BiPAC 7800NL

802.11n ADSL2+ Firewall Router

User Manual

Version released: 2.02a.dc1

Last revised date: 09-8-2010

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 7800NL router, an all-in-one ADSL2+ Router with wireless-N technology. The BiPAC 7800NL 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 7800NL 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 7800NL 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 7800NL 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 7800NL 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 2128 (about 3.4×1038) 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[*2]
- 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 7800NL A only)
- Compliant with ADSL2+ Standard
  - G.dmt.bis plus (ITU G.992.5)
  - ADSL2+ Annex M (ITU G.992.5 Annex M) (BiPAC 7800NL 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[*2]

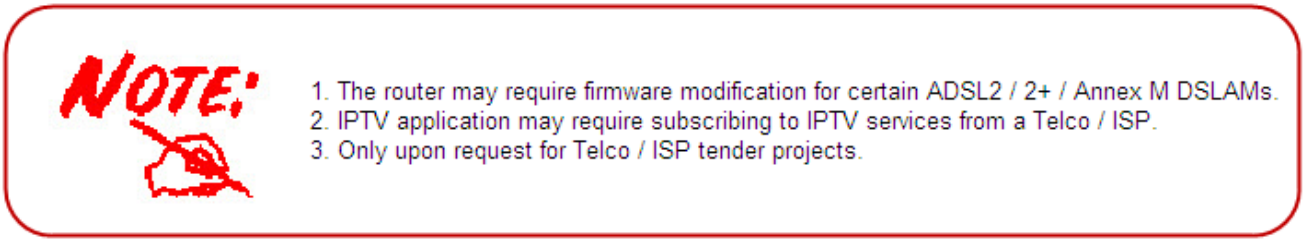
- Virtual LAN (VLAN)
- Quality of Service (QoS)
- IGMP Snooping & IGMP Proxy
- MLD Snooping & proxy
- VLAN MUX support

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[*3] supports remote management
- SNMP v1/v2/V3 supports remote and local management



Hardware Specifications

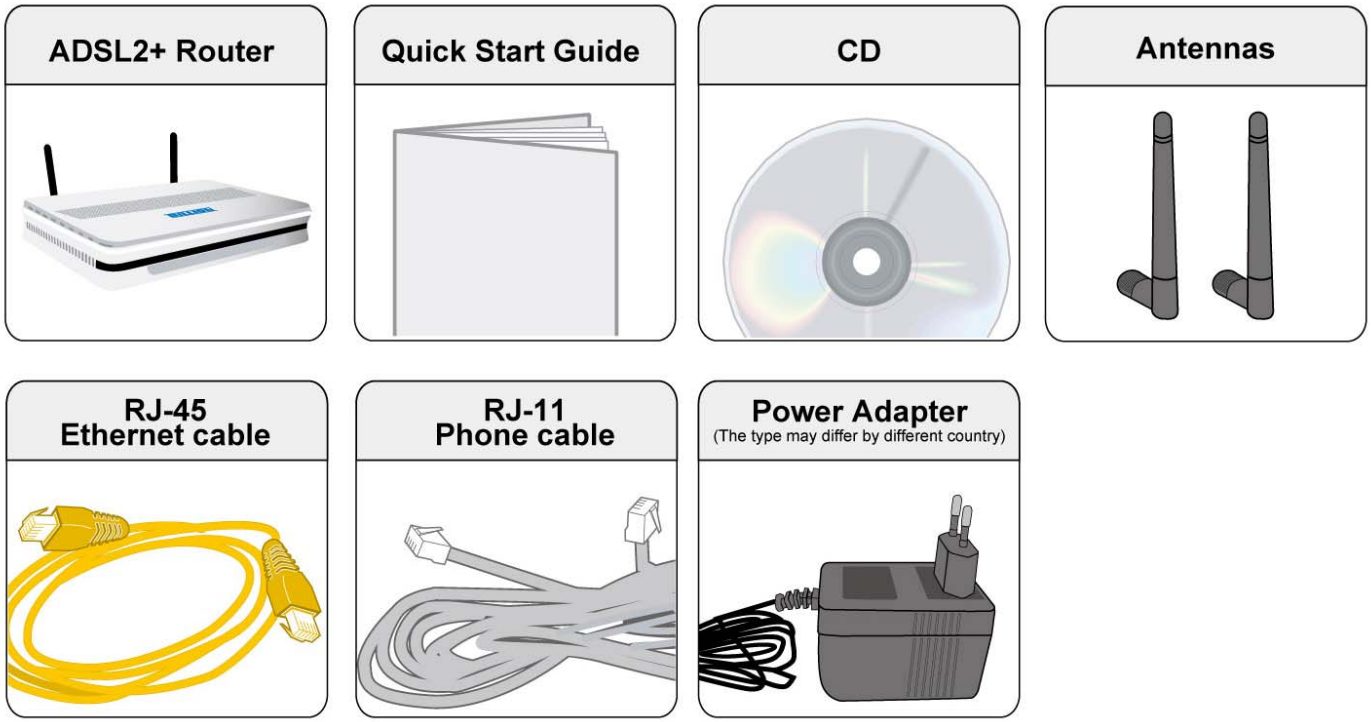
Physical Interface

- 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 7800NL 802.11n 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

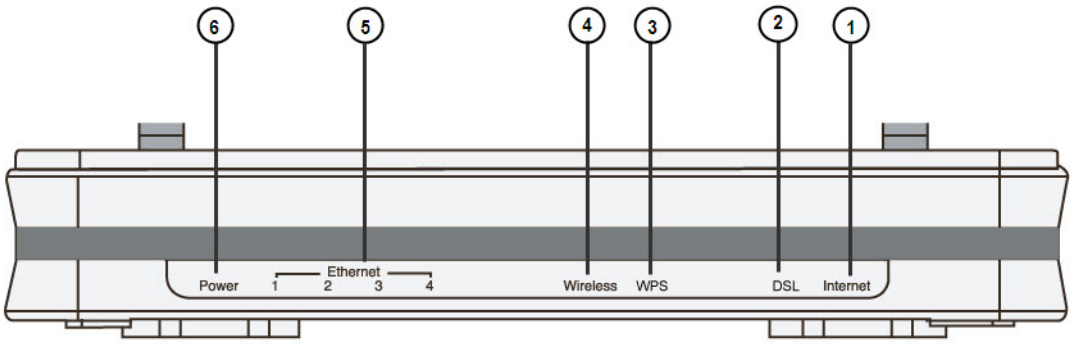
- Do not use the router in high humidity or high temperatures.
- Do not use the same power source for the router as other equipment.
- Do not open or repair the case yourself. If the router is too hot, turn off the power immediately and have it repaired at a qualified service center.
- Avoid using this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

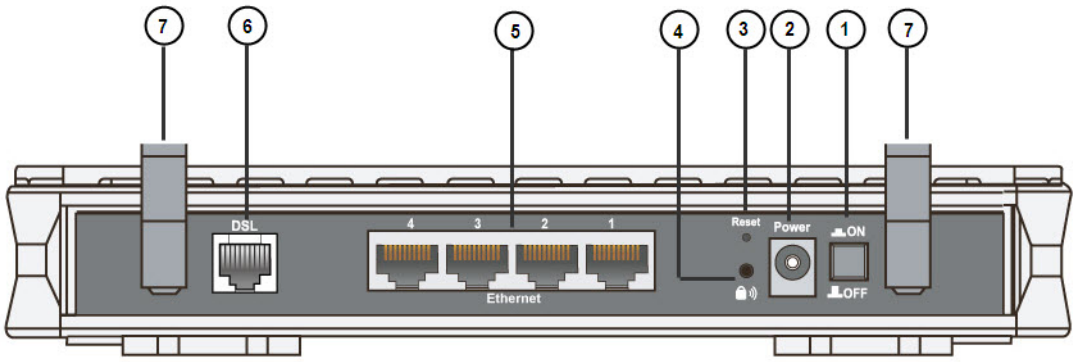
Device Description

The Front LEDs



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

The Rear Ports



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

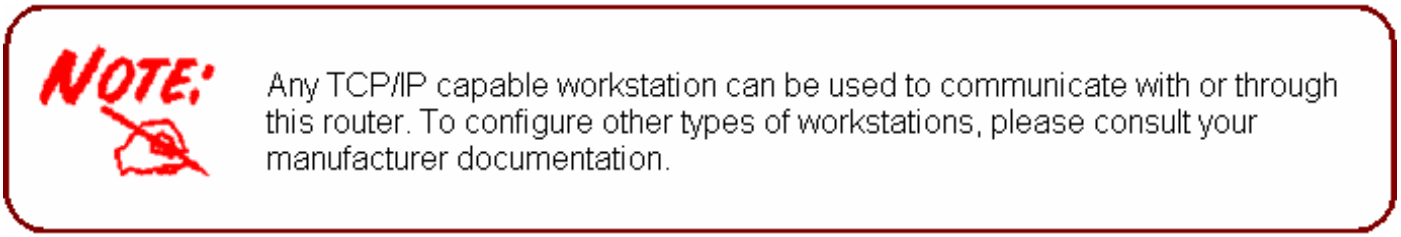
Chapter 3: Basic Installation

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.

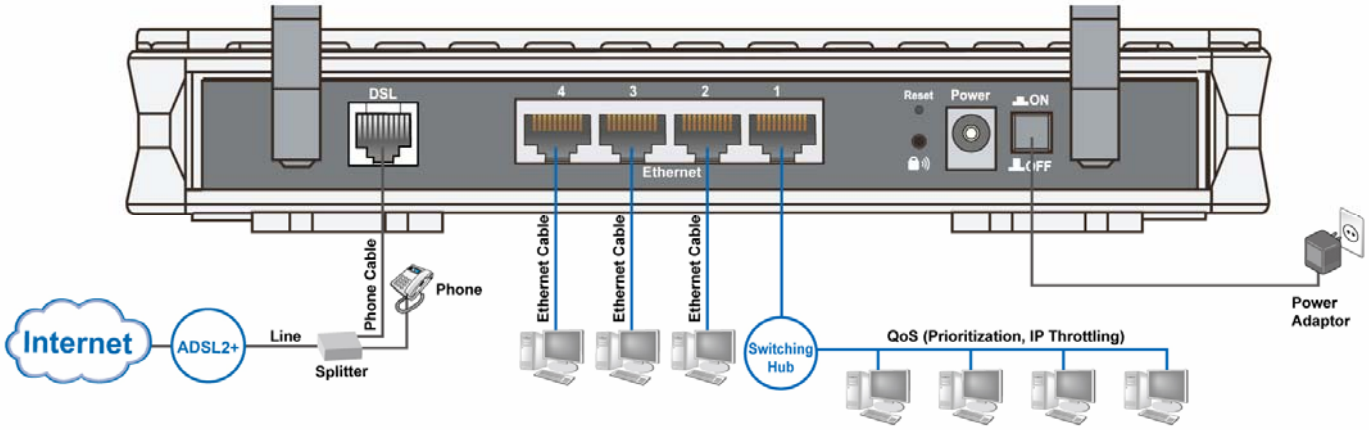
There are ways to connect the router, either through an external repeater hub or connect directly to your PCs. However, make sure that your PCs have an Ethernet interface installed properly prior to connecting the router device. You ought to configure your PCs to obtain an IP address through a DHCP server 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.



Connecting Your Router

Users can connect the ADSL2+ router as the following.

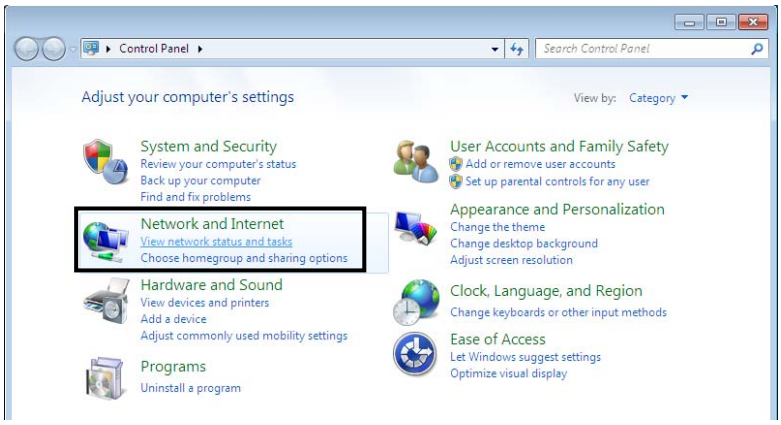


Network Configuration

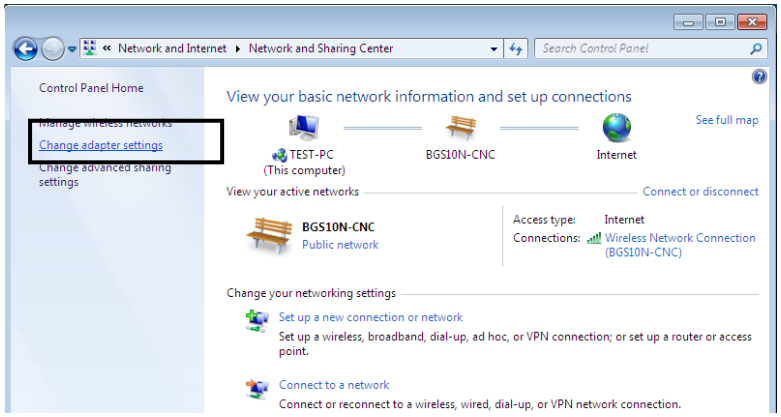
Configuring PC in windows 7

1. Go to Start. Click on Control Panel.

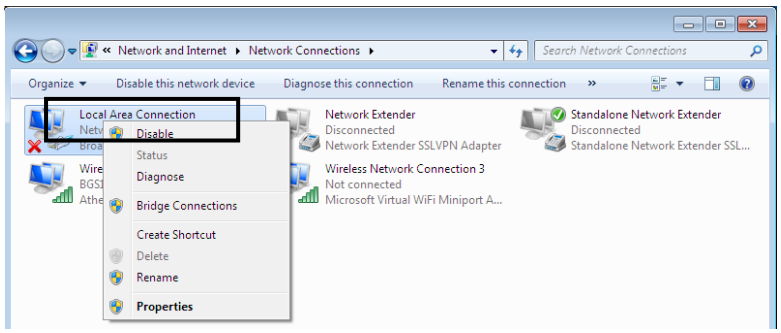
Then click on Network and Internet.



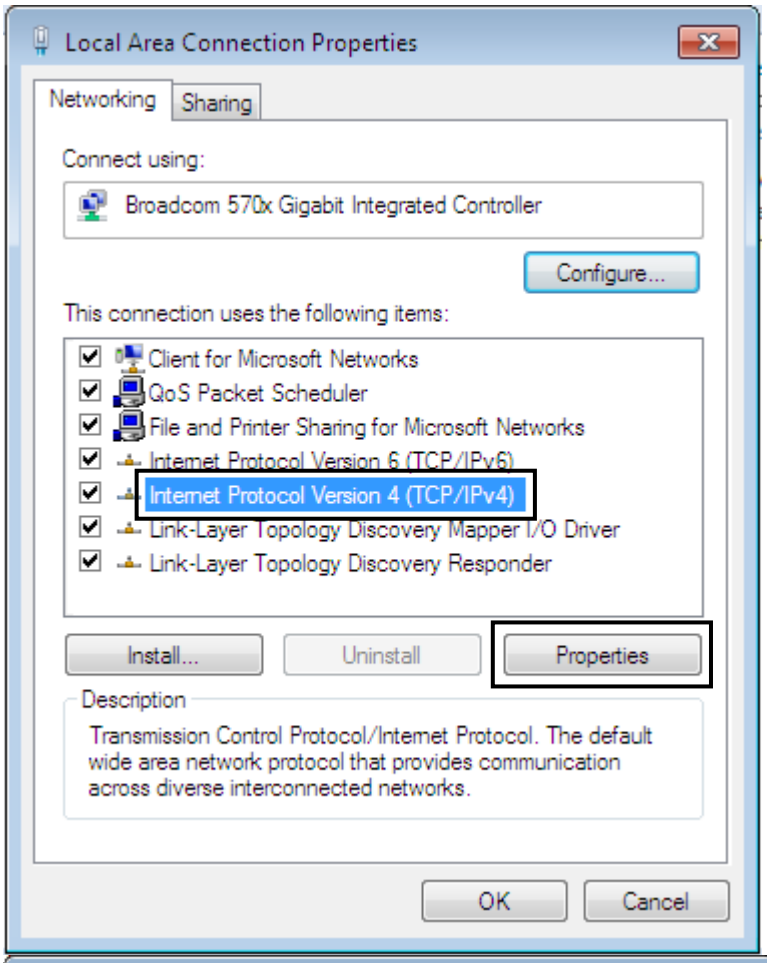
2. When the Network and Sharing Center window pops up, select and click on Change adapter settings on the left window panel.



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

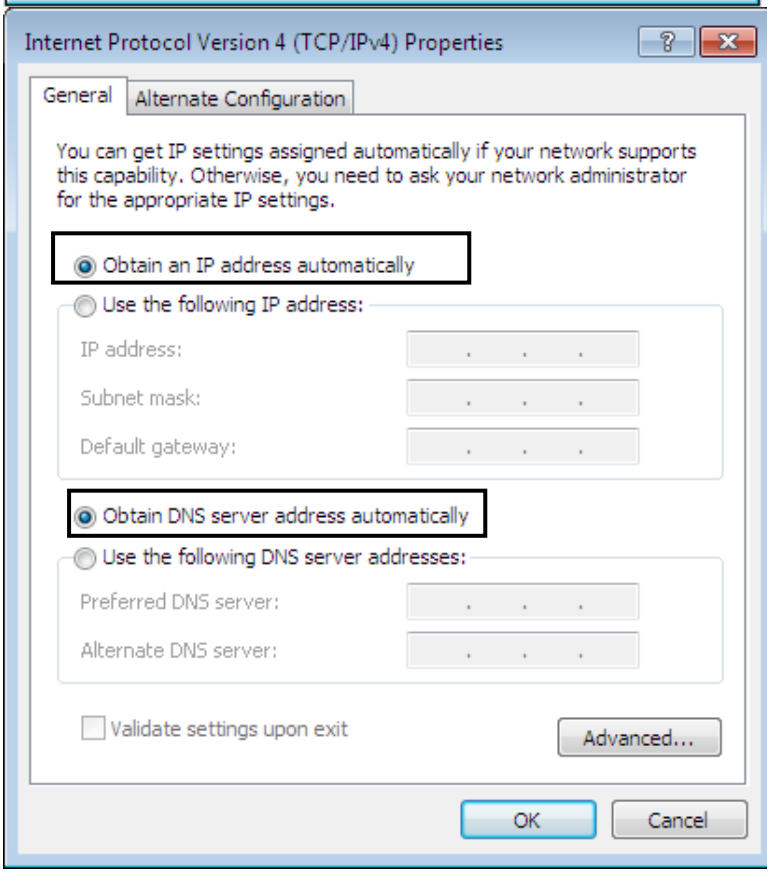


4. Select Internet Protocol Version 4 (TCP/IPv4) then click Properties.



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.

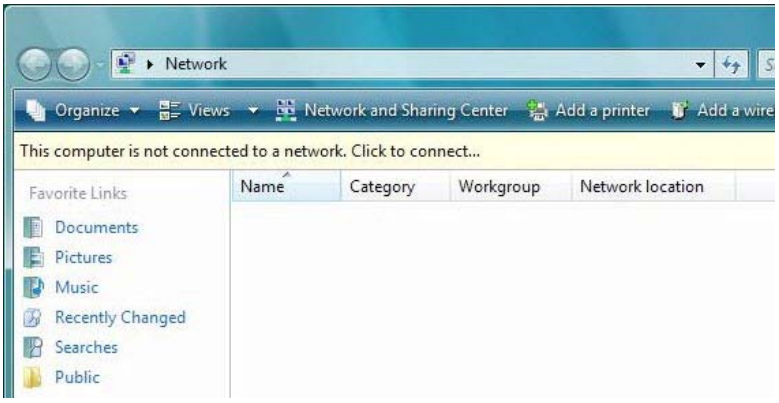
6. Click OK again in the Local Area Connection Properties window to apply the new configuration.



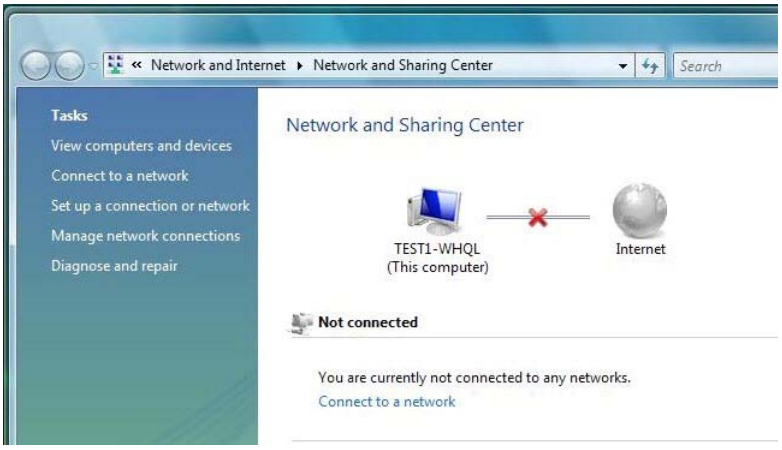
Configuring PC in Windows Vista

1. Go to Start. Click on Network.

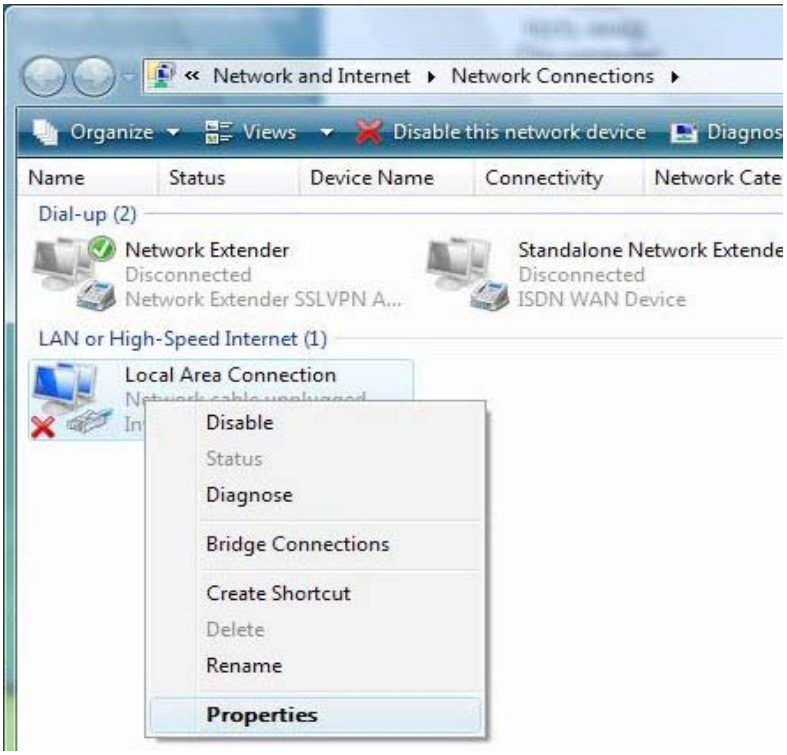
2. Then click on Network and Sharing Center at the top bar.



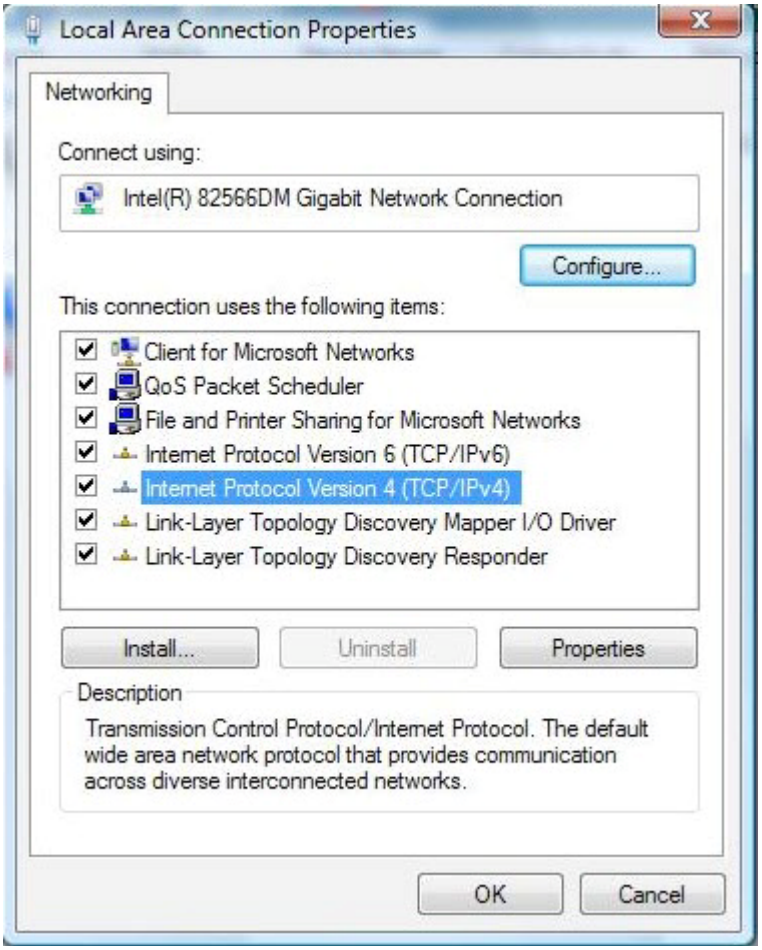
3. When the Network and Sharing Center window pops up, select and click on Manage network connections on the left window column.



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

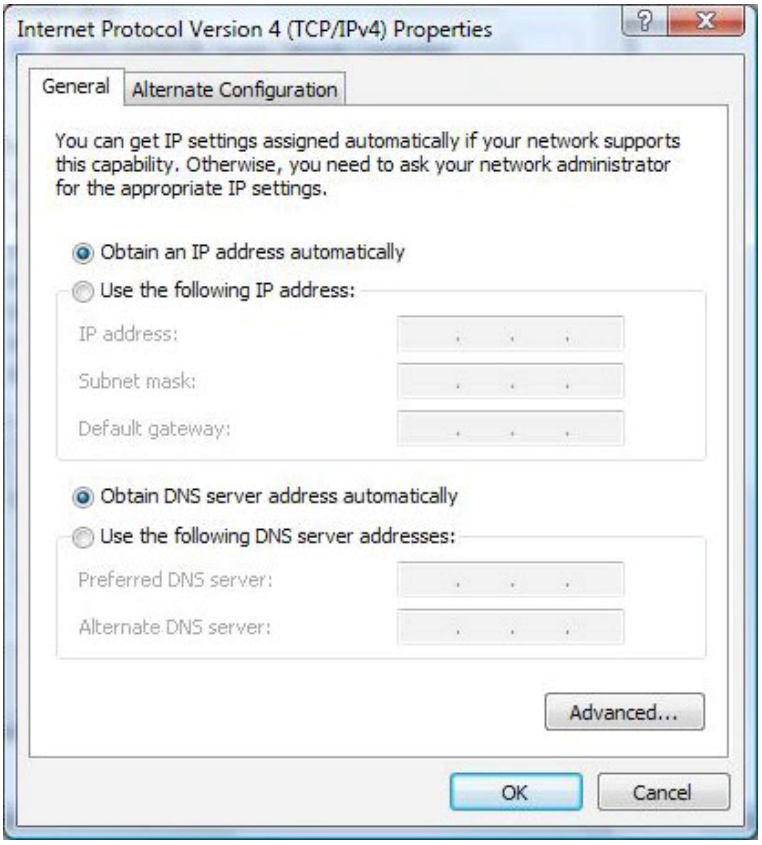


5. Select Internet Protocol Version 4 (TCP/IPv4) then click Properties.



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.

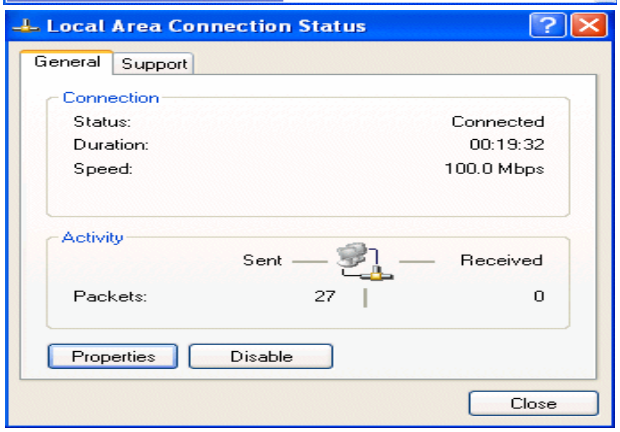
7. Click OK again in the Local Area Connection Properties window to apply the new configuration.



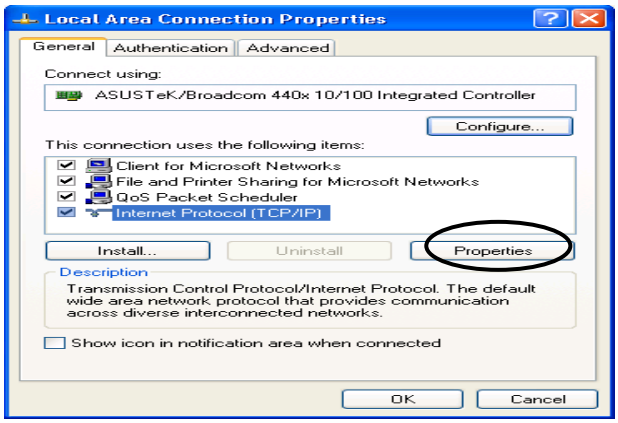
Configuring PC in Windows XP

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.

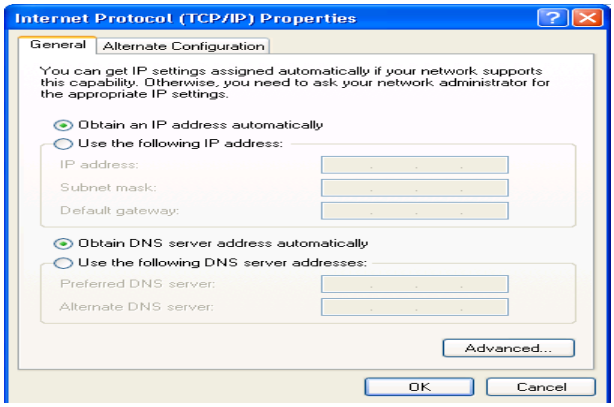


4. Select Internet Protocol (TCP/IP) and click Properties.



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

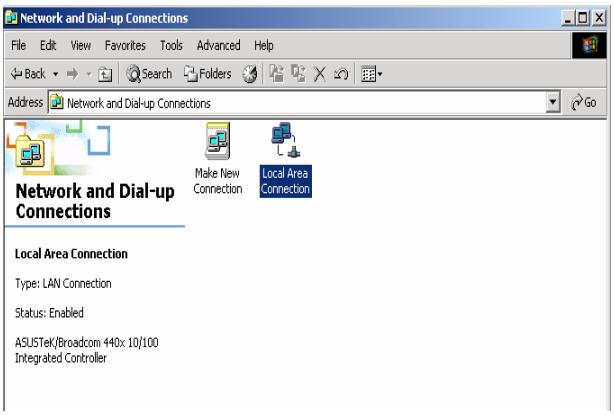
6. Click OK to finish the configuration.



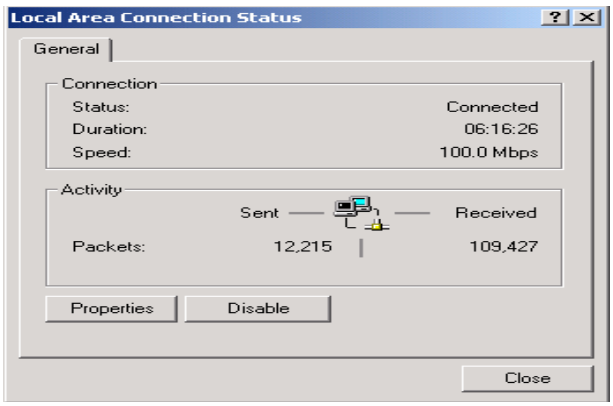
Configuring PC in Windows 2000

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

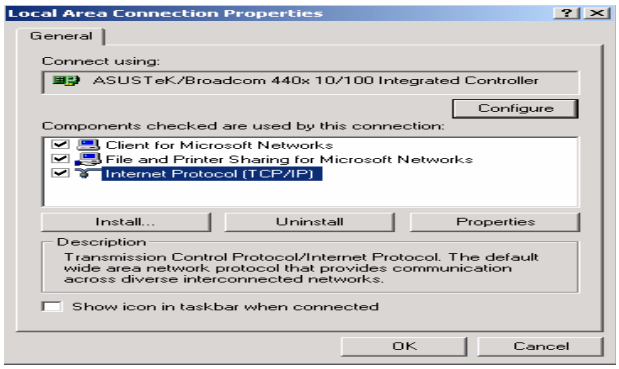
2. Double-click Local Area Connection.



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

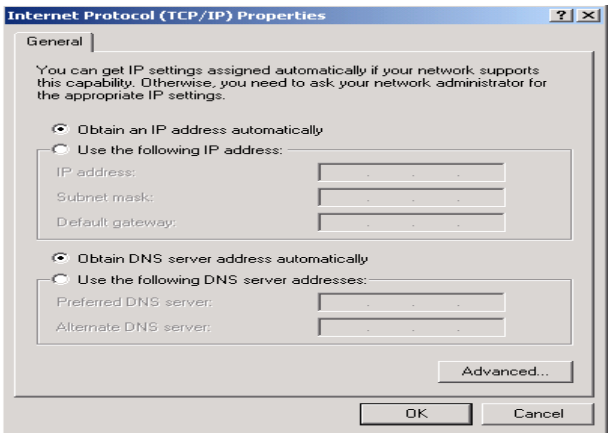


4. Select Internet Protocol (TCP/IP) and click Properties.



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

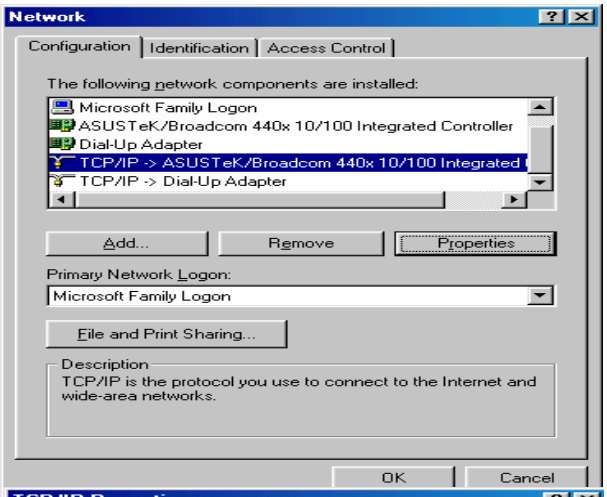
6. Click OK to finish the configuration.



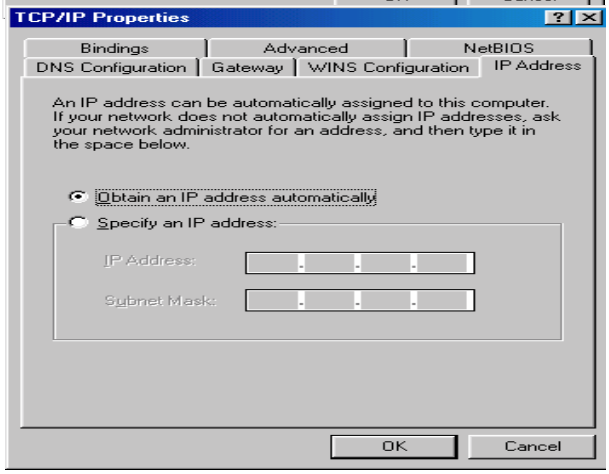
Configuring PC in Windows 95/98/Me

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.

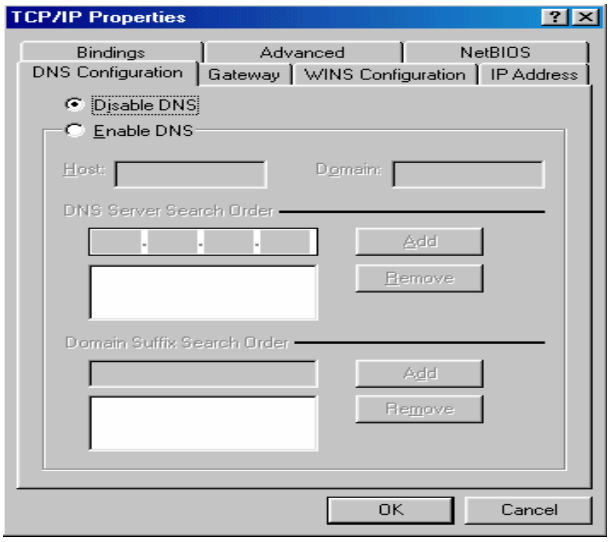


3. Select the Obtain an IP address automatically radio button.



4. Then select the DNS Configuration tab.

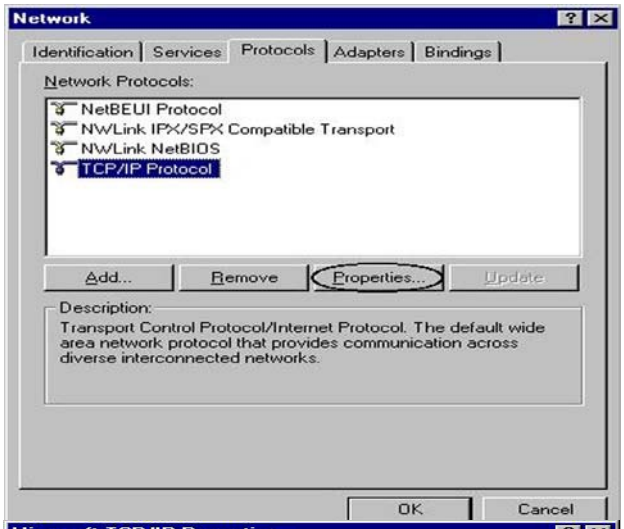
5. Select the Disable DNS radio button and click OK to finish the configuration.



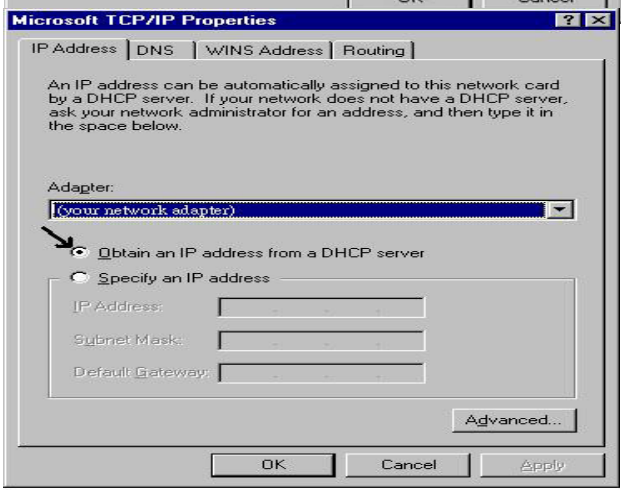
Configuring PC in Windows NT4.0

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

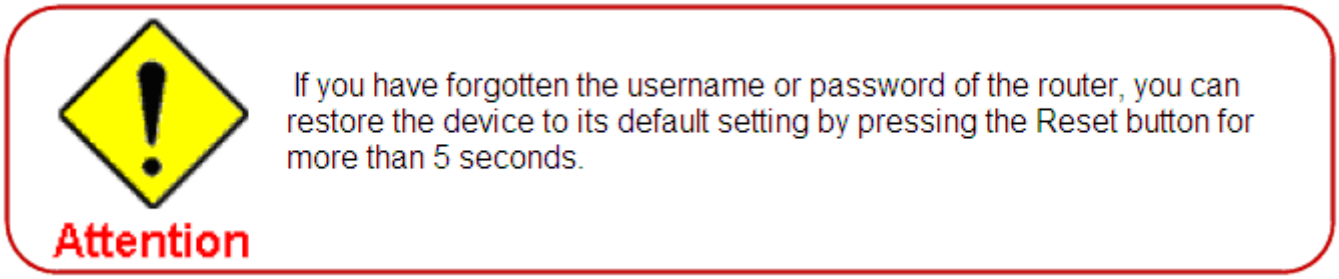
- Username: admin
- Password: admin

Local

- Username: user
- Password: user

Remote

- Username: support
- Password: support



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

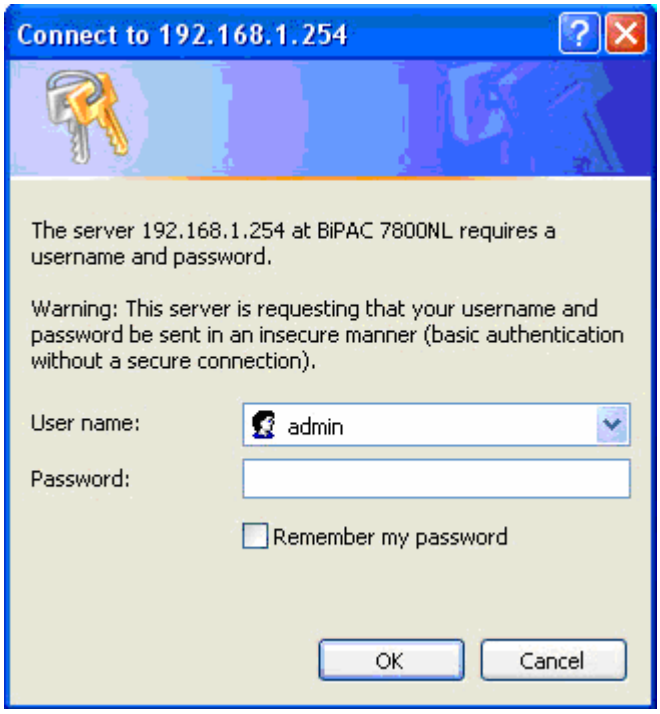
Before configuring this device, you have to check with your ISP (Internet Service Provider) to find out what kind of service is provided such as DHCP (Obtain an IP Address Automatically, Static IP (Fixed IP Address) or PPPoE.

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.

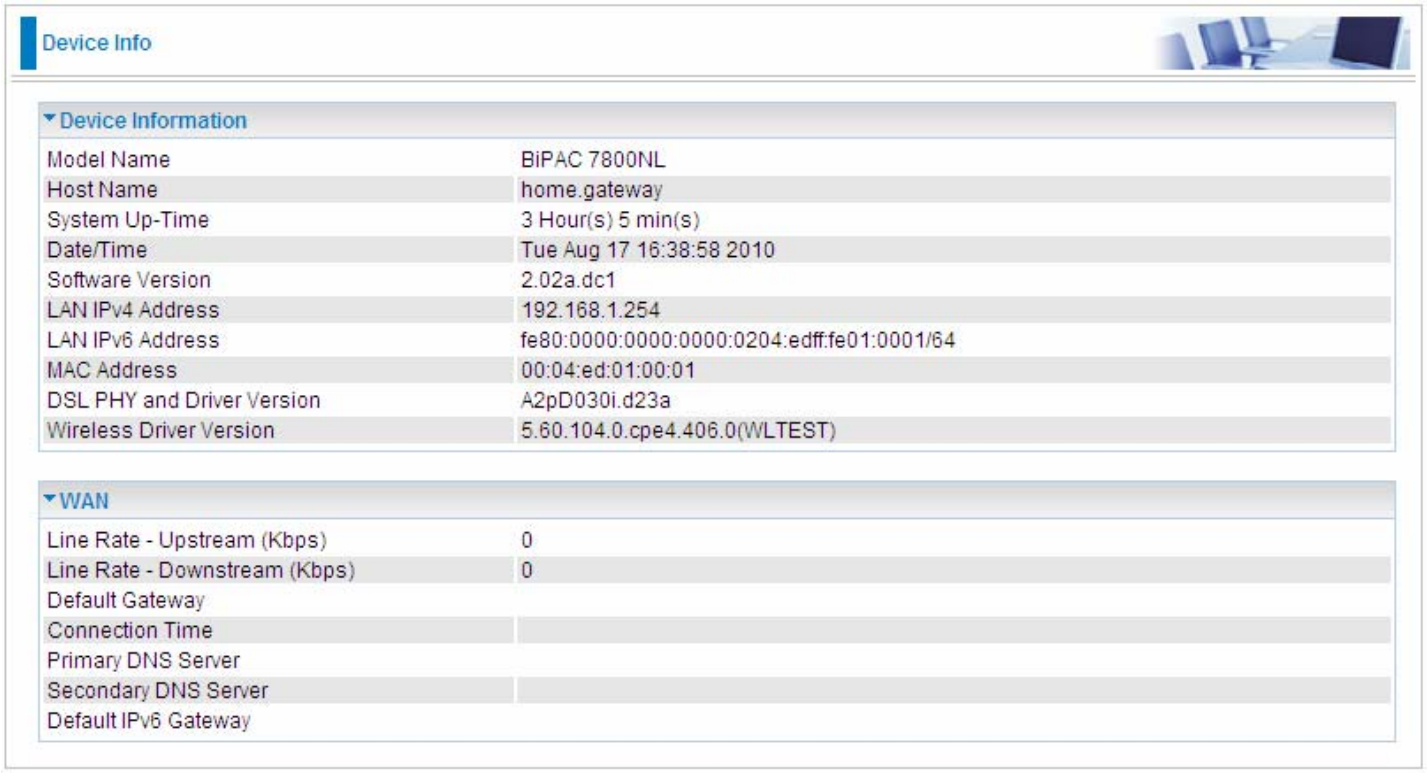
Configuration via Web Interface

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.



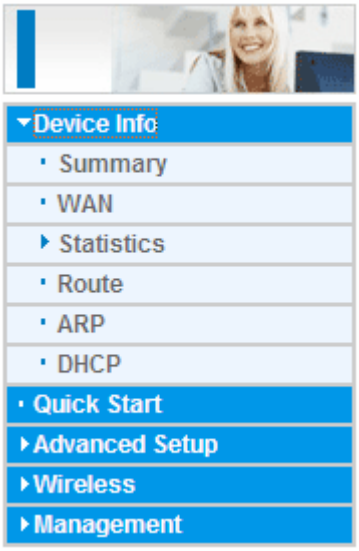
Chapter 4: Configuration

Once you have logged on to your BiPAC 7800NL 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)

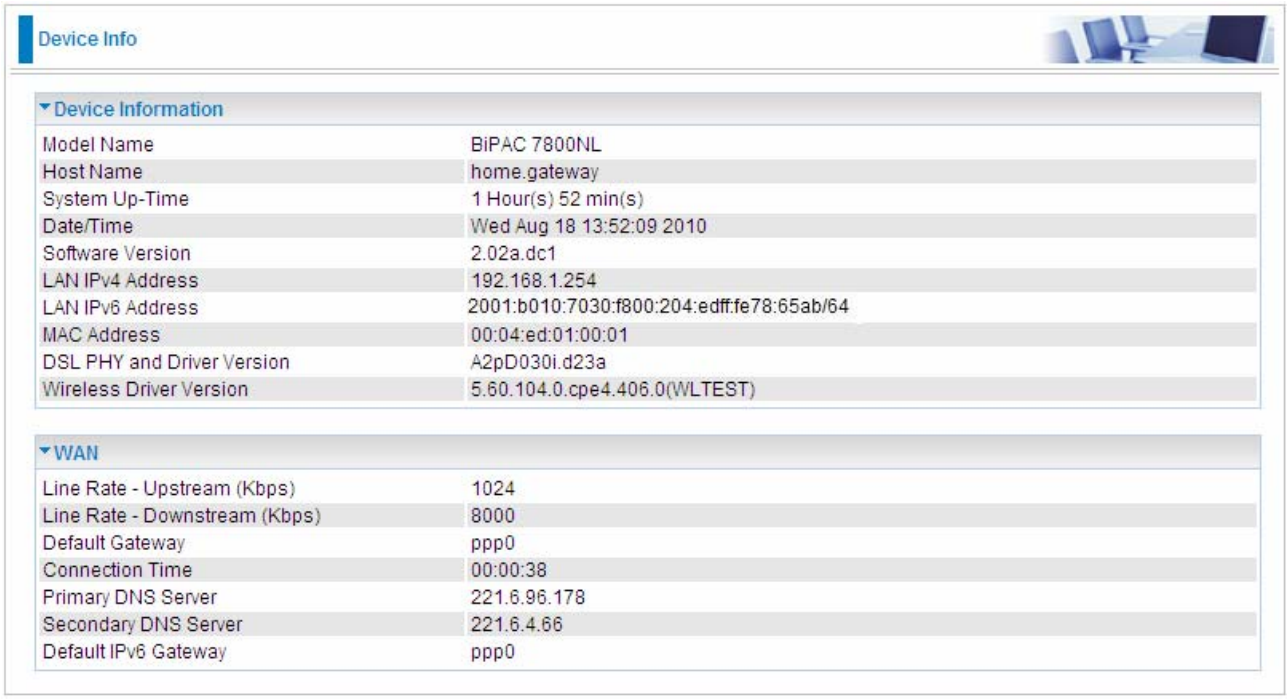
Device Info

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).



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.

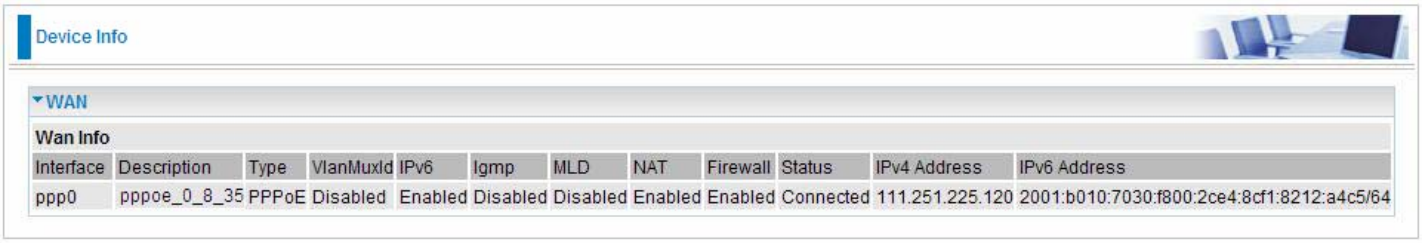
Primary DNS Server: Display IPV4 address of Primary DNS Server.

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.



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.

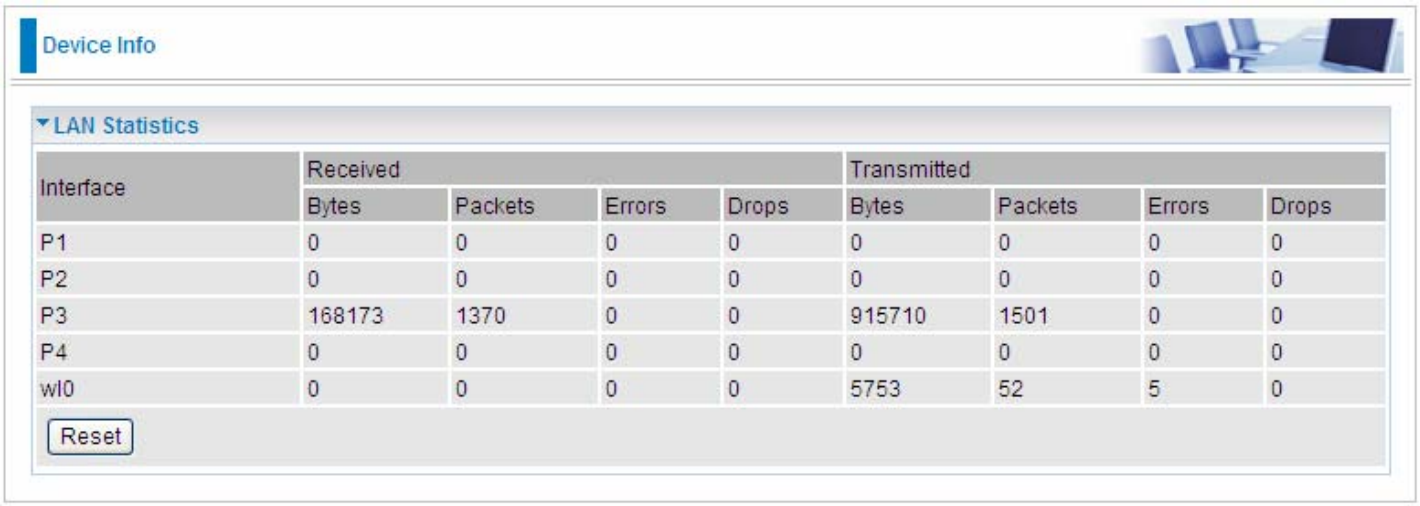
IPv4 Address: the WAN IPv4 Address the device obtained.

IPv6 Address: the WAN IPv6 Address the device obtained.

Statistics

LAN

The table shows the statistics of LAN.



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.

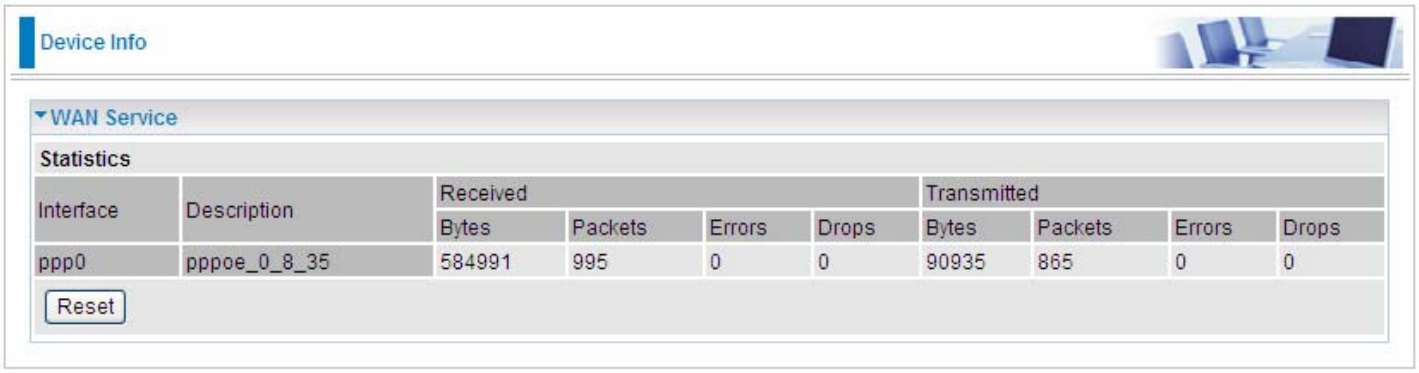
Errors: Display the statistics of errors arising in Receiving or Transmitting data.

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.



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 Packests.

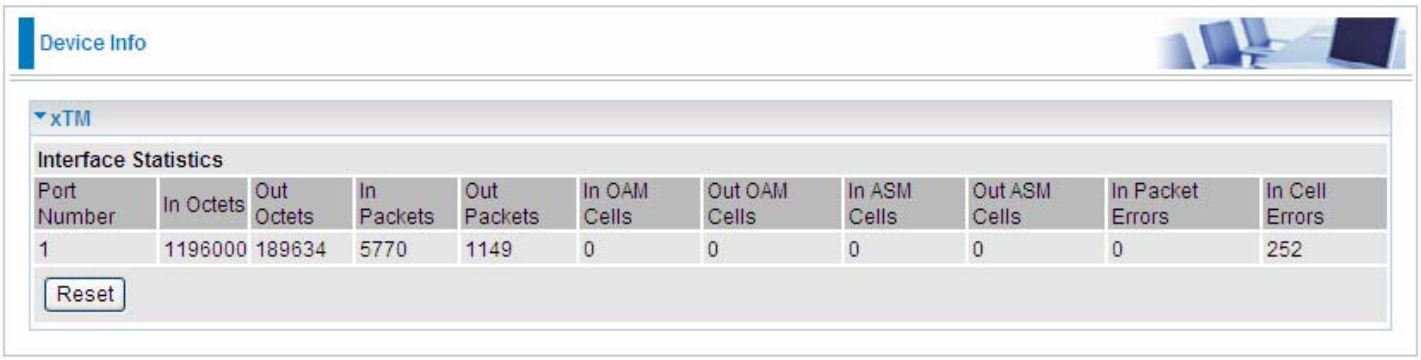
Errors: Display the statistics of errors arising in Receiving or Transmitting data.

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



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

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

xDSL BER Test 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.

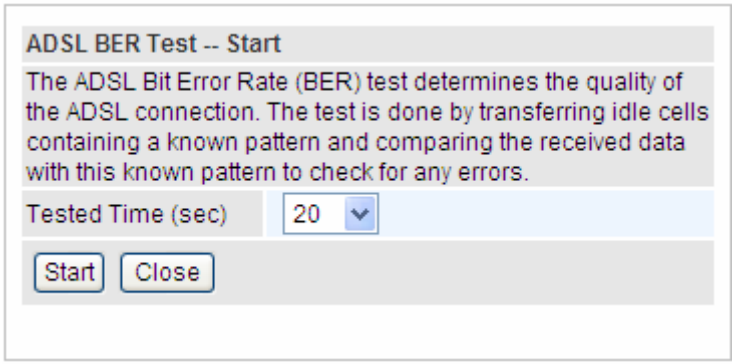
Bit Errors: Total number of bit errors.

Total ES: Total Number of Errored Seconds.

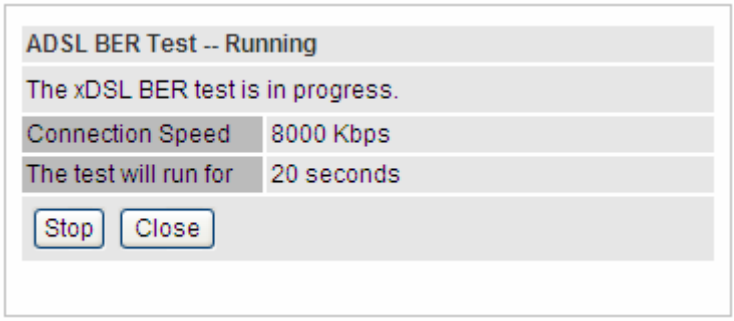
Total SES: Total Number of Severely Errored Seconds.

Total UAS: Total Number of Unavailable Seconds.

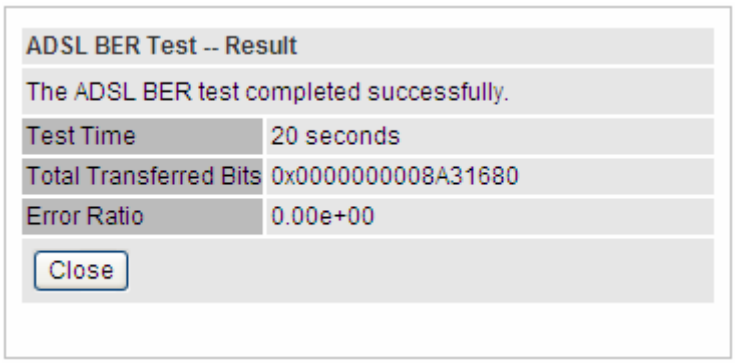
xDSL BER Test: Click this button to start a bit Error Rate Test. The ADSL Bit Error Rate (BER) test determines the quality of the ADSL connection. The test is done by transferring idle cells containing a known pattern and comparing the received data with this known pattern to check for any errors.



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

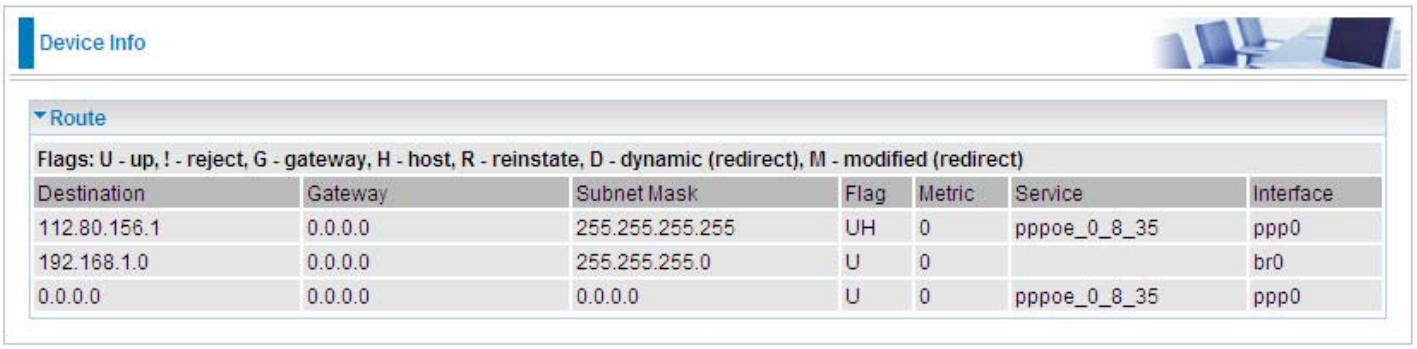


When it is OK, the following test result window will appear. You can view the quality of ADSL connection. Here the connection is OK.



Reset : Click this button to reset the statistics.

Route



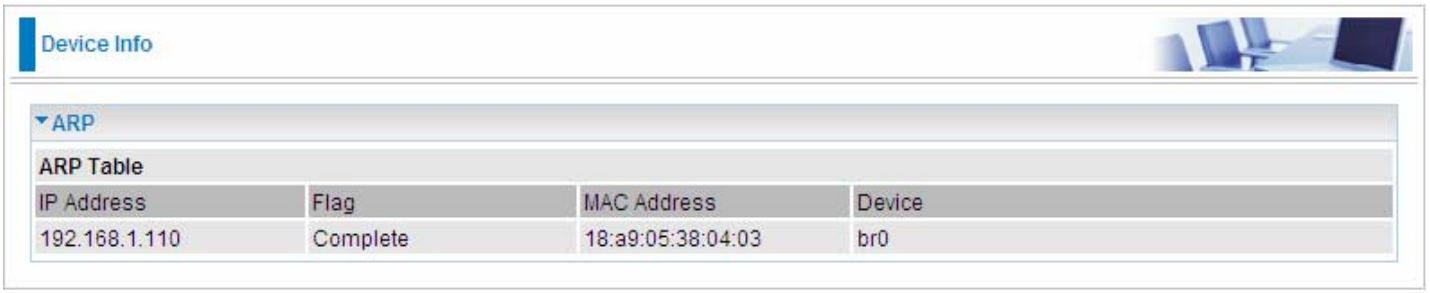
Destination: the IP address of destination network.
Gateway: the IP address of the gateway this route uses.
Subnet Mask: the destination subnet mask.
Flag: show the status of the route.

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



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

Flag: Shows the current status of the ARP entries.

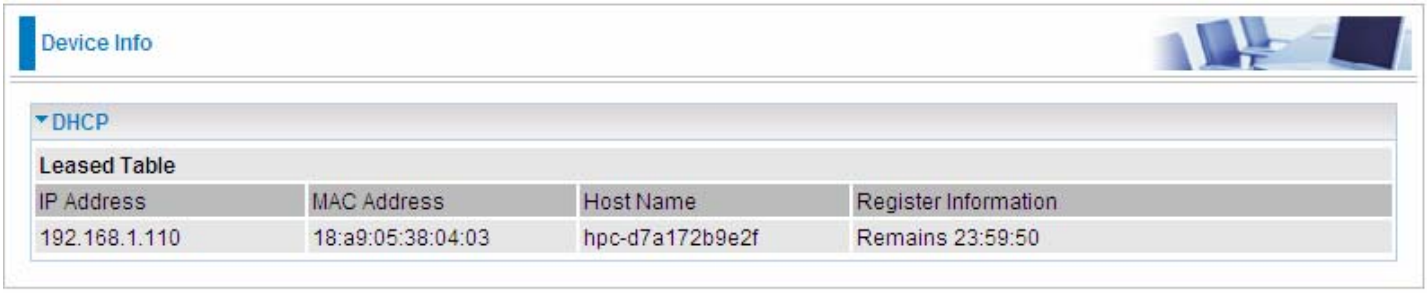
- Complete: the route resolving is processing well.
- M(Marked as permanent entry): the route is permanent.
- P (publish entry): publish this route item.

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.



