

BiPAC 5200W

Wireless-N

ADSL2+ Firewall Router

User Manual

Table of Contents

Chapter 1	1
1.1 Introducing the BiPAC 5200W Router	1
1.1.1 Express Internet Access	1
1.1.2 Upgrade Wireless Access	2
1.1.3 Robust Firewall Security and Smooth Traffic	2
1.1.4 Easy Network Management	2
1.2 Features	3
1.2.1 ADSL Compliance	3
1.2.2 Network Protocols and Features	4
1.2.3 Firewall & Virtual Private Network (VPN)	4
1.2.4 Quality of Service Control	4
1.2.5 Wireless LAN	5
1.2.6 ATM and PPP Protocols	5
1.2.7 Management	5
1.3 Hardware Specifications	6
1.3.1 Physical Interface	6
1.4 Applications for the BiPAC 5200W	7
Chapter 2	8
2.1 Important note for using the BiPAC 5200W	8
2.2 Package Contents	9
2.3 The Front LEDs	10
2.4 The Rear Ports	11
2.5 Cabling	12
Chapter 3	13
3.1 Before Configuration	13
3.1.1 Configuring PC in windows 7	14
3.1.2 Configuring PC in Windows XP	16
3.1.3 Configuring PC in Windows 2000	17
3.1.4 Configuring PC in Windows 98/Me	18
3.1.5 Configuring PC in Windows NT4.0	19
3.2 Step-by-Step Installation	20
3.3 Factory Default Settings	23
3.3.1 Username and Password	23
3.4 LAN and WAN Port Addresses	24

3.5 Information from your ISP	24
3.6 Configuring with your Web Browser	25
Chapter 4.....	26
4.1 Quick Start.....	27
4.2 Interface Setup	31
4.2.1 Internet	31
4.2.2 LAN.....	35
4.2.3 Wireless.....	37
4.3 Advanced Setup	43
4.3.1 Firewall	43
4.3.2 Routing	44
4.3.3 NAT.....	46
4.3.4 QoS	52
4.3.5 ADSL	55
4.4 Access Management.....	56
4.4.1 ACL.....	56
4.4.2 Filter.....	57
4.4.3 SNMP	61
4.4.4 UPnP	62
4.4.5 DDNS	63
4.5 Maintenance.....	64
4.5.1 Administrator.....	64
4.5.2 Time Zone.....	65
4.5.3 Firmware.....	66
4.5.4 SysRestart	67
4.5.5 Diagnostics	68
4.6 Status	69
4.6.1 Device Info.....	69
4.6.2 System Log.....	71
4.6.3 Statistics	72
4.7 Help.....	75
Chapter 5.....	76
APPENDIX.....	78

1.1 Introducing the BiPAC 5200W Router

The BiPAC 5200W is an economical ADSL2+ router ideal for Home and SOHO users to enjoy improved Wireless Access Speed with a maximum operational speed of 150Mbps. It delivers the highest level of security with higher speed and better coverage of wireless-g solutions. The BiPAC 5200W has integrated SOHO firewall security, providing protection for your valuable but vulnerable data and network against potential hack attacks, and at the same time provides Quality of Service function, helping to prioritize queues of data traffic and ensure a smooth Internet connection. With a built-in antenna, the BiPAC 5200W is able to search for wireless signals inherently and intuitively, effectively reaching optimal connectivity; you can surf the Internet with the convenience and fun of mobility from every corner of your home or office. This device allows you to enjoy all Internet applications like music downloads, online gaming, video streaming, and file sharing with your family or colleagues!

1.1.1 Express Internet Access

Complying with worldwide ADSL standards, the BiPAC 5200W supports downstream data transmission rates up to 12/24 Mbps with ADSL2/2+, 8 Mbps with ADSL, and performs at upstream rates of up to 1 Mbps. Even more; the BiPAC 5200W includes Annex M technology that supports the latest ADSL2/2+ standard for higher upload speeds by increasing the upstream data rate to approximately 2.5Mbps (up to 3Mbps under ideal conditions). With this technology, you can enjoy even high-speed broadband multimedia applications such as interactive gaming, video streaming and real-time audios that run faster and easier than ever.

1.1.2 Upgrade Wireless Access

With an integrated Wireless-N Wireless Access Point that supports up to 150Mbps wireless data rate, your wireless connection is truly improved compared to 802.11b/g standard, yet the router can backward complies your existing 802.11b/g network devices. Wi-Fi Protected Access (WPA-PSK / WPA2-PSK) and Wired Equivalent Privacy (WEP) features enhance the level of transmission security and access control over your Wireless LAN.

1.1.3 Robust Firewall Security and Smooth Traffic

The NAT default firewall has an advanced anti-hacker pattern-filtering protection features that can automatically detect and block Denial of Service (DoS) attacks. In addition, Packet Filtering provides high-level security for access control. Built with Stateful Packet Inspection (SPI), the router enables users to determine whether a data packet is allowed to pass through the firewall to the private LAN. Quality of Service Control prioritizes the traffic and allows users to enjoy smooth traffic while running applications such as P2P or multimedia through the Internet.

1.1.4 Easy Network Management

A user-friendly, web-based user interface makes installing and managing the BiPAC 5200W extremely easy. With support for both DHCP client and server, system administrators can manage IP assignment without having to reconfigure other stations and fitting the router into existing network environments as easy as a breeze!

1.2 Features

- Base on Wireless-N Technology, and compliant with IEEE 802.11g, 802.11b standards
- High-speed wireless connection up to 150Mbps
- Wireless-N AP with Wi-Fi Protected Access (WPA-PSK/WPA2-PSK) and Wired Equivalent Privacy (WEP) support
- High speed Internet access with ADSL2/2+; backward compatible with ADSL
- Integrated with 4-port Ethernet switch
- SOHO firewall security with DoS prevention and SPI
- Universal Plug and Play (UPnP) Compliant
- Supports Virtual Private Network (VPN) pass-through
- Quality of Service Control
- Dynamic Domain Name System (DDNS)
- Easy Network Management

1.2.1 ADSL Compliance

- Compliant with ADSL Standards
 - Full-rate ANSI T1.413 Issue 2
 - G.dmt (ITU G.992.1)
 - G.lite (ITU G.992.2)
 - G.hs (ITU G.994.1)
 - ADSL over ISDN/U-R2
- Compliant with ADSL2 Standards
 - G.dmt.bis (ITU G.992.3)
 - ADSL2 Annex M (ITU G.992.3 Annex M) (available for BiPAC 5200WA model only)

- Compliant with ADSL2+ Standards
 - G.dmt.bis plus (ITU G.992.5)
 - ADSL2+ Annex M (ITU G.992.5 Annex M) (available for BiPAC 5200WA model only)

1.2.2 Network Protocols and Features

- NAT, static routing and RIP-1/2
- Multi-to-multi NAT
- Transparent Bridging
- Dynamic Domain Name System (DDNS)
- Virtual Server and DMZ
- SNTP, DNS relay and IGMP proxy

1.2.3 Firewall & Virtual Private Network (VPN)

- Built-in NAT Firewall
- Stateful Packet Inspection (SPI)
- Prevents DoS attacks including Land Attack, Ping of Death, etc.
- Anti probe function
- Packet filtering, MAC filtering, URL filtering
- Password protection for system management
- VPN pass-through

1.2.4 Quality of Service Control

- Supports the DiffServ approach
- Traffic prioritization based-on IP protocol, port number and address

1.2.5 Wireless LAN

- Compatible with IEEE 802.11g, 802.11b standards.
- Up to 150Mbps wireless operation rate
- 2.4 GHz–2.484 GHz frequency range
- 64/128 bits WEP supported for encryption
- Wireless Security with WPA-PSK/ WPA2-PSK support

1.2.6 ATM and PPP Protocols

- ATM Adaptation Layer Type 5 (AAL5)
- Multiple Protocol over AAL5 (RFC 2684, formerly RFC 1483)
- Bridged or routed Ethernet encapsulation
- VC and LLC based multiplexing
- PPP over Ethernet (PPPoE)
- PPP over ATM (RFC 2364)
- OAM F4/F5
- ATM QoS: UBR, CBR, VBR-rt, VBR-nrt

1.2.7 Management

- Web-based configuration
- Firmware upgrades and configuration data upload/download via web-based interface
- SNMP v1/v2, MIB supported
- Supports DHCP server/client/relay



This router may require firmware modification for certain ADSL2/2+/Annex M DSLAMs.

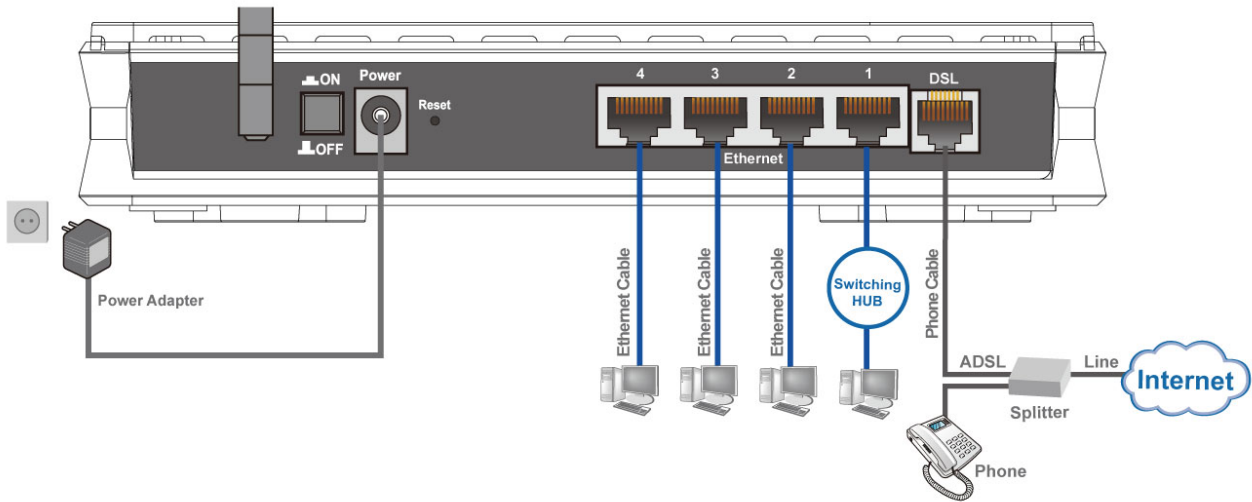
1.3 Hardware Specifications

1.3.1 Physical Interface

- DSL: ADSL port
- Ethernet: 4-port 10/100M auto-crossover (MDI/MDI-X) switch
- Factory default reset button
- Power jack
- Power switch
- WLAN: 1 antenna

1.4 Applications for the BiPAC 5200W

BiPAC 5200W



2.1 Important note for using the BiPAC 5200W



Warning

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



Attention

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

2.2 Package Contents

- **BiPAC 5200W ADSL2+ Firewall Router**
- **Quick Start Guide**
- **CD containing user manual**
- **Ethernet (CAT-5 LAN) cable**
- **RJ-11 ADSL/telephone cable**
- **Power adapter**
- **Splitter/ Micro-filter (Optional)**

ADSL2+ Router



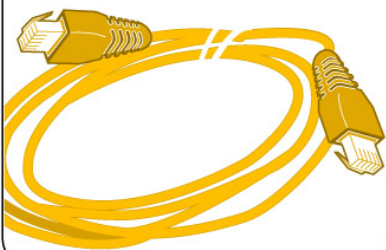
Quick Start Guide



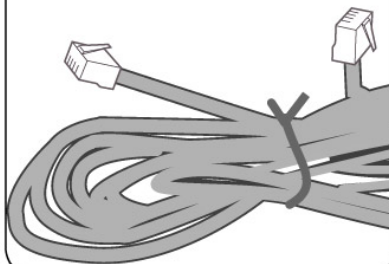
CD



**RJ-45
Ethernet cable**

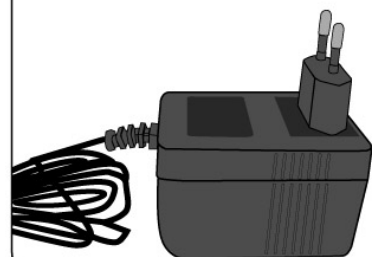


**RJ-11
Phone cable**



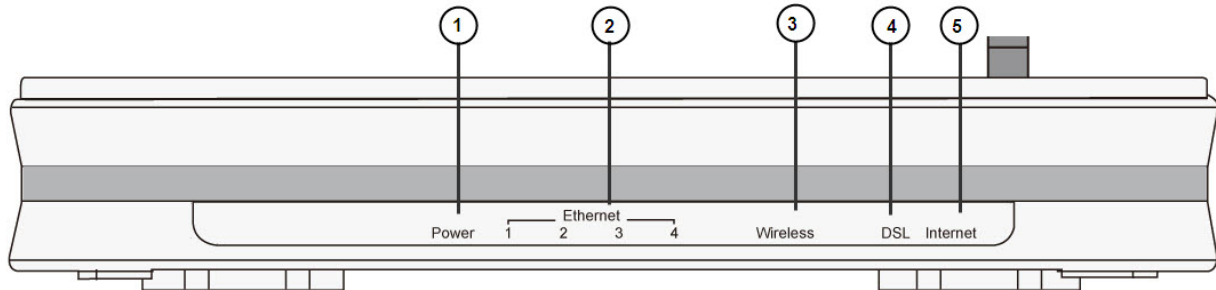
Power Adapter

(The type may differ by different country)



2.3 The Front LEDs

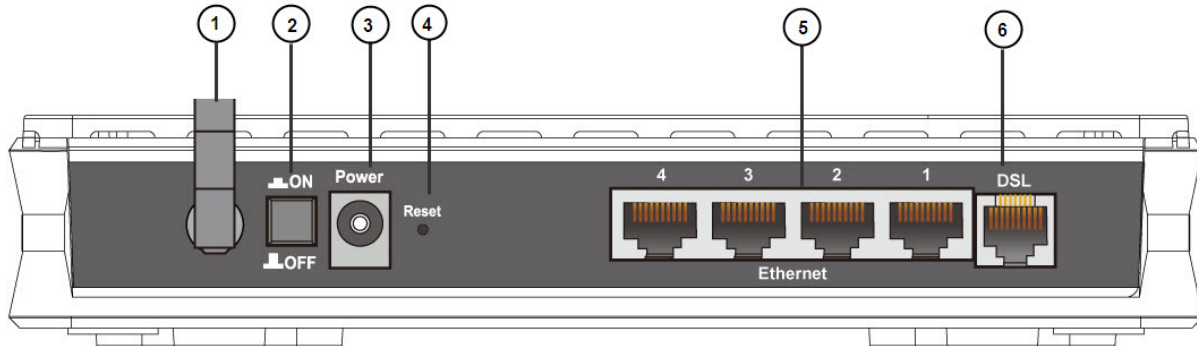
BiPAC 5200W



LED		Meaning
1	Power	<ul style="list-style-type: none"> ● Lit Red when the power is plugged in, and when the system is ready, it will lit Green. Whilst the system is rebooting or firmware upgrading, the LED light flashes.
2	Ethernet Port 1-4	<ul style="list-style-type: none"> ● Lit green when connected to an Ethernet device. ● Blinking when data is Transmitted / Received.
3.	Wireless	<ul style="list-style-type: none"> ● Lit green when the wireless connection is established. ● Flashes when sending/receiving data.
4	DSL	<ul style="list-style-type: none"> ● Lit green when successfully connected to an ADSL DSLAM ("line sync"). ● Flash green when not connected to an ADSL DSLAM.
5	Internet	<ul style="list-style-type: none"> ● Lit red when WAN port fails to get IP address. ● Lit green when WAN port gets IP address successfully.

2.4 The Rear Ports

BiPAC 5200W



Port		Meaning
1	Antenna	Connect the antenna to this port.
2	Power Switch	Power on/off switch.
3	Power	Connect the supplied power adapter to this jack.
4	Reset	After the device is powered on, press it to reset the device or restore to factory default settings. 0-3 seconds: reset the device 6 seconds above: restore to factory default settings (this is used when you can not login to the router, e.g. forgot the password).
5	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.
6	DSL (LINE)	Connect the supplied RJ-11 ("telephone") cable to this port when connecting to the ADSL/telephone network.

2.5 Cabling

One of the most common causes of problems is 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, 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.

Chapter 3

Basic Installation

The router can be configured with your web browser. A web browser is included as a standard application in the following operating systems: Windows 98/NT/2000/XP/7/Me, MAC, Linux, etc. The product provides a very easy and user-friendly interface for configuration.

3.1 Before Configuration

PCs must have an Ethernet interface installed properly and be connected to the router either directly or through an external repeater hub, and 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 of 192.168.1.1 to 192.168.1.253). The best and easiest way is to configure the PC to get an IP address automatically from the router using DHCP. If you encounter any problems accessing the router's web interface it may also be advisable to **uninstall** any kind of software firewall on your PCs, as they can cause problems accessing the 192.168.1.254 IP address of the router. Users should make their own decisions on how to best protect their network.

Please follow the steps below for your PC's network environment installation. First of all, please 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.

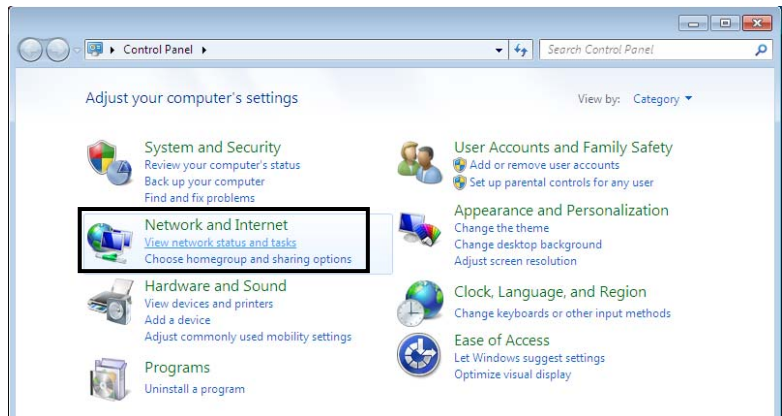


Any TCP/IP capable workstation can be used to communicate with or through the BiPAC 5200W. To configure other types of workstations, please consult the manufacturer's documentation.

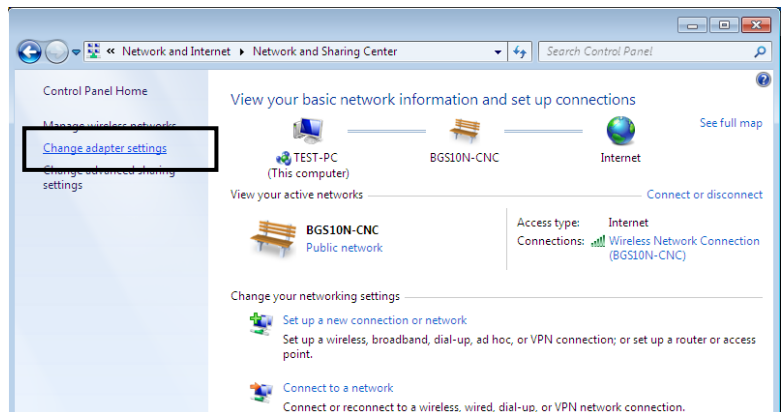
3.1.1 Configuring PC in windows 7

1. Go to **Start**. Click on **Control Panel**.

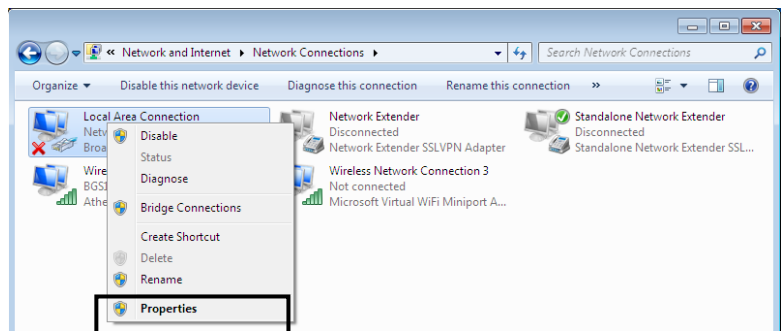
Then click on **Network and Internet**.



