



BiPAC 7800(N)

**(802.11n) Dual WAN
ADSL2+ Firewall Router**

User Manual

Table of Contents

Chapter 1: Introduction	1
Introduction to your Router	1
Features	2
Chapter 2: Installing the Router	5
Important note for using this router	5
Package Contents	6
Device Description.....	7
The Front LEDs.....	7
The Rear Ports	8
Cabling.....	9
Chapter 3: Basic Installation	10
Connecting Your Router	11
Network Configuration	12
Factory Default Settings.....	18
Information from your ISP	19
Chapter 4: Configuration	20
Easy Sign-On (EZSO).....	20
Configuration via Web Interface.....	23
Quick Start	24
Status (Basic Mode).....	34
Cofiguration (Basic Mode)	35
WAN – Main Port (ADSL).....	35
WAN – Main Port (EWAN)	40
WLAN (only for BiPAC 7800N).....	42
Status (Advanced Mode).....	45
ADSL.....	46
ARP.....	47
DHCP.....	47
System Log.....	48
Configuration (Advanced Mode)	49

LAN	49
Ethernet	49
IP Alias.....	49
Wireless (only for BiPAC 7800N).....	50
Wireless Security (only for BiPAC 7800N).....	52
WPS (only for BiPAC 7800N)	54
DHCP Server	66
WAN.....	67
WAN Profile (ADSL)	67
WAN Profile – Main Port (EWAN).....	74
ADSL Mode	78
System	79
Time Zone	79
Firmware Upgrade	80
Backup / Restore	81
Restart	82
User Management.....	82
Firewall.....	83
Packet Filter.....	83
MAC Filter	84
Block WAN Ping	84
QoS.....	85
Virtual Server	88
Port Mapping.....	89
DMZ	90
Advanced	91
Static Route	91
Static ARP	91
Dynamic DNS.....	92
VLAN.....	93
Device Management.....	95
IGMP	101

TR-069 Client	102
Remote Access.....	103
Appendix: Product Support & Contact	104

Chapter 1: Introduction

Introduction to your Router

Thank you for purchasing BiPAC 7800(N) Router. Your new router is an all-in-one unit that combines an ADSL modem, ADSL2/2+ router and Ethernet network switch to provide everything you need to get the machines on your network connected to the Internet over an ADSL broadband connection.

BiPAC 7800(N) router complies with ADSL2+ standards for deployment worldwide and supports downstream rates of up to 24 Mbps and upstream rates of up to 1 Mbps. Designed for small office, home office and residential users, the router enables even faster Internet connections. You can enjoy ADSL services and broadband multimedia applications such as interactive gaming, video streaming and real-time audio much easier and faster than ever before.

BiPAC 7800(N) supports PPPoA (RFC 2364 – PPP (Point-to-Point Protocol) over ATM Adaptation Layer 5), RFC 1483 encapsulation over ATM (bridged or routed), PPP over Ethernet (RFC 2516) to establish a connection with your ISP. Your new router also supports VC-based and LLC-based multiplexing.

The perfect solution for connecting a small group of PCs to a high-speed broadband Internet connection, BiPAC 7800(N) allows multiple users to have high-speed Internet access simultaneously.

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

BiPAC 7800(N) provides two levels of security support. First, it masks LAN IP addresses making them invisible to outside users on the Internet, so it is much more difficult for a hacker to target a machine on your network. Second, it can block and redirect certain ports to limit the services that outside users can access. To ensure that games and other Internet applications run properly, you can open specific ports for outside users to access internal services on your network.

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

For advanced users, Virtual Service (port mapping) functions allow the product to provide limited visibility to local machines with specific services for outside users. For instance, a dedicated web server can be connected to the Internet via the router and then incoming requests for web pages that are received by the router can be rerouted to your dedicated local web server, even though the server now has a different IP address.

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

Features

Express Internet Access

The router complies with ADSL worldwide standards. It supports downstream rate up to 12/24 Mbps with ADSL2/2+, 8Mbps with ADSL. Users enjoy not only high-speed ADSL services but also broadband multimedia applications such as interactive gaming, video streaming and real-time audio much easier and faster than ever. It is compliant with Multi-Mode standard (ANSI T1.413, Issue 2; G.dmt (ITU G.992.1); G.lite (ITU G.992.2); G.hs (ITU G994.1); G.dmt.bis (ITU G.992.3); G.dmt.bis. plus (ITU G.992.5)).

EWAN

BiPAC 7800(N) EWAN port provides user an alternative means to connect to Cable Modems, VDSL, fiber optic lines and PON besides using ADSL for internet connection. If one uses ADSL to connect to the internet, EWAN can act as the 5th Ethernet port of the LAN. This alternative provides users with more flexibility & a faster way to get online.

Fast Ethernet Switch

A 4-port 1000Mbps fast Ethernet switch is built in with automatic switching between MDI and MDI-X. An Ethernet straight or crossover cable can be used directly for auto detection.

Multi-Protocol to Establish a Connection

It supports PPPoA (RFC 2364 - PPP over ATM Adaptation Layer 5), RFC 1483 encapsulation over ATM (bridged or routed), PPP over Ethernet (RFC 2516), and IPoA (RFC1577) to establish a connection with the ISP. The product also supports VC-based and LLC-based multiplexing.

PPP over Ethernet (PPPoE)

BiPAC 7800(N) provides an embedded PPPoE client function to establish a connection. You get greater access speed without changing the operation concept, while sharing the same ISP account and paying for one access account. No PPPoE client software is required for the local computer. Automatic Reconnect and Disconnect Timeout (Idle Timer) functions are also provided.

Universal Plug and Play (UPnP) and UPnP NAT Traversal

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

Network Address Translation (NAT)

Allows multi-users to access outside resources such as the Internet simultaneously with one IP address/one Internet access account. Many application layer gateway (ALG) are supported such as

web browser, ICQ, FTP, Telnet, E-mail, News, Net2phone, Ping, NetMeeting, IP phone and others.

Domain Name System (DNS) Relay

It provides an easy way to map the domain name (a friendly name for users such as www.yahoo.com) and IP address. When a local machine sets its DNS server with this router's IP address, every DNS conversion request packet from the PC to this router will be forwarded to the real DNS in the outside network.

Dynamic Domain Name System (DDNS)

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname. This dynamic IP address is the WAN IP address. For example, to use the service, you must first apply for an account from a DDNS service like <http://www.dyndns.org/>. More than 5 DDNS servers are supported.

Virtual Server

Users can specify some services to be visible from outside users. The router can detect incoming service requests and forward either a single port or a range of ports to the specific local computer to handle it. For example, a user can assign a PC in the LAN acting as a WEB server inside and expose it to the outside network. Outside users can browse inside web servers directly while it is protected by NAT. A DMZ host setting is also provided to a local computer exposed to the outside network, Internet.

Rich Packet Filtering

Not only filters the packet based on IP address, but also based on Port numbers. It will filter packets from the Internet and vice versa, in addition to providing a higher level of security control.

Dynamic Host Configuration Protocol (DHCP) Client and Server

In the WAN site, the DHCP client can get an IP address from the Internet Service Provider (ISP) automatically. In the LAN site, the DHCP server can allocate a range of client IP addresses and distribute them including IP address, subnet mask as well as DNS IP address to local computers. It provides an easy way to manage the local IP network.

802.11n Wireless AP with WPA Support

With an integrated 802.11n Wireless Access Point in the router, the device delivers up to 6 times faster speeds and 3 times farther range than an 802.11b/g wireless network. It supports a fast data transfer rate up to 300Mbps and is fully compatible with 802.11b/11g equipments. The supported features of Wireless Protected Access (WPA-PSK/ WPA2-PSK) and Wireless Encryption Protocol (WEP) enhance the security level of data protection and access control via Wireless LAN. The router also supports Wi-Fi Protected Setup (WPS) that features the establishment of a secured wireless network. The built-in Wireless Distribution System (WDS) also facilitates the flexibility for wireless network expansion without the need for any external wires or cables.

Web based GUI

It supports web based GUI for configuration and management. It is user-friendly and comes with on-line help. It also supports remote management capability for remote users to configure and manage this product.

Firmware Upgradeable

Device can be upgraded to the latest firmware through the WEB based GUI.

Chapter 2: Installing the Router

Important note for using this router



Warning

- Do not use this router in a high humidity or high temperature environment.
- Do not apply the same power source for this router to other types of equipments.
- Do not open or repair the case yourself. If the device becomes too hot, turn it off immediately and have it repaired at a qualified service center.
- Avoid using this product and all its accessories outdoor.

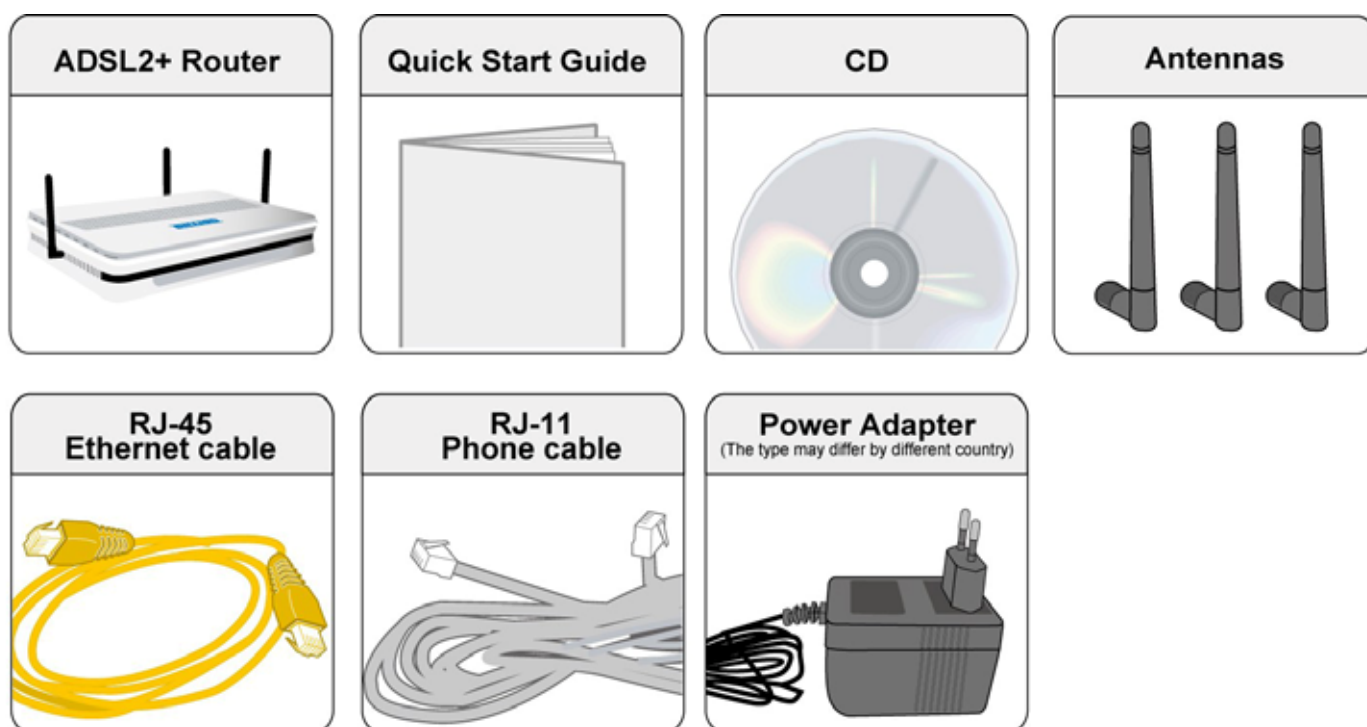


Attention

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

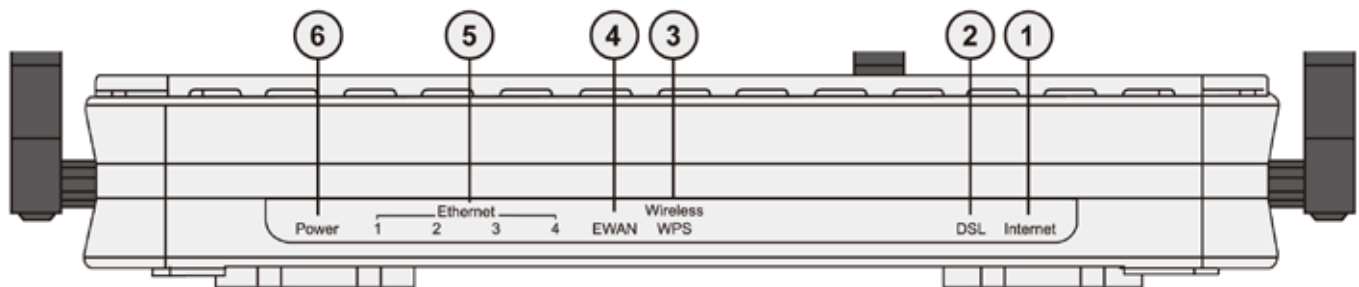
Package Contents

- BiPAC 7800(N) (802.11n) Dual WAN ADSL2+ Firewall Router
- CD containing the online manual
- RJ-11 ADSL/Telephone cable
- Ethernet (RJ-45) cable
- Three 2dBi detachable antennas (Wireless model only)
- Power adapter
- Quick Start Guide
- Splitter / Microfilter (Optional)



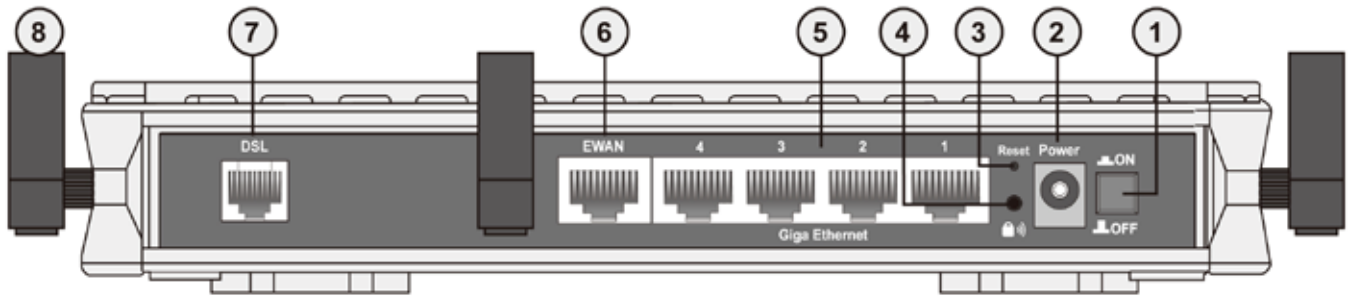
Device Description

The Front LEDs



LED		Meaning
1	Internet	<p>Lit orange when WAN port fails to get IP address.</p> <p>Lit green when WAN port gets IP address.</p> <p>Lit off when device in bridged mode or ADSL connection not present.</p>
2	DSL	<p>Lit Green when the device is successfully connected to an ADSL DSLAM. ("line sync").</p>
3	Wireless / WPS (only available for BiPAC 7800N)	<p>Lit green when a wireless connection is established.</p> <p>Flash orange when WPS configuration is in progress. However, if WPS fails the LED will only lit for 1 min before goes off.</p> <p>Flash green when data is sent / received.</p>
4	EWAN	<p>Lit orange when connected to a broadband connection device.</p> <p>Lit orange for 10/100Mbps.</p> <p>Blinking when data is Transmitted / Received.</p>
5	Ethernet port 1X — 4X (RJ-45 connector)	<p>Lit orange when one of LAN ports is connected to an Ethernet device.</p> <p>Lit green when the speed of transmission hits 1000Mbps; Lit orange when the speed of transmission hits 10/100Mbps.</p> <p>Blink when data is being Transmitted / Received.</p>
6	Power	<p>When the device is booting, the green light will lit while the orange light will flash.</p> <p>When the system is ready, it will lit green.</p> <p>Lit orange when the device fails to boot or when the device is in emergency mode.</p>

The Rear Ports



Port		Meaning
1	Power Switch	Power ON/OFF switch.
2	Power	Connect it with the supplied power adapter.
3	RESET	Press more than 1 second to restore the device to its default mode.
4	WPS (only for BiPAC 7800N)	Push WPS button to trigger Wi-Fi Protected Setup function.
5	Giga Ethernet	Connect to a PC or an office/home network of 10Mbps, 100Mbps or 1000Mbps using the provided RJ-45 Ethernet cables.
6	EWAN	WAN 10/100Mbps Ethernet port (with auto crossover support). Connect to Cable Modem, VDSL, Fiber Modem or PON optic lines with your RJ-45 cable.
7	DSL	Connect this port to the ADSL/telephone network with the RJ-11 cable (telephone) provided.
8	Antenna (BiPAC 7800N only)	Connect the detachable antenna to this port.

Cabling

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

Make sure that all devices (e.g. telephones, fax machines, analogue modems) connected to the same telephone line as your router have a line filter connected between them and the wall outlet (unless you are using a Central Splitter or Central Filter installed by a qualified and licensed electrician), and that all line filters are correctly installed in a right way. If line filter is not installed and connected properly, it may cause problem to your ADSL connection or may result in frequent disconnections.

Chapter 3: Basic Installation

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

Please check your PC 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.

There are ways to connect the router, either through an external repeater hub or connect directly to your PCs. However, make sure that your PCs have an Ethernet interface installed properly prior to connecting the router device. You ought to configure your PCs to obtain an IP address through a DHCP server or a fixed IP address that must be in the same subnet as the router. The default IP address of the router is 192.168.1.254 and the subnet mask is 255.255.255.0 (i.e. any attached PC must be in the same subnet, and have an IP address in the range of 192.168.1.1 to 192.168.1.253). The best and easiest way is to configure the PC to get an IP address automatically from the router using DHCP. If you encounter any problem accessing the router web interface it is advisable to uninstall your firewall program on your PCs, as they can cause problems accessing the IP address of the router. Users should make their own decisions on what is best to protect their network.

Please follow the following steps to configure your PC network environment.

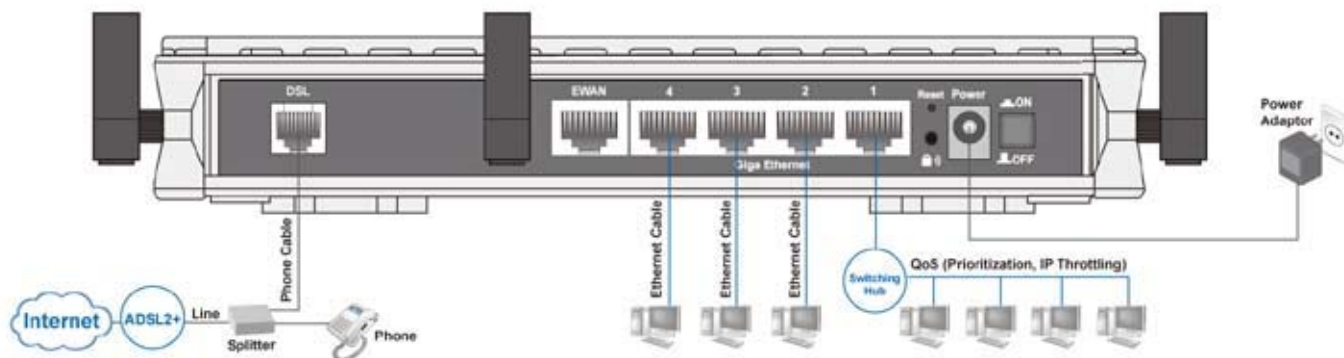


Any TCP/IP capable workstation can be used to communicate with or through this router. To configure other types of workstations, please consult your manufacturer documentation.

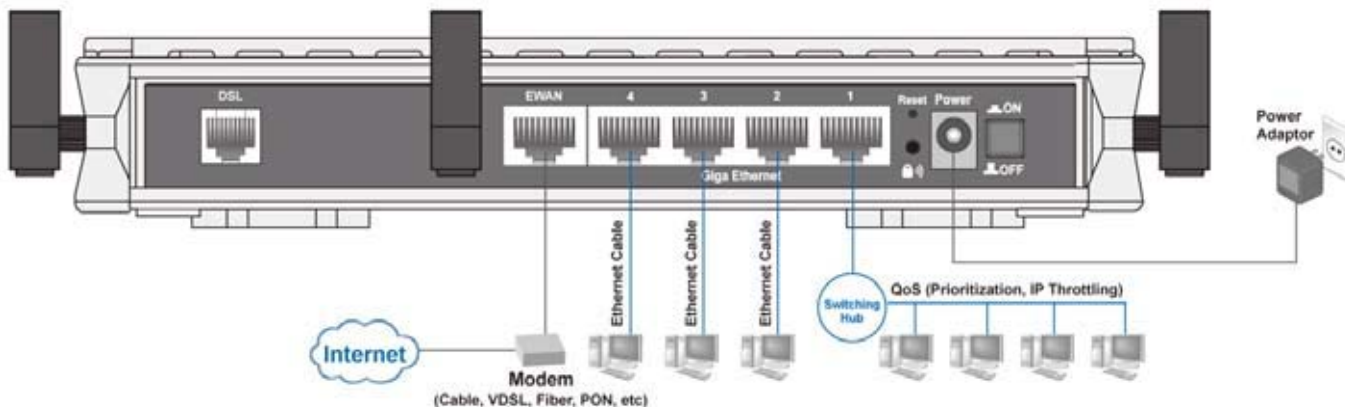
Connecting Your Router

Users will not be able to connect to the internet through EWAN if DSL is already connected to the internet. Only one connection type (EWAN or DSL) is allowed to connect to the internet at one time.

ADSL Router Mode



Broadband Router Mode



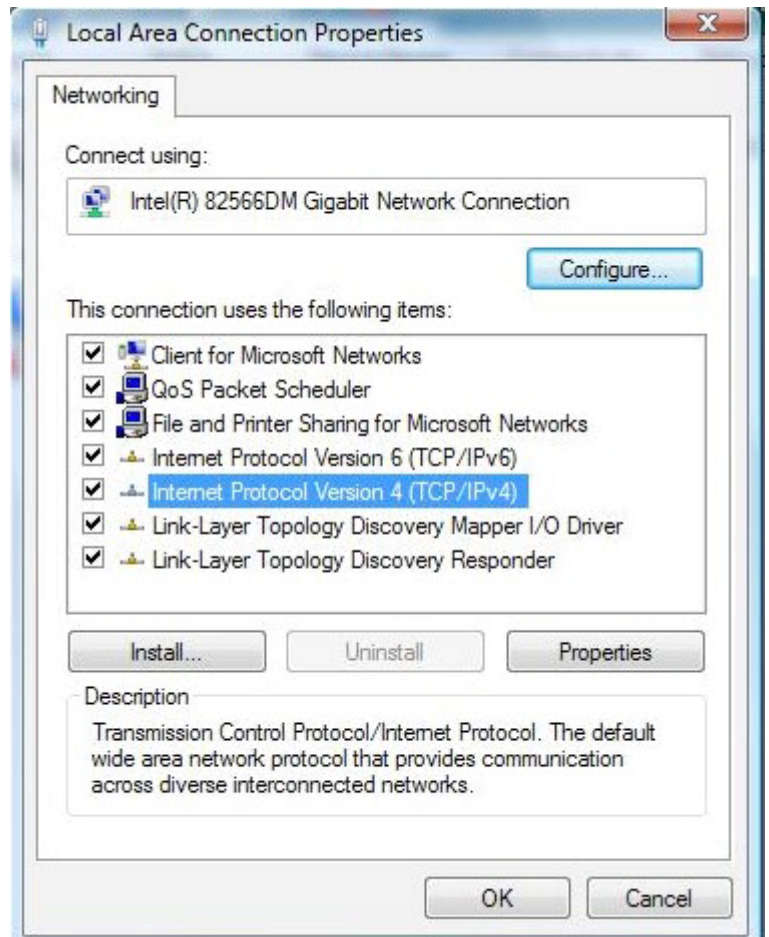
Network Configuration

Configuring PC in Windows Vista

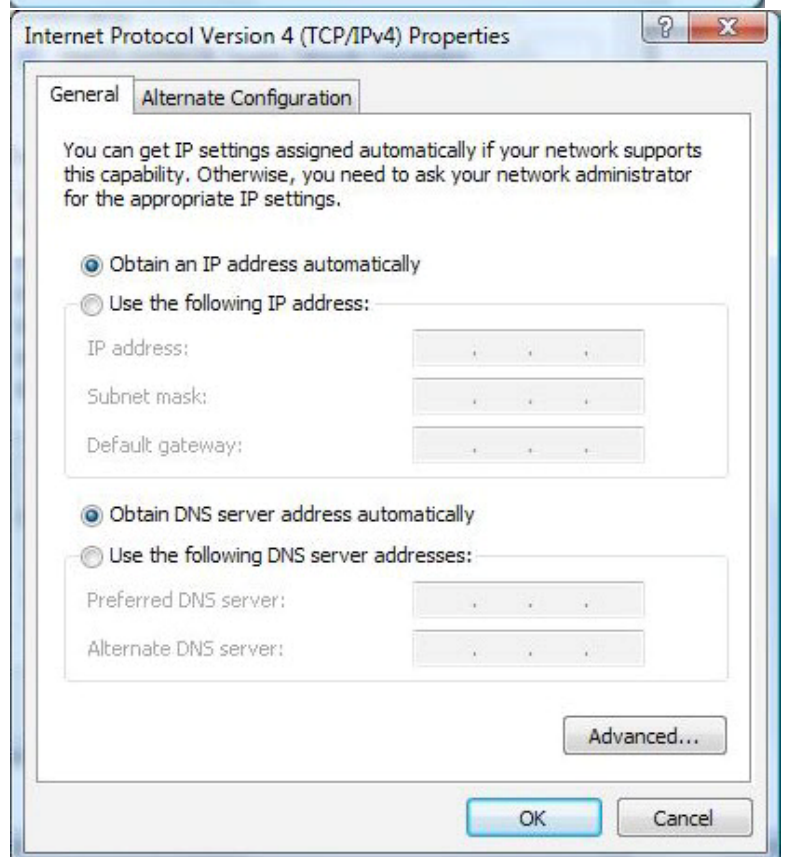
1. Go to Start. Click on Network.
2. Then click on Network and Sharing Center at the top bar.
3. When the Network and Sharing Center window pops up, select and click on Manage network connections on the left window column.
4. Select the Local Area Connection, and right click the icon to select Properties.



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

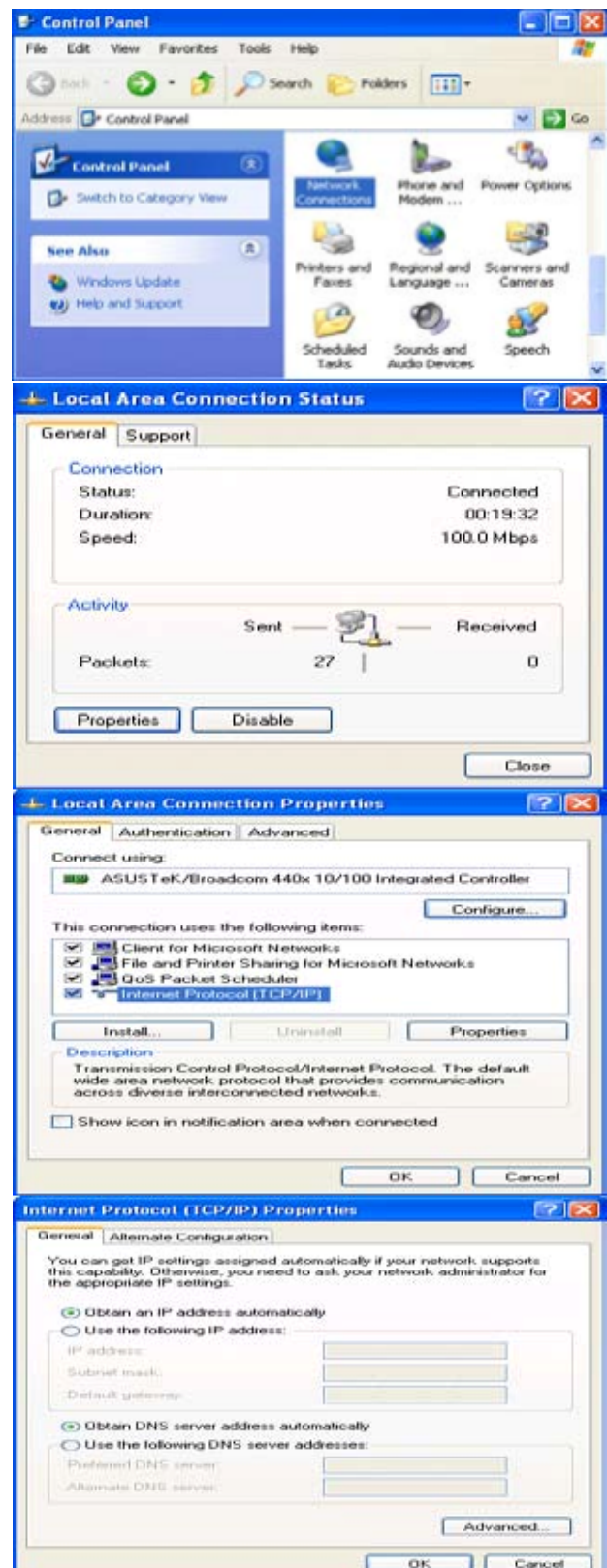


6. In the TCP/IPv4 properties window, select the Obtain an IP address automatically and Obtain DNS Server address automatically radio buttons. Then click OK to exit the setting.
7. Click OK again in the Local Area Connection Properties window to apply the new configuration.



Configuring PC in Windows XP

1. Go to Start > Control Panel (in Classic View). In the Control Panel, double-click on Network Connections
2. Double-click Local Area Connection.
3. In the Local Area Connection Status window, click Properties.
4. Select Internet Protocol (TCP/IP) and click Properties.
5. Select the Obtain an IP address automatically and the Obtain DNS server address automatically radio buttons.
6. Click OK to finish the configuration.



