



# **BiPAC 7800NEXL**

**3G / Wireless-N Dual WAN ADSL2+  
Firewall Router**

## **User Manual**

# Table of Contents

Chapter 1: Introduction .....	1
Introduction to your Router .....	1
Features .....	4
ADSL Compliance.....	4
Network Protocols and Features .....	4
Firewall.....	5
Quality of Service Control.....	5
ATM, PTM and PPP Protocols.....	5
IPTV Applications.....	6
Wireless LAN.....	6
Management.....	6
Hardware Specifications .....	7
Physical Interface.....	7
Chapter 2: Installing the Router .....	8
Package Contents .....	8
Important note for using this router.....	9
Device Description.....	10
The Front LEDs.....	10
The Rear Ports.....	11
Cabling .....	12
Chapter 3: Basic Installation .....	13
Connecting Your Router.....	14
Network Configuration .....	15
Configuring PC in windows 7.....	15
Configuring PC in Windows Vista.....	17
Configuring PC in Windows XP.....	19
Configuring PC in Windows 2000.....	20
Configuring PC in Windows 95/98/Me.....	21
Configuring PC in Windows NT4.0.....	22
Factory Default Settings .....	23
Information from your ISP.....	25
Configuration via Web Interface .....	26
Chapter 4: Configuration.....	27
Device Info .....	28
Summary.....	29
WAN.....	30
Statistics.....	31
LAN .....	31
WAN Service.....	31
xTM.....	32
xDSL .....	33
Route.....	36
ARP .....	37
DHCP .....	38
Quick Start.....	39
Advanced setup.....	43
WAN-Wide Area Network.....	44
WAN Interface.....	44
WAN Service.....	49
LAN - Local Area Network.....	72
IPv6 Autoconfig.....	75
NAT.....	78
Virtual Servers .....	78

ALG.....	81
DMZ Host.....	82
Security.....	83
Packet Filter.....	83
Parental Control.....	86
Time Restriction.....	86
URL Filter.....	87
QoS - Quality of Service.....	90
Queue Config.....	92
QoS Classification.....	95
Routing.....	104
Default Gateway.....	104
Static Route.....	105
Policy Routing.....	107
RIP.....	108
DNS.....	109
IPv6 DNS Server.....	109
Dynamic DNS.....	110
DSL.....	111
UPnP.....	113
DNS Proxy.....	120
Interface Grouping.....	121
Certificate.....	123
Multicast.....	126
Wireless.....	128
Basic.....	129
Security.....	131
MAC Filter.....	145
Wireless Bridge.....	146
Advanced.....	148
Station Info.....	150
Management.....	151
System Log.....	152
SNMP Agent.....	154
TR-069 Client.....	155
Internet Time.....	157
Mail Alert.....	158
Wake on LAN.....	159
Access Control.....	160
Remote Access.....	161
Update Software.....	162
Backup / Update.....	163
Restart.....	164
Chapter 5: Troubleshooting.....	165
Appendix: Product Support & Contact.....	167

# Chapter 1: Introduction

## Introduction to your Router

Thank you for purchasing BiPAC 7800NEXL router, an all-in-one ADSL2+ Router with wireless-N technology. The BiPAC 7800NEXL is an ADSL2+ Router that offers users affordable expanded wireless coverage and speedy Internet connection. By supporting Internet Protocol, IPv6, this All-in-One Router allows users to make internet connections between existing IPv4 networks and future IPv6 network upgrades when greater security, high quality QoS and larger addressing are required. With an integrated 802.11n Access Point, the BiPAC 7800NEXL can automatically adopt an optimal connection to deliver smooth, constant signal reception even if obstacles are present. Robust Firewall security is featured to protect Internet access against hacker attacks. The Quality of Service and VLAN enables intelligent steaming for HD video or multiple applications such as music downloads, online gaming, video streaming and file sharing simultaneously.

### Optimal Wireless Speeds and Coverage

With an integrated 802.11n Wireless Access Point, this router supports a data rates up to 300Mbps and delivers up to 6 times the speed and 3 times the wireless coverage of an 802.11b/g network device. If the network requires wider coverage, the built-in Wireless Distribution System (WDS) repeater function allows users to expand the wireless network without the need for any external wires or cables.

### Jitter-free, Reliable Net Traffic

Quality of Service (QoS) gives full control over outgoing data traffic. Priority can be assigned by the router to ensure that important transmissions like gaming packets, VoIP calls or IPTV / streaming content passes through the router at lightning speed, even when there is heavy Internet traffic. The transfer speed of different types of outgoing data passing through the router is also controlled to ensure that users do not saturate bandwidth with their browsing activities. The VLAN support is also capable of establishing reliable high-speed transmissions for wide bandwidth applications such as IPTV, VOD, or online gaming without consuming bandwidth.

### High-speed Internet Access

The BiPAC 7800NEXL is compliant with worldwide ADSL standards, and supports download rates of up to 12 / 24Mbps using ADSL2 / 2+, 8Mbps using ADSL and an upload rate of up to 1Mbps. The integrated Annex M standard supports ADSL2 / 2+ for higher uploads by doubling the upload data rate. The 4-port Ethernet Switch incorporated into the BiPAC 7800NEXL enables users to connect to multiple computers or wired-Ethernet devices easily and enjoy blistering LAN transmission for multimedia applications such as interactive gaming, IPTV video streaming and real-time audio.

### Simple Setup, Ease of Management

Easy Sign-On (EZSO), WPS push button and Auto-scan ADSL settings allow users to manage the device functions effortlessly! The user-friendly, web-based user interface makes installing and managing the BiPAC 7800NEXL extremely easy. With support for both DHCP client and server, system administrators can manage IP assignment without having to reconfigure other stations and fitting the router into existing network environments.

## **IPv6 supported**

Internet Protocol version 6 (IPv6) is a version of the Internet Protocol that is designed to succeed IPv4. IPv6 has a vastly larger address space than IPv4. This results from the use of a 128-bit address, whereas IPv4 uses only 32 bits. The new address space thus supports 2<sup>128</sup> (about 3.4×10<sup>38</sup>) addresses. This expansion provides flexibility in allocating addresses and routing traffic and eliminates the primary need for network address translation (NAT), which gained widespread deployment as an effort to alleviate IPv4 address exhaustion.

IPv6 also implements new features that simplify aspects of address assignment (stateless address autoconfiguration) and network renumbering (prefix and router announcements) when changing Internet connectivity providers. The IPv6 subnet size has been standardized by fixing the size of the host identifier portion of an address to 64 bits to facilitate an automatic mechanism for forming the host identifier from Link Layer media addressing information (MAC address).

Network security is integrated into the design of the IPv6 architecture. Internet Protocol Security (IPsec) was originally developed for IPv6, but found widespread optional deployment first in IPv4 (into which it was back-engineered). The IPv6 specifications mandate IPsec implementation as a fundamental interoperability requirement.

## **VLAN MUX**

A Virtual LAN, commonly known as a VLAN, is a group of hosts with the common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of the physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same network switch.

The most commonly used Virtual LAN is defined by 802.1Q tagging protocol, which expended the original Ethernet frame header to include VLAN ID (tag) and priority bits. With the support of network equipments, multiple virtual networks can coexist over the same physical network. Ethernet frames are used to transfer data over ADSL line when bridging, MER or PPPoE mode is used.

While the DSL connection we usually configured is to use a PVC match a single service, PPPoE PPPoA, bridging, etc. With the VLAN tag, we can make virtual interfaces to create multiple separate WAN connections within the same PVC. It allows multiple services over the same PVC. The VLAN Mux feature is designed for this purpose. For example, you have an ATM interface, PVC with VPI/VCI 8/35, you can set the PPPoE, IPoE, and Bridge connection via the PVC without respectively assigning the three services to three different PVCs.

## **Virtual AP**

A “Virtual Access Point” is a logical entity that exists within a physical Access Point (AP). When a single physical AP supports multiple “Virtual APs”, each Virtual AP appears to stations (STAs) to be an independent physical AP, even though only a single physical AP is present. For example, multiple Virtual APs might exist within a single physical AP, each advertising a distinct SSID and capability set. Alternatively, multiple Virtual APs might advertise the same SSID but a different capability set – allowing access to be provided via Web Portal, WEP, and WPA simultaneously. Where APs are shared by multiple providers, Virtual APs provide each provider with separate authentication and accounting data for their users, as well as diagnostic information, without sharing sensitive management traffic or data between providers. You can enable the virtual AP.

## **Web Based GUI**

It supports web based GUI for configuration and management. It is user-friendly and comes with online 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.

# Features

- IPv6 ready (IPv4/IPv6 dual stack)
- Supports Multiple LAN segment for multiple network application
- 4-port 10 / 100Mbps Ethernet switch integrated
- High-speed Internet Access via ADSL2 / 2+; Backward Compatible with ADSL
- 802.11n Wireless Access Point with Wi-Fi Protected Setup (WPS), Wi-Fi Protected Access (WPA-PSK/ WPA2-PSK) and Wired Equivalent Privacy (WEP) support
- Wireless speed up to 300Mbps
- Quality of Service Control for traffic prioritization and bandwidth management
- SOHO Firewall security with DoS Prevention and Packet Filtering
- Universal Plug and Play (UPnP) Compliance
- Dynamic Domain Name System (DDNS)
- Available Syslog
- Ease of Use with Quick Installation Wizard and Auto-scan ADSL settings
- Supports IPTV Application<sup>\*2</sup>
- Easy Sign-On (EZSO)

## ADSL Compliance

- Compliant with ADSL Standard
  - Full-rate ANSI T1.413 Issue 2
  - G.dmt (ITU G.992.1)
  - G.lite (ITU G.992.2)
  - G.hs (ITU G.994.1)
  - ADSL over ISDN / U-R2
- Compliant with ADSL2 Standard
  - G.dmt.bis (ITU G.992.3)
  - ADSL2 Annex M (ITU G.992.3 Annex M) (BiPAC 7800NEXL A only)
- Compliant with ADSL2+ Standard
  - G.dmt.bis plus (ITU G.992.5)
  - ADSL2+ Annex M (ITU G.992.5 Annex M) (BiPAC 7800NEXL A only)

## Network Protocols and Features

- IPv4 or IPv4 / IPv6 Dual Stack
- NAT, static (v4/v6) routing and RIP-1 / 2
- IPv6 Stateless/ Stateful Address Auto-configuration
- IPv6 Router Advertisement
- IPv6 over PPP

- DHCPv6
- Universal Plug and Play (UPnP) Compliant
- Dynamic Domain Name System (DDNS)
- Virtual Server and DMZ
- SNTP, DNS relay and IGMP proxy
- IGMP snooping for video service
- Management based-on IP protocol, port number and address

## **Firewall**

- Built-in NAT Firewall
- Stateful Packet Inspection (SPI)
- Prevents DoS attacks including Land Attack, Ping of Death, etc.
- Remote access control for web base access
- Packet Filtering (v4/v6) - port, source IP address, destination IP address, MAC address
- URL Content Filtering - string or domain name detection in URL string
- Password protection for system management
- VPN pass-through

## **Quality of Service Control**

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

## **ATM, PTM and PPP Protocols**

- ATM Adaptation Layer Type 5 (AAL5)
- Classical IP over ATM (IPoA) (RFC 2225 / RFC 1577)
- Bridged or routed Ethernet encapsulation
- VC and LLC based multiplexing
- PPP over Ethernet (PPPoE)
- PPP over ATM (RFC 2364)
- MAC Encapsulated Routing (RFC 1483 MER)
- OAM F4 / F5



## **IPTV Applications<sup>\*2</sup>**

- Virtual LAN (VLAN)
- Quality of Service (QoS)
- IGMP Snooping & IGMP Proxy
- MLD Snooping & proxy
- VLAN MUX support

## **Wireless LAN**

- Compliant with IEEE 802.11n, 802.11g and 802.11b standards
- 2.4 GHz - 2.484 GHz frequency range
- Up to 300Mbps wireless operation rate
- 64 / 128 bits WEP supported for encryption
- WPS (Wi-Fi Protected Setup) for easy setup
- Wireless Security with WPA-PSK / WPA2-PSK support
- WDS repeater function support
- 802.1x radius supported
- Web-based GUI for WLAN on/off switch

## **Management**

- Easy Sign-On (EZSO) and Auto-scan ADSL settings
- Web-based GUI for remote and local management (IPv4 / IPv6)
- Firmware upgrades and configuration data upload and download via web-based GUI
- Embedded Telnet server for remote and local management
- Available Syslog
- Mail alert for WAN IP changed
- Wake on LAN
- Supports DHCP server / client / relay
- TR-069<sup>\*3</sup> supports remote management
- SNMP v1/v2/V3 supports remote and local management



1. The router may require firmware modification for certain ADSL2 / 2+ / Annex M DSLAMs.
2. IPTV application may require subscribing to IPTV services from a Telco / ISP.
3. Only upon request for Telco / ISP tender projects.

# Hardware Specifications

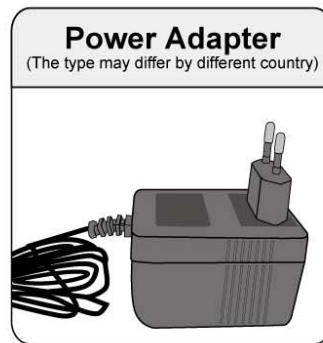
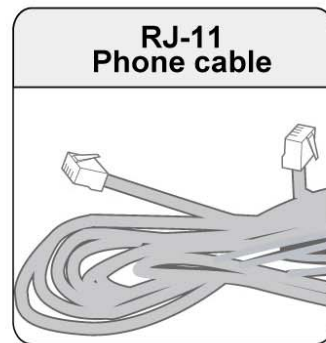
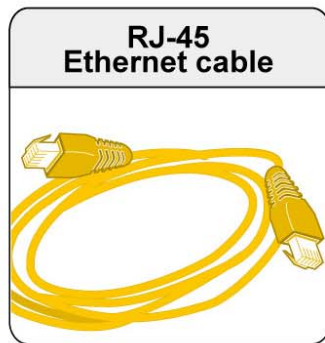
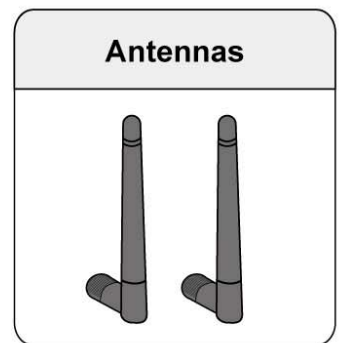
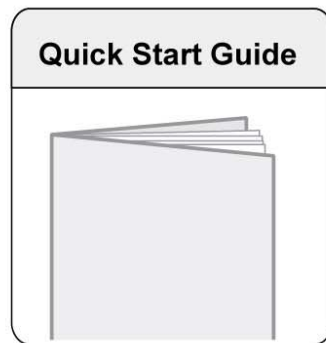
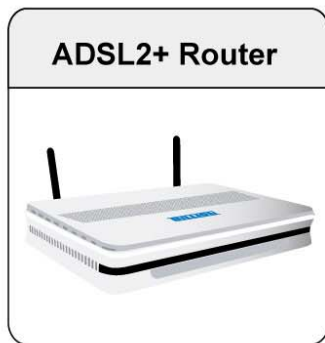
## Physical Interface

- WLAN: 2 x 2dbi detachable antennas
- DSL: ADSL port
- Ethernet: 4-port 10 / 100Mbps auto-crossover (MDI / MDI-X) Switch
- Factory default reset button
- WPS push button
- Power jack
- Power switch

# Chapter 2: Installing the Router

## Package Contents

- BiPAC 7800NEXL 3G / Wireless-N Dual WAN ADSL2+ Firewall Router
- Quick Start Guide
- CD containing the on-line manual
- Two 2dBi detachable antennas
- Ethernet (RJ-45) cable
- RJ-11 ADSL/ telephone cable
- Power adapter
- Splitter / Micro-filter (Optional)



## Important note for using this router



### Warning

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

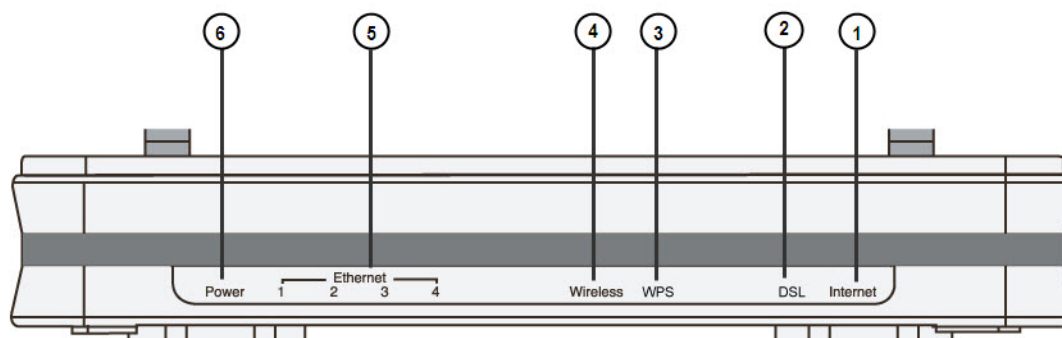


### Attention

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

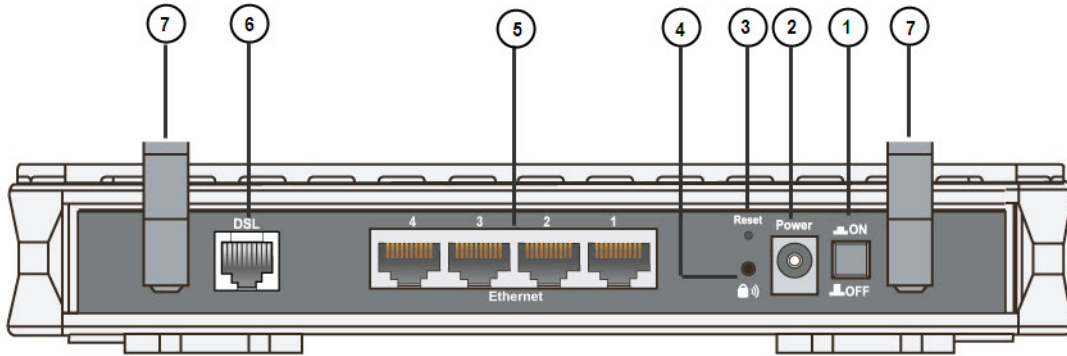
# Device Description

## The Front LEDs



LED		Meaning
1	Internet	<p>Lit red when WAN port fails to get IP address.</p> <p>Lit green when WAN port gets IP address successfully.</p> <p>Unlit when the device is in bridge mode or WAN connection is absent.</p>
2	DSL	<p>Lit green when the device is successfully connected to an ADSL DSLAM. ("line sync")</p>
3	WPS	<p>Flash green when WPS configuration is in progress.</p> <p>Unlit when WPS fails.</p>
4	Wireless	<p>Lit green when a wireless connection is established.</p> <p>Unlit when wireless is disabled.</p>
5	Ethernet port 1X - 4X (RJ-45 connector)	<p>Lit green when successfully connected to an Ethernet device.</p> <p>Blinking when data is being transmitted / received.</p>
6	Power	<p>When the system is ready, it will be lit green.</p> <p>Lit red when the device fails to boot or when the device is in emergency mode</p>

# The Rear Ports



Port		Meaning
1	<b>Power Switch</b>	Power ON/OFF switch.
2	<b>Power</b>	Connect it with the supplied power adapter.
3	<b>Reset</b>	Press for more than 5 seconds to restore the device to its factory default mode.
4	<b>WPS</b>	Push WPS button to trigger Wi-Fi Protected Setup function. For WPS configuration details, please refer to <a href="#">WPS</a> Setup section of this User Manual.
5	<b>Ethernet</b>	Connect your computer to a LAN port using the included Ethernet cable (with RJ-45 cable)
6	<b>DSL</b>	Connect the supplied RJ-11 cable to this port when connecting to the ADSL/telephone network
7	<b>Wireless Antenna</b>	Connect the detachable antenna for wireless connection.

## 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. If the error persists, you may have a hardware problem. In this case you should contact technical support.

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

# 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 7 / 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.

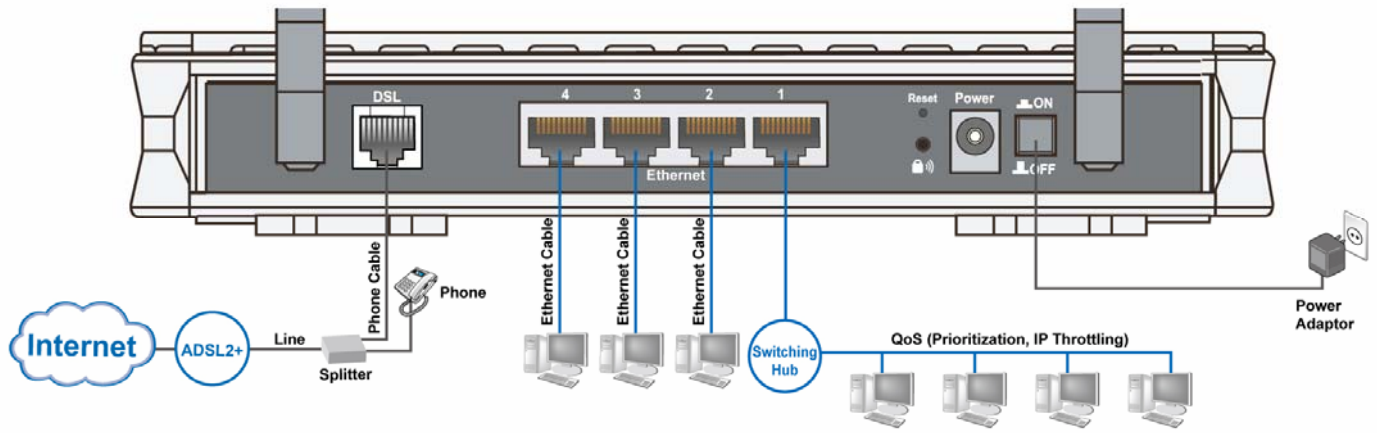


Any TCP/IP capable workstation can be used to communicate with or through this router. To configure other types of workstations, please consult your manufacturer documentation.



# Connecting Your Router

Users can connect the ADSL2+ router as the following.

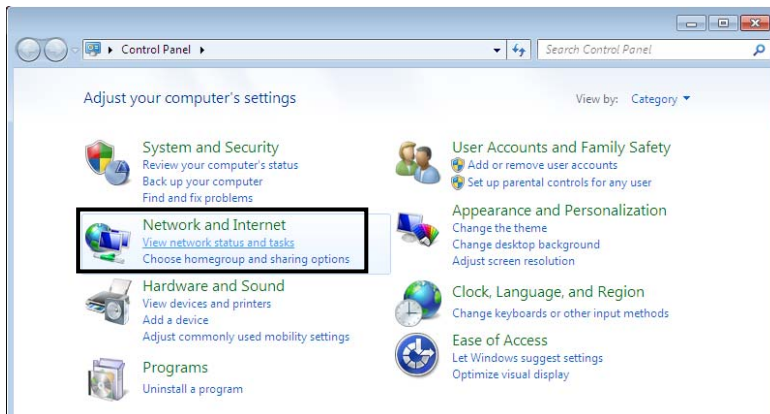


# Network Configuration

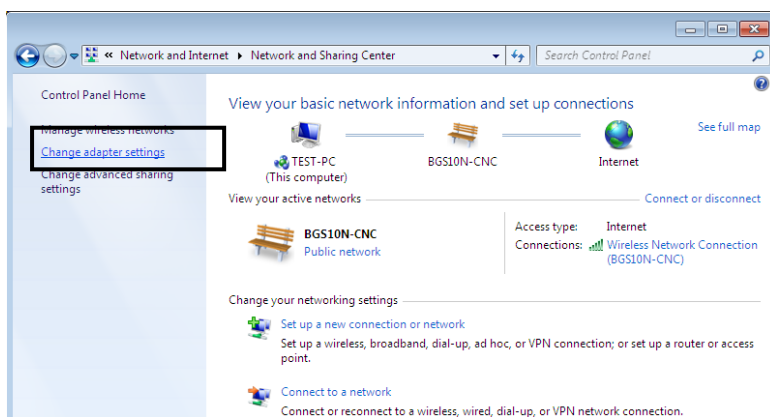
## Configuring PC in windows 7

1. Go to Start. Click on Control Panel.

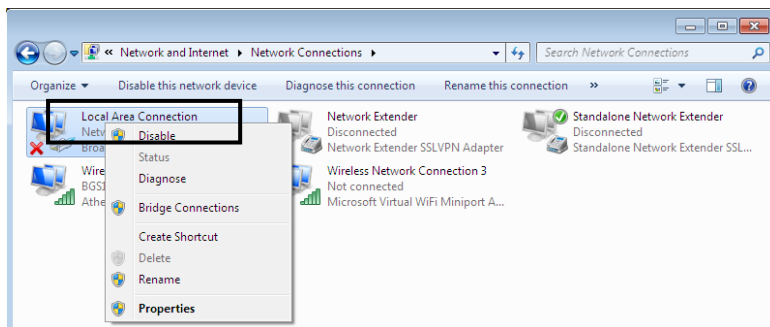
Then click on Network and Internet.



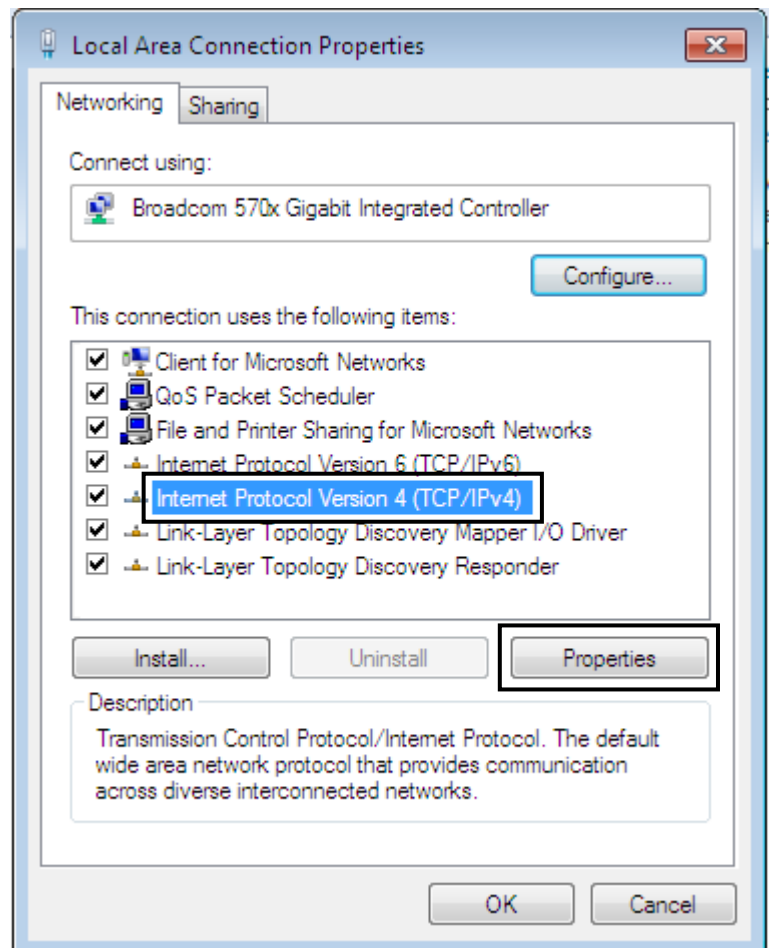
2. When the Network and Sharing Center window pops up, select and click on Change adapter settings on the left window panel.



