on the modem begins to flash and then it will reboot with factory default settings. The login name will be reset to *admin* and the password will be reset to *admin*, and the modem will be accessible via its default IP address at <http://192.168.1.254/>



Before powering on the router to enter the recovery process, please configure the IP address of the PC as **192.168.0.1** and proceed with the following step by step guide.

1. Power the router off.
2. Hold the "Reset Button".
3. Power on the router. Then Router's IP will reset to Emergency IP address (Say 192.168.0.254)
4. Download the firmware.

2.5 Cabling

One of the most common causes of problems is because of bad cabling or ADSL line(s). 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 ADSL line LEDs are lit. If they are not, verify that you are using the proper cables.

Ensure that all other devices connected to the same telephone line as your Billion router (e.g. telephones, fax machines, analog modems) have a line filter connected between them and the wall socket (unless you are using a Central Splitter or Central Filter installed by a qualified and licensed electrician), and to ensure that all line filters are correctly installed and the right way around. Missing line filters or line filters installed being the wrong way around can cause problems with your ADSL connection, which includes frequent disconnections.

Chapter 3

Installation

You can configure the BiPAC 7300GX 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.

3.1 Before Configuration

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

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



Any TCP/IP capable workstation can be used to communicate with or through the BiPAC 7300GX. To configure other types of workstations, please consult the manufacturer's documentation.

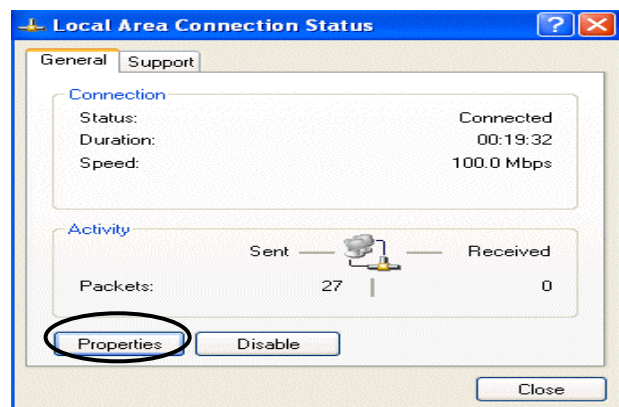
Configuring a PC in Windows XP

1. Go to **Start / Control Panel (in Classic View)**. In the Control Panel, double-click on **Network Connections**

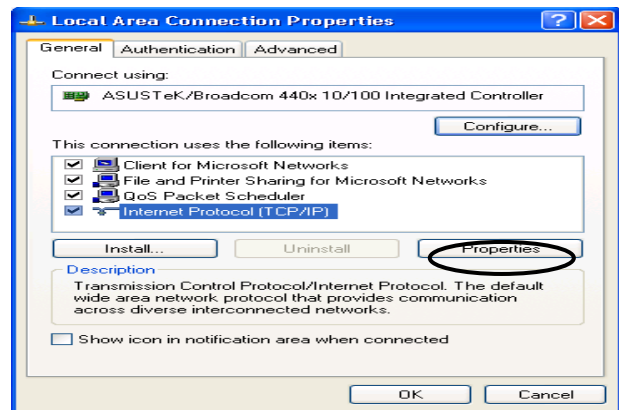


2. Double-click **Local Area Connection**.

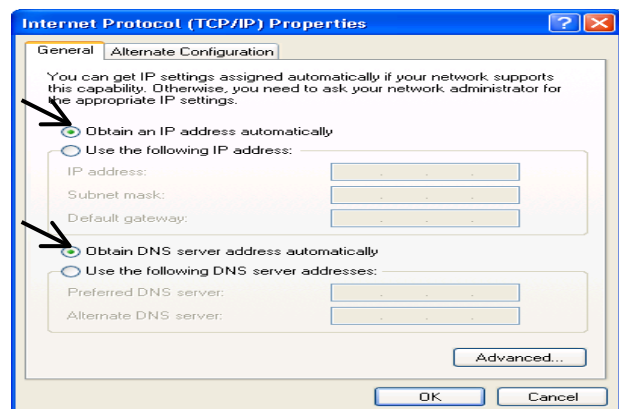
3. In the **Local Area Connection Status** window, click **Properties**.



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 a PC in Windows 2000

1. Go to **Start / Settings / Control Panel**.

In the Control Panel, double-click on **Network and Dial-up Connections**.

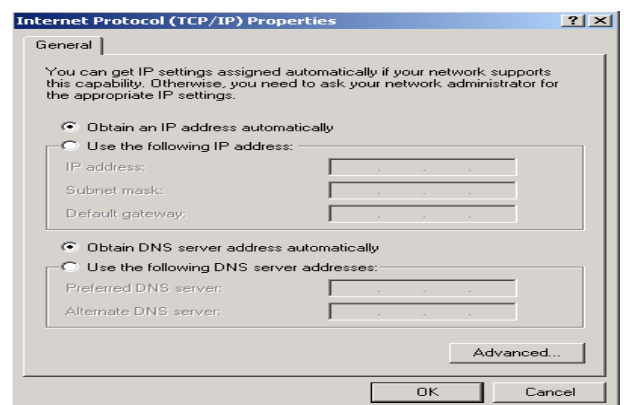
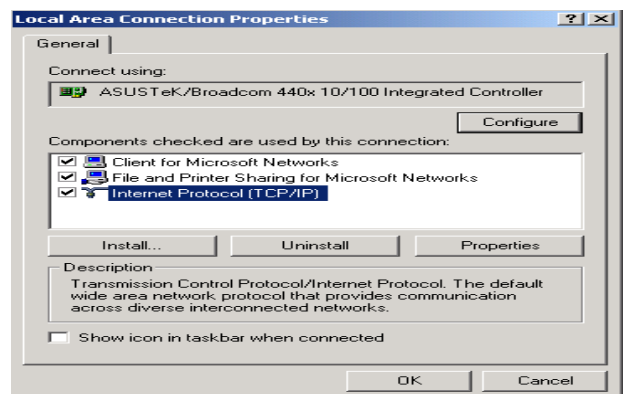
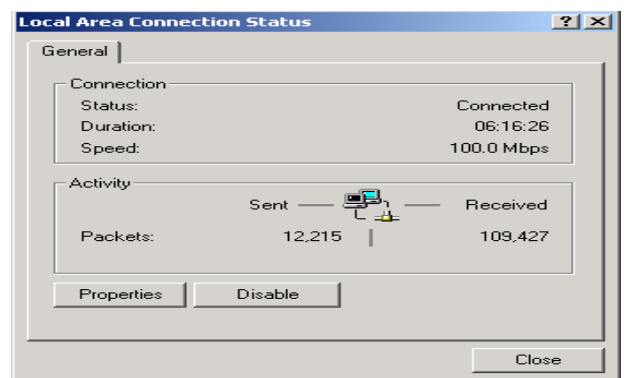
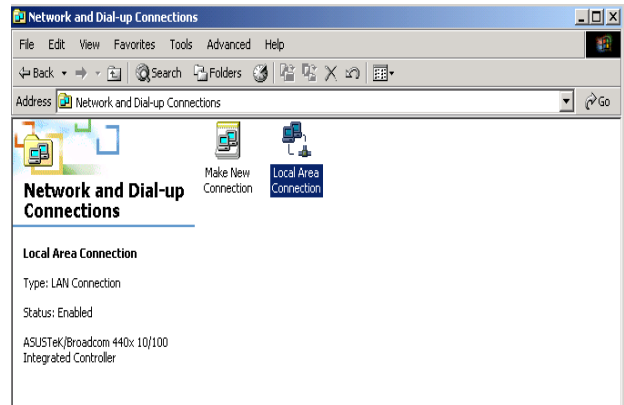
2. Double-click **Local Area Connection**.

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.

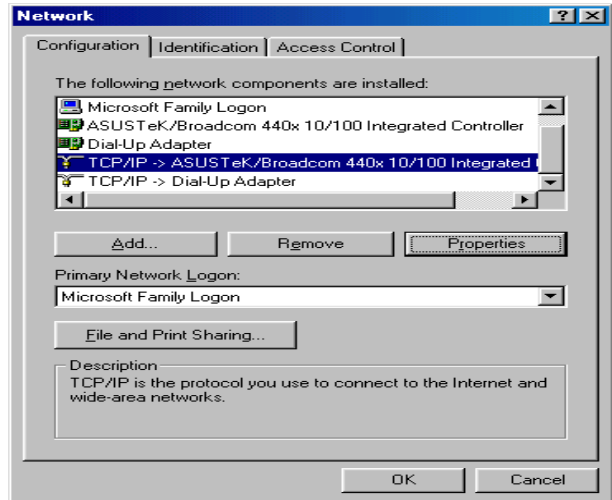


Configuring PC in Windows 98/Me

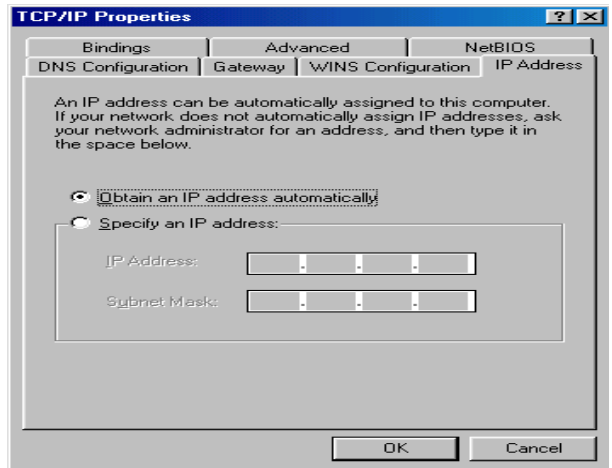
1. Go to **Start / Settings / Control Panel**.

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.

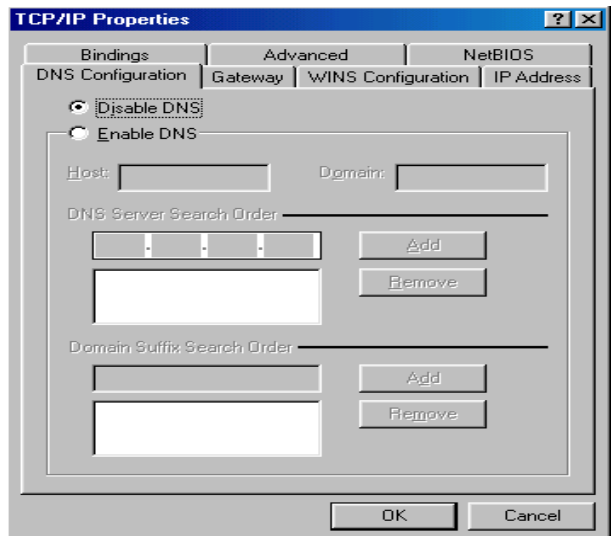


3. Select the **Obtain an IP address automatically** radio button.



4. Then select the **DNS Configuration** tab.

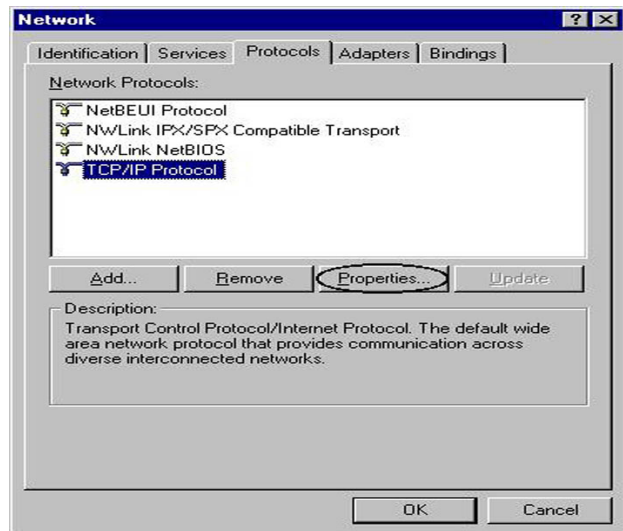
5. Select the **Disable DNS** radio button and click **OK** to finish the configuration.



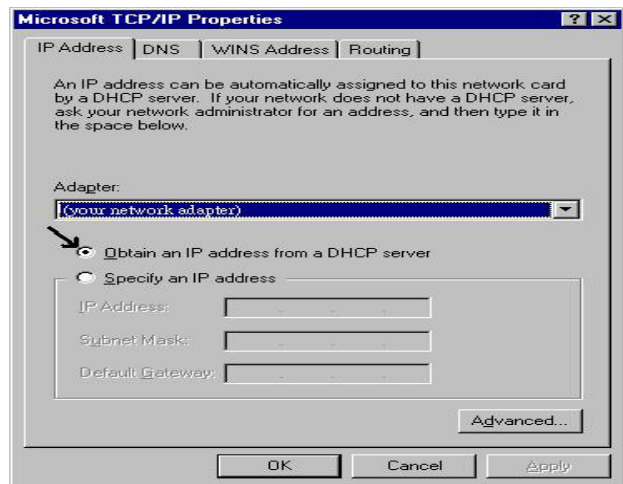
Configuring PC in Windows NT4.0

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**.



3.2 Factory Default Settings

Before configuring the BiPAC 7300GX 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.

● LAN Device IP Settings:

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

● ISP setting in WAN site:

- ✘ PPPoE

● DHCP Server:

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

3.3 LAN and WAN Port Addresses

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

LAN Port		WAN Port
IP address	192.168.1.254	The PPPoE function is <i>enabled</i> to automatically get the WAN port configuration from the ISP, but you have to set the username and password first.
Subnet Mask	255.255.255.0	
DHCP server function	Enabled	
IP addresses for distribution to PCs	100 IP addresses continuing from 192.168.1.100 through 192.168.1.199	

3.4 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, PPPoA, MPoA or Pure Bridge.

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

PPPoE	VPI/VCI, VC-based/LLC-based multiplexing, 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).
PPPoA	VPI/VCI, VC-based/LLC-based multiplexing, Username, Password, and Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually).
RFC1483 Bridged	VPI/VCI, VC-based/LLC-based multiplexing to use Bridged Mode.
RFC1483 Routed	VPI/VCI, VC-based/LLC-based multiplexing, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is fixed IP address).
IPoA	VPI/VCI, VC-based/LLC-based multiplexing, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is fixed IP address).

3.5 Configuring with your BiPAC 7300GX



1. To configure this device, you must have IE 5.0 / Netscape 4.5 or above installed
2. You may configure the router for Internet access in two ways:
(A) Easy Sign-On (EZSO) **(B) Web Configuration**

Easy Sign On:

After setting up the router with appropriate cables plugged, proceed to load the internet browser to surf Internet, the EZSO WEB GUI will be popped up and request you to input some basic information you get from ISP. After this, you can surf Internet right away.

Follow the Easy Sign-On configuration wizard and it will guide you to complete the basic network configuration.

1. Select the connect mode which you wants to set up and than click continue. (There are two mode that you may select, one is “ADSL” another is “3G”)

BILLION ADSL Firewall Router Powering communications with Security

Easy Sign On

WAN Port (WAN > Wireless)

Select WAN Port

Connect Mode	ADSL (Recommended)
Protocol	PPPoE (RFC2516, PPP over Ethernet)
VPI / VCI	8 / 35
Username	Username
IP Address	0.0.0.0

Continue Jump to Wireless setting Done

2. Choose “Auto” or “Manually” to scan ADSL information.

BILLION ADSL Firewall Router Powering communications with Security

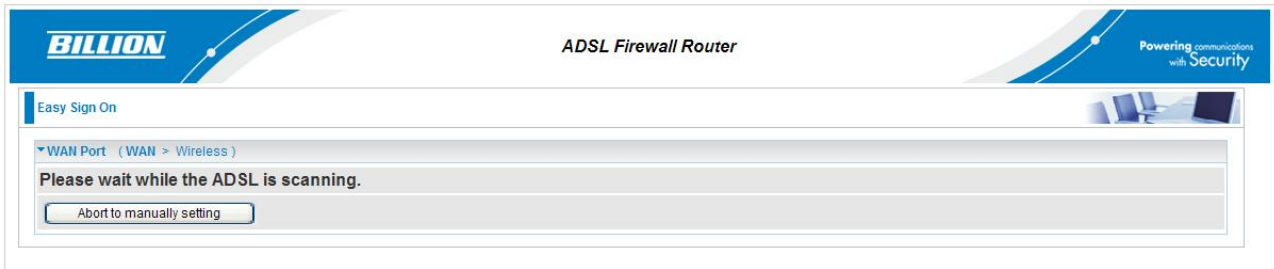
Easy Sign On

WAN Port (WAN > Wireless)

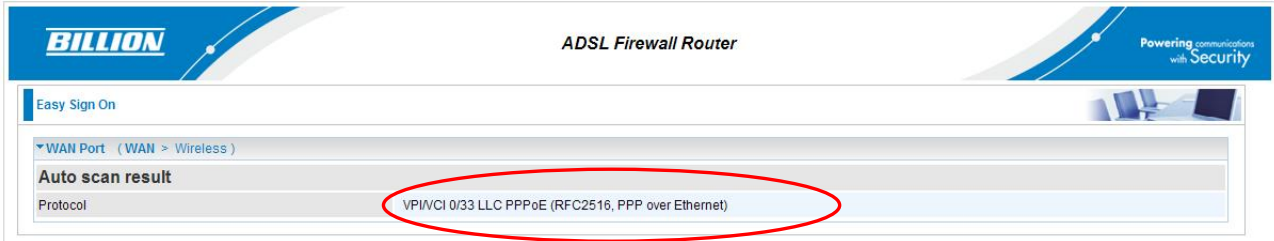
ADSL Line Is Ready.

Auto scan Auto Manually

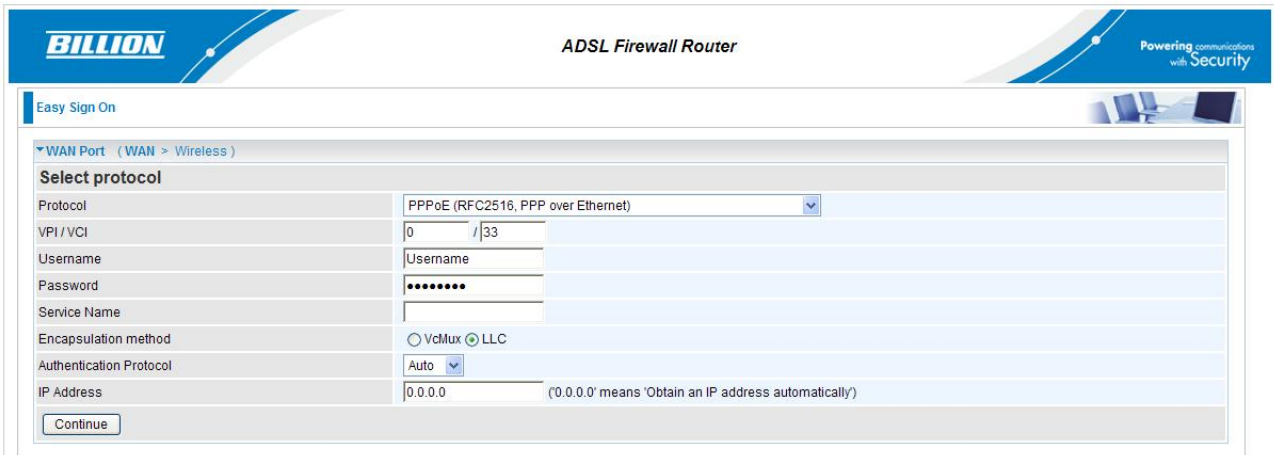
Continue



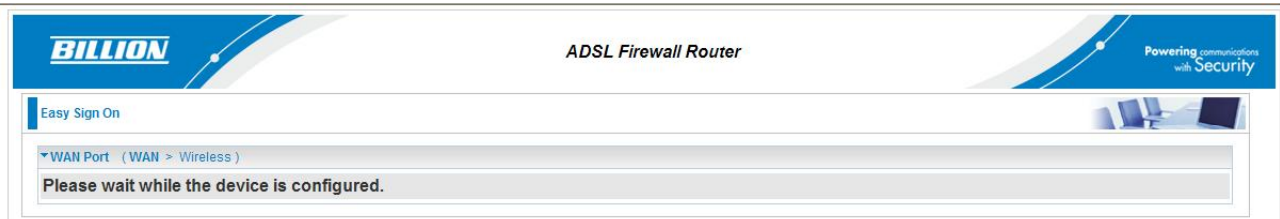
3. Show Auto scan result - Protocol information.



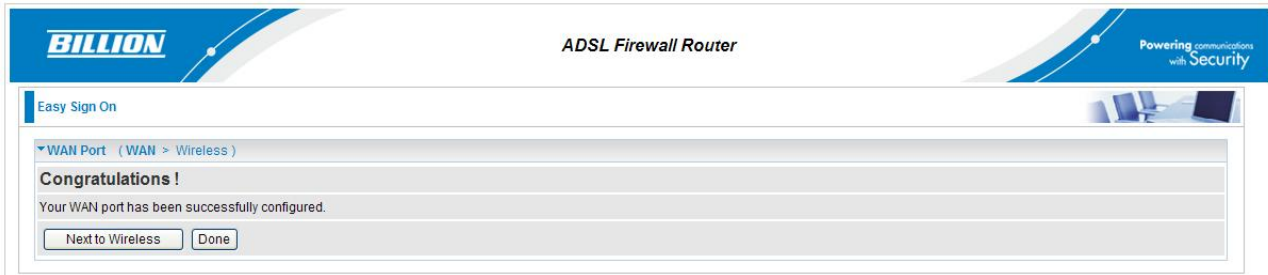
4. Please enter "Username" and "Password" as supplied by your ISP (Internet Service Provider) and click continue.



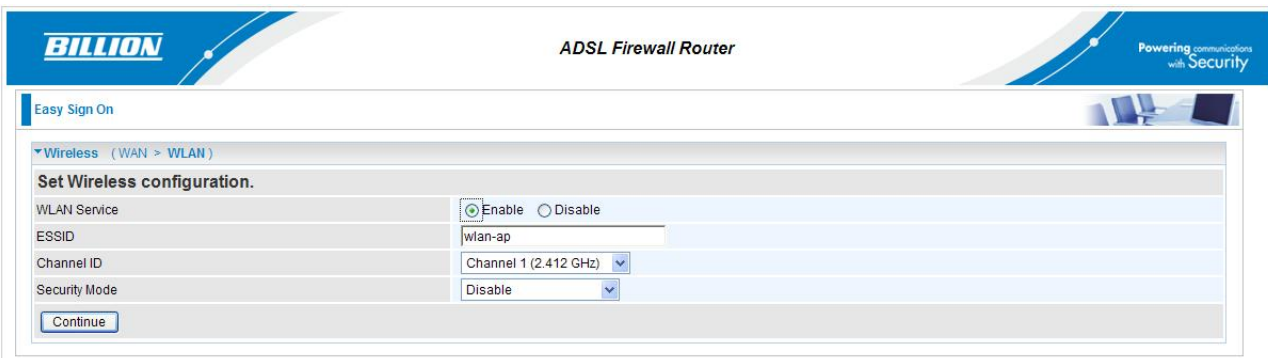
5. Wait for the device to be configured.



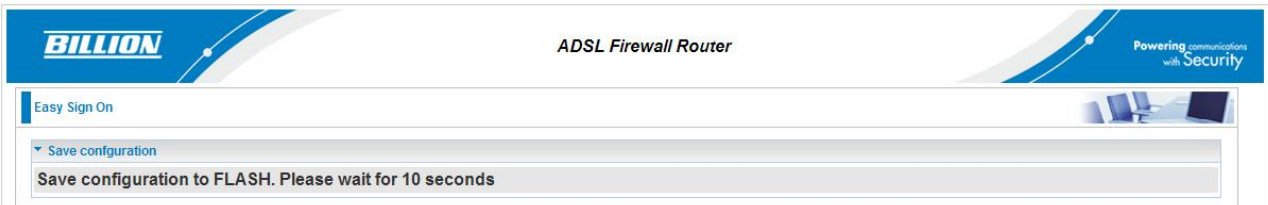
6. You've have completed the WAN port setup and now click "next to wireless" to proceed to the wireless configuration.



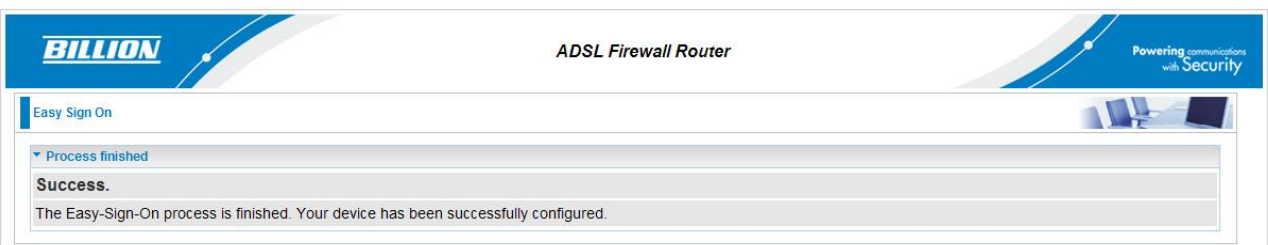
7. Please configure the Wireless LAN setting and click Continue.



8. Save Configuration.

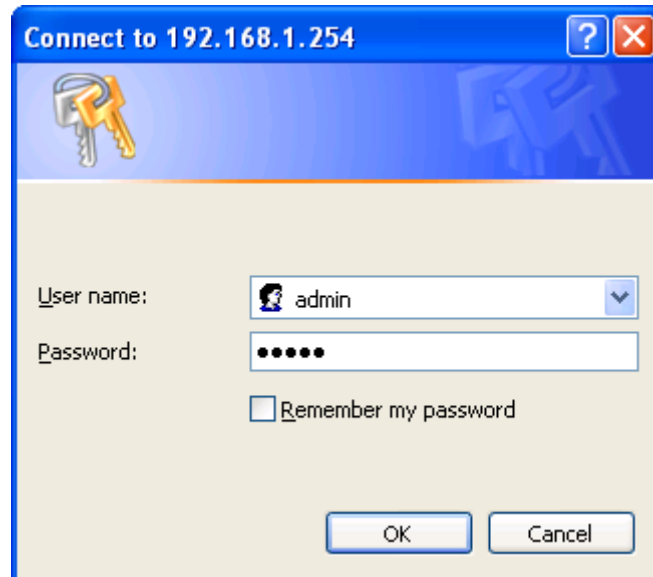


9. Congratulations!! You've completed the setup procedure and you are now ready to surf the Internet, enjoy.



Web Configuration:

Open your web browser, enter the IP address of your router, which by default is **192.168.1.254**, and click “Go”, a user name and password window prompt appears. The default username and password are “**admin**” and “**admin**”.