Configuring PC in Windows 2000

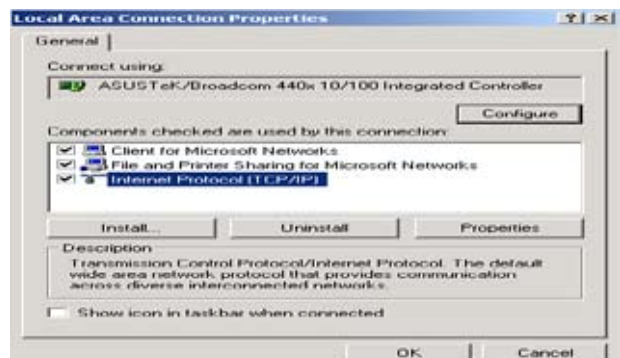
1. Go to Start > Settings > Control Panel. In the Control Panel, double-click on Network and Dial-up Connections.
2. Double-click Local Area Connection.



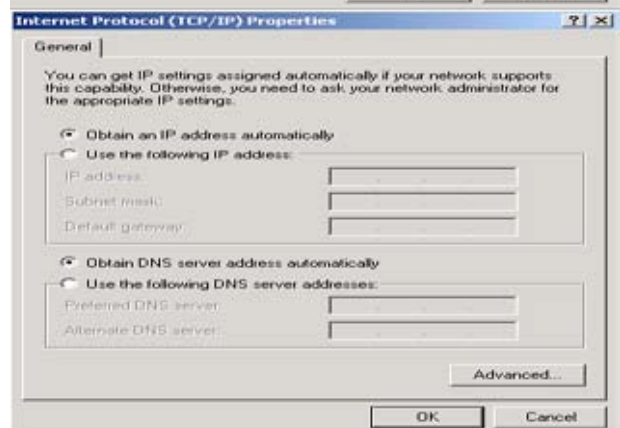
3. In the Local Area Connection Status window click Properties.



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

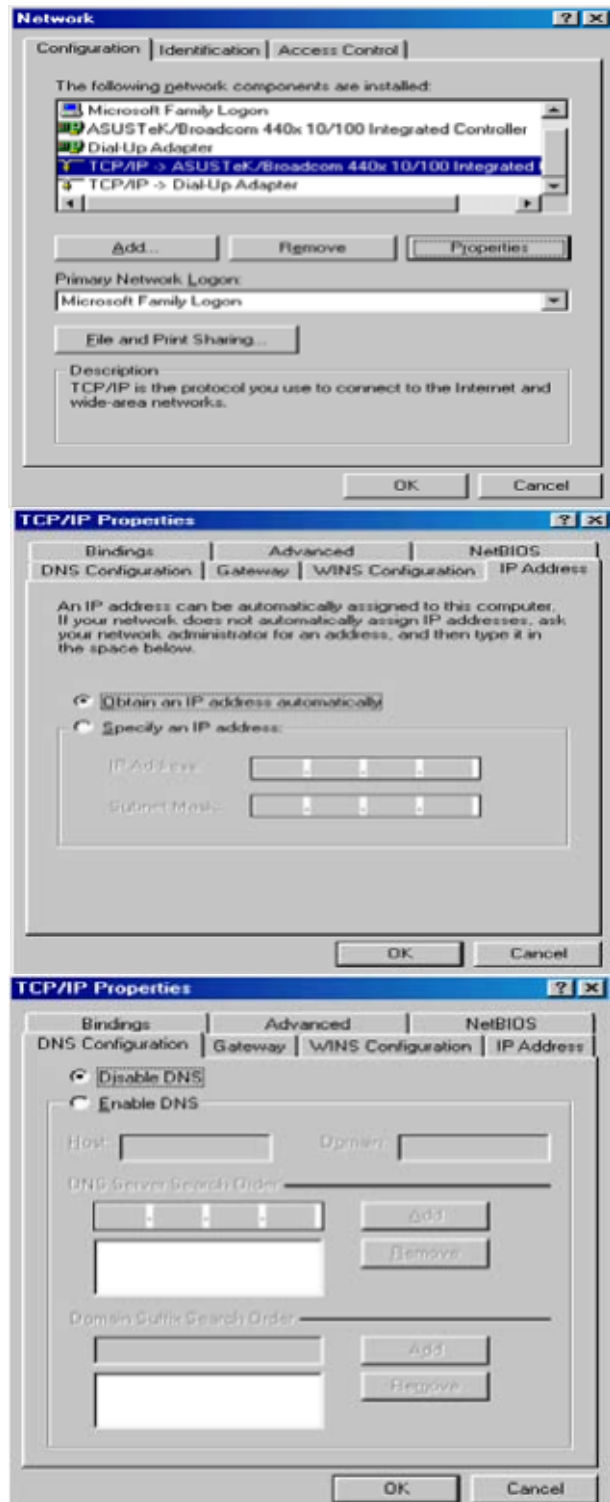


5. Select the Obtain an IP address automatically and the Obtain DNS server address automatically radio buttons.
6. Click OK to finish the configuration.



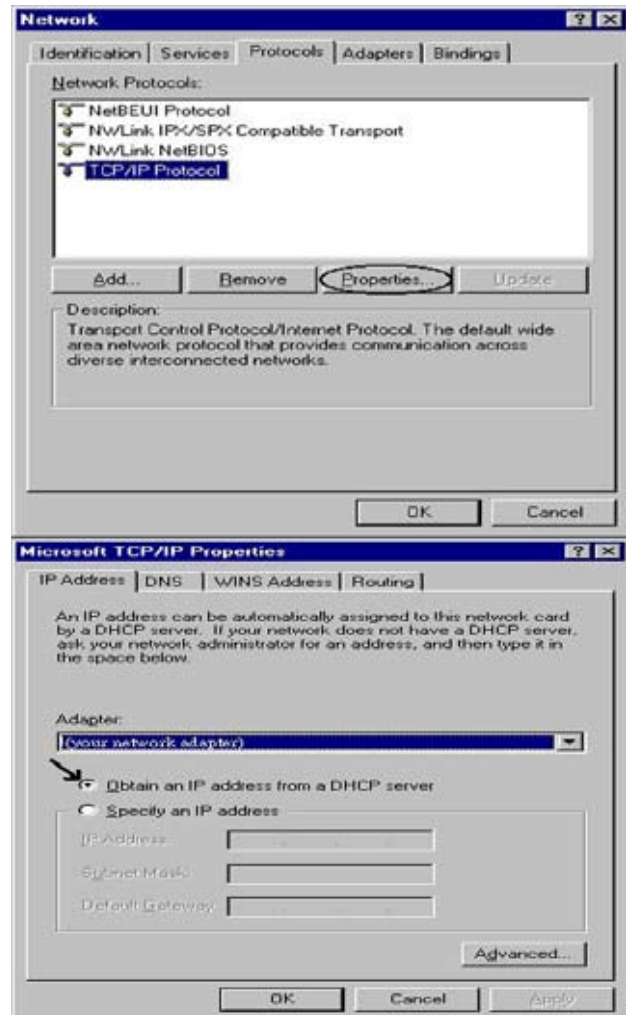
Configuring PC in Windows 95/98/Me

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



Configuring PC in Windows NT4.0

1. Go to Start > Settings > Control Panel. In the Control Panel, double-click on Network and choose the Protocols tab.
2. Select TCP/IP Protocol and click Properties.
3. Select the Obtain an IP address from a DHCP server radio button and click OK.



Factory Default Settings

Before configuring your 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 have forgotten your username or password for the router, you can restore your device to its default setting by pressing the Reset button for more than 1 second.

Device LAN 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

LAN and WAN Port Addresses

The parameters of LAN and WAN ports are pre-set in the factory. The default values are shown in the table.

	LAN Port	WAN Port
IP address	192.168.1.254	The PPPoE function is enabled to automatically get the WAN port configuration from the ISP.
Subnet Mask	255.255.255.0	
DHCP server function	Enabled	
IP addresses for distribution to PCs	100 IP addresses continuing from 192.168.1.100 through 192.168.1.199	

Information from your ISP

Before configuring this device, you have to check with your ISP (Internet Service Provider) to find out what kind of service is provided such as DHCP (Obtain an IP Address Automatically, Static IP (Fixed IP Address) or PPPoE.

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

PPPoE(RFC2516)	VPI/VCI, VC / 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(RFC2364)	VPI/VCI, VC / 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).
MPoA(RFC1483/ RFC2684)	VPI/VCI, VC / LLC-based multiplexing, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is a fixed IP address).
IPoA(RFC1577)	VPI/VCI, VC / LLC-based multiplexing, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is a fixed IP address).
Pure Bridge	VPI/VCI, VC / LLC-based multiplexing to use Bridged Mode.

Chapter 4: Configuration

To easily configure this device for internet access, you must have IE 5.0 / Netscape 4.5 or above installed on your computer. There are basically 2 ways to configure your router before you are able to connect to the internet: **Easy Sign-On** & **Web Interface**. Configuration of each method will be discussed in detail in the following sections.

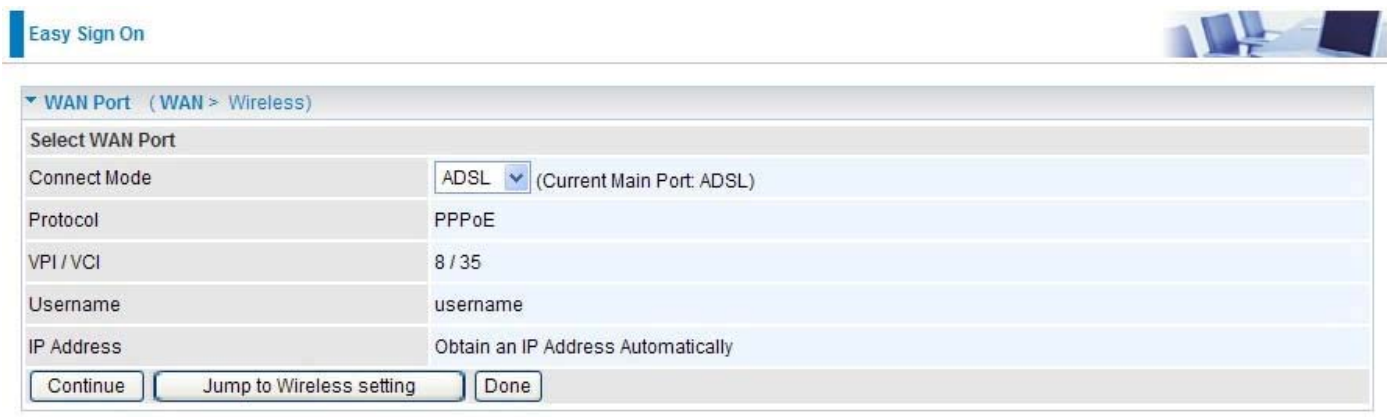
Easy Sign-On (EZSO)

This special feature makes it easier for you to configure your router so that you can connect to the internet in a matter of seconds without having to logon to the router GUI for any detail configuration. This configuration method is usually auto initiated if user is to connect to the internet via Billion's router for the first time.

After setting up the router with all the appropriate cables plugged-in, open up your IE browser, the EZSO WEB GUI will automatically pop up and request that you enter some basic information that you have obtained from your ISP. By following the instructions given carefully and through the information you provide, the router will be configured in no time and you will find yourself surfing the internet sooner than you realize.

Follow the Easy Sign-On configuration wizard to complete the basic network configuration.

1. Connect your router with all the appropriate cables. Then, load your IE / netscape browser.
2. When the EZSO configuration wizard pops up, select the connect mode which you want to set up and then click continue.




The screenshot shows the 'Easy Sign On' configuration wizard. At the top left, there is a blue header with the text 'Easy Sign On'. Below this, the main configuration area is titled 'WAN Port (WAN > Wireless)'. Underneath, there is a section 'Select WAN Port' with several fields:

Connect Mode	ADSL (Current Main Port: ADSL)
Protocol	PPPoE
VPI / VCI	8 / 35
Username	username
IP Address	Obtain an IP Address Automatically

At the bottom of the configuration area, there are three buttons: 'Continue', 'Jump to Wireless setting', and 'Done'.

3. Please enter all the information in the blanks provided and then click continue.


Easy Sign On 

▼ WAN Port (WAN > Wireless)

Select protocol


Protocol	PPPoE (RFC2516, PPP over Ethernet)	▼
VPI / VCI	0	33
Username	t0083328	
Password	••••••••	
Service Name		
Encapsulation method	LLC/SNAP-BRIDGING	▼
Authentication Protocol	Auto	▼
IP Address	0.0.0.0	(0.0.0.0 means 'Obtain an IP address automatically')
MTU	1492	

4. The device will reboot and then load the new configuration.

Easy Sign On 

▼ Restart

Since settings are changed, the router will reboot to make the changes take effect! Please wait for seconds.

total :  4%

5. If all information provided is valid and the device successfully connects to WAN, a dialog box will appear to signify the completion of the WAN port setup. At this point you can either click Done to finish the EZSO configuration or you can click Next to wireless to proceed to the wireless configuration if you have.

Easy Sign On

▼ WAN Port (WAN > Wireless)

Congratulations !

Your WAN port has been successfully configured.

6. However, if any error occurs during device configuration that results in WAN connection failure, the system will prompt that the setup has failed.


Easy Sign On 

▼ WAN Port

Fail!!!

WAN port setting is not successful (authentication fail), you can do this procedure again.

7. Select Enable and enter the necessary information in the blanks provided for the Wireless LAN setting (wireless setting is only available for BiPAC 7800N) if you would like to use this feature and then click Continue.


Easy Sign On 

▼ Wireless (WAN > Wireless)

Set Wireless configuration.

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

8. The system will save your new configuration and complete the setup. You can test the connection by clicking on the URL link provided. If the setup is successful you will be redirected to website.

Easy Sign On 

▼ Process finished

Success.

The Easy-Sign-On process is finished. Your device has been successfully configured.

You can now:

1. Log onto the router management interface for more advanced settings on 192.168.1.254
2. Continue to tw.yahoo.com/index.html

Configuration via Web Interface

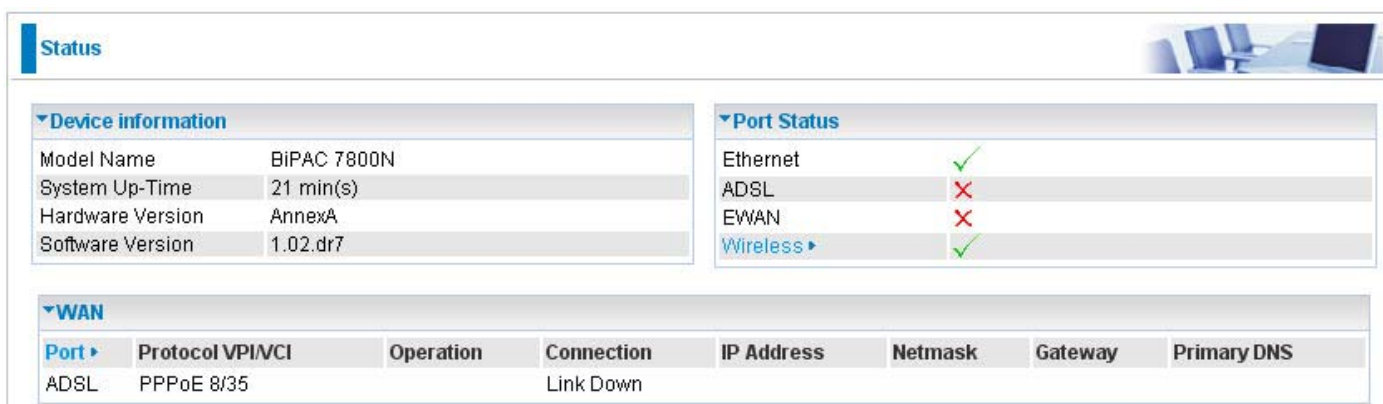
Open your web browser, enter the IP address of your router, which by default is 192.168.1.254, and click “Go”, a login window prompt will appear. The default username and password are “admin” and “admin” respectively.



The image shows a login window titled "Connect to 192.168.1.254". It features a blue header with a key icon and a "BiPAC 7800N" label. Below this, there are input fields for "User name:" and "Password:". The "User name:" field has a dropdown menu with a user icon. There is a checkbox labeled "Remember my password" and two buttons at the bottom: "OK" and "Cancel".

Congratulations! You are now successfully logon to the Firewall Router!

If the authentication succeeds, the homepage “Device Info - Summary” will appear on the screen.



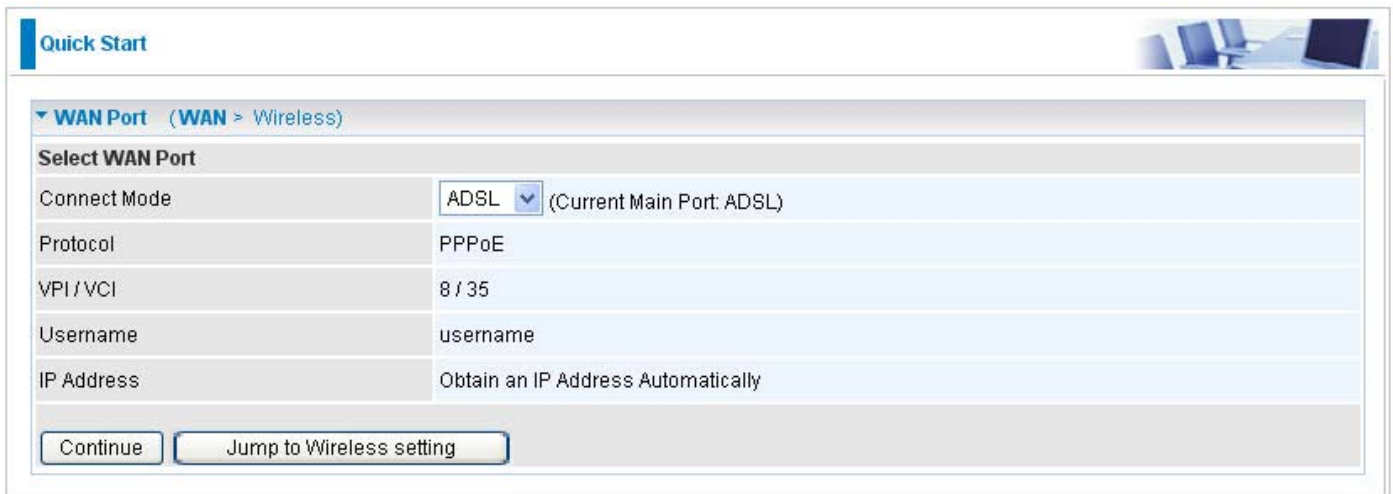
The image shows the "Status" page of the router's web interface. It includes a "Status" tab and a small image of a router. The page is divided into three main sections: "Device information", "Port Status", and "WAN".

Device information	
Model Name	BiPAC 7800N
System Up-Time	21 min(s)
Hardware Version	AnnexA
Software Version	1.02.dr7

Port Status	
Ethernet	✓
ADSL	✗
EWAN	✗
Wireless ▶	✓

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

Quick Start



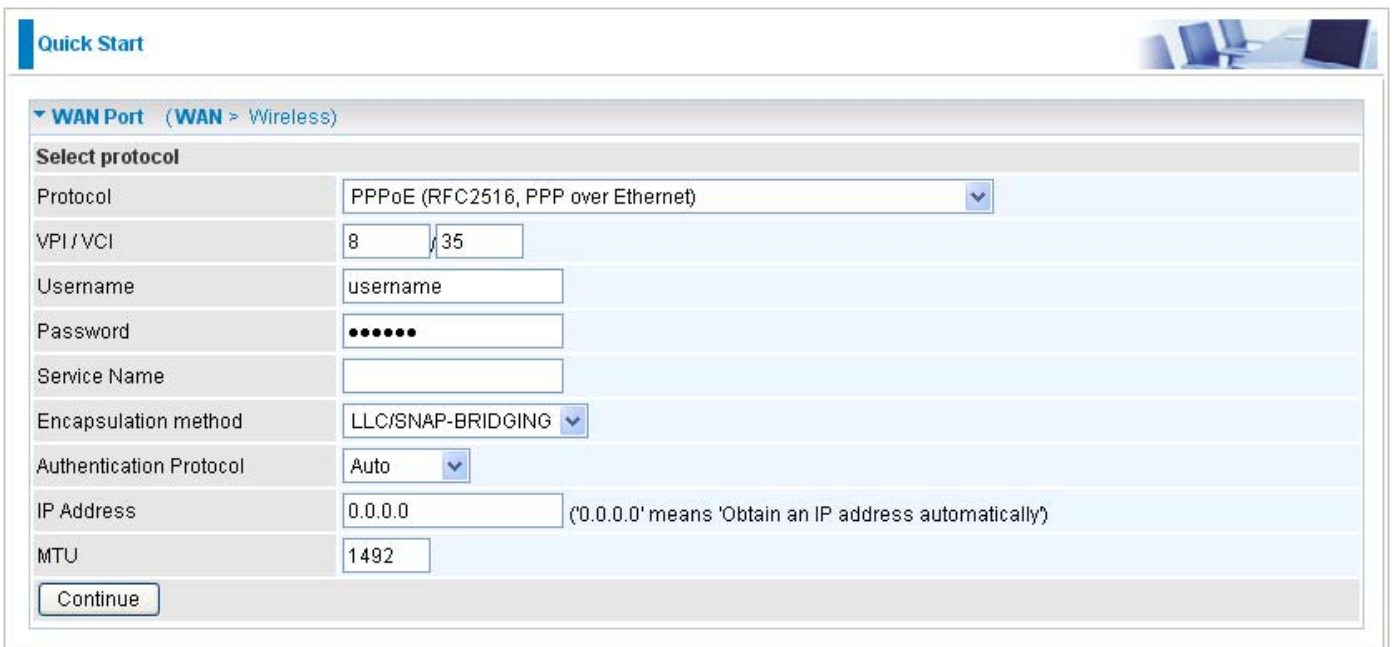
Quick Start

▼ WAN Port (WAN > Wireless)

Select WAN Port

Connect Mode	ADSL ▼ (Current Main Port: ADSL)
Protocol	PPPoE
VPI / VCI	8 / 35
Username	username
IP Address	Obtain an IP Address Automatically

Step 1: Select WAN port connect mode from the connect mode drop down menu. There are two types of connect mode to choose from: ADSL or EWAN



Quick Start

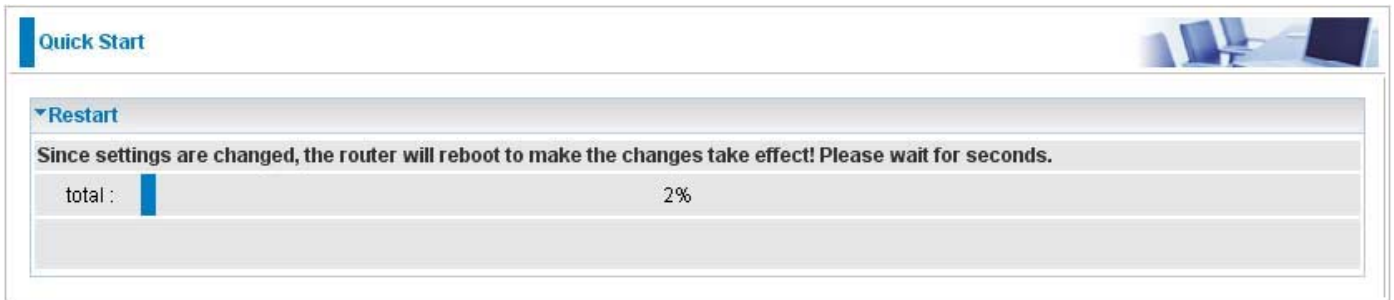
▼ WAN Port (WAN > Wireless)

Select protocol

Protocol	PPPoE (RFC2516, PPP over Ethernet) ▼
VPI / VCI	8 / 35
Username	username
Password	••••••
Service Name	
Encapsulation method	LLC/SNAP-BRIDGING ▼
Authentication Protocol	Auto ▼
IP Address	0.0.0.0 ('0.0.0.0' means 'Obtain an IP address automatically')
MTU	1492

Step 2: After selecting the connect mode, press Continue to move on to the next configuring page. There are 5 types of connection protocols available under ADSL connect mode while there are 3 types of connection protocols available for EWAN connect mode. **Each type of connection mode is described in the following sections of ADSL Connect mode and EWAN Connect mode.**

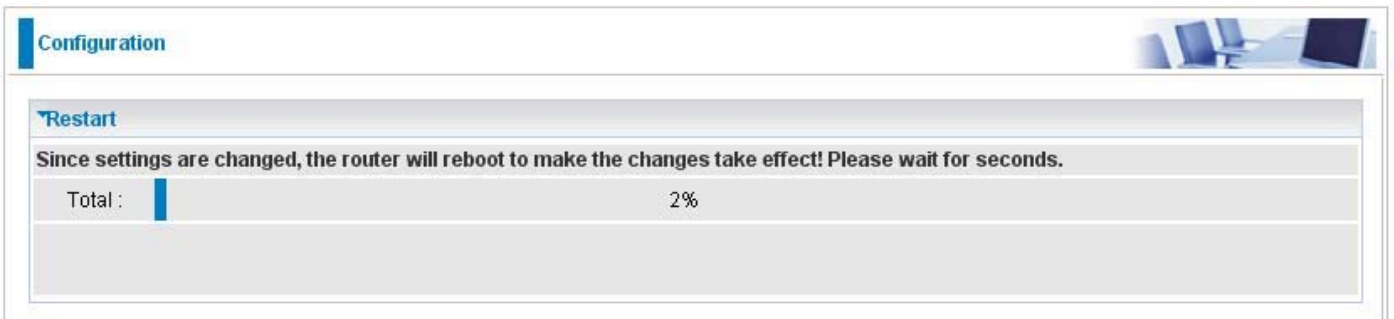
Step 3: After finishing configuring the WAN port connection, click Continue to proceed. The system will upload and apply the new WAN port configuration to the device.



Step 4: After the configuration is successful, you may proceed to configure the Wireless setting. There are 4 types of security mode: WPA, WPA2, WPA/WPA2 Preshared Key & WEP. Please refer to the Wireless Setting Mode section for detail description of each security mode.



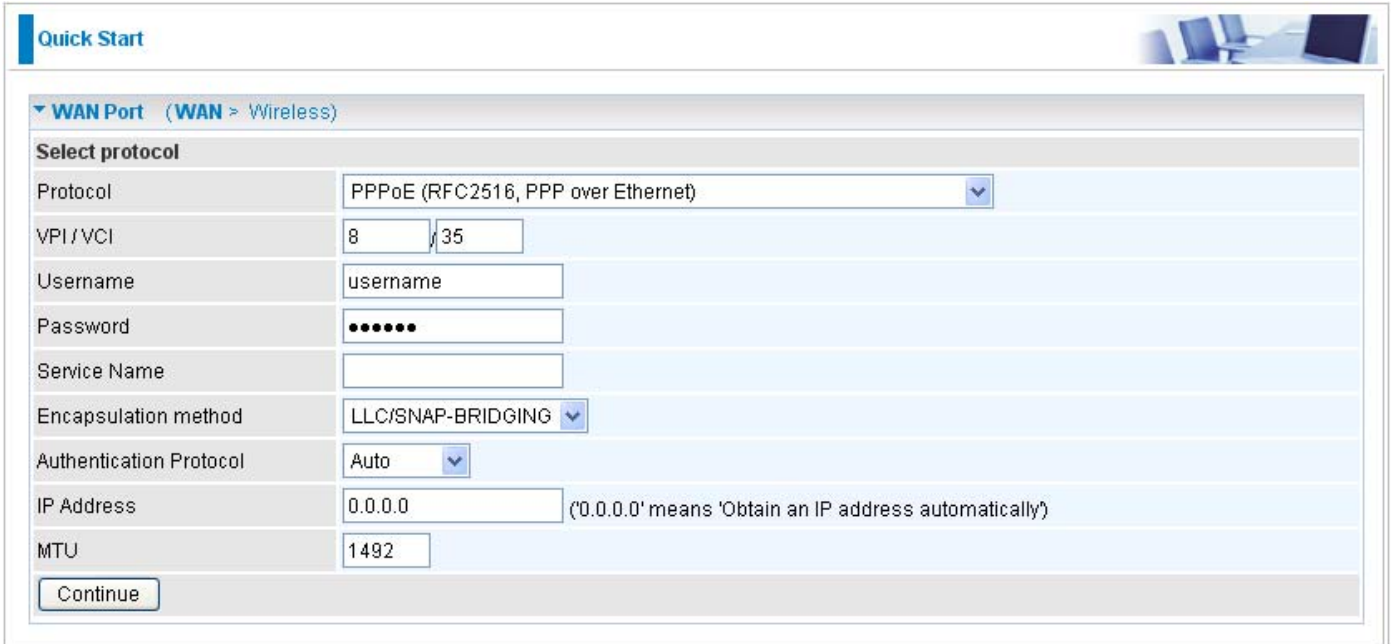
Step 5: After finishing configuring the WLAN setting, press Continue to finish the QuickStart.



ADSL Connect Mode

For ADSL connect mode there are 5 types of connection protocols: **PPPoE**, **PPPoA**, **IPoA**, **MPoA** and **Pure Bridge**.

PPPoE



The screenshot shows a web-based configuration interface for a WAN port. At the top left, there is a 'Quick Start' link. The main heading is 'WAN Port (WAN > Wireless)'. Below this, there is a 'Select protocol' section with a dropdown menu set to 'PPPoE (RFC2516, PPP over Ethernet)'. The form includes several input fields: 'VPI/VCI' with values '8' and '35', 'Username' with 'username', 'Password' with masked characters, 'Service Name' (empty), 'Encapsulation method' with a dropdown set to 'LLC/SNAP-BRIDGING', 'Authentication Protocol' with a dropdown set to 'Auto', 'IP Address' with '0.0.0.0' and a note '(0.0.0.0' means 'Obtain an IP address automatically)', and 'MTU' with '1492'. A 'Continue' button is at the bottom left.

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

Username: Enter the username provided by your ISP. You can input up to 256 alphanumeric characters (case sensitive).

Password: Enter the password provided by your ISP. You can input up to 32 alphanumeric characters (case sensitive).

Service Name: This item is for identification purposes. If it is required, your ISP will provide you the necessary information. Maximum input is 32 alphanumeric characters.