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

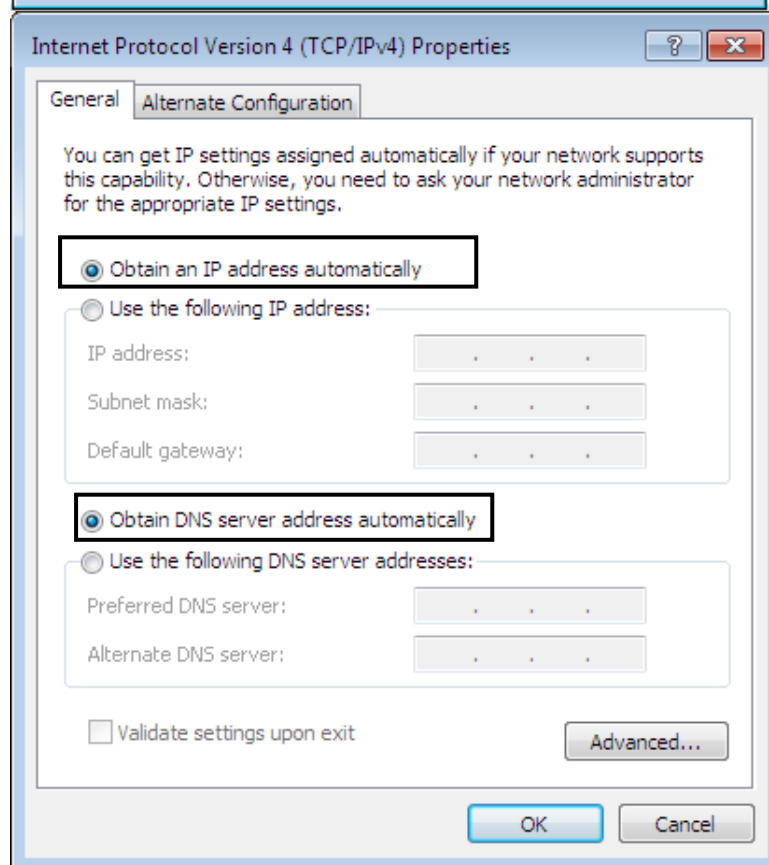


4. Select Internet Protocol Version 4 (TCP/IPv4) then click Properties.



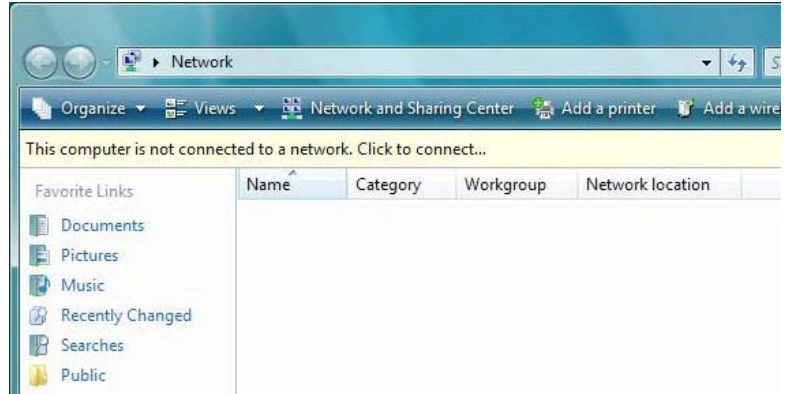
5. In the TCP/IPv4 properties window, select the Obtain an IP address automatically and Obtain DNS Server address automatically radio buttons. Then click OK to exit the setting.

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

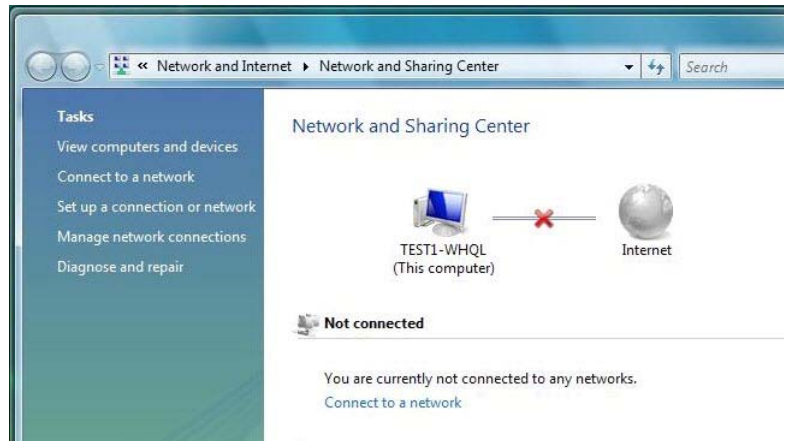


# Configuring PC in Windows Vista

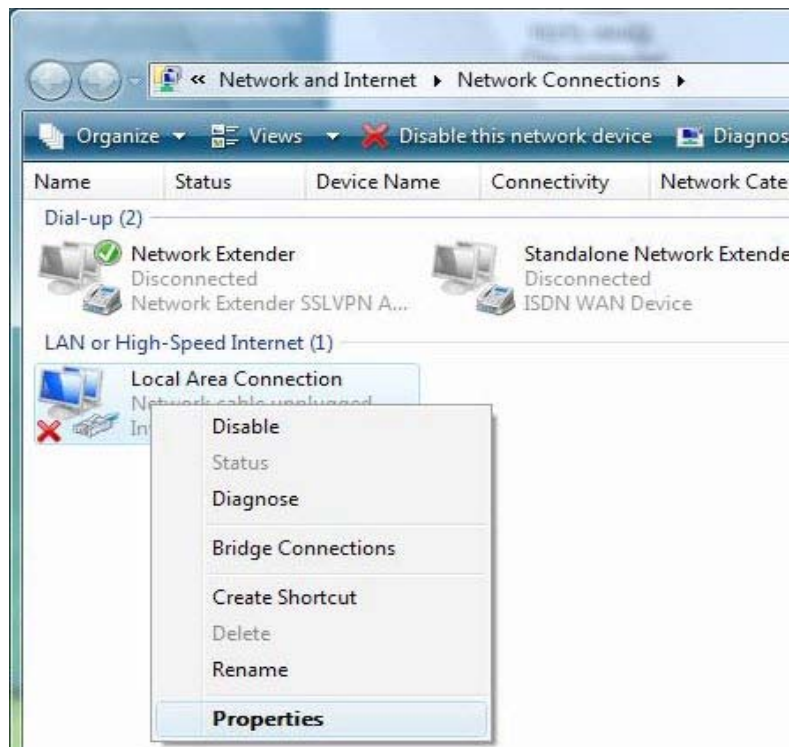
1. Go to Start. Click on Network.
2. Then click on Network and Sharing Center at the top bar.



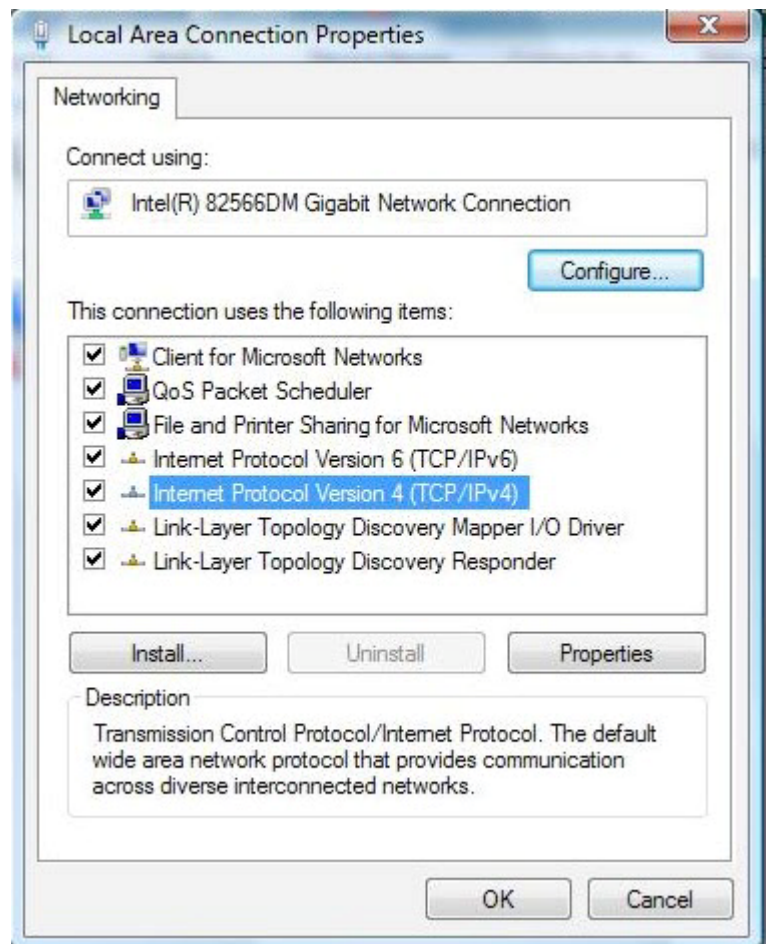
3. When the Network and Sharing Center window pops up, select and click on Manage network connections on the left window column.



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

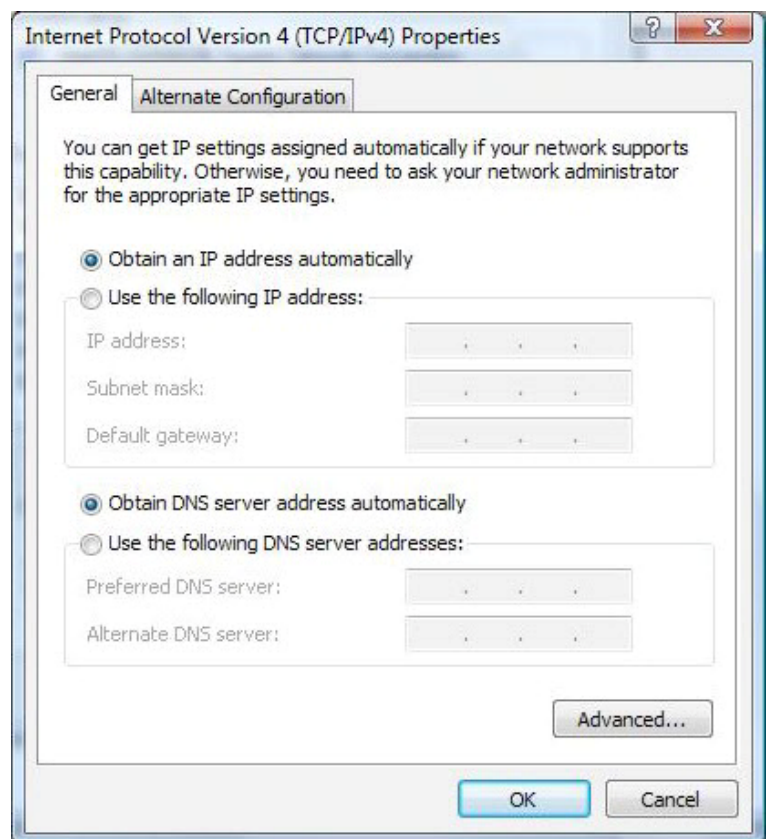


5. Select Internet Protocol Version 4 (TCP/IPv4) then click Properties.



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

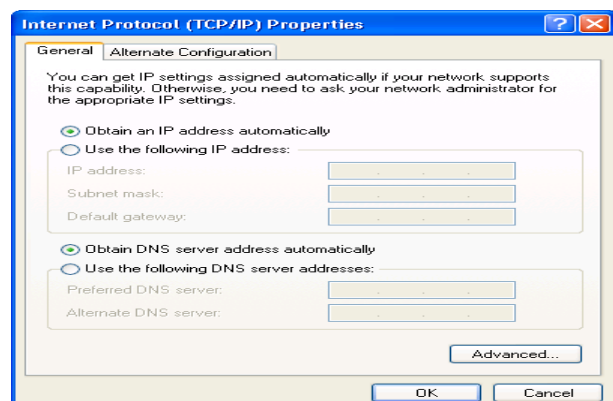
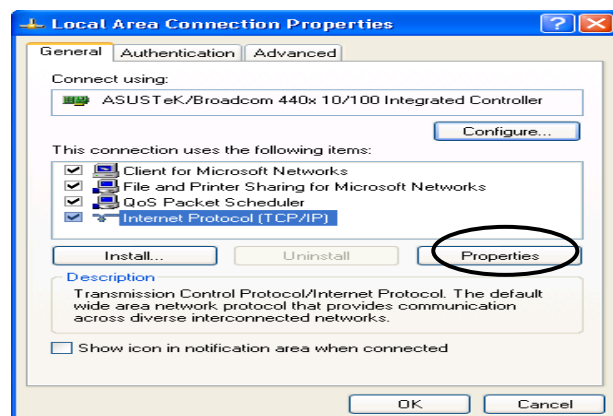
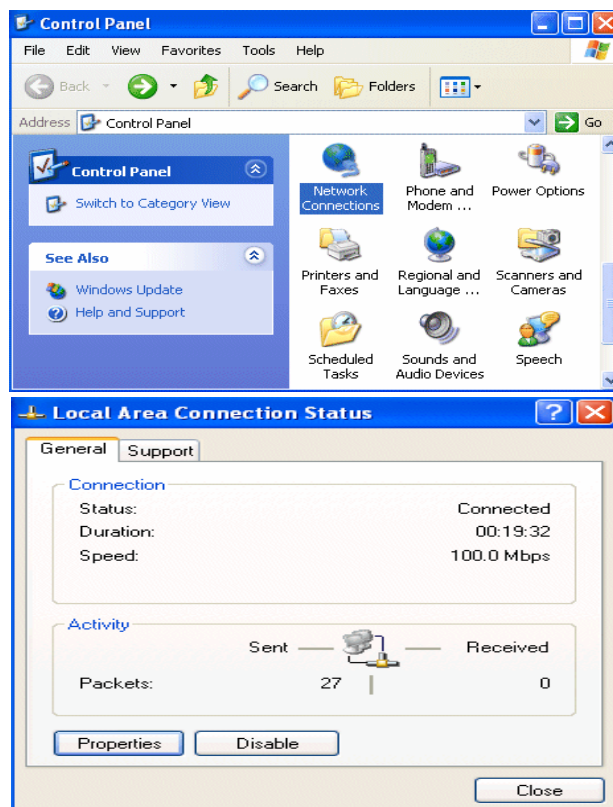
1. Go to Start > Control Panel (in Classic View). In the Control Panel, double-click on Network Connections
2. Double-click Local Area Connection.

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.

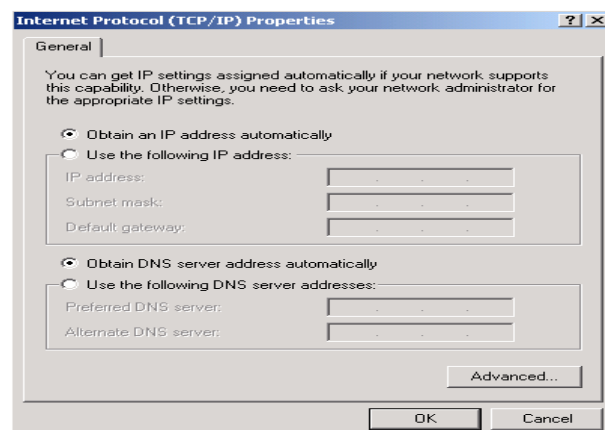
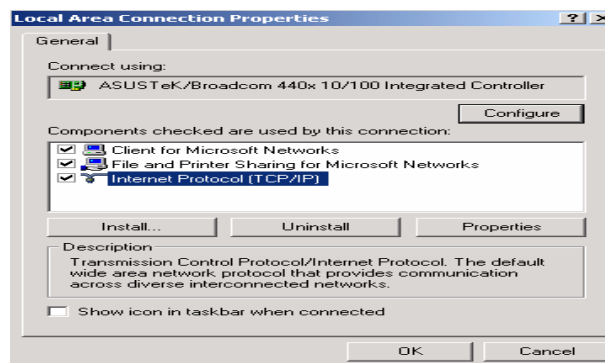
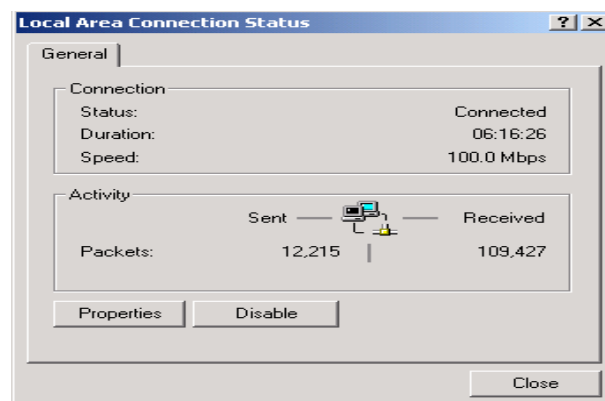
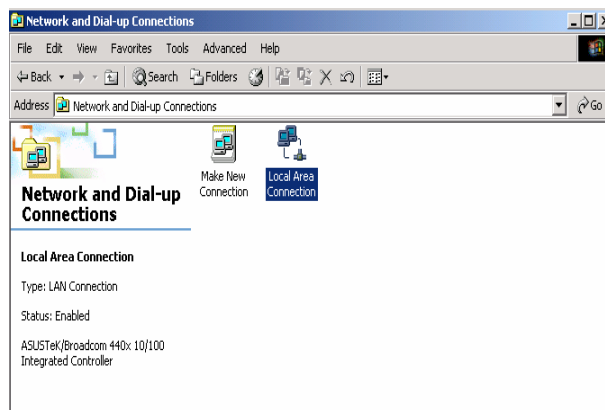
2. Double-click Local Area Connection.

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

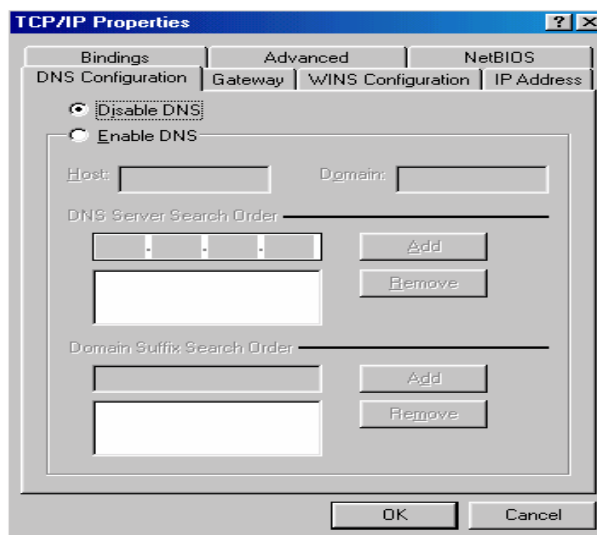
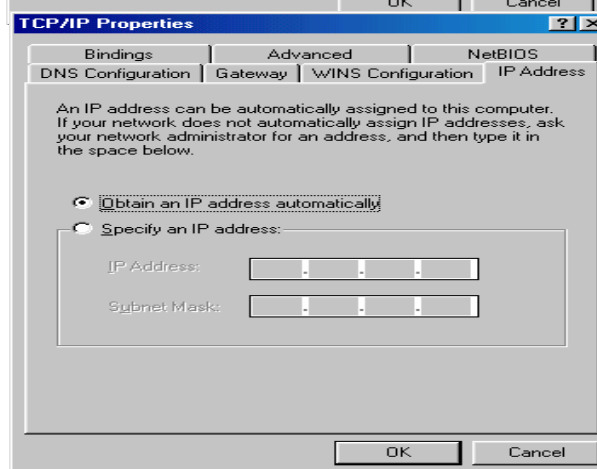
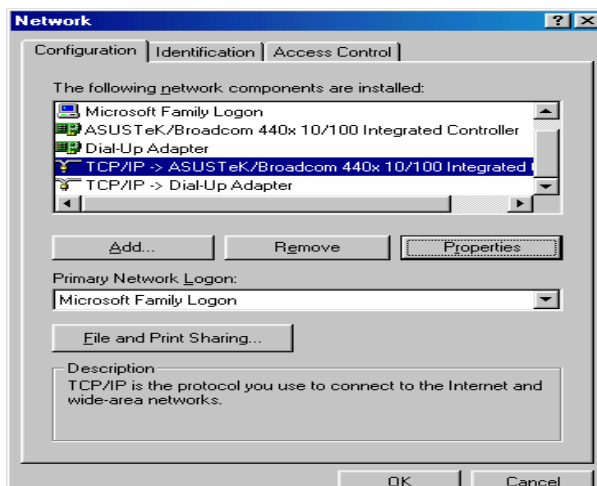
1. Go to Start > Settings > Control Panel. In the Control Panel, double-click on Network and choose the Configuration tab.

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.



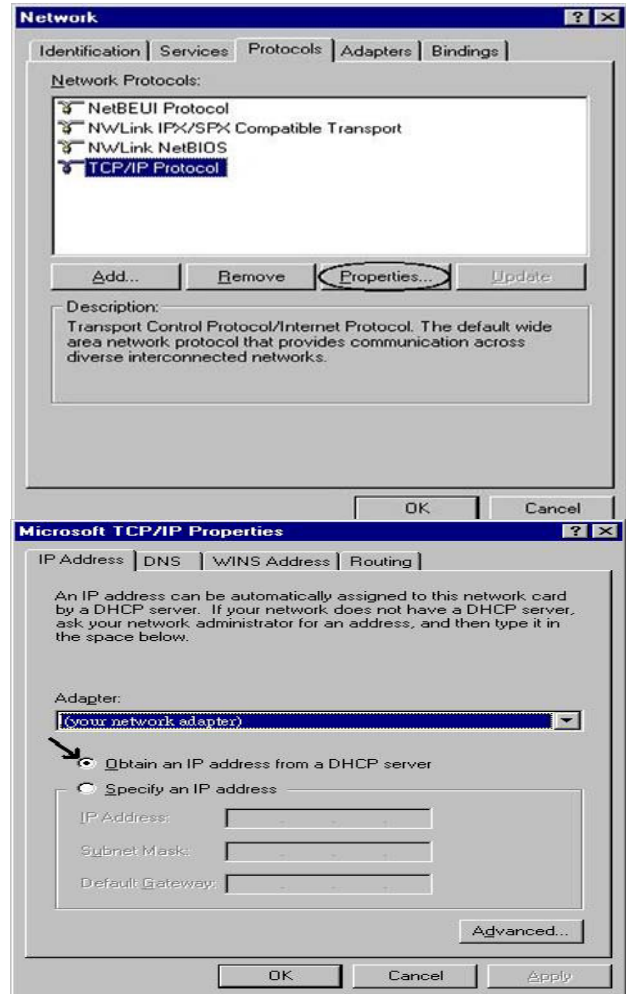


# Configuring PC in Windows NT4.0

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)

Three user levels are provided by this router, thus **Administrator**, **Remote** and **Local** respectively. (Note: Administrator admin, is enabled by default, but the other two users need to be enabled through manual settings by administrator. See [Access Control](#) section.)

### Administrator

- ▶ Username: admin
- ▶ Password: admin

### Local

- ▶ Username: user
- ▶ Password: user

### Remote

- ▶ Username: support
- ▶ Password: support



If you have forgotten the username or password of the router, you can restore the device to its default setting by pressing the Reset button for more than 5 seconds.

**Attention**

## Device LAN IPv4 settings

- ▶ IPv4 Address: 192.168.1.254
- ▶ Subnet Mask: 255.255.255.0

## Device LAN IPv6 settings

- ▶ IPv6 Address / prefix: Default is a link-local address and is different from each other as MAC address is different from one to one. For example: fe80:0000:0000:0000:0204:edff:fe01:0001 / 64, the prefix initiates by fe80::

## DHCP server for IPv4

- ▶ 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.

### IPv4

LAN Port		WAN Port
IPv4 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	

### IPv6

LAN Port		WAN Port
IPv6 address/prefix	Default is a link-local address and is different from each other as MAC address is different from one to one. For example : fe80:0000:0000:0000:0204:edff:fe01:0001/64, the prefix initiates by fe80::	The PPPoE function is enabled to automatically get the WAN port configuration from the ISP.
DHCP server function	Enabled	


## Information from your ISP

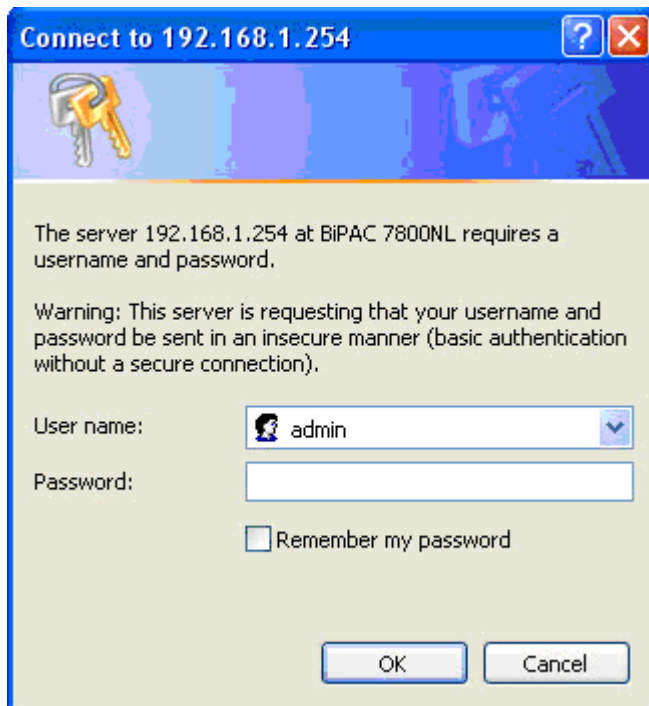
Before configuring this device, you have to check with your ISP (Internet Service Provider) to find out what kind of service is provided such as DHCP (Obtain an IP Address Automatically, Static IP (Fixed IP Address) or PPPoE.

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).
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.