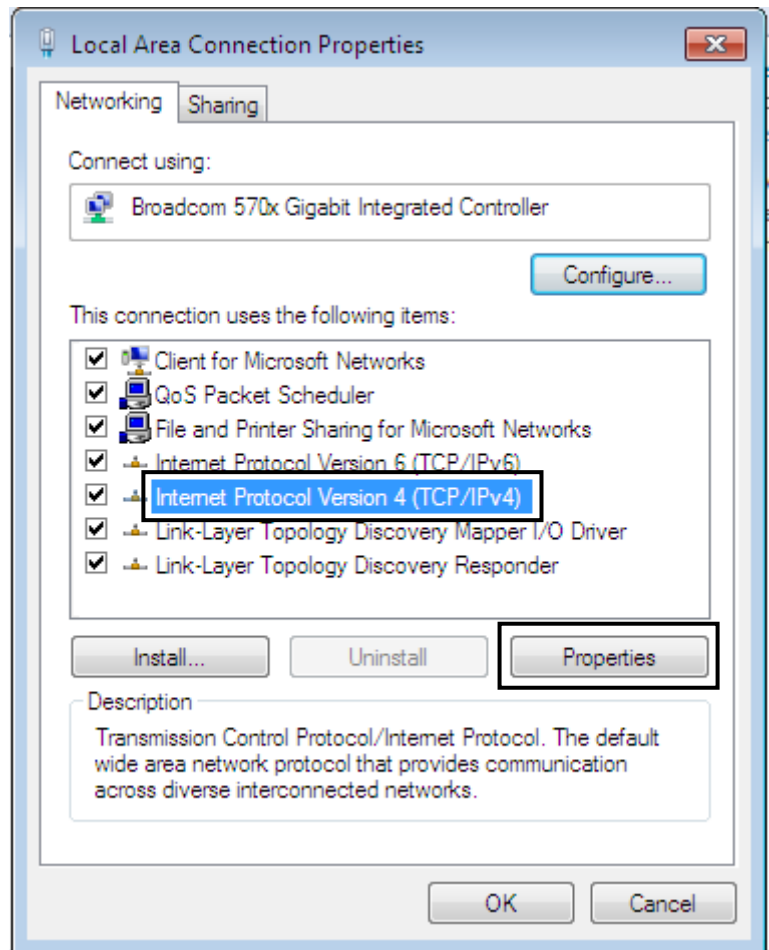
2. When the Network and Sharing Center window pops up, select and click on **Change adapter settings** on the left window panel.



3. Select the **Local Area Connection**, and right click the icon to select **Properties**.

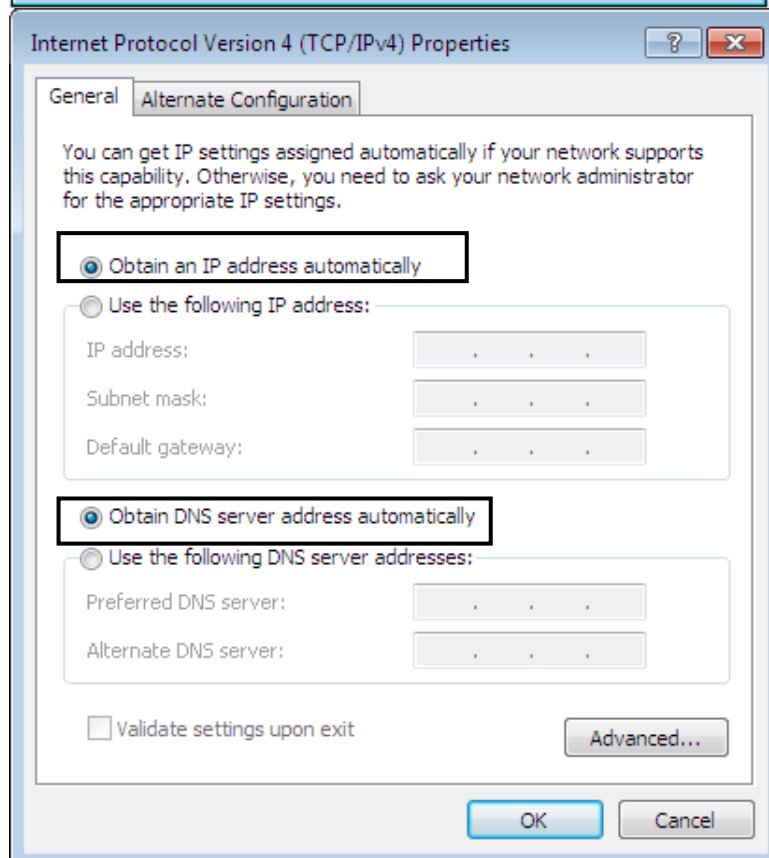


4. Select **Internet Protocol Version 4 (TCP/IPv4)** then click **Properties**.



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

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



3.1.2 Configuring PC in Windows XP

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

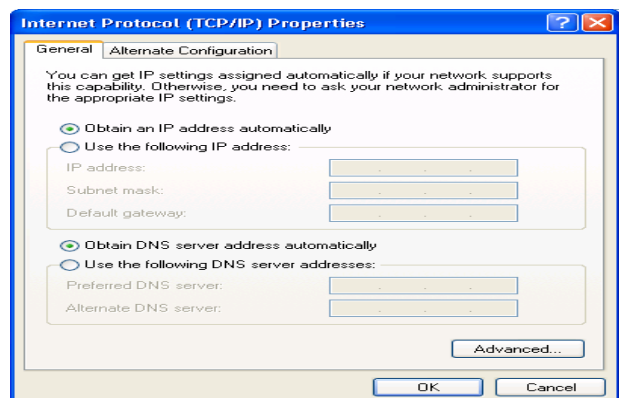
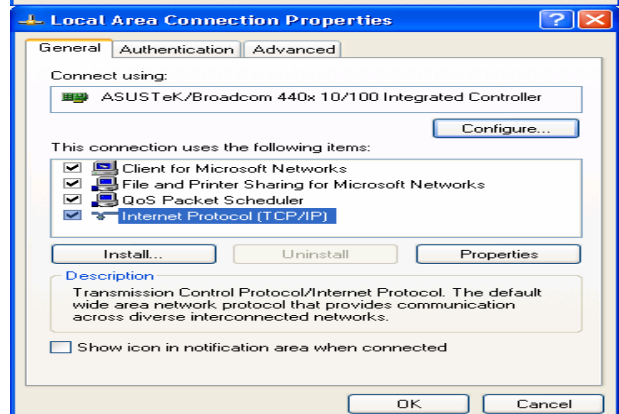
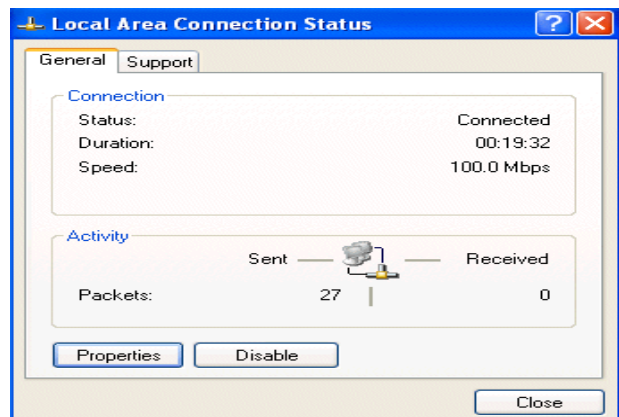
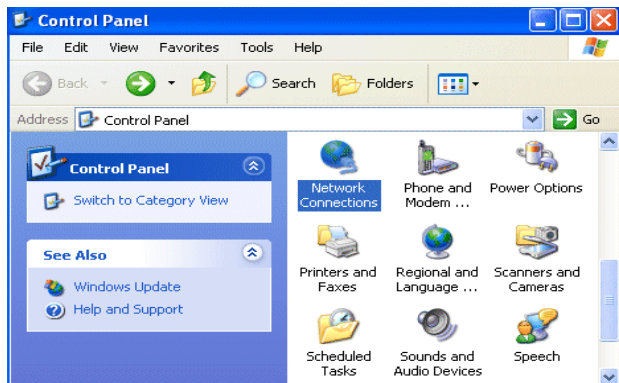
2. Double-click **Local Area Connection**.

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.

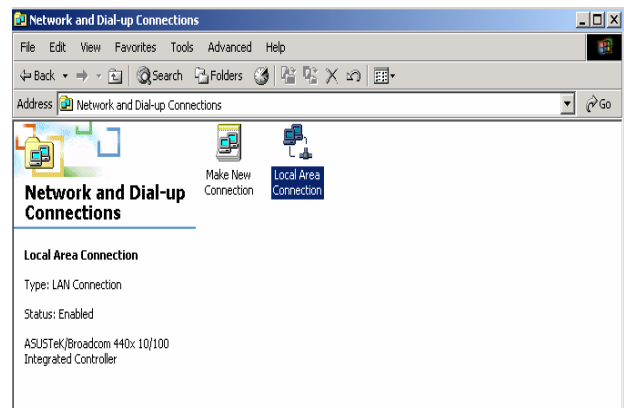
6. Click **OK** to finish the configuration.



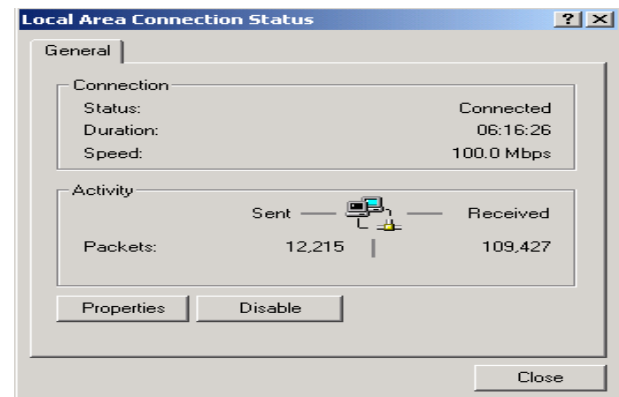
3.1.3 Configuring PC in Windows 2000

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

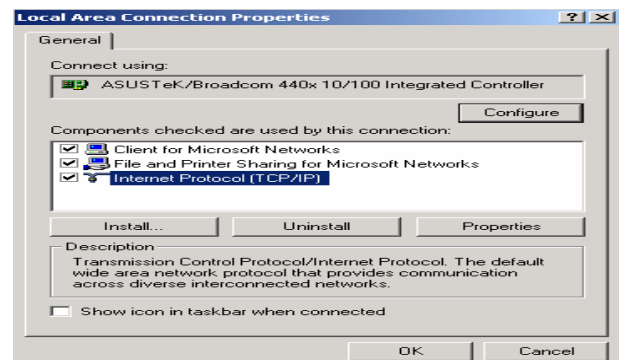
2. Double-click **Local Area Connection**.



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

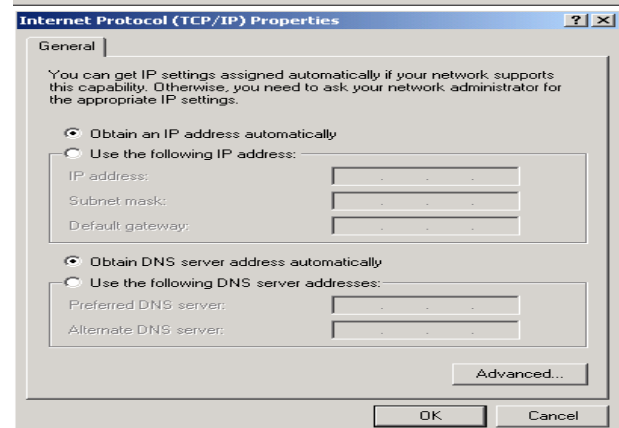


4. Select **Internet Protocol (TCP/IP)** and click **Properties**.



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

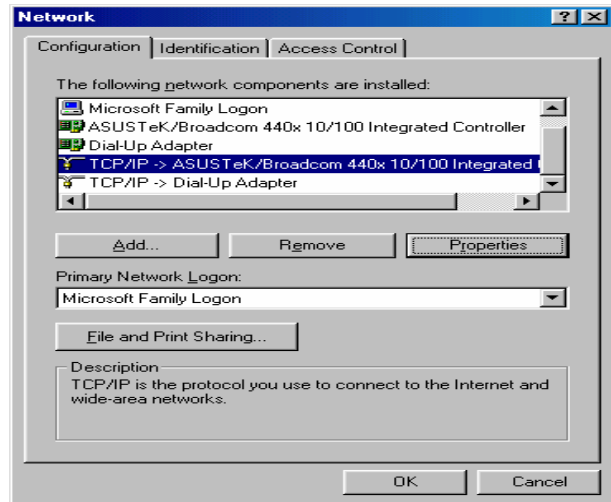
6. Click **OK** to finish the configuration.



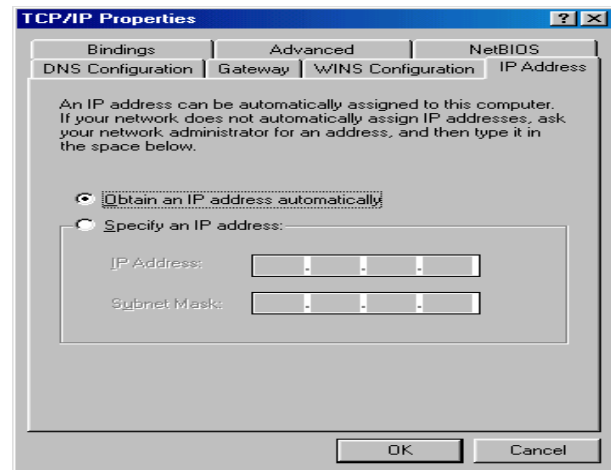
3.1.4 Configuring PC in Windows 98/Me

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.

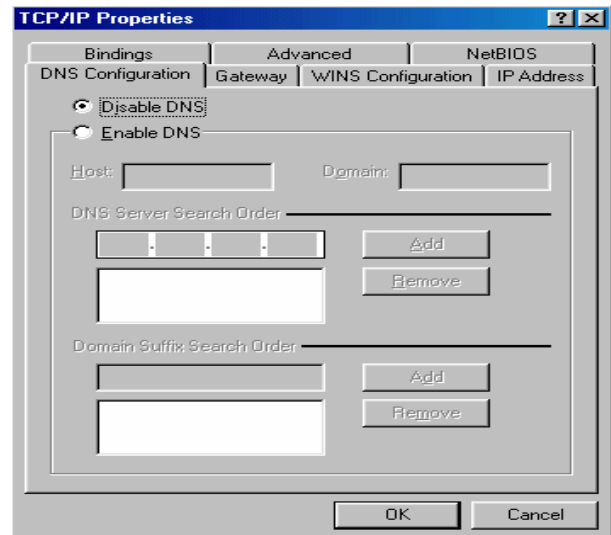


3. Select the **Obtain an IP address automatically** radio button.



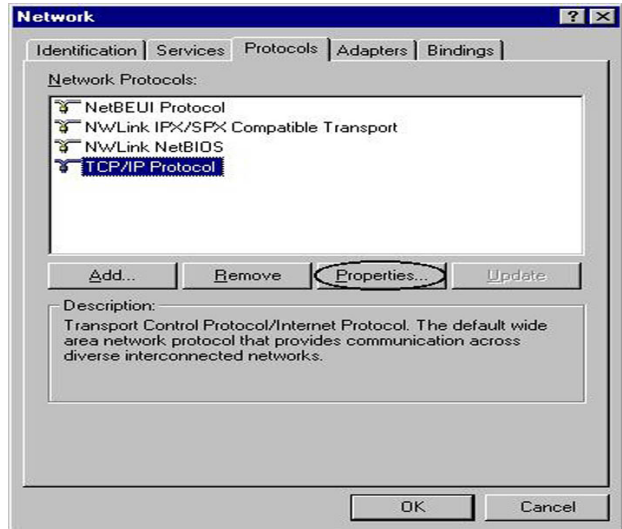
4. Then select the **DNS Configuration** tab.

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

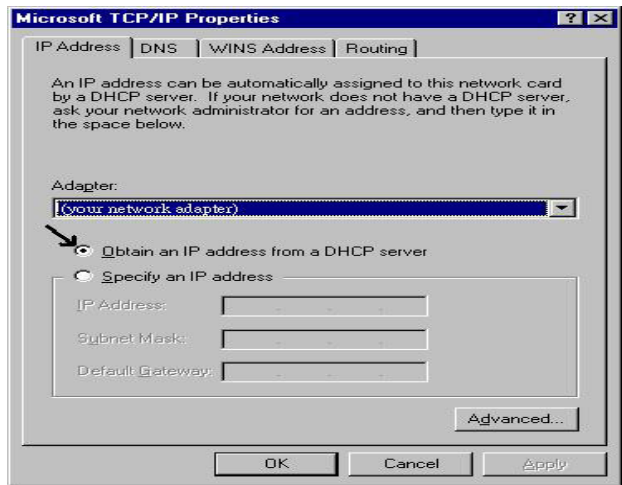


3.1.5 Configuring PC in Windows NT4.0

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**.

