



BiPAC 7300W

Wireless-N ADSL2+ Firewall Router

User Manual

Version Released: 1.02 (FW: v2.01.RC1)

Last Revised on April 14, 2010

Table of Contents

Chapter 1	1
1.1 Introducing the BiPAC 7300W	1
1.2 Features	3
1.3 Hardware Specifications	7
1.3 Applications of the BiPAC 7300W	8
Chapter 2	9
2.1 Important Notes	9
2.2 Package Contents	10
2.3 The Front LEDs	11
2.4 The Rear Ports	12
2.5 Cabling	14
Chapter 3	15
3.1 Before Configuration.....	15
3.2 Network Configuration	16
3.2.1 Configuring a PC in Windows 7	16
3.2.2 Configuring a PC in Windows Vista	18
3.2.3 Configuring a PC in Windows XP	20
3.2.4 Configuring a PC in Windows 2000	21
3.2.5 Configuring PC in Windows 98/Me	22
3.2.6 Configuring PC in Windows NT4.0	23
3.3 Factory Default Settings	24
3.4 LAN and WAN Port Addresses	25
3.5 Information from your ISP	25
3.6 Configuring with your BiPAC 7300W	26
Chapter 4	30
4.2 Quick Start	32
4.3 WAN	33
4.4 WLAN	34
Chapter 5	40
5.1 Status	41
5.1.1 ADSL Status.....	43
5.1.2 ARP Table	44
5.1.3 DHCP Table	44
5.1.4 System Log.....	45
5.1.5 Firewall Log	46
5.1.6 UPnP Portmap.....	46
5.2 Quick Start	47
5.3 Configuration	52
5.3.1 LAN (Local Area Network)	52
5.3.1.1 Ethernet.....	52
5.3.1.2 IP Alias	53
5.3.1.3 Wireless.....	54
5.3.1.4 Wireless Security.....	57
5.3.1.5 WPS	61
5.3.1.6 DHCP Server.....	74

5.3.2 WAN (Wide Area Network)	76
5.3.2.1 WAN Profile	77
5.3.2.3 ADSL Mode	86
5.3.3 System	87
5.3.3.1 Time Zone	88
5.3.3.2 Firmware Upgrade.....	89
5.3.3.3 Backup / Restore.....	90
5.3.3.4 Restart Router	91
5.3.3.5 User Management.....	91
5.3.3.6 Mail Alert.....	92
5.3.4 Firewall	93
5.3.4.1 Packet Filter	95
5.3.4.2 MAC Filter	97
5.3.4.3 Intrusion Detection.....	98
5.3.4.4 Block WAN PING.....	100
5.3.4.5 URL Filter	100
5.3.5 QoS (Quality of Service).....	103
5.3.6 Virtual Server.....	109
5.3.6.1 Port Mapping	111
5.3.6.2 DMZ.....	113
5.3.6.3 ALG	114
5.3.7 Wake on LAN.....	115
5.3.8 Time Schedule.....	116
5.3.9 Advanced.....	117
5.3.9.1 Static Route	118
5.3.9.2 Static ARP	118
5.3.9.3 Dynamic DNS.....	119
5.3.9.4 VLAN	120
5.3.9.5 Device Management.....	121
5.3.9.6 IGMP	128
5.3.9.7 SNMP Access Control	128
5.3.9.8 Remote Access	131
5.4 Save Configuration to Flash	132
5.5 Restart.....	132
5.6 Logout	133
Chapter 6.....	134
Problems starting up the router	134
Problems with the WAN Interface.....	134
Problems with the LAN Interface	135
APPENDIX.....	136

Chapter 1

Introduction

1.1 Introducing the BiPAC 7300W

The BiPAC 7300W is an economical ADSL2+ router ideal for Home and SOHO users to have an improved wireless access 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 7300W 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 7300W 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!

High speed Access

Complying with worldwide ADSL standards, the BiPAC 7300W 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. The BiPAC 7300W 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 a Wireless-N Access Point that supports up to 150Mbps wireless data rate, the BiPAC 7300W is truly an upgrade Wireless LAN solution compared to your existing 802.11b/g standard. With all these technologies, users can enjoy high-speed access for broadband multimedia applications such as interactive gaming, video streaming and real-time audios that run faster and easier than ever.

Multiple Options for Internet Access

Among 4 Ethernet ports, the port 1 can be configured as WAN port for connecting a to ADSL/Cable/VDSL/Fiber modem device, providing more options for users to access

Internet. So the SOHO or small office users can even deploy the BiPAC 7300W for FTTx (Fiber-to-the-building, noed, or home) applications over a VDSL or Fiber device connected.

Rich Security

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. 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.

Ease of Set up and Management

Easy Sign-ON (EZSO), WPS push button and Auto-scan ADSL settings allow users to manage the device functions without too much effort! The user-friendly, web-based user interface makes installing and managing the BiPAC 7300W 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.

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 Setup (WPS), Wi-Fi Protected Access (WPA-PSK/ WPA2-PSK) and Wired Equivalent Privacy (WEP) support
- Wireless On/Off time schedule control
- High speed Internet access with ADSL2/2+; backward compatible with ADSL
- Integrated with 4-port Ethernet switch, one port can be configured to WAN port for connecting to ADSL/Cable/VDSL/Fiber modem device
- 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 Sign-ON (EZSO)

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 7300WA 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 7300WA model only)

Network Protocols and Features

- NAT, static routing and RIP-1/2
- Universal Plug and Play (UPnP) Compliant
- Transparent Bridging
- Dynamic Domain Name System (DDNS)
- Virtual Server and DMZ
- SNTP, DNS relay and IGMP proxy
- IGMP snooping for video service
- Management based-on IP protocol, port number and address
- SMTP Client

Firewall & Virtual Private Network(VPN)

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

Quality of Service Control

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

Wireless LAN

- Base on Wireless-N Technology, and compliant with IEEE 802.11g, 802.11b standards
- Up to 150Mbps wireless operation rate
- 2.4 GHz–2.484 GHz frequency range
- WPS (Wi-Fi Protected Setup)
- 64/128 bits WEP supported for encryption
- Wireless Security with WPA-PSK/ WPA2-PSK support
- 802.1x radius supported
- WDS repeater function support
- WLAN on/off time schedule control

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)
- Classical IP over ATM (RFC 1577)
- MAC Encapsulated Routing (RFC 1483 MER)
- OAM F4/F5
- ATM QoS: UBR, CBR, VBR-rt, VBR-nrt

Management

- Easy Sign-ON (EZSO) and Auto-scan ADSL settings
- Web-based GUI for remote and local management
- Firmware upgrades and configuration data upload/download via web-based interface
- Embedded Telnet server for remote and local management
- Available syslog
- Supports DHCP server/client/relay
- SNMP v1/v2, MIB supported
- Wake on LAN
- Mail Alert for WAN IP changed



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

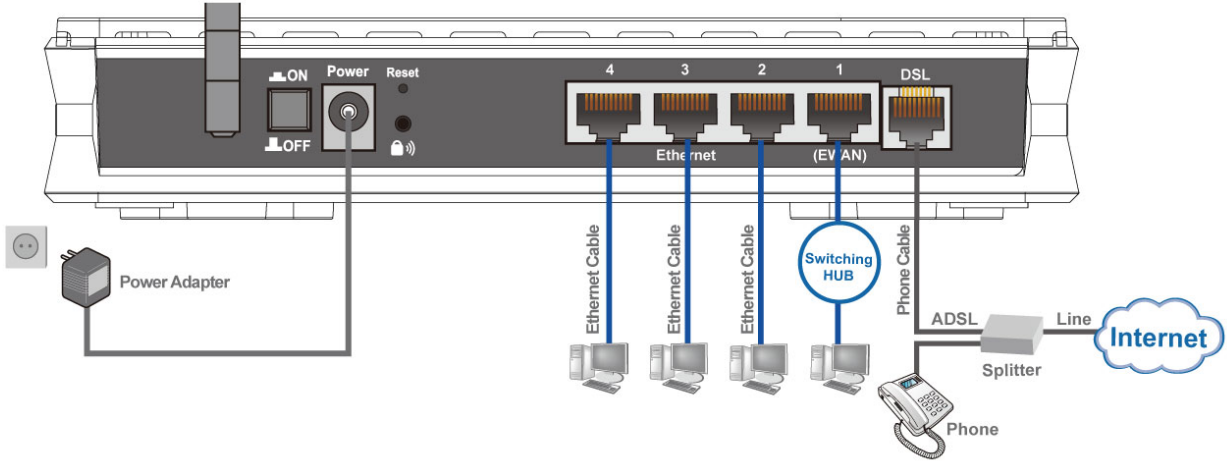
1.3 Hardware Specifications

Physical Interface

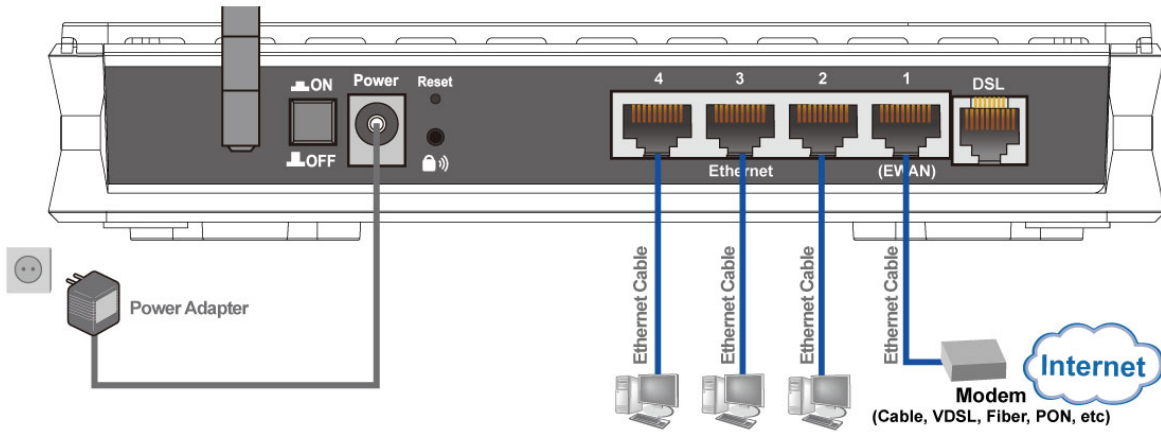
- DSL: ADSL port
- EWAN: Ethernet port #1 can be configured to WAN port for connecting to ADSL/Cable/VDSL/Fiber modem device
- Ethernet: 4-port 10/100M auto-crossover (MDI/MDI-X) switch
- Factory default reset button
- WPS push button
- Power jack
- Power switch
- WLAN: 1 antenna

1.3 Applications of the BiPAC 7300W

ADSL Router Mode



Broadband Router Mode



Chapter 2

Product Overview

2.1 Important Notes



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.

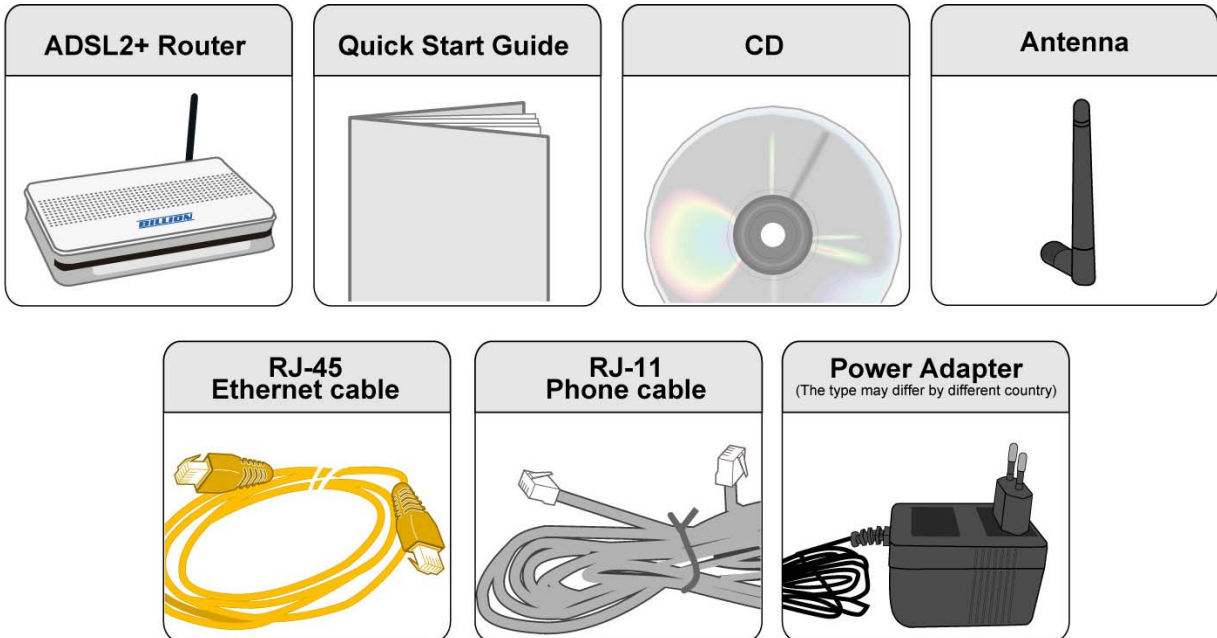


Attention

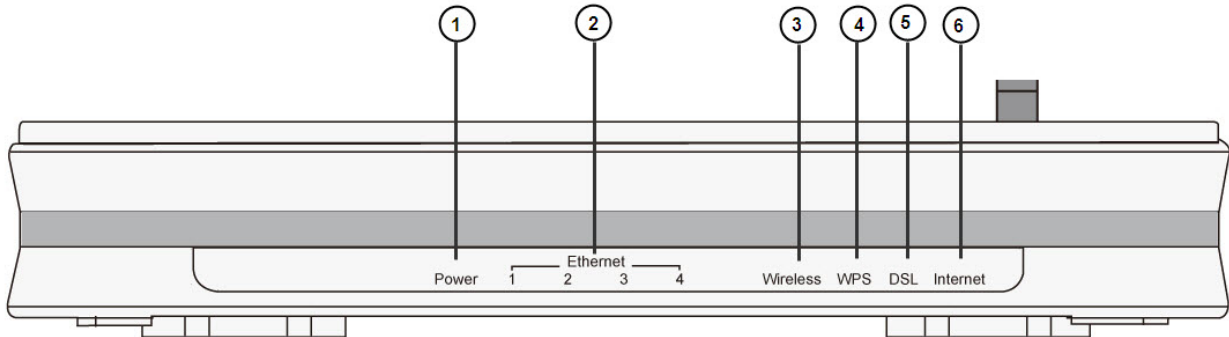
- ✓ Place the router on a stable surface.
- ✓ Only use the power adapter that comes with the package. Using a different voltage rating power adaptor may damage the router.

2.2 Package Contents

- BiPAC 7300W Wireless-N ADSL2+ Firewall Router
- CD-ROM containing the online manual
- RJ-11 ADSL/telephone Cable (1.8M)
- Ethernet (CAT-5 LAN) Cable (1.8M Straight)
- Power Adapter (12V DC, 1A)
- Quick Start Guide (105*150 mm)
- Antennas (1 pcs)

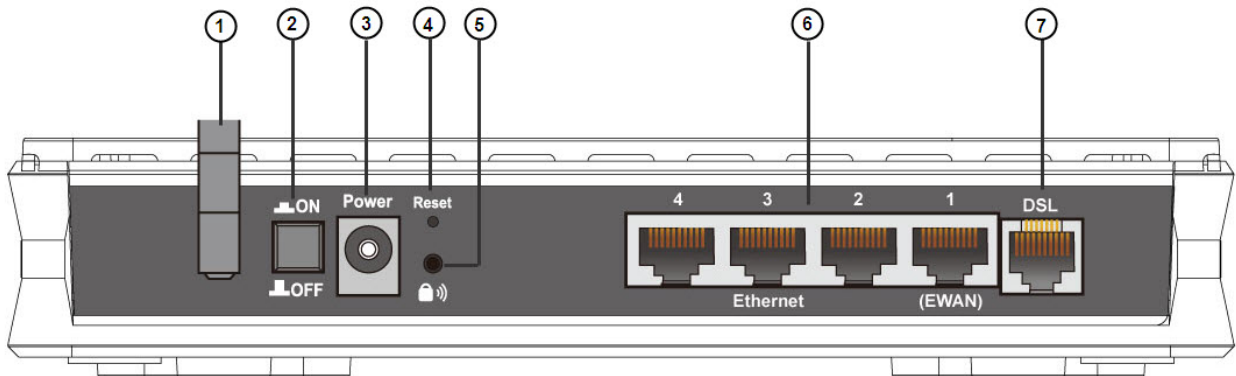


2.3 The Front LEDs



LED		Meaning
1	Power	Lit red while the flash is damage and cannot bring the system up. Lit green when the system is ready. Flashes green when the the system is rebooting or firmware upgrading.
2	Ethernet Port 1 - 4	Lit when connected to an Ethernet device. Green for 100Mbps; Orange for 10Mbps. Blinking when data is Transmitted / Received.
3	Wireless	Lit green when the wireless connection is established. Flashes when sending/receiving data.
4	WPS	Blinking when WPS is in progress.
5	DSL	Lit green when successfully connected to an ADSL DSLAM ("linesync").
6	Internet	Lit red when WAN port fails to get IP address. Lit green when WAN port gets IP address successfully.

2.4 The Rear Ports



Port		Description
1	Antenna	Connect the antenna to this port.
2	ON/OFF	Power ON/OFF switch.
3	Power	Connect the supplied power adapter to this jack.
4	Reset	<p>After the router is powered on, press this reset button using the end of paper clip or other small pointed object for 6 seconds and above to restore it to factory default settings.</p> <ol style="list-style-type: none"> 1. Recovery procedures for non-working routers (e.g. after a failed firmware upgrade flash). 2. Recovery procedures for a lost web interface password.
5	WPS	<p>Press the WPS button according to the following two to achieve different functions.</p> <p>2-5 seconds: start WPS.</p> <p>5 seconds above: switch to enable/disable WLAN.</p>
6	Ethernet	<p>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.</p> <p>Note: Only Ethernet port 1 can be used for EWAN.</p>
7	DSL	Connect the supplied RJ-11 (“telephone”) cable to this port when connecting to the ADSL/telephone network.

● The detail instruction in Reset Button

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

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



Before powering on the router to enter the recovery process, please configure the IP address of the PC as **192.168.0.100** and proceed with the following step by step guide.

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

2.5 Cabling

One of the most common causes of problems is because of bad cabling or ADSL line(s). Make sure that all connected devices are turned on. On the front of the product is a bank of LEDs. Verify that the LAN Link and ADSL line LEDs are lit. If they are not, verify that you are using the proper cables.

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

Chapter 3

Installation

You can configure the BiPAC 7300W router through the convenient and user-friendly interface of a web browser. Most popular operating systems such as Linux and Windows 7/Vista/98/NT/2000/XP/Me include a web browser as a standard application.

3.1 Before Configuration

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

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



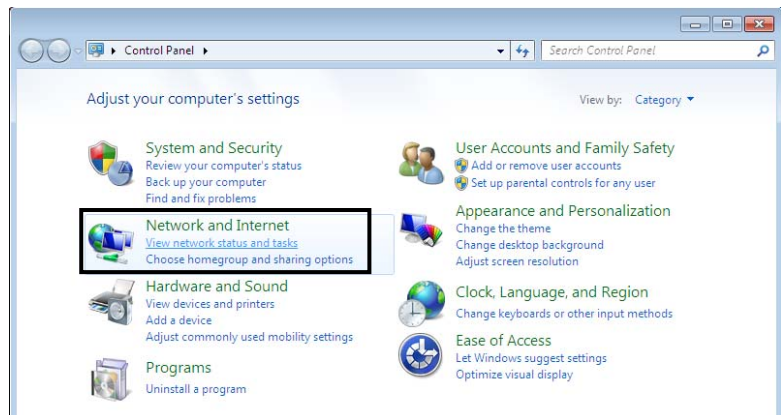
Any TCP/IP capable workstation can be used to communicate with or through the BiPAC 7300W. To configure other types of workstations, please consult the manufacturer's documentation.

3.2 Network Configuration

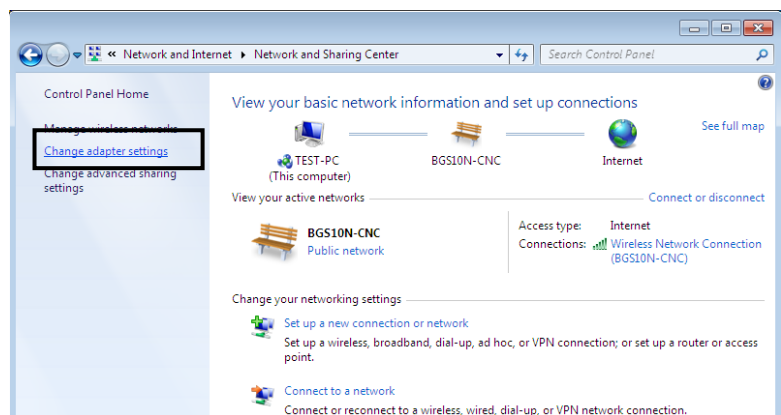
3.2.1 Configuring a PC in Windows 7

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

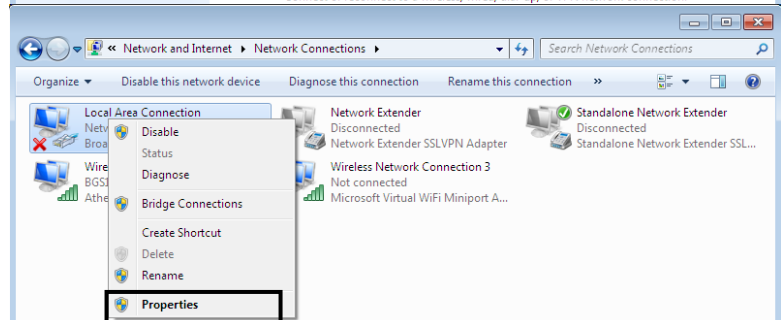
Then click on **Network and Internet**.



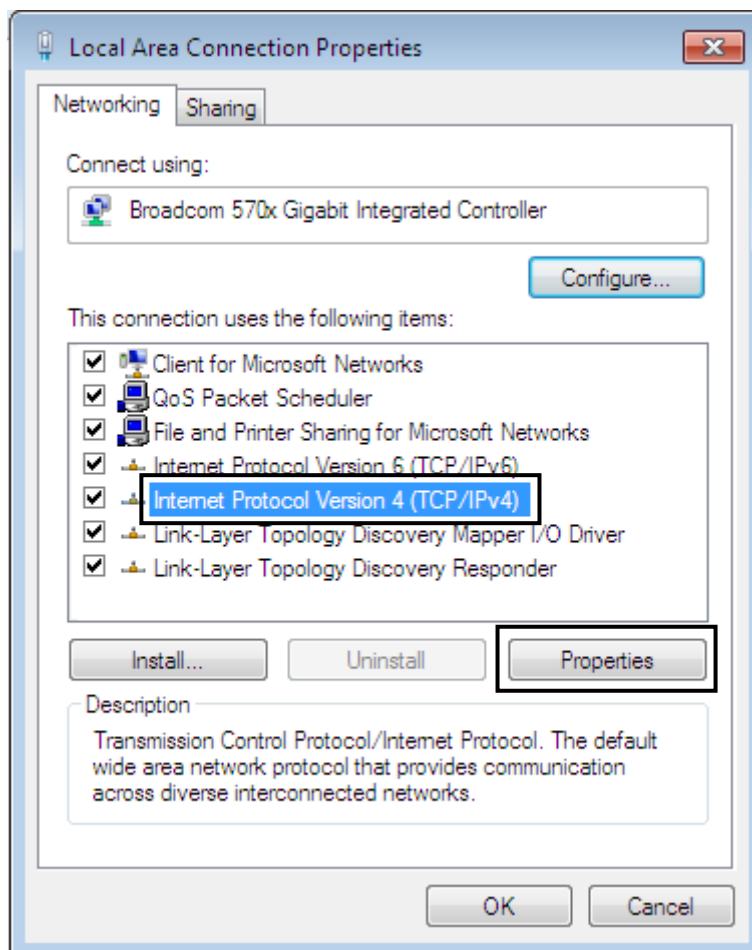
2. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.



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

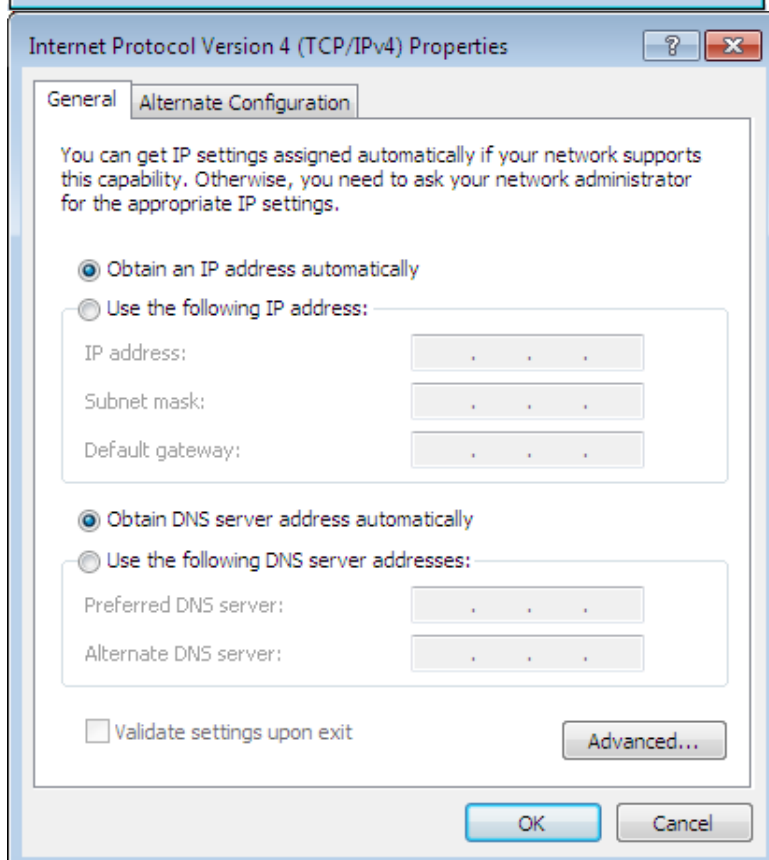


4. Select **Internet Protocol Version 4 (TCP/IPv4)** then click **Properties**.



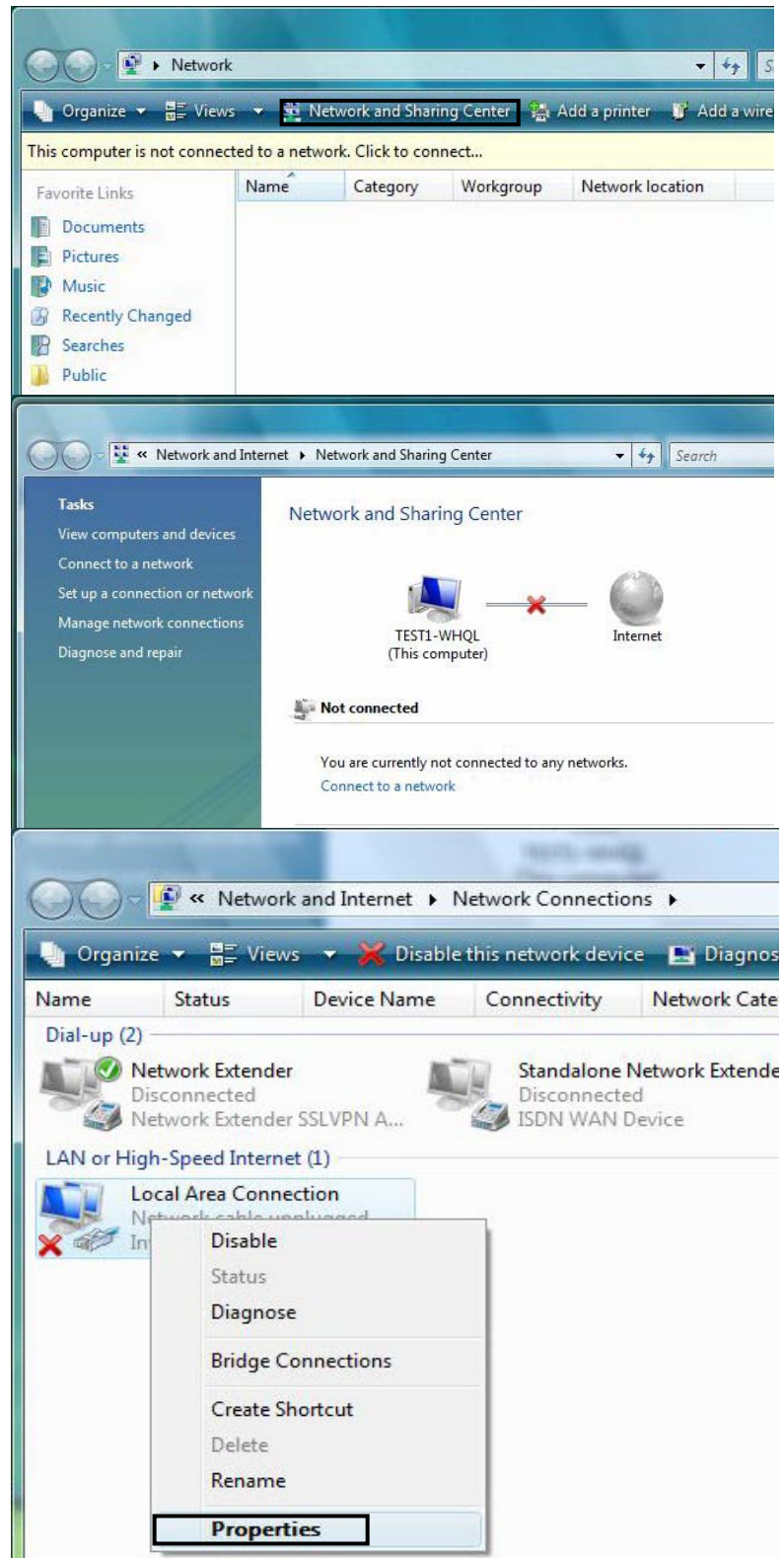
5. In the **TCP/IPv4 properties** window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

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

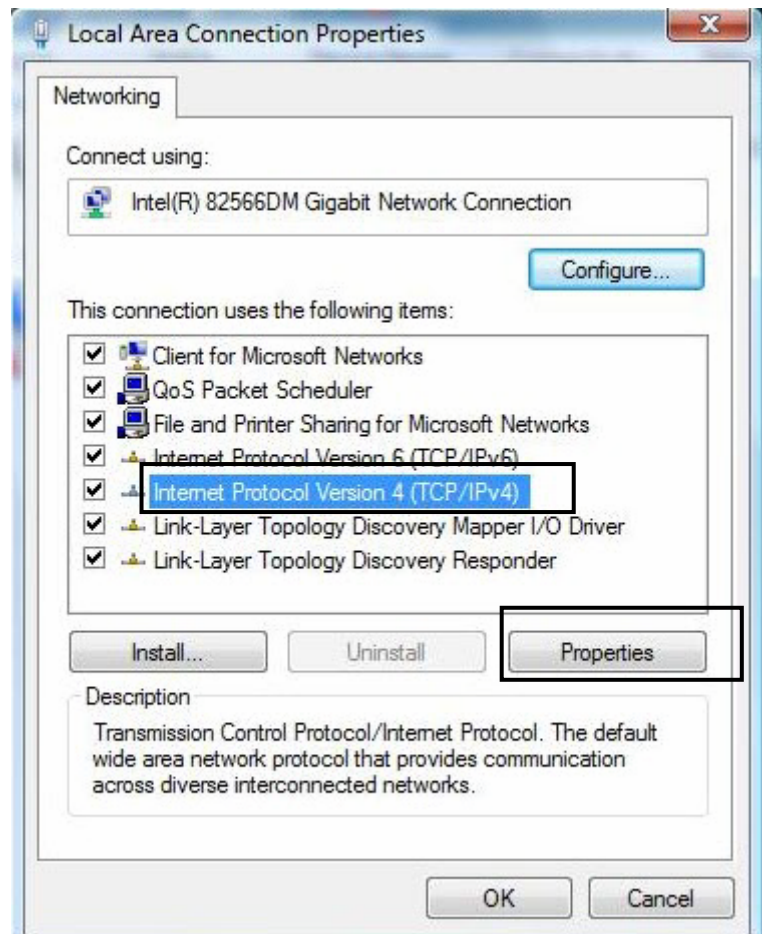


3.2.2 Configuring a PC in Windows Vista

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

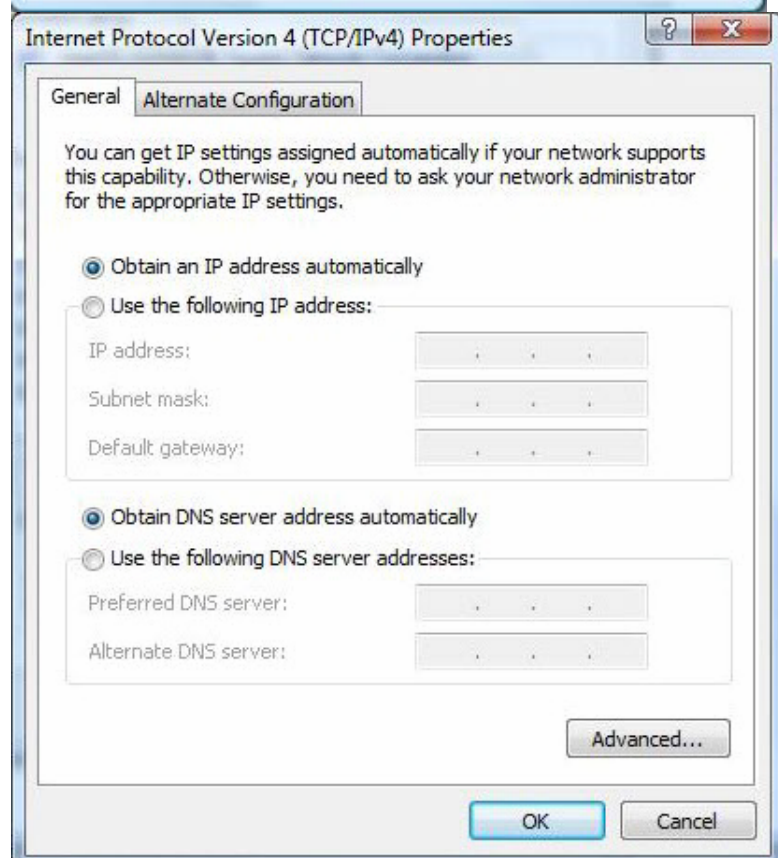


5. Select **Internet Protocol Version 4 (TCP/IPv4)** then click **Properties**.



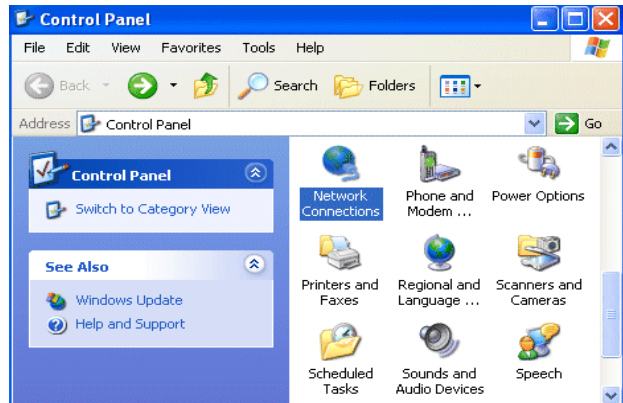
6. In the **TCP/IPv4 properties** window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

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

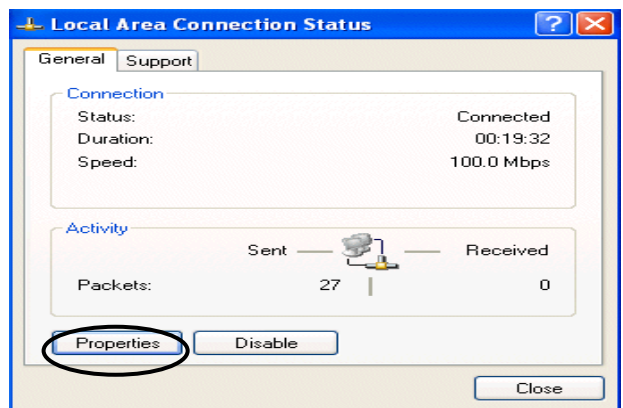


3.2.3 Configuring a PC in Windows XP

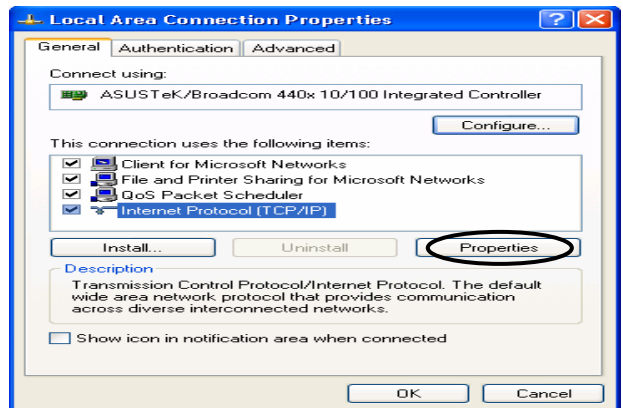
1. Go to **Start / Control Panel (in Classic View)**. In the Control Panel, double-click on **Network Connections**
2. Double-click **Local Area Connection**.