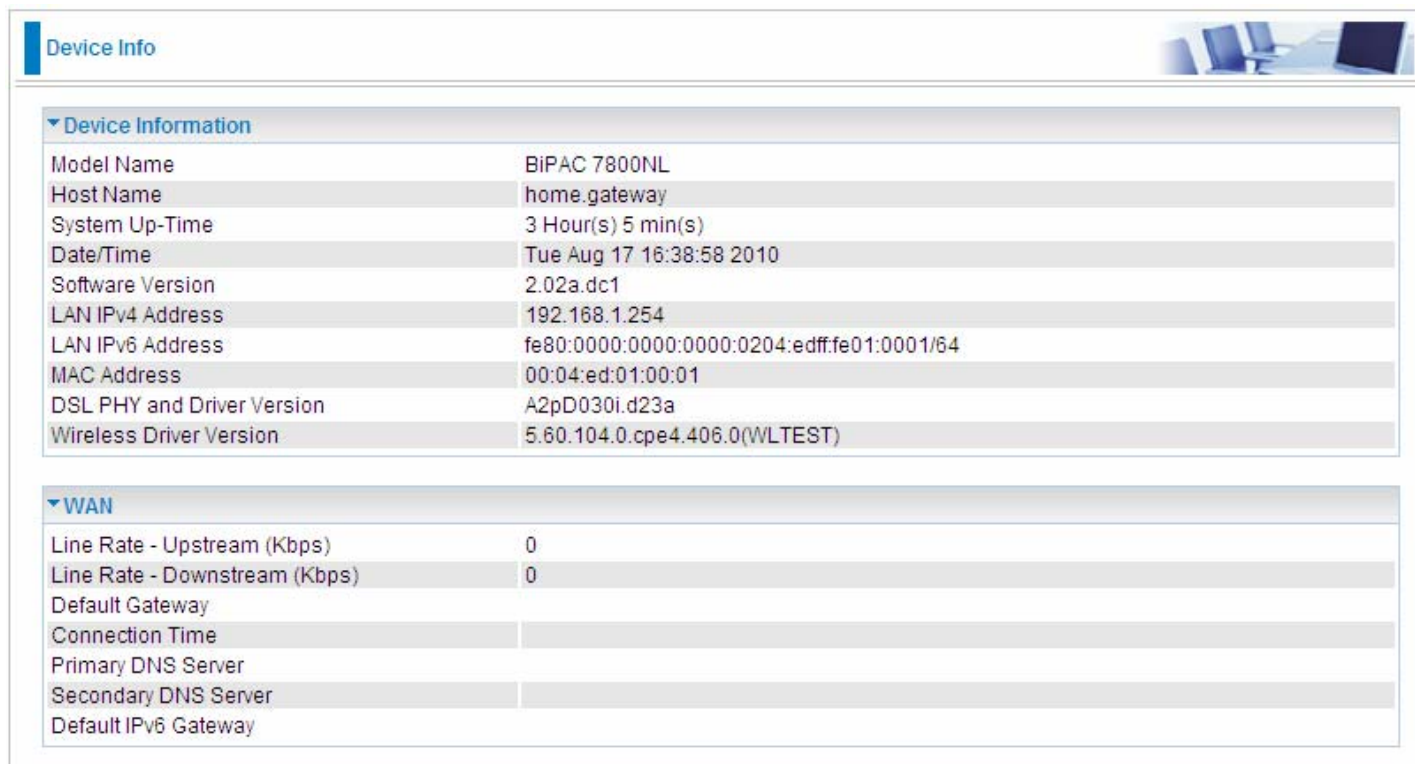
# Configuration via Web Interface

Open your web browser; enter the IP address of your router, which by default is 192.168.1.254, and click  or press 'Enter' key on the keyboard, a login prompt window will appear. The default root username and password are "admin" and "admin" respectively.



**Congratulations! You are now successfully logged in to the Firewall Router!**

If the authentication succeeds, the Status page below will appear on the screen.



The screenshot shows the "Device Info" page of a web interface. At the top left, there is a blue bar with the text "Device Info". To the right of this bar is a small image of a computer monitor and keyboard. Below the bar is a table of device information. The table has two sections: "Device Information" and "WAN".

Device Information	
Model Name	BiPAC 7800NL
Host Name	home.gateway
System Up-Time	3 Hour(s) 5 min(s)
Date/Time	Tue Aug 17 16:38:58 2010
Software Version	2.02a.dc1
LAN IPv4 Address	192.168.1.254
LAN IPv6 Address	fe80:0000:0000:0000:0204:edff:fe01:0001/64
MAC Address	00:04:ed:01:00:01
DSL PHY and Driver Version	A2pD030i.d23a
Wireless Driver Version	5.60.104.0.cpe4.406.0(WLTEST)

WAN	
Line Rate - Upstream (Kbps)	0
Line Rate - Downstream (Kbps)	0
Default Gateway	
Connection Time	
Primary DNS Server	
Secondary DNS Server	
Default IPv6 Gateway	

# Chapter 4: Configuration

Once you have logged on to your BiPAC 7800NEXL Router via your web browser, you can begin to set it up according to your requirements. On the configuration homepage, the left navigation pane links you directly to the setup pages, which include:

- **Device Info** (Summary, WAN, Statistics, Route, ARP, DHCP)

- **Quick Start**

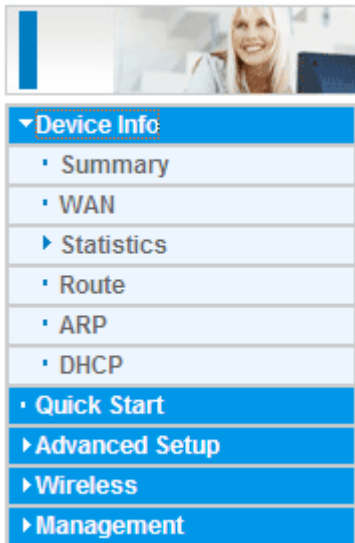
- **Advanced Setup** (WAN, LAN, NAT, Security, Parental Control, Quality of Service, Routing, DNS, DSL, UPnP, DNS Proxy, Interface Grouping, Certificate, Multicast)

- **Wireless** (Basic, Security, MAC Filter, Wireless Bridge, Advanced, Station Info)

- **Management** (System Log, SNMP Agent, TR-069 Client, Internet Time, Mail Alert, Wake on LAN, Access Control, Remote Access, Update Software, Backup/Update)

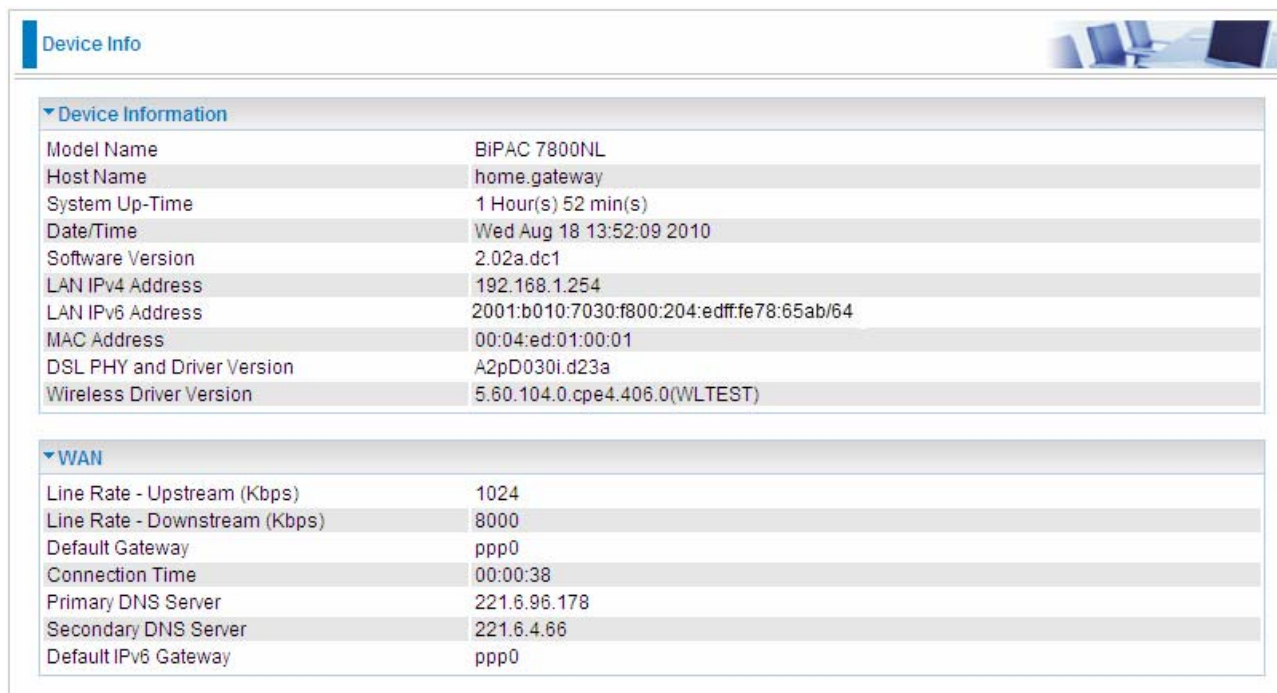
# Device Info

This Section gives users an easy access to the information about the working router and view the current status of the router. Here **Summary**, **WAN**, **Statistics**, **Router**, **ARP** and **DHCP** six subsections are included.



# Summary

The basic information about the device is provided here (the following is a configured screenshots to let users understand clearly).



The screenshot shows a web interface for a network device. At the top left, there is a 'Device Info' tab. Below it, there are two expandable sections: 'Device Information' and 'WAN'. The 'Device Information' section contains the following data:

Model Name	BIPAC 7800NL
Host Name	home.gateway
System Up-Time	1 Hour(s) 52 min(s)
Date/Time	Wed Aug 18 13:52:09 2010
Software Version	2.02a.dc1
LAN IPv4 Address	192.168.1.254
LAN IPv6 Address	2001:b010:7030:f800:204:edff:fe78:65ab/64
MAC Address	00:04:ed:01:00:01
DSL PHY and Driver Version	A2pD030i.d23a
Wireless Driver Version	5.60.104.0.cpe4.406.0(WLTEST)

The 'WAN' section contains the following data:

Line Rate - Upstream (Kbps)	1024
Line Rate - Downstream (Kbps)	8000
Default Gateway	ppp0
Connection Time	00:00:38
Primary DNS Server	221.6.96.178
Secondary DNS Server	221.6.4.66
Default IPv6 Gateway	ppp0

## Device Information

**Model Name:** Display the model name.

**Host Name:** Display the name of the router.

**System Up-Time:** Display the elapsed time since the device is on.

**Date/Time:** Display the current exact date and time.

**Software Version:** Firmware version.

**LAN IPv4 Address:** Display the LAN IPv4 address.

**LAN IPv6 Address:** Display the LAN IPv6 address. Default is a Link-Local address, but when connects to ISP, it will display the Global Address, like above figure.

**MAC Address:** Display the MAC address.

**DSL PHY and Driver Version:** Display DSL PHY and Driver version.

**Wireless Driver Version:** Display wireless driver version.

## WAN

**Line Rate – Upstream (Kbps):** Display Upstream line Rate in Kbps.

**Line Rate – Downstream (Kbps):** Display Downstream line Rate in Kbps.

**Default Gateway:** Display Default Gateway.

**Connection Time:** Display the elapsed time since ADSL connection is up.

**Primary DNS Server:** Display IPV4 address of Primary DNS Server.

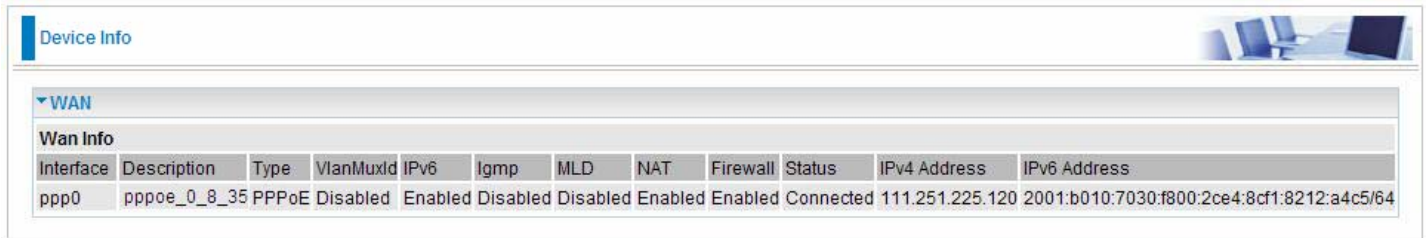
**Secondary DNS Server:** Display IPV4 address of Secondary DNS Server.

**Default IPv6 Gateway:** Display the IPv6 Gateway used.



# WAN

This table displays the information of the WAN connections, users can turn here for WAN connection information.



The screenshot shows a 'Device Info' section with a 'WAN' tab selected. Below the tab is a 'Wan Info' table with the following data:

Interface	Description	Type	VlanMuxId	IPv6	Igmp	MLD	NAT	Firewall	Status	IPv4 Address	IPv6 Address
ppp0	pppoe_0_8_35	PPPoE	Disabled	Enabled	Disabled	Disabled	Enabled	Enabled	Connected	111.251.225.120	2001:b010:7030:f800:2ce4:8cf1:8212:a4c5/64

**Interface:** the WAN connection interface.

**Description:** the description of this connection.

**Type:** the protocol used by this connection.

**VlanMuxId:** Show the status of the VLANMuxId, VLAN ID or disabled. If VLAN ID is -1, then disabled is shown in this field, while if VLAN ID isn't -1, the exact VLAN ID is shown here in this field.

**Igmp:** Display the status of IGMP, disabled or enabled.

**NAT:** Display the status of NAT, disabled or enabled.

**Firewall:** Display the status of Firewall, disabled or enabled.

**Status:** Display the status of this WAN connection.

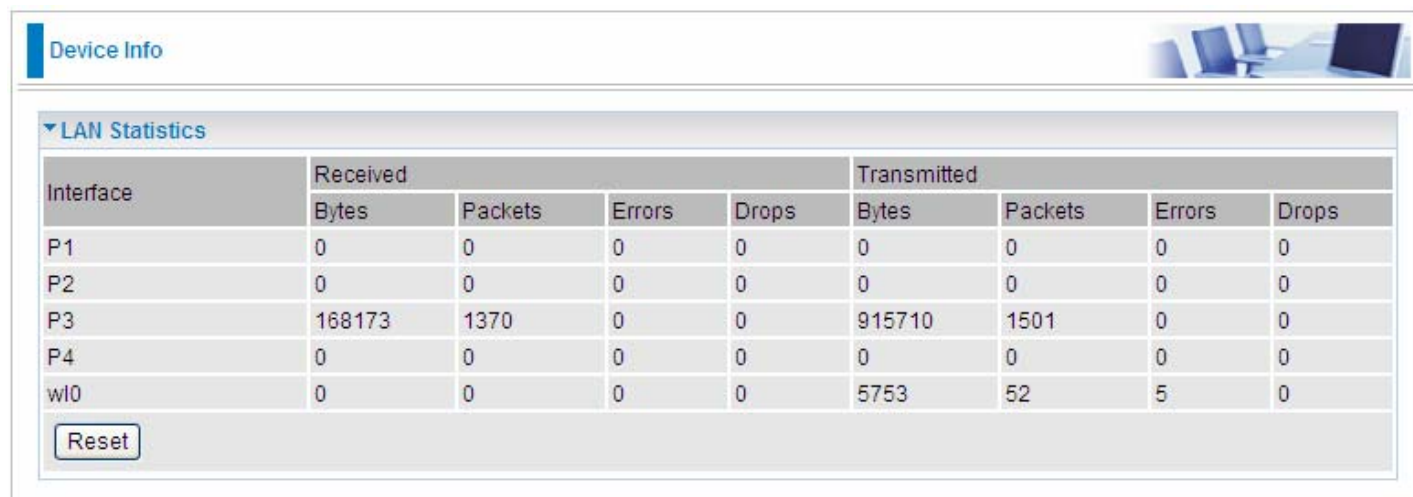
**IPv4 Address:** the WAN IPv4 Address the device obtained.

**IPv6 Address:** the WAN IPv6 Address the device obtained.

# Statistics

## LAN

The table shows the statistics of LAN.



The screenshot shows a web interface with a 'Device Info' header and a 'LAN Statistics' section. The table below displays statistics for five interfaces: P1, P2, P3, P4, and wl0. P3 shows the highest activity with 168173 bytes received and 915710 bytes transmitted. A 'Reset' button is located at the bottom left of the table.

Interface	Received				Transmitted			
	Bytes	Packets	Errors	Drops	Bytes	Packets	Errors	Drops
P1	0	0	0	0	0	0	0	0
P2	0	0	0	0	0	0	0	0
P3	168173	1370	0	0	915710	1501	0	0
P4	0	0	0	0	0	0	0	0
wl0	0	0	0	0	5753	52	5	0

**Interface:** List each LAN interface. P1-P4 indicate the four LAN interfaces.

**Bytes:** Display the Received and Transmitted traffic statistics in Bytes.

**Packets:** Display the Received and Transmitted traffic statistics in Packets.

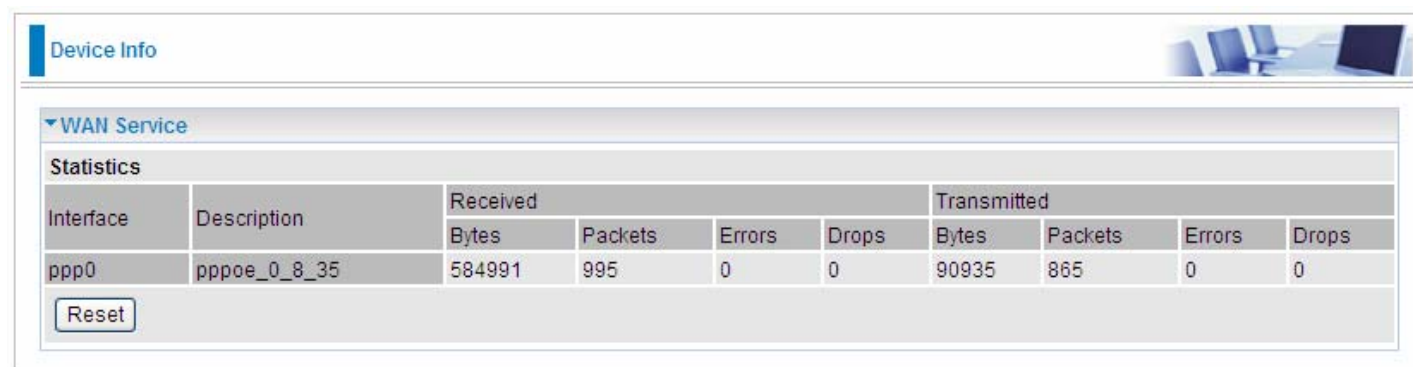
**Errors:** Display the statistics of errors arising in Receiving or Transmitting data.

**Drops:** Display the statistics of drops arising in Receiving or Transmitting data.

**Reset:** Press this button to get the latest information.

## WAN Service

The table shows the statistics of LAN.



The screenshot shows a web interface with a 'Device Info' header and a 'WAN Service' section. The table below displays statistics for the ppp0 interface. It shows 584991 bytes received and 90935 bytes transmitted. A 'Reset' button is located at the bottom left of the table.

Interface	Description	Received				Transmitted			
		Bytes	Packets	Errors	Drops	Bytes	Packets	Errors	Drops
ppp0	pppoe_0_8_35	584991	995	0	0	90935	865	0	0

**Interface:** Display the connection interface.

**Description:** the description for the connection.

**Bytes:** Display the WAN Received and Transmitted traffic statistics in Bytes.

**Packets:** Display the WAN Received and Transmitted traffic statistics in Packets.

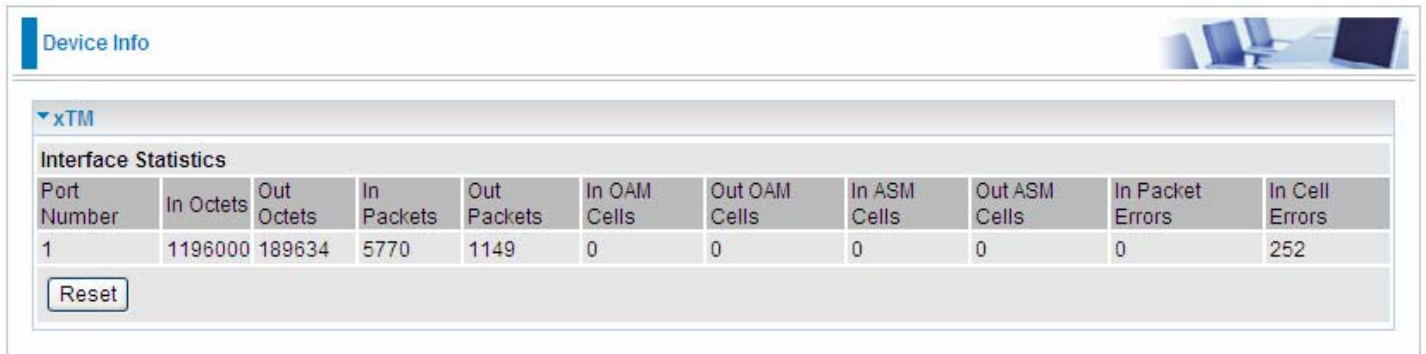
**Errors:** Display the statistics of errors arising in Receiving or Transmitting data.

**Drops:** Display the statistics of drops arising in Receiving or Transmitting data.

**Reset:** Press this button to get the latest information.

## xTM

The Statistics-xTM screen displays all the xTM statistics



The screenshot shows a web interface for 'Device Info' with a section for 'xTM'. Under 'Interface Statistics', there is a table with 11 columns: Port Number, In Octets, Out Octets, In Packets, Out Packets, In OAM Cells, Out OAM Cells, In ASM Cells, Out ASM Cells, In Packet Errors, and In Cell Errors. The data for port 1 is as follows:

Port Number	In Octets	Out Octets	In Packets	Out Packets	In OAM Cells	Out OAM Cells	In ASM Cells	Out ASM Cells	In Packet Errors	In Cell Errors
1	1196000	189634	5770	1149	0	0	0	0	0	252

Below the table is a 'Reset' button.

**Port Number:** Shows number of the port for xTM.

**In Octets:** Number of received octets over the interface.

**Out Octets:** Number of transmitted octets over the interface.

**In Packets:** Number of received packets over the interface.

**Out Packets:** Number of transmitted packets over the interface.

**In OAM Cells:** Number of OAM cells received.

**Out OAM Cells:** Number of OAM cells transmitted.

**In ASM Cells:** Number of ASM cells received.

**Out ASM Cells:** Number of ASM cells transmitted.

**In Packet Errors:** Number of received packets with errors.

**In Cell Errors:** Number of received cells with errors.

**Reset:** Click to reset the statistics.

## xDSL

xDSL		
Mode	ADSL_G.dmt	
Traffic Type	ATM	
Status	Up	
Link Power State	L0	
	Downstream	Upstream
Line Coding (Trellis)	On	On
SNR Margin (0.1 dB)	194	110
Attenuation (0.1 dB)	0	0
Output Power (0.1 dBm)	78	123
Attainable Rate (Kbps)	11776	1284
Rate (Kbps)	8000	1024
K (number of bytes in DMT frame)	251	33
R (number of check bytes in RS code word)	2	4
S (RS code word size in DMT frame)	1.00	1.00
D (interleaver depth)	16	4
Delay (msec)	4.00	4.00
INP (DMT symbol)	0.06	0.05
Super Frames	104901	104901
Super Frame Errors	0	0
RS Words	7133251	1781277
RS Correctable Errors	0	0
RS Uncorrectable Errors	0	0
HEC Errors	0	0
OCD Errors	0	0
LCD Errors	0	0
Total Cells	34783189	0
Data Cells	23703	0
Bit Errors	0	0
Total ES	0	0
Total SES	0	0
Total UAS	12	12
<input type="button" value="xDSL BER Test"/> <input type="button" value="Reset"/>		

**Mode:** Modulation protocol, including G.dmt, G.lite, T1.413, ADSL2, AnnexL, ADSL2+ and AnnexM.

**Traffic Type:** transfer mode, here supports ATM and PTM.

**Status:** Show the status of DSL link.

**Link Power State:** Show link output power state.

**Line Coding (Trellis):** Trellis on/off.

**SNR Margin (0.1 dB):** show the Signal to Noise Ratio(SNR) margin.

**Attenuation (0.1 dB):** This is estimate of average loop attenuation of signal.

**Output Power (0.1 dBm):** show the output power.

**Attainable Rate (Kbps) :** The sync rate you would obtain.

**Rate (Kbps):** show the downstream and upstream rate in Kbps.

**K (number of bytes in DMT frame):** show the number of bytes in DMT frame.

**R (number of check bytes in RS code word):** show the number of check bytes in RS code word.

**S (RS code word size in DMT frame):** show the RS code word size in DMT frame.

**D (interleaver depth):** show the interleaver depth.

**Delay (msec):** show the delay time in msec.

**INP (DMT symbol):** show the DMT symbol.

**Super Frames: the total number of super frames.**

**Super Frame Errors: the total number of super frame errors.**

**RS Words:** Total number of Reed-Solomon code errors.

**RS Correctable Errors:** Total number of RS with correctable errors.

**RS Uncorrectable Errors:** Total number of RS words with uncorrectable errors.

**HEC Errors:** Total number of Header Error Checksum errors.

**OCD Errors:** Total number of out-of-cell Delineation errors.

**LCD Errors:** Total number of Loss of Cell Delineation.

**Total Cells:** Total number of cells.

**Data Cells:** Total number of data cells.

**Bit Errors:** Total number of bit errors.

**Total ES:** Total Number of Errored Seconds.

**Total SES:** Total Number of Severely Errored Seconds.

**Total UAS:** Total Number of Unavailable Seconds.

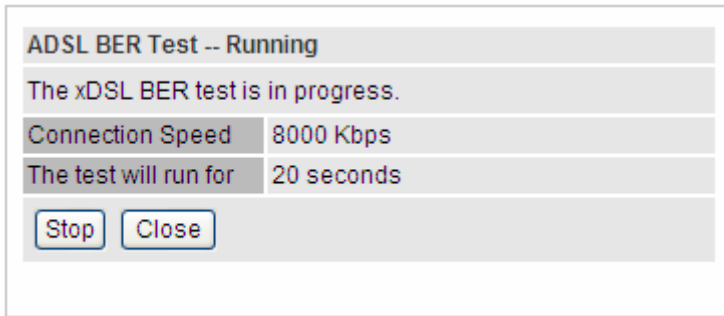
**xDSL BER Test:** Click this button to start a bit Error Rate Test. The ADSL Bit Error Rate (BER) test determines the quality of the ADSL connection. The test is done by transferring idle cells containing a known pattern and comparing the received data with this known pattern to check for any errors.

**ADSL BER Test -- Start**

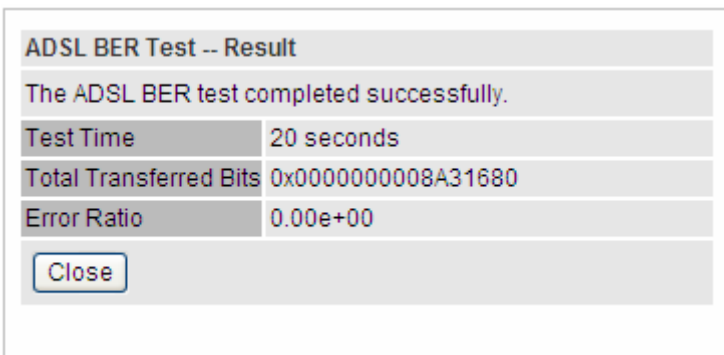
The ADSL Bit Error Rate (BER) test determines the quality of the ADSL connection. The test is done by transferring idle cells containing a known pattern and comparing the received data with this known pattern to check for any errors.

Tested Time (sec)

Select the Tested Time(sec), press **Start** to start test.