Congratulations! You have successfully logged on to your BiPAC 7300GX ADSL2+ Router!

Chapter 4

Basic Configuration

Once you have logged on to your BiPAC 7300GX ADSL2+ 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:

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

BILLION ADSL Firewall Router Powering communications with Security

Basic

- Advance
- Status
- Quick Start
- WAN
- WLAN

Status

▼ **Device Information**

Model Name	BiPAC 7300GX
System Up-Time	15 Hour(s) 46 min(s)
Hardware Version	7300GX
Software Version	1.03A-RC2

▼ **Port Status**

Ethernet	✓
ADSL	✗ 0 / 0 kbps
3G	✗
Wireless ▶	✓

▼ **WAN**

Port ▶	Protocol VPI/VCI	Operation	Connection	IP Address	Netmask	Gateway	Primary DNS
ADSL	PPPoE 8/35		Link Down				

Save Config Restart Logout

Copyright © Billion Electric Co., Ltd. All rights reserved.

4.1 Status

Device Information	
Model Name	BIPAC 7300GX
System Up-Time	1 Hour(s) 45 min(s)
Hardware Version	7300GX
Software Version	1.03A-RC2

Port Status	
Ethernet	✓
ADSL	✗ 0 / 0 kbps
3G	✗
Wireless ▶	✓

WAN							
Port ▶	Protocol VPI/VCI	Operation	Connection	IP Address	Netmask	Gateway	Primary DNS
ADSL	PPPoE 8/35		Link Down				

Device Information

- **Model Name:** Provide a name for the router for identification purposes.
- **System Up-Time:** Records system up-time.
- **Hardware Version:** Device version
- **Software Version:** Firmware version

Port Status

- **Port Status :** User can look up to see if they are connected to Ethernet, ADSL, 3G or Wireless.

WAN

- **Port:** Name of the WAN connection.
- **Protocol VPI/VCI:** Virtual Path Identifier and Virtual Channel Identifier
- **Operation:** The current status in WAN interface.
- **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.

4.2 Quick Start

The screenshot shows the configuration interface for a BILLION ADSL Firewall Router. The page title is "ADSL Firewall Router" and it features the slogan "Powering communications with Security". A navigation menu on the left includes "Basic", "Advance", "Status", "Quick Start" (highlighted), "WAN", and "WLAN". The main content area is titled "Quick Start" and shows the "WAN Port" configuration page. The "Select WAN Port" section has the following fields:

Connect Mode	ADSL (Recommended)
Protocol	PPPoE (RFC2516, PPP over Ethernet)
VPI / VCI	8 / 35
Username	Username
IP Address	0.0.0.0

At the bottom of this section are two buttons: "Continue" and "Jump to Wireless setting".

At the bottom of the page are three icons: "Save Config", "Restart", and "Logout". The footer contains the text: "Copyright © Billion Electric Co., Ltd. All rights reserved."

Select WAN Port

This screenshot shows the "Select WAN Port" configuration page with the "Connect Mode" set to "3G". The fields are as follows:

Connect Mode	3G
TEL No.	*99***1#
Username	
APN	internet

Buttons "Continue" and "Jump to Wireless setting" are visible at the bottom of the form.

- **Connect Mode:** User can choose either "ADSL" or "3G" mode.
- **TEL No.:** The dial string to make a GPRS / 3G user internetworking call.
- **Username:** 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.

Quick Start

WAN Port (WAN > Wireless)

Select WAN Port

Connect Mode	ADSL (Recommended) ▾
Protocol	PPPoE (RFC2516, PPP over Ethernet)
VPI / VCI	8 / 35
Username	Username
IP Address	0.0.0.0

Continue Jump to Wireless setting

- **Protocol:** The current ATM protocol in the device.
- **VPI / VCI:** The current value of VPI/VCI in the device.
- **Username:** To show current authentication username.
- **IP Address:** To show current value of IP address in the device.

■ Set Wireless configuration

Quick Start

Wireless (WAN > WLAN)

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 ▾

Continue

- **WLAN Service:** Default setting is set to **Enable**. If you don't want to use wireless, both 802.11g and 802.11b, device in your network, you can select **Disable**.
- **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**.

4.3 WAN

The screenshot shows the configuration interface for a BILLION ADSL Firewall Router. The page title is "ADSL Firewall Router" and it includes the BILLION logo and the tagline "Powering communications with Security". On the left, there is a navigation menu with options: Basic, Advance, Status, Quick Start, WAN (highlighted), and WLAN. The main content area is titled "Configuration" and shows the "WAN Port" settings. Under "WAN Connection", the "Main Port" is set to "ADSL" (Current Main Port: ADSL). Under "Parameters", the "Protocol" is "PPPoE (RFC2516, PPP over Ethernet)", "VPI / VCI" is "8 / 35", "Username" is "Username", "Password" is masked with dots, "Service Name" is empty, "Encap. method" has "VcMux" selected and "LLC" unselected, "Auth. Protocol" is "Auto", and "IP Address" is "0.0.0.0" (with a note: '(0.0.0.0' means 'Obtain an IP address automatically)'). There is an "Apply" button at the bottom of the form. At the bottom right of the page, there are buttons for "Save Config", "Restart", and "Logout". The footer contains the copyright notice: "Copyright © Billion Electric Co., Ltd. All rights reserved."

■ 3G Mode (Main Port : 3G)

The screenshot shows the configuration interface for a BILLION router in 3G Mode. The page title is "Quick Start" and it includes the BILLION logo and the tagline "Powering communications with Security". On the left, there is a navigation menu with options: Basic, Advance, Status, Quick Start, WAN (highlighted), and WLAN. The main content area is titled "Configuration" and shows the "WAN Port" settings. Under "WAN Connection", the "Main Port" is set to "3G" (Current Main Port: ADSL). Under "Parameters", the "APN" is "internet", "Username" is empty, "Password" is empty, and "PIN" is empty. There is a warning message: "*Warning: Entering the wrong PIN code three times will lock the SIM." There are "Apply" and "Cancel" buttons at the bottom of the form.

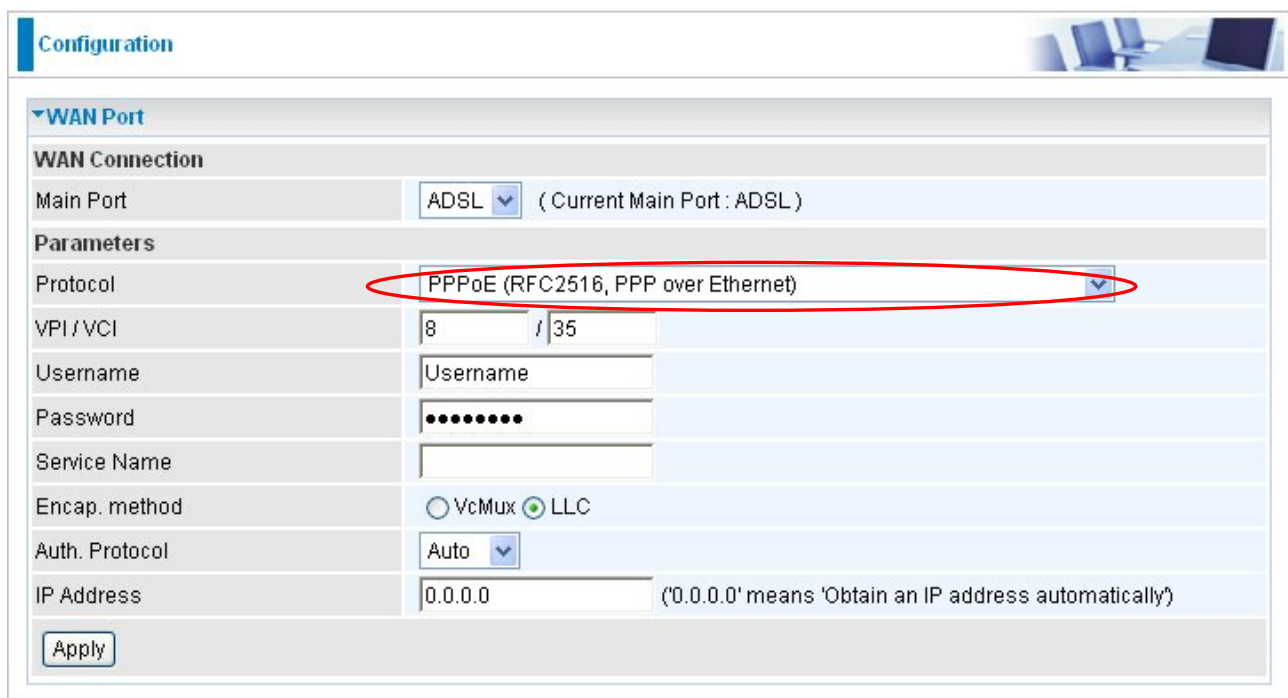
● **APN:** An APN is similar to a URL on the WWW, it is what the unit makes a GPRS / UMTS call. The service provider is able to attach anything to an APN to create a data connection, requirements for APNs varies between different service providers. Most service providers have an internet portal which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

- **Username:** Enter the username provided by your service provider.
- **Password:** Enter the password provided by your service provider.
- **PIN:** PIN stands for **P**ersonal **I**dentification **N**umber. A PIN code is a numeric value used in certain systems as a password to gain access, and authenticate. 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 you will require a PUK code from your network/service provider.

■ ADSL Mode (Main Port : ADSL)

● PPPoE Connection

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



The screenshot shows a configuration page for a WAN Port. Under the 'WAN Connection' section, the 'Main Port' is set to 'ADSL'. In the 'Parameters' section, the 'Protocol' dropdown menu is highlighted with a red oval and contains the text 'PPPoE (RFC2516, PPP over Ethernet)'. Other fields include VPI/VCI (8 / 35), Username (Username), Password (masked with dots), Service Name (empty), Encap. method (LLC selected), Auth. Protocol (Auto), and IP Address (0.0.0.0).

- **VPI/VCI:** Enter the VPI and VCI information provided by your ISP.
- **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.
- **Encap. method:** Select the encapsulation format, the default is LLC. Select the one

provided by your ISP

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

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

● **PPPoA Connection**

PPPoA stands for Point to Point Protocol over ATM Adaptation Layer 5 (AAL5). It provides access control and billing functionality in a manner similar to dial-up services using PPP.

The screenshot shows a configuration page for a WAN Port. The 'WAN Connection' section is expanded. Under 'Parameters', the 'Protocol' dropdown is set to 'PPPoA (RFC2864, PPP over AAL5)'. Other parameters include: Main Port: ADSL; VPI/VCI: 8 / 35; Username: Username; Password: masked with dots; Encap. method: LLC (selected); Auth. Protocol: Auto; IP Address: 0.0.0.0. A red oval highlights the 'Protocol' dropdown.

● **VPI/VCI:** Enter the VPI and VCI information provided by your ISP.

● **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).

● **Encap. method:** Select the encapsulation format, the default is LLC. Select the one provided by your ISP

● **Auth. Protocol:** Default is **Auto**. Your ISP should advise you on whether to use **Chap** or **Pap**.

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

● **MPoA Connection**

Configuration

▼ WAN Port

WAN Connection

Main Port: ADSL (Current Main Port : ADSL)

Parameters

Protocol: MPoA (RFC1483/RFC2684, Multiprotocol Encapsulation over AAL5)

VPI / VCI: 8 / 35

Encap. method: VcMux LLC

Encap. mode: Bridged Routed

IP Address: 0.0.0.0 ('0.0.0.0' means 'Obtain an IP address automatically')

Netmask: 255.255.255.0

Gateway:

Apply

- **VPI and VCI:** Enter the VPI and VCI information provided by your ISP.
- **Encap. method:** Select the encapsulation format, the default is LLC. Select the one provided by your ISP.
- **Encap. mode:** Choose whether you want the packets in WAN interface as bridged packet or routed packet.
- **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 255.255.255.0. User can change it to other such as 255.255.255.128. Type the subnet mask assigned to you by your ISP (if given).
- **Gateway:** Enter the IP address of the default gateway (if given).

● Pure Bridge Connections

Configuration

▼ WAN Port

WAN Connection

Main Port: ADSL (Current Main Port : ADSL)

Parameters

Protocol: Pure Bridge

VPI / VCI: 8 / 35

Encap. method: VcMux LLC

Apply

- **VPI/VCI:** Enter the VPI and VCI information provided by your ISP.
- **Encap. method:** Select the encapsulation format, this is provided by your ISP.

4.4 WLAN

The screenshot shows the configuration interface for the BILLION ADSL Firewall Router. The page is titled "ADSL Firewall Router" and features the BILLION logo and the slogan "Powering communications with Security". The navigation menu on the left includes "Basic", "Advance", "Status", "Quick Start", "WAN", and "WLAN". The main configuration area is titled "Configuration" and contains a "WLAN" section. Under "Wireless Parameters", the "WLAN Service" is set to "Enable", the "ESSID" is "wlan-ap", "Hide ESSID" is set to "Disable", the "Regulation Domain" is "N.America", and the "Channel ID" is "Channel 1 (2.412 GHz)". Under "Security Parameters", the "Security Mode" is set to "Disable". There are "Apply" and "Cancel" buttons at the bottom of the configuration area. At the bottom of the page, there are "Save Config", "Restart", and "Logout" buttons, along with a copyright notice: "Copyright © Billion Electric Co., Ltd. All rights reserved."

Wireless Parameters

● **WLAN Service:** Default setting is set to **Enable**. If you don't want to use wireless, both 802.11g and 802.11b, device in your network, you can select **Disable**.

● **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	WPA1 Pre-Shared Key ▼
WPA Shared Key	<input type="text"/>
Group Key Renewal	3600 seconds
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

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

● WPA Pre-Shared Key

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

● **WPA2 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

Wireless Security

Parameters

Security Mode	WEP
WEP Authentication	Open System
Default Used WEP Key	4
Passphrase (Generate Key)	<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?!dbd3ert.

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

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

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

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

Chapter 5

Advance Configuration

Once you have logged on to your BiPAC 7300GX ADSL2+ 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** (ADSL Status, 3G Status, ARP Table, DHCP Table, System Log, Firewall Log)
- **Quick Start**
- **Configuration** (LAN, WAN, System, Firewall, QoS, Virtual Server, Time Schedule and Advanced)

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

5.1 Status

BILLION ADSL Firewall Router Powering communications with Security

Advance

- Basic
- Status**
- ADSL Status
- 3G Status
- ARP Table
- DHCP Table
- System Log
- Firewall Log
- Quick Start
- Configuration

Status

Device Information

Model Name	BIPAC 7300GX
Host Name	home.gateway
System Up-Time	15 Hour(s) 51 min(s)
Current Time	Sat Jan 1 15:51:25 2000
Hardware Version	7300GX
Software Version	1.03A-RC2
MAC Address	00:04:ed:aa:bb:cc

Port Status

Ethernet	✓
ADSL	✗ 0 / 0 kbps
3G	✗
Wireless	✓

WAN

Port	Protocol	VPI/VCI	Operation	Connection	IP Address	Netmask	Gateway	Primary DNS
ADSL	PPPoE	8/35		Link Down				

[Save Config](#)
[Restart](#)
[Logout](#)

Copyright © Billion Electric Co., Ltd. All rights reserved.

Status

Device Information

Model Name	BIPAC 7300GX
Host Name	home.gateway
System Up-Time	1 Hour(s) 48 min(s)
Current Time	Sat Jan 1 01:48:08 2000
Hardware Version	7300GX
Software Version	1.03A-RC2
MAC Address	00:04:ed:aa:bb:cc

Port Status

Ethernet	✓
ADSL	✗ 0 / 0 kbps
3G	✗
Wireless	✓

WAN

Port	Protocol	VPI/VCI	Operation	Connection	IP Address	Netmask	Gateway	Primary DNS
ADSL	PPPoE	8/35		Link Down				

Device Information

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

Configuration

Device Management

Device Host Name

Host Name

Embedded Web Server

HTTP Port (The default HTTP port number is 80.)

Expire to auto-logout min(s)

Universal Plug and Play (UPnP)

UPnP Enable Disable

UPnP Port

- **System Up-Time:** Records system up-time.
- **Current time:** Set the current time. See the Time Zone section for more information.
- **Hardware Version:** Device version.
- **Software Version:** Firmware version.
- **MAC Address:** The LAN MAC address.

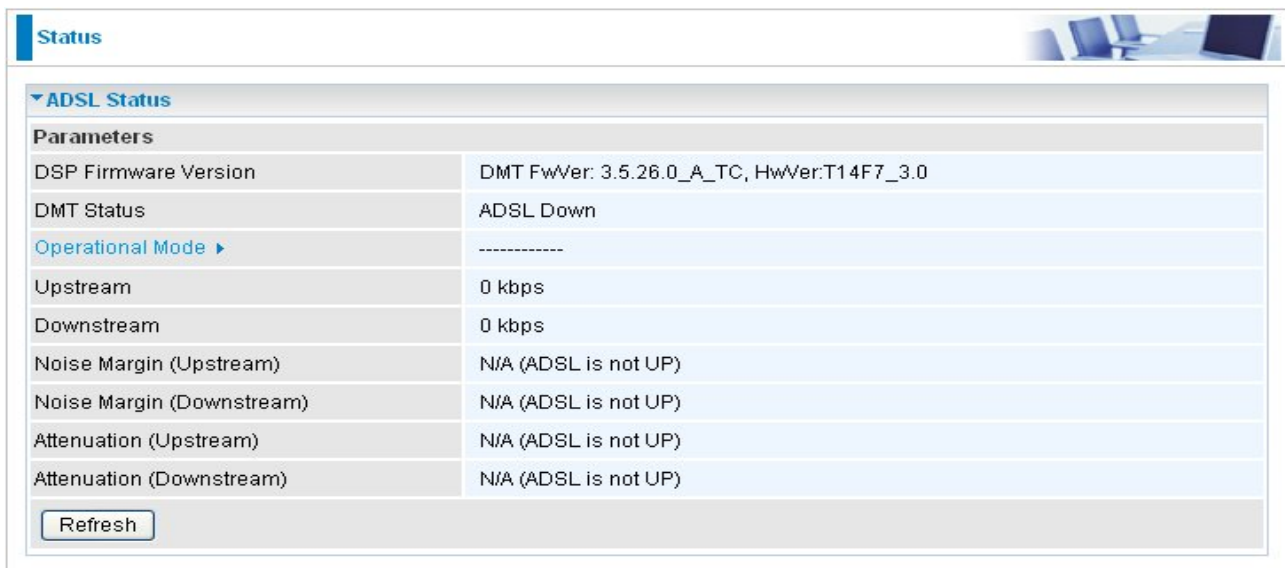
WAN

- **Port:** Name of the WAN connection.
- **Protocol VPI/VCI:** Virtual Path Identifier and Virtual Channel Identifier
- **Operation:** The current status in WAN interface.
- **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.

Port Status

- **Port Status :** User can look up to see if they are connected to Ethernet, ADSL, 3G or Wireless.

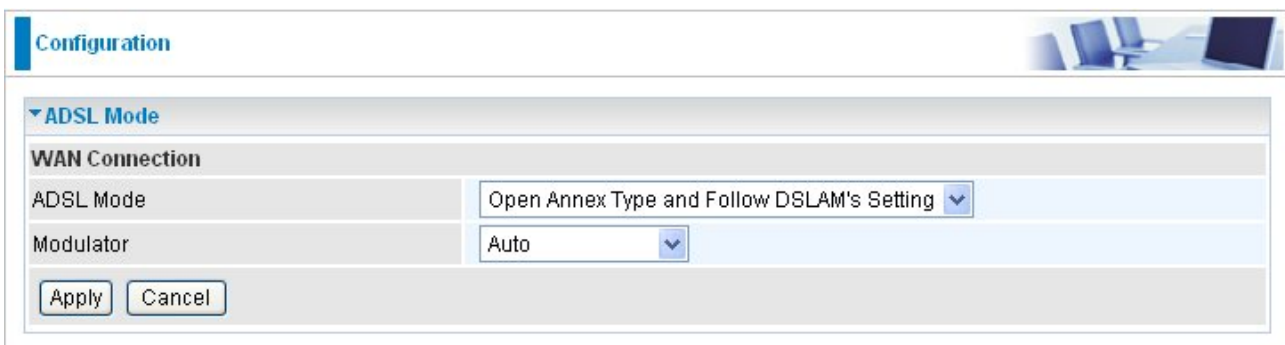
5.1.1 ADSL Status



Parameters	
DSP Firmware Version	DMT FwVer: 3.5.26.0_A_TC, HwVer:T14F7_3.0
DMT Status	ADSL Down
Operational Mode ▶	-----
Upstream	0 kbps
Downstream	0 kbps
Noise Margin (Upstream)	N/A (ADSL is not UP)
Noise Margin (Downstream)	N/A (ADSL is not UP)
Attenuation (Upstream)	N/A (ADSL is not UP)
Attenuation (Downstream)	N/A (ADSL is not UP)

Refresh

- **DSP Firmware Version:** DSP code version
- **DMT Status:** Current DMT Status
- **Operational Mode:** To show the state when user select “AUTO” on connect mode.
- **Upstream:** Upstream rate.
- **Downstream:** Downstream rate.
- **Noise Margin (Upstream):** This is noise margin in upstream.
- **Noise Margin (Downstream):** This is noise margin in downstream.
- **Attenuation (Upstream):** This is attenuation of signal in upstream.
- **Attenuation (Downstream):** This is attenuation of signal in downstream.



ADSL Mode

WAN Connection

ADSL Mode: Open Annex Type and Follow DSLAM's Setting

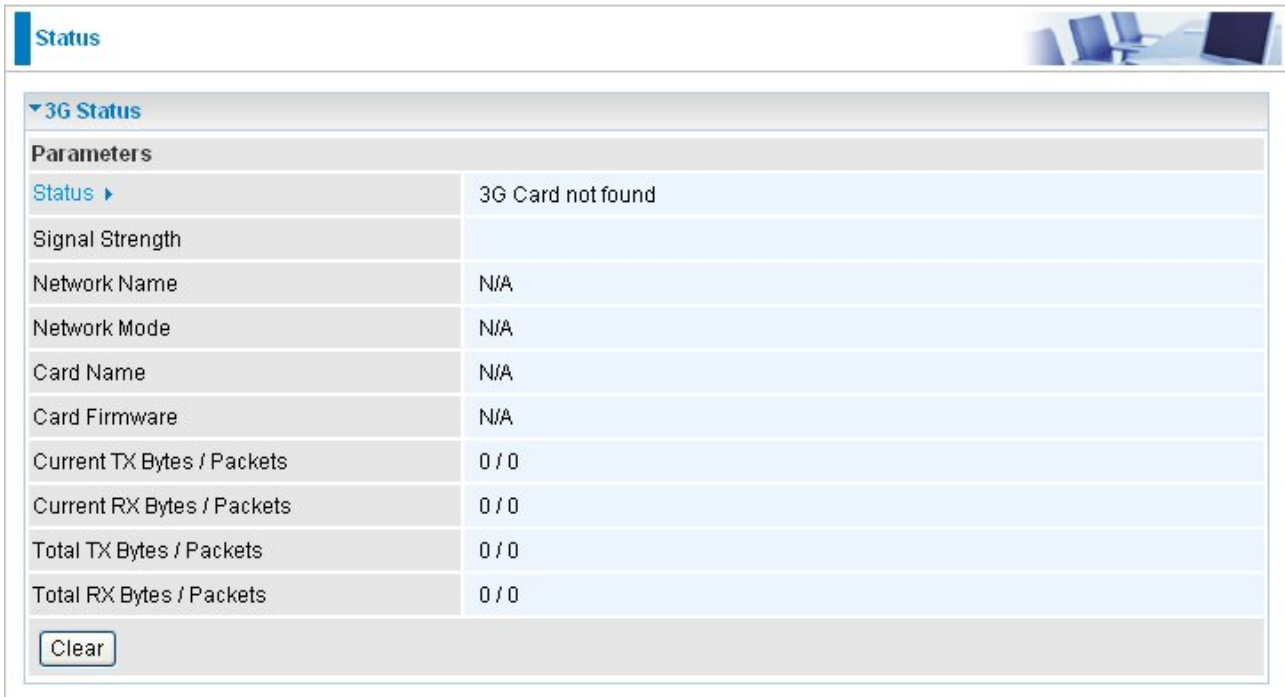
Modulator: Auto

Apply Cancel

- **ADSL Mode:** There are four modes “Open Annex Type and Follow DSLAM’s Setting”, “Annex A”, “Annex L”, “Annex M” and “Annex J” that user can select for this connection.
- **Modulator:** There are seven modes “AUTO”, “ADSL multimode”, “ADSL2”, “ADSL2+”, “G.Lite”, “T1.413” and “G.DMT” that user can select for this connection.

5.1.2 3G Status

This section displays the 3G Card's overall status, which shows you a number of helpful information such as the current signal strength and statistics on current and total bytes transferred and received.



The screenshot shows a web interface titled "Status" with a sub-section "3G Status". Below this, there is a "Parameters" table with the following data:

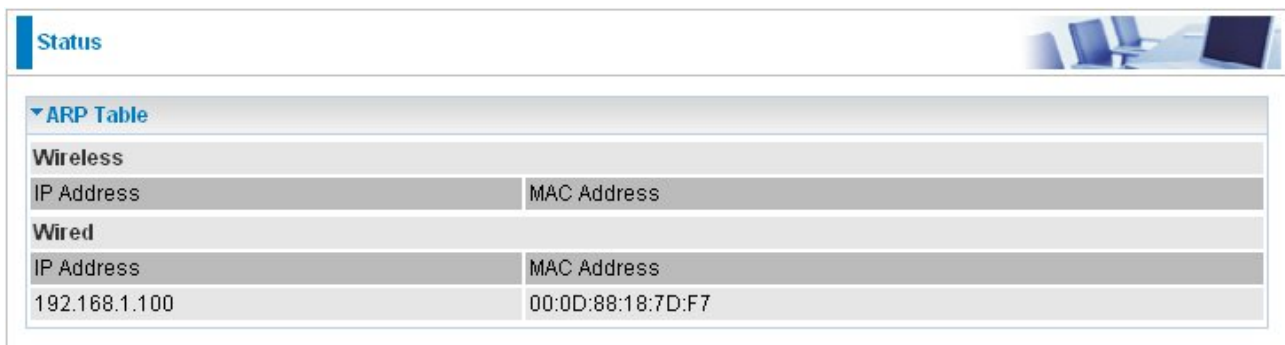
Parameters	
Status ▶	3G Card not found
Signal Strength	
Network Name	N/A
Network Mode	N/A
Card Name	N/A
Card Firmware	N/A
Current TX Bytes / Packets	0 / 0
Current RX Bytes / Packets	0 / 0
Total TX Bytes / Packets	0 / 0
Total RX Bytes / Packets	0 / 0

At the bottom of the table is a "Clear" button.