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

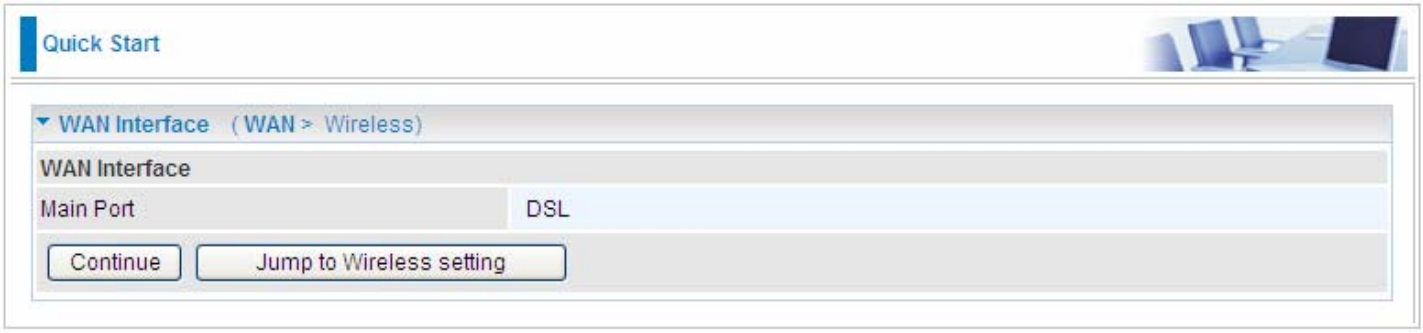
MAC Address: The MAC Address of internal DHCP client host.

Host Name: The Host Name of DHCP client.

Register Information: Show the remaining time information during registration.

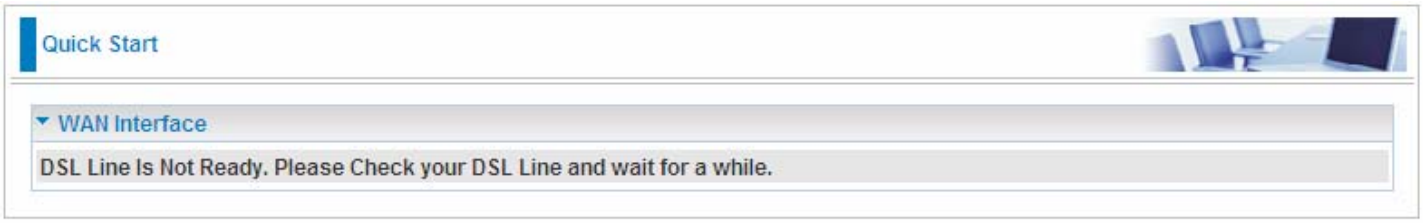
Quick Start

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

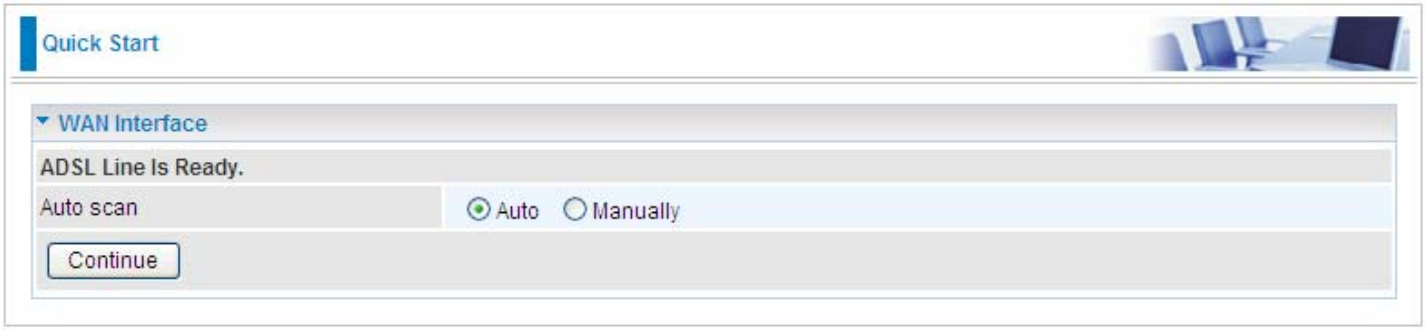


1. To configure DSL, press **Continue** to go on to next step, or if you only want to configure Wireless, press **Jump to Wireless setting** to go to step 8.

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.

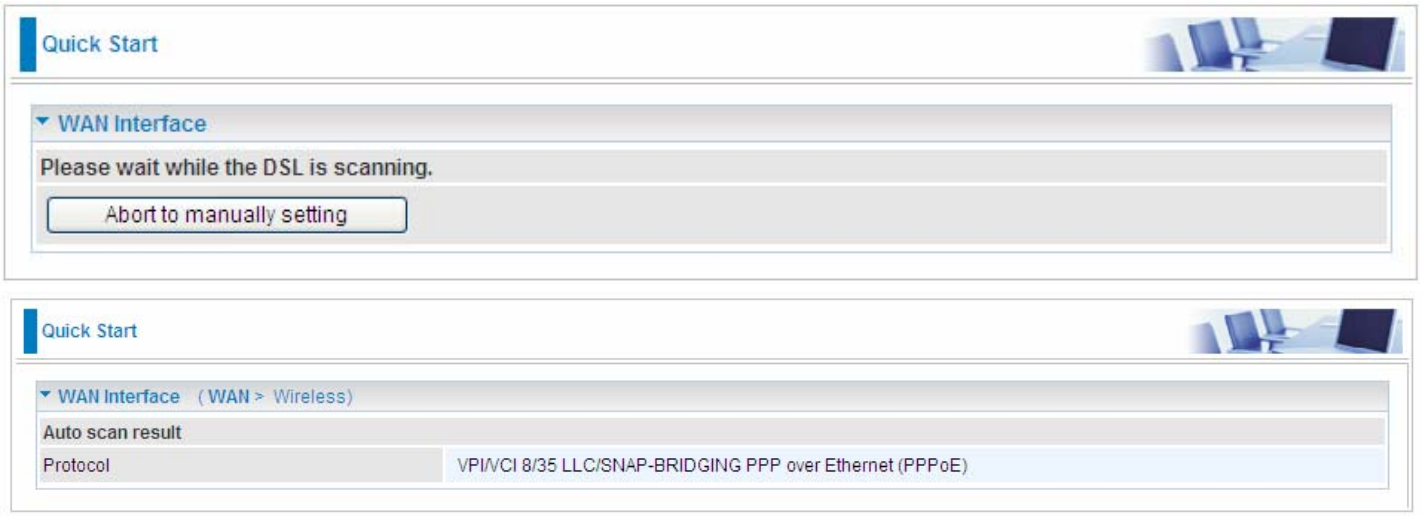


Screen 1



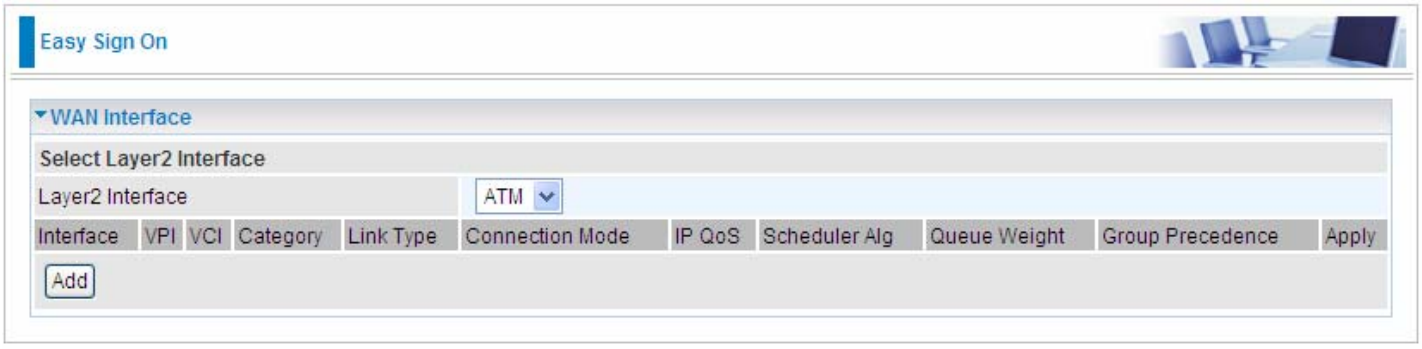
Screen 2

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.

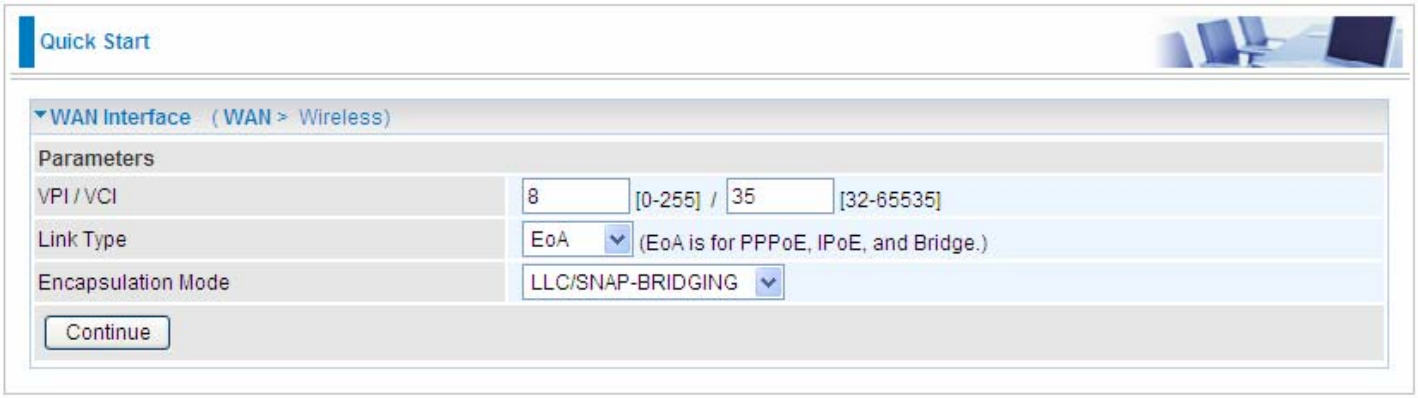


Screen 3

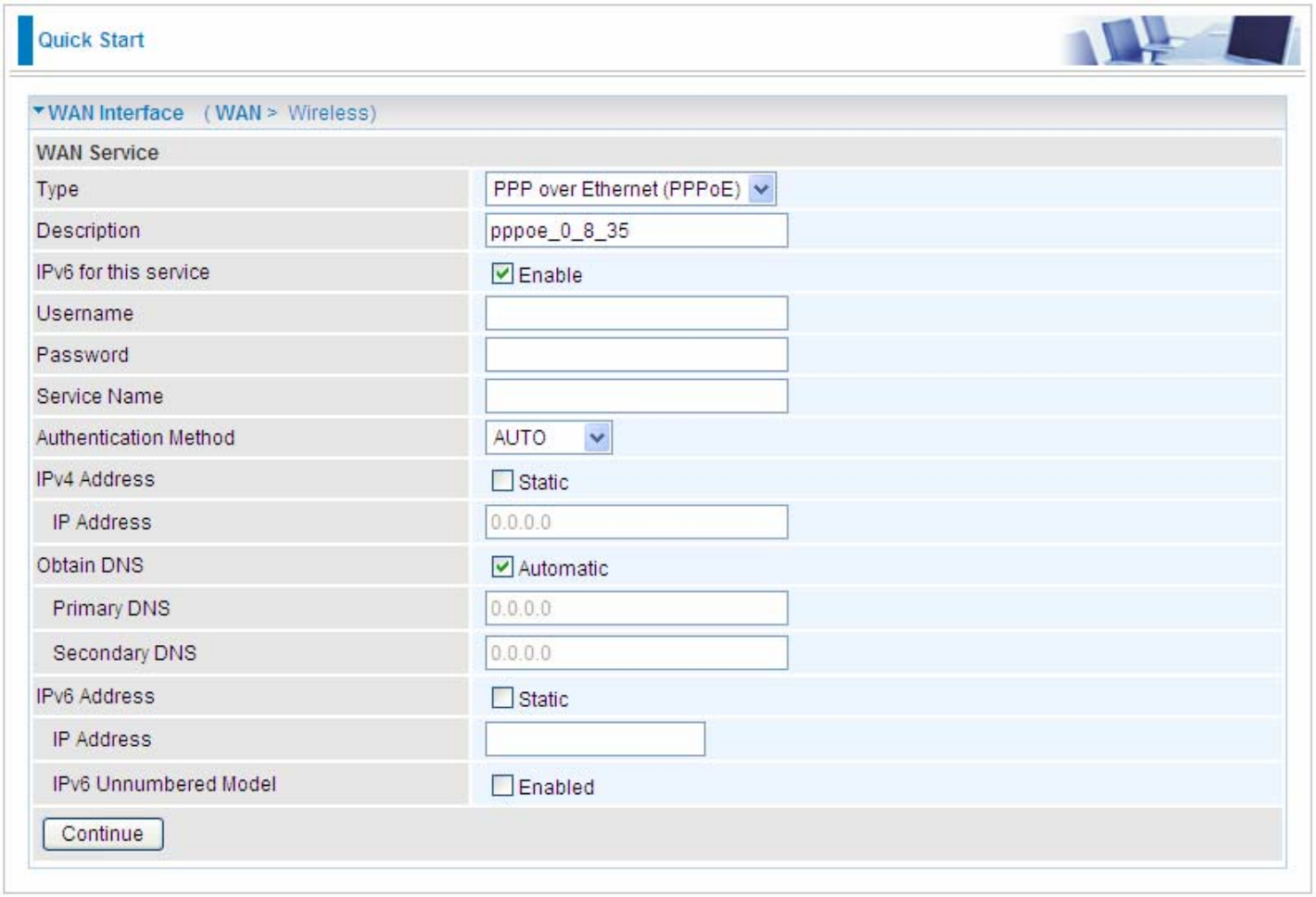
4. Here you should select the Layer2 Interface. ATM and PTM are two kinds of transmission mode. You can select according to your ISP. Select ATM for example. Click **Add** to add WAN Interface.



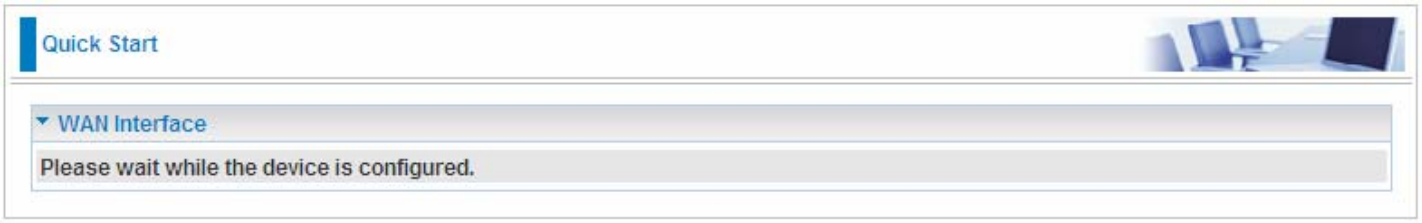
5. Enter the VPI/VCI from your ISP.



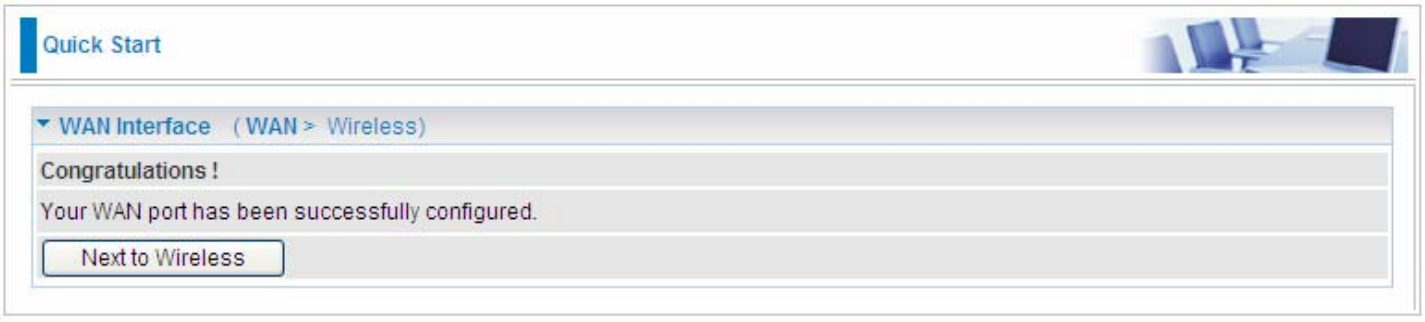
6. Enter the username, password from your ISP, for IP and DNS settings, also refer to your ISP. Here IPv6 service is enabled by default.



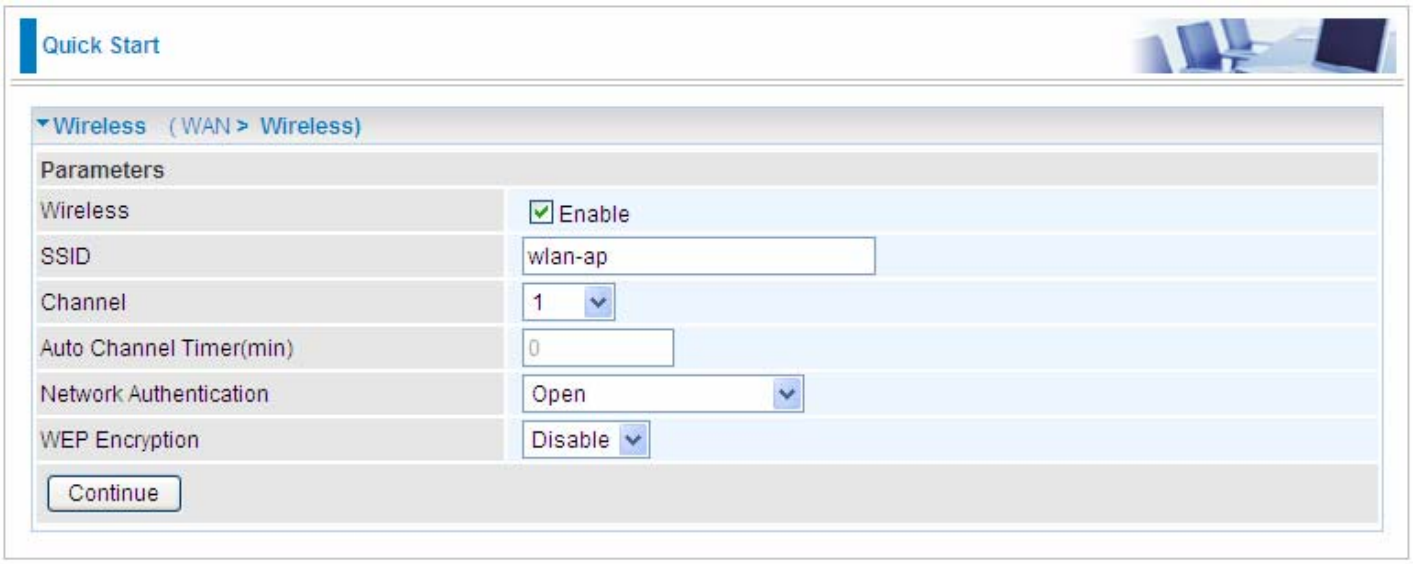
7. Wait while the device is configured.



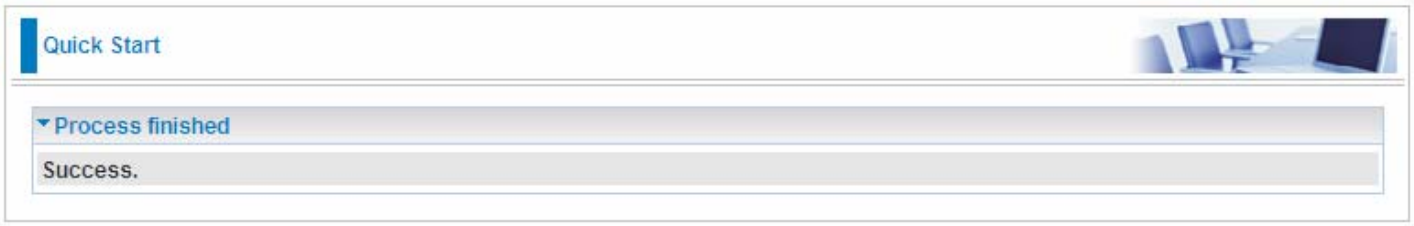
8. WAN port configuration is success.



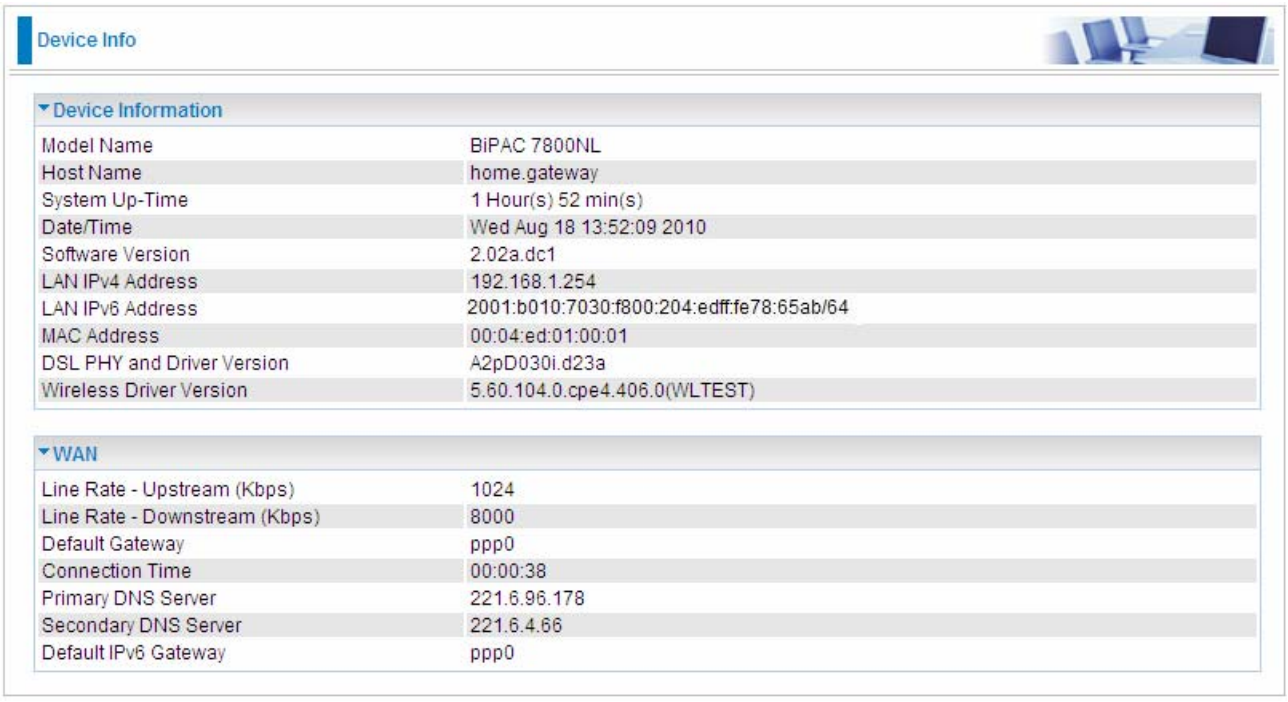
9. After the configuration is successful, click **Next to Wireless** button and you may proceed to configure the Wireless setting. For security information, please turn to **wireless>security** section in this manual for help.



10. Configuration's success.



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

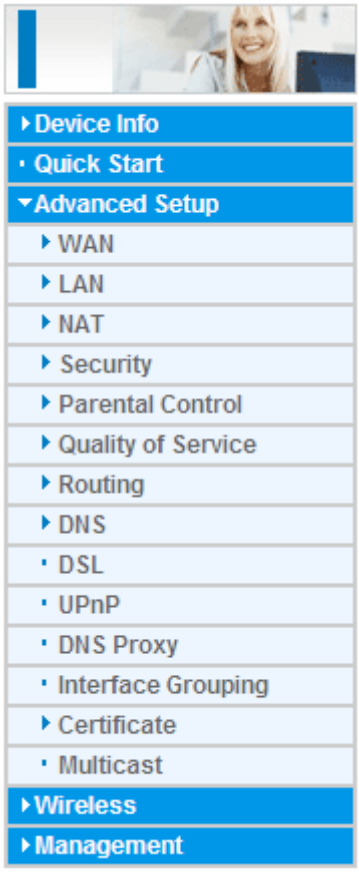


For more information, turn to **Advanced setup** for help.

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

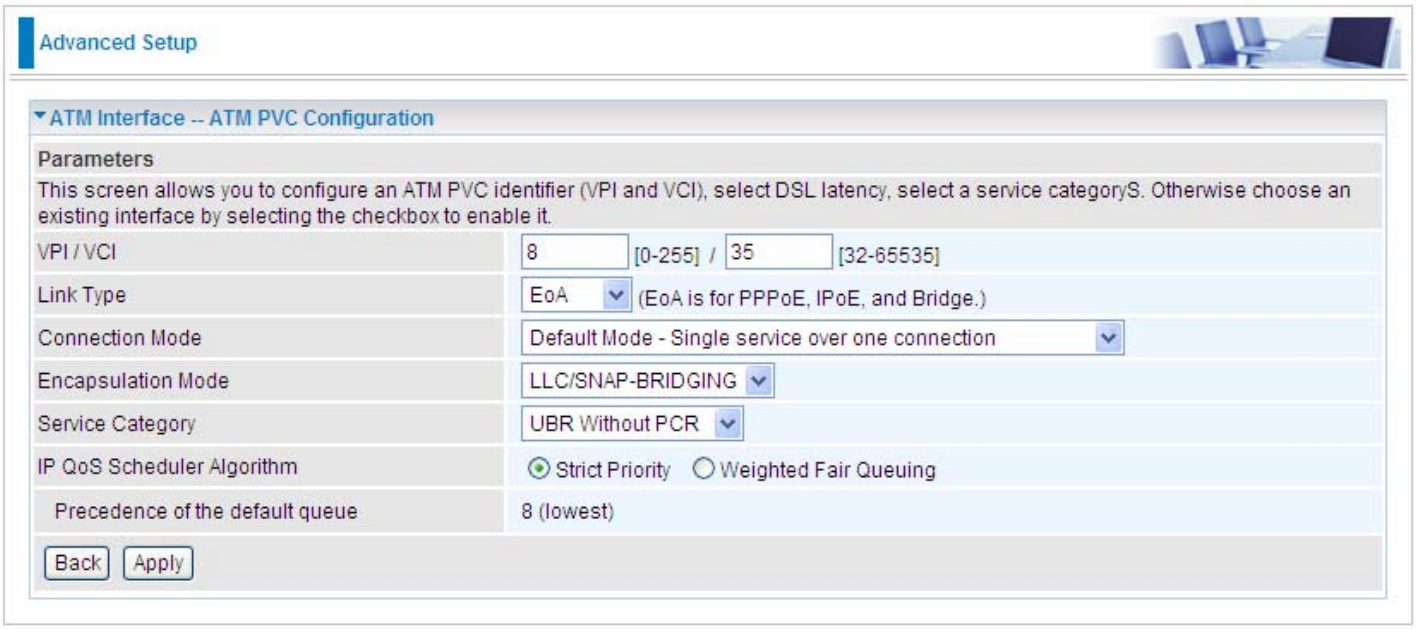
A WAN (Wide Area Network) is a computer network that covers a broad geographical area (eg. Internet) that is used to connect LAN and other types of network systems. There are the items within the WAN section: **WAN Interface** and **WAN Service**.

WAN Interface

ATM

Layer2 Interface: 2 transfer mode, ATM or PTM.

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



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

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

Connection Mode:

- **Default Mode:** this mode only allows single service over one connection.
- **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**

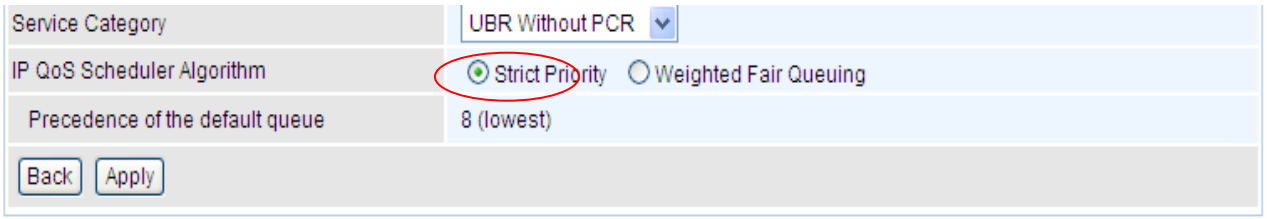
Mode Parameter will be hided if you select PPPoA or IPoA in Link Type.

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.

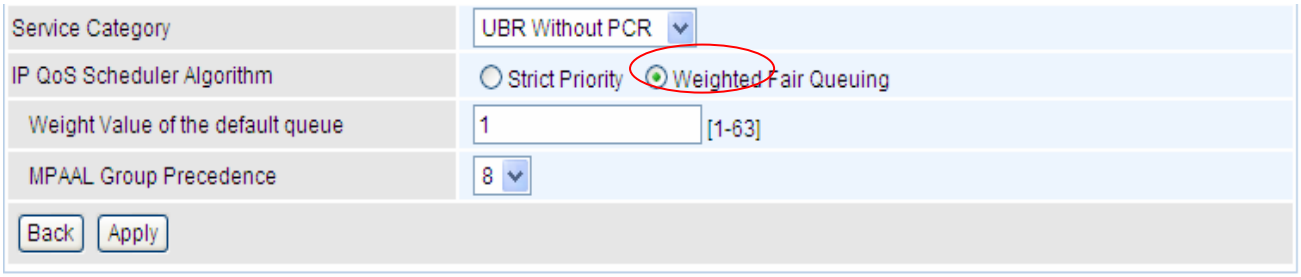
- **UBR without PCR: UBR(Unspecified Bit Rate), PCR(Peak cell Rate)**

  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.



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)

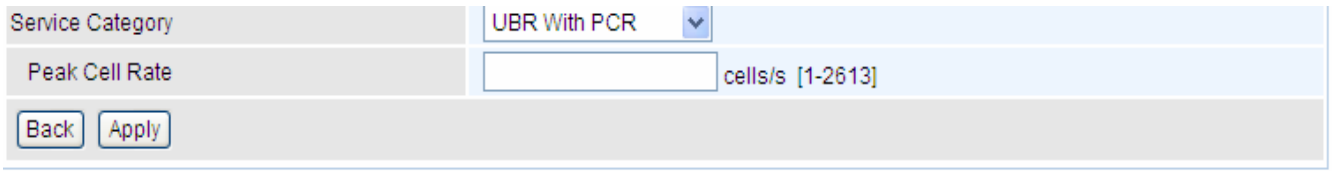


Weight Value of default queue: enter the value, 1-63, the highest is 63.

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

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

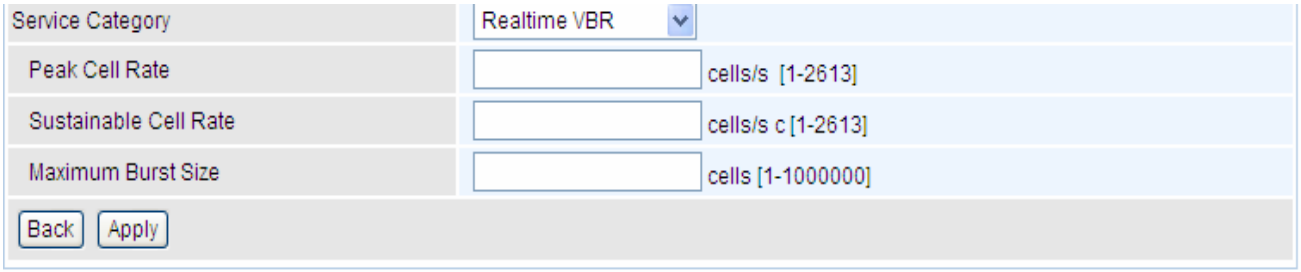
UBR is a kind of service providing constant rate service, is idea for timely and fixed bandwidth needed service.



Peak Cell Rate: enter Peak Cell Rate.

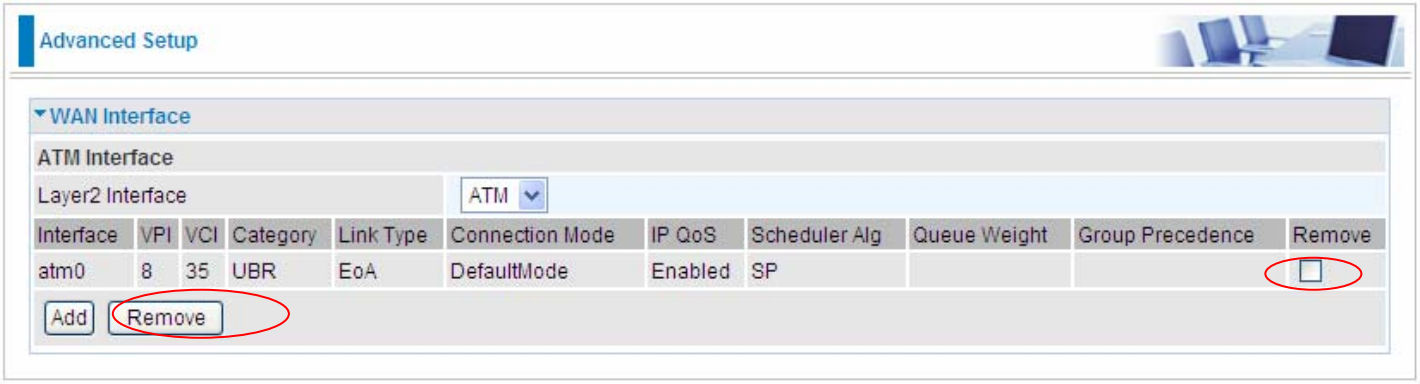
ⓘ None Realtime VBR/ Realtime VBR(Variable Bit Rate)

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.



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

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

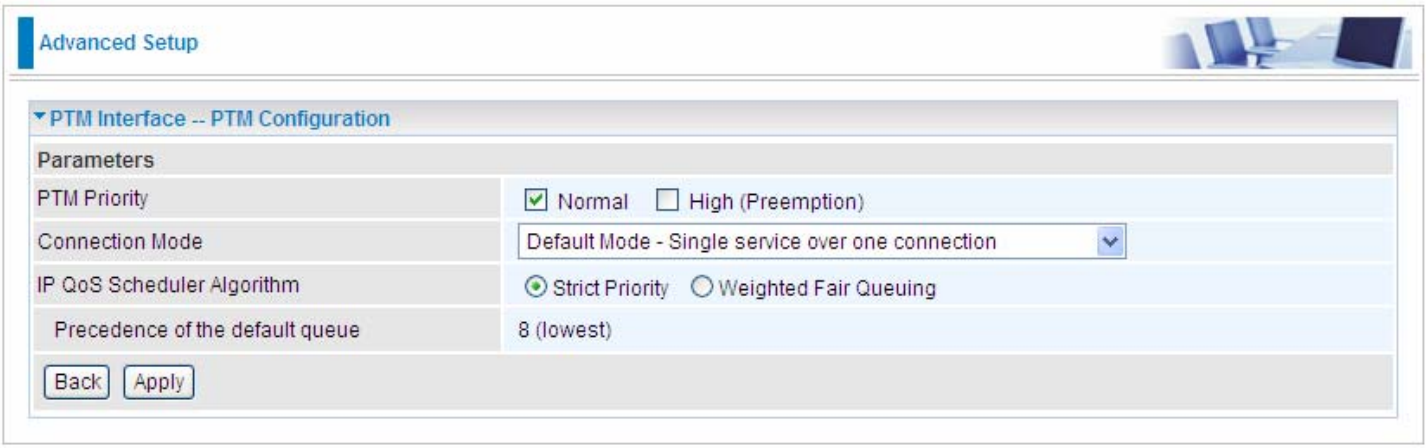


Check the remove checkbox, then press **Remove** to delete it only if this interface are not used by a WAN Service, if it is used by a WAN service, first remove the WAN service, then turn back to remove the interface.

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

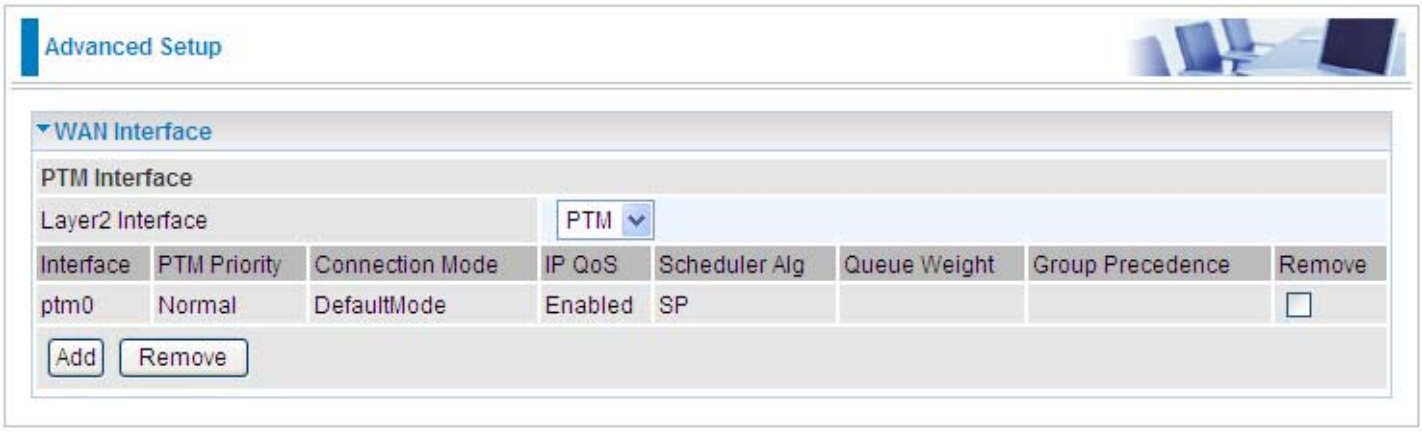
PTM

PTM Setting is similar to ATM.

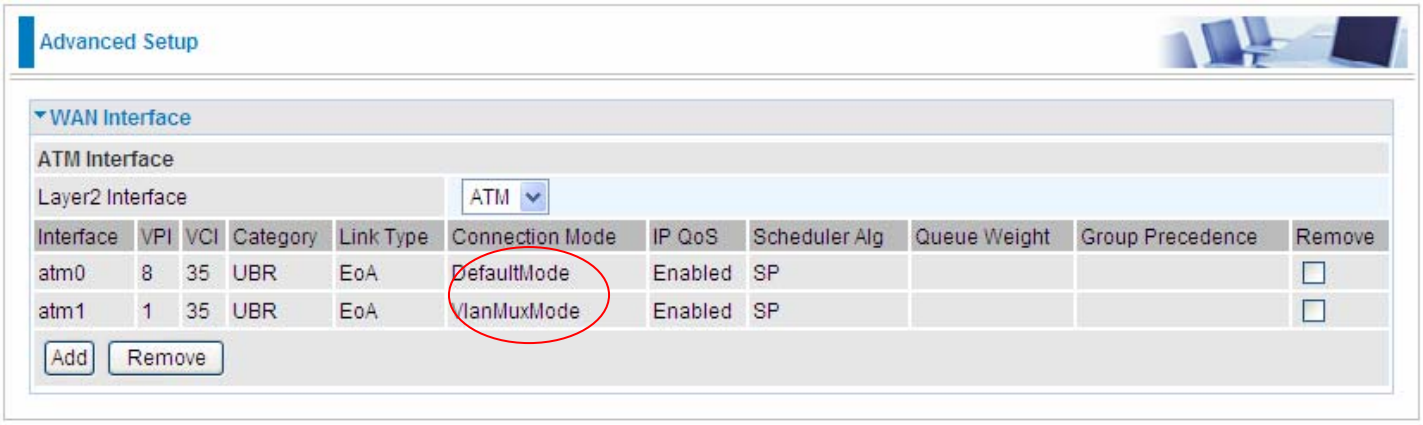


PTM Priority: Select the PTM priority, Normal or High.

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

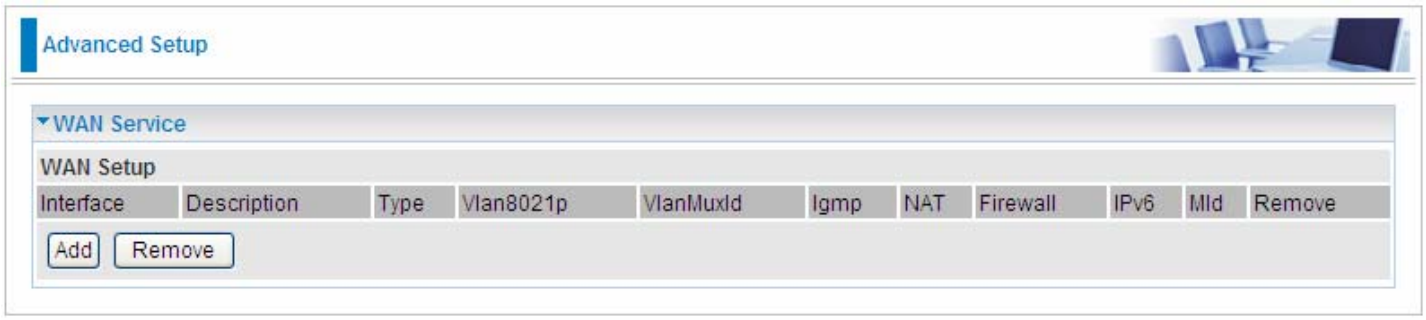


Now follow the above steps, we set two ATM WAN interfaces for future illustration, one is of DefaultMode, and one is of VlanMuxMode.



WAN Service

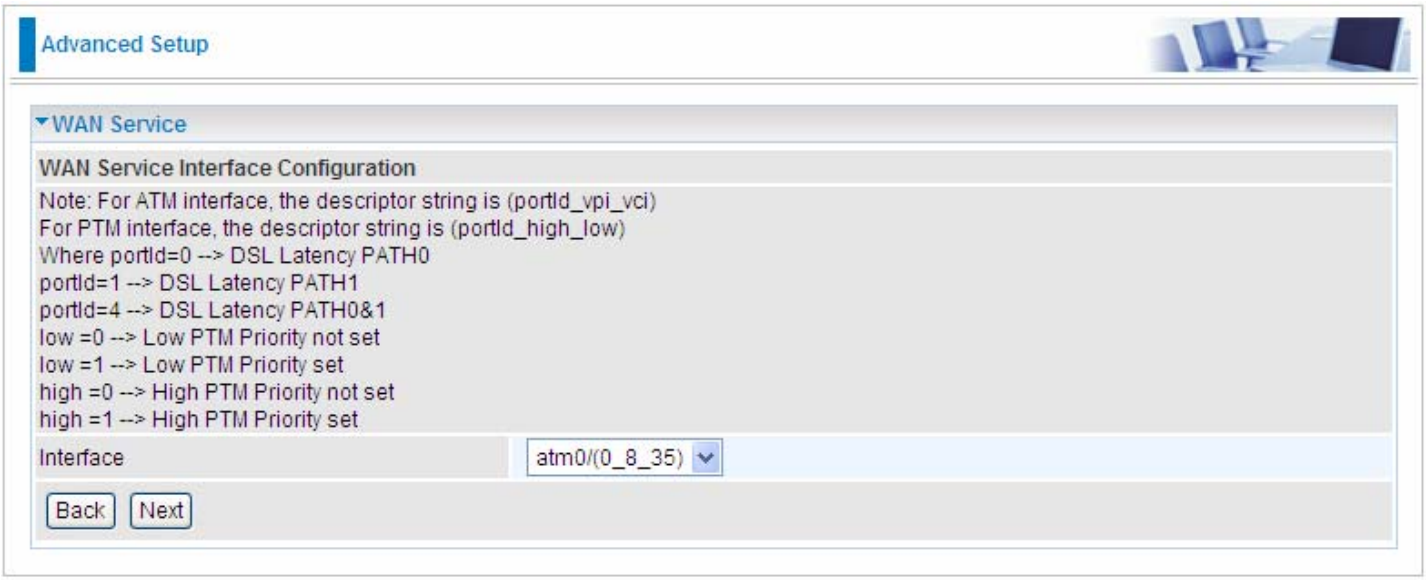
WAN Service allows you configure one or more services over one interface (connection). The following is the WAN Service listing table. Your configured WAN service will be listed here.



Default Connection mode

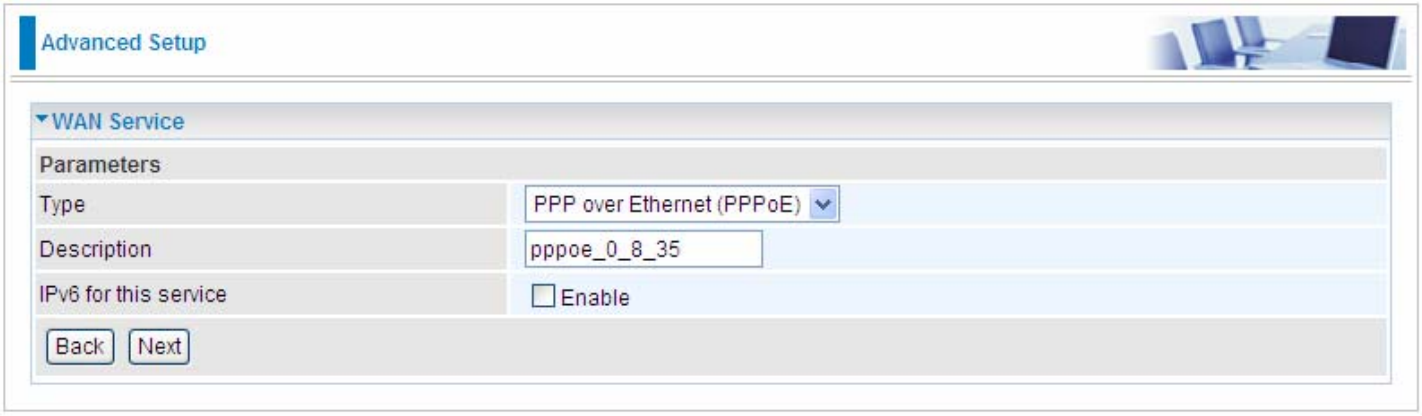
Select the interface which is a Default mode connection configured in WAN Service, here for example, in the following, atm0/(0_8_35) is a Default mode connection.

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



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

PPPoE



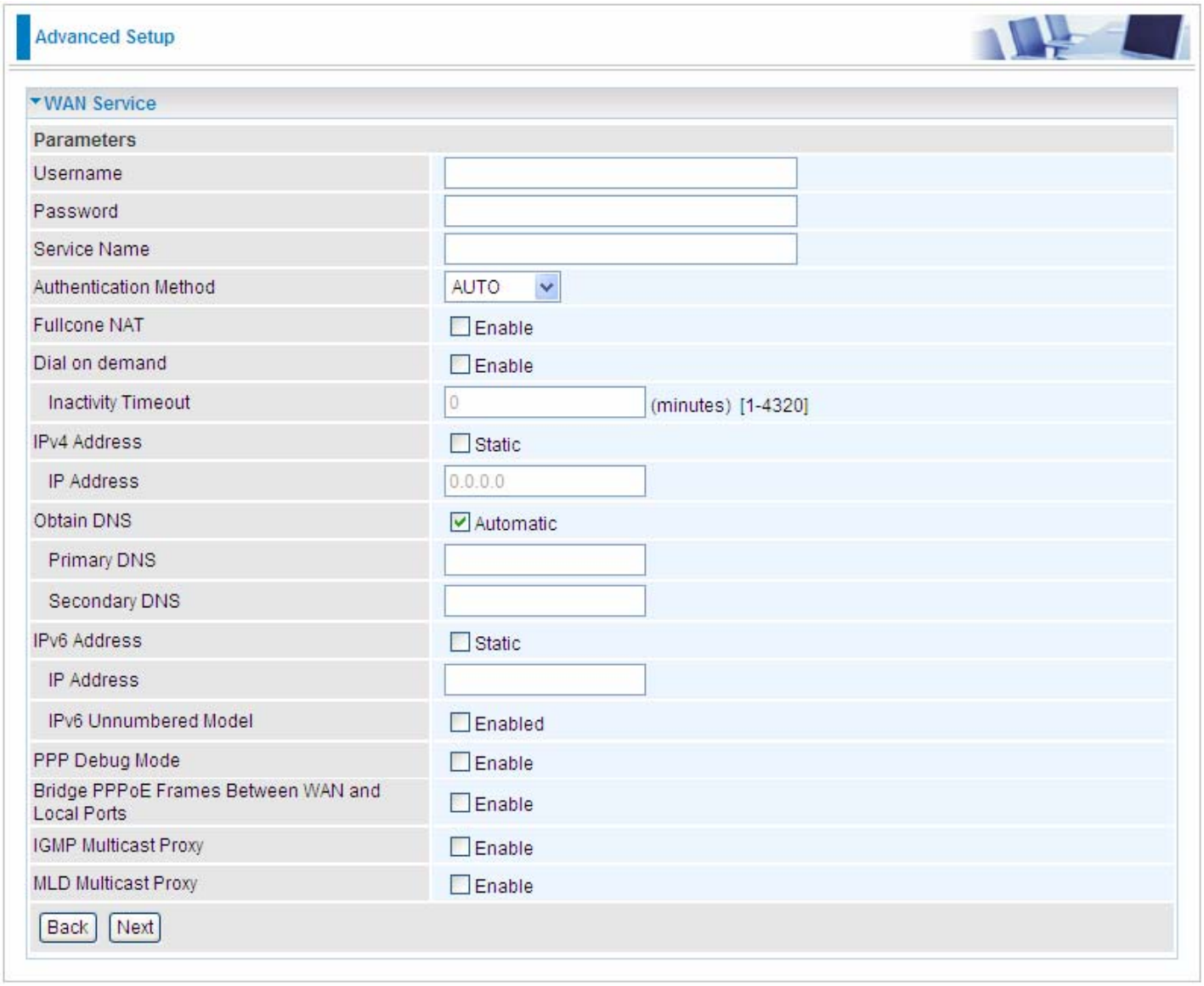
Type: select the protocol advised by your ISP, here select PPPoE.

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



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.

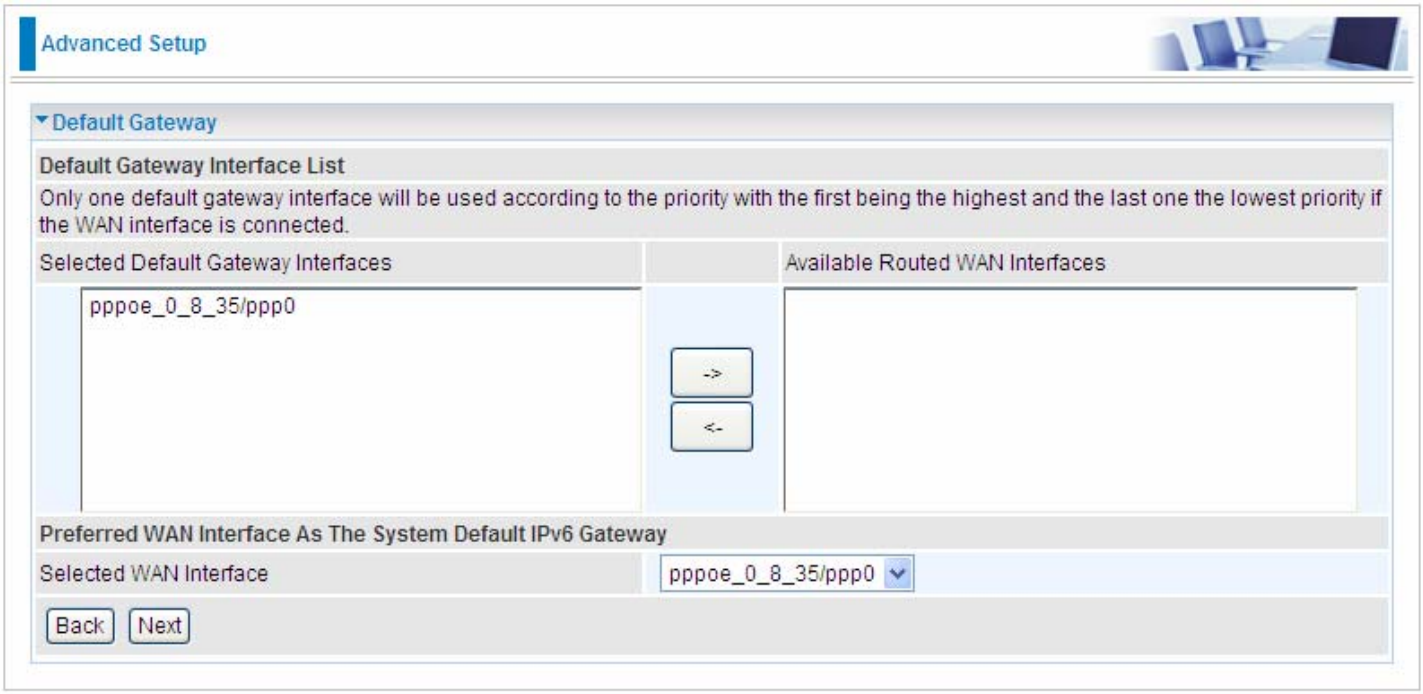
PPPoE Debug mode: check whether to enable this function, it is used to debug PPPoE link, and the debug message will be seen in **System log.**

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 (**Internet Group Management** Protocol) Proxy intercepts the IGMP request from Clients and forwards it to the router after some dealings.

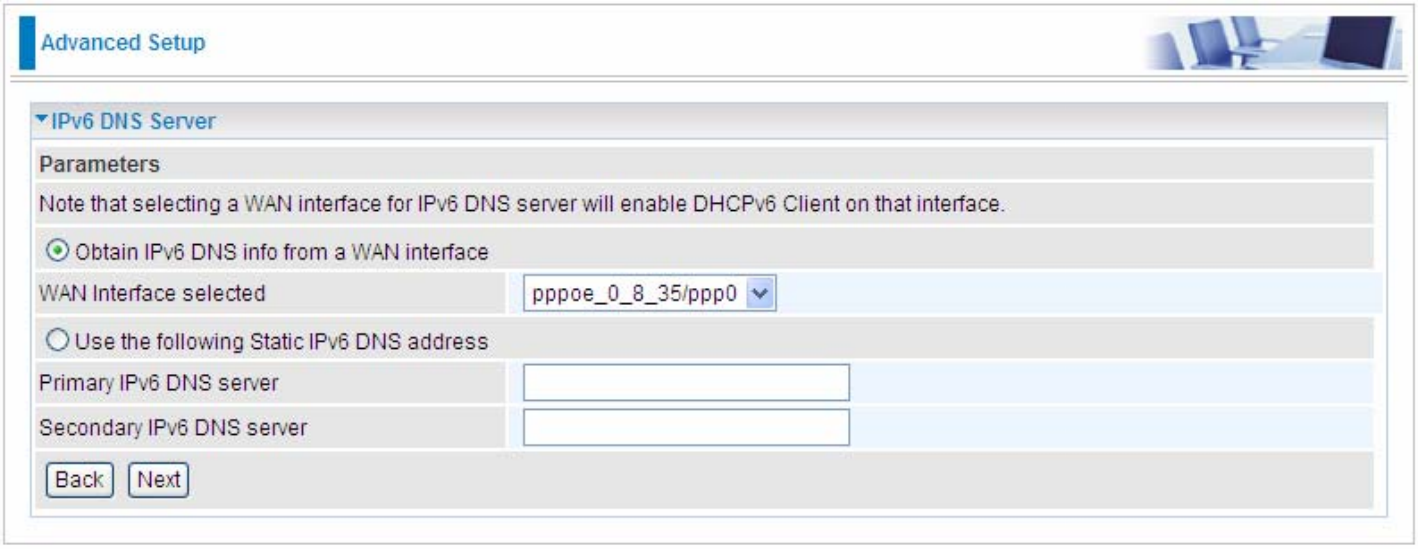
MLD Multicast Proxy: check whether to enable this function. MLD (**Multicast Listener Discovery** Protocol) Proxy intercepts the MLD request from Clients and forwards it to the router after some dealings. Support MLDv1 and MLDv2.

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



Set the default gateway and the default IPv6 gateway.

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



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

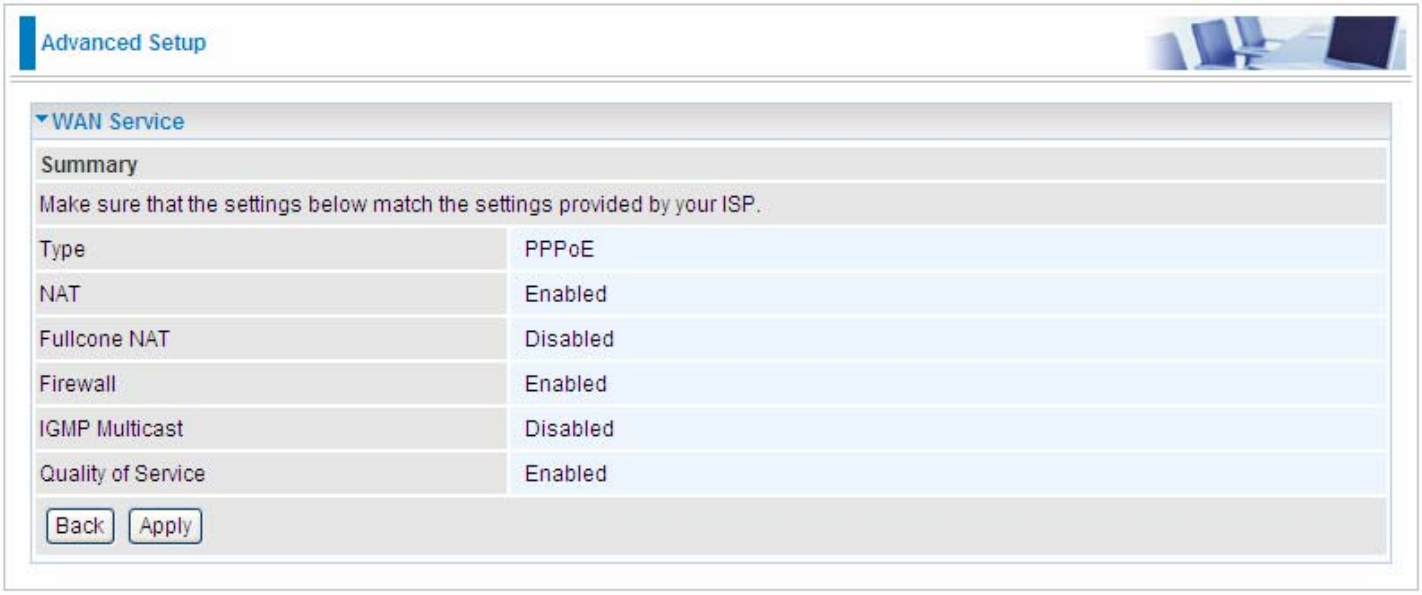
Obtain IPv6 DNS info from a WAN interface

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

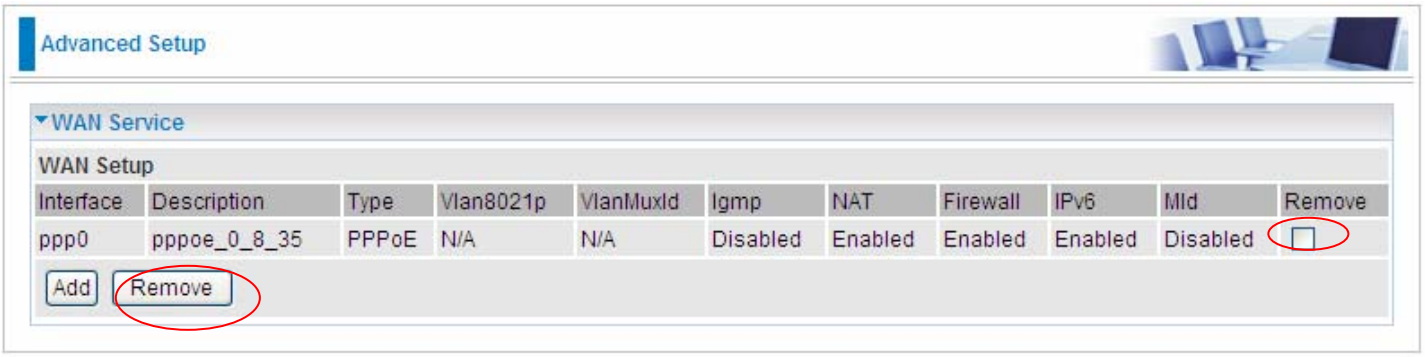
Use the following Static IPv6 DNS address

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

Click **Next** to check the settings.

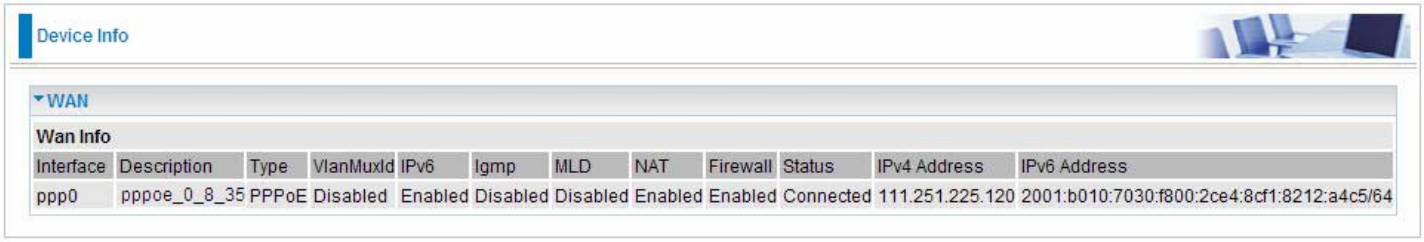


If you confirm, click Apply to submit the settings and return to WAN service page.

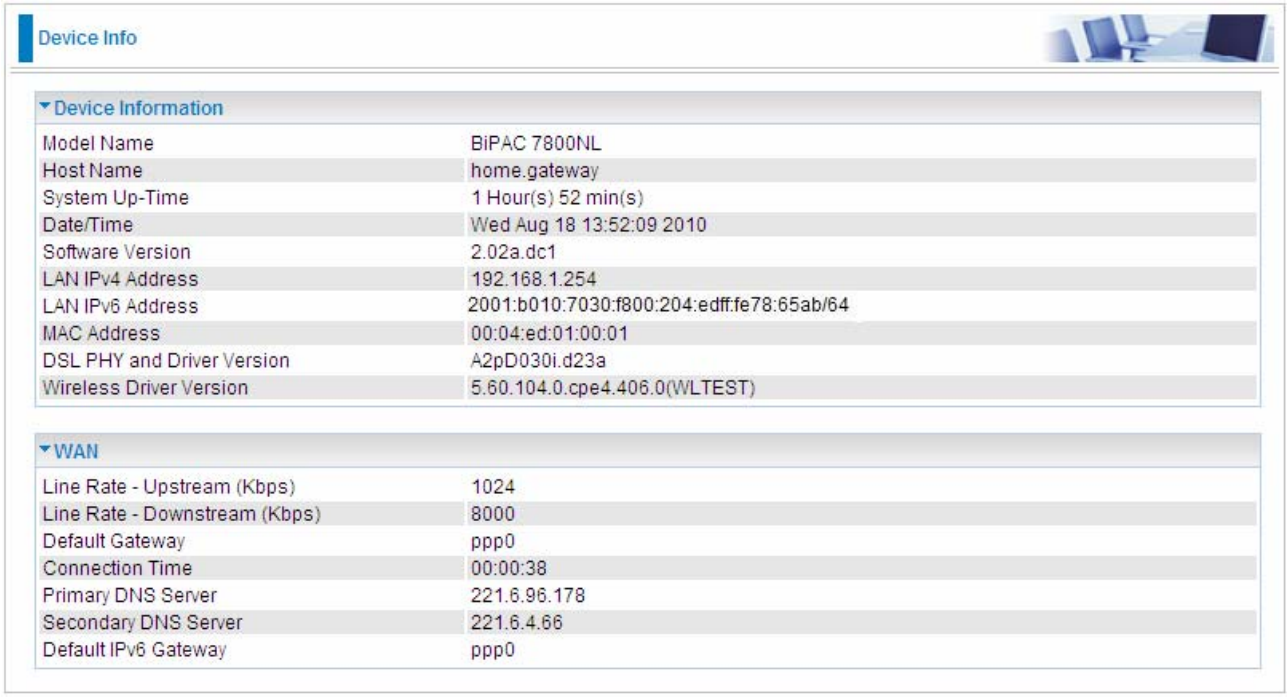


If you don not need the service, select the item you want to remove, check the checkbox, then press **Remove**, it will be OK.