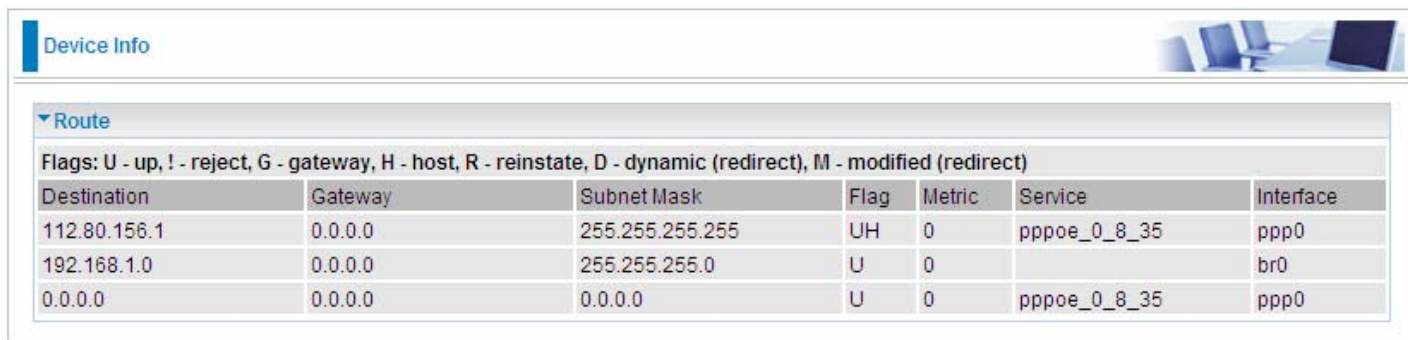


When it is OK, the following test result window will appear. You can view the quality of ADSL connection. Here the connection is OK.



**Reset** : Click this button to reset the statistics.

# Route



The screenshot shows a 'Device Info' window with a 'Route' section. It includes a legend for flags and a table with columns for Destination, Gateway, Subnet Mask, Flag, Metric, Service, and Interface.

Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate, D - dynamic (redirect), M - modified (redirect)

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
112.80.156.1	0.0.0.0	255.255.255.255	UH	0	pppoe_0_8_35	ppp0
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0
0.0.0.0	0.0.0.0	0.0.0.0	U	0	pppoe_0_8_35	ppp0

**Destination:** the IP address of destination network.

**Gateway:** the IP address of the gateway this route uses.

**Subnet Mask:** the destination subnet mask.

**Flag:** show the status of the route.

- ① **U:** show the route is activated or enabled.
- ① **H (host):** destination is host not the subnet.
- ① **G:** show that the outside gateway is needed to forward packets in this route.
- ① **R:** show that the route is reinstated from dynamic routing.
- ① **D:** show that the route is dynamically installed by daemon or redirecting.
- ① **M:** show the route is modified from routing daemon or redirect.

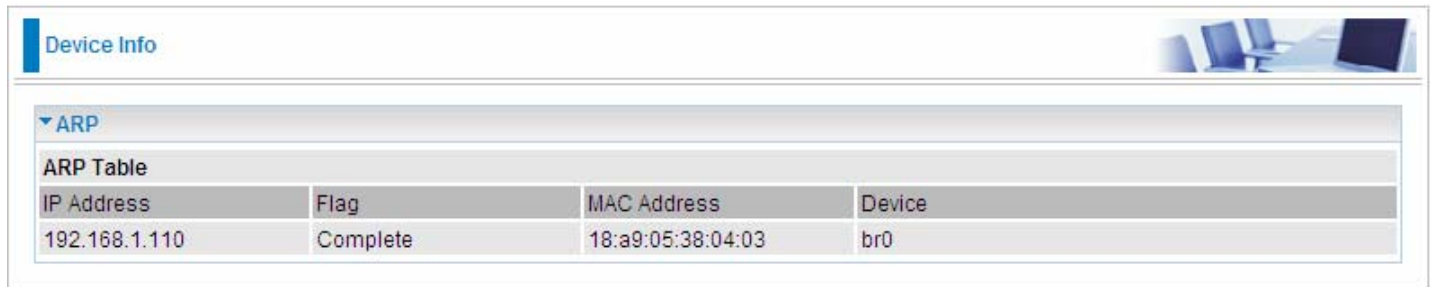
**Metric:** Display the number of hops counted as the Metric of the route.

**Service:** Display the service that this route uses.

**Interface:** Display the existing interface this route uses.

# ARP

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



The screenshot shows a web interface titled "Device Info" with a sub-section for "ARP". Underneath, there is an "ARP Table" with the following data:

IP Address	Flag	MAC Address	Device
192.168.1.110	Complete	18:a9:05:38:04:03	br0

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

**Flag:** Shows the current status of the ARP entries.

- ① Complete: the route resolving is processing well.
- ① M(Marked as permanent entry): the route is permanent.
- ① P (publish entry): publish this route item.

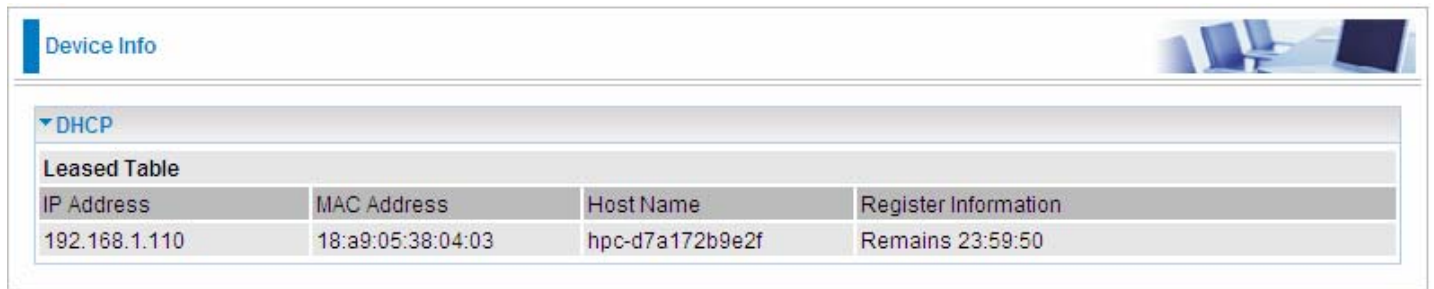
**MAC Address:** Shows the MAC address that is corresponded to the IP address of the device it is mapped to.

**Device:** here refers to the physical interface, it is a concept to identify Clients from LAN or WAN. For example, the Clients in LAN, here displays "br0".



# DHCP

The DHCP Table lists the DHCP lease information for all IP addresses assigned by the DHCP server in the device.



The screenshot shows a web-based interface for network management. At the top left, there is a 'Device Info' tab. Below it, a 'DHCP' section is expanded to show a 'Leased Table'. The table has four columns: 'IP Address', 'MAC Address', 'Host Name', and 'Register Information'. A single row of data is visible, showing the IP address 192.168.1.110, MAC address 18:a9:05:38:04:03, host name hpc-d7a172b9e2f, and a remaining registration time of 23:59:50.

IP Address	MAC Address	Host Name	Register Information
192.168.1.110	18:a9:05:38:04:03	hpc-d7a172b9e2f	Remains 23:59:50

**IP Address:** The IP address which is assigned to the host with this MAC address.

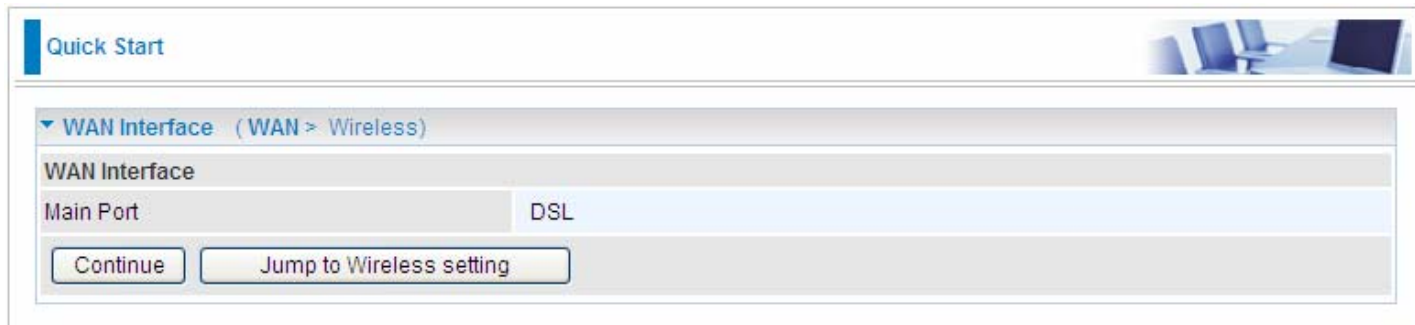
**MAC Address:** The MAC Address of internal DHCP client host.

**Host Name:** The Host Name of DHCP client.

**Register Information:** Show the remaining time information during registration.

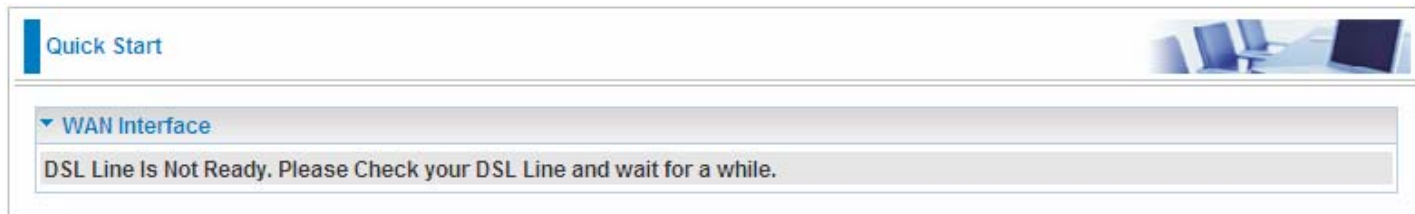
# Quick Start

This part is to let you quickly configure and start your router to access internet.

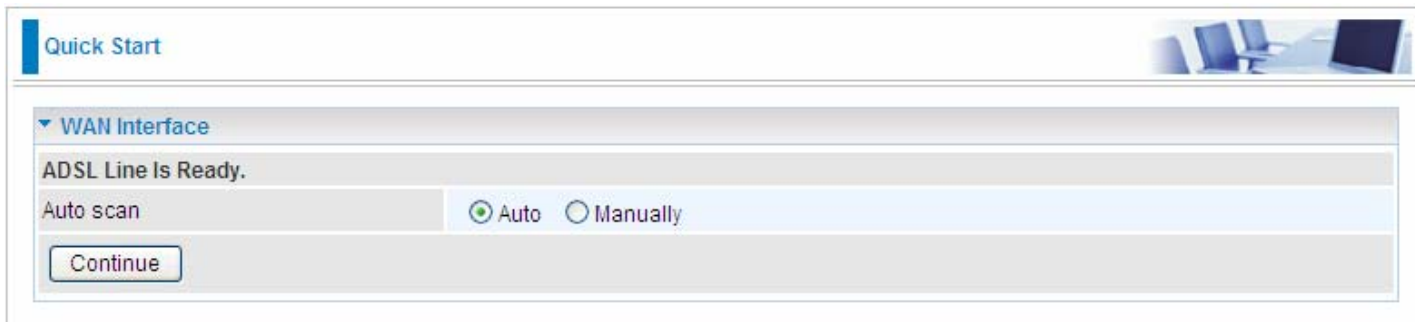


1. To configure DSL, press **Continue** to go on to next step, or if you only want to configure Wireless, press **Jump to Wireless setting** to go to step 8.

2. When ADSL line is not ready, the screen1 below will appear to remind you. Then you should connect the ADSL line. While ADSL line is ready, the screen 2 below will appear to let you go on. Here you can select Auto or Manually. Select Auto will go to step 3, and select manually will go to step 4.

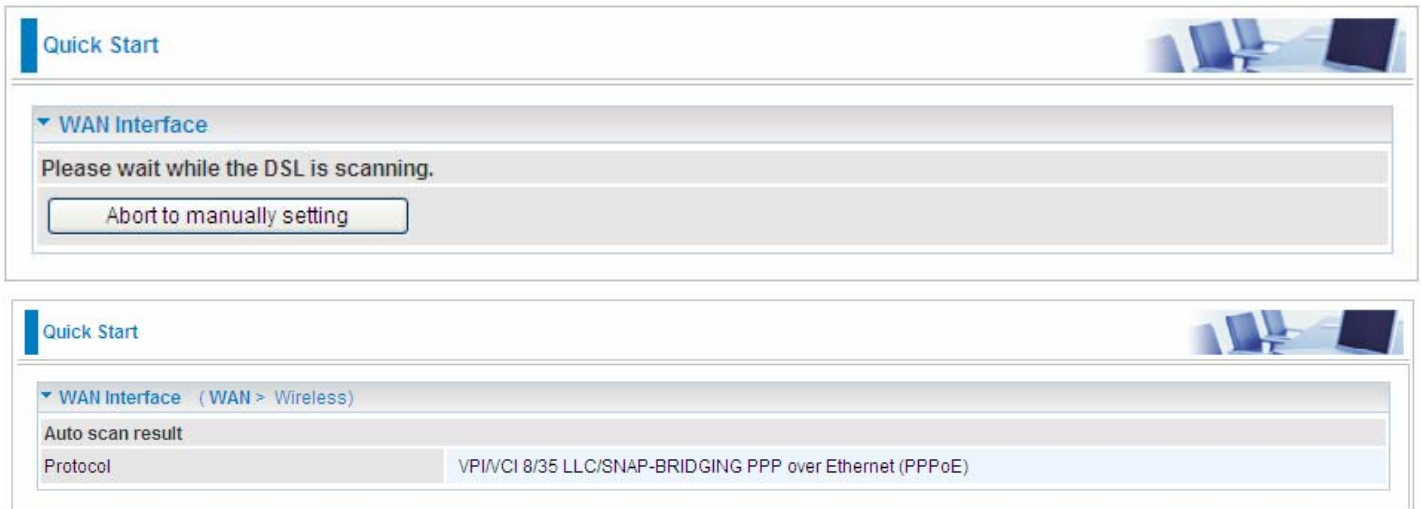


Screen 1



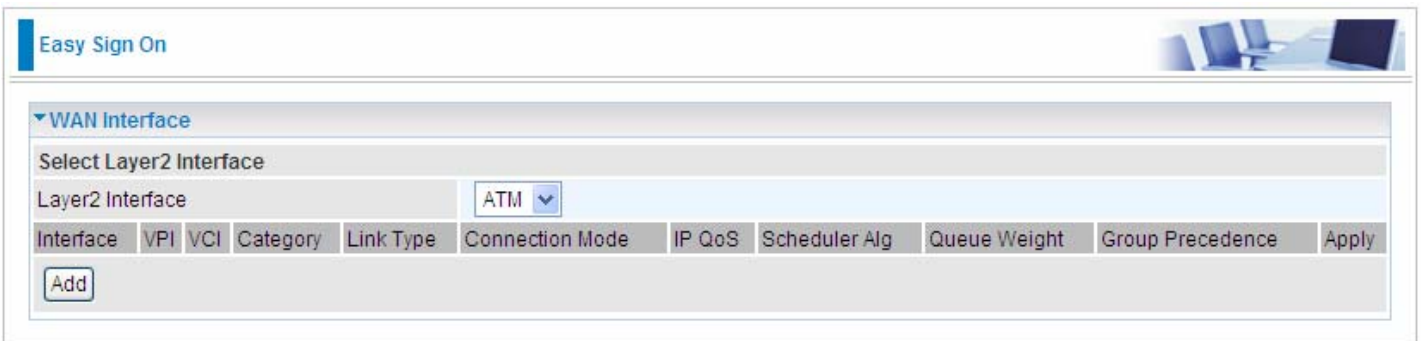
Screen 2

3. Here wait while the DSL is scanning, when the scanning is OK, the scanning result will appear, see screen 3, and then it will quickly goes to step 6. Or you can **Abort to manually setting** to step 4.

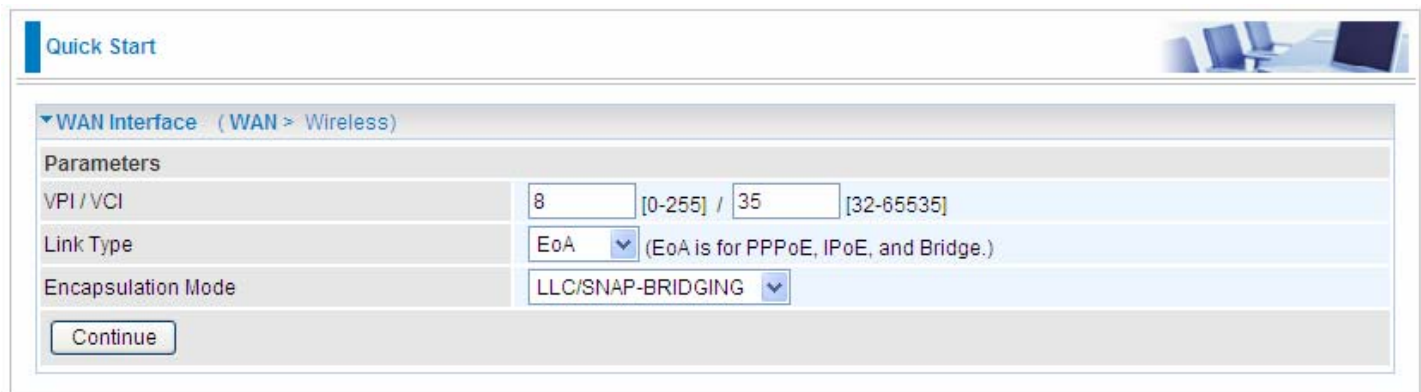


Screen 3

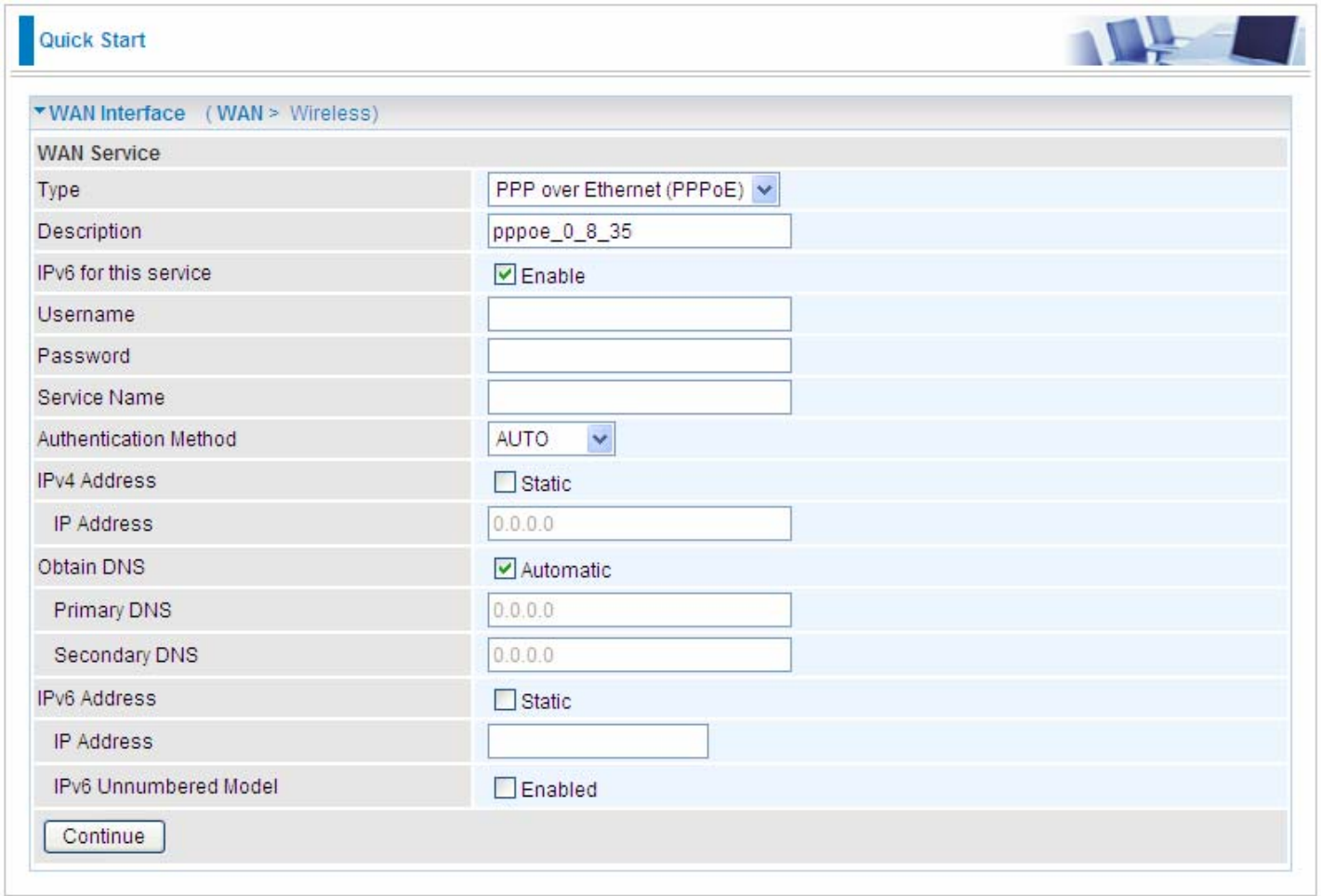
4. Here you should select the Layer2 Interface. ATM and PTM are two kinds of transmission mode. You can select according to your ISP. Select ATM for example. Click **Add** to add WAN Interface.



5. Enter the VPI/VCI from your ISP.



6. Enter the username, password from your ISP, for IP and DNS settings, also refer to your ISP. Here IPv6 service is enabled by default.



Quick Start

WAN Interface (WAN > Wireless)

WAN Service

Type	PPP over Ethernet (PPPoE) ▾
Description	pppoe_0_8_35
IPv6 for this service	<input checked="" type="checkbox"/> Enable
Username	<input type="text"/>
Password	<input type="text"/>
Service Name	<input type="text"/>
Authentication Method	AUTO ▾
IPv4 Address	<input type="checkbox"/> Static
IP Address	0.0.0.0
Obtain DNS	<input checked="" type="checkbox"/> Automatic
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
IPv6 Address	<input type="checkbox"/> Static
IP Address	<input type="text"/>
IPv6 Unnumbered Model	<input type="checkbox"/> Enabled

7. Wait while the device is configured.



Quick Start

WAN Interface

Please wait while the device is configured.

8. WAN port configuration is success.



Quick Start

WAN Interface (WAN > Wireless)

Congratulations !

Your WAN port has been successfully configured.

9. After the configuration is successful, click **Next to Wireless** button and you may proceed to configure the Wireless setting. For security information, please turn to **wireless>security** section in this manual for help.

The screenshot shows the 'Quick Start' configuration page for the Wireless section. The page title is 'Quick Start' and the breadcrumb is '(WAN > Wireless)'. Under the 'Parameters' section, the following settings are visible:

- Wireless:  Enable
- SSID: wlan-ap
- Channel: 1
- Auto Channel Timer(min): 0
- Network Authentication: Open
- WEP Encryption: Disable

A 'Continue' button is located at the bottom left of the configuration area.

10. Configuration's success.

The screenshot shows the 'Quick Start' configuration page after successful completion. The page title is 'Quick Start' and the breadcrumb is '(WAN > Wireless)'. A message box titled 'Process finished' displays the text 'Success.'.

Then you successfully quick configured your router and can access the internet, turn to Device Info, you will see the basic information.

The screenshot shows the 'Device Info' page. The page title is 'Device Info' and the breadcrumb is '(WAN > Device Info)'. The page is divided into two sections:

**Device Information**

Model Name	BiPAC 7800NL
Host Name	home.gateway
System Up-Time	1 Hour(s) 52 min(s)
Date/Time	Wed Aug 18 13:52:09 2010
Software Version	2.02a.dc1
LAN IPv4 Address	192.168.1.254
LAN IPv6 Address	2001:b010:7030:f800:204:edff:fe78:65ab/64
MAC Address	00:04:ed:01:00:01
DSL PHY and Driver Version	A2pD030i.d23a
Wireless Driver Version	5.60.104.0.cpe4.406.0(WLTEST)

**WAN**

Line Rate - Upstream (Kbps)	1024
Line Rate - Downstream (Kbps)	8000
Default Gateway	ppp0
Connection Time	00:00:38
Primary DNS Server	221.6.96.178
Secondary DNS Server	221.6.4.66
Default IPv6 Gateway	ppp0

For more information, turn to **Advanced setup** for help.

# Advanced setup

When you click this item, the column will expand to display the sub-items that will allow you to further configure your router.

[WAN](#), [LAN](#), [NAT](#), [Security](#), [Parental Control](#), [Quality of Service](#), [Routing](#), [DNS](#), [DSL](#), [UPnP](#), [DNS Proxy](#), [Interface Grouping](#), [Certificate](#) and [Multicast](#).



The function of each configuration sub-item is described in the following sections.

# WAN-Wide Area Network

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 the items within the WAN section: [WAN Interface](#) and [WAN Service](#).

## WAN Interface

### ATM

Interface	VPI	VCI	Category	Link Type	Connection Mode	IP QoS	Scheduler Alg	Queue Weight	Group Precedence	Remove
-----------	-----	-----	----------	-----------	-----------------	--------	---------------	--------------	------------------	--------

**Layer2 Interface:** 2 transfer mode, ATM or PTM.

The following is the interface listing table.  
Click **Add** to add WAN interface.

Parameters

This screen allows you to configure an ATM PVC identifier (VPI and VCI), select DSL latency, select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.

VPI / VCI: 8 [0-255] / 35 [32-65535]

Link Type: EoA (EoA is for PPPoE, IPoE, and Bridge.)

Connection Mode: Default Mode - Single service over one connection

Encapsulation Mode: LLC/SNAP-BRIDGING

Service Category: UBR Without PCR

IP QoS Scheduler Algorithm:  Strict Priority  Weighted Fair Queuing

Precedence of the default queue: 8 (lowest)

**VCI/VPI:** enter the VCI/VPI from your ISP.

**Link Type:** select the link type (protocol), EOA, PPPoA, IPoA.

**Connection Mode:**

- ① **Default Mode:** this mode only allows single service over one connection.
- ① **VLAN MUX Mode:** this mode allows multiple services over one PVC.

The two modes can be different in WAN service configuration. And PPPoA and IPoA do not use Ethernet frames for data transfer so they cannot work with VLAN Mux feature. Thus, **Connection**

**Mode** Parameter will be hidden if you select PPPoA or IPoA in Link Type.

**Encapsulation Mode:** select the encapsulation mode from the drop-down menu according to the link Type.

**Service Category:** select the service category from the drop-down menu to determine your service category.

① **UBR without PCR: UBR(Unspecified Bit Rate), PCR(Peak cell Rate)**

UBR is a kind of QoS, which doesn't provide assurance about the cell latency, the bit loss rate etc, it is a best-effort service.

Service Category	UBR Without PCR
IP QoS Scheduler Algorithm	<input checked="" type="radio"/> Strict Priority <input type="radio"/> Weighted Fair Queuing
Precedence of the default queue	8 (lowest)
<input type="button" value="Back"/> <input type="button" value="Apply"/>	

**IP QoS Schedule Algorithm:** select the Schedule Algorithm, SP(Strict Priority), always sends the packets with the highest priority, WFQ(Weighted Fair Queuing), an automatically bandwidth adjusting method, sharing the available bandwidth when congestion happens, the bandwidth is assigned according to the priority and the weight value. Turn to the **Quality of Service > Queue Config** section for more information.