- **Status:** The current status of the 3G card.
- **Signal Strength:** The signal strength bar indicates current 3G signal strength.
- **Network Name:** The network name that the device is connected to.
- **Network Mode:** The current operation mode in 3G card, it depends on service provider and card's limitation. It may be UMTS (3G),GPRS, EDGE, or GSM .
 - Card Name: The name of the 3G card.
 - Card Firmware: The current firmware for the 3G card.
- **Current TX Bytes / Packets:** The statistics of transmission, count for this call.
- **Current RX Bytes / Packets:** The statistics of receive, count for this call.
- **Total TX Bytes / Packets:** The statistics of transmission, count from system ready
- **Total RX Bytes / Packets:** The statistics of receive, count from system ready
- **Clear:** Click Clear button to reset the statistics value of Total TX/RX.

5.1.2 ARP Table

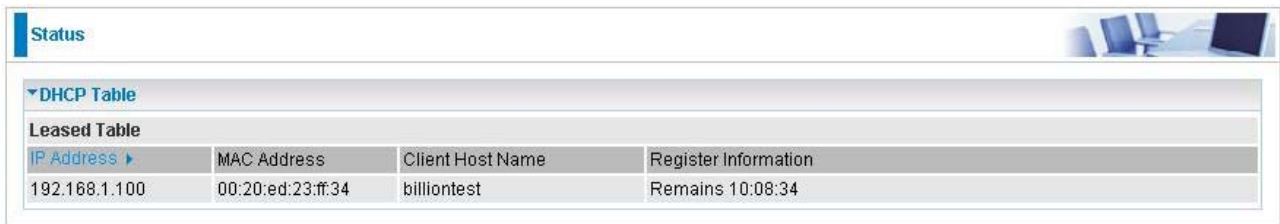
This section displays the router's ARP (Address Resolution Protocol) Table, which shows the mapping of Internet (IP) addresses to Ethernet (MAC) addresses. This is useful as a quick way of determining the MAC address of the network interface of your PCs to use with the router's **Firewall – MAC Address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



Wireless	
IP Address	MAC Address
192.168.1.100	00:0D:88:18:7D:F7

- **IP Address:** It is IP Address of internal host that join this network.
- **MAC Address:** The MAC address of internal host.

5.1.3 DHCP Table



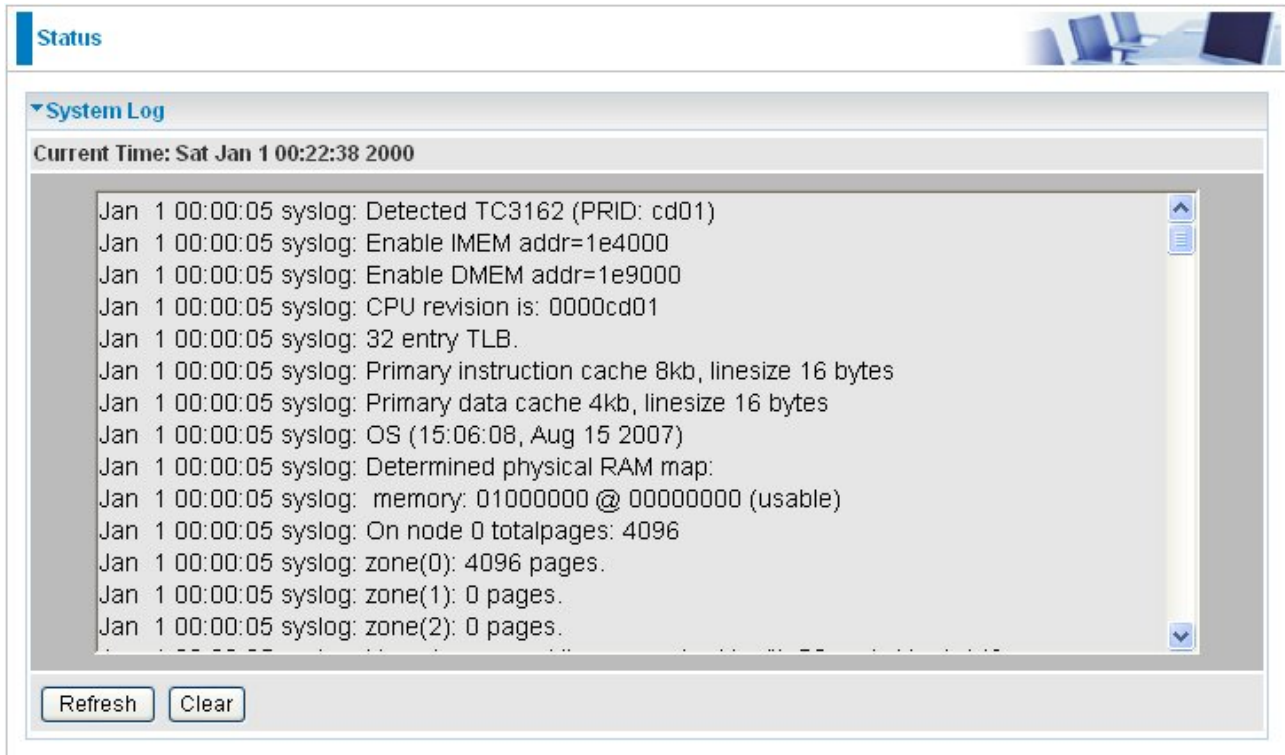
The screenshot shows a web interface with a 'Status' tab. Underneath, there is a 'DHCP Table' section. A sub-section titled 'Leased Table' contains a table with the following data:

IP Address	MAC Address	Client Host Name	Register Information
192.168.1.100	00:20:ed:23:ff:34	billiontest	Remains 10:08:34

- **IP Address:** The current corresponding DHCP-assigned dynamic IP address of the device.
- **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

5.1.4 System Log

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



The screenshot shows a web interface with a 'Status' tab and a 'System Log' section. The 'System Log' section displays a list of log entries for 'Jan 1 00:00:05' from the 'syslog' service. The entries include system boot information such as hardware detection, memory enablement, CPU revision, cache sizes, OS version, and RAM map details. At the bottom of the log area, there are 'Refresh' and 'Clear' buttons.

Status

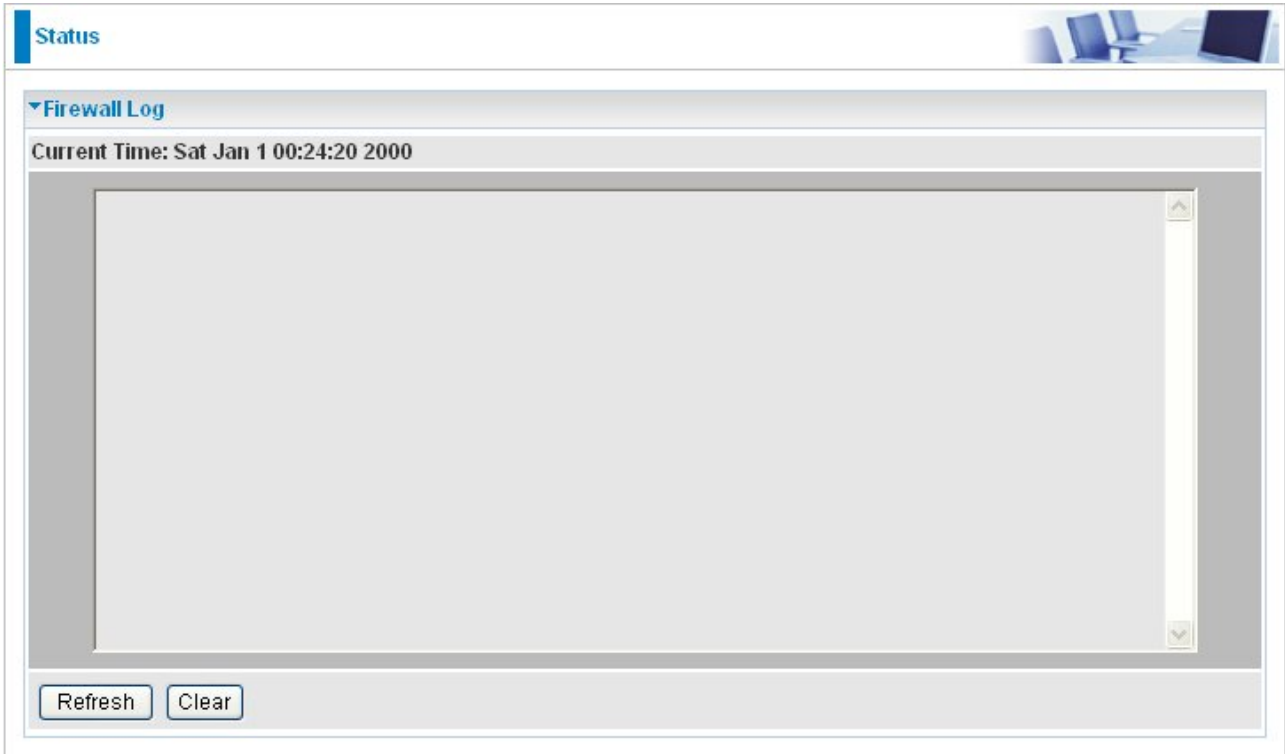
System Log

Current Time: Sat Jan 1 00:22:38 2000

```
Jan 1 00:00:05 syslog: Detected TC3162 (PRID: cd01)
Jan 1 00:00:05 syslog: Enable IMEM addr=1e4000
Jan 1 00:00:05 syslog: Enable DMEM addr=1e9000
Jan 1 00:00:05 syslog: CPU revision is: 0000cd01
Jan 1 00:00:05 syslog: 32 entry TLB.
Jan 1 00:00:05 syslog: Primary instruction cache 8kb, linesize 16 bytes
Jan 1 00:00:05 syslog: Primary data cache 4kb, linesize 16 bytes
Jan 1 00:00:05 syslog: OS (15:06:08, Aug 15 2007)
Jan 1 00:00:05 syslog: Determined physical RAM map:
Jan 1 00:00:05 syslog: memory: 01000000 @ 00000000 (usable)
Jan 1 00:00:05 syslog: On node 0 totalpages: 4096
Jan 1 00:00:05 syslog: zone(0): 4096 pages.
Jan 1 00:00:05 syslog: zone(1): 0 pages.
Jan 1 00:00:05 syslog: zone(2): 0 pages.
```

5.1.5 Firewall Log

Firewall Log display 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.



5.2 Quick Start

The screenshot displays the configuration interface for a BILLION ADSL Firewall Router. The page title is "ADSL Firewall Router" and it features the slogan "Powering communications with Security". A navigation menu on the left includes "Advance" (with a user icon), "Basic", "Status", "Quick Start" (highlighted), and "Configuration". The main content area is titled "Quick Start" and shows a breadcrumb path "WAN Port (WAN > Wireless)". The "Select WAN Port" section contains the following configuration fields:

Connect Mode	ADSL (Recommended) ▼
Protocol	PPPoE (RFC2516, PPP over Ethernet)
VPI / VCI	8 / 35
Username	Username
IP Address	0.0.0.0

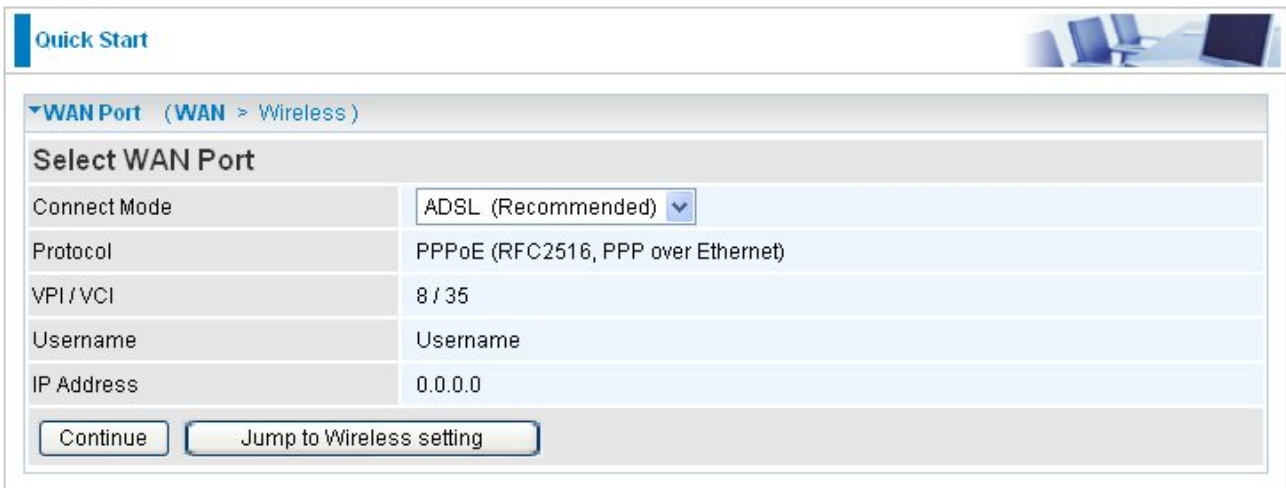
At the bottom of the configuration area are two buttons: "Continue" and "Jump to Wireless setting". The footer of the interface includes "Save Config", "Restart", and "Logout" buttons, along with the copyright notice: "Copyright © Billion Electric Co., Ltd. All rights reserved."

For detailed instructions on configuring WAN settings, see the **WAN** section of this manual.

The information you need for the Quick Start wizard to get you online are your login (often in the form of *username@ispname*), your password, and the encapsulation type.

Your ISP can supply all the details you need. Alternatively, if you have deleted the current WAN Connection in the **WAN – ISP** section of the interface, you can use the router's PVC Scan feature to determine the Encapsulation types offered by your ISP.

Select WAN Port



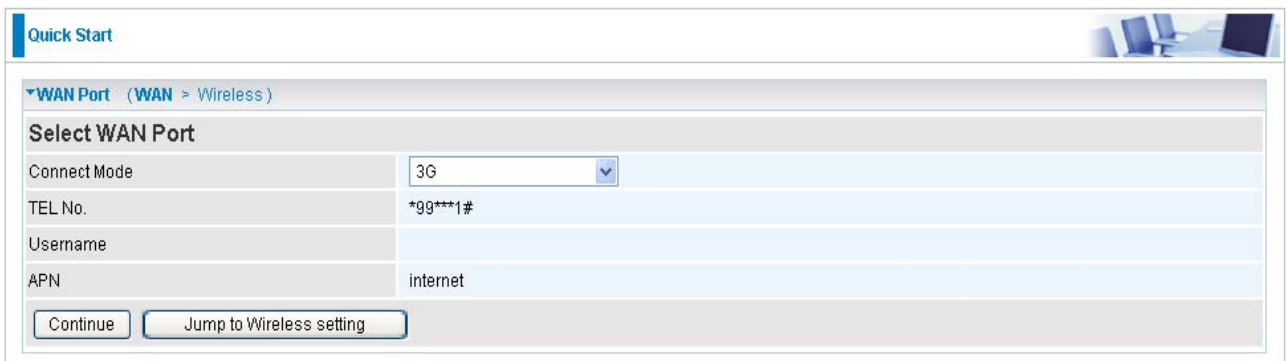
Quick Start

WAN Port (WAN > Wireless)

Select WAN Port

Connect Mode	ADSL (Recommended)
Protocol	PPPoE (RFC2516, PPP over Ethernet)
VPI / VCI	8 / 35
Username	Username
IP Address	0.0.0.0

- **Connect Mode:** User can choose either “ADSL” or “3G” mode.
- **Protocol:** The current ATM protocol in the device.
- **VPI / VCI:** The current value of VPI/VCI in the device.
- **Username:** To show current authentication username.
- **IP Address:** To show current value of IP address in the device.



Quick Start

WAN Port (WAN > Wireless)

Select WAN Port

Connect Mode	3G
TEL No.	*99***1#
Username	
APN	internet

- **TEL No.:** The dial string to make a GPRS / 3G user interneting call.
- **Username:** 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.

Set Wireless configuration

The screenshot shows a web-based configuration interface for a router. At the top left, there is a 'Quick Start' header. Below it, a breadcrumb trail reads 'Wireless (WAN > WLAN)'. The main section is titled 'Set Wireless configuration.' and contains the following settings:

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"/>

At the bottom left of the configuration area, there is a 'Continue' button.

● **WLAN Service:** Default setting is set to **Enable**. If you don't want to use wireless, both 802.11g and 802.11b, device in your network, you can select **Disable**.

● **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**.

5.3 Configuration

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

These functions are described in the following sections.

The screenshot displays the configuration interface for a BILLION ADSL Firewall Router. The top header includes the BILLION logo, the product name 'ADSL Firewall Router', and the slogan 'Powering communications with Security'. The left sidebar contains a navigation menu with the following items: Advance, Basic, Status, Quick Start, Configuration (highlighted and circled in red), LAN, WAN, System, Firewall, QoS, Virtual Server, Time Schedule, and Advanced. The main configuration area is titled 'Configuration' and shows the 'Ethernet' settings. The 'Parameters' section includes the following fields:

Parameters	
IP Address	192.168.1.254
Netmask	255.255.255.0
RIP	Disable

Buttons for 'Apply' and 'Cancel' are located below the parameters. At the bottom of the interface, there are buttons for 'Save Config', 'Restart', and 'Logout'. The footer contains the copyright notice: 'Copyright © Billion Electric Co., Ltd. All rights reserved.'

5.3.1 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**.

The screenshot displays the configuration interface for a BILLION ADSL Firewall Router. The top header includes the BILLION logo, the product name 'ADSL Firewall Router', and the slogan 'Powering communications with Security'. The left sidebar contains a navigation menu with categories like 'Advance', 'Basic', 'Status', 'Quick Start', and 'Configuration'. Under 'Configuration', the 'LAN' section is expanded, and 'Ethernet' is highlighted with a red circle. The main configuration area shows the 'Ethernet' settings, including IP Address (192.168.1.254), Netmask (255.255.255.0), and RIP (Disable). At the bottom, there are buttons for 'Apply', 'Cancel', 'Save Config', 'Restart', and 'Logout'. The footer contains the copyright notice: 'Copyright © Billion Electric Co., Ltd. All rights reserved.'

■ 5.3.1.1 Ethernet

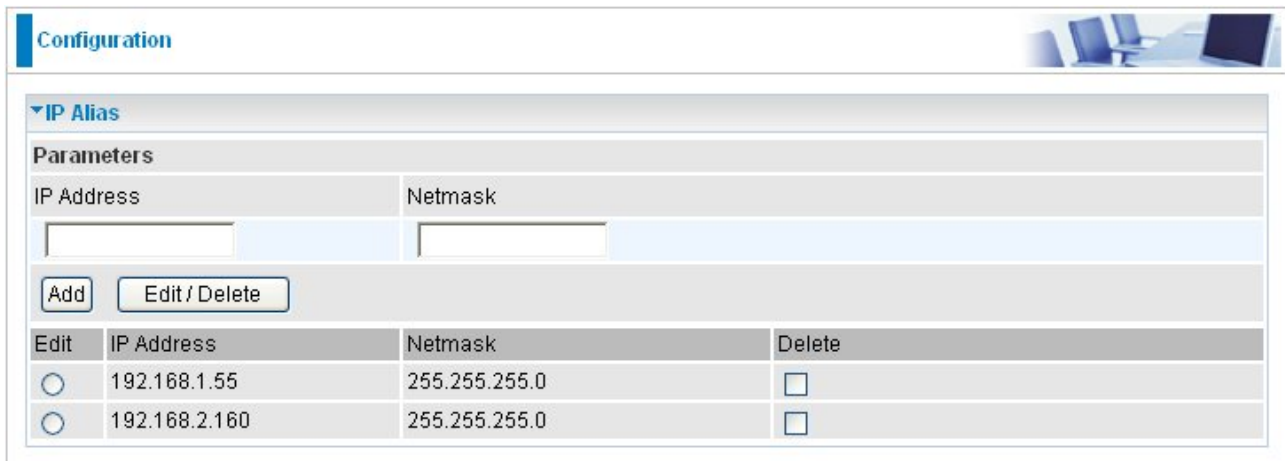
This is a close-up view of the Ethernet configuration section from the previous screenshot. It shows the 'Parameters' section with the following settings: IP Address is 192.168.1.254, Netmask is 255.255.255.0, and RIP is set to 'Disable'. There are 'Apply' and 'Cancel' buttons at the bottom of the configuration area.

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

- **IP Address:** The default IP on this router.
- **Netmask:** The default subnet mask on this router.
- **RIP:** RIP v1, RIP v2, RIP v1+v2 and RIP v2 Multicast.

■ 5.3.1.2 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.



IP Alias			
Parameters			
IP Address		Netmask	
<input type="text"/>		<input type="text"/>	
<input type="button" value="Add"/>		<input type="button" value="Edit / Delete"/>	
Edit	IP Address	Netmask	Delete
<input type="radio"/>	192.168.1.55	255.255.255.0	<input type="checkbox"/>
<input type="radio"/>	192.168.2.160	255.255.255.0	<input type="checkbox"/>

- **IP Address:** Specify an IP address on this virtual interface.
- **Netmask:** Specify a subnet mask on this virtual interface.

5.3.1.3 Wireless

Configuration

Wireless

Parameters

WLAN Service Enable Disable

Mode 802.11b + g

ESSID wlan-ap

Hide ESSID Enable Disable

Regulation Domain N.America

Channel ID Channel 1 (2.412 GHz)

Tx PowerLevel 100 (0 ~ 255)

AP MAC Address 00:19:DB:0D:C5:AF

AP Firmware Version RT2561T 1.1.0.0

WPS State Configured Unconfigured

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

Parameters

● **WLAN Service:** Default setting is set to **Enable**. If you don't want to use wireless, both 802.11g and 802.11b, device in your network, you can select **Disable**.

● **Mode:** The default setting is **802.11b+g** (Mixed mode). If you do not know or have both 11g and 11b 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**.

● **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.

● **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 255.

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 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.

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.

In addition, WDS enhances its link connection security in WEP mode, WEP key encryption must be the same for both access points.

Note: WDS function will disappear automatically if wireless security is not in WEP mode.

● **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.

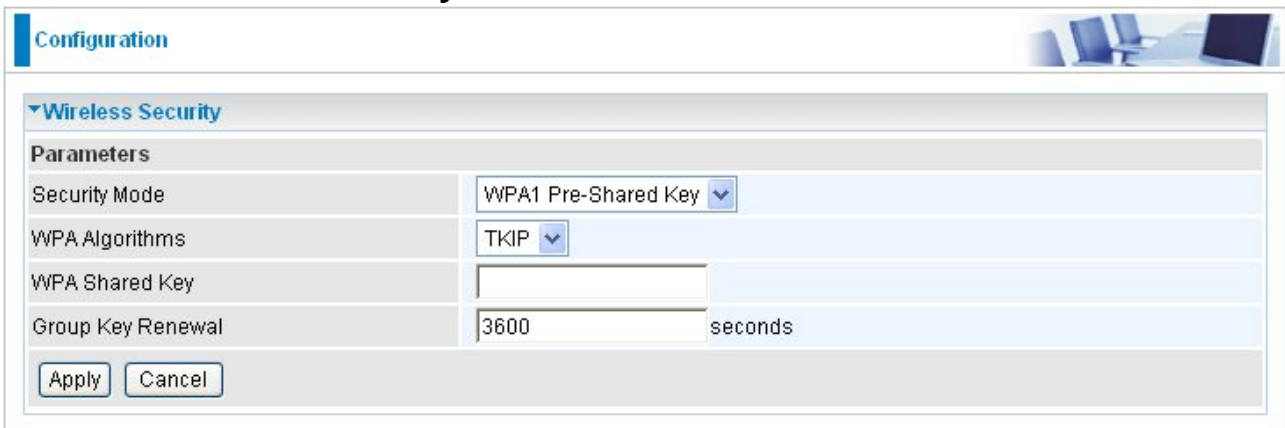
■ 5.3.1.4 Wireless Security

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



The screenshot shows a web-based configuration interface for wireless security. At the top, there is a 'Configuration' header. Below it, a section titled 'Wireless Security' is expanded. Under the 'Parameters' section, the 'Security Mode' is set to 'Disable' in a dropdown menu. At the bottom of the configuration area, there are 'Apply' and 'Cancel' buttons.