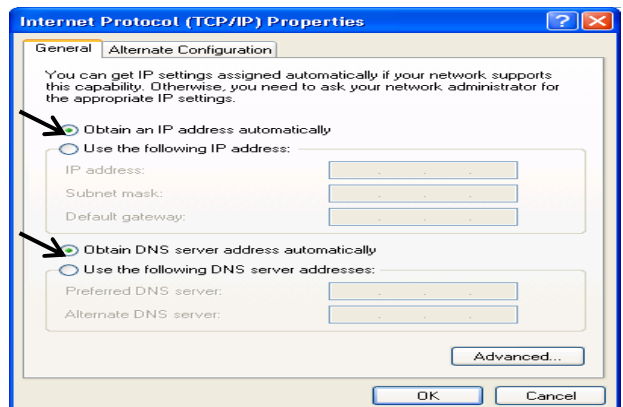
3. In the **Local Area Connection Status** window, click **Properties**.



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



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

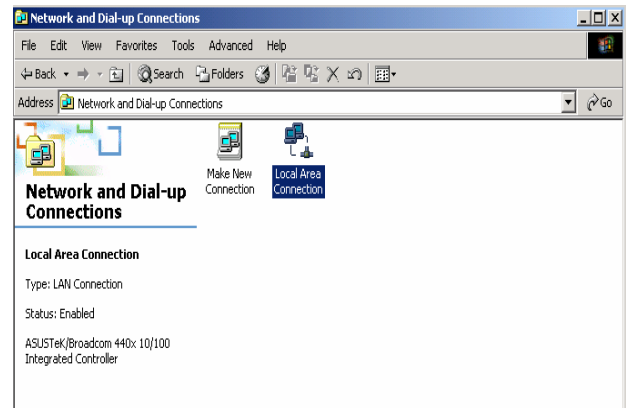


6. Click **OK** to finish the configuration.

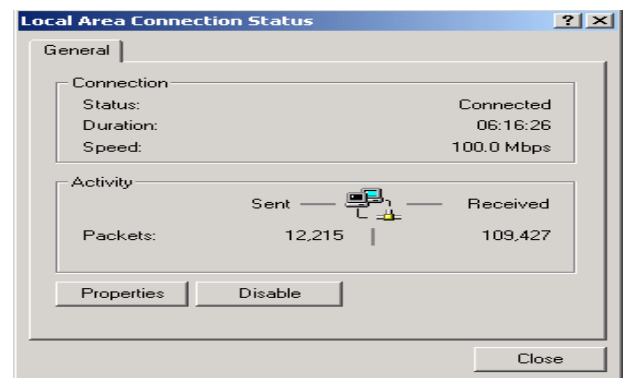
3.2.4 Configuring a PC in Windows 2000

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

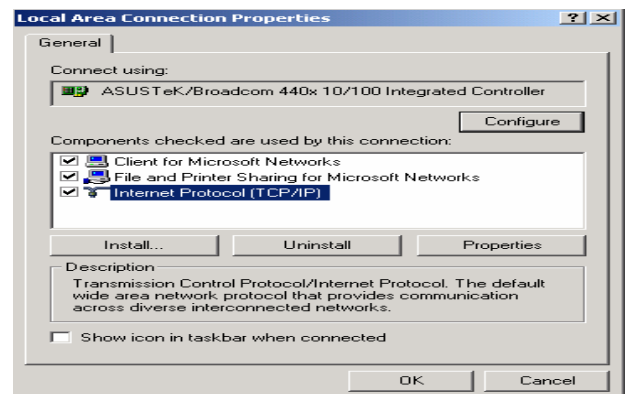
2. Double-click **Local Area Connection**.



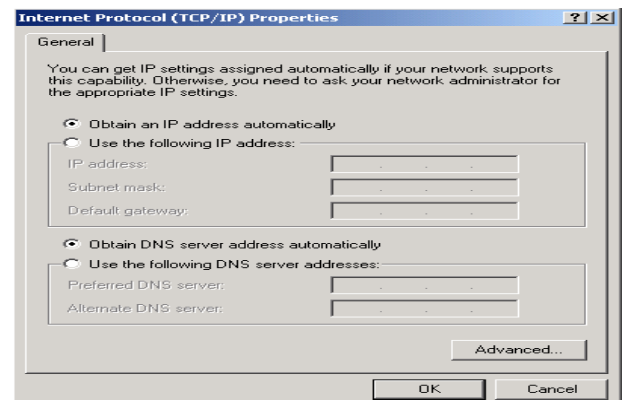
3. In the **Local Area Connection Status** window click **Properties**.



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



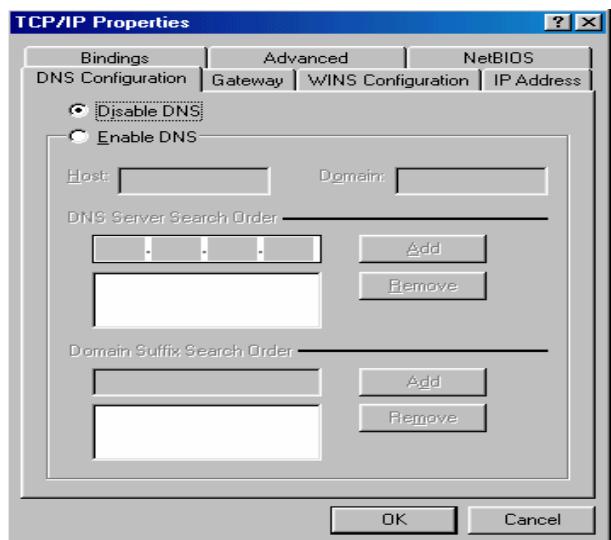
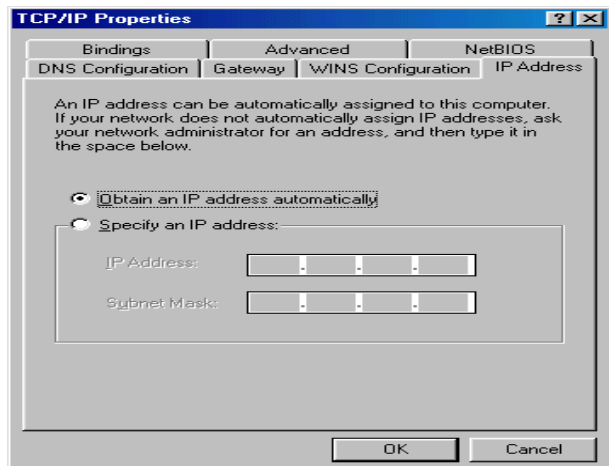
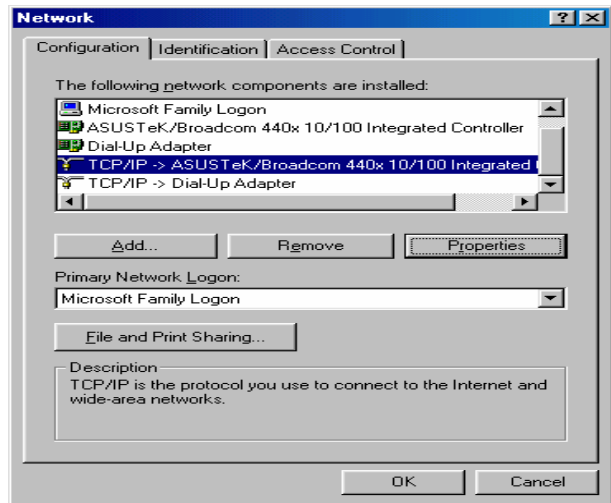
5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.



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

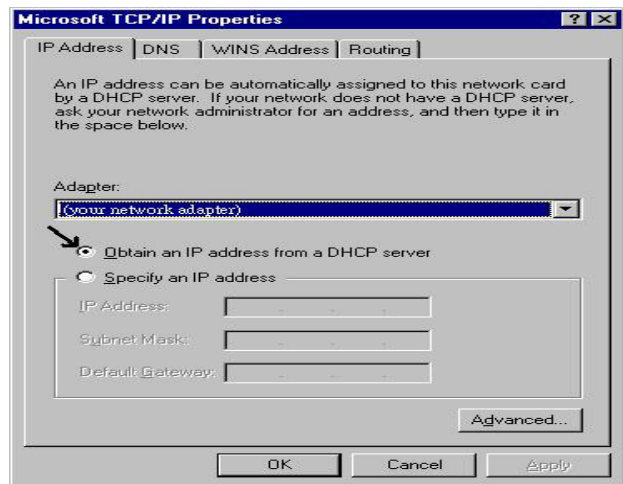
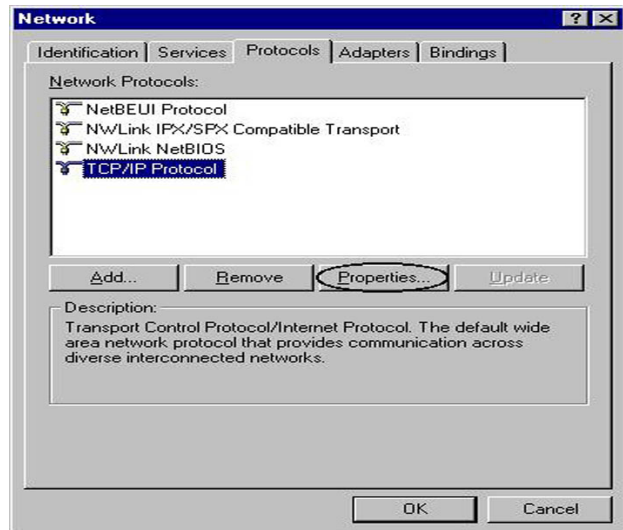
3.2.5 Configuring PC in Windows 98/Me

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.



3.2.6 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**.



3.3 Factory Default Settings

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

● Web Interface: (Username and Password)

- ✘ Username: admin
- ✘ Password: admin

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



Attention

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

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

● LAN Device IP Settings:

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

● ISP setting in WAN site:

- ✘ PPPoE

● DHCP Server:

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

3.4 LAN and WAN Port Addresses

The parameters of LAN and WAN ports are preset 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 in ports 1, 2, 3 and 4	
IP addresses for distribution to PCs	100 IP addresses continuing from 192.168.1.100 through 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 services are provided, such as PPPoE, PPPoA, MPoA or Pure Bridge.

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

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

3.6 Configuring with your BiPAC 7300W



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

Easy Sign On

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

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

1. Click continue.

Easy Sign On

WAN Port (WAN > Wireless)

Select WAN Port

Connect Mode: ADSL (Recommended)

Protocol: PPPoE (RFC2516, PPP over Ethernet)

VPI / VCI: 8 / 35

Username: Username

IP Address: Obtain an IP Address Automatically

Continue Jump to Wireless setting Done

2. Choose "Auto" or "Manually" to scan ADSL information.

Easy Sign On

WAN Port (WAN > Wireless)

ADSL Line Is Ready.

Auto scan: Auto Manually

Continue

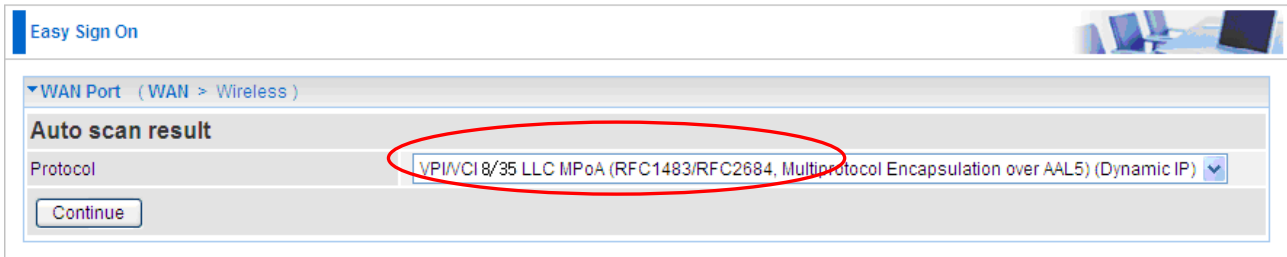
Easy Sign On

WAN Port (WAN > Wireless)

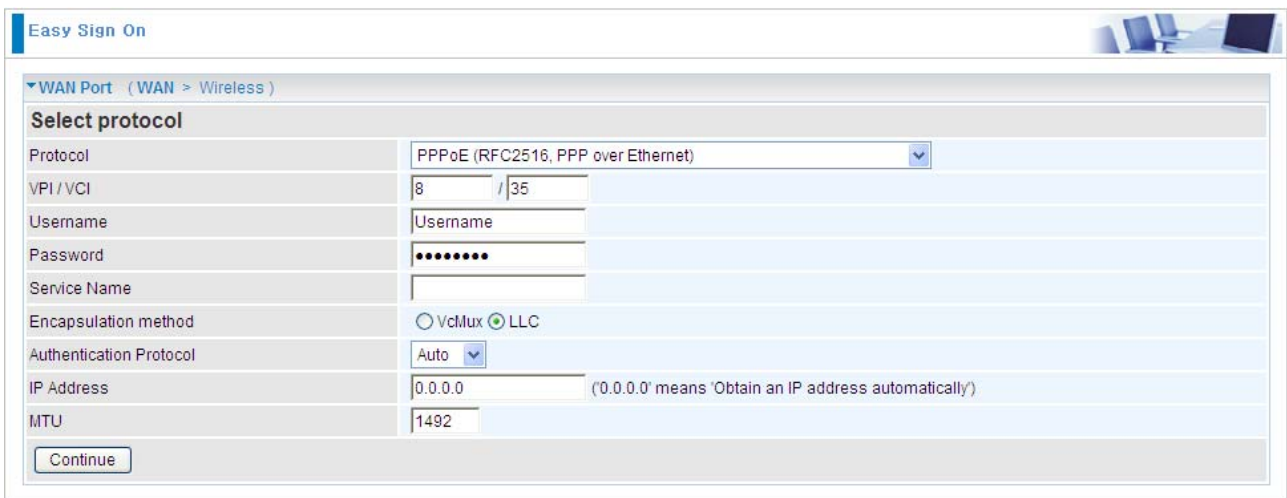
Please wait while the ADSL is scanning.

Abort to manually setting

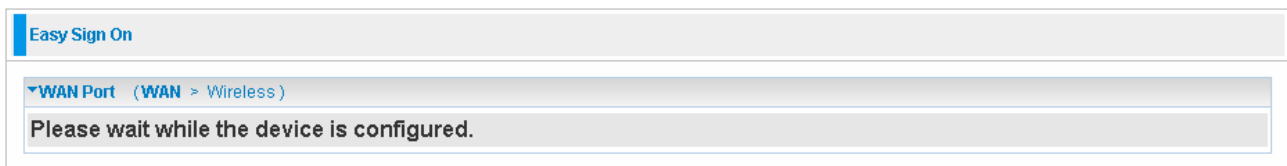
3. Show Auto scan result - Protocol information.



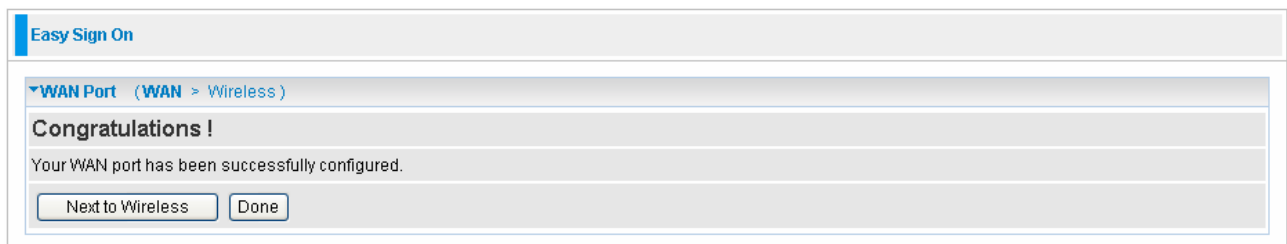
4. Please enter “Username” and “Password” as supplied by your ISP (Internet Service Provider) and click continue.



5. Wait for the device to be configured.



6. You've have completed the WAN port setup and now click “Next to Wireless” to proceed to the wireless configuration.



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

The screenshot shows the 'Easy Sign On' interface. At the top, there is a blue header with the text 'Easy Sign On'. Below this, a navigation bar shows 'Wireless (WAN > Wireless)'. The main section is titled 'Set Wireless configuration.' and contains the following fields:

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

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

8. Save Configuration.

The screenshot shows the 'Easy Sign On' interface. At the top, there is a blue header with the text 'Easy Sign On'. Below this, a navigation bar shows 'Save configuration'. The main section contains the text: 'Save configuration to FLASH. Please wait for 10 seconds'.

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

The screenshot shows the 'Easy Sign On' interface. At the top, there is a blue header with the text 'Easy Sign On'. Below this, a navigation bar shows 'Process finished'. The main section contains the text: 'Success. The Easy-Sign-On process is finished. Your device has been successfully configured.'

Web Configuration

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



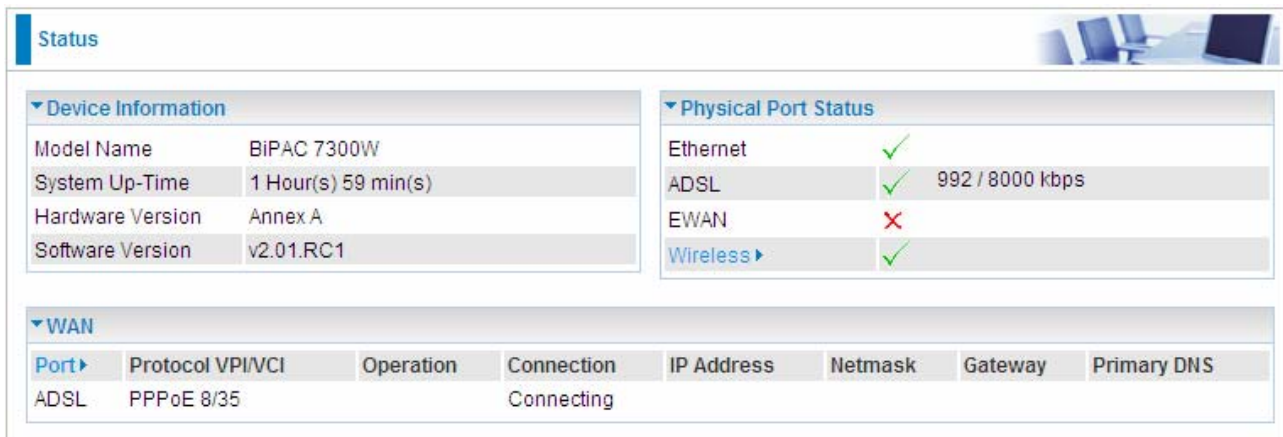
Congratulations! You have successfully logged on to your BiPAC 7300W Router!

Chapter 4

Basic Configuration

Once you have logged on to your BiPAC 7300W Router via your web browser, you can begin to set it up according to your requirements. On the configuration homepage, the left navigation pane links you directly to the setup pages, which include:

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



The screenshot displays the 'Status' page of the BiPAC 7300W Router. It is divided into three main sections: Device Information, Physical Port Status, and WAN.

Device Information:

Model Name	BiPAC 7300W
System Up-Time	1 Hour(s) 59 min(s)
Hardware Version	Annex A
Software Version	v2.01.RC1

Physical Port Status:

Ethernet	✓	
ADSL	✓	992 / 8000 kbps
EWAN	✗	
Wireless ▶	✓	

WAN:

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

4.1 Status

Status							
▼ Device Information				▼ Physical Port Status			
Model Name	BIPAC 7300W			Ethernet	✓		
System Up-Time	1 Hour(s) 59 min(s)			ADSL	✓ 992 / 8000 kbps		
Hardware Version	Annex A			EWAN	✗		
Software Version	v2.01.RC1			Wireless ▶	✓		
▼ WAN							
Port ▶	Protocol VPI/VCI	Operation	Connection	IP Address	Netmask	Gateway	Primary DNS
ADSL	PPPoE 8/35		Connecting				

Device Information

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

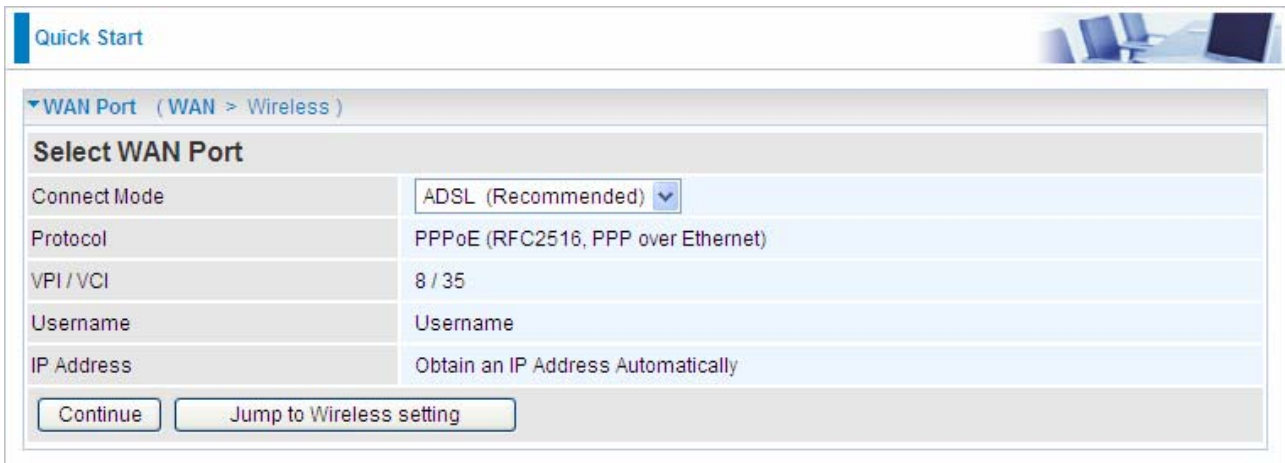
Physical Port Status

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

WAN

- **Port:** Name of the WAN connection.
- **Protocol VPI/VCI:** Virtual Path Identifier and Virtual Channel Identifier
- **Operation:** Current available operation.
- **Connection:** The current connection status.
- **IP Address:** WAN port IP address.
- **Net mask:** WAN port IP subnet mask.
- **Gateway:** The IP address of the default gateway.
- **Primary DNS:** The IP address of the primary DNS server.

4.2 Quick Start



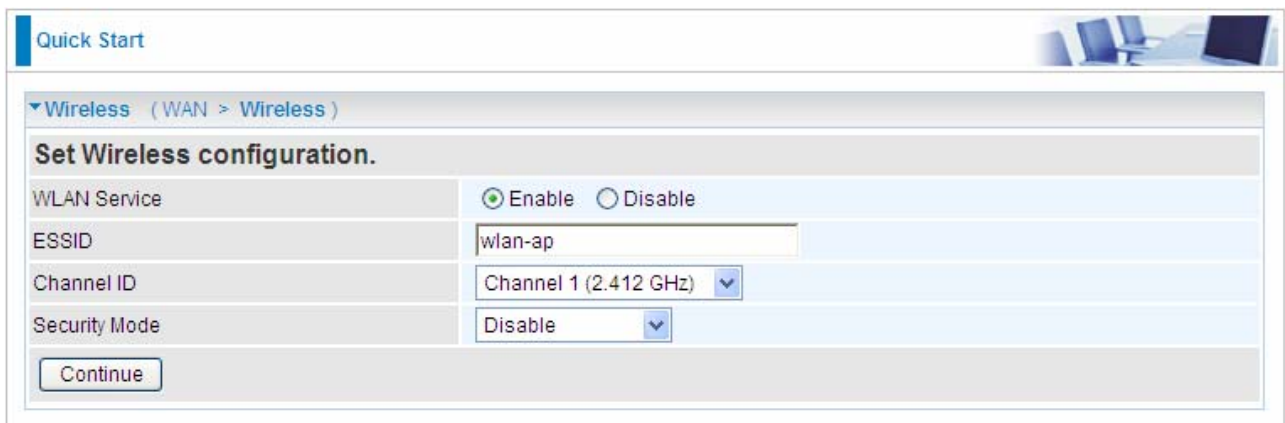
The screenshot shows the 'Quick Start' configuration page for WAN Port settings. The page title is 'Quick Start' and the breadcrumb is '(WAN > Wireless)'. The main heading is 'Select WAN Port'. The configuration fields are as follows:

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

At the bottom, there are two buttons: 'Continue' and 'Jump to Wireless setting'.

For the exactly steps, turn to **Advanced –Quick Start** on page 47 for help.

■ Set Wireless configuration



The screenshot shows the 'Quick Start' configuration page for Wireless settings. The page title is 'Quick Start' and the breadcrumb is '(WAN > Wireless)'. The main heading is 'Set Wireless configuration.'. The configuration fields are as follows:

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

At the bottom, there is a 'Continue' button.

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

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

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

● **Security Mode:** You can disable or enable with WPA or WEP for protecting wireless network. The default mode of wireless security is **Disable**. For more information , turn to page 35-37 for help.

4.3 WAN

Configuration

▼ WAN Port

WAN Connection

Main Port: ADSL (Current Main Port: ADSL)

Parameters

Protocol: PPPoE (RFC2516, PPP over Ethernet)

VPI/VCI: 8 / 35

Username: Username

Password: ●●●●●●

Service Name:

Encap. method: VcMux LLC

Auth. Protocol: Auto

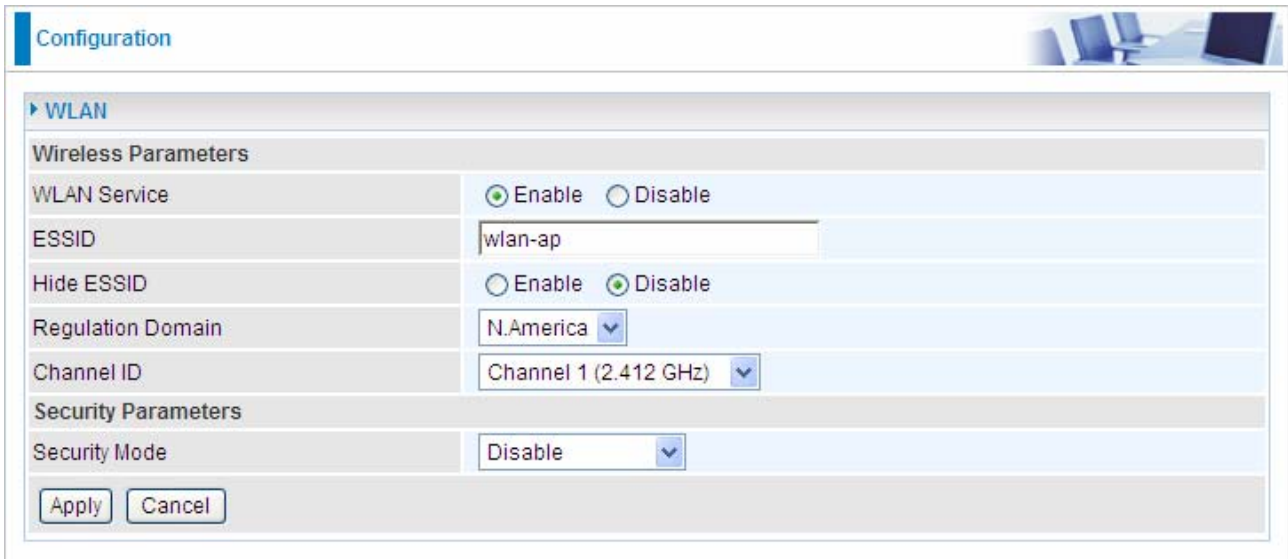
IP Address: 0.0.0.0 (0.0.0.0 means 'Obtain an IP address automatically')

MTU: 1492

Apply

- **Main Port:** Select the connection mode from the drop-down menu, ADSL or EWAN.
- **VPI/VCI:** Enter the VPI and VCI information provided by your ISP.
- **Username:** Enter the username provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive). This is in the format of “username@ispname” instead of simply “username”.
- **Password:** Enter the password provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive)
- **Service Name:** This item is for identification purposes. If it is required, your ISP provides you the information. Maximum input is **15** alphanumeric characters.
- **Encap. method:** Select the encapsulation format, the default is LLC. Select the one provided by your ISP
- **Auth. Protocol:** Default is **Auto**. Your ISP advises on using **Chap** or **Pap**.
- **IP Address:** Your WAN IP address. Leave this at 0.0.0.0 to automatically obtain an IP address from your ISP.
- **MTU:** Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

4.4 WLAN



The screenshot shows a configuration window titled "Configuration" with a "WLAN" section. Under "Wireless Parameters", the "WLAN Service" is set to "Enable" (radio button selected), "ESSID" is "wlan-ap", "Hide ESSID" is "Disable" (radio button selected), "Regulation Domain" is "N.America", and "Channel ID" is "Channel 1 (2.412 GHz)". Under "Security Parameters", the "Security Mode" is set to "Disable". "Apply" and "Cancel" buttons are at the bottom.