**Precedence of the default queue:** default 8(lowest)

Service Category	UBR Without PCR
IP QoS Scheduler Algorithm	<input type="radio"/> Strict Priority <input checked="" type="radio"/> Weighted Fair Queuing
Weight Value of the default queue	1 [1-63]
MPAAL Group Precedence	8
<input type="button" value="Back"/> <input type="button" value="Apply"/>	

**Weight Value of default queue:** enter the value, 1-63, the highest is 63.

**MPAAL Group Precedence:** select the precedence identification, 1-8, the highest is 1.

① **UBR with PCR/ CBR(Constant Bit Rate)**

UBR is a kind of service providing constant rate service, is idea for timely and fixed bandwidth needed service.

Service Category	UBR With PCR
Peak Cell Rate	<input type="text"/> cells/s [1-2613]
<input type="button" value="Back"/> <input type="button" value="Apply"/>	

**Peak Cell Rate:** enter Peak Cell Rate.



### ① None Realtime VBR/ Realtime VBR(Variable Bit Rate)

VBR is a kind of service providing some assurance about latency and bit loss rate and is often associated with video and time sensitive service. NR-VBR allows more time delay to R-VBR.

Service Category	Realtime VBR	
Peak Cell Rate	<input type="text"/>	cells/s [1-2613]
Sustainable Cell Rate	<input type="text"/>	cells/s c [1-2613]
Maximum Burst Size	<input type="text"/>	cells [1-1000000]
<input type="button" value="Back"/> <input type="button" value="Apply"/>		

Enter Peak Cell Rate, Sustainable Cell Rate and Maximum Burst Rate.

Click **Apply** to apply the WAN interface.

Advanced Setup

WAN Interface

ATM Interface

Layer2 Interface: ATM

Interface	VPI	VCI	Category	Link Type	Connection Mode	IP QoS	Scheduler Alg	Queue Weight	Group Precedence	Remove
atm0	8	35	UBR	EoA	DefaultMode	Enabled	SP			<input type="checkbox"/>

Check the remove checkbox, then press **Remove** to delete it only if this interface are not used by a WAN Service, if it is used by a WAN service, first remove the WAN service, then turn back to remove the interface.


Don't feel confused, it will remind you by the following prompt window.

Error

Configuration Error

You CANNOT remove this DSL Interface if it is used by a WAN Service.  
You need to remove the WAN Service before you can remove this DSL interface.

PTM Setting is similar to ATM.


Advanced Setup 

▼ WAN Interface

PTM Interface

Layer2 Interface PTM ▼

Interface	PTM Priority	Connection Mode	IP QoS	Scheduler Alg	Queue Weight	Group Precedence	Remove
<span>Add</span> <span>Remove</span>							

Advanced Setup 

▼ PTM Interface -- PTM Configuration

Parameters

PTM Priority  Normal  High (Preemption)

Connection Mode Default Mode - Single service over one connection ▼


IP QoS Scheduler Algorithm  Strict Priority  Weighted Fair Queuing

Precedence of the default queue 8 (lowest)

Back Apply

**PTM Priority:** Select the PTM priority, Normal or High.

Click **Apply** to save your settings. The interface will be added to the PTM Interface listing table.

Advanced Setup 


▼ WAN Interface

PTM Interface

Layer2 Interface PTM ▼

Interface	PTM Priority	Connection Mode	IP QoS	Scheduler Alg	Queue Weight	Group Precedence	Remove
ptm0	Normal	DefaultMode	Enabled	SP			<input type="checkbox"/>
<span>Add</span> <span>Remove</span>							

Now follow the above steps, we set two ATM WAN interfaces for future illustration, one is of DefaultMode, and one is of VlanMuxMode.

Advanced Setup 

▼ WAN Interface

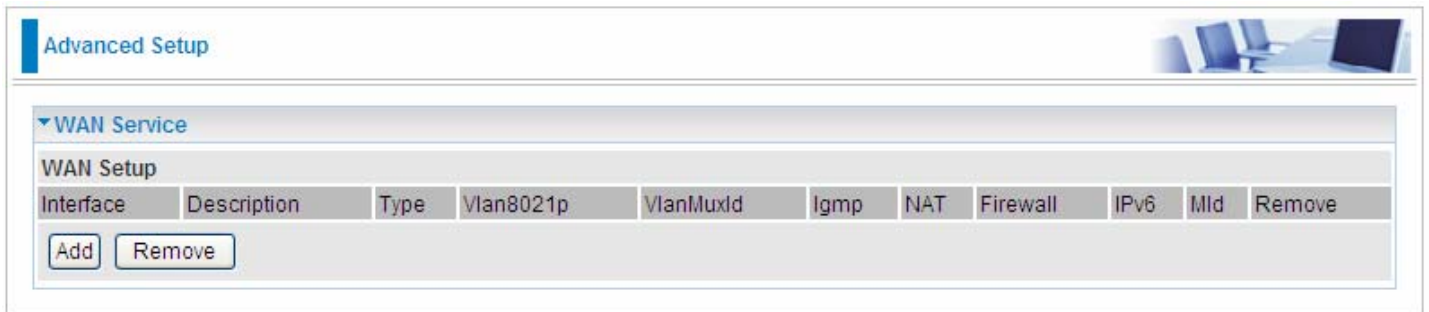
ATM Interface

Layer2 Interface ATM ▼

Interface	VPI	VCI	Category	Link Type	Connection Mode	IP QoS	Scheduler Alg	Queue Weight	Group Precedence	Remove
atm0	8	35	UBR	EoA	DefaultMode	Enabled	SP			<input type="checkbox"/>
atm1	1	35	UBR	EoA	VlanMuxMode	Enabled	SP			<input type="checkbox"/>

## WAN Service

WAN Service allows you configure one or more services over one interface (connection). The following is the WAN Service listing table. Your configured WAN service will be listed here.



The screenshot shows the 'Advanced Setup' interface with a 'WAN Service' section. Below the section title is a 'WAN Setup' table with columns: Interface, Description, Type, Vlan8021p, VlanMuxId, Igmp, NAT, Firewall, IPv6, MId, and Remove. Below the table are 'Add' and 'Remove' buttons.

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	MId	Remove
-----------	-------------	------	-----------	-----------	------	-----	----------	------	-----	--------

## Default Connection mode

Select the interface which is a Default mode connection configured in WAN Service, here for example, in the following, atm0/(0\_8\_35) is a Default mode connection.

Click **Add** to create one WAN service.



The screenshot shows the 'Advanced Setup' interface with a 'WAN Service' section. Below the section title is a 'WAN Service Interface Configuration' form. It contains a note about descriptor strings for ATM and PTM interfaces, followed by a list of options for portId and low/high PTM priority. The 'Interface' field is a dropdown menu currently showing 'atm0/(0\_8\_35)'. Below the form are 'Back' and 'Next' buttons.

Note: For ATM interface, the descriptor string is (portId\_vpi\_vci)  
For PTM interface, the descriptor string is (portId\_high\_low)  
Where portId=0 --> DSL Latency PATH0  
portId=1 --> DSL Latency PATH1  
portId=4 --> DSL Latency PATH0&1  
low =0 --> Low PTM Priority not set  
low =1 --> Low PTM Priority set  
high =0 --> High PTM Priority not set  
high =1 --> High PTM Priority set

Interface: atm0/(0\_8\_35)

Select the interface, the listed interfaces are the one you configured in WAN interface section. Click **Next** to further configure.

**Advanced Setup**

▼ WAN Service

Parameters

Type	PPP over Ethernet (PPPoE) ▼
Description	pppoe_0_8_35
IPv6 for this service	<input type="checkbox"/> Enable

Back Next

**Type:** select the protocol advised by your ISP, here select PPPoE.

**Description:** user-defined description.

**IPv6 for this service:** check whether to enable IPv6 for this service.

Click **Next** to go on. See [IPv6 enabled](#) and [IPv6 disabled](#).

### IPv6 enabled

**Advanced Setup**

▼ WAN Service

Parameters

Username	<input type="text"/>
Password	<input type="text"/>
Service Name	<input type="text"/>
Authentication Method	AUTO ▼
Fullcone NAT	<input type="checkbox"/> Enable
Dial on demand	<input type="checkbox"/> Enable
Inactivity Timeout	0 (minutes) [1-4320]
IPv4 Address	<input type="checkbox"/> Static
IP Address	0.0.0.0
Obtain DNS	<input checked="" type="checkbox"/> Automatic
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>
IPv6 Address	<input type="checkbox"/> Static
IP Address	<input type="text"/>
IPv6 Unnumbered Model	<input type="checkbox"/> Enabled
PPP Debug Mode	<input type="checkbox"/> Enable
Bridge PPPoE Frames Between WAN and Local Ports	<input type="checkbox"/> Enable
IGMP Multicast Proxy	<input type="checkbox"/> Enable
MLD Multicast Proxy	<input type="checkbox"/> Enable

Back Next

**Username:** enter ISP account.

**Password:** enter the password.

**Service name:** user-defined name.

**Authentication method:** select the authentication method.

**Fullcone NAT:** enable or disable fullcone NAT. Fullcone is a kind of NAT, in this mode, all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address.

**Note:** In PPPoE connection, NAT is enabled by default, you can determine whether to enable Fullcone NAT. And while you disabled Fullcone NAT and only use NAT, the default NAT type is Port Restricted cone NAT. Of Port-Restricted cone NAT, the restriction includes port numbers. Specifically, an external host can send a packet, with source IP address X and source port P, to the internal host only if the internal host had previously sent a packet to IP address X and port P

**Dial on demand:** enable or disable, if you want to Dial on demand, enable this function.

**Inactivity timeout:** available when you enable Dial on demand function. Enter the **Inactivity timeout** interval.

**IPv4 Address:** enable or disable to assign static IPv4 address to PPPoE link.

**IP Address:** enter the Static IPv4 address if you enable Static IP Address.

**Obtain DNS:** check whether to obtain DNS address automatically.

**Primary/Secondary DNS:** if you uncheck Obtain DNS, then enter then primary/secondary DNS address.

**IPv6 Address:** enable to assign static IPv6 address, else to obtain Ipv6 address automatically.

**IP Address:** enter the Static IPv6 address if you enable Static IPv6 Address.

**IPv6 Unnumbered Model:** Enables or disables IPv6 processing on an interface without assigning an explicit IPv6 address to that interface.

**Note:** Suggest having IPv6 configured as default, this router can automatically assign address to your PC, or you can have an advanced administrator to help.

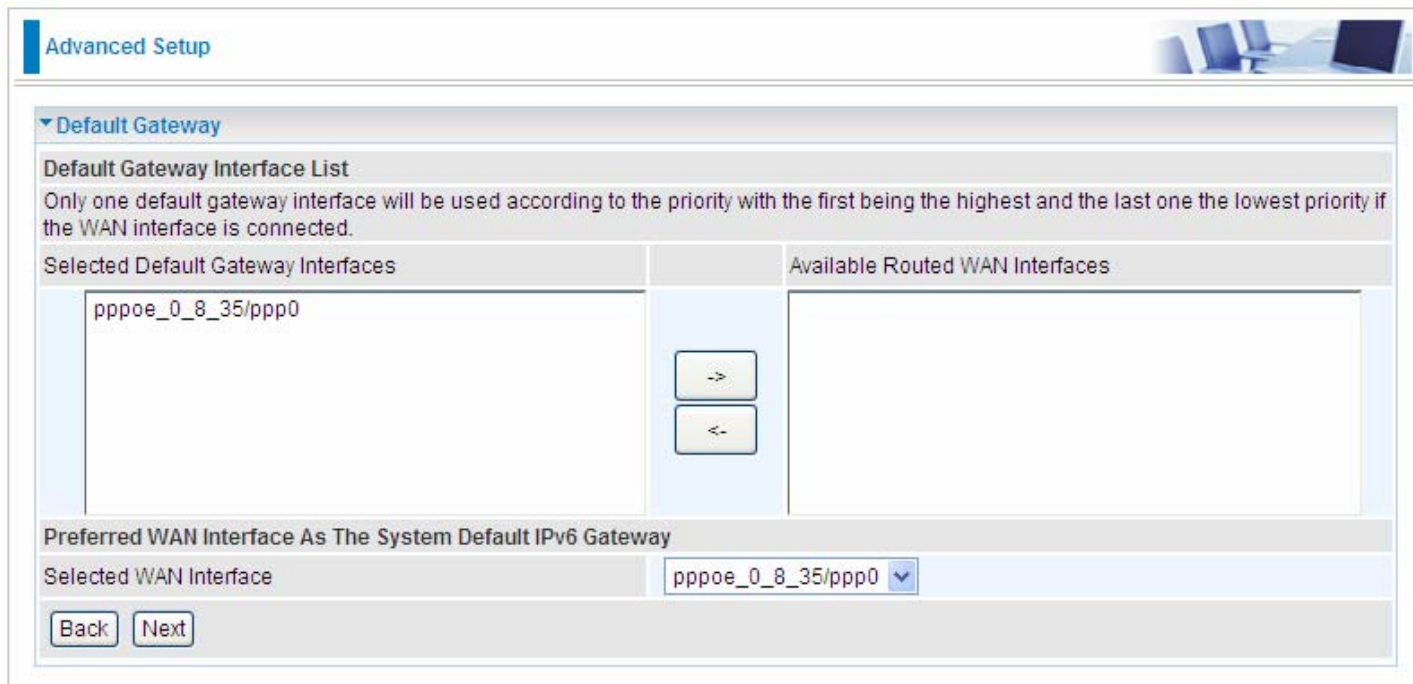
**PPPoE Debug mode:** check whether to enable this function, it is used to debug PPPoE link, and the debug message will be seen in **System log**.

**Bridge PPPoE Frame between WAN and Local Ports:** check whether to enable this function. It allows PC in LAN to set up its own PPP link, or the PC will access internet via the PPP link in WAN port.

**IGMP Multicast Proxy:** check whether to enable this function. IGMP (**I**nternet **G**roup **M**anagement Protocol) Proxy intercepts the IGMP request from Clients and forwards it to the router after some dealings.

**MLD Multicast Proxy:** check whether to enable this function. MLD (**M**ulticast **L**istener **D**iscovery Protocol) Proxy intercepts the MLD request from Clients and forwards it to the router after some dealings. Support MLDv1 and MLDv2.

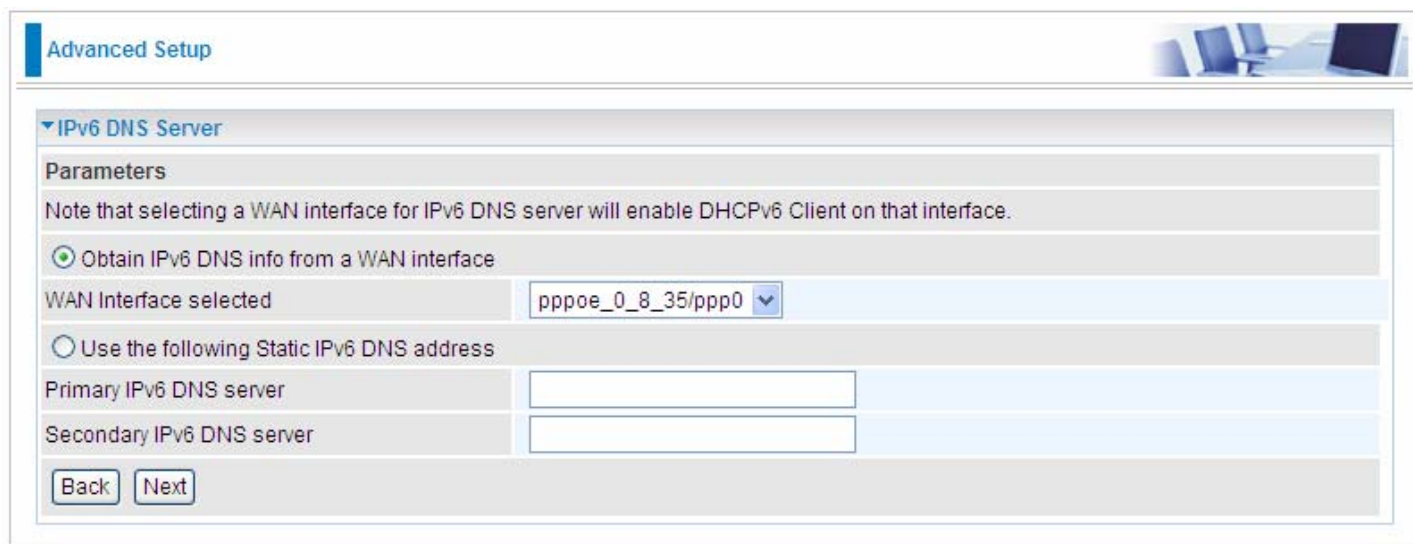
Click **Next** to go on to the Default Gateway setting.



The screenshot shows the 'Advanced Setup' page for 'Default Gateway'. It features a section titled 'Default Gateway Interface List' with a note: 'Only one default gateway interface will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected.' Below this is a table with two columns: 'Selected Default Gateway Interfaces' and 'Available Routed WAN Interfaces'. The 'Selected' column contains 'pppoe\_0\_8\_35/ppp0'. Between the columns are two buttons: a right-pointing arrow and a left-pointing arrow. Below the table is a section titled 'Preferred WAN Interface As The System Default IPv6 Gateway' with a dropdown menu for 'Selected WAN Interface' set to 'pppoe\_0\_8\_35/ppp0'. At the bottom are 'Back' and 'Next' buttons.

Set the default gateway and the default IPv6 gateway.

Click **Next** to go on to IPv6 DNS Server setting.



The screenshot shows the 'Advanced Setup' page for 'IPv6 DNS Server'. It features a section titled 'Parameters' with a note: 'Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface.' Below this are two radio button options. The first option, 'Obtain IPv6 DNS info from a WAN interface', is selected. Below it is a dropdown menu for 'WAN Interface selected' set to 'pppoe\_0\_8\_35/ppp0'. The second option, 'Use the following Static IPv6 DNS address', is unselected. Below it are two text input fields for 'Primary IPv6 DNS server' and 'Secondary IPv6 DNS server'. At the bottom are 'Back' and 'Next' buttons.

IPv6 DNS Server's operation is similar to IPv4 DNS server. There are two modes to get DNS server address: Auto and static mode.

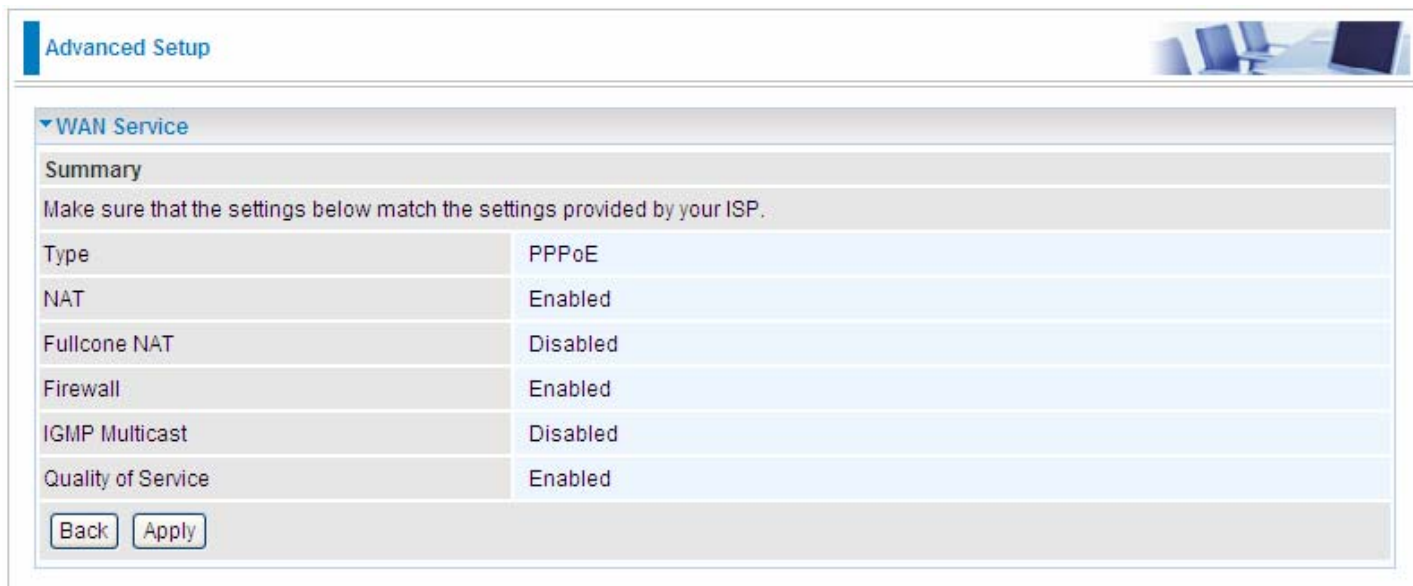
### Obtain IPv6 DNS info from a WAN interface

**WAN Interface selected:** select one configured IPv6 WAN connection from the drop-down menu to be as an IPv6 DNS.

### Use the following Static IPv6 DNS address

**Primary IPv6 DNS Server / Secondary IPv6 DNS Server:** type the specific primary and secondary IPv6 DNS Server address.

Click **Next** to check the settings.



**Advanced Setup**

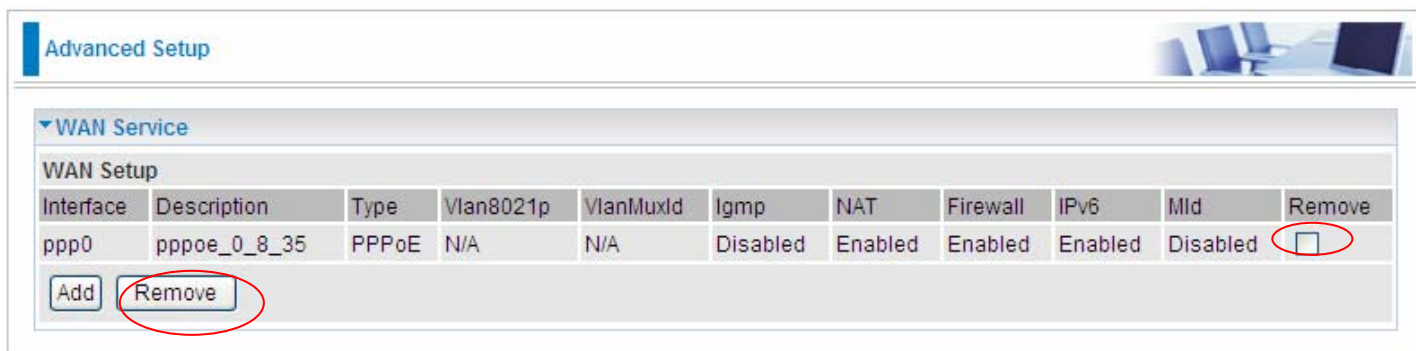
▼ WAN Service

**Summary**

Make sure that the settings below match the settings provided by your ISP.

Type	PPPoE
NAT	Enabled
Fullcone NAT	Disabled
Firewall	Enabled
IGMP Multicast	Disabled
Quality of Service	Enabled

If you confirm, click Apply to submit the settings and return to WAN service page.



**Advanced Setup**

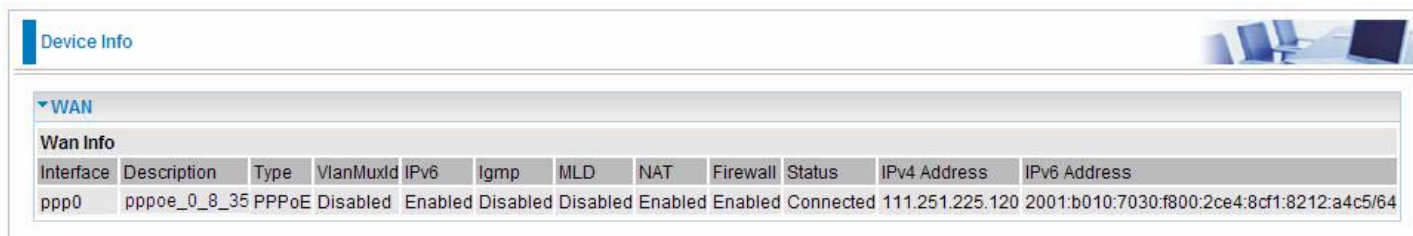
▼ WAN Service

**WAN Setup**

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Remove
ppp0	pppoe_0_8_35	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Disabled	<input type="checkbox"/>

If you do not need the service, select the item you want to remove, check the checkbox, then press **Remove**, it will be OK.

Here the corresponding WAN interface and WAN Service have been configured, if it is OK, you can access the internet. You can go to **Device Info>WAN** or **Summary** to view the WAN connection information (if your ISP provides IPv6 service, then you will obtain an IPv6 address).



**Device Info**

▼ WAN

**Wan Info**

Interface	Description	Type	VlanMuxId	IPv6	Igmp	MLD	NAT	Firewall	Status	IPv4 Address	IPv6 Address
ppp0	pppoe_0_8_35	PPPoE	Disabled	Enabled	Disabled	Disabled	Enabled	Enabled	Connected	111.251.225.120	2001:b010:7030:f800:2ce4:8cf1:8212:a4c5/64



## The device summary information

Device Info	
<b>▼ Device Information</b>	
Model Name	BiPAC 7800NL
Host Name	home.gateway
System Up-Time	1 Hour(s) 52 min(s)
Date/Time	Wed Aug 18 13:52:09 2010
Software Version	2.02a.dc1
LAN IPv4 Address	192.168.1.254
LAN IPv6 Address	2001:b010:7030:f800:204:edff:fe78:65ab/64
MAC Address	00:04:ed:01:00:01
DSL PHY and Driver Version	A2pD030i.d23a
Wireless Driver Version	5.60.104.0.cpe4.406.0(WLTEST)
<b>▼ WAN</b>	
Line Rate - Upstream (Kbps)	1024
Line Rate - Downstream (Kbps)	8000
Default Gateway	ppp0
Connection Time	00:00:38
Primary DNS Server	221.6.96.178
Secondary DNS Server	221.6.4.66
Default IPv6 Gateway	ppp0

## IPv6 disabled

Advanced Setup

WAN Service

Parameters

Username	<input type="text"/>
Password	<input type="text"/>
Service Name	<input type="text"/>
Authentication Method	AUTO <input type="button" value="v"/>
Fullcone NAT	<input type="checkbox"/> Enable
Dial on demand	<input type="checkbox"/> Enable
Inactivity Timeout	<input type="text" value="0"/> (minutes) [1-4320]
IPv4 Address	<input type="checkbox"/> Static
IP Address	<input type="text" value="0.0.0.0"/>
Obtain DNS	<input checked="" type="checkbox"/> Automatic
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>
PPP Debug Mode	<input type="checkbox"/> Enable
Bridge PPPoE Frames Between WAN and Local Ports	<input type="checkbox"/> Enable
IGMP Multicast Proxy	<input type="checkbox"/> Enable

**Username:** enter ISP account.

**Password:** enter the password.

**Service name:** user-defined name.

**Authentication method:** select the authentication method.

**Fullcone NAT:** enable or disable fullcone NAT. Fullcone is a kind of NAT, in this mode, all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address.