● WPA1 Pre-Shared Key



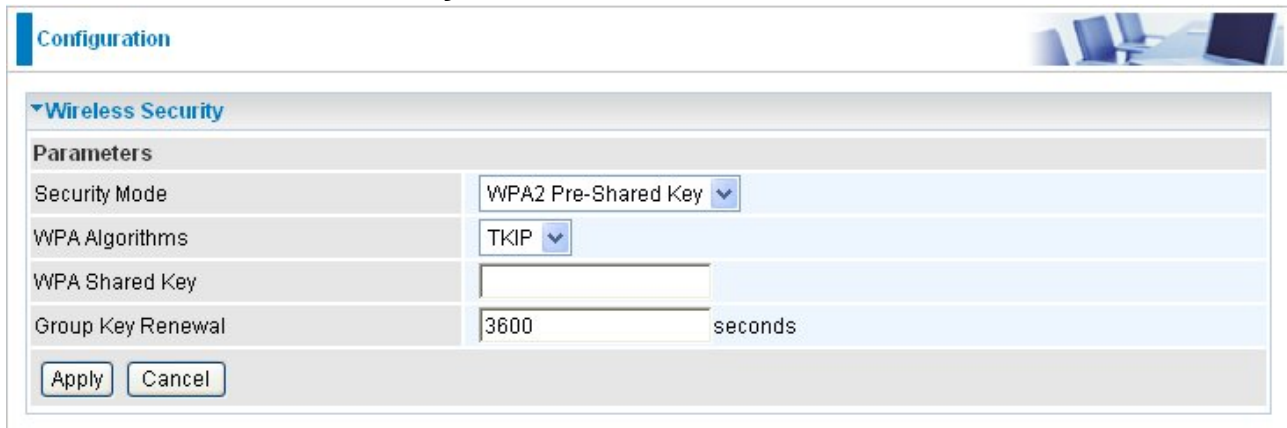
The screenshot shows the same web-based configuration interface, but now the 'Security Mode' is set to 'WPA1 Pre-Shared Key'. Below this, the 'WPA Algorithms' are set to 'TKIP'. The 'WPA Shared Key' field is empty. The 'Group Key Renewal' is set to '3600' seconds. 'Apply' and 'Cancel' buttons are visible 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 the 'Configuration' page for wireless security. Under the 'Wireless Security' section, the 'Parameters' are set as follows:

Security Mode	WPA2 Pre-Shared Key
WPA Algorithms	TKIP
WPA Shared Key	
Group Key Renewal	3600 seconds

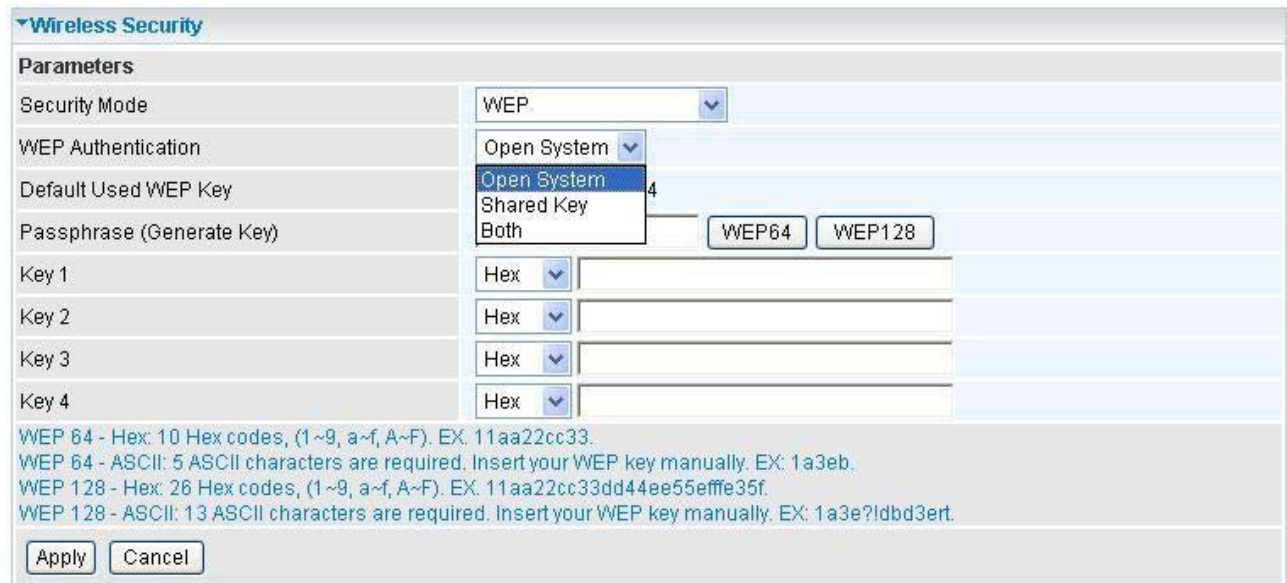
Buttons for 'Apply' and 'Cancel' are visible at the bottom of the configuration area.

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

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

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

WEP



The screenshot shows the 'Wireless Security' configuration page with WEP settings. The 'Parameters' section is as follows:

Security Mode	WEP
WEP Authentication	Open System
Default Used WEP Key	Open System
Passphrase (Generate Key)	Both
Key 1	Hex
Key 2	Hex
Key 3	Hex
Key 4	Hex

Buttons for 'Apply' and 'Cancel' are visible at the bottom. A dropdown menu for 'Default Used WEP Key' is open, showing 'Open System', 'Shared Key', and 'Both'. 'WEP64' and 'WEP128' buttons are also present.

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.

● **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.

■ 5.3.1.5 WPS

Billion WPS feature is follow Wi-Fi Alliance WPS standard and it ease set up of security-enabled Wi-Fi networks in the home and small office environment. Reduces by half the user steps to configure a network and supports two methods that are familiar to most consumers to configure a network and enable security.

Parameters	
Role	<input checked="" type="radio"/> Registrar <input type="radio"/> Enrollee
WPS PIN	78749887
Enrollee's PIN	<input type="text"/>

Set up of security-enabled Wi-Fi network

Step 1: Note down the AP's PIN from Web (Ex: 78749887).

Step 2: Open wireless client's WPS utility (Ex: Atheros Jumpstart WPS utility), select "Configure a wireless network" and apply "next" button.



Step 3: Enter AP's PIN into the utility and click on the "next" button.

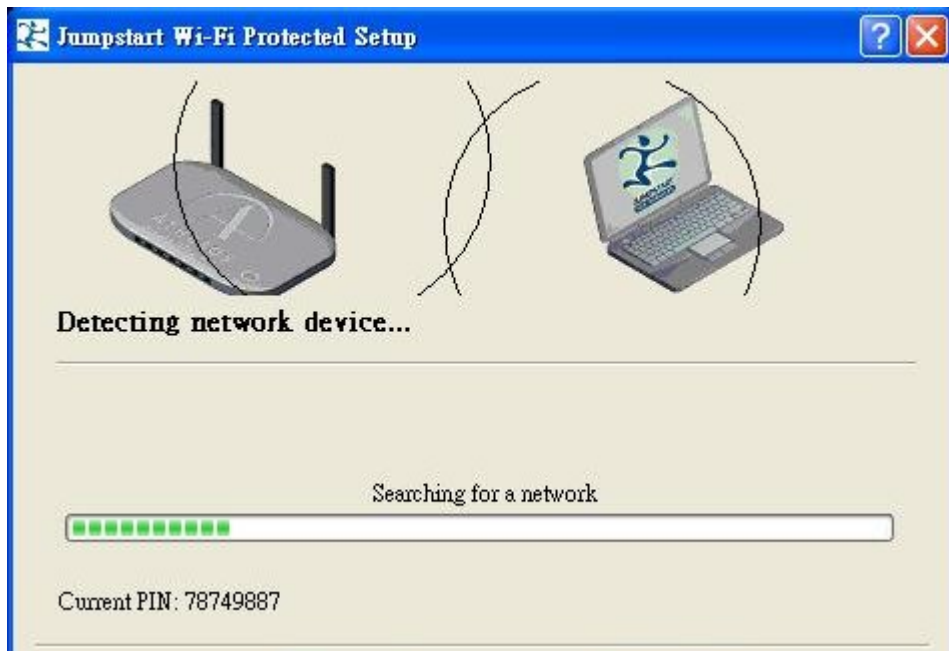


Step 4: These are two ways to trigger AP as Enrollee role, you can choose one to do it.

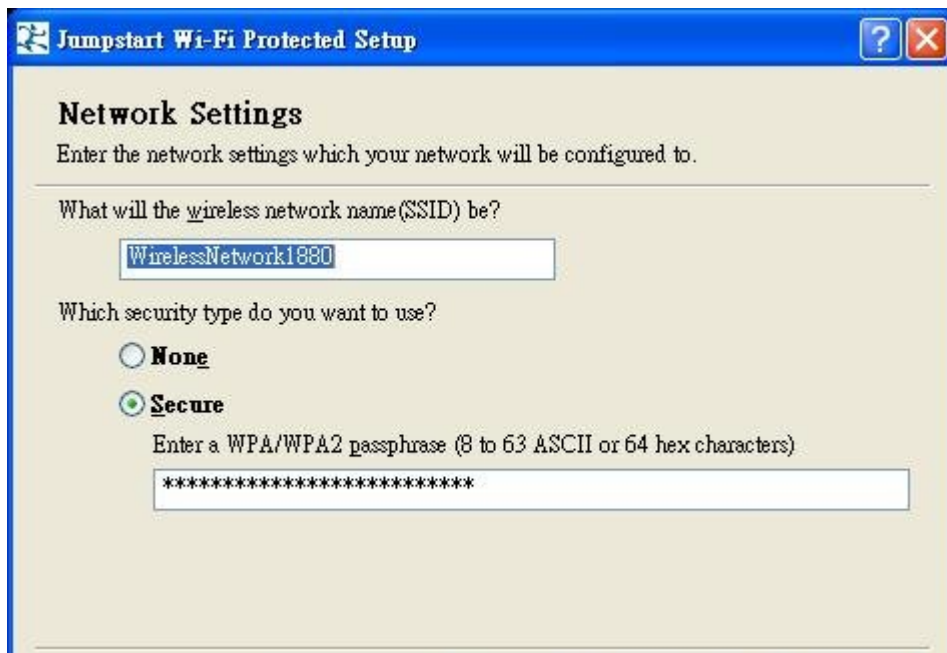
- Push AP's WPS button 1 second and release it. Or
- In the AP's WPS configuration page, change Role to "Enrollee" and apply "Start" button.



Step 5: Jumpstart WPS utility search WPS AP.



Step 6: SSID and security will be generated automatically (You can change it) and apply “next” button.



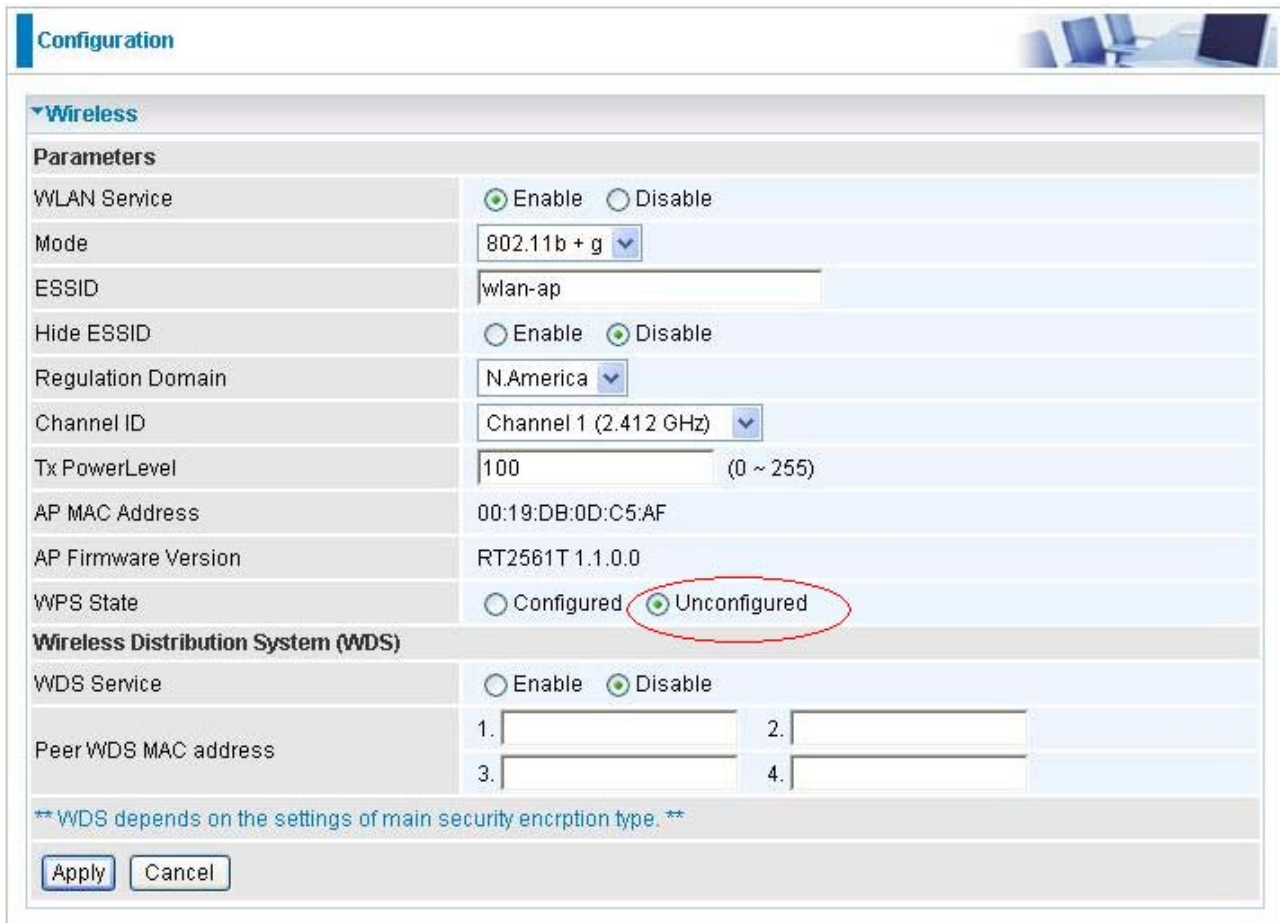
Step 7: WPS set up complete. And you have set up security-enabled Wi-Fi networks.



Set up of security-enabled Wi-Fi network using WCN in Vista

Step 1: Note down the AP's PIN from Web (Ex: 78749887).

Step 2: Set WPS State to "Unconfigured" at Wireless page and click "Apply".



Configuration

Wireless

Parameters

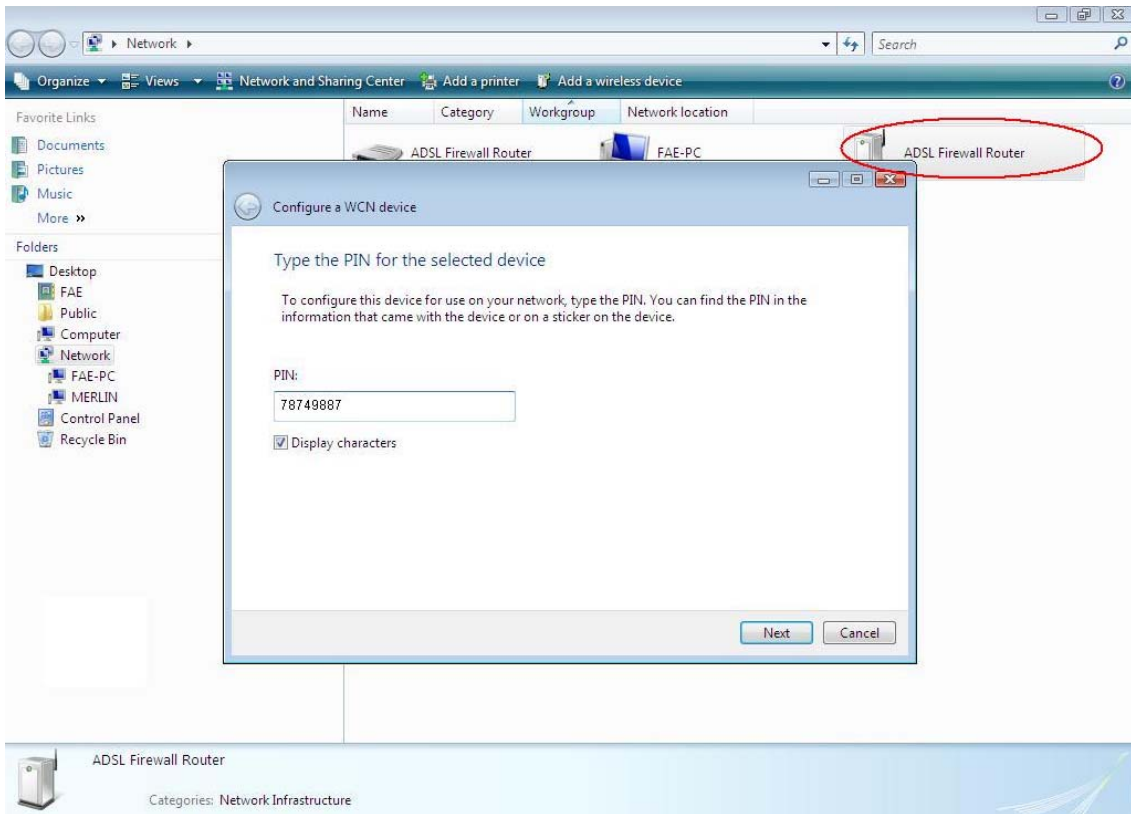
WLAN Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Mode	802.11b + g
ESSID	wlan-ap
Hide ESSID	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Regulation Domain	N.America
Channel ID	Channel 1 (2.412 GHz)
Tx PowerLevel	100 (0 ~ 255)
AP MAC Address	00:19:DB:0D:C5:AF
AP Firmware Version	RT2561T 1.1.0.0
WPS State	<input type="radio"/> Configured <input checked="" type="radio"/> Unconfigured

Wireless Distribution System (WDS)

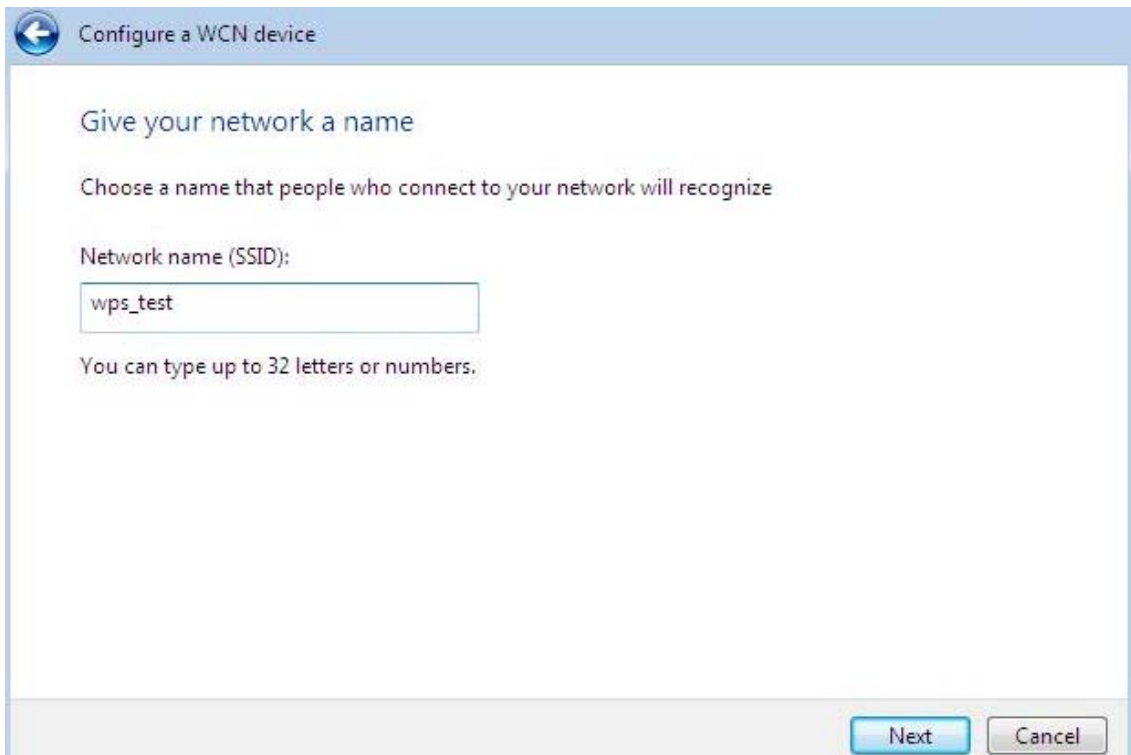
WDS Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Peer WDS MAC address	1. <input type="text"/> 2. <input type="text"/> 3. <input type="text"/> 4. <input type="text"/>

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

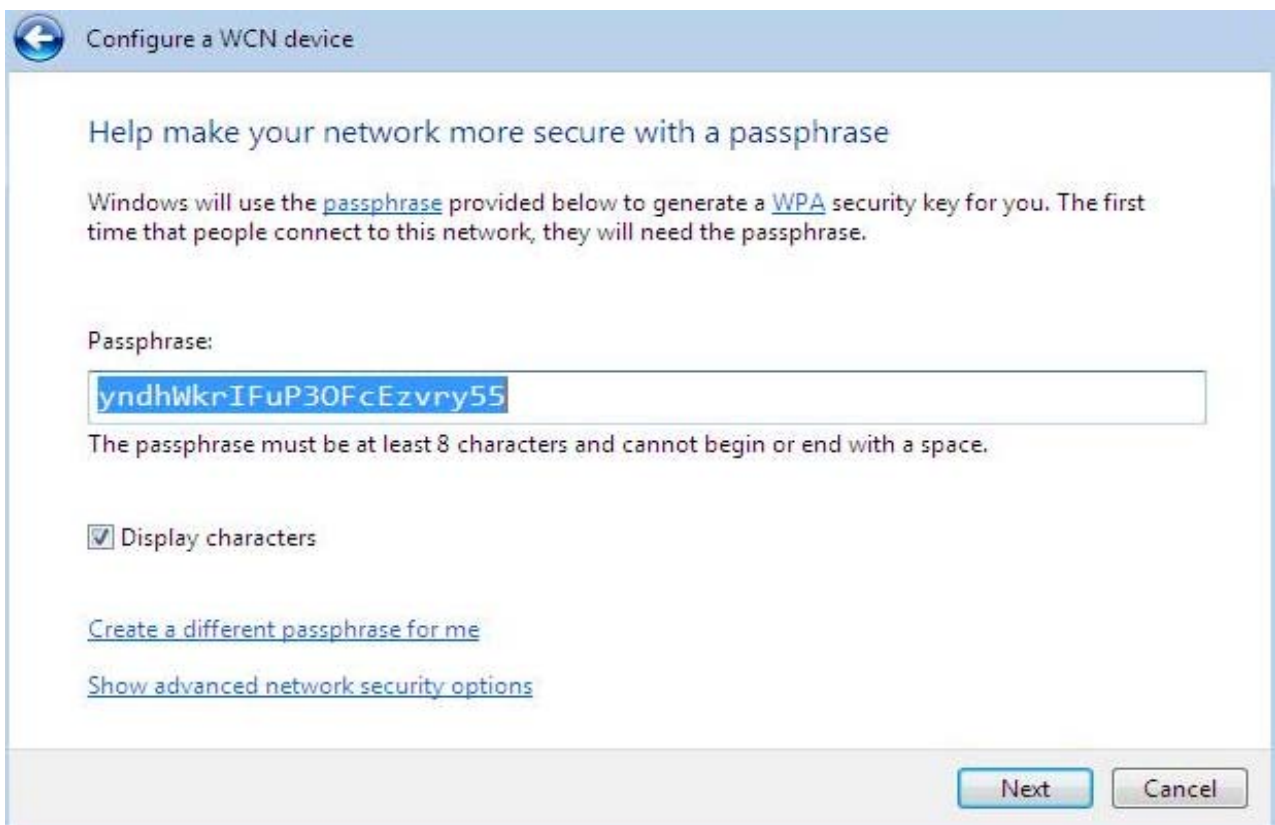
Step 3: In Vista's Control Panel, select **Network and Internet** and choose **View network computers and devices**. Double click the "ADSL Firewall Router" icon and enter the AP's PIN code then click "Next".



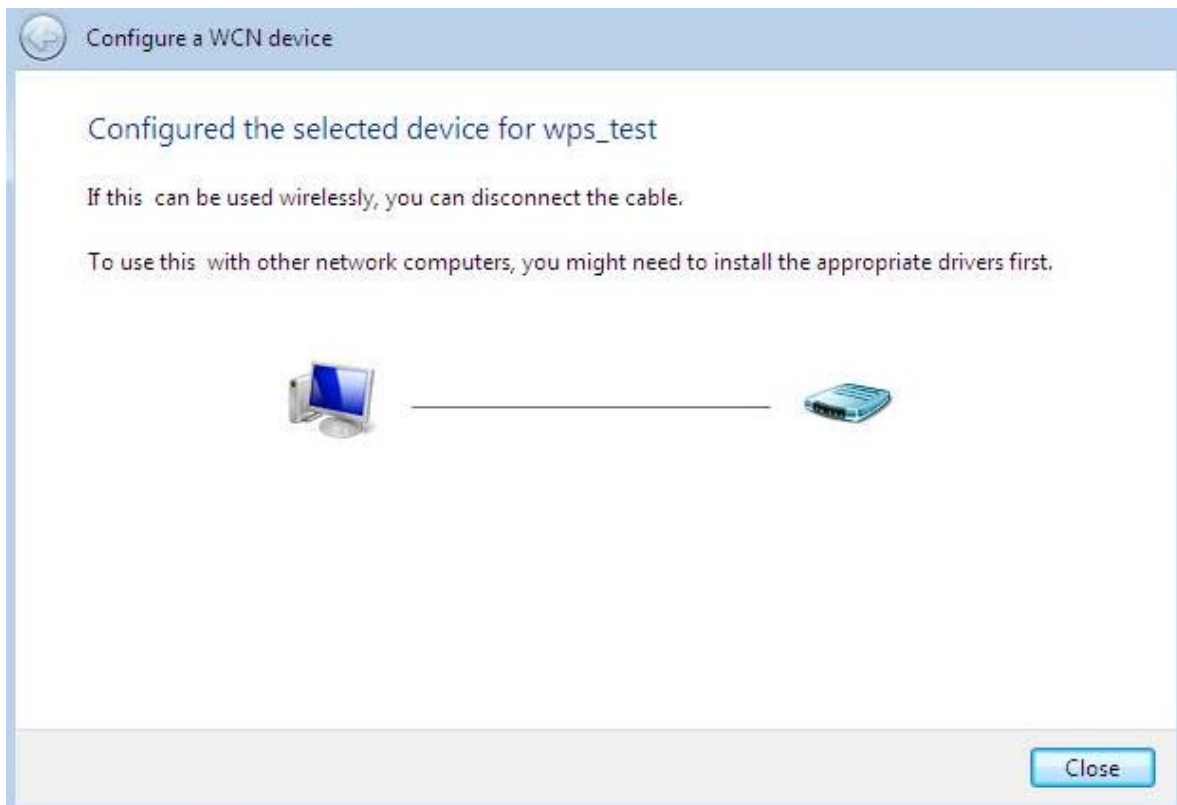
Step 4: Enter the AP SSID and apply “Next” button.



Step 5: Enter the Passphrase and apply “Next” button.



Step 6: WCN set up complete. And you have set up security-enabled Wi-Fi networks.