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

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

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

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

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

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

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

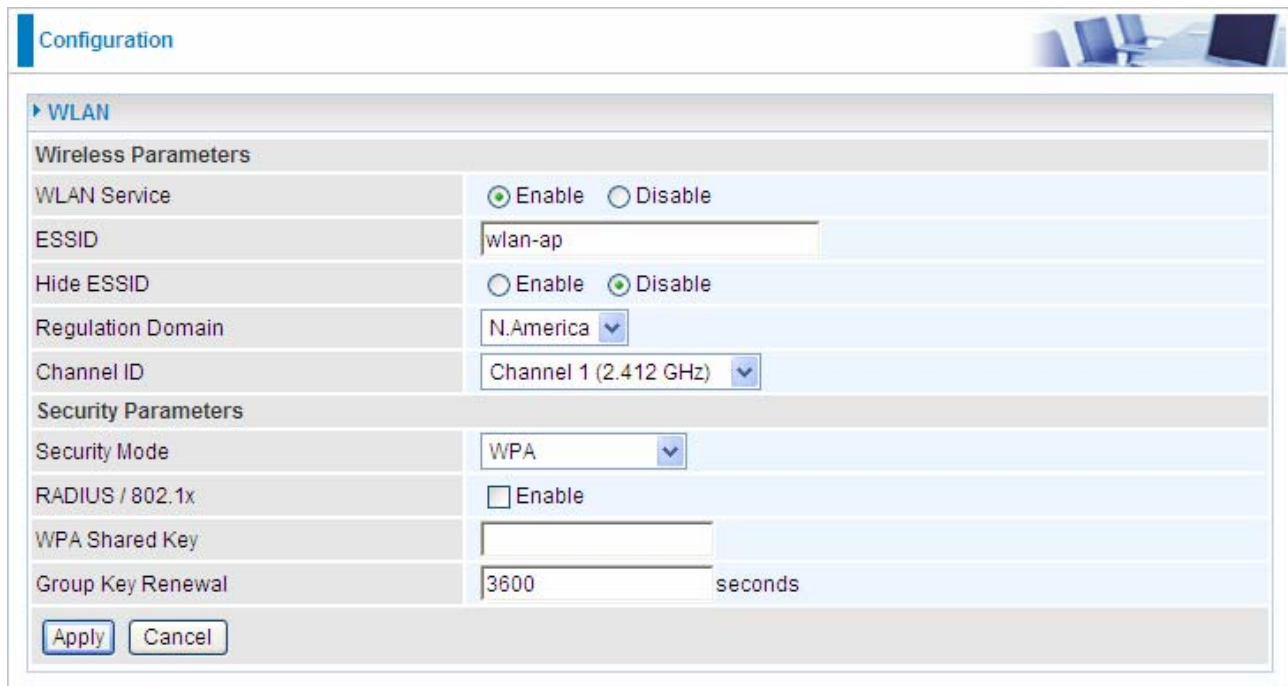
● **Channel ID:** Select the ID channel that you would like to use.

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

Security Parameters

● WPA or WPA2

WPA and WPA2 pre-shared keys are an authentication mechanism in which users provide some form of credentials to verify that they should be allowed access to a network. This requires a single password entered into each WLAN node (Access Points, Wireless Routers, client adapters, bridges). As long as the passwords match, a client will be granted access to a WLAN.



The screenshot shows a configuration page for WLAN settings. The page is titled "Configuration" and has a "WLAN" section. Under "Wireless Parameters", the "WLAN Service" is set to "Enable" (radio button selected). The "ESSID" is "wlan-ap", "Hide ESSID" is "Disable" (radio button selected), "Regulation Domain" is "N.America", and "Channel ID" is "Channel 1 (2.412 GHz)". Under "Security Parameters", the "Security Mode" is "WPA", "RADIUS / 802.1x" is "Enable" (checkbox unchecked), "WPA Shared Key" is empty, and "Group Key Renewal" is "3600 seconds". There are "Apply" and "Cancel" buttons at the bottom.

● **WLAN Service:** Default setting is set to Enable. If you want to use wireless, you can select Enable.

● **ESSID:** The ESSID is the unique name of a wireless access point (AP) used to distinguish one from another. For security propose, change to a unique ID name which is already built into the router wireless interface. It is case sensitive and must not exceed 32 characters. Make sure your wireless clients have exactly the ESSID as the device in order to connect to your network.

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

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

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

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

● **Security Mode:** You can disable or enable with WPA or WEP to protect wireless network.

The default mode of wireless security is **Disable**.

● **RADIUS/802.1x:** You can enable or disable the RADIUS(Remote Authentication Dial In User Service) service.

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

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

If you want to enable the RADIUS function, check Enable and then do the following settings.

Security Mode	WPA
RADIUS / 802.1x	<input checked="" type="checkbox"/> Enable
Group Key Renewal	3600 seconds
RADIUS Server IP Address	
RADIUS Port	1812
RADIUS Shared Secret	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

● **RADIUS Server IP Address:** The IP address of RADIUS authentication server.

● **RADIUS Server Port:** The port number of RADIUS authentication server here. Default value is 1812.

● **RADIUS Shared Secret:** The password of RADIUS authentication server.

● WPA / WPA2 Pre-Shared Key

Configuration

WLAN

Wireless Parameters

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

Security Parameters

Security Mode	WPA/WPA2-PSK
WPA Shared Key	
Group Key Renewal	3600 seconds

● **WLAN Service:** Default setting is set to Enable. If you want to use wireless, you can

select Enable.

● **ESSID:** The ESSID is the unique name of a wireless access point (AP) used to distinguish one from another. For security propose, change to a unique ID name which is already built into the router wireless interface. It is case sensitive and must not exceed 32 characters. Make sure your wireless clients have exactly the ESSID as the device in order to connect to your network.

● **Hide ESSID:** This function enables the router to become invisible on the network. Thus, any clients using the wireless setting to search for available or specific router on the network will not be able to discover the router whose Hide ESSID function is set to enabled. The default setting is disabled.

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

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

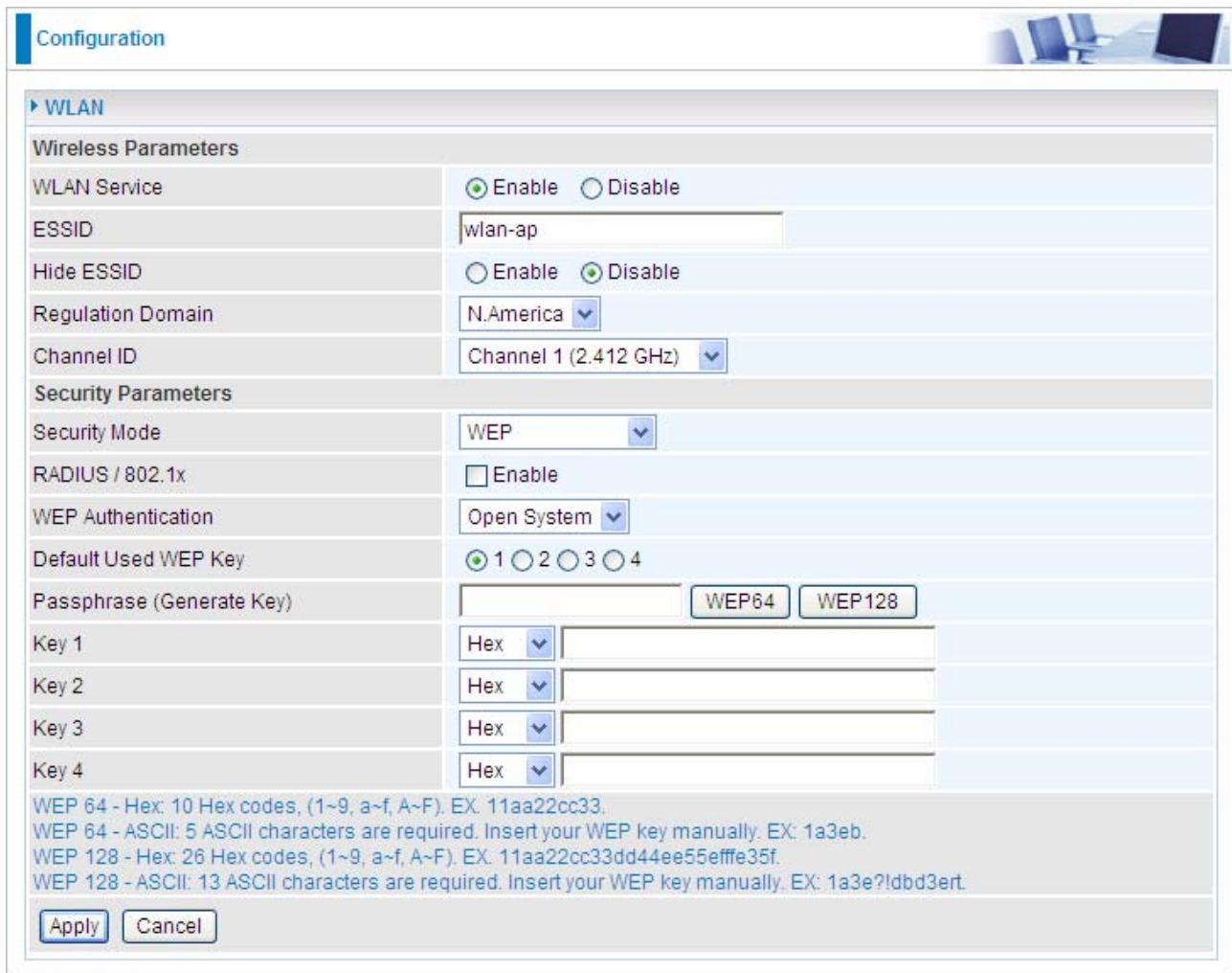
● **Security Mode:** You can disable or enable with WPA or WEP to protect wireless network. The default mode of wireless security is **Disable**.

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

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

Note: *Wireless performance may degrade if the selected channel ID is already being occupied by other AP(s).*

WEP



The screenshot shows a web-based configuration interface for WLAN settings. The page is titled "Configuration" and has a "WLAN" section expanded. Under "Wireless Parameters", the "WLAN Service" is set to "Enable", the "ESSID" is "wlan-ap", "Hide ESSID" is "Disable", "Regulation Domain" is "N.America", and "Channel ID" is "Channel 1 (2.412 GHz)". Under "Security Parameters", the "Security Mode" is set to "WEP", "RADIUS / 802.1x" is disabled, and "WEP Authentication" is "Open System". The "Default Used WEP Key" is set to "1". There are buttons for "WEP64" and "WEP128". Below these are four "Key" fields, each with a "Hex" dropdown menu. At the bottom, there are "Apply" and "Cancel" buttons. A small text block at the bottom of the form provides examples for WEP 64 and WEP 128 in both Hex and ASCII formats.

Wireless Parameters	
WLAN Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
ESSID	<input type="text" value="wlan-ap"/>
Hide ESSID	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Regulation Domain	<input type="text" value="N.America"/>
Channel ID	<input type="text" value="Channel 1 (2.412 GHz)"/>
Security Parameters	
Security Mode	<input type="text" value="WEP"/>
RADIUS / 802.1x	<input type="checkbox"/> Enable
WEP Authentication	<input type="text" value="Open System"/>
Default Used WEP Key	<input checked="" type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4
Passphrase (Generate Key)	<input type="text"/> <input type="button" value="WEP64"/> <input type="button" value="WEP128"/>
Key 1	<input type="text" value="Hex"/>
Key 2	<input type="text" value="Hex"/>
Key 3	<input type="text" value="Hex"/>
Key 4	<input type="text" value="Hex"/>

WEP 64 - Hex: 10 Hex codes, (1~9, a~f, A~F). EX: 11aa22cc33.
WEP 64 - ASCII: 5 ASCII characters are required. Insert your WEP key manually. EX: 1a3eb.
WEP 128 - Hex: 26 Hex codes, (1~9, a~f, A~F). EX: 11aa22cc33dd44ee55effe35f.
WEP 128 - ASCII: 13 ASCII characters are required. Insert your WEP key manually. EX: 1a3e?!dbd3ert.

● **WLAN Service:** Default setting is set to Enable. If you do not have any wireless, select Disable.

● **ESSID:** The ESSID is the unique name of a wireless access point (AP) used to distinguish one from another. For security propose, change to a unique ID name which is already built into the router wireless interface. It is case sensitive and must not exceed 32 characters. Make sure your wireless clients have exactly the ESSID as the device in order to connect to your network.

● **Hide ESSID:** This function enables the router to become invisible on the network. Thus, any clients using the wireless setting to search for available or specific router on the network will not be able to discover the router whose Hide ESSID function is set to enabled. The default setting is disabled.

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

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

Note: *Wireless performance may degrade if the selected channel ID is already being occupied*

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

● **RADIUS / 802.1x:** You can disable or enable the RADIUS service.

● **WEP Authentication:** To prevent an unauthorized wireless station from accessing the data transmitted over the network, the router offers a secure data encryption, known as WEP. There are 3 options to select from: **Open System, Shared key** or **both**.

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

● **Passphrase:** This is used to generate WEP keys automatically based upon the input string and a pre-defined algorithm in WEP64 or WEP128.

● **Key (1-4):** Enter the key to encrypt wireless data. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as the router. There are four keys for your selection. The input format can be either HEX style or ASCII format, 10 and 26 HEX codes or 5 and 13 ASCII codes are required for WEP64 and WEP128 respectively.

If you want to enable the RADIUS function, check **Enable** and then do the following settings.

Security Parameters	
Security Mode	WEP
RADIUS / 802.1x	<input checked="" type="checkbox"/> Enable
WEP Authentication	Open System
RADIUS Server IP Address	<input type="text"/>
RADIUS Port	1812
RADIUS Shared Secret	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

● **RADIUS Server IP Address:** The IP address of RADIUS authentication server.

● **RADIUS Server Port:** The port number of RADIUS authentication server here. Default value is 1812.

● **RADIUS Shared Secret:** The password of RADIUS authentication server.

Click Apply to confirm the settings.

Chapter 5

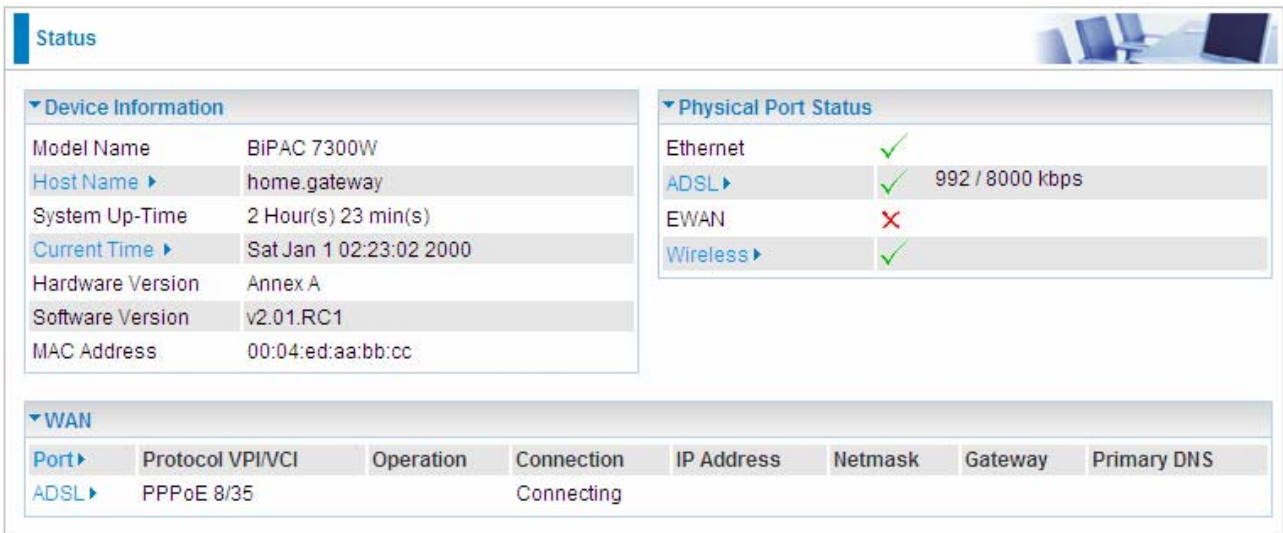
Advanced Configuration

Once you have logged on to your BiPAC 7300W Router via your web browser, you can begin to set it up according to your requirements. On the configuration homepage, the left navigation pane links you directly to the setup pages, which include:

- **Basic** (Switch to Basic Configuration Mode)
- **Status** (ADSL Status, ARP Table, DHCP Table, System Log, Firewall Log, UPnP Portmap)
- **Quick Start**
- **Configuration** (LAN, WAN, System, Firewall, QoS, Virtual Server, Wake on LAN, Time Schedule and Advanced)

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

5.1 Status



Status

Device Information

Model Name	BIPAC 7300W
Host Name	home.gateway
System Up-Time	2 Hour(s) 23 min(s)
Current Time	Sat Jan 1 02:23:02 2000
Hardware Version	Annex A
Software Version	v2.01.RC1
MAC Address	00:04:ed:aa:bb:cc

Physical Port Status

Ethernet	✓	
ADSL	✓	992 / 8000 kbps
EWAN	✗	
Wireless	✓	

WAN

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

Device Information

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



Configuration

Device Management

Device Host Name

Host Name

Embedded Web Server

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

Expire to auto-logout min(s)

Universal Plug and Play (UPnP)

UPnP Enable Disable

UPnP Port

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

WAN

- **Port:** Name of the WAN connection.
- **Protocol VPI/VCI:** Virtual Path Identifier and Virtual Channel Identifier
- **Operation:** Current available operation.
- **Connection:** The current connection status.
- **IP Address:** WAN port IP address.
- **Net mask:** WAN port IP subnet mask.
- **Gateway:** The IP address of the default gateway.
- **Primary DNS:** The IP address of the primary DNS server.

Physical Port Status

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

5.1.1 ADSL Status

Parameters	
DSP Firmware Version	DMT FwVer: 3.12.8.8_A_TC, HwVer:T14F7_7.0
DMT Status	Up
Operational Mode ▶	ADSL G.DMT
Upstream	992 kbps
Downstream	8000 kbps
SNR Margin (Upstream)	6.0 db
SNR Margin (Downstream)	17.0 db
Line Attenuation (Upstream)	1.0 db
Line Attenuation (Downstream)	0.0 db

- **DSP Firmware Version:** DSP code version
- **DMT Status:** Current DMT Status
- **Operational Mode:** To show the state when user select “AUTO” on connect mode. Click the link, the following will appear.

WAN Connection	
ADSL Mode	Open Annex Type and Follow DSLAM's Setting ▼
Modulator	Auto ▼

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

- **Upstream:** Upstream rate.
- **Downstream:** Downstream rate.
- **SNR Margin (Upstream):** This is noise margin in upstream.

- **SNR Margin (Downstream):** This is noise margin in downstream.
- **Line Attenuation (Upstream):** This is attenuation of signal in upstream.
- **Line Attenuation (Downstream):** This is attenuation of signal in downstream.
- **Refresh:** Press this button to get the latest statistics.

5.1.2 ARP Table

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

Wireless			
IP Address	MAC Address	Interface	Static ARP
Wired			
IP Address	MAC Address	Interface	Static ARP
192.168.1.63	00:24:21:5C:81:C8	lan	No

- **IP Address:** It is IP Address of internal host that join this network.
- **MAC Address:** The MAC address of internal host.
- **Interface:** The interface name (on the router) that this IP address connects to.
- **Static ARP:** Shows the status of static ARP.

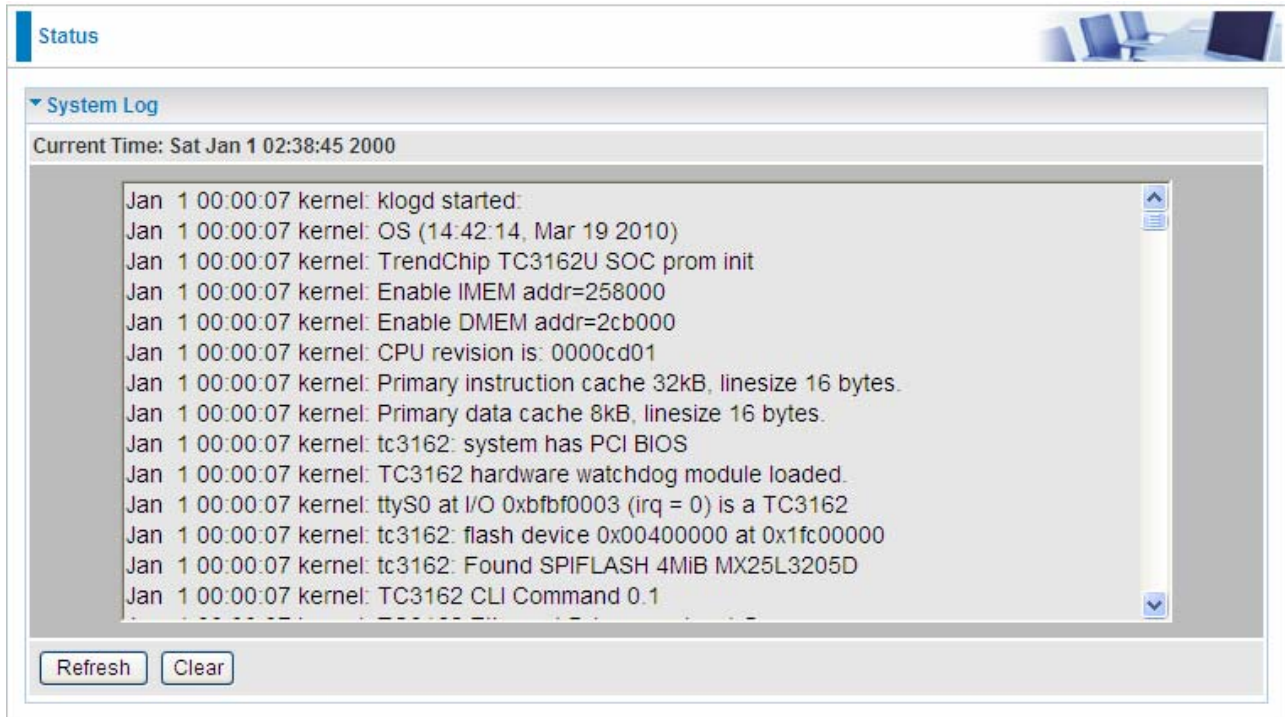
5.1.3 DHCP Table

IP Address	MAC Address	Client Host Name	Register Information

- **IP Address:** The current corresponding DHCP-assigned dynamic IP address of the device.
- **MAC Address:** The MAC Address of internal DHCP client host.
- **Client Host Name:** The Host Name of internal DHCP client.
- **Register Information:** Register time information.

5.1.4 System Log

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



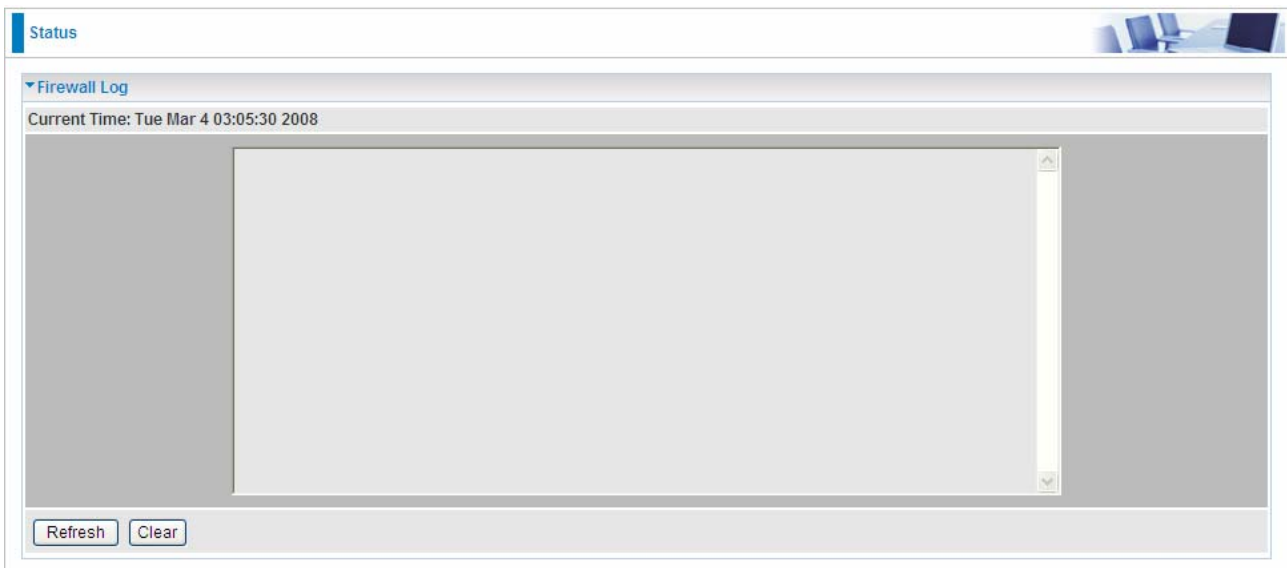
The screenshot displays a web-based interface for viewing system logs. At the top left, there is a 'Status' tab. Below it, the 'System Log' section is expanded, showing the current time as 'Sat Jan 1 02:38:45 2000'. The log content is displayed in a scrollable area with a vertical scrollbar on the right. The log entries are as follows:

```
Jan 1 00:00:07 kernel: klogd started:
Jan 1 00:00:07 kernel: OS (14:42:14, Mar 19 2010)
Jan 1 00:00:07 kernel: TrendChip TC3162U SOC prom init
Jan 1 00:00:07 kernel: Enable IMEM addr=258000
Jan 1 00:00:07 kernel: Enable DMEM addr=2cb000
Jan 1 00:00:07 kernel: CPU revision is: 0000cd01
Jan 1 00:00:07 kernel: Primary instruction cache 32kB, linesize 16 bytes.
Jan 1 00:00:07 kernel: Primary data cache 8kB, linesize 16 bytes.
Jan 1 00:00:07 kernel: tc3162: system has PCI BIOS
Jan 1 00:00:07 kernel: TC3162 hardware watchdog module loaded.
Jan 1 00:00:07 kernel: ttyS0 at I/O 0xbfbf0003 (irq = 0) is a TC3162
Jan 1 00:00:07 kernel: tc3162: flash device 0x00400000 at 0x1fc00000
Jan 1 00:00:07 kernel: tc3162: Found SPIFLASH 4MIB MX25L3205D
Jan 1 00:00:07 kernel: TC3162 CLI Command 0.1
```

At the bottom of the log area, there are two buttons: 'Refresh' and 'Clear'.

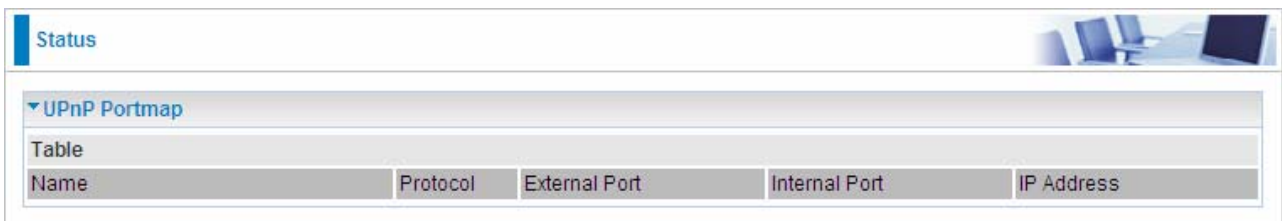
5.1.5 Firewall Log

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



5.1.6 UPnP Portmap

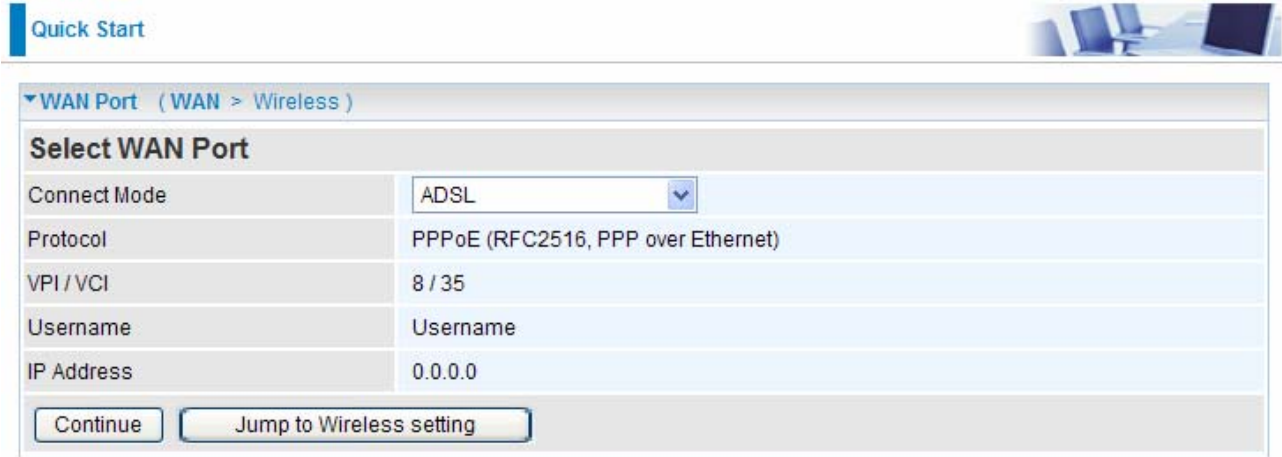
The section lists all port-mapping established using UPnP (Universal Plug and Play). Please see the Advanced section of this manual for more details on UPnP and the router's UPnP configuration options.



- **Name:** the description of this application.
- **Protocol:** the protocol used by UpnP NAT Mapping.
- **External Port:** the external service port transformed by the mapping, thus the remote port or the port in the WAN wanting to connect in.
- **Internal Port:** the internal service port.
- **IP Address:** the internal host IP address.

5.2 Quick Start

ADSL



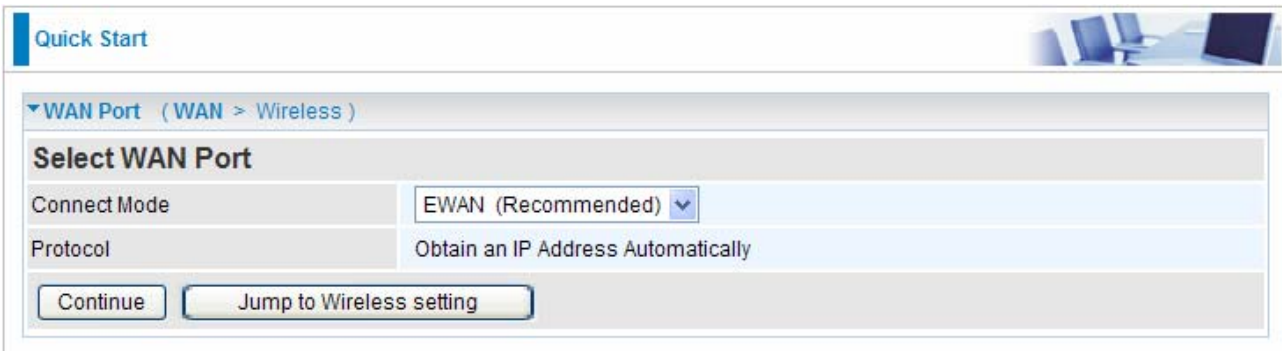
The screenshot shows a web interface for configuring a WAN port. At the top, there is a 'Quick Start' button and a breadcrumb trail '(WAN > Wireless)'. Below this is a section titled 'Select WAN Port'. It contains a table with the following fields:

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

At the bottom of the form, there are two buttons: 'Continue' and 'Jump to Wireless setting'.

- **Connect mode:** ADSL
- **Protocol:** The current ATM protocol in the device
- **VPI / VCI:** The current value of VPI / VCI in the device
- **IP address:** To show current value of IP address in the device.

EWAN



The screenshot shows a web interface for configuring a WAN port. At the top, there is a 'Quick Start' button and a breadcrumb trail '(WAN > Wireless)'. Below this is a section titled 'Select WAN Port'. It contains a table with the following fields:

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

At the bottom of the form, there are two buttons: 'Continue' and 'Jump to Wireless setting'.

Click on **Continue** to choose the Protocol to connect with EWAN or click **Jump to Wireless Setting** to use Protocol: Obtain an IP Address Automatically to connect and setup wireless settings at the same time.

Obtain an IP Address Automatically

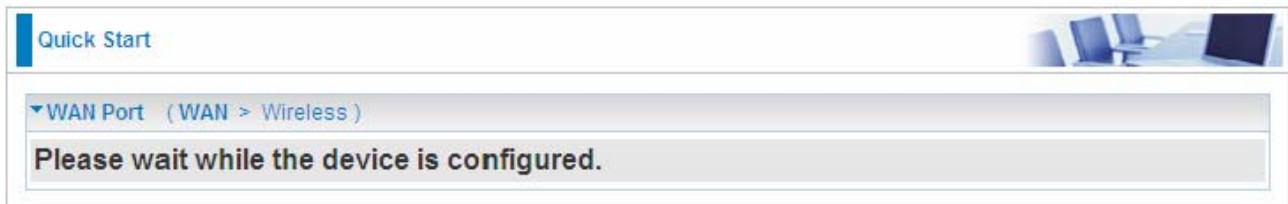
When connecting to the ISP, BiPAC 7300W also functions as a DHCP client. BiPAC 7300W can automatically obtain an IP address, subnet mask, gateway address, and DNS server addresses if the ISP assigns this information via DHCP.