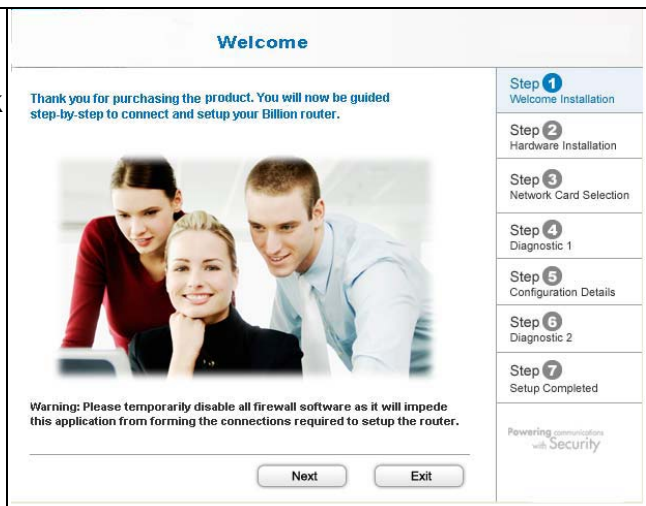


3. Select the **Obtain an IP address from a DHCP server** radio button and click **OK**.

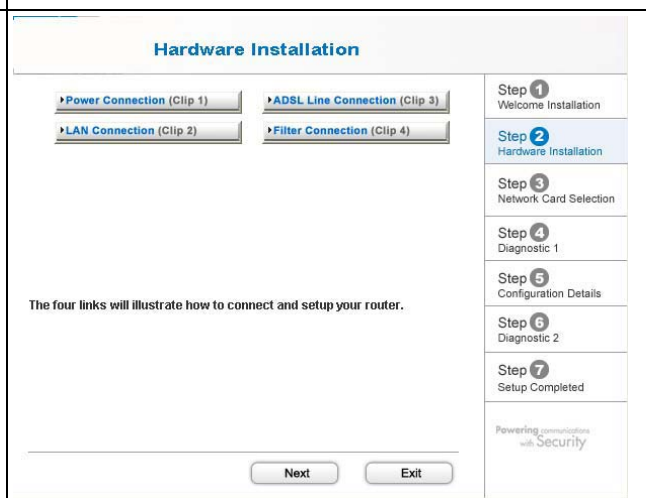


3.2 Step-by-Step Installation

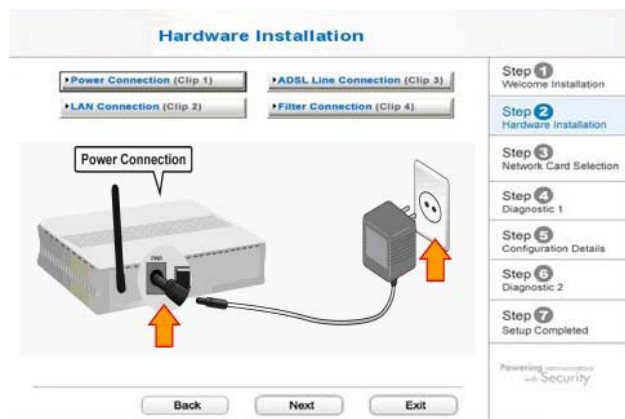
1. Insert the CD-ROM into CD-ROM drive
2. Execute Windows Utility
3. The Welcome screen will appear, click Next.



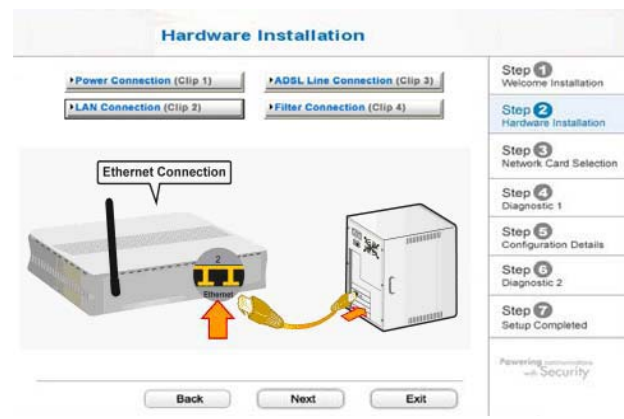
4. The Hardware Installation screen will appear. Four links are shown on the screen. Click them one by one and follow the guidelines to complete hardware installation.



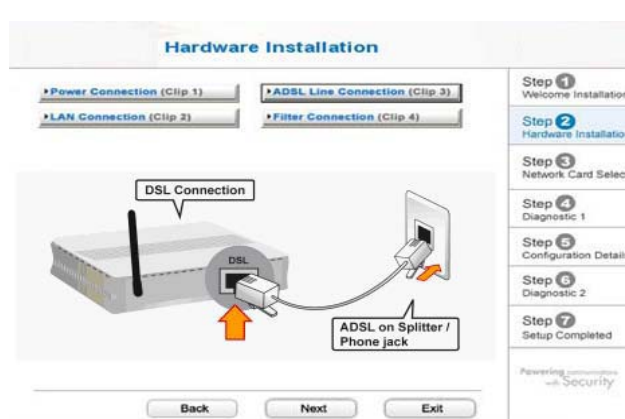
4.1 Power connection



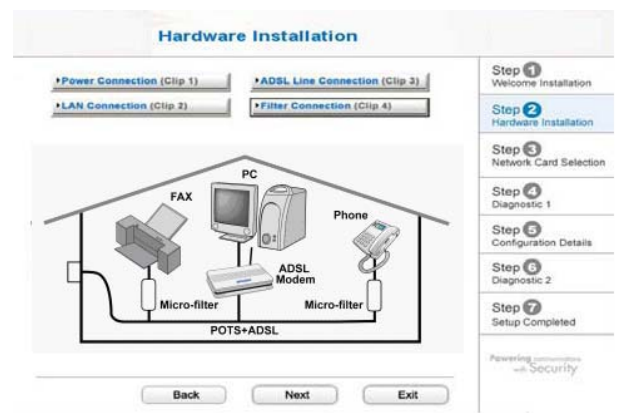
4.2 LAN connection



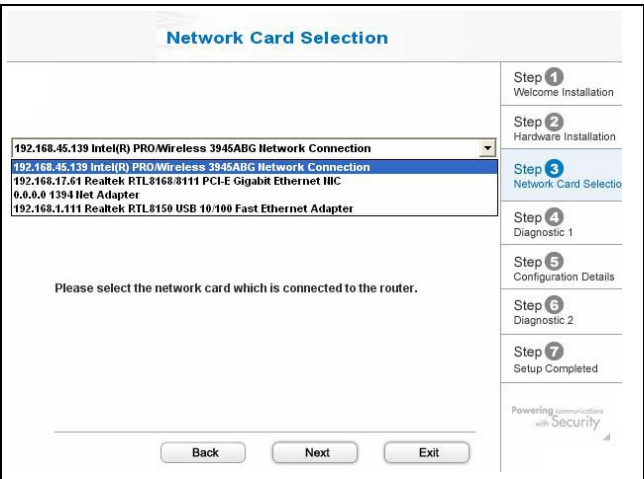
4.3 ADSL Line connection



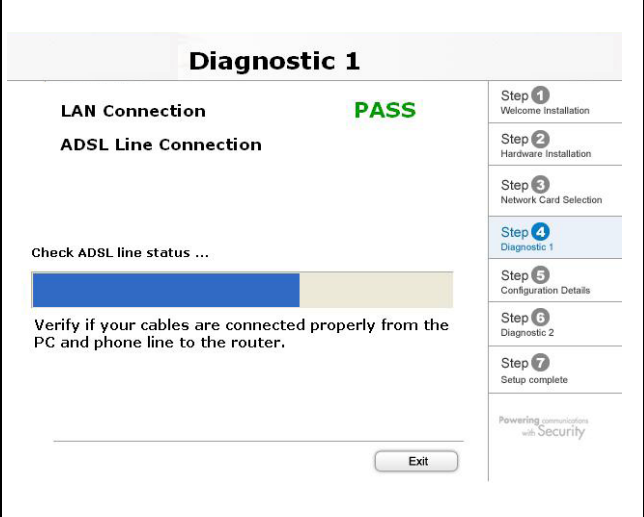
4.4 Filter connection



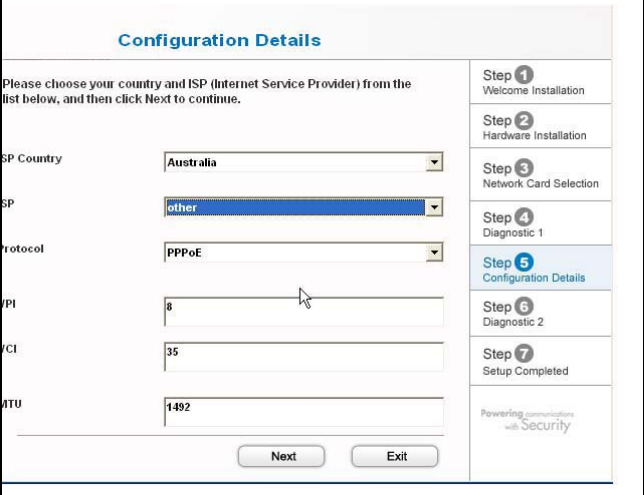
5. When finished Hardware Installation, click “Next” to proceed to next step, Network Card Selection.



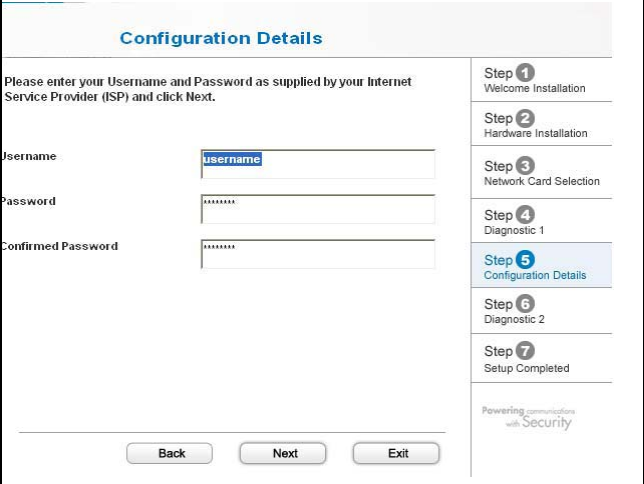
6. Diagnostic screen.
 (If connection fails, the screen will show “FAIL”, please check your router is connected correctly.)
 7. Click Next to enter Configuration Details



8. Set up more detailed settings such as VPI, VCI and MTU.

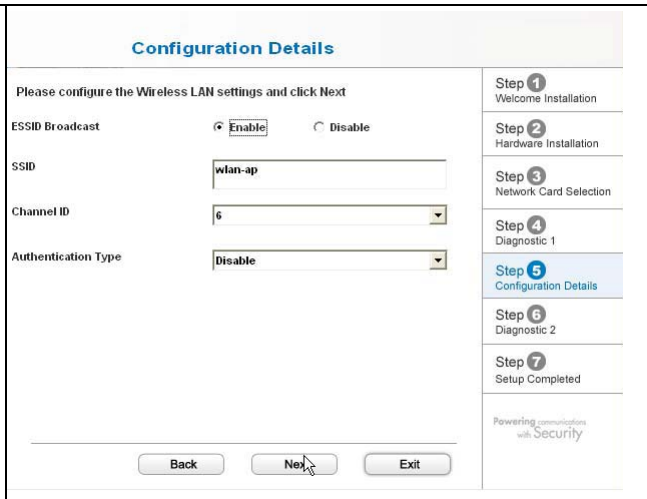


9. Please enter “Username” and “Password” as supplied by your ISP (Internet Service Provider) and click next.

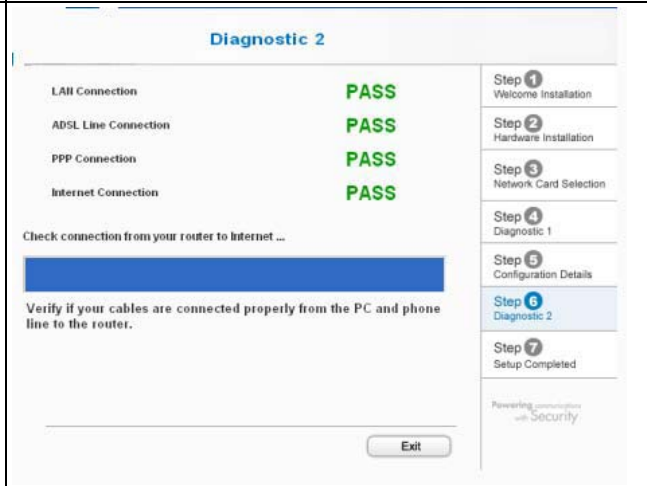


10. Please configure the Wireless LAN setting and click next.

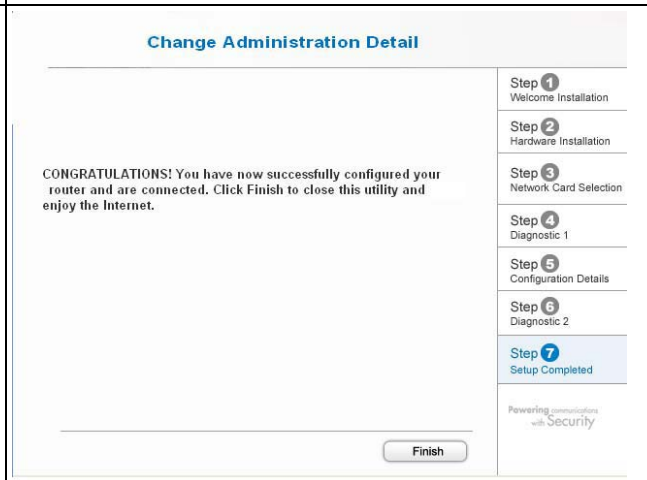
(If your router does not support wireless, please ignore this screen and it will not appear.)



11. Click Next to proceed to Diagnostic screen



12. Congratulations!! You've completed the setup procedure and are ready for surfing the Internet.



13. The IE browser will be opened automatically when you finish installing.



3.3 Factory Default Settings

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

● Web Interface:

- ✘ Username: admin
- ✘ Password: admin

● 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

3.3.1 Username and Password

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



Attention

If you ever forget the password to log in, you may press the RESET button up to 6 seconds to restore to the factory default settings.

3.4 LAN and WAN Port Addresses

The parameters of LAN and WAN ports are pre-set in 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.
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 to 192.168.1.199	

3.5 Information from your ISP

Before configuring this device, you have to check with your ISP (Internet Service Provider) which kind of service is provided such as PPPoE, PPPoA, RFC1483, or IPoA.

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).

3.6 Configuring with your Web Browser

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



Congratulation! You are now successfully logon to the BiPAC 5200W ADSL2+ Router!

Chapter 4

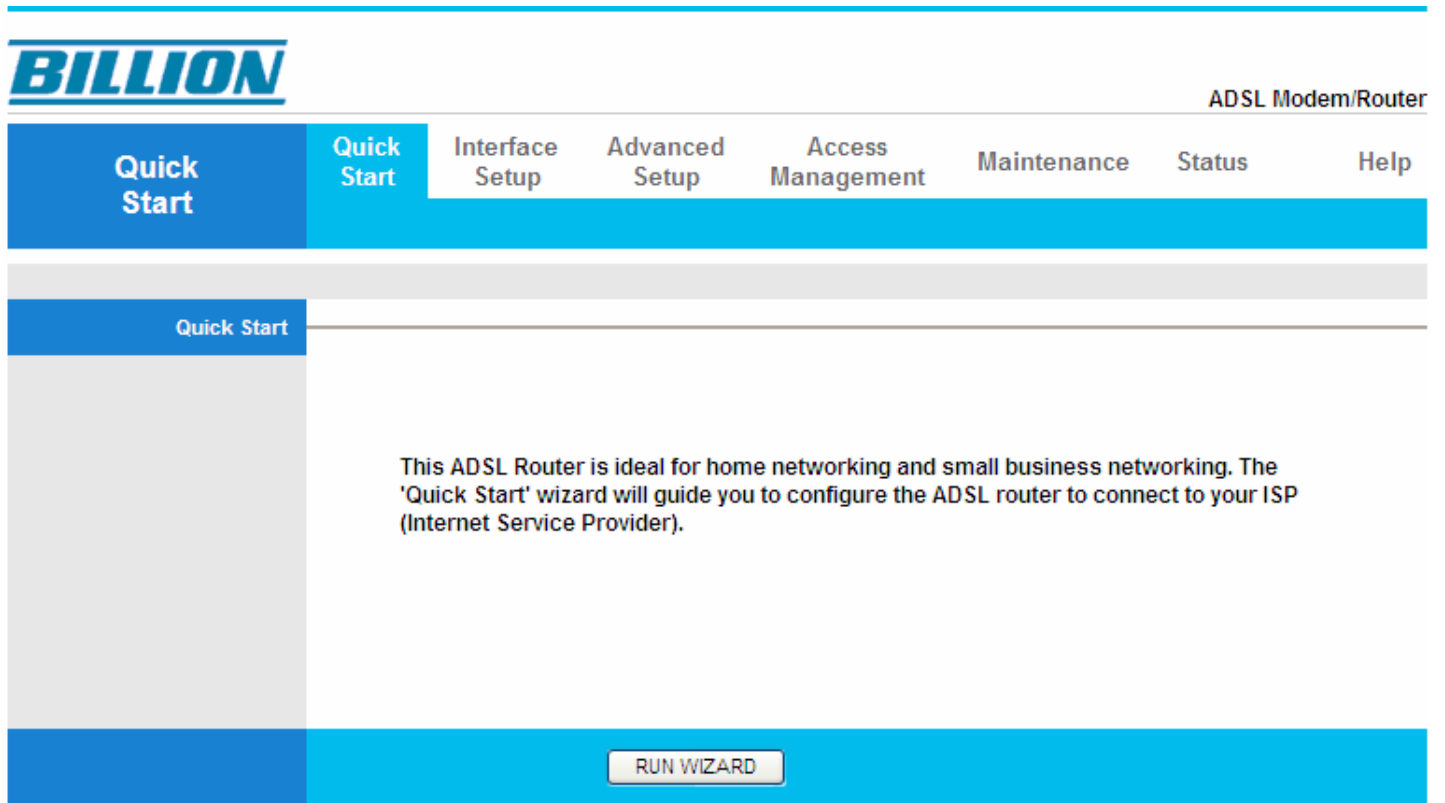
Configuration

At the configuration homepage, the top navigation pane where bookmarks links you directly to the desired setup page, including:

- **Quick Start** (wizard setup)
- **Interface Setup** (Internet, LAN, Wireless)
- **Advanced Setup** (Firewall, Routing, NAT, QoS, ADSL)
- **Access Management** (ACL, Filter, SNMP, UPnP, DDNS)
- **Maintenance** (Administration, Time Zone, Firmware, SysRestart, Diagnostics)
- **Status** (Device Info, System Log, Statistics)
- **Help**

Please see the relevant sections of this manual for detailed instructions on how to configure your Billion Router.