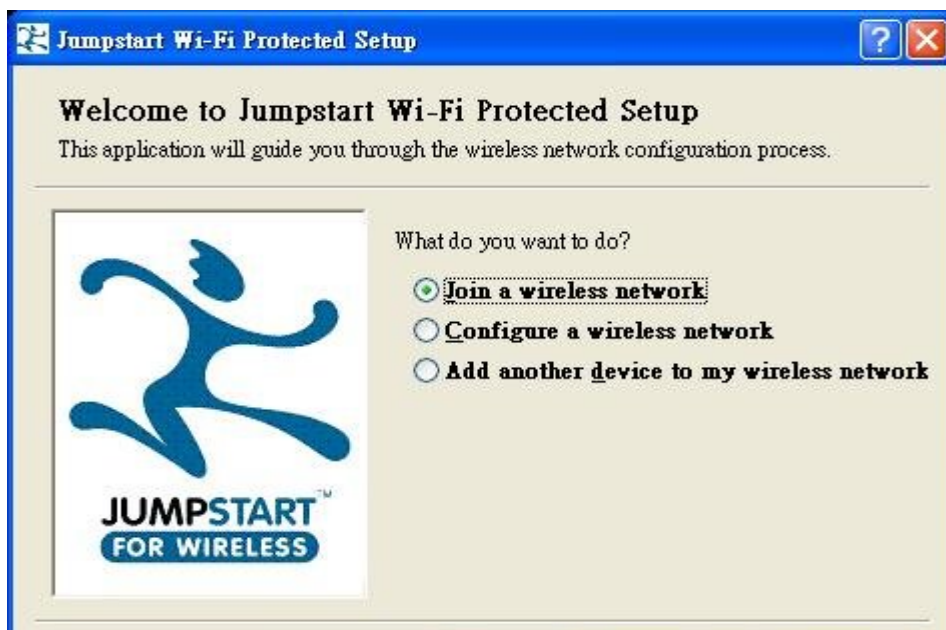


Adding a new WPS device (wireless client) to a network - Use PBC Method

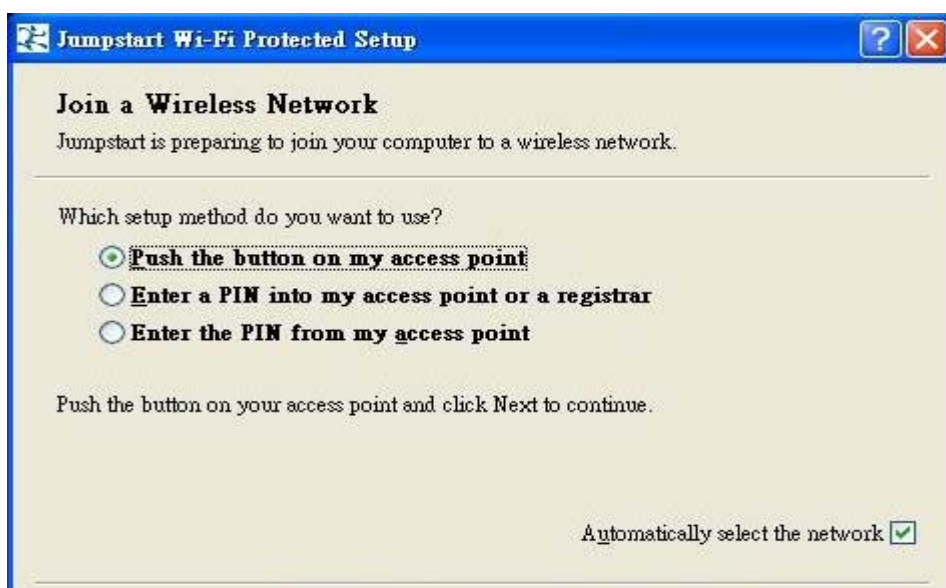
Step 1: Push AP's WPS button more than one second and you will see AP's WLAN led will flashing per second.

Step 2: Open wireless client's WPS utility, select "Join a wireless network" and apply "next" button.

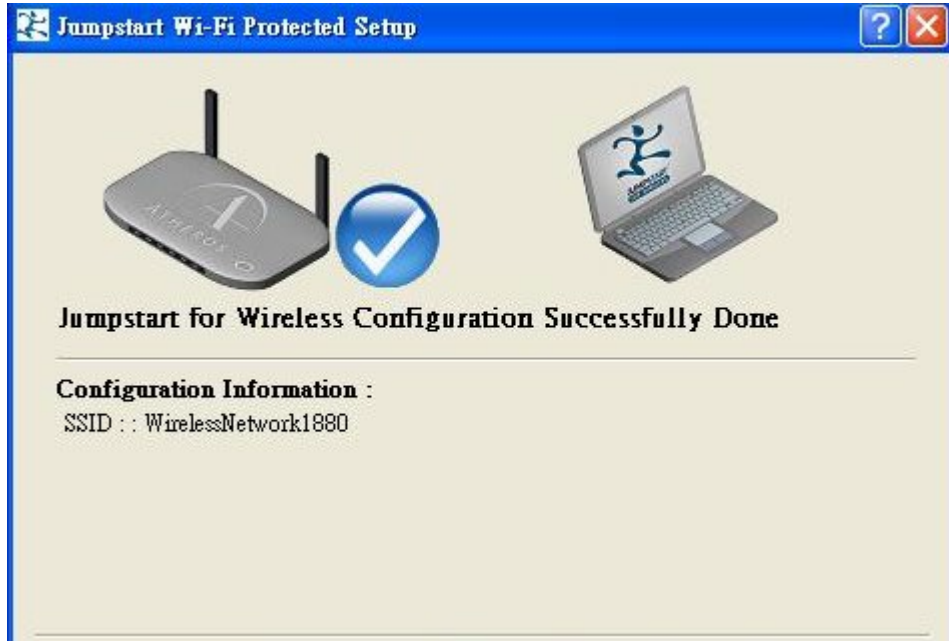
Note: After you push AP's WPS button, below steps should be completed between 2 minutes.



Step 3: Select "Push the button on my access point" and apply "next" button.

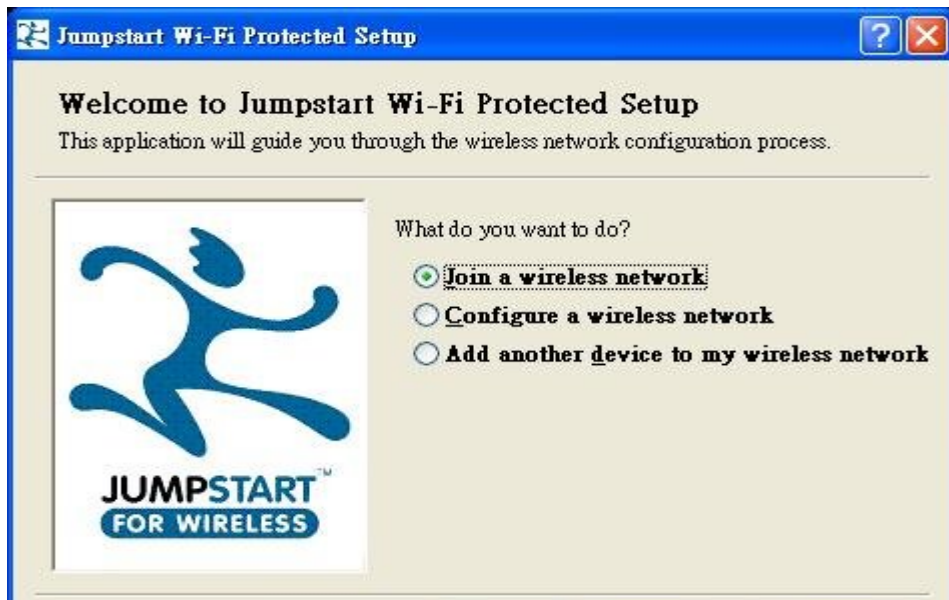


Step 4: New WPS device have join into the wireless network.

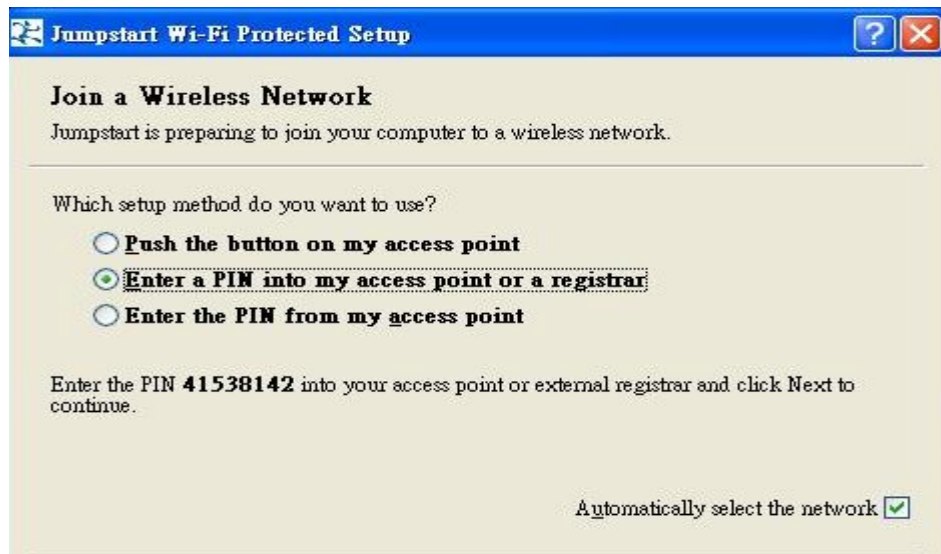


Adding a new WPS device (wireless client) to a network - Use PIN Method

Step 1: Open wireless client's WPS utility, select "Join a wireless network" and apply "next" button.



Step 2: Note down the wireless client's PIN (Ex: 41538142) and apply "Start" button for active wireless client WPS PIN method.



Step 3: Enter wireless client's PIN into "Enrollee's PIN" of Web and apply "Start" button.



Step 4: New WPS device have join into the wireless network.



Adding a new WPS device (wireless client) to a network - Use PIN Method

Step 1: Open wireless client's WPS utility, select "Join a wireless network" and apply "next" button.

■ 5.3.1.6 DHCP Server

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

● DHCP Server Mode: Disable

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

Configuration

▼ **DHCP Server**

Parameters

DHCP Server Mode:

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 ADSL 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:

Domain Name:

Range Start:

Range End:

Default Lease Time: seconds

Maximum Lease Time: seconds

Use Router as DNS Server:

Primary DNS Server Address:

Secondary DNS Server Address:

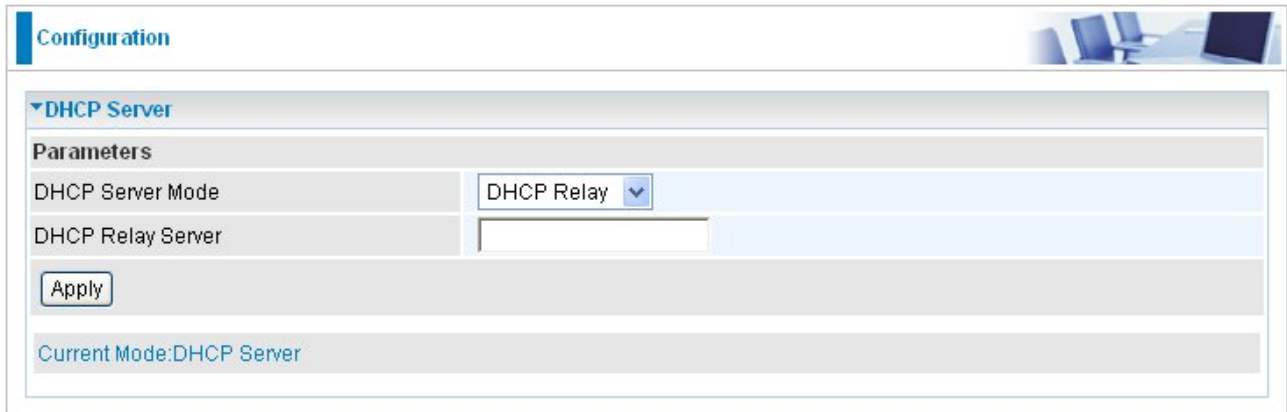
[Fixed Host ▶](#)

Current Mode: DHCP Server

● 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.



The screenshot shows a configuration window titled "Configuration" with a sub-section for "DHCP Server". Under the "Parameters" section, there are two fields: "DHCP Server Mode" with a dropdown menu set to "DHCP Relay", and "DHCP Relay Server" with an empty text input field. Below these fields is an "Apply" button. At the bottom of the configuration area, it displays "Current Mode: DHCP Server".

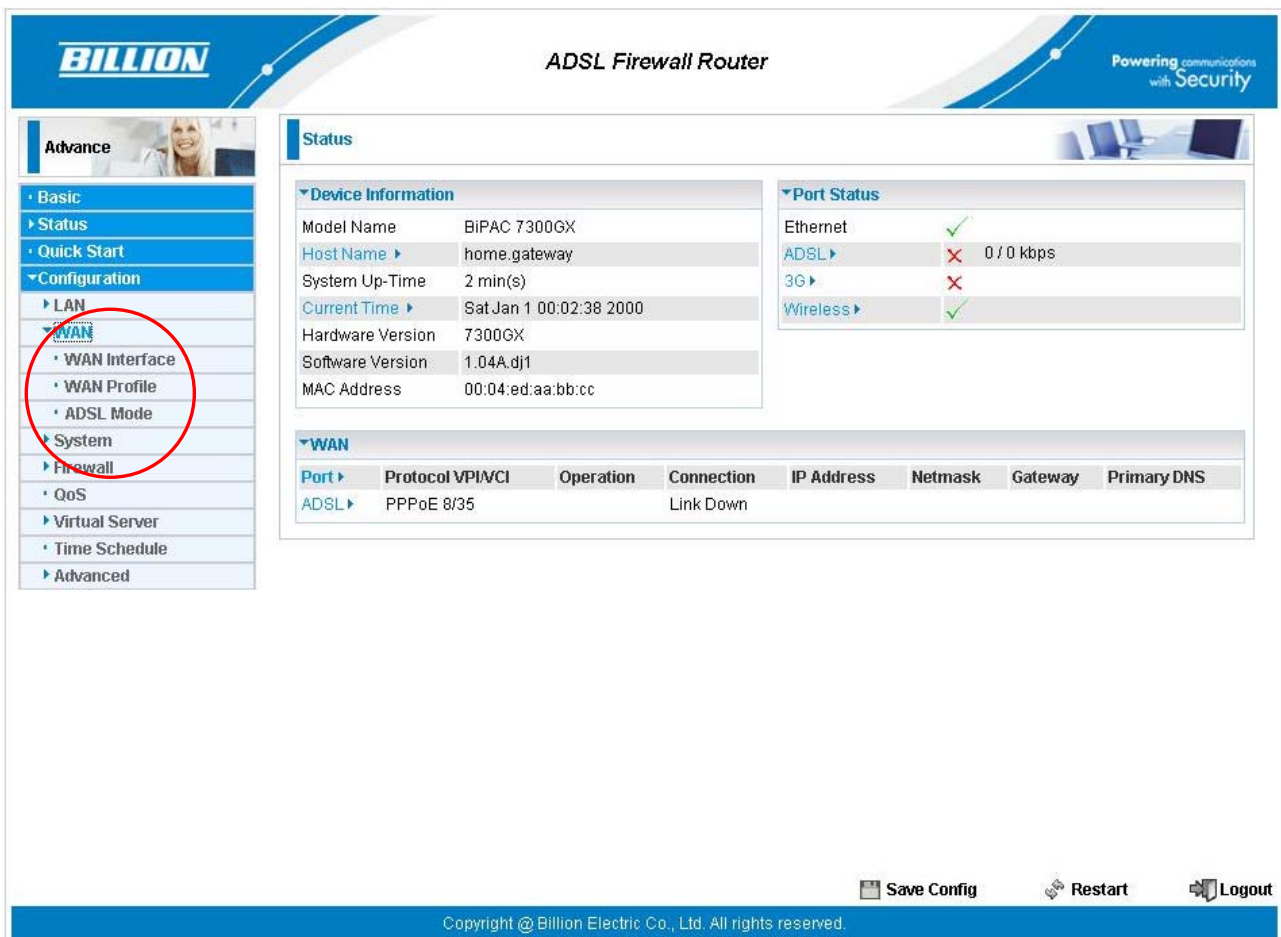
Parameters	
DHCP Server Mode	DHCP Relay
DHCP Relay Server	

Apply

Current Mode: DHCP Server

5.3.2 WAN (Wide Area Network)

A WAN (Wide Area Network) is an outside connection to another network or the Internet. There are three items within the **WAN** section: **WAN Interface**, **WAN Profile** and **ADSL Mode**.



The screenshot displays the web interface of a BILLION ADSL Firewall Router. The top navigation bar includes the BILLION logo, the product name 'ADSL Firewall Router', and the slogan 'Powering communications with Security'. The left sidebar contains a menu with categories like 'Basic', 'Status', 'Quick Start', 'Configuration', 'System', 'Firewall', 'QoS', 'Virtual Server', 'Time Schedule', and 'Advanced'. The 'Configuration' section is expanded to show 'LAN', 'WAN', and 'System'. The 'WAN' option is highlighted with a red circle. The main content area is titled 'Status' and is divided into two panels: 'Device Information' and 'Port Status'. The 'Device Information' panel lists details such as Model Name (BIPAC 7300GX), Host Name (home.gateway), System Up-Time (2 min(s)), Current Time (Sat Jan 1 00:02:38 2000), Hardware Version (7300GX), Software Version (1.04A.dj1), and MAC Address (00:04:ed:aa:bb:cc). The 'Port Status' panel shows the status of Ethernet (checked), ADSL (unchecked, 0 / 0 kbps), 3G (unchecked), and Wireless (checked). Below these panels is a table for the WAN connection status.

Port	Protocol	VPI/VCI	Operation	Connection	IP Address	Netmask	Gateway	Primary DNS
ADSL	PPPoE	8/35		Link Down				

At the bottom of the interface, there are buttons for 'Save Config', 'Restart', and 'Logout'. The footer contains the copyright notice: 'Copyright © Billion Electric Co., Ltd. All rights reserved.'

■ 5.3.2.1 WAN Interface

The factory default has the Connection Mode as ADSL and the Protocol as PPPoE.

WAN Connection-ADSL Mode

Configuration

▼ **WAN Interface**

WAN Connection

Main Port: ADSL (Current Main Port : ADSL)

Failover Parameters

Failover / Failback: Enable

Backup Port: 3G ▶

Connectivity Decision: Not in service when probing failed after 5 consecutive times.

Failover Probe Cycle: Every 60 seconds.

Failback Probe Cycle: Every 3 seconds.

Detect Rule (either one):

- ADSL Down
- Ping Fail
 - No Ping
 - Ping Gateway
 - Ping Host []

Notification: Enable

Recipient's E-mail: []

SMTP Server: []

Apply Cancel

- **Main Port:** User can select either “ADSL” or “3G” mode.
- **Failover / Failback:** Set **Enable** to trigger ADSL / 3G failover / failback function ready.
Note: If 3G is set for main port, then there can be no option for failover/failback.
- **Backup Port:** It links to backup port configuration page. It is necessary to configure it when Failover/Failback be set.
- **Connectivity Decision:** Set how many times of 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 set is for each probe cycle, but the decision to change to the backup port is determined by **Probe Cycle duration** multiplied by **connection Decision amount** (e.g. From the image above it will be 60 seconds multiplied by 5 consecutive fails).
- **Failback Probe Cycle:** Set the time duration for the **Failback Probe Cycle** to determine when the router will switch back to the main connection (main port) from the backup connection (backup port) once the main connection is communicating again.
Note: The time set is for each probe cycle, but the decision to change to the backup port is determined by **Probe Cycle duration** multiplied by **Connection Decision amount** (e.g. From the image above it will be 60 seconds multiplied by 5 consecutive fails).
- **Detect Rule:**

Rule 1. ADSL Down

Rule 2. Ping Fail

No Ping: It will not send any ping packet to determine the connection. It means to disable the ping fail detection.

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.

Notification: Select **Enable** to send mail to notify the Failover/Failback occurred.

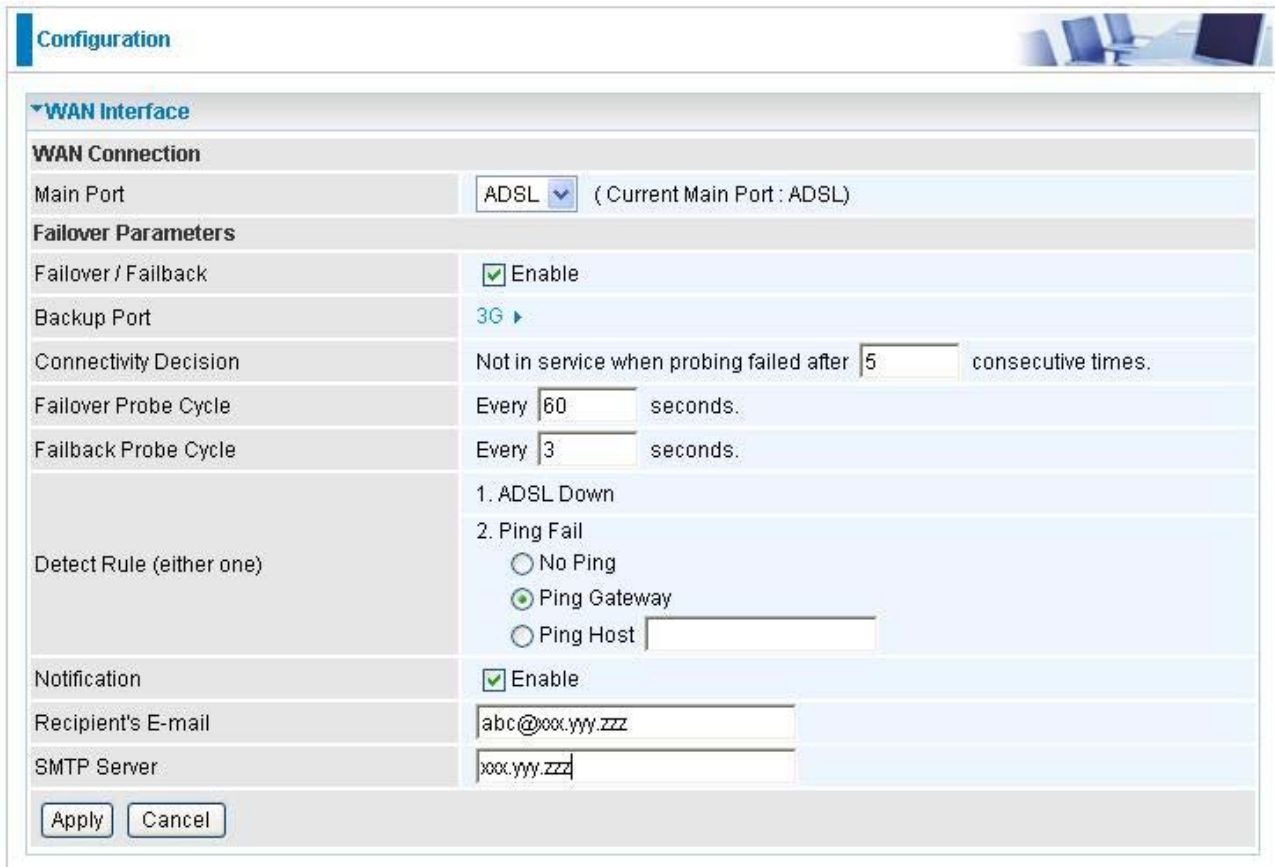
Recipient's E-mail: Set the Recipient's email address to which the email notification is sent.

SMTP Server: Set the SMTP (mail) server address.

Failover / Failback

Failover/Failback function is a mechanism to cover internet service when it is down. In this mode, 3G port is the only backup interface when ADSL service is not in service. It is necessary to set up the 3G card ready in device before power up. The Failover/Failback follows the rules base on "Failover Parameters" that user has defined.

An example for Failover / Failback



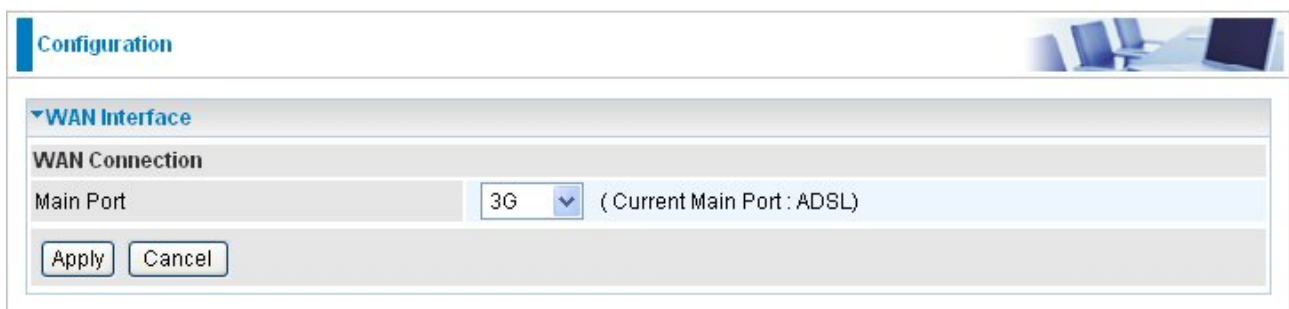
The screenshot shows a configuration window titled "Configuration" with a "WAN Interface" section. The "WAN Connection" is set to "ADSL". Under "Failover Parameters", "Failover / Failback" is checked and set to "Enable". The "Backup Port" is "3G". "Connectivity Decision" is "Not in service when probing failed after 5 consecutive times". "Failover Probe Cycle" is "Every 60 seconds" and "Failback Probe Cycle" is "Every 3 seconds". Under "Detect Rule (either one)", "1. ADSL Down" and "2. Ping Fail" are listed. Under "2. Ping Fail", "Ping Gateway" is selected. "Notification" is checked and set to "Enable". "Recipient's E-mail" is "abc@xxx.yyy.zzz" and "SMTP Server" is "xxx.yyy.zzz". "Apply" and "Cancel" buttons are at the bottom.

Configuration	
WAN Interface	
WAN Connection	
Main Port	ADSL (Current Main Port : ADSL)
Failover Parameters	
Failover / Failback	<input checked="" type="checkbox"/> Enable
Backup Port	3G
Connectivity Decision	Not in service when probing failed after 5 consecutive times.
Failover Probe Cycle	Every 60 seconds.
Failback Probe Cycle	Every 3 seconds.
Detect Rule (either one)	1. ADSL Down 2. Ping Fail <input type="radio"/> No Ping <input checked="" type="radio"/> Ping Gateway <input type="radio"/> Ping Host
Notification	<input checked="" type="checkbox"/> Enable
Recipient's E-mail	abc@xxx.yyy.zzz
SMTP Server	xxx.yyy.zzz
Apply Cancel	

This is an example of Failover/Failback function. The device will determine ADSL status and send ping packet to Gateway every 60 seconds. It will determine if the ADSL is Down or not replying from Gateway. If this happens 5 times continuously, the device will switch to 3G mode and try to establish the internet connection. Device will send a mail to abc@xxx.yyy.zzz via smtp server xxx.yyy.zzz to tell user(abc@xxx.yyy.zzz) this event had occurred.