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

Protocol: The current ATM protocol in the device

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



The screenshot shows the 'Quick Start' section of the WAN Port configuration page. The breadcrumb trail is 'WAN Port (WAN > Wireless)'. The main heading is 'Please wait while the device is configured.'.

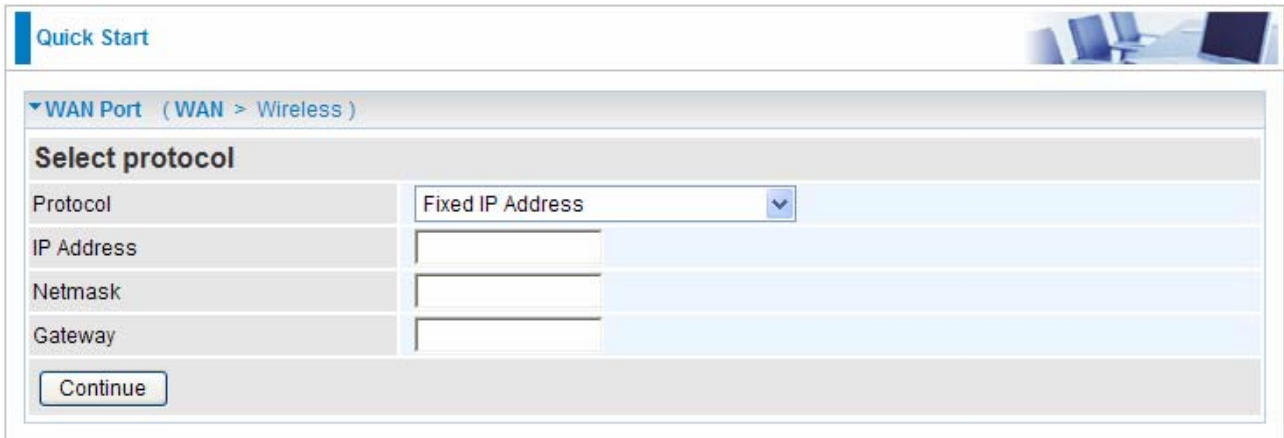
If connection is successful the following image will be shown.



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

Fixed IP Address

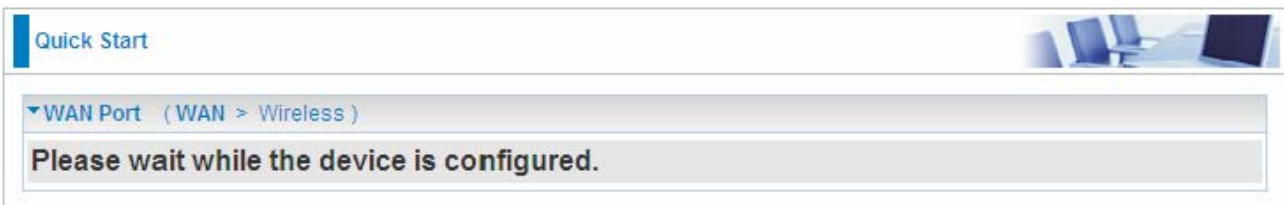
Select this option to set static IP information. You will need to enter in the Connection type, IP address, Netmask, and gateway address, provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which is four IP octets separated by a dot (x.x.x.x). The Router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



The screenshot shows the 'Quick Start' section of a router's configuration interface. Under the 'WAN Port (WAN > Wireless)' tab, the 'Select protocol' section is active. The 'Protocol' dropdown menu is set to 'Fixed IP Address'. Below this, there are three empty input fields for 'IP Address', 'Netmask', and 'Gateway'. A 'Continue' button is located at the bottom left of the configuration area.

- **Protocol:** The current ATM protocol in the device
- **IP Address:** Enter your WAN IP address.
- **Netmask:** Type the subnet mask assigned to you by your ISP (if given).
- **Gateway:** You must specify a gateway IP address (supplied by your ISP)

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



The screenshot shows the 'Quick Start' section of the router's configuration interface. Under the 'WAN Port (WAN > Wireless)' tab, a message box displays the text: 'Please wait while the device is configured.'

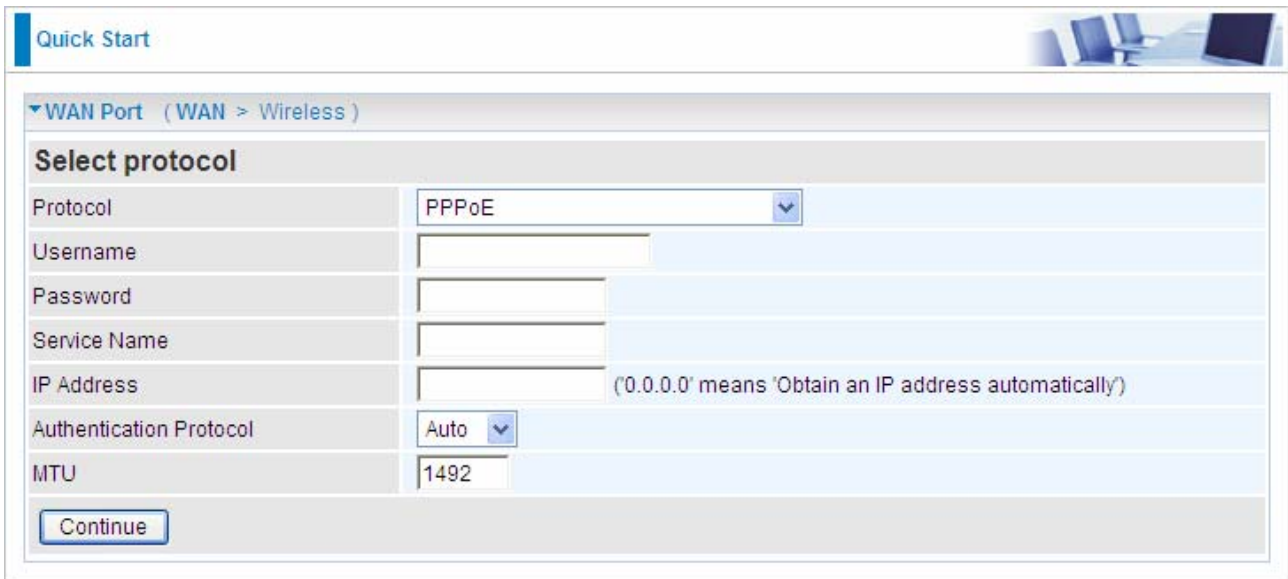
If connection is successful the following image will be shown.



The screenshot shows the 'Quick Start' section of the router's configuration interface. Under the 'WAN Port (WAN > Wireless)' tab, a message box displays the text: 'Congratulations! Your WAN port has been successfully configured.' Below the message is a 'Next to Wireless' button.

PPPoE

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

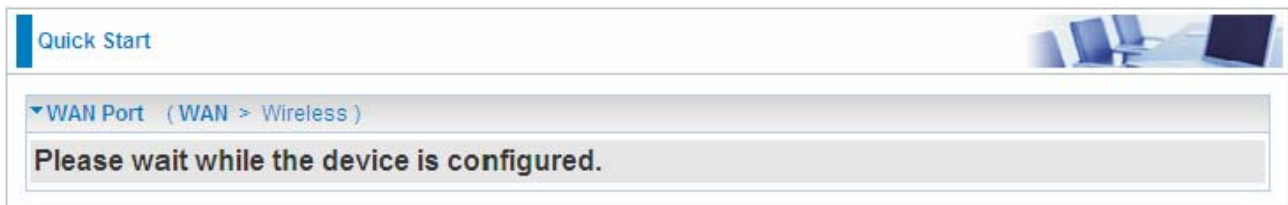


The screenshot shows a web interface for configuring a WAN port. The page is titled "Quick Start" and "WAN Port (WAN > Wireless)". Under the heading "Select protocol", there is a form with the following fields:

Protocol	PPPoE
Username	<input type="text"/>
Password	<input type="password"/>
Service Name	<input type="text"/>
IP Address	<input type="text"/> ('0.0.0.0' means 'Obtain an IP address automatically')
Authentication Protocol	Auto
MTU	1492

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

- **Protocol:** The current ATM protocol in the device
 - **Username:** Enter the username provided by your ISP. You can input up to 128 alphanumeric characters (case sensitive). This is in the format of "username@ispname" instead of simply "username".
 - **Password:** Enter the password provided by your ISP. You can input up to 128 alphanumeric characters (case sensitive).
 - **Service Name:** Enter a name for this connection.
 - **IP Address:** Your WAN IP address. Leave this at 0.0.0.0 to automatically obtain an IP address from your ISP.
 - **Auth. Protocol:** Default is Auto. Your ISP advises on using Chap or Pap.
 - **MTU:** Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) an IP attempts to send through the interface.
- Click on the **Continue** button and wait for your connection to be connected.

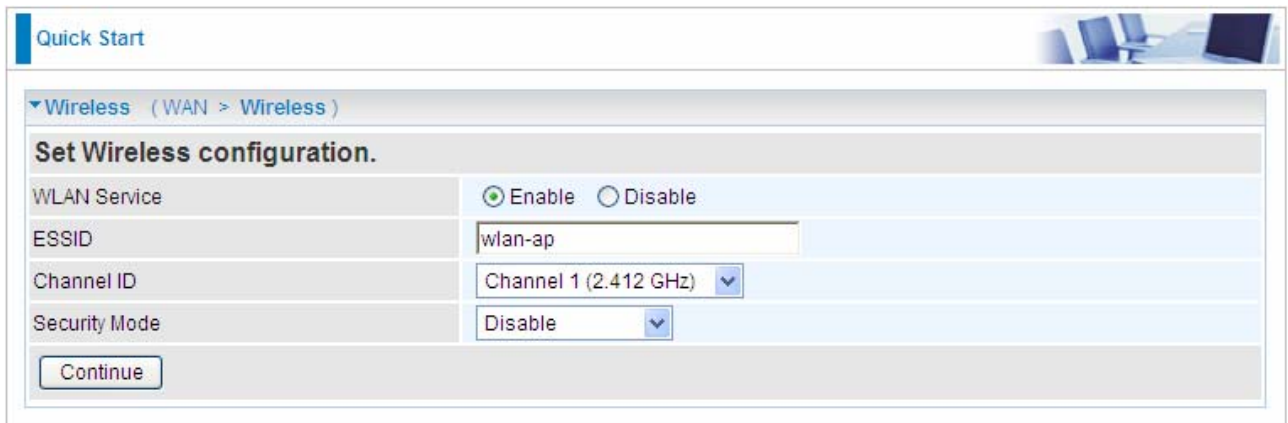


The screenshot shows the same web interface as above, but now displaying a message: "Please wait while the device is configured." The "Continue" button is no longer visible.

If connection is successful the following image will be shown.



■ Set Wireless configuration



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

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

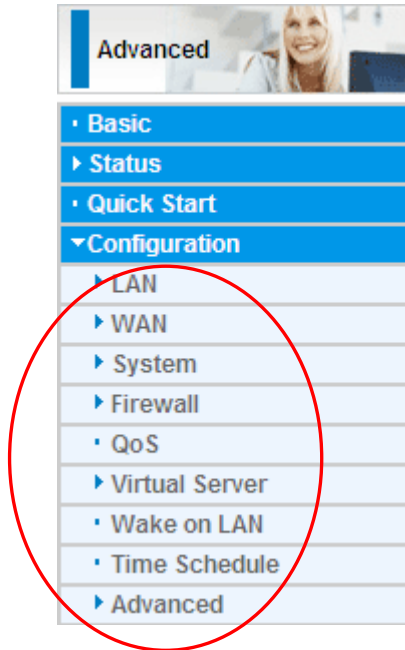
● **Channel ID:** Select the ID channel that you would like to use.

● **Security Mode:** You can disable or enable with WPA or WEP for protecting wireless network. The default mode of wireless security is **Disable**. Turn to page 35-37 for help.

5.3 Configuration

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

These functions are described in the following sections.

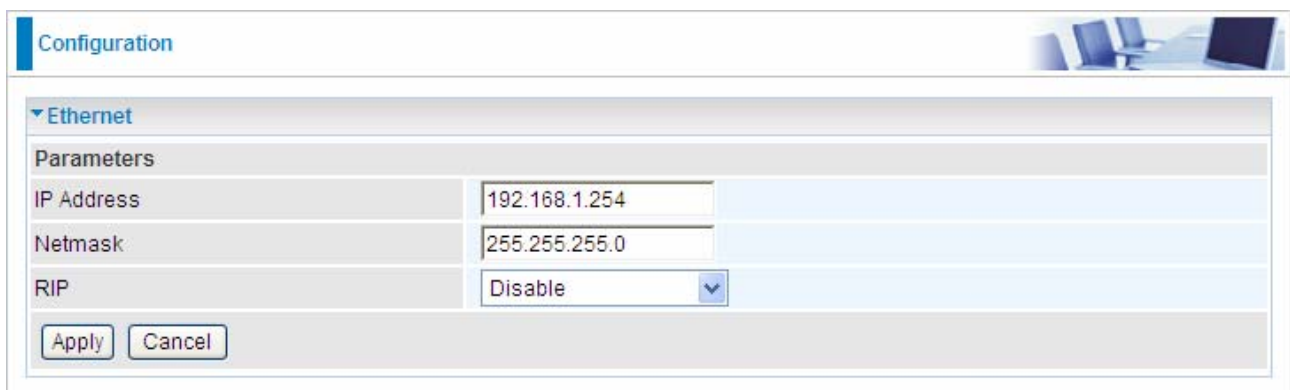


5.3.1 LAN (Local Area Network)

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

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

5.3.1.1 Ethernet

A screenshot of the "Configuration" page in a web-based interface. The page title is "Configuration". Below the title, there is a section for "Ethernet" configuration. Under the "Ethernet" section, there is a "Parameters" section with three rows of configuration options: "IP Address" with a text input field containing "192.168.1.254", "Netmask" with a text input field containing "255.255.255.0", and "RIP" with a dropdown menu set to "Disable". At the bottom of the configuration area, there are two buttons: "Apply" and "Cancel".

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

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

5.3.1.2 IP Alias

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

The screenshot shows a web interface for configuring IP Aliases. At the top, there is a 'Configuration' header. Below it, a section titled 'IP Alias' contains a 'Parameters' table with two columns: 'IP Address' and 'Netmask'. Both columns have empty text input fields. Below the input fields are two buttons: 'Add' and 'Edit / Delete'.

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

Press Add to apply and the corresponding information will be listed below.

The screenshot shows the same web interface as before, but now with a table listing the configured IP aliases. The 'Add' button has been pressed, and the table below the input fields contains one entry. The 'Edit / Delete' button is still present.

Edit	IP Address	Netmask	Delete
	192.168.1.253	255.255.255.0	<input type="checkbox"/>

Click **Edit** radio button, then the item you want to reedit will be displayed above just as showed below.

Configuration

▼ IP Alias

Parameters

IP Address: 192.168.1.253 Netmask: 255.255.255.0

Add **Edit / Delete**

Edit	IP Address	Netmask	Delete
<input checked="" type="radio"/>	192.168.1.253	255.255.255.0	<input type="checkbox"/>

Press **Edit/Delete** to apply your modification.

Check **Delete** if you want to delete the item, then press **Edit/Delete**, the deleting prompt window will appear to remind you, do as you like.

5.3.1.3 Wireless

Configuration

▼ Wireless

Parameters

WLAN Service: Enable Disable

Time Schedule: 1. Always On 2. TimeSlot1

Mode: 802.11g + n

ESSID: wlan-ap

Hide ESSID: Enable Disable

Regulation Domain: N.America

Channel ID: Channel 1 (2.412 GHz)

Channel Width: 20/40MHZ

Tx PowerLevel: 100 (0 ~ 100)

AP MAC Address: 00:04:ED:AA:BB:CC

AP Firmware Version: 2.4.0.0

WPS Service: Enable Disable

WPS State: Configured Unconfigured

WMM: Enable Disable

Wireless Distribution System (WDS)

WDS Service: Enable Disable

Peer WDS MAC address:

1.	<input type="text"/>	2.	<input type="text"/>
3.	<input type="text"/>	4.	<input type="text"/>

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

Apply Cancel Security settings ▶

Parameters

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

● **Time Schedule:** A self-defined time period. You may specify a time schedule for your prioritization policy.

Here we provide two groups of **Time Schedule** setting. You can flexibly set the time you want the wireless connection works.

If you select **Always On** in group1, then the group2 is disabled.

While if you select any other item from the group1 drop-down menu, the group2 will be activated. Select the timeslot you want, then the wireless will work according to the time of the two time schedule settings. That is to say you can flexibly set the time the wireless works.

For example, if you select TimeSlot1 in group1, then the group2 is activated, you can select a timeslot from the drop-down menu, then the wireless connection will perform according to the two timeslots you have set.

For setup and detail, refer to **Time Schedule** section.

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

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

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

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

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

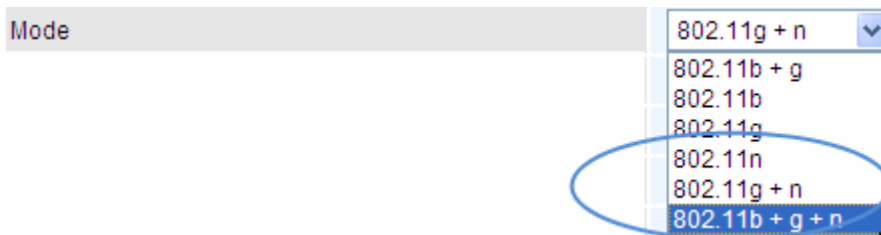
⊙ **Disable:** When Disable is selected, you can allow anybody with a wireless client to be able to locate the Access Point (AP) of your router.

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

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

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

Note: This parameter appears only when you select one of the item as the following graph



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

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

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

● **AP Firmware Version:** The Access Point firmware version.

● **WPS service:** Enable / disable

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

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

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

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

● **Enable:** Check to activate WMM feature.

● **Disable:** Check to deactivate WMM feature.

Wireless Distribution System (WDS)

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

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

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

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

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

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

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

5.3.1.4 Wireless Security

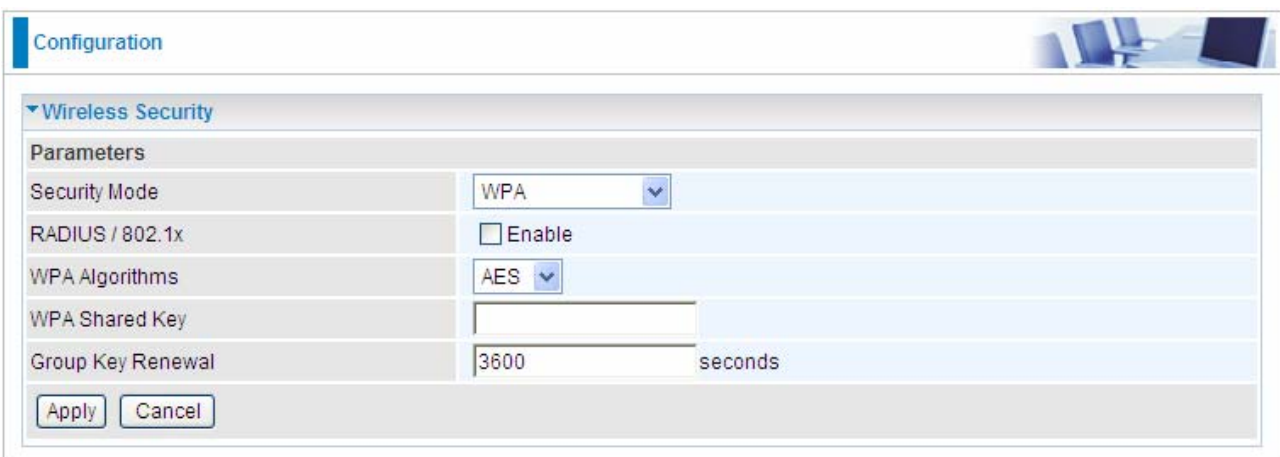
You can disable or enable with WPA or WEP for protecting wireless network. The default mode of wireless security is **Disable**.



The screenshot shows a configuration window titled "Configuration" with a sub-section "Wireless Security". Under "Parameters", the "Security Mode" is set to "Disable" in a dropdown menu. There are "Apply" and "Cancel" buttons at the bottom.

WPA or WPA2

Here take **WPA** for example.



The screenshot shows the "Wireless Security" configuration page with "Security Mode" set to "WPA". Other settings include "RADIUS / 802.1x" (unchecked), "WPA Algorithms" set to "AES", an empty "WPA Shared Key" field, and "Group Key Renewal" set to "3600 seconds". "Apply" and "Cancel" buttons are at the bottom.

● **Security Mode:** You can choose the type of security mode you want to apply from the drop down menu.

● **RADIUS/802.1x:** Whether to enable RADIUS function or not (For WPA/WPA2/WEP encryption).

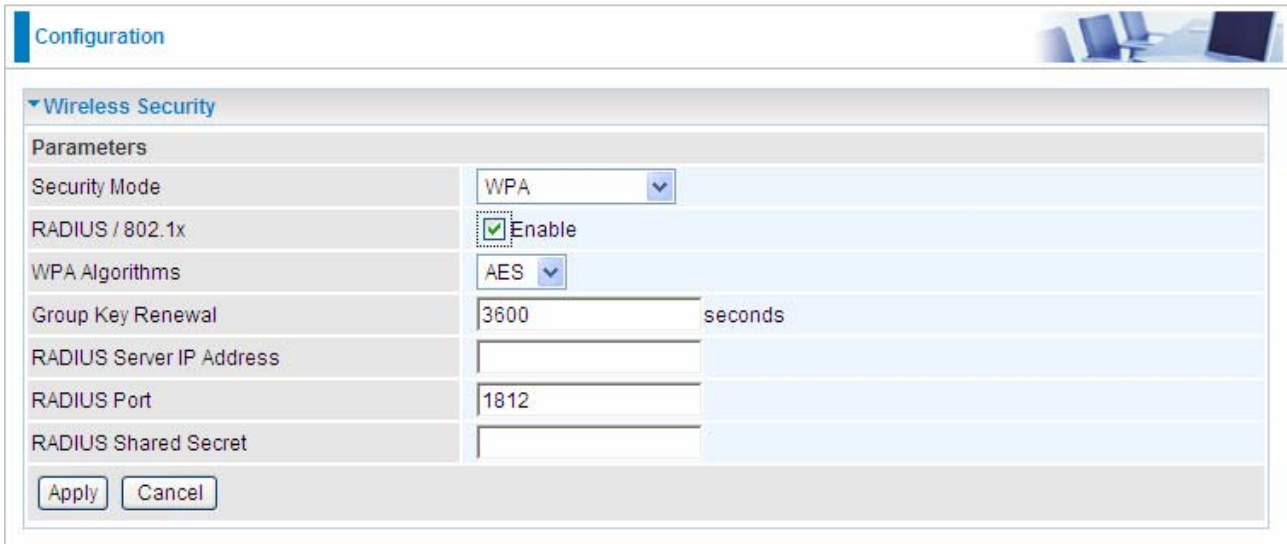
● **WPA Algorithms:** There are two Algorithms, AES (Advanced Encryption Standard) and TKIP(Temporal Key Integrity Protocol) which help to protect the wireless communication. The Default algorithms is AES.

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

● **Group Key Renewal:** The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). Default value is 3600

seconds.

If you want to enable the RADIUS service, check Enable and then do the following settings.



The screenshot shows the 'Configuration' window for 'Wireless Security'. Under the 'Parameters' section, the following settings are visible:

Security Mode	WPA
RADIUS / 802.1x	<input checked="" type="checkbox"/> Enable
WPA Algorithms	AES
Group Key Renewal	3600 seconds
RADIUS Server IP Address	
RADIUS Port	1812
RADIUS Shared Secret	

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

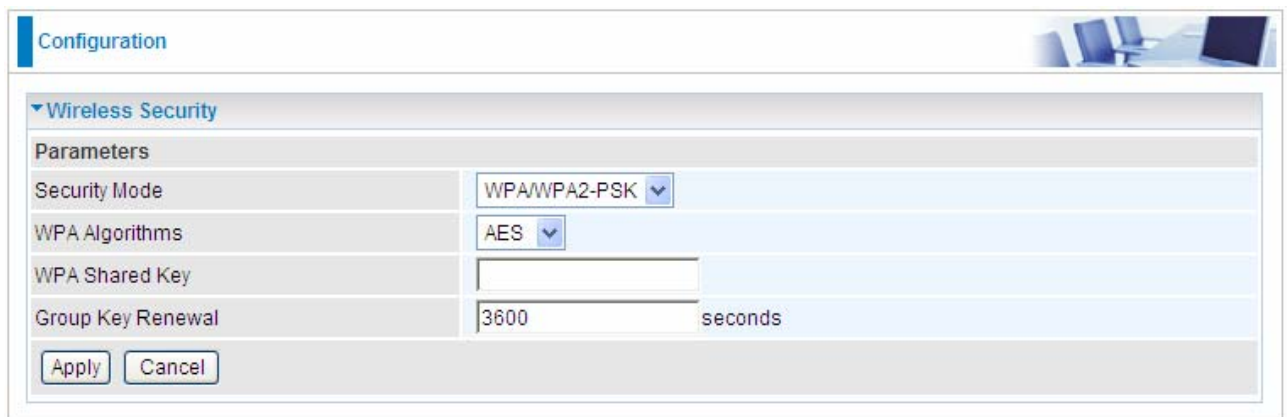
● **RADIUS Server IP Address:** Enter the IP address of RADIUS authentication server.

● **RADIUS Server Port:** Enter the port number of RADIUS authentication server here. Default value is 1812.

● **RADIUS Shared Secret:** Enter the password of RADIUS authentication server.

Click Apply to confirm the settings.

WPA / WPA2 - PSK



The screenshot shows the 'Configuration' window for 'Wireless Security'. Under the 'Parameters' section, the following settings are visible:

Security Mode	WPA/WPA2-PSK
WPA Algorithms	AES
WPA Shared Key	
Group Key Renewal	3600 seconds

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

● **Security Mode:** You can choose the type of security mode you want to apply from the drop-down menu.

● **WPA Algorithms:** There are two Algorithms, AES (Advanced Encryption Standard) and TKIP(Temporal Key Integrity Protocol) which help to protect the wireless communication. The Default algorithm is AES.

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

● **Group Key Renewal:** The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). Default value is 3600 seconds.

Click Apply to confirm the settings.

WEP

The screenshot shows a configuration page titled "Configuration" with a sub-section "Wireless Security". Under "Parameters", the following settings are visible:

- Security Mode: WEP (dropdown)
- RADIUS / 802.1x: Enable
- WEP Authentication: Open System (dropdown)
- Default Used WEP Key: 1 (radio button selected, others 2, 3, 4 are unselected)
- Passphrase (Generate Key): [text input] [WEP64] [WEP128]
- Key 1: Hex [dropdown] [text input]
- Key 2: Hex [dropdown] [text input]
- Key 3: Hex [dropdown] [text input]
- Key 4: Hex [dropdown] [text input]

Below the keys, there is explanatory text:

- WEP 64 - Hex: 10 Hex codes, (1~9, a~f, A~F). EX: 11aa22cc33.
- WEP 64 - ASCII: 5 ASCII characters are required. Insert your WEP key manually. EX: 1a3eb.
- WEP 128 - Hex: 26 Hex codes, (1~9, a~f, A~F). EX: 11aa22cc33dd44ee55effe35f.
- WEP 128 - ASCII: 13 ASCII characters are required. Insert your WEP key manually. EX: 1a3e?!dbd3ert.

At the bottom, there are "Apply" and "Cancel" buttons.

● **RADIUS / 802.1x:** Whether to enable RADIUS / 802.1x.

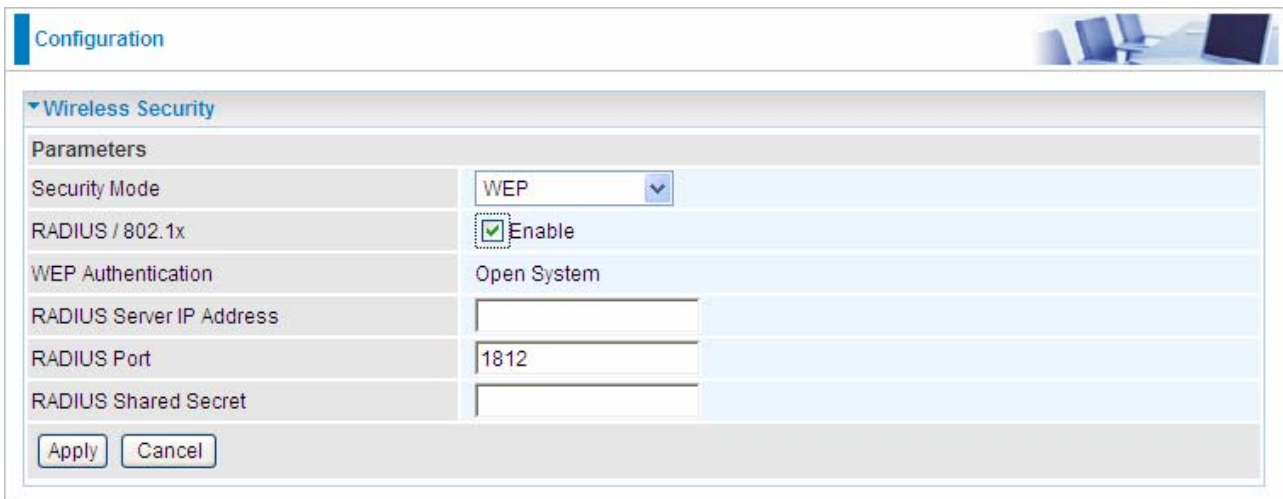
● **WEP Authentication:** To prevent unauthorized wireless stations from accessing data transmitted over the network, the router offers secure data encryption, known as WEP. There are 3 options to select from: **Open System**, **Shared key** or **both**.

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

● **Passphrase:** This is used to generate WEP keys automatically based upon the input string and a pre-defined algorithm in WEP64 or WEP128.

● **Key (1-4):** Enter the key to encrypt wireless data. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as the router. There are four keys for your selection. The input format can be either HEX style or ASCII format, 10 and 26 HEX codes or 5 and 13 ASCII codes are required for WEP64 and WEP128 respectively.

If you want to enable the RADIUS service, check Enable and then do the following settings.



The screenshot shows a configuration window titled "Configuration" with a sub-section for "Wireless Security". Under "Parameters", the following settings are visible:

Parameters	
Security Mode	WEP
RADIUS / 802.1x	<input checked="" type="checkbox"/> Enable
WEP Authentication	Open System
RADIUS Server IP Address	<input type="text"/>
RADIUS Port	1812
RADIUS Shared Secret	<input type="text"/>

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

● **WEP Authentication:** If you enable **RADIUS/802.1x**, then the default **WEP Authentication** is **Open System**.

● **RADIUS Server IP Address:** Enter the IP address of RADIUS authentication server.

● **RADIUS Server Port:** Enter the port number of RADIUS authentication server here. Default value is 1812.

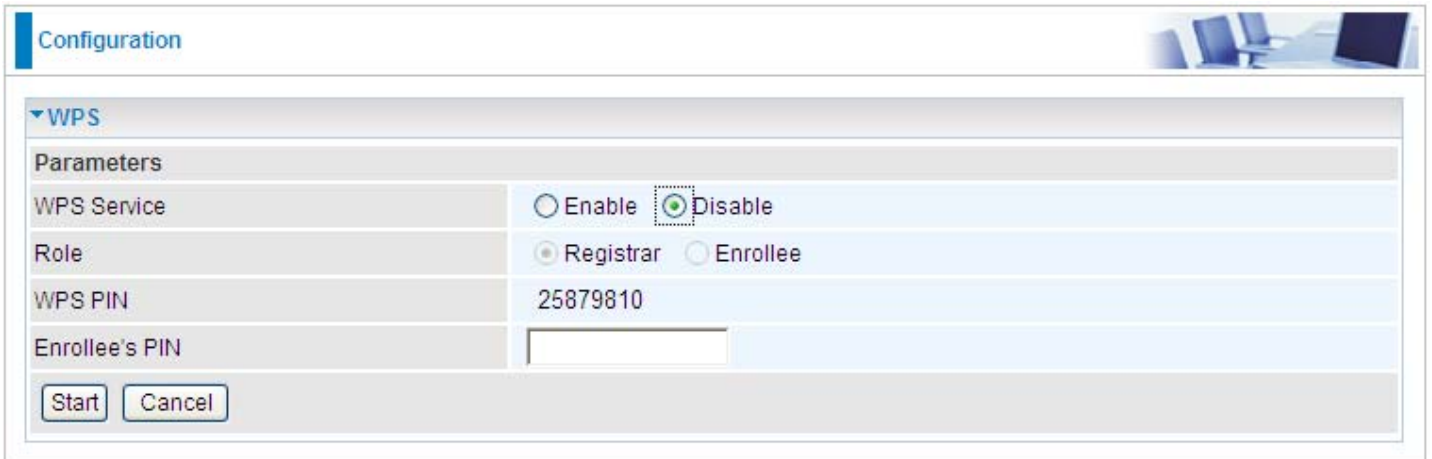
● **RADIUS Shared Secret:** Enter the password of RADIUS authentication server.