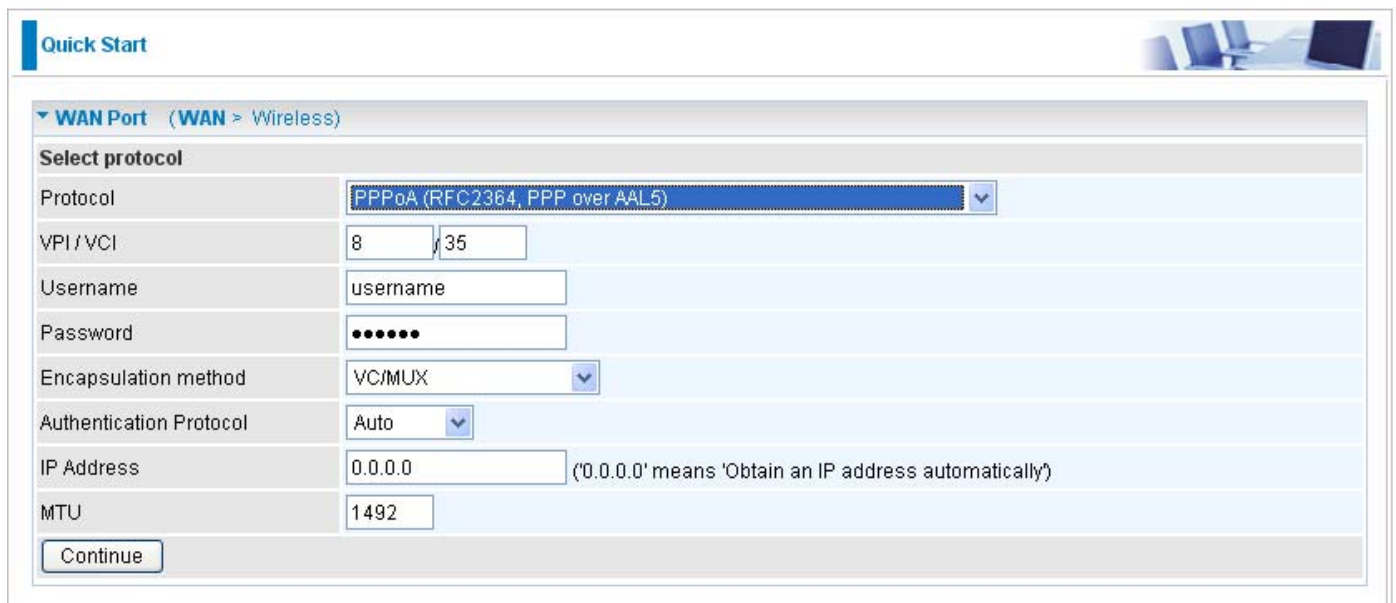
Encapsulation method: Select the encapsulation format. Select the one provided by your ISP.

Authentication method: Default is Auto. Please consult your ISP on whether to use Chap, Pap or MSCHAP.

IP Address: Your WAN IP address. Leave the IP address as 0.0.0.0 to enable the device 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.

PPPoA



The screenshot shows a web-based configuration interface for a WAN port. At the top left, there is a 'Quick Start' tab. The main heading is 'WAN Port (WAN > Wireless)'. Below this, there is a 'Select protocol' section with a dropdown menu set to 'PPPoA (RFC2364, PPP over AAL5)'. The configuration fields are as follows:

Field	Value
Protocol	PPPoA (RFC2364, PPP over AAL5)
VPI/VCI	8 / 35
Username	username
Password	••••••
Encapsulation method	VC/MUX
Authentication Protocol	Auto
IP Address	0.0.0.0 (0.0.0.0 means 'Obtain an IP address automatically')
MTU	1492

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

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

Username: Enter the username provided by your ISP. You can input up to 256 alphanumeric characters (case sensitive).

Password: Enter the password provided by your ISP. You can input up to 32 alphanumeric characters (case sensitive).

Encapsulation method: Select the encapsulation format. Select the one provided by your ISP.

Authentication method: Default is Auto. Please consult your ISP on whether to use Chap, Pap or MSCHAP.

IP Address: Your WAN IP address. Leave the IP address as 0.0.0.0 to enable the device 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.

IPoA Connection

Quick Start

▼ **WAN Port** (WAN > Wireless)

Select protocol

Protocol	IPoA (RFC1577, Classic IP and ARP over ATM)
VPI / VCI	8 / 35
Encapsulation method	LLC/SNAP-ROUTING
IP Address	0.0.0.0
Netmask	
Gateway	

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

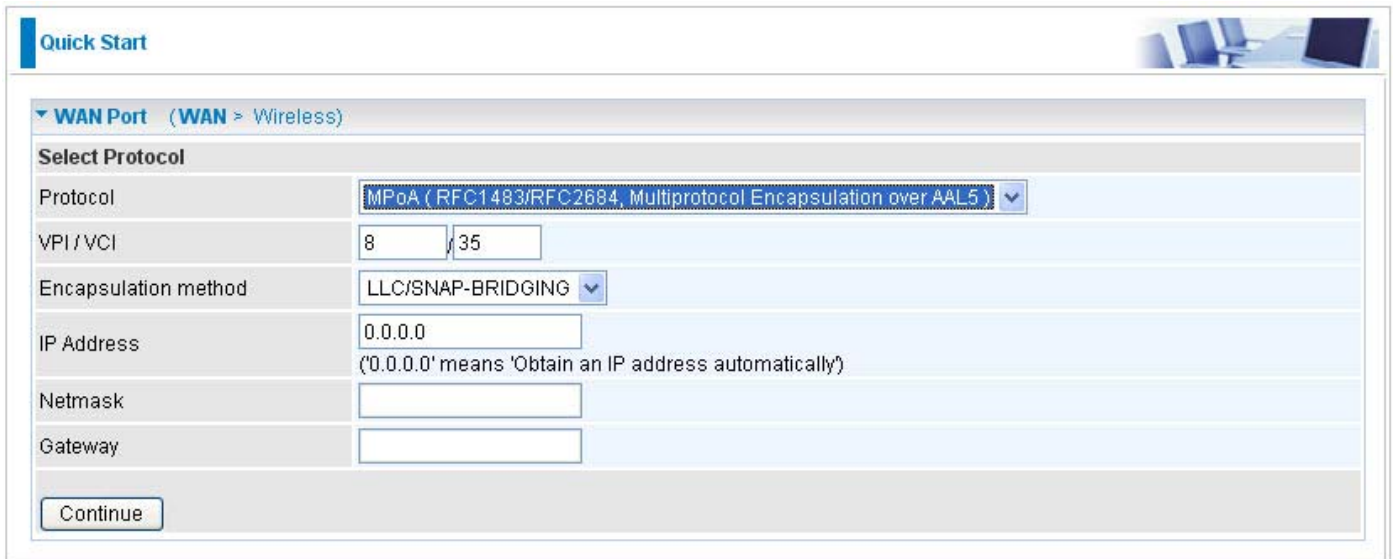
Encapsulation method: Select the encapsulation format. Select the one provided by your ISP.

IP Address: IPOA WAN IP address can only set fixed IP address.

Netmask: User can change it to others 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.

MPoA Connection



The screenshot shows a web interface for configuring a WAN port. At the top left, there is a 'Quick Start' tab. Below it, a breadcrumb trail reads 'WAN Port (WAN > Wireless)'. The main section is titled 'Select Protocol'. The 'Protocol' dropdown menu is set to 'MPoA (RFC1483/RFC2684, Multiprotocol Encapsulation over AAL5)'. The 'VPI/VCI' field has two input boxes containing '8' and '35'. The 'Encapsulation method' dropdown is set to 'LLC/SNAP-BRIDGING'. The 'IP Address' field contains '0.0.0.0', with a note below it stating '(0.0.0.0' means 'Obtain an IP address automatically)'. The 'Netmask' and 'Gateway' fields are empty. A 'Continue' button is located at the bottom left of the configuration area.

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

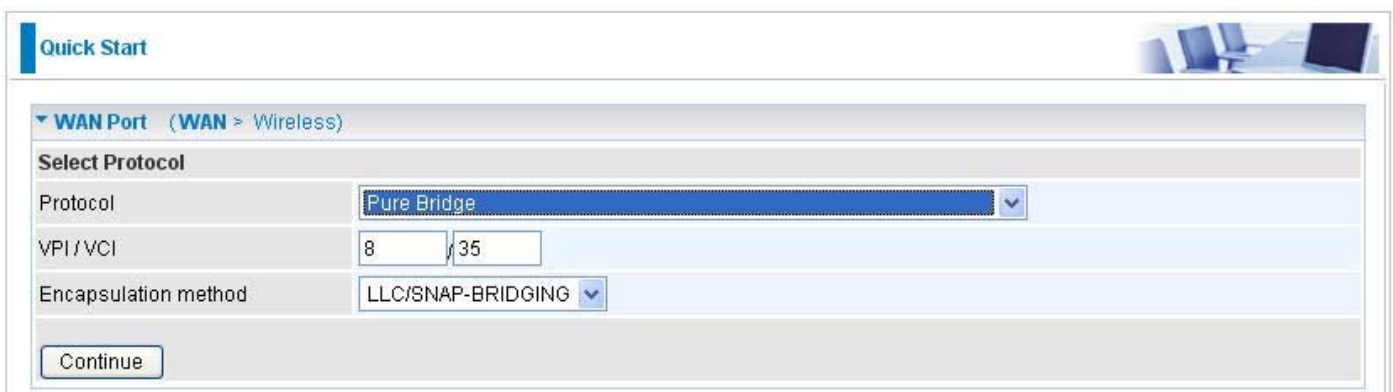
Encapsulation method: Select the encapsulation format. Select the one provided by your ISP.

IP Address: Your WAN IP address. If the IP is set to 0.0.0.0 (auto IP detect), both netmask and gateway may be left blank.

Netmask: User can change it to others 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.

Pure Bridge connection



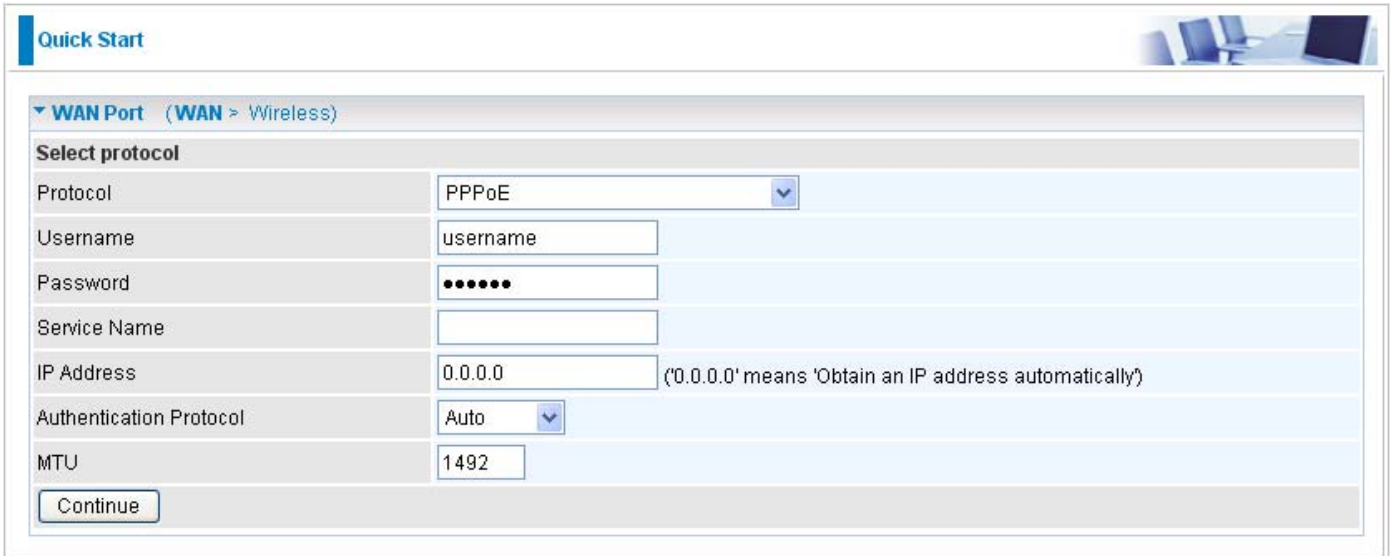
The screenshot shows a web interface for configuring a WAN port. At the top left, there is a 'Quick Start' tab. Below it, a breadcrumb trail reads 'WAN Port (WAN > Wireless)'. The main section is titled 'Select Protocol'. The 'Protocol' dropdown menu is set to 'Pure Bridge'. The 'VPI/VCI' field has two input boxes containing '8' and '35'. The 'Encapsulation method' dropdown is set to 'LLC/SNAP-BRIDGING'. A 'Continue' button is located at the bottom left of the configuration area.

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

Encapsulation method: Select the encapsulation format. Select the one provided by your ISP.

EWAN Connect Mode

PPPoE connection



Quick Start

▼ **WAN Port** (WAN > Wireless)

Select protocol

Protocol	PPPoE
Username	username
Password	••••••
Service Name	
IP Address	0.0.0.0 (0.0.0.0' means 'Obtain an IP address automatically')
Authentication Protocol	Auto
MTU	1492

Username: Enter the username provided by your ISP. You can input up to 256 alphanumeric characters (case sensitive).

Password: Enter the password provided by your ISP. You can input up to 32 alphanumeric characters (case sensitive).

Service Name: This item is for identification purposes. If it is required, your ISP will provide you the necessary information. Maximum input is 32 alphanumeric characters.

IP Address: Enter your fixed IP address.

Authentication Protocol: Default is Auto. Please consult your ISP on whether to use Chap, Pap or MSCHAP.

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

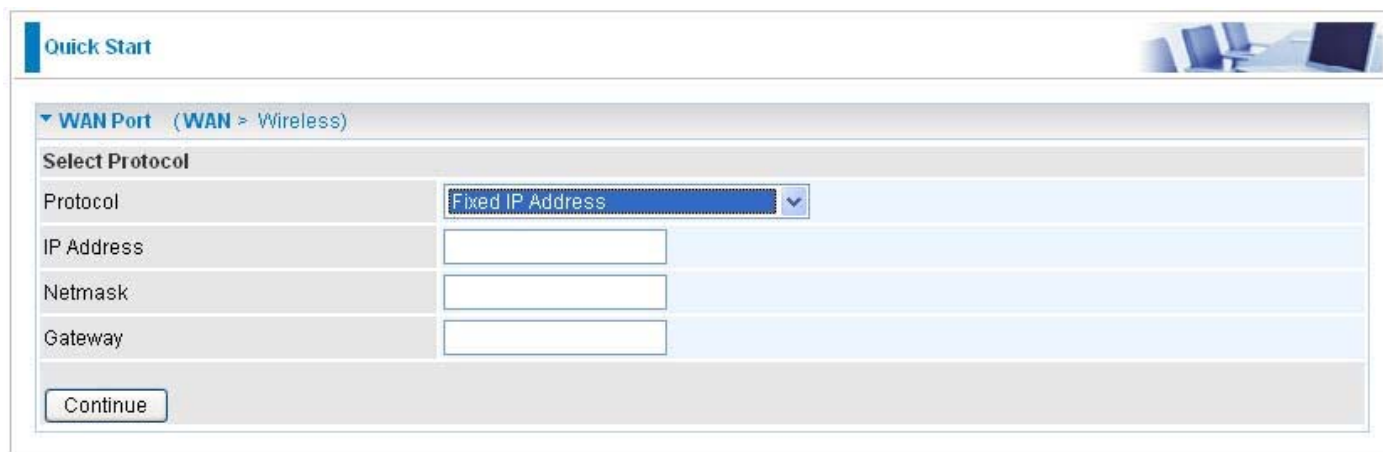
Obtain an IP Address Automatically

Select this protocol enables the device to automatically retrieve IP address.



The screenshot shows a web interface for configuring a WAN port. At the top left, there is a 'Quick Start' tab. Below it, a breadcrumb trail reads 'WAN Port (WAN > Wireless)'. The main section is titled 'Select Protocol'. Under this heading, there is a 'Protocol' dropdown menu with 'Obtain an IP Address Automatically' selected. A 'Continue' button is located at the bottom left of the form.

Fixed IP Address



The screenshot shows the same web interface as above, but with 'Fixed IP Address' selected in the 'Protocol' dropdown menu. Below the protocol selection, there are three input fields: 'IP Address', 'Netmask', and 'Gateway'. A 'Continue' button is located at the bottom left of the form.

IP Address: Enter your fixed IP address.

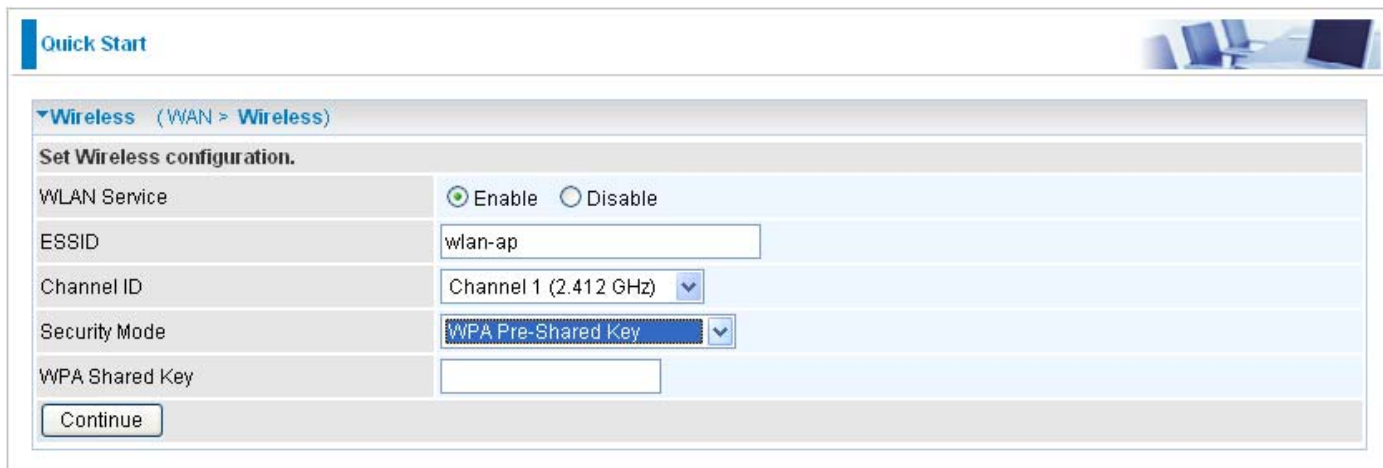
Netmask: User can change it to others such as 255.255.255.128. Type the netmask assigned to you by your ISP (if given).

Gateway: Enter the IP address of the default gateway.

Wireless Setting Mode (only for BiPAC 7800N)

WPA / WPA2 / WPA/WPA2 Pre-shared Key

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.



Quick Start

▼Wireless (WAN > Wireless)

Set Wireless configuration.

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

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.

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

Quick Start

▼ **Wireless** (WAN > **Wireless**)

Set Wireless configuration.

WLAN Service Enable Disabled

ESSID

Channel ID

Security Mode

Default Used WEP Key 1 2 3 4

Key

WEP 64 - Hex: 10 Hex codes, (1~9, a~f, A~F). EX: 11aa22cc33.
WEP 64 - ASCII: 5 ASCII characters are required. Insert your WEP key manually. EX: 1a3eb.
WEP 128 - Hex: 26 Hex codes, (1~9, a~f, A~F). EX: 11aa22cc33dd44ee55efffe35f.
WEP 128 - ASCII: 13 ASCII characters are required. Insert your WEP key manually. EX: 1a3e?lddb3ert.

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.


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**.

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

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 either be HEX style or ASCII format, 10 and 26 HEX codes or 5 and 13 ASCII codes are required for WEP64 and WEP128 respectively.

Status (Basic Mode)

Status 

Device Information

Model Name	BIPAC 7800N
System Up-Time	1 Hour(s) 13 min(s)
Hardware Version	Annex A
Software Version	1.02b.RC3

Port Status

Ethernet	✓
ADSL	✗
EWAN	✗
Wireless ▶	✓

WAN

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

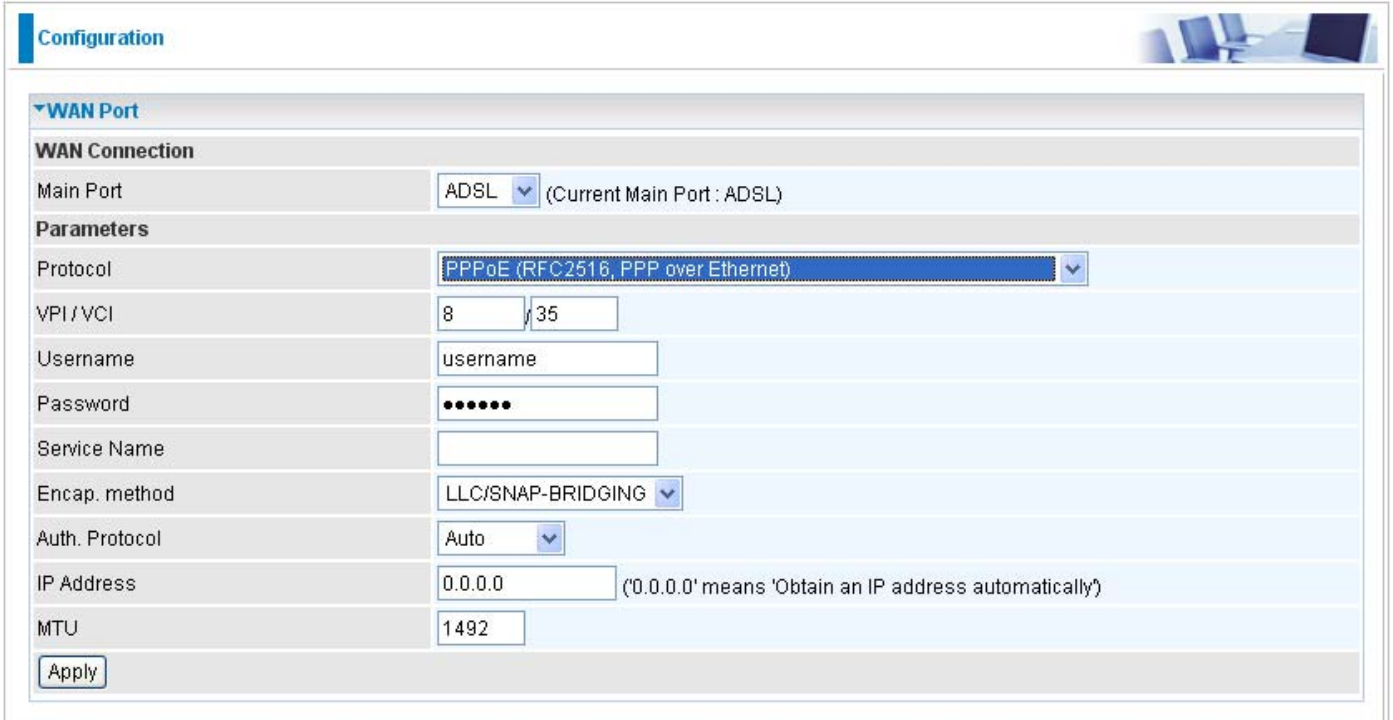
Configuration (Basic Mode)

A WAN (Wide Area Network) is an outside connection to another network or the Internet.

WAN – 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 a configuration page titled "Configuration" with a sub-section "WAN Port". Under "WAN Connection", the "Main Port" is set to "ADSL" (Current Main Port: ADSL). The "Parameters" section includes:

- Protocol: PPPoE (RFC2516, PPP over Ethernet)
- VPI/VCI: 8 / 35
- Username: username
- Password: masked with dots
- Service Name: empty
- Encap. method: LLC/SNAP-BRIDGING
- Auth. Protocol: Auto
- IP Address: 0.0.0.0 (Note: '0.0.0.0' means 'Obtain an IP address automatically')
- MTU: 1492

An "Apply" button is located at the bottom left of the configuration area.

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

Username: Enter the username provided by your ISP. You can input up to 256 alphanumeric characters (case sensitive).

Password: Enter the password provided by your ISP. You can input up to 32 alphanumeric characters (case sensitive).

Service Name: This item is for identification purposes. If it is required, your ISP will provide you the necessary information. Maximum input is 32 alphanumeric characters.

Encap. method: Select the encapsulation format. Select the one provided by your ISP.

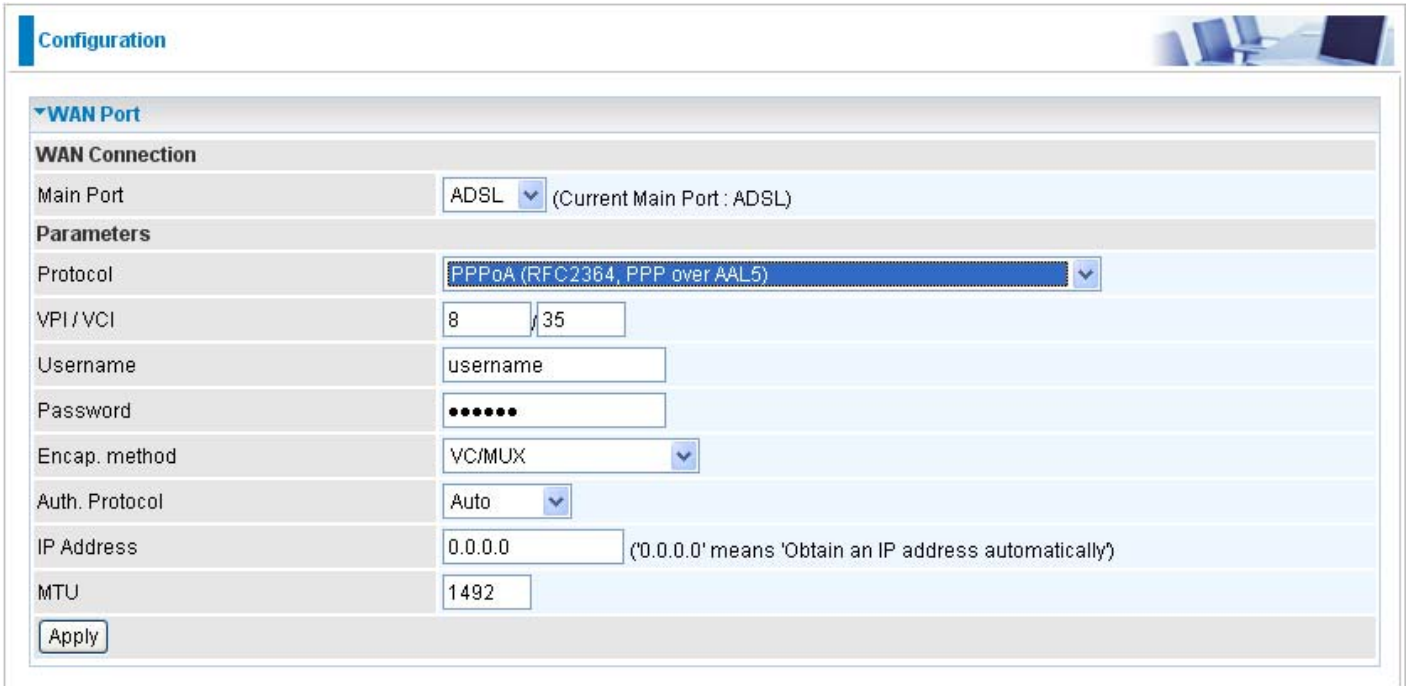
Auth. Protocol: Default is Auto. Please consult your ISP on whether to use Chap, Pap or MSCHAP.

IP Address(0.0.0.0:Auto): Your WAN IP address. Leave this at 0.0.0.0 to obtain automatically 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.

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.



The screenshot shows a configuration window titled "Configuration" with a sub-section "WAN Port". Under "WAN Connection", the "Main Port" is set to "ADSL" (Current Main Port : ADSL). The "Parameters" section includes: "Protocol" set to "PPPoA (RFC2364, PPP over AAL5)", "VPI/VCI" set to "8/35", "Username" set to "username", "Password" masked with "*****", "Encap. method" set to "VC/MUX", "Auth. Protocol" set to "Auto", "IP Address" set to "0.0.0.0" (with a note: "(0.0.0.0' means 'Obtain an IP address automatically)'), and "MTU" set to "1492". An "Apply" button is located at the bottom left of the configuration area.

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

Username: Enter the username provided by your ISP. You can input up to 256 alphanumeric characters (case sensitive).

Password: Enter the password provided by your ISP. You can input up to 32 alphanumeric characters (case sensitive).

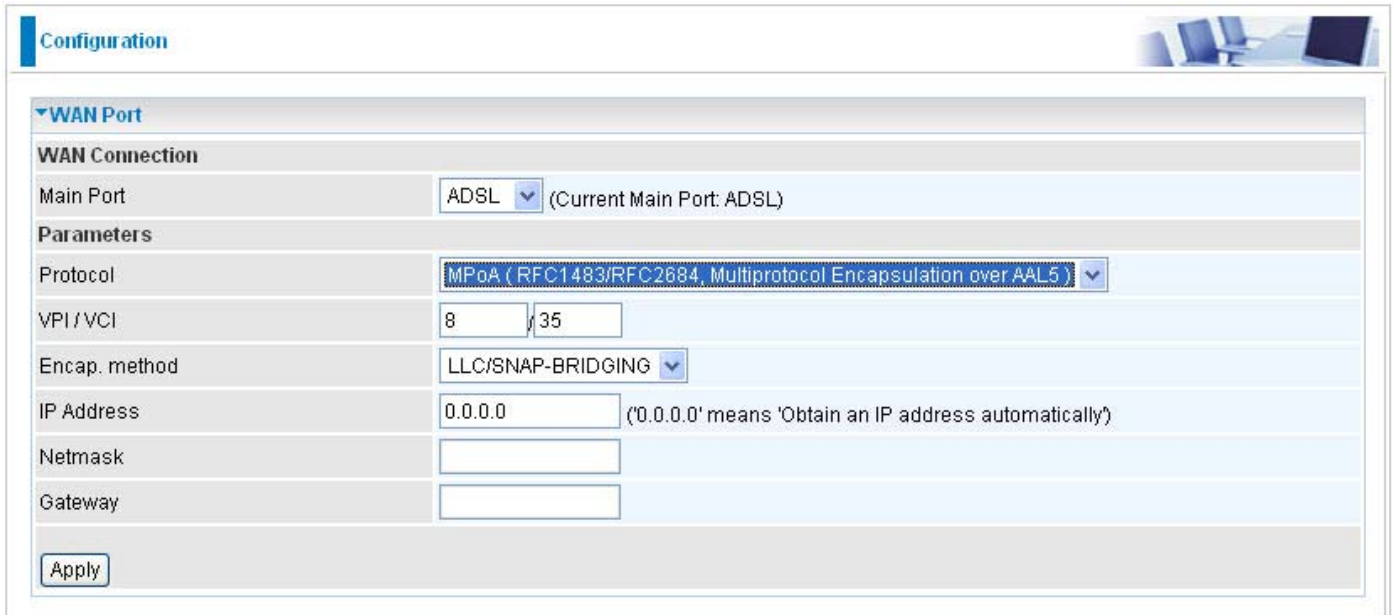
Encap. method: Select the encapsulation format. Select the one provided by your ISP.