After switching to 3G mode, device will still check for the ADSL status and send ping packet to Gateway every 3 seconds. The device will then go back to ADSL mode after it determines that the ADSL is now UP. It only does this after it gets reply from Gateway 5 times consecutively. Just like the previous state of change, the device will send email to notify the user of the event change.

WAN Connection-3G Mode



■ 5.3.2.2 WAN Profile

Profile Port--ADSL

● PPPoE Connection

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

Configuration

WAN Profile

Parameters

Profile Port: ADSL

Protocol: PPPoE (RFC2516, PPP over Ethernet)

Description: [] VPI/VCI: 8 / 35 Encap. method: LLC

Username: [Username] Password: [] Service Name: []

NAT: Enable IP (0.0.0.0: Auto): 0.0.0.0 Auth. Protocol: Auto

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

Connection: Always On Idle Timeout: 0 min(s) MTU: 1492

[Edit]

Protocol	Interface	Description	VPI	VCI	Encap. method	NAT	IP
PPPoE	wan_main		8	35	LLC	Enable	0.0.0.0

- **Description:** A user-definable name for this connection.
- **VPI/VCI:** Enter the VPI and VCI information provided by your ISP.
- **Encap. method:** Select the encapsulation format, the default is LLC. Select the one provided by your ISP
- **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.

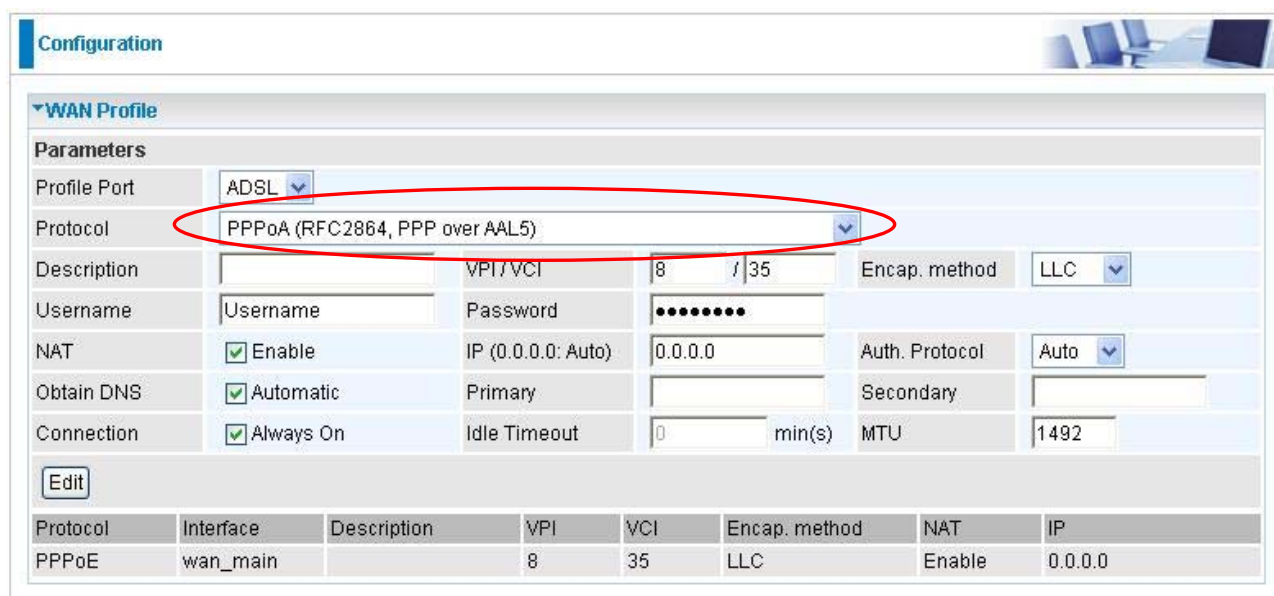
- **NAT:** The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single ISP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.
- **IP Address:** Your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

● PPPoA Connection

PPPoA stands for Point to Point Protocol over ATM Adaptation Layer 5 (AAL5). It provides access control and billing functionality in a manner similar to dial-up services using PPP.



The screenshot shows the 'Configuration' window for a WAN Profile. The 'WAN Profile' section is expanded, showing the 'Parameters' tab. The 'Protocol' dropdown menu is highlighted with a red circle and set to 'PPPoA (RFC2864, PPP over AAL5)'. Other visible settings include Profile Port (ADSL), VPI/VCI (8/35), Encap. method (LLC), Username, Password (masked), NAT (checked), Obtain DNS (checked), Connection (checked), and Idle Timeout (0 min(s)).

Protocol	Interface	Description	VPI	VCI	Encap. method	NAT	IP
PPPoE	wan_main		8	35	LLC	Enable	0.0.0.0

- **Description:** User-definable name for the connection.
- **VPI/VCI:** Enter the VPI and VCI information provided by your ISP.
- **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).
- **Encapsulation method:** Select the encapsulation format, the default is LLC. Select the one provided by your ISP
- **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.

● **Authentication Protocol Type:** Default is **Auto**. Your ISP should advise you on whether to use **Chap** or **Pap**.

● **Connection:**

⊙ **Always on:** The router will establish a PPPoA session when starting up and to automatically re-establish the PPPoA session when disconnected by the ISP.

⊙ **Connect to Demand (un-select Always On):** If you want to establish a PPPoA 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) that the IP attempts to send through the interface.

● **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 subnet mask.

● MPoA Connection

Configuration

WAN Profile

Parameters

Profile Port	ADSL	Protocol		MPoA (RFC1483/RFC2684, Multiprotocol Encapsulation over AAL5)			
Description		VPI/VCI	8 / 35	Encap. method	LLC		
Encap. mode	Bridged	NAT	<input checked="" type="checkbox"/> Enable				
IP (0.0.0.0: Auto)	0.0.0.0	Netmask	255.255.255.0	Gateway			
Obtain DNS	<input checked="" type="checkbox"/> Automatic	Primary		Secondary			

Protocol	Interface	Description	VPI	VCI	Encap. method	NAT	IP
PPPoE	wan_main		8	35	LLC	Enable	0.0.0.0

● **Description:** Your description of this connection.

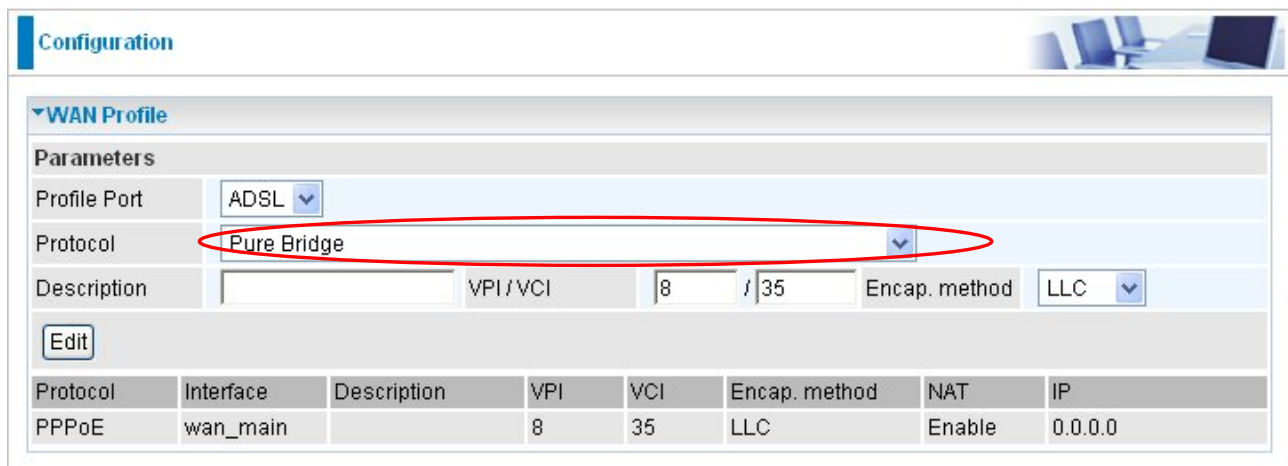
● **VPI and VCI:** Enter the VPI and VCI information provided by your ISP.

● **Encap. method:** Select the encapsulation format, the default is LLC. Select the one

provided by your ISP.

- **Encap. mode:** Choose whether you want the device to function as bridge mode or routing mode.
- **NAT:** The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing the 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.
- **Netmask:** The default is 255.255.255.0. User can change it to other such as 255.255.255.128. Type the subnet mask assigned to you by your ISP (if given)
- **Gateway:** Enter the IP address of the default gateway.
- **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 subnet mask.

● Pure Bridge Connections



The screenshot shows the 'Configuration' page for a WAN Profile. The 'Protocol' dropdown menu is set to 'Pure Bridge', which is circled in red. Below the form is a table showing the configuration details for the selected profile.

Protocol	Interface	Description	VPI	VCI	Encap. method	NAT	IP
PPPoE	wan_main		8	35	LLC	Enable	0.0.0.0

- **Description:** A user-definable name for this connection.
- **VPI/VCI:** Enter the VPI and VCI information provided by your ISP.
- **Encap. method:** Select the encapsulation format, this is provided by your ISP.

Profile Port--3G

Configuration

WAN Profile

Parameters

Profile Port	3G
TEL No.	*99***1#
APN	internet
Username	
Password	
PIN	
Connection	<input type="radio"/> Always On <input checked="" type="radio"/> Connect on Demand
Idle Timeout	600 seconds
Obtain DNS Automatically	<input checked="" type="checkbox"/> Enable
Primary DNS / Secondary DNS	/

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

Apply Cancel

● **TEL No.:** The dial string to make a GPRS / 3G user interneting call. It may provide 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's to be assigned 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.

● **PIN:** PIN stands for **P**ersonal **I**dentification **N**umber. A PIN code is a numeric value used in certain systems as a password to gain access, and authenticate. 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 you will require a PUK code from your network/service provider.

● **Connection:**

PIN	
Connection	<input checked="" type="radio"/> Always On <input type="radio"/> Connect on Demand
Keep Alive	<input type="checkbox"/> Enable
Obtain DNS Automatically	<input checked="" type="checkbox"/> Enable

⊙ **Always On:** The router will make UMTS/GPRS call when starting up. Enabling **Always On**, will give you an option of **Keep Alive**.

⊙ **Keep Alive:** Set **Enable** to allow the router automatically reconnects the connection when ISP disconnects it.

PIN	<input type="text"/>
Connection	<input type="radio"/> Always On <input checked="" type="radio"/> Connect on Demand
Idle Timeout	<input type="text" value="600"/> seconds
Obtain DNS Automatically	<input checked="" type="checkbox"/> Enable

⊙ **Connect to 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**.

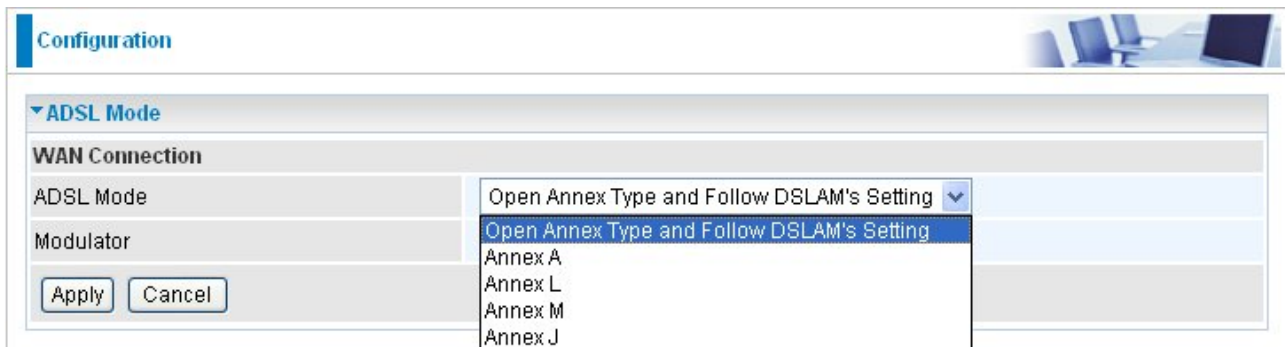
⊙ **Idle Timeout:** Auto-disconnect the connection when there is no activity on this call for a predetermined period of time. The default value is 600 seconds, and Idle Timeout not allow be set under 10 seconds.

● **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 subnet mask.

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

■ 5.3.2.3 ADSL Mode



Configuration

▼ ADSL Mode

WAN Connection

ADSL Mode: Open Annex Type and Follow DSLAM's Setting

Modulator: Open Annex Type and Follow DSLAM's Setting

Annex A

Annex L

Annex M

Annex J

Apply Cancel

● **ADSL Mode:** There are four modes “**Open Annex Type and Follow DSLAM's Setting**”, “**Annex A**”, “**Annex L**”, “**Annex M**” and “**Annex J**” that user can select for this connection.

● **Modulator:** There are seven modes “**AUTO**”, “**ADSL multimode**”, “**ADSL2**”, “**ADSL2+**”, “**G.Lite:**”, “**T1.413**” and “**G.DMT**” that user can select for this connection.



▼ ADSL Mode

WAN Connection

ADSL Mode Open Annex Type and Follow DSLAM's Setting ▼

Modulator Auto ▼

Apply Cancel

- Auto
- ADSL Multimode
- ADSL2
- ADSL2+
- G.Lite
- T1.413
- G.DMT

5.3.3 System

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

The screenshot displays the configuration interface for a BILLION ADSL Firewall Router. The page is titled "ADSL Firewall Router" and features the BILLION logo and the slogan "Powering communications with Security". The left sidebar contains a navigation menu with categories: "Advance", "Basic", "Status", "Quick Start", "Configuration", "System", "FireWall", "QoS", "Virtual Server", "Time Schedule", and "Advanced". The "System" category is expanded, and the "Time Zone" option is highlighted with a red circle. The main content area shows the "Time Zone" configuration page with the following parameters:

Parameters	
Time Zone	<input checked="" type="radio"/> Enable <input type="radio"/> 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	<input checked="" type="checkbox"/> Automatic
Resync Period	1440 minutes

Below the parameters is a world map showing the selected time zone. At the bottom of the configuration area are "Apply" and "Cancel" buttons. The footer of the page includes "Save Config", "Restart", and "Logout" buttons, along with the copyright notice: "Copyright © Billion Electric Co., Ltd. All rights reserved."


5.3.3.1 Time Zone

Time Zone

Parameters

Time Zone	<input checked="" type="radio"/> Enable <input type="radio"/> 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	<input checked="" type="checkbox"/> Automatic	
Resync Period	1440 minutes	

v



Apply Cancel

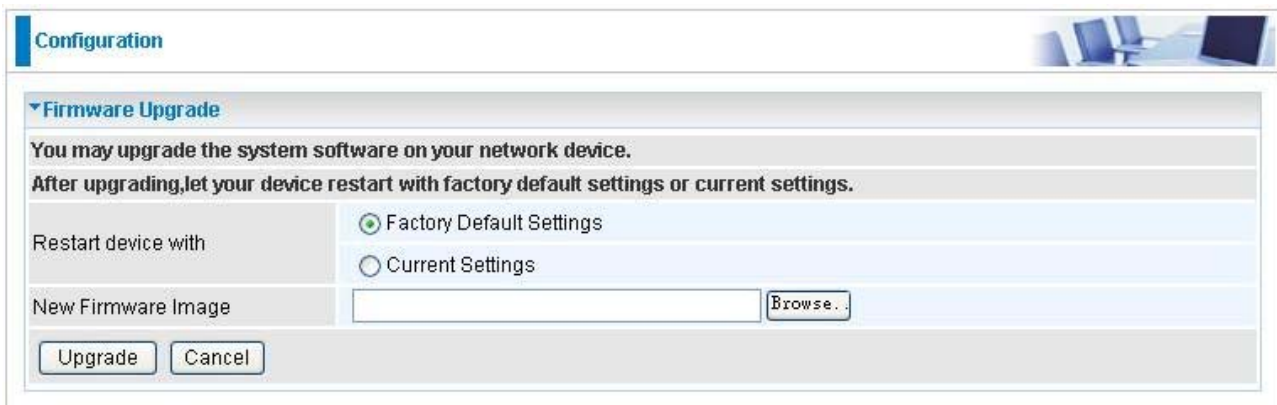
The router does not have a real time clock on board; instead, it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server outside your network. Choose your local time zone, click **Enable** and click the **Apply** button. After a successful connection to the Internet,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

■ 5.3.3.2 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 configuring a router. At the top, there is a 'Configuration' header. Below it, a section titled 'Firmware Upgrade' contains the following elements: a warning message 'You may upgrade the system software on your network device. After upgrading, let your device restart with factory default settings or current settings.', a 'Restart device with' section with two radio button options: 'Factory Default Settings' (which is selected) and 'Current Settings', a 'New Firmware Image' section with a text input field and a 'Browse...' button, and finally 'Upgrade' and 'Cancel' buttons at the bottom.

● **Restart Router 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.

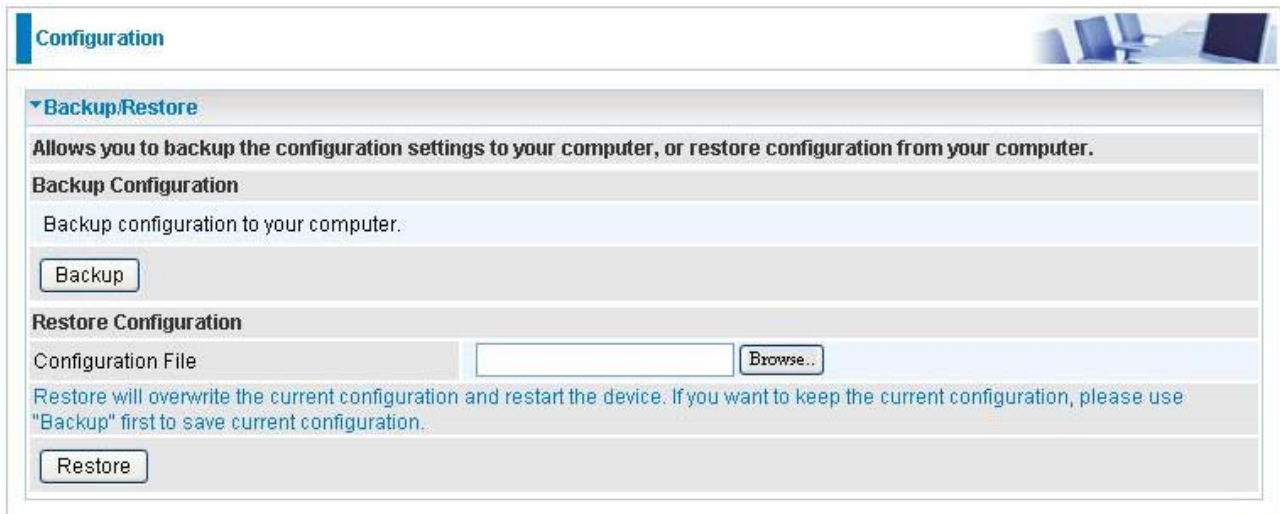
● **Upgrade:** Click **upgrade** to begin the upload process. This process may take up to three minutes.



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.

5.3.3.3 Backup / Restore



The screenshot shows a web interface titled "Configuration" with a sub-section "Backup/Restore". The sub-section contains the following elements:

- A header: "Backup/Restore"
- A description: "Allows you to backup the configuration settings to your computer, or restore configuration from your computer."
- A section titled "Backup Configuration" with the text "Backup configuration to your computer." and a "Backup" button.
- A section titled "Restore Configuration" with a "Configuration File" label, an empty text input field, and a "Browse.." button.
- A warning: "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."
- 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.

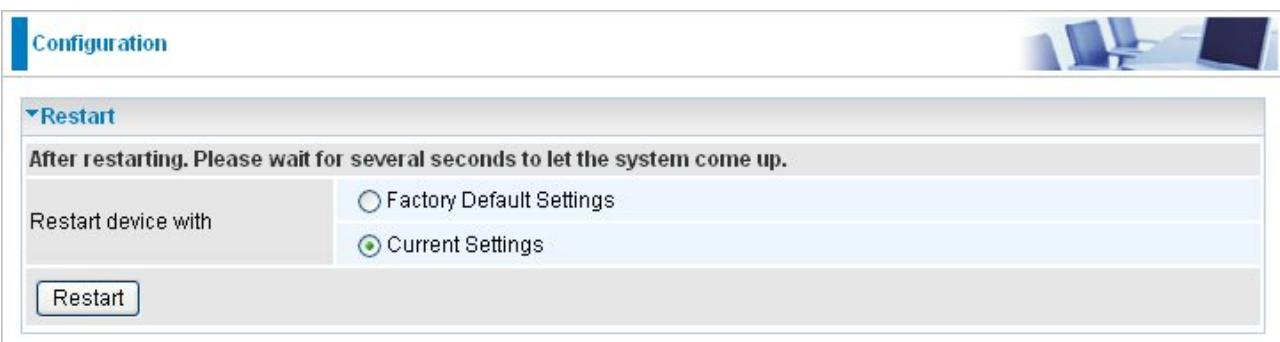
Press **Backup** to select where on your local PC to save the settings file. You may also change the name of the file when saving if you wish to keep multiple backups.

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.

5.3.3.4 Restart Router

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



The screenshot shows a web interface titled "Configuration" with a sub-section "Restart". The sub-section contains the following elements:

- A header: "Restart"
- A warning: "After restarting. Please wait for several seconds to let the system come up."
- A section titled "Restart device with" with two radio button options: "Factory Default Settings" and "Current Settings". The "Current Settings" option is selected.
- A "Restart" button.

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.

You may also reset your router to factory settings by holding the small Reset pinhole button more than 6 seconds on the back of your router.

Caution: After pressing the RESET button for more than 6 seconds and release it, the system will be restarted with the factory setting.

5.3.3.5 User Management

Valid	User	Password	Confirm
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Edit	Valid	User	Delete
<input type="radio"/>	true	admin	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.

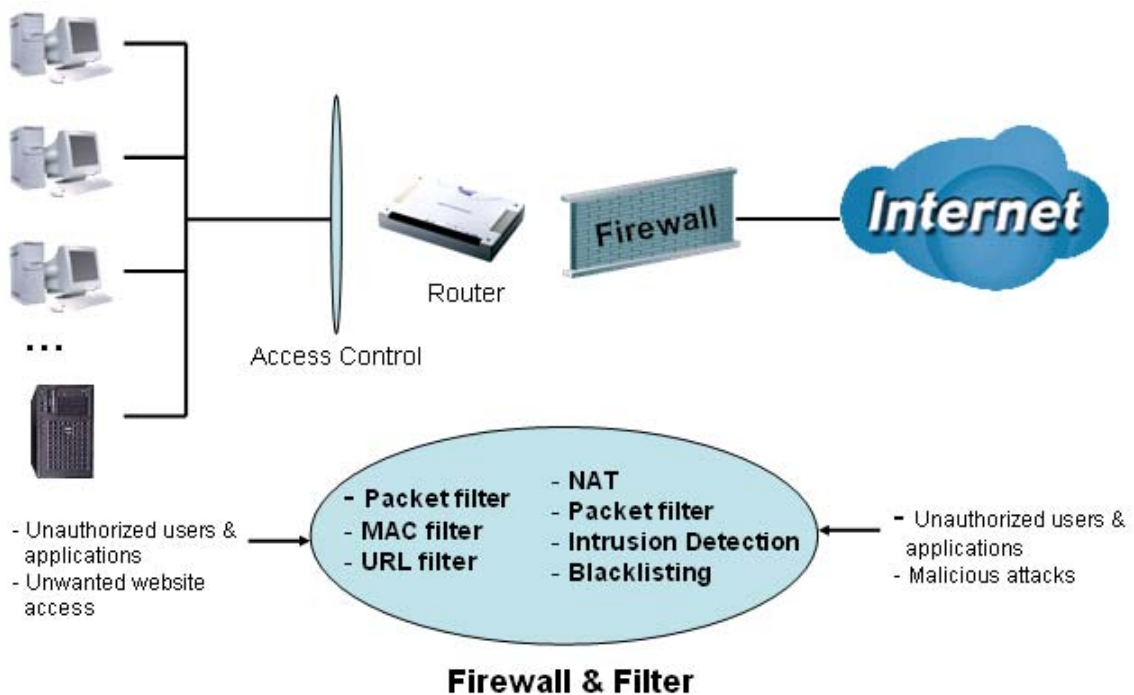
You can change the user's **password**, whether their account is active and **Valid**. These options are the same when creating a user account, with the exception that once created you cannot change the username. You cannot delete the default admin account; however you can delete any other created accounts 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.

5.3.4 Firewall

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.



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 Address Filter**, **Intrusion detection**, **Block WAN PING** and **URL Filter**.



■ 5.3.4.1 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	<input type="text"/>	<<	--select--	▼	(type or select from listbox)
Internal IP Address	<input type="text"/>	~	<input type="text"/>		
External IP Address	<input type="text"/>	~	<input type="text"/>		
Protocol	TCP	▼	Action	forward	▼
Internal Port	<input type="text"/>	~	<input type="text"/>	External Port	<input type="text"/> ~ <input type="text"/>
Direction	outgoing	▼	Time Schedule	Always On	▼
				Log	<input type="checkbox"/>

- **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 listbox.
- **Internal IP Address / External IP Address:** This is the Address-Filter used to allow or block traffic to/from particular IP address(es). Input the range you want to filter out. If you leave empty or 0.0.0.0, it means any IP address.
- **Protocol:** Specify the packet type (TCP, UDP, ICMP, etc.) that the rule applies to. Select **TCP** if you wish to search for the connection-based application service on the remote server using the port number. Or select **UDP** if you want to search for the connectionless application service on the remote server using the port number.
- **Action:** If a packet matches this filter rule, **Forward (allows the packets to pass)** or **Drop (disallow the packets to pass)** this packet.
- **Internal Port:** This Port or Port Range defines the ports allowed to be used by the Remote/WAN to connect to the application. Default is set from range **0 ~ 65535**. It is recommended that this option be configured by an advanced user.
- **External Port:** This is the Port or Port Range that defines the application.
- **Direction:** Determine whether the rule is for outgoing packets or for incoming packets.
- **Time Schedule:** It is self-defined time period. You may specify a time schedule for your prioritization policy. For setup and detail, refer to **Time Schedule** section.
- **Log:** Choose "log" if you wish to generate logs when the filter rule is applied to a packet.
- **Add:** Click this button to add a new packet filter rule and the added rule will appear at the bottom table.
- **Edit:** Check the Rule No. you wish to edit, and then click "Edit".
- **Delete:** Check the Rule No. you wish to delete, and then click "Delete".