Click Apply to confirm the settings.

Note: For information about settling Radius/802.1x, please refer to WLAN setup section.

5.3.1.5 WPS

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



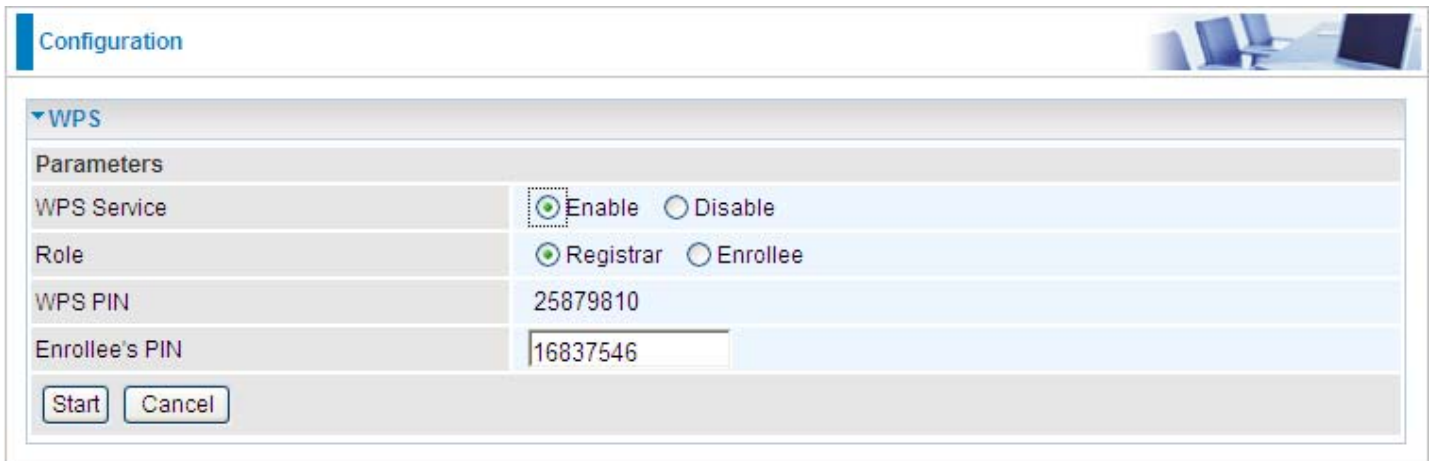
The screenshot shows a configuration window titled "Configuration" with a "WPS" section. Under "Parameters", the "WPS Service" is set to "Disable" (selected with a radio button), "Role" is set to "Registrar", "WPS PIN" is "25879810", and "Enrollee's PIN" is an empty text box. "Start" and "Cancel" buttons are at the bottom.

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

Wi-Fi Network Setup

PIN Method: Configure AP as Registrar

1. Jot down the client's Pin (eg. 16837546).
2. Enter the Enrollee's PIN number and then press Start.



The screenshot shows the same configuration window as above, but now "WPS Service" is set to "Enable" (selected with a radio button) and "Enrollee's PIN" is "16837546".

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

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

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

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

ID	AP Name	MAC Address	Count
0x0000	wlan-ap	00-1D-92-C0-13-CD	1
	wlan-ap	00-04-ED-00-00-01	1
- WPS Profile List:** (Empty)
- Control Panel:**
 - Buttons:** PIN, PBC, WPS Associate IE (checked), WPS Probe IE (checked), Progress >> 0%, WPS status is disconnected.
 - Right Panel:** Rescan, Information, Pin Code (16837546, Renew), Config Mode (Enrollee), Detail, Connect, Rotate, Disconnect, Export Profile, Delete.
- Status and Metrics:**
 - Status >> Disconnected
 - Link Quality >> 0%
 - Signal Strength 1 >> 0%
 - Signal Strength 2 >> 0%
 - Noise Strength >> 0%
 - Transmit: Link Speed >> Max, Throughput >> 0.000 Kbps
 - Receive: Link Speed >> Max, Throughput >> 0.000 Kbps
 - HT: BW >> n/a, SNR0 >> n/a, GI >> n/a, MCS >> n/a, SNR1 >> n/a

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

WPS AP List

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

WPS Profile List

wlan-ap

PIN
 PBC

WPS Associate IE
 WPS Probe IE

Progress >> 100%

PIN - Get WPS profile successfully.

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

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

HT

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

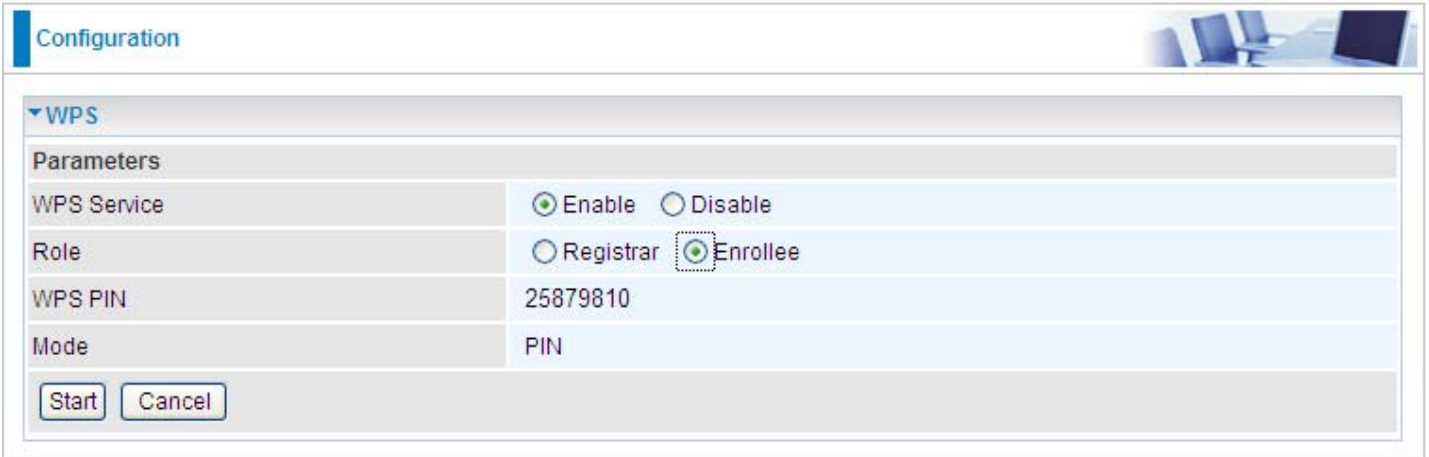
Link Quality >> 100%
 Signal Strength 1 >> 64%
 Signal Strength 2 >> 34%
 Noise Strength >> 26%

Transmit
 Link Speed >> 270.0 Mbps
 Throughput >> 5.600 Kbps

Receive
 Link Speed >> 54.0 Mbps
 Throughput >> 81.608 Kbps

PIN Method: Configure AP as Enrollee

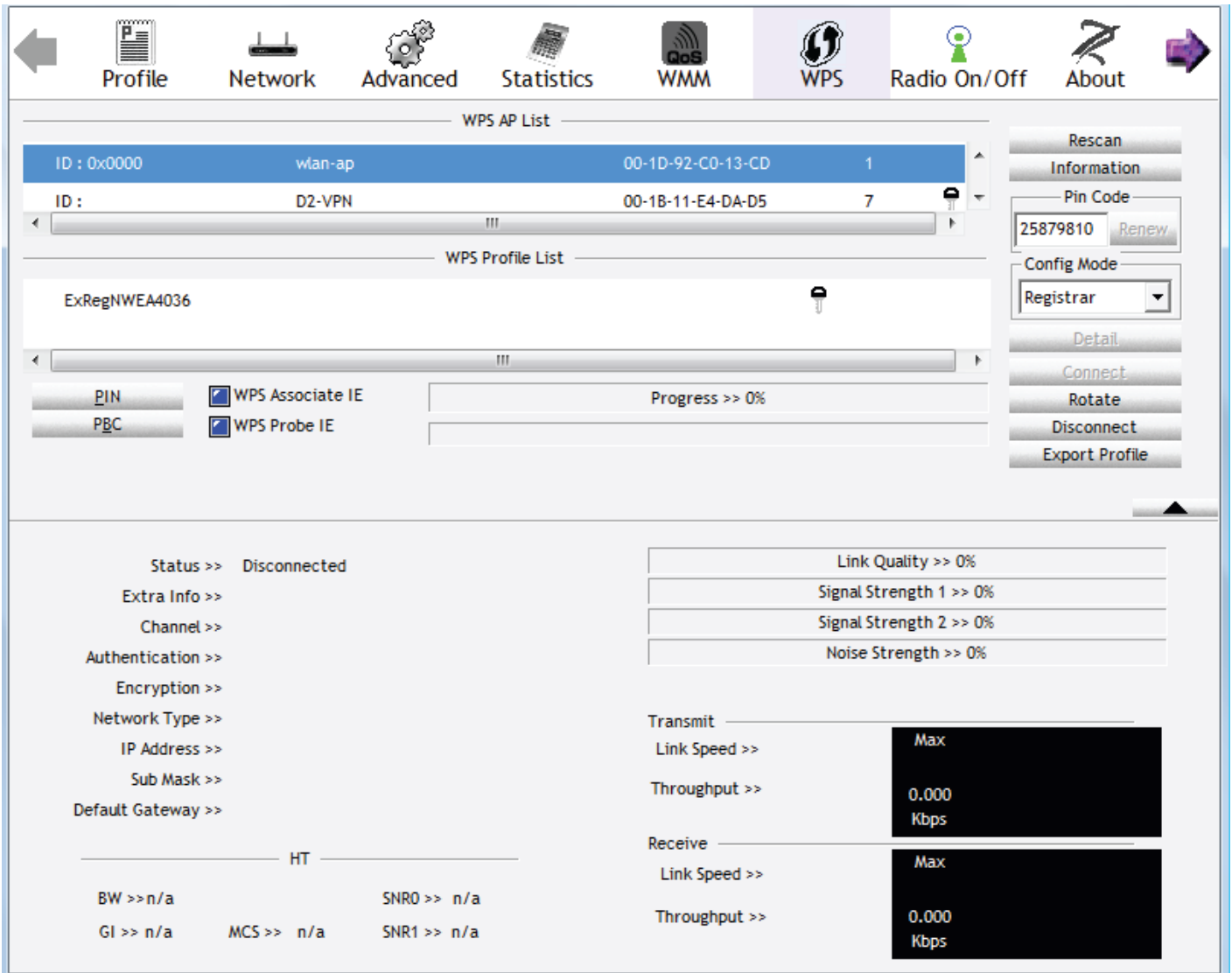
1. In the WPS configuration page, change the Role to Enrollee. Then press Start.
2. Jot down the WPS PIN (eg. 25879810).



The screenshot shows a 'Configuration' window with a 'WPS' section. Under 'Parameters', the 'WPS Service' is set to 'Enable', the 'Role' is set to 'Enrollee', and the 'WPS PIN' is '25879810'. The 'Mode' is set to 'PIN'. There are 'Start' and 'Cancel' buttons at the bottom.

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

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



The screenshot shows the Ralink Utility WPS interface. The 'WPS AP List' section contains the following table:

ID	AP Name	MAC Address	Priority
0x0000	wlan-ap	00-1D-92-C0-13-CD	1
D2-VPN		00-1B-11-E4-DA-D5	7

The 'WPS Profile List' section shows a profile named 'ExRegNWEA4036'. Below this, there are checkboxes for 'WPS Associate IE' and 'WPS Probe IE', both of which are checked. A 'Progress' bar shows 0%.

The interface also includes a 'PIN' button, a 'PIN Code' field with the value '25879810', and a 'Config Mode' dropdown set to 'Registrar'. Other buttons include 'Rescan', 'Information', 'Detail', 'Connect', 'Rotate', 'Disconnect', and 'Export Profile'.

At the bottom, there are sections for 'Status' (Disconnected), 'Link Quality' (0%), 'Signal Strength 1' (0%), 'Signal Strength 2' (0%), 'Noise Strength' (0%), 'Transmit' (Link Speed: Max, Throughput: 0.000 Kbps), and 'Receive' (Link Speed: Max, Throughput: 0.000 Kbps).

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

The screenshot displays the WPS configuration interface on a router. At the top, there is a navigation bar with icons for Profile, Network, Advanced, Statistics, WMM, WPS (selected), Radio On/Off, and About. Below this, the 'WPS AP List' section shows two entries:

ID	AP Name	MAC Address	Count
ExRegNWEA4036		00-1D-92-C0-13-CD	1
wlan-ap		00-04-ED-38-F7-2E	1

Below the AP list is the 'WPS Profile List' section, which shows the profile 'ExRegNWEA4036'. Underneath, there are checkboxes for 'WPS Associate IE' and 'WPS Probe IE', both of which are checked. A progress bar indicates 'Progress >> 100%' and a message states 'PIN - Get WPS profile successfully.'.

On the right side, there are several control buttons: Rescan, Information, Pin Code (with a text input field containing '25879810' and a 'Renew' button), Config Mode (a dropdown menu set to 'Registrar'), Detail, Connect, Rotate, Disconnect, and Export Profile.

The bottom section of the interface provides detailed status and performance metrics:

- Status >>** ExRegNWEA4036 <-> 00-1D-92-C0-13-CD
- Extra Info >>** Link is Up [TxPower:100%]
- Channel >>** 1 <-> 2412 MHz; central channel : 3
- Authentication >>** WPA2-PSK
- Encryption >>** AES
- Network Type >>** Infrastructure
- IP Address >>** 192.168.1.100
- Sub Mask >>** 255.255.255.0
- Default Gateway >>** 192.168.1.254

Performance metrics are shown in a table:

Metric	Value
Link Quality	>> 100%
Signal Strength 1	>> 65%
Signal Strength 2	>> 39%
Noise Strength	>> 26%

Transmission and reception statistics are also provided:

- Transmit:** Link Speed >> 243.0 Mbps, Throughput >> 0.000 Kbps. A bar chart shows a maximum throughput of 5.392 Kbps.
- Receive:** Link Speed >> 40.5 Mbps, Throughput >> 98.612 Kbps. A bar chart shows a maximum throughput of 118.432 Kbps.

Additional HT (High Throughput) parameters are listed at the bottom:

- BW >>** 40
- GI >>** long
- MCS >>** 14
- SNR0 >>** 20
- SNR1 >>** n/a

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

The screenshot displays the WPS configuration interface. At the top, the 'WPS' menu item is selected. The 'WPS AP List' section contains the following data:

ID	SSID	MAC	Count
wlan-ap	wlan-ap	00-1D-92-C0-13-CD	1
wlan-ap	wlan-ap	00-04-ED-22-22-23	1

The 'WPS Profile List' shows a single profile: 'ExRegNWEA4036'. Below this, the 'WPS Associate IE' and 'WPS Probe IE' checkboxes are checked. The progress bar indicates 'Progress >> 0%' and the status is 'WPS status is disconnected'. On the right-hand side, the 'Pin Code' is set to '25879810' and the 'Config Mode' is set to 'Registrar'. A dialog box at the bottom provides the following configuration details:

- SSID >> ExRegNWEA4036
- BSSID >> 00-00-00-00-00-00
- Authentication Type >> WPA2-PSK
- Encryption Type >> AES
- Key Length >> 5
- Key Index >> 1
- Key Material >> 811B5B9F3403DCB08BA73BF3E4787581C37DC4BDD147C4E62526D4E8C39D8F78
- Show Password

Buttons for 'OK' and 'Cancel' are located at the bottom of the dialog box.

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

Configuration

Wireless

Parameters

WLAN Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Time Schedule	1. Always On <input type="checkbox"/> 2. TimeSlot1 <input type="checkbox"/>
Mode	802.11g + n
ESSID	wlan-ap
Hide ESSID	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Regulation Domain	N.America
Channel ID	Channel 1 (2.412 GHz)
Channel Width	20/40MHZ
Tx PowerLevel	100 (0 ~ 100)
AP MAC Address	00:1D:92:C0:13:CD
AP Firmware Version	2.4.0.0
WPS Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
WPS State	<input type="radio"/> Configured <input checked="" type="radio"/> Unconfigured
WMM	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Wireless Distribution System (WDS)	
WDS Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Peer WDS MAC address	1. <input type="text"/> 2. <input type="text"/> 3. <input type="text"/> 4. <input type="text"/>

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

[Security settings ▶](#)

Configuration

Wireless Security

Parameters

Security Mode	WPAWPA2-PSK
WPA Algorithms	AES
WPA Shared Key	811B5B9F3403DCB08
Group Key Renewal	3600 seconds

PBC Method:

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

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

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

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

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


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

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

ID	SSID	MAC Address	Priority
wlan-ap	wlan-ap	00-1D-92-C0-13-CD	1
wlan-ap	wlan-ap	00-04-ED-38-F7-2E	1
- WPS Profile List:** Shows the selected profile 'wlan-ap'.
- Configuration Options:**
 - WPS Associate IE
 - WPS Probe IE
- Buttons:** PIN, PBC, Rescan, Information, Pin Code (16837546), Renew, Config Mode (Enrollee), Detail, Connect, Rotate, Disconnect, Export Profile, Delete.
- Progress Bar:** Shows 'Progress >> 100%' and a message: 'PBC - Get WPS profile successfully.'
- Status and Link Quality:**
 - Status >> wlan-ap <-> 00-1D-92-C0-13-CD
 - Extra Info >> Link is Up [TxPower:100%]
 - Channel >> 1 <-> 2412 MHz; central channel : 3
 - Authentication >> Open
 - Encryption >> NONE
 - Network Type >> Infrastructure
 - IP Address >> 192.168.1.100
 - Sub Mask >> 255.255.255.0
 - Default Gateway >> 192.168.1.254
- HT (High Throughput) Information:**
 - BW >> 40
 - GI >> long
 - MCS >> 14
 - SNR0 >> 20
 - SNR1 >> n/a
- Transmit and Receive Performance:**
 - Transmit: Link Speed >> 243.0 Mbps, Throughput >> 0.192 Kbps. Signal strength bars show Link Quality >> 100%, Signal Strength 1 >> 60%, Signal Strength 2 >> 44%, and Noise Strength >> 26%.
 - Receive: Link Speed >> 81.0 Mbps, Throughput >> 93.732 Kbps.

Wi-Fi Network Setup with Windows Vista WCN:

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

Configuration 

▼ Wireless

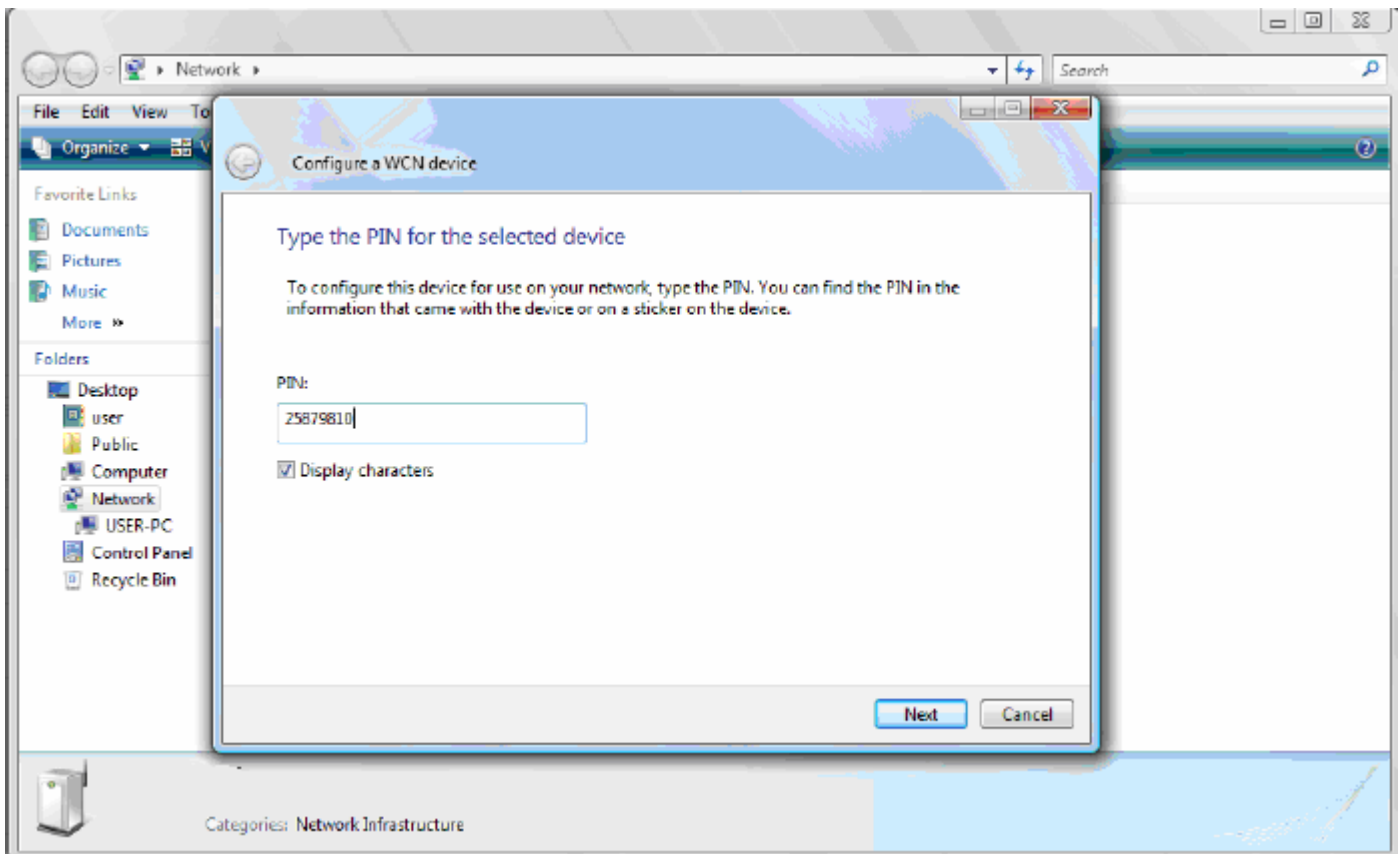
Parameters

WLAN Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Time Schedule	1. <input type="checkbox"/> Always On <input checked="" type="checkbox"/> 2. <input type="checkbox"/> TimeSlot1
Mode	802.11g + n
ESSID	wlan-ap
Hide ESSID	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Regulation Domain	N.America
Channel ID	Channel 1 (2.412 GHz)
Channel Width	20/40MHZ
Tx PowerLevel	100 (0 ~ 100)
AP MAC Address	00:1D:92:C0:13:CD
AP Firmware Version	2.4.0.0
WPS Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
WPS State	<input type="radio"/> Configured <input checked="" type="radio"/> Unconfigured
WMM	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Wireless Distribution System (WDS)	
WDS Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Peer WDS MAC address	1. <input type="text"/> 2. <input type="text"/> 3. <input type="text"/> 4. <input type="text"/>

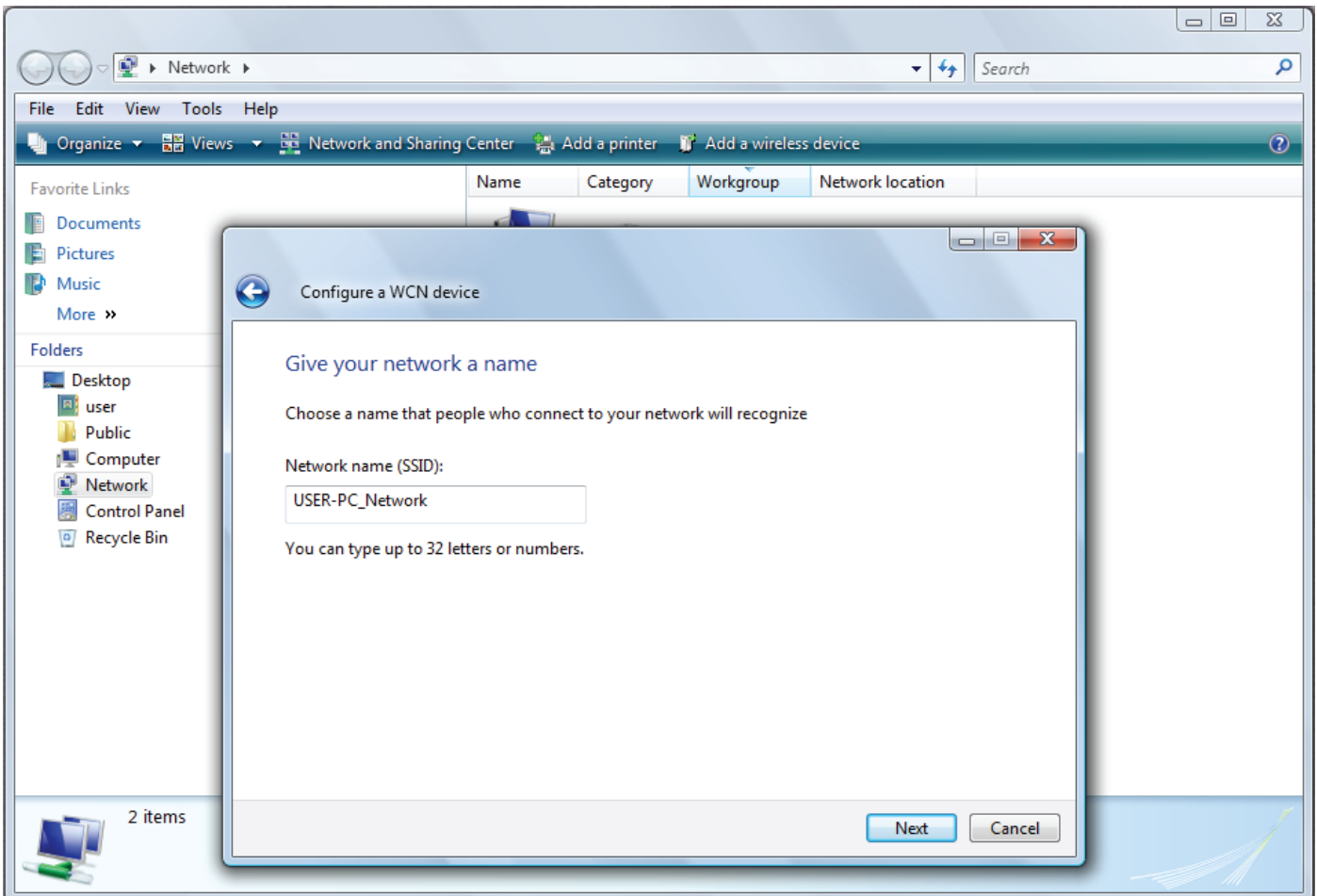
** WDS depends on the settings of main security encryption type. **

[Security settings ▶](#)

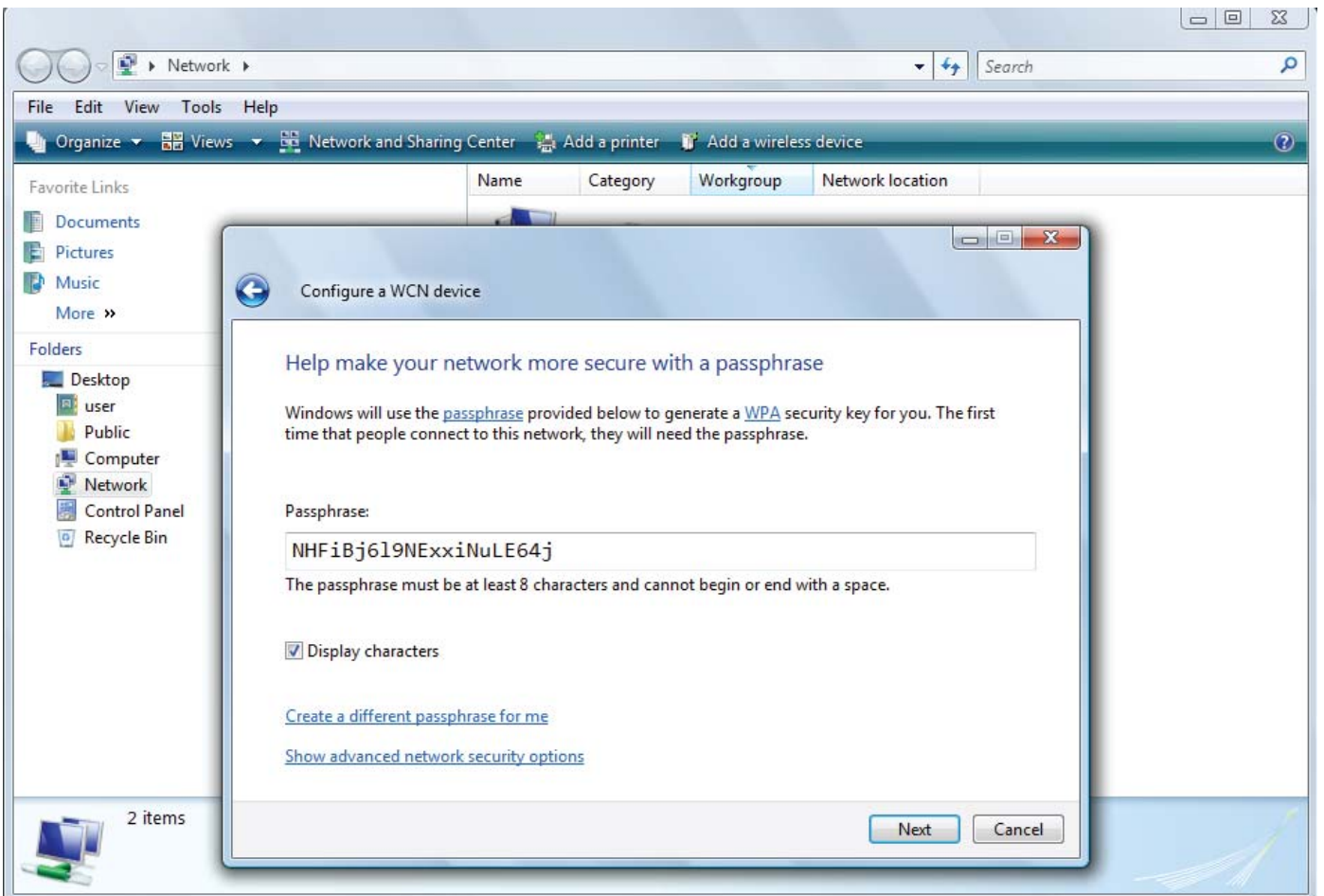
3. In your Vista operating system, access the Control Panel page, then select Network and Internet > View Network Computers and Devices. Double click on the BiPAC 7300W icon and enter the AP PIN in the column provided then press Next.



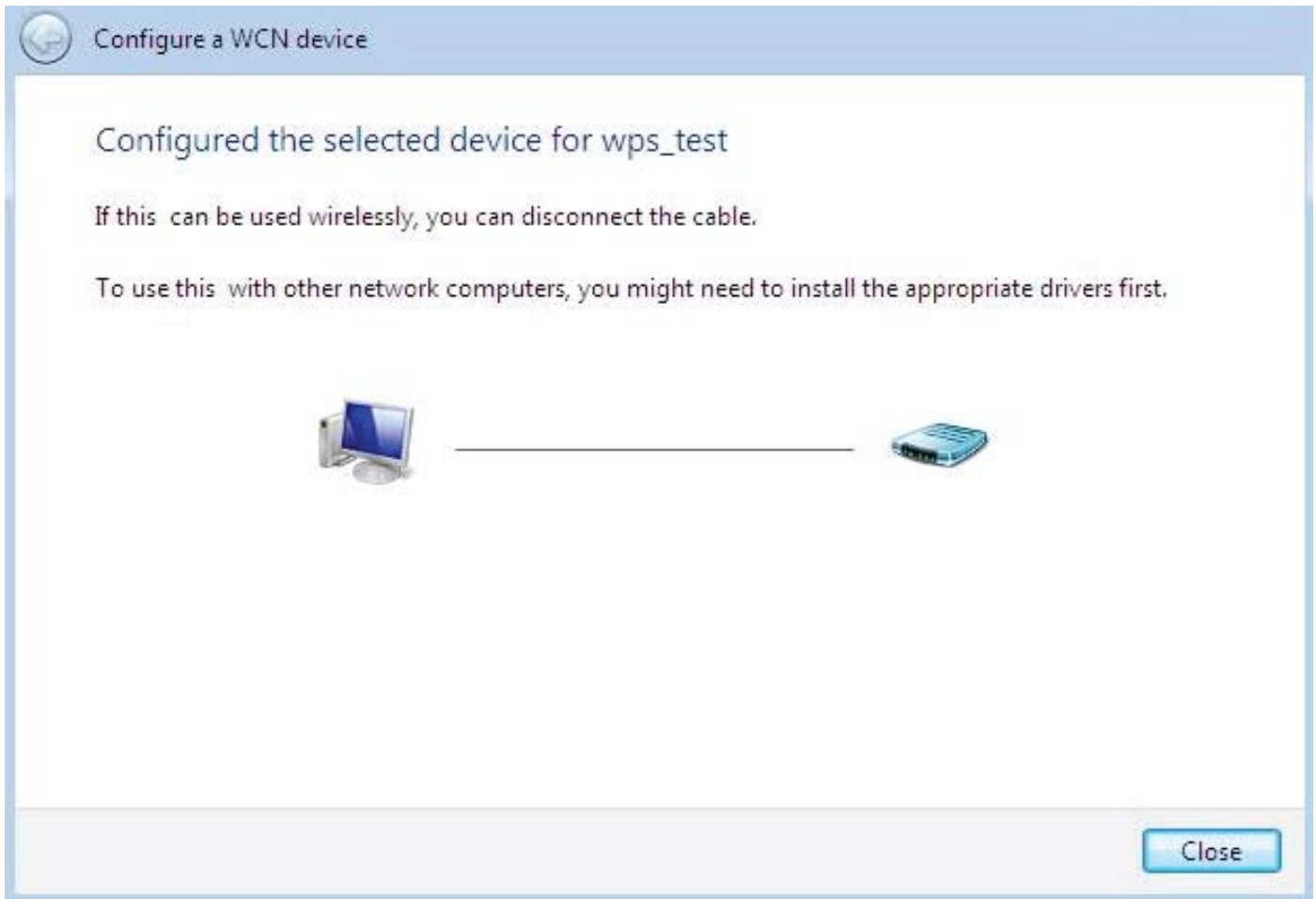
4. Enter the AP SSID then click Next.