Auth. Protocol: Default is Auto. Please consult your ISP on whether to use Chap, Pap or MSCHAP.

IP Address(0.0.0.0:Auto): Your WAN IP address. Leave the IP address as 0.0.0.0 to enable the device 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.

MPoA Connection (ADSL)



The screenshot shows a configuration page titled "Configuration" with a sub-section "WAN Port". Under "WAN Connection", the "Main Port" is set to "ADSL" with a note "(Current Main Port: ADSL)". The "Parameters" section includes:

- Protocol:** A dropdown menu showing "MPoA (RFC1483/RFC2684, Multiprotocol Encapsulation over AAL5)".
- VPI / VCI:** Two input fields containing "8" and "35".
- Encap. method:** A dropdown menu showing "LLC/SNAP-BRIDGING".
- IP Address:** An input field containing "0.0.0.0" with a note "(0.0.0.0' means 'Obtain an IP address automatically)".
- Netmask:** An empty input field.
- Gateway:** An empty input field.

An "Apply" button is located at the bottom left of the configuration area.

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

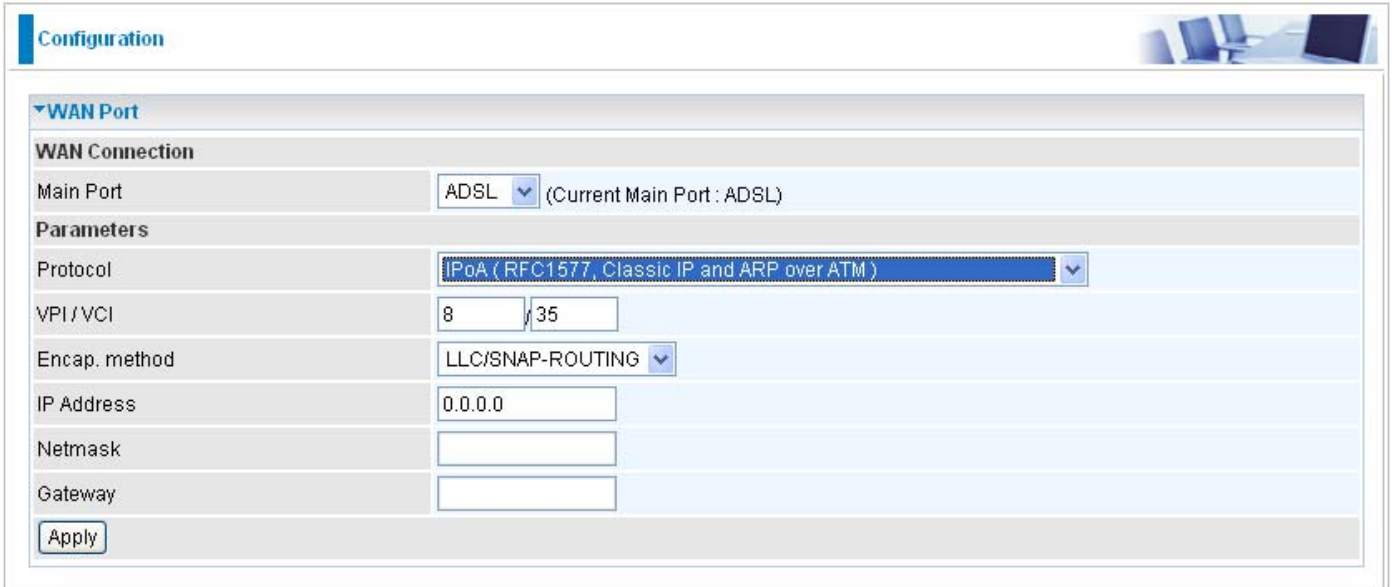
Encap. method: Select the encapsulation format. Select the one provided by your ISP.

IP Address: Your WAN IP address. If the IP is set to 0.0.0.0 (auto IP detect), both netmask and gateway may be left blank.

Netmask: User can change it to others 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.

IPoA Connections (ADSL)



The screenshot shows a configuration window titled "Configuration" with a sub-section "WAN Port". Under "WAN Connection", the "Main Port" is set to "ADSL" with a note "(Current Main Port : ADSL)". The "Parameters" section includes:

- Protocol:** A dropdown menu showing "IPoA (RFC1577, Classic IP and ARP over ATM)".
- VPI / VCI:** Two input fields containing "8" and "35".
- Encap. method:** A dropdown menu showing "LLC/SNAP-ROUTING".
- IP Address:** An input field containing "0.0.0.0".
- Netmask:** An empty input field.
- Gateway:** An empty input field.

An "Apply" button is located at the bottom left of the configuration area.

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

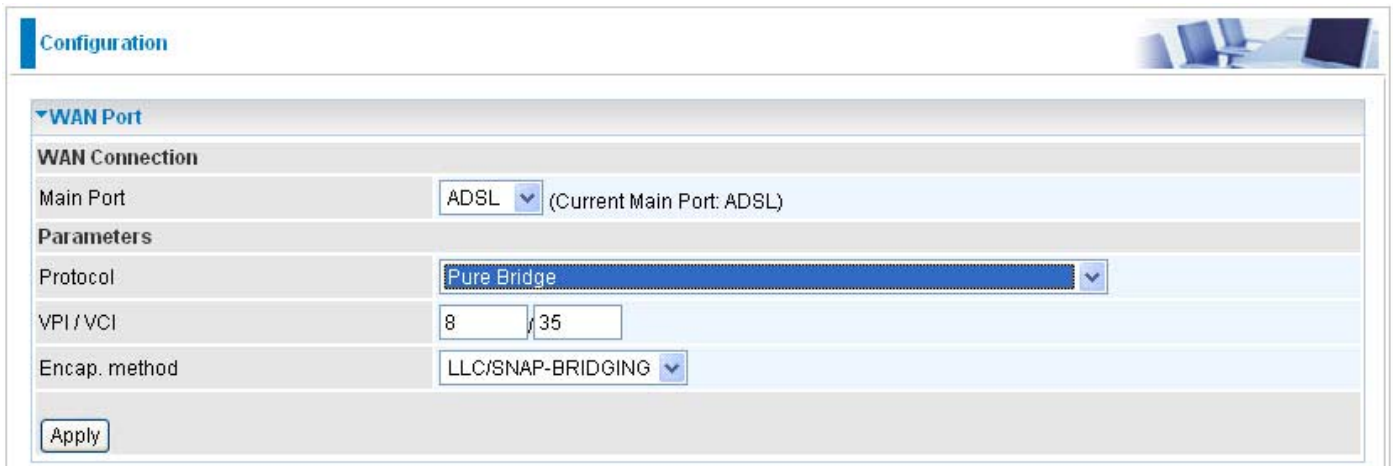
Encap. method: Select the encapsulation format. Select the one provided by your ISP.

IP Address: Enter your fixed IP address.

Netmask: User can change it to others 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.

Pure Bridge Connections (ADSL)



The screenshot shows a configuration window titled "Configuration" with a sub-section for "WAN Port". Under "WAN Connection", the "Main Port" is set to "ADSL" with a note "(Current Main Port: ADSL)". Under "Parameters", the "Protocol" is set to "Pure Bridge", "VPI/VCI" is set to "8/35", and "Encap. method" is set to "LLC/SNAP-BRIDGING". An "Apply" button is located at the bottom left of the configuration area.

WAN Connection	
Main Port	ADSL (Current Main Port: ADSL)
Parameters	
Protocol	Pure Bridge
VPI/VCI	8/35
Encap. method	LLC/SNAP-BRIDGING

Apply

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

Encap. method: Select the encapsulation format. Select the one provided by your ISP.

WAN – Main Port (EWAN)

Besides using ADSL to get connected to the Internet, EWAN port of BiPAC 7800(N) can be used as an alternative to connect to Cable Modems, VDSL and fiber optic lines. This alternative not only provides faster connection to the Internet, it also provides users with more flexibility to get online.

PPPoE (EWAN)

The screenshot shows a web-based configuration interface for a WAN port. The main heading is 'Configuration'. Below it, there's a section for 'WAN Port'. Under 'WAN Connection', the 'Main Port' is set to 'EWAN' (Current Main Port: ADSL). Under 'Parameters', the 'Protocol' is set to 'PPPoE', 'Username' is 'username', 'Password' is masked with dots, 'Service Name' is empty, 'Auth. Protocol' is 'Auto', 'IP Address' is '0.0.0.0' (with a note that '0.0.0.0' means 'Obtain an IP address automatically'), and 'MTU' is '1492'. An 'Apply' button is at the bottom left.

Username: Enter the username provided by your ISP. You can input up to 256 alphanumeric characters (case sensitive).

Password: Enter the password provided by your ISP. You can input up to 32 alphanumeric characters (case sensitive).

Service Name: This item is for identification purposes. If it is required, your ISP will provide you the necessary information. Maximum input is 32 alphanumeric characters.

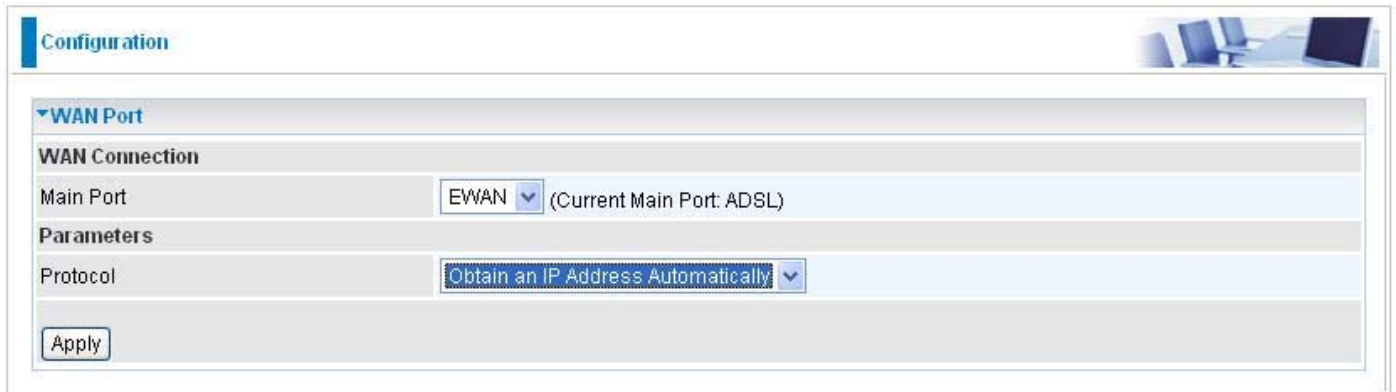
Auth. Protocol: Default is Auto. Please consult your ISP on whether to use Chap, Pap or MSCHAP.

IP Address: Enter your fixed IP address.

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

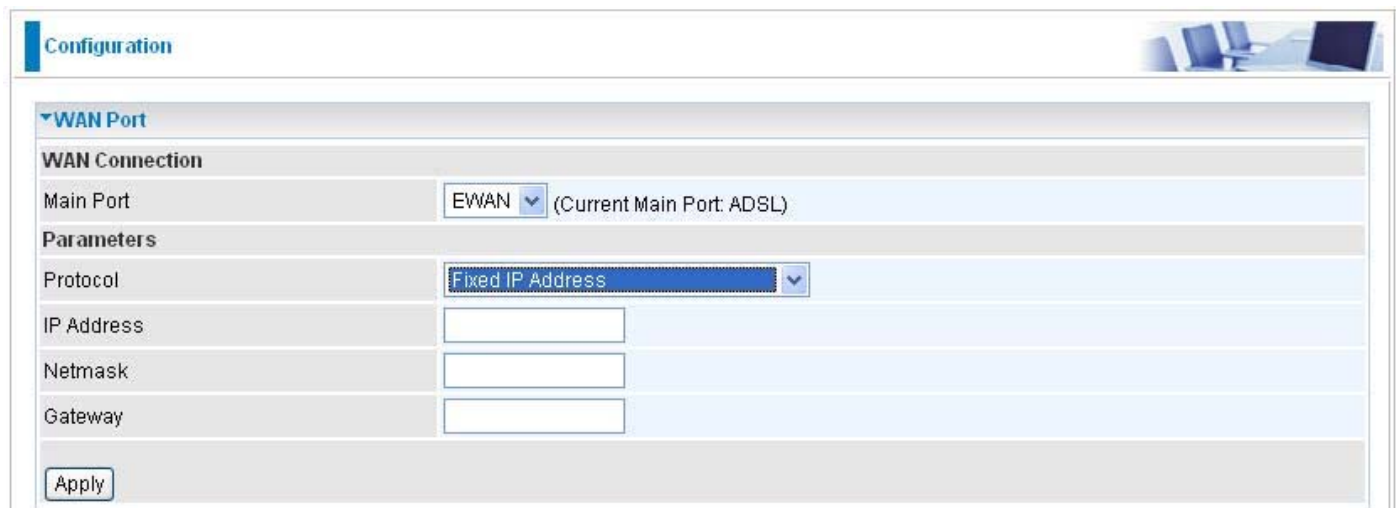
Obtain IP Address Automatically (EWAN)

Select this protocol enables the device to automatically retrieve IP address.



The screenshot shows a web interface for configuring a WAN port. The page is titled 'Configuration' and has a sub-section 'WAN Port'. Under 'WAN Connection', the 'Main Port' is set to 'EWAN' (Current Main Port: ADSL). Under 'Parameters', the 'Protocol' is set to 'Obtain an IP Address Automatically'. There is an 'Apply' button at the bottom left.

Fixed IP Address (EWAN)



The screenshot shows the same web interface for configuring a WAN port. The 'Protocol' is now set to 'Fixed IP Address'. Below this, there are three input fields for 'IP Address', 'Netmask', and 'Gateway'. There is an 'Apply' button at the bottom left.

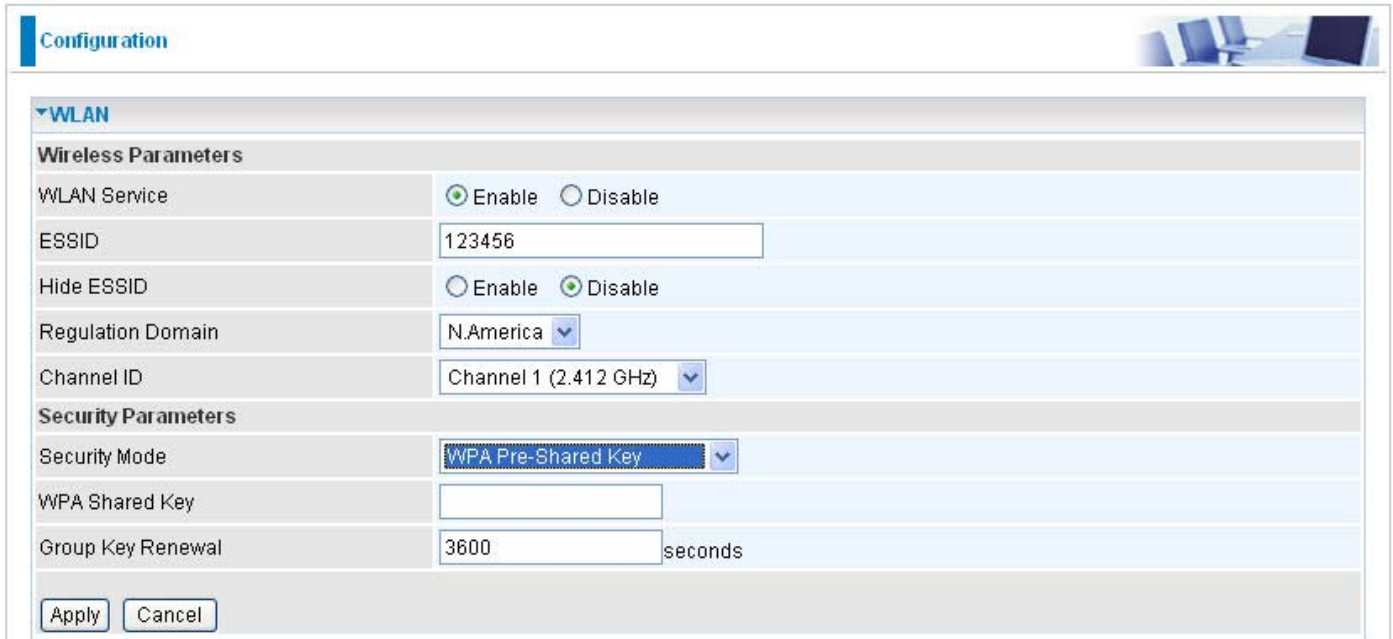
IP Address: Enter your fixed IP address.

Netmask: User can change it to others 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.

WLAN (only for BiPAC 7800N)

WPA / WPA2 / WPA/WPA2 Pre-Shared Key



Configuration

WLAN

Wireless Parameters

WLAN Service: Enable Disable

ESSID:

Hide ESSID: Enable Disable

Regulation Domain:

Channel ID:

Security Parameters

Security Mode:

WPA Shared Key:

Group Key Renewal: seconds

Wireless Parameters

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 by other AP(s).*

Security Parameters

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 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.

WEP

Configuration

WLAN

Wireless Parameters

WLAN Service Enable Disable

ESSID

Hide ESSID Enable Disable

Regulation Domain

Channel ID

Security Parameters

Security Mode

WEP Authentication

Default Used WEP Key 1 2 3 4

Passphrase(Generate Key)

Key 1

Key 2

Key 3

Key 4

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?lddb3ert.

Parameters

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 by other AP(s).*

Security Parameters

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

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.

Status (Advanced Mode)

Status



Device Information

Model Name	BIPAC 7800N
Host Name ▶	home.gateway
System Up-Time	41 min(s)
Current Time ▶	Sat Jan 1 00:41:18 2000
Hardware Version	Annex A
Software Version	1.02b.RC3
MAC Address	00:04:ed:78:00:d8

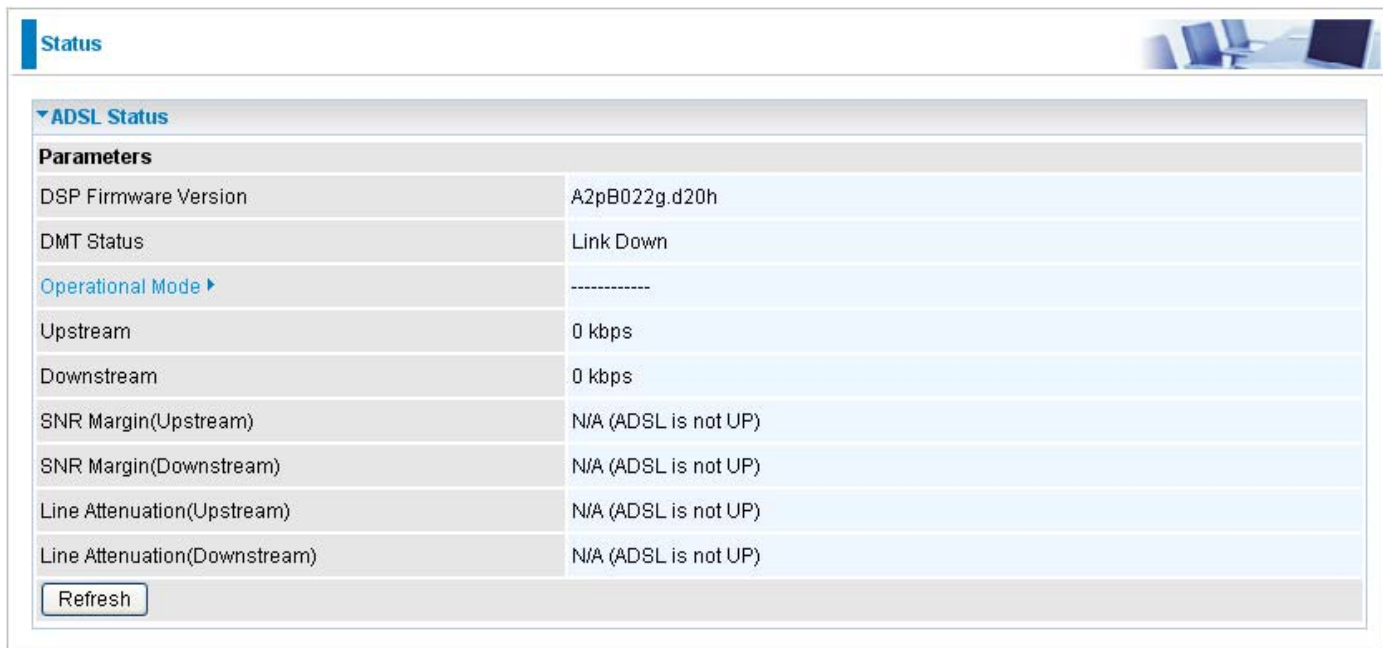
Port Status

Ethernet	✓
ADSL ▶	✗
EWAN	✗
Wireless ▶	✓

WAN

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

ADSL

The screenshot shows a web interface for ADSL status. At the top left, there is a 'Status' tab. Below it, a section titled 'ADSL Status' is expanded. Underneath, a 'Parameters' section contains a table with various ADSL metrics and their current values. A 'Refresh' button is located at the bottom of the table.

Parameters	
DSP Firmware Version	A2pB022g.d20h
DMT Status	Link Down
Operational Mode ▶	-----
Upstream	0 kbps
Downstream	0 kbps
SNR Margin(Upstream)	N/A (ADSL is not UP)
SNR Margin(Downstream)	N/A (ADSL is not UP)
Line Attenuation(Upstream)	N/A (ADSL is not UP)
Line Attenuation(Downstream)	N/A (ADSL is not UP)

DSP Firmware Version: DSP code version.

DMT Status: Current DMT Status.

Operational Mode: Display the ADSL state when the connect mode is set to AUTO.

Upstream: Upstream rate.

Downstream: Downstream rate.

SNR Margin (Upstream): This shows the SNR margin for upstream rate.

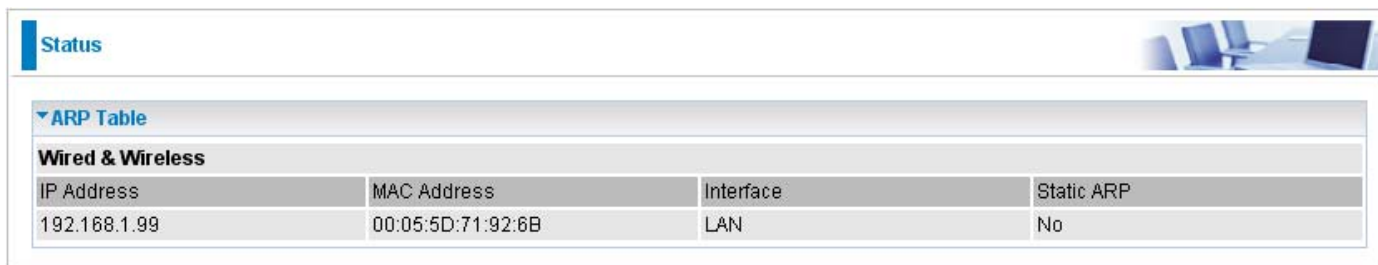
SNR Margin (Downstream): This shows the SNR margin for downstream rate.

Line Attenuation (Upstream): This is attenuation of signal in upstream.

Line Attenuation (Downstream): This is attenuation of signal in downstream.

ARP

This table stores mapping information that the device uses to find the Layer 2 Media Access Control (MAC) address that corresponds to the Layer 3 IP address of the device via the Address Resolution Protocol (ARP) feature.



▼ ARP Table			
Wired & Wireless			
IP Address	MAC Address	Interface	Static ARP
192.168.1.99	00:05:5D:71:92:6B	LAN	No

IP Address: Shows the IP Address of the device that the MAC address maps to.

MAC Address: Shows the MAC address that is corresponded to the IP address of the device it is mapped to.

Interface: The interface name (on the router) that this IP address connects to.

Static ARP: Shows the status of static ARP.

DHCP



▼ DHCP Table			
Leased Table			
IP Address ▶	MAC Address	Client Host Name	Register Information
192.168.1.100	00:21:5D:A7:06:64		Remains 35
192.168.1.101	00:05:5D:71:92:6B	chris-7c4c197a4	Remains 23:59:47

IP Address: This is the IP address that is assigned to the host with this MAC address.


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

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

Register Information: Shows the information provided during registration.

System Log

Display all the system logs that have been recorded up to the present time.

Status 

▼ System Log

Current Time : Sat Jan 1 08:15:05 2000

```
Jan 1 00:00:27 user kernel: eth0: MAC Address: 00:04:ED:78:01:D0
Jan 1 00:00:27 user kernel: Broadcom BCM6358A1 Ethernet Network Device v0.3 Nov 20 2008
16:32:44
Jan 1 00:00:27 user kernel: Config Ethernet Switch Through MDIO Pseudo PHY Interface
Jan 1 00:00:28 user kernel: ethsw: found bcm5395!
Jan 1 00:00:28 user kernel: dgas: kerSysRegisterDyingGaspHandler: eth1 registered
Jan 1 00:00:28 user kernel: eth1: MAC Address: 00:04:ED:78:01:D0
Jan 1 00:00:28 user kernel: rt2880_iNIC: falsely claims to have parameter bridge
Jan 1 00:00:28 user kernel: RT2880 iNIC: 802.11n WLAN PCI driver v1.1.7.0 (Feb 15, 2008)
Jan 1 00:00:28 user kernel: RT2880 iNIC: pci dev 0000:00:01.0 (id 1814:0801 rev 00)
Jan 1 00:00:28 user kernel: PCI: Enabling device 0000:00:01.0 (0000 -> 0002)
Jan 1 00:00:28 user kernel: rt->regs = b00000000
Jan 1 00:00:28 user kernel: ra0: Ralink iNIC at 0xb0000000, 00:00:00:00:00:00, IRQ 39
Jan 1 00:00:28 user kernel: PCI: Setting latency timer of device 0000:00:01.0 to 64
Jan 1 00:00:28 user kernel: ==> Get MAC from iNIC
Jan 1 00:00:28 user kernel: ===== Init Thread =====
Jan 1 00:00:28 user kernel: RacfgTaskThread pid = 74
Jan 1 00:00:28 user kernel: RacfgBacklogThread pid = 75
Jan 1 00:00:28 user kernel: eth1 Link UP.
Jan 1 00:00:28 user kernel: BcmAdsl_Initialize=0xC005E3C8, g_pFnNotifyCallback=0xC0077294
```

Refresh Clear

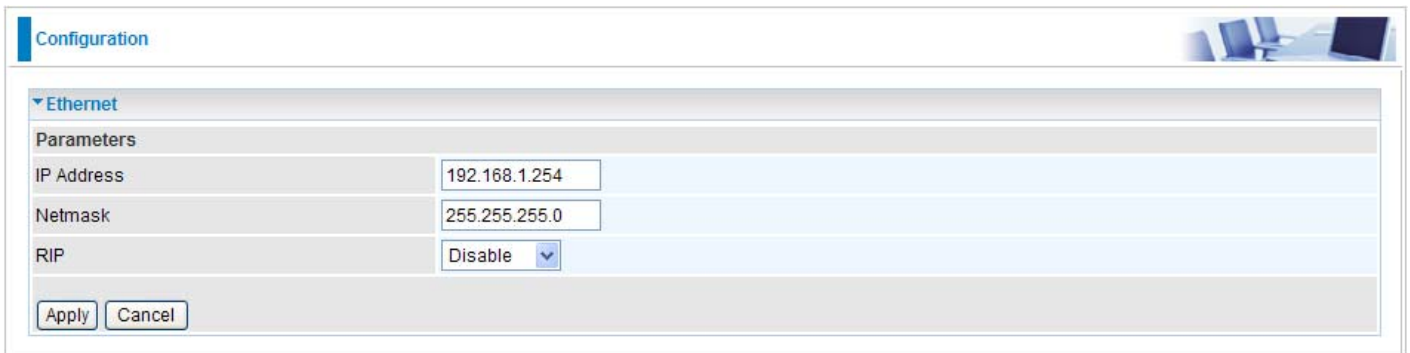
Configuration (Advanced Mode)

LAN

A Local Area Network (LAN) is a shared communication system network where many computers are connected. This type of network is area defined and is usually limited to a confined region within a building or just within the same storey of a building. There are 5 items within the LAN section: **Ethernet**, **IP Alias**, **Wireless (7800N only)**, **Wireless Security (7800N only)** and **DHCP Server**.

Ethernet

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



The screenshot shows the 'Configuration' page for the router. Under the 'Ethernet' section, there is a 'Parameters' table with the following values:

Parameters	
IP Address	192.168.1.254
Netmask	255.255.255.0
RIP	Disable

At the bottom of the form, there are 'Apply' and 'Cancel' buttons.

subnet in their LAN. The default IP address for the router is 192.168.1.254.

IP Address: The default IP on this router.

Netmask: The default subnet mask on this router.

RIP: RIP v1, RIP v2 & RIP v1+v2.

IP Alias

This function allows the addition an IP alias to the network interface. This further allows user the flexibility to assign a specific function to use this IP.



The screenshot shows the 'Configuration' page for the router. Under the 'IP Alias' section, there is a 'Parameters' table with the following values:

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

At the bottom of the form, there are 'Apply' and 'Cancel' buttons.

IP Address: Enter the IP address to be added to the network.

Netmask: Specify a subnet mask for the IP to be added.

Wireless (only for BiPAC 7800N)

Configuration

Wireless

Parameters

WLAN Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
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 Power Level	100 (0 ~ 100)
AP MAC Address	00:1D:92:1C:0F:E3
AP Firmware Version	1.1.7.0
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"/>

Apply Cancel [Security settings ▶](#)

Parameters

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

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

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 by other AP(s).*

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

TX PowerLevel: It is a 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 premise environment, 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: Select Enable if you would like to activate WPS service.