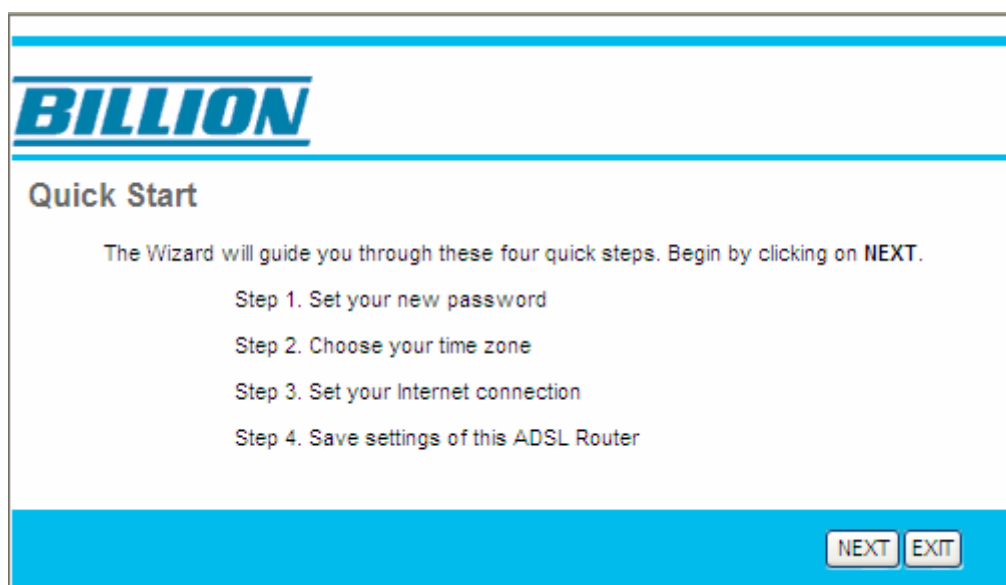
4.1 Quick Start



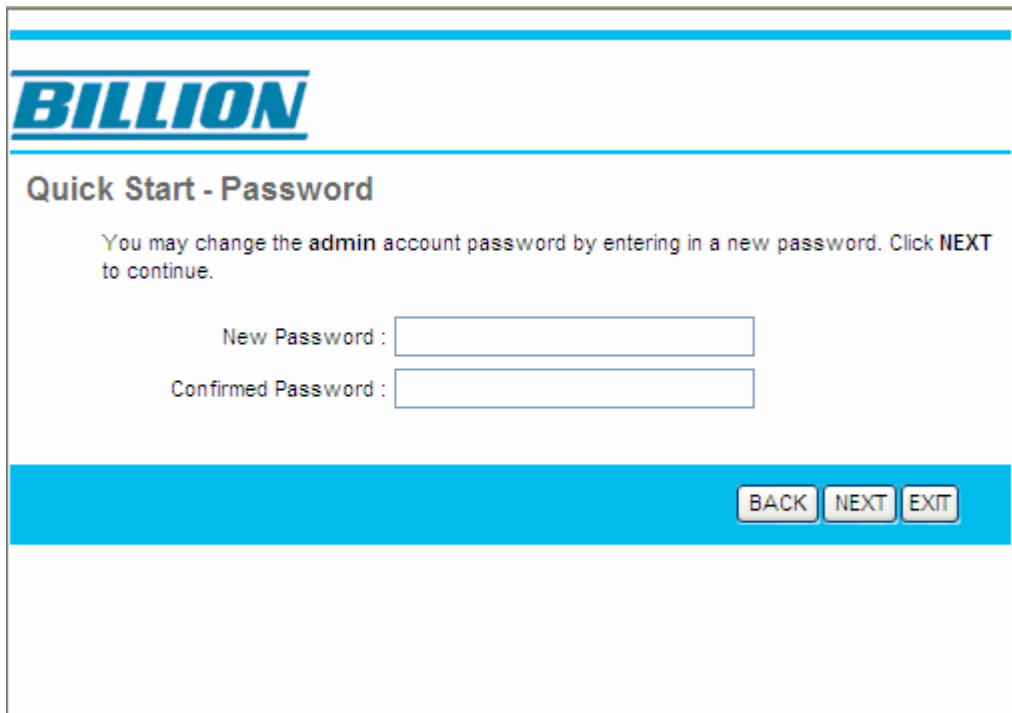
For detailed instructions on configuring WAN settings, see the **Interface Setup** section of this manual.

The Quick Start Wizard is a useful and easy utility to help setup the device to quickly connect to your ISP (Internet Service Provider) with only a few steps required. It will guide you step by step to configure the password, time zone, and WAN settings of your device. The Quick Start Wizard is a helpful guide for first time users to the device.

Follow the given steps to configure your router, input the information from your ISP.

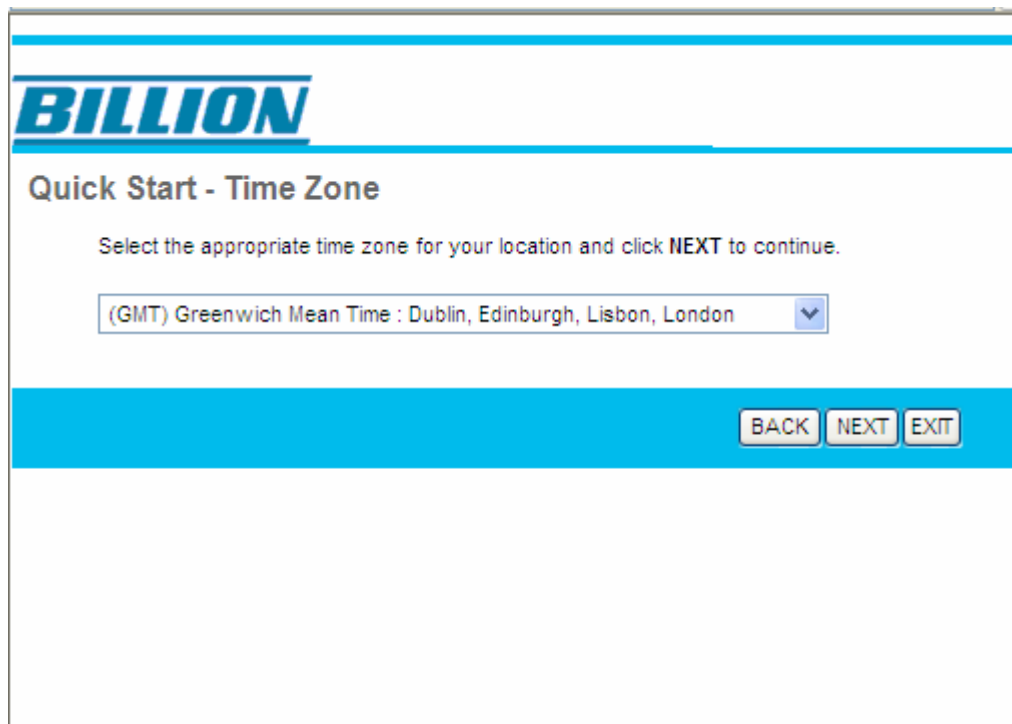


Step1. Set your new password.




The screenshot shows the 'BILLION' logo at the top left. Below it, the title 'Quick Start - Password' is displayed. A paragraph of text reads: 'You may change the admin account password by entering in a new password. Click NEXT to continue.' Below this text are two input fields: 'New Password :' and 'Confirmed Password :'. At the bottom right, there is a blue bar containing three buttons: 'BACK', 'NEXT', and 'EXIT'.

Step2: Choose your time zone.



The screenshot shows the 'BILLION' logo at the top left. Below it, the title 'Quick Start - Time Zone' is displayed. A paragraph of text reads: 'Select the appropriate time zone for your location and click NEXT to continue.' Below this text is a dropdown menu with the text '(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London' and a downward arrow. At the bottom right, there is a blue bar containing three buttons: 'BACK', 'NEXT', and 'EXIT'.

Step3: Set your Internet connection



Quick Start - ISP Connection Type


Select the Internet connection type to connect to your ISP. Click **NEXT** to continue.

Dynamic IP Address Choose this option to obtain a IP address automatically from your ISP.

Static IP Address Choose this option to set static IP information provided to you by your ISP.

PPPoE/PPPoA Choose this option if your ISP uses PPPoE/PPPoA. (For most DSL users)

Bridge Mode Choose this option if your ISP uses Bridge Mode.



Quick Start - PPPoE/PPPoA

Enter the PPPoE/PPPoA information provided to you by your ISP. Click **NEXT** to continue.

Username:

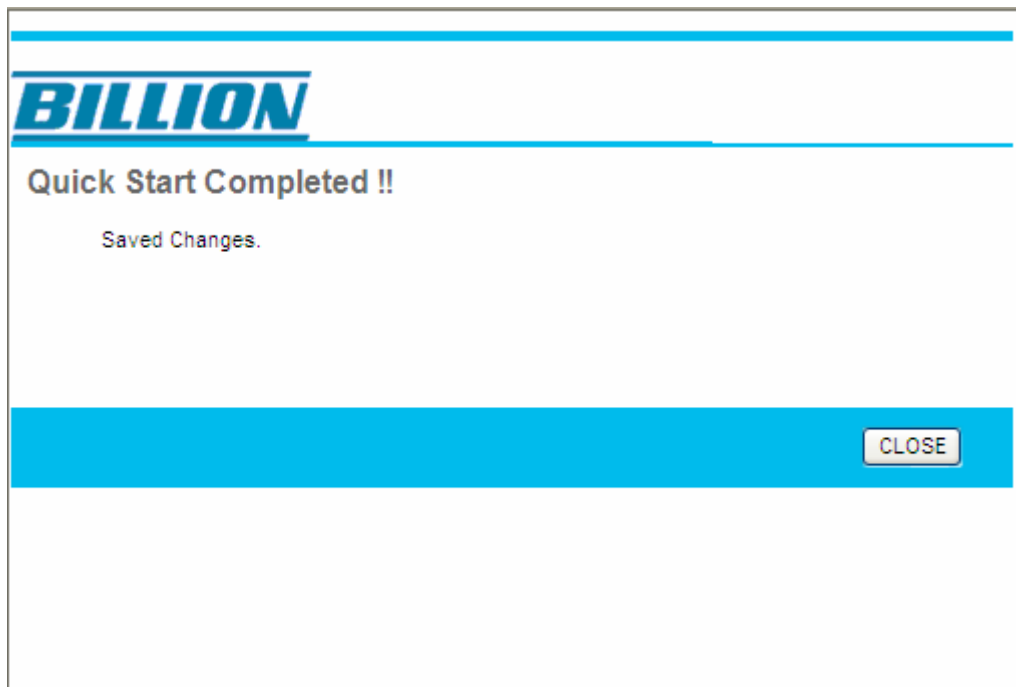
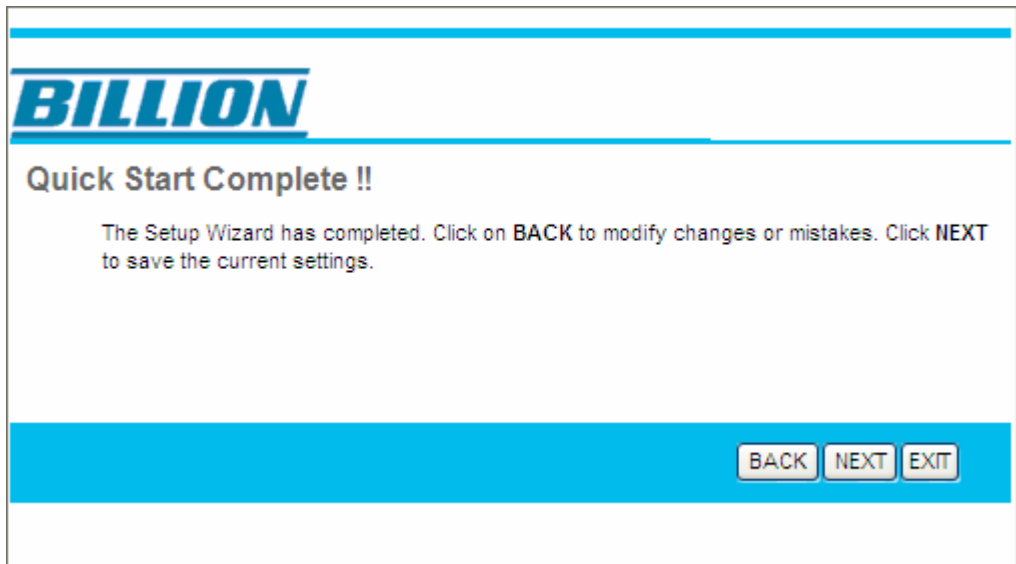
Password:

VPI: (0~255)

VCI: (1~65535)

Connection Type: ▼

Step4: Save settings of this ADSL router.




4.2 Interface Setup

Click this item to access the following sub-items that configure the ADSL2+ router: **Internet, LAN, and Wireless.**

These functions are described in the following sections.

4.2.1 Internet

ADSL Modem/Router

InterfaceQuick StartInterface SetupAdvanced SetupAccess ManagementMaintenanceStatusHelp

InternetLANWireless

ATM VC

QoS

Virtual Circuit: PVC0 PVCs Summary

Status: Activated Deactivated

VPI: (range: 0~255)

VCI: (range: 1~65535)

ATM QoS: UBR

PCR: cells/second

SCR: cells/second

MBS: cells

Encapsulation

Connection Setting

ISP: Dynamic IP Address

Static IP Address

PPPoA/PPPoE

Bridge Mode

PPPoE/PPPoA

IP Address

Servicename:

Username:

Password:

Encapsulation: PPPoE LLC

Half Bridge: Activated Deactivated

Connection: Always On (Recommended)

Connect On-Demand (Close if idle for minutes)

Connect Manually

TCP MSS Option: TCP MSS(0:default) bytes

Get IP Address: Static Dynamic

Static IP Address:

IP Subnet Mask:

Gateway:

NAT: Enable

Default Route: Yes No

TCP MTU Option: TCP MTU(0:default) bytes

Dynamic Route: RIP1 Direction: None

Multicast: Disabled

MAC Spoofing: Enabled Disabled

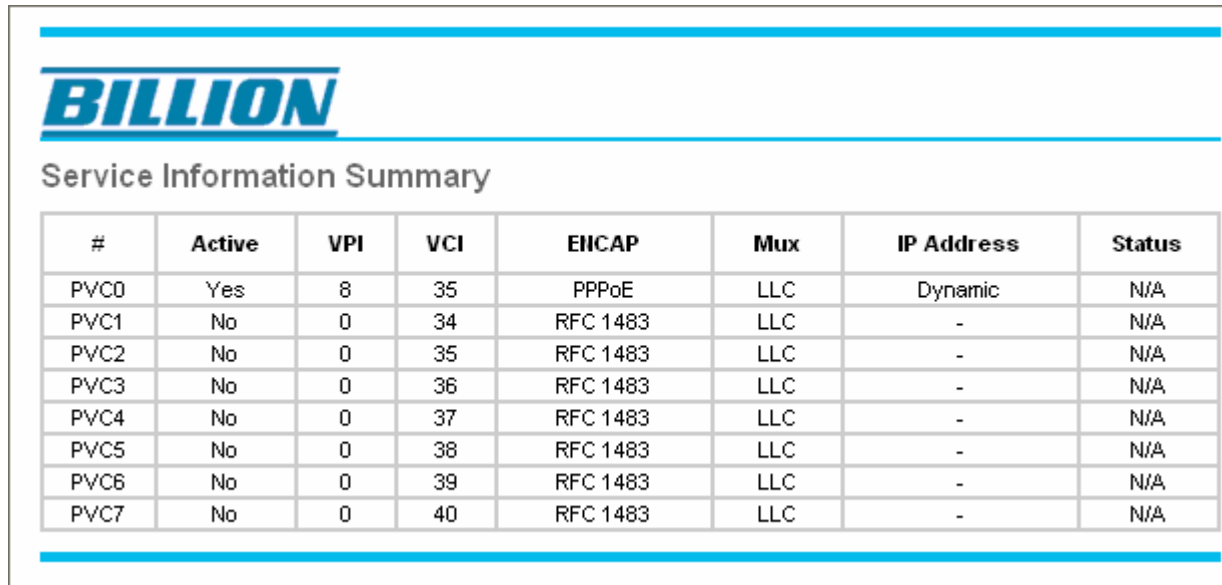
SAVE

■ ATM VC

ATM settings are used to connect to your ISP. Your ISP provides VPI, VCI settings to you. In this Device, you can totally setup 8 VCs on different encapsulations, if you apply 8 different virtual circuits from your ISP. You need to activate the VC to take effect. For PVCs management, you can use ATM QoS to setup each PVC traffic line's priority.

● **Virtual Circuit:** VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit.

● **PVC Summary:** list the PVCs message.



The screenshot shows a web interface with the 'BILLION' logo at the top. Below the logo is a section titled 'Service Information Summary' containing a table with 8 columns: '#', 'Active', 'VPI', 'VCI', 'ENCAP', 'Mux', 'IP Address', and 'Status'. The table lists PVC0 through PVC7 with their respective configurations.

#	Active	VPI	VCI	ENCAP	Mux	IP Address	Status
PVC0	Yes	8	35	PPPoE	LLC	Dynamic	N/A
PVC1	No	0	34	RFC 1483	LLC	-	N/A
PVC2	No	0	35	RFC 1483	LLC	-	N/A
PVC3	No	0	36	RFC 1483	LLC	-	N/A
PVC4	No	0	37	RFC 1483	LLC	-	N/A
PVC5	No	0	38	RFC 1483	LLC	-	N/A
PVC6	No	0	39	RFC 1483	LLC	-	N/A
PVC7	No	0	40	RFC 1483	LLC	-	N/A

● **Status:** indicate the status of the PVCs above. You can select the Activated or deactivated to activate or deactivate the PVC.

● **VPI:** The valid range for the VPI is 0 to 255. Enter the VPI assigned to you. This field may already be configured.

● **VCI:** The valid range for the VCI is 1 to 65535. Enter the VCI assigned to you. This field may already be configured.

● **ATM QoS:** Select the Quality of Service types for this Virtual Circuit. The ATM QoS types include CBR (Constant Bit Rate), VBR (Variable Bit Rate) and UBR (Unspecified Bit Rate). These QoS types are all controlled by the parameters specified below, including PCR, SCR and MBS. Select CBR to specify fixed (always-on) bandwidth for voice or data traffic. Select UBR for applications that are non-time sensitive, such as e-mail. Select VBR for burst traffic and bandwidth sharing with other applications.

● **PCR:** Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells.

● **SCR:** The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted.

● **MBS:** Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535

■ Encapsulation:

● **ISP:** Select the encapsulation type your ISP uses from the **Encapsulation** list.

Choices vary depending on what you select in the **Mode** field.

① **Dynamic IP:** Select this option if your ISP provides you an IP address automatically. This option is typically used for Cable services. Please enter the Dynamic IP information accordingly.

① **Static IP:** Select this option to set static IP information. You will need to enter in the Connection type, IP address, subnet mask, and gateway address, provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which is four IP octets separated by a dot (x.x.x.x). The Router will not accept the IP address if it is not in this format.

① **PPPoA/PPPoE:** Select this option if your ISP requires you to use a PPPoE connection. This option is typically used for DSL services. Select Dynamic PPPoE to obtain an IP address automatically for your PPPoE connection. Select Static PPPoE to use a static IP address for your PPPoE connection. Please enter the information accordingly.

① **Bridge Mode:** Mainly use the MAC address to determine whether to forward data, in this way, the router works like a switch. Select this mode if your ISP uses this mode.

■ PPPoE/PPPoA

Select this option if your ISP requires you to use a PPPoE connection. This option is typically used for DSL services. Select Dynamic PPPoE to obtain an IP address automatically for your PPPoE connection. Select Static PPPoE to use a static IP address for your PPPoE connection. Please enter the information accordingly.

● **Servicename:** Enter a name for the PPPoE/PPoA connection.

● **Username:** Enter the user name exactly as your ISP assigned.

● **Password:** Enter the password associated with the user name above.

● **Encapsulation:** select in the Mode field, select PPPoE LLC, PPPoE VC-Mux, PPPoA LLC, PPPoA VC-Mux.

● **Half Bridge:** The Half Bridge mode can only be used when a single IP address has been assigned by the ISP. It is used when the use of NAT is not desired and there is a single computer attached to the router.

● **Connection:** The schedule rule(s) have priority over your Connection settings.

① **Always on:** Select Always on Connection when you want your connection up all the time.

① **Connect on Demand:** Select Connect on Demand when you don't want the connection up all the time and specify an idle time-out in the Max Idle Timeout field.

① **Connect manually:** Select this mode if you want to connect manually.