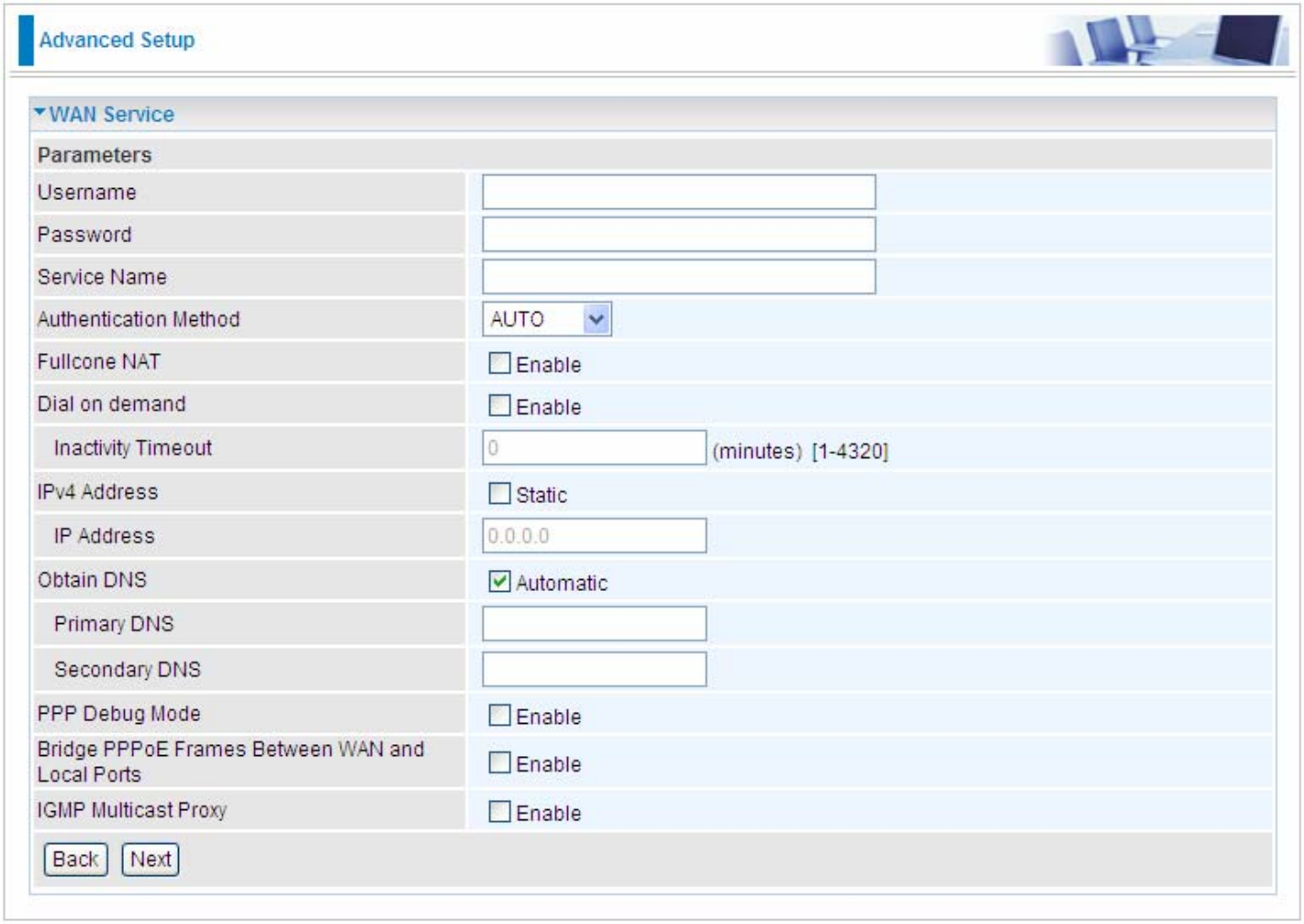
Here the corresponding WAN interface and WAN Service have been configured, if it is OK, you can access the internet. You can go to **Device Info>WAN** or **Summary** to view the WAN connection information (if your ISP provides IPv6 service, then you will obtain an IPv6 address).



The device summary information



IPv6 disabled



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.

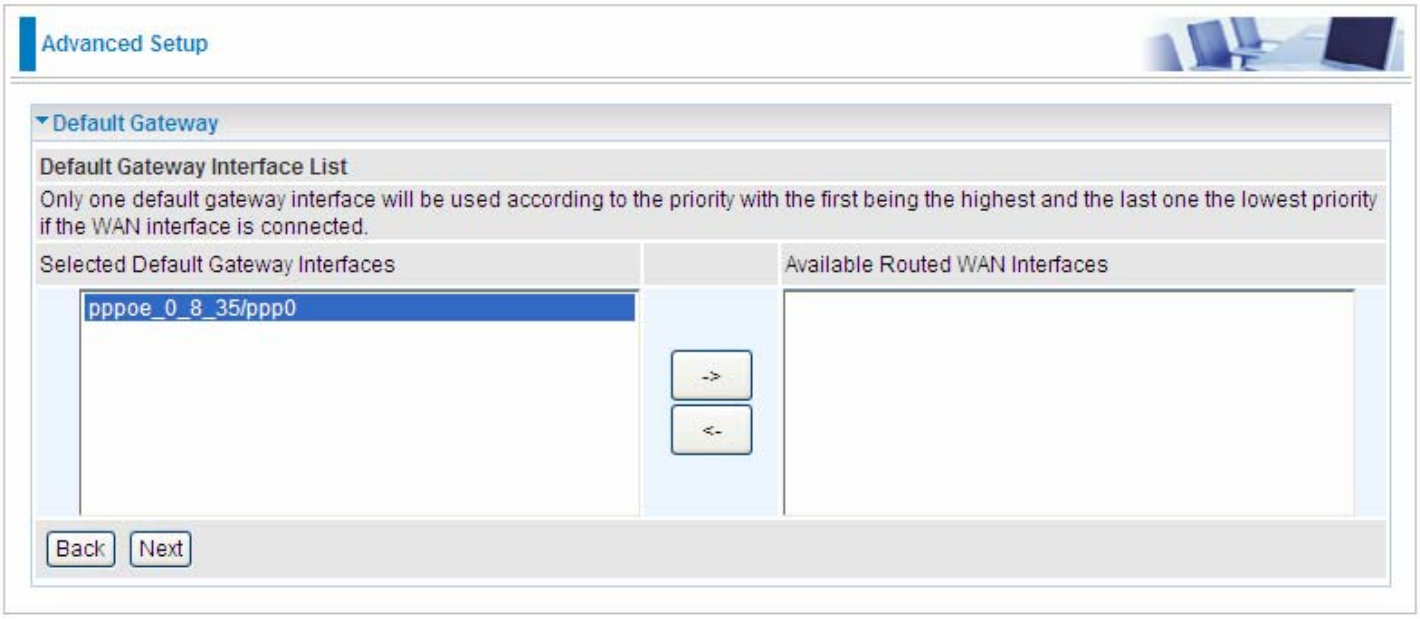
Primary/Secondary DNS: if you uncheck Obtain DNS, then enter then primary/secondary DNS address.

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.**

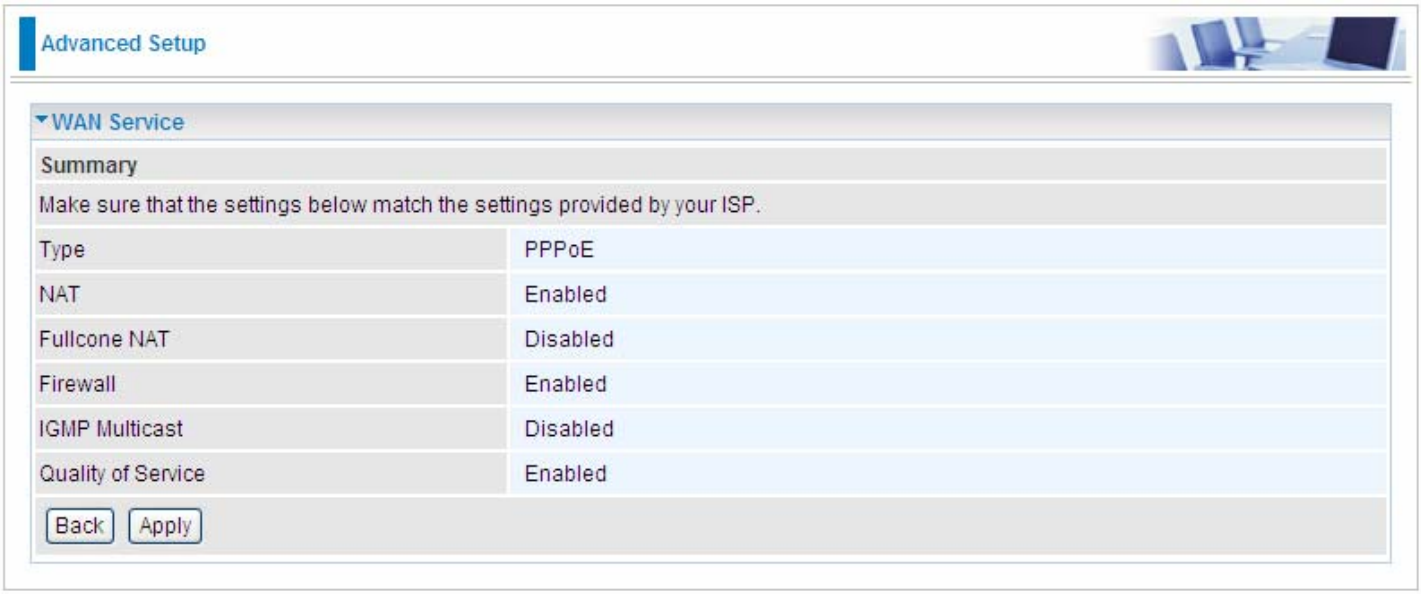
Bridge PPPoE Frame between WAN and Local Ports: check whether to enable this function. It allows PC in LAN to set up its own PPP link, or the PC will access internet via the PPP link in WAN port.

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.

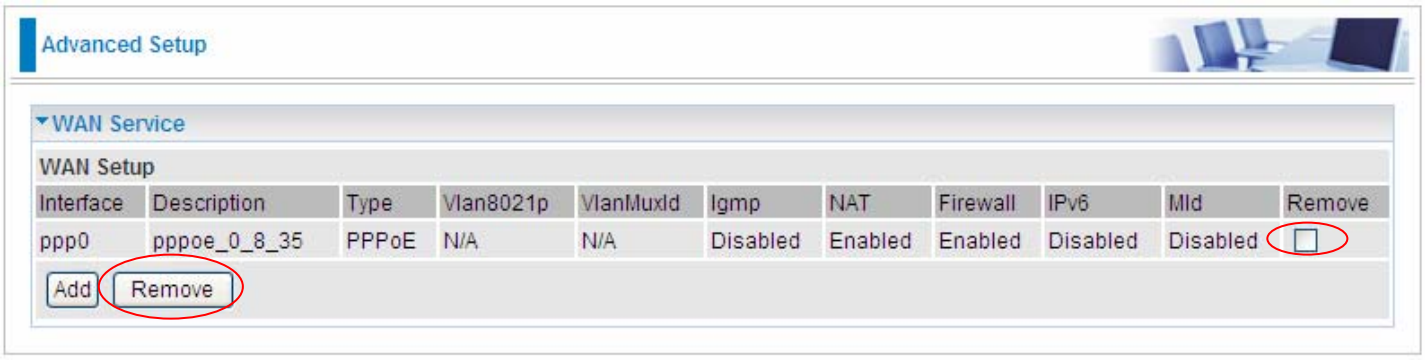
Click **Next** to go on to the Default Gateway setting.



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

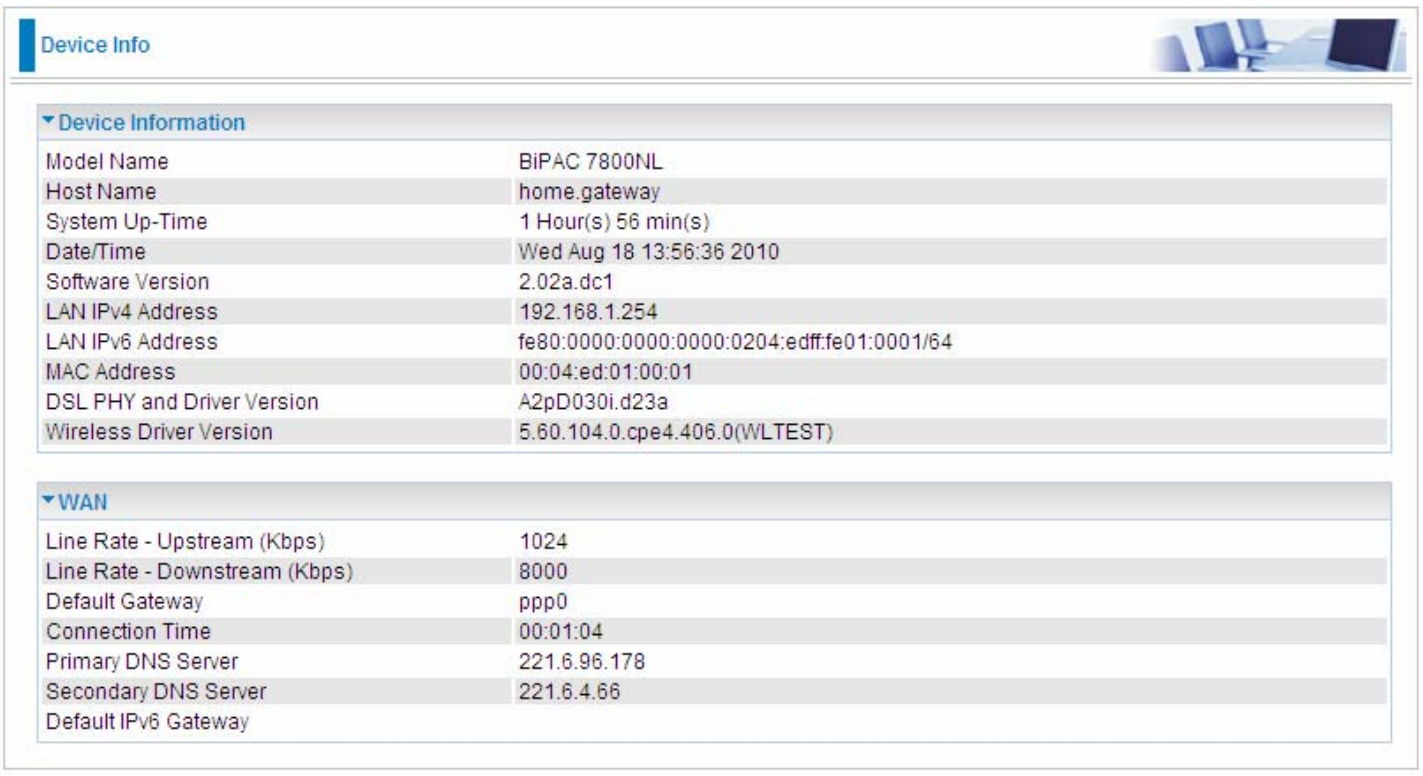


If you confirm about the above settings, click **Apply** to apply your settings. Then the service will be listed as follows.

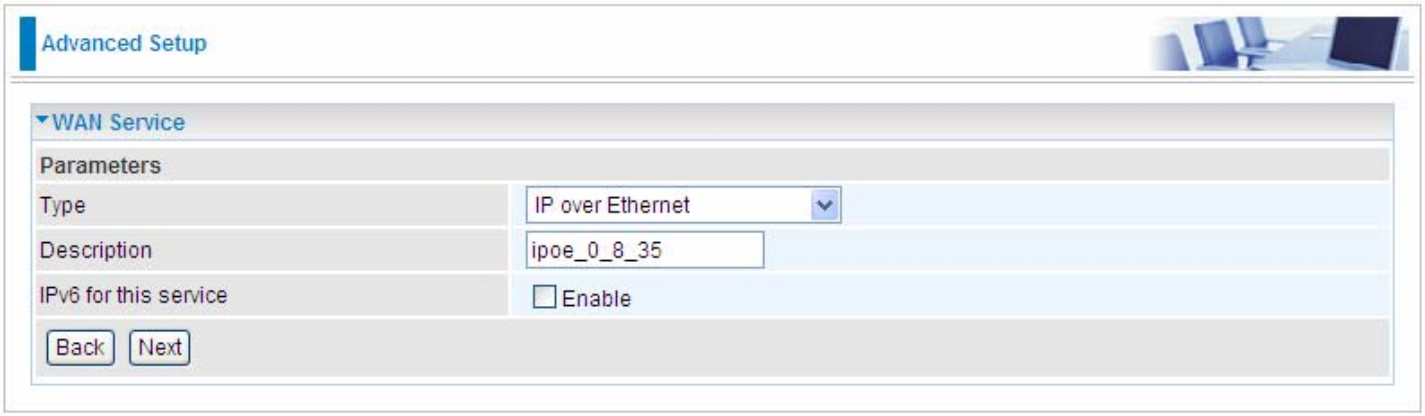


If you don not need the service, select the item you want to remove, check the checkbox, then press **Remove**, it will be OK.

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.



IP over Ethernet

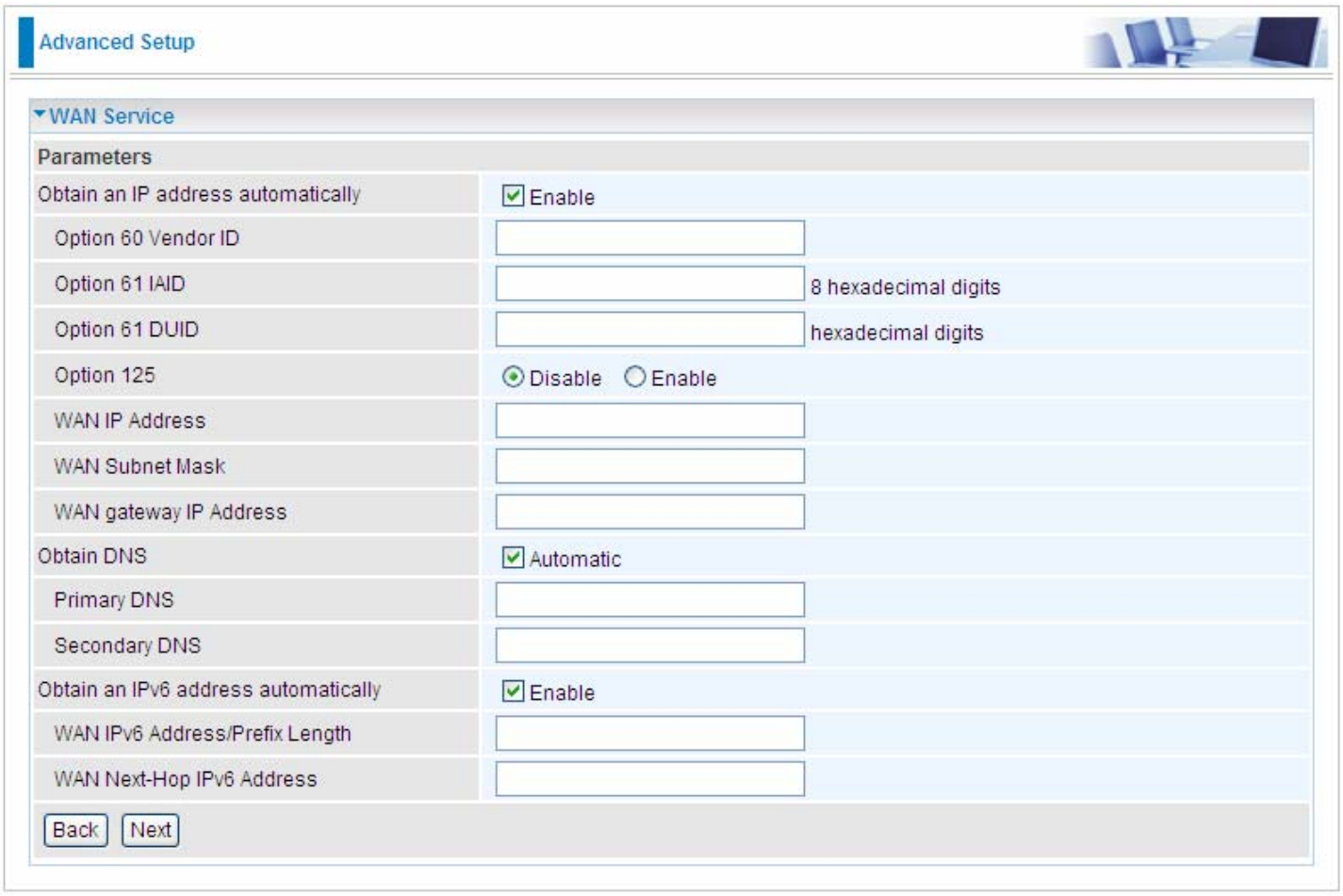


Type: Select IP over Ethernet.

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



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.

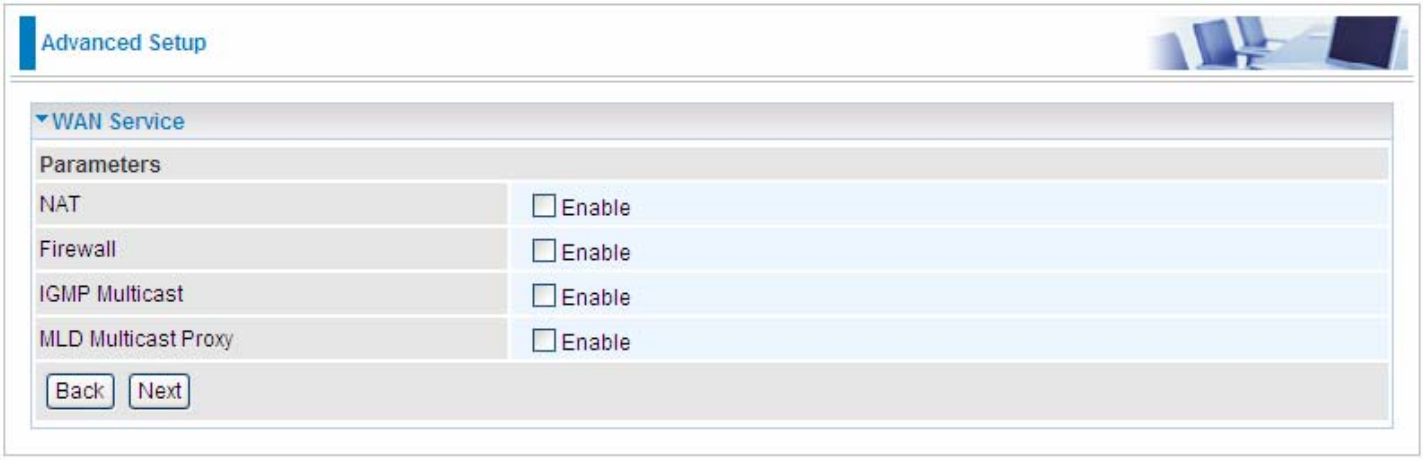
Obtain an IPv6 address automatically: check whether to enable or disable this feature.

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.



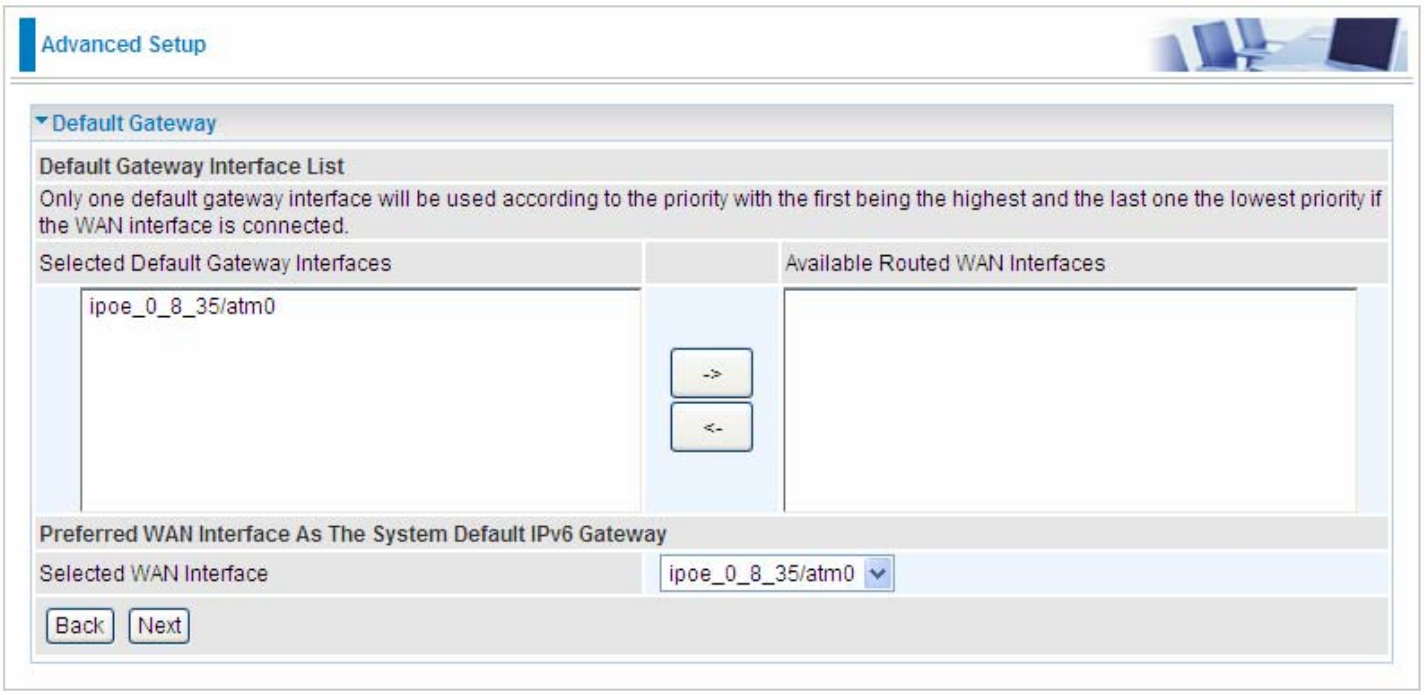
NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account by sharing the single IP address. If users on your LAN have their own public IP addresses to access the Internet, NAT function can be disabled. When enabled, a Fullcone NAT parameter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

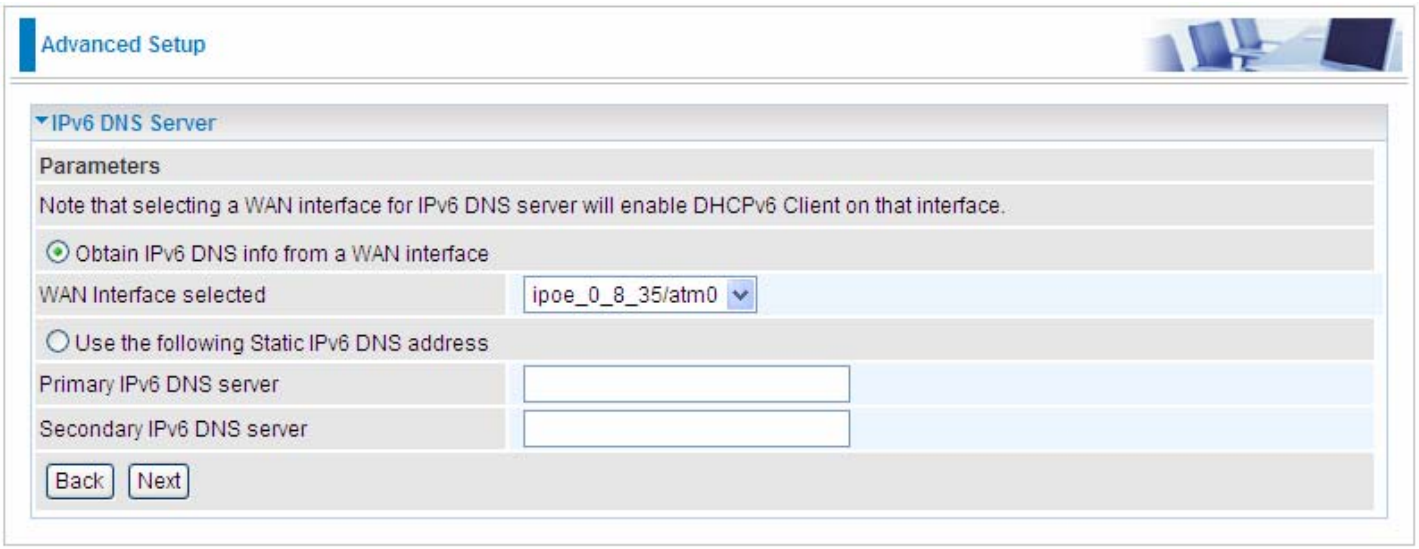
MLD Multicast Proxy: check whether to enable this function. MLD (**Multicast Listener Discovery** Protocol) Proxy intercept the MLD request from Clients and forward it to the router after some dealings. Support MLDv1 and MLDv2.

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



Set the default gateway and the default IPv6 gateway.

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



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

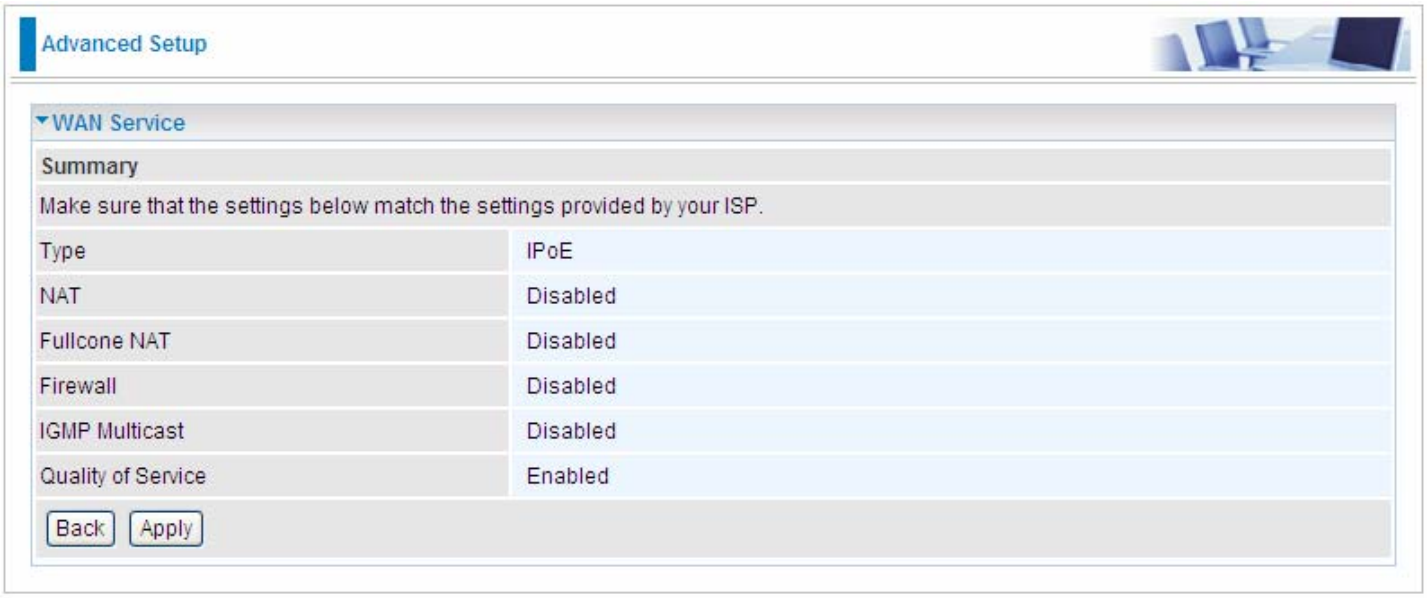
Obtain IPv6 DNS info from a WAN interface

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

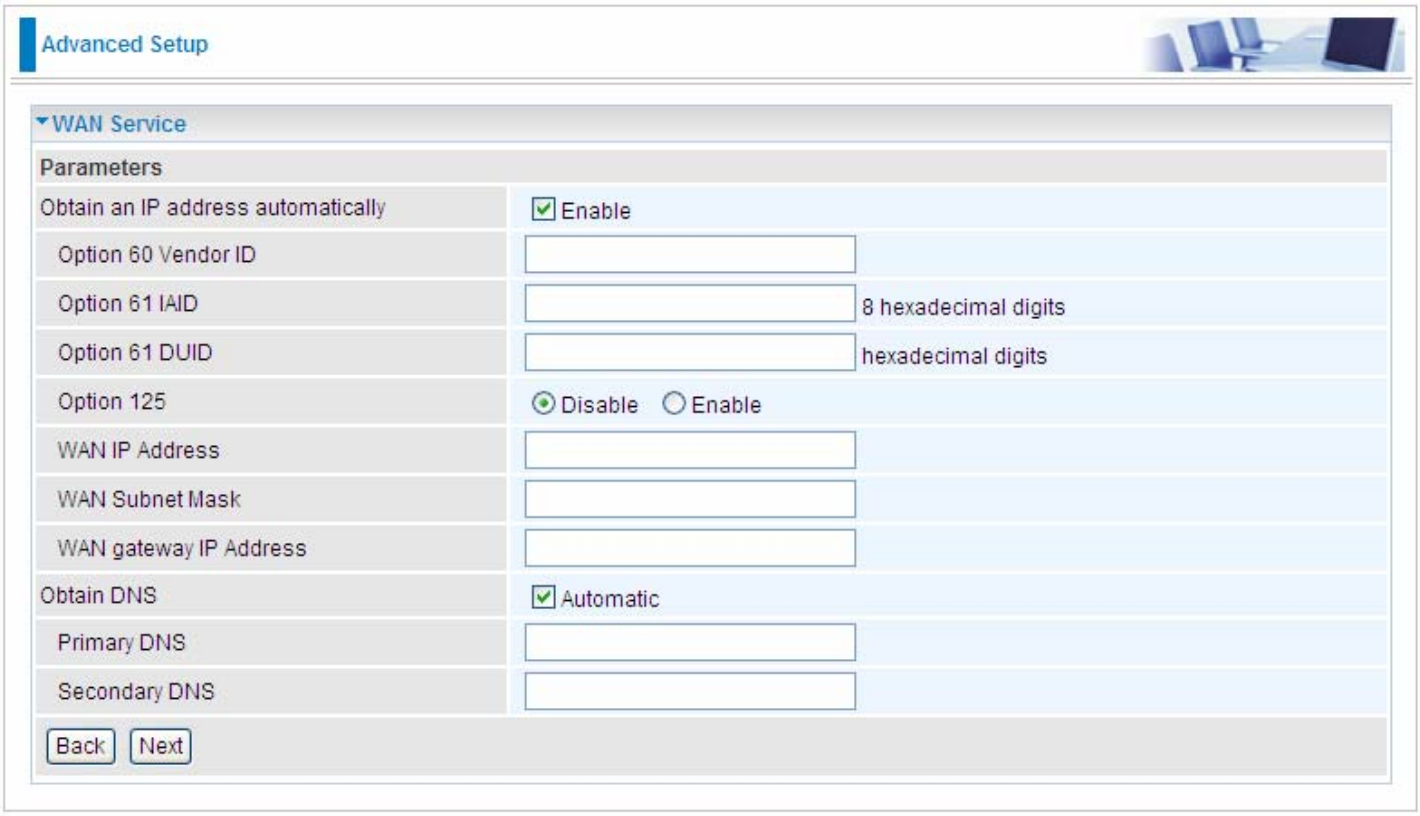
Primary IPv6 DNS Server / Secondary IPv6 DNS Server: type the specific primary and secondary IPv6 DNS Server address.

Click **Next** to check the settings.



If you confirm, click Apply to submit the settings.

IPv6 disabled



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.

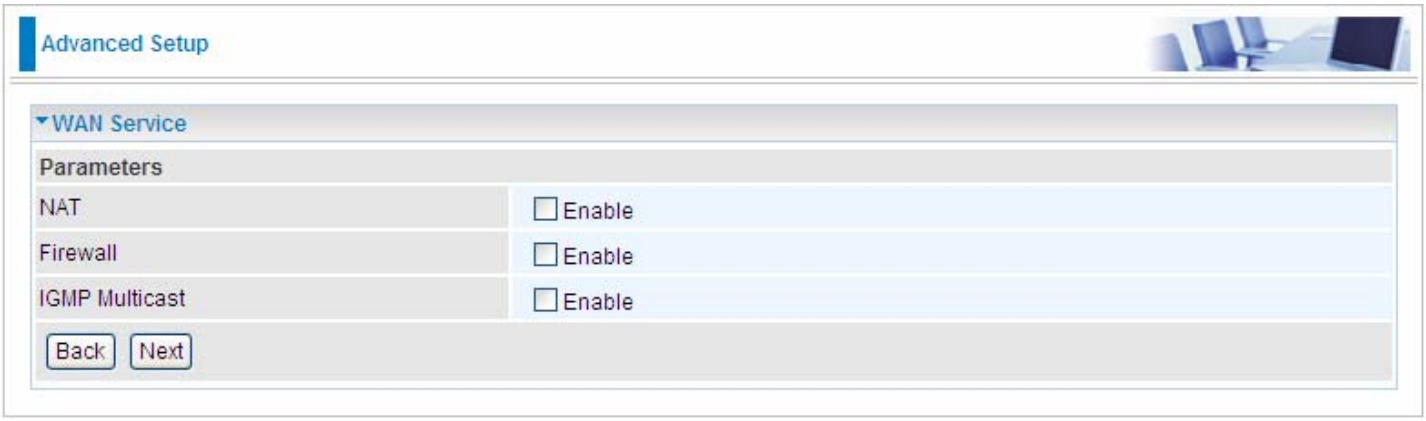
WAN gateway IP Address: Enter your gateway IP address to the device provided by your ISP.

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.

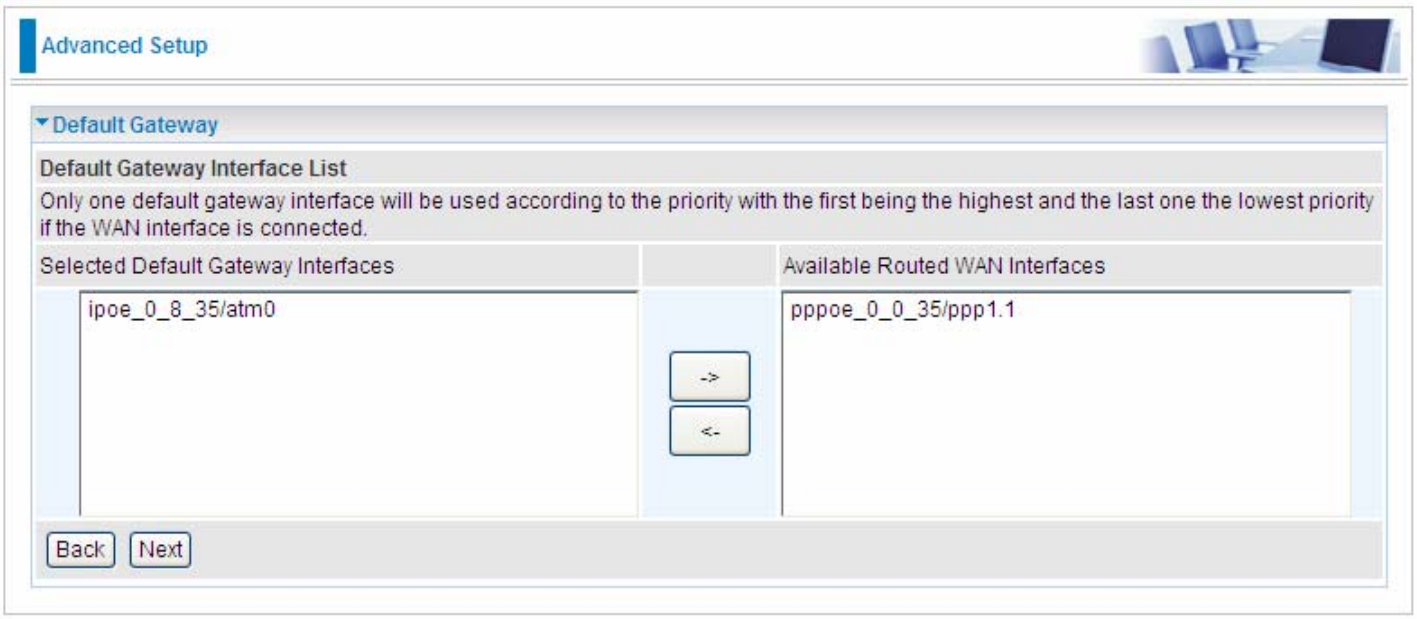


NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account by sharing the single IP address. If users on your LAN have their own public IP addresses to access the Internet, NAT function can be disabled. When enabled, a Fullcone NAT parameter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

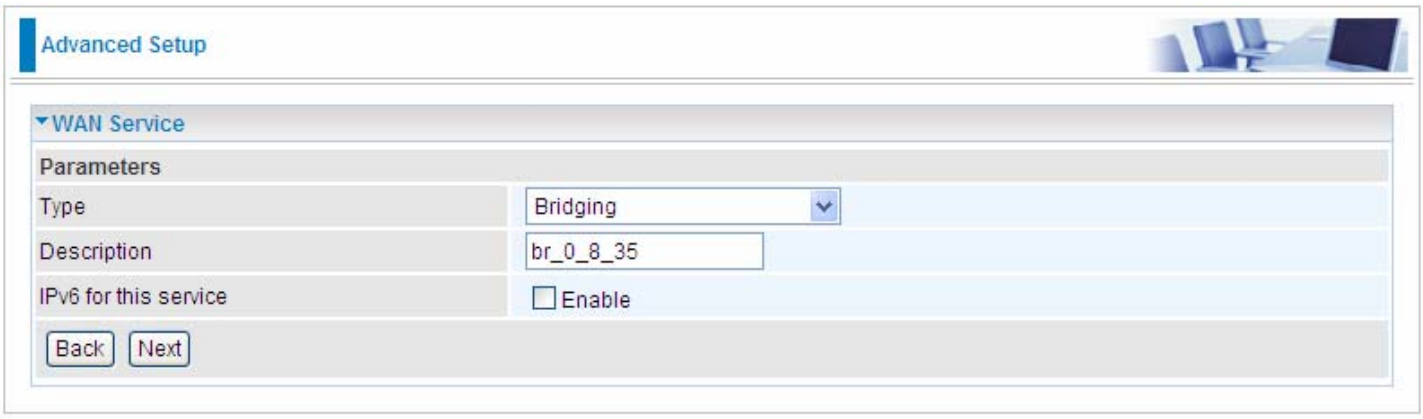
Click **Next** to go to set default gateway.



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

Click **Apply** to apply your settings.

Bridging



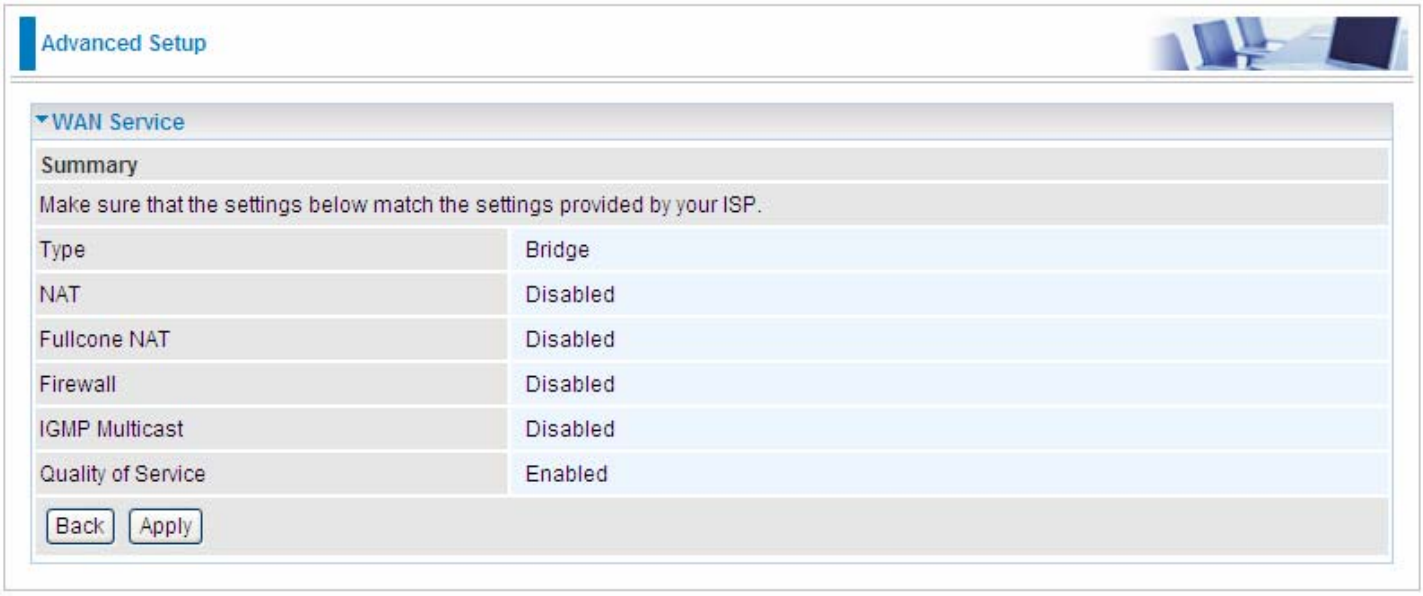
Type: Select Bridging.

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

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

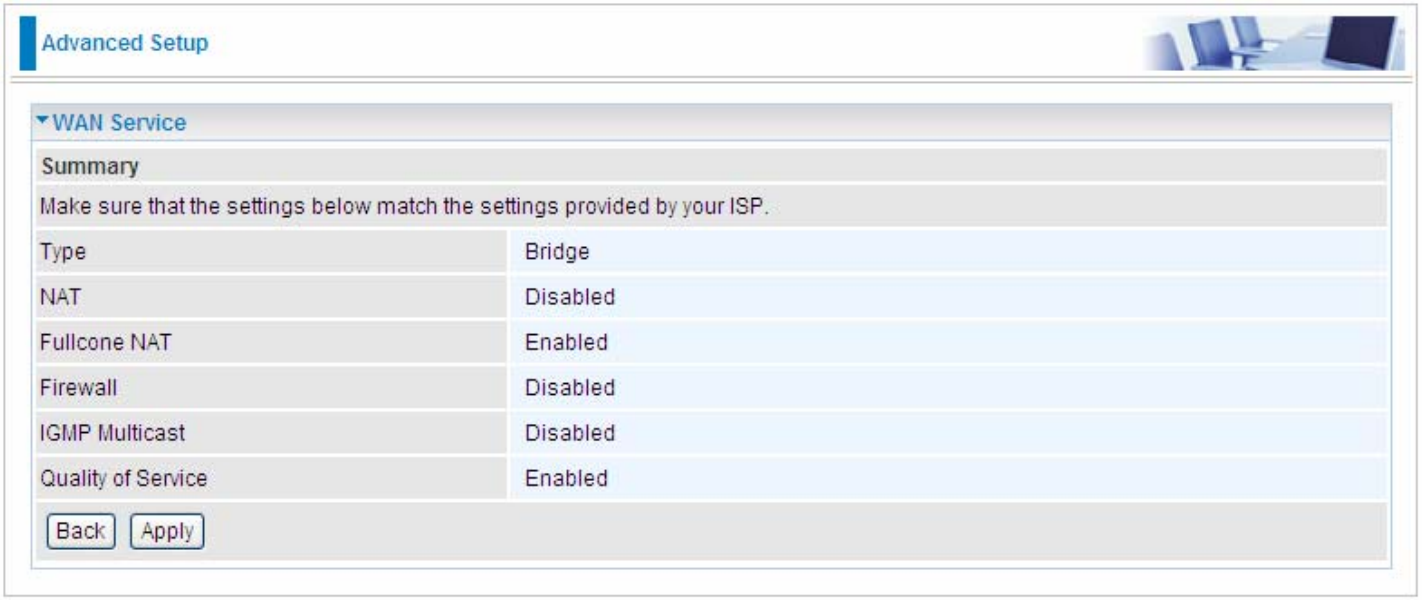
Click **Next** to go to next step. See IPv6 enabled and IPv6 disabled .

IPv6 enabled



Click **Apply** to apply your settings.

IPv6 disabled

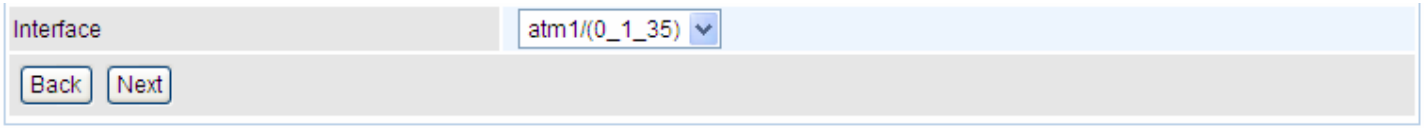


Click **Apply** to apply your settings.

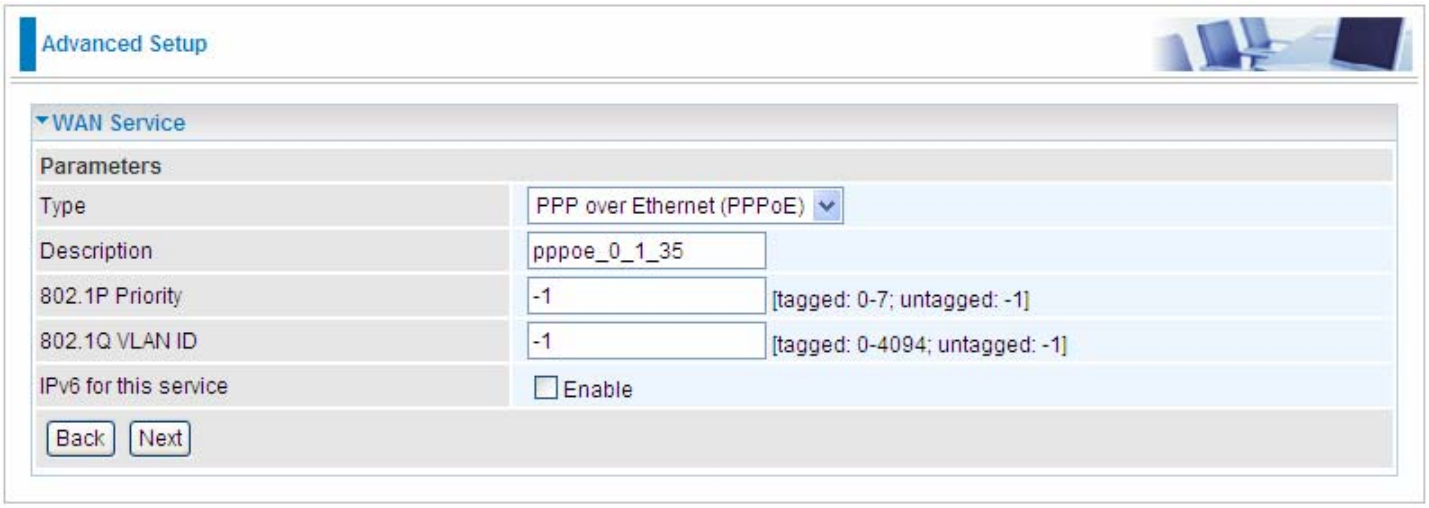
VLAN MUX Connection Mode

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).



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



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.

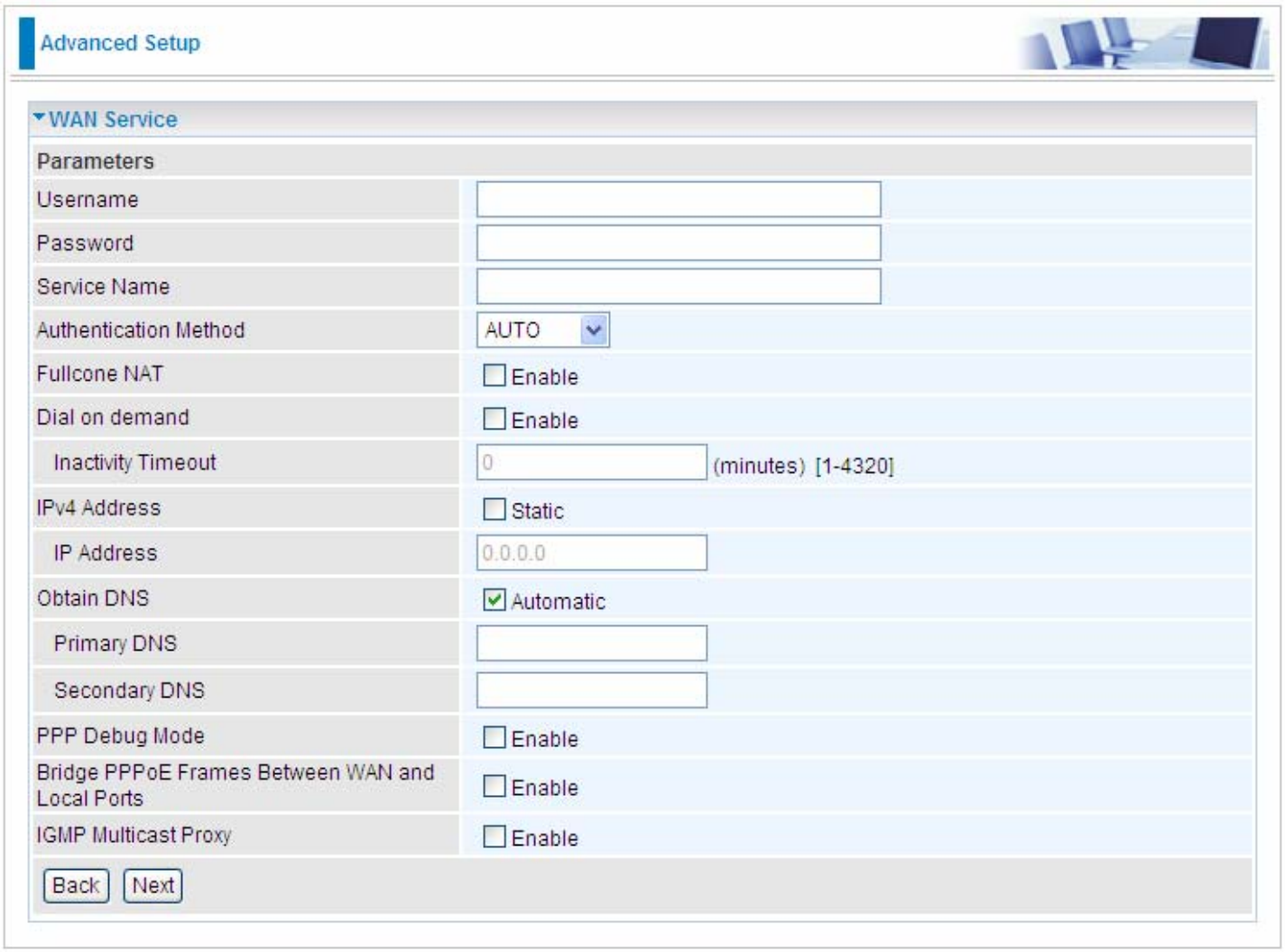
802.1Q VLAN ID: It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 0-4094, untagged:-1.

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.

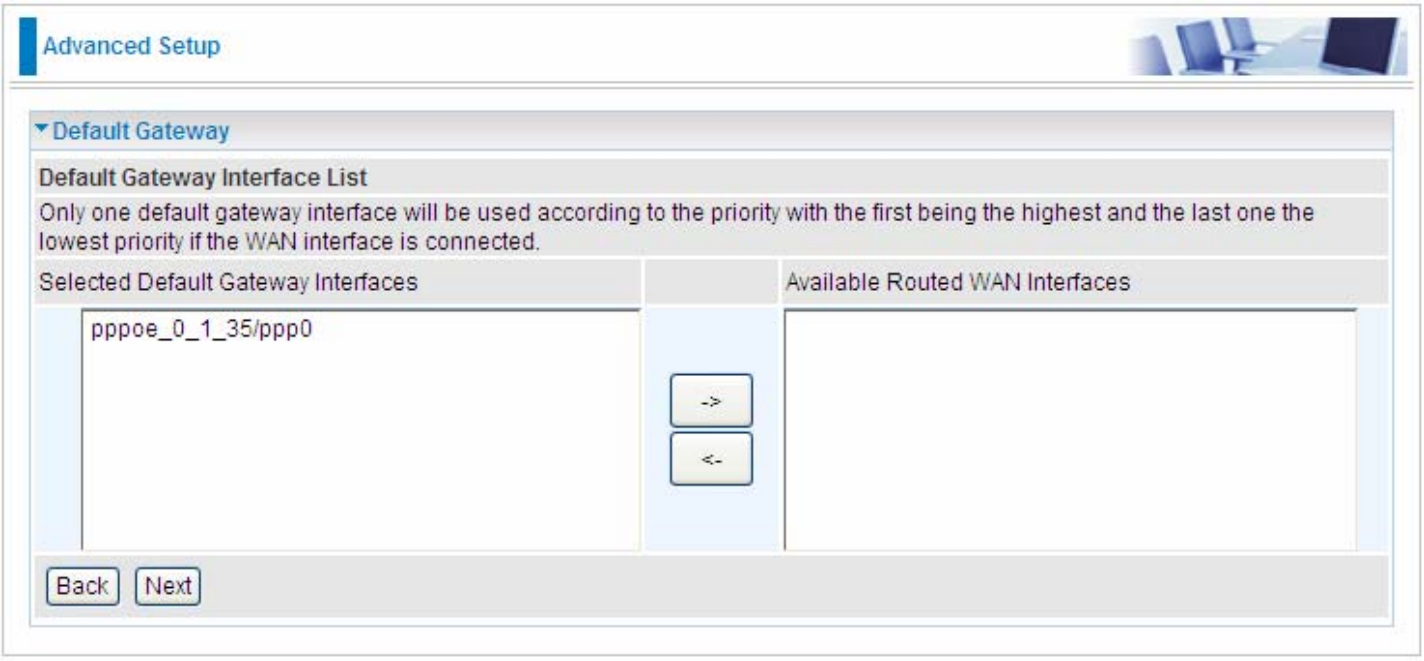
IPv6 for this service: check whether to enable IPv6 service.

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.

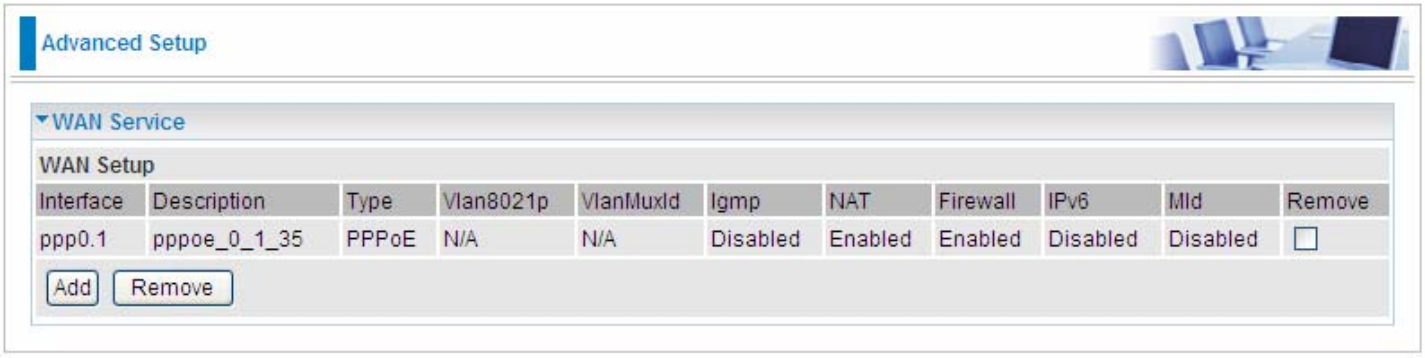


Click **Next** to set the default gateway of this connection.

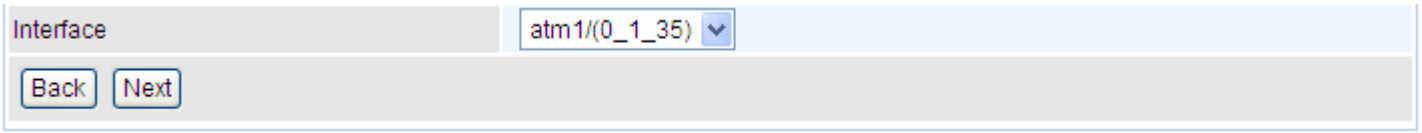


Click **Next** to view the information you have set to the connection, then click **Apply** to save your settings.

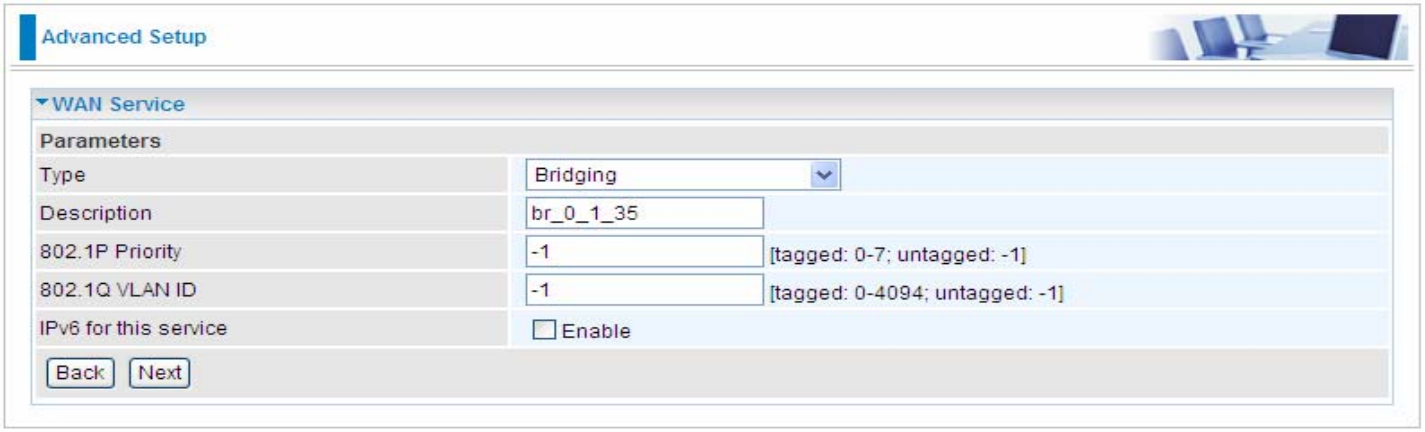
Then you can see the PPPoE connection is listed below. Here it is just one service over atm1/(0_1_35).



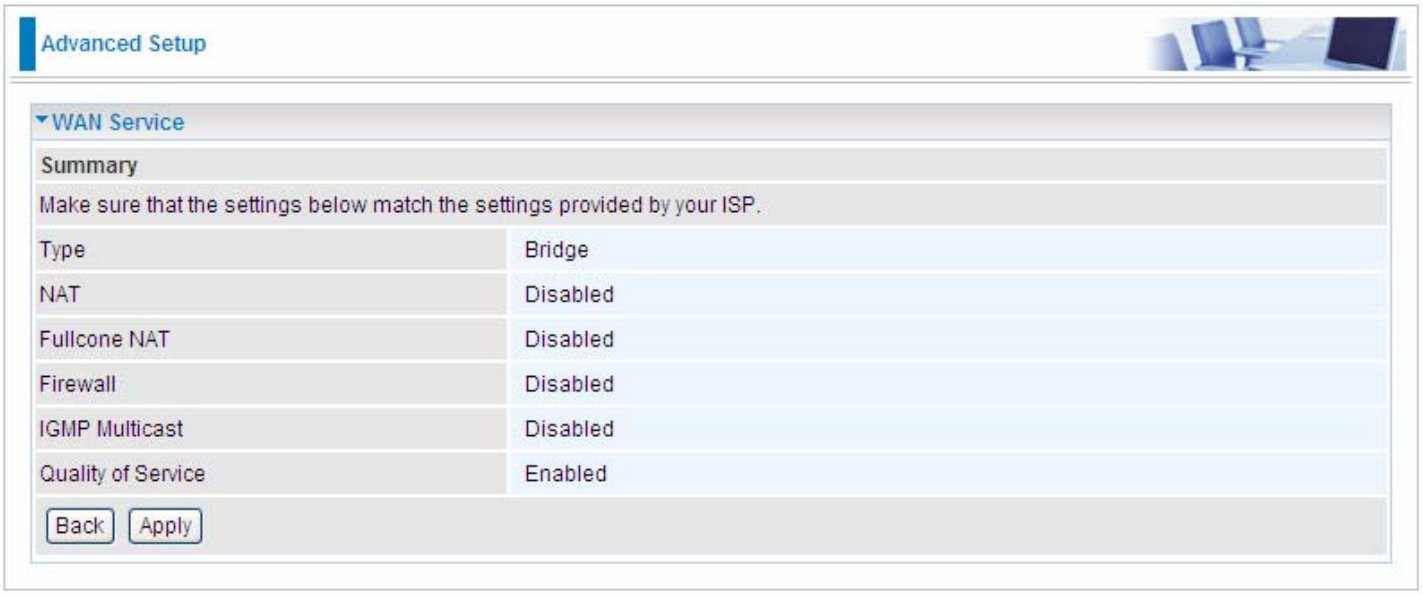
Then we can again set a Bridging connection over atm1/(0_1_35) interface. Click Add in the above page, the atm1/(0_1_35) also is listed for selection to add services.