WPS State: This column allows you to set the status of the device wireless setting whether it has been configured or unconfigured. For WPS configuration please refer to the section on [Wi-Fi Network Setup](#) for detail.

WMM: This feature is used to control the prioritization of traffic according to 4 Access categories: Voice, Video, Best Effort and Background. Default is set to disable.

[Wireless Distribution System \(WDS\)](#)

It is a wireless access point mode that enables wireless link and communication with other access points. It is easy to install simply by defining the peer's MAC address of the connected AP. WDS takes advantages of the cost saving and flexibility which no extra wireless client device is required to bridge between two access points and extending an existing wired or wireless infrastructure network to create a larger network. It can connect up to 4 wireless APs for extending cover range at the same time.

In addition, WDS also enhances its link connection security mode. Key encryption and channel must be the same for both access points.

WDS Service: The default setting is **Disabled**. 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, the format can be: xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx*

Wireless Security (only for BiPAC 7800N)

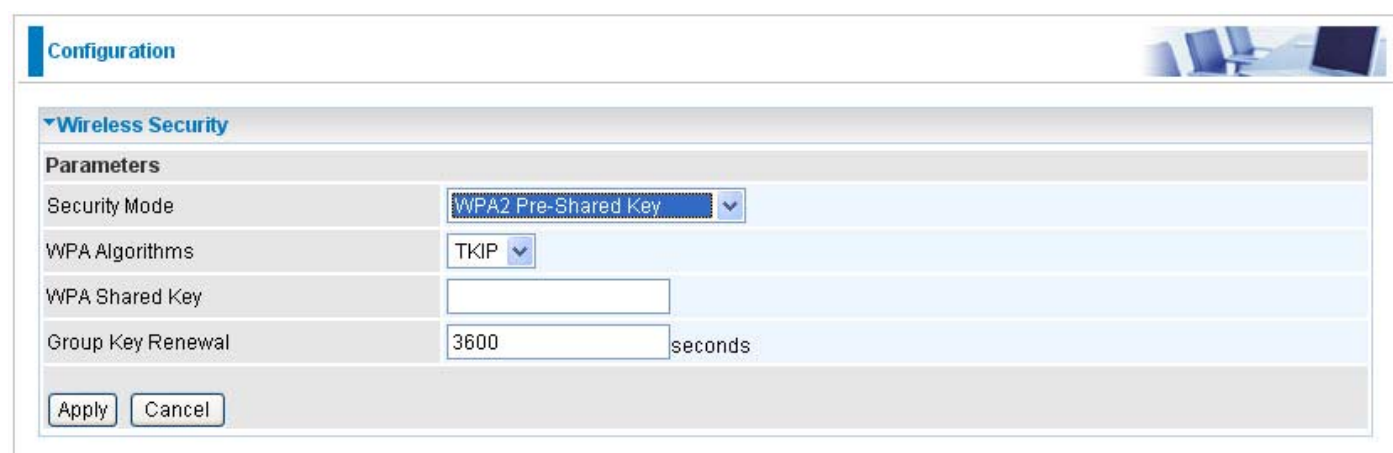
You can disable or enable wireless security with WPA or WEP for protecting wireless network.

The default mode of wireless security is disabled.



The screenshot shows the 'Configuration' page with a 'Wireless Security' section. Under 'Parameters', the 'Security Mode' dropdown menu is set to 'Disable'. There are 'Apply' and 'Cancel' buttons at the bottom of the section.

WPA / WPA2 / WPA/WPA2 Pre-Shared Key



The screenshot shows the 'Configuration' page with a 'Wireless Security' section. Under 'Parameters', the 'Security Mode' dropdown menu is set to 'WPA2 Pre-Shared Key', 'WPA Algorithms' is set to 'TKIP', 'WPA Shared Key' is an empty text input field, and 'Group Key Renewal' is set to '3600' with the unit 'seconds'. There are 'Apply' and 'Cancel' buttons at the bottom of the section.

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

WPA Algorithms: There are 3 types of the WPA-PSK, WPA2-PSK & WPA/WPA2-PSK. The WPA-PSK adapts the TKIP (Temporal Key Integrity Protocol) encrypted algorithms, which incorporates Message Integrity Code (MIC) to provide protection against hackers. The WPA2-PSK adapts CCMP (Cipher Block Chaining Message Authentication Code Protocol) of the AES (Advanced Encryption Security) algorithms.

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.

WEP

Configuration

Wireless Security

Parameters

Security Mode: WEP

WEP Authentication: Open System

Default Used WEP Key: 1 2 3 4

Passphrase (Generate Key): WEP64 WEP128

Key 1: Hex

Key 2: Hex

Key 3: Hex

Key 4: 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?ldbd3ert.

Apply Cancel

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**.

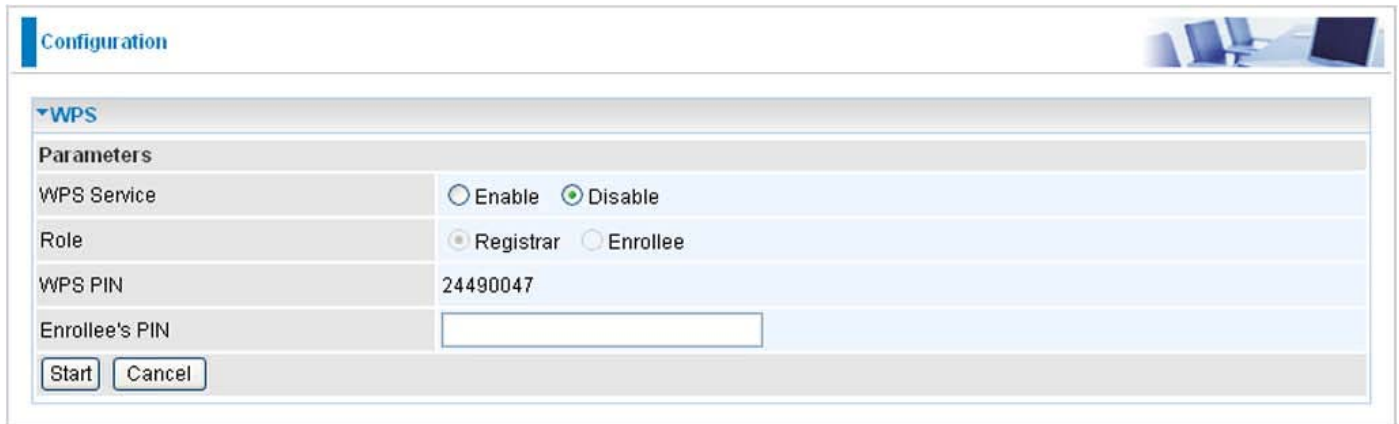
Default Used WEP Key: Select the encryption key ID; please refer to **Key (1~4)** below.

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.

WPS (only for BiPAC 7800N)

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 networks for a residential or an office setting. WPS supports 2 types of configuration methods which are commonly known among consumers: **PIN Method** & **PBC Method**.

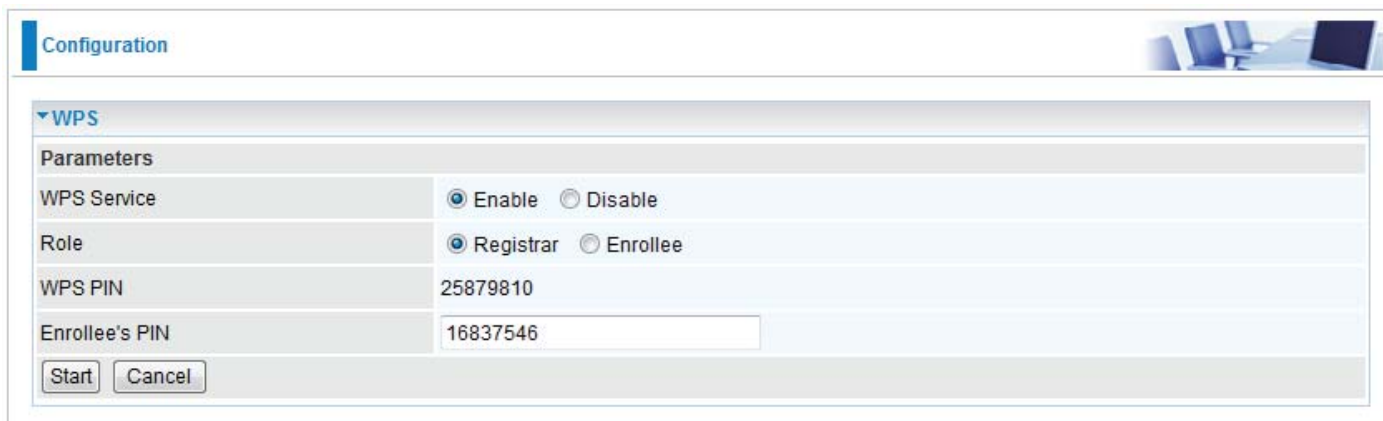


Parameters	
WPS Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Role	<input checked="" type="radio"/> Registrar <input type="radio"/> Enrollee
WPS PIN	24490047
Enrollee's PIN	<input type="text"/>

Wi-Fi Network Setup (only for BiPAC 7800N)

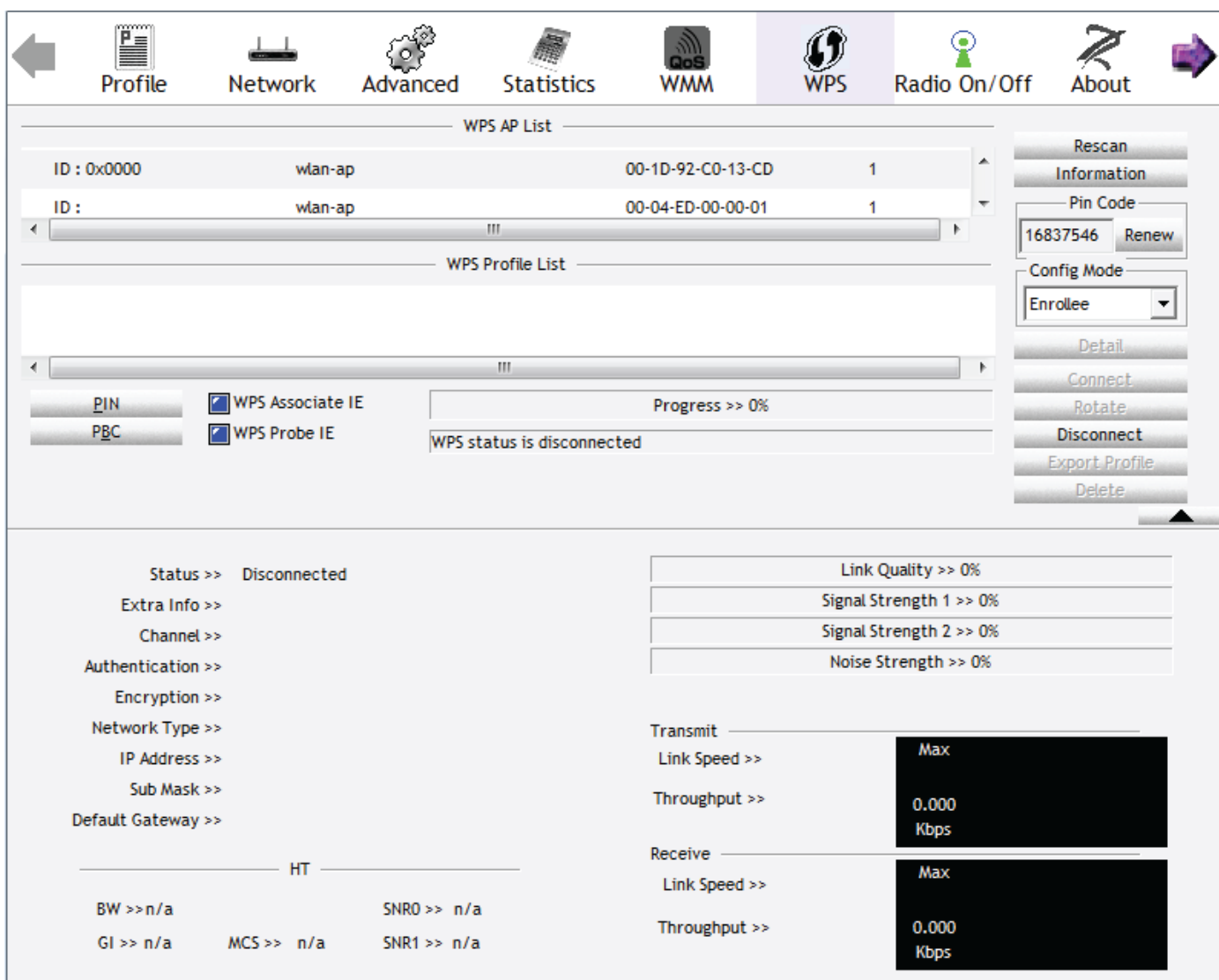
PIN Method: Configure AP as Registrar

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



The screenshot shows the 'Configuration' page with the 'WPS' section expanded. Under 'Parameters', 'WPS Service' is set to 'Enable', 'Role' is set to 'Registrar', 'WPS PIN' is '25879810', and 'Enrollee's PIN' is '16837546'. There are 'Start' and 'Cancel' buttons at the bottom.

2. Enter the Enrollee's PIN number and then press Start.
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 shows the WPS utility interface. The top navigation bar includes Profile, Network, Advanced, Statistics, WMM, WPS, Radio On/Off, and About. The main area is divided into 'WPS AP List' and 'WPS Profile List'. The 'WPS AP List' table shows two entries:

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

The 'WPS Profile List' is currently empty. On the right side, there are buttons for 'Rescan', 'Information', 'Pin Code' (with a field containing '16837546' and a 'Renew' button), 'Config Mode' (set to 'Enrollee'), 'Detail', 'Connect', 'Rotate', 'Disconnect', 'Export Profile', and 'Delete'. At the bottom left, there are 'PIN' and 'PBC' buttons, and checkboxes for 'WPS Associate IE' and 'WPS Probe IE'. The 'Progress' bar shows 'Progress >> 0%' and the status is 'WPS status is disconnected'. The bottom right section shows 'Status >> Disconnected' and various performance metrics like Link Quality, Signal Strength, and Noise Strength, all showing 0%.

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

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

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

ID :	wlan-ap	00-1D-92-C0-13-CD	1
ID :	wlan-ap	00-04-ED-38-F7-2E	1
- WPS Profile List:**
 - Profile: wlan-ap
 - Buttons: PIN, PBC
 - Options: WPS Associate IE, WPS Probe IE
 - Progress: Progress >> 100%
 - Status: PIN - Get WPS profile successfully.
- Right Panel:** Rescan, Information, Pin Code (16837546, Renew), Config Mode (Enrollee), Detail, Connect, Rotate, Disconnect, Export Profile, Delete.
- Status & Performance:**
 - Status >> wlan-ap <-> 00-1D-92-C0-13-CD
 - Extra Info >> Link is Up [TxPower:100%]
 - Channel >> 1 <-> 2412 MHz; central channel : 3
 - Authentication >> Open
 - Encryption >> NONE
 - Network Type >> Infrastructure
 - IP Address >> 192.168.1.100
 - Sub Mask >> 255.255.255.0
 - Default Gateway >> 192.168.1.254
- HT (High Throughput) Parameters:**
 - BW >> 40
 - GI >> long
 - MCS >> 15
 - SNR0 >> 19
 - SNR1 >> n/a
- Link Quality & Signal Strength:**
 - Link Quality >> 100%
 - Signal Strength 1 >> 64%
 - Signal Strength 2 >> 34%
 - Noise Strength >> 26%
- Transmit Performance:**
 - Link Speed >> 270.0 Mbps
 - Throughput >> 5.600 Kbps
- Receive Performance:**
 - Link Speed >> 54.0 Mbps
 - Throughput >> 81.608 Kbps

PIN Method: Configure AP as Enrollee

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

Configuration

WPS

Parameters

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

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.

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

WPS AP List

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

WPS Profile List

ExRegNWEA4036

WPS Associate IE

Progress >> 0%

WPS Probe IE

Pin Code

25879810

Config Mode

Registrar

Status >> Disconnected

Extra Info >>

Channel >>

Authentication >>

Encryption >>

Network Type >>

IP Address >>

Sub Mask >>

Default Gateway >>

Link Quality >> 0%
Signal Strength 1 >> 0%
Signal Strength 2 >> 0%
Noise Strength >> 0%

HT

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

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

Transmit

Link Speed >> Max

Throughput >> 0.000 Kbps

Receive

Link Speed >> Max

Throughput >> 0.000 Kbps

- 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 of 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 the navigation bar, the 'WPS AP List' section shows two entries:

ID	SSID	MAC	Priority
ExRegNWEA4036	00-1D-92-C0-13-CD	1	
wlan-ap	00-04-ED-38-F7-2E	1	

Below this is the 'WPS Profile List' section, which shows the selected 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.' To the right of the profile list, there are several buttons: Rescan, Information, Pin Code (with input field '25879810' and a Renew button), Config Mode (set to Registrar), Detail, Connect, Rotate, Disconnect, and Export Profile.

The bottom section of the interface provides detailed connection statistics for the selected profile:

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

Additional statistics include:

- Link Quality >> 100%
- Signal Strength 1 >> 65%
- Signal Strength 2 >> 39%
- Noise Strength >> 26%
- Transmit Link Speed >> 243.0 Mbps
- Transmit Throughput >> 0.000 Kbps
- Receive Link Speed >> 40.5 Mbps
- Receive Throughput >> 98.612 Kbps

HT (High Throughput) parameters are also listed:

- 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.

WPS AP List

ID :	wlan-ap	00-1D-92-C0-13-CD	1
ID :	wlan-ap	00-04-ED-22-22-23	1

WPS Profile List

ExRegNWEA4036

PIN WPS Associate IE Progress >> 0%
 PBC WPS Probe IE WPS status is disconnected

Rescan
 Information
 Pin Code
 25879810
 Config Mode
 Registrar
 Detail
 Connect
 Rotate
 Disconnect
 Export Profile

SSID >> ExRegNWEA4036
 BSSID >> 00-00-00-00-00-00
 Authentication Type >> WPA2-PSK Encryption Type >> AES
 Key Length >> 5 Key Index >> 1
 Key Material >> 811B5B9F3403DCB08BA738F3E4787581C37DC4BDD147C4E62526D4E8C39DBF78
 Show Password

▼ Wireless

Parameters

WLAN Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Mode	802.11g + n
ESSID	ExRegNWEA4036
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 Power Level	100 (0 ~ 100)
AP MAC Address	00:1D:92:C0:13:CD
AP Firmware Version	1.1.7.0
WPS Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
WPS State	<input checked="" type="radio"/> Configured <input type="radio"/> Unconfigured
WMM	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Wireless Distribution System (WDS)	
WDS Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Peer WDS MAC address	1. <input type="text"/> 2. <input type="text"/> 3. <input type="text"/> 4. <input type="text"/>

 [Security settings ▶](#)

Wireless Security

Parameters

Security Mode	WPA2 Pre-Shared Key
WPA Algorithms	AES
WPA Shared Key	811B5B9F3403DCB08!
Group Key Renewal	3600 seconds

Apply Cancel

PBC Method:

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

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

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

ID	SSID	MAC	Priority
ID :	wlan-ap	00-04-ED-00-00-01	1
ID : 0x0004	wlan-ap	00-1D-92-C0-13-CD	1
- WPS Profile List:** (Empty)
- 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
 - Receive: Link Speed >> 147.408 Kbps
 - HT: BW >> n/a, SNR0 >> n/a, GI >> n/a, MCS >> n/a, SNR1 >> n/a

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

The screenshot displays the WPS configuration interface on a router. At the top, there is a navigation bar with icons for Profile, Network, Advanced, Statistics, WMM, WPS, Radio On/Off, and About. The WPS tab is currently active.

WPS AP List

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

WPS Profile List

wlan-ap

WPS Configuration:

- WPS Associate IE
- WPS Probe IE

Progress >> 100%

PBC - Get WPS profile successfully.

Connection Status:

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

HT (High Throughput) Parameters:

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

Link Quality & Signal Strength:

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

Transmit Statistics:

- Link Speed >> 243.0 Mbps
- Throughput >> 0.192 Kbps
- Current Throughput: 37.696 Kbps

Receive Statistics:

- Link Speed >> 81.0 Mbps
- Throughput >> 93.732 Kbps
- Current Throughput: 1.798 Mbps

Wi-Fi Network Setup with Windows Vista WCN:

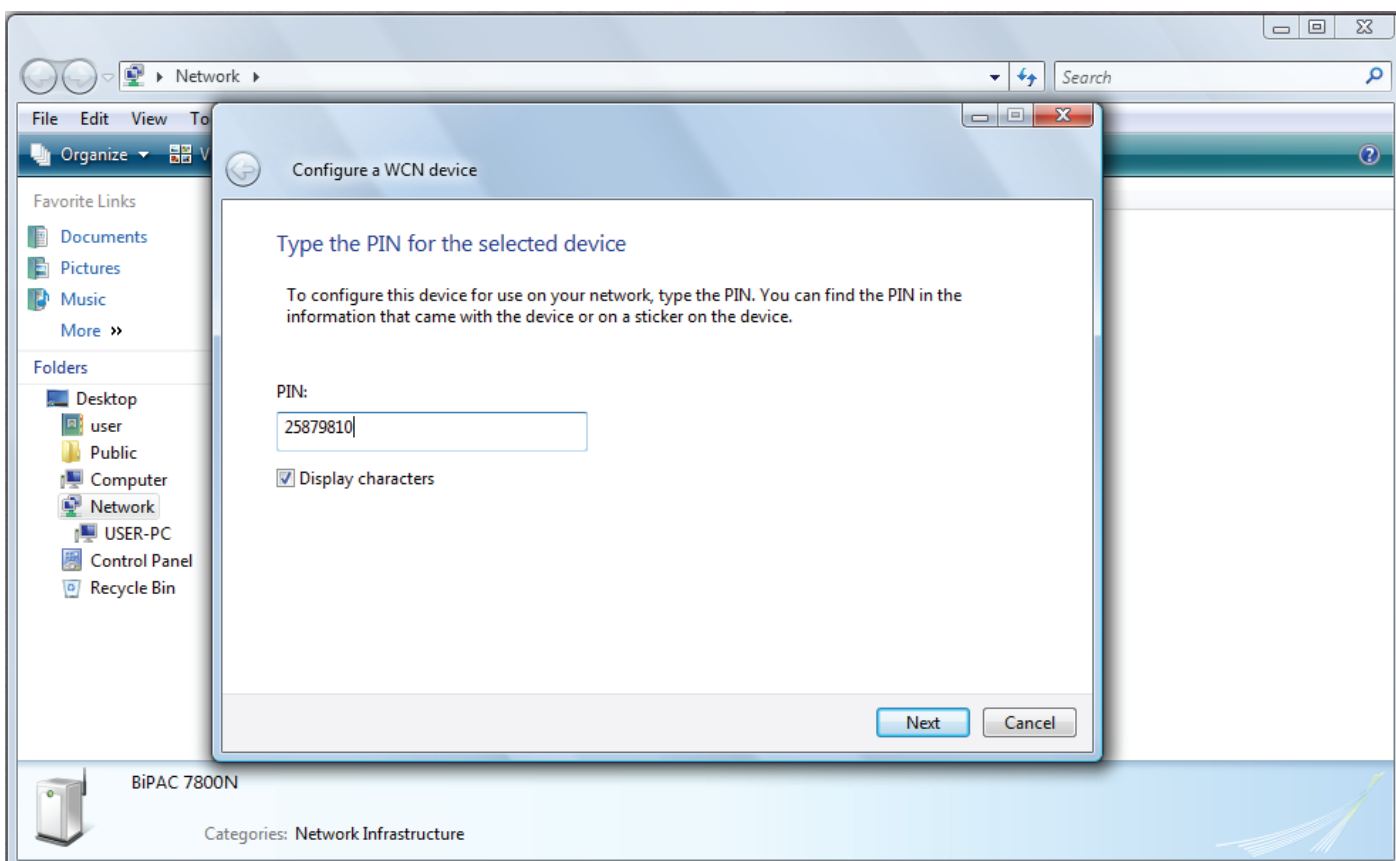
1. Jot down the AP PIN from the Web (eg. 25879810).
2. Access the Wireless configuration of the web GUI. Set the WPS State to Unconfigured then click Apply.

The screenshot shows a web-based configuration interface for wireless settings. The 'Wireless' section is expanded, showing various parameters. The 'WPS State' is set to 'Unconfigured'. Other settings include WLAN Service (Enabled), Mode (802.11g+n), ESSID (wlan-ap), Regulation Domain (N.America), Channel ID (Channel 1 (2.412 GHz)), Channel Width (20/40MHZ), Tx Power Level (100), AP MAC Address (00:1D:92:C0:13:CD), AP Firmware Version (1.1.7.0), WPS Service (Enabled), WMM (Disabled), and Wireless Distribution System (WDS) (Disabled). There are 'Apply' and 'Cancel' buttons at the bottom, along with a link to 'Security settings'.

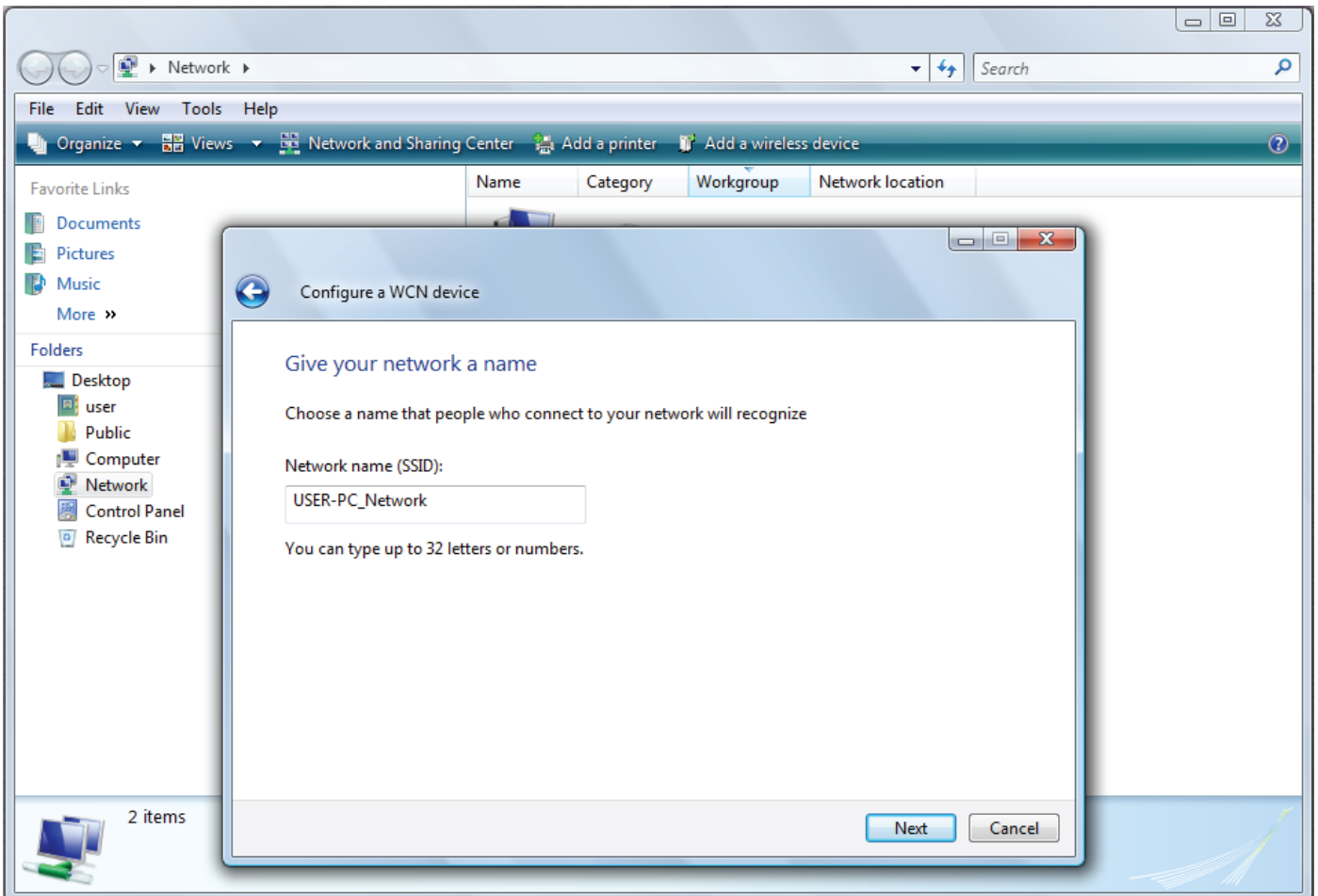
Parameters	
WLAN Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Mode	802.11g + n
ESSID	wlan-ap
Hide ESSID	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Regulation Domain	N.America
Channel ID	Channel 1 (2.412 GHz)
Channel Width	20/40MHZ
Tx Power Level	100 (0 ~ 100)
AP MAC Address	00:1D:92:C0:13:CD
AP Firmware Version	1.1.7.0
WPS Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
WPS State	<input type="radio"/> Configured <input checked="" type="radio"/> Unconfigured
WMM	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Wireless Distribution System (WDS)	
WDS Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Peer WDS MAC address	1. <input type="text"/> 2. <input type="text"/> 3. <input type="text"/> 4. <input type="text"/>

Apply Cancel [Security settings](#)

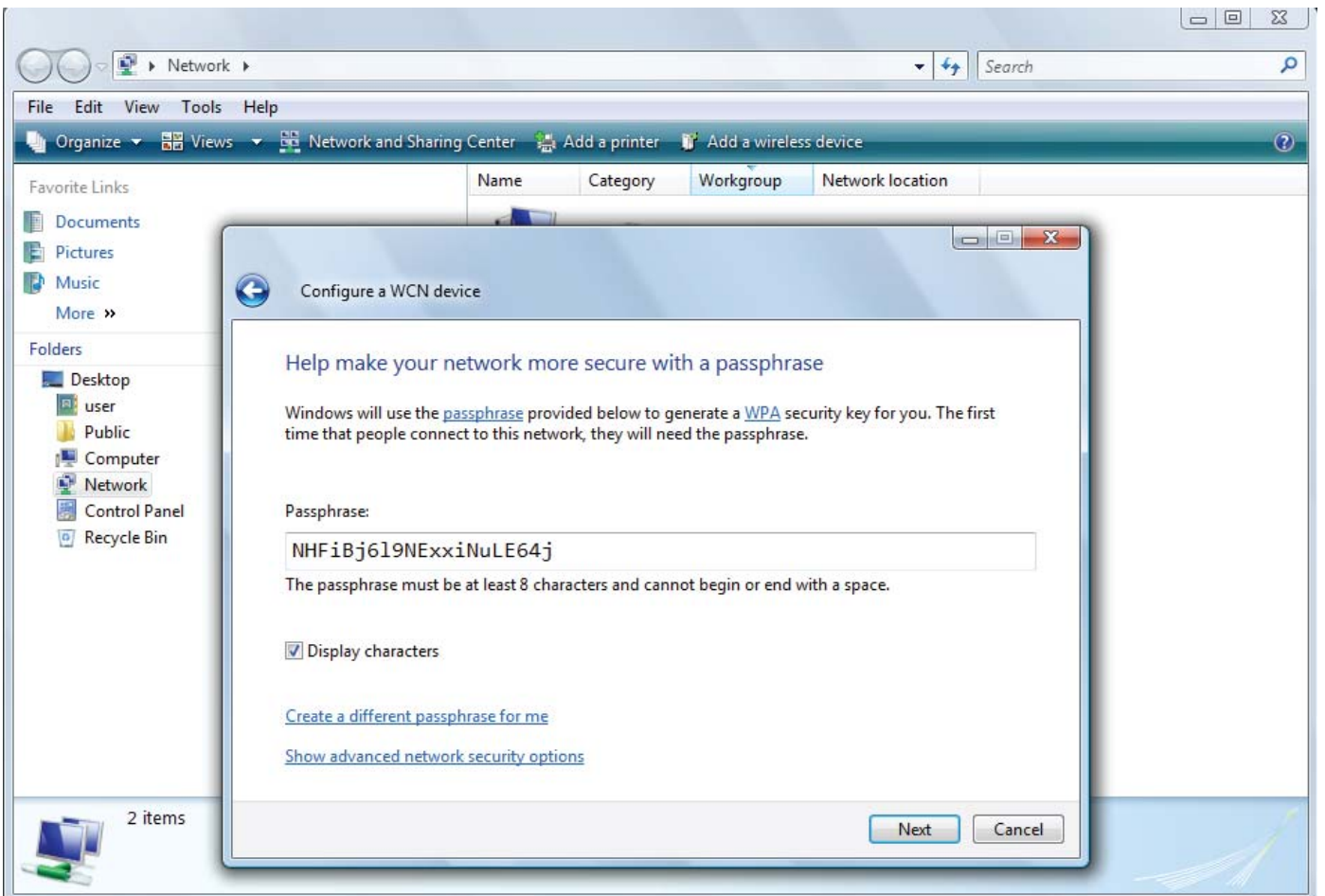
3. In your Vista operating system, access the Control Panel page, then select Network and Internet > View Network Computers and Devices. Double click on the BiPAC 7800N icon and enter the AP PIN in the column provided then press Next.