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



Attention

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

5.3.4.2 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.

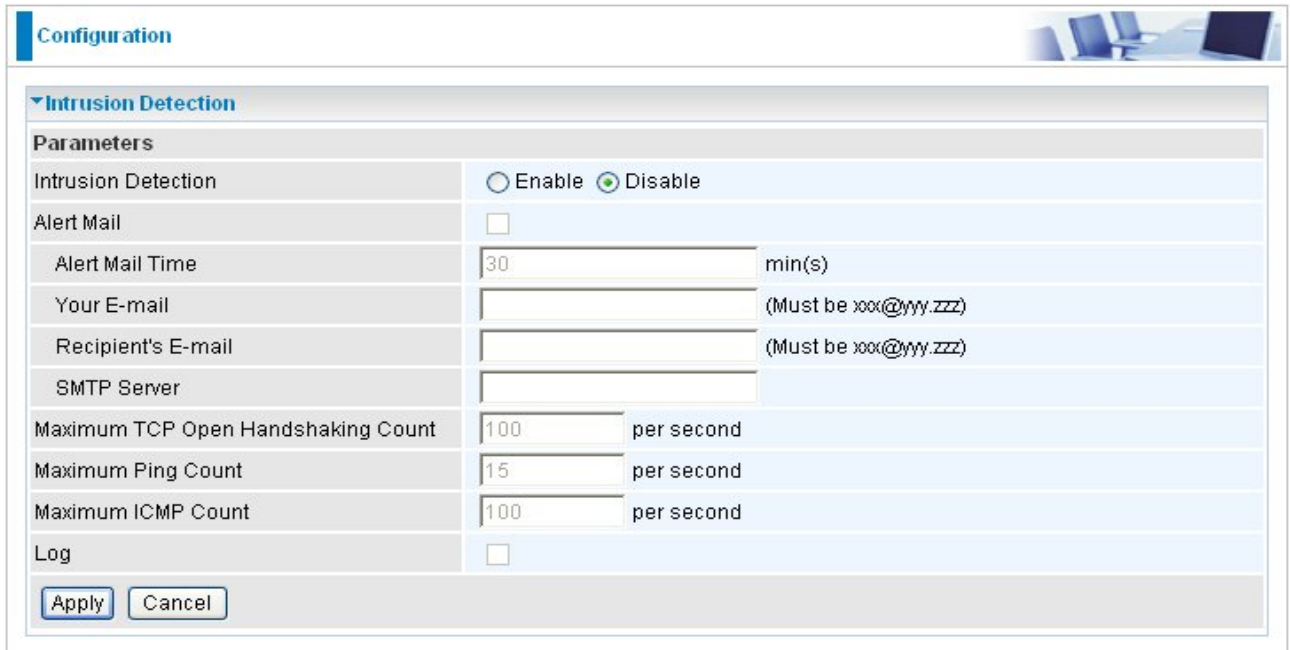
The screenshot shows a web-based configuration interface for a router. At the top, there is a 'Configuration' tab. Below it, the 'MAC Filter' section is expanded. Under 'Parameters', there is a 'MAC Address' field with a dropdown menu and a '(type or select from listbox)' label, and a 'Time Schedule' dropdown menu set to 'Always On'. Below the parameters are 'Add' and 'Edit / Delete' buttons. A table below shows two existing filter rules:

Edit	MAC Address	Time Schedule	Delete
<input type="radio"/>	00:04:ED:11:22:33	Always On	<input type="checkbox"/>
<input type="radio"/>	00:04:ED:12:34:56	Always On	<input type="checkbox"/>

- **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.

5.3.4.3 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
Alert Mail	<input type="checkbox"/>
Alert Mail Time	<input type="text" value="30"/> min(s)
Your E-mail	<input type="text"/> (Must be xxx@yyy.zzz)
Recipient's E-mail	<input type="text"/> (Must be xxx@yyy.zzz)
SMTP Server	<input type="text"/>
Maximum TCP Open Handshaking Count	<input type="text" value="100"/> per second
Maximum Ping Count	<input type="text" value="15"/> per second
Maximum ICMP Count	<input type="text" value="100"/> per second
Log	<input type="checkbox"/>

- **Intrusion Detection:** Check Enable if you wish to detect intruders accessing your computer without permission.
- **Alert Mail:** Select this check box to use Alert Mail.
- **Alert Mail Time:** Set the time for receiving Alert mail.
- **Your E-Mail:** Set your email address.
- **Recipient's E-mail:** Set the Recipient's email address to which the email notification is sent.
- **SMTP server:** Set the SMTP (mail) server address.
- **Maximum TCP Open Handshaking Count:** This is a threshold value to decide whether a SYN Flood attempt is occurring or not. Default value is 100 TCP SYN per seconds.
- **Maximum Ping Count:** This is a threshold value to decide whether an ICMP Echo Storm is occurring or not. Default value is 15 ICMP Echo Requests (PING) per second.
- **Maximum ICMP Count:** This is a threshold to decide whether an ICMP flood is occurring or not. Default value is 100 ICMP packets per seconds except ICMP Echo Requests (PING).
- **Log:** Check Log if you wish to generate logs when the filter rule is applied to the

Intrusion Detection.

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

Hacker attack types recognized by the IDS

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

	(Default 100 c/sec)				
ICMP Flood	Max ICMP Count (Default 100 c/sec)				Yes
ICMP Echo	Max PING Count (Default 15 c/sec)				Yes

Src IP: Source IP

Src Port: Source Port

Dst Port: Destination Port

Dst IP: Destination IP

■ 5.3.4.4 Block WAN PING

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

The screenshot shows the 'Configuration' page for 'Block WAN PING'. Under the 'Parameters' section, there is a checkbox for 'Block WAN PING' which is currently unchecked. To its right are two radio buttons: 'Enable' (unchecked) and 'Disable' (checked). Below these options are 'Apply' and 'Cancel' buttons.

■ 5.3.4.5 URL Filter

URL (Uniform Resource Locator – e.g. an address in the form of <http://www.billion.com> or <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.

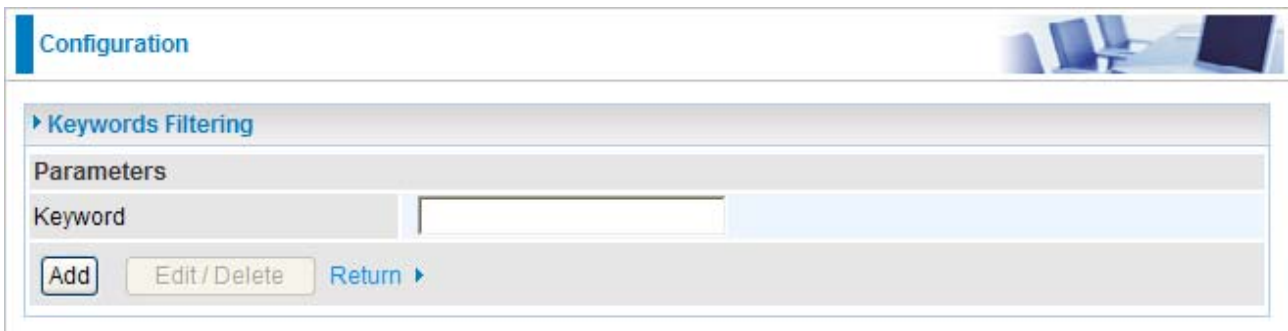
The screenshot shows the 'Configuration' page for 'URL Filter'. Under the 'Parameters' section, there are several settings:

- '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 (dropdown menu)
- 'Log':

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

● **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.



The screenshot shows a web interface for configuration. At the top, there is a blue header with the word "Configuration" and a small image of a computer monitor. Below the header, there is a section titled "Keywords Filtering" with a blue arrow icon. Underneath, there is a "Parameters" section. It contains a text input field labeled "Keyword" which is currently empty. Below the input field, there are three buttons: "Add", "Edit / Delete", and "Return" with a right-pointing arrow.

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

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

Configuration 

▸ Domains Filtering

Parameters

Domain Name Type Forbidden Domain ▾

[Return ▸](#)

Forbidden Domain

Edit	Domain Name	Delete
<input type="radio"/>	www.google	<input type="checkbox"/>

Trusted Domain

Edit	Domain Name	Delete
<input type="radio"/>	www.abc	<input type="checkbox"/>

● **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:**

Configuration 

▸ Except IP Address

Parameters

Internal IP Address ~

[Return ▸](#)

Edit	Internal IP Address	Delete
<input type="radio"/>	168.15.216.1 ~ 168.15.216.254	<input type="checkbox"/>

● **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.

5.3.5 QoS (Quality of Service)

Quality of Service Introduction

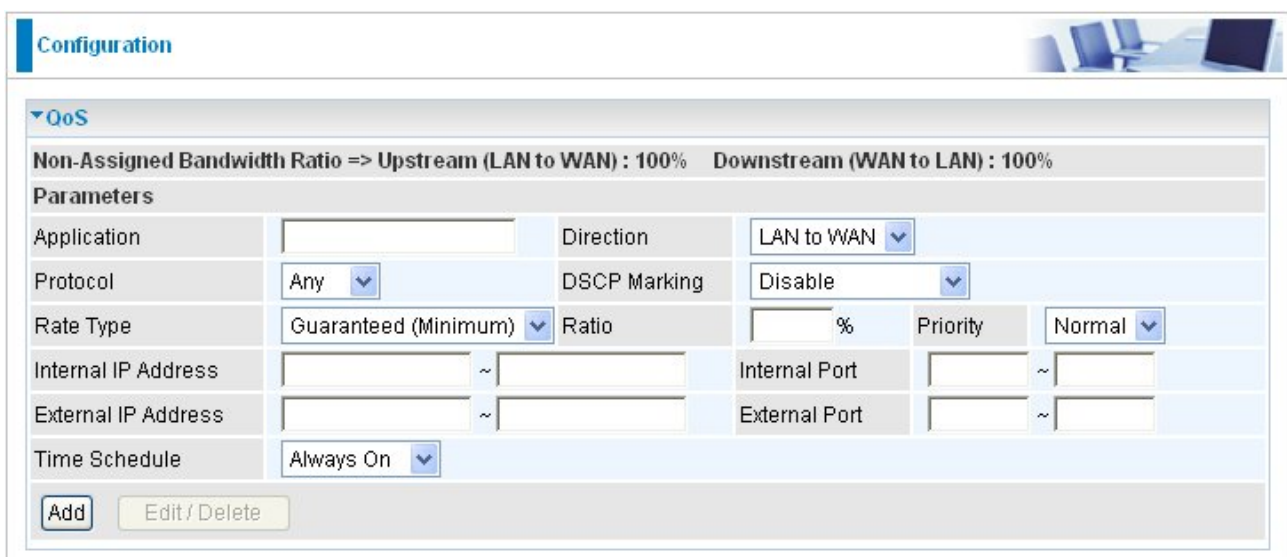
If you've ever found your 'net' speed has slowed to a crawl because another family member is using a P2P file sharing program, you'll understand why the Quality of Service features in Billion's routers is such a breakthrough for home users and office users.

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' page of a router. The 'QoS' section is expanded, showing a table of QoS policies. The table has columns for Application, Direction, Protocol, DSCP Marking, Rate Type, Ratio, Priority, Internal IP Address, Internal Port, External IP Address, and External Port. The 'Non-Assigned Bandwidth Ratio' is shown as 100% for both Upstream (LAN to WAN) and Downstream (WAN to LAN). The 'Parameters' section is visible, showing fields for Application, Direction (LAN to WAN), Protocol (Any), DSCP Marking (Disable), Rate Type (Guaranteed (Minimum)), Ratio (%), Priority (Normal), Internal IP Address, Internal Port, External IP Address, External Port, and Time Schedule (Always On). There are 'Add' and 'Edit / Delete' buttons at the bottom of the table.

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:** For PPTP VPN Connections.

● **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.

DSCP Mapping Table	
ADSL2+ 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. If you have ADSL LINE with 256K/bps.rate, the estimated data rate, in kbps, for this rule is $20\% * 256 * 0.9 = 46\text{kbps}$. (For 0.9 is an estimated factor for the effective data transfer rate for a ADSL LINE from LAN to WAN. For WAN-to-LAN, it is 0.85 to 0.8).

● **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.)

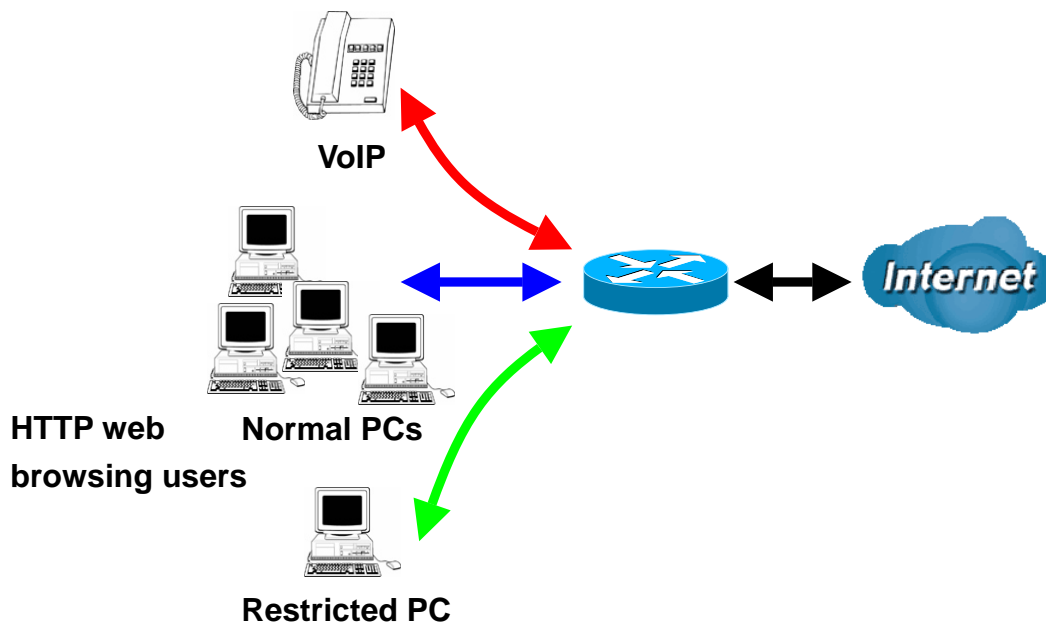
● **External IP Address:** The IP address values for Remote WAN machines you want to control. (For IP packets from LAN to WAN, it is the destination IP address. For IP packages from WAN to LAN, it is the source IP address.)

● **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.

■ QoS example for your Network

Connection Diagram



ADSL Subscription Rate

Upstream: 256 kbps

Downstream: 2048 Mbps

Example QoS Plan

Application	IP or Ports	Control Flow	Data Rate	Time Schedule
VoIP User	192.168.0.1	Outgoing	Minimal 20% with high priority for non-used bandwidth with	Always

			DSCP marking Class 1 Gold Service.	
FTP Sever	192.168.0.100	Incoming and Outgoing	outgoing :minimal 30%. Data rate. incoming :minimal 30%. Data rate. Both with low priority for non-used bandwidth.	Only Working Hours 9:00 to 17:00 Monday to Friday.
HTTP web browsing users	80	Incoming and Outgoing	outgoing : limited 20%. Data rate. incoming : limited 30%. Data rate.	Always

Example QoS Setup

Configuration

QoS

Non-Assigned Bandwidth Ratio => Upstream (LAN to WAN) : 45% Downstream (WAN to LAN) : 65%

Parameters

Application: [] Direction: LAN to WAN

Protocol: Any DSCP Marking: Disable

Rate Type: Guaranteed (Minimum) Ratio: [] % Priority: Normal

Internal IP Address: [] ~ [] Internal Port: [] ~ []

External IP Address: [] ~ [] External Port: [] ~ []

Time Schedule: Always On

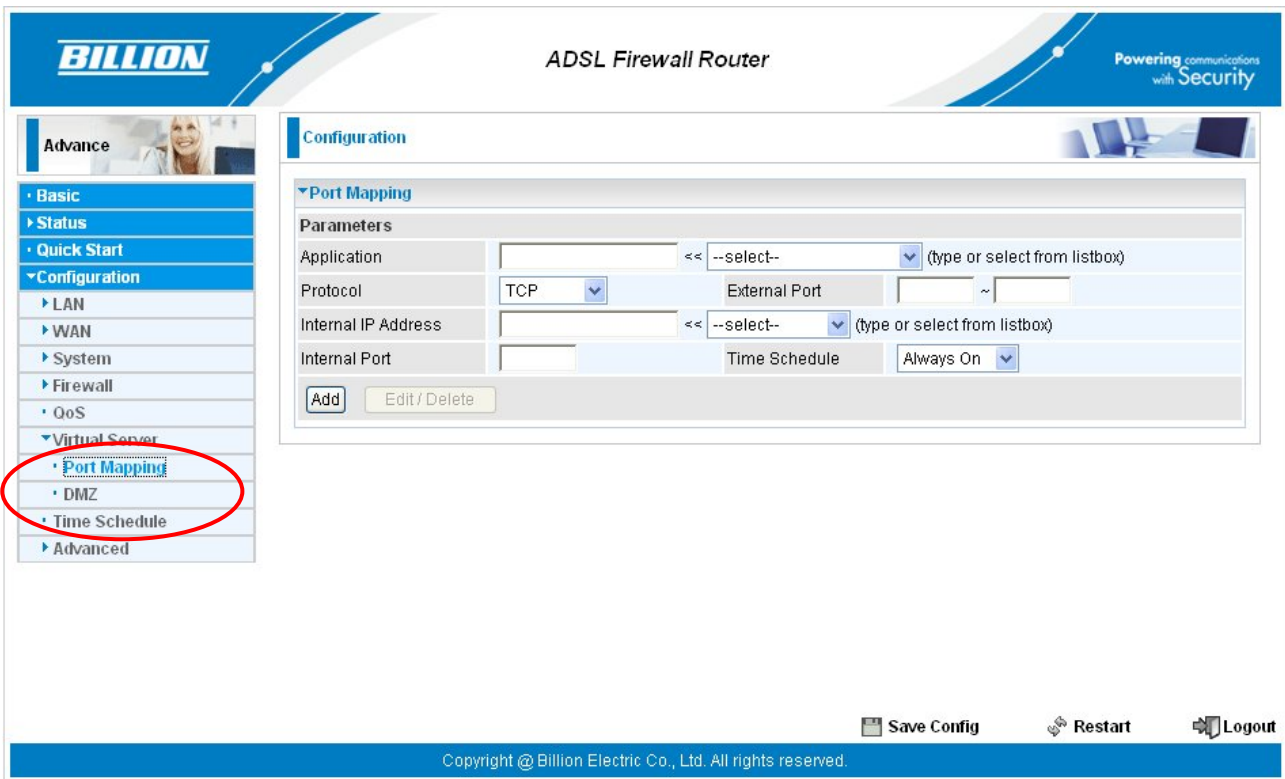
[Add] [Edit / Delete]

Edit	Application	Direction	Rate Type	Ratio	Time Schedule	Delete
<input type="radio"/>	VOIP	LAN to WAN	Guaranteed	20%	Always On	<input type="checkbox"/>
<input type="radio"/>	FTP Server	LAN to WAN	Guaranteed	15%	TimeSlot1	<input type="checkbox"/>
<input type="radio"/>	FTP Server (IN)	WAN to LAN	Guaranteed	15%	TimeSlot1	<input type="checkbox"/>
<input type="radio"/>	HTTP Browsing (OUT)	LAN to WAN	Limited	20%	Always On	<input type="checkbox"/>
<input type="radio"/>	HTPP Browsing (IN)	WAN to LAN	Limited	20%	Always On	<input type="checkbox"/>

VoIP application

Voice is latency-sensitive application. Most VoIP devices are used SIP protocol and the port number will be assigned by SIP module automatically. Better to use fixed IP address for catching VoIP packets as high priority.

5.3.6 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>

For help on determining which private port numbers are used by common applications on this list, please see the FAQs (Frequently Asked Questions) at: <http://www.billion.com>

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

5.3.6.1 Port Mapping

The screenshot shows a web-based configuration interface for port mapping. The main heading is 'Configuration' with a sub-heading 'Port Mapping'. Below this is a 'Parameters' section. It includes the following fields: 'Application' (a dropdown menu with '--select--' and '(type or select from listbox)'), 'Protocol' (a dropdown menu with 'TCP'), 'External Port' (a range input with '~' between two boxes), 'Internal IP Address' (a dropdown menu with '--select--' and '(type or select from listbox)'), 'Internal Port' (a text input), and 'Time Schedule' (a dropdown menu with 'Always On'). At the bottom of the parameters section are two buttons: 'Add' and 'Edit/Delete'.

- **Application:** Select the service you wish to configure
- **Protocol:** Automatic when you choose Application from listbox 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

Edit	Application	Protocol	External Port	Internal IP Address	Internal Port	Time Schedule	Delete
<input type="radio"/>	FTP	TCP	21~21	192.168.1.25	0	Always On	<input type="checkbox"/>
<input type="radio"/>	HTTP	TCP	80~80	192.168.1.2	0	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.

5.3.6.2 DMZ

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



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

1. If you disable the NAT option in the WAN-ISP section, the Virtual Server function becomes invalid.
2. If the DHCP server 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 a static IP address to each virtual server PC, with an address that does not fall into the range of IP addresses that are 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.

5.3.7 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 : End Time :

Edit	Name	Day in a week	Start Time	End Time	Clear
<input type="radio"/>	TimeSlot1	smtwfs	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot2	smtwfs	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot3	smtwfs	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot4	smtwfs	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot5	smtwfs	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot6	smtwfs	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot7	smtwfs	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot8	smtwfs	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot9	smtwfs	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot10	smtwfs	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot11	smtwfs	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot12	smtwfs	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot13	smtwfs	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot14	smtwfs	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot15	smtwfs	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot16	smtwfs	08:00	18:00	<input type="checkbox"/>

- **Name:** A user-define description to identify this time portfolio.
- **Day:** The default is set from Sunday through Saturday. You may specify the days for the schedule to be applied.

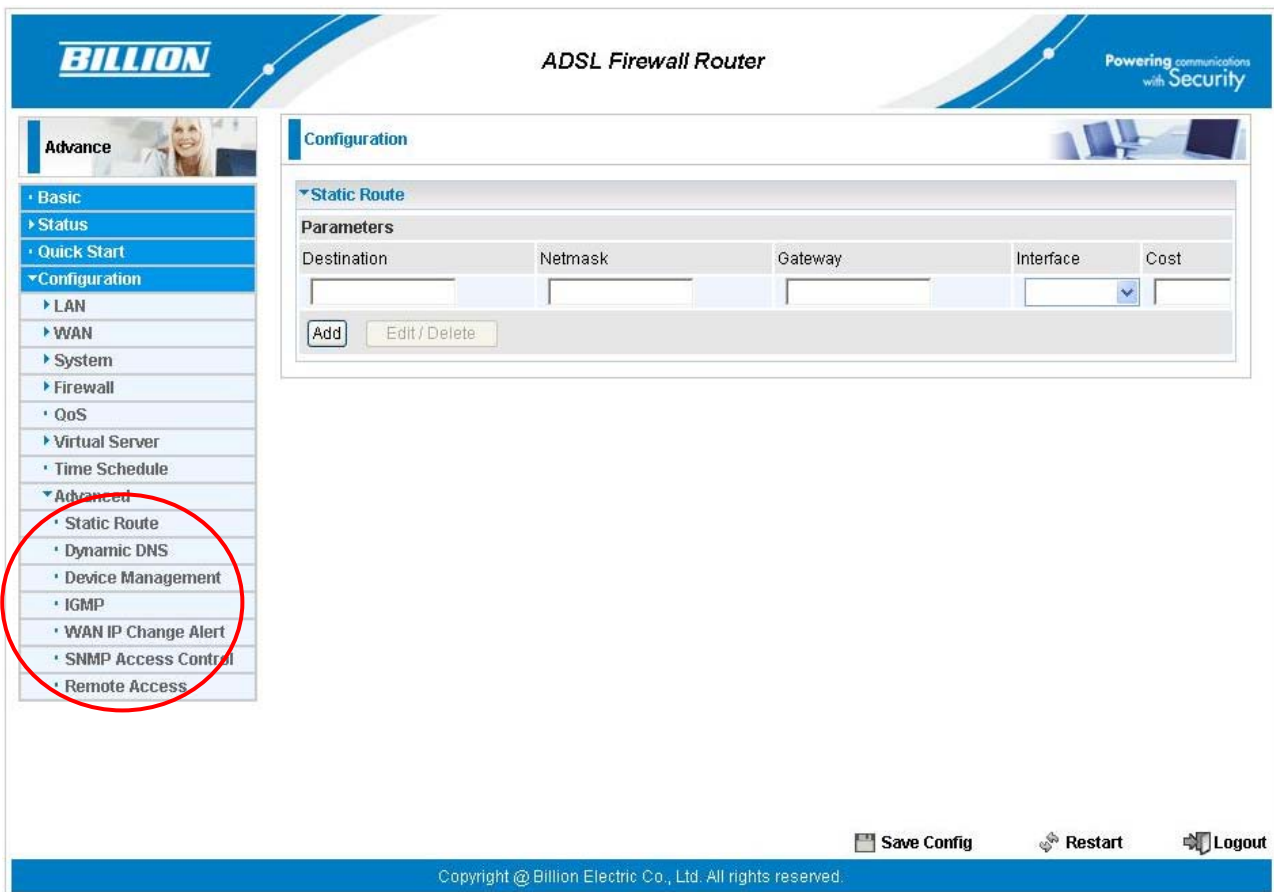
● **Start Time:** The default is set at 8:00 AM. You may specify the start time of the schedule.

● **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.

5.3.8 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**, **Dynamic DNS**, **Device Management**, **IGMP**, **WAN IP Change Alert**, **SNMP Access Control** and **Remote Access**.



■ 5.3.8.1 Static Route

Configuration

Static Route

Parameters

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.