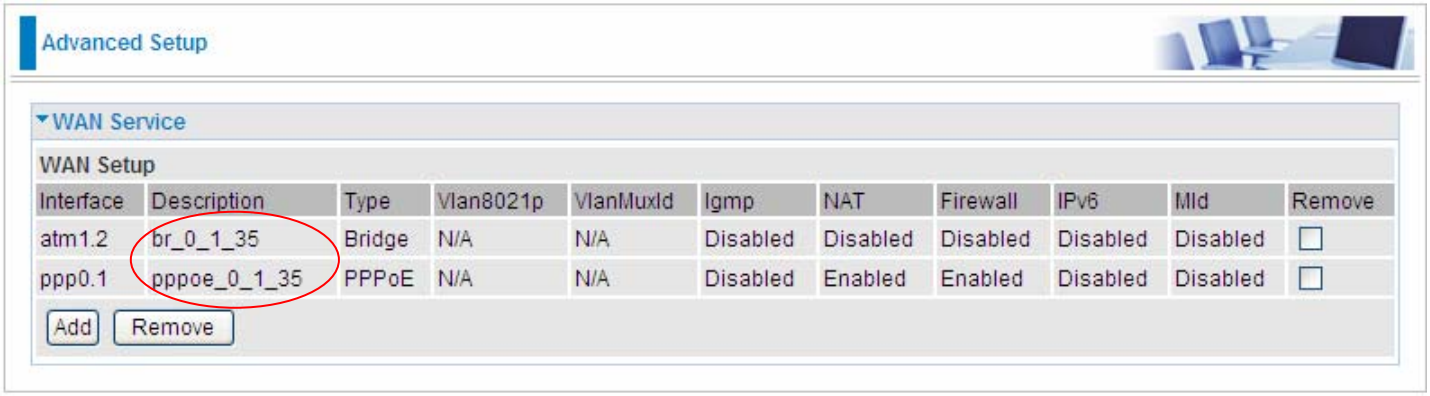


Continue clicking Next to select Bridging connection type.

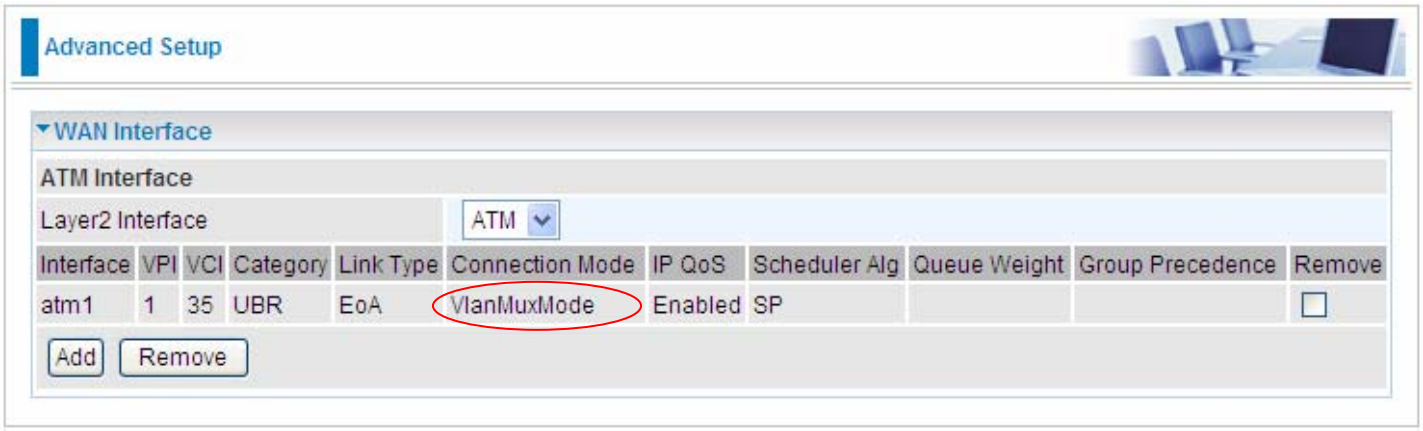


Click Next to make sure your settings below match the settings provided by your ISP. And Click **Apply** to save your settings.





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



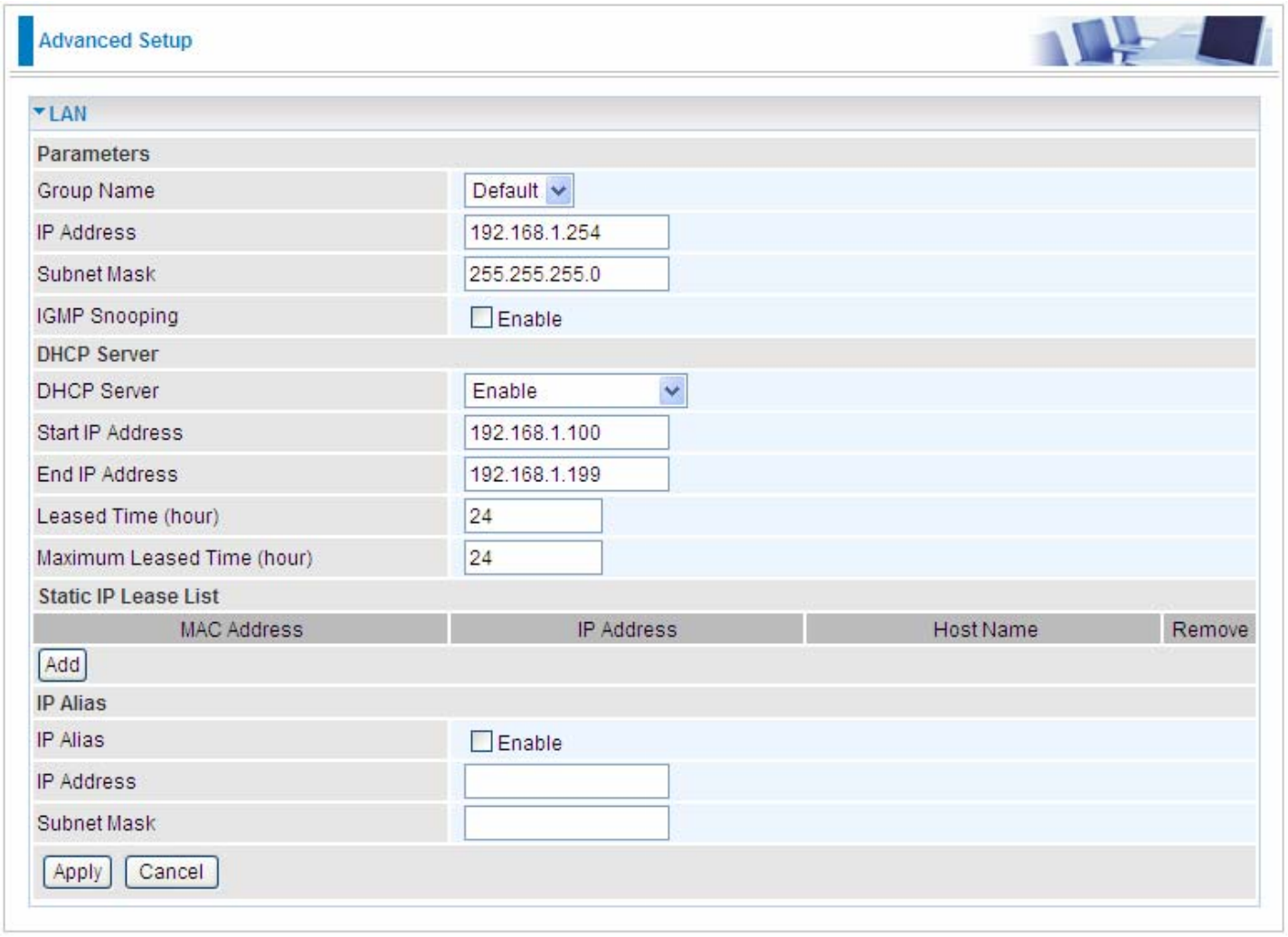
The below is WAN connection status, here you can see clearly the multiple services over one PVC.

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.



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."

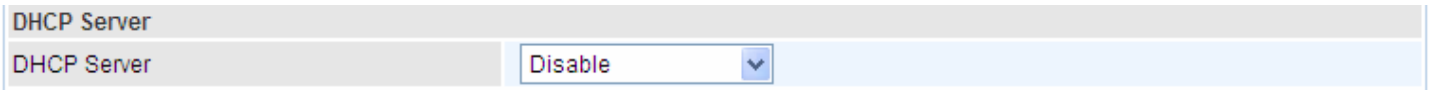
When enabled, you will see two modes:

- **Standard Mode:** In standard mode, multicast traffic will flood to all bridge ports when no client subscribes to a multicast group.
- **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.

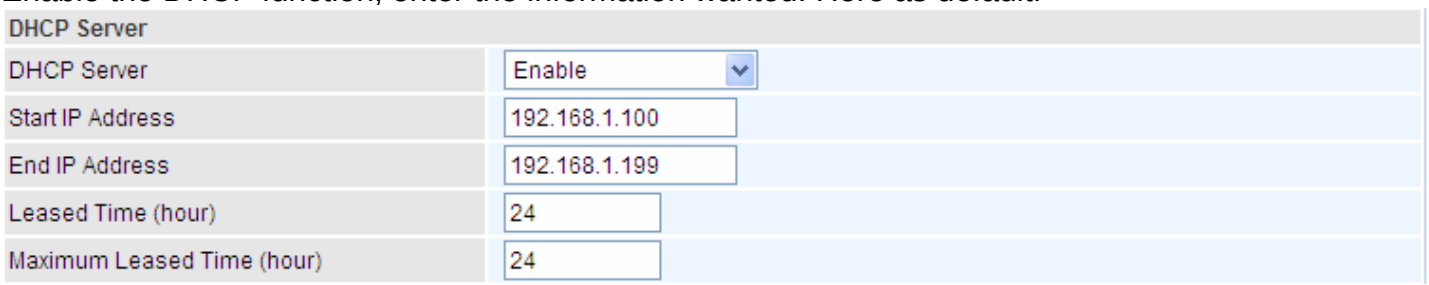
ⓘ Disable



Disable the DHCP Server function.

ⓘ Enable

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



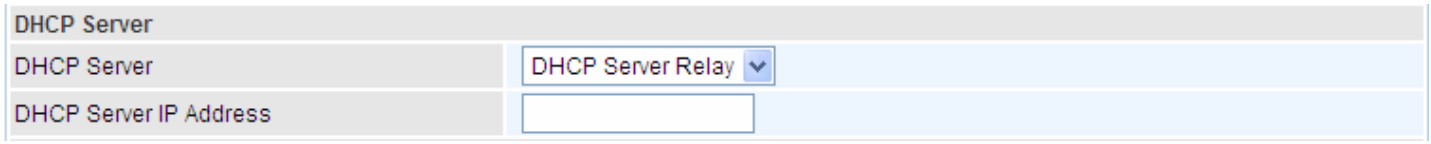
Start IP Address: the start IP address of the range the DHCP Server used to assign to the Clients.

End IP Address: the end IP address f 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).

ⓘ DHCP Server Relay

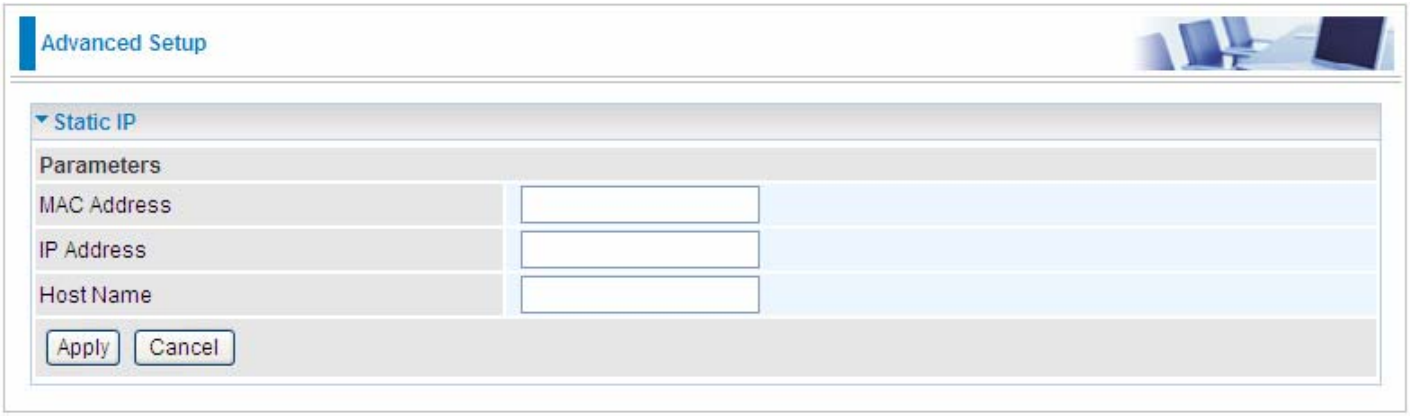


If you check **DHCP Relay** and then you must enter the IP address of the DHCP server which assigns an IP address back to the DHCP client in the LAN. Use this function only if advised to do so by your network administrator or ISP.

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.

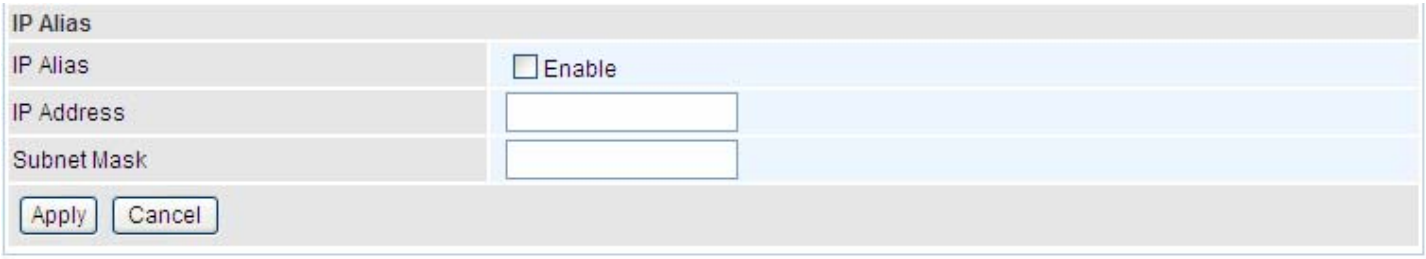
Press **Add** to the Static IP List.



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: 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.

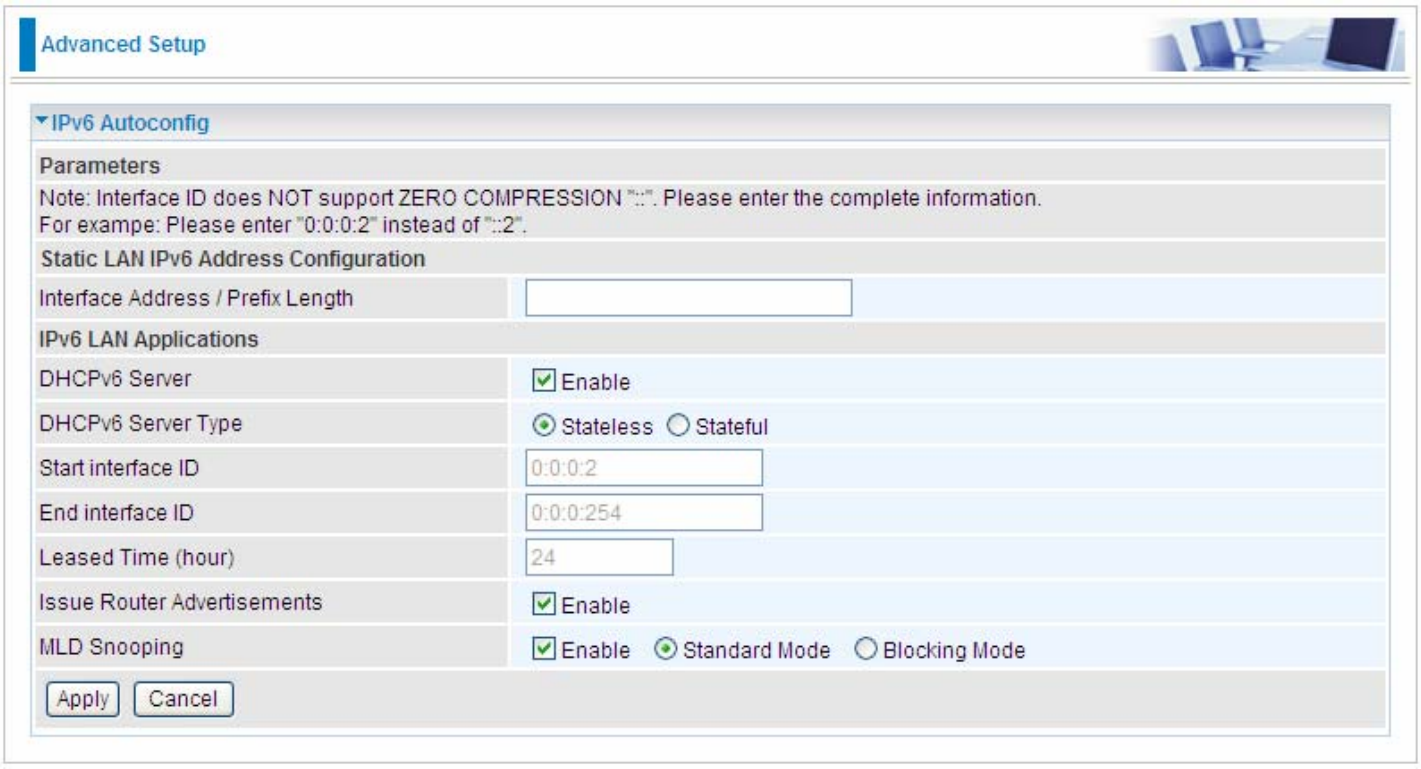
Click **Apply** to apply your settings.

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.



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.

- **Standard Mode:** In standard mode, multicast traffic will flood to all bridge ports when no client subscribes to a multicast group.
- **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.

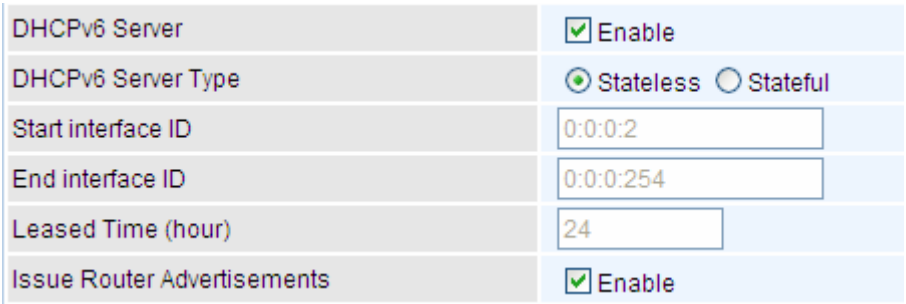
Stateless and Stateful IPv6 address Configuration

Stateless: two methods can be adopted.

- With DHCPv6 disabled, but Issue Router Advertisement Enabled

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.

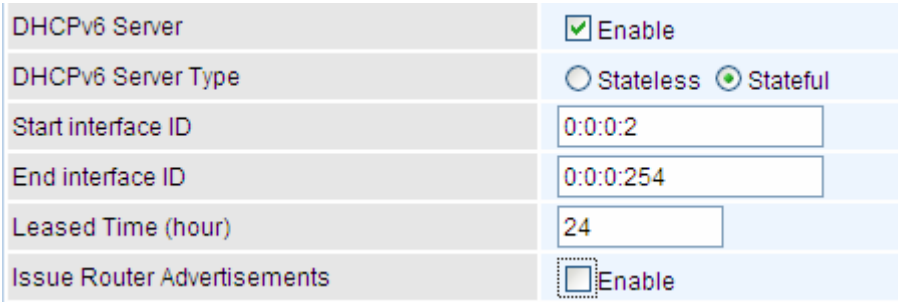
- With both DHCPv6 and Issue Router Advertisement Enabled



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

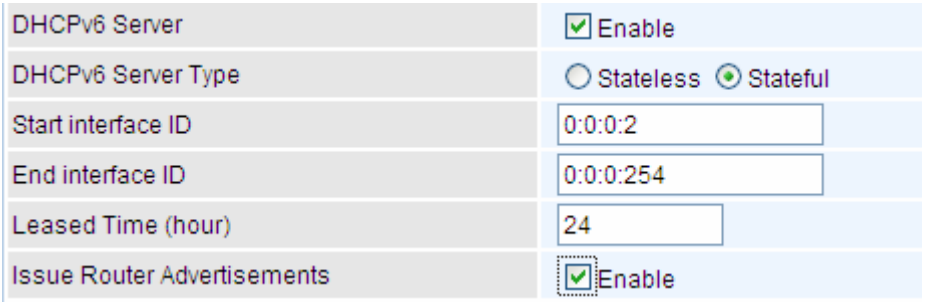
Stateful: two methods can be adopted.

ⓘ With only DHCPv6 enabled



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

ⓘ With both DHCPv6 and Issue Router Advertisement Enabled



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

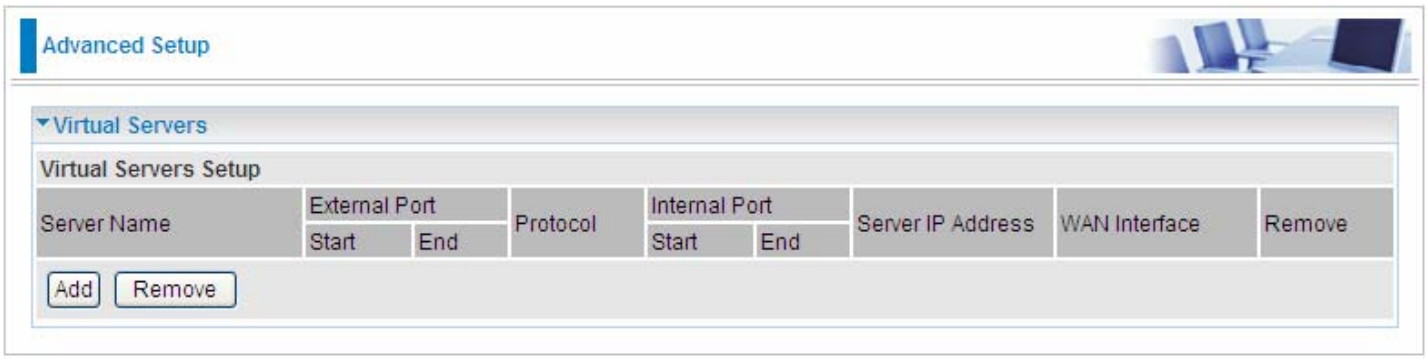
In TCP/IP and UDP networks a port is a 16-bit number used to identify which application program (usually a server) incoming connections should be delivered to. Some ports have numbers that are pre-assigned to them by the IANA (the Internet Assigned Numbers Authority), and these are referred to as “well-known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

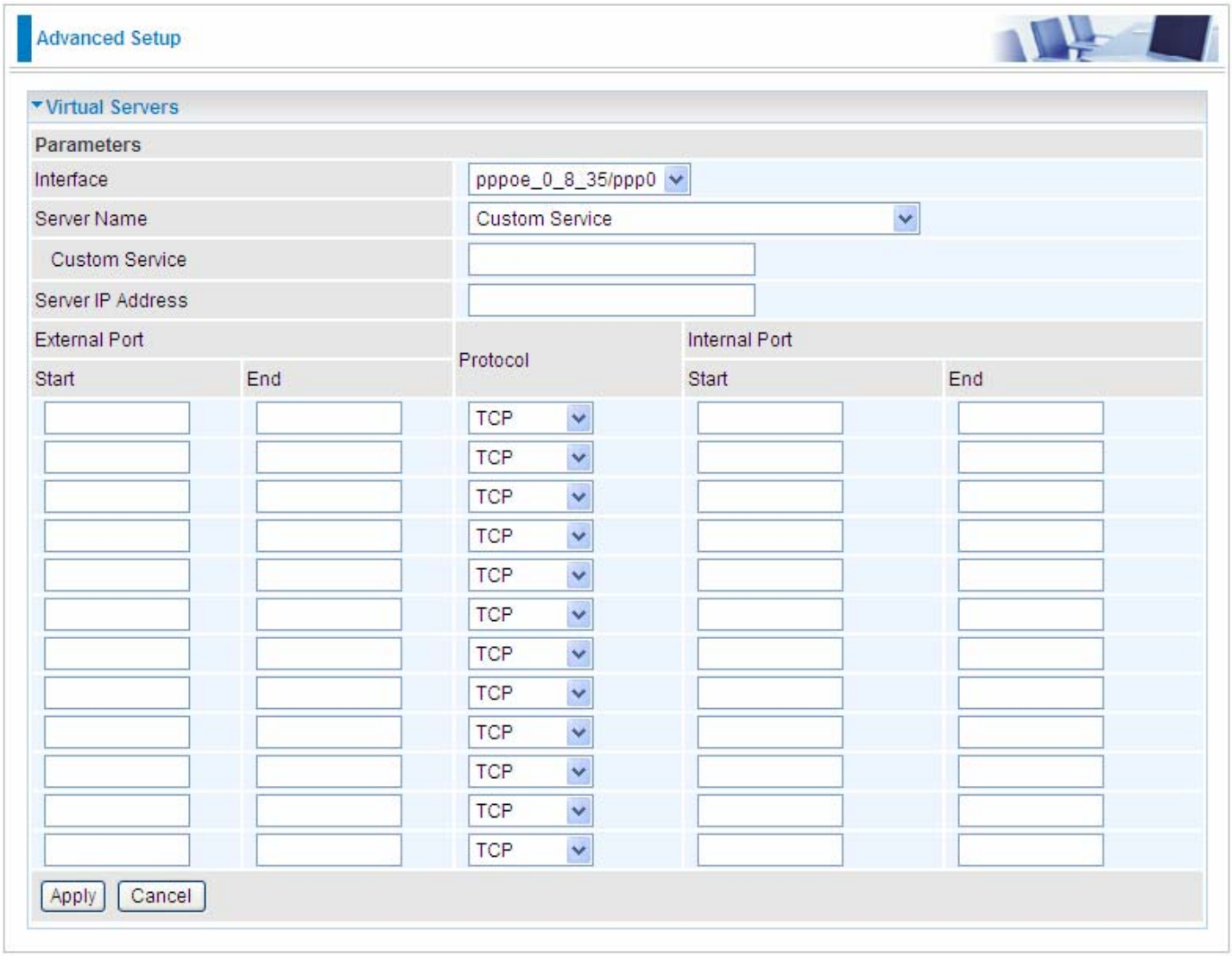
The device can be configured as a virtual server so that remote users accessing services such as Web or FTP services via the public (WAN) IP address can be automatically redirected to local servers in the LAN network. Depending on the requested service (TCP/UDP port number), the device redirects the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



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

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

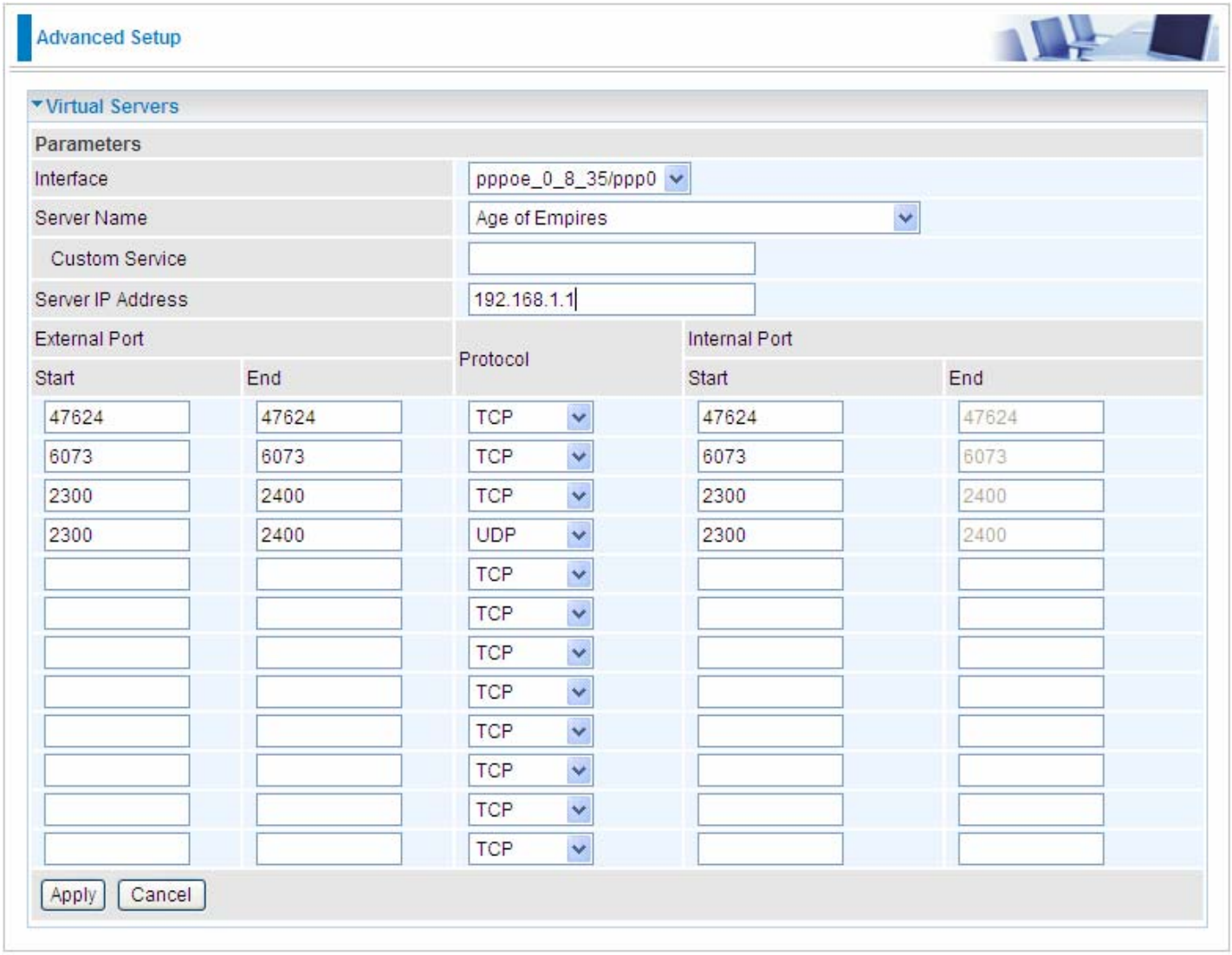
Internal Port

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

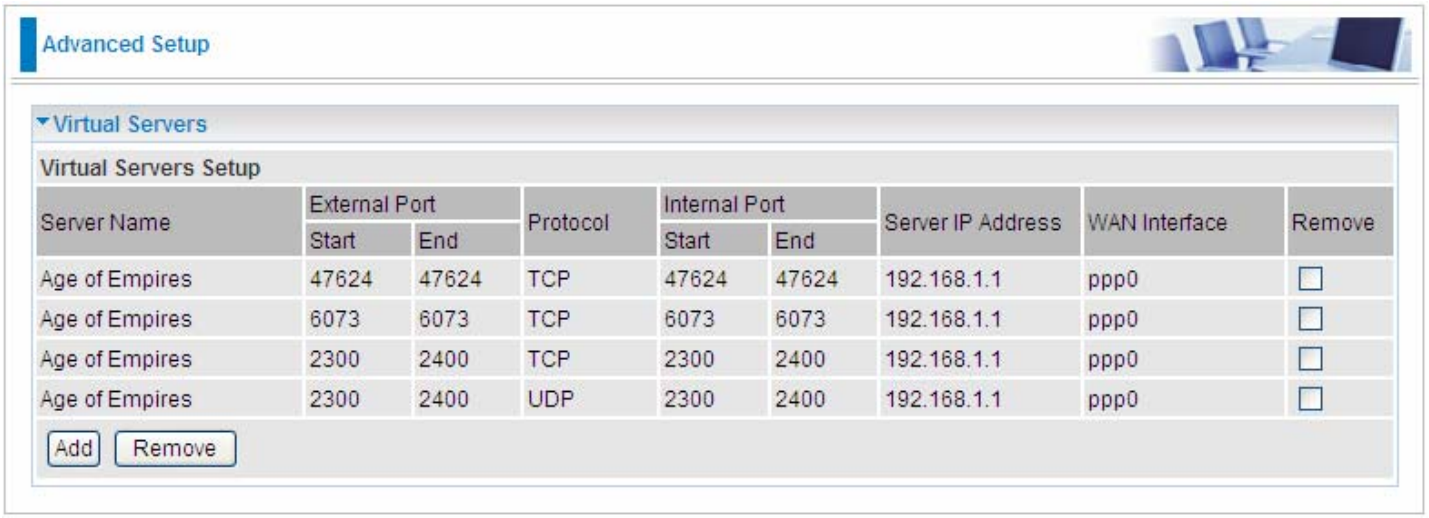
Protocol: select the protocol this service used: TCP/UDP, TCP, UDP.

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.

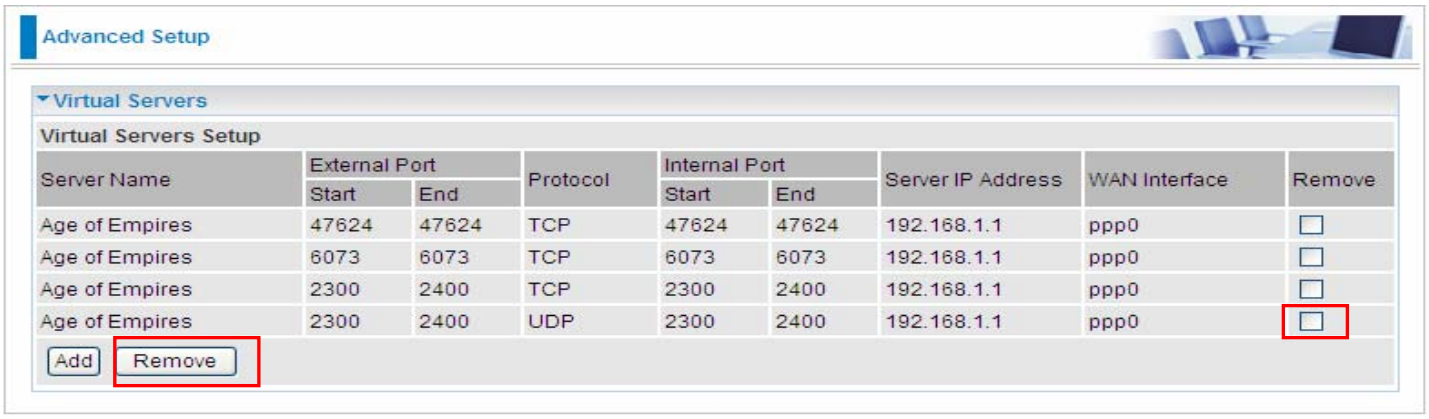


2. Press **Apply** to conform, and the items will be list in the **Virtual Servers Setup** table.



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.

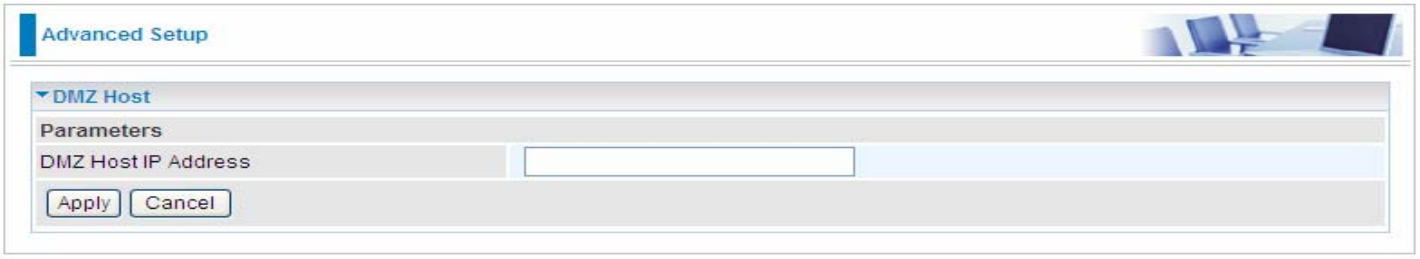


ALG

The ALG Controls enable or disable protocols over application layer.

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.



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

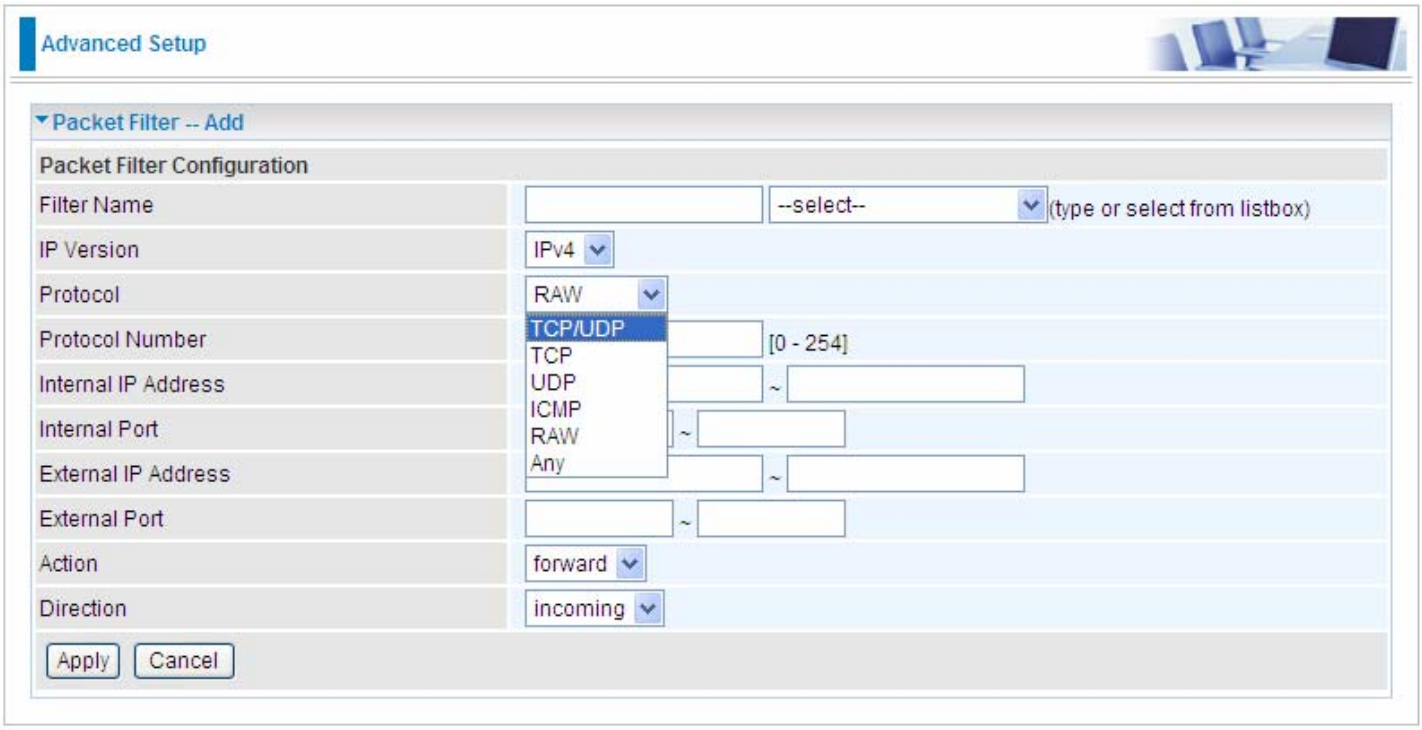
If you have disabled the NAT option in the WAN-ISP section, the Virtual Server function will hence be invalid.
If the DHCP server option is enabled, you have to be very careful in assigning the IP addresses of the virtual servers in order to avoid conflicts. The easiest way of configuring Virtual Servers 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.

Security

Packet Filter

Packet filtering enables you to configure your router to block specified internal/external users (**IP address**) from Internet access, or you can disable specific service requests (**Port number**) to /from Internet. The relationship among all filters is **"or"** operation, which means that the router checks these different filter rules one by one, starting from the first rule. As long as one of the rules is satisfied, the specified action will be taken.

Above is the listing table. Click **Add** to add new configurations.



Filter name: a user-defined filter name or you can select from the drop-down menu the application, and leave the automatically generated name as the Filter name.

IP Version: Select the IP Version， IPv4 or IPv6.

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

Protocol: Specify the packet type (TCP/UDP，TCP, UDP, ICMP, RAW and Any) that the rule applies

to. Only when **RAW** is selected, then you can type the protocol number (0-254) to identify the protocol that you want the filter applies to. When **Any** is selected, it means the filter will applies to any protocol.

Internal Port: This Port or Port Range defines the ports allowed to be used by the Remote/WAN to connect to the application. Default is set from range **1 ~ 65535.** It is recommended that this option be configured by an advanced user.

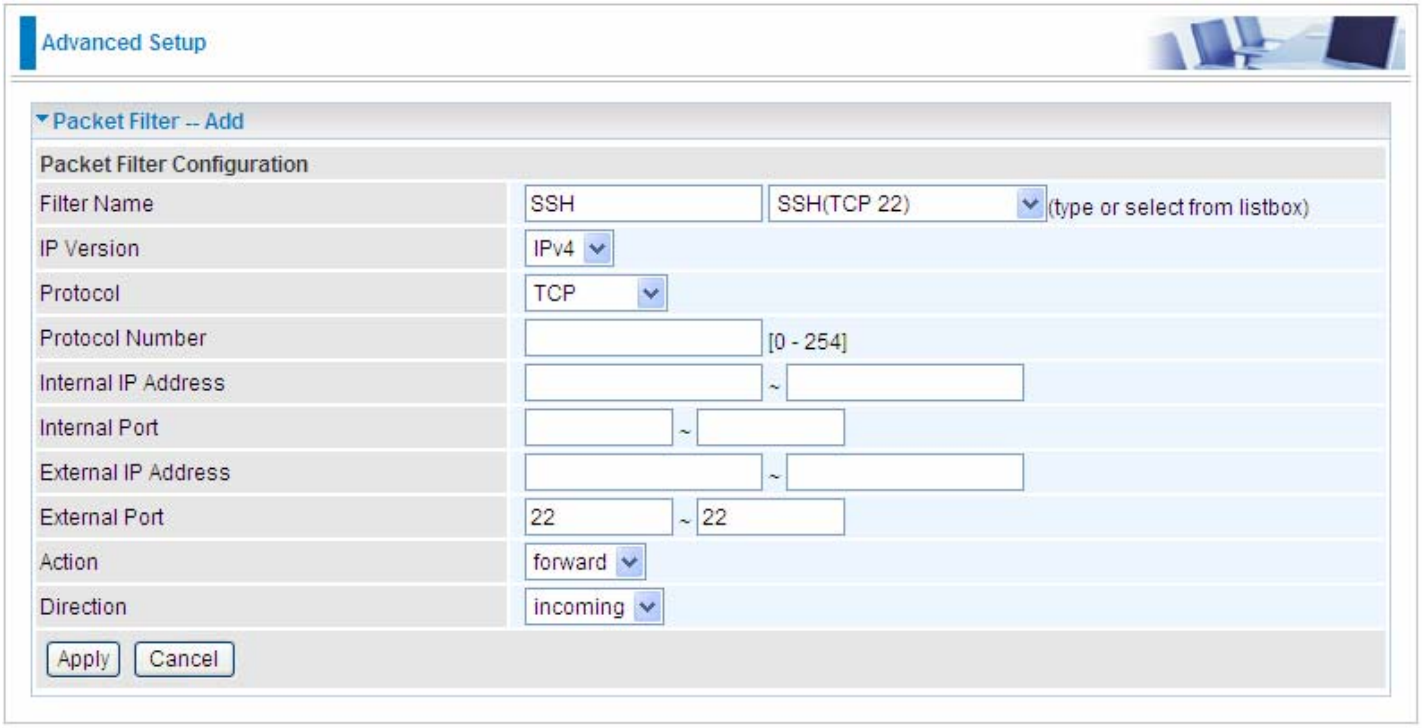
External Port: This is the Port or Port Range that defines the application. Default is set from range **1 ~ 65535.**

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

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

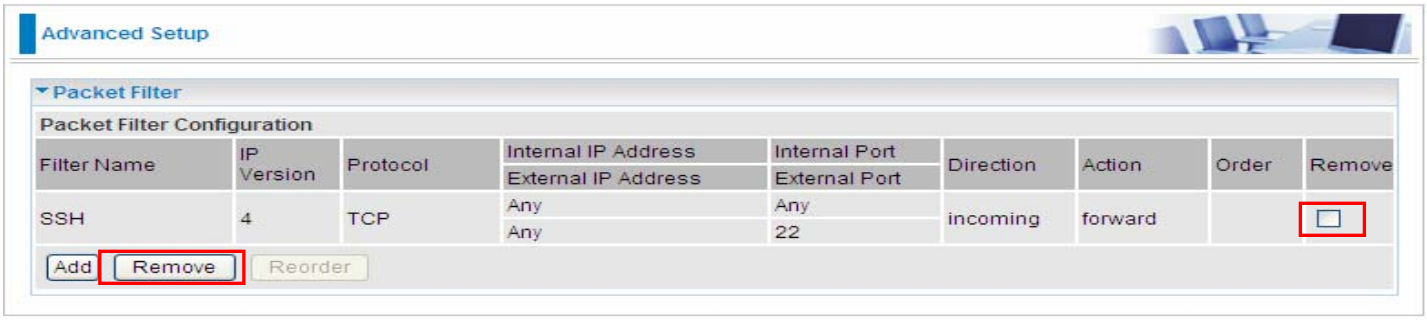
Set up

Select the application you want to filter, input the information or leave it as default according to yourself.



Press **Apply** to confirm and the item will be listed in the following table.

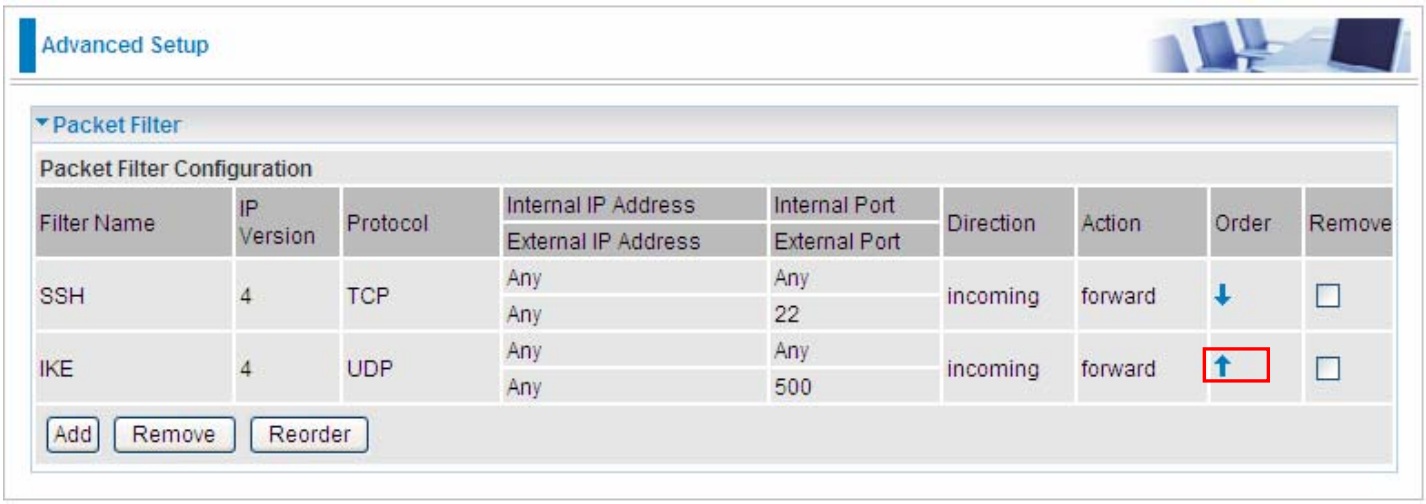
Remove



Check the checkbox, press **Remove**, the item will be removed.

Reorder

When there are more than one Filter application, you can reorder them to the priority you want. The former is prior to the latter one.



Click ↑ or ↓ to change the priority of the filter, then press Reorder to confirm.

Time Restriction

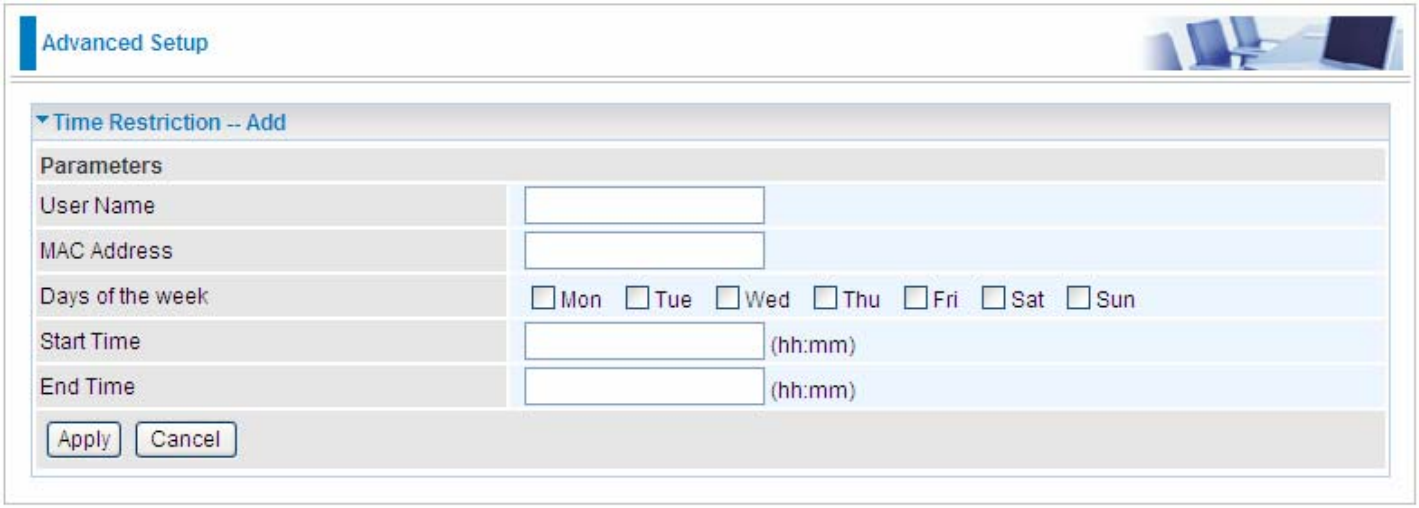
A MAC (Media Access Control) address is the unique network hardware identifier for each PC on your network's interface (i.e. its Network Interface Card or Ethernet card). Using your router's MAC Address Filter function, you can configure the network to block specific machines from accessing your LAN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

Action:

- **Disable:** disable the **Time Restriction** function.
- **Allow:** allow the members in the following table to access the router.
- **Block:** block the members listed in the following table from accessing the router.

Note: here users should add the rules first, then select the wanted action.

Click **Add** to add the rules.



Username: user-defined name.

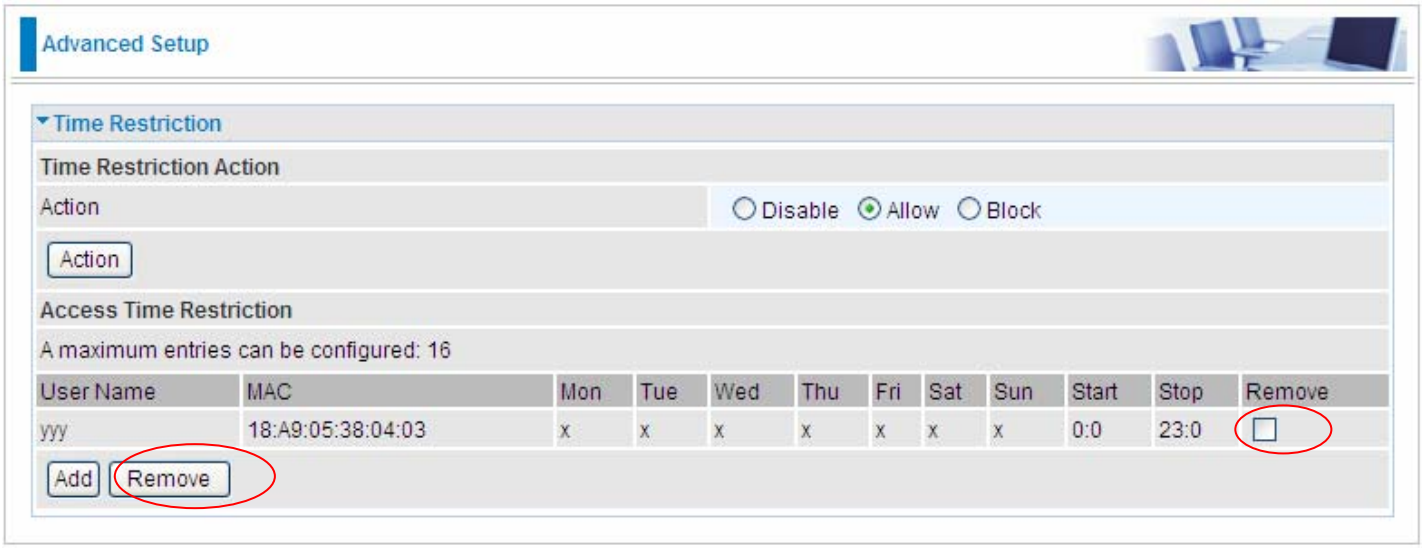
MAC Address: enter the MAC address(es) you want to allow or block to access the router and LAN. The format of MAC address could be: xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.

Days of the week: select the days of a week this rule takes efforts.

Start Time: enter the start time of each day in hh:mm format. Leaving it empty means 00:00.

End Time: enter the end time of each day in hh:mm format. Leaving it empty means 23:59.

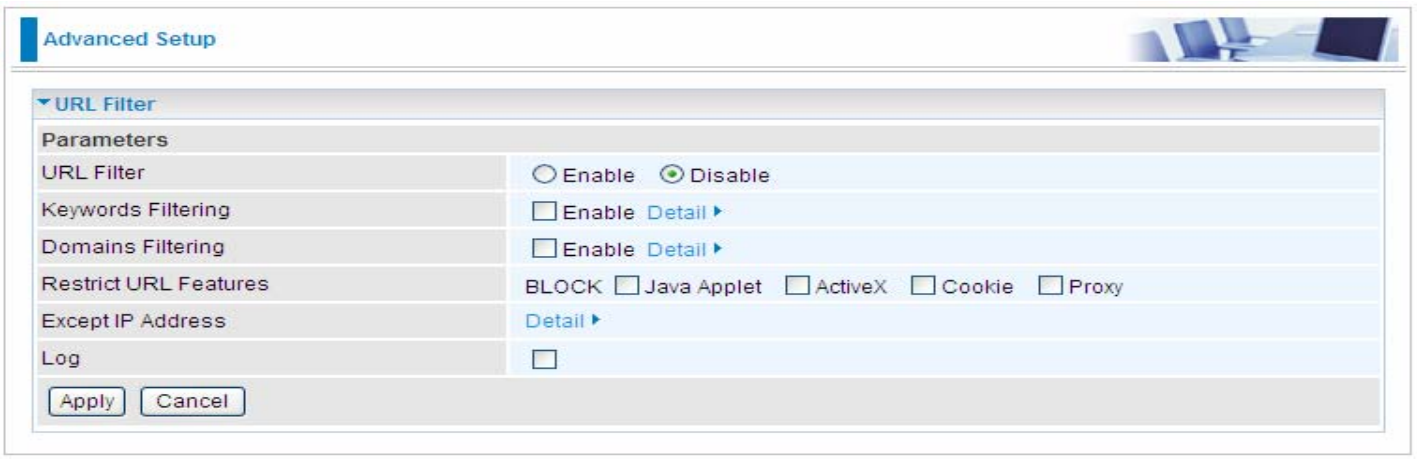
Click **Apply** to confirm your settings. The following prompt window will appear to remind you of the attention.



If you needn't this rule, you can check the box, press Remove, it will be OK.

URL Filter

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



URL Filtering: select to enable or disable URL Filtering feature.

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

Domains Filtering: This function checks the whole URL address but not the IP address against your list of domains to block or allow. If it is matched, the URL request will either be sent (Trusted) or dropped (Forbidden).

Restrict URL Features: Click Block Java Applet to filter web access with Java Applet components. Click Block ActiveX to filter web access with ActiveX components. Click Block Cookie to filter web access with Cookie components. Click Block Proxy to filter web proxy access.

Exception IP Address: You can input a list of IP addresses as the exception list for URL filtering.

Log: Select Enable for this option if you will like to capture the logs for this URL filter policy.

Keywords Filtering

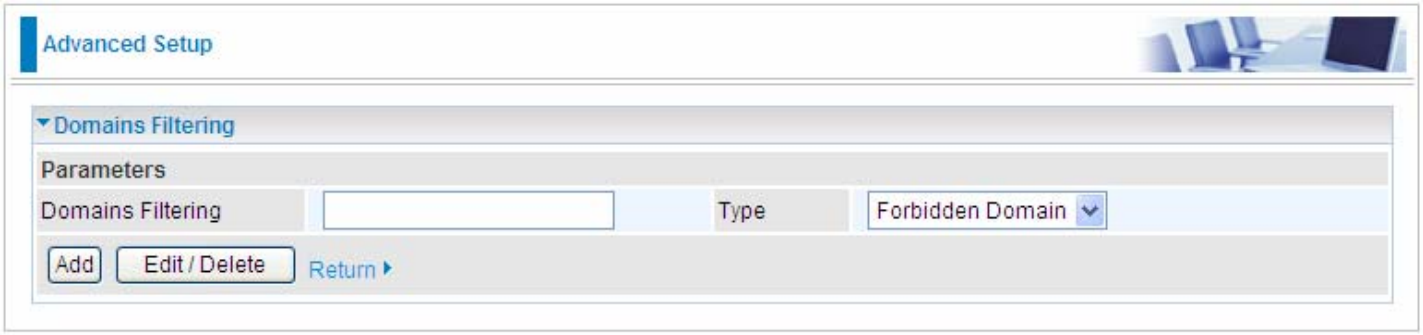
Click Detail ▸ to add the keywords.

Enter the Keyword, for example image, then click **Add.**

You can add other keyword like this. The keywords you add will be listed as above. If you want to reedit the keyword, press the Edit radio button left beside the item, and the word will listed in the Keyword field, edit, then press **Edit/Delete** to confirm. If you want to delete certain keyword, check Delete checkbox right beside the item, and press **Edit/Delete**. Click **Return** to be back to the previous page.

Domain Filtering

Click Detail to add Domains.



Domains Filtering: enter the domain you want this filter applies to.

Type: select the action this filter deals with the Domain.

- **Forbidden Domain:** the domain is the forbidden to access.
- **Trusted Domain:** the domain is trusted and allowed access.

Enter a domain and select whether this domain is trusted or forbidden with the pull-down menu. Next, click **Add**. Your new domain will be added to either the Trusted Domain or Forbidden Domain listing, depending on which you selected previously. For specific process, please refer to **Keywords filtering.**

Exception IP Address

Click Detail to add the IP Addresses.

Enter the except IP address. Click **Add** to save your changes. The IP address will be entered into the Exception List, and excluded from the URL filtering rules in effect. For specific process, please refer to **Keywords filtering.**

At the URL Filter page, press **Apply** to confirm your settings.

QoS - Quality of Service

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

Quality of Service: Check to activate this function and the following field will be available.

If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier.
If Enable Qos checkbox is not selected, all QoS will be disabled for all interfaces.

Select Default DSCP Mark: Select the default DSCP mark from the list-box. Differentiated Services Code Point (DSCP) is the first 6 bits in the ToS byte. DSCP Mark allows users to classify the traffic of the application to be executed according to the DSCP value. The default DSCP mark is used to mark all egress packets that do not match any classification rules.

Note: Before configuring Queue config and QoS Classification section, you must enable QoS function, for the reason that the queues' activation will depend on this, the classification will also depend on this.

The corresponding IP precedence and DSCP mapping table is listed below.

IP Precedence and DSCP Mapping Table

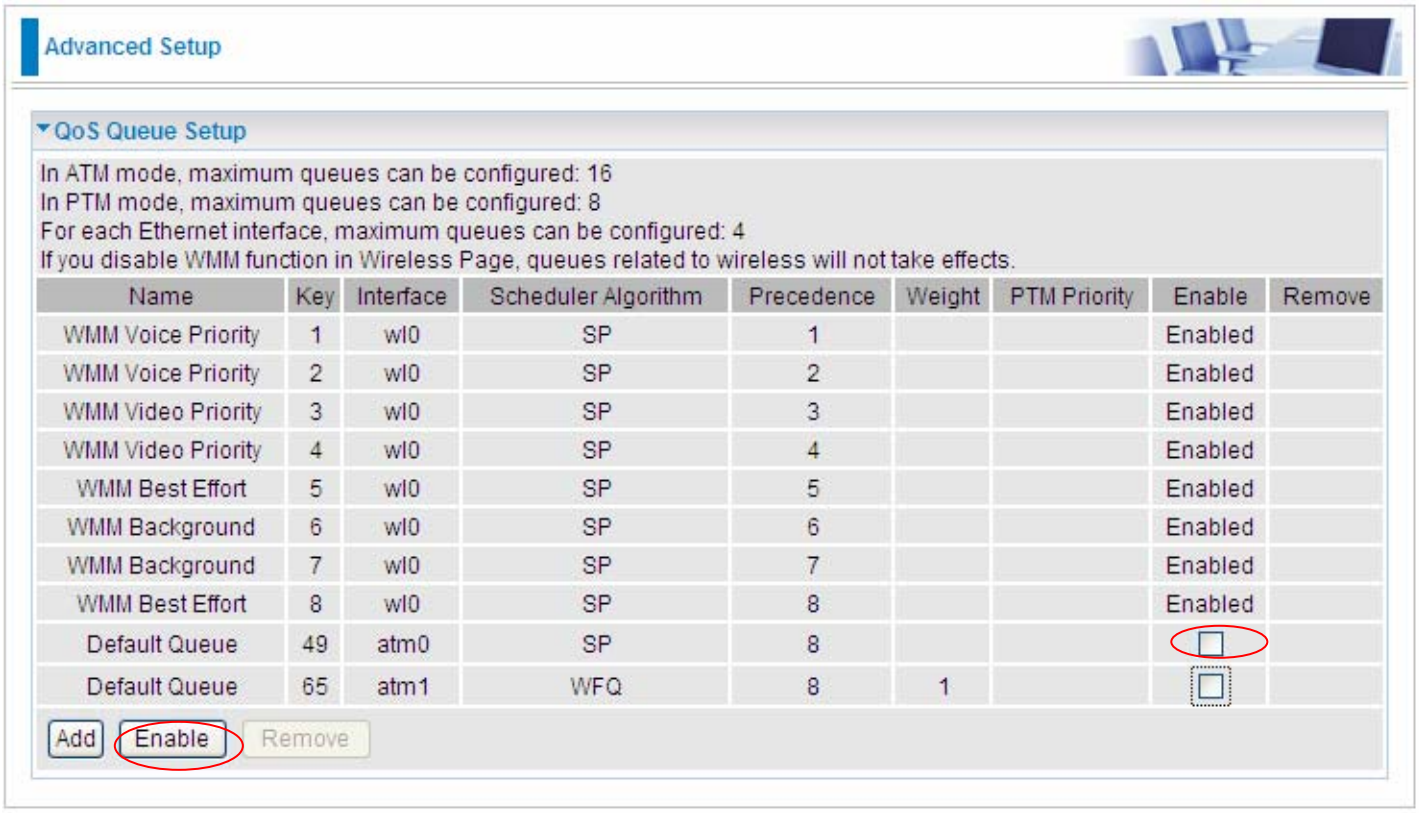
Mapping Table	
Default (000000)	Best Effort
EF(101110)	Expedited Forwarding
AF11 (001010)	Assured Forwarding Class1(L)
AF12 (001100)	Assured Forwarding Class1(M)
AF13 (001110)	Assured Forwarding Class1(H)
AF21 (010010)	Assured Forwarding Class1(L)
AF22 (010100)	Assured Forwarding Class1(M)
AF23 (010110)	Assured Forwarding Class1(H)
AF31 (011010)	Assured Forwarding Class1(L)
AF32 (011100)	Assured Forwarding Class1(M)
AF33 (011110)	Assured Forwarding Class1(H)
AF41 (100010)	Assured Forwarding Class1(L)
AF42 (100100)	Assured Forwarding Class1(M)
AF43 (100110)	Assured Forwarding Class1(H)
CS1(001000)	Class Selector(IP precedence)1
CS2(010000)	Class Selector(IP precedence) 2
CS3(011000)	Class Selector(IP precedence)3
CS4(100000)	Class Selector(IP precedence) 4
CS5(101000)	Class Selector(IP precedence) 5
CS6(110000)	Class Selector(IP precedence) 6
CS7(111000)	Class Selector(IP precedence) 7

DSCP indicates three kinds of service, Class Selector (CS), Assured Forwarding (AF) and Expedited Forwarding (EF). AF1, AF2, AF3 and AF4 are four kinds of assured forwarding services. Each AF has three different packet loss priorities from high, medium, to low. Also, CS1-CS7 indicates the IP precedence.