**Note:** In PPPoE connection, NAT is enabled by default, you can determine whether to enable Fullcone NAT. And while you disabled Fullcone NAT and only use NAT, the default NAT type is Port Restricted cone NAT. Of Port-Restricted cone NAT, the restriction includes port numbers. Specifically, an external host can send a packet, with source IP address X and source port P, to the internal host only if the internal host had previously sent a packet to IP address X and port P

**Dial on demand:** enable or disable, if you want to Dial on demand, enable this function.

**Inactivity timeout:** available when you enable Dial on demand function. Enter the **Inactivity timeout** interval.

**IPv4 Address:** enable or disable to assign static IP address to PPPoE link.

**IP Address:** enter the Static IP address if you enable Static IP Address.

**Obtain DNS:** check whether to obtain DNS address automatically.

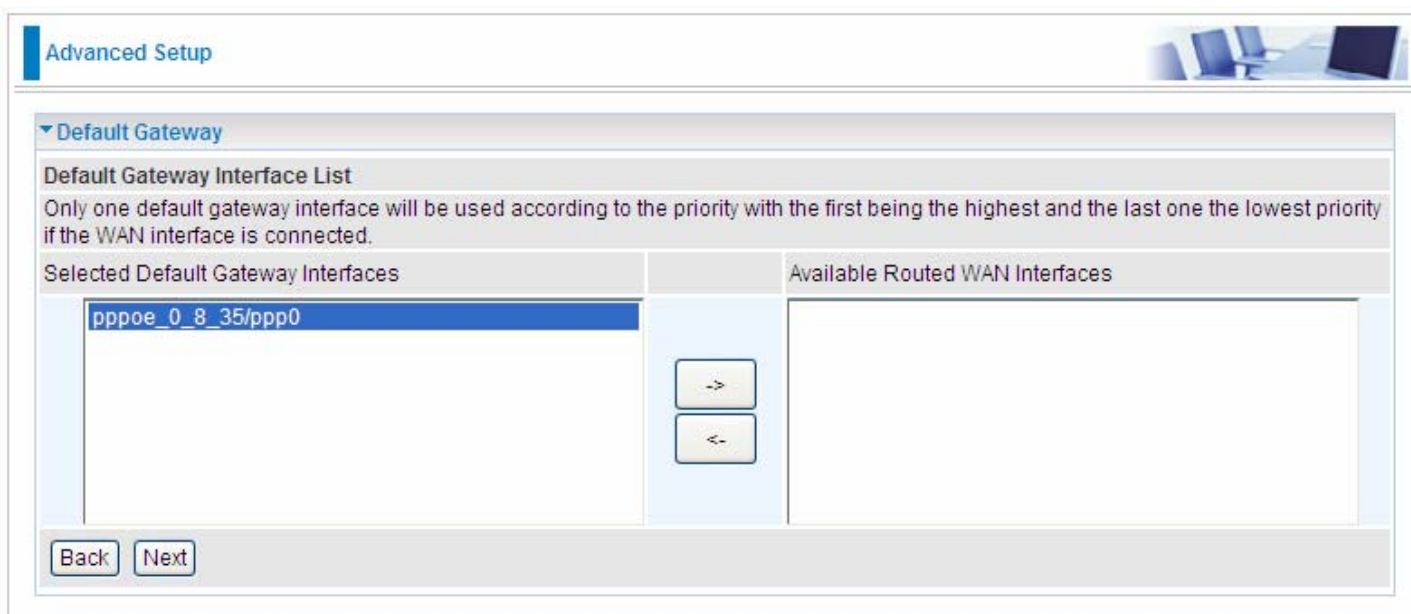
**Primary/Secondary DNS:** if you uncheck Obtain DNS, then enter then primary/secondary DNS address.

**PPPoE Debug mode:** check whether to enable this function, it is used to debug PPPoE link, and the debug message will be seen in **System log**.

**Bridge PPPoE Frame between WAN and Local Ports:** check whether to enable this function. It allows PC in LAN to set up its own PPP link, or the PC will access internet via the PPP link in WAN port.

**IGMP Multicast Proxy:** check whether to enable this function. IGMP (Internet Group Management Protocol) Proxy intercept the IGMP request from Clients and forward it to the router after some dealings.

Click **Next** to go on to the Default Gateway setting.



Advanced Setup

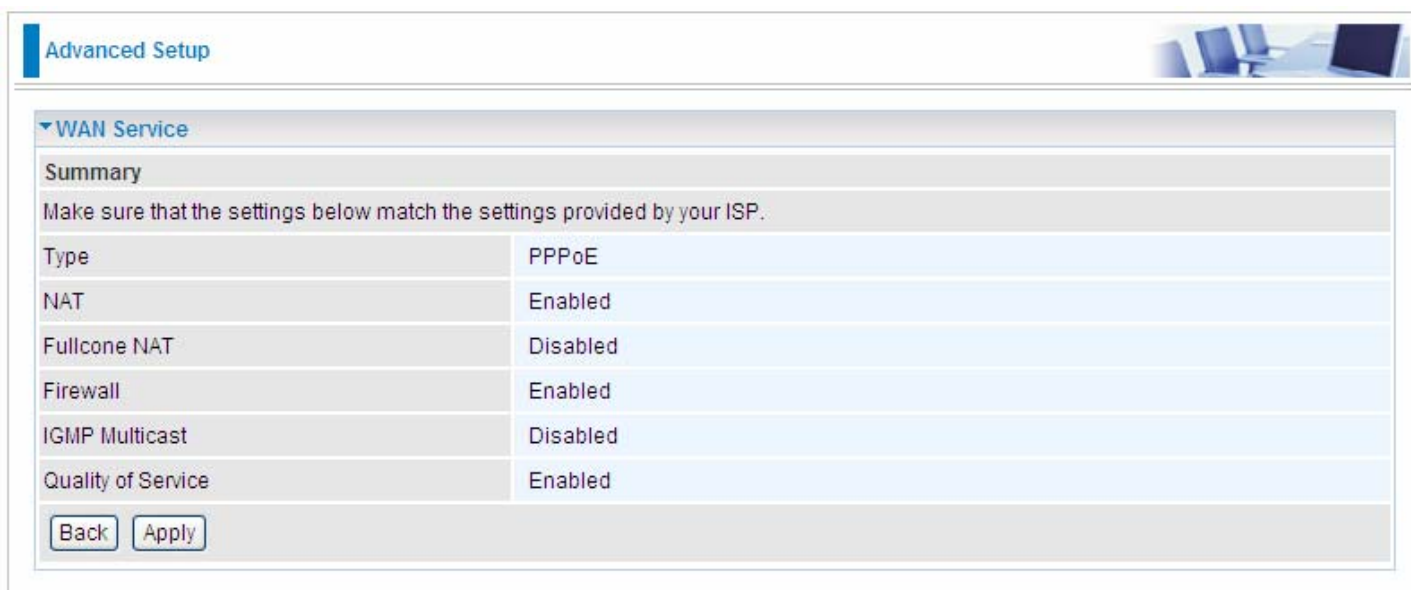
▼ Default Gateway

**Default Gateway Interface List**  
Only one default gateway interface will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected.

Selected Default Gateway Interfaces	Available Routed WAN Interfaces
pppoe_0_8_35/ppp0	

Back Next

Click **Next** to go on. Then you can view the information about your settings.



Advanced Setup

▼ WAN Service

**Summary**  
Make sure that the settings below match the settings provided by your ISP.

Type	PPPoE
NAT	Enabled
Fullcone NAT	Disabled
Firewall	Enabled
IGMP Multicast	Disabled
Quality of Service	Enabled

Back Apply

If you confirm about the above settings, click **Apply** to apply your settings. Then the service will be listed as follows.

**Advanced Setup**

▼ WAN Service

WAN Setup

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Remove
ppp0	pppoe_0_8_35	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Disabled	Disabled	<input type="checkbox"/>

Add Remove

If you do not need the service, select the item you want to remove, check the checkbox, then press **Remove**, it will be OK.

Here the corresponding WAN interface and WAN Service have been configured, if it is OK, you can access the internet. You can go to **Device Info>WAN** or **Summary** to view the WAN connection information.

**Device Info**

▼ WAN

Wan Info

Interface	Description	Type	VlanMuxId	IPv6	Igmp	MLD	NAT	Firewall	Status	IPv4 Address	IPv6 Address
ppp0	pppoe_0_8_35	PPPoE	Disabled	Disabled	Disabled	Disabled	Enabled	Enabled	Connected	112.80.156.130	

**Device Info**

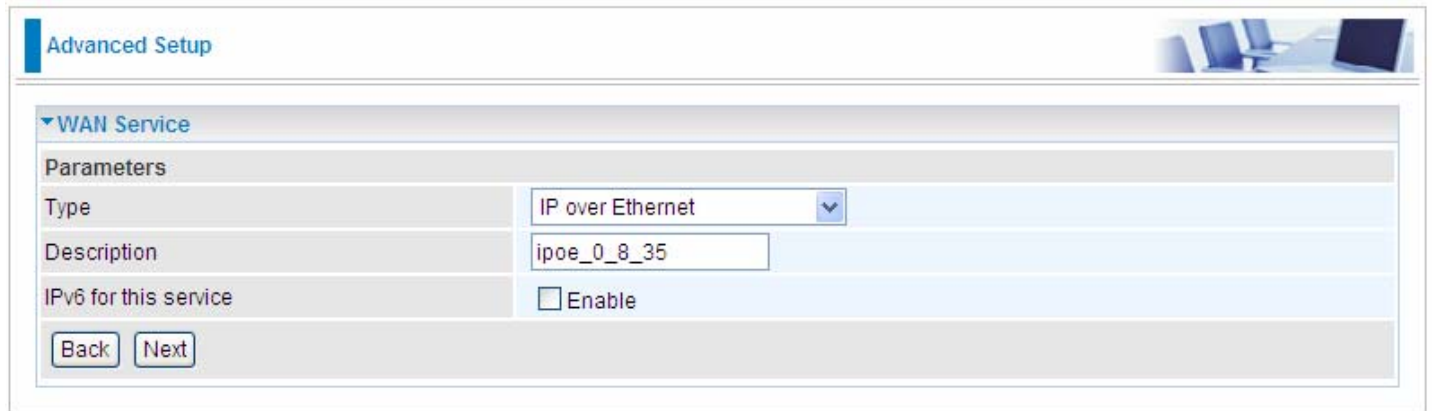
▼ Device Information

Model Name	BIPAC 7800NL
Host Name	home.gateway
System Up-Time	1 Hour(s) 56 min(s)
Date/Time	Wed Aug 18 13:56:36 2010
Software Version	2.02a.dc1
LAN IPv4 Address	192.168.1.254
LAN IPv6 Address	fe80:0000:0000:0000:0204:edff:fe01:0001/64
MAC Address	00:04:ed:01:00:01
DSL PHY and Driver Version	A2pD030i.d23a
Wireless Driver Version	5.60.104.0.cpe4.406.0(WLTEST)

▼ WAN

Line Rate - Upstream (Kbps)	1024
Line Rate - Downstream (Kbps)	8000
Default Gateway	ppp0
Connection Time	00:01:04
Primary DNS Server	221.6.96.178
Secondary DNS Server	221.6.4.66
Default IPv6 Gateway	

## IP over Ethernet



Advanced Setup

WAN Service

Parameters

Type	IP over Ethernet
Description	ipoe_0_8_35
IPv6 for this service	<input type="checkbox"/> Enable

Back Next

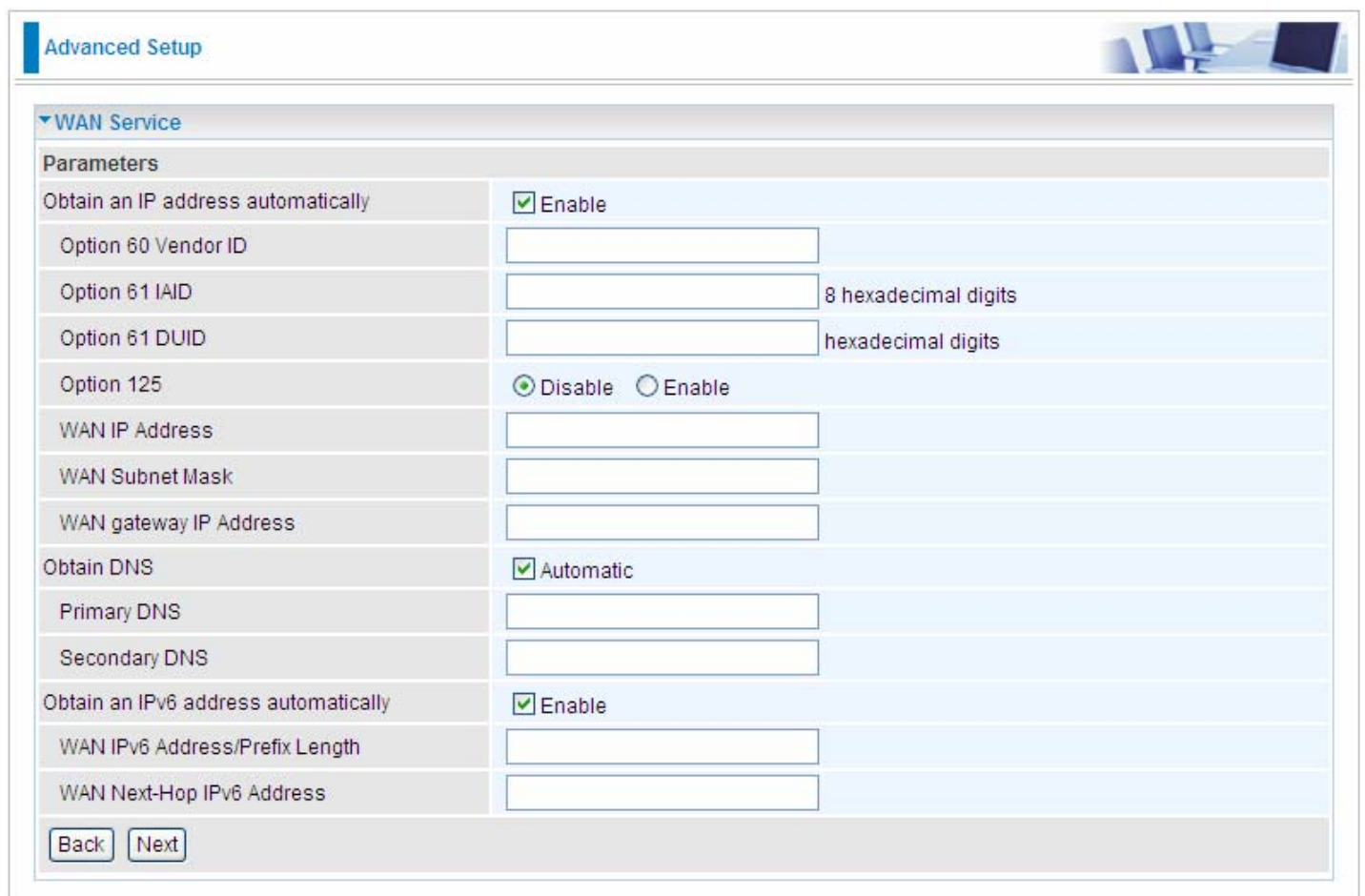
**Type:** Select IP over Ethernet.

**Description:** You are allowed to enter the user defined name for this service.

**IPv6 for this service:** check whether to enable IPv6 feature.

Click **Next** to go to next step. See [IPv6 enabled](#) and [IPv6 disabled](#).

### IPv6 enabled



Advanced Setup

WAN Service

Parameters

Obtain an IP address automatically	<input checked="" type="checkbox"/> Enable
Option 60 Vendor ID	<input type="text"/>
Option 61 IAID	<input type="text"/> 8 hexadecimal digits
Option 61 DUID	<input type="text"/> hexadecimal digits
Option 125	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
WAN IP Address	<input type="text"/>
WAN Subnet Mask	<input type="text"/>
WAN gateway IP Address	<input type="text"/>
Obtain DNS	<input checked="" type="checkbox"/> Automatic
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>
Obtain an IPv6 address automatically	<input checked="" type="checkbox"/> Enable
WAN IPv6 Address/Prefix Length	<input type="text"/>
WAN Next-Hop IPv6 Address	<input type="text"/>

Back Next

Here two modes are supported for users to deal with the IP and DNS. You can select obtain automatically or manually input the information according to your ISP.

**Obtain an IP address automatically:** check whether to enable this function.

**Option 60 Vendor ID:** Enter the associated information by your ISP. This option is used by DHCP clients to optionally identify the vendor type and configuration of a DHCP client. The information is a string of n octets, interpreted by servers. Vendors may choose to define specific vendor class

identifiers to convey particular configuration or other identification information about a client.

**Option 61 IAID:** Enter the associated information provided by your ISP. You should input 8 hexadecimal numbers.

**Option 61 DUID:** Enter the associated information provided by your ISP. You should input hexadecimal number(s).

**Option 125:** Option 125 is a complementary standard of DHCP protocol, it is used to encapsulate option 125 message into DHCP offer packet before forward it to clients. After the clients receive the packet, it check the option 125 field in the packet with the prestored message, if it is matched, then the client accepts this offer, otherwise it will be abandoned. Check Enable or Disable this function. Default setting is Disable.

**WAN IP Address:** Enter your IPv4 address to the device provided by your ISP.

**WAN Subnet Mask:** Enter your submask to the device provided by your ISP.

**WAN gateway IP Address:** Enter your gateway IP address to the device provided by your ISP.

**Obtain DNS:** check whether to enable obtain DNS function.

**Primary/Secondary DNS:** enter the primay/secondary DNS address when you uncheck Obtain DNS checkbox.

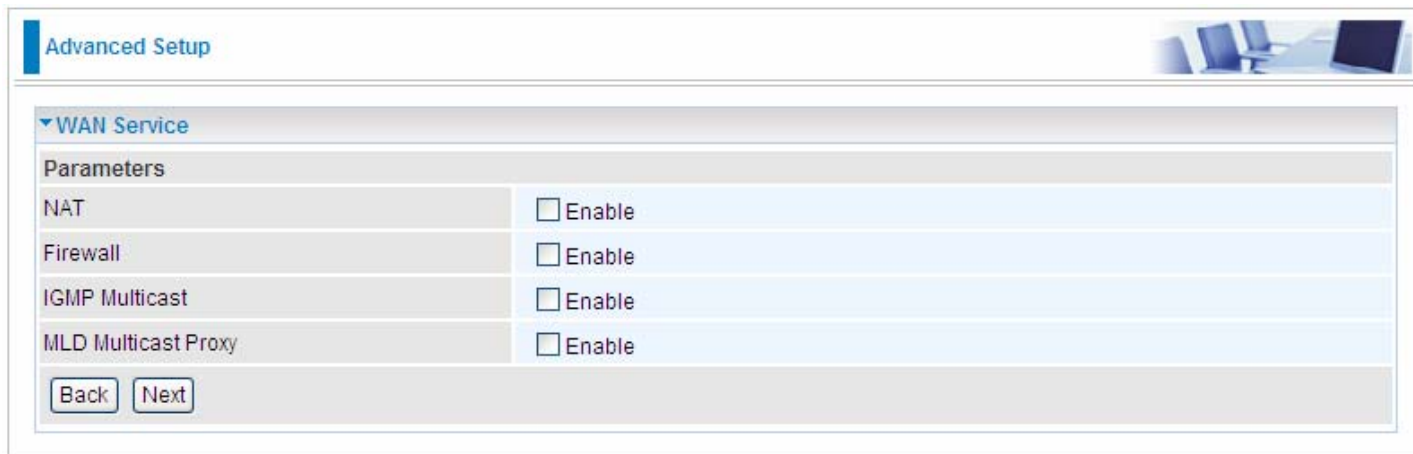
**Obtain an IPv6 address automatically:** check whether to enable or disable this feature.

**WAN IPv6 Address/Prefix Length:** Enter the WAN IPv6 Address/Prefix Length from your ISP.

**WAN Next-Hop IPv6 Address:** Enter the WAN Next-Hop IPv6 Address from your ISP.

**Note:** If you don't know well about the DHCP Option, you can leave it empty or leave it as default.

Click **Next** to go to next step.



Advanced Setup

WAN Service

Parameters	
NAT	<input type="checkbox"/> Enable
Firewall	<input type="checkbox"/> Enable
IGMP Multicast	<input type="checkbox"/> Enable
MLD Multicast Proxy	<input type="checkbox"/> Enable

Back Next

**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. When enabled, a Fullcone NAT parameter will appear, you can determine whether to enable Fullcone NAT. While only NAT enabled, the default NAT type Port-Restricted cone NAT will be used. For detail, please turn to page 47 for help.

**Firewall:** Check/uncheck this item to enable/disable firewall function.

**IGMP Multicast:** IGMP (**I**nternet **G**roup **M**embership Protocol) is a protocol used by IP hosts to report their multicast group memberships to any immediately neighboring multicast routers. Check this item to enable IGMP multicast on that WAN interface for multicast forwarding.

**MLD Multicast Proxy:** check whether to enable this function. MLD (**M**ulticast **L**istener **D**iscovery Protocol) Proxy intercept the MLD request from Clients and forward it to the router after some dealings. Support MLDv1 and MLDv2.

Click **Next** to go to set default gateway.

The screenshot shows the 'Advanced Setup' page for 'Default Gateway'. The page title is 'Advanced Setup' and the section is 'Default Gateway'. Below the title is a 'Default Gateway Interface List' section with a note: 'Only one default gateway interface will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected.' There are two columns: 'Selected Default Gateway Interfaces' and 'Available Routed WAN Interfaces'. The 'Selected' column contains 'ipoe\_0\_8\_35/atm0'. Between the columns are two buttons: a right-pointing arrow and a left-pointing arrow. Below the columns is a section titled 'Preferred WAN Interface As The System Default IPv6 Gateway' with a dropdown menu for 'Selected WAN Interface' set to 'ipoe\_0\_8\_35/atm0'. At the bottom are 'Back' and 'Next' buttons.

Set the default gateway and the default IPv6 gateway.

Click **Next** to go on to IPv6 DNS server setting.

The screenshot shows the 'Advanced Setup' page for 'IPv6 DNS Server'. The page title is 'Advanced Setup' and the section is 'IPv6 DNS Server'. Below the title is a 'Parameters' section with a note: 'Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface.' There are two radio buttons: 'Obtain IPv6 DNS info from a WAN interface' (selected) and 'Use the following Static IPv6 DNS address'. Below the radio buttons is a dropdown menu for 'WAN Interface selected' set to 'ipoe\_0\_8\_35/atm0'. Below that are two text input fields for 'Primary IPv6 DNS server' and 'Secondary IPv6 DNS server'. At the bottom are 'Back' and 'Next' buttons.

IPv6 DNS Server's operation is similar to IPv4 DNS server. There are two modes to get DNS server address: Auto and static mode.


### Obtain IPv6 DNS info from a WAN interface

**WAN Interface selected:** select one configured IPv6 WAN connection from the drop-down menu to be as an IPv6 DNS.

### Use the following Static IPv6 DNS address

**Primary IPv6 DNS Server / Secondary IPv6 DNS Server:** type the specific primary and secondary IPv6 DNS Server address.

Click **Next** to check the settings.

Advanced Setup 

▼ WAN Service

**Summary**

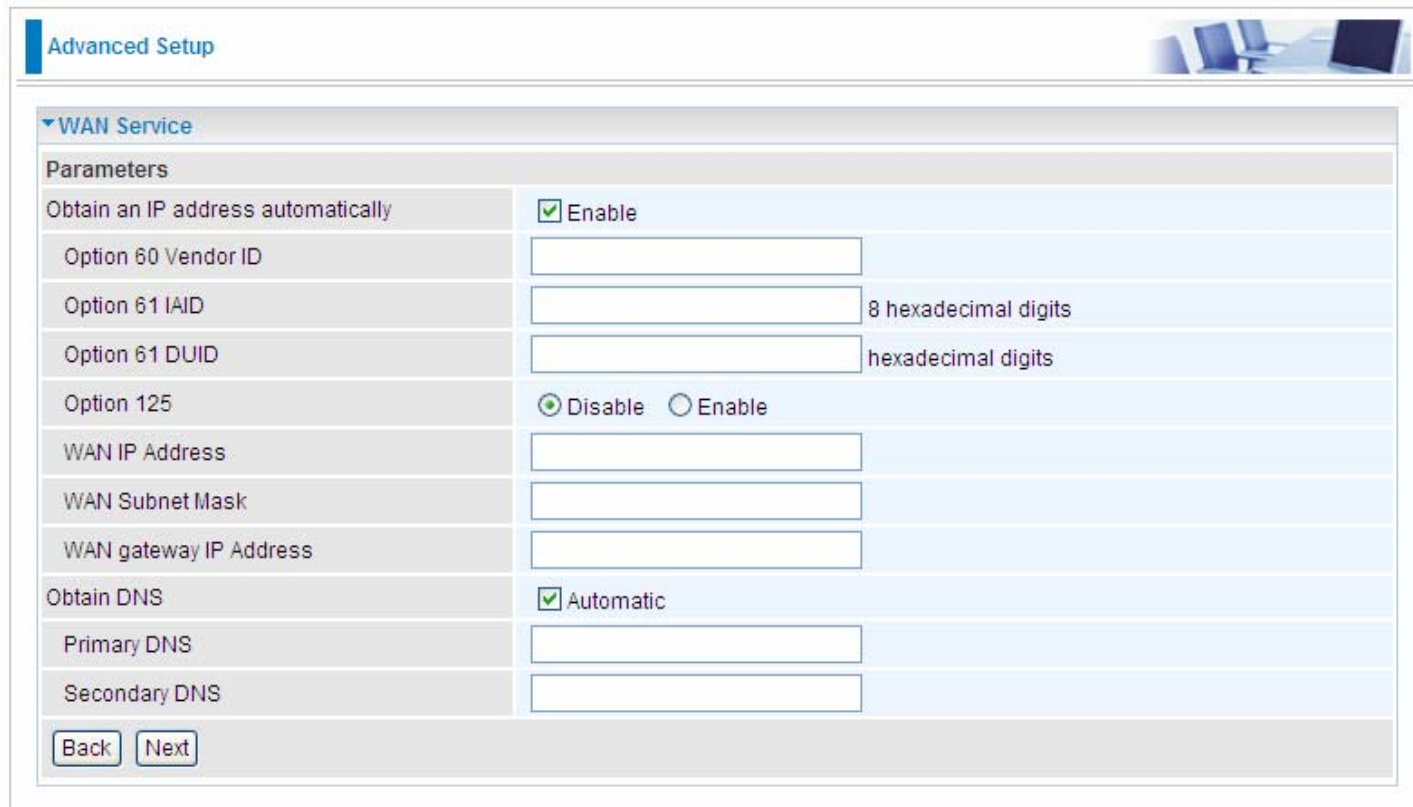
Make sure that the settings below match the settings provided by your ISP.

Type	IPoE
NAT	Disabled
Fullcone NAT	Disabled
Firewall	Disabled
IGMP Multicast	Disabled
Quality of Service	Enabled

If you confirm, click **Apply** to submit the settings.