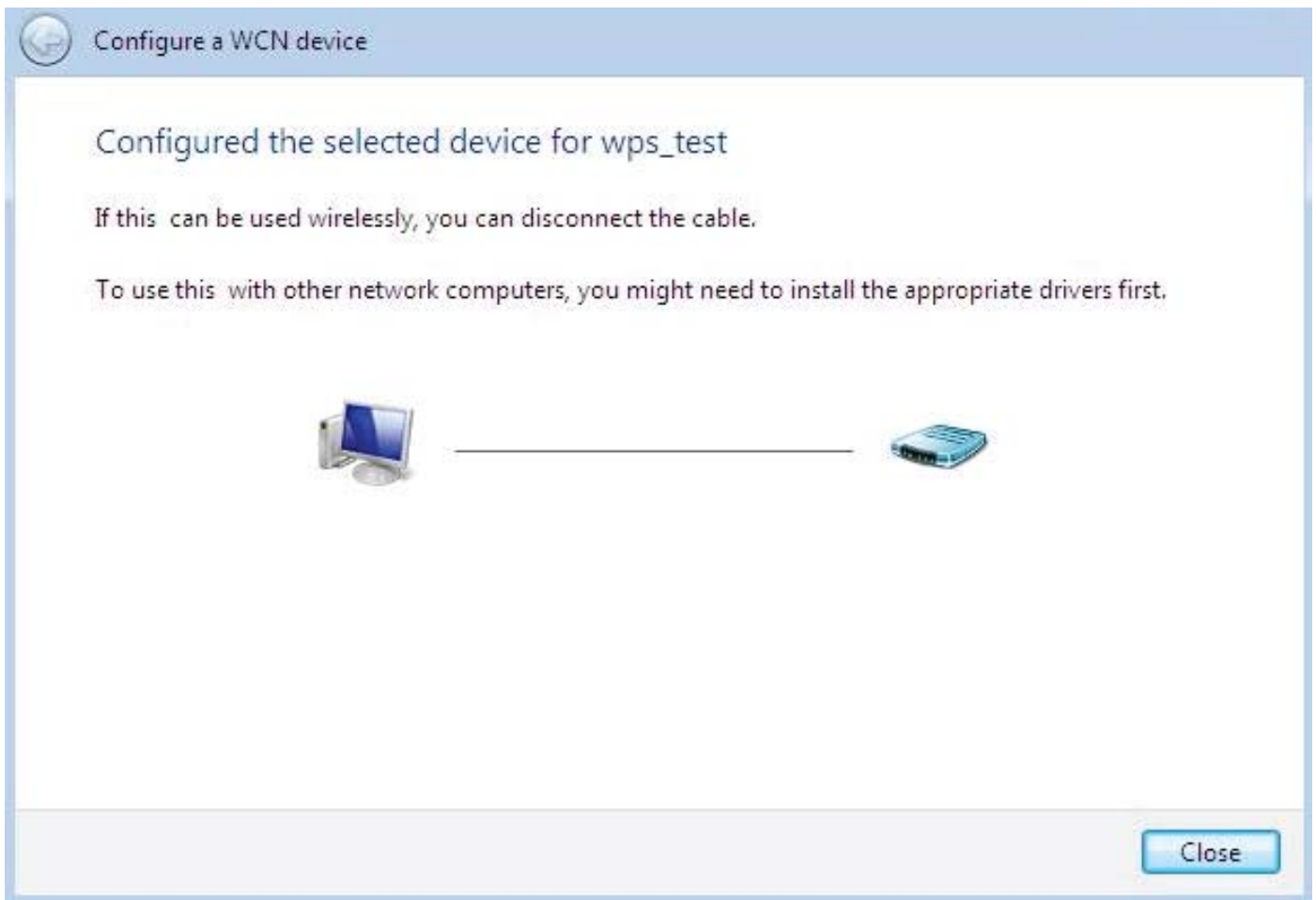
4. Enter the AP SSID then click Next.



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.



DHCP Server

Configuration

▼ DHCP Server

Parameters

DHCP Server Mode	<input type="text" value="DHCP Server"/>
Domain Name	<input type="text" value="home.gateway"/>
Range Start	<input type="text" value="192.168.1.100"/>
Range End	<input type="text" value="192.168.1.199"/>
Default Lease Time	<input type="text" value="24"/> hours
Maximum Lease Time	<input type="text" value="24"/> hours
Use Router as DNS Server	<input checked="" type="checkbox"/>
Primary DNS Server Address	<input type="text"/>
Secondary DNS Server Address	<input type="text"/>

[Fixed Host ▶](#)

Current Mode : DHCP Server

DHCP allows networked devices to obtain information on the parameter of IP, Netmask, Gateway as well as DNS through the Ethernet Address of the device. If you check the DHCP Relay you must enter the IP address of the DHCP server that assigns an IP address 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.

WAN

A WAN (Wide Area Network) is a computer network that covers a broad geographical area (eg. Internet) that is used to connect LAN and other types of network systems. There are two items within the WAN section: **WAN Profile** and **ADSL Mode**.

WAN Profile (ADSL)

PPPoE Connection (ADSL)

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

Configuration

WAN Profile

Parameters

Main Port: ADSL (Current Main Port: ADSL)

Protocol: PPPoE (RFC2516, PPP over Ethernet)

Description: pppoe_0_8_35_1 | VPI / VCI: 8 / 35 | Encap. method: LLC/SNAP-BRIDGING

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:

When you finish configuring all WAN settings, please click the 'Restart' button for these changes to take effect.

Add | Apply / Edit / Delete

Edit	Protocol	Interface	Description	VPI	VCI	Encap. method	NAT	IP	Delete
<input checked="" type="radio"/>	PPPoE	ppp_0_8_35_1	pppoe_0_8_35_1	8	35	LLC/SNAP-BRIDGING	Enable	0.0.0.0	

Description: A given name for the connection.

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

Encap. method: Select the encapsulation format. Select the one provided by your ISP.

Username: Enter the username provided by your ISP. You can input up to 256 alphanumeric characters (case sensitive).

Password: Enter the password provided by your ISP. You can input up to 32 alphanumeric characters (case sensitive).

Service Name: This item is for identification purposes. If it is required, your ISP will provide you the necessary information. Maximum input is 32 alphanumeric characters.

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

IP (0.0.0.0:Auto): Your WAN IP address. Leave the IP address as 0.0.0.0 to enable the device to automatically obtain an IP address from your ISP.

Auth. Protocol: Default is Auto. Please consult your ISP on whether to use Chap, Pap or MSCHAP.

Obtain DNS: A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address of a specific domain name. Check the checkbox to obtain DNS automatically.

Primary DNS: Enter the primary DNS.

Secondary DNS: Enter the secondary DNS.

Connection: Click on **Always on** to establish a PPPoE session during start up and to automatically re-establish the PPPoE session when disconnected by the ISP. You may uncheck the item to disable this function.

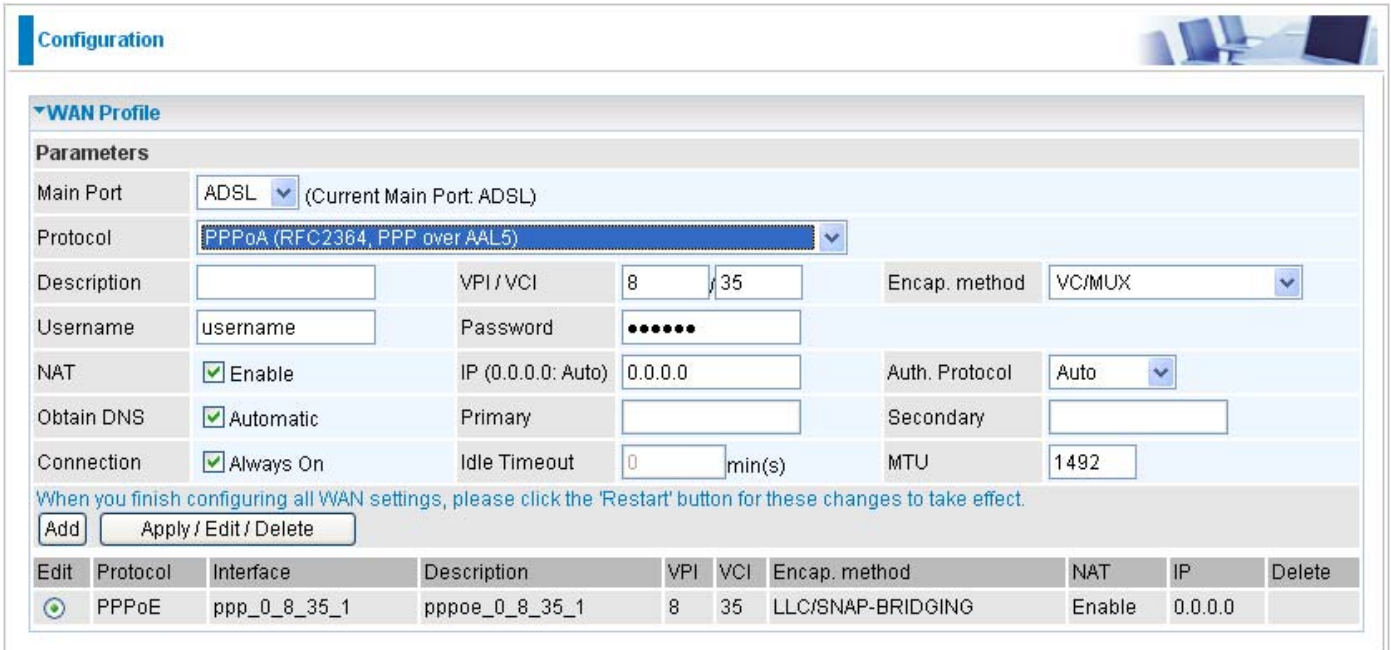
Idle Timeout: Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time.

MTU: Control the maximum Ethernet packet size your PC will send.

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 functions in a manner similar to dial-up services using PPP.



Configuration

WAN Profile

Parameters

Main Port: ADSL (Current Main Port: ADSL)

Protocol: PPPoA (RFC2364, PPP over AAL5)

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

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

When you finish configuring all WAN settings, please click the 'Restart' button for these changes to take effect.

Add [] Apply / Edit / Delete []

Edit	Protocol	Interface	Description	VPI	VCI	Encap. method	NAT	IP	Delete
<input checked="" type="radio"/>	PPPoE	ppp_0_8_35_1	pppoe_0_8_35_1	8	35	LLC/SNAP-BRIDGING	Enable	0.0.0.0	[]

Description: A given name for the connection.

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

Encap. method: Select the encapsulation format. Select the one provided by your ISP.

Username: Enter the username provided by your ISP. You can input up to 256 alphanumeric characters (case sensitive).

Password: Enter the password provided by your ISP. You can input up to 32 alphanumeric characters (case sensitive).

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

IP (0.0.0.0:Auto): Your WAN IP address. Leave the IP address as 0.0.0.0 to enable the device to automatically obtain an IP address from your ISP.

Auth. Protocol: Default is Auto. Please consult your ISP on whether to use Chap, Pap or MSCHAP.

Obtain DNS: A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address of a specific domain name. Check the checkbox to obtain DNS automatically.

Primary DNS: Enter the primary DNS.

Secondary DNS: Enter the secondary DNS.

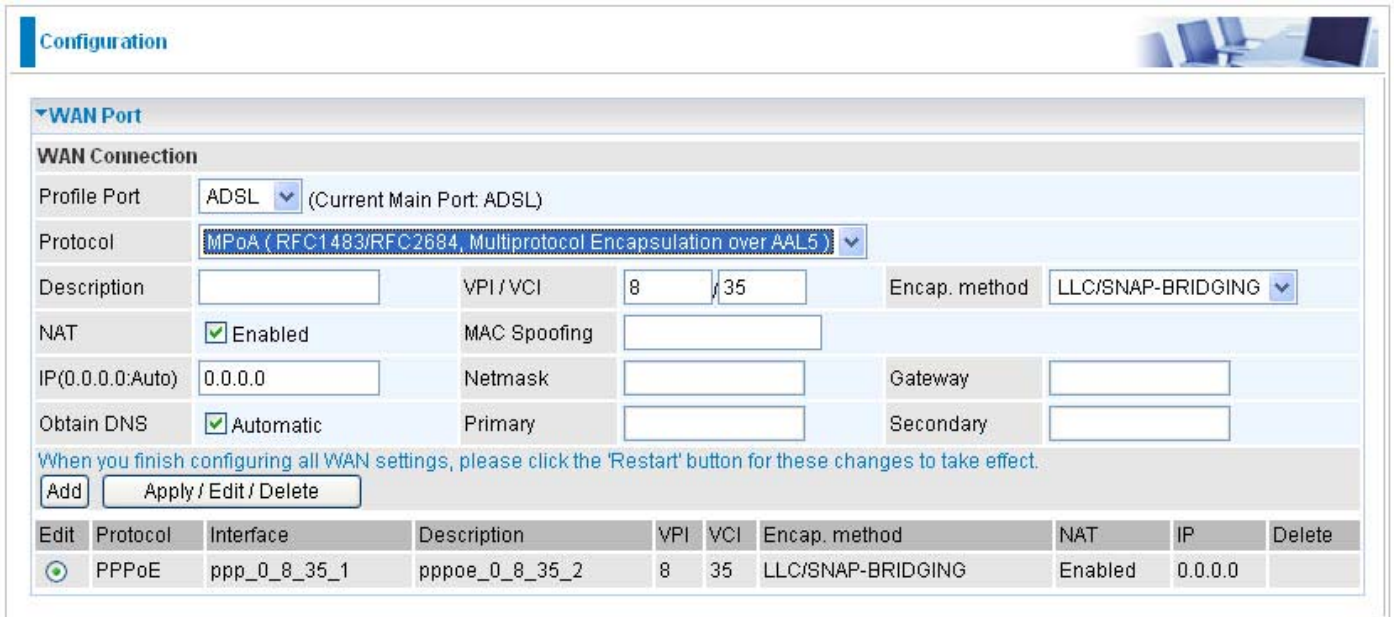
Connection: Click on **Always on** to establish a PPPoE session during start up and to automatically re-establish the PPPoE session when disconnected by the ISP. You may uncheck the item to disable this function.

Idle Timeout: Auto-disconnect the broadband firewall gateway

when there is no activity on the line for a predetermined period of time.

MTU: Control the maximum Ethernet packet size your PC will send.

MPoA Connection (ADSL)



The screenshot shows a configuration page for a WAN Port. The 'WAN Connection' section is active, showing settings for a profile named 'ADSL'. The protocol is set to 'MPoA (RFC1483/RFC2684, Multiprotocol Encapsulation over AAL5)'. The VPI/VCI is set to 8/35, and the encapsulation method is LLC/SNAP-BRIDGING. NAT is enabled, and the IP address is 0.0.0.0. The interface name is ppp_0_8_35_1, and the description is pppoe_0_8_35_2. A table at the bottom lists the active connection.

Edit	Protocol	Interface	Description	VPI	VCI	Encap. method	NAT	IP	Delete
<input checked="" type="checkbox"/>	PPPoE	ppp_0_8_35_1	pppoe_0_8_35_2	8	35	LLC/SNAP-BRIDGING	Enabled	0.0.0.0	

Description: A given name for the connection.

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

Encap. method: Select the encapsulation format. Select the one provided by your ISP.

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

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.

IP Address: Your WAN IP address. If the IP is set to 0.0.0.0 (auto IP detect), both netmask and gateway can be left blank.

Netmask: 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 activate 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.

IPoA Connections (ADSL)

Configuration

WAN Port

WAN Connection

Profile Port: ADSL (Current Main Port: ADSL)

Protocol: IPoA (RFC1577, Classic IP and ARP over ATM)

Description: VPI/VCI: 8 / 35 Encap. method: LLC/SNAP-ROUTING

NAT: Enabled

IP(0.0.0.0:Auto): 0.0.0.0 Netmask: Gateway:

Obtain DNS: Automatic Primary: Secondary:

When you finish configuring all WAN settings, please click the 'Restart' button for these changes to take effect.

Edit	Protocol	Interface	Description	VPI	VCI	Encap. method	NAT	IP	Delete
<input checked="" type="radio"/>	PPPoE	ppp_0_8_35_1	pppoe_0_8_35_2	8	35	LLC/SNAP-BRIDGING	Enabled	0.0.0.0	

Description: A given name for the connection.

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

Encap. method: Select the encapsulation format. Select the one provided by your ISP.

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

IP Address: Enter your fixed IP address.


Netmask: 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 activate 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.

Pure Bridge Connections (ADSL)

Configuration 

▼ WAN Port

WAN Connection

Profile Port: ADSL (Current Main Port: ADSL)

Protocol: Pure Bridge

Description: VPI/VCI: 8 / 35 Encap. method: LLC/SNAP-BRIDGING

When you finish configuring all WAN settings, please click the 'Restart' button for these changes to take effect.

Edit	Protocol	Interface	Description	VPI	VCI	Encap. method	NAT	IP	Delete
<input checked="" type="radio"/>	PPPoE	ppp_0_8_35_1	pppoe_0_8_35_2	8	35	LLC/SNAP-BRIDGING	Enabled	0.0.0.0	

Description: A given name for the connection.

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

Encap. method: Select the encapsulation format. Select the one provided by your ISP.

WAN Profile – Main Port (EWAN)

Besides using ADSL to connect to the Internet, BiPAC 7800(N) EWAN port is also an alternative to connect to Cable Modems, VDSL and fiber optic lines. This alternative provides users with faster connection & flexibility to connect to the Internet.

PPPoE (EWAN)

The screenshot shows a web-based configuration interface for a WAN profile. The title is 'Configuration' and the section is 'WAN Profile'. Under 'Parameters', the following settings are visible:

Main Port	EWAN	(Current Main Port: ADSL)			
Protocol	PPPoE				
Username	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		Secondary	
Connection	<input checked="" type="checkbox"/> Always On	Idle Timeout	0 min(s)	MTU	1492
MAC Spoofing					

When you finish configuring all WAN settings, please click the 'Restart' button for these changes to take effect.

Apply

Username: Enter the username provided by your ISP. You can input up to 256 alphanumeric characters (case sensitive).

Password: Enter the password provided by your ISP. You can input up to 32 alphanumeric characters (case sensitive).

Service Name: This item is for identification purposes. If it is required, your ISP will provide you the necessary information. Maximum input is 32 alphanumeric characters.

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

IP (0.0.0.0.Auto): Enter your fixed IP address.

Auth. Protocol: Default is Auto. Please consult your ISP on whether to use Chap, Pap or MSCHAP.

Obtain DNS Automatically: Select this check box to activate 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.

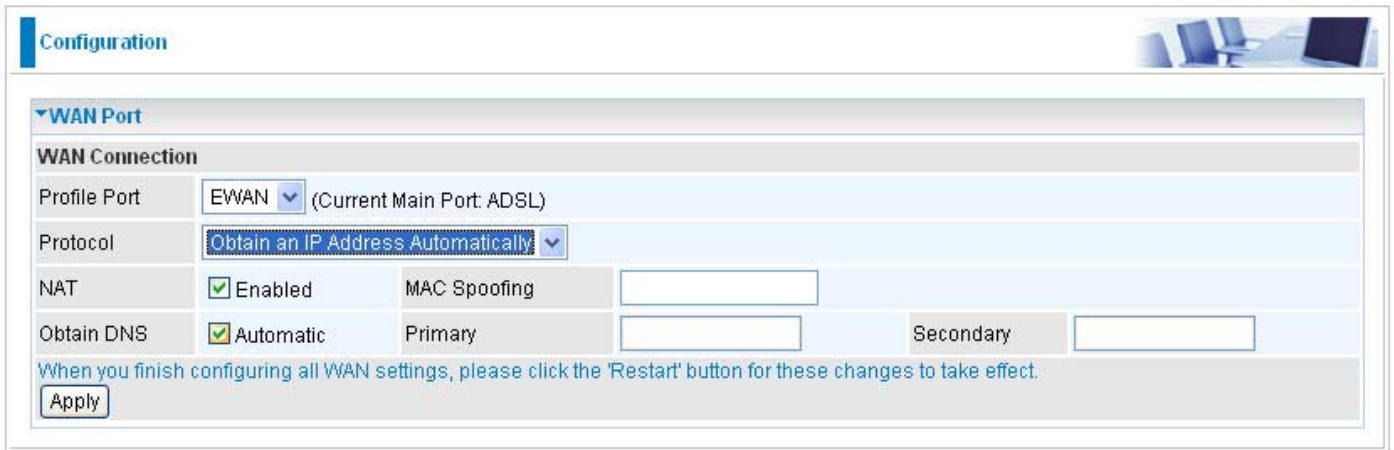
Connection: Click on **Always on** to establish a PPPoE session during start up and to automatically re-establish the PPPoE session when disconnected by the ISP. You may uncheck the item to disable this function.

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

MTU: Control the maximum Ethernet packet size your PC will send.

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.

Obtain an IP Address Automatically



The screenshot shows a 'Configuration' window with a 'WAN Port' section. Under 'WAN Connection', the 'Profile Port' is set to 'EWAN' (Current Main Port: ADSL). The 'Protocol' is set to 'Obtain an IP Address Automatically'. The 'NAT' checkbox is checked and labeled 'Enabled'. The 'MAC Spoofing' checkbox is unchecked. The 'Obtain DNS' checkbox is checked and labeled 'Automatic'. There are input fields for 'Primary' and 'Secondary' DNS servers. A note at the bottom states: 'When you finish configuring all WAN settings, please click the 'Restart' button for these changes to take effect.' An 'Apply' button is located at the bottom left.

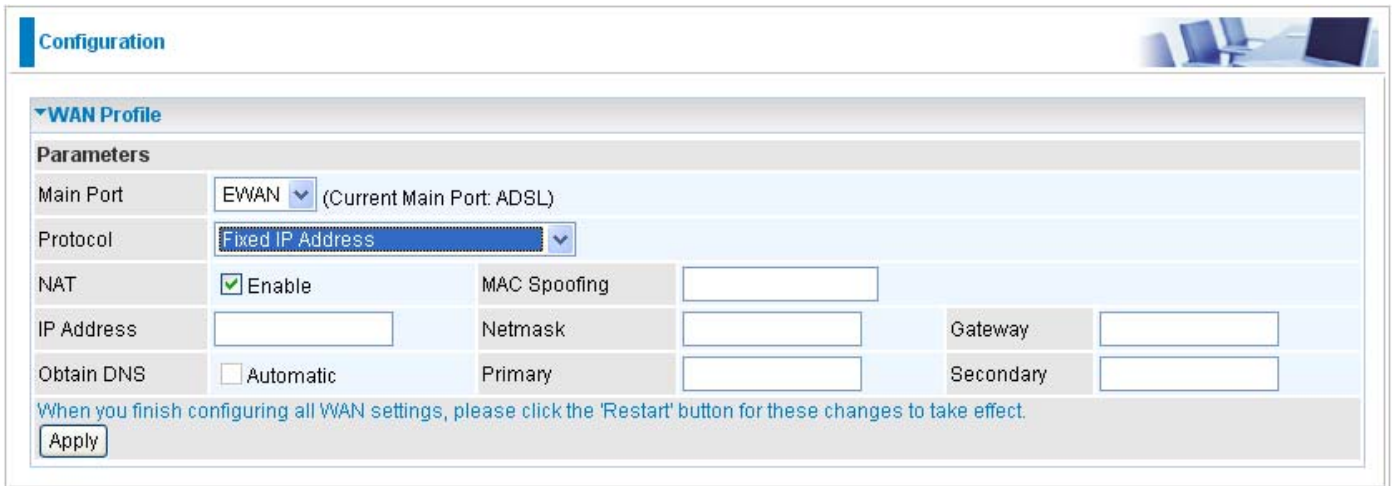
NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account by sharing the single IP address. If users on your LAN have their own public IP addresses to access the Internet, NAT function can be disabled.

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.

Obtain DNS: Select this check box to activate 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.

Fixed IP Address



The screenshot shows a 'Configuration' window with a 'WAN Profile' section. Under 'Parameters', the 'Main Port' is set to 'EWAN' (Current Main Port: ADSL). The 'Protocol' is set to 'Fixed IP Address'. The 'NAT' checkbox is checked and labeled 'Enable'. The 'MAC Spoofing' field is empty. The 'IP Address', 'Netmask', and 'Gateway' fields are empty. The 'Obtain DNS' checkbox is unchecked and labeled 'Automatic'. The 'Primary' and 'Secondary' DNS fields are empty. A note at the bottom states: 'When you finish configuring all WAN settings, please click the 'Restart' button for these changes to take effect.' An 'Apply' button is located at the bottom left.

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

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.

IP Address: Enter your fixed IP address.

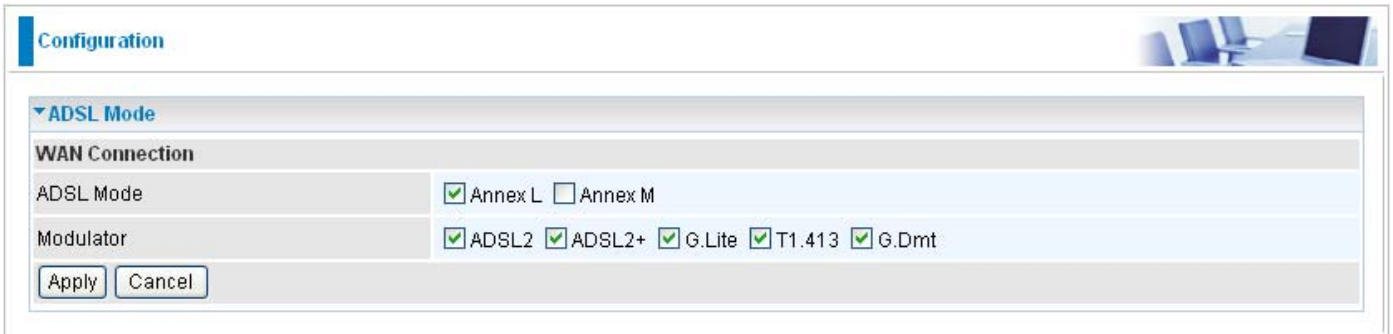
Netmask: User can change it to others such as 255.255.255.128. Type the netmask assigned to you by your ISP (if given)

Gateway: Enter the IP address of the default gateway.

Obtain DNS: Select this check box to activate 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.

ADSL Mode



The screenshot shows a web-based configuration page for ADSL Mode. At the top left, there is a 'Configuration' tab. Below it, the 'ADSL Mode' section is expanded. Under the 'WAN Connection' heading, there are two rows of configuration options. The first row is 'ADSL Mode' with two radio buttons: 'Annex L' (checked) and 'Annex M' (unchecked). The second row is 'Modulator' with five checkboxes: 'ADSL2' (checked), 'ADSL2+' (checked), 'G.Lite' (checked), 'T1.413' (checked), and 'G.Dmt' (checked). At the bottom of the configuration area, there are two buttons: 'Apply' and 'Cancel'.