Click **Apply** to confirm the settings.

Queue Config

Queue is a technology of managing congestion providing precautions with the packets storing and scheduling. Queue Config allows you to configure a QoS queue entry and assign it to a specific network interface. Each queue entry set here will be used by the classfier to place ingress packets appropriately.



Note: the interface set in the **WAN**> **WAN Interface** will be list as Default Queue here, and the parameters listed above can be configured there. For detail, please turn to **WAN** > **WAN Interface** section for help. You can also add other queues to the ATM and PTM interfaces despite of the default queue.

And Wireless Service queue will be enabled by default if you enable wireless. Also if you enable virtual APs, the corresponding WMM service queues will be enabled as well.

Name: the queue name.

Key: the item number.

Interface: the queue interface.

Scheduler Algorithm: the QoS Scheduler Algorithm, SP(Strict Priority) or WFQ(Weight Fair Queuing)

Precedence: the priority identification.

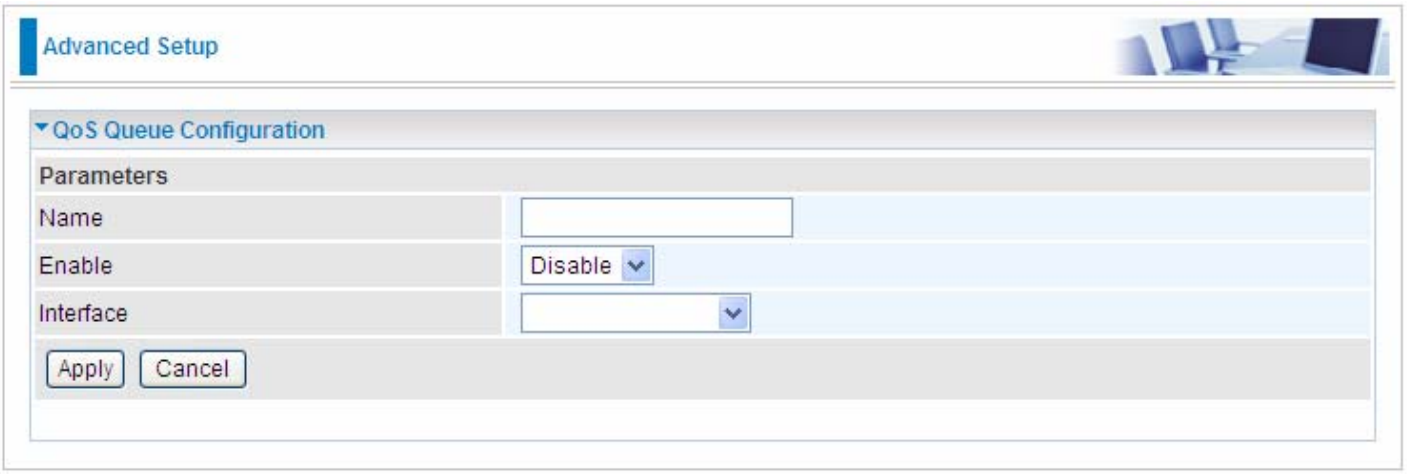
Weight: the weight value, 1-63. the highest is 63.

PTM Priority: the PTM priority, normal or high.

Enable: check the enable check-box, then press **Enable** to activate the queue. If you want to disable this queue, you can uncheck the corresponding check-box and press Enable, the queue will be disabled.

If the queue is enabled, you will see a tick, like . Otherwise, the queue is disabled.

Click **Add** to create a queue.

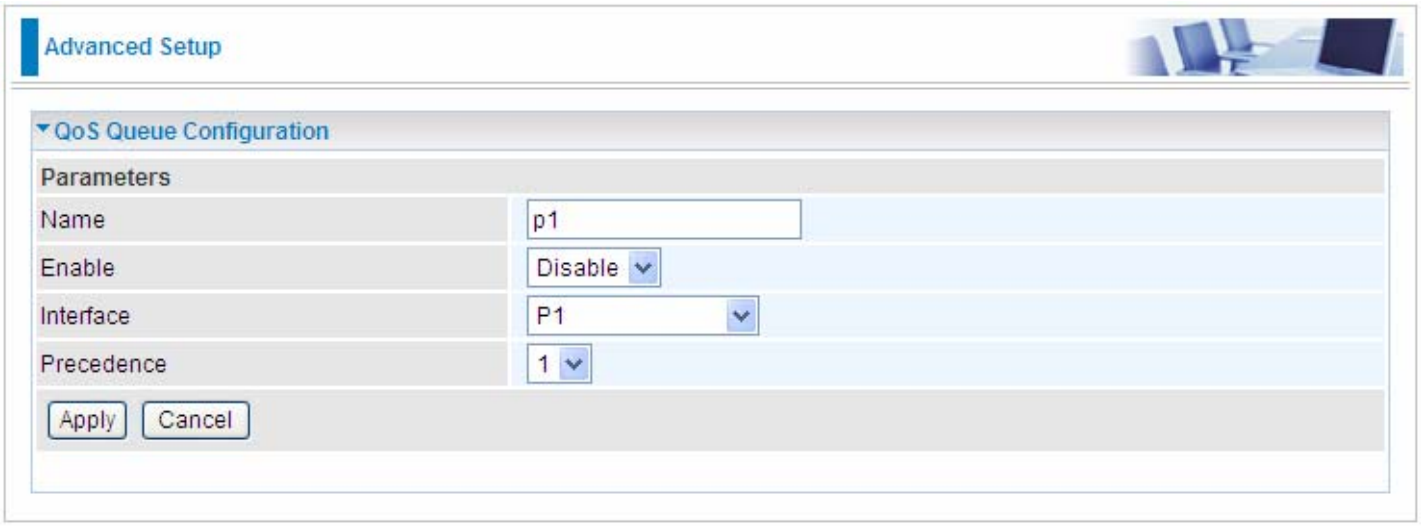


Name: Type the name of the queue.

Enable: Select whether to enable the queue.

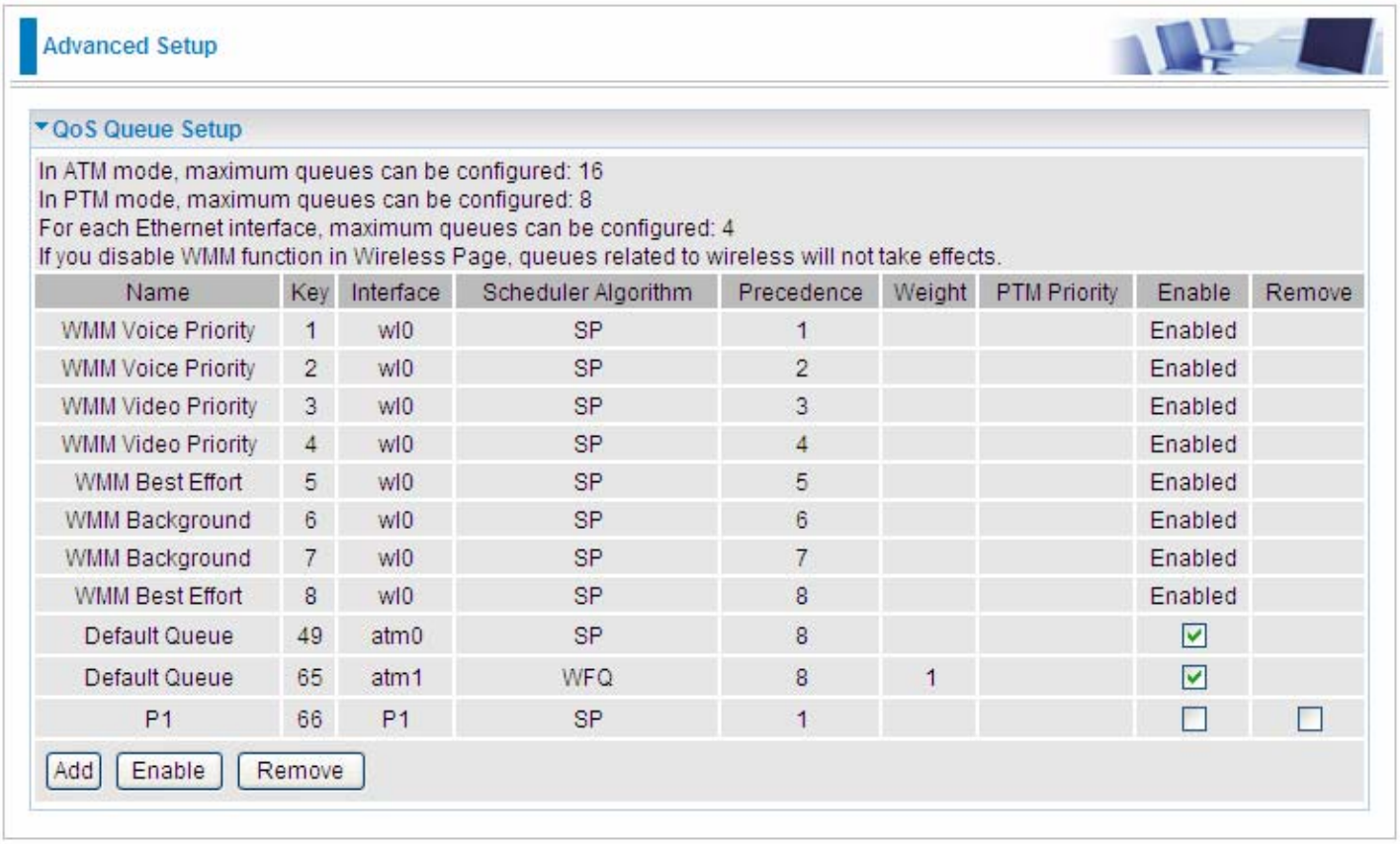
Interface: Select which interface this queue applies to.

Select interface, the following corresponding parameters will appear to let you configure, Enter the information, Click Apply to conform. Then the item will be listed in the table.



Precedence: the precedence of the queue, interface P1-P4, 4 levels from high to low are 1-4. ATM or PTM interfaces, 7 levels from high to low are 1-7, for the precedence of the default queue with the interface of SP Scheduler Algorithm is 8. Here if the interface is of WFQ Scheduler Algorithm, you should enter the weight of the queue.

Click **Apply** to save and the added queue will be listed as below.



Advanced Setup

QoS Queue Setup

In ATM mode, maximum queues can be configured: 16
In PTM mode, maximum queues can be configured: 8
For each Ethernet interface, maximum queues can be configured: 4
If you disable WMM function in Wireless Page, queues related to wireless will not take effects.

Name	Key	Interface	Scheduler Algorithm	Precedence	Weight	PTM Priority	Enable	Remove
WMM Voice Priority	1	wl0	SP	1			Enabled	
WMM Voice Priority	2	wl0	SP	2			Enabled	
WMM Video Priority	3	wl0	SP	3			Enabled	
WMM Video Priority	4	wl0	SP	4			Enabled	
WMM Best Effort	5	wl0	SP	5			Enabled	
WMM Background	6	wl0	SP	6			Enabled	
WMM Background	7	wl0	SP	7			Enabled	
WMM Best Effort	8	wl0	SP	8			Enabled	
Default Queue	49	atm0	SP	8			☑	
Default Queue	65	atm1	WFQ	8	1		☑	
P1	66	P1	SP	1			☐	☐

Add Enable Remove

Enable: check the enable check-box, then press **Enable** to activate the queue. If you want to disable this queue, you can uncheck the corresponding check-box and press Enable, the queue will be disabled.

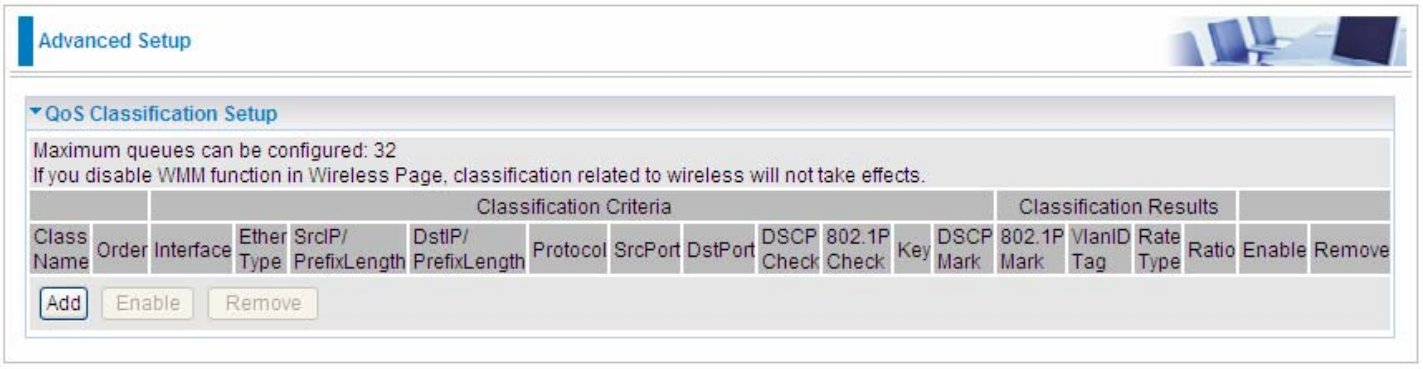
Remove: To delete the QoS rule from the table, check Remove checkbox then click **Remove button** to delete the selected item.

Note: only the queue added via the above mode can be directly removed here, the default queue can’t be removed here, if you want to remove them, remove the interface in **WAN** > **WAN Interface** section.

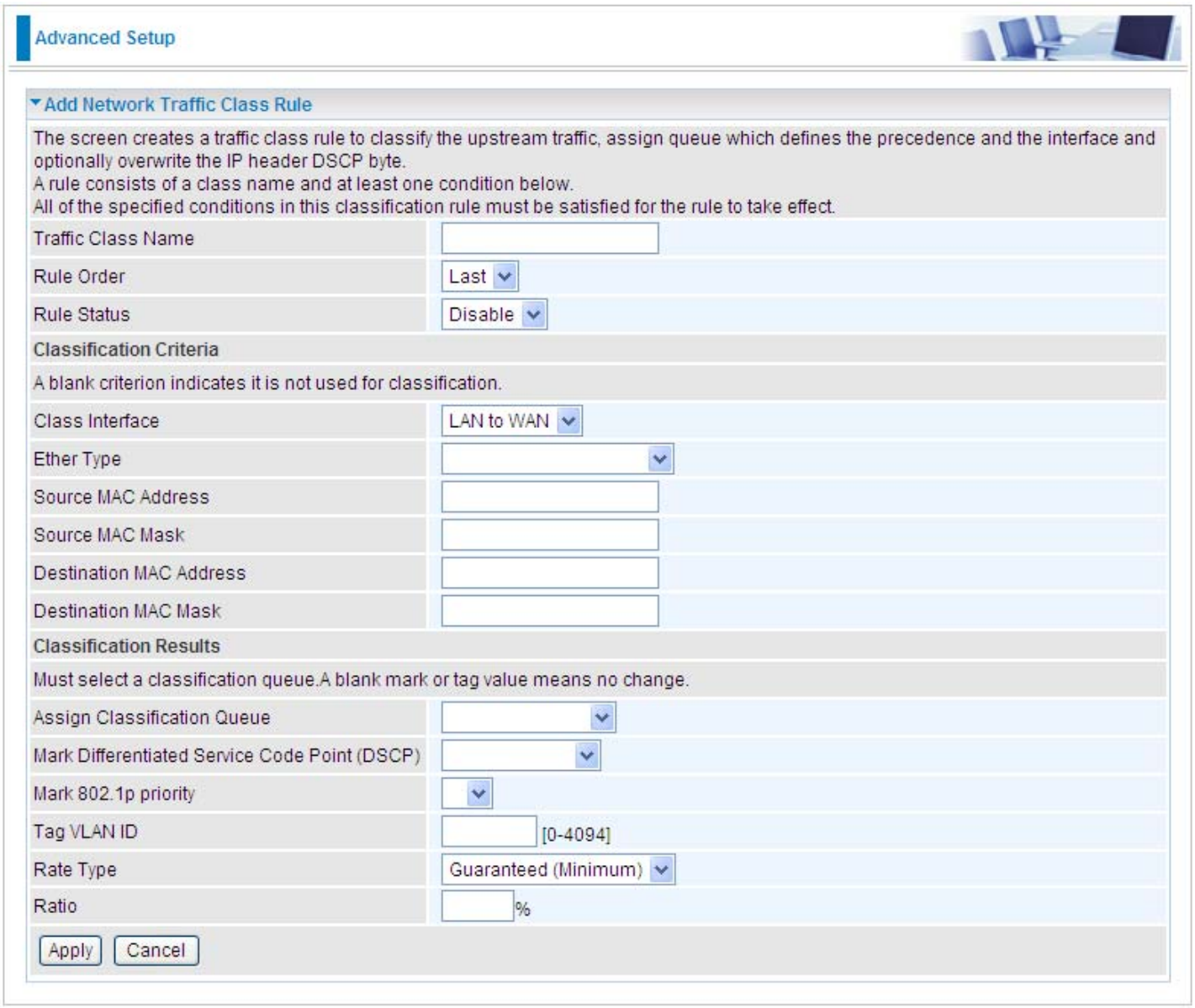
Note: In ATM mode, maximum queues can be configured: 16
In PTM mode, maximum queues can be configured: 8
For each Ethernet interface, maximum queues can be configured: 4
If you disable WMM function in Wireless Page, queues related to wireless will not take effects.

QoS Classification

This screen displays a packet QoS summary table and allows user to add or remove a QoS classification class. This is the main place to configure the classification, marking and queuing rules.



Click **Add** to add Network Traffic Class Rule.



The classification rule is a ‘AND’ mode, that is a rule takes effect only when all of the specified conditions must be satisfied.

Parameters

Traffic Class Name: Assign a name for this class to uniquely identify the others among multiple classes.

Rule Order: Select the priority for this class rule.

Rule Status: Select **Enable** to activate this class rule.

Specify Classification Criteria

The following parameters are to be classification rule. Enter or select appropriate parameters on the following fields. A blank criterion indicates it is not used for classification.

Class Interface: select the interface you want to be the one aspect of the classification criteria. Here ”LAN->WAN” and ”WAN->LAN” can be viewed as IP QoS, the others can be viewed as ported-based QoS, which means that control the QoS of certain port such. For example, if you select P1 port, then criteria applies to this port, that is ported-based QoS.

Entry Type: select the application type.

Source/destination MAC Address: enter the source and destination MAC address as the QoS Classification Criteria. The format should be xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.

Source/destination MAC Mask: MAC mask is similar to IP mask, and the format also should be xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx. It is used to hide some information of the MAC address. ‘1’, means needed and ‘0’ means ignored. For example, MAC address e0:3b:4a:c2:ca:e2 and MAC mask ff:ff:ff:00:00:00, that is whatever MAC address while matches e0:3b:4a:XX:XX:XX, will be accepted.

Specify Classification Results

Enter or select appropriate parameters you want for the packets matched the above classification criteria in the following fields. You have to choose a classification queue. A blank mark or tag value means no change.

Assign Classification Queue: assign classification queue from the drop-down box. If you want to select the queue, you should make sure the specific queue is enabled in **Queue Config** section.

Mark Differentiated Service Code Point (DSCP): select the DSCP you want to be the new DSCP for the packets which matched the above classification criteria.

Mark 802.1p priority: it is a LAN Layer 2 QoS/CoS Protocol for Traffic Prioritization. It is interoperable with IEEE 802.1Q. 802.1p has 8 kinds of priority.

Tag VLAN ID: enter the tag VLAN ID, 0-4094, used to determine the VLAN the frame belongs to.

Rate Type: You can choose Limited or Guaranteed.

Ratio: The rate percent in contrast to that on WAN interface.

Note: 802.1p/vlan tag feature be supported only when in bridge mode, DSL WAN interface.

Click Apply to confirm the settings and you will be returned to the QoS Classification page.

Enable: To disable the item, please uncheck Enable check box then click Enable button.

Remove: To delete the QoS class from the table, check Remove checkbox then click Remove button to delete the selected item.

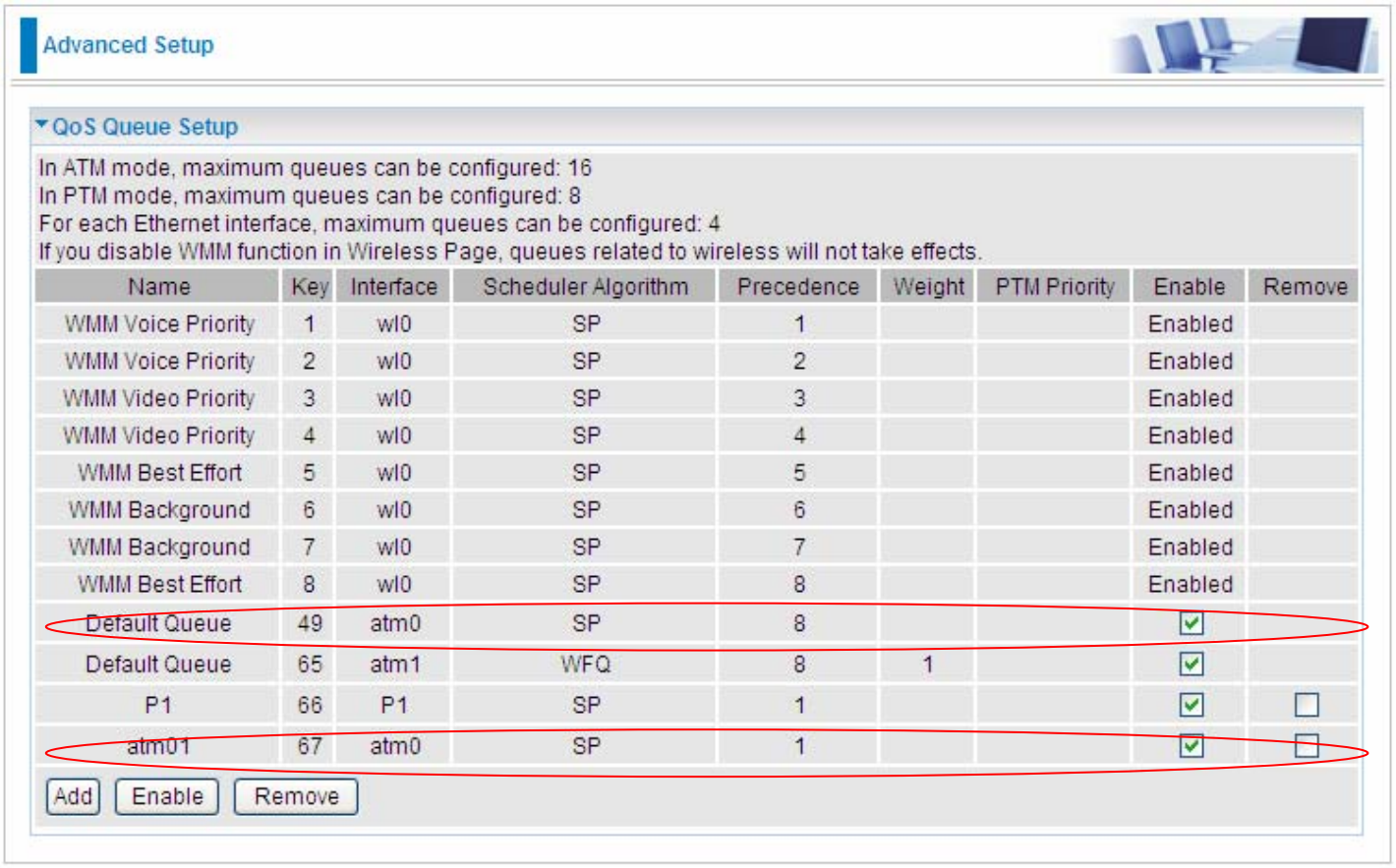
Set up a QoS Classification

IP QoS

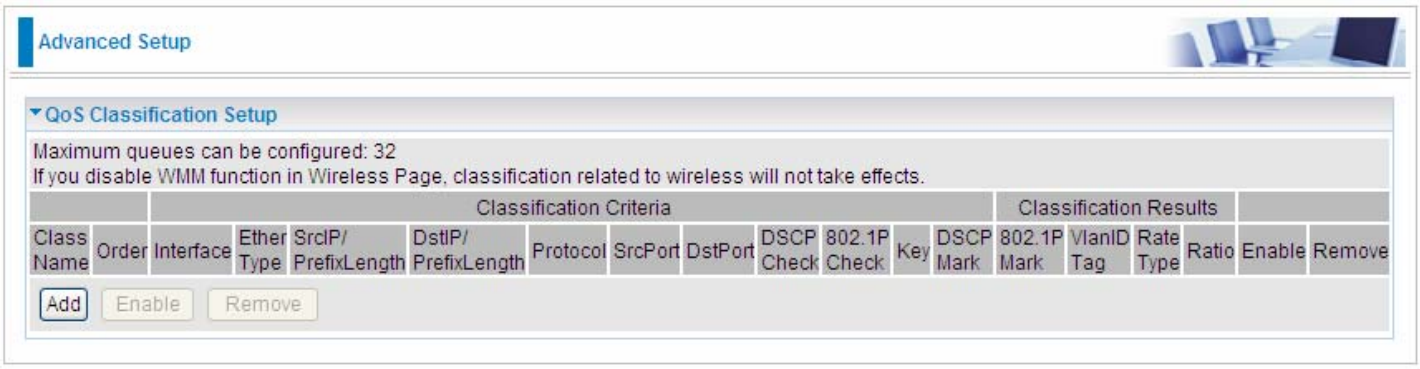
LAN to WAN IP QoS

1. It is a QoS controlling the traffic from LAN to WAN. So first make sure there is at least one WAN queue. If you have configured WAN interface and it will appeared as a default queue, you can also add other queues of the specific interface. See **Queue Config**.

Here we have a atm0 (WAN interface), the interface has a default queue and an added queue. Make sure to enable the queue.

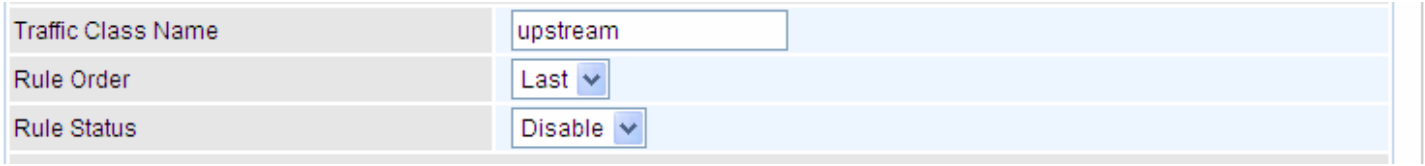


2. In QoS Classification Setup page, Click **Add** to add a Qos Classification.

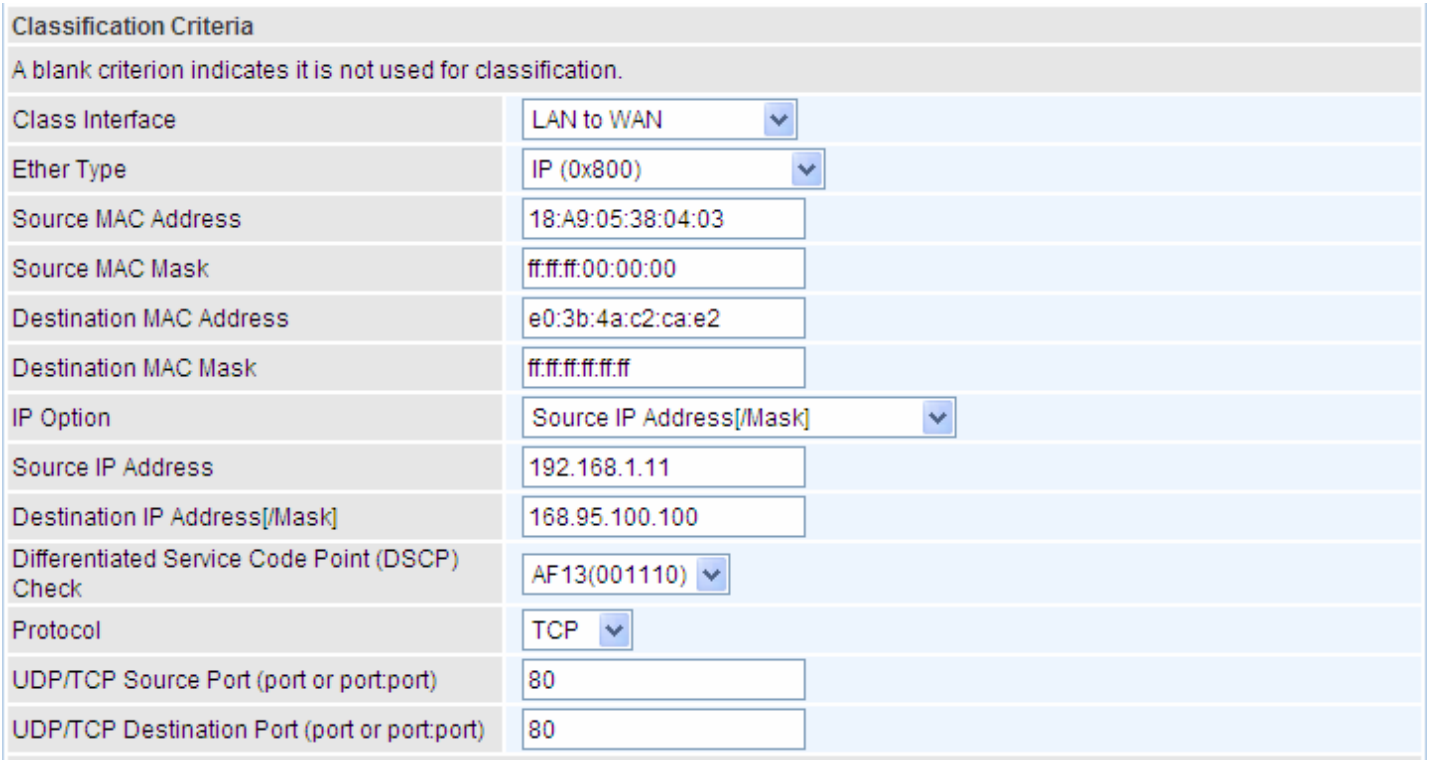


Then in the appeared Add Network Traffic Class Rule page, enter the information to set up a rule.

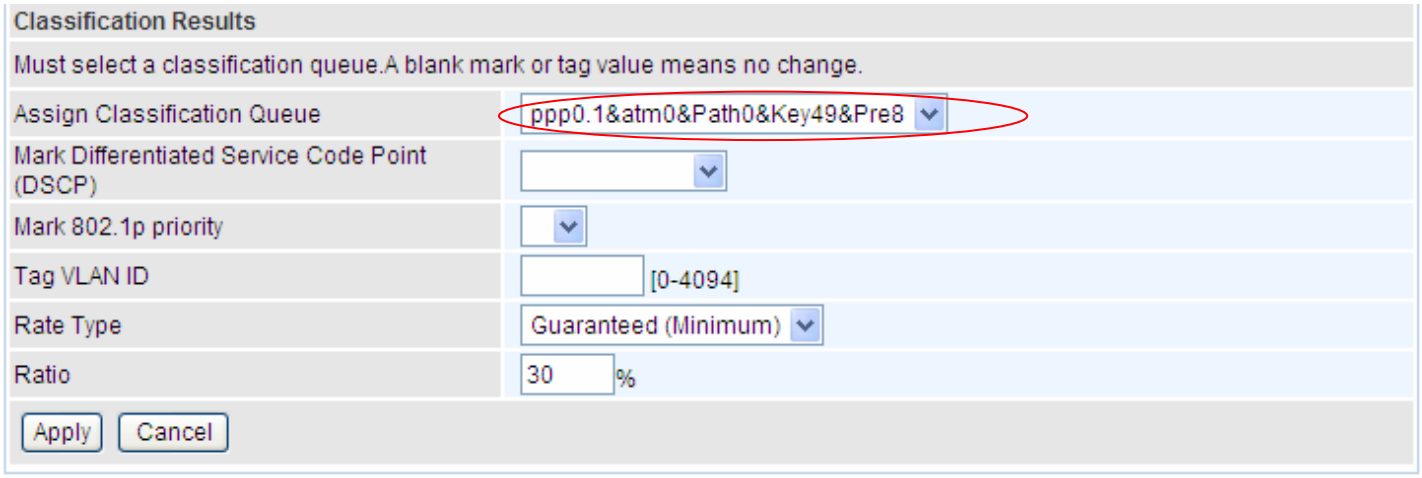
1) Specify the rule name, rule order, and rule status.



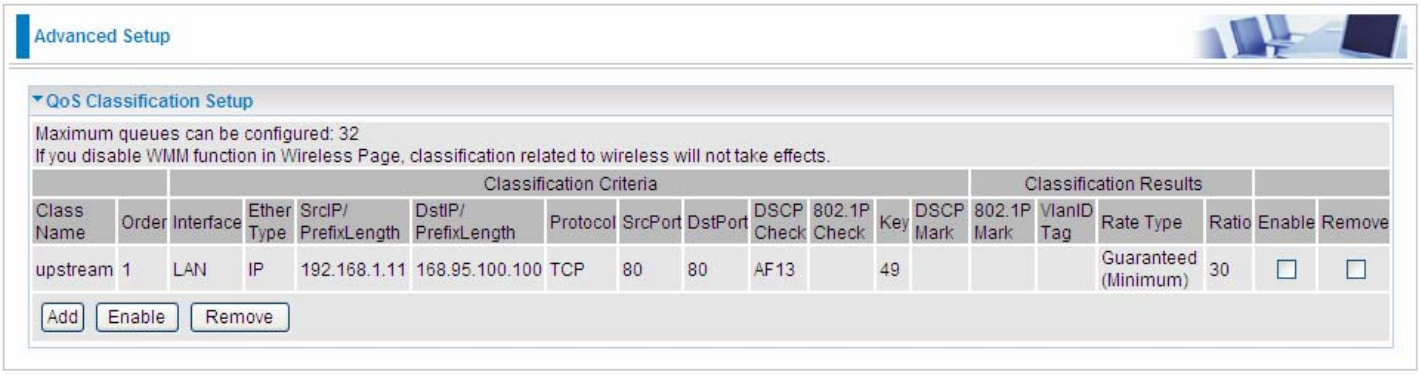
2) Specify the classification criteria. Here you can set every parameter to strictly control the specific traffic or you can set several parameters to let them be the key elements to control the traffic. A blank criterion indicates it is not used for classification.



3) Specify the classification results. Here you must Assign Classification Queue. Whether the following parameters are needed is according to your needs. If you do not want to change the original information, please leave it empty. The queues listed here in the Assign Classification Queue are WAN interface queues set in Queue Config section. Select the needed queue. If you find none queues here, turn back to check whether you have configured a queue and enable it.



3. Click **Apply** to save your settings. The added rule will listed as below.



Enable: check the enable check-box, then press **Enable** to activate the rule. If you want to disable this rule, you can uncheck the corresponding check-box and press **Enable** button, the rule will be disabled.

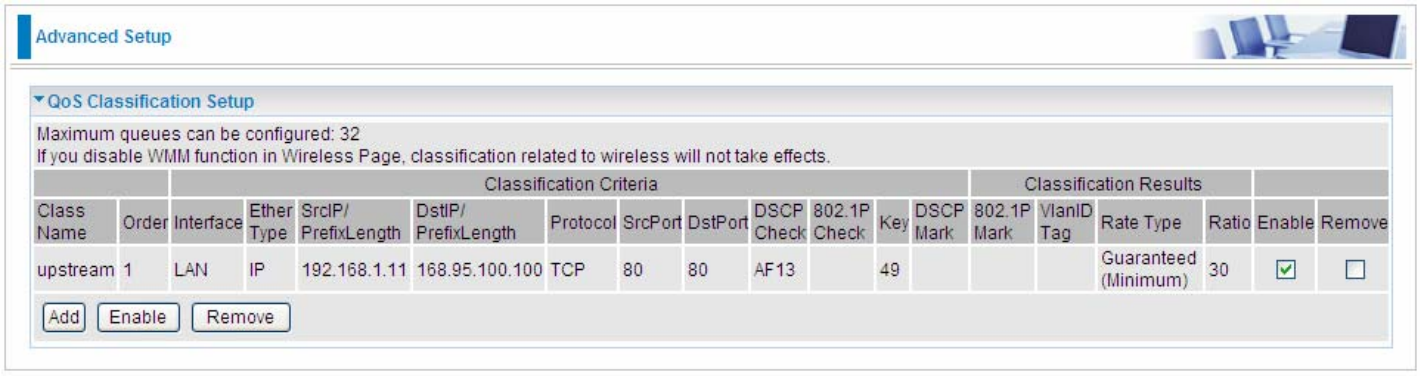
Remove: To delete the QoS class from the table, check Remove checkbox then click **Remove** button to delete the selected item.

WAN to LAN IP QoS

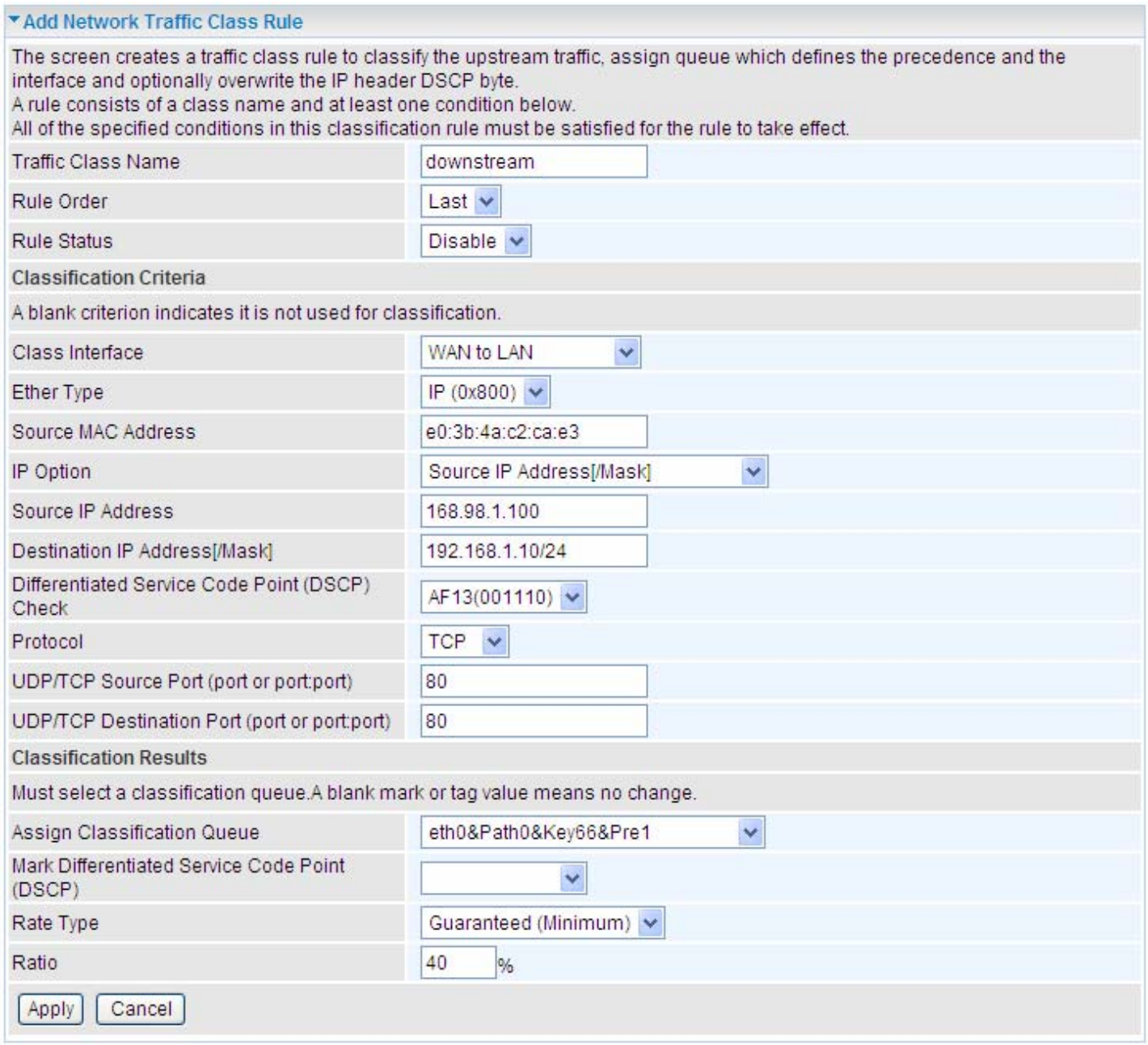
1. Here we take WAN to LAN (P1) QoS for example. Make sure there are enabled port P1 based queues here. LAN queues need your configuration. You can enable wireless to enable WMM queues by default or add P1-P4 ported based queues manually.

P1	66	P1	SP	1			☑	☐

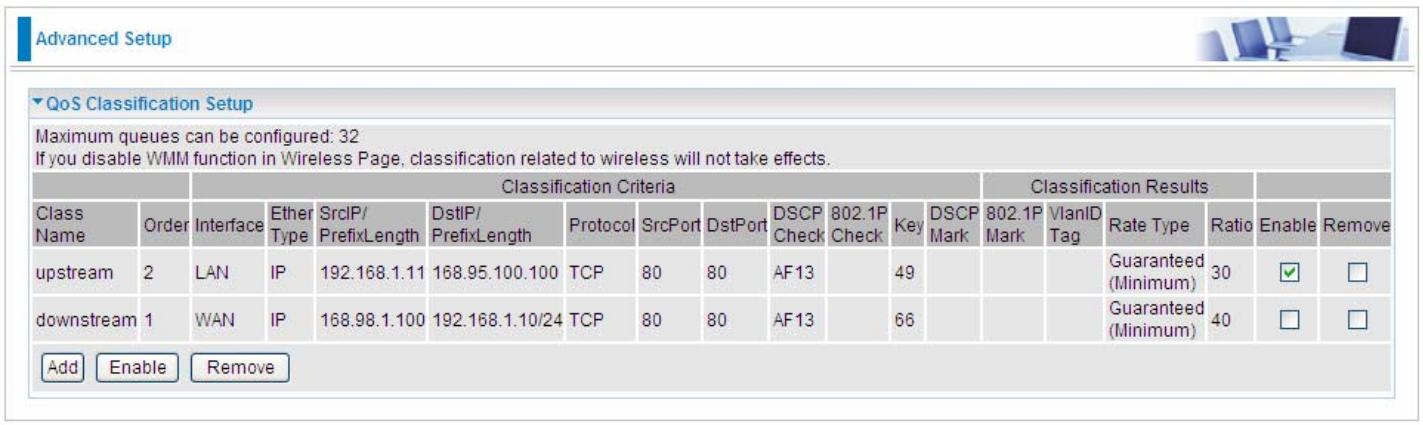
2. In QoS Classification Setup page, Click **Add** to add a Qos Classification.



Then in the Add Network Traffic Class Rule page, enter the information to set up a rule.



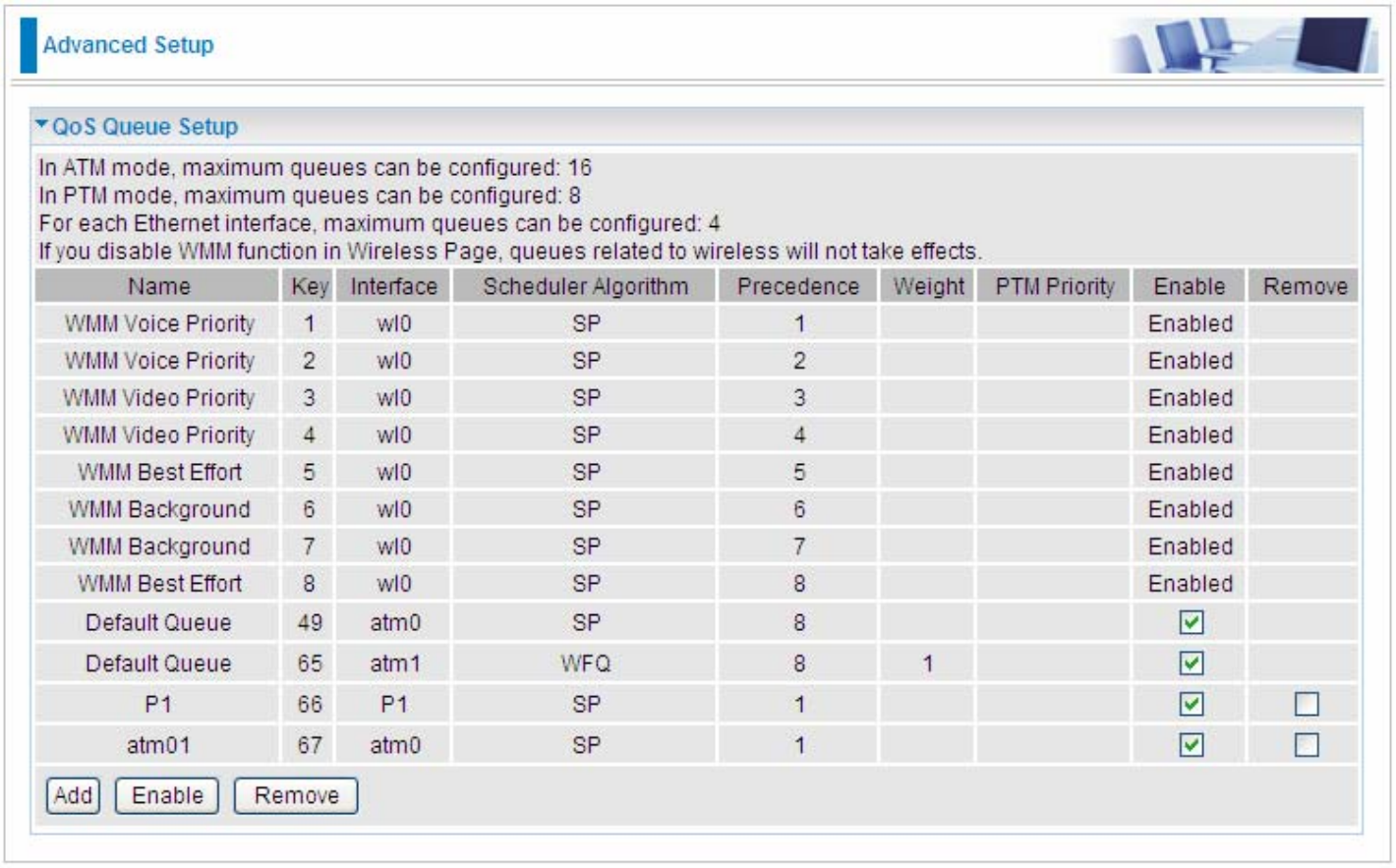
3. Click **Apply** to save your settings. The added rule will be listed as below.



Port-based QoS

Take port P1 to WAN QoS for example.

1. First make sure there is at least a WAN queue and it is enabled.



Advanced Setup

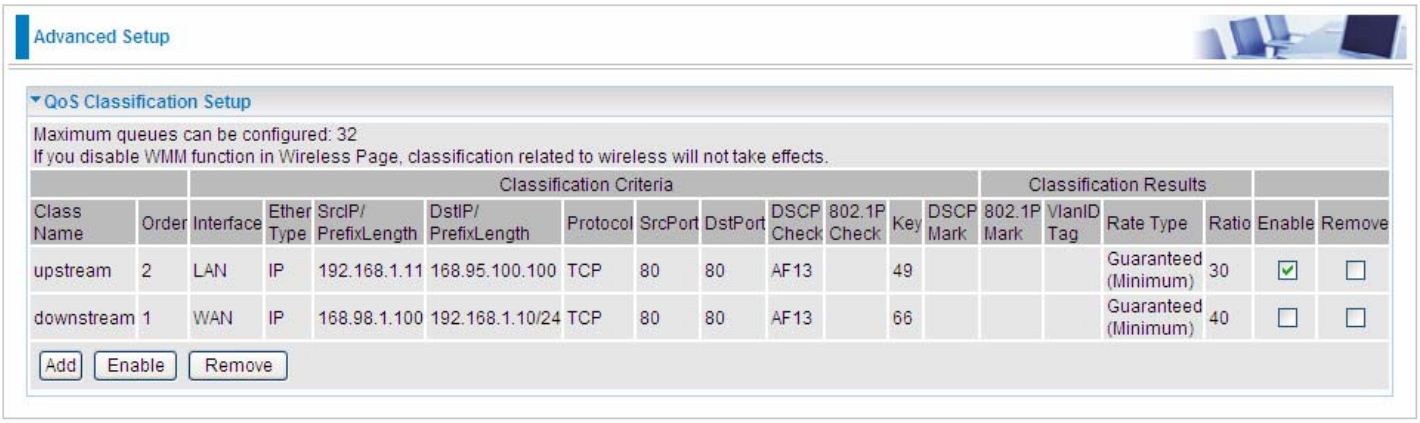
QoS Queue Setup

In ATM mode, maximum queues can be configured: 16
In PTM mode, maximum queues can be configured: 8
For each Ethernet interface, maximum queues can be configured: 4
If you disable WMM function in Wireless Page, queues related to wireless will not take effects.

Name	Key	Interface	Scheduler Algorithm	Precedence	Weight	PTM Priority	Enable	Remove
WMM Voice Priority	1	wl0	SP	1			Enabled	
WMM Voice Priority	2	wl0	SP	2			Enabled	
WMM Video Priority	3	wl0	SP	3			Enabled	
WMM Video Priority	4	wl0	SP	4			Enabled	
WMM Best Effort	5	wl0	SP	5			Enabled	
WMM Background	6	wl0	SP	6			Enabled	
WMM Background	7	wl0	SP	7			Enabled	
WMM Best Effort	8	wl0	SP	8			Enabled	
Default Queue	49	atm0	SP	8			☑	
Default Queue	65	atm1	WFQ	8	1		☑	
P1	66	P1	SP	1			☑	☐
atm01	67	atm0	SP	1			☑	☐

Add Enable Remove

2. In QoS Classification Setup page, Click **Add** to add a QoS Classification.



Advanced Setup

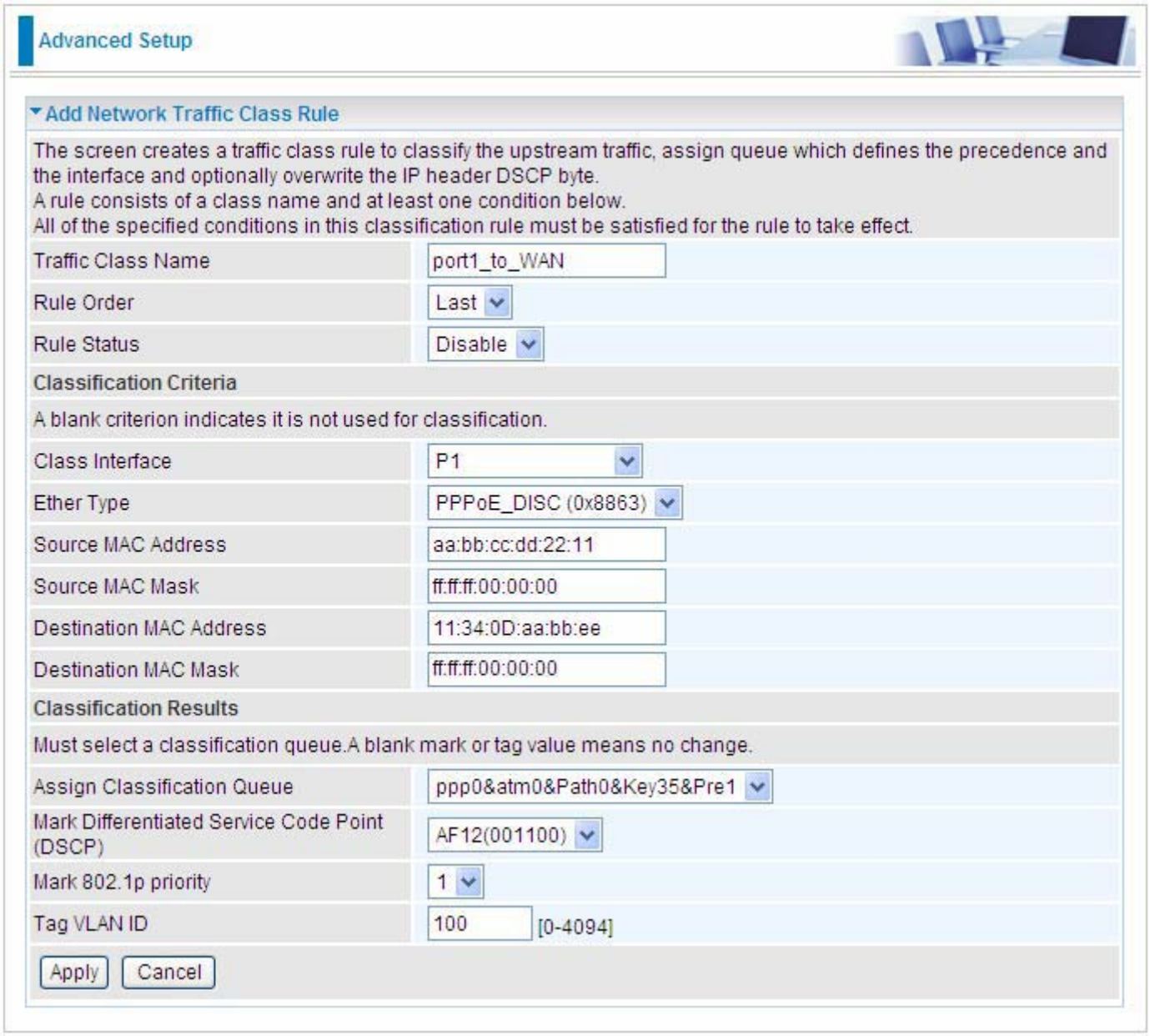
QoS Classification Setup

Maximum queues can be configured: 32
If you disable WMM function in Wireless Page, classification related to wireless will not take effects.

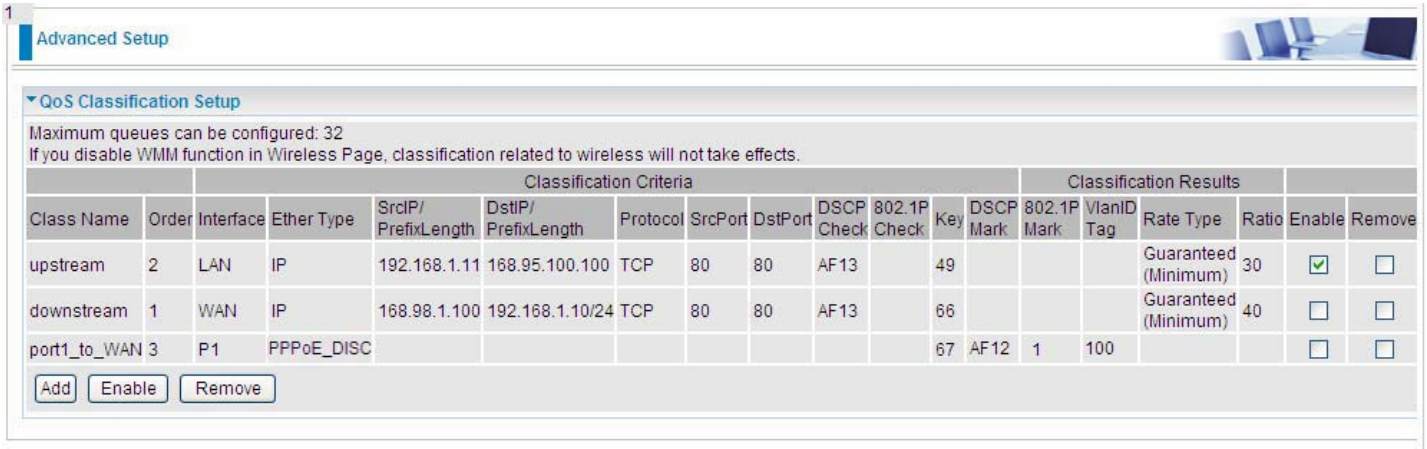
		Classification Criteria										Classification Results					
Class Name	Order	Interface	Ether Type	SrcIP/ PrefixLength	DstIP/ PrefixLength	Protocol	SrcPort	DstPort	DSCP Check	802.1P Check	Key	DSCP Mark	802.1P Mark	VlanID Tag	Rate Type	Ratio	Enable	Remove
upstream	2	LAN	IP	192.168.1.11	168.95.100.100	TCP	80	80	AF13		49				Guaranteed (Minimum)	30	☑	☐
downstream	1	WAN	IP	168.98.1.100	192.168.1.10/24	TCP	80	80	AF13		66				Guaranteed (Minimum)	40	☐	☐

Add Enable Remove

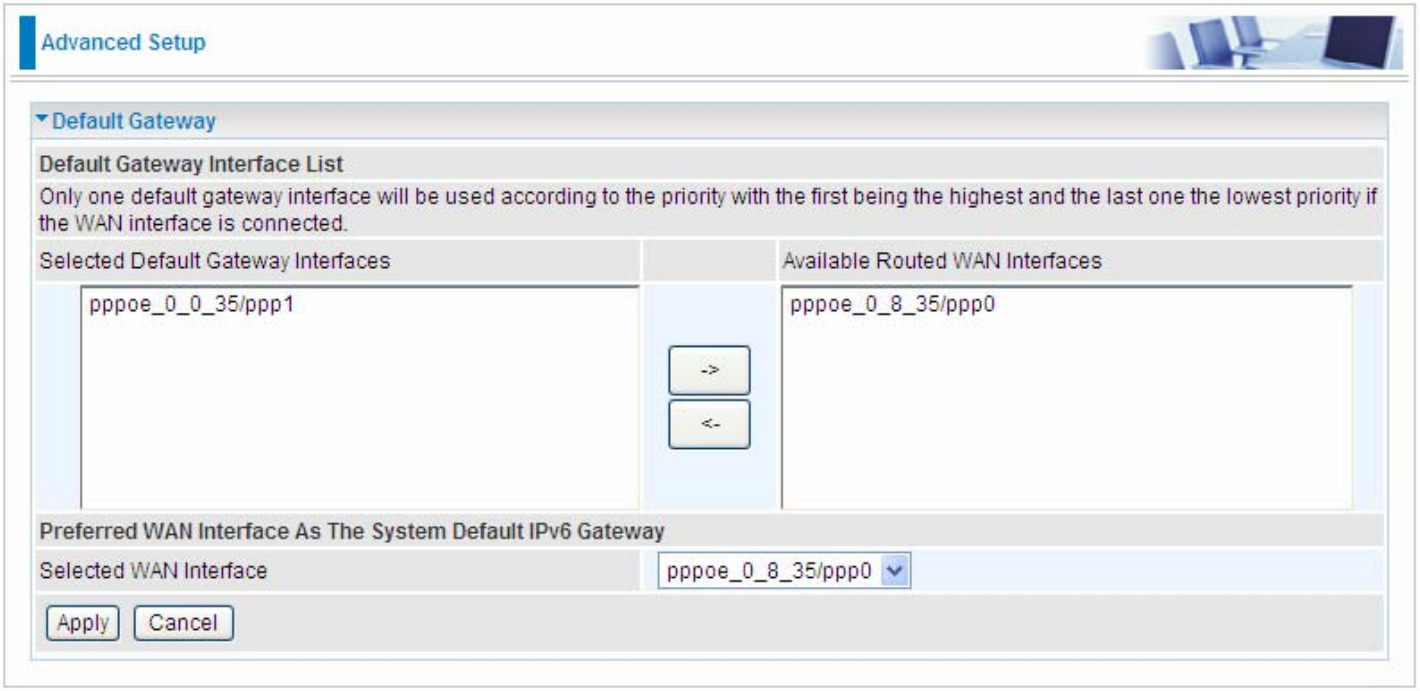
Then in the Add Network Traffic Class Rule page, enter the information to set up a rule to your needs. To Assign Classification queue, select the needed WAN queue.



3. Click **Apply** to save your settings and the added rule will be listed as below.



Default Gateway

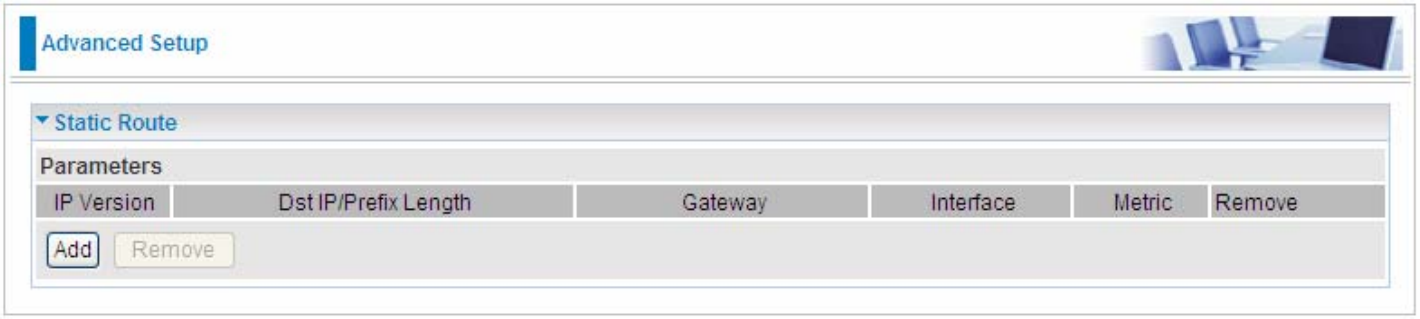


To set default gateway and Available Routed WAN Interface. This interfaces are the ones you have set in WAN section, here select the one you want to be the default gateway by moving the interface via -> or <-. And select a Default IPv6 Gateway from the drop-down menu.

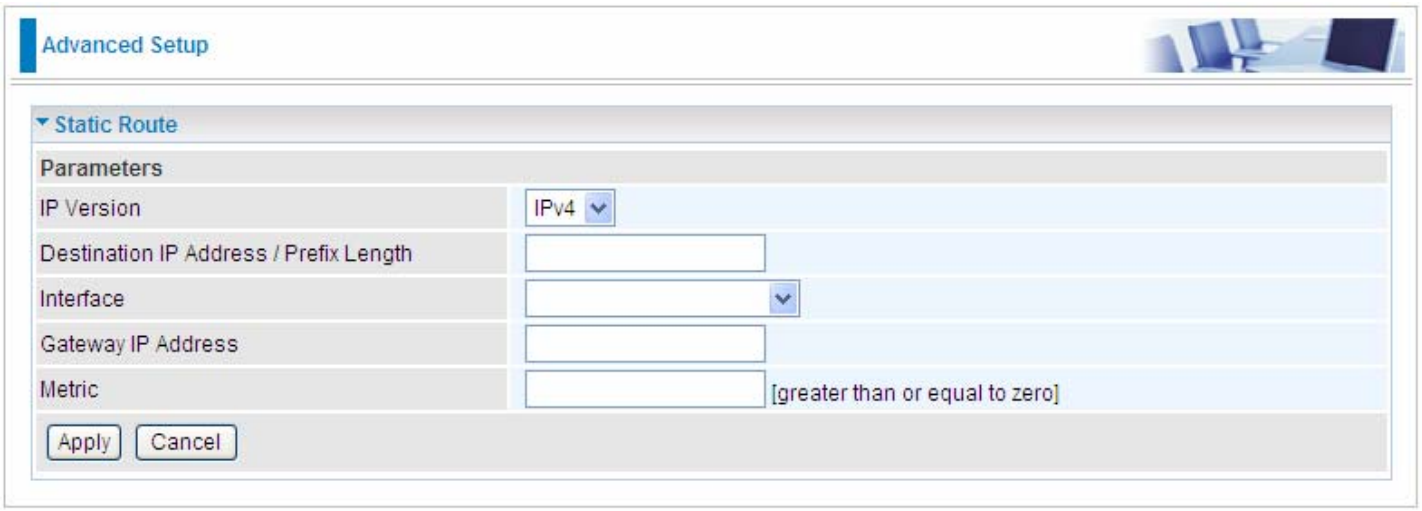
Note: Only one default gateway interface will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected.

Static Route

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



Above is the static route listing table, click Add to create static routing.



IP Version: select the IP version, IPv4 or IPv6.