## IPv6 disabled



Advanced Setup

WAN Service

Parameters

Obtain an IP address automatically	<input checked="" type="checkbox"/> Enable
Option 60 Vendor ID	<input type="text"/>
Option 61 IAID	<input type="text"/> 8 hexadecimal digits
Option 61 DUID	<input type="text"/> hexadecimal digits
Option 125	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
WAN IP Address	<input type="text"/>
WAN Subnet Mask	<input type="text"/>
WAN gateway IP Address	<input type="text"/>
Obtain DNS	<input checked="" type="checkbox"/> Automatic
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>

Back Next

Here two modes are supported for users to deal with the IP and DNS. You can select obtain automatically or manually input the information according to your ISP.

**Obtain an IP address automatically:** check whether to enable this function.

**Option 60 Vendor ID:** Enter the associated information by your ISP. This option is used by DHCP clients to optionally identify the vendor type and configuration of a DHCP client. The information is a string of n octets, interpreted by servers. Vendors may choose to define specific vendor class identifiers to convey particular configuration or other identification information about a client.

**Option 61 IAID:** Enter the associated information provided by your ISP. You should input 8 hexadecimal numbers.

**Option 61 DUID:** Enter the associated information provided by your ISP. You should input hexadecimal number(s).

**Option 125:** Option 125 is a complementary standard of DHCP protocol, it is used to encapsulate option 125 message into DHCP offer packet before forward it to clients. After the clients receive the packet, it check the option 125 field in the packet with the prestored message, if it is matched, then the client accepts this offer, otherwise it will be abandoned. Check Enable or Disable this function. Default setting is Disable.

**WAN IP Address:** Enter your IP address to the device provided by your ISP. If Fixed IP Address is selected in the IPv4 Protocol field, default value 0.0.0.0 will display in this field.

**WAN Subnet Mask:** Enter your submask to the device provided by your ISP.

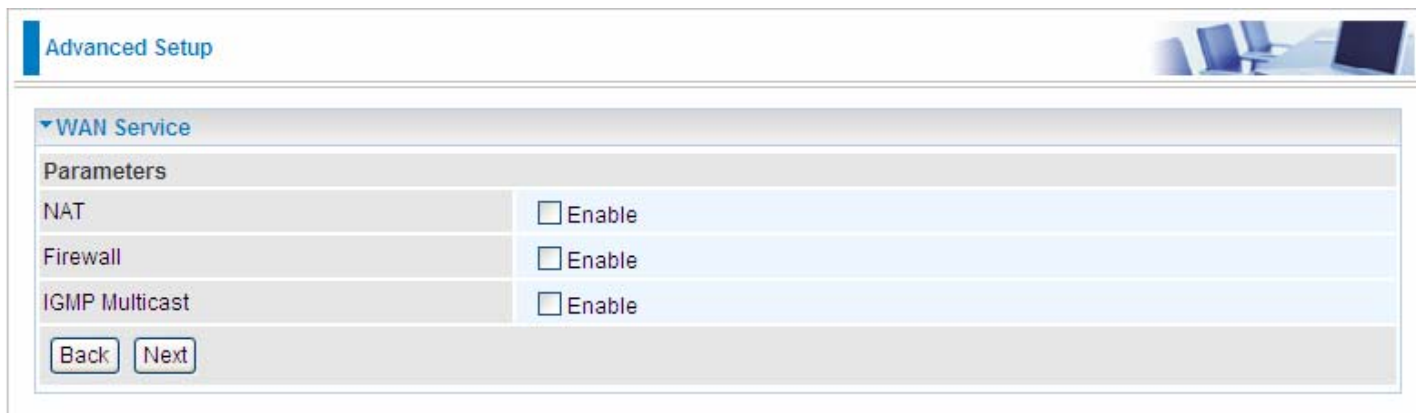
**WAN gateway IP Address:** Enter your gateway IP address to the device provided by your ISP.

**Obtain DNS:** check whether to enable obtain DNS function.

**Primary/Secondary DNS:** enter the primay/secondary DNS address when you uncheck Obtain DNS checkbox.

**Note:** If you don't know well about the DHCP Option, you can leave it empty or leave it as default.

Click **Next** to go to next step.



The screenshot shows the 'Advanced Setup' page for WAN Service. The 'WAN Service' section is expanded, showing a 'Parameters' table with three rows: 'NAT', 'Firewall', and 'IGMP Multicast'. Each row has an 'Enable' checkbox, all of which are currently unchecked. Below the table are 'Back' and 'Next' buttons.

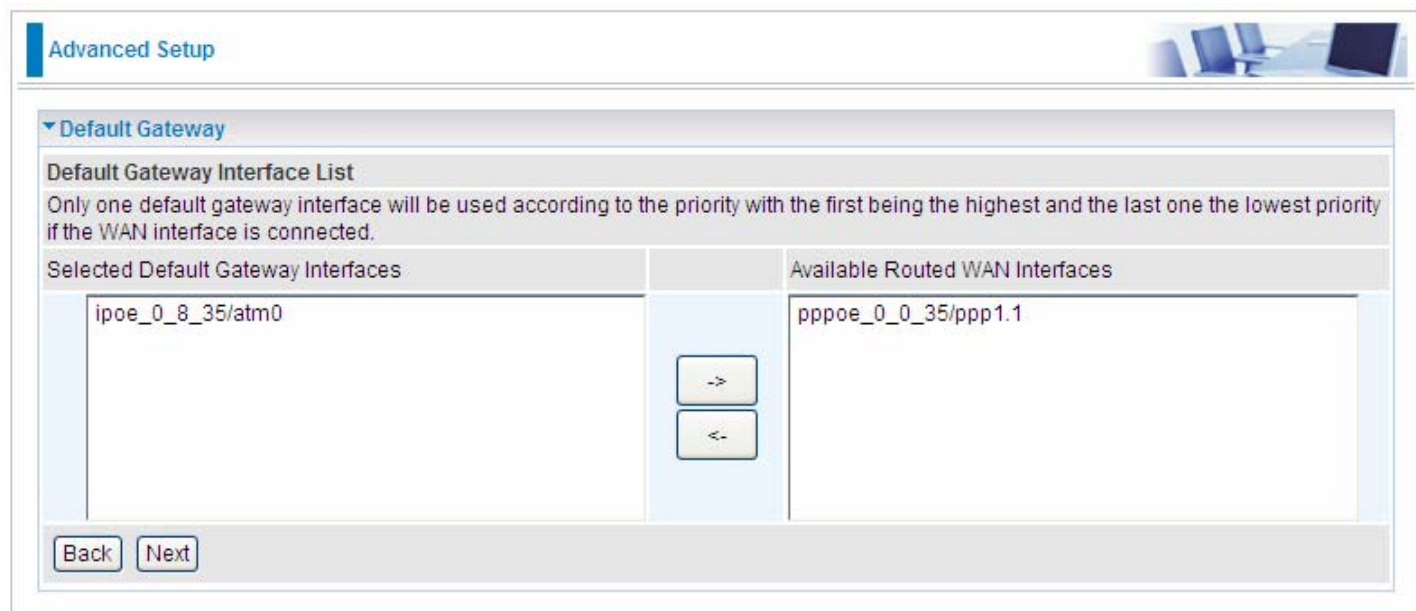
Parameters	
NAT	<input type="checkbox"/> Enable
Firewall	<input type="checkbox"/> Enable
IGMP Multicast	<input type="checkbox"/> Enable

**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. When enabled, a Fullcone NAT parameter will appear, you can determine whether to enable Fullcone NAT. While only NAT enabled, the default NAT type Port-Restricted cone NAT will be used. For detail, please turn to page 47 for help.

**Firewall:** Check/uncheck this item to enable/disable firewall function.

**IGMP Multicast:** IGMP (Internet Group Membership Protocol) is a protocol used by IP hosts to report their multicast group memberships to any immediately neighboring multicast routers. Check this item to enable IGMP multicast on that WAN interface for multicast forwarding.


Click **Next** to go to set default gateway.



The screenshot shows the 'Advanced Setup' page for Default Gateway configuration. The 'Default Gateway' section is expanded, showing a 'Default Gateway Interface List' with a descriptive text: 'Only one default gateway interface will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected.' Below this is a table with two columns: 'Selected Default Gateway Interfaces' and 'Available Routed WAN Interfaces'. The first column contains 'ipoe\_0\_8\_35/atm0' and the second column contains 'pppoe\_0\_0\_35/ppp1.1'. Between the columns are two buttons: '->' and '<-'.

Selected Default Gateway Interfaces	Available Routed WAN Interfaces
ipoe_0_8_35/atm0	pppoe_0_0_35/ppp1.1

Click **Next** to go on to check the settings.

Advanced Setup 

▼ WAN Service

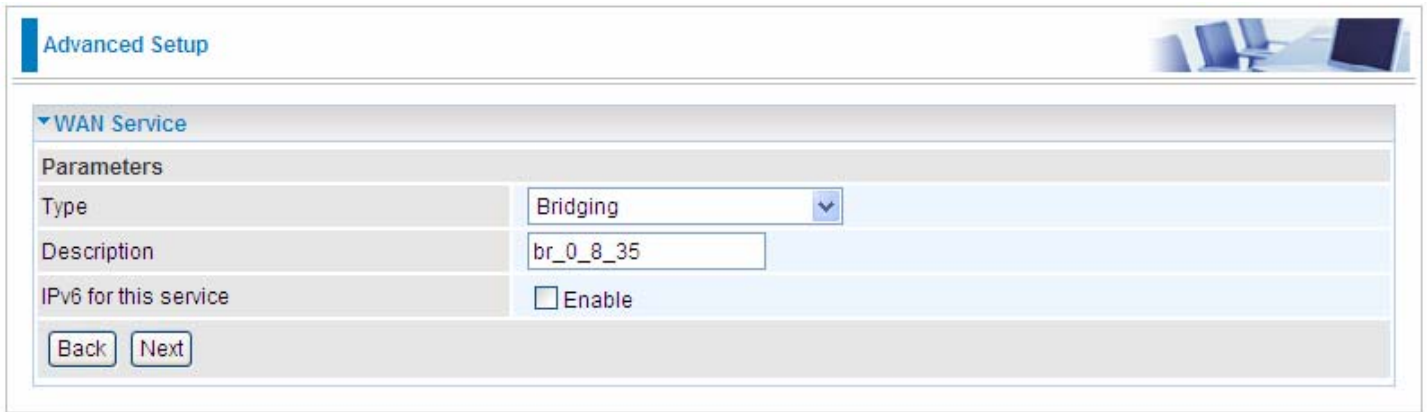
Summary

Make sure that the settings below match the settings provided by your ISP.

Type	IPoE
NAT	Enabled
Fullcone NAT	Enabled
Firewall	Enabled
IGMP Multicast	Enabled
Quality of Service	Disabled

Click **Apply** to apply your settings.

## Bridging



Advanced Setup

WAN Service

Parameters

Type	Bridging
Description	br_0_8_35
IPv6 for this service	<input type="checkbox"/> Enable

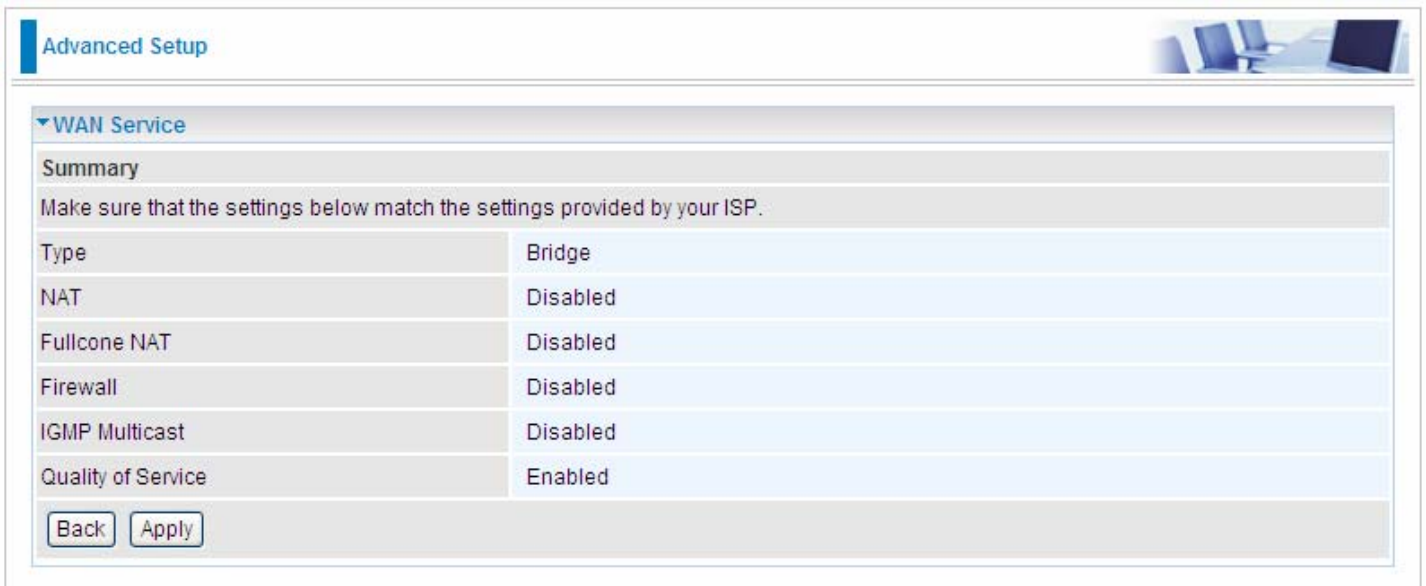
**Type:** Select Bridging.

**Description:** You are allowed to enter the user defined name for this service.

**IPv6 for this service:** check whether to enable IPv6 service.

Click **Next** to go to next step. See [IPv6 enabled](#) and [IPv6 disabled](#) .

### IPv6 enabled



Advanced Setup

WAN Service

Summary

Make sure that the settings below match the settings provided by your ISP .

Type	Bridge
NAT	Disabled
Fullcone NAT	Disabled
Firewall	Disabled
IGMP Multicast	Disabled
Quality of Service	Enabled

Click **Apply** to apply your settings.

## IPv6 disabled

Advanced Setup 

▼ WAN Service

**Summary**

Make sure that the settings below match the settings provided by your ISP.

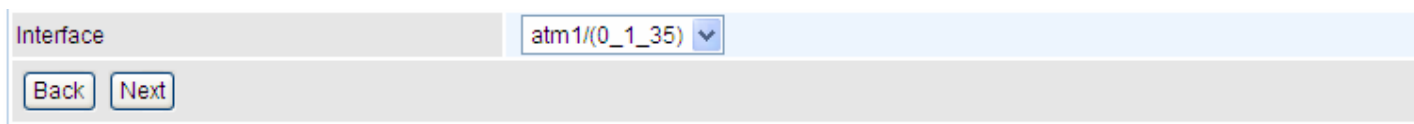
Type	Bridge
NAT	Disabled
Fullcone NAT	Enabled
Firewall	Disabled
IGMP Multicast	Disabled
Quality of Service	Enabled

Click **Apply** to apply your settings.

## VLAN MUX Connection Mode

It is similar to Default Connection in configuration. Select the interface which is a VLAN MUX mode connection configured in WAN Service, here for example, in the following, atm1/(0\_1\_35) is a VLAN MUX mode connection.

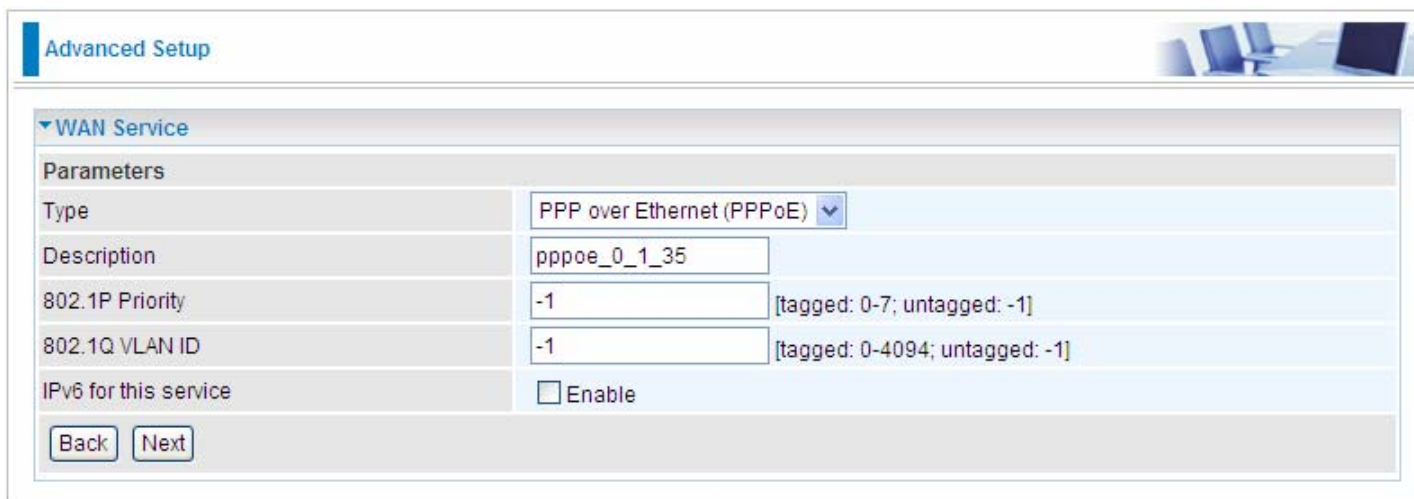
select interface(VLAN MUX mode).



Interface: atm1/(0\_1\_35) ▼

Back Next

Click **Next** to go on to next step.



Advanced Setup

WAN Service

Parameters

Type	PPP over Ethernet (PPPoE) ▼
Description	pppoe_0_1_35
802.1P Priority	-1 [tagged: 0-7; untagged: -1]
802.1Q VLAN ID	-1 [tagged: 0-4094; untagged: -1]
IPv6 for this service	<input type="checkbox"/> Enable

Back Next

**Type:** select the protocol, PPPoE, IP over Internet, Bridge.

**Description:** user-defined description.

**802.1P Priority:** It indicates the frame priority level from 0 (lowest) to 7 (highest), which can be used to prioritize different classes of traffic (voice, video, data, etc). Enter the priority identification, tagged:0-7, untagged:-1.

**802.1Q VLAN ID:** It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 0-4094, untagged:-1.

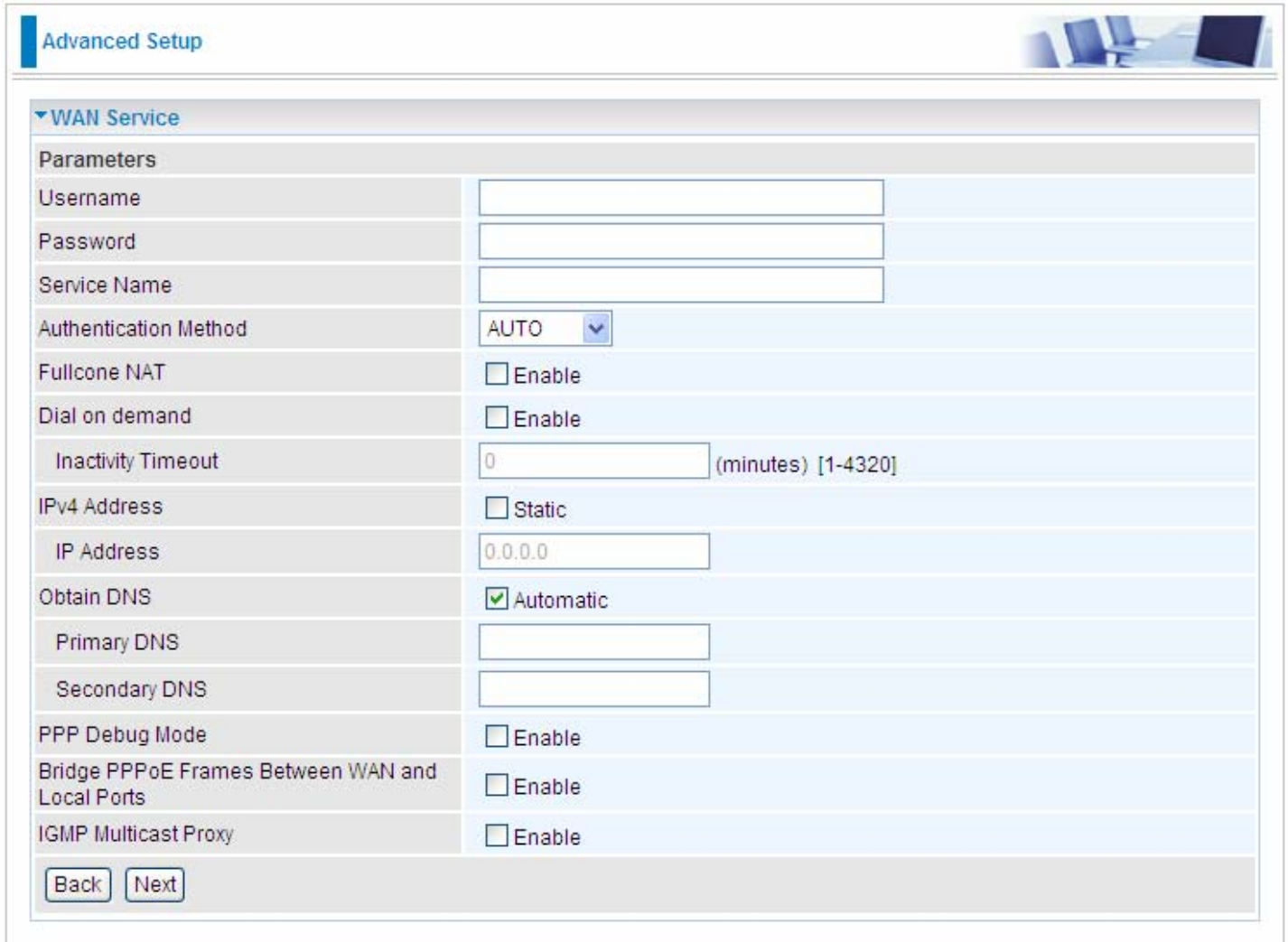
You can leave 802.1P Priority and 802.1Q VLAN ID as default setting,-1, means untagged, in this mode, the vlan tag header will not be contained, but if you want to allow one service for the specific vlan, here you should set the two parameters, the vlan tag header will be contained.

**IPv6 for this service:** check whether to enable IPv6 service.

The following steps are similar to Default Connection settings, for help turn to [Default Connection settings](#).

Take an example with IPv6 disabled, let's look at a scenario in which 1 PPPoE and 1 Bridge service needed by user.

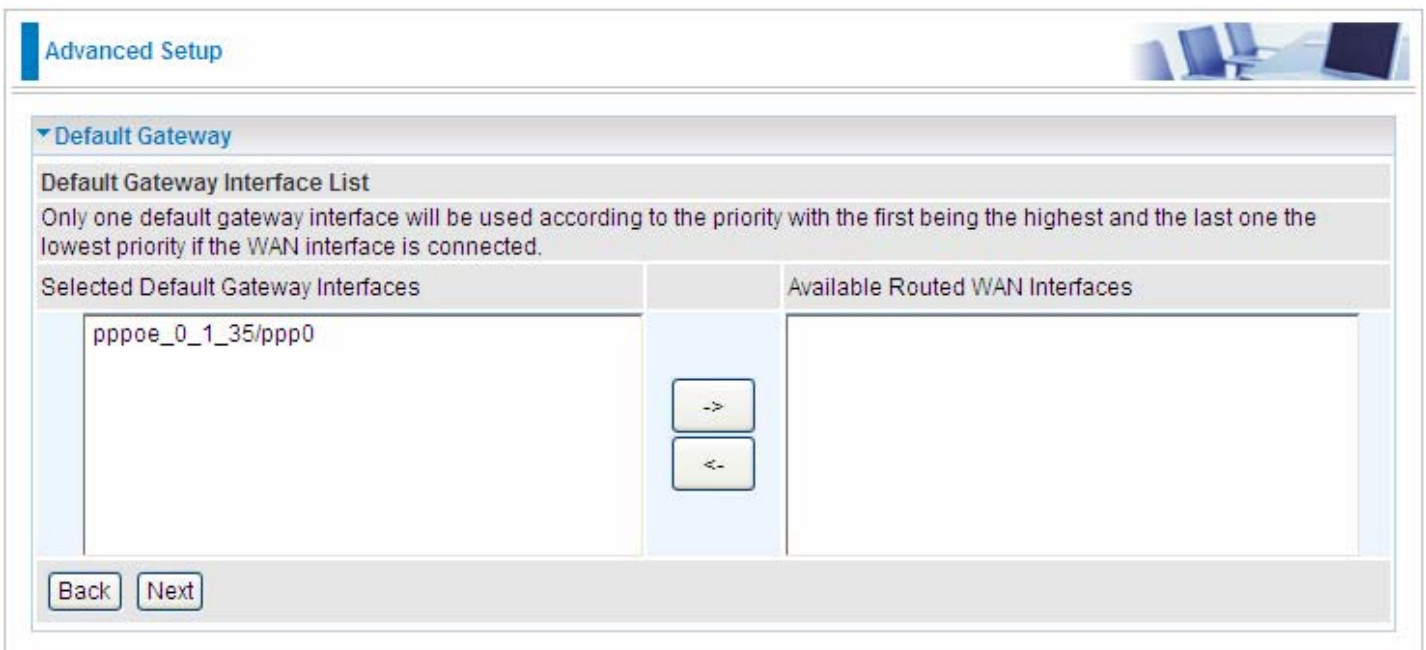
In the above page, click **Next** to set WAN service parameters.



The screenshot shows the 'Advanced Setup' page for WAN Service configuration. The 'WAN Service' section is expanded, showing various parameters. The 'Authentication Method' is set to 'AUTO'. The 'IPv4 Address' section has 'Static' selected, with the IP address set to '0.0.0.0'. The 'Obtain DNS' option is checked and set to 'Automatic'. There are 'Back' and 'Next' buttons at the bottom of the configuration area.

Parameters	
Username	<input type="text"/>
Password	<input type="password"/>
Service Name	<input type="text"/>
Authentication Method	AUTO <input type="button" value="v"/>
Fullcone NAT	<input type="checkbox"/> Enable
Dial on demand	<input type="checkbox"/> Enable
Inactivity Timeout	<input type="text" value="0"/> (minutes) [1-4320]
IPv4 Address	<input type="checkbox"/> Static
IP Address	<input type="text" value="0.0.0.0"/>
Obtain DNS	<input checked="" type="checkbox"/> Automatic
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>
PPP Debug Mode	<input type="checkbox"/> Enable
Bridge PPPoE Frames Between WAN and Local Ports	<input type="checkbox"/> Enable
IGMP Multicast Proxy	<input type="checkbox"/> Enable

Click **Next** to set the default gateway of this connection.



The screenshot shows the 'Advanced Setup' page for Default Gateway configuration. The 'Default Gateway' section is expanded, showing a 'Default Gateway Interface List'. Below the list, there are two columns: 'Selected Default Gateway Interfaces' and 'Available Routed WAN Interfaces'. The 'Selected Default Gateway Interfaces' column contains the entry 'pppoe\_0\_1\_35/ppp0'. There are two buttons with arrows pointing right and left between the columns. There are 'Back' and 'Next' buttons at the bottom of the configuration area.