● **TCP MSS Option:** Enter the TCP Maximum Segment Size (MSS)

● **Get IP Address:** Choose Static or Dynamic

● **Static IP Address:** Enter the IP address of ADSL Router in dotted decimal notation, for example, xx.xx.xx.xx.

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

● **Gateway:** You must specify a gateway IP address (supplied by your ISP) when you use **1483 Bridged IP** in the **Encapsulation** field in the previous screen.

● **NAT:** Select this option to Disabled/Enable the NAT (Network Address Translation) function for this VC. The NAT function can be activated or deactivated per PVC basis

● **Default Route:** If enable this function, the current PVC will be the default gateway to internet from this device

● **TCP MTU Option:** Enter the TCP maximum transmission unit (MTU)

● **Dynamic Route:**

- ① **RIP Version:** (Routing Information protocol) Select this option to specify the RIP version, including RIP-1, RIP-2M and RIP-2B. RIP-2M and RIP-2B are both sent in RIP-2 format; the difference is that RIP-2M using Multicast and RIP-2B using Broadcast format
- ① **RIP Direction:** Select this option to specify the RIP direction. None is for disabling the RIP function. Both means the ADSL Router will periodically send routing information and accept routing information then incorporate into routing table. IN only means the ADSL router will only accept but will not send RIP packet. OUT only means the ADSL router will only send but will not accept RIP packet.

● **Multicast:** IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. The BiPAC 5200W supports both IGMP version 1 (IGMP-v1), IGMP-v2, and IGMP-v3. Select Disabled to disable it

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

4.2.2 LAN

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.

BILLION ADSL Modem/Router

Interface | Quick Start | **Interface Setup** | Advanced Setup | Access Management | Maintenance | Status | Help

Internet | **LAN** | Wireless

Router Local IP

IP Address : 192.168.1.254
IP Subnet Mask : 255.255.255.0
Dynamic Route : RIP1 | Direction : None
Multicast : Disabled
IGMP Snoop : Disabled Enabled

DHCP

DHCP : Disabled Enabled Relay

DHCP Server

Starting IP Address : 192.168.1.100 | Current Pool Summary
IP Pool Count : 100
Lease Time : 86400 seconds (0 sets to default value of 259200)
Physical Ports : 1 2 3 4

DNS

DNS Relay : Use Auto Discovered DNS Server Only
Primary DNS Server : N/A
Secondary DNS Server : N/A

SAVE CANCEL

Router Local IP

IP Address: Enter the IP address of ADSL Router in dotted decimal notation, for example, 192.168.1.254 (factory default).

IP Subnet Mask: The default is 255.255.255.0. User can change it to other such as 255.255.255.128.

Dynamic Route: Select the RIP version from RIP-1, RIP-2B and RIP-2M.

RIP Direction: Select the RIP direction from None, Both, In Only and Out Only.

Multicast: IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. The BiPAC 5200W supports both IGMP version 1 (IGMP-v1), IGMP-v2 and IGMP-v3. Select Disabled to disable it.

IGMP Snoop: Internet Group Management Protocol Snoop, running in layer 2 devices in order to manage and control multicast group. Choose Disabled or Enabled IGMP Snoop function.

■ DHCP

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server.

● **DHCP:** If set to **Enabled**, your BiPAC 5200W can assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT and other systems that support the DHCP client.

If set to **Disabled**, the DHCP server will be disabled.

If set to **Relay**, the BiPAC 5200W acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the Remote DHCP Server field in this case.

When DHCP is used, the following items need to be set.

● **Starting IP Address:** This field specifies the first of the contiguous addresses in the IP address pool.

● **IP Pool Count:** This field specifies the size or count of the IP address pool.

● **Lease Time:** The current lease time of client.

● **Physical port:** There are four physical ports.

● **DNS Relay:** Use the Local computer as a DNS Server, but without any resolution, it pass the work to another DNS Server which the DNS Relay points to. The specified Server do the resolution work and pass the result to the Local server and then the local server pass the received result to the client. Select from the drop-down menu to specify the another server which does the resolution work.

● **Primary DNS Server:** 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.

● **Secondary DNS Server:** 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.

4.2.3 Wireless

This section introduces the wireless LAN and some basic configurations. Wireless LANs can be as simple as two computers with wireless LAN cards communicating in a peer-to-peer network or as complex as a number of computers with wireless LAN cards communicating through access points which bridge network traffic to the wired LAN.

BILLION ADSL Modem/Router

Interface	Quick Start	Interface Setup	Advanced Setup	Access Management	Maintenance	Status	Help
	Internet	LAN	Wireless				

Access Point Settings

Access Point : Activated Deactivated

Channel : 01 Current Channel: 1

Beacon Interval(ms) : 100 (range: 20~1000)

RTS/CTS Threshold : 2347 (range: 1500~2347)

Fragmentation Threshold (bytes) : 2346 (range: 256~2346, even numbers only)

DTIM(ms) : 1 (range: 1~255)

Wireless Mode : 802.11b+g+n

11n Settings

Channel Bandwidth : 20/40 MHz

Extension Channel : above the control channel

Guard Interval : AUTO

MCS : AUTO

Multiple SSIDs Settings

SSID Index : 1

Broadcast SSID : Yes No

SSID : wlan-ap

Authentication Type : Disabled

WDS Settings

WDS Mode : On Off

Mac Address #1 : 00:00:00:00:00:00

Mac Address #2 : 00:00:00:00:00:00

Mac Address #3 : 00:00:00:00:00:00

Mac Address #4 : 00:00:00:00:00:00

Wireless MAC Address Filter

Active : Activated Deactivated

Action : Allow Association the follow Wireless LAN station(s) association.

Mac Address #1 : 00:00:00:00:00:00

Mac Address #2 : 00:00:00:00:00:00

Mac Address #3 : 00:00:00:00:00:00

Mac Address #4 : 00:00:00:00:00:00

Mac Address #5 : 00:00:00:00:00:00

Mac Address #6 : 00:00:00:00:00:00

Mac Address #7 : 00:00:00:00:00:00

Mac Address #8 : 00:00:00:00:00:00

■ Access Point Settings

● **Access Point:** Default setting is set to **Activated**. If you do not have any wireless device in your network, select **Deactivated**.

● **Channel ID:** The range of radio frequencies used by IEEE 802.11b/g/n wireless devices is called a channel. Select a channel from the drop-down list box.

● **Current Channel:** indicate the current channel used.

● **Beacon interval:** The Beacon Interval value indicates the frequency interval of the beacon. Enter a value between 20 and 1000. A beacon is a packet broadcast by the Router to synchronize the wireless network.

● **RTS/CTS Threshold:** The RTS (Request To Send) threshold (number of bytes) for enabling RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be larger than the maximum MSDU (MAC service data unit) size turns off the RTS/CTS handshake. Setting this attribute to zero turns on the RTS/CTS handshake. Enter a value between 1500 and 2347.

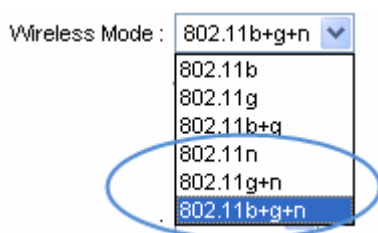
● **Fragmentation Threshold:** The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter a value between 256 and 2346.

● **DTIM:** This value, between 1 and 255, indicates the interval of the Delivery Traffic Indication Message (DTIM).

● **Wireless Mode:** The default setting is **802.11b+g+n** (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** and if you only have 802.11n then select **802.11n**.

■ 11n Settings

Note: this setting can only be activated when you select the item which includes a 'n' from the wireless mode above.



● **Channel Bandwidth:** Select either **20 MHz** or **20/40 MHz** for the channel bandwidth. The higher

the bandwidth the better the performance will be.

● **Guard Interval:** Select either **Auto** or **800nsec** for the guard interval. The guard interval is here to ensure that data transmission do not interfere with each other, it also prevents propagation delays, echoing and reflections.

● **MCS:** There are options **0~15** and **AUTO** to select for the **Modulation and Coding Scheme**. We recommend users selecting **AUTO**.

■ Multiple SSID Settings

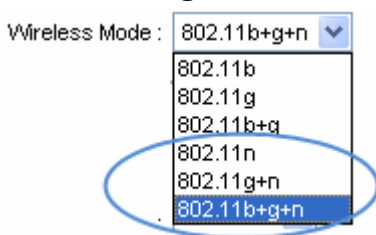
● **SSID Index:** Default SSID index is “1”.

● **Broadcast SSID:** Select **Yes** to make the SSID visible so a station can obtain the SSID through passive scanning. Select **No** to hide the SSID in so a station cannot obtain the SSID through passive scanning.

● **SSID:** The SSID is the unique name of a wireless access point (AP) to be distinguished from another. For security propose, change the default **wlan-ap** 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 30 characters. Make sure your wireless clients have exactly the SSID as the device, in order to get connected to your network.

● **WMM:** WMM (Wi-Fi Multimedia) is a simple QoS which prioritizes traffic based on 4 AC (Access Categories) voice, video, best effort and background but it does not provide a guarantee throughput. Choose **Enable** to activate the function or else leave it as **Disable**.

Note: When you select one of **802.11n/802.11g+n/802.11b+g+n** in the **Wireless mode** of **Access Point Settings** section, the WMM function will not exist, that is to say this function is invalid.

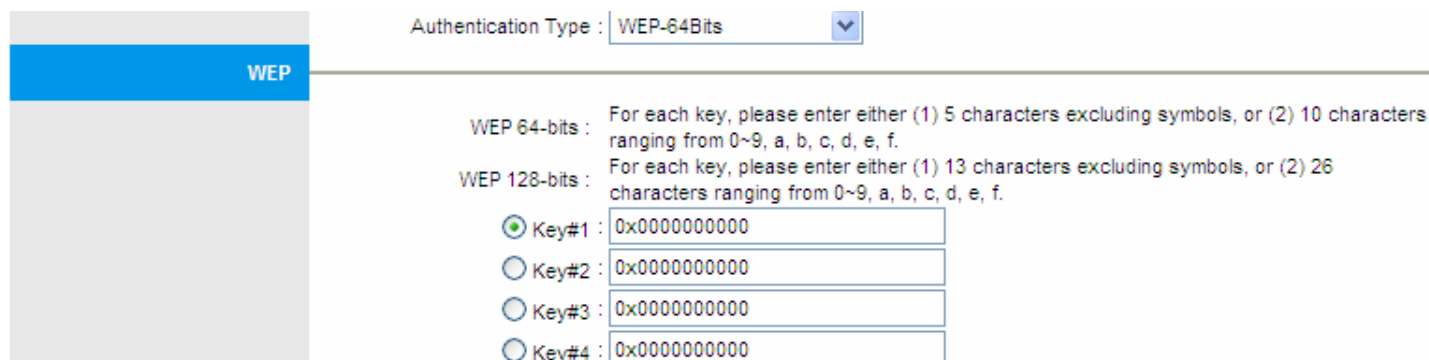


● **Authentication Type:** To prevent unauthorized wireless stations from accessing data transmitted over the network, the router offers highly secure data encryption, known as WEP&WPA. If you require high security for transmissions, there are four alternatives to select from: **64-bit WEP**, **128-bit WEP**, **WPA-PSK** and **WPA2-PSK**, **WPA-PSK/WPA-PSK**, **Radius**, **WPA Enterprise**, **WPA2 Enterprise**, **WPA /WPA2 Enterprise**.

You can disable or enable with WPA or WEP for protecting wireless network. The default type of wireless is **WPA-PSK** and to allow all wireless computers to communicate with the access points

without any data encryption

WEP



The screenshot shows a configuration interface for WEP. On the left, there is a vertical sidebar with a blue header labeled 'WEP'. The main area has a dropdown menu for 'Authentication Type' set to 'WEP-64Bits'. Below this, there are instructions for 'WEP 64-bits' and 'WEP 128-bits'. Under 'WEP 128-bits', there are four radio buttons labeled 'Key#1' through 'Key#4', each followed by a text input field containing '0x0000000000'. The 'Key#1' radio button is selected.

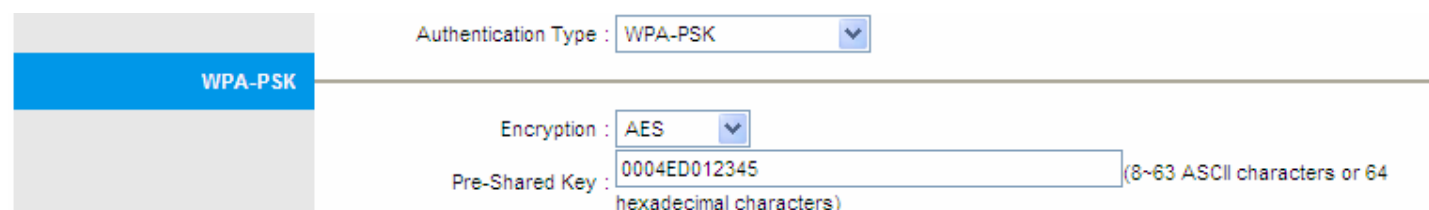
Key 1 to Key 4: Enter the key to encrypt wireless data. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as the router. There are four keys for your selection. The input format can be in HEX style, 10 and 26 HEX codes are required for 64-bit WEP and 128-bit WEP respectively.

If you chose **WEP 64-bits**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F").

If you chose **WEP 128-bits**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").

You must configure all four keys, but only one key can be activated at any one time. The default key is key 1.

WPA-PSK & WPA2-PSK & WPA-PSK / WPA2-PSK Mixed mode



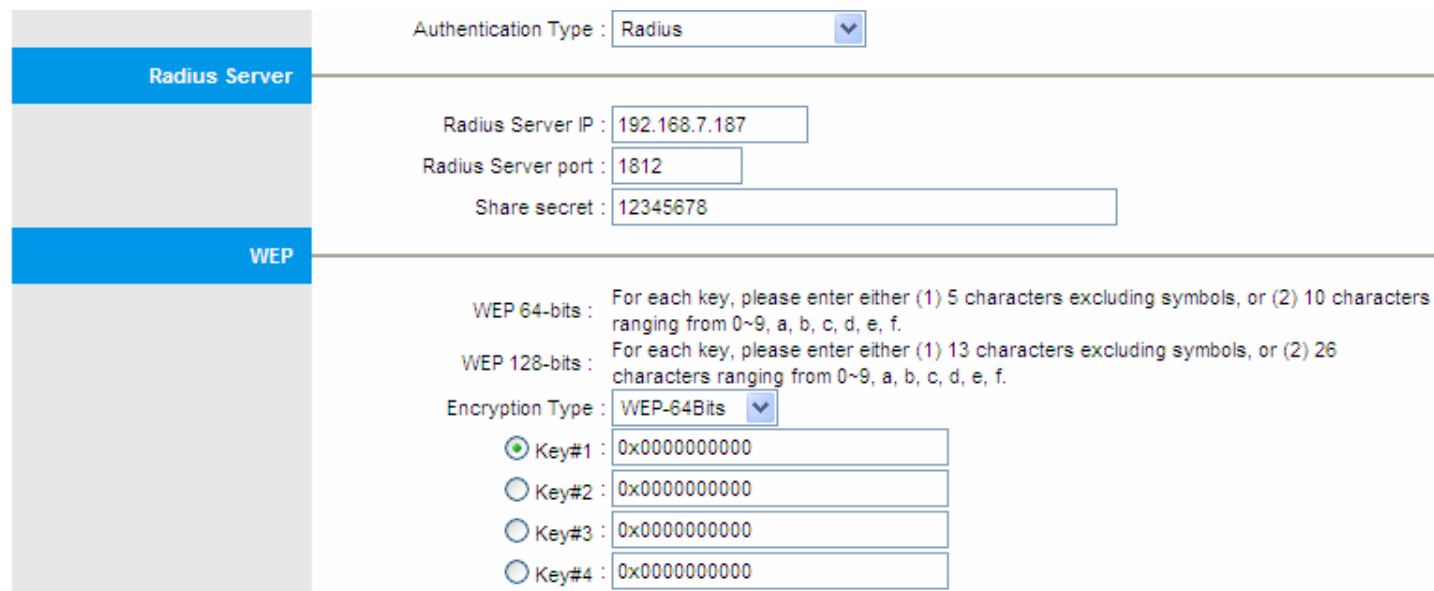
The screenshot shows a configuration interface for WPA-PSK. On the left, there is a vertical sidebar with a blue header labeled 'WPA-PSK'. The main area has a dropdown menu for 'Authentication Type' set to 'WPA-PSK'. Below this, there is a dropdown menu for 'Encryption' set to 'AES'. Underneath, there is a text input field for 'Pre-Shared Key' containing '0004ED012345'. To the right of the input field, there is a note: '(8-63 ASCII characters or 64 hexadecimal characters)'.

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

Pre-Shared key: The key for network authentication. The input format should be 8-63 ASCII characters or 64 hexadecimal characters.

Radius

Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for computers to connect and use a network service. RADIUS is a client/server protocol that runs in the application layer, using UDP as transport.



The screenshot shows a configuration interface for RADIUS. On the left, there are two vertical tabs: 'Radius Server' (selected) and 'WEP'. The main area is divided into two sections. The top section, under 'Radius Server', contains the following fields: 'Authentication Type' (dropdown menu set to 'Radius'), 'Radius Server IP' (text box with '192.168.7.187'), 'Radius Server port' (text box with '1812'), and 'Share secret' (text box with '12345678'). The bottom section, under 'WEP', contains: 'WEP 64-bits' (text with instructions), 'WEP 128-bits' (text with instructions), 'Encryption Type' (dropdown menu set to 'WEP-64Bits'), and four radio buttons labeled 'Key#1' through 'Key#4', each with a corresponding text box containing '0x0000000000'.

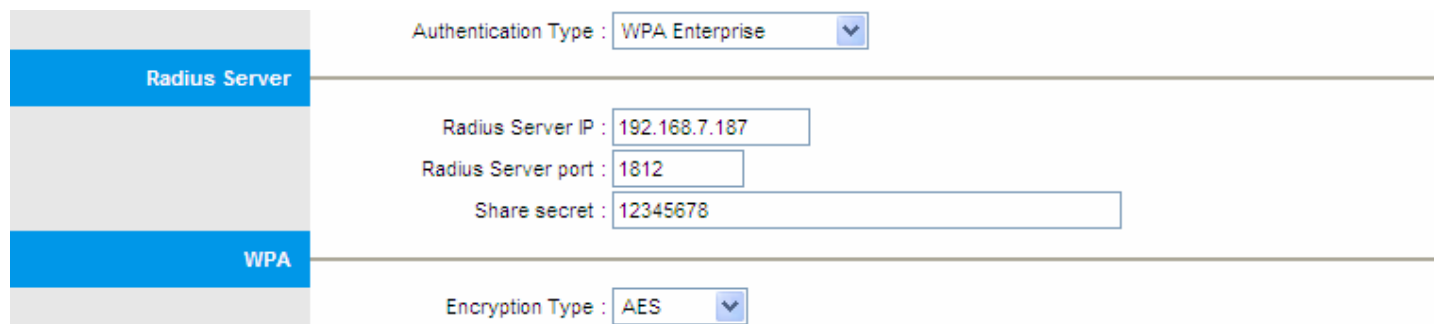
Radius Server IP: enter the IP of Radius server.