■ 5.3.8.2 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 ADSL 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/>

Configuration

Dynamic DNS

Parameters

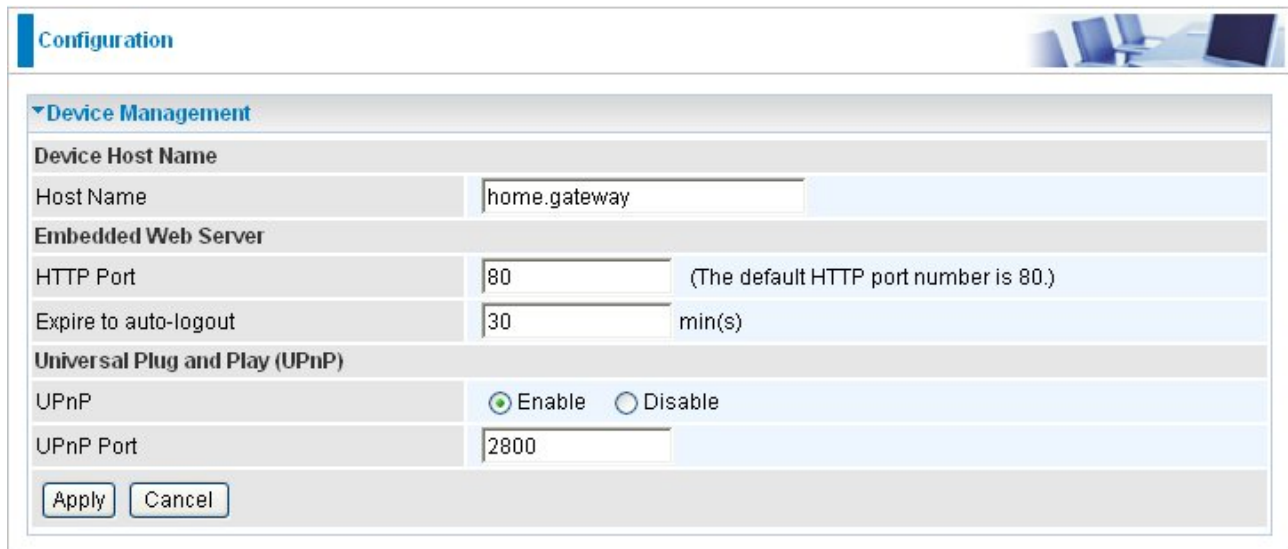
Dynamic DNS	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Dynamic DNS Server	www.dyndns.org
Wildcard	<input type="checkbox"/> Enable
Domain Name	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
Period	28 Day(s)

There are more than 5 DDNS services supported.

- **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.

5.3.8.3 Device Management

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



The screenshot shows the 'Configuration' page of a router, specifically the 'Device Management' section. The 'Device Host Name' field is set to 'home.gateway'. Under 'Embedded Web Server', the 'HTTP Port' is set to 80 (with a note: '(The default HTTP port number is 80.)') and 'Expire to auto-logout' is set to 30 min(s). Under 'Universal Plug and Play (UPnP)', the 'UPnP' checkbox is checked (Enable) and the 'UPnP Port' is set to 2800. At the bottom, there 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 **192.168.1.55**, and sets the logout time to be **100** minutes. The router only allows User A access from the IP address **192.168.1.55** to logon to the Web GUI by typing: <http://192.168.1.254:100> in their web browser. After 100 minutes, the device automatically logs out User A.

Universal Plug and Play (UPnP):

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

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

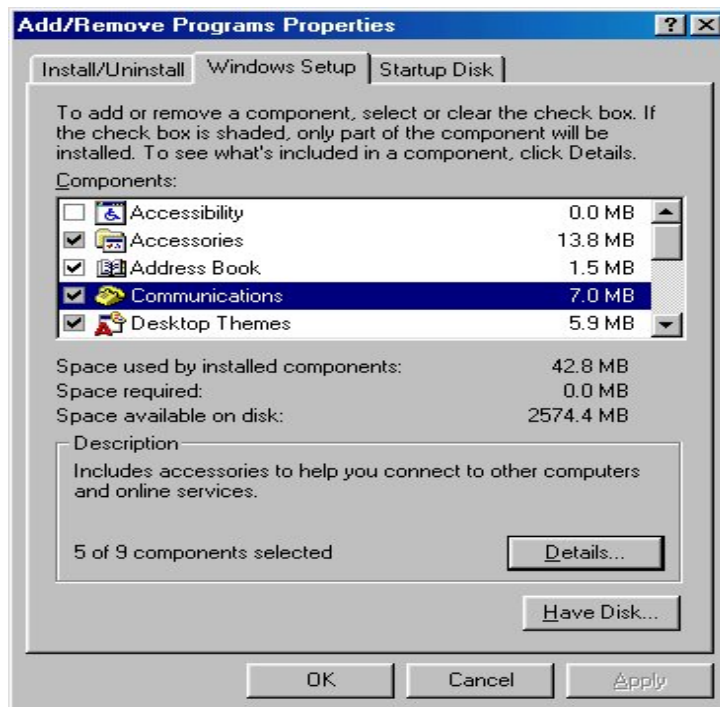
- **Disable:** Check to disable the router's UPnP functionality.
- **Enable:** Check to enable the router's UPnP functionality.
- **UPnP Port:** The Default setting is 2800. It is highly recommended you use this port value. If this value conflicts with other ports already in use you may wish to change the port.

Installing UPnP in Windows Example

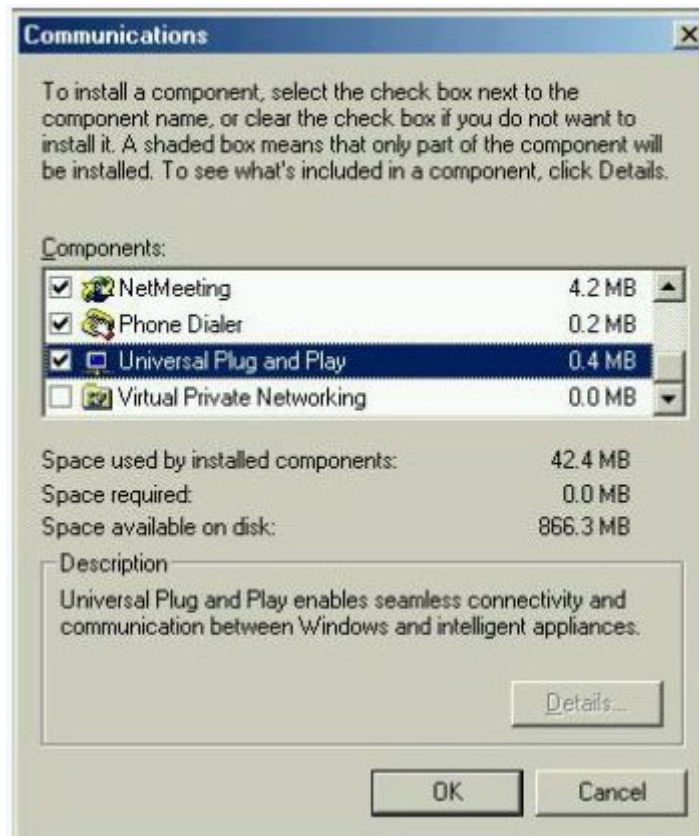
Follow the steps below to install the UPnP in Windows Me.

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

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



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



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

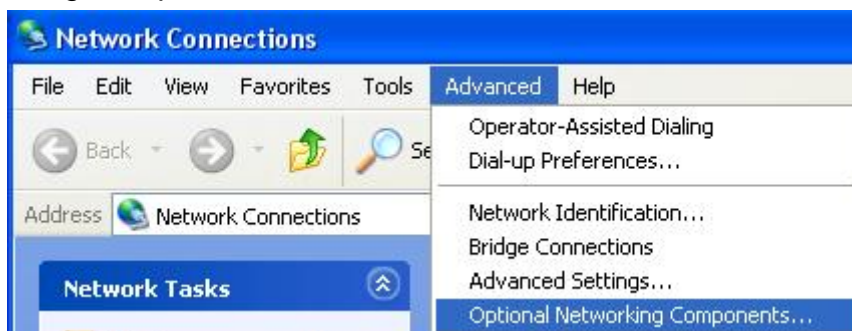
Step 5: Restart the computer when prompted.

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

Step 1: Click Start and Control Panel.

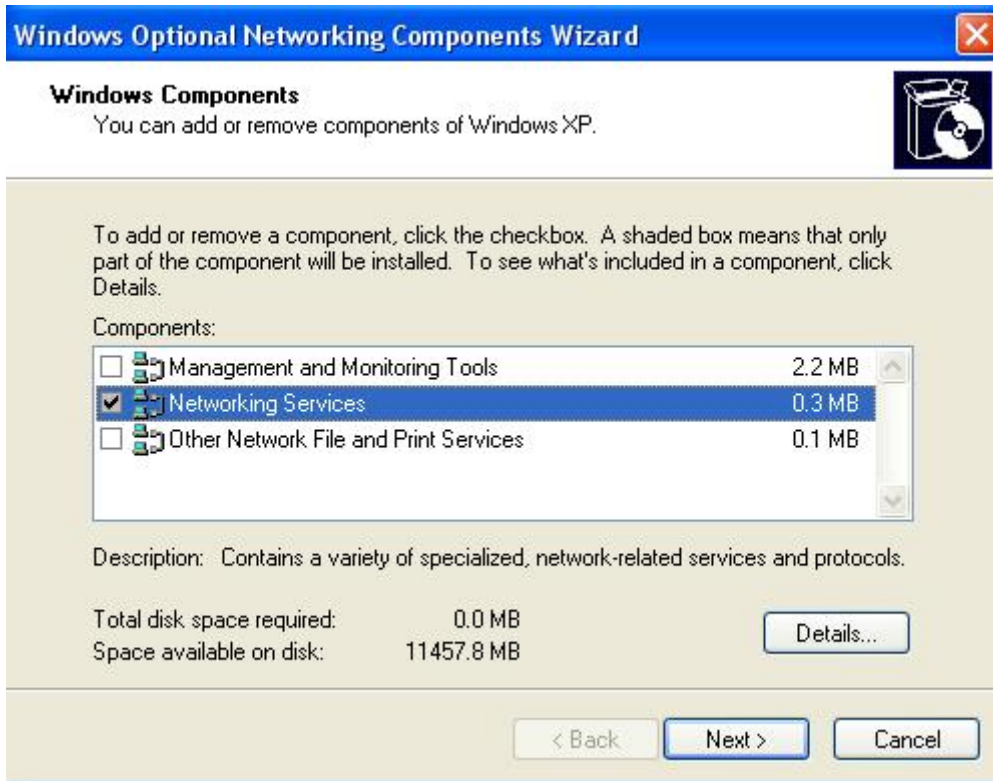
Step 2: Double-click Network Connections.

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



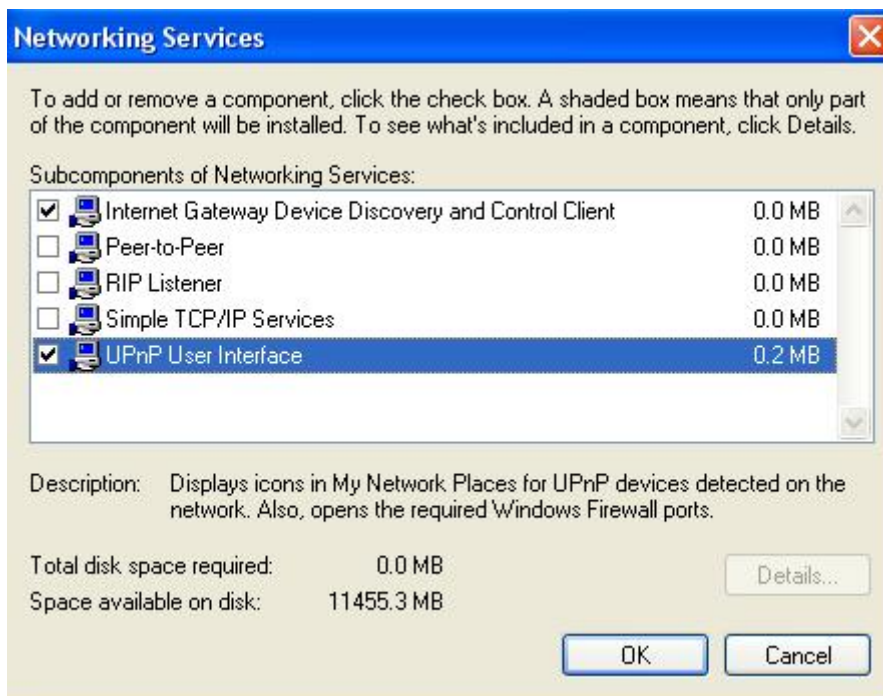
The Windows Optional Networking Components Wizard window displays.

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



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

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



Auto-discover Your UPnP-enabled Network Device

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

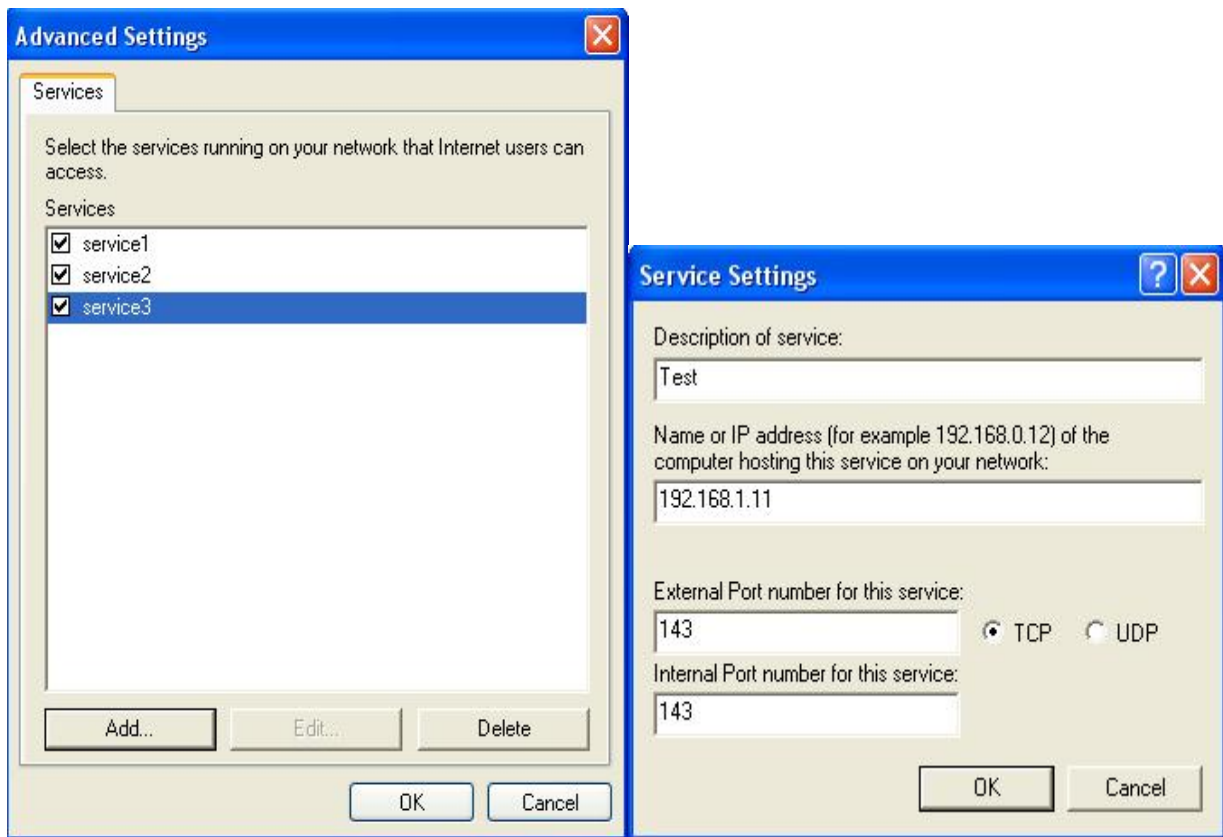
Step 2: Right-click the icon and select Properties.



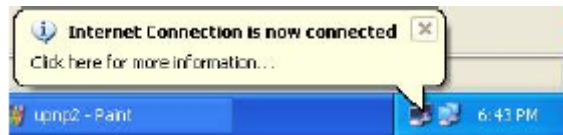
Step 3: In the Internet Connection Properties window, click Settings to see the port mappings that were automatically created.



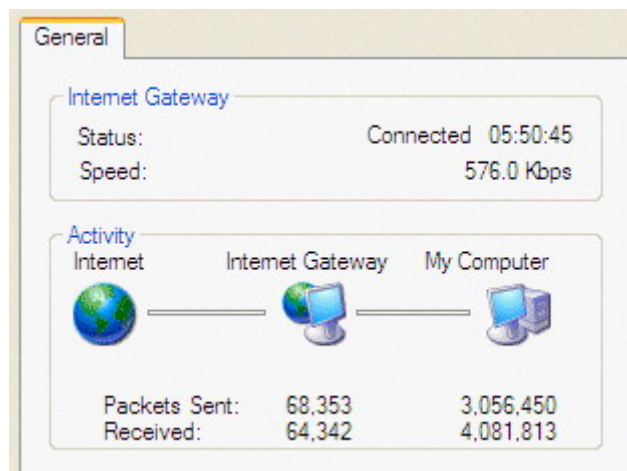
Step 4: You may edit or delete the port mappings or click Add to manually add port mappings.



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



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



Web Configurator Easy Access

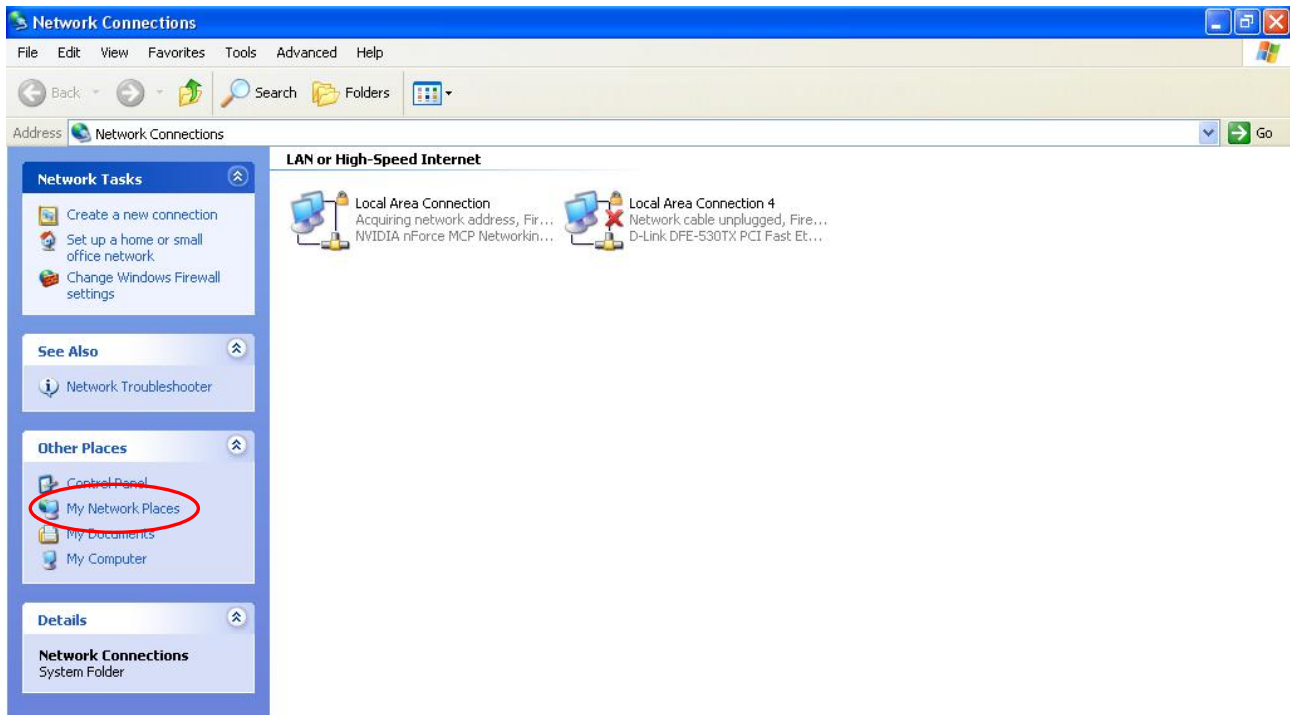
With UPnP, you can access web-based configuration for the BiPAC 7300GX without first finding out the IP address of the router. This helps if you do not know the router's IP address.

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 BiPAC 7300GX and select Invoke. The web configuration login screen displays.

Step 6: Right-click on the icon of your BiPAC 7300GX and select Properties. A properties window displays basic information about the BiPAC 7300GX.

■ 5.3.8.4 IGMP

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

● **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**.

■ 5.3.8.5 WAN IP Change Alert

● **Send a log via Email When WAN IP is changed.** Default is set to **Disable**.

● **Recipient's E-mail:** Set the Recipient's email address to which the email notification is sent.

● **SMTP server:** Set the SMTP (mail) server address.

■ 5.3.8.6 SNMP Access Control

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

Configuration

SNMP Access Control

Parameters

SNMP Enable Disable

SNMP V1 and V2

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

SNMP V3

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

SNMP V1 and V2:

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

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

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

SNMP V3:

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

SNMP Version: SNMPV2c and SNMPv3

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

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

Traps supported: Cold Start, Authentication Failure.

The following MIBs are supported:

From RFC 1213 (MIB-II):

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

From RFC1650 (EtherLike-MIB):

- dot3Stats

From RFC 1493 (Bridge MIB):

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

From RFC 1471 (PPP/LCP MIB):

- pppLink group
- pppLqr group

From RFC 1472 (PPP/Security MIB):

- PPP Security Group)

From RFC 1473 (PPP/IP MIB):

- PPP IP Group

From RFC 1474 (PPP/Bridge MIB):

- PPP Bridge Group

From RFC1573 (IfMIB):

ifMIBObjects Group

From RFC1695 (atmMIB):

atmMIBObjects

From RFC 1907 (SNMPv2):

only snmpSetSerialNo OID

5.3.8.7 Remote Access

The screenshot shows a configuration page titled "Configuration" with a sub-section "Remote Access". Under "Remote Access", there are two main sections: "Parameters" and "Allowed Access IP Address Range".

Parameters: This section contains a "Remote Access Control" field with an "Enable" checkbox (currently unchecked) and a "Duration" field with a text input box and a label "min(s) (0: Always On)". An "Apply" button is located below these fields.

Allowed Access IP Address Range: This section contains a "Valid" checkbox (checked) and an "IP Address Range" field with two text input boxes separated by a tilde (~). Below this section are "Add" and "Edit / Delete" buttons.

Remote Access Control:

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

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


Allowed Access IP Address Range:

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

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

5.4 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.

 Save Config


Configuration 

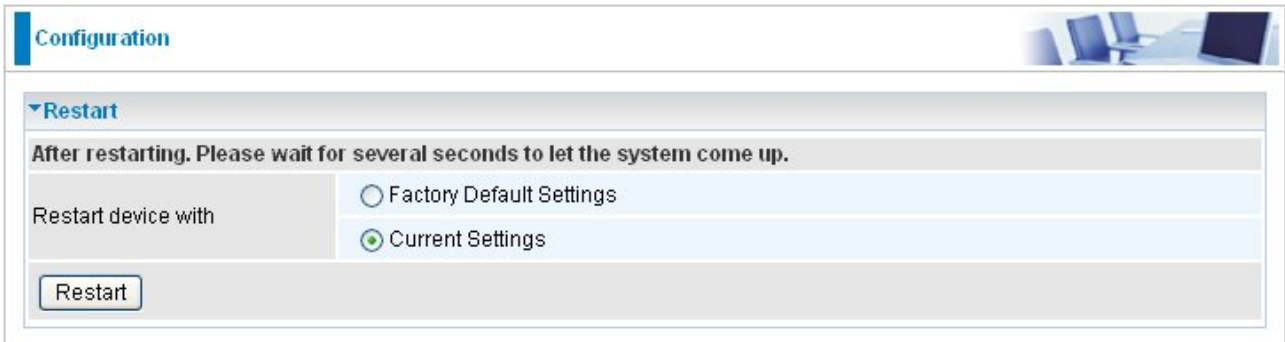
▼ Save Config to FLASH

Write settings to FLASH

5.5 Restart

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

 **Restart**



The screenshot shows the 'Configuration' page of a router. At the top, there is a blue header with the word 'Configuration' and a small image of a router. Below the header, there is a section titled 'Restart' with a dropdown arrow. Underneath, a message reads: 'After restarting. Please wait for several seconds to let the system come up.' Below this message, there is a label 'Restart device with' followed by two radio button options: 'Factory Default Settings' and 'Current Settings'. The 'Current Settings' option is selected. At the bottom of this section, there is a 'Restart' button.


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.

You may also reset your router to factory settings by holding in the small Reset pinhole button on the back of your router over 6 seconds then release it. The router will restart and reset to factory default setting.

5.6 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 30 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.

 Logout

Chapter 6

Troubleshooting

If your ADSL Router is not functioning properly, you can refer first to this chapter for simple troubleshooting before contacting your service provider or Billion support. This can save you time and effort but if symptoms persist, consult your service provider.

Problems starting up the router

None of the LEDs are on when you turn on the router.	Check the connection between the adapter and the router. If the error persists, you may have a hardware problem. In this case you should contact technical support.
You have forgotten your router login and/or password.	Try the default login and password, please refer to Chapter 3. If this fails, you can restore your router to its factory settings by holding the Reset button on the back of your router for 6 seconds or more.

Problems with the WAN Interface

Initialization of the PVC connection (“linesync”) failed.	Ensure that the telephone cable is connected properly from the ADSL port to the wall jack. The ADSL LED on the front panel of the router should be on. Check that your VPI, VCI, encapsulation type and type of multiplexing settings are the same as those provided by your ISP. Reboot the router . If you still have problems, you may need to verify these settings with your ISP.

<p>Frequent loss of ADSL linesync (disconnections).</p>	<p>Ensure that all other devices connected to the same telephone line as your router (e.g. telephones, fax machines, analogue modems) have a line filter connected between them and the wall socket (unless you are using a Central Splitter or Central Filter installed by a qualified and licensed electrician), and ensure that all line filters are correctly installed and the right way around. Missing line filters or line filters installed the wrong way around can cause problems with your ADSL connection, including causing frequent disconnections. If you have a back-to-base alarm system you should contact your security provider for a technician to make any necessary changes.</p>
--	--

Problems with the LAN Interface

<p>Can't ping any PCs on the LAN.</p>	<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>