Destination IP Address / Prefix Length: enter the destination IP address and the prefix length. For IPv4, the prefix length means the number of '1' in the submask, it is another mode of presenting submask. One IPv4 address,192.168.1.0/24, submask is 255.255.255.0. While in IPv6, IPv6 address composes of two parts, thus, the prefix and the interface ID, the prefix is like the net ID in IPv4, and the interface ID is like the host ID in IPv4. The prefix length is to identify the net ID in the address. One IPv6 address, 3FFE:FFFF:0:CD30:0:0:0:0 / 64, the prefix is 3FFE:FFFF:0:CD3.

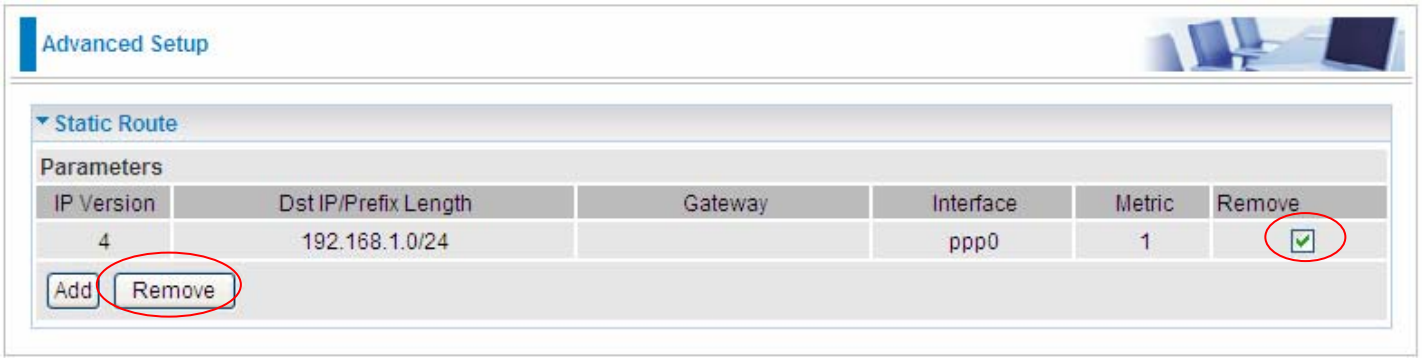
Interface: select an interface this route associated.

Gateway IP Address: enter the gateway IP address.

Metric: Metric is a policy for router to commit router, to determine the optimal route. Enter one number greater than or equal to 0.

Click **Apply** to apply this route and it will be listed in the route listing table.

In listing table you can remove the one you don't want by checking the checking box and press **Remove** button.



Policy Routing

Here users can set a route for the host (source IP) in a LAN interface to access outside through a specified Default Gateway or a WAN interface.

The following is the policy Routing listing table.

Click **Add** to create a policy route.

Policy Name: user-defined name.

Physical LAN Port: select the LAN port.

Source IP: enter the Host Source IP.

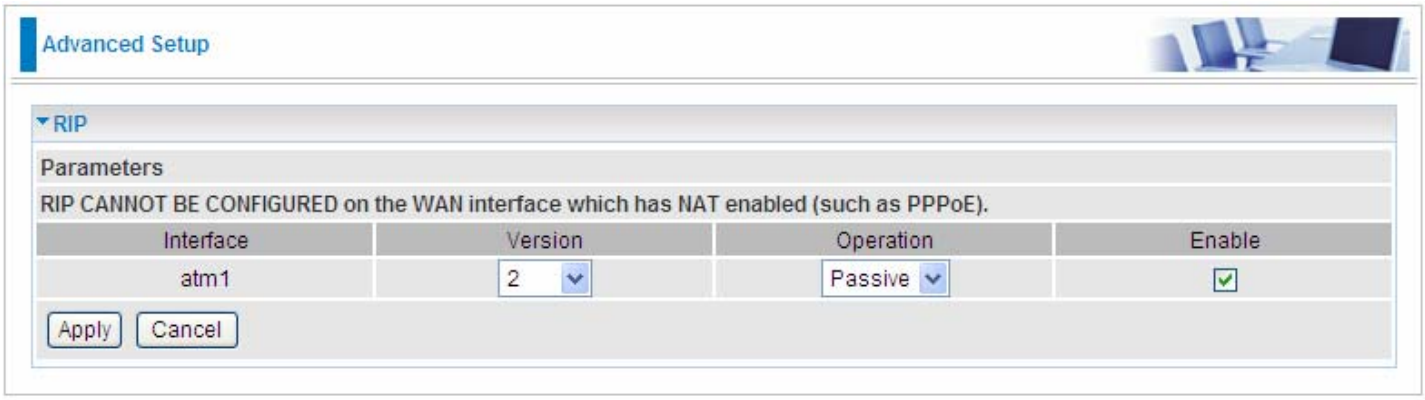
Interface: select the WAN interface which you want the Source IP to access outside through.

Default Gateway: enter the default gateway which you want the Source IP to access outside through.

Click **Apply** to apply your settings. And the item will be listed in the policy Routing listing table. Here if you want to remove the route, check the remove checkbox and press Remove to delete it.

RIP

RIP, Router Information Protocol, is a simple Interior Gateway Protocol (IGP). RIP has two versions, RIP-1 and RIP-2.



Interface: the interface the rule applies to.

Version: select the RIP version, there are two versions, RIP-1 and RIP-2.

Operation: RIP has two operation mode.

- **Passive:** only receive the routing information broadcasted by other routers and modifies its routing table according to the received information.
- **Active:** working in this mode, the router sends and receives RIP routing information and modifies routing table according to the received information.

Enable: check the checkbox to enable RIP rule for the interface.

Note: RIP can not be configured on the WAN interface which has NAT enabled (such as PPPoE).

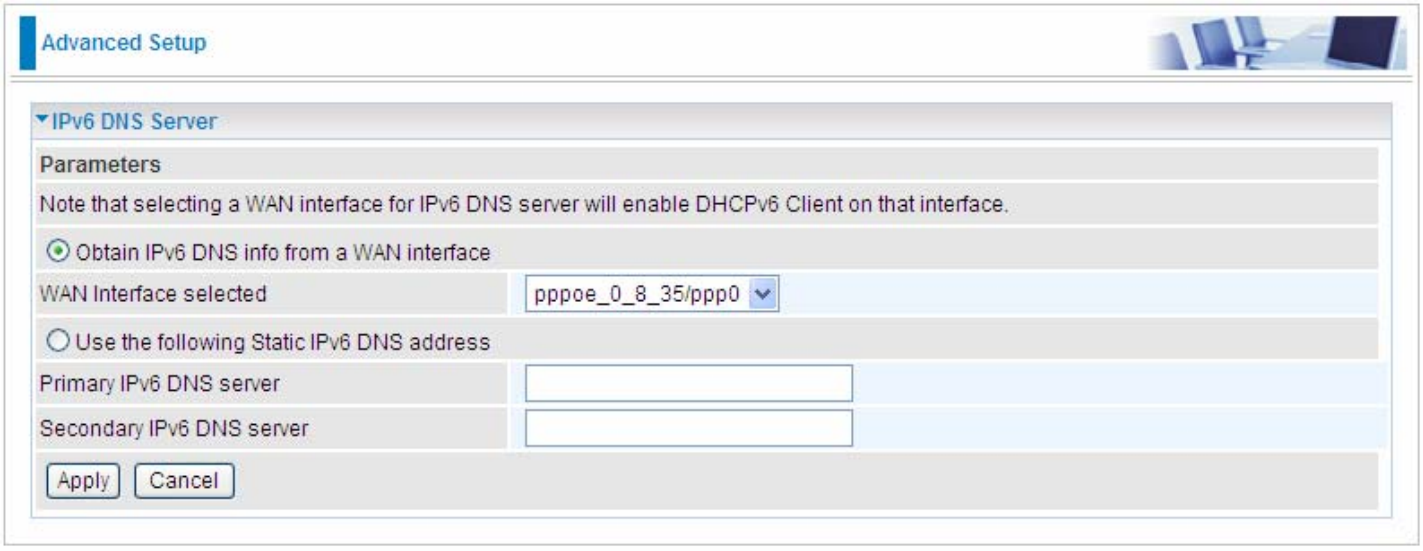
Click **Apply** to apply your settings.

DNS

DNS, Domain Name System, is a distributed database of TCP/IP application. DNS provides translation of Domain name to IP.

IPv6 DNS Server

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

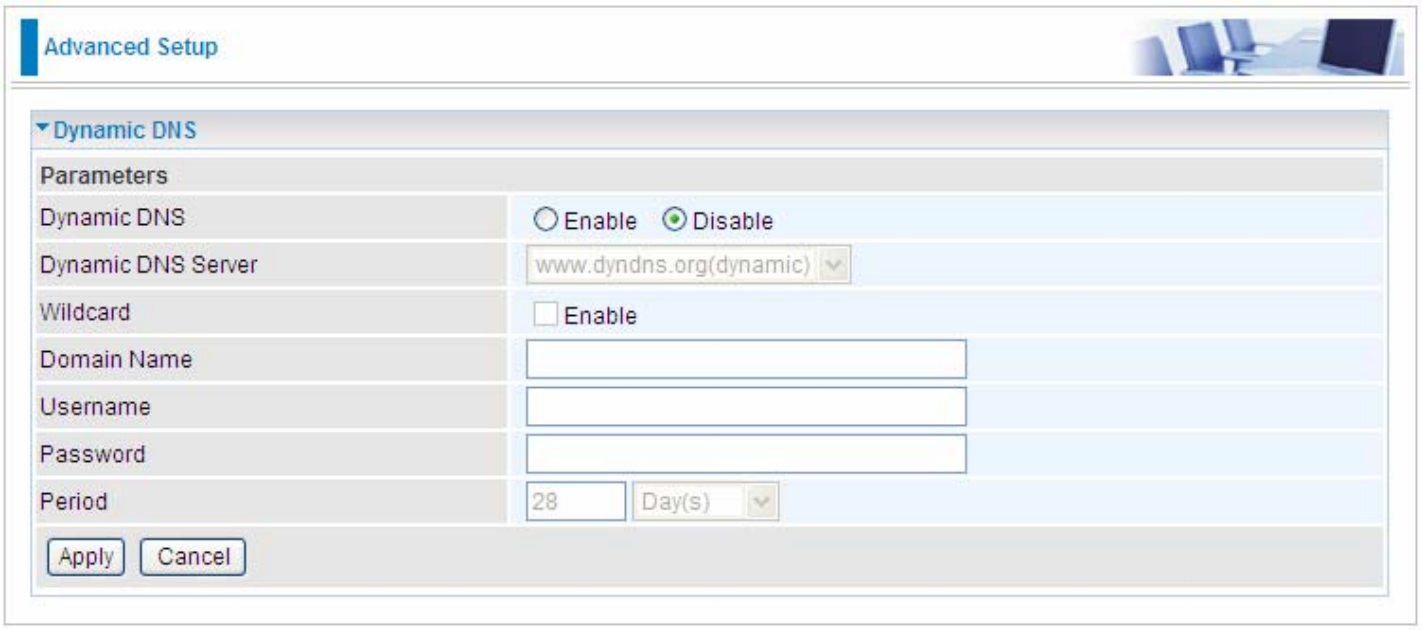
WAN Interface selected: select one configured IPv6 WAN connection from the drop-down menu to be as an IPv6 DNS.

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.

Dynamic DNS

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



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

Dynamic DNS:

- **Disable:** Check to disable the Dynamic DNS function.
- **Enable:** Check to enable the Dynamic DNS function. The following fields will be activated and required.

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

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

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

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

DSL

This screen allows you to set DSL parameters. DSL knowledge is required to configure these settings. Contact your ISP to make sure that these parameters are correct.

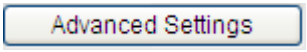
Modulation: There are 7 modes “G.Dmt”, “G.lite”, “T1.413”, “ADSL2”, “AnnexL”, ”ADSL2+”, “AnnexM” that user can select for this connection.

Phone line pair: This is for reserved only. You can choose "Inner Pair" or "Outer Pair".

Capability: There are 2 options “Bitswap Enable” and “SRA Enable” that user can select for this connection.

- **Bitswap Enable:** Allows bitswaping function.
- **SRA Enable:** Allows seamless rate adaptation.

Click Apply to confirm the settings.

Click  to future configure DSL.

Select the Test Mode, or leave it as default.

Tone Selection: suggesting you to leave it as default or let it configured by an advanced user.

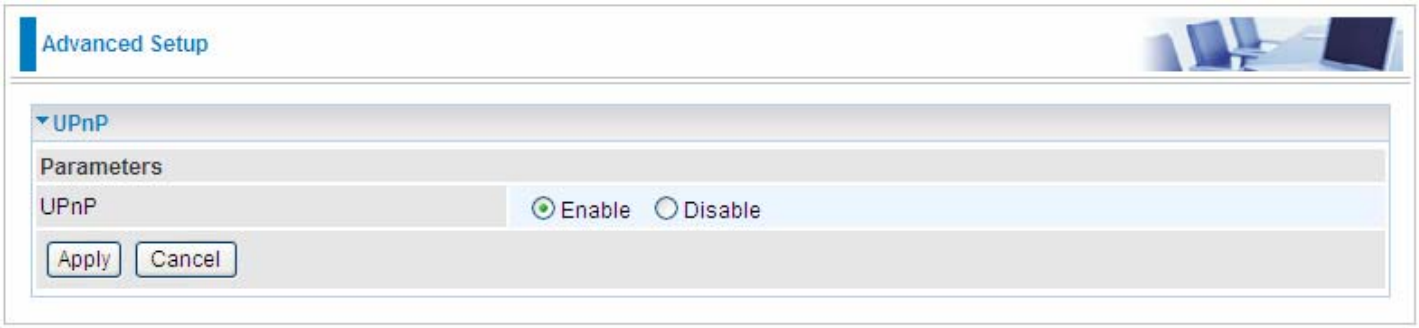
The frequency band of ADSL is split up into 256 separate tones, each spaced 4.3125 kHz apart.

With each tone carrying separate data, the technique operates as if 256 separate modems were running in parallel. The tone range is from 0 to 31 for upstream and from 32 to 255 for downstream。

UPnP

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

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



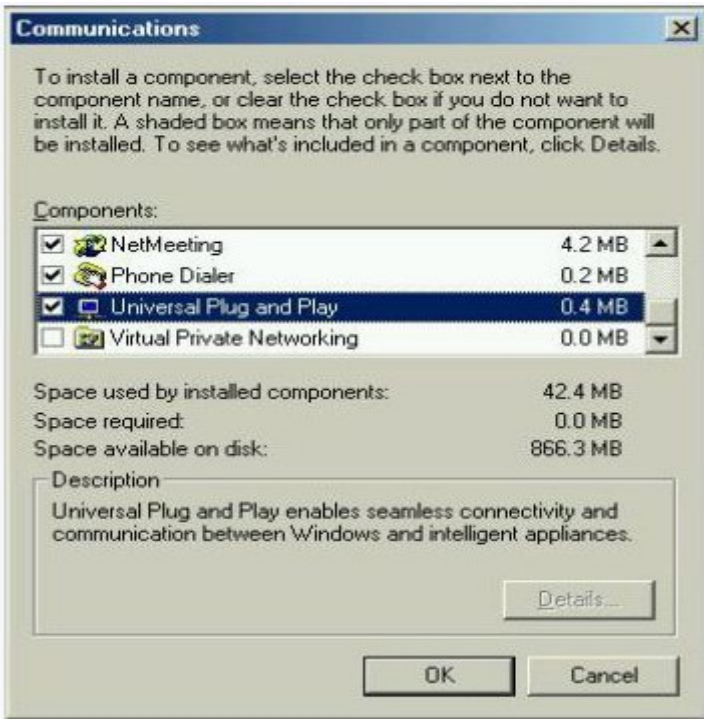
UPnP:

- **Enable:** Check to enable the router's UPnP functionality.
- **Disable:** Check to disable the router's UPnP functionality.

Installing UPnP in Windows Example

Follow the steps below to install the UPnP in Windows Me.
Step 1: Click Start and Control Panel. Double-click Add/Remove Programs.
Step 2: Click on the Windows Setup tab and select Communication in the Components selection box. Click Details.

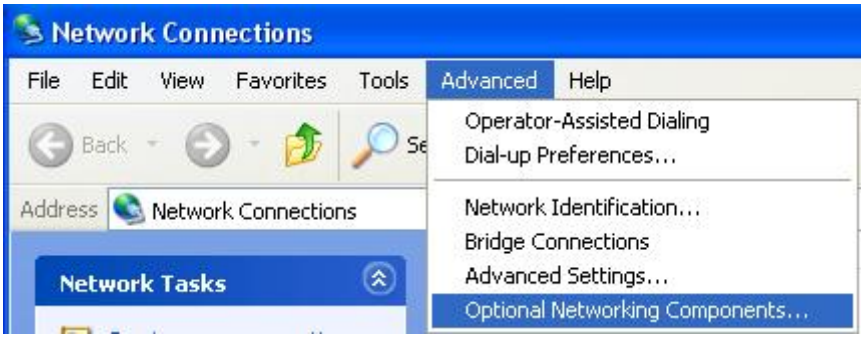
Step 3: In the Communications window, select the Universal Plug and Play check box in the Components selection box.



Step 4: Click OK to go back to the Add/Remove Programs Properties window. Click Next.
Step 5: Restart the computer when prompted.

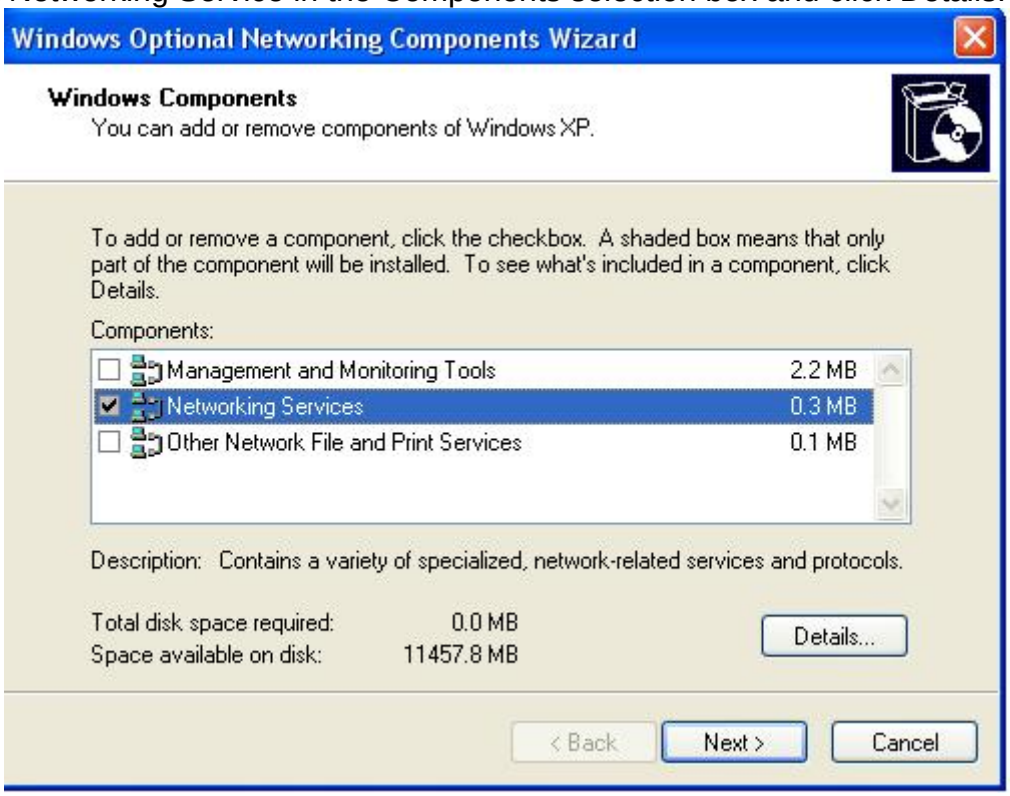
Follow the steps below to install the UPnP in Windows XP.

Step 1: Click Start and Control Panel.
Step 2: Double-click Network Connections.
Step 3: In the Network Connections window, click Advanced in the main menu and select Optional Networking Components ….

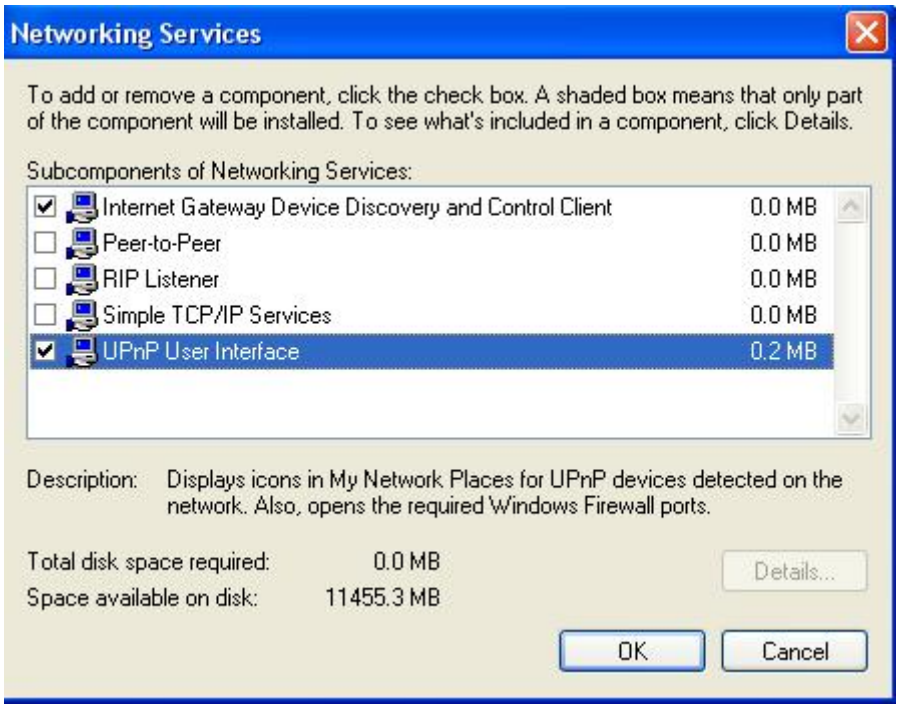


The Windows Optional Networking Components Wizard window displays.

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

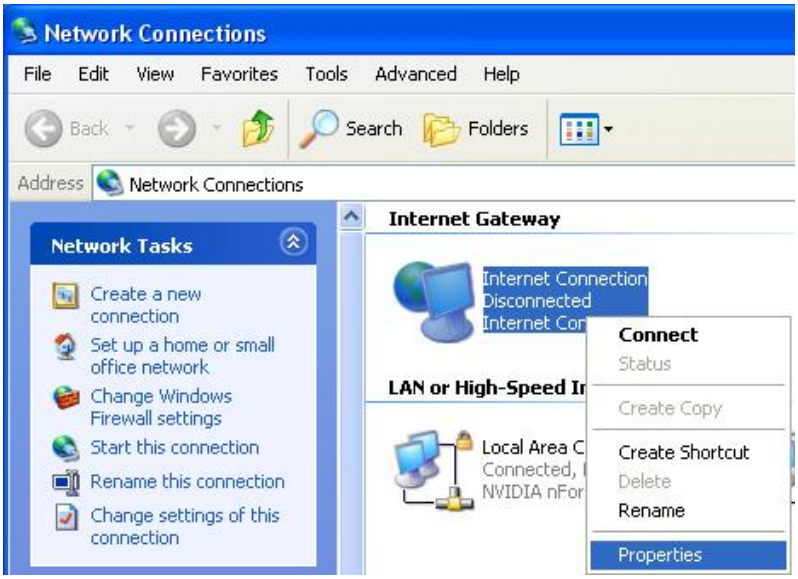


Step 5: In the Networking Services window, select the Universal Plug and Play check box.
Step 6: Click **OK** to go back to the Windows Optional Networking Component Wizard window and click **Next**.

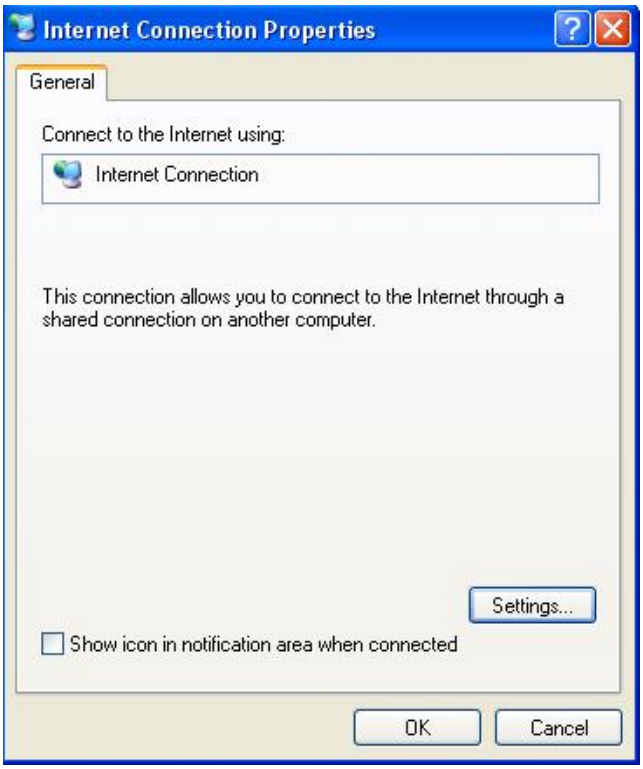


Auto-discover Your UPnP-enabled Network Device

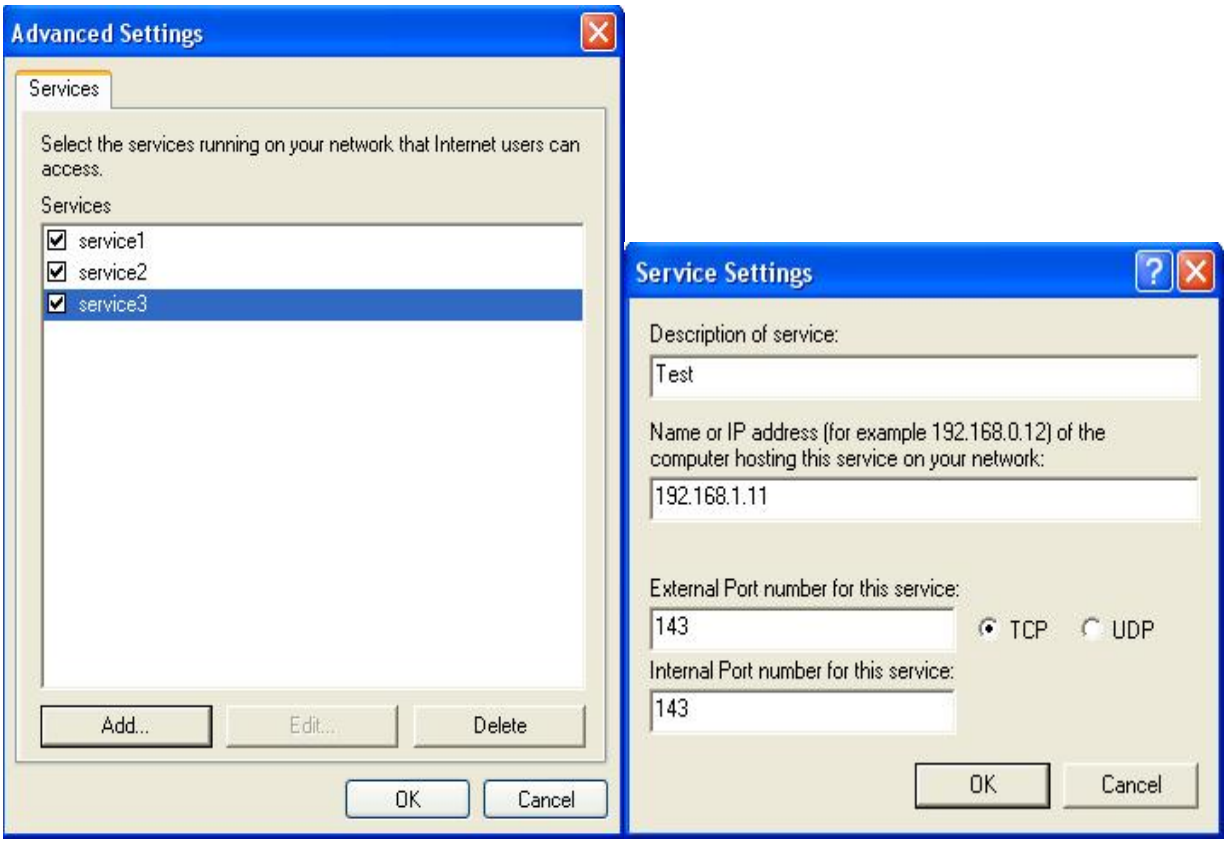
Step 1: Click start and Control Panel. Double-click Network Connections. An icon displays under Internet Gateway.
Step 2: Right-click the icon and select Properties.



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

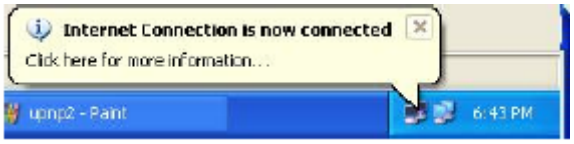


Step 4: You may edit or delete the port mappings or click Add to manually add port mappings.

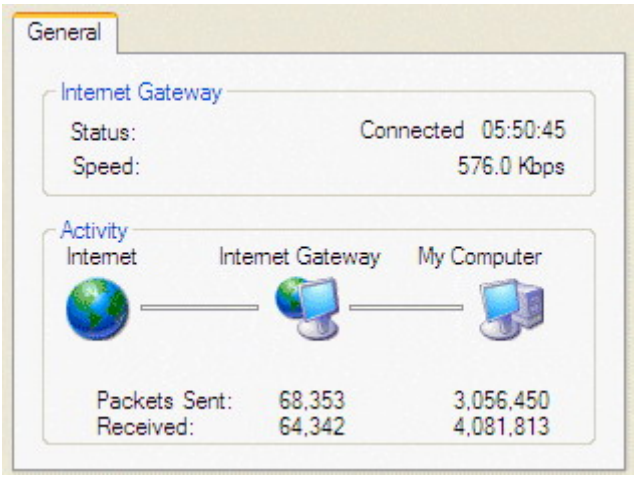


Step 5: Select Show icon in notification area when connected option and click OK. An icon displays

in the system tray



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



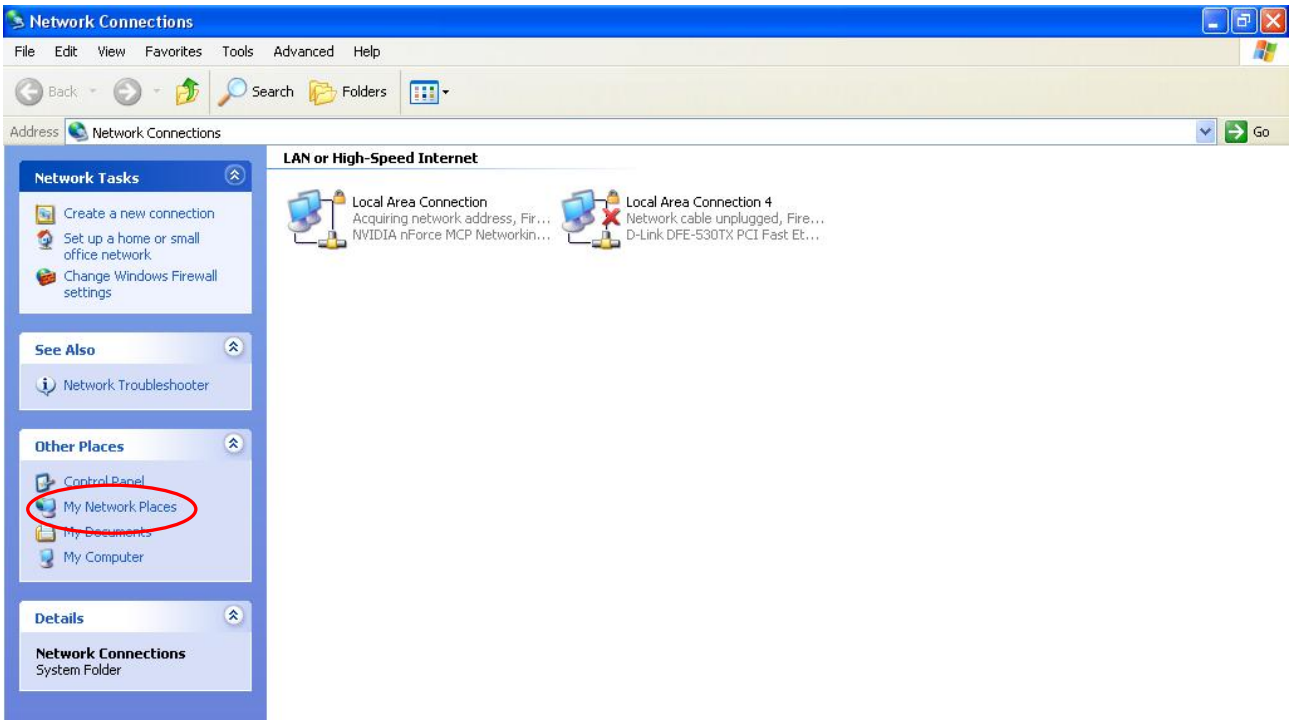
Web Configurator Easy Access

With UPnP, you can access web-based configuration for the BiPAC 7800NL without first finding out the IP address of the router. This helps if you do not know the router's IP address.
Follow the steps below to access web configuration.

Step 1: Click Start and then Control Panel.

Step 2: Double-click Network Connections.

Step 3: Select My Network Places under Other Places.



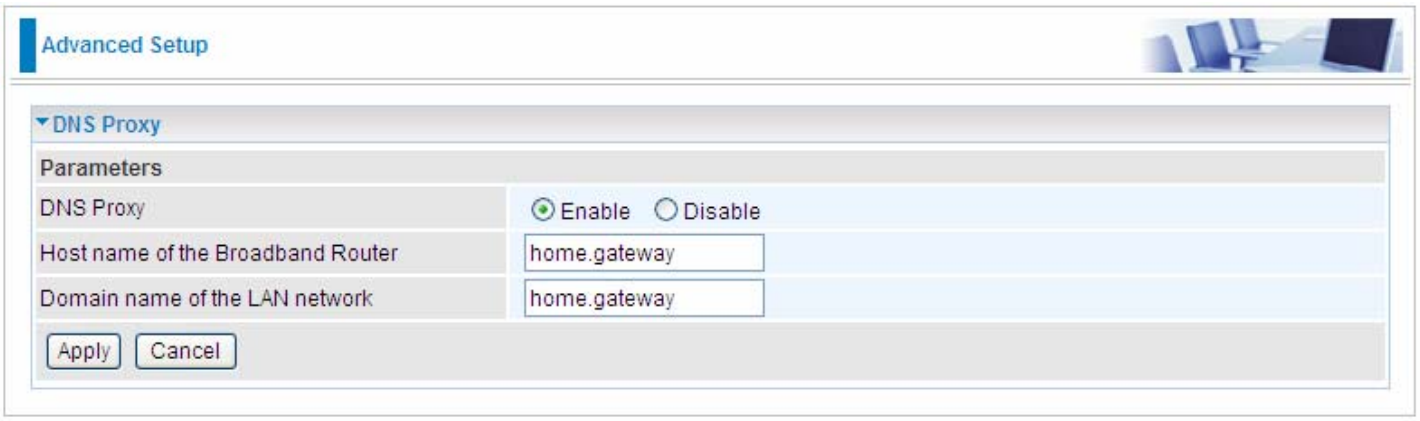
Step 4: An icon describing each UPnP-enabled device shows under Local Network.

Step 5: Right-click on the icon of your BiPAC 7800NL and select Invoke. The web configuration login screen displays.

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

DNS Proxy

DNS proxy is used to forward request and response message between DNS Client and DNS Server. Hosts in LAN can use router serving as a DNS proxy to connect to the DNS Server in public to correctly resolve Domain name to access the internet.



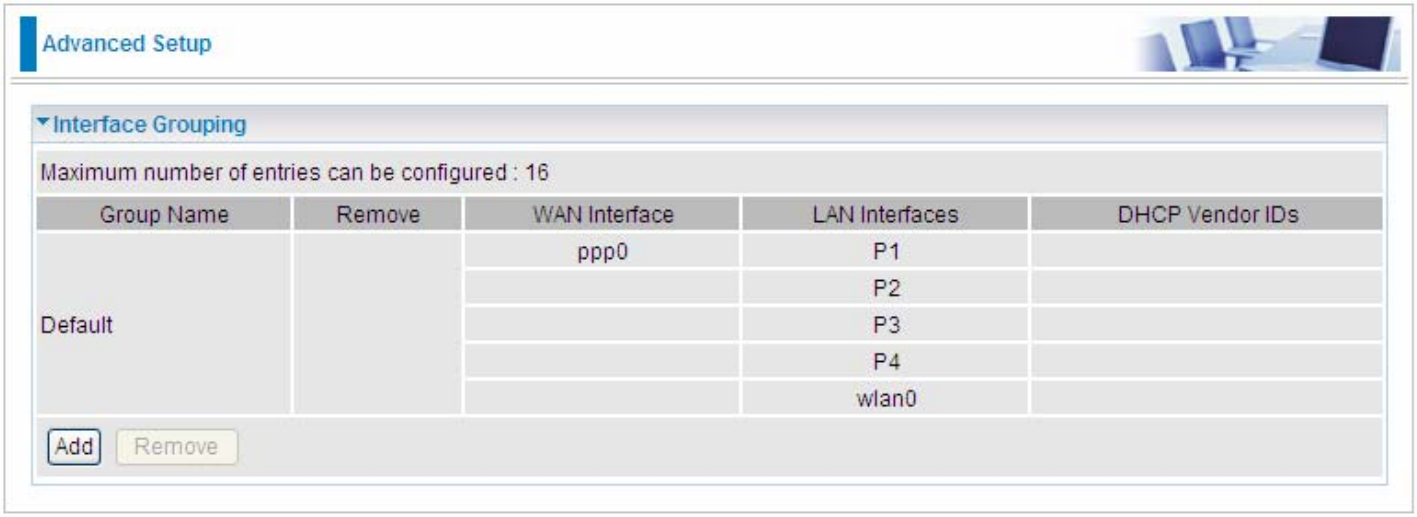
DNS Proxy: select whether to enable or disable DNS Proxy function, default is enabled.

Host name of the Broadband Router: enter the host name of the router. Default is home.gateway.

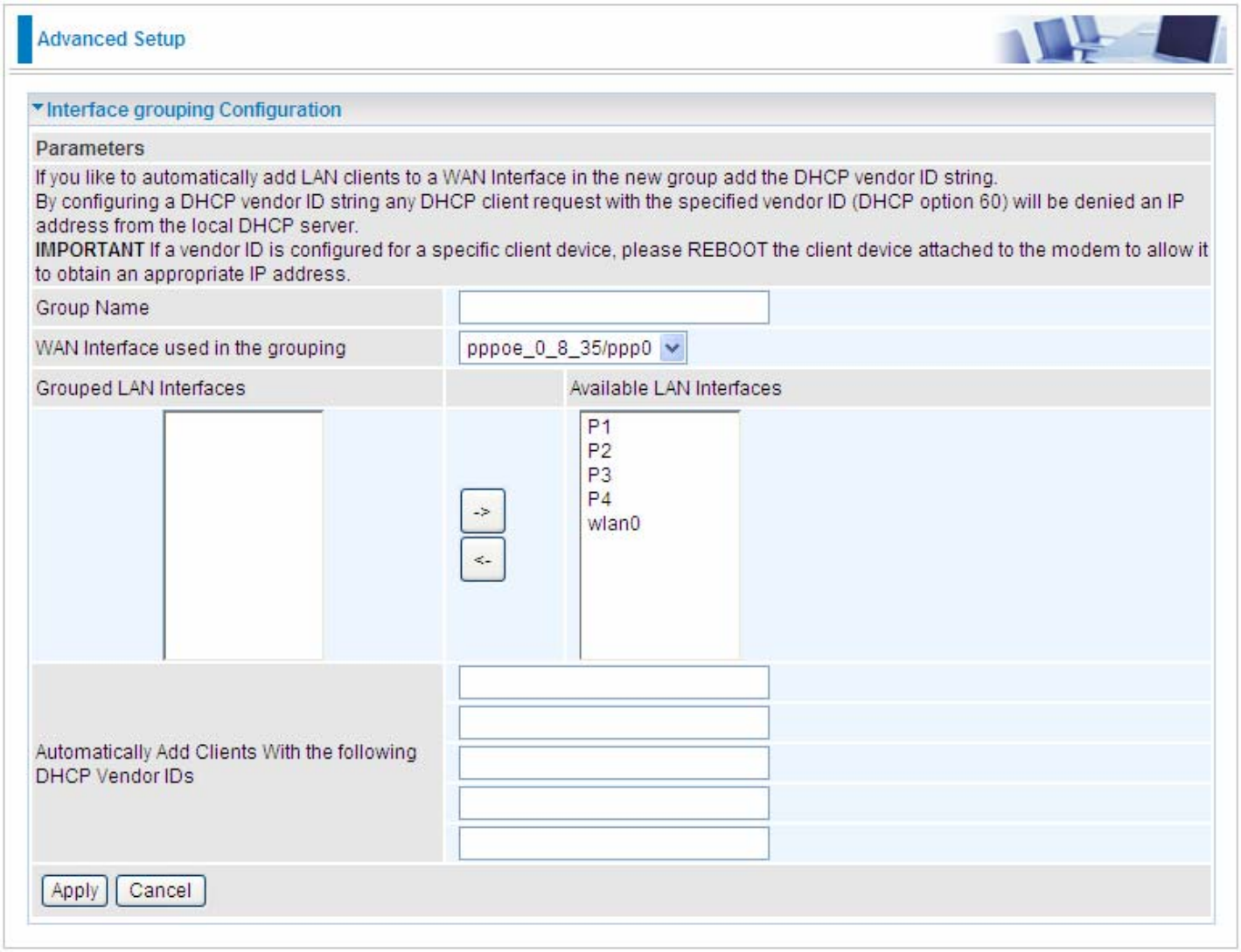
Domain name of the LAN network: enter the domain name of the LAN network. home.gateway.

Interface Grouping

Interface grouping is a function to group interfaces, known as VLAN. 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.



Click **Add** to add groups. But note that the maximum number can be 16.



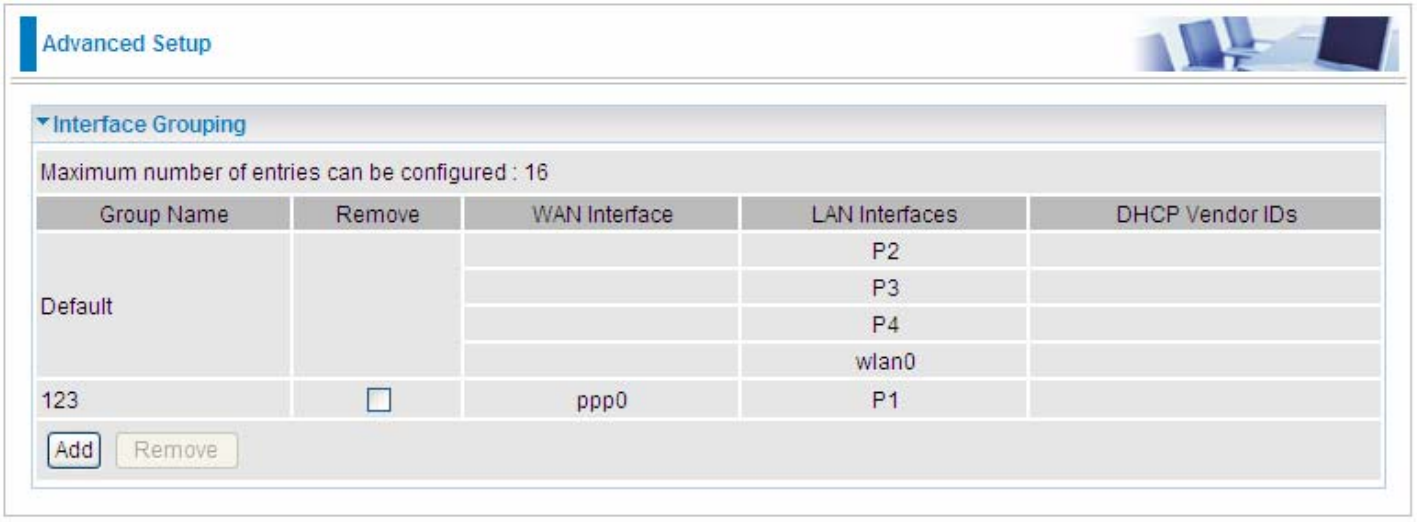
Group Name: type a group name.

WAN interface used in the grouping: select from the drop-down box the WAN interface you want to applied in the group.

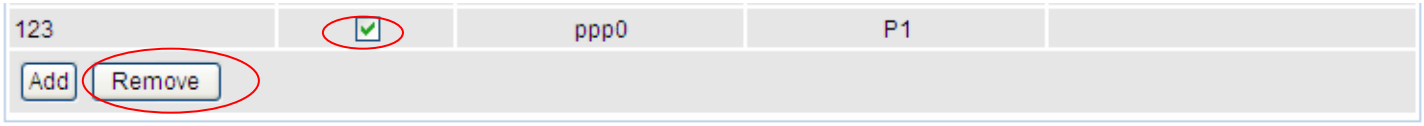
Grouped LAN Interfaces: select the LAN interfaces you want to group as a single group from **Available LAN Interfaces**.

Automatically Add Clients With following DHCP Vendor IDs: enter the DHCP Vendor IDs for which you want the Clients automatically added into the group. DHCP vendor ID (DHCP 60) is an Authentication for DHCP Messages.

Click **Apply** to confirm your settings and your added group will be listed in the Interface Grouping table below.



If you want to remove the group, check the box as the following and press **Remove**.



Note: If you like to automatically add LAN clients to a WAN Interface in the new group add the DHCP vendor ID string.

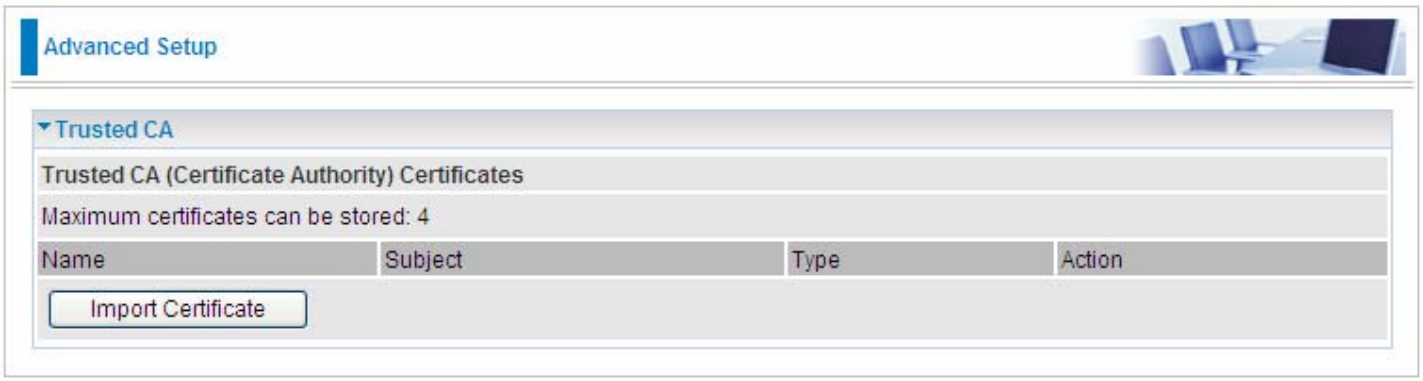
By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.

If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address.

Each LAN interface can only be added into one group and one WAN interface can only be used in one group.

Certificate

This feature is used for TR069 ACS Server authentication of the device used certificate, if necessary. If the imported certificate doesn't match the authorized certificate of the ACS Server, the device will have no access to the server.



Certificate Name: the certificate identification name.

Subject: the certificate subject.

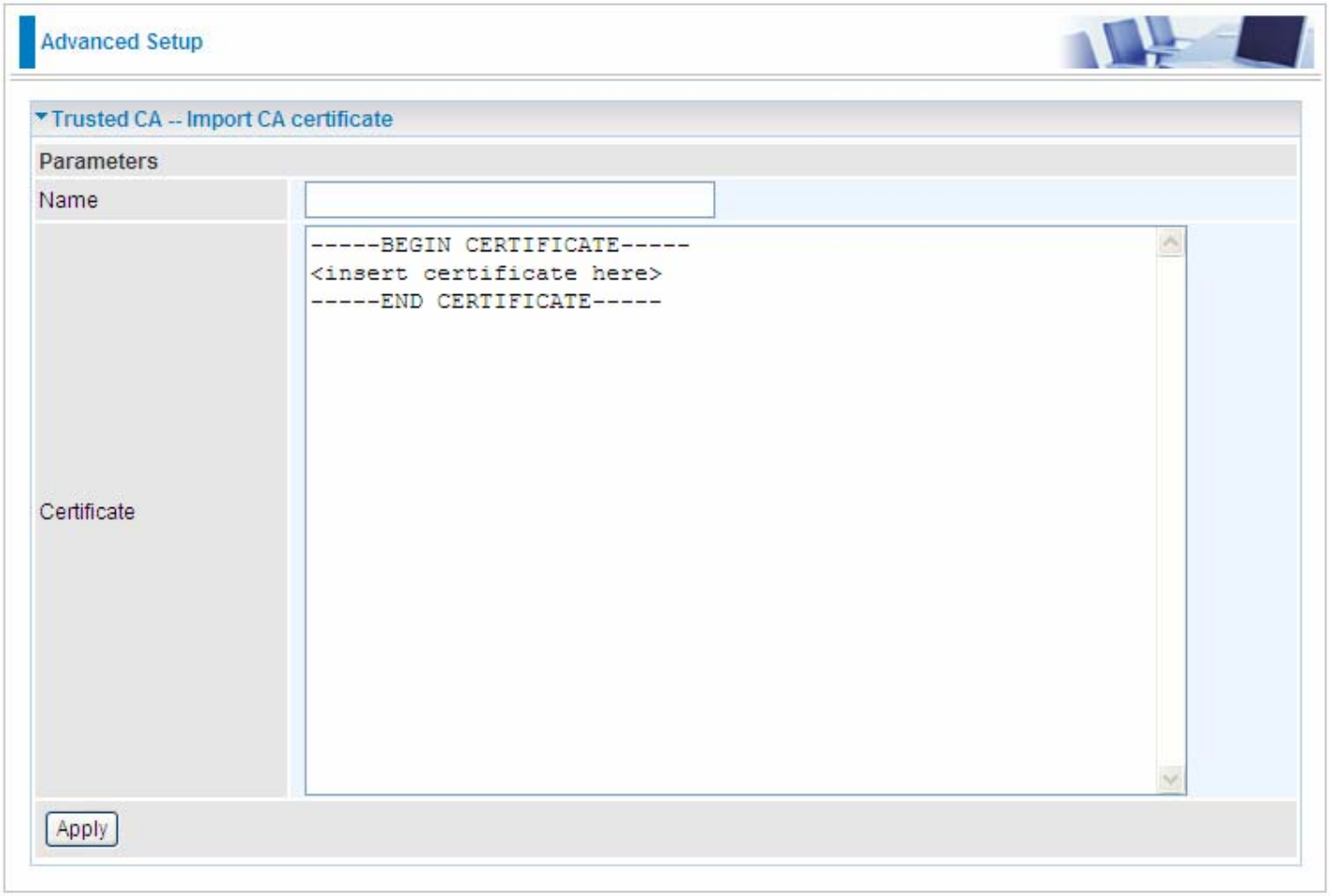
Type: the certificate type information. "ca", indicates that the certificate is a CA-signed certificate. "self", indicates that the certificate is a certificate owner signed one.

"x.509", indicates the certificate is the one created and signed according to the definition of Public-Key System suggested by x.509.

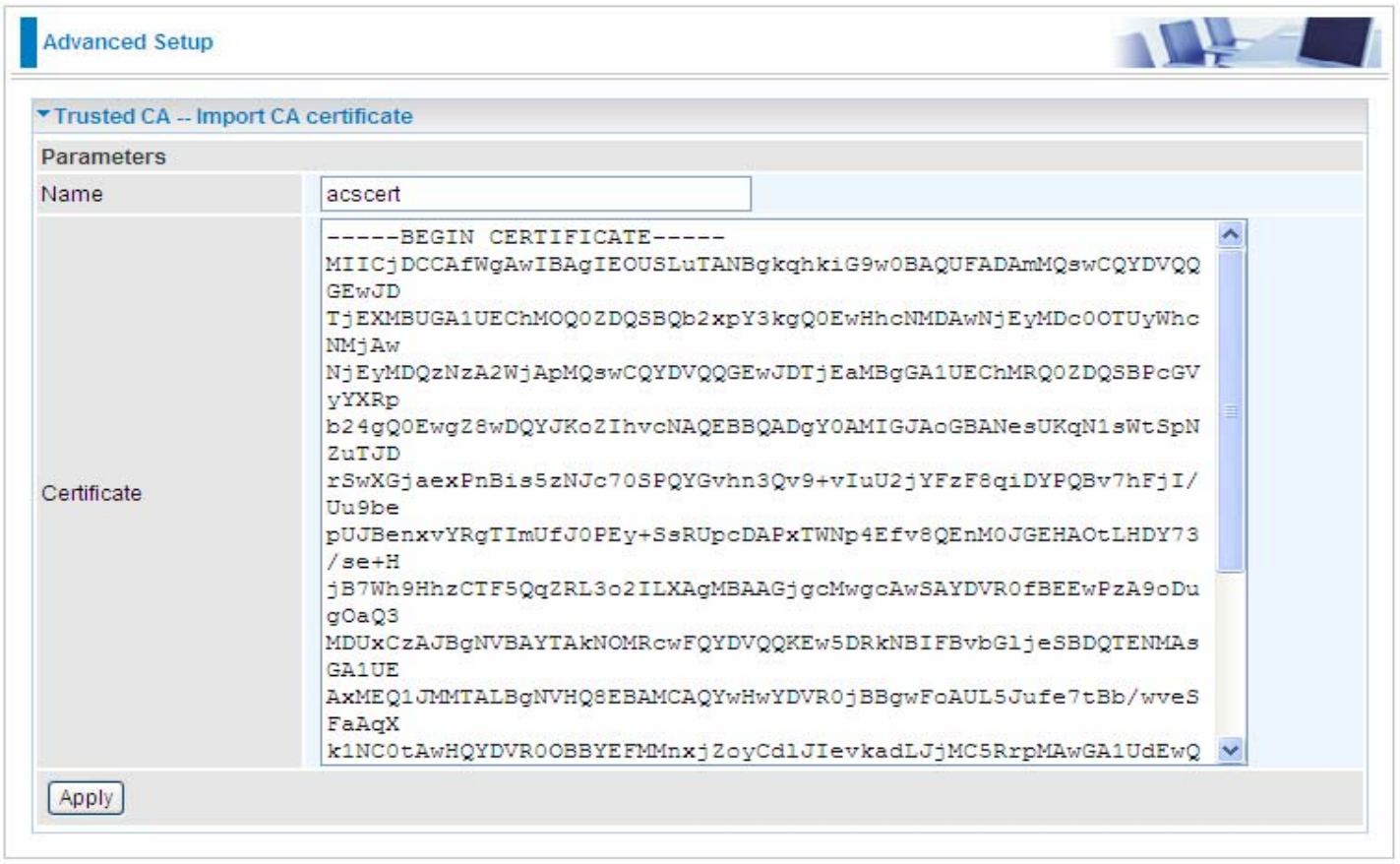
Action:

- View: view the certificate.
- Remove: remove the certificate.

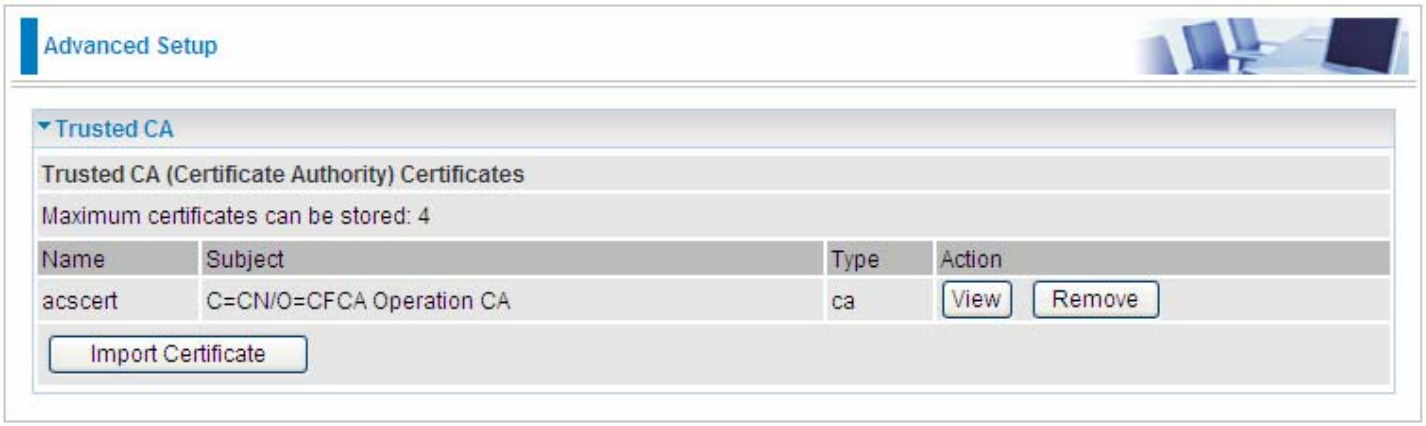
Click **Import Certificate** button to import your certificate.



Enter the certificate name and insert the certificate.



Click Apply to confirm your settings.

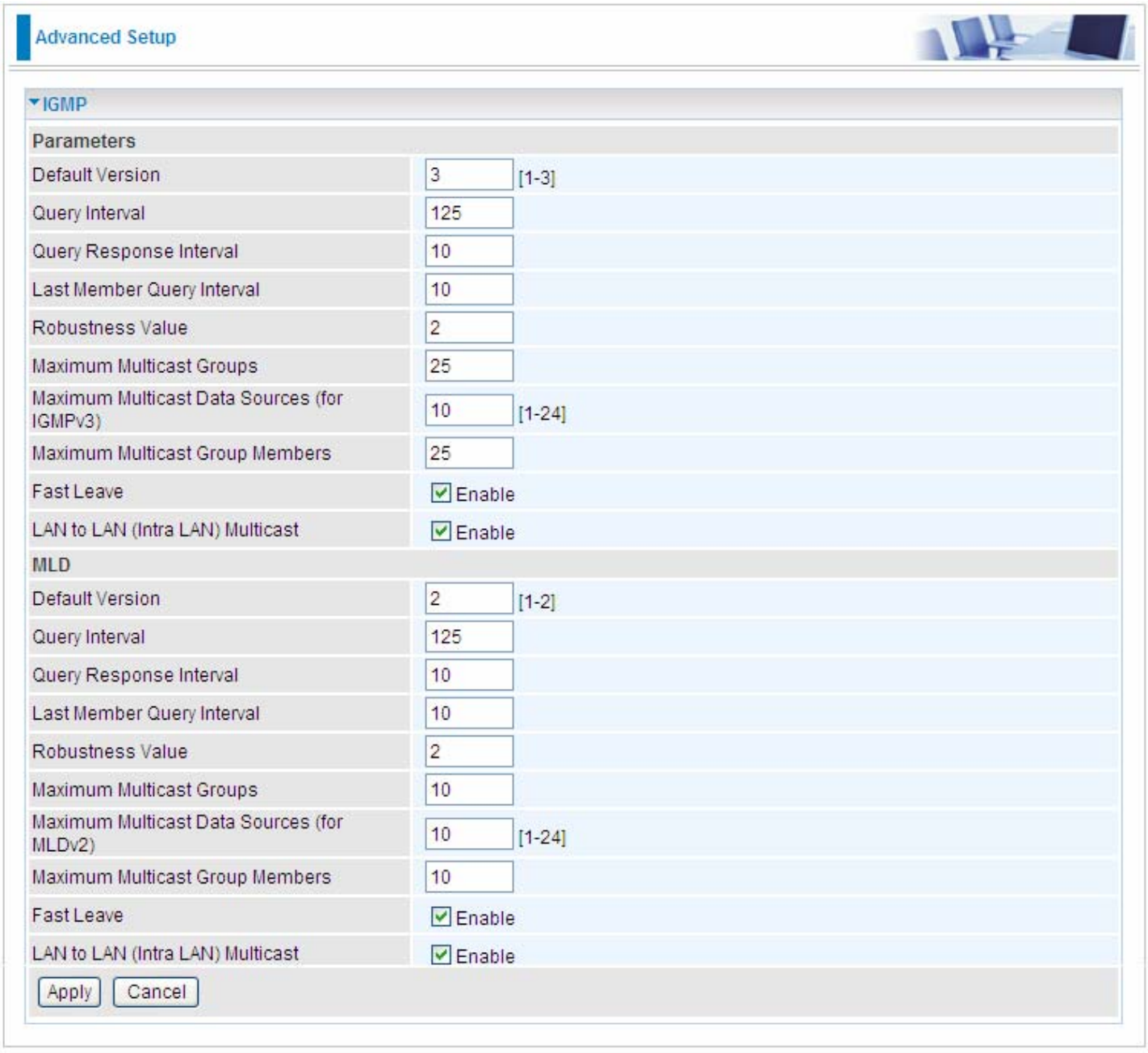


Multicast

Multicast is one of the three network transmission modes, Unicast, Multicast, Broadcast. It is a transmission mode that supports point-to-multipoint connections between the sender and the recipient. IGMP protocol is used to establish and maintain the relationship between IP host and the host directly connected multicast router.

IGMP stands for **Internet Group Management Protocol** is a communications protocols used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and the adjacent multicast routers to establish multicast group members. There are three versions for IGMP, that is IGMPv1, IGMPv2 and IGMPv3.

MLD, short for **Multicast Listener Discovery** protocol, is a component if the Internet Protocol version 6(IPv6) suite. MLD is used by IPv6 to discover multicast listeners on a directly attached link, much as IGMP used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol. MLDv1 is similar to IGMPv2 and MLDv2 is similar to IGMPv3.



IGMP

Default Version: enter the supported IGMP version, 1-3, default is IGMP v3.

Query Interval: enter the periodic query interval time (sec) the multicast router sending the query message to hosts to understand the group membership information.

Query Response Interval: enter the response interval time (sec).

Last Member Query Interval: enter the interval time (sec) the multicast router query the specified group after it has received leave message.

Robustness Value: enter the router robustness parameter, 2-7, the greater the robustness value, the more robust the Querier is.

Maximum Multicast Groups: enter the Maximum Multicast Groups.

Maximum Multicast Data Sources(for IGMP v3): enter the Maximum Multicast Data Sources,1-24.

Maximum Multicast Group Members: enter the Maximum Multicast Group Members.

Fast leave: check to determine whether to support fast leave. If this value is enabled, IGMP proxy removes the membership of a group member immediately without sending an IGMP membership query on downstream. This is very helpful if user wants fast channel (group change) changing in cases like IPTV environment.

LAN to LAN (Intra LAN) Multicast: check to determine whether to support LAN to LAN (Intra LAN) Multicast. If user want to have a multicast data source on LAN side and he want to get IGMP snooping enabled, then this LAN-to-LAN multicast feature should be enabled.

MLD

Default Version: enter the supported MLD version, 1-2, default is MLDv2.

Query Interval: enter the periodic query interval time (sec) the multicast router sending the query message to hosts to understand the group membership information.

Query Response Interval: enter the response interval time (sec).

Last Member Query Interval: enter the interval time (sec) the multicast router query the specified group after it has received leave message.

Robustness Value: enter the router robustness parameter, default is 2, the greater the robustness value, the more robust the Querier is.

Maximum Multicast Groups: enter the Maximum Multicast Groups.

Maximum Multicast Data Sources(for MLDv2): enter the Maximum Multicast Data Sources,1-24.

Maximum Multicast Group Members: enter the Maximum Multicast Group Members.

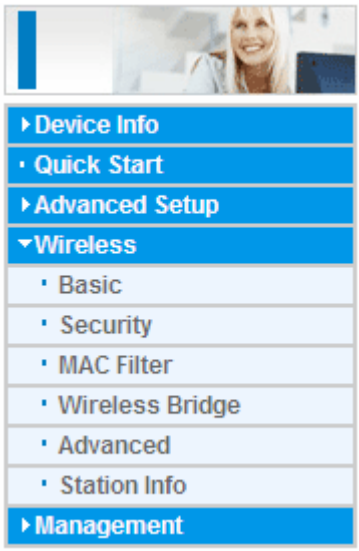
Fast leave: check to determine whether to support fast leave. If this value is enabled, MLD proxy removes the membership of a group member immediately without sending an MLD membership query on downstream. This is very helpful if user wants fast channel (group change) changing in cases like IPTV environment.