Radius Server port: enter the port of Radius server, default is 1812.

Shared secret: it is the shared secret between Radius server and NAS to protect the security communication, enter the shared secret.

Encryption Type: select the WEP encryption methods, refer to [WEP](#).

WPA Enterprise & WPA2 Enterprise & WPA /WPA2 Enterprise



The screenshot shows a configuration interface for WPA Enterprise. On the left, there are two vertical tabs: 'Radius Server' and 'WPA' (selected). The main area is divided into two sections. The top section, under 'Radius Server', contains the following fields: 'Authentication Type' (dropdown menu set to 'WPA Enterprise'), 'Radius Server IP' (text box with '192.168.7.187'), 'Radius Server port' (text box with '1812'), and 'Share secret' (text box with '12345678'). The bottom section, under 'WPA', contains 'Encryption Type' (dropdown menu set to 'AES').

Radius Server IP: enter the IP of Radius server.

Radius Server port: enter the port of Radius server, default is 1812.

Shared secret: it is the shared secret between Radius server and NAS, enter the shared secret.

Encryption Type: AES (Advanced Encryption Standard) and TKIP(Temporal Key Integrity Protocol),

helps to protect the wireless communication.

■ WDS Settings

WDS is a wireless access point mode that enables wireless link and communication with other access point. It is easy to be installed simply to define 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. It can connect up to 4 wireless APs for extending cover range at the same time. In addition, WDS enhances its link connection security in WEP mode, WEP key encryption must be the same for both access points.

WDS Mode: The default setting is off, select on to activate the WDS function.

1. **Mac Address #1:** 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. **Mac Address #2:** It is the second associated AP's MAC Address.
3. **Mac Address #3:** It is the third associated AP's MAC Address.
4. **Mac Address #4:** It is the fourth associated AP's MAC Address.

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

■ Wireless MAC Address Filter

The MAC filter screen allows you to configure the router to give exclusive access to up to 8 devices (Allow Association) or exclude up to 8 devices from accessing the router (Deny Association). Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:AA:BB:00:00:02. You need to know the MAC address of the devices to configure this screen.

● **Active:** Select **Activated** to enable MAC address filtering.

● **Action:** Define the filter action for the list of MAC addresses in the MAC address filter table. Select **Deny Association** to block access to the router, MAC addresses not listed will be allowed to access the router. Select **Allow Association** to permit access to the router, MAC addresses not listed will be denied access to the router.

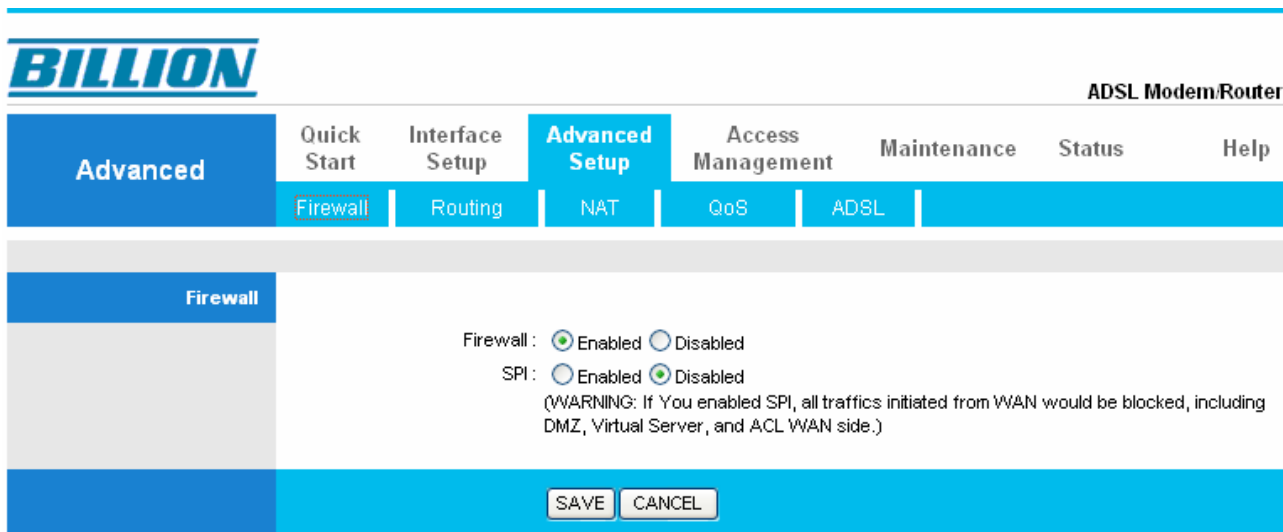
● **MAC Address:** Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the wireless station that are allowed or denied access to the router in these address fields.

Press **SAVE** to apply your configuration.

4.3 Advanced Setup

4.3.1 Firewall

Your router includes a firewall for controlling Internet access from your LAN and 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.



● **Firewall:** to automatically detect and block Denial of Service (DoS) attacks, such as Ping of Death, SYN Flood, Port Scan and Land Attack.

⊙ **Enabled:** Set in default setting, it activates your firewall function.

⊙ **Disabled:** It disables the firewall function.

● **SPI:** If you enabled SPI, all traffics initiated from WAN would be blocked, including DMZ, Virtual Server, and ACL WAN side.

⊙ **Enabled:** Set in default setting, it activates your SPI function.

⊙ **Disabled:** It disables the SPI function.

Press **SAVE** to apply your settings.

4.3.2 Routing

If you have another router with a LAN-to-LAN connection, you may create a static routing on the router that is the gateway to Internet.

The screenshot shows the configuration interface for a BILLION ADSL Modem/Router. The 'Advanced Setup' menu is selected, and the 'Routing' sub-menu is active. Below the navigation tabs, a 'Routing Table List' table is displayed with the following data:

#	Dest IP	Mask	Gateway IP	Metric	Device	Use	Edit	Drop
1	192.168.1.0	24	192.168.1.254	1	enet0	896		
2	default	0	Node1	2	Idle	160		

Below the table is an 'ADD ROUTE' button.

● #: Item number

● **Dest IP:** IP address of the destination network

● **Mask:** The destination mask address. Here mask refers to the number of the amount of '1' in submask, it is the length of net-id. For example, 24 means the submask is 255.255.255.0.

● **Gateway IP:** IP address of the gateway or existing interface that this route uses, also known as the next hop.

● **Metric:** It represents the cost of transmission for routing purposes.

● **Device:** Media/channel selected to append the route.

● **Use:** the statistics of the packets received and transmitted.

● **Edit:** Edit the route; this icon is not shown for system default route.

● **Drop:** Drop the route; this icon is not shown for system default route.

ADD Route

The screenshot shows the configuration interface for a BILLION ADSL Modem/Router. The top navigation bar includes 'Quick Start', 'Interface Setup', 'Advanced Setup', 'Access Management', 'Maintenance', 'Status', and 'Help'. The 'Advanced Setup' menu is expanded to show 'Firewall', 'Routing', 'NAT', 'QoS', and 'ADSL'. The 'Static Route' configuration form is displayed with the following fields:

- Destination IP Address : 0.0.0.0
- IP Subnet Mask : 0.0.0.0
- Gateway IP Address : 0.0.0.0 (selected with a radio button)
- Metric : 0
- Announced in RIP : Yes (selected with a dropdown arrow)

At the bottom of the form, there are four buttons: 'SAVE', 'DELETE', 'BACK', and 'CANCEL'.

● **Destination IP Address:** This is the destination subnet IP address.

● **IP Subnet Mask:** A subnet mask allows IP networks to be subdivided for security and performance purposes.

● **Gateway IP Address:** This is the gateway IP address to which packets are to be forwarded.

● **Metric:** It represents the cost of transmission for routing purposes. The number need not be precise, but it must be between 1 and 15.

● **Announced in RIP:** This parameter determines if the Prestige will include the route to the remote node in its RIP broadcasts. Set "No", it is kept private and is not included in RIP broadcasts. Set "Yes", the remote node will be propagated to other hosts through RIP broadcasts.

Press **SAVE** to apply your settings and the item you added will be listed in the **Routing Table List**.

4.3.3 NAT

The NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet. The default setting is **Dynamic NAT**. It provides dynamic Network Address Translation capability between LAN and multiple WAN connections, and the LAN traffic is routed to appropriate WAN connections based on the destination IP addresses and Route Table. This eliminates the need for the static NAT session configuration between multiple LAN clients and multiple WAN connections.

The screenshot shows the BILLION ADSL Modem/Router web interface. The top navigation bar includes 'Advanced', 'Quick Start', 'Interface Setup', 'Advanced Setup', 'Access Management', 'Maintenance', 'Status', and 'Help'. The 'Advanced Setup' menu is expanded to show 'Firewall', 'Routing', 'NAT', 'QoS', and 'ADSL'. The 'NAT' page is active, displaying the following configuration options:

- Virtual Circuit: PVC0 (dropdown menu)
- NAT Status: Activated
- Number of IPs: Single Multiple
- DMZ (toggle button)
- Virtual Server (toggle button)

● **Virtual Circuit:** VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. There are eight groups of PVC can be defined and used.

● **NAT Status:** Show the NAT status, Activated or Deactivated.

● **Number of IPs:** Users can select Single or Multiple. Select Multiple to trigger IP Address Mapping.

The screenshot shows the BILLION ADSL Modem/Router web interface. The top navigation bar is the same as in the previous screenshot. The 'DMZ' page is active, displaying the following configuration options:

- DMZ setting for: PVC0 - Multiple IP Account
- DMZ: Enabled Disabled
- DMZ Host IP Address: 0.0.0.0 (text input field)
- SAVE (button)
- BACK (button)

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 will be checked by the Firewall and NAT algorithms then passed to the DMZ host, when a packet received does not use a port number used by any other Virtual Server entries.

The screenshot shows the BILLION ADSL Modem/Router web interface. The top navigation bar includes 'Advanced', 'Quick Start', 'Interface Setup', 'Advanced Setup', 'Access Management', 'Maintenance', 'Status', and 'Help'. Under 'Advanced Setup', there are sub-menus for 'Firewall', 'Routing', 'NAT', 'QoS', and 'ADSL'. The 'DMZ' section is active, showing 'DMZ setting for : Single IP Account'. The 'DMZ' radio buttons are set to 'Disabled'. The 'DMZ Host IP Address' is set to '0.0.0.0'. At the bottom, there are 'SAVE' and 'BACK' buttons.

● **DMZ setting for:** indicate the related LAN PC and PVC ports which allow outside network to connect in and communicate.

● **DMZ:** **Enabled** **Disabled:** As set in default setting, it disables the DMZ function.

Enabled: It activates your DMZ function.

● **DMZ Host IP Address:** Give a static IP address to the DMZ Host when **Enabled** radio button is checked. Be aware that this IP will be exposed to the WAN/Internet.

Select the **SAVE** button to apply your changes.

Virtual Server

In TCP/IP 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 will usually need to configure your router to forward these incoming connection attempts using specific ports to the PC on your network running the application. You will also need to use port forwarding if you want to host an online game server.

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

The device can be configured as a virtual server so that remote users accessing services such as Web or FTP services via the public (WAN) IP address can be automatically redirected to local servers in the LAN network. Depending on the requested service (TCP/UDP port number), the device redirects the external service request to the appropriate server within the LAN network.

BILLION ADSL Modem/Router

Advanced | Quick Start | Interface Setup | **Advanced Setup** | Access Management | Maintenance | Status | Help

Firewall | Routing | **NAT** | QoS | ADSL

Virtual Server

Virtual Server for : Single IP Account

Rule Index : 1

Application : -

Protocol : ALL

Start Port Number : 0

End Port Number : 0

Local IP Address : 0.0.0.0

Virtual Server Listing

Rule	Application	Protocol	Start Port	End Port	Local IP Address
1	-	-	0	0	0.0.0.0
2	-	-	0	0	0.0.0.0
3	-	-	0	0	0.0.0.0
4	-	-	0	0	0.0.0.0
5	-	-	0	0	0.0.0.0
6	-	-	0	0	0.0.0.0
7	-	-	0	0	0.0.0.0
8	-	-	0	0	0.0.0.0
9	-	-	0	0	0.0.0.0
10	-	-	0	0	0.0.0.0
11	-	-	0	0	0.0.0.0
12	-	-	0	0	0.0.0.0
13	-	-	0	0	0.0.0.0
14	-	-	0	0	0.0.0.0
15	-	-	0	0	0.0.0.0
16	-	-	0	0	0.0.0.0

SAVE DELETE BACK CANCEL

- **Rule Index:** Choose the rule number.
- **Application:** Choose the predefined rule from Application drop-down menu or enter a custom name.
- **Protocol:** Choose the Protocol Type, ALL, TCP or UDP.

● **Start Port Number:** Enter a port number as the beginning number of the range which you want to give to devices to access in this field.

● **End Port Number:** Enter a port number as the end number of the range which you want to give to devices to access in this field.

● **Local IP Address:** Enter your server IP address in this field.

Press **SAVE** to confirm your settings, and the item you added will be listed in the **Virtual Server Listing** table below.

Select the rule index of the item you want to delete from the **Rule Index** drop-down menu, press **DELETE** and you will delete it.

IP Address Mapping



ADSL Modem/Router

Advanced
Quick Start
Interface Setup
Advanced Setup
Access Management
Maintenance
Status
Help

Firewall
Routing
NAT
QoS
ADSL

IP Address Mapping

Address Mapping Rule : PVC0

Rule Index :

Rule Type :

Local Start IP :

Local End IP :

Public Start IP : (0.0.0.0 for modem's WAN IP)

Public End IP :

Address Mapping List

Rule	Type	Local Start IP	Local End IP	Public Start IP	Public End IP
1	M-1	0.0.0.0	255.255.255.255	0.0.0.0	...
2	-
3	-
4	-
5	-
6	-
7	-
8	-

● **Address Mapping Rule:** Shows the PVC where the rule will be applied to.

● **Rule Index:** Choose the rule number.

● **Rule Type:**

- ① One-to-one: This is the mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type.
- ① Many-to-One: This is the mode maps multiple local IP addresses to one global IP address. This is equivalent to Many to One (i.e., PAT, port address translation).
- ① Many-to-Many Overload: This mode maps multiple local IP addresses to shared global IP addresses.
- ① Many-to-Many No Overload: This mode maps each local IP address to a unique global IP addresses.
- ① Server: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.

● **Local Start IP:** This is the starting range for Inside Local IP Address (ILA). Local IP addresses are

N/A for Server port mapping.

● **Local End IP:** This is the end range for Inside Local IP Address (ILA). If your rule is for all local IP addresses, then enter 0.0.0.0 as the Local Start IP address and 255.255.255.255 as the Local End IP address. This field is N/A for One-to-one and Server mapping types.

● **Public Start IP:** This is the start range for Inside Public IP Address. Enter 0.0.0.0 here if you have a dynamic IP address from your ISP.

● **Public End IP:** This is the end range for Inside Public IP Address. This field is N/A for One-to-one, Many-to-One and Server mapping types.

Press **SAVE** to confirm your settings, and the corresponding settings will be listed in the **Address Mapping List** table.

Select the rule index of the item you want to delete from the **Rule Index** drop-down menu, press **DELETE** and you will delete it.



Using port forwarding does have security implications, as outside users will be 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 using DMZ. As doing so will result in all connections from the WAN attempt to access to your public IP of the DMZ PC specified.



Attention

If you have disabled the NAT option in the WAN-ISP section, the Virtual Server function will hence be invalid.

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 static IP address to each virtual server PC, with an address that does not fall into the range of IP addresses that are to be issued by the DHCP server. You can configure the virtual server IP address manually, but it must still be in the same subnet as the router.

4.3.4 QoS

Quality of Service (QoS) helps to prioritize data as it enters your router. By attaching special identification marks or headers to incoming packets, QoS determines which queue the packets enter, based on priority. This is useful when there are certain types of data you want to give higher priority to, such as voice data packets given higher priority than Web data packets.

The main goal of QoS is prioritizing incoming data, preventing data loss due to factors such as jitter, delay and dropping. Another important aspect of QoS is ensuring that prioritizing one data flow doesn't interfere with other data flows.

QoS can be toggled Activated and Deactivated. QoS must be activated before you can edit the following options. When you are done making changes, click on **Add** to save your changes.

Click on **QoS Settings Summary** to view the list of QoS rules that have been added.

The screenshot shows the configuration interface for a BILLION ADSL Modem/Router. The top navigation bar includes 'Advanced', 'Quick Start', 'Interface Setup', 'Advanced Setup', 'Access Management', 'Maintenance', 'Status', and 'Help'. Under 'Advanced Setup', there are sub-menus for 'Firewall', 'Routing', 'NAT', 'QoS', and 'ADSL'. The 'QoS' menu is selected, showing 'QoS : Activated Deactivated' and a 'Summary : QoS Settings Summary' button. The 'Rule' section contains fields for 'Rule Index' (1), 'Active' (Activated Deactivated), 'Application' (dropdown), 'Physical Ports' (checkboxes for WLAN, Enet1, Enet2, Enet3, Enet4), 'Destination MAC' (IP, Mask, Port Range), 'Source MAC' (IP, Mask, Port Range), 'Protocol ID' (dropdown), 'Vlan ID Range' (dropdown), 'IPP/DS Field' (IPP/TOS DSCP), 'IP Precedence Range' (dropdowns), 'Type of Service' (dropdown), 'DSCP Range' (dropdowns, Value Range: 0 ~ 63), and '802.1p' (dropdowns). The 'Action' section includes 'IPP/DS Field' (IPP/TOS DSCP), 'IP Precedence Remarking' (dropdown), 'Type of Service Remarking' (dropdown), 'DSCP Remarking' (dropdown, Value Range: 0 ~ 63), '802.1p Remarking' (dropdowns), and 'Queue #' (dropdown). At the bottom, there are 'ADD', 'DELETE', and 'CANCEL' buttons.

Rule

You can set 16 different QoS rules. Each QoS rule has its detail setting conditions like: 802.1p application, DSCP, IP, MAC, Protocol, TOS, VLAN etc, you can modify the default value to any new one you wish. Please notice that only when the packet fulfill every detail setting conditions here, then this packet will be remarked as the priority queue of each rule. The non-selected setting part will be treated as “don’t care” and the system will not handle this setting part. If the original packet does not have 802.1q tagged header, system will not add header for this packet even the detail setting condition has adding 802.1p priority ability.

Quality of Service

QoS : Activated Deactivated

Summary : [QoS Settings Summary](#)

Rule

Rule Index :

Active : Activated Deactivated

Application :

Physical Ports : WLAN Enet1 Enet2 Enet3 Enet4

Destination MAC :

IP :

Mask :

Port Range : ~

Source MAC :

IP :

Mask :

Port Range : ~

Protocol ID :

Vlan ID Range : ~

IPP/DS Field : IPP/TOS DSCP

IP Precedence Range : ~

Type of Service :

DSCP Range : ~ (Value Range: 0 ~ 63)

802.1p : ~

● **QoS:** Select **Activated** to activate the following configuration, and if your select **Deactivated**, the following will be gray, that is, the configuration is unavailable.

● **Summary:** the settings of this QOS configuration.

● **Rule Index:** Select 16 different rules, each rule’s detail can be set and saved.

● **Active:** Select QoS rule is activated or deactivated.