5. Enter the Passphrase then click Next.



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

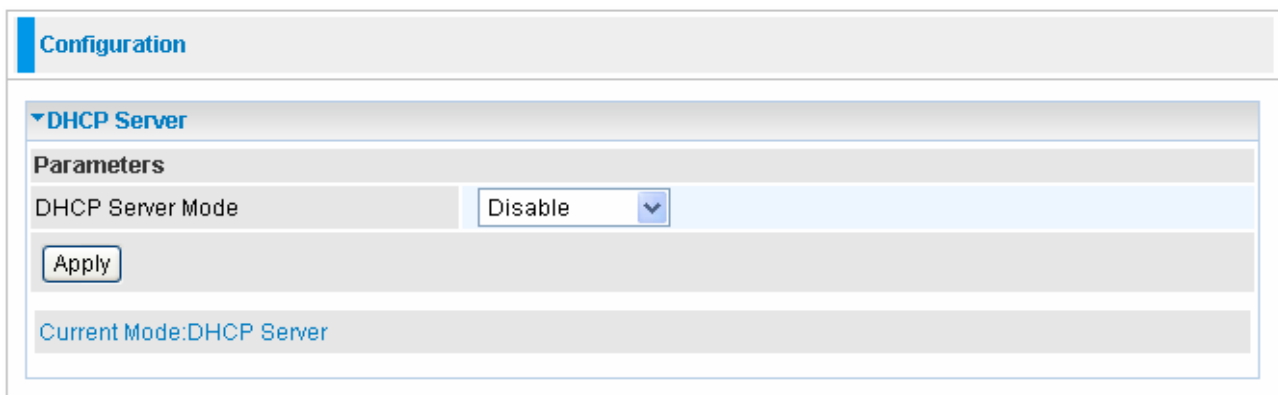


5.3.1.6 DHCP Server

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

DHCP Server Mode: Disable

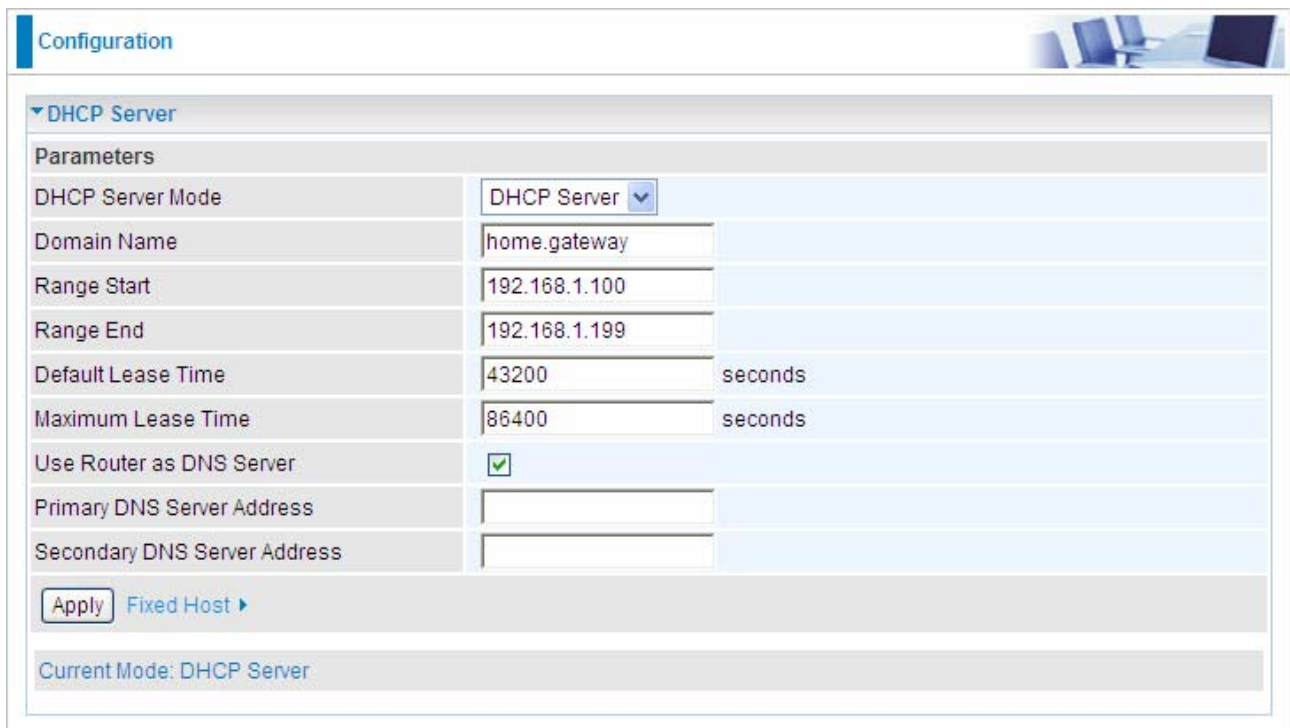
To disable the router's DHCP Server, check **Disabled** and then click **Apply**. When the DHCP Server is disabled, you will need to manually assign a fixed IP address to each PC on your network, and set the default gateway for each PC to the IP address of the router (the default is 192.168.1.254).



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

DHCP Server Mode: DHCP Server

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



The screenshot shows the 'Configuration' page for the DHCP Server. The 'DHCP Server' section is expanded, showing the following parameters:

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

Buttons: [Apply](#) [Fixed Host ▶](#)

Current Mode: DHCP Server

Fixed Host: click Fixed Host link to enter, the following will appear. The Specified IP Address will be assigned to the corresponding MAC address by DHCP.



The screenshot shows the 'Fixed Host' configuration page. The 'Fixed Host' section is expanded, showing a table with the following columns:

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

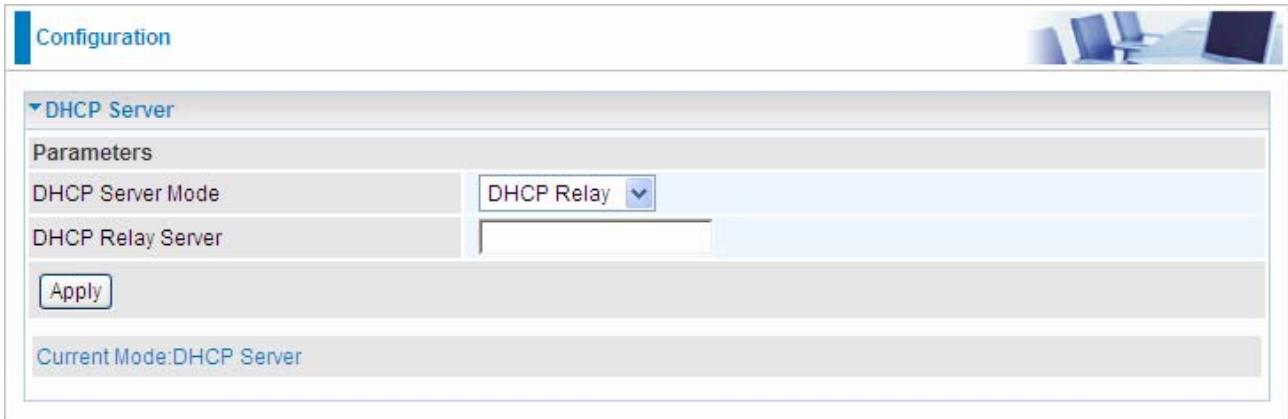
** Please note that the IP Address cannot be set within the DHCP server's range. **

Buttons: [Add](#) [Edit / Delete](#) [Return ▶](#)

Note: the IP Address you want to enter can't be within the DHCP Server range. Click Add to add the item, and the corresponding message will be listed below.

DHCP Server Mode: DHCP Relay

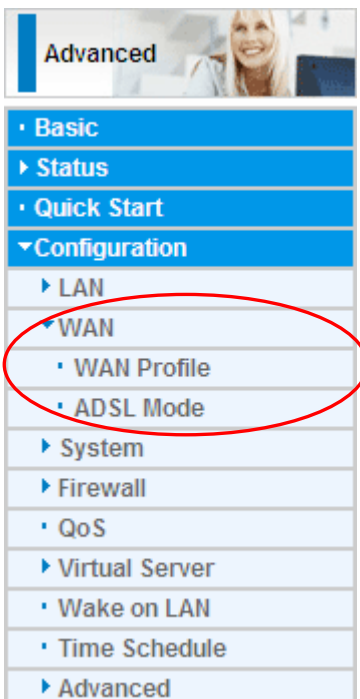
If you check **DHCP Relay** and then you must enter the IP address of the DHCP server which assigns an IP address back to the DHCP client in the LAN. Use this function only if advised to do so by your network administrator or ISP. Click **Apply** to enable this function.



The screenshot shows a web interface for configuring a DHCP server. At the top, there is a 'Configuration' tab. Below it, the 'DHCP Server' section is expanded. Under 'Parameters', the 'DHCP Server Mode' is set to 'DHCP Relay' via a dropdown menu. The 'DHCP Relay Server' field is empty. An 'Apply' button is visible below the fields. At the bottom, it indicates 'Current Mode: DHCP Server'.

5.3.2 WAN (Wide Area Network)

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



5.3.2.1 WAN Profile

Main Port--ADSL

● PPPoE Connection (ADSL)

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

The screenshot shows the 'Configuration' page for a WAN Profile. The 'WAN Profile' section is expanded, showing 'Parameters'. The 'Main Port' is set to 'ADSL' (Current Main Port: EWAN). The 'Protocol' is set to 'PPPoE (RFC2516, PPP over Ethernet)', which is circled in red. Other settings include: Description (empty), VPI/VCI (8/35), Encap. method (LLC), Username (Username), Password (masked with dots), Service Name (empty), NAT (checked Enable), IP (0.0.0.0: Auto), Auth. Protocol (Auto), Obtain DNS (checked Automatic), Primary (empty), Secondary (empty), Connection (checked Always On), Idle Timeout (0 min(s)), MTU (1492), and MAC Spoofing (unchecked Enable). Below the parameters are 'Add' and 'Apply / Edit / Delete' buttons. At the bottom is a table with columns: Edit, Protocol, Interface, Description, VPI, VCI, Encap. method, NAT, IP, and Delete. The table contains one entry: a green plus icon, PPPoE, wan_main, (empty), 8, 35, LLC, Enable, 0.0.0.0, and (empty).

- **Description:** A user-definable name for this connection.
- **VPI/VCI:** Enter the VPI and VCI information provided by your ISP.
- **Encap. method:** Select the encapsulation format, the default is LLC. Select the one provided by your ISP
- **Username:** Enter the username provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive). This is in the format of “username@ispname” instead of simply “username”.
- **Password:** Enter the password provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive)
- **Service Name:** This item is for identification purposes. If it is required, your ISP provides you the information. Maximum input is **15** alphanumeric characters.
- **NAT:** The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single ISP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

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

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

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

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

● **Connection:**

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

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

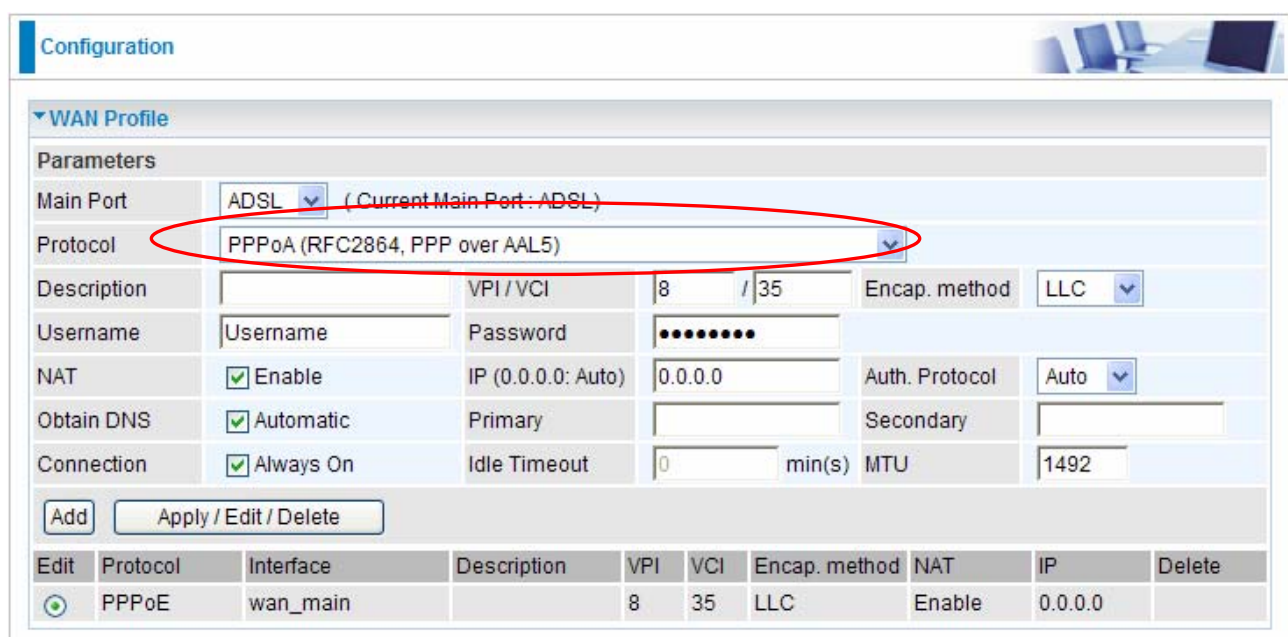
● **Idle Timeout:** Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time. The minimum value is 10 minutes.

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

● **MAC Spoofing:** This option is required by some service Providers. You must fill the MAC address specified by your service provider when this information is required. The default setting is set to disable.

● PPPoA Connection (ADSL)

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



Configuration

WAN Profile

Parameters

Main Port: ADSL (Current Main Port: ADSL)

Protocol: PPPoA (RFC2864, PPP over AAL5)

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

Username: Username Password:

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

Obtain DNS: Automatic Primary: Secondary:

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

Add Apply / Edit / Delete

Edit	Protocol	Interface	Description	VPI	VCI	Encap. method	NAT	IP	Delete
<input checked="" type="radio"/>	PPPoE	wan_main		8	35	LLC	Enable	0.0.0.0	

- **Description:** User-definable name for the connection.
- **VPI/VCI:** Enter the VPI and VCI information provided by your ISP.
- **Encapsulation method:** Select the encapsulation format, the default is LLC. Select the one provided by your ISP
- **Username:** Enter the username provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive). This is in the format of “username@ispname” instead of simply “username”.
- **Password:** Enter the password provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive).
- **NAT:** The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.
- **IP Address:** Your WAN IP address. Leave this at 0.0.0.0 to automatically obtain an IP address from your ISP.
- **Authentication Protocol:** Default is **Auto**. Your ISP should advise you on whether to use **Chap** or **Pap**.
- **Obtain DNS Automatically:** Select this check box to use DNS.
- **Primary DNS/ Secondary DNS:** Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the Netmask.
- **Connection:**
 - ⊙ **Always on:** The router will establish a PPPoA session when starting up and to automatically re-establish the PPPoA session when disconnected by the ISP.
 - ⊙ **Connect to Demand (un-select Always On):** If you want to establish a PPPoA session only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet). In this mode, you must set Idle Timeout value at same time.
- **Idle Timeout:** Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time. The minimum value is 10 minutes.
- **MTU:** Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that the IP attempts to send through the interface.

MPoA Connection (ADSL)

Configuration

WAN Profile

Parameters

Main Port: ADSL (Current Main Port: EWAN)

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

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

Encap. mode: Bridged NAT: Enable Keep Alive: Enable

IP (0.0.0.0: Auto): 0.0.0.0 Netmask: 255.255.255.0 Gateway: []

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

MAC Spoofing: Enable []

Add Apply / Edit / Delete

Edit	Protocol	Interface	Description	VPI	VCI	Encap. method	NAT	IP	Delete
<input checked="" type="checkbox"/>	PPPoE	wan_main		8	35	LLC	Enable	0.0.0.0	

- **Description:** Your description of this connection.
- **VPI and VCI:** Enter the VPI and VCI information provided by your ISP.
- **Encap. method:** Select the encapsulation format, the default is LLC. Select the one provided by your ISP.
- **Encap. mode:** Choose whether you want the device to function as bridge mode or routing mode.
- **NAT:** The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing the single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.
- **Keep Alive:** Set Enable to keep the router on line and prevent to be disconnected by the ISP when they think there is no activity on the line.
- **IP Address:** Your WAN IP address. Leave this at 0.0.0.0 to automatically obtain an IP address from your ISP.
- **Netmask:** The default is 255.255.255.0. User can change it to other such as 255.255.255.128. Type the netmask assigned to you by your ISP (if given)
- **Gateway:** Enter the IP address of the default gateway.
- **Obtain DNS Automatically:** Select this check box to use DNS.
- **Primary DNS/ Secondary DNS:** Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the netmask.
- **MAC Spoofing:** This option is required by some service Providers. You must fill the MAC address specified by your service provider when this information is required. The default setting is set to disable.

● Pure Bridge Connections (ADSL)

Configuration

WAN Profile

Parameters

Main Port: ADSL (Current Main Port: ADSL)

Protocol: Pure Bridge

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

Add Apply / Edit / Delete

Edit	Protocol	Interface	Description	VPI	VCI	Encap. method	NAT	IP	Delete
<input checked="" type="radio"/>	PPPoE	wan_main		8	35	LLC	Enable	0.0.0.0	

● **Description:** A user-definable name for this connection.

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

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

● PPPoE with Pass-through (ADSL)

Configuration

WAN Profile

Parameters

Main Port: ADSL (Current Main Port: ADSL)

Protocol: PPPoE with Pass-through

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

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

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

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

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

MAC Spoofing: Enable []

Add Apply / Edit / Delete

Edit	Protocol	Interface	Description	VPI	VCI	Encap. method	NAT	IP	Delete
<input checked="" type="radio"/>	PPPoE	wan_main		8	35	LLC	Enable	0.0.0.0	

● **Description:** A user-definable name for this connection.

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

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

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

● **Password:** Enter the password provided by your ISP. You can input up to 128

alphanumeric characters (case sensitive)

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

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

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

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

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

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

● **Connection:**

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

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

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

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

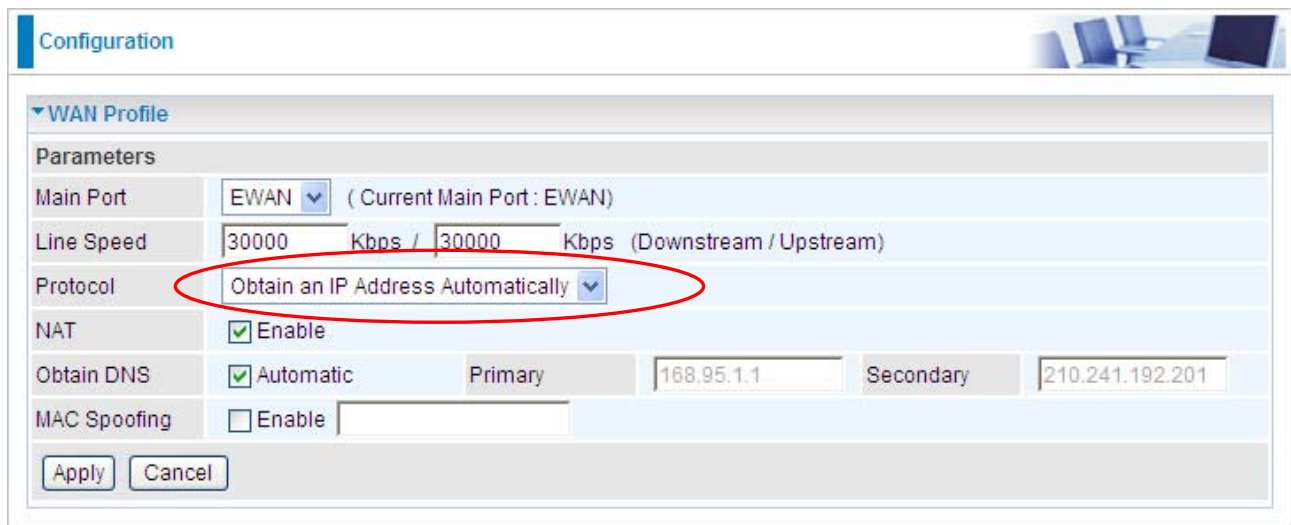
● **MAC Spoofing:** This option is required by some service Providers. You must fill the MAC address specified by your service provider when this information is required. The default setting is set to disable.

Main Port—EWAN

Besides using ADSL to get connected to the Internet, BiPAC 7300W offers its Ethernet port 1 as a WAN port to be used to connect to Cable Modems, VDSL and fibre optic lines. This alternative, yet faster method to connect to the internet will provide users with more flexibility to get online

● Obtain an IP Address Automatically (EWAN)

When connecting to the ISP, BiPAC 7300W also functions as a DHCP client. BiPAC 7300W can automatically obtain an IP address, netmask, gateway address, and DNS server addresses if the ISP assigns this information via DHCP.



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

Main Port	EWAN	(Current Main Port : EWAN)
Line Speed	30000 Kbps / 30000 Kbps	(Downstream / Upstream)
Protocol	Obtain an IP Address Automatically	
NAT	<input checked="" type="checkbox"/> Enable	
Obtain DNS	<input checked="" type="checkbox"/> Automatic	Primary: 168.95.1.1, Secondary: 210.241.192.201
MAC Spoofing	<input type="checkbox"/> Enable	

Buttons: Apply, Cancel

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

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

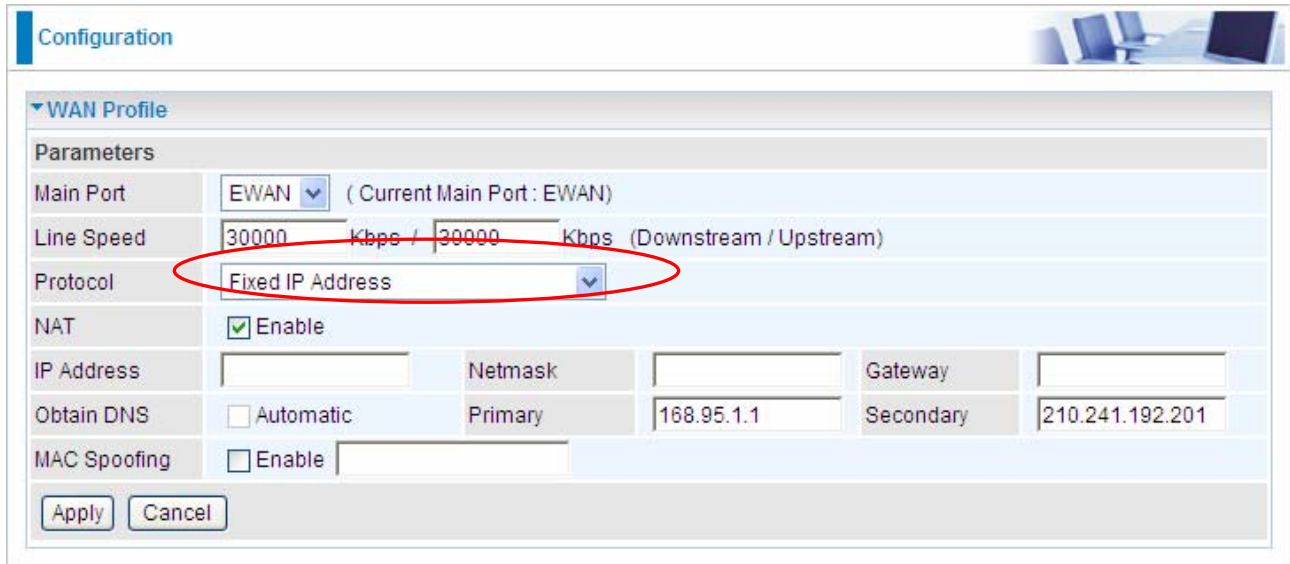
● **Obtain DNS Automatically:** Select this check box to use DNS.

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

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

● Fixed IP Address (EWAN)

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



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

- Main Port:** EWAN (Current Main Port: EWAN)
- Line Speed:** 30000 Kbps / 30000 Kbps (Downstream / Upstream)
- Protocol:** Fixed IP Address (highlighted with a red circle)
- NAT:** Enable
- IP Address:** [Empty field]
- Netmask:** [Empty field]
- Gateway:** [Empty field]
- Obtain DNS:** Automatic
- Primary DNS:** 168.95.1.1
- Secondary DNS:** 210.241.192.201
- MAC Spoofing:** Enable [Empty field]

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

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

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

● **IP Address:** Enter your WAN IP address.

● **IP Netmask:** Type the netmask assigned to you by your ISP (if given).

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

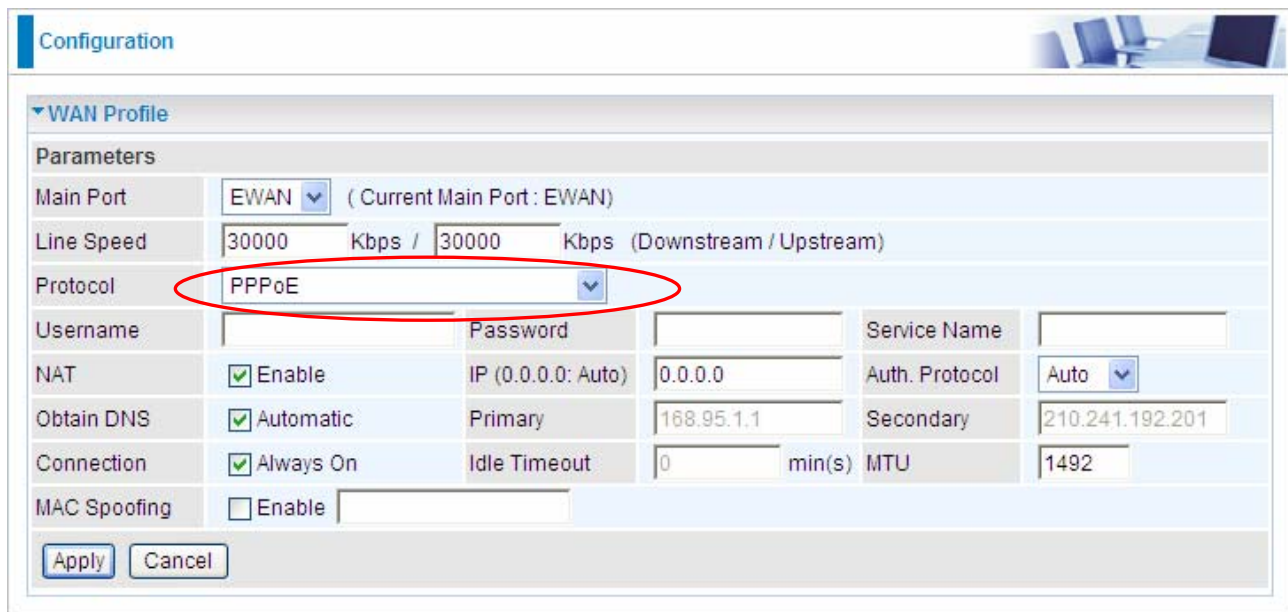
● **Obtain DNS Automatically:** Select this check box to use DNS.

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

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

● PPPoE (EWAN)

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



The screenshot shows a configuration page titled "Configuration" with a "WAN Profile" section. The "Parameters" table is as follows:

Parameters					
Main Port	EWAN	(Current Main Port : EWAN)			
Line Speed	30000	Kbps /	30000	Kbps	(Downstream / Upstream)
Protocol	PPPoE				
Username		Password		Service Name	
NAT	<input checked="" type="checkbox"/> Enable	IP (0.0.0.0: Auto)	0.0.0.0	Auth. Protocol	Auto
Obtain DNS	<input checked="" type="checkbox"/> Automatic	Primary	168.95.1.1	Secondary	210.241.192.201
Connection	<input checked="" type="checkbox"/> Always On	Idle Timeout	0	min(s)	MTU
MAC Spoofing	<input type="checkbox"/> Enable				1492

Buttons: Apply, Cancel

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

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

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

● **Service Name:** Enter a name for this connection.

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

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

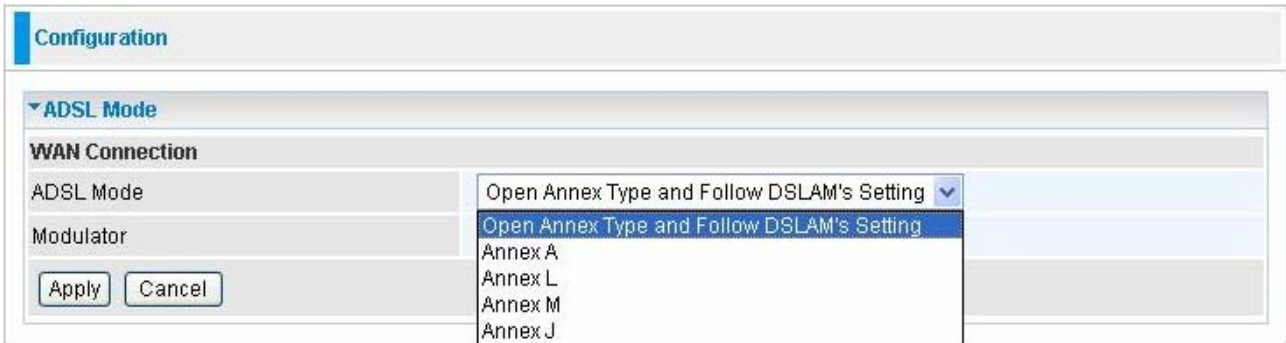
● **Auth. Protocol:** Default is **Auto**. Your ISP advises on using **Chap** or **Pap**.

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

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

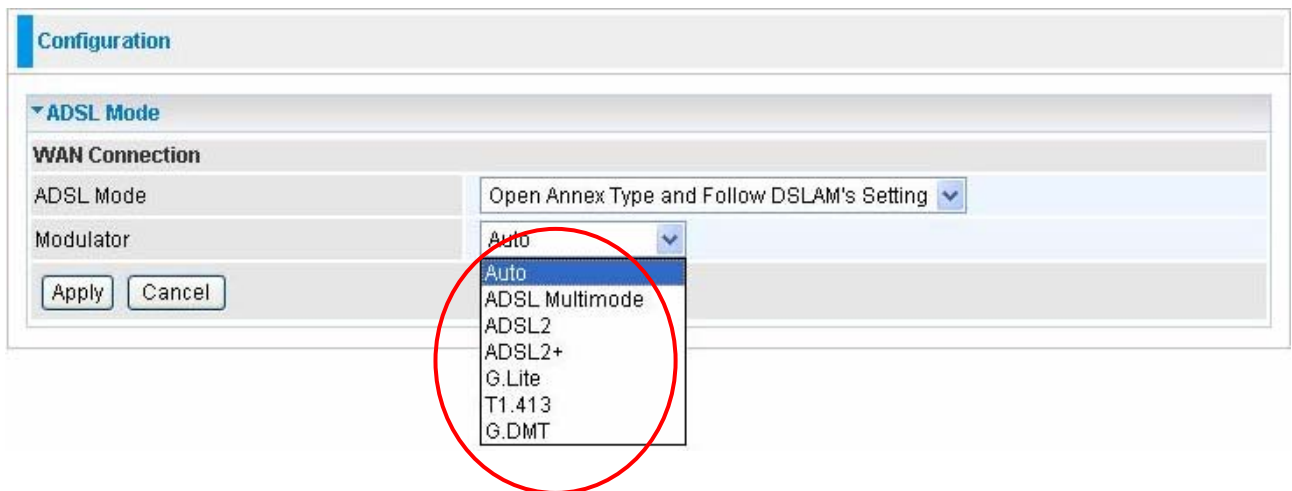
● **MAC Spoofing:** Select Enable and enter a MAC address that will temporarily change your router’s MAC address to the one you have specified in this field. Leave it as Disabled if you do not wish to change the MAC address of your router.