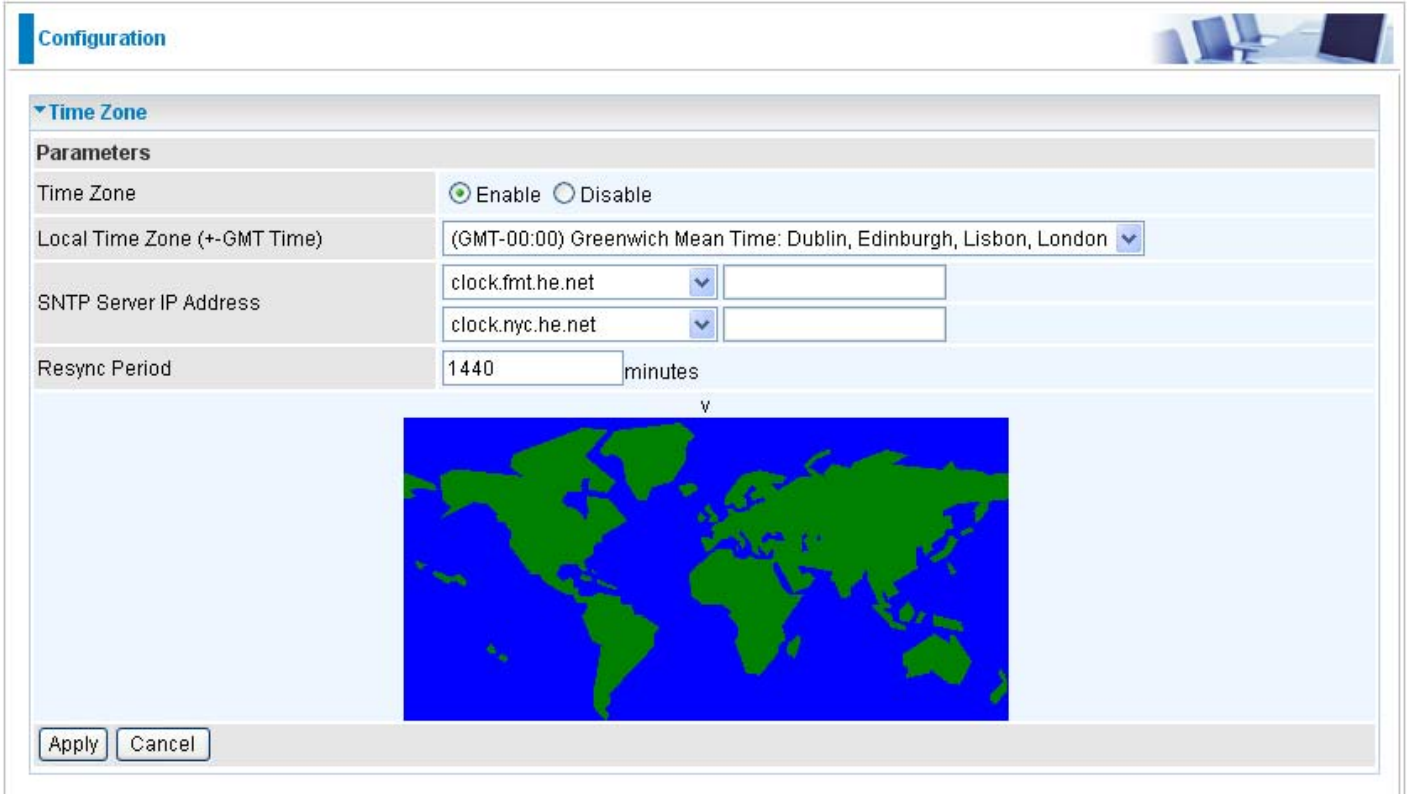
ADSL Mode: There are 2 modes “Annex L” and “Annex M” that user can select for this connection.

Modulator: There are 5 modes “ADSL2”, “ADSL2+”, “G.Lite:”, “T1.413” and “G.DMT” that user can select for this connection.

System

There are five items within the System section: [Time Zone](#), [Firmware Upgrade](#), [Backup/Restore](#), [Restart](#) and [User Management](#).

Time Zone



The screenshot shows a web configuration page titled "Configuration" with a sub-section for "Time Zone". The "Parameters" section includes:

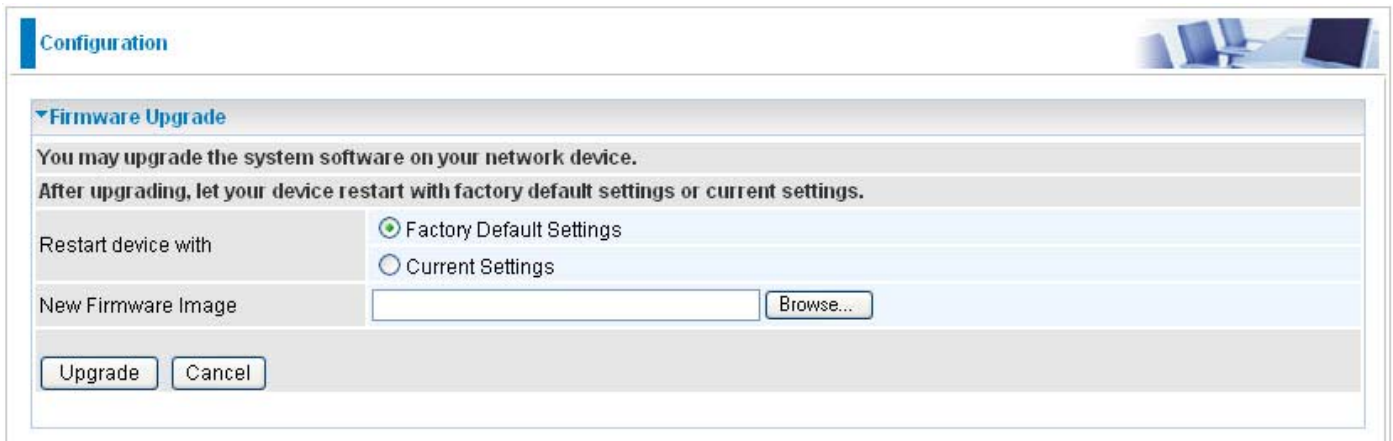
- Time Zone:** Radio buttons for "Enable" (selected) and "Disable".
- Local Time Zone (+-GMT Time):** A dropdown menu showing "(GMT-00:00) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London".
- SNTP Server IP Address:** Two rows, each with a dropdown menu (showing "clock.fmt.he.net" and "clock.nyc.he.net" respectively) and an adjacent empty text input field.
- Resync Period:** A text input field containing "1440" followed by the label "minutes".

Below the form is a world map with a small "v" cursor over it. At the bottom left are "Apply" and "Cancel" buttons.

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

Resync Period (in minutes) is the periodic interval the router will wait before it re-synchronizes the router's time with that of the specified SNTP server. In order 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. The default value is set at 1440 minutes.

Firmware Upgrade



The screenshot shows a web configuration page titled "Configuration" with a sub-section for "Firmware Upgrade". The page contains the following elements:

- A header bar with "Configuration" on the left and a small image of a network device on the right.
- A section header "Firmware Upgrade" with a downward arrow.
- Two lines of instructional text: "You may upgrade the system software on your network device." and "After upgrading, let your device restart with factory default settings or current settings."
- A "Restart device with" section containing two radio button options: "Factory Default Settings" (which is selected) and "Current Settings".
- A "New Firmware Image" section with a text input field and a "Browse..." button.
- At the bottom, two buttons: "Upgrade" and "Cancel".

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 that runs in your router. Thus, by upgrading the newly improved version of the firmware allows you the advantage to use newly integrated features.

Factory Default Settings: If select this setting, the device will reboot to restore the parameters of all its applications to its default values.

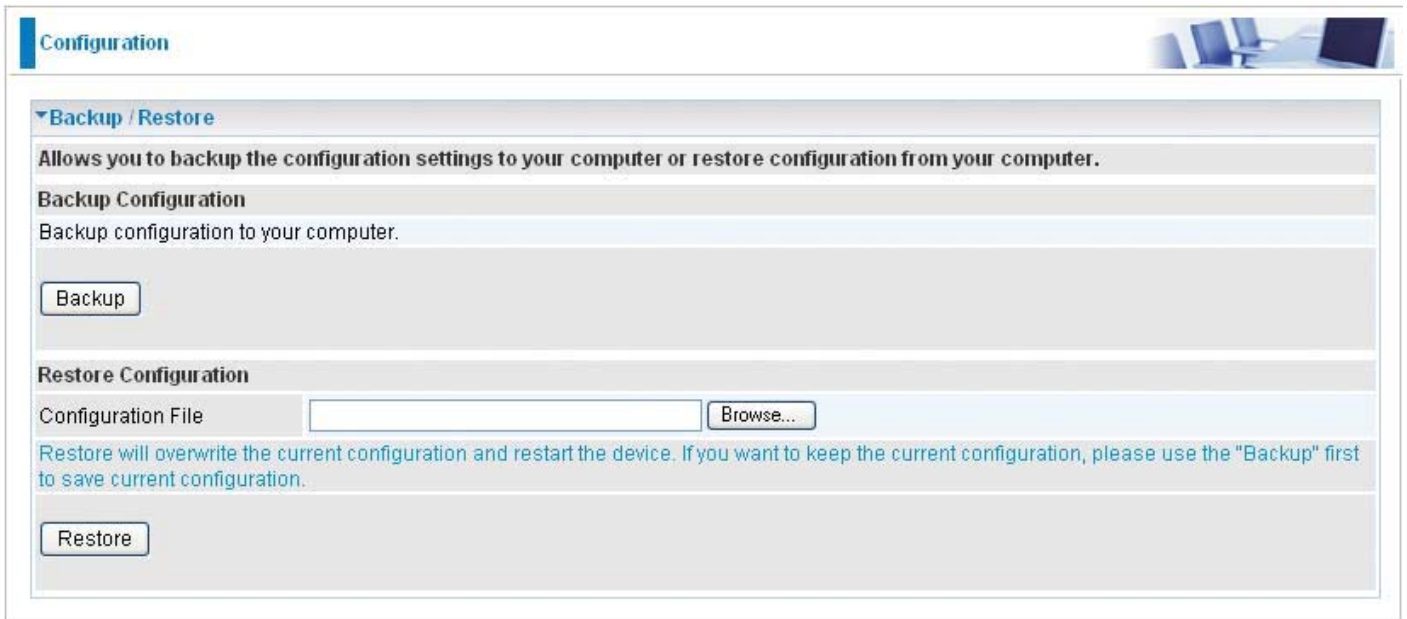
Current Settings: If select this setting, the device will reboot and retain the customized settings of all applications.

Click on Browse 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 to your router.



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

Backup / Restore



The screenshot shows a web interface for router configuration. At the top left, there is a 'Configuration' menu. The main content area is titled 'Backup / Restore' and contains the following elements:

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

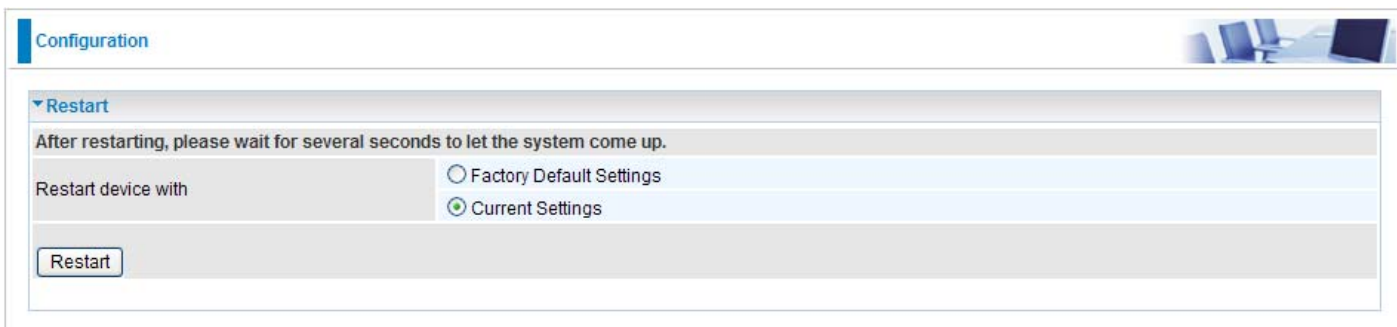
These functions allow you to save a backup of the current configuration of your router to a defined location on your PC, or to restore a previously saved configuration. This is useful if you wish to experiment with different settings, knowing that you have a backup in hand in case any mistakes occur.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

Press Backup Settings to select where on your local PC you want to store your setting file. You may also want to 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 your router setting that has been generated by the Backup function which is created with the current version of the router 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 Update Settings to load the setting into the router.

Restart



Configuration

▼ Restart

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

Restart device with

Factory Default Settings

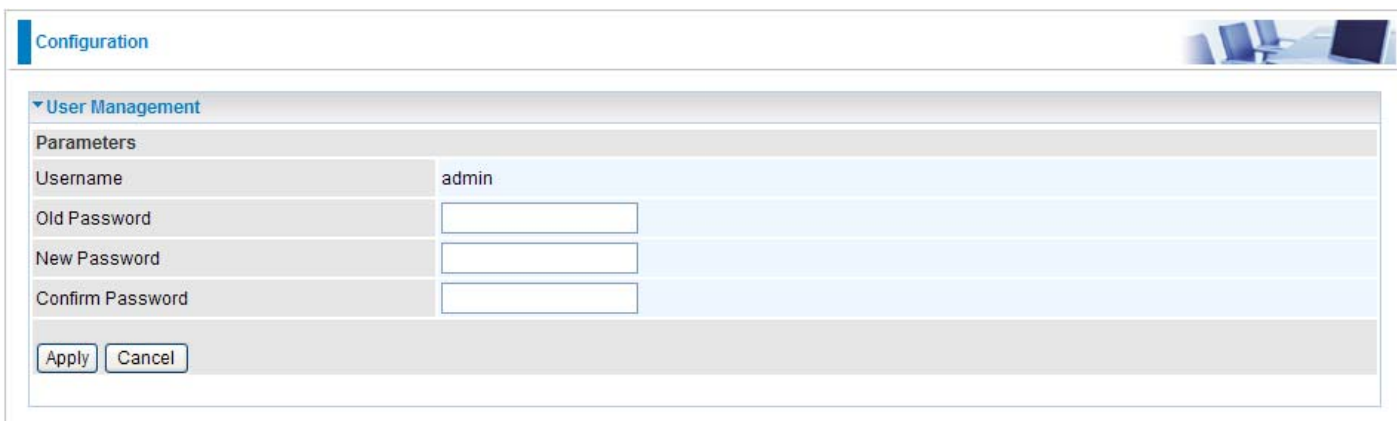
Current Settings

Restart

There are 2 options for you to choose from before restarting the your 7800(N) device. You can either choose to restart your device to restore it to the Factory Default Settings or to restart the device with your current settings applied. Restarting your device to Factory Default Setting will be useful especially after you have accidentally changed your settings that may result in undesirable outcome.

After selecting the type of setting you want the device to restart with, click the Restart button to initiate the process. After restarting, please wait several minutes to let the selected setting applied to the system.

User Management



Configuration

▼ User Management

Parameters

Username admin

Old Password

New Password

Confirm Password

Apply Cancel

In order to prevent unauthorized access to your router configuration interface, it requires all users to login with a username and password. Therefore only system administrator can access the system. It is highly recommended that you change your password upon receiving your router. The default password is “admin”.

To change your password, simply enter the old password in the Old Password blank. Then enter your new password in the New Password and Confirm Password blanks provided. When this is done, press Apply to save changes.

Firewall

Packet Filter

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

Configuration

Packet Filter

Parameters

Rule Name: << --select-- (type or select from listbox)

Source IP address: ~ Source Port: ~

Destination IP address: ~ Destination Port: ~

Protocol: Direction: Action : Blocked

Edit	Rule Name	Source IP	Destination IP	Protocol	Source Port	Destination Port	Direction	Delete
	Default	Any	Any	Any	Any	Any	outgoing (forward)	

Rule Name: User defined description for entry identification. The maximum name length is 32 characters, and then can choose an application that they want from the listbox.

Source IP address: This is an Address-Filter used to allow or block traffic from particular IP address(es). Enter the IP range that you want to filter. If only the first IP block is filled, it means only that IP entered will be targeted. If you leave both IP blocks empty, it means any IP address.

Destination IP address: This is an Address-Filter used to allow or block traffic to particular IP address(es). Enter the IP range that you want to filter. If only the first IP block is filled, it means only that IP entered will be targeted. If you leave both IP blocks empty, it means any IP address.

Source Port: This is the Port Range that defines the ports allowed by the Remote/WAN to connect to the application. Default is set from range 0 ~ 65535. It is recommended that only advance user is to configure this feature.

Destination Port: This is the Port Range that defines the port of the application.

Protocol: Specify the packet type (TCP, UDP, TCP/UDP) 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.

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

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”.

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 the network to block specific machines from accessing your LAN.

To filter a specific MAC address, enter the MAC address in the blank provided then press Add.



The screenshot shows a web interface for configuring a MAC Filter. At the top, there is a 'Configuration' header. Below it, a section titled 'MAC Filter' is expanded. Underneath, there is a 'Parameters' section with a 'MAC Address' label and an empty text input field. At the bottom of this section, there are two buttons: 'Add' and 'Edit / Delete'.

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

Block WAN Ping

This feature is to be enabled when you want the public WAN IP address on your router not to respond to any ping command.

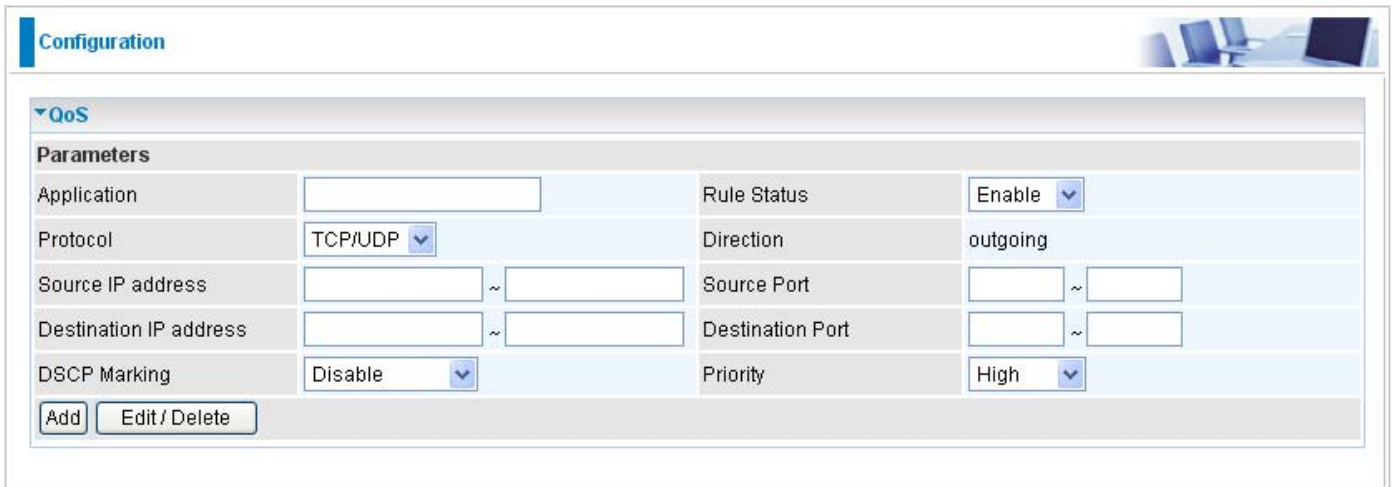
To activate the Block WAN PING feature, check the Enable box then click the Apply button. This feature is disabled by default.



The screenshot shows a web interface for configuring the Block WAN PING feature. At the top, there is a 'Configuration' header. Below it, a section titled 'Block WAN PING' is expanded. Underneath, there is a 'Parameters' section with a 'Block WAN PING' label and two radio buttons: 'Enable' and 'Disable'. The 'Disable' radio button is selected. At the bottom of this section, there are two buttons: 'Apply' and 'Cancel'.

QoS

QoS helps you to control the data upload traffic of each application from LAN (Ethernet and/ or Wireless) to WAN (Internet). It facilitates you the features to control the quality and speed of throughput for each application when the system is running with full upstream load.



The screenshot shows a web-based configuration interface for QoS. At the top left, there is a 'Configuration' tab. Below it, a section titled 'QoS' contains a table with the following columns: Application, Protocol, Source IP address, Destination IP address, DSCP Marking, Rule Status, Direction, Source Port, Destination Port, and Priority. The table is currently empty. Below the table, there are two buttons: 'Add' and 'Edit / Delete'.

Application: Assign a name that identifies the new QoS application rule.

Rule Status: You can choose to enable or disable rule status display from the drop down menu.

Protocol: Select the supported protocol from the drop down list.

Direction: Shows the direction mode of the QoS application.

Source IP Address: This is used to classify the traffic of a specific range of source IP address. Enter the IP range that you want to classify. If only the first IP block is filled, only that IP will be classified. If IP is left empty, it means classify any IP.

Destination IP Address: This is used to classify the traffic of a specific range of destination IP address. Enter the IP range that you want to classify. If only the first IP block is filled, only that IP will be classified. If IP is left empty, it means classify any IP.

Source Port: This is the Port Range that defines the ports allowed by the Remote/WAN to connect to the application. Default is set from range 0 ~ 65535. It is recommended that only advance user is to configure this feature.

Destination Port: This is the Port Range that defines the port of the application.

DSCP Marking: Differentiated Services Code Point (DSCP), it is the first 6 bits in the ToS byte. DSCP Marking allows users to classify the traffic of the application to be executed according to the DSCP value.

Note: *Make sure that the router(s) in the network backbone are capable to execute and check the DSCP throughout the QoS network.*

Priority: The priority given to each policy/application. Its default setting is set to High. You may adjust this setting to fit your policy / application.

Example 1: Optimize Your Home Network with QoS

If you are actively engaged in using P2P and are afraid of slowing down internet access throughput of other users within your network, you can thus use QoS function to set different priorities for the different applications that members of your network will be using to avoid bandwidth traffic from getting overloaded.

Therefore, in order to assign the priority status of each application, we must first create a new QoS rule for each application.

The figures below show the different settings for assigning a High Priority status to Web Browsing, Email send & receive.

For Web Browsing

QoS			
Parameters			
Application	HTTP	Rule Status	Enable
Protocol	TCP	Direction	outgoing
Source IP address	~	Source Port	~
Destination IP address	~	Destination Port	80 ~
DSCP Marking	Disable	Priority	High

For Mail Sending

QoS			
Parameters			
Application	SMTP	Rule Status	Enable
Protocol	TCP	Direction	outgoing
Source IP address	~	Source Port	~
Destination IP address	~	Destination Port	25 ~
DSCP Marking	Default	Priority	High

For Mail Receiving

QoS			
Parameters			
Application	POP3	Rule Status	Enable
Protocol	TCP	Direction	outgoing
Source IP address	~	Source Port	~
Destination IP address	~	Destination Port	110 ~
DSCP Marking	Disable	Priority	High

QoS Rules created

Edit	Application	Rule Status	Source IP address Destination IP address	Protocol	Source Port Destination Port	DSCP Marking	Priority	Delete
<input type="radio"/>	HTTP	Enable	Any Any	TCP	Any 80	default	High	<input type="checkbox"/>
<input type="radio"/>	SMTP	Enable	Any Any	TCP	Any 25	default	High	<input type="checkbox"/>
<input type="radio"/>	POP3	Enable	Any Any	TCP	Any 110	default	High	<input type="checkbox"/>

Example 2: Optimize Your Home Network with QoS

If you are running a lot of standard applications you can just create a QoS rule that has its port range set from 1 ~ 1024 and its priority set to High. This port range is defined in RFC and so it can be used by all standard applications like FTP, Telnet, HTTPS etc.

▼ QoS

Parameters

Application	standard	Rule Status	Enable
Protocol	TCP/UDP	Direction	outgoing
Source IP address	~	Source Port	~
Destination IP address	~	Destination Port	1 ~ 1024
DSCP Marking	Default	Priority	High

Edit	Application	Rule Status	Source IP address	Protocol	Source Port	DSCP Marking	Priority	Delete
			Destination IP address		Destination Port			
<input type="radio"/>	standard	Enable	Any	TCP/UDP	Any	default	High	<input type="checkbox"/>
			Any		1 ~ 1024			

Example 3: Optimize Your Home Network with QoS

If you are only using a specific PC for the P2P application, you can create a rule that has a low priority. In this way, P2P application will not congest the data transmission rate when there are other applications present.

▼ QoS

Parameters

Application	P2P	Rule Status	Enable
Protocol	TCP/UDP	Direction	outgoing
Source IP address	192.168.1.200 ~	Source Port	~
Destination IP address	~	Destination Port	~
DSCP Marking	Disable	Priority	Low

Edit	Application	Rule Status	Source IP address	Protocol	Source Port	DSCP Marking	Priority	Delete
			Destination IP address		Destination Port			
<input type="radio"/>	P2P	Enable	192.168.1.200	TCP/UDP	Any	disable	Low	<input type="checkbox"/>
			Any		Any			

Virtual Server

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side.

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.

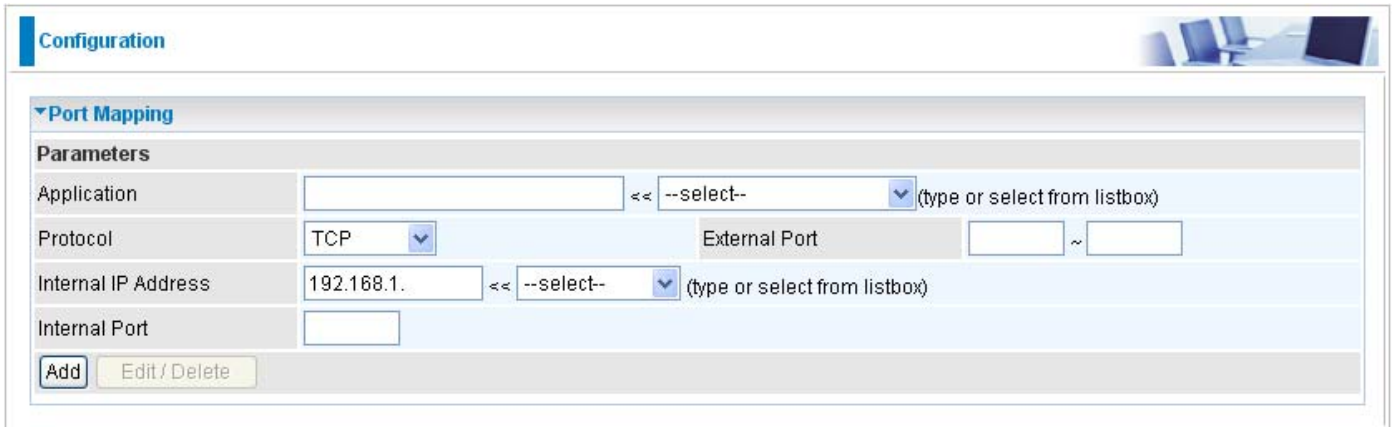
If you wish to run a server on your network that can be accessed from the WAN (i.e. from other machines on the Internet that are outside your local network), or any application that can accept incoming connections (e.g. Peer-to-peer/P2P software such as instant messaging applications and P2P file-sharing 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.

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	TEInet
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	Real Audio

Port Mapping



The screenshot shows a web-based configuration interface for port mapping. At the top left, there is a 'Configuration' tab. Below it, a section titled 'Port Mapping' contains a 'Parameters' table. The table has four rows: 'Application' with a dropdown menu (currently showing '--select--'), 'Protocol' with a dropdown menu (currently showing 'TCP'), 'Internal IP Address' with a text input field (containing '192.168.1.') and a dropdown menu (showing '--select--'), and 'Internal Port' with a text input field. To the right of the 'Internal IP Address' field is an 'External Port' field with a range indicator '~'. At the bottom of the form are two buttons: 'Add' and 'Edit/Delete'.

Application: Select the service you wish to configure.

Protocol: A protocol is automatically applied when an Application is selected from the listbox or you may 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 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.

Delete: To remove a port mapping application, check the Remove box of the selected application then click the Edit/Delete button.

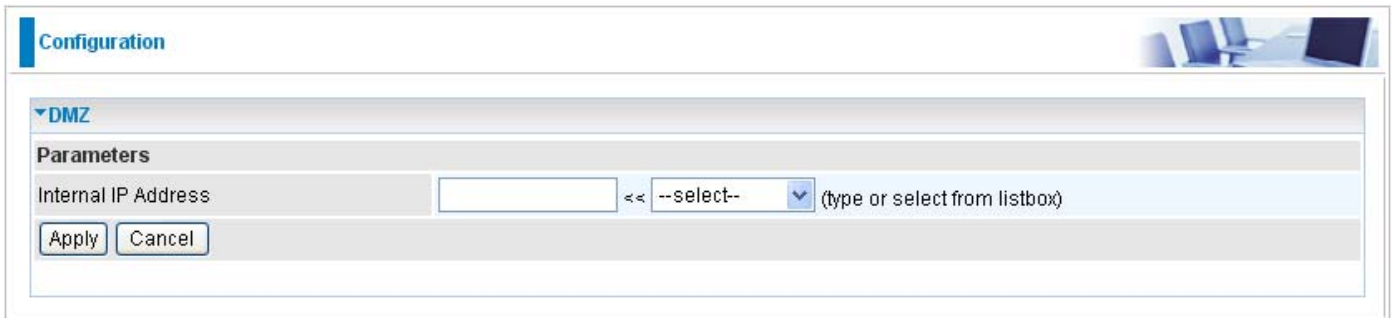
Since NAT acts as a “natural” Internet firewall, your router protects your network from accessed by outside users, as all incoming connection attempts point to your router unless you specifically create Virtual Server entries to forward those ports to a PC on your network. When your router needs to allow 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 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.

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

DMZ

The DMZ Host is a local computer exposed to the Internet. When setting a particular internal IP address as the DMZ Host, all incoming packets that do not use a port number which is already used by any other Virtual Server entries will first be checked by the Firewall and NAT algorithms before it is passed to the DMZ host.