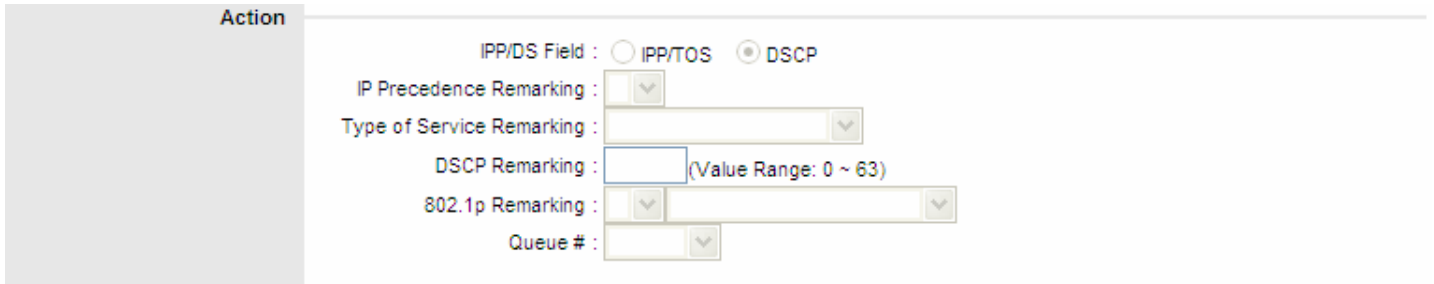
● **Application:** Select 11 different applications: IGMP, SIP, H.323, MGCP, SNMP, DNS, DHCP, RIP, RSTP, RTCP, RTP.

● **Physical Ports:** this function is to allow you to decide which physical port you want to configure ,before you begin to configure, please make sure QoS is activated.

- **Destination MAC:** Set the Ethernet MAC value that you want to filter in destination side.
- **IP:** Set the IP address value that you want to filter in destination side.
- **Mask:** Set the subnet mask value that you want to filter in destination side.
- **Range:** Set the port range value that you want to filter in destination side.
- **Source MAC:** Set the Ethernet MAC value that you want to filter in source side.
- **IP:** Set the IP address value that you want to filter in source side.
- **Mask:** Set the subnet mask value that you want to filter in source side.
- **Port Range:** Set the port range value that you want to filter in source side.
- **Protocol ID:** Set the protocol ID type that you want to filter.
- **Vlan ID Range:** Set the Vlan value that you want to filter.
- **IPP/DS Field:** Select IP QoS format: IPP/TOS, DSCP.
- **IP Precedence Range:** Select the IP precedence range (unavailable when you select DSCP in IPP/DS Field)
- **Type of Service:** Select 5 different type of service (unavailable when you select DSCP in IPP/DS Field).
- **DSCP Range:** Set the DSCP value that you want to filter (unavailable when you select IPP/TOS in IPP/DS Field).
- **802.1p:** Set the remarked new 802.1p priority value on the packet that fulfill every detail setting condition of each rule.

■ Action

After finishing all rules detail condition setting, select the rule you want to execute and action here.



The screenshot shows the 'Action' configuration panel. At the top, there are two radio buttons for 'IPP/DS Field': 'IPP/TOS' (unselected) and 'DSCP' (selected). Below this are five rows of configuration options, each with a dropdown menu:

- IP Precedence Remarking : [dropdown]
- Type of Service Remarking : [dropdown]
- DSCP Remarking : [text input] (Value Range: 0 ~ 63)
- 802.1p Remarking : [dropdown]
- Queue # : [dropdown]

- **IPP/DS Field:** Select IP QoS format.
- **IP Precedence Remarking:** Select the remarking value of IP precedence (unavailable when you select DSCP in IPP/DS Field).
- **Type of service Remarking:** Select the remarking value of type of service (unavailable when you select DSCP in IPP/DS Field).
- **DSCP Remarking:** Select the remarking value of DSCP (unavailable when you select IPP/TOS in IPP/DS Field).
- **802.1p Remarking:** Select the remarking value of 802.1p.
- **Queue #:** Select four types of Queue: Low, Medium, High, Highest.

4.3.5 ADSL

The screenshot displays the configuration interface for a BILLION ADSL Modem/Router. The top navigation bar includes 'Advanced', 'Quick Start', 'Interface Setup', 'Advanced Setup', 'Access Management', 'Maintenance', 'Status', and 'Help'. Under 'Advanced Setup', there are sub-menus for 'Firewall', 'Routing', 'NAT', 'QoS', and 'ADSL'. The 'ADSL' sub-menu is active, showing a configuration area with two dropdown menus: 'ADSL Mode' set to 'Auto Sync-Up' and 'ADSL Type' set to 'ANNEX A/I/J/L/M'. A 'SAVE' button is located at the bottom of the configuration area.

● **ADSL Mode:** The default setting is **Auto Sync-Up**. This mode will automatically detect your ADSL2, ADSL2+, ADSL2, G.DMT, G.lite, and T1.413. But in some area, multimode cannot detect the ADSL line code well. If it is the case, please adjust the ADSL line code to G.DMT or T1.413 first. If it still fails, please try the other values such as ALCTL, ADI, etc.

● **ADSL Type:** There are five modes "Annex A", "Annex I", "Annex A/L", "Annex M" and "Annex A/I/J/L/M" that user can select for this connection.

Press **SAVE** to apply your settings.

4.4 Access Management

4.4.1 ACL

Access Control Listing allows you to determine which services/protocols can access BiPAC 5200W interface from which computers.

BILLION ADSL Modem/Router

Access Management Quick Start Interface Setup Advanced Setup **Access Management** Maintenance Status Help

ACL Filter SNMP UPnP DDNS

Access Control Setup

ACL : Activated Deactivated

Access Control Editing

ACL Rule Index : 1

Active : Yes No

Secure IP Address : 0.0.0.0 ~ 0.0.0.0 (0.0.0.0 ~ 0.0.0.0 means all IPs)

Application : ALL

Interface : LAN

Access Control Listing

Index	Active	Secure IP Address	Application	Interface
1	Yes	0.0.0.0-0.0.0.0	ALL	LAN

SAVE DELETE CANCEL

● **ACL:** Select whether to activate to configure this ACL function. If you select Deactivated, then the following is not available.

● **ACL Rule Index:** This is item number.

● **Active:** Select Yes to activate the ACL function of this item or No to disable ACL function of this item.

● **Secure IP Address:** The default 0.0.0.0 allows any client to use this service to remotely manage the BiPAC 5200W. Type an IP address to restrict access to a client with a matching IP address.

● **Application:** Choose a service that you may use to remotely manage the BiPAC 5200W.

● **Interface:** Select the access interface. Choices are **LAN**, **WAN** and **Both**.

Press **SAVE** to confirm your settings, and the corresponding settings will be listed in the **Address Control Listing** table.

Select the rule index of the item you want to delete from the **ACL Rule Index** drop-down menu, press **DELETE** and you will delete it.

4.4.2 Filter

You can filter the packages by IP port, MAC and Application.

ADSL Modem/Router

Access Management | Quick Start | Interface Setup | Advanced Setup | **Access Management** | Maintenance | Status | Help

ACL | **Filter** | SNMP | UPnP | DDNS

Filter Type

Filter Type Selection : IP / MAC Filter

IP / MAC Filter Set Editing

IP / MAC Filter Set Index : 1
 Interface : PVC0
 Direction : Both

IP / MAC Filter Rule Editing

IP / MAC Filter Rule Index : 1
 Rule Type : IP
 Active : Yes No

Source IP Address : (0.0.0.0 means Don't care)
 Subnet Mask :
 Port Number : 0 (0 means Don't care)

Destination IP Address : (0.0.0.0 means Don't care)
 Subnet Mask :
 Port Number : 0 (0 means Don't care)

Protocol : TCP
 Rule Unmatched : Forward

IP / MAC Filter Listing

IP / MAC Filter Set Index		Interface		Direction			
#	Active	Src Address/Mask	Dest IP/Mask	Src Port	Dest Port	Protocol	Unmatched
1	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-

SAVE DELETE CANCEL

Filter Type

Filter Type Selection: There are three types “IP/MAC Filter”, “Application Filter”, and “URL Filter” that user can select for this connection.

■ IP/MAC Filter Set Editing

- **IP/MAC Filter Set Index:** This is item number
- **Interface:** Select which interface to configure, PVC or LAN.
- **Direction:** Select the access to the Internet (“**Outgoing**”) or from the Internet (“**Incoming**”).or **Both**.

■ IP/MAC Filter Rule Editing

- **IP/MAC Filter Rule Index:** This is item number
- **Rule Type:** Choose “IP” or “MAC” rules
- **Active:** Select **Yes** from the drop down list box to enable IP filter rule.
- **Source IP Address:** The source IP address or range of packets to be monitored.
- **Subnet Mask:** It is the source IP addresses based on above source subnet IP
- **Source Port Number:** This Port or Port Ranges defines the port 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.
- **Destination IP Address:** This is the destination subnet IP address.
- **Subnet Mask:** It is the destination IP addresses based on above destination subnet IP
- **Destination Port Number:** This is the Port or Port Ranges that defines the application.
- **Protocol:** It is the packet protocol type used by the application, select either **TCP** or **UDP** or **ICMP**
- **Rule Unmatched:** Select action for the traffic unmatching current rule; Forward to leave it pass through, and NEXT to check it by the next rule.

■ IP/MAC Filter Listing

- **#:** Item number.
- **Active:** Whether the connection is currently active.
- **Src Address/Mask:** The source IP address or range of packets to be monitored.
- **Dest IP/Mask:** This is the destination subnet IP address.
- **Src port:** This Port or Port Ranges defines the port 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.
- **Dest Port:** This is the Port or Port Ranges that defines the application.
- **Protocol:** It is the packet protocol type used by the application, select either **TCP** or **UDP** or **ICMP**
- **Unmatched:** It shows this profile's setting: Forward or NEXT

Press **SAVE** to confirm your settings, and the corresponding settings will be listed in the **IP/MAC Filter Listing** table.

Select the rule index of the item you want to delete from the **IP/MAC Filter set Index** drop-down menu, press **DELETE** and you will delete it.

Application Filter

The screenshot shows the BILLION ADSL Modem/Router web interface. The top navigation bar includes the BILLION logo and the text "ADSL Modem/Router". Below the logo is a menu with "Access Management" selected, and other options: "Quick Start", "Interface Setup", "Advanced Setup", "Access Management", "Maintenance", "Status", and "Help". Under "Access Management", there are sub-menus: "ACL", "Filter", "SNMP", "UPnP", and "DDNS". The "Filter" sub-menu is active, showing "Filter Type" and "Application Filter Editing". The "Filter Type Selection" dropdown is set to "Application Filter". The "Application Filter" section has radio buttons for "Activated" and "Deactivated", with "Deactivated" selected. Below this are radio buttons for "Allow" and "Deny" for "ICQ", "MSN", "YMSG", and "Real Audio/Video", all with "Allow" selected. At the bottom, there are "SAVE" and "CANCEL" buttons.

- **Application Filter:** Select this option to Activated/Deactivated the Application filter.
- **ICQ:** Select this option to Allow/Deny ICQ.
- **MSN:** Select this option to Allow/Deny MSN.
- **YMSG:** Select this option to Allow/Deny Yahoo messenger.
- **Real Audio/Video:** Select this option to Allow/Deny Real Audio/Video.

Press **SAVE** to apply your settings.

URL Filter

BILLION ADSL Modem/Router

Access Management | Quick Start | Interface Setup | Advanced Setup | **Access Management** | Maintenance | Status | Help

ACL | Filter | SNMP | UPnP | DDNS

Filter

Filter Type

Filter Type Selection : URL Filter

URL Filter Editing

Active : Yes No

URL Index : 1

URL :

URL Filter Listing

Index	URL
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	

SAVE DELETE CANCEL

● **Active:** Select **Yes** to enable URL Filter.

● **URL Index:** This is item number.

● **URL:** Allow you to prevent users on your network from accessing particular websites by their URL. Input the URL you want to filter in this field.

Press **SAVE** to confirm your settings, and the corresponding settings will be listed in the **URL Filter Listing** table.

Select the rule index of the item you want to delete from the **URL Index** drop-down menu, press **DELETE** and you will delete it.

4.4.3 SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. BiPAC 5200W supports SNMP agent functionality which allows a manager station to manage and monitor the router through the network.

The screenshot shows the configuration interface for a BILLION ADSL Modem/Router. The top navigation bar includes 'Access Management', 'Quick Start', 'Interface Setup', 'Advanced Setup', 'Access Management', 'Maintenance', 'Status', and 'Help'. Under 'Access Management', there are sub-menus for 'ACL', 'Filter', 'SNMP', 'UPnP', and 'DDNS'. The 'SNMP' sub-menu is selected, showing a configuration table with two rows: 'Get Community' and 'Set Community', both with the value 'public'. A 'SAVE' button is located at the bottom of the configuration area.

SNMP	Get Community	Set Community
	public	public

SAVE

● **Get Community:** Type the Get Community, which is the password for the incoming Get-and-GetNext requests from the management station.

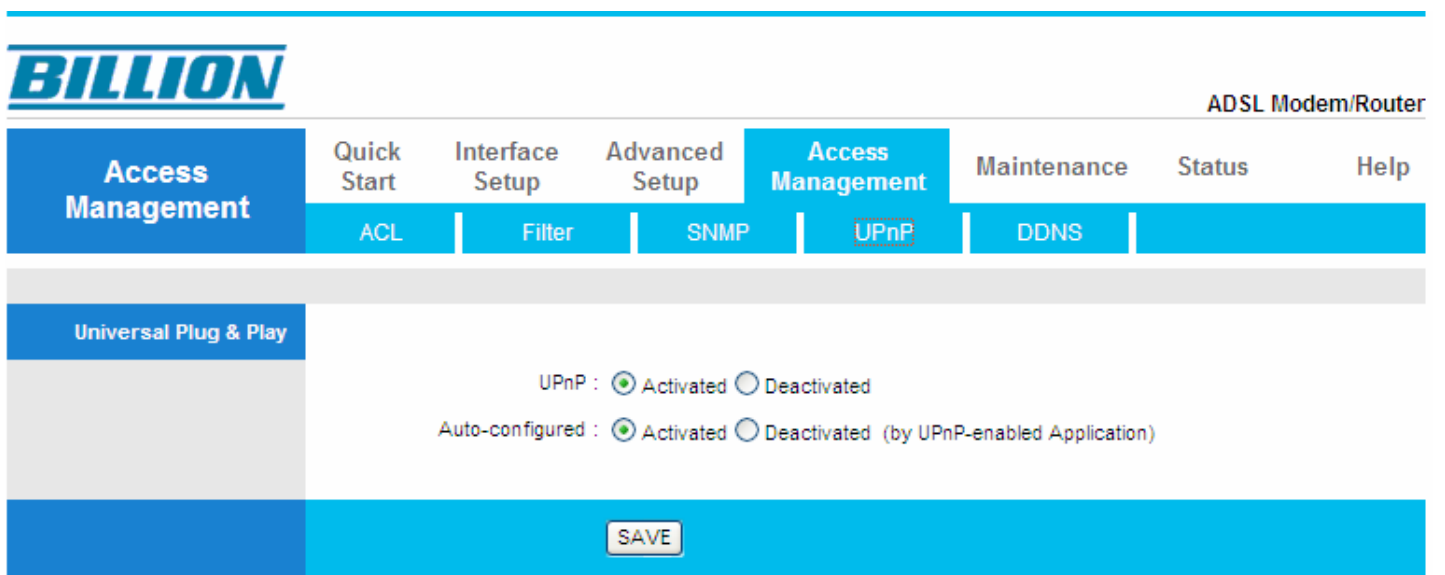
● **Set Community:** Type the Set Community, which is the password for incoming Set requests from the management station.

Press **SAVE** to apply your settings.

4.4.4 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.



● **UPnP:** Select this checkbox to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the BiPAC 5200W's IP address.

● **Auto-configured:** Select this check box to allow UPnP-enabled applications to automatically configure the BiPAC 5200W so that they can communicate through the BiPAC 5200W, for example by using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.

Press **SAVE** to apply your settings.

4.4.5 DDNS

The Dynamic DNS function allows you to alias a dynamic IP address to a static hostname, allowing users whose ISP does not assign them a static IP address to 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.

The screenshot shows the configuration page for Dynamic DNS on a BILLION ADSL Modem/Router. The page has a blue header with the 'BILLION' logo and 'ADSL Modem/Router' text. Below the logo is a navigation menu with tabs: 'Access Management', 'Quick Start', 'Interface Setup', 'Advanced Setup', 'Access Management', 'Maintenance', 'Status', and 'Help'. Under 'Access Management', there are sub-tabs: 'ACL', 'Filter', 'SNMP', 'UPnP', and 'DDNS'. The 'DDNS' sub-tab is selected, showing the 'Dynamic DNS' configuration form. The form includes a 'Dynamic DNS' status selector (radio buttons for 'Activated' and 'Deactivated', with 'Deactivated' selected), a 'Service Provider' field (pre-filled with 'www.dyndns.org'), and four input fields for 'My Host Name', 'E-mail Address', 'Username', and 'Password'. At the bottom, there is a 'Wildcard support' selector (radio buttons for 'Yes' and 'No', with 'No' selected) and a 'SAVE' button.

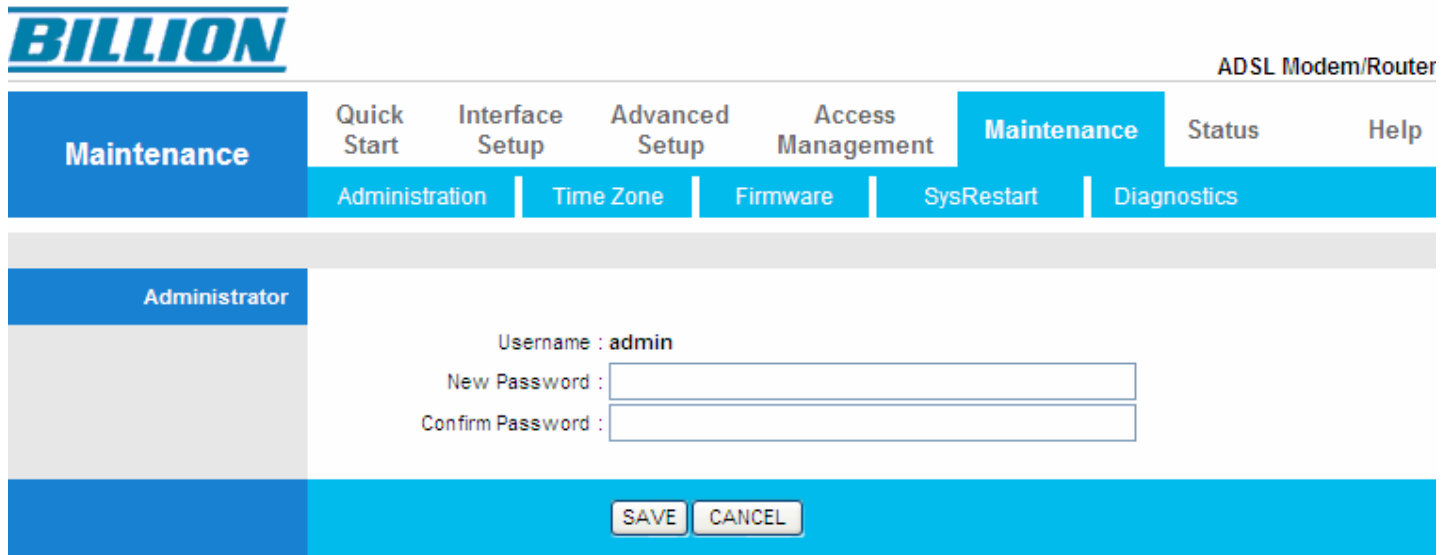
- **Dynamic DNS:** Select this check box to use Dynamic DNS.
- **Service Provider:** www.dyndns.org
- **My Host Name:** Type the domain name assigned to your BiPAC 5200W by your Dynamic DNS provider.
- **E-mail Address:** Type your e-mail address.
- **Username:** Type your user name.
- **Password:** Type the password assigned to you.
- **Wildcard support:** Select this check box to enable DYNDNS Wildcard.