5.3.2.3 ADSL Mode



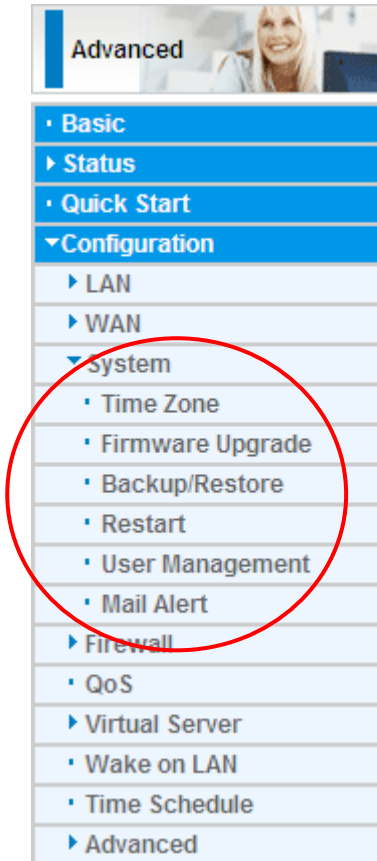
● **ADSL Mode:** There are four modes “Open Annex Type and Follow DSLAM’s Setting”, “Annex A”, “Annex L”, “Annex M” and “Annex J” that user can select for this connection.

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



5.3.3 System

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




5.3.3.1 Time Zone

Time Zone

Parameters

Time Zone	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Local Time Zone (+-GMT Time)	(GMT) Greenwich Mean Time ▼	
SNTP Server IP Address	192.43.244.18	128.138.140.44
	129.6.15.29	131.107.1.10
Daylight Saving	<input checked="" type="checkbox"/> Automatic	
Resync Period	1440 minutes	

v



Apply Cancel

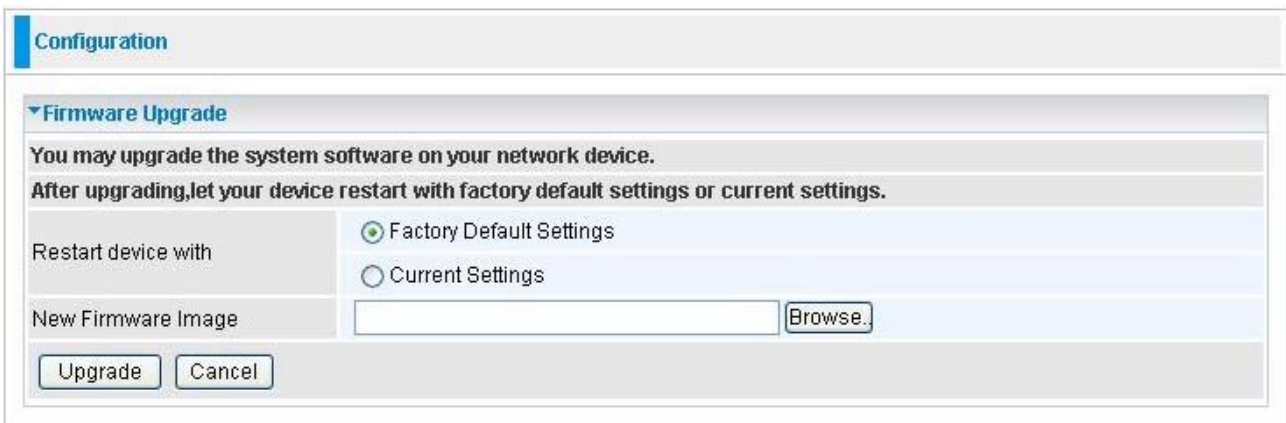
The router does not have a real time clock on board; instead, it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server outside your network. Choose your local time zone, click **Enable** and click the **Apply** button. After a successful connection to the Internet,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

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

5.3.3.2 Firmware Upgrade

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

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



The screenshot shows a web interface for configuring a firmware upgrade. At the top, there is a 'Configuration' tab. Below it, the 'Firmware Upgrade' section is expanded. The page contains the following elements:

- A heading: "You may upgrade the system software on your network device."
- A sub-heading: "After upgrading, let your device restart with factory default settings or current settings."
- A section labeled "Restart device with" containing two radio buttons: "Factory Default Settings" (which is selected) and "Current Settings".
- A section labeled "New Firmware Image" containing a text input field and a "Browse..." button.
- At the bottom, there are two buttons: "Upgrade" and "Cancel".

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

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

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

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



Warning

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

5.3.3.3 Backup / Restore

The screenshot shows a web interface for router configuration. At the top, there is a 'Configuration' tab. Below it, a section titled 'Backup/Restore' is expanded. This section contains a description: 'Allows you to backup the configuration settings to your computer, or restore configuration from your computer.' Underneath, there are two main sections: 'Backup Configuration' and 'Restore Configuration'. The 'Backup Configuration' section has a single button labeled 'Backup'. The 'Restore Configuration' section includes a text input field for 'Configuration File' followed by a 'Browse...' button. Below the input field, there is a warning message: 'Restore will overwrite the current configuration and restart the device. If you want to keep the current configuration, please use "Backup" first to save current configuration.' At the bottom of the 'Restore Configuration' section is a button labeled 'Restore'.

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

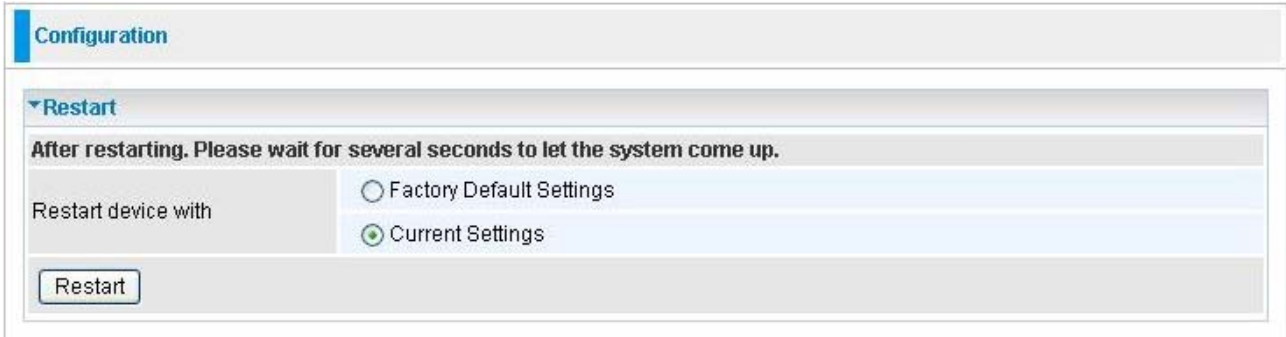
Press **Backup** to select where on your local PC to save the settings file. You may also change the name of the file when saving if you wish to keep multiple backups.

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

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

5.3.3.4 Restart Router

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



Configuration

Restart

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

Restart device with

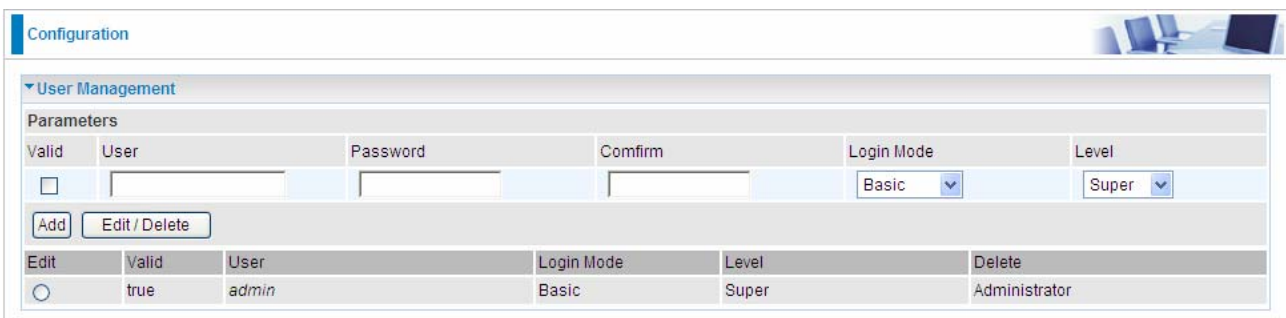
Factory Default Settings

Current Settings

Restart

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

5.3.3.5 User Management



Configuration

User Management

Parameters

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

Add Edit / Delete

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

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

You are able to **Edit** existing users and **Add** new users who are able to access the device's configuration interface. Once you have clicked **Edit** on the account you want to edit, the information of the account will be displayed above. Just go ahead and change the password. You can change the user's **password**, whether their account is active and **Valid**. These options are the same when creating a user account, with the exception that once created you cannot change the username. You cannot delete the default admin account; however you can delete any other created accounts by clicking ticking the box under **Delete** and then press the **Edit/Delete** button.

You are strongly advised to change the password on the default "**admin**" account when you

receive your router, and any time you reset your configuration to Factory Defaults.

5.3.3.6 Mail Alert

Send a log via email, if WAN IP is changed or if intruders accessing your computer without permission.

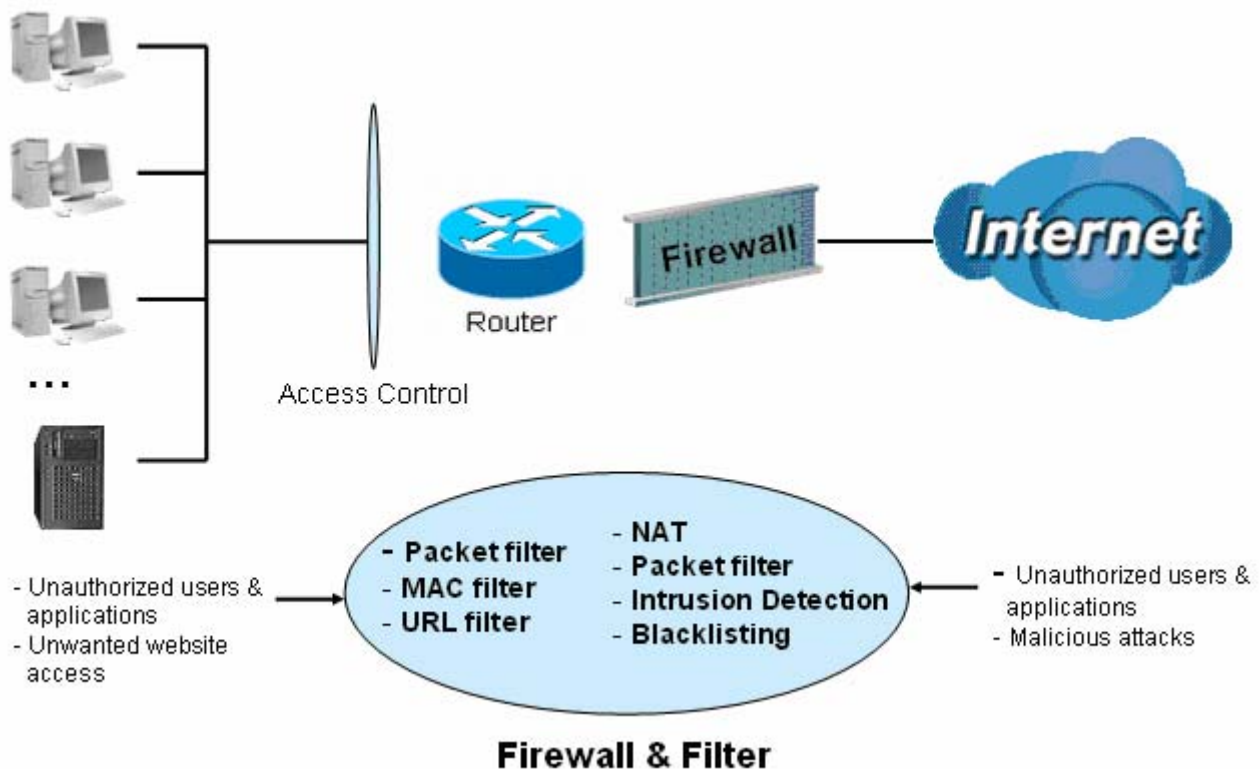
Mail Alert		
Server Information		
SMTP Server	<input type="text"/>	
Username	<input type="text"/>	
Password	<input type="text"/>	
Sender's E-mail	<input type="text"/>	(Must be xxx@yyy.zzz)
WAN IP Change Alert		
Recipient's E-mail	<input type="text"/>	(Must be xxx@yyy.zzz)
Intrusion Detection		
Alert Mail Time	<input type="text" value="30"/>	min(s)
Recipient's E-mail	<input type="text"/>	(Must be xxx@yyy.zzz)
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

- **SMTP Server:** Enter the SMTP server that you would like to use for sending emails.
- **Username:** Enter the username of your email account to be used by the SMTP server.
- **Password:** Enter the password of your email account.
- **Sender's Email:** Enter your email address.
- **Recipient's Email (WAN IP Change Alert):** Enter the email address that will receive the alert message once a computer / network server failover occurs.
- **Alert Mail Time (Intrusion Detection):** The interval for sending alert mail.
- **Recipient's Email (Intrusion Detection):** Enter the email address that will receive the alert message once intrusion has been detected.

5.3.4 Firewall

Firewall and Access Control

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



Firewall: Prevents access from outside your network.

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



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

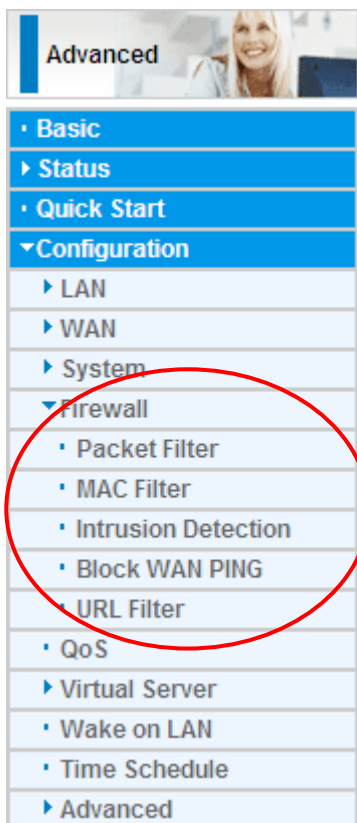
Firewall Security and Policy (General Settings): Inbound direction of Packet Filter rules prevent unauthorized computers or applications accessing your local network from the Internet.

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

MAC Filter rules: Prevents unauthorized computers accessing the Internet.

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

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



5.3.4.1 Packet Filter

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

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

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

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

● **Protocol:** Specify the packet type (TCP, UDP, ICMP, etc.) that the rule applies to. Select **TCP** if you wish to search for the connection-based application service on the remote server using the port number. Or select **UDP** if you want to search for the connectionless application service on the remote server using the port number.

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

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

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

- **Direction:** Determine whether the rule is for outgoing packets or for incoming packets.
- **Time Schedule:** It is self-defined time period. You may specify a time schedule for your prioritization policy. For setup and detail, refer to **Time Schedule** section.
- **Log:** Choose “log” if you wish to generate logs when the filter rule is applied to a packet.
- **Add:** Click this button to add a new packet filter rule and the added rule will appear at the bottom table.
- **Edit:** Check the Rule No. you wish to edit, and then click “Edit”.
- **Delete:** Check the Rule No. you wish to delete, and then click “Delete”.

- **Reorder:** Be aware that packet filtering parameters appear in priority order i.e. the first one takes precedence over all other rules. There is a sort function next to the Rule Name column, you can move the rule to higher or lower priority by clicking the Order arrow, and press “Reorder” to save the new priority.

Click **Add** to add the item configured and the corresponding information will be listed below just as the following.

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

Press **Edit** radio button, the item you want to re-edit will be displayed in the editing area, edit then press **Edit/Delete** to confirm your modification. If you want to delete the rule, check Delete, then press **Edit/Delete** to delete the rule.



Attention

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

5.3.4.2 MAC Filter

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

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



The format of MAC address could be: xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.

Filter Action

● **Action:** Select an action for MAC Filter. This feature is disabled by default. Check Allow or Block to activate the filter.

Parameters

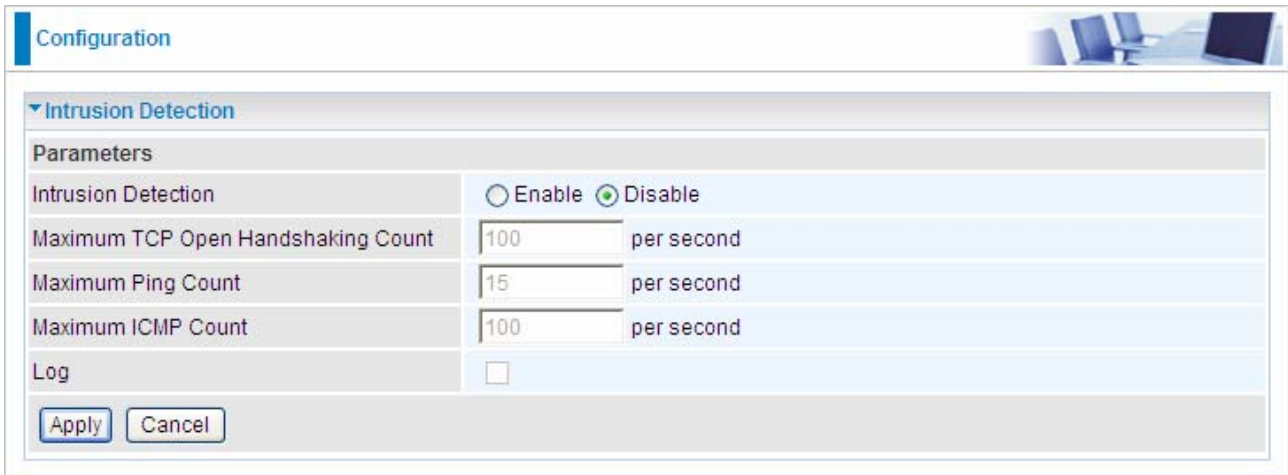
● **MAC Address:** Enter the Ethernet MAC addresses you wish to have the filter rule applies to.

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

For Add, Edit, Delete, see the **Packet filter**.

5.3.4.3 Intrusion Detection

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



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

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

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

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

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

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

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

Hacker attack types recognized by the IDS

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

Src IP: Source IP

Src Port: Source Port

Dst Port: Destination Port

Dst IP: Destination IP

5.3.4.4 Block WAN PING

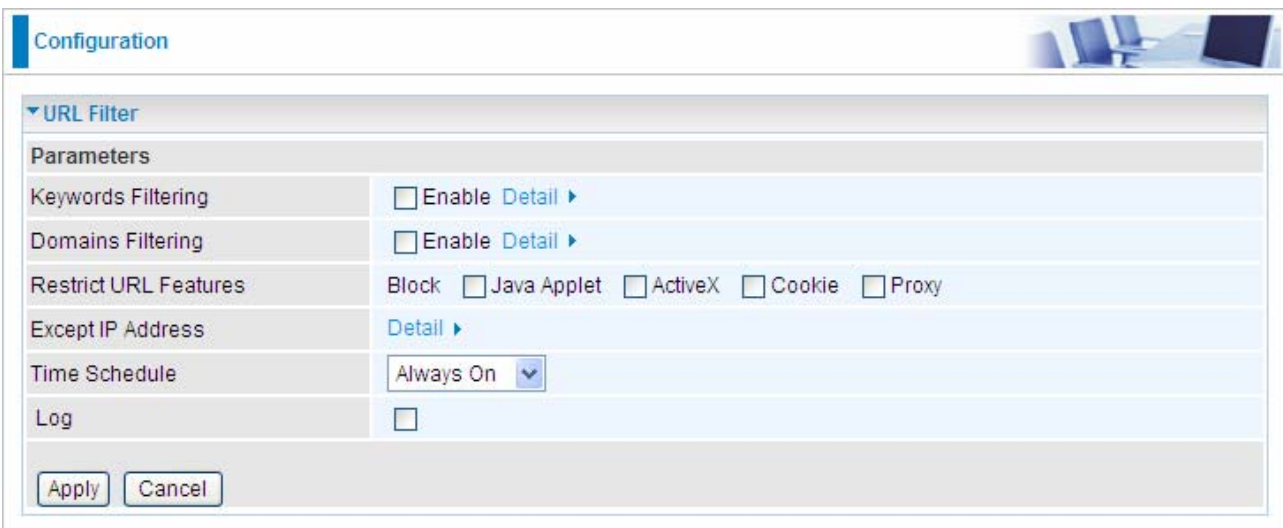
Check Enable if you wish to exclude outside PING requests from reaching this router.



Configuration	
▼ Block WAN PING	
Parameters	
Block WAN PING	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

5.3.4.5 URL Filter

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



Configuration	
▼ URL Filter	
Parameters	
Keywords Filtering	<input type="checkbox"/> Enable Detail ▶
Domains Filtering	<input type="checkbox"/> Enable Detail ▶
Restrict URL Features	Block <input type="checkbox"/> Java Applet <input type="checkbox"/> ActiveX <input type="checkbox"/> Cookie <input type="checkbox"/> Proxy
Except IP Address	Detail ▶
Time Schedule	Always On ▼
Log	<input type="checkbox"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

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

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

“abcde” occurs in the URL.

Configuration

Keywords Filtering

Parameters

Keyword

[Return ▶](#)

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

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

Configuration

Domains Filtering

Parameters

Domain Name Type

[Return ▶](#)

Forbidden Domain

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

Trusted Domain

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

Restrict URL Features: This function enhances the restriction to your URL rules.

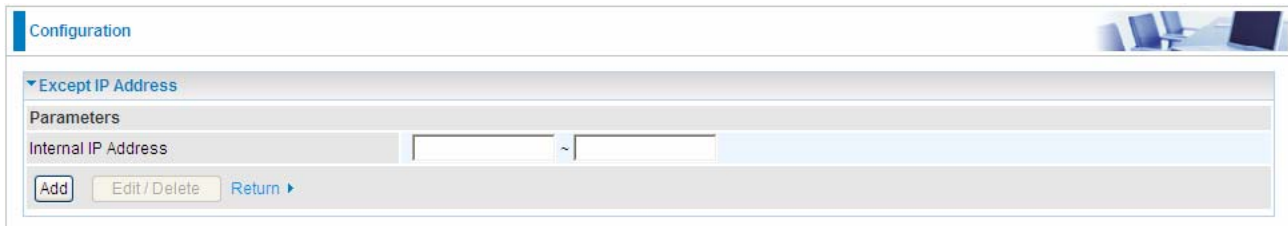
⊙ **Block Java Applet:** Blocks Web content which includes the Java Applet to prevent someone who wants to damage your system via the standard HTTP protocol.

⊙ **Block ActiveX:** Blocks ActiveX

⊙ Block Cookies: Blocks Cookies

⊙ Block Proxy: Blocks Proxy

● Except IP Address:



The screenshot shows a web-based configuration interface. At the top, there is a header bar with the word "Configuration" on the left and a small graphic of a desk with a laptop on the right. Below the header, there is a section titled "Except IP Address" with a dropdown arrow on the left. Underneath this title is a "Parameters" section. The "Internal IP Address" parameter is shown with two input fields separated by a tilde (~) symbol. At the bottom of the parameters section, there are three buttons: "Add", "Edit/Delete", and "Return" with a right-pointing arrow.

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

● **Log:** Click "Log" if you wish to generate logs when the filter rule is applied to the URL Filter.

5.3.5 QoS (Quality of Service)

Quality of Service Introduction

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

QoS: Keeping Your Net Connection Fast and Responsive

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

QoS Setup

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

Configuration

▼ QoS

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

Parameters

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

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

● **Application:** A name that identifies an existing policy.

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

There are two settings to be provided in the Router:

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

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

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

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

⊙ **TCP**

⊙ **UDP**

⊙ **ICMP**

⊙ **GRE:** For PPTP VPN Connections.

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

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

DSCP Mapping Table	
ADSL2+ Router	Standard DSCP
Disabled	None
Best Effort	Best Effort (000000)
Premium	Express Forwarding (101110)
Gold service (L)	Class 1, Gold (001010)
Gold service (M)	Class 1, Silver (001100)
Gold service (H)	Class 1, Bronze (001110)
Silver service (L)	Class 2, Gold (010010)
Silver service (M)	Class 2, Silver (010100)
Silver service (H)	Class 2, Bronze (010110)
Bronze service (L)	Class 3, Gold (011010)
Bronze service (M)	Class 3, Silver (011100)
Bronze service (H)	Class 3, Bronze (011110)

● **Rate Type:** 2 types are provided:

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

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

● **Ratio:** Assign the data ratio for this policy to be controlled. For examples, we want to only allow 20% of the total data transfer rate for the LAN-to-WAN direction to be used for FTP server. Then we can specify here with data ratio = 20. If you have ADSL LINE with 256K/bps.rate, the estimated data rate, in kbps, for this rule is $20\% * 256 * 0.9 = 46\text{kbps}$. (For 0.9 is an estimated factor for the effective data transfer rate for an ADSL LINE from LAN to WAN. For WAN-to-LAN, it is 0.85 to 0.8).

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

⊙ **High**

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

⊙ **Low**

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

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

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

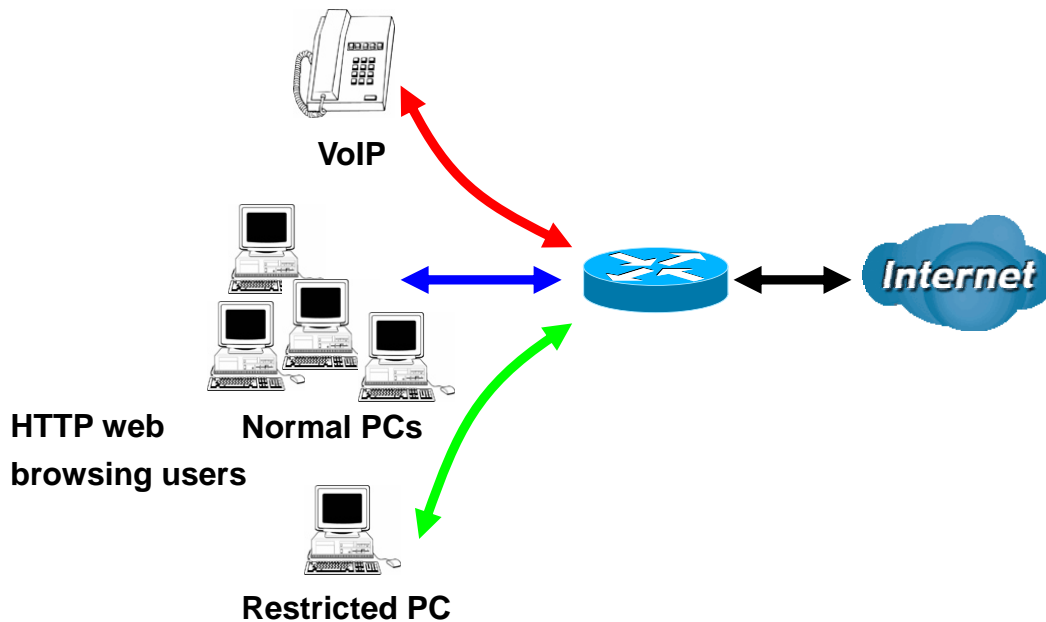
● **External IP Address:** The IP address values for Remote WAN machines you want to control. (For IP packets from LAN to WAN, it is the destination IP address. For IP packages from WAN to LAN, it is the source IP address.)

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

● **Time Schedule:** Scheduling your prioritization policy.

■ QoS example for your Network

Connection Diagram



ADSL Subscription Rate

Upstream: 256 kbps

Downstream: 2048 Mbps

Example QoS Plan

Application	IP or Ports	Control Flow	Data Rate	Time Schedule
VoIP User	192.168.1.1	Outgoing	Minimal 20% with high priority for non-used bandwidth with DSCP marking Class 1 Gold Service.	Always
FTP Sever	192.168.1.100	Incoming and Outgoing	outgoing: minimal 30%. Data rate. incoming: minimal 30%. Data rate. Both with low priority for non-used bandwidth.	Only Working Hours 9:00 to 17:00 Monday to Friday.
HTTP web browsing users	80	Incoming and Outgoing	outgoing: limited 20%. Data rate. incoming: limited 30%. Data rate.	Always

Example QoS Setup

Configuration

QoS

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

Parameters

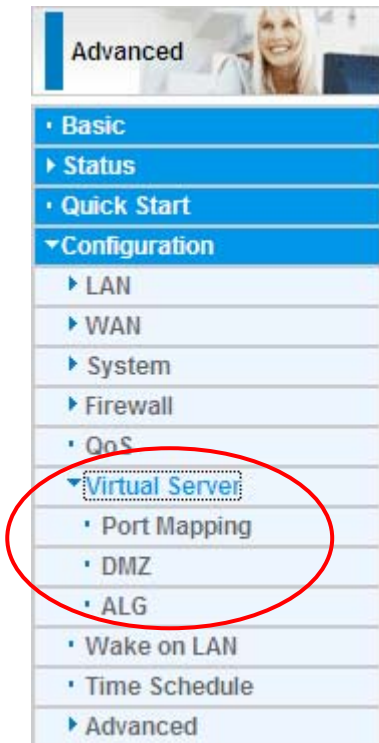
Application		Direction	LAN to WAN ▼	
Protocol	Any ▼	DSCP Marking	Disable ▼	
Rate Type	Guaranteed (Minimum) ▼	Ratio	<input type="text" value=""/> %	Priority ▼ Normal
Internal IP Address	<input type="text"/>	~	<input type="text"/>	Internal Port <input type="text"/>
External IP Address	<input type="text"/>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

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

VoIP application

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

5.3.6 Virtual Server



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

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

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

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

designated as “well-known ports”. The registered ports are numbered from 1024 through 49151. The remaining ports, referred to as dynamic ports, or private ports, are numbered from 49152 through 65535.

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

Well-known and Registered Ports

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

5.3.6.1 Port Mapping

The screenshot shows a web-based configuration interface for port mapping. It is titled 'Configuration' and has a sub-section 'Port Mapping'. Under 'Parameters', there are several fields: 'Application' is a listbox with '--select--' and a note '(type or select from listbox)'; 'Protocol' is a dropdown menu with 'TCP'; 'Internal IP Address' is a listbox with '--select--' and a note '(type or select from listbox)'; 'Internal Port' is a text input field; 'External Port' is a range input field with a tilde symbol; and 'Time Schedule' is a dropdown menu with 'Always On'. At the bottom of the configuration area, there are two buttons: 'Add' and 'Edit / Delete'.

- **Application:** Select the service you wish to configure
- **Protocol:** Automatic when you choose Application from listbox or select a protocol type which you want.
- **External Port & Internal Port:** Enter the public port number & range you wish to configure.
- **Internal IP Address:** Enter the IP address of a specific internal server to which requests from the specified port is forwarded.
- **Add:** Click to add a new virtual server rule. Click again and the next figure appears.
- **Edit:** Check the Rule No. you wish to edit and then click “Edit/Delete”.
- **Delete:** Check the Rule No. you wish to delete then click “Edit/Delete”.

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

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

Configuration

Port Mapping

Parameters

Application: << --select-- (type or select from listbox)

Protocol: External Port: ~

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

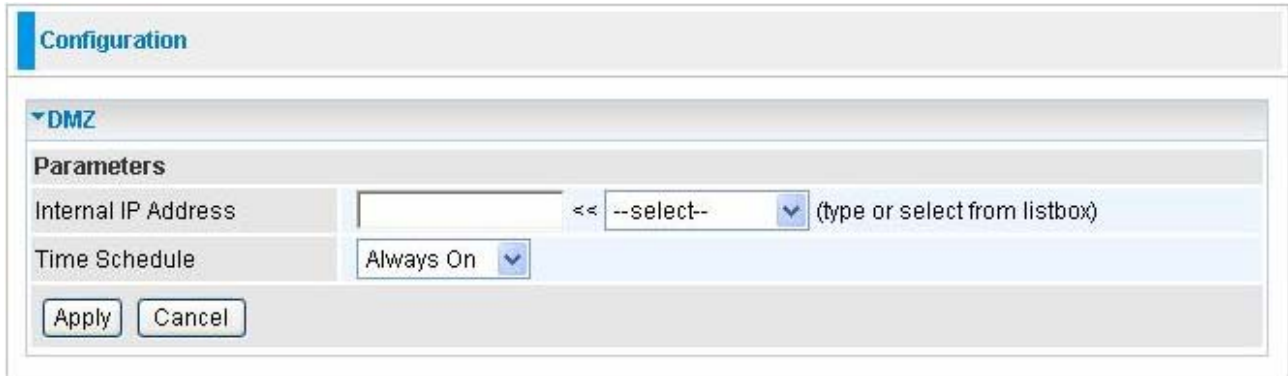
Internal Port: Time Schedule:

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

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

5.3.6.2 DMZ

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



The image shows a configuration window titled "Configuration" with a sub-section for "DMZ". Under the "Parameters" heading, there are two fields: "Internal IP Address" and "Time Schedule". The "Internal IP Address" field contains a text input box, a dropdown menu with "--select--", and a note "(type or select from listbox)". The "Time Schedule" field contains a dropdown menu with "Always On". At the bottom of the window are "Apply" and "Cancel" buttons.

DMZ Parameters	
Internal IP Address	<input type="text"/> << --select-- (type or select from listbox)
Time Schedule	Always On

5.3.6.3 ALG

Controls enable or disable various protocols over application layer.



For example, SIP ALG:

Enable: When SIP phone need ALG to pass through the NAT.

Disable: When SIP phone included NAT-Traversal algorithm. Turn off the SIP ALG.