**Default Gateway Interface List**  
Only one default gateway interface will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected.

Selected Default Gateway Interfaces		Available Routed WAN Interfaces
pppoe_0_1_35/ppp0	<input type="button" value="→"/> <input type="button" value="←"/>	

Click **Next** to view the information you have set to the connection, then click **Apply** to save your settings.

**Advanced Setup**

▼ WAN Service

**Summary**

Make sure that the settings below match the settings provided by your ISP.

Type	PPPoE
NAT	Enabled
Fullcone NAT	Disabled
Firewall	Enabled
IGMP Multicast	Disabled
Quality of Service	Enabled

Then you can see the PPPoE connection is listed below. Here it is just one service over atm1/(0\_1\_35).

**Advanced Setup**

▼ WAN Service

**WAN Setup**

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Remove
ppp0.1	pppoe_0_1_35	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Disabled	Disabled	<input type="checkbox"/>

Then we can again set a Bridging connection over atm1/(0\_1\_35) interface. Click Add in the above page, the atm1/(0\_1\_35) also is listed for selection to add services.

**Advanced Setup**

Interface: atm1/(0\_1\_35) ▼

Continue clicking Next to select Bridging connection type.

**Advanced Setup**

▼ WAN Service

**Parameters**

Type	Bridging	
Description	br_0_1_35	
802.1P Priority	-1	[tagged: 0-7; untagged: -1]
802.1Q VLAN ID	-1	[tagged: 0-4094; untagged: -1]
IPv6 for this service	<input type="checkbox"/> Enable	



Click Next to make sure your settings below match the settings provided by your ISP. And Click **Apply** to save your settings.

**Advanced Setup**

▼ WAN Service

Summary

Make sure that the settings below match the settings provided by your ISP.

Type	Bridge
NAT	Disabled
Fullcone NAT	Disabled
Firewall	Disabled
IGMP Multicast	Disabled
Quality of Service	Enabled

Back Apply

**Advanced Setup**

▼ WAN Service

WAN Setup

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Remove
atm1.2	br_0_1_35	Bridge	N/A	N/A	Disabled	Disabled	Disabled	Disabled	Disabled	<input type="checkbox"/>
ppp0.1	pppoe_0_1_35	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Disabled	Disabled	<input type="checkbox"/>

Add Remove

This screen is the interface we set previous, here used for understanding.

**Advanced Setup**

▼ WAN Interface

ATM Interface

Layer2 Interface ATM

Interface	VPI	VCI	Category	Link Type	Connection Mode	IP QoS	Scheduler Alg	Queue Weight	Group Precedence	Remove
atm1	1	35	UBR	EoA	VlanMuxMode	Enabled	SP			<input type="checkbox"/>

Add Remove

The below is WAN connection status, here you can see clearly the multiple services over one PVC.

**Device Info**

▼ WAN

Wan Info

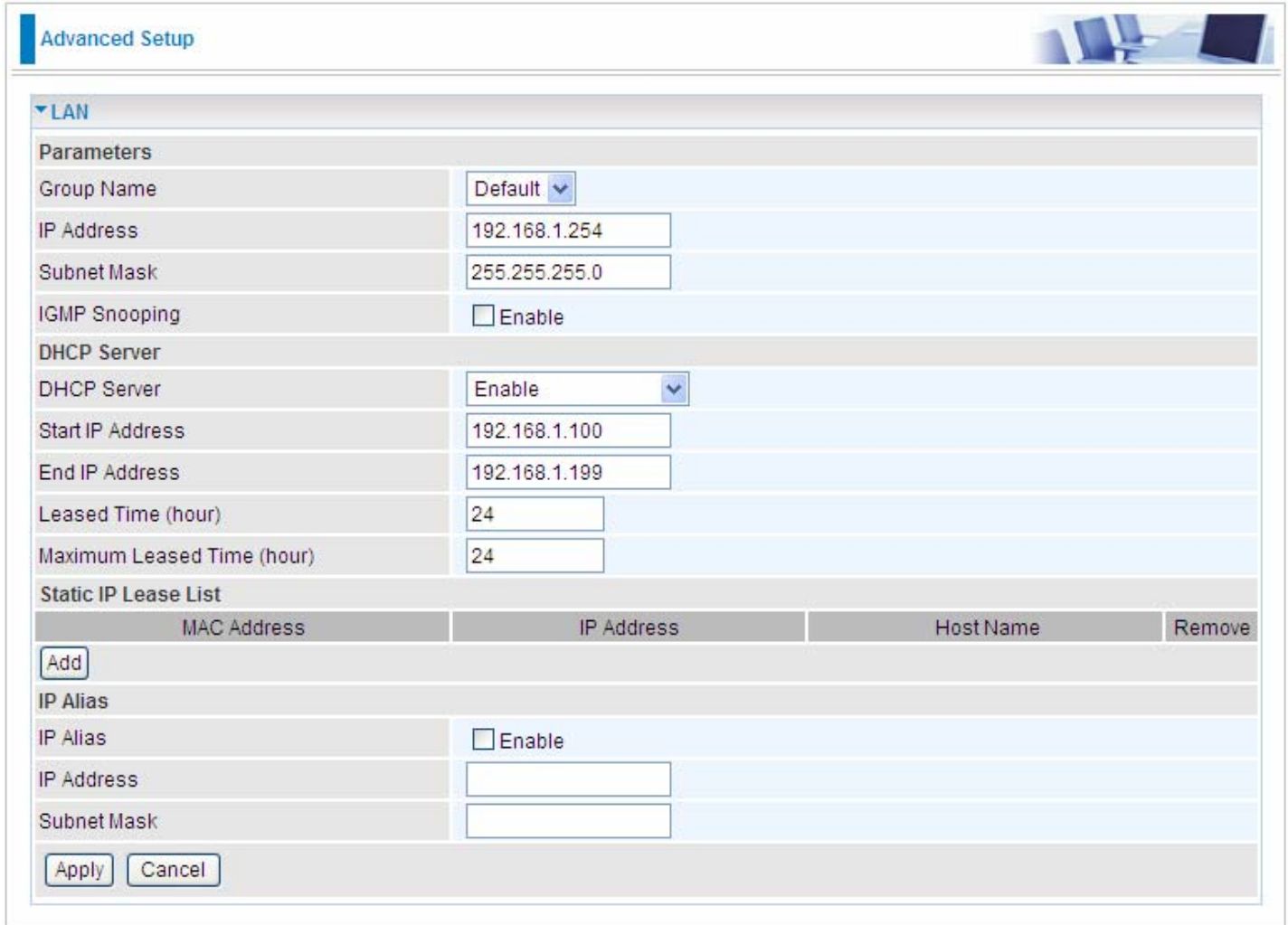
Interface	Description	Type	VlanMuxId	IPv6	Igmp	MLD	NAT	Firewall	Status	IPv4 Address	IPv6 Address
atm1.2	br_0_1_35	Bridge	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Connected	0.0.0.0	
ppp0.1	pppoe_0_1_35	PPPoE	Disabled	Disabled	Disabled	Disabled	Enabled	Enabled	Connected	112.80.156.130	

See from the above diagrams, we have set one PVC, it is VPI/VCI 1/35. But we have set two services on the same PVC, they are bridging and PPPoE services.

While in contrast to Default connection mode, one PVC can only hold one service, if you want to more than one service over one PVC, you should apply from your ISP more PVCs to meet your needs.

# LAN - Local Area Network

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.



**Advanced Setup**

**LAN**

**Parameters**

Group Name	Default
IP Address	192.168.1.254
Subnet Mask	255.255.255.0
IGMP Snooping	<input type="checkbox"/> Enable
<b>DHCP Server</b>	
DHCP Server	Enable
Start IP Address	192.168.1.100
End IP Address	192.168.1.199
Leased Time (hour)	24
Maximum Leased Time (hour)	24

**Static IP Lease List**

MAC Address	IP Address	Host Name	Remove
<input type="button" value="Add"/>			

**IP Alias**

IP Alias	<input type="checkbox"/> Enable
IP Address	
Subnet Mask	

## Parameters

**Group Name:** here group refers to the group you set in **Interface Grouping** section, you can set the parameters for the specific group. Select the group by the drop-down box. For more information please refer to **Interface Grouping** of this manual.

**IP address:** the IP address of the router. Default is 192.168.1.254.

**Subnet Mask:** the default Subnet mask on the router.

**IGMP Snooping:** Enable or disable the IGMP Snooping function. Without IGMP snooping, multicast traffic is treated in the same manner as broadcast traffic - that is, it is forwarded to all ports. With IGMP snooping, multicast traffic of a group is only forwarded to ports that have members of that group.”

When enabled, you will see two modes:

- ① **Standard Mode:** In standard mode, multicast traffic will flood to all bridge ports when no client subscribes to a multicast group.
- ① **Blocking Mode:** In blocking mode, the multicast data will be blocked when there are no client subscribes to a multicast group, it won't flood to the bridge ports.

## DHCP Server

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

### ① Disable

DHCP Server	
DHCP Server	Disable

Disable the DHCP Server function.

### ① Enable

Enable the DHCP function, enter the information wanted. Here as default.

DHCP Server	
DHCP Server	Enable
Start IP Address	192.168.1.100
End IP Address	192.168.1.199
Leased Time (hour)	24
Maximum Leased Time (hour)	24

**Start IP Address:** the start IP address of the range the DHCP Server used to assign to the Clients.

**End IP Address:** the end IP address of the range the DHCP Server used to assign to the Clients.

**Leased Time:** the leased time for each DHCP Client.

**Maximum Leased Time(hour):** the Maximum Leased Time(hour).

### ① DHCP Server Relay

DHCP Server	
DHCP Server	DHCP Server Relay
DHCP Server IP Address	


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

## Static IP List

The specified IP will be assigned to the corresponding MAC Address listed in the following table when DHCP Server assign IP Addresses to Clients.

Static IP Lease List			
MAC Address	IP Address	Host Name	Remove
<input type="button" value="Add"/>			

Press **Add** to the Static IP List.

Advanced Setup 

▼ Static IP

Parameters

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

Enter the MAC Address, IP Address and Host Name, then click Apply to confirm your settings.

## IP Alias

This function allows the creation of multiple virtual IP interfaces on this router. It helps to connect two or more local networks to the ISP or remote node.

IP Alias

IP Alias	<input type="checkbox"/> Enable
IP Address	<input type="text"/>
Subnet Mask	<input type="text"/>

**IP Alias:** check whether to enable this function.

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

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

Click **Apply** to apply your settings.

## IPv6 Autoconfig

The IPv6 address composes of two parts, thus, the prefix and the interface ID.

There are two ways to dynamically configure IPv6 address on hosts. One is statefull configuration, for example using DHCPv6 (which resembles its counterpart DHCP in IPv4.) In the stateful autoconfiguration model, hosts obtain interface addresses and/or configuration information and parameters from a DHCPv6 server. The Server maintains a database that keeps track of which addresses have been assigned to which hosts.

The second way is stateless configuration. Stateless auto-configuration requires no manual configuration of hosts, minimal (if any) configuration of routers, and no additional servers. The stateless mechanism allows a host to generate its own addresses using a combination of locally available information (MAC address) and information (prefix) advertised by routers. Routers advertise prefixes that identify the subnet(s) associated with a link, while hosts generate an "interface identifier" that uniquely identifies an interface on a subnet. An address is formed by combining the two. When using stateless configuration, you needn't configure anything on the client.

Advanced Setup

IPv6 Autoconfig

Parameters

Note: Interface ID does NOT support ZERO COMPRESSION "::". Please enter the complete information.  
For example: Please enter "0:0:0:2" instead of "::2".

Static LAN IPv6 Address Configuration

Interface Address / Prefix Length

IPv6 LAN Applications

DHCPv6 Server  Enable

DHCPv6 Server Type  Stateless  Stateful

Start interface ID

End interface ID

Leased Time (hour)

Issue Router Advertisements  Enable

MLD Snooping  Enable  Standard Mode  Blocking Mode

Apply Cancel

### Static LAN IPv6 Address Configuration

**Interface Address / Prefix Length:** enter the static LAN IPv6 address.

### IPv6 LAN application

**DHCPv6 Server:** check whether to enable DHCPv6 server.

**DHCPv6 Server Type:** select Stateless or Stateful. When DHCPv6 is enabled, this parameter is available. **Stateless:** if selected, the PCs in LAN are configured through RA mode, thus, the PCs in LAN are configured through RA mode, to obtain the prefix message and generate an address using a combination of locally available information (MAC address) and information (prefix) advertised by routers, but they can obtain such information like DNS from DHCPv6 Server. **Stateful:** if selected, the PCs in LAN will be configured like in IPv4 mode, thus obtain addresses and DNS information

from DHCPv6 server.

**Start interface ID:** enter the start interface ID. The IPv6 address composed of two parts, thus, the prefix and the interface ID. Interface is like the Host ID compared to IPv4.

**End interface ID:** enter the end interface ID.

Note: Interface ID does NOT support ZERO COMPRESSION ":::". Please enter the complete information.

For example: Please enter "0:0:0:2" instead of "::2".

**Leased Time (hour):** the leased time, similar to leased time in DHCPv4, is a time limit assigned to clients, when expires, the assigned ID will be recycled and reassigned.

**Issue Router Advertisement:** check whether to enable issue Router Advertisement feature. It is to send Router Advertisement messages periodically.

**MLD snooping:** similar to IGMP snooping, listens in on the MLD conversation between hosts and routers by processing MLD packets sent in a multicast network, and it analyzes all MLD packets between hosts and the connected multicast routers in the network. Without MLD snooping, multicast traffic is treated in the same manner as broadcast traffic - that is, it is forwarded to all ports. With MLD snooping, multicast traffic of a group is only forwarded to ports that have members of that group.

- ① **Standard Mode:** In standard mode, multicast traffic will flood to all bridge ports when no client subscribes to a multicast group.
- ① **Blocking Mode:** In blocking mode, the multicast data will be blocked when there is no client subscribes to a multicast group, it won't flood to the bridge ports.

## Stateless and Stateful IPv6 address Configuration

**Stateless:** two methods can be adopted.

- ① With DHCPv6 disabled, but Issue Router Advertisement Enabled

DHCPv6 Server	<input type="checkbox"/> Enable
Issue Router Advertisements	<input checked="" type="checkbox"/> Enable

With this method, the PCs in LAN are configured through RA mode, thus, the PCs in LAN are configured through RA mode, to obtain the prefix message and generate an address using a combination of locally available information (MAC address) and information (prefix) advertised by routers.

- ① With both DHCPv6 and Issue Router Advertisement Enabled

DHCPv6 Server	<input checked="" type="checkbox"/> Enable
DHCPv6 Server Type	<input checked="" type="radio"/> Stateless <input type="radio"/> Stateful
Start interface ID	<input type="text" value="0:0:0:2"/>
End interface ID	<input type="text" value="0:0:0:254"/>
Leased Time (hour)	<input type="text" value="24"/>
Issue Router Advertisements	<input checked="" type="checkbox"/> Enable

With this method, the PCs' addresses in LAN are configured like above method, but they can obtain such information like DNS from DHCPv6 Server.

**Stateful:** two methods can be adopted.

① With only DHCPv6 enabled

DHCPv6 Server	<input checked="" type="checkbox"/> Enable
DHCPv6 Server Type	<input type="radio"/> Stateless <input checked="" type="radio"/> Stateful
Start interface ID	<input type="text" value="0:0:0:2"/>
End interface ID	<input type="text" value="0:0:0:254"/>
Leased Time (hour)	<input type="text" value="24"/>
Issue Router Advertisements	<input type="checkbox"/> Enable

With this method, the PCs' addresses are configured the same as in IPv4, that is addresses are assigned by DHCPv6 server.

① With both DHCPv6 and Issue Router Advertisement Enabled

DHCPv6 Server	<input checked="" type="checkbox"/> Enable
DHCPv6 Server Type	<input type="radio"/> Stateless <input checked="" type="radio"/> Stateful
Start interface ID	<input type="text" value="0:0:0:2"/>
End interface ID	<input type="text" value="0:0:0:254"/>
Leased Time (hour)	<input type="text" value="24"/>
Issue Router Advertisements	<input checked="" type="checkbox"/> Enable

With this method, the PCs' addresses are configured the same like above, and the address information in RA packets will be neglected.



# NAT

NAT (Network Address Translation) feature translates a private IP to a public IP, allowing multiple users to access the Internet through a single IP account, sharing the single IP address. It is a natural firewall for the private network.

## Virtual Servers

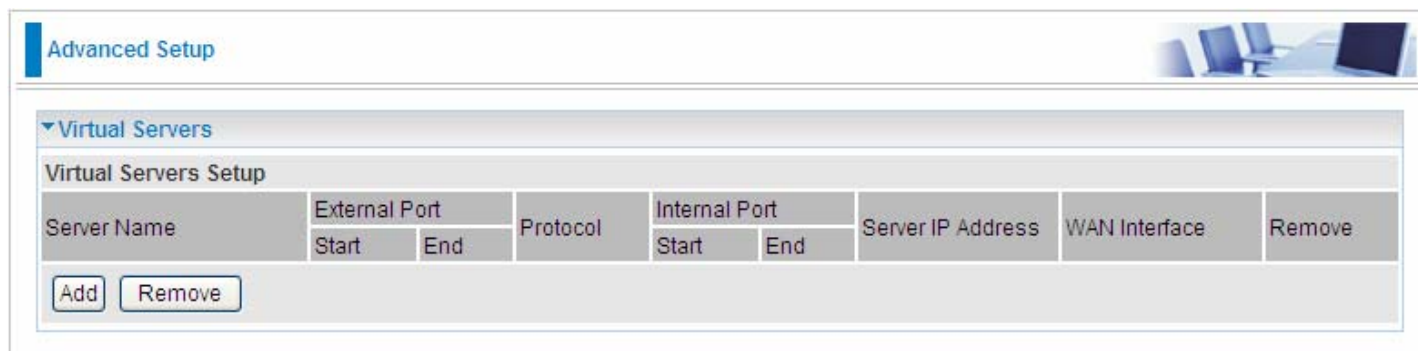
In TCP/IP and UDP networks a port is a 16-bit number used to identify which application program (usually a server) incoming connections should be delivered to. Some ports have numbers that are pre-assigned to them by the IANA (the Internet Assigned Numbers Authority), and these are referred to as “well-known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

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

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

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

This part is only available when NAT is enabled.



It is virtual server listing table as you see, Click Add to configure.

The following configuration page will appear to let you configure.

**Advanced Setup**

**Virtual Servers**

**Parameters**

Interface: pppoe\_0\_8\_35/ppp0

Server Name: Custom Service

Custom Service:

Server IP Address:

External Port		Protocol	Internal Port	
Start	End		Start	End
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>

Apply Cancel

**Interface:** select from the drop-down menu the interface you want the virtual server(s) applies to.

**Server Name:** select the server name from the drop-down menu.

**Custom Service:** it is a kind of service to let users customize the service they want. Enter the user-defined service name here. It is a parameter only available when users select **Custom Service** in the above parameter.

**Server IP Address:** Enter your server IP Address here.

#### External Port

- ① **Start:** Enter a port number as the external starting number for the range you want to give access to internal network.
- ① **End:** Enter a port number as the external ending number for the range you want to give access to internal network.

#### Internal Port

- ① **Start:** Enter a port number as the internal starting number.
- ① **End:** Here it will generate automatically according to the End port number of External port and can't be modified.

**Protocol:** select the protocol this service used: TCP/UDP, TCP, UDP.

## ● Set up

1. Select a Server Name from the drop-down menu, then the port will automatically appear, modify some as you like, or you can just leave it as default. Remember to enter your server IP Address.

Advanced Setup

▼ Virtual Servers

Parameters

Interface	pppoe_0_8_35/ppp0 ▼
Server Name	Age of Empires ▼
Custom Service	<input type="text"/>
Server IP Address	192.168.1.1

External Port		Protocol	Internal Port	
Start	End		Start	End
<input type="text" value="47624"/>	<input type="text" value="47624"/>	TCP ▼	<input type="text" value="47624"/>	<input type="text" value="47624"/>
<input type="text" value="6073"/>	<input type="text" value="6073"/>	TCP ▼	<input type="text" value="6073"/>	<input type="text" value="6073"/>
<input type="text" value="2300"/>	<input type="text" value="2400"/>	TCP ▼	<input type="text" value="2300"/>	<input type="text" value="2400"/>
<input type="text" value="2300"/>	<input type="text" value="2400"/>	UDP ▼	<input type="text" value="2300"/>	<input type="text" value="2400"/>
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>

2. Press **Apply** to conform, and the items will be list in the **Virtual Servers Setup** table.

Advanced Setup

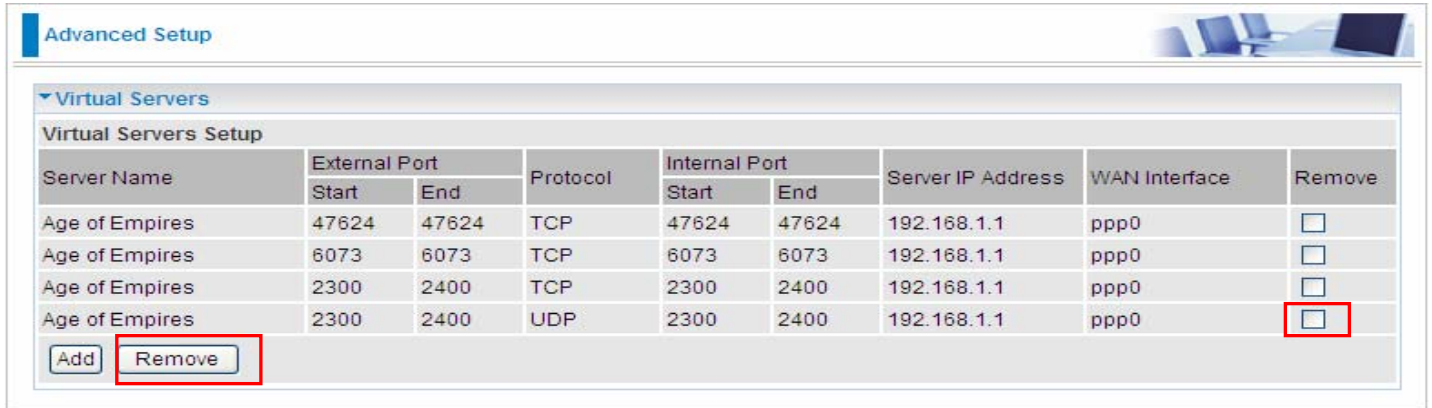
▼ Virtual Servers

Virtual Servers Setup

Server Name	External Port		Protocol	Internal Port		Server IP Address	WAN Interface	Remove
	Start	End		Start	End			
Age of Empires	47624	47624	TCP	47624	47624	192.168.1.1	ppp0	<input type="checkbox"/>
Age of Empires	6073	6073	TCP	6073	6073	192.168.1.1	ppp0	<input type="checkbox"/>
Age of Empires	2300	2400	TCP	2300	2400	192.168.1.1	ppp0	<input type="checkbox"/>
Age of Empires	2300	2400	UDP	2300	2400	192.168.1.1	ppp0	<input type="checkbox"/>

## Remove

If you don't need a specified Server, you can remove it. Check the check box beside the item you want to remove, then press **Remove**, it will be OK.



Advanced Setup

Virtual Servers

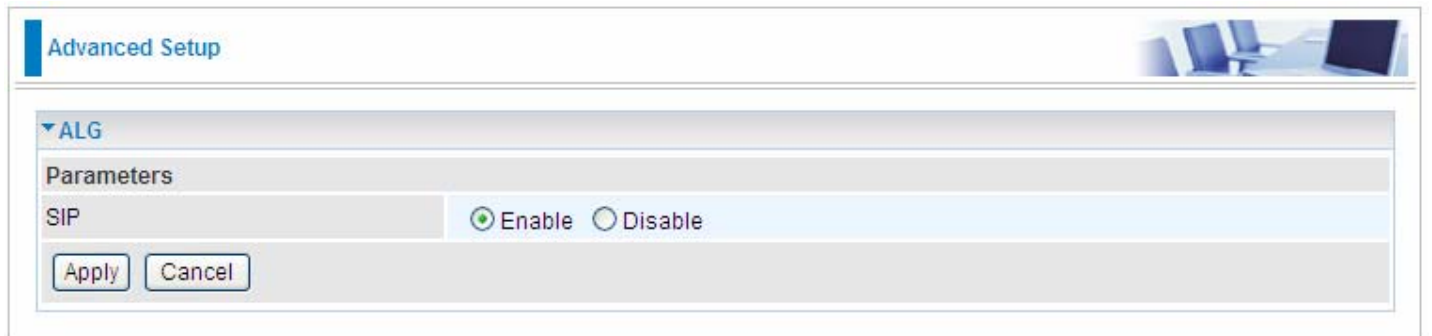
Virtual Servers Setup

Server Name	External Port		Protocol	Internal Port		Server IP Address	WAN Interface	Remove
	Start	End		Start	End			
Age of Empires	47624	47624	TCP	47624	47624	192.168.1.1	ppp0	<input type="checkbox"/>
Age of Empires	6073	6073	TCP	6073	6073	192.168.1.1	ppp0	<input type="checkbox"/>
Age of Empires	2300	2400	TCP	2300	2400	192.168.1.1	ppp0	<input type="checkbox"/>
Age of Empires	2300	2400	UDP	2300	2400	192.168.1.1	ppp0	<input checked="" type="checkbox"/>

Add Remove

## ALG

The ALG Controls enable or disable protocols over application layer.



Advanced Setup

ALG

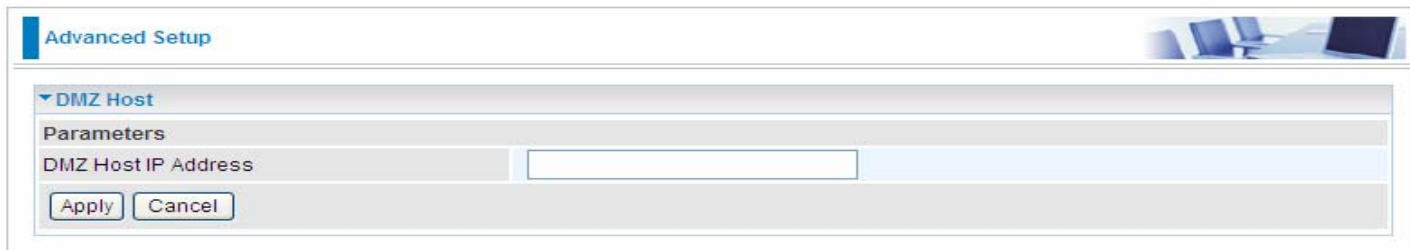
Parameters

SIP  Enable  Disable

Apply Cancel

## DMZ Host

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



The screenshot shows a software window titled "Advanced Setup" with a sub-section for "DMZ Host". Under "Parameters", there is a label "DMZ Host IP Address" followed by an empty text input field. Below the input field are two buttons: "Apply" and "Cancel".

**DMZ Host IP Address:** Enter the IP Address of a host you want it to be a DMZ host.



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



### **Attention**

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