LAN to LAN (Intra LAN) Multicast: check to determine whether to support LAN to LAN (Intra LAN) Multicast. If user want to have a multicast data source on LAN side and he want to get MLD snooping enabled, then this LAN-to-LAN multicast feature should be enabled.

Wireless

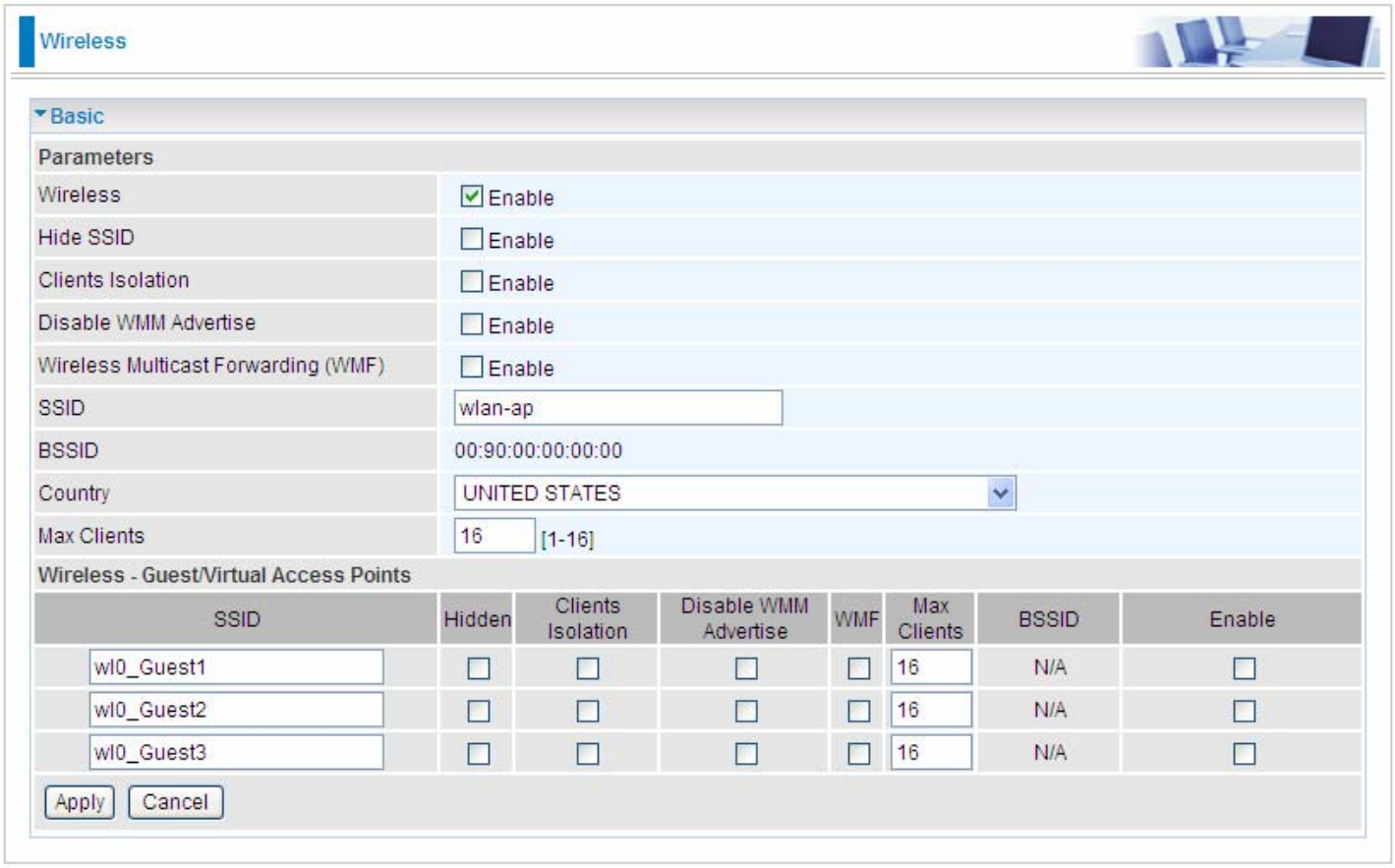
This section provides you ways to configure wireless access. When you click this item, the column will expand to display the sub-items that will lead you to configure your router.

Basic, **Secturity**, **MAC Filter**, **Wireless Bridge**, **Advanced** and **Station Info** are included here.



Basic

It let you determine whether to enable Wireless function and set the basic parameters of an AP and the Virtual APs.



Wireless: Default setting is set to Enable. If you do not have any wireless devices, check the checkbox again to unselect.

Hide SSID: It is function in which transmits its SSID to the air so that when wireless client searches for a network, router can then be discovered and recognized. Check the checkbox to determine whether you want to hide SSID.

Clients Isolation: if you enabled this function, then each of your wireless clients will not be communicate with each other.

Disable WMM Advertise: Stop the router from 'advertising' its Wireless Multimedia (WMM) functionality, which provides basic quality of service for time-sensitive applications (e.g. VoIP, Video).

Check to disable or enable this function.

Wireless multicast Forwarding (WMF): check to enable or disable wireless multicast forwarding.

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

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

BSSID: Basic Set Service Identifier, it is a local managed IEEE MAC address, and is 48 bits value.

Country: Different countries have different wireless band resources, so you can select the appropriate Country according to the area where you want to device used.

Max Clients: enter the number of max clients the wireless network can supports,1-16.

Max-Guest/virtual Access points: A "Virtual Access Point" is a logical entity that exists within a

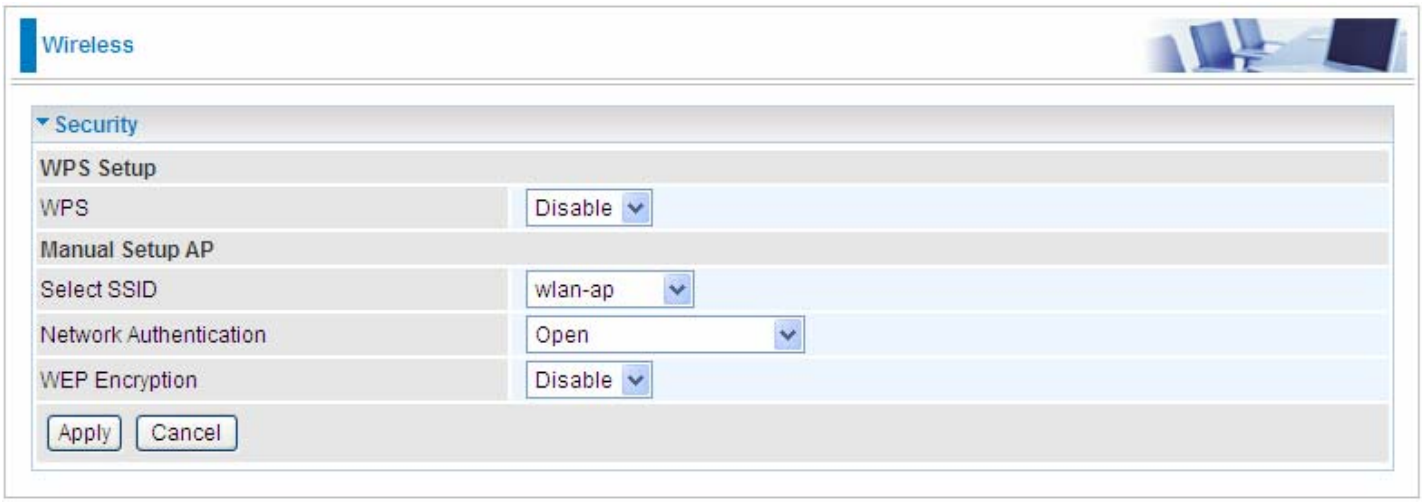
physical Access Point (AP). When a single physical AP supports multiple “Virtual APs”, each Virtual AP appears to stations (STAs) to be an independent physical AP, even though only a single physical AP is present. For example, multiple Virtual APs might exist within a single physical AP, each advertising 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.

Here you can enable some Virtual APs according to the request. And the other parameters of virtual APs are the same to the above.

Click **Apply** to apply your settings.

Security

Wireless security is the prevention of unauthorized access or damage to computers using wireless network.

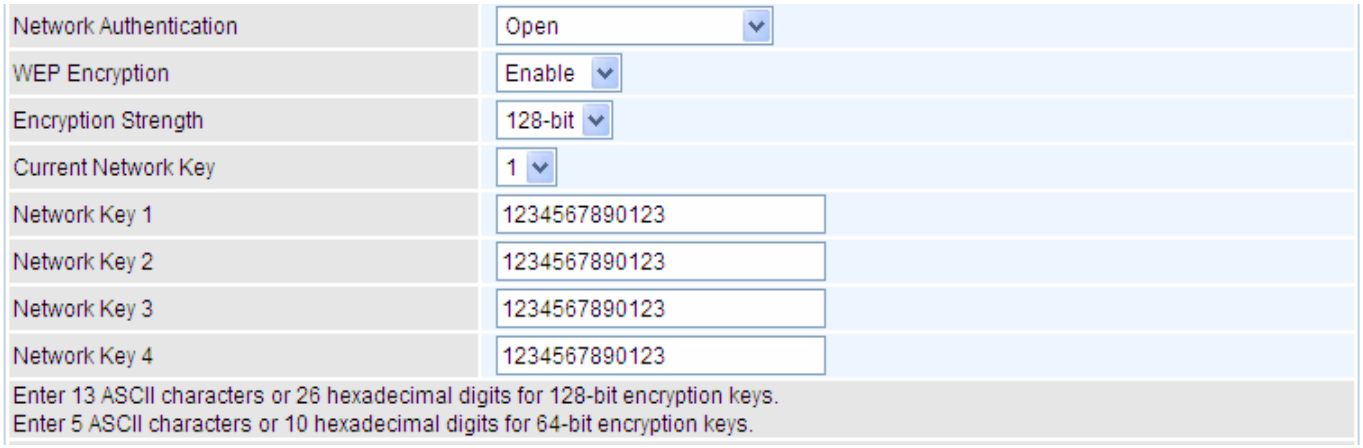


Manual Setup AP

Select SSID: select the SSID you want these settings apply to.

Network Authentication

ⓘ **Open**



WEP Encryption: select to enable or disable WEP Encryption. Here select Enable.

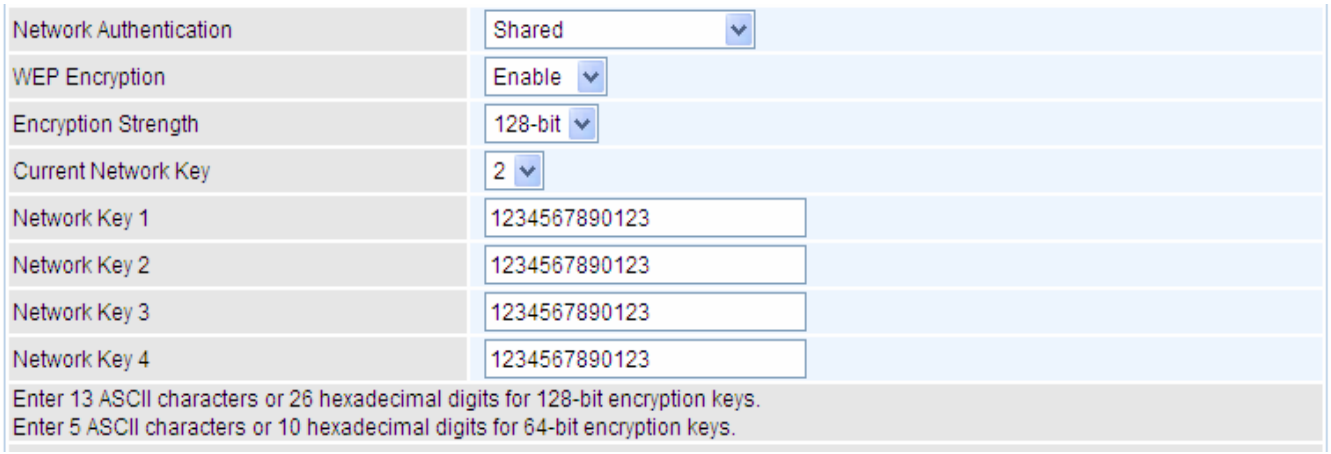
Encryption Strength: select the strength, 128-bit or 64-bit.

Current Network Key: select the one to be the current network key. Please refer to key 1- 4 below.

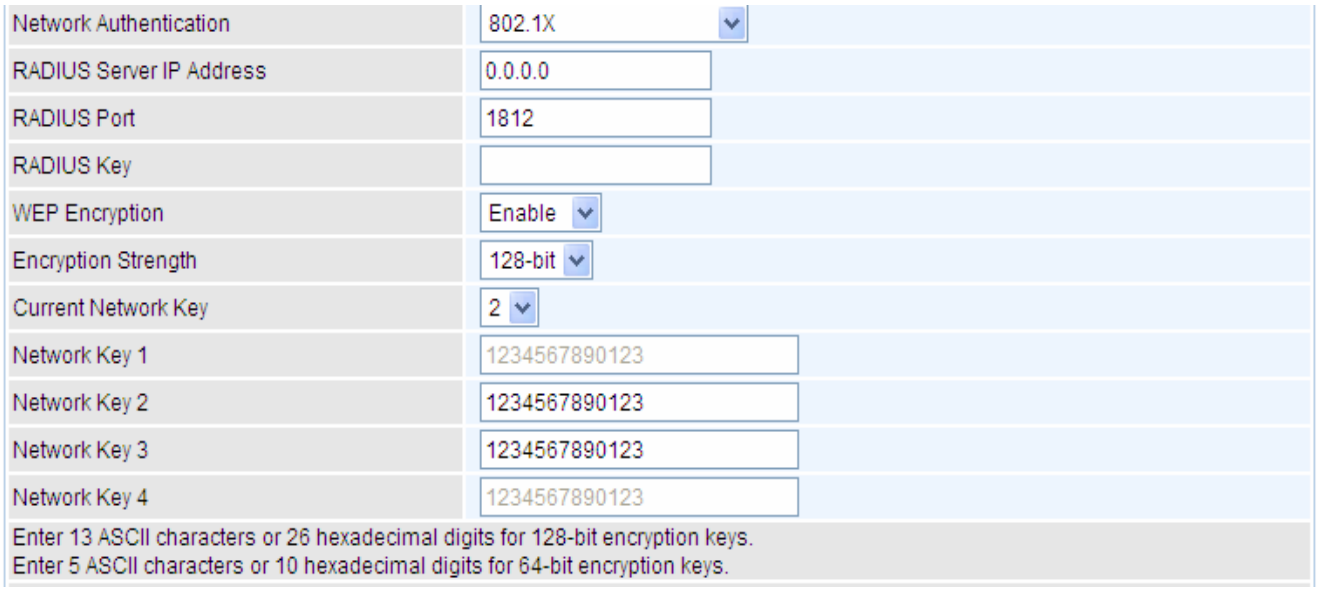
Network Key (1- 4): Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys.Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.

ⓘ Shared

It is similar to network authentication ‘Open’. But here the WEP Encryption must be enabled.



ⓘ 802.1x



RADIUS Server IP Address: RADIUS(Remote Authentication Dial In User Service), Enter the IP address of RADIUS authentication server.

RADIUS Server Port: Enter the port number of RADIUS authentication server here.

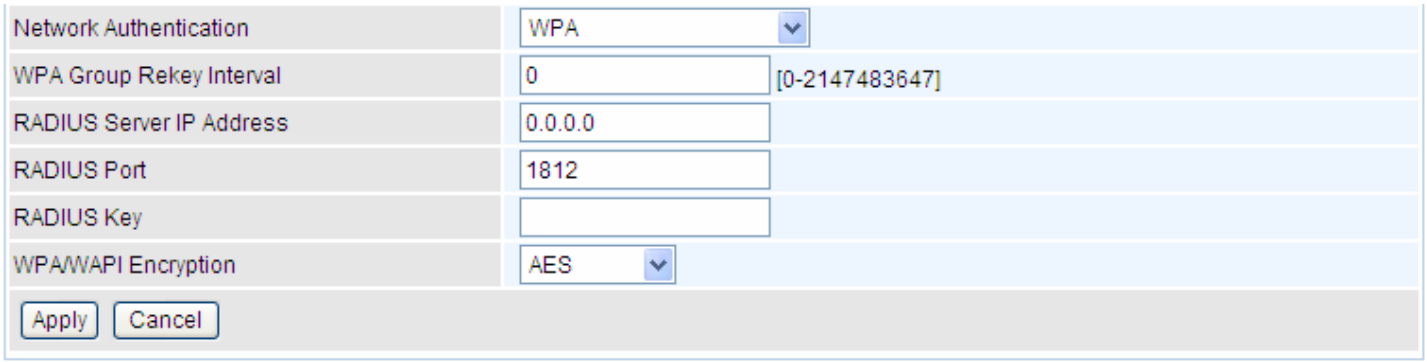
RADIUS Key: Enter the password of RADIUS authentication server.

WEP Encryption: select to enable or disable WEP Encryption. Here select Enable.

Current Network Key: select the one to be the current network key. Please refer to key 2- 3 below.

Network Key (1- 4): Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys.Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.

ⓘ WPA



WPA Group ReKey Internal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). The unit is second.

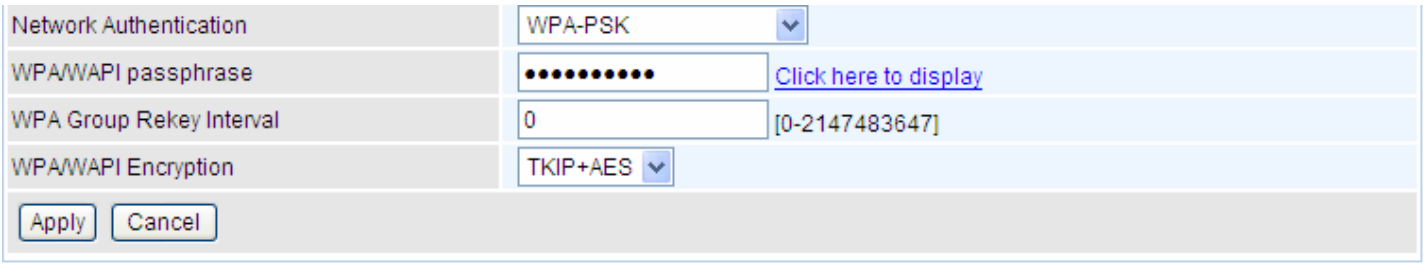
RADIUS Server IP Address: RADIUS(Remote Authentication Dial In User Service), Enter the IP address of RADIUS authentication server.

RADIUS Server Port: Enter the port number of RADIUS authentication server here.

RADIUS Key: Enter the password of RADIUS authentication server.

WPA/WAPI Encryption: There are two Algorithms, AES (Advanced Encryption Standard) and TKIP(Temporal Key Integrity Protocol) which help to protect the wireless communication.

ⓘ WPA-PSK / WPA2-PSK

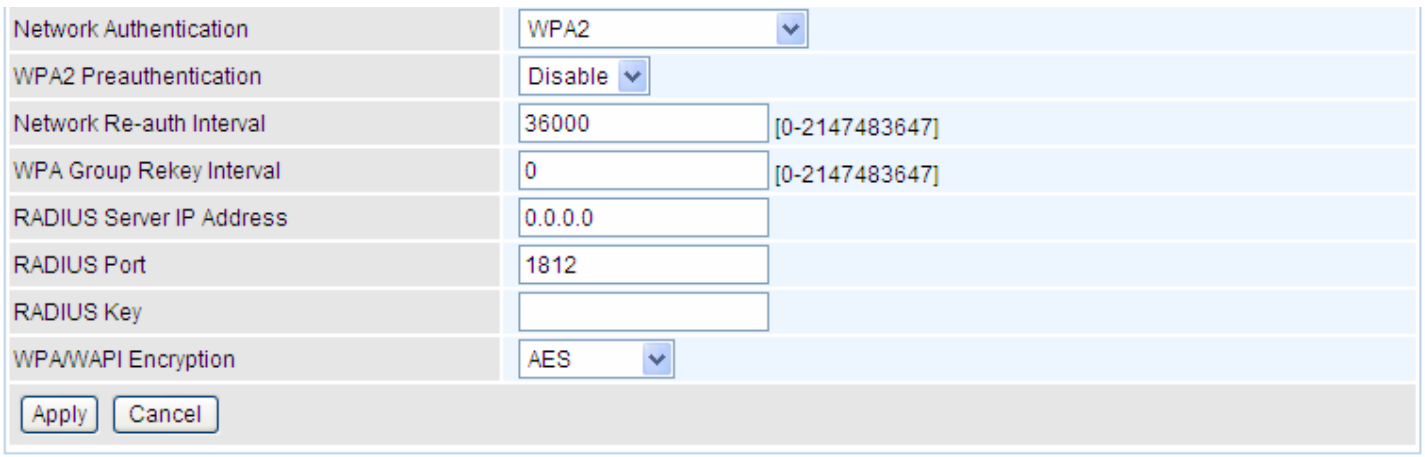


WPA/WAPI passphrase: enter the WPA.WAPI passphrase, you can **click here to display** to view it.

WPA Group ReKey Internal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). The unit is second.

WPA/WAPI Encryption: There are two Algorithms, AES (Advanced Encryption Standard) and TKIP(Temporal Key Integrity Protocol) which help to protect the wireless communication.

ⓘ WPA2



WPA2 Preauthentication: When a wireless client wants to handoff to another AP, with

preauthentication, it can perform 802.1X authentications to the new AP, and when handoff happens, this mode will help reduce the association time used.

Network Re-auth Interval: the interval for network Re-authentication. The unit is second.

WPA Group ReKey Internal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). The unit is second.

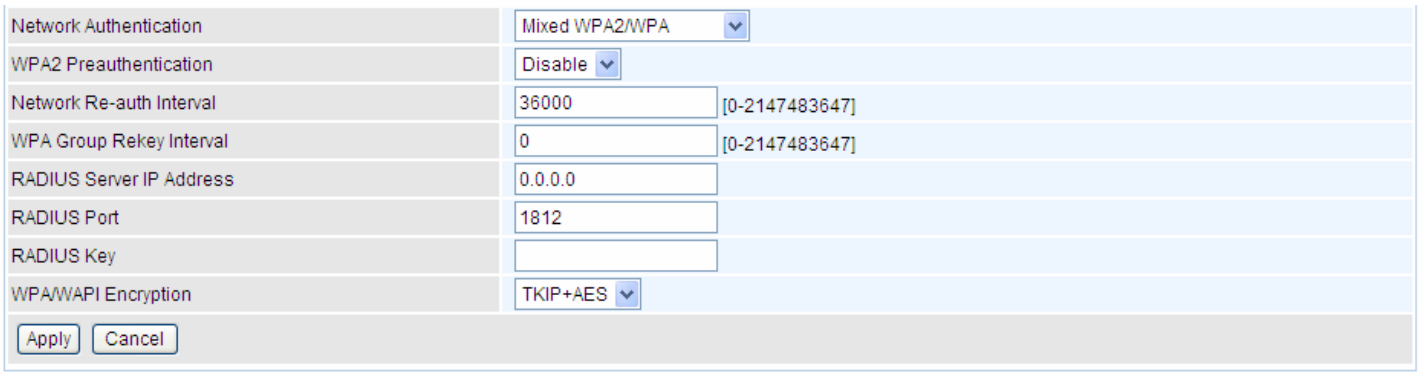
RADIUS Server IP Address: RADIUS(Remote Authentication Dial In User Service), Enter the IP address of RADIUS authentication server. The unit is second.

RADIUS Server Port: Enter the port number of RADIUS authentication server here.

RADIUS Key: Enter the password of RADIUS authentication server.

WPA/WAPI Encryption: There are two Algorithms, AES (Advanced Encryption Standard) and TKIP(Temporal Key Integrity Protocol) which help to protect the wireless communication.

ⓘ Mixed WPA2/WPA



WPA2 Preauthentication: When a wireless client wants to handoff to another AP, with preauthentication, it can perform 802.1X authentications to the new AP, and when handoff happens, this mode will help reduce the association time used.

Network Re-auth Interval: the interval for network Re-authentication. The unit is second.

WPA Group ReKey Internal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). The unit is second.

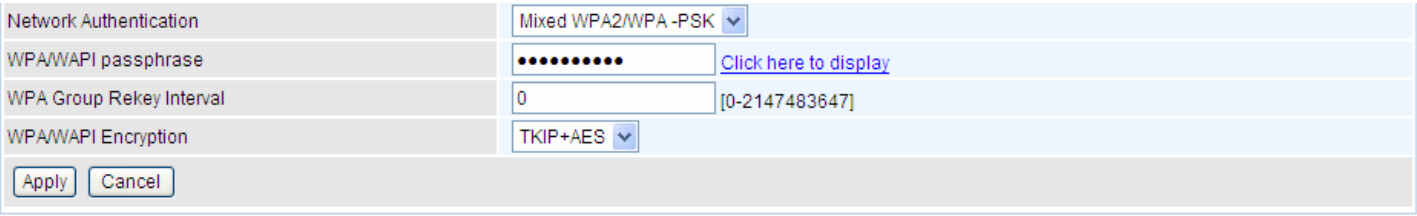
RADIUS Server IP Address: RADIUS(Remote Authentication Dial In User Service), Enter the IP address of RADIUS authentication server.

RADIUS Server Port: Enter the port number of RADIUS authentication server here.

RADIUS Key: Enter the password of RADIUS authentication server.

WPA/WAPI Encryption: There are two Algorithms, AES (Advanced Encryption Standard) and TKIP(Temporal Key Integrity Protocol) which help to protect the wireless communication.

ⓘ Mixed WPA2/WPA-PSk



WPA/WAPI passphrase: enter the WPA.WAPI passphrase, you can **click here to display** to view it.

WPA Group ReKey Internal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). The unit is second.

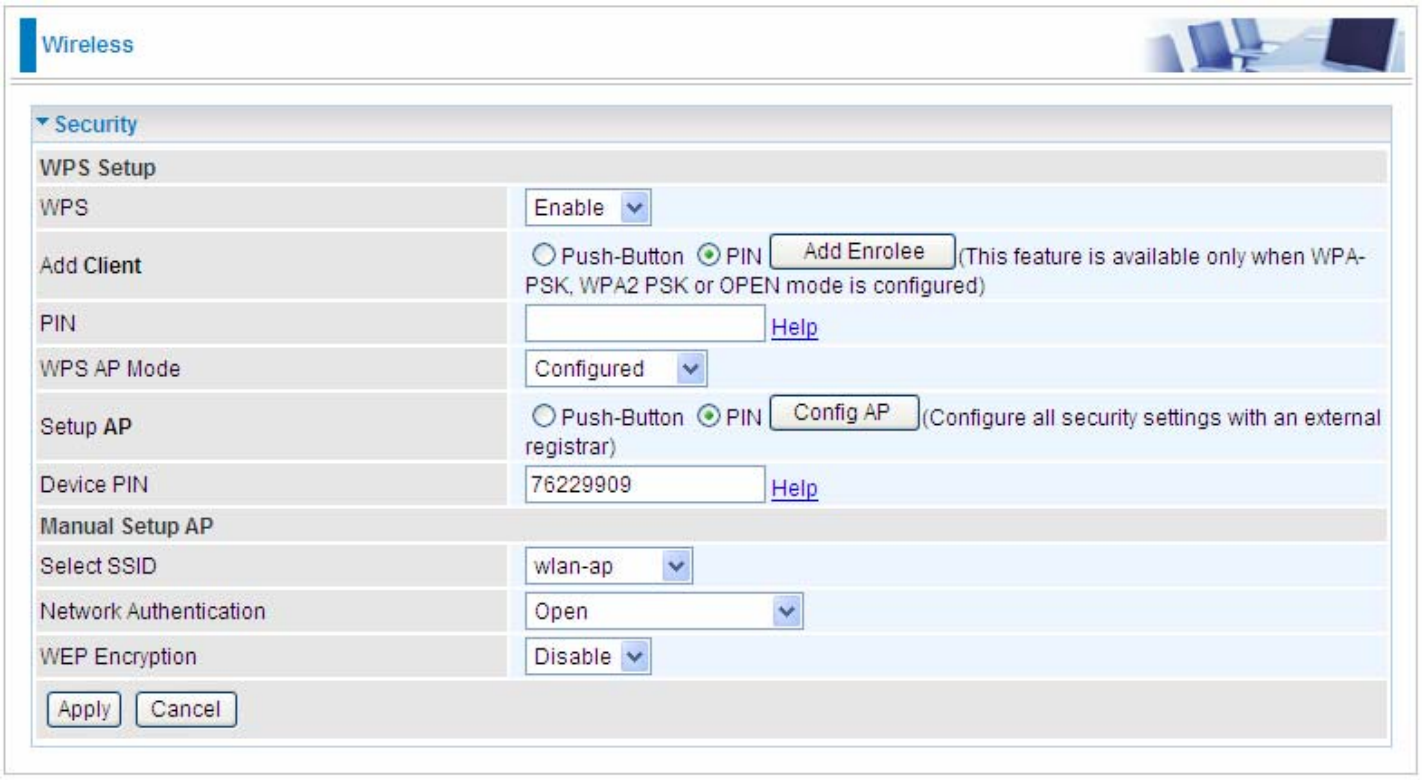
WPA/WAPI Encryption: There are two Algorithms, AES (Advanced Encryption Standard) and TKIP(Temporal Key Integrity Protocol) which help to protect the wireless communication.

WPS Setup

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

WPS: select enable to enable WPS function. As you see, WPS can only be available when WPA-PSK, WPA2 PSK or OPEN mode is configured.

Note: here wireless can be configured as Registrar and Enrolee mode respectively. When AP is configured as Registrar, you should select Configured in the WPS AP Mode below, and default WPS AP Mode is Configured. When AP is configured as Enrolee, the WPS AP Mode below should changed to Unconfigured. Follow the following steps.

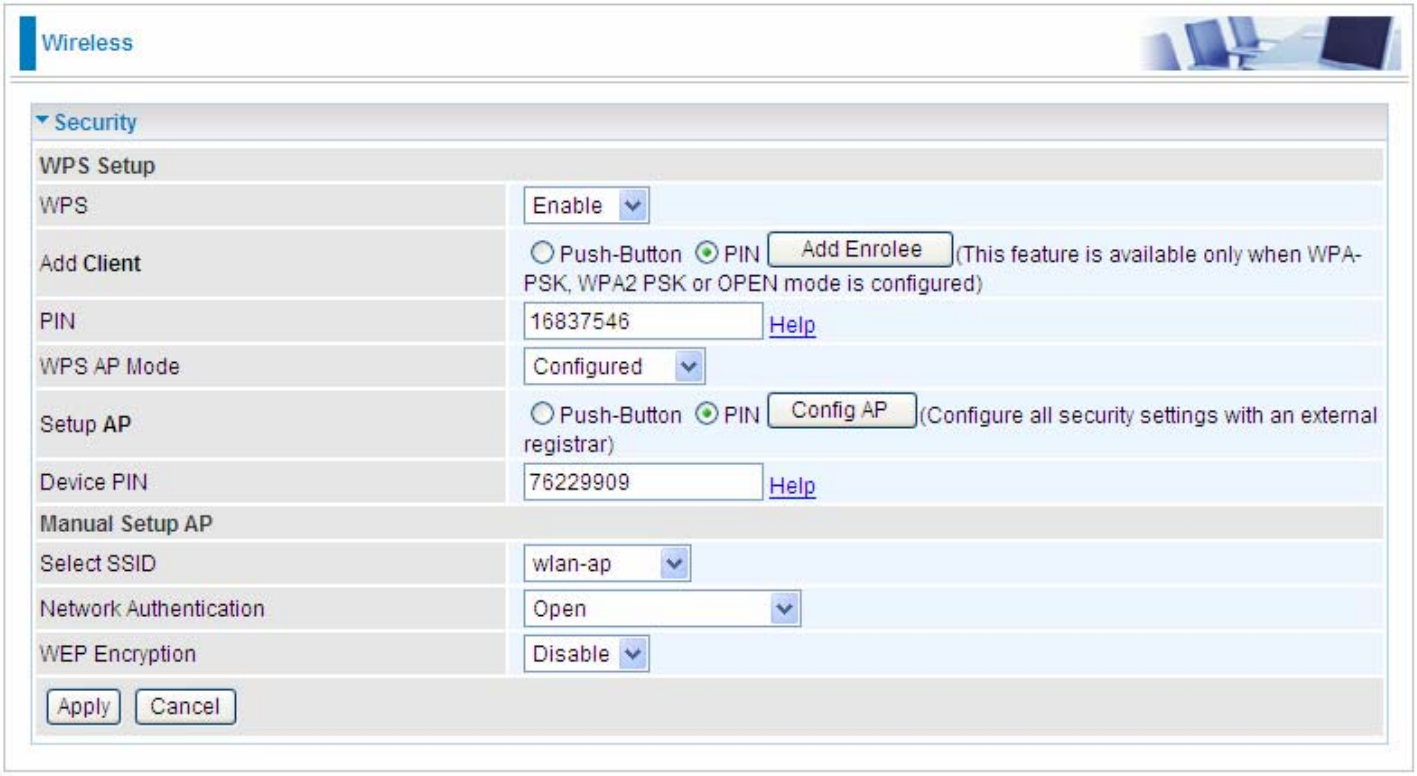


Configure AP as Registrar

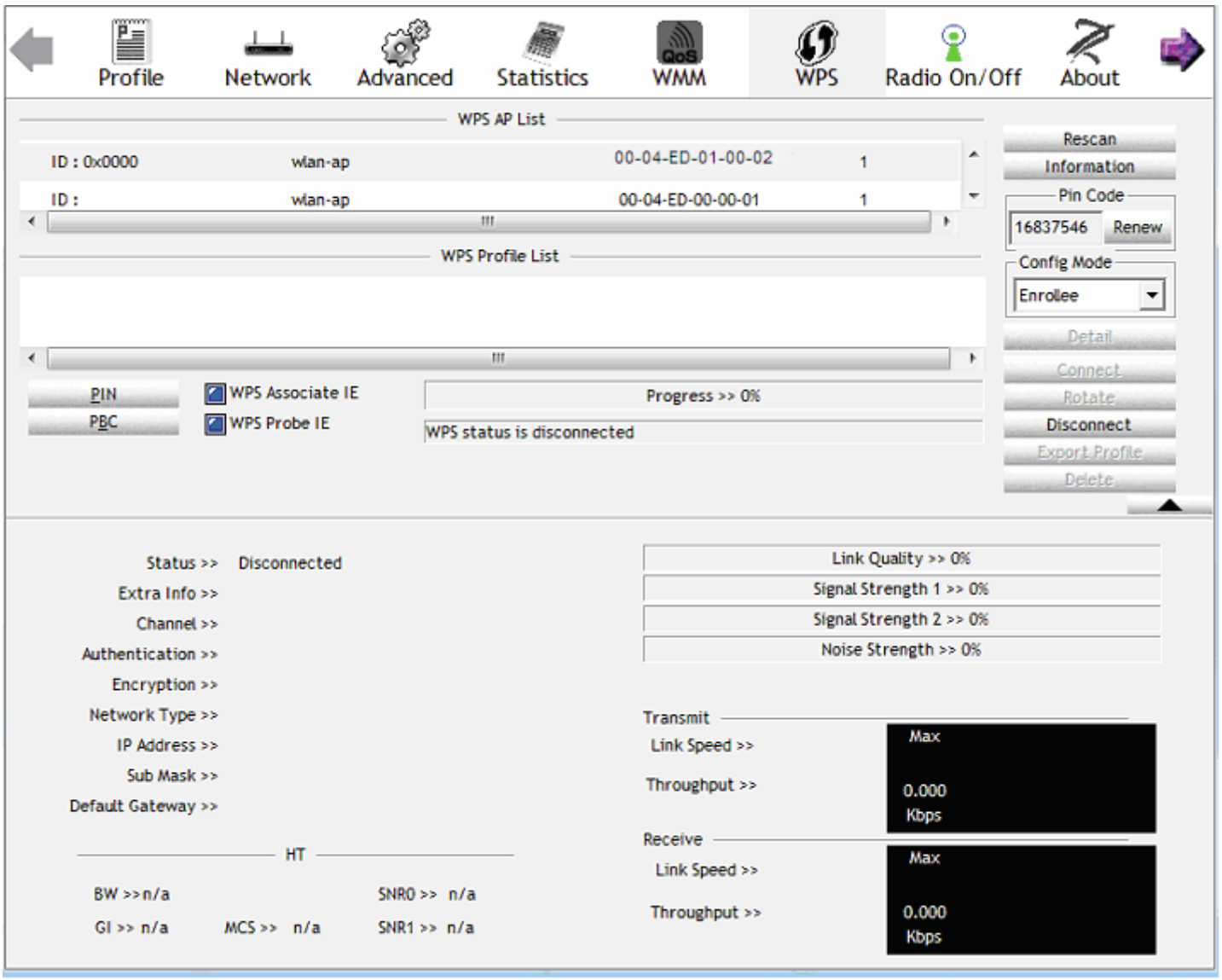
Add Enrollee with PIN method

1. select radio button ‘PIN’.
2. Input PIN from Enrollee Station (16837546 in this example). Help: it is to help users to understand PIN.

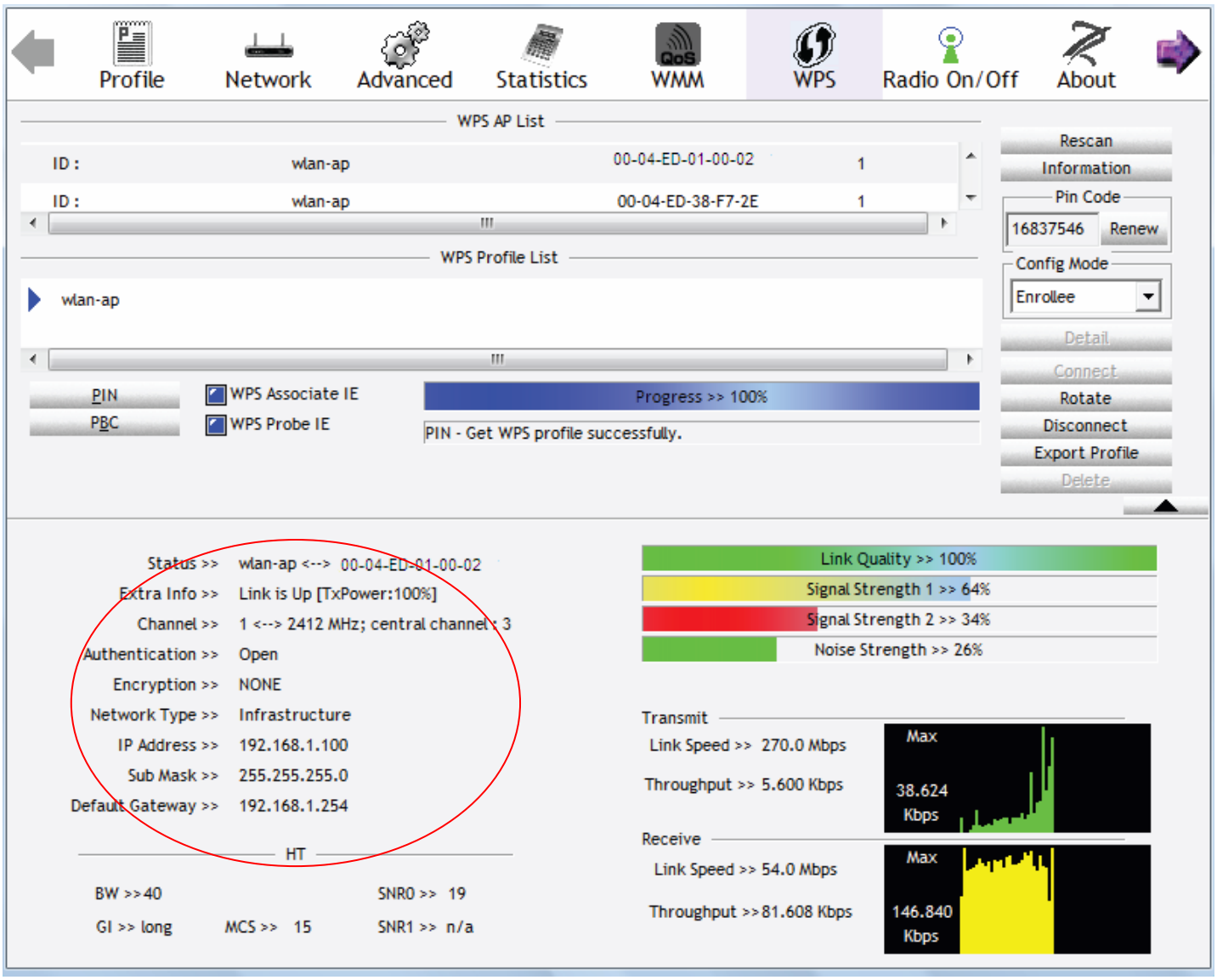
3.Click Add Enrolee.



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



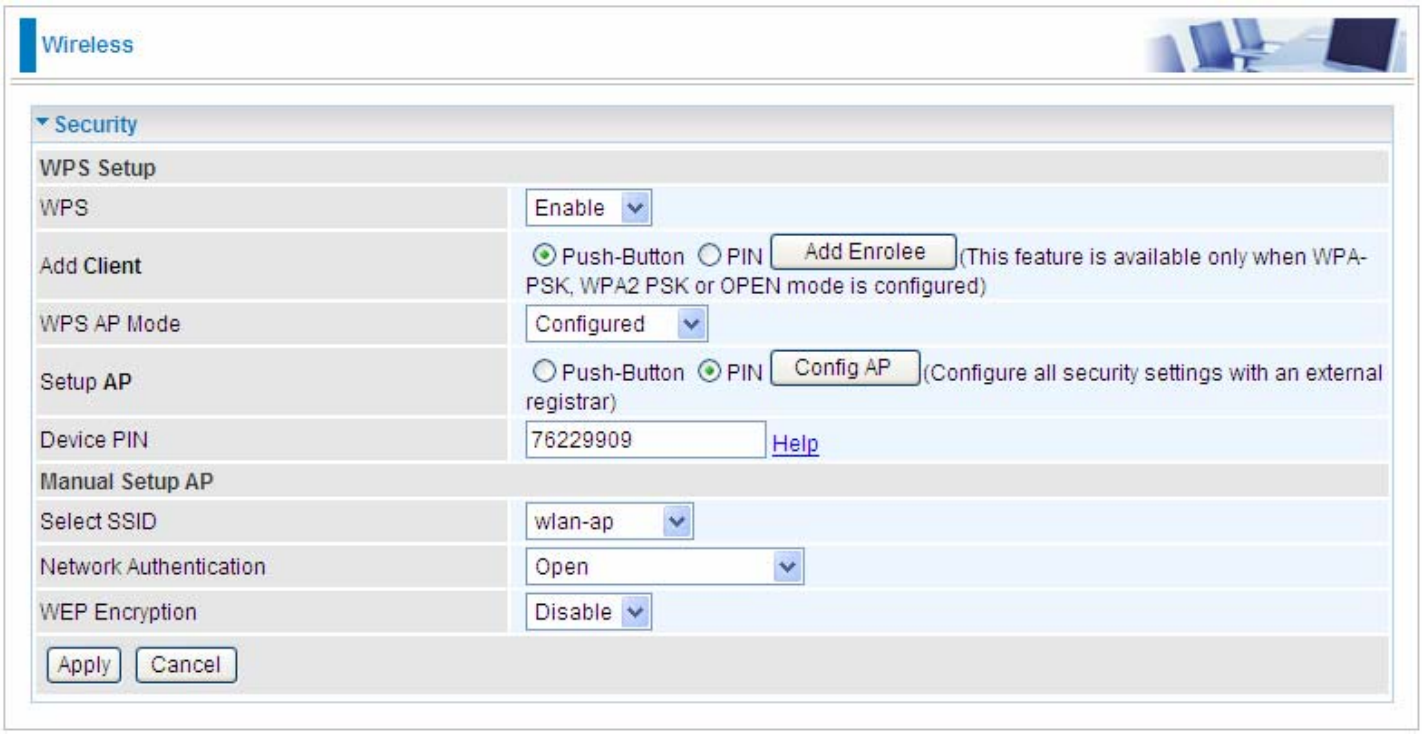
4. The client's SSID and security setting will now be configured to match the SSID and security setting of the registrar.



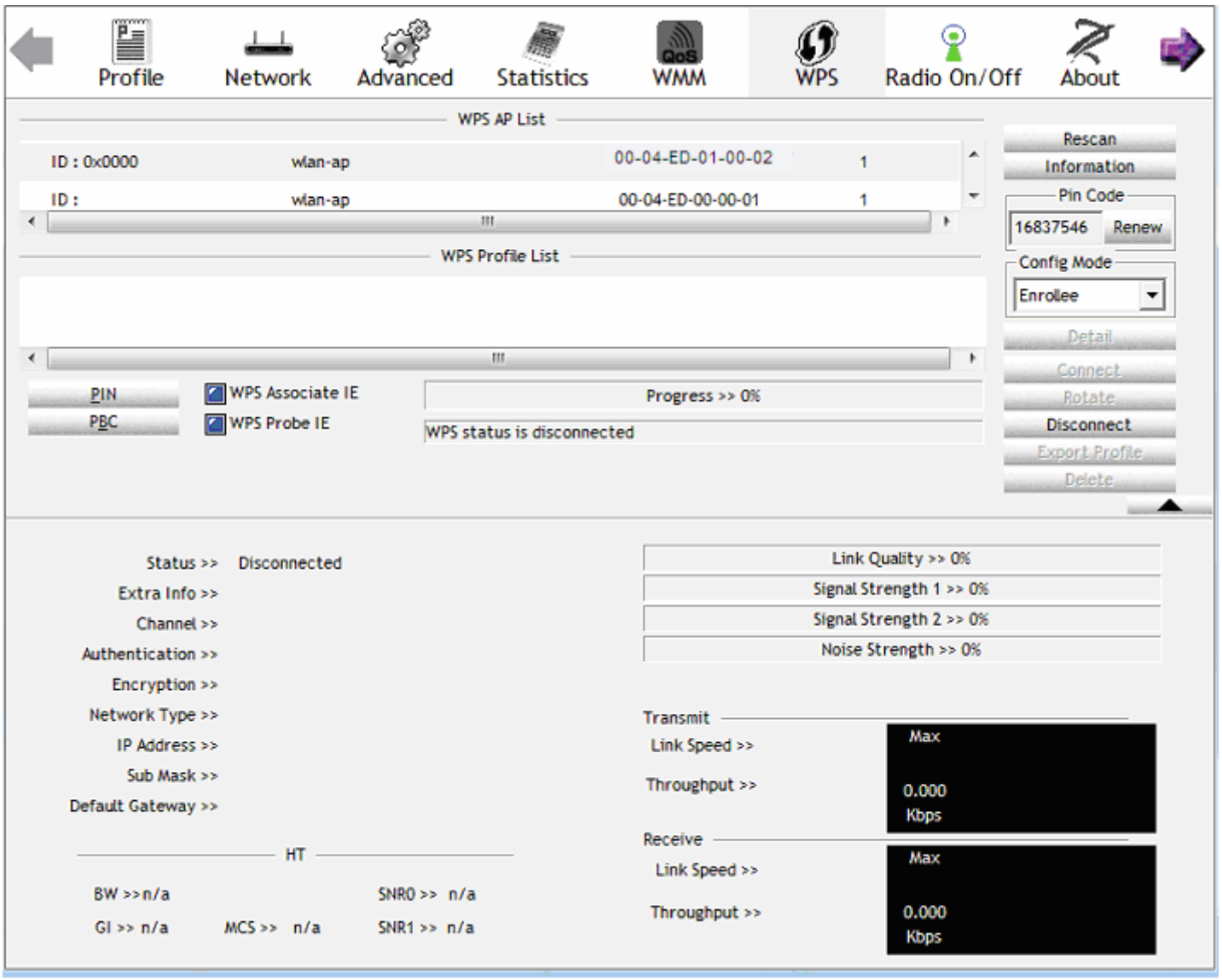
You can check the message in the red ellipse with the security parameters you set, here we all use the default.

Add Enrollee with PBC Method

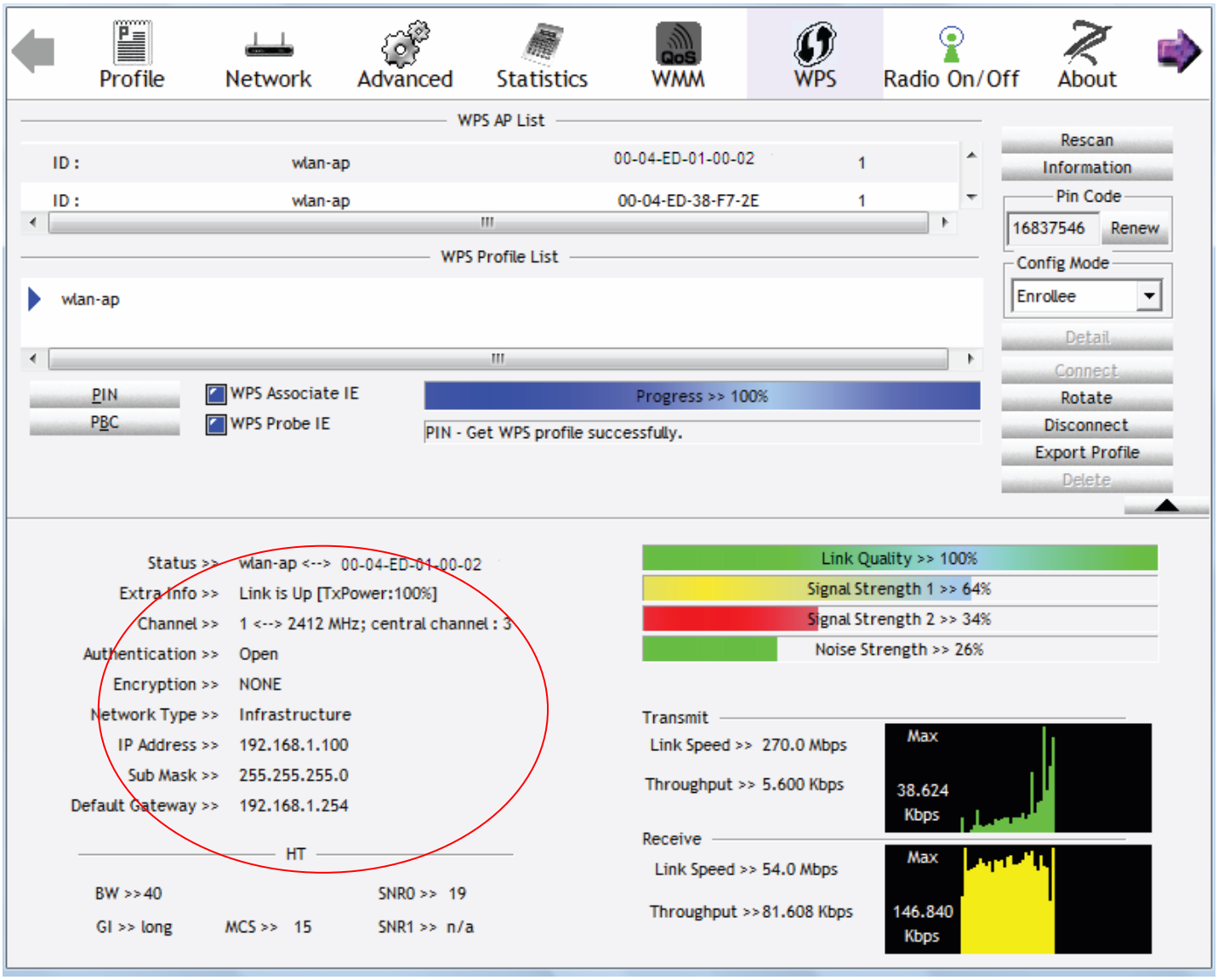
1. Select radio button “Push-Button” and Click Add Enrolee Or Press the physical button on router.



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



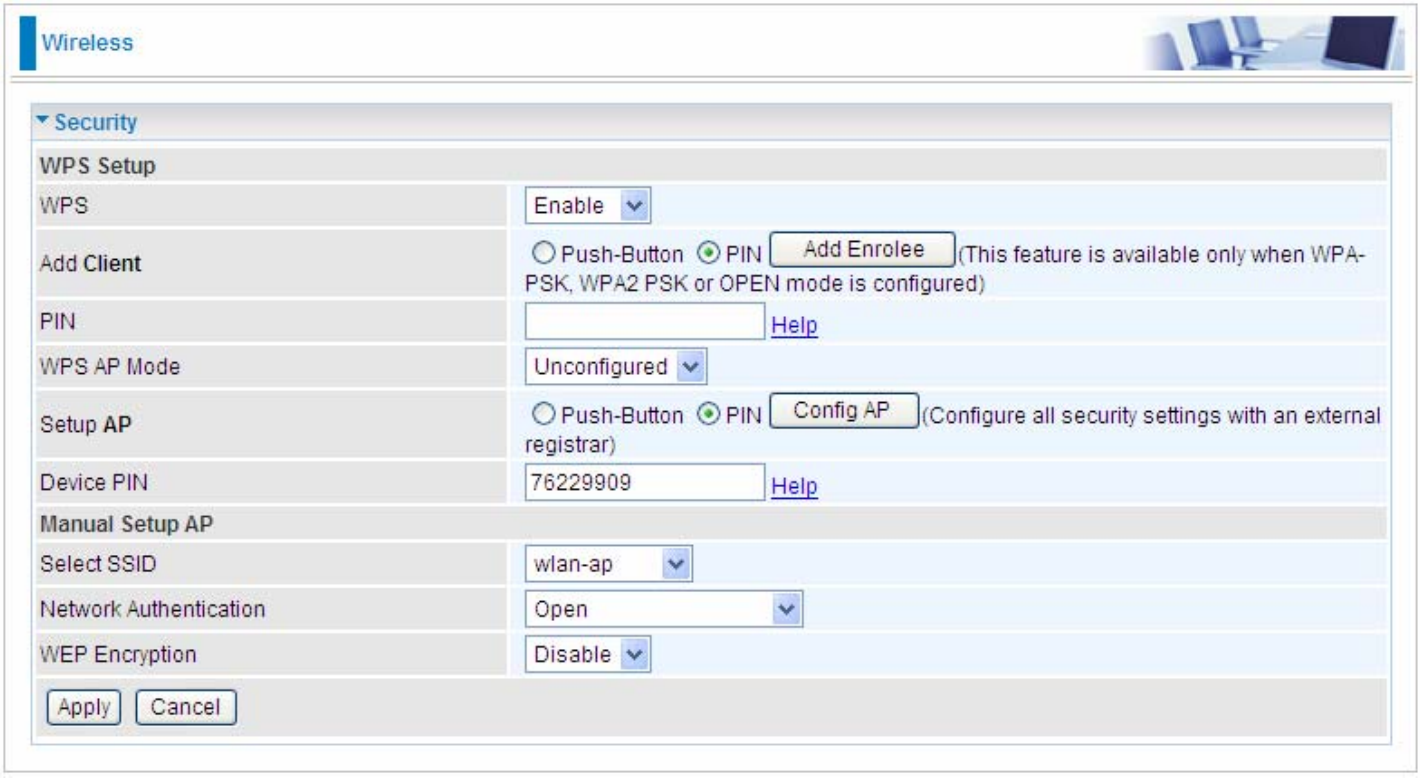
3. When the PBC button is pushed, a wireless communication will be established between your router and the PC. The client's SSID and security setting will now be configured to match the SSID and security setting of the router.



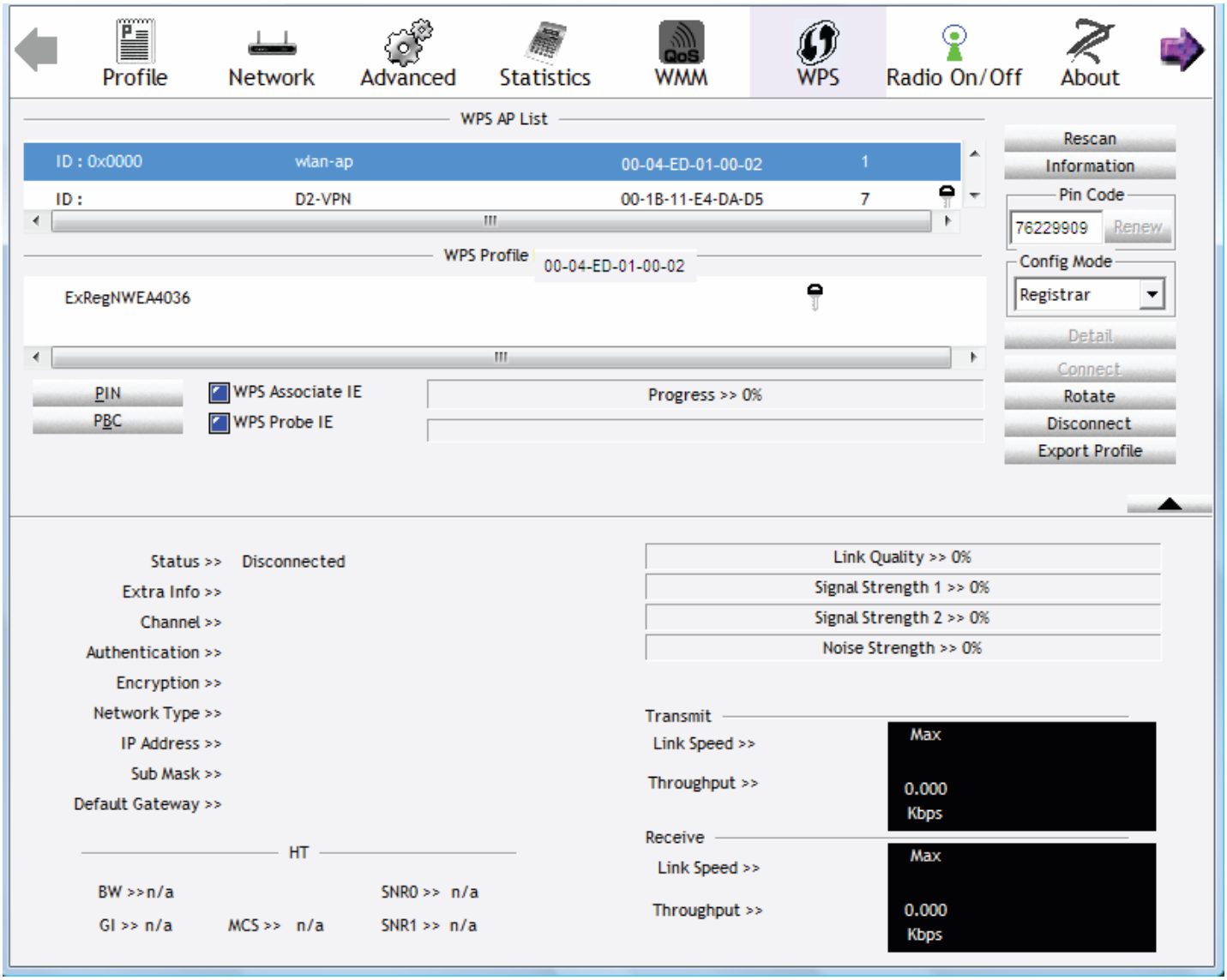
Configure AP as Enrollee

Add Registrar with PIN Method

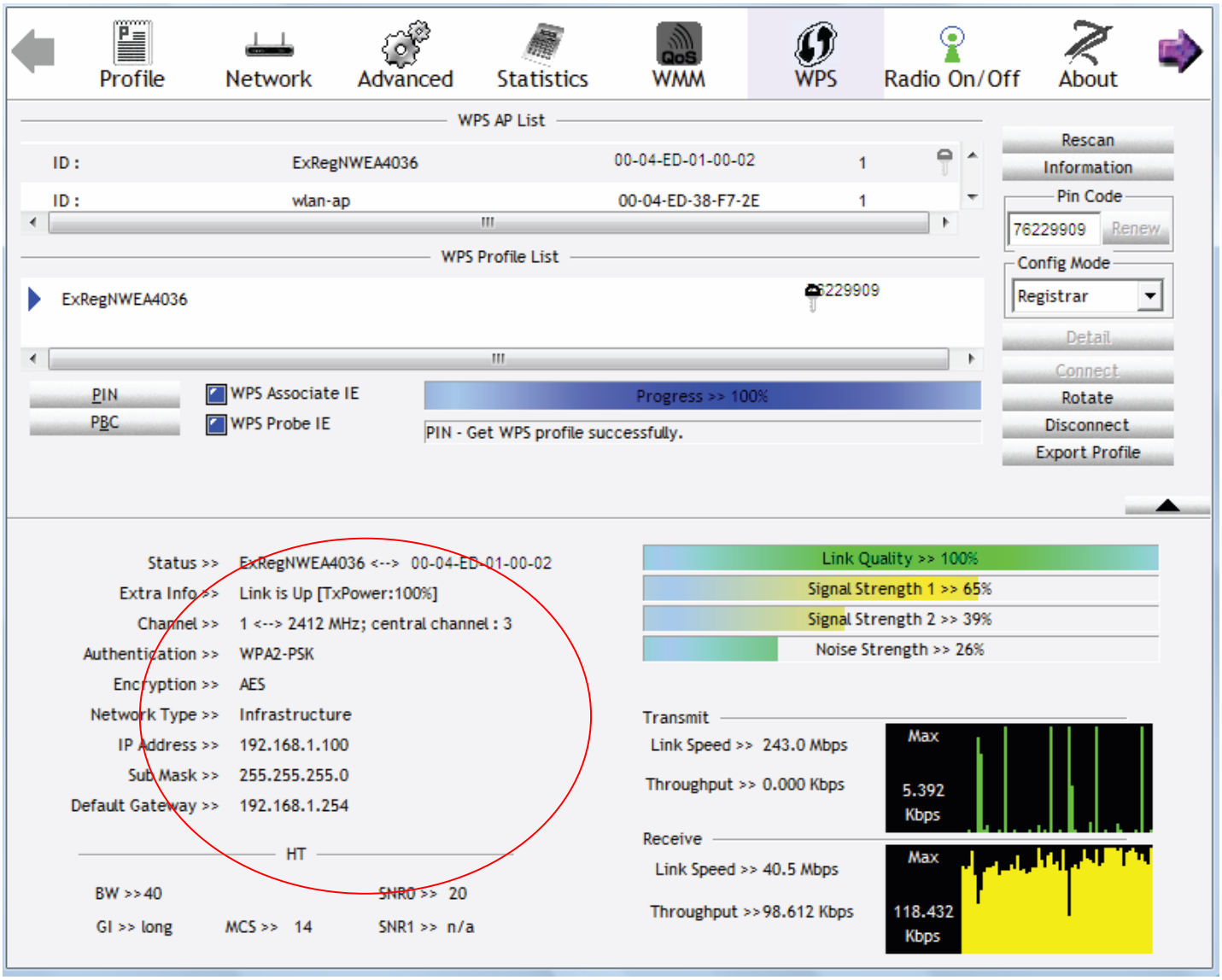
1. Set AP to “Unconfigured Mode” and Click “Config AP” button.



2. Launch the wireless client's WPS utility (eg. Ralink Utility). Set the Config Mode as Registrar. Enter the PIN number (76229909 for example) in the PIN Code column then choose the correct AP (eg. wlan-ap) from the WPS AP List section before pressing the PIN button to run the scan.

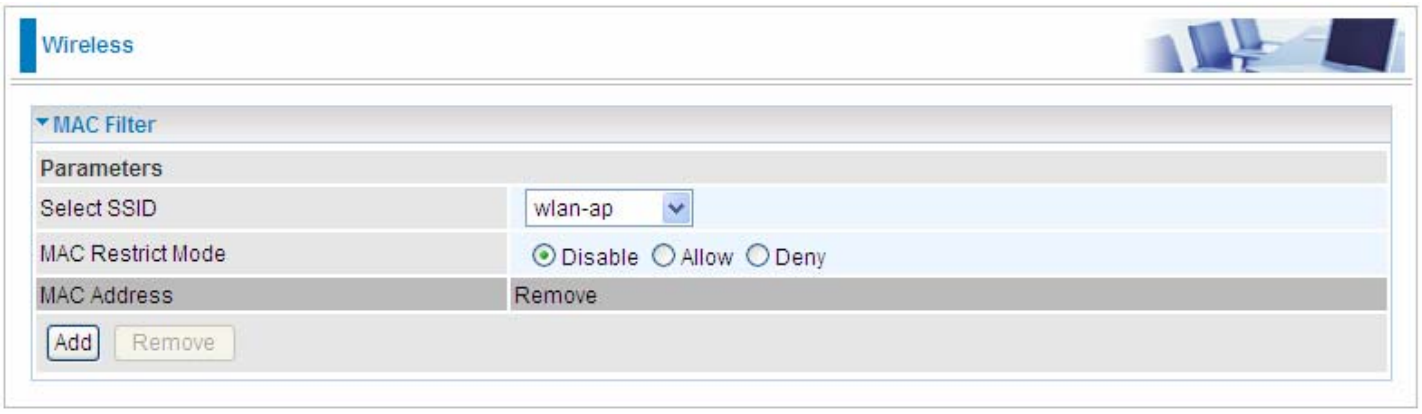


3. The router's (AP's) SSID and security setting will now be configured to match the SSID and security setting of the registrar.