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

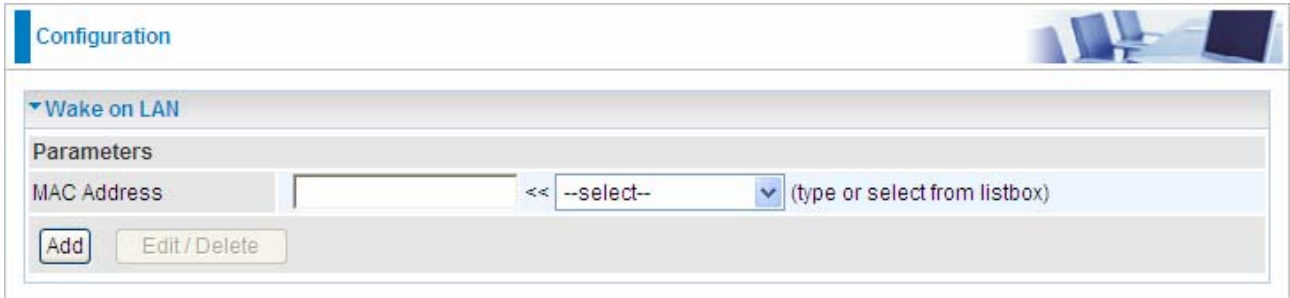


Attention

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

5.3.7 Wake on LAN

This feature provides greater flexibility for users to turn on / boot the computer of the network from a remotely site.



The screenshot shows a web-based configuration interface. At the top, there is a blue header with the word "Configuration" and a small image of a computer workstation. Below the header, there is a section titled "Wake on LAN" with a dropdown arrow. Underneath, there is a "Parameters" section. The "MAC Address" field is highlighted in light blue and contains a text input box followed by a dropdown menu showing "--select--" and a "(type or select from listbox)" prompt. Below the input field are two buttons: "Add" and "Edit / Delete".

MAC Address: Enter the MAC address of the target computer or you can select the MAC address directly from the Select drop down menu on the right.

: You can select the MAC from this list.

5.3.8 Time Schedule

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

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

Configuration

Time Schedule

Parameters

Name

Day in a week Sun Mon Tue Wed Thu Fri Sat

Start Time :

End Time :

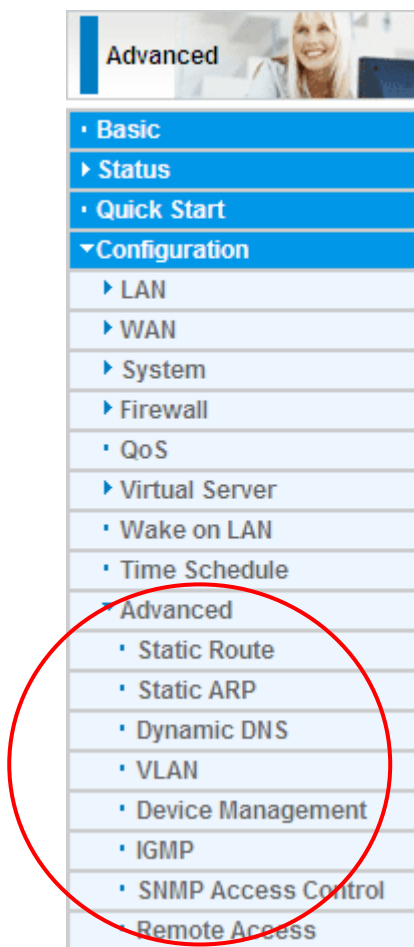
Edit	Name	Day in a week	Start Time	End Time	Clear
<input type="radio"/>	TimeSlot1	smtwfs	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot2	smtwfs	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot3	smtwfs	08:00	18:00	<input type="checkbox"/>
<input type="radio"/>	TimeSlot4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

- **Name:** A user-define description to identify this time portfolio.
- **Day in a week:** The default is set from Sunday through Saturday. You may specify the days for the schedule to be applied.
- **Start Time:** The default is set at 8:00 AM. You may specify the start time of the schedule.
- **End Time:** The default is set at 18:00 (6:00PM). You may specify the end time of the schedule. Select the **Apply** button to apply your changes.

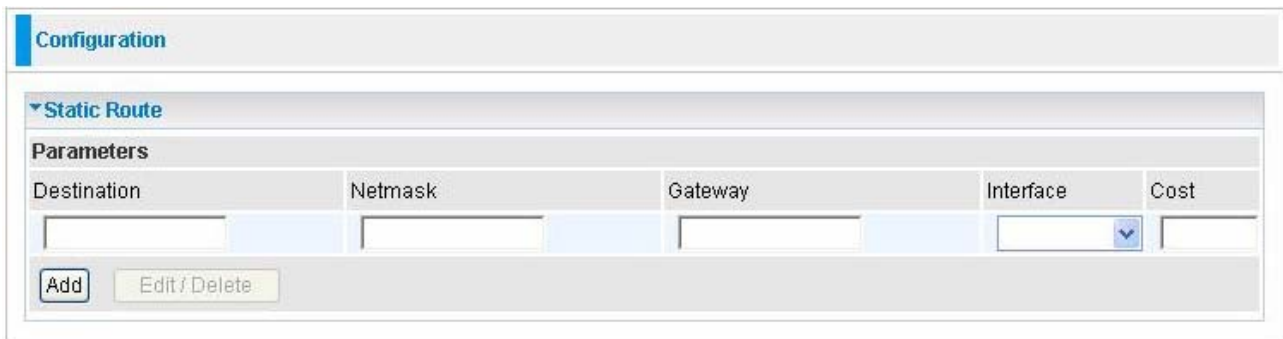
5.3.9 Advanced

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

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



5.3.9.1 Static Route

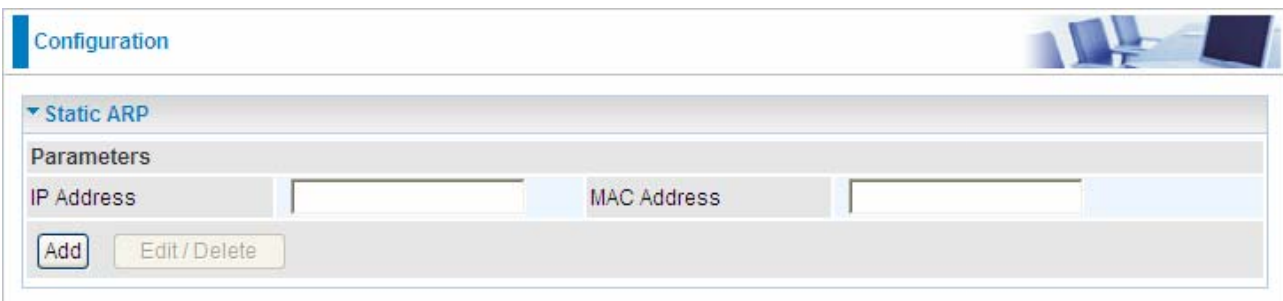


The screenshot shows a web-based configuration interface for a Static Route. At the top, there is a 'Configuration' header. Below it, a section titled 'Static Route' is expanded. Underneath, a 'Parameters' section contains five input fields: 'Destination', 'Netmask', 'Gateway', 'Interface', and 'Cost'.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

- **Destination:** The destination subnet IP address.
- **Netmask:** Subnet mask of the destination IP addresses based on above destination.
- **Gateway:** The gateway IP address to which packets are forwarded.
- **Interface:** Select the interface through which packets are forwarded.
- **Cost:** Represents the cost of transmission for routing purposes. The number need not be precise, but it must be between 0 and 65535.

5.3.9.2 Static ARP

This feature allows you to map the layer-2 MAC (Media Access Control) address that corresponds to the layer-3 IP address of the device.



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

IP Address: Enter the IP of the device that the corresponding MAC address will be mapped to.

MAC Address: Enter the MAC address that corresponds to the IP address of the device. Click Add to confirm the settings.

Edit: Check the Edit radio button to display the parameter of the selected application, then after changing the parameters click the "Edit/Delete" button to apply the changes.

The screenshot shows the 'Static ARP' configuration section. It includes a 'Parameters' section with input fields for 'IP Address' and 'MAC Address', and buttons for 'Add' and 'Edit / Delete'. Below this is a table with the following data:

Edit	IP Address	MAC Address	Delete
<input type="radio"/>	192.168.1.20	AA:BB:CC:DD:EE:FF	<input type="checkbox"/>

Delete: To remove a static ARP entry, check the Delete box of the selected entry then click the "Edit/Delete" button.

5.3.9.3 Dynamic DNS

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

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

The screenshot shows the 'Dynamic DNS' configuration section. It includes a 'Parameters' section with the following fields and options:

- Dynamic DNS:** Enable Disable
- Dynamic DNS Server:** www.dyndns.org (dynamic) (dropdown menu)
- Wildcard:** Enable
- Domain Name:** (text input field)
- Username:** (text input field)
- Password:** (text input field)
- Period:** 28 (text input) Day(s) (dropdown menu)

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

- **Disable:** Check to disable the Dynamic DNS function.
- **Enable:** Check to enable the Dynamic DNS function. The fields following are activated and required.
- **Dynamic DNS Server:** Select the DDNS service you have established an account with.
- **Wildcard:** Select this check box to enable the DYNDNS Wildcard.

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

Period: Set the time period between updates, for the Router to exchange information with the DDNS server. In addition to updating periodically as per your settings, the router will perform an update when your dynamic IP address changes. If the period is 0, the router will check the DNS server every 5 min.

5.3.9.4 VLAN

VLAN (Virtual Local Area Network) is a group of devices on different physical LAN segments that can communicate with each other as if they were all on the same physical LAN segment.

Configuration

▼ VLAN

Parameters

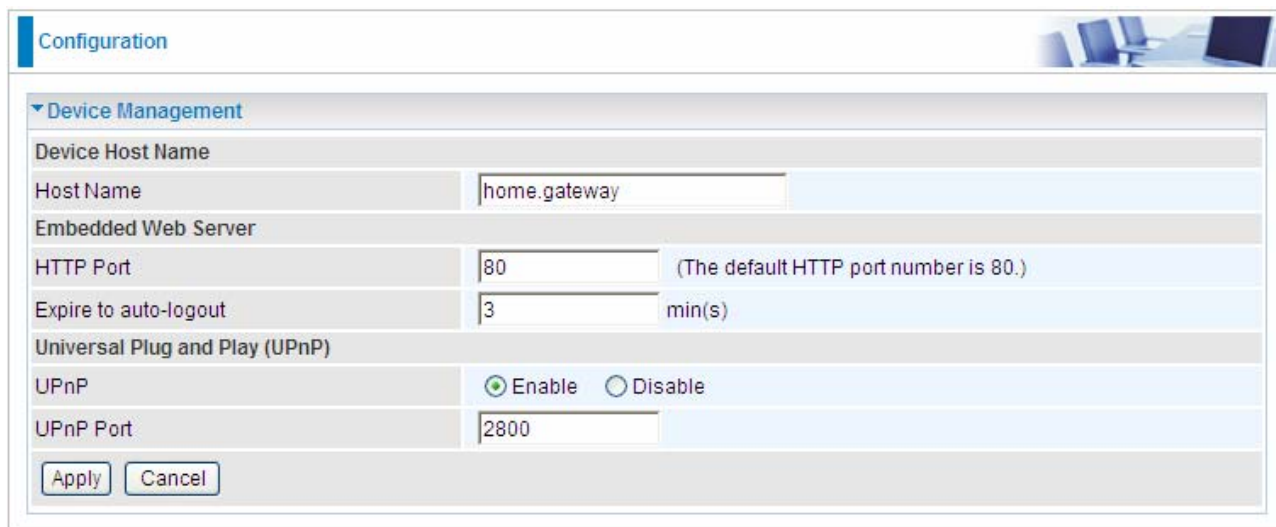
VLAN Group Name	VLAN ID	Ethernet Port				WLAN	Link VLAN Group to WAN Connection interface / WAN Tagging
		#1	#2	#3	#4		
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No <input type="button" value="v"/> / <input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No <input type="button" value="v"/> / <input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No <input type="button" value="v"/> / <input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No <input type="button" value="v"/> / <input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No <input type="button" value="v"/> / <input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No <input type="button" value="v"/> / <input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No <input type="button" value="v"/> / <input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No <input type="button" value="v"/> / <input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No <input type="button" value="v"/> / <input type="checkbox"/>

LAN Tagging

LAN Tagging: Insert or keep VLAN tag of the packets flow through the specific ethernet port.
 WAN Tagging: Insert or keep VLAN tag of the packets flow through the specific Bridged WAN interface.(Only for Bridge)

5.3.9.5 Device Management

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



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

Embedded Web Server:

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

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

Universal Plug and Play (UPnP):

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

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

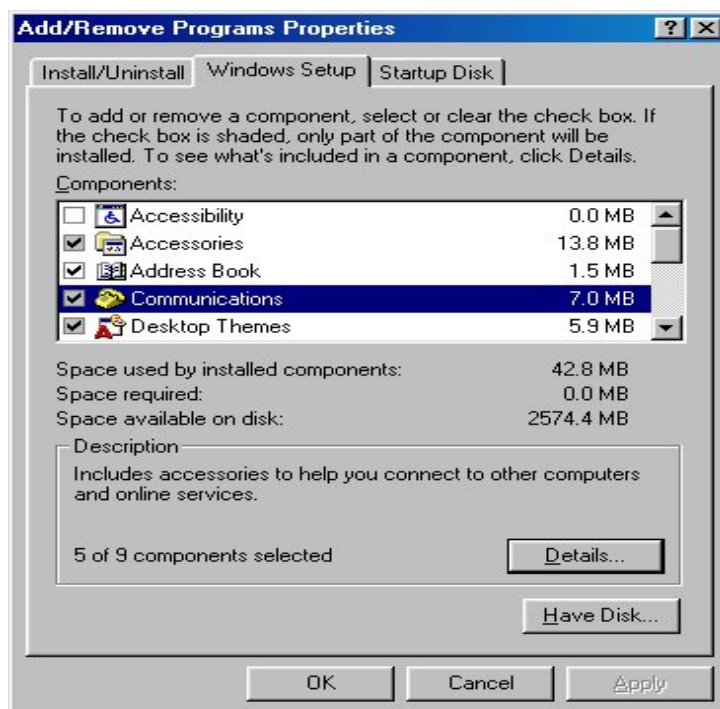
- **Disable:** Check to disable the router's UPnP functionality.
- **Enable:** Check to enable the router's UPnP functionality.
- **UPnP Port:** The Default setting is 2800. It is highly recommended you use this port value. If this value conflicts with other ports already in use you may wish to change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

Installing UPnP in Windows Example

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

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

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



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



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

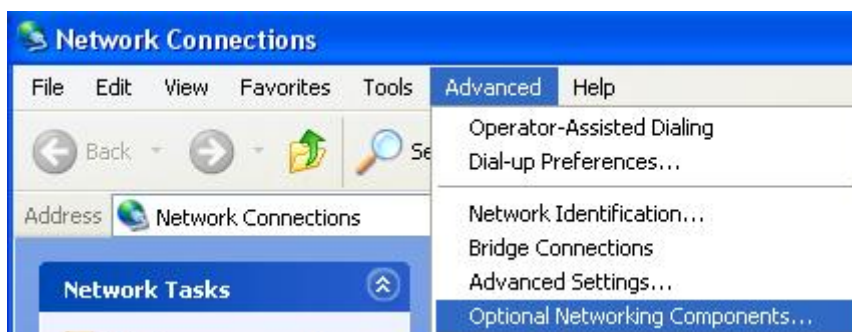
Step 5: Restart the computer when prompted.

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

Step 1: Click Start and Control Panel.

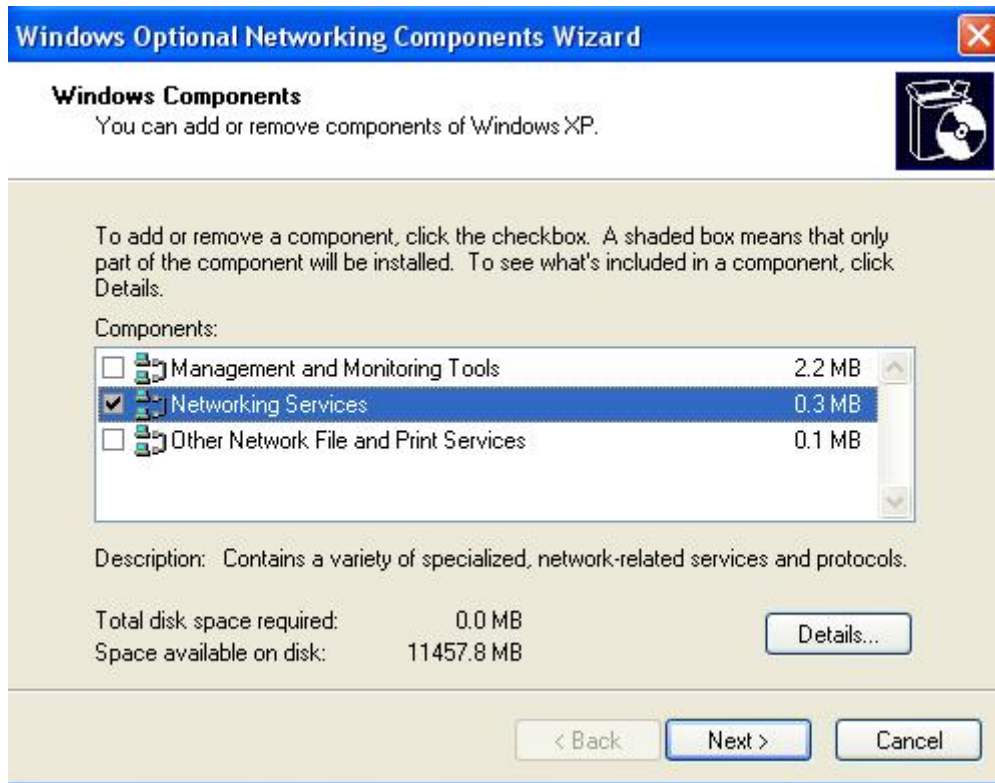
Step 2: Double-click Network Connections.

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



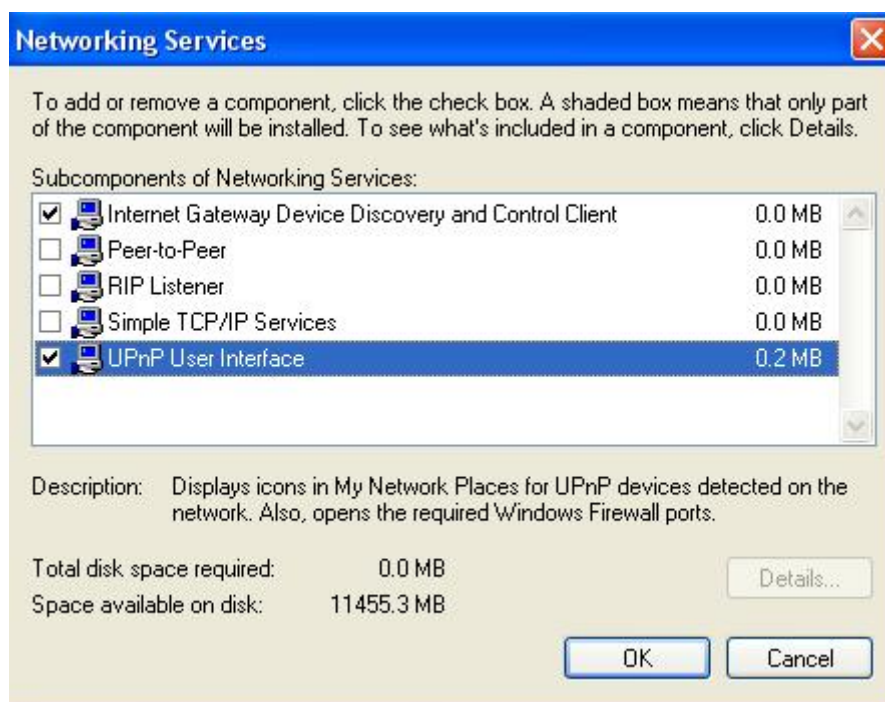
The Windows Optional Networking Components Wizard window displays.

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



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

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



Auto-discover Your UPnP-enabled Network Device

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

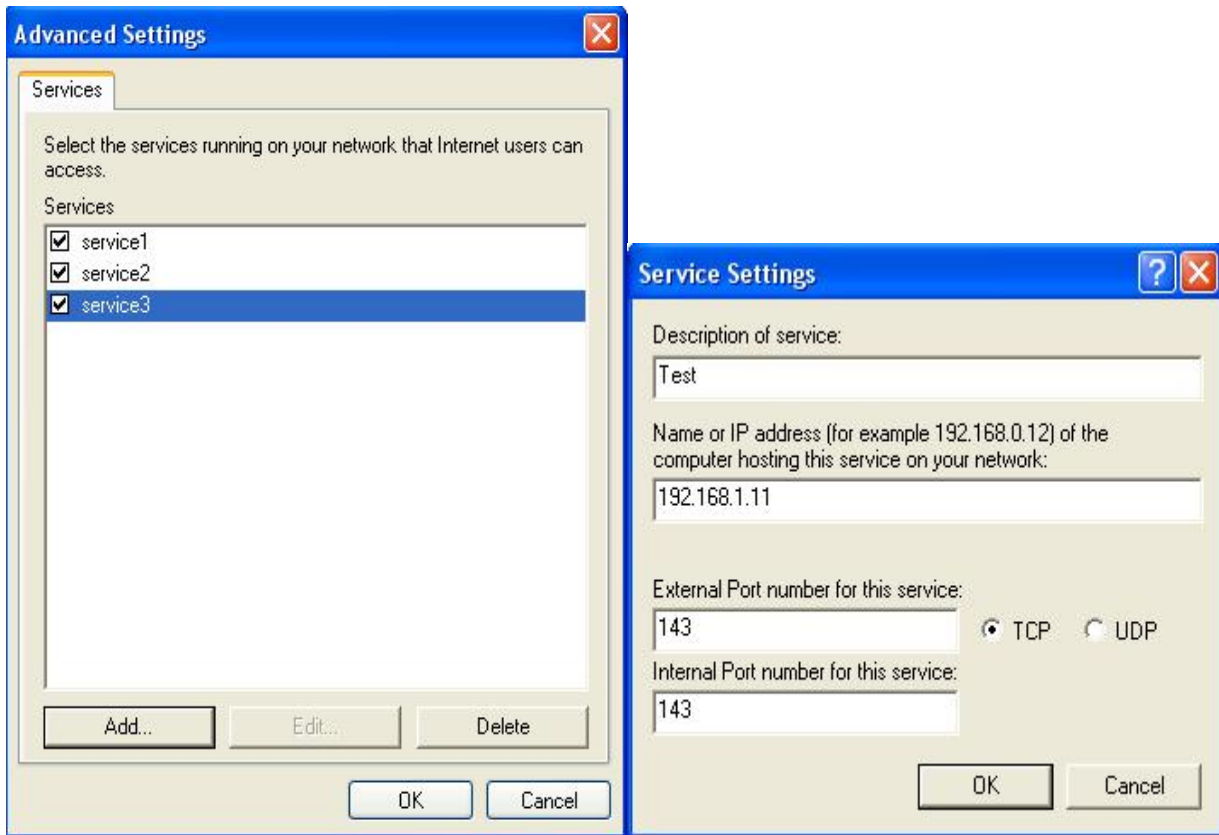
Step 2: Right-click the icon and select Properties.



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



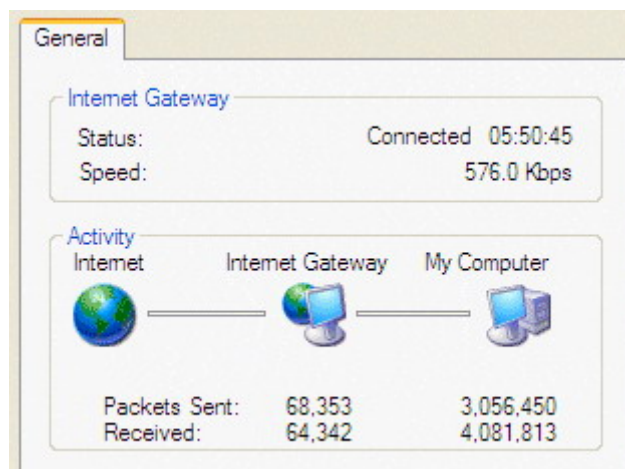
Step 4: You may edit or delete the port mappings or click Add to manually add port mappings.



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



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



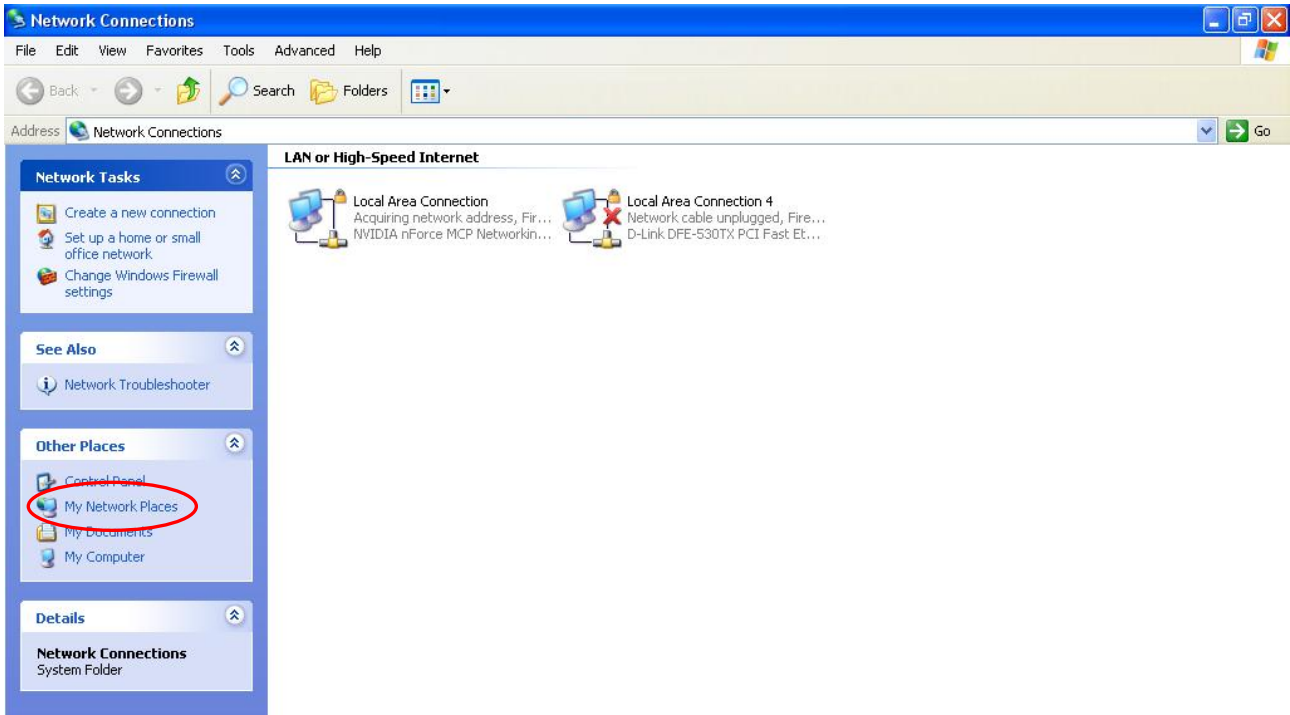
Web Configurator Easy Access

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

Step 1: Click Start and then Control Panel.

Step 2: Double-click Network Connections.

Step 3: Select My Network Places under Other Places.



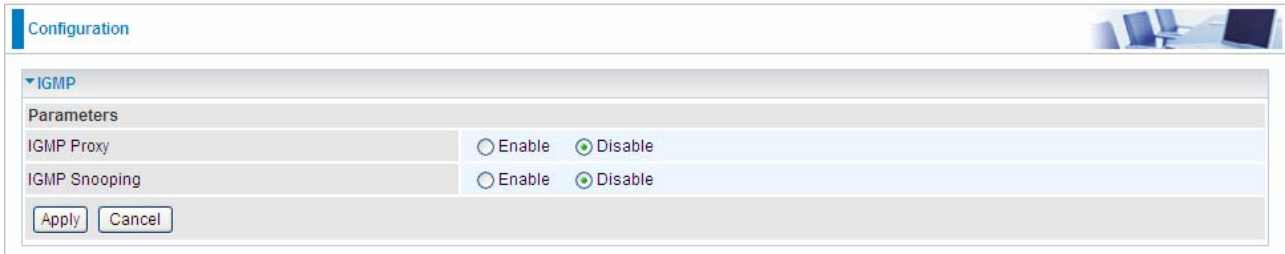
Step 4: An icon describing each UPnP-enabled device shows under Local Network.

Step 5: Right-click on the icon of your BiPAC 7300W and select Invoke. The web configuration login screen displays.

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

5.3.9.6 IGMP

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



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

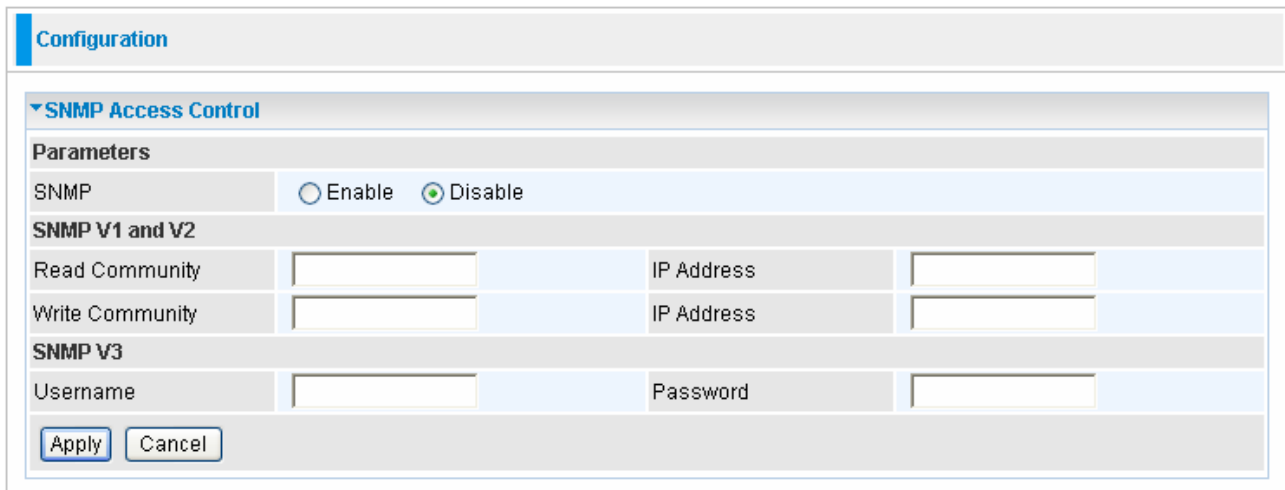
Apply Cancel

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

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

5.3.9.7 SNMP Access Control

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



Parameters			
SNMP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
SNMP V1 and V2			
Read Community	<input type="text"/>	IP Address	<input type="text"/>
Write Community	<input type="text"/>	IP Address	<input type="text"/>
SNMP V3			
Username	<input type="text"/>	Password	<input type="text"/>

Apply Cancel

SNMP V1 and V2:

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

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

view and modify the data.

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

SNMP V3:

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

SNMP Version: SNMPV2c and SNMPv3

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

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

Traps supported: Cold Start, Authentication Failure.

The following MIBs are supported:

From RFC 1213 (MIB-II):

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

From RFC1650 (EtherLike-MIB):

- dot3Stats

From RFC 1493 (Bridge MIB):

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

From RFC 1471 (PPP/LCP MIB):

- pppLink group
- pppLqr group

From RFC 1472 (PPP/Security MIB):

- PPP Security Group)

From RFC 1473 (PPP/IP MIB):

- PPP IP Group

From RFC 1474 (PPP/Bridge MIB):

- PPP Bridge Group

From RFC1573 (IfMIB):

- ifMIBObjects Group

From RFC1695 (atmMIB):

- atmMIBObjects

From RFC 1907 (SNMPv2):

only snmpSetSerialNo OID

5.3.9.8 Remote Access

Configuration

Remote Access

Parameters

Remote Access Control Enable Duration min(s) (0: Always On)

Apply

Allowed Access IP Address Range

Valid IP Address Range ~

Add Edit / Delete

Remote Access Control:

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

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


Allowed Access IP Address Range:

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

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

5.4 Save Configuration to Flash

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

 Save Config

Configuration


▼ Save Config to FLASH

Write settings to FLASH

Apply

5.5 Restart

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

 Restart

Configuration

▼ Restart

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

Restart device with

Factory Default Settings

Current Settings

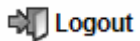
Restart

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

5.6 Logout

To exit the router's web interface, choose **Logout**. Please ensure that you have saved the configuration settings before you logout.

Be aware that the router is restricted to only one PC accessing the configuration web pages at a time. Once a PC has logged into the web interface, other PCs cannot get access until the current PC has logged out of the web interface. If the previous PC forgets to logout, the second PC can access the page after a user-defined period, by default 3 minutes. You can modify this value using the **Advanced – Device Management** section of the web interface. Please see the **Advanced** section of this manual for more information.



Chapter 6

Troubleshooting

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

Problems starting up the router

Problem	Corrective Action
None of the LEDs are on when you turn on the router.	Check the connection between the adapter and the router. If the error persists, you may have a hardware problem. In this case you should contact technical support.

Problems with the WAN Interface

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

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

Problems with the LAN Interface

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

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.