Configuration

DMZ

Parameters

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

Apply Cancel



Attention

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

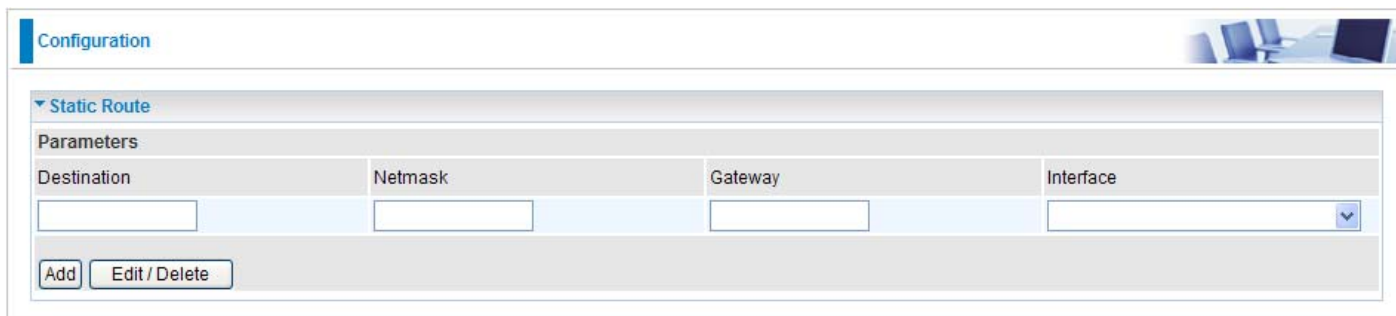


Since outside users are able to connect to the PCs on your network, port mapping utilization imposes security implications. You are therefore advised to use specific Virtual Server entries just for those ports that your applications require.

Advanced

Static Route

With static route feature, you are equipped with the capability to control the routing of the all the traffic across your network. With each routing rule created, you can specifically assign the destination where the traffic will be routed to.



The screenshot shows a web-based configuration interface for a network device. At the top, there is a 'Configuration' tab. Below it, a section titled 'Static Route' is expanded. Underneath, there is a 'Parameters' section with four input fields: 'Destination', 'Netmask', 'Gateway', and 'Interface'. The 'Interface' field is a dropdown menu. At the bottom of the parameters section, there are two buttons: 'Add' and 'Edit / Delete'.

Destination: Enter the destination IP where the traffic is to be forwarded.

Netmask: Enter the netmask of the destination.

Gateway: Enter the gateway address for the traffic.

Interface: Select an appropriate interface for the new routing rule from the drop down menu.

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 network device. At the top, there is a 'Configuration' tab. Below it, a section titled 'Static ARP' is expanded. Underneath, there is a 'Parameters' section with two input fields: 'IP Address' and 'MAC Address'. At the bottom of the parameters section, there are two buttons: 'Add' and 'Edit / Delete'.

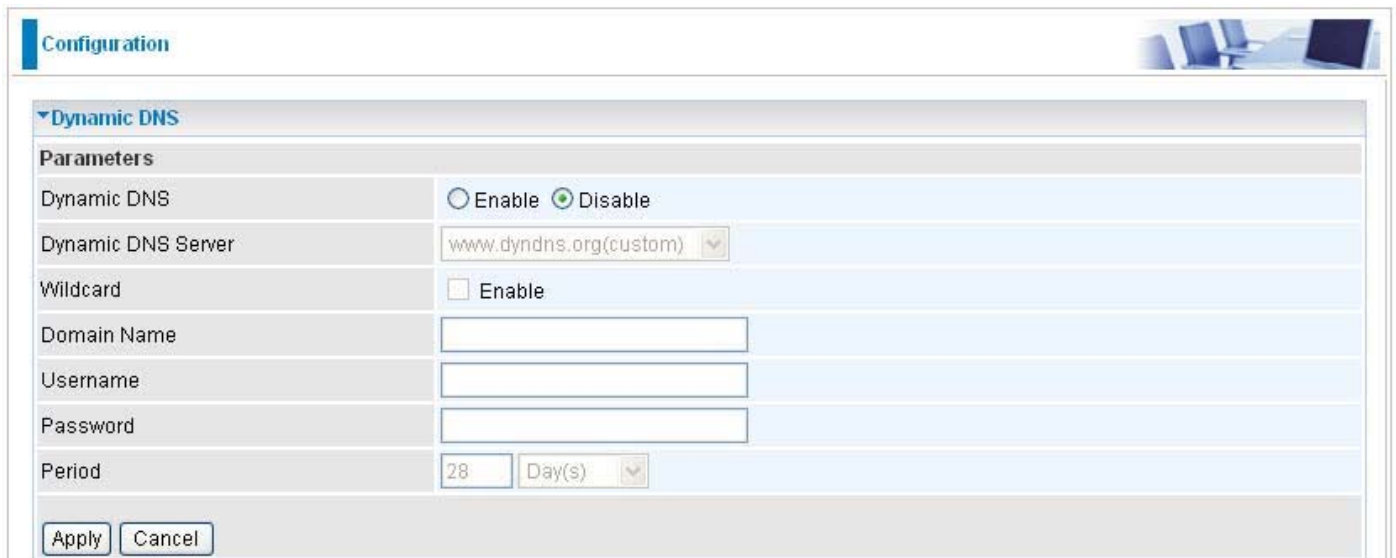
IP Address: Enter the IP of the device that the corresponding MAC address will be mapped to.

MAC Address: Enter the MAC address that corresponds to the IP address of the device.

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 when hosting servers via your ADSL connection, so that anyone wishing to connect to you may use your domain name, rather than the dynamic IP address which is assigned to you by ISP.

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



The screenshot shows a configuration window titled "Configuration" with a sub-section for "Dynamic DNS". Under "Parameters", there are several fields:

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

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

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


Wildcard: When enabled, you allow the system to lookup on domain names that do not exist to have MX records synthesized for them.

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

Period: Enter the length of the period in the blank, you can set the period unit in day (d), hour (H) or minute (M).

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	Ethernet Port					WLAN	Link VLAN Group to WAN connection Interface
	EWAN	#4	#3	#2	#1		
<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Example: IPTV Service Setting



Attention

This example is only to illustrate how to connect an Ethernet port to STB (Set Top Box) in a way to avoid IPTV traffic from affecting your home network. Nevertheless, the actual IPTV service setting still depends on the one offered by your local service provider.

Go to Advanced mode > Configuration > WAN > WAN Profile. Add a new WAN profile using the Pure Bridge protocol. Information should be provided by your local service provider.

Note: Description name should not contain any space.

WAN Profile

Parameters

Main Port: ADSL (Current Main Port: ADSL)

Protocol: Pure Bridge

Description: IPTV VPI / VCI: 0 / 35 Encap. method: LLC/SNAP-BRIDGING

When you finish configuring all WAN settings, please click the "Restart" button for these changes to take effect.

Edit	Protocol	Interface	Description	VPI	VCI	Encap. method	NAT	IP	Delete
<input checked="" type="radio"/>	PPPoE	ppp_0_8_35_1	pppoe_0_8_35_1	8	35	LLC/SNAP-BRIDGING	Enable	0.0.0.0	
<input type="radio"/>	Bridge	nas_0_0_35	IPTV	0	35	LLC/SNAP-BRIDGING	Disable		<input type="checkbox"/>

Then go to Advanced mode > Configuration > Advanced > VLAN. Then configure a port that will use the IPTV application. The example below is a setting that illustrates that only Ethernet port #4 can connect to STB and use IPTV.

Note: The VLAN setting illustrated bridges both WAN Profile and the Ethernet Port 4 so that the Ethernet port can connect to STB and get the IP directly from the IPTV Service Network. Thus, Ethernet port 4 can no longer be used for internet access and WEB management.

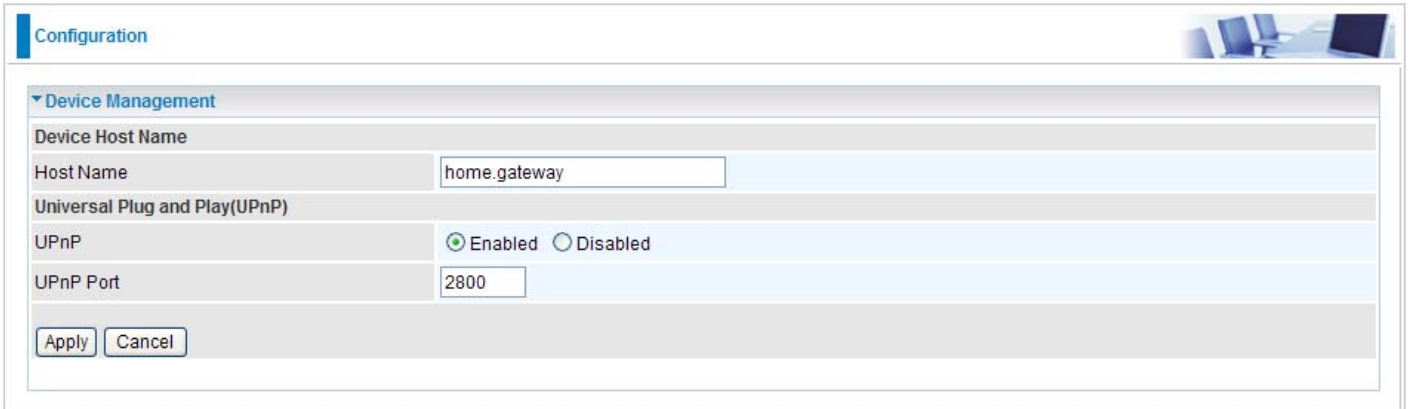
VLAN

Parameters

VLAN Group Name	Ethernet Port					WLAN	Link VLAN Group to WAN Connection interface
	EWAN	#4	#3	#2	#1		
IPTV	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> nas_0_0_35
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> nas_0_0_35
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> nas_0_0_35
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> nas_0_0_35
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> nas_0_0_35
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> nas_0_0_35
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> nas_0_0_35
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> nas_0_0_35

Device Management

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



The screenshot shows a web-based configuration interface for a router. At the top, there is a 'Configuration' tab. Below it, a 'Device Management' section is expanded. This section contains several settings:

- Device Host Name:** A sub-section containing a 'Host Name' field with the value 'home.gateway'.
- Universal Plug and Play (UPnP):** A sub-section containing a radio button for 'UPnP' which is currently selected as 'Enabled', and an option for 'Disabled'.
- UPnP Port:** A text input field containing the value '2800'.

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

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

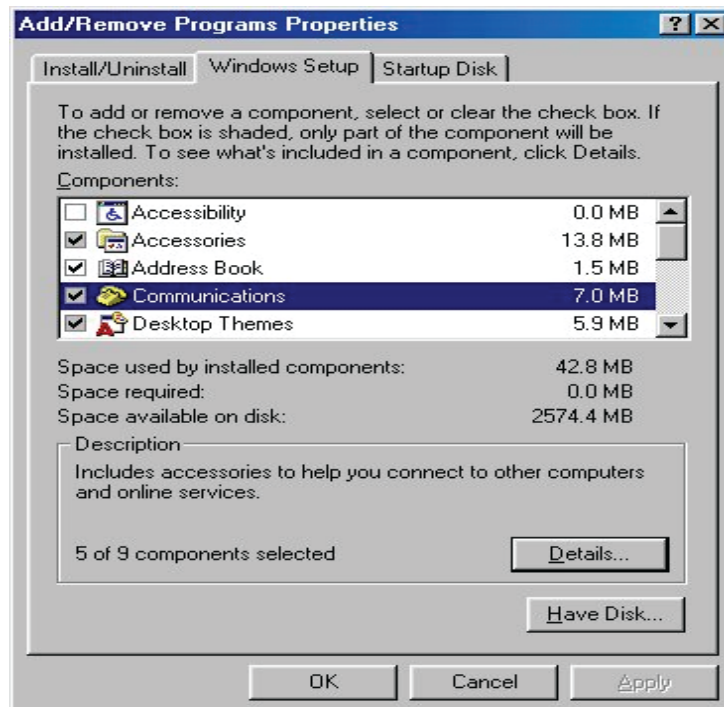
Both user's Operating System and its relevant applications must support UPnP in addition to the router. Windows XP and Windows Me have a native built-in support for UPnP (when the component is installed). Windows 98 users may have to install the Internet Connection Sharing client from Windows XP in order to support UpnP feature. Windows 2000 does not support UPnP.

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.

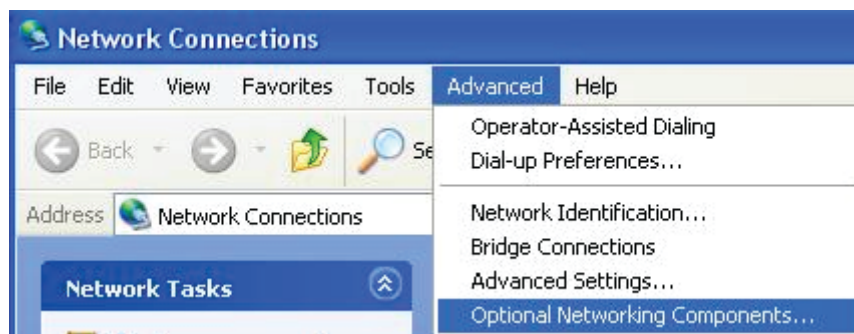
Step 5: Restart the computer when prompted.

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

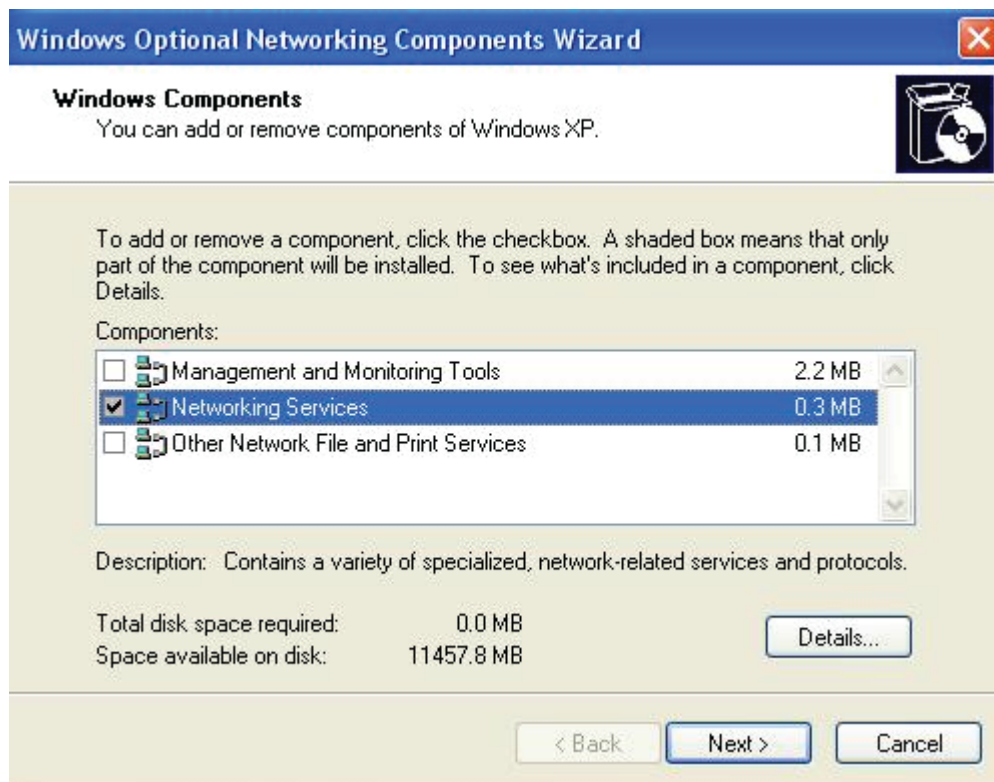
Step 1: Click Start and Control Panel.

Step 2: Double-click Network Connections.

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

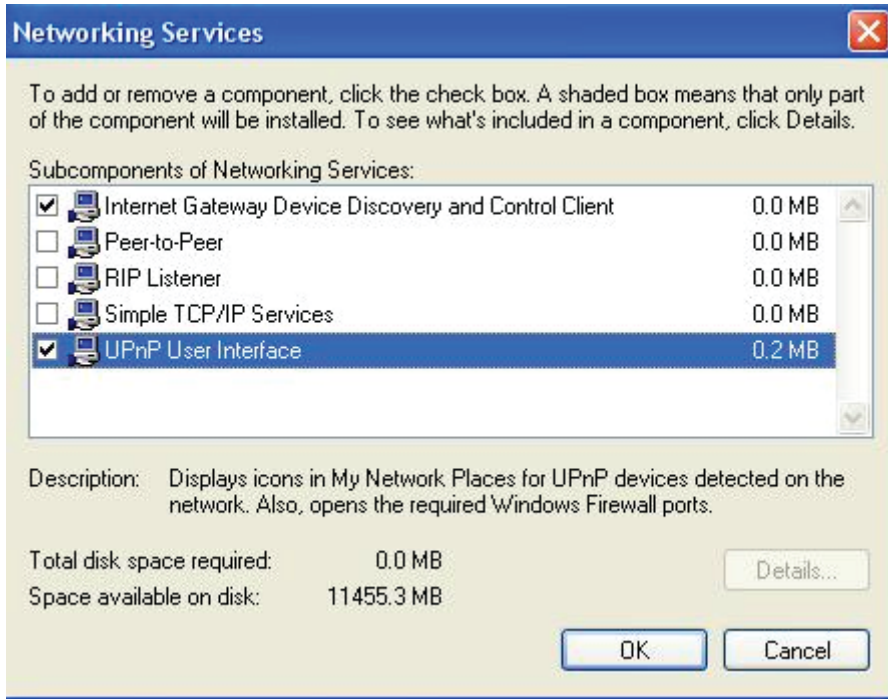


Step 4: When the Windows Optional Networking Components Wizard window appears, select Networking Service in the Components selection box and click Details.



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

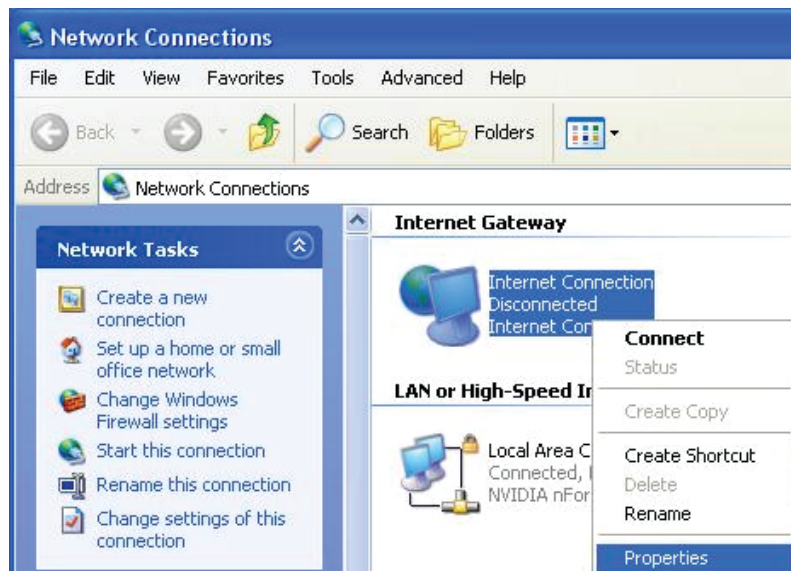
Step 6: Click OK to go back to the Windows Optional Networking Component Wizard window and click Next.



Auto-discover Your UPnP-enabled Network Device

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

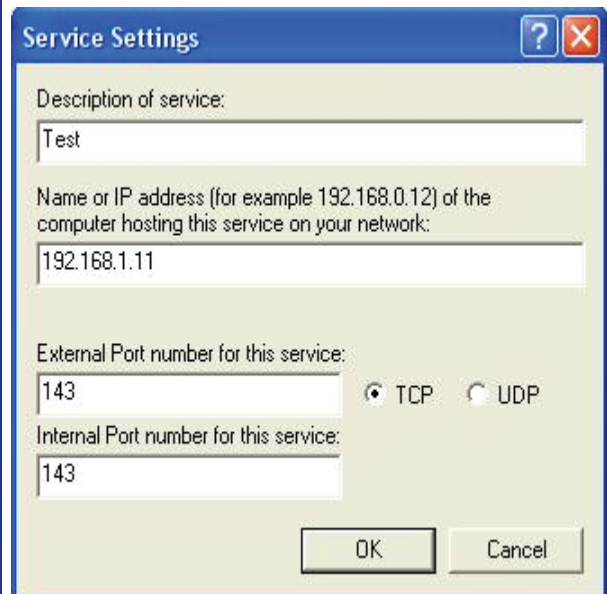
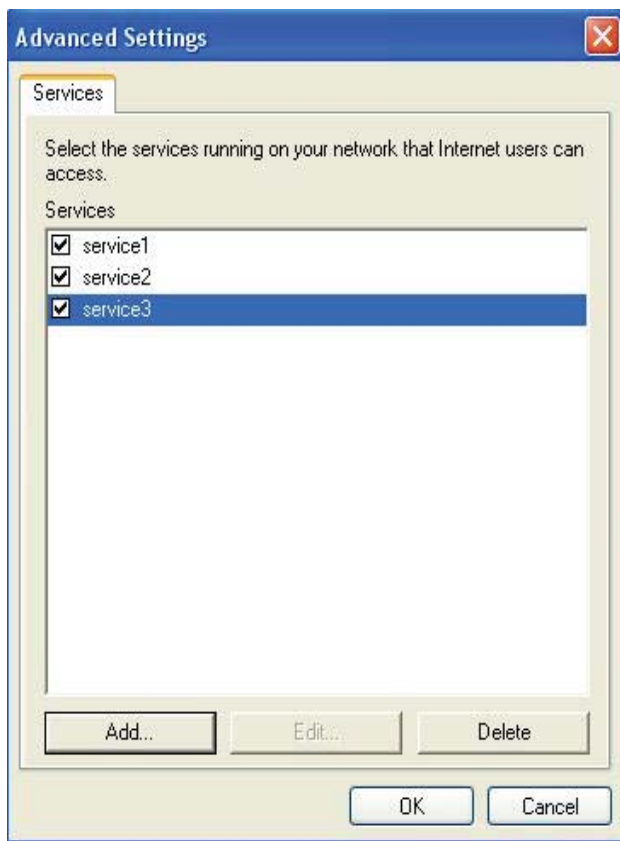
Step 2: Right-click the icon and select Properties.



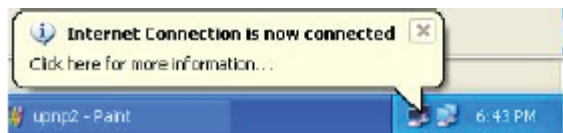
Step 3: In the Internet Connection Properties window, click Settings to see the port mappings that were automatically created.



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

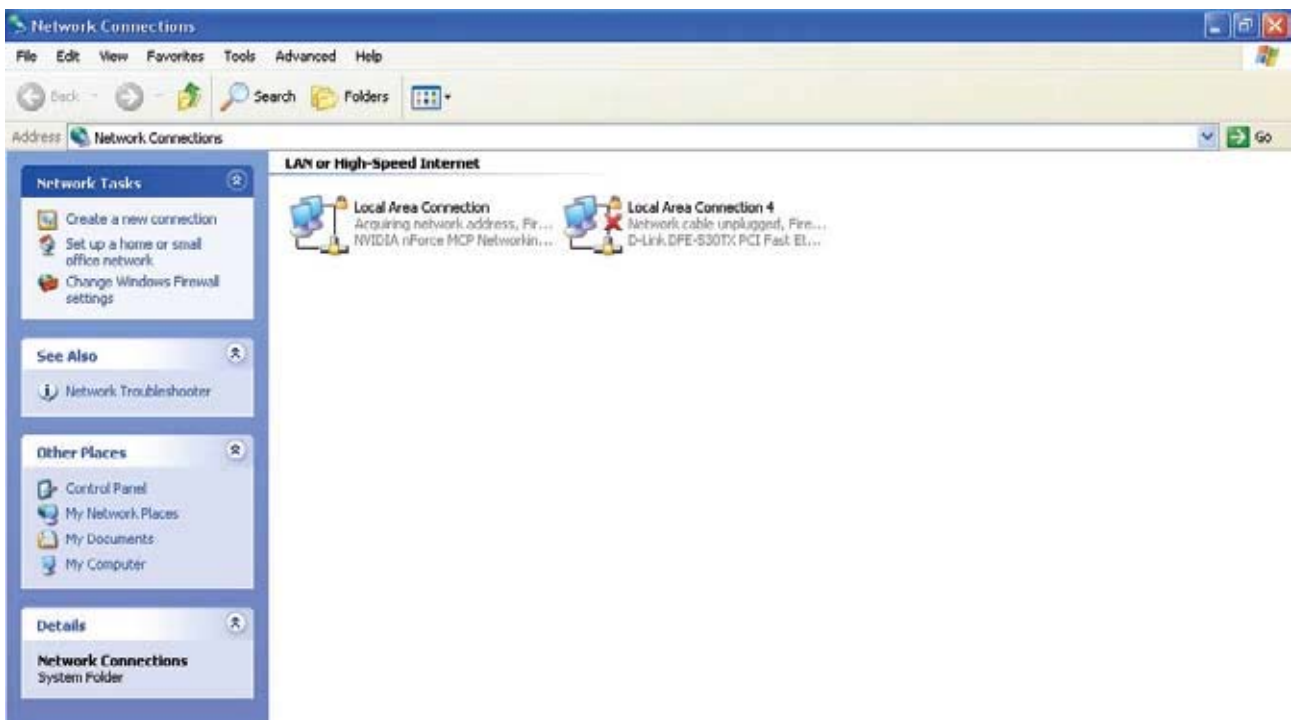
With UPnP, you can access web-based configuration for the BiPAC 7800(N) without first finding out the IP address of the router. This helps if you do not know the router's IP address.

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 7800(N) and select Invoke. The web configuration login screen displays.

Step 6: Right-click on the icon of your BiPAC 7800(N) and select Properties. A properties window displays basic information about the BiPAC 7800(N).

IGMP

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



IGMP Proxy: IGMP proxy enables the system to issue IGMP host messages on behalf of the hosts that the system has discovered through standard IGMP interfaces. The system acts as a proxy for its hosts.

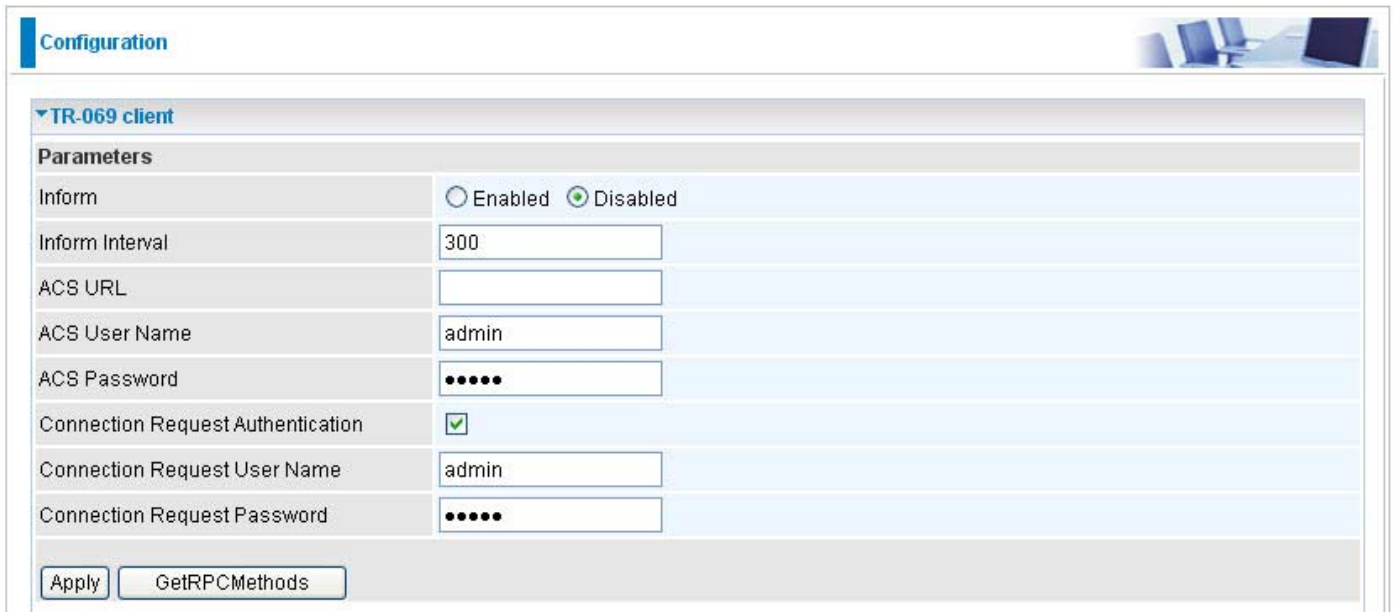
IGMP Snooping: Allows a layer 2 switch to manage the transmission of any incoming IGMP multicast packet groups between the host and the router. Default is set to Disable.

Example:

When IGMP snooping is enabled, the feature will analyze all incoming IGMP packets between the hosts that are connected to the switch and the multicast routers in the network. When the layer 2 switch receives an IGMP report from a host requesting for a given multicast group, the switch will add the host's port number to the multicast list for that multicast group to be forwarded to. And, when the layer 2 switch has detected that an IGMP has left, it will remove the host's port from the table entry.

TR-069 Client

Please contact your ISP for the information of TR069.



Parameters	
Inform	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Inform Interval	<input type="text" value="300"/>
ACS URL	<input type="text"/>
ACS User Name	<input type="text" value="admin"/>
ACS Password	<input type="password" value="••••"/>
Connection Request Authentication	<input checked="" type="checkbox"/>
Connection Request User Name	<input type="text" value="admin"/>
Connection Request Password	<input type="password" value="••••"/>

Inform: You may enable or disable the periodic inform feature.

Inform Interval: Enter the length of the periodic inform interval (unit: seconds).

ACS URL: Enter the ACS URL address.

ACS User Name: Enter the ACS server login name.

ACS Password: Enter the ACS server login password.

Connection Request Authentication: Check off to enable connection request authentication feature.

Connection Request User Name: Enter the username for ACS server to make connection request.

Connection Request Password: Enter the password for ACS server to make connection request.

GetRPCMethod: Detect the types of methods that ACS supports and is in communication with.

Remote Access

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



The screenshot shows a configuration window titled "Configuration" in the top left corner. Below the title bar, there is a section for "Remote Access" with a dropdown arrow. Underneath, a "Parameters" section contains a single entry: "Remote Access Control" with a checkbox labeled "Enable". The checkbox is currently unchecked. At the bottom of the configuration area, there are two buttons: "Apply" and "Cancel".

Appendix: Product Support & Contact

If you come across any problems please contact the dealer from where you purchased your product.

Contact Billion

Worldwide:

<http://www.billion.com>

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

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