4. Do Web Page refresh after ER complete AP Configuration to check the new parameters setting.

MAC Filter

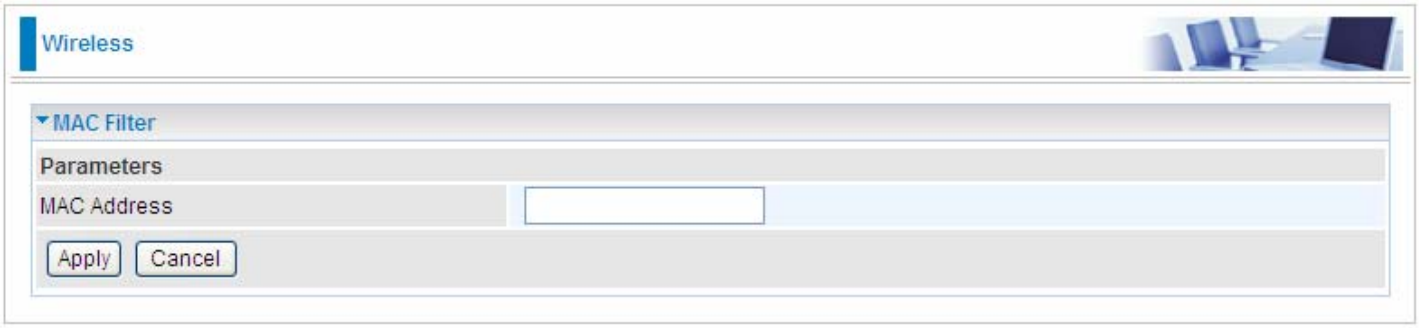


Select SSID: select the SSID you want this filter applies to.

MAC Restrict Mode:

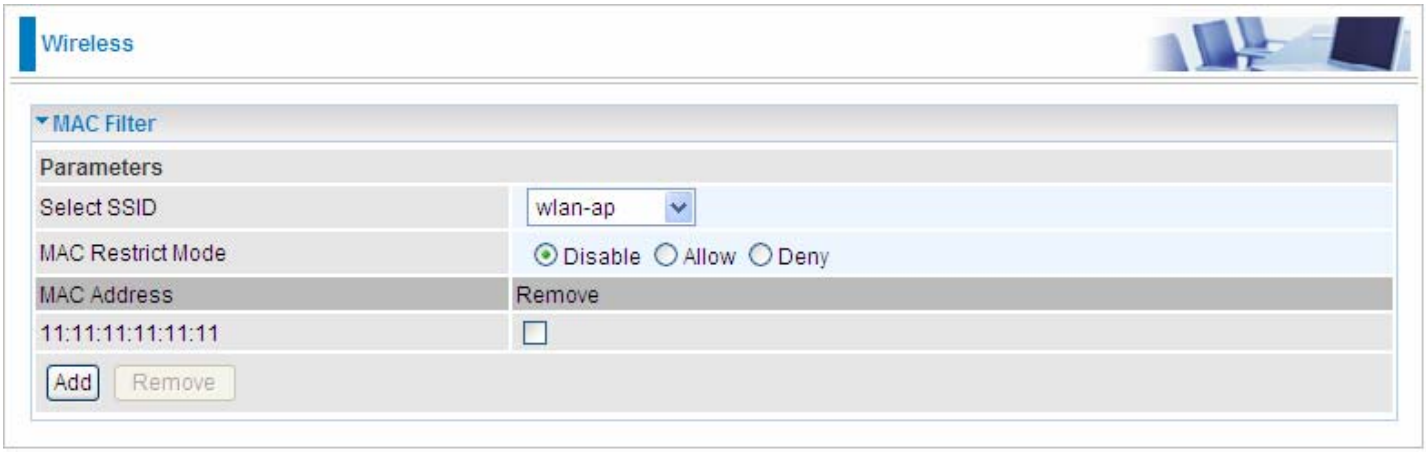
- **Disable:** disable the MAC Filter function.
- **Allow**: allow the hosts with the following listed MACs to access the wireless network.
- **Deny**: deny the hosts with the following listed MACs to access the wireless network.

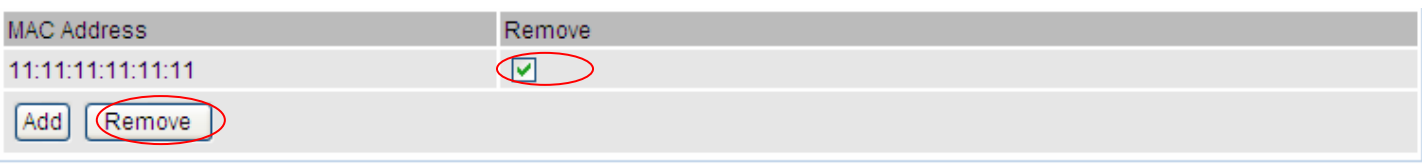
Click **Add** to add the MACs.



MAC Address: enter the MAC address(es). The format of MAC address could be: xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.

Click **Apply** to apply your settings and the item will be listed below.



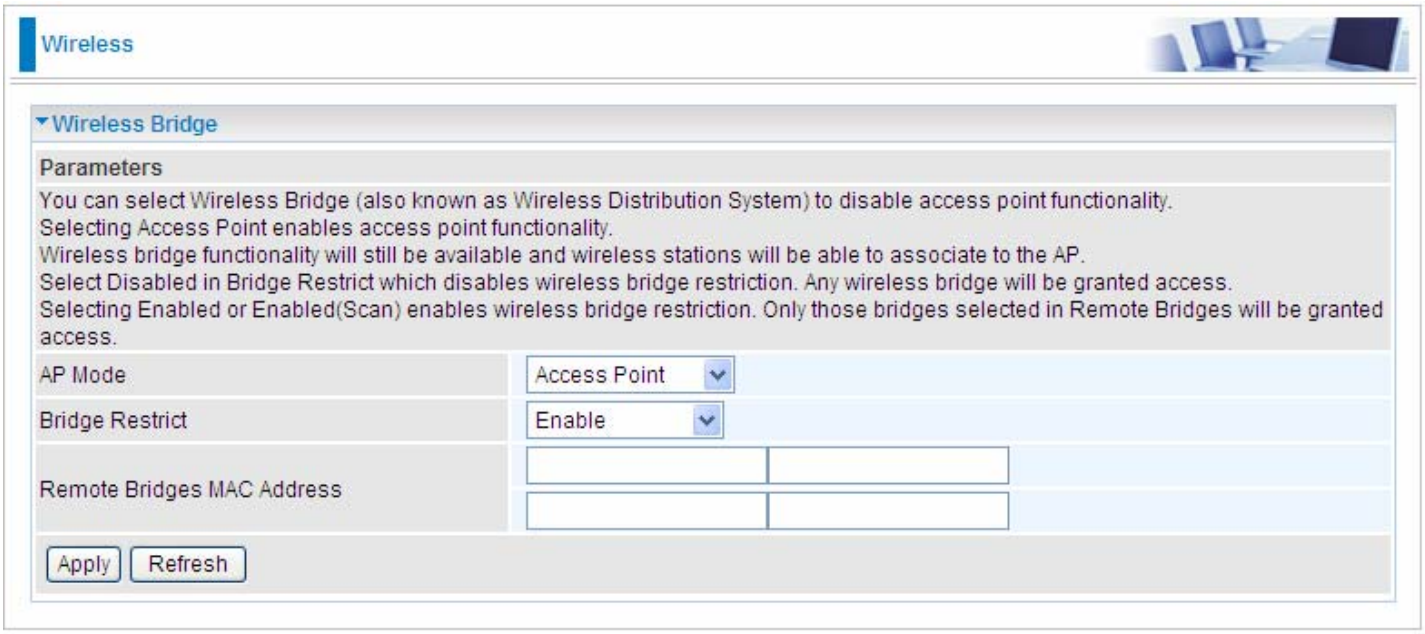


If you need not the rules, check the remove checkbox and press **Remove** to delete it.

Wireless Bridge

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

Here you can select to decide what role the AP servers as, AP or wireless bridge (WDS).



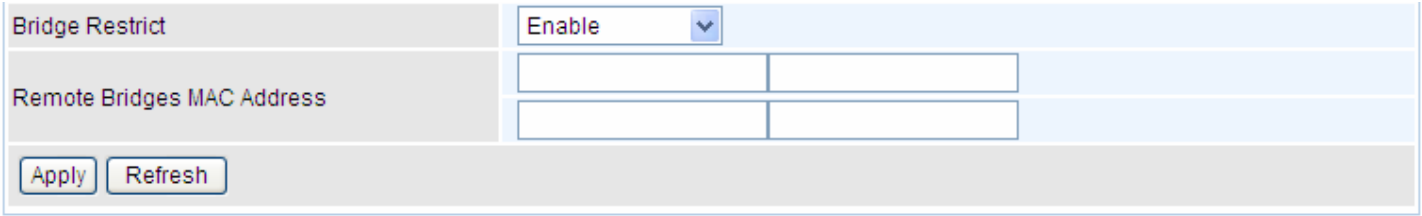
AP Mode: determines whether the gateway will act as an Access point or as a Bridge.

- **Access Point**: the gateway communicates with both clients and bridges.
- **Wireless Bridge**: the gateway communicates with other WDS devices only. In this mode, the gateway doesn't communicate with client devices.

If your wireless network includes repeaters that use WDS, the gateway in wireless bridge mode will also communicate with your repeaters. The gateway in wireless bridge mode will not communicate with a repeater that uses a proprietary (non-WDS) mode.

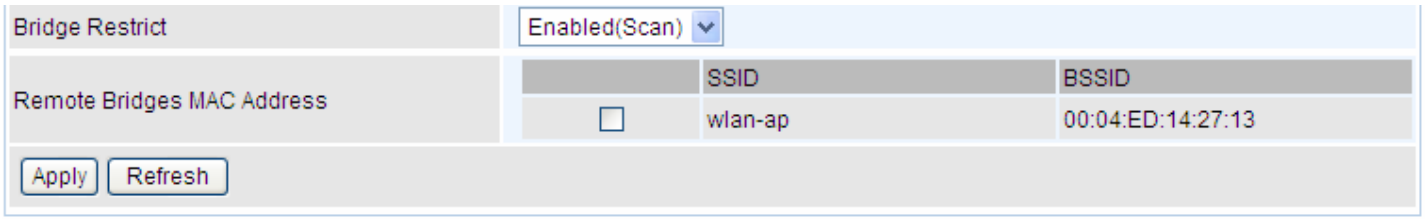
Bridge Restrict: When **AP Mode** is set to **Wireless Bridge**, this determines whether the gateway will communicate with all other bridges or only specific ones:

- **Enable:** to enable wireless bridge restriction. Only those specified in the Remote MAC Address the gateway can communicate with.



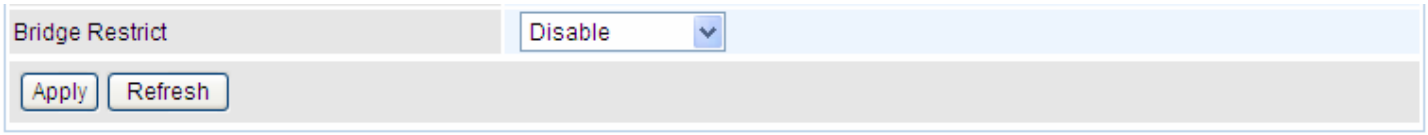
Remote Bridge MAC Address: enter the remote bridge MAC addresses. Here up to 4 bridge MAC addresses are supported.

ⓘ **Enabled (Scan):** to enable wireless bridge restriction. Only those been scanned the gateway can communicate with.



Remote Bridge MAC Address: select the remote bridge MAC addresses.

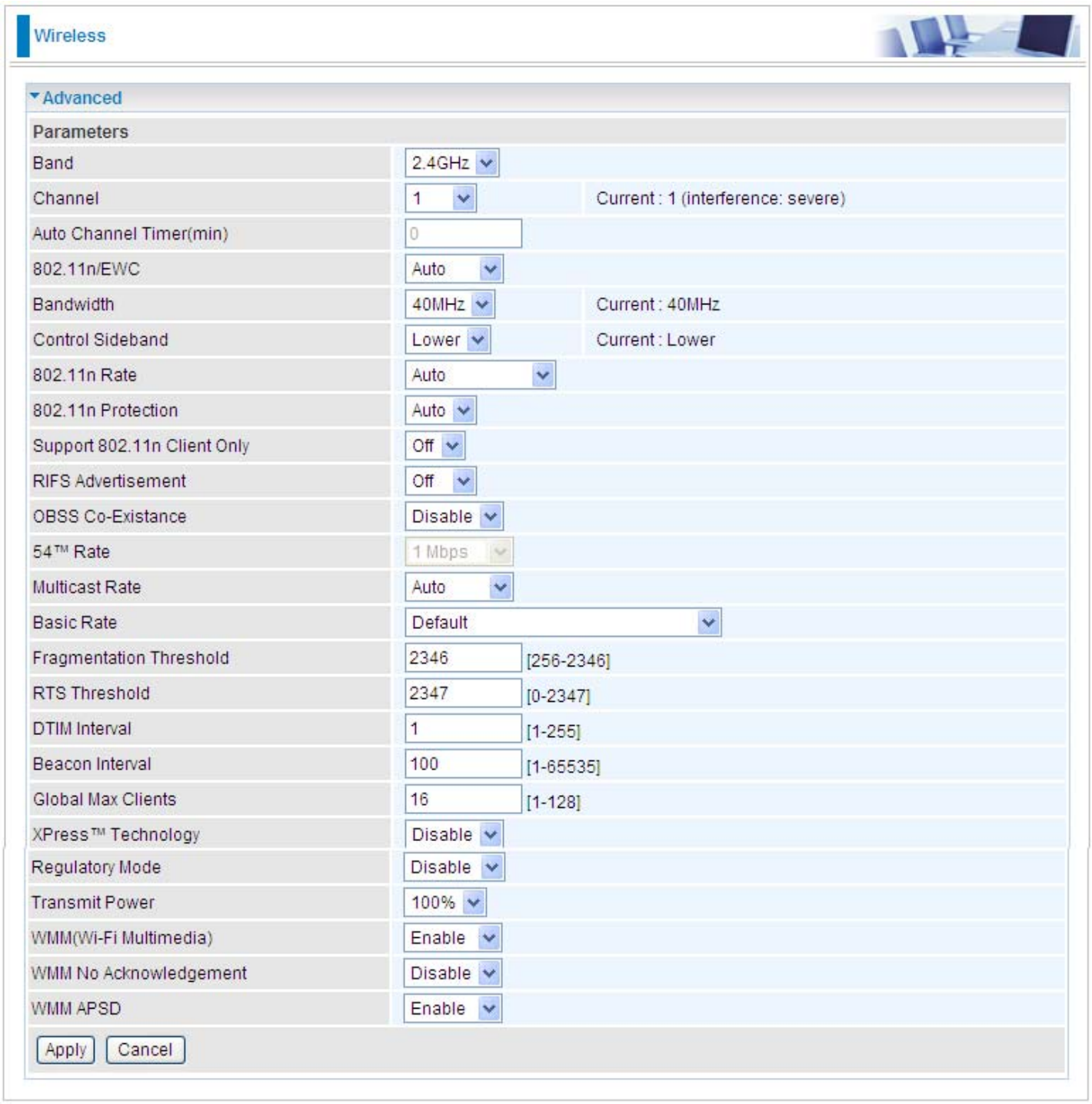
ⓘ **Disable:** Does not restrict the gateway to communicating with bridges that have their MAC address listed, but it is still open to communicate with all bridges that are in the same network.



Click **Apply** to apply your settings.

Advanced

Here users can set some advanced parameters about wireless.



Band: select frequency band. Here 2.4GHZ.

Channel: Allows channel selection of a specific channel (1-7) or Auto mode.

Auto Channel Timer(min): the auto channel times length it takes to scan in minutes. Only available for auto channel mode.

802.11n/EWC: select to auto enable or disable 802.11n.

Bandwidth: Select bandwidth. The higher the bandwidth the better the performance will be.

Control Sideband: only available for 40MHz. It allows you to select upper sideband or lower sideband. Sideband refers to the frequency band either above (**upper sideband**) or below (**lower sideband**) the carrier frequency, within which fall the spectral components produced by modulation of a carrier wave.

802.11n Rate: It allows you to select the fixed transmission rate or auto.

802.11n Protection: turn off for maximized throughput. Auto for greater security.

Support 802.11n Client Only: turn on the option is to only provide wireless access to the clients operating at 802.11n speeds.

RIFS Advertisement: Reduced Inter-frame Spacing (RIFS) is a 802.11n feature that also improves performance by reducing the amount of dead time required between OFDM transmissions. Select Off to disable this function or auto to enable this function.

OBSS Co-Existance: coexistence (or not) between 20 MHZ and 40 MHZ overlapping basic service sets (OBSS) in wireless local area networks.

Multicast Rate: Setting for multicast packets transmission rate.

Basic Rate: Setting for basic transmission rate. It is not a certain kind of rate, it is a series of rates supported. When set to Default, the router can transmit with all kinds of standardized rates.

Fragmentation Threshold: A threshold (in bytes) whether the packets will be fragmented and at what size. Packets succeeding the fragmentation threshold of 802.11n WLAN will be split into smaller units suitable for circuit size. While the packets smaller than fragmentation threshold will not be fragmented. Default is 2346, setting the fragmentation too low may result in poor performance.

RTS Threshold: Request to Send (RTS) threshold specifies the packet size, when exceeds the size, the RTS/CTS will be triggered. The default setting of 2347(max length) will disable the RTS.

DTIM Interval: Delivery Traffic Indication Message (DTIM). The entry range is a value between 1 and 255. A DTIM is countdown variable that informs clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM interval value. AP clients hear the beacons and awaken to receive the broadcast and multicast messages. The default is 1.

Beacon Interval: The amount of time between beacon transmissions in is milliseconds. The default is 100ms and the acceptable is 1- 65535. The beacon transmissions identify the presence of an access point.

Global Max Clients: Here you have the option of setting the limit of the number of clients who can connect to your wireless network.

XPress™ Technology: It has been designed to improve the wireless network efficiency. Default is disabled.

Regulatory Mode: select to deny any regulatory mode. There are two regulatory modes:

802.11h: The standard solves interference problems with e.g. satellites and radar using the same 5 GHz band as 802.11a or 802.11n dual-band access points.

802.11d: This standard automatically adjusts its allowed frequencies, power levels and bandwidth accordingly to the country it's located in.
This means that manufacturers don't need to make country specific products.

Transmit Power: select the transmitting power of your wireless signal.

WMM (Wi-Fi Multimedia): you can choose to enable or disable this function which allows for priority of certain data over wireless network.

WMM No Acknowledgement: Refers to the acknowledge policy at the MAC level. Enabling WMM No Acknowledgement can result in more efficient throughput but higher error rates in noisy Radio Frequency (RF) environment.

WMM APSD: Automatic Power Save Delivery. Enable this to save power.

Station Info

Here you can view the information about the wireless clients.

MAC Address: the MAC address of the wireless clients.

Associated: List all the stations that are associated with the Access Point. If a station is idle for too long, it is removed from this list

Authorized: List those devices with authorized access**.**

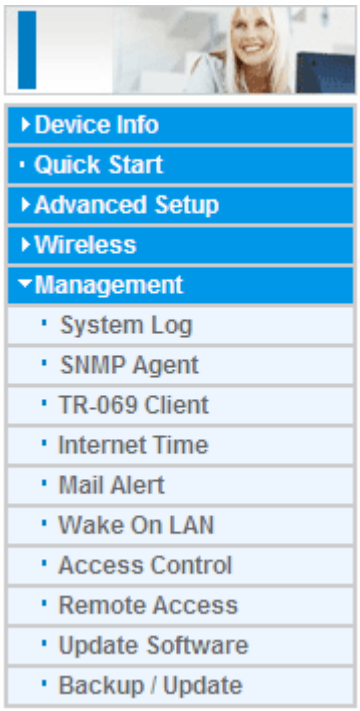
SSID: show the current SSID of the client.

Interface: to show which interface the wireless client is connected to.

Refresh: to get the latest information.

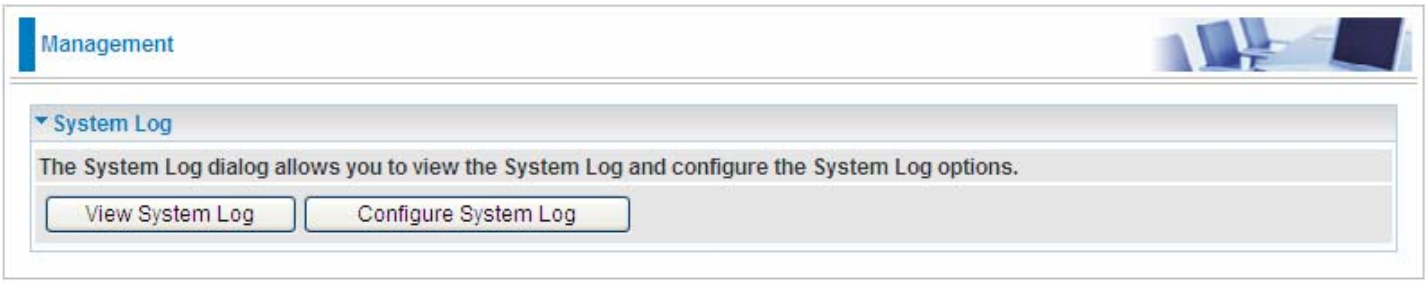
Management

There are 9 items within the System section: **System Log**, **SNMP Agent**, **TR-069 Client, Internet Time**, **Mail Alert, Wake on LAN, Access Control, Remote Access**, **Update Software** and **Backup/Update.**

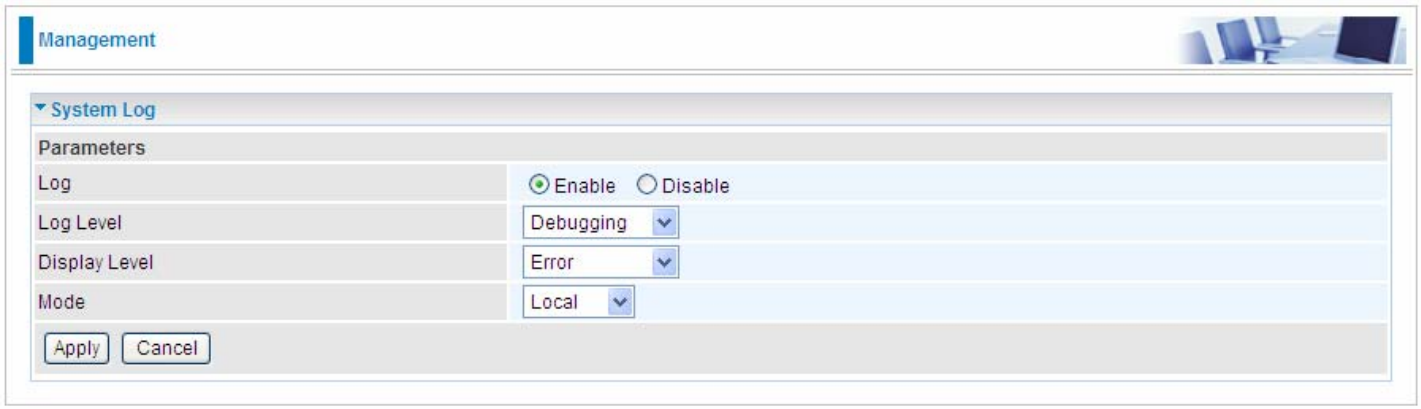


System Log

To let users view or configure System Log.



Click Configure System Log to configure the log.



Log: enable or disable this function.

Log level: select your log level. The log level allows you to configure which types of events are loged. There are eight log levels from high to low are displayed below:

- **Emergency** = system is unusable (these appear in red in the log)
- **Alert** = action must be taken immediately (pale red)
- **Critical** = critical conditions (orange)
- **Error** = error conditions (yellow)
- **Warning** = warning conditions (green)
- **Notice** = normal but significant conditions (blue)
- **Informational** = information events (white)
- **Debugging** = debug-level messages (dark grey on cream)

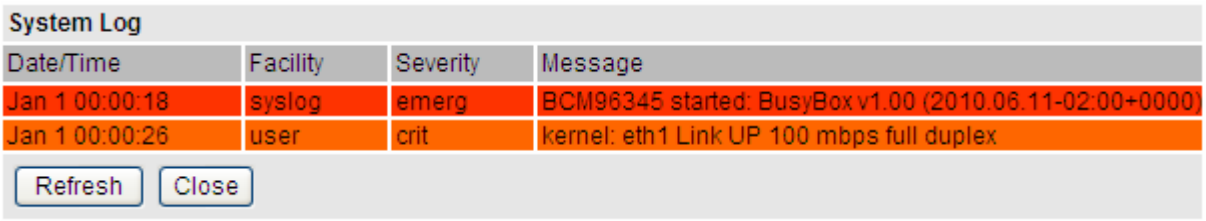
The gateway records all log events at the chosen level and above. For instance, if you set the log level to Critical, all critical, alert, and emergency events are logged, but none of the others are recorded

Display Level: display the log according to the level you set when you view system log. Once you set the display level, the logs of the same or higher priority will be displayed.

Mode: select the mode the system log adopted. Three modes: local, Remote and Both.

- **Local**: select this mode to store the logs in the router's local memory.
- **Remote**: select this mode to send the log information to a remote log server. Then you must assign the remote log server and port, 514 is often used.
- **Both**: logs stored adopting above two ways.

Click View System Log to see the System log of this router. The logs will be listed as configured above. Click **refresh** to get the latest information.



Click **Apply** to save your settings.

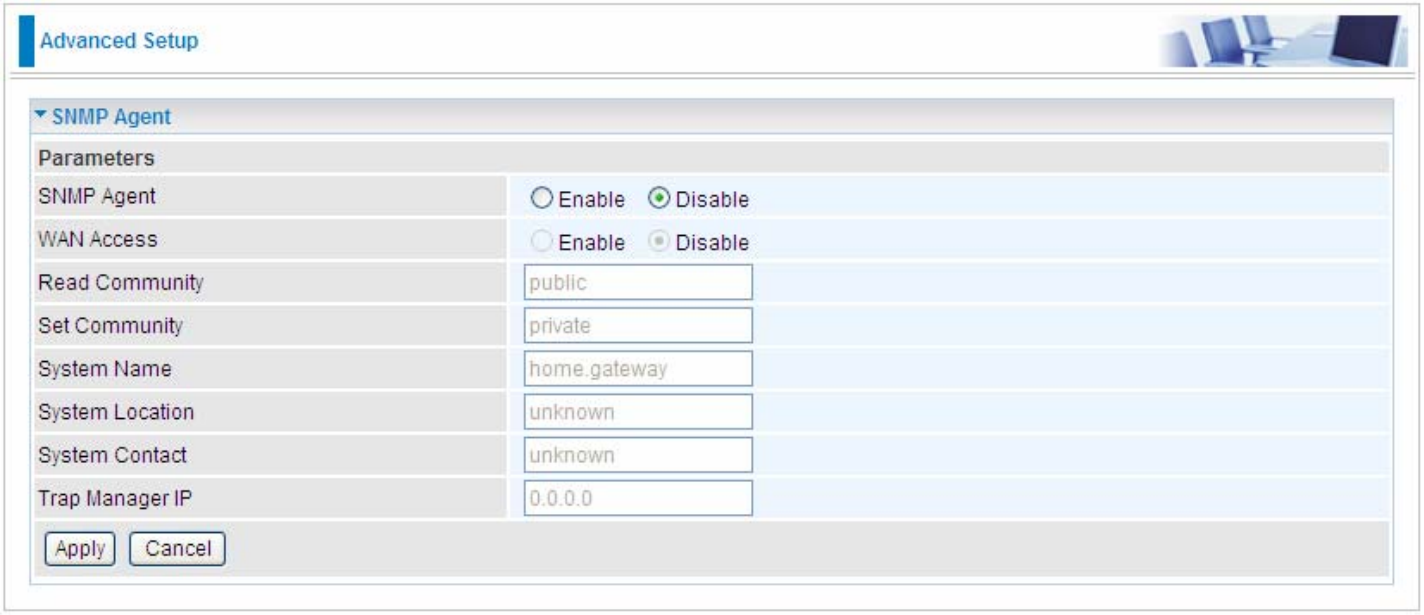
SNMP Agent

SNMP, Simple Network Management Protocol, is the most popular one in network. It consists of SNMP Manager，SNMP Agent and MIB. Every network device supporting SNMP will have a SNMP Agent which is a management software running in the device.

SNMP Manager, the management software running the server, is to use SNMP protocol to send GetRequest、GetNextRequest, SetRequest message to Agent to view and change the information of the device.

SNMP Agents, the management software running in the device, accepts the message from the manager, Reads or Writes the management variable in MIB accordingly and then generates Response message to send it to the manager. Also, agent will send Trap message to the manager when agent finds some exceptions.

Trap message, is the message automatically sent by the managed device without request to the manager about the emergency events.



SNMP Agent: enable or disable SNMP Agent.

WAN Access: enable or disable WAN access which allows PCs in WAN side read or set the SNMP related MIB pamareters.

Read Community: Type the Get Community, which is the authentication for the incoming Get-and GetNext requests from the management station.

Set Community: Type the Set Community, which is the authentication for incoming Set requests from the management station.

System Name: here it refers to your router.

System Location: user-defined location.

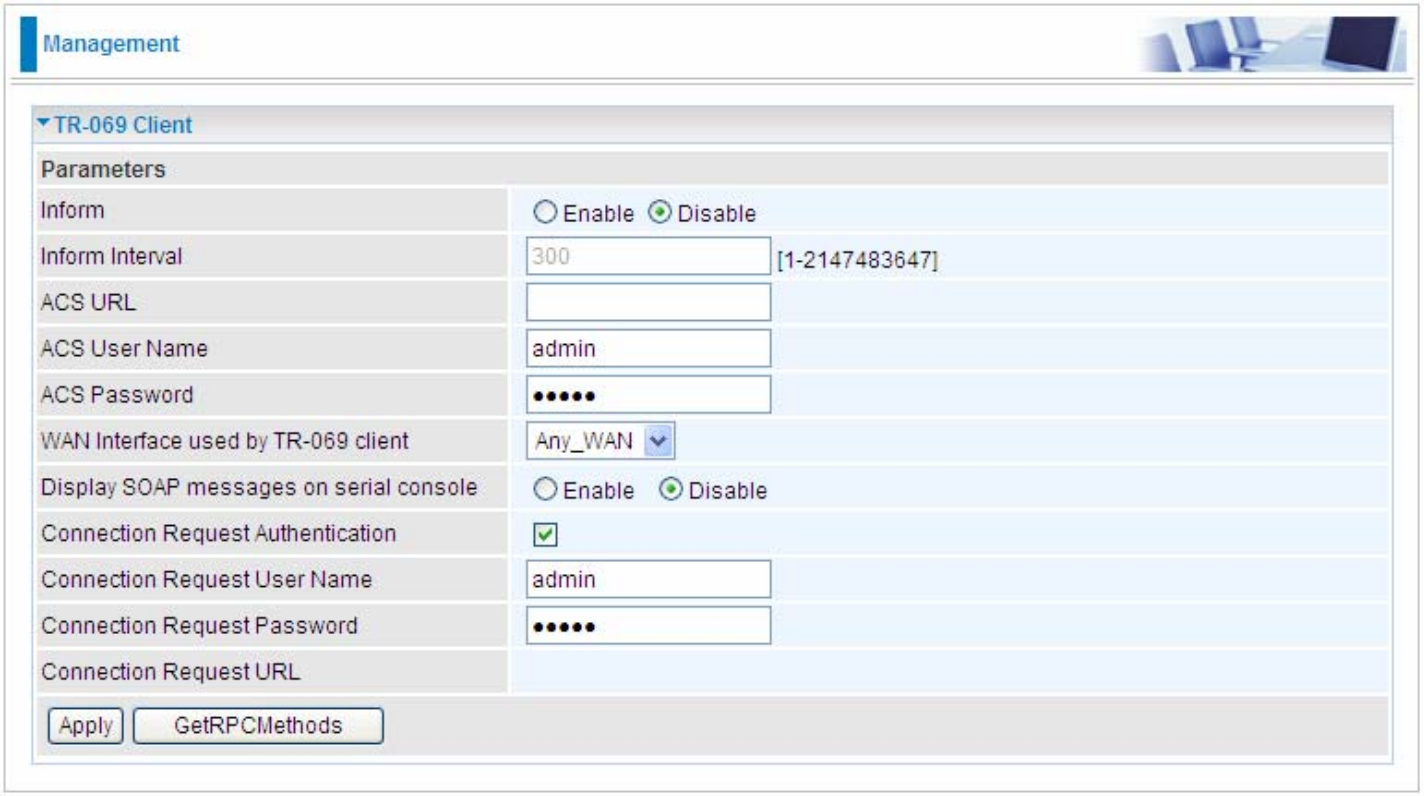
System Contact: user-defined contact message.

Trap manager IP: enter the IP address of the server receiving the trap sent by SNMP agent.

TR- 069 Client

TR-069 (short for Technical Report 069) is a DSL Forum (which was later renamed as Broadband Forum) technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices. It defines an application layer protocol for remote management of end-user devices.

As a bidirectional SOAP/HTTP based protocol it can provides the communication between customer premises equipment (CPE) and Auto Configuration Server (ACS). It includes both a safe configuration and the control of other CPE management functions within an integrated framework. In the course of the booming broadband market, the number of different internet access possibilities grew as well (e.g. modems, routers, gateways, set-top box, VoIP-phones).At the same time the configuration of this equipment became more complicated –too complicated for end-users. For this reason, TR-069 was developed. It provides the possibility of auto configuration of the access types. Using TR-069 the terminals can get in contact with the Auto Configuration Servers (ACS) and establish the configuration automatically and let ACS configure CPE automatically.



Inform: select enable to let CPE be authorized to send Inform message to automatically connect to ACS.

Inform Interval: Specify the inform interval time (sec) which CPE used to periodically send inform message to automatically connect to ACS. When the inform interval time arrives, the CPE will send inform message to automatically connect to ACS.

ACS URL: Enter the ACS server login name.

ACS User Name: Specify the ACS User Name for ACS authentication to the connection from CPE.

ACS password: Enter the ACS server login password.

WAN interface used by TR-069: select the interface used by TR-069.

Display SOAP message on serial console: select whether to display SOAP message on serial console.

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

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

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

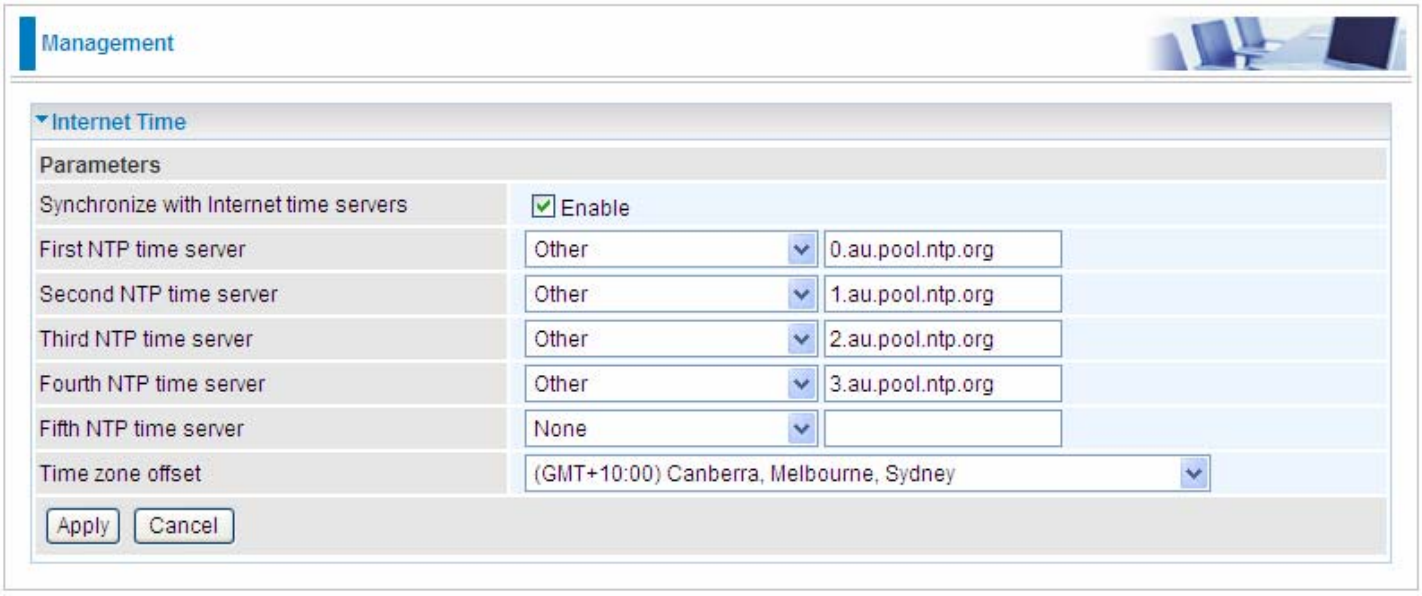
GetRPCMethods： supported by both CPE and ACS, display the supported RFC listing methods.

Click **Apply** to apply your settings.

Internet Time

The router does not have a real time clock on board; instead, it uses the Network Time Protocol (NTP) to get the most current time from an NTP server.

NTP is a protocol for synchronization of computers. It can enable computers synchronize to the NTP server or clock source with a high accuracy.



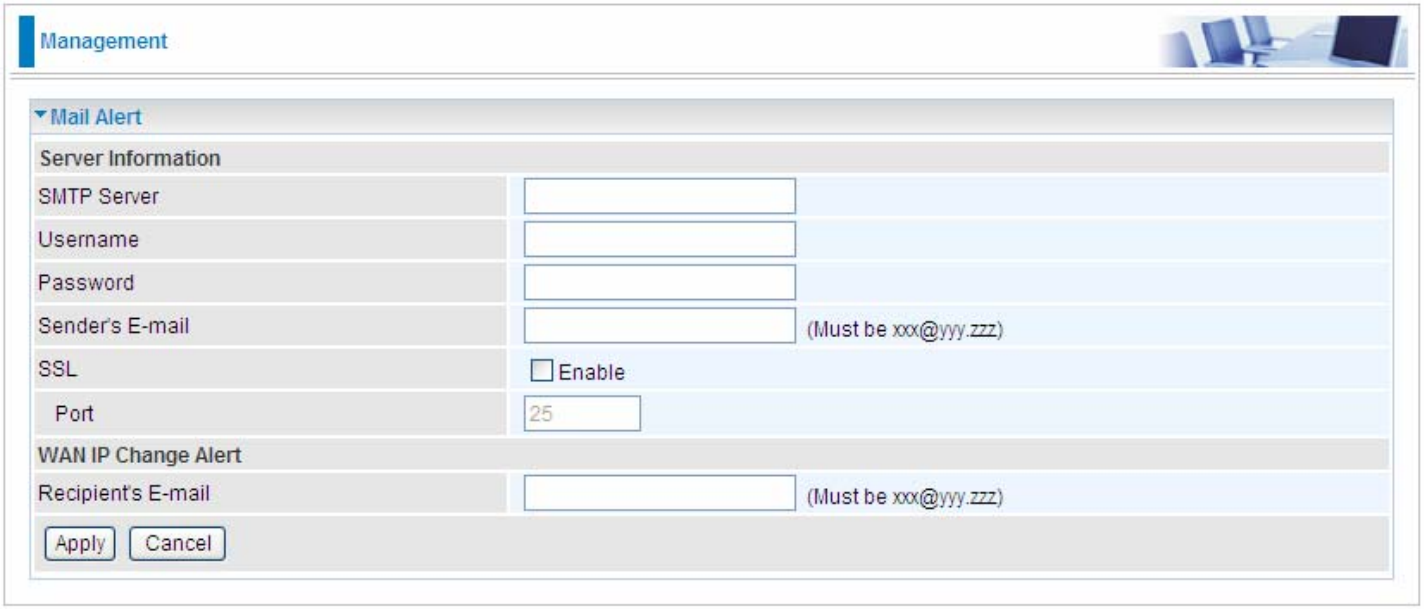
Choose the NTP time server from the drop-down menu, If you prefer to specify an NTP server other than those in the drop-down list, simply enter its IP address in their appropriate blanks provided as shown above. Your ISP may also provide an SNTP server for you to use.

Choose your local time zone from the drop-down menu. After a successful connection to the Internet, the router will retrieve the correct local time from the NTP server you have specified. If you prefer to specify an NTP server other than those in the drop-down list, simply enter its IP address in their appropriate blanks provided as shown above. Your ISP may also provide an NTP server for you to use.

Click **Apply** to apply your settings.

Mail Alert

Mail alert is designed to keep system administrator or other relevant personnels alerted of any unexpected events that might have occured to the network computers or server for monitoring efficiency. With this alert system, appropriate solutions may be tackled to fix problems that may have arisen so that the server can be properly maintained.



SMTP Server: Enter the SMTP server that you would like to use for sending emails.

Username: Enter the username of your email account to be used by the SMTP server.

Password: Enter the password of your email account.

Sender's Email: Enter your email address.

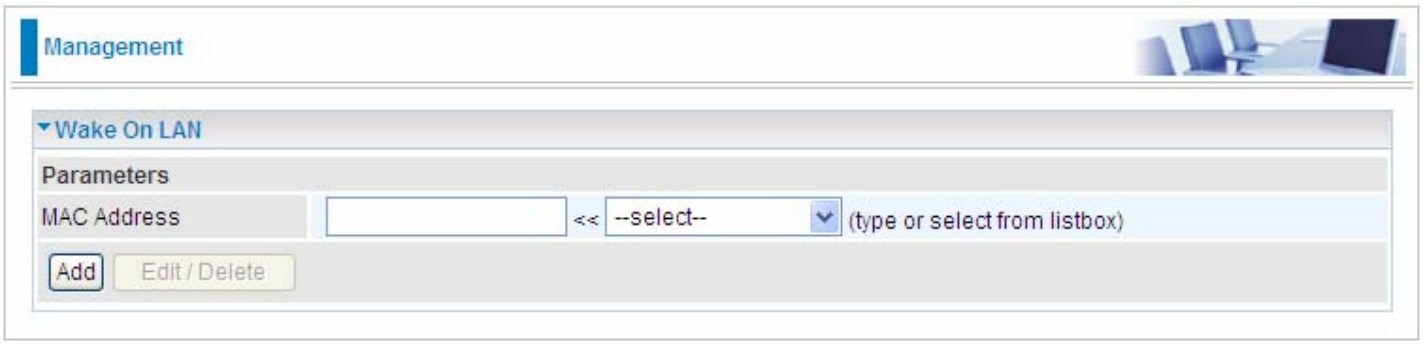
SSL: check to whether to enable SSL encryption feature.

Port: the port, default is 25.

Recipient's Email (WAN IP Change Alert): Enter the email address that will receive the alert message once an WAN IP change has been detected.

Wake on LAN

Wake on LAN (WOL, sometimes WoL) is an Ethernet computer networking standard that allows a computer to be turned on or woken up remotely by a network message.



Select: Select MAC address of the computer that you want to wake up or turn on remotely.

Add: After selecting, click Add then you can perform the Wake-up action.

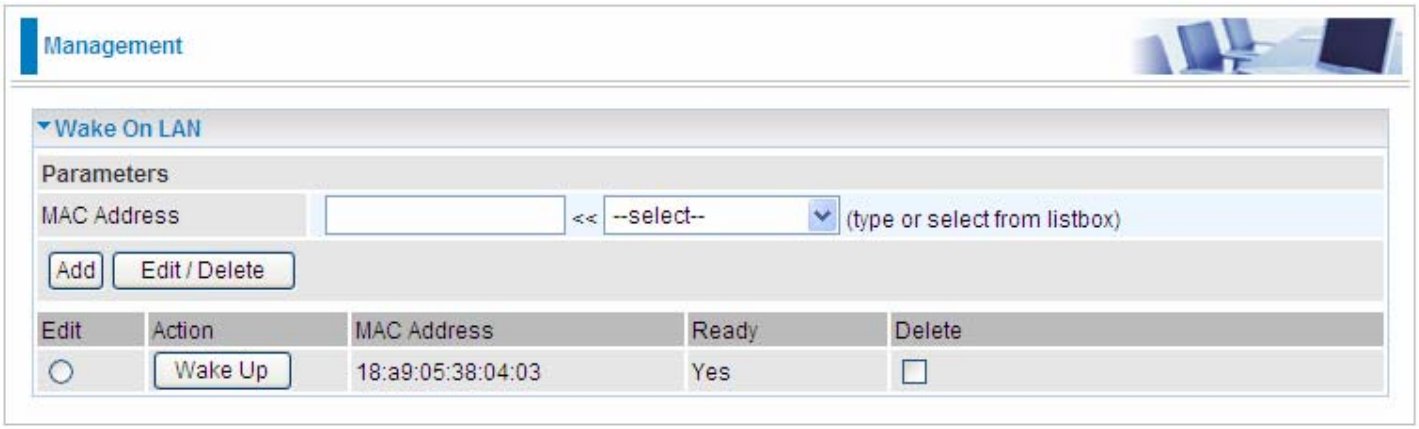
Edit/Delete: Click to edit or delete the selected MAC address.

Ready:

"Yes" indicating the remote computer is ready for your waking up.

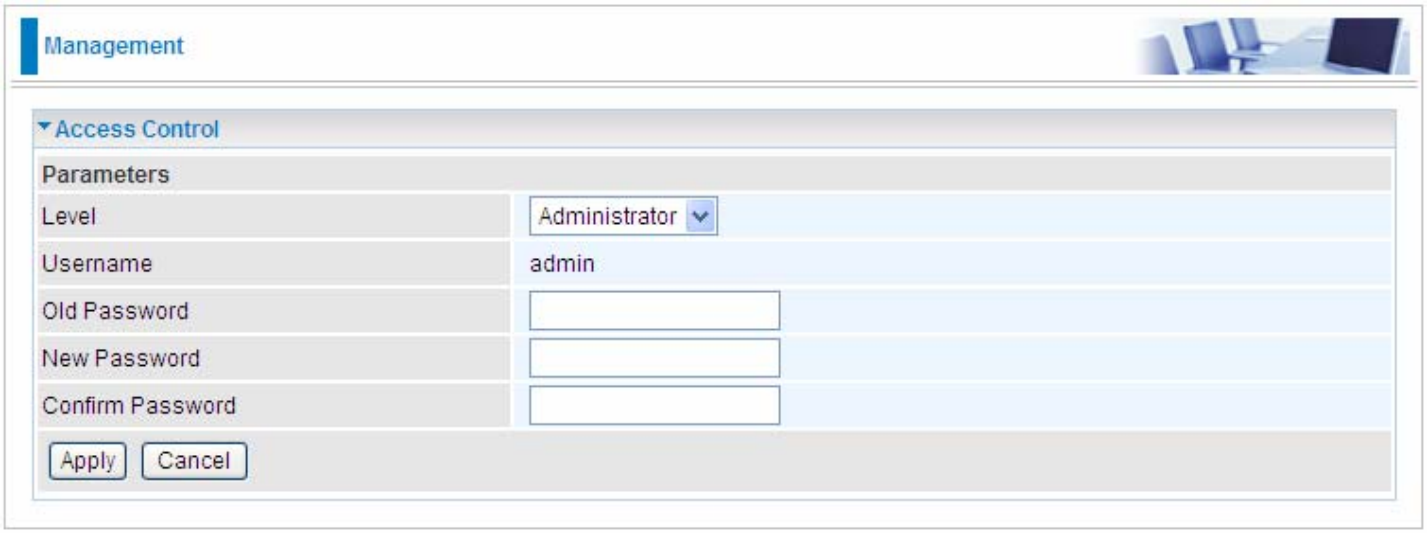
"No" indicating the machine is not ready for your waking up.

Delete: Delete the selected MAC address.



Access Control

Access Control is used to prevent unauthorized access to the router configuration page. Here you can change the login user password. Three user levels are provided here. Each user level there's a default provided user. You must access the router with the appropriate username and password. Here the corresponding passwords are allowed to change.



Level: select which level you want to change password to. There are three default levels.

- **Administrator:** the root user, corresponding default username and password are admin and admin respectively.
- **Remote:** username for the remote user to login, corresponding default username and password are support and support respectively.
- **Local:** username for the general user, corresponding default username password are user and user respectivley.

Username: the default username for each user level.

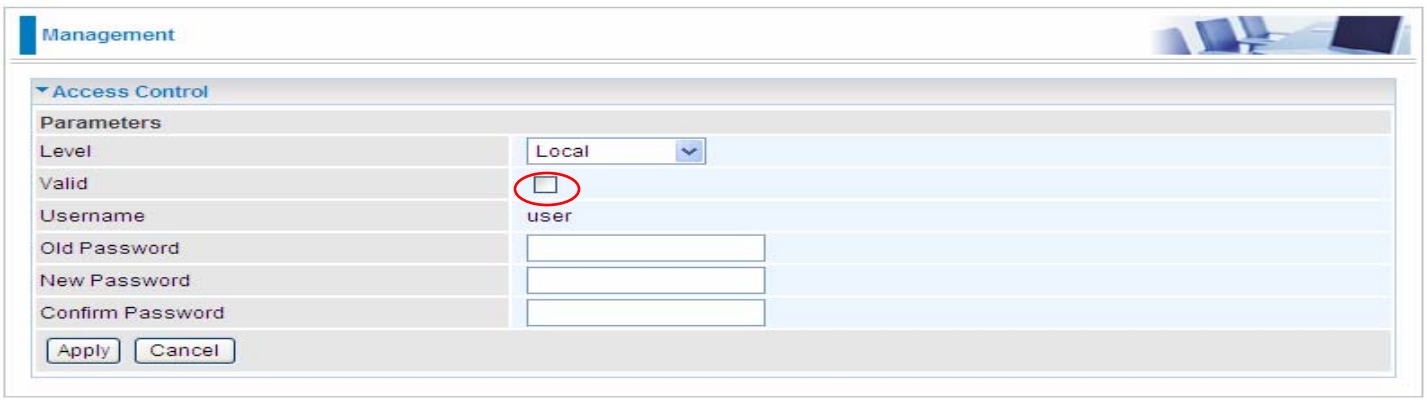
Old Password: Enter the old password.

New Password: Enter the new password.

Confirm Password: Enter again the new password to confirm.

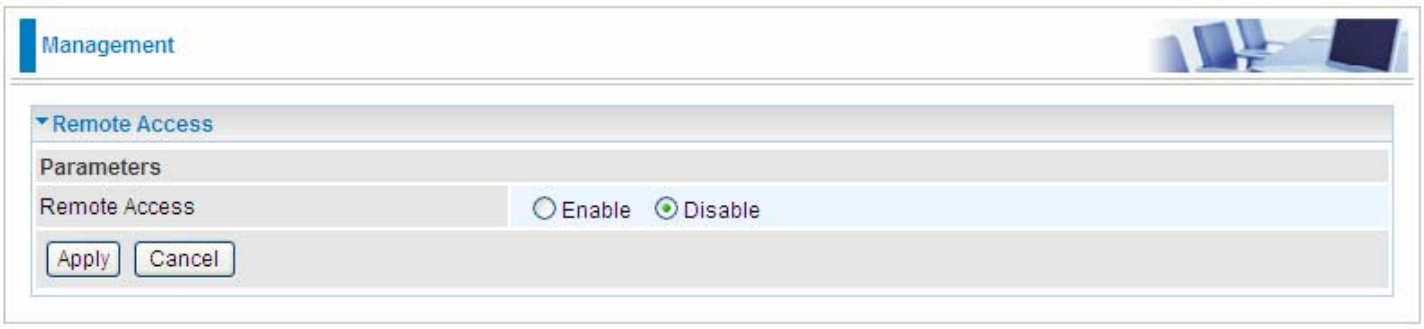
Click **Apply** to apply your new settings.

Note: by default the other two users of level Local and level Remote, thus user and support, are not available, if you want to use the two accounts, check **Valid** and set their passwords.



Remote Access

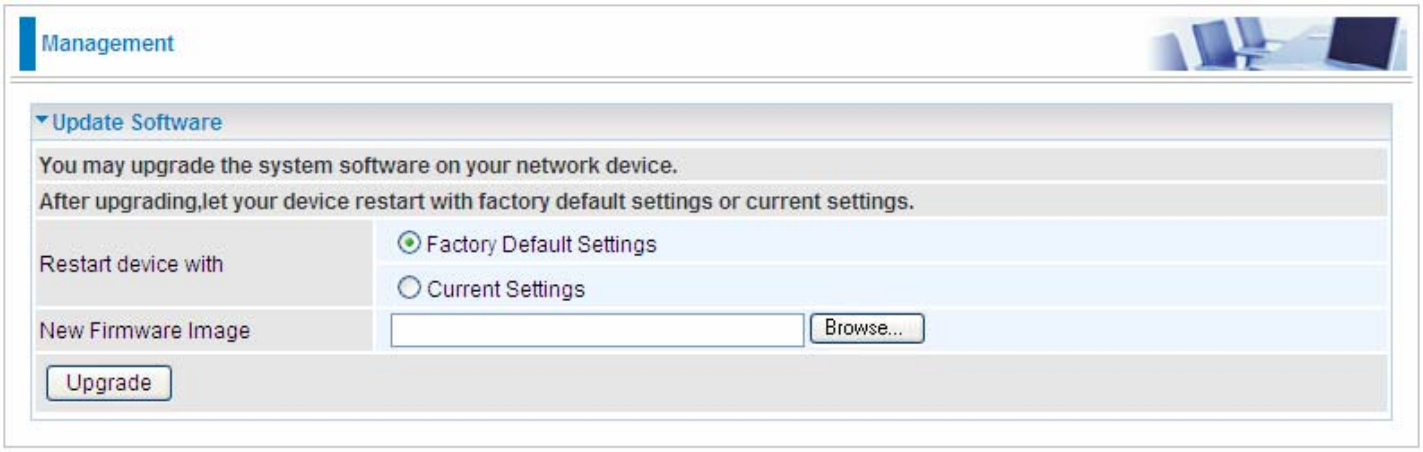
It is to allow remote access to the router to view or configure.



Remote: Select to enable or disable Remote Access functionality.

Update Software

Software upgrading lets you experience the new and integral function of your router.



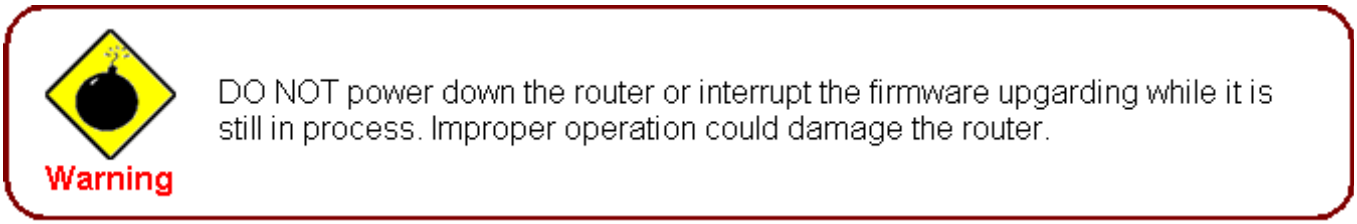
Restart device with:

- **Factory Default Settings:** Restart the device with factory default settings automatically when finished upgrading.
- **Current Settings:** Restart the device with the current settings automatically when finished upgrading.

Your router's "firmware" is the software that allows it to operate and provides all its functionality.

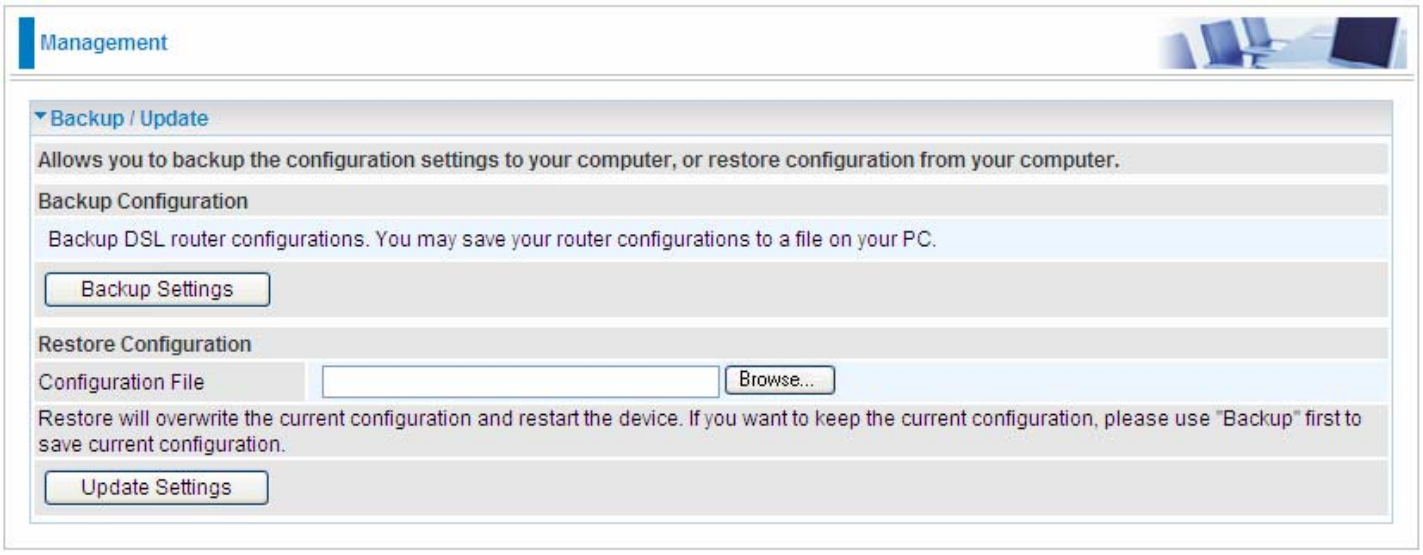
Think of your router as a dedicated computer, and the firmware as the software it runs. Over time this software may be improved and revised, and your router allows you to upgrade the software it runs to take advantage of these changes.

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



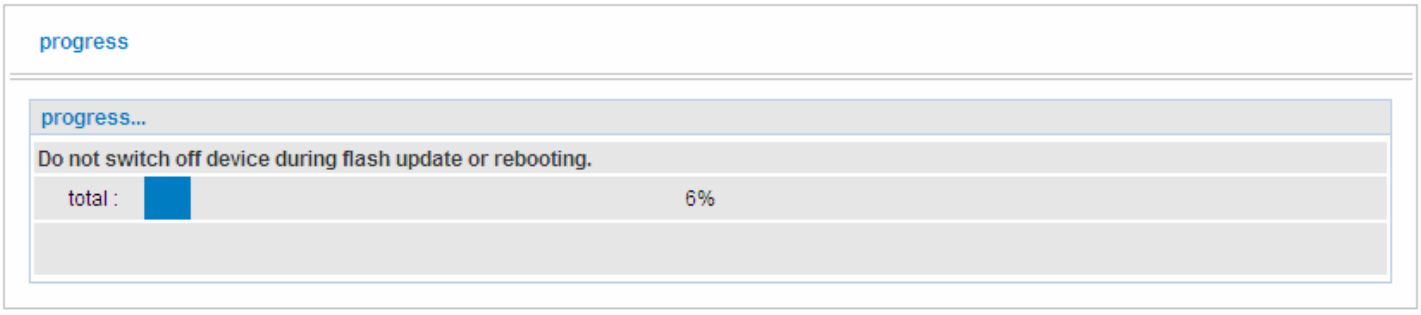
Backup / Update

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



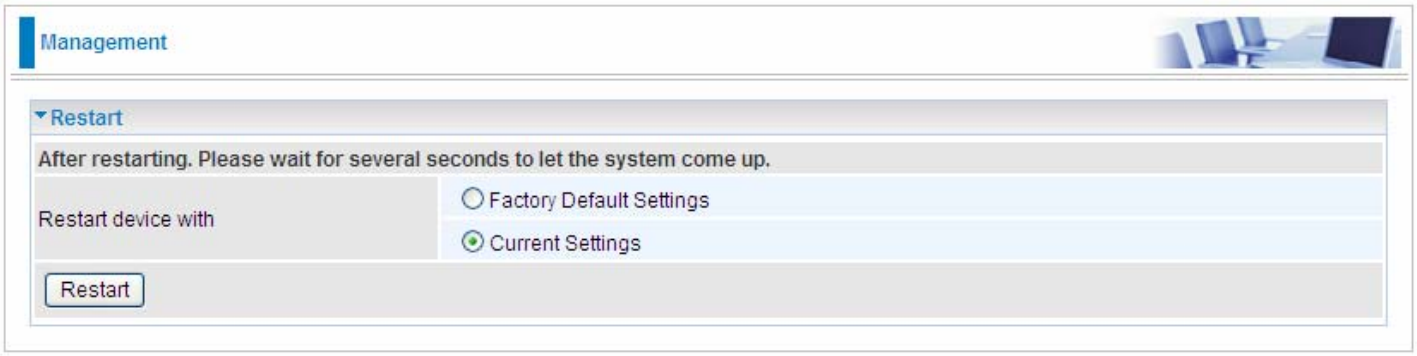
Click **Backup Settings**, a window appears, click save , then browse the location where you want to save the backup file.

Click **Browse** and browse to the location where your backup file is saved, the click **Open.** Then in the above page, click **Update Settings**, the following process indicating screen will appear. Let it update to 100%, it will automatically turn to the Device Info page.

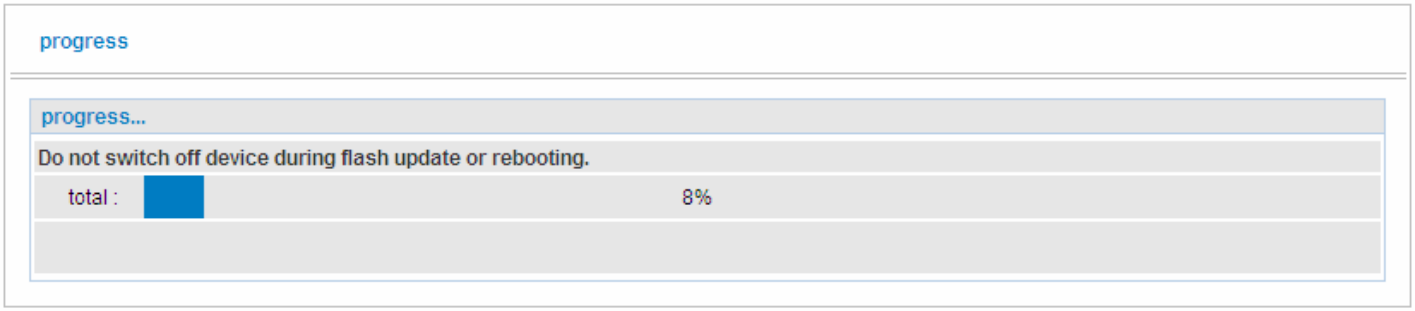


Restart

This section lets you restart your router if necessary. Click Restart in the low right corner of each configuration page.



If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select Factory Default Settings to reset to factory default settings. Or you just want to restart after the current setting, the select the Current Settings, and Click Restart.



Chapter 5: Troubleshooting

If your router is not functioning properly, please refer to the suggested solutions provided in this chapter. If your problems persist or the suggested solutions do not meet your needs, please kindly contact your service provider or Billion for support.

Problems with the router

Problem	Suggested Action
None of the LEDs is on when you turn on the router	Check the connection between the router and the adapter. If the problem persists, most likely it is due to the malfunction of your hardware. Please contact your service provider or Billion for technical support.
You have forgotten your login username or password	Try the default username "admin" and password "admin". If this fails, you can restore your router to its factory settings by pressing the reset button on the device rear side.

Problems with WAN interface

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

Problem with LAN interface

Problem	Suggested Action
Cannot PING any PC on LAN	Check the Ethernet LEDs on the front panel. The LED should be on for the port that has a PC connected. If it does not lit, check to see if the cable between your router and the PC is properly connected. Make sure you have first uninstalled your firewall program before troubleshooting.
	Verify that the IP address and the subnet mask are consistent for both the router and the workstations.

Appendix: Product Support & Contact

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

Contact Billion

Worldwide:

http://www.billion.com

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

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