Press **SAVE** to apply your settings.

4.5 Maintenance

4.5.1 Administrator

In factory setting, the default password is **admin**, and that for user is also password. You can change the default password to ensure that someone cannot adjust your settings without your permission. Every time you change your password, please record the password and keep it at a safe place.



The screenshot shows the BILLION ADSL Modem/Router web interface. The top navigation bar includes the BILLION logo and the text "ADSL Modem/Router". Below the logo is a menu with "Maintenance" selected. The "Maintenance" menu is expanded to show sub-options: Administration, Time Zone, Firmware, SysRestart, and Diagnostics. The "Administrator" section is active, displaying the following form:

Username : admin

New Password :

Confirm Password :

At the bottom of the form are two buttons: "SAVE" and "CANCEL".

● **New Password:** Type the new password in this field

● **Confirm Password:** Type the new password again in this field.

Press **SAVE** to apply your settings.

4.5.2 Time Zone

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. After a successful connection to the Internet, the router will retrieve 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.

The screenshot shows the BILLION ADSL Modem/Router web interface. The top navigation bar includes 'Maintenance' (selected), 'Quick Start', 'Interface Setup', 'Advanced Setup', 'Access Management', 'Status', and 'Help'. Below this, a secondary navigation bar has 'Administration', 'Time Zone' (selected), 'Firmware', 'SysRestart', and 'Diagnostics'. The main content area is titled 'Time Zone' and shows 'Current Date/Time : 01/01/2000 00:14:51'. Under 'Time Synchronization', there are three radio button options: 'NTP Server automatically' (selected), 'PC's Clock', and 'Manually'. A 'Time Zone' dropdown menu is set to '(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London'. Below this, 'Daylight Saving' has 'Enabled' and 'Disabled' (selected) radio buttons. Two text input fields for 'NTP Server Address' and 'NTP Server2 Address' both contain '0.0.0.0' with '(0.0.0.0: Default Value)' to their right. At the bottom, there are 'SAVE' and 'CANCEL' buttons.

● **Synchronize time with:** Select the time service protocol that your time server sends when you turn on the Router.

● **Time Zone:** Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).

● **Daylight Saving:** Select this option if you use daylight savings time.

● **NTP Server Address/NTP Server2 Address:** Enter the IP address of your time server. Check with your ISP/network administrator if you are unsure of this information.

Press **SAVE** to apply your settings.

4.5.3 Firmware

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, and your router allows you to upgrade the software it runs to take advantage of these changes.

To upgrade the firmware of BiPAC 5200W, you should download or copy the firmware to your local environment first. Press the "**Browse...**" button to specify the path of the firmware file. Then, click "**Upgrade**" to start upgrading. When the procedure is completed, BiPAC 5200W will reset automatically to make the new firmware work.

BILLION ADSL Modem/Router

Maintenance Quick Start Interface Setup Advanced Setup Access Management Maintenance Status Help

Administration Time Zone Firmware SysRestart Diagnostics


Firmware/Romfile Upgrade

Current Firmware Version : 2.12.24.0(SRE2.C3)3.12.8.200

New Firmware Location :

New Romfile Location :

Romfile Backup :

Status :  It might take several minutes, don't power off it during upgrading. Device will restart after the upgrade.

● **New Firmware Location:** Type in the location of the file you want to upload in this field or click **Browse** to find it.

● **New Romfile Location:** Romfile means the configuration file. Type in the location of the file you want to upload in this field or click **Browse** to find it.


● **Browse:** Click **Browse...** to find the .ras file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.

● **Romfile Backup:** Click **ROMFILE SAVE** button to save current configuration file to your PC.

● **UPGRADE:** Click **UPGRADE** to begin the upload process. This process may take up to two minutes.

After two minutes, log in again and check your new firmware version in the System Status screen. If the upload was not successful, the following screen will appear. Click Back to go back to the

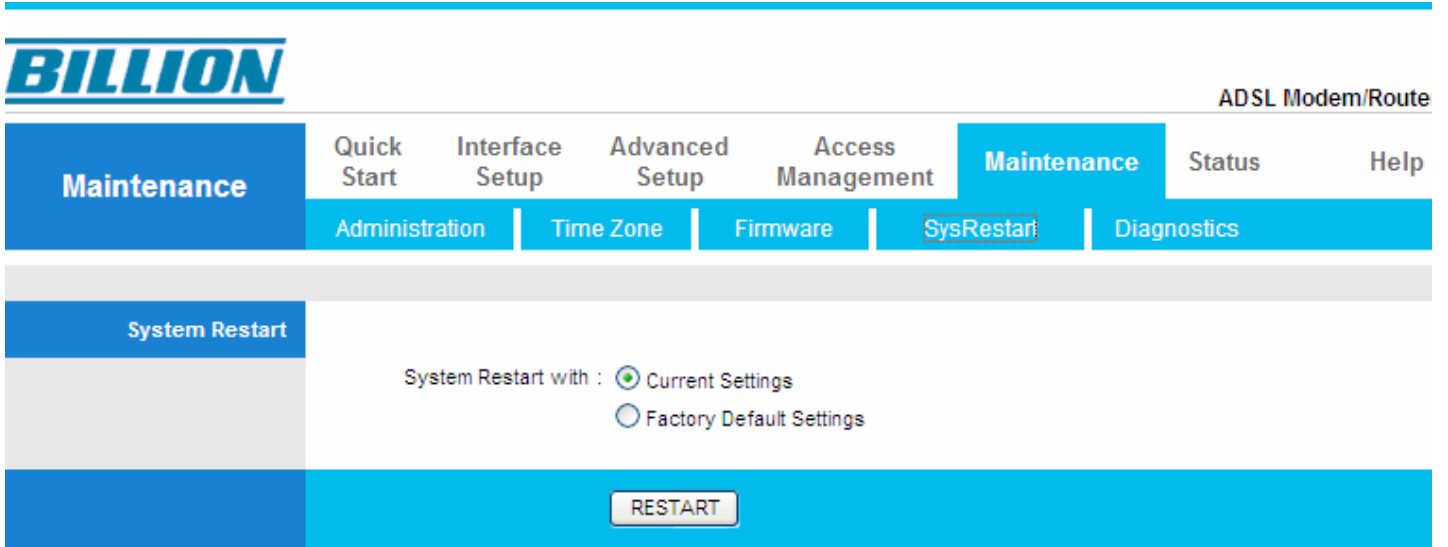
Firmware screen.



DO NOT power down the router or interrupt the firmware upgrading while it is still in process. Improper operation could damage the router.

4.5.4 SysRestart

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



The screenshot shows the BILLION router web interface. At the top left is the BILLION logo. On the right, it says "ADSL Modem/Route". Below the logo is a navigation menu with tabs: Maintenance, Quick Start, Interface Setup, Advanced Setup, Access Management, Maintenance (highlighted), Status, and Help. Under the highlighted Maintenance tab, there are sub-tabs: Administration, Time Zone, Firmware, SysRestart (highlighted), and Diagnostics. Below this is a "System Restart" section. It contains the text "System Restart with :" followed by two radio button options: "Current Settings" (which is selected) and "Factory Default Settings". At the bottom of this section 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 the small Reset pinhole button on the back of your router in about more than 6 seconds whilst the router is turned on.

4.5.5 Diagnostics

The Diagnostic Test page shows the test results for the connectivity of the physical layer and protocol layer for both LAN and WAN sides.

The screenshot displays the web interface of a BILLION ADSL Modem/Router. The top navigation bar includes the following tabs: Quick Start, Interface Setup, Advanced Setup, Access Management, Maintenance (selected), Status, and Help. Below this, a secondary navigation bar contains: Administration, Time Zone, Firmware, SysRestart, and Diagnostics (selected). The main content area is titled "Diagnostic Test" and features a dropdown menu for "Virtual Circuit" set to "PVC0". The test results are as follows:

Test Description	Result
>> Testing Ethernet LAN connection ...	PASS
>> Testing ADSL Synchronization .	SKIPPED
>> Testing ATM OAM segment ping ...	SKIPPED
>> Testing ATM OAM end to end ping ...	SKIPPED
>> Ping Primary Domain Name Server .	SKIPPED
>> Ping www.yahoo.com ...	SKIPPED

4.6 Status

4.6.1 Device Info

This page displays the current information for the ADSL Router. It will display the Firmware version, LAN, WAN, and MAC address information.

BILLION ADSL Modem/Router

Quick Start | Interface Setup | Advanced Setup | Access Management | Maintenance | **Status** | Help

Device Info | System Log | Statistics

Device Information

Firmware Version : 2.12.24.0(SRE2.C3)3.12.8.200
MAC Address : 00:04:ed:01:23:45

LAN

IP Address : 192.168.1.254
Subnet Mask : 255.255.255.0
DHCP Server : Enabled

WAN

Virtual Circuit : PVC0
Status : Not Connected
Connection Type : PPPoE
IP Address : 0.0.0.0
Subnet Mask : 0.0.0.0
Default Gateway : 0.0.0.0
Primary DNS : 0.0.0.0
Secondary DNS : 0.0.0.0
NAT : Enabled

ADSL

ADSL Firmware Version : FwVer:3.12.8.200_TC3086 HwVer:T14.F7_7.0
Line State : Down
Modulation : N/A
Annex Mode : N/A

	Downstream	Upstream	
SNR Margin :	N/A	N/A	db
Line Attenuation :	N/A	N/A	db
Data Rate :	N/A	N/A	kbps

Device Information

● **Firmware Version:** This is the Firmware version

● **MAC Address:** This is the MAC Address

■ LAN

- **IP Address:** LAN port IP address.
- **Sub Net Mask:** LAN port IP subnet mask.
- **DHCP Server:** LAN port DHCP role - Enabled, Relay or disabled

■ WAN

- **Virtual Circuit:** There are eight groups of PVC can be defined.
- **VPI:** The valid range for the VPI is 0 to 255
- **VCI:** The valid range for the VCI is 1 to 65535
- **Status:** "Not connected" or "Connected".
- **Connection Type:** Name of the WAN connection.
- **IP Address:** WAN port IP address.
- **Subnet Mask:** WAN port IP subnet mask.
- **Default Gateway:** The IP address of the default gateway.
- **Primary DNS:** the address of the primary DNS server.
- **Secondary DNS:** the address of the secondary DNS server.
- **NAT:** Enabled or Disabled NAT function

■ ADSL

- **ADSL Firmware Version:** This is the DSL firmware version associated with your router
- **Line State:** This is the status of your ADSL link.
- **Modulation:** This field displays the ADSL modulation status for G.dmt or T1.413.
- **Annex Mode:** To show the router's type, e.g. Annex A, Annex B
- **SNR Margin:** To show the router's SNR margin for Downstream/Upstream
- **Line Attenuation:** To show the router's for Downstream/Upstream
- **Data Rate:** To show the router's data rate for Downstream/Upstream

4.6.2 System Log

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

The screenshot displays the web interface of a BILLION ADSL Modem/Router. The top navigation bar includes the following tabs: Status (selected), Quick Start, Interface Setup, Advanced Setup, Access Management, Maintenance, Status, and Help. Below the navigation bar, there are three sub-tabs: Device Info, System Log (selected), and Statistics. The main content area is titled "System Log" and contains a scrollable text box with the following log entries:

```
1/1/2000 0:18:54> Call Failed
1/1/2000 0:19:24> Call Failed
1/1/2000 0:19:34> MPOA Link Down
1/1/2000 0:19:34> mpoaChannDown: ch<0> null iface
1/1/2000 0:19:54> Call Failed
1/1/2000 0:39:14> No DNS server available
1/1/2000 0:39:14> Last errorlog repeat 10 Times
1/1/2000 0:39:14> adjTimeTask fail: no server
available
1/1/2000 0:39:14> adjtime task pause 60 seconds
1/1/2000 0:39:14> No DNS server available
1/1/2000 0:39:14> Last errorlog repeat 10 Times
1/1/2000 0:39:14> adjTimeTask fail: no server
available
1/1/2000 0:39:14> adjtime task pause 60 seconds
1/1/2000 0:39:14> No DNS server available
1/1/2000 0:39:14> Last errorlog repeat 10 Times
1/1/2000 0:39:14> adjTimeTask fail: no server
available
1/1/2000 0:39:14> adjtime task pause 1 day
```

At the bottom of the interface, there are two buttons: "CLEAR LOG" and "SAVE LOG".

4.6.3 Statistics

Read-only information here includes port status and packet specific statistics. Also provided are "Transmit Statistics" and "Receive Statistics".

Ethernet

The screenshot shows the BILLION ADSL Modem/Router web interface. The top navigation bar includes 'Quick Start', 'Interface Setup', 'Advanced Setup', 'Access Management', 'Maintenance', 'Status', and 'Help'. The 'Status' page is active, with sub-tabs for 'Device Info', 'System Log', and 'Statistics'. The 'Traffic Statistics' section is selected, showing the 'Interface' as 'Ethernet' (selected), 'ADSL', and 'WLAN'. Below this is a table with 'Transmit Statistics' and 'Receive Statistics' columns. A 'REFRESH' button is located at the bottom of the statistics area.

Transmit Statistics		Receive Statistics	
Transmit Frames	1852	Receive Frames	1555
Transmit Multicast Frames	2	Receive Multicast Frames	206
Transmit total Bytes	1694595	Receive total Bytes	259781
Transmit Collision	0	Receive CRC Errors	0
Transmit Error Frames	0	Receive Under-size Frames	0

- **Interface:** This field displays the type of port
- **Transmit Frames:** This field displays the number of frames transmitted in the last second.
- **Transmit Multicast Frames:** This field displays the number of multicast frames transmitted in the last second.
- **Transmit total Bytes:** This field displays the number of bytes transmitted in the last second.
- **Transmit Collision:** This is the number of collisions on this port.
- **Transmit Error Frames:** This field displays the number of error packets on this port.
- **Receive Frames:** This field displays the number of frames received in the last second.
- **Receive Multicast Frames:** This field displays the number of multicast frames received in the last second.
- **Receive total Bytes:** This field displays the number of bytes received in the last second.
- **Receive CRC Errors:** This field displays the number of error packets on this port.
- **Receive Under-size Frames:** This field displays the number of under-size frames received in the last second.

Press **REFRESH** to get the latest statistics.

ADSL



ADSL Modem/Router

Navigation menu: Quick Start, Interface Setup, Advanced Setup, Access Management, Maintenance, Status, Help

Sub-menu: Device Info, System Log, Statistics

Traffic Statistics

Interface: Ethernet ADSL WLAN

Transmit Statistics		Receive Statistics	
Transmit total PDUs	0	Receive total PDUs	0
Transmit total Error Counts	0	Receive total Error Counts	0

REFRESH

- **Transmit total PDUs:** This field displays the number of total PDU transmitted in the last second.
- **Transmit total Error Counts:** This field displays the number of total error transmitted in the last second.
- **Receive total PDUs:** This field displays the number of total PDU received in the last second.
- **Receive total Error Counts:** This field displays the number of total error received in the last second.

Press **REFRESH** to get the latest statistics.



Navigation menu: Quick Start, Interface Setup, Advanced Setup, Access Management, Maintenance, Status, Help

Sub-menu: Device Info, System Log, Statistics

Traffic Statistics

Interface: Ethernet ADSL WLAN

Transmit Statistics		Receive Statistics	
Tx Frames Count	652	Rx Frames Count	966
Tx Errors Count	374	Rx Errors Count	379
Tx Drops Count	374	Rx Drops Count	0

REFRESH

- **Tx Frames Count:** This field displays the number of frames transmitted in the last second.
- **Tx Errors Count:** This field displays the number of errors frames transmitted in the last second.
- **Tx Drops Count:** This field displays the number of drops frames transmitted in the last second.
- **Rx Frames Count:** This field displays the number of frames received in the last second.
- **Rx Errors Count:** This field displays the number of errors frames received in the last second.
- **Rx Drops Count:** This field displays the number of drops frames received in the last second.

Press **REFRESH** to get the latest statistics.

4.7 Help



ADSL Modem/Router

Help	Quick Start	Interface Setup	Advanced Setup	Access Management	Maintenance	Status	Help
Quick Start			<ul style="list-style-type: none">▶ Quick Start				
Interface Setup			<ul style="list-style-type: none">▶ Internet Settings▶ LAN Settings▶ Wireless LAN Settings				
Advanced Setup			<ul style="list-style-type: none">▶ Firewall▶ Routing▶ NAT▶ QoS▶ ADSL				
Access Management			<ul style="list-style-type: none">▶ ACL▶ IP Filter▶ SNMP▶ UPnP▶ DDNS				
Maintenance			<ul style="list-style-type: none">▶ Administration▶ Time Zone▶ Firmware▶ SysRestart▶ Diagnostics				
Status			<ul style="list-style-type: none">▶ Device Info▶ System Log▶ Statistics				

This help page provides you some useful messages such as the introductions of some concepts and some guides.

When some problems are encountered, you can turn to this page for help.

For example, if you don't understand what is Quick Start, you can go to this page, click on Quick Start, then you'll see some messages about it, and understand it quickly. This function provides you an easy way to help yourself.

Chapter 5

Troubleshooting

If the ADSL2+ Router is not functioning properly, you can refer first to this chapter for simple troubleshooting before contacting your service provider. This could save your time and effort but if the symptoms persist, then consult your service provider.

Problems with starting up the router

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

Problems with the WAN Interface

Problem	Corrective Action
Initialization of the PVC connection (“line sync”) 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 GE. If you still have problems, you may need to verify these settings with your ISP.
Frequent loss of ADSL line sync (disconnections).	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.

Problems with the LAN Interface

Problem	Corrective Action
Can't ping any PCs on the LAN.	Check the Ethernet LEDs on the front panel. The LED should be on for a port that has a PC connected. If it is off, check the cables between your router and the PC. Make sure you have uninstalled any software firewall for troubleshooting.
	Verify that the IP address and the subnet mask are consistent between the router and the workstations.

Product Support and Contact Information

Most problems can be solved by referring to the **Troubleshooting** section in the User's Manual. If you cannot resolve the problem with the **Troubleshooting** chapter, please contact the dealer where you purchased this product.

Contact Billion

WORLDWIDE

<http://www.billion.com>

MAC OS is a registered Trademark of Apple Computer, Inc.

Windows 7/98, Windows NT, Windows 2000, Windows Me, Windows XP and Windows Vista are registered Trademarks of Microsoft Corporation.