User's Manual

802.11n Wireless ADSL 2/2+ Router

► **ADN-4102**

www.PLANET.com.tw

Copyright

PLANET makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not PLANET, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, PLANET reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio technician for help.

FCC Caution

To assure continued compliance, use only shielded interface cables when connecting to computer or peripheral devices. Any changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this Device must accept any interference received, including interference that may cause undesired operation.

Federal Communication Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

CE Mark Warning

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

WEEE Regulation

To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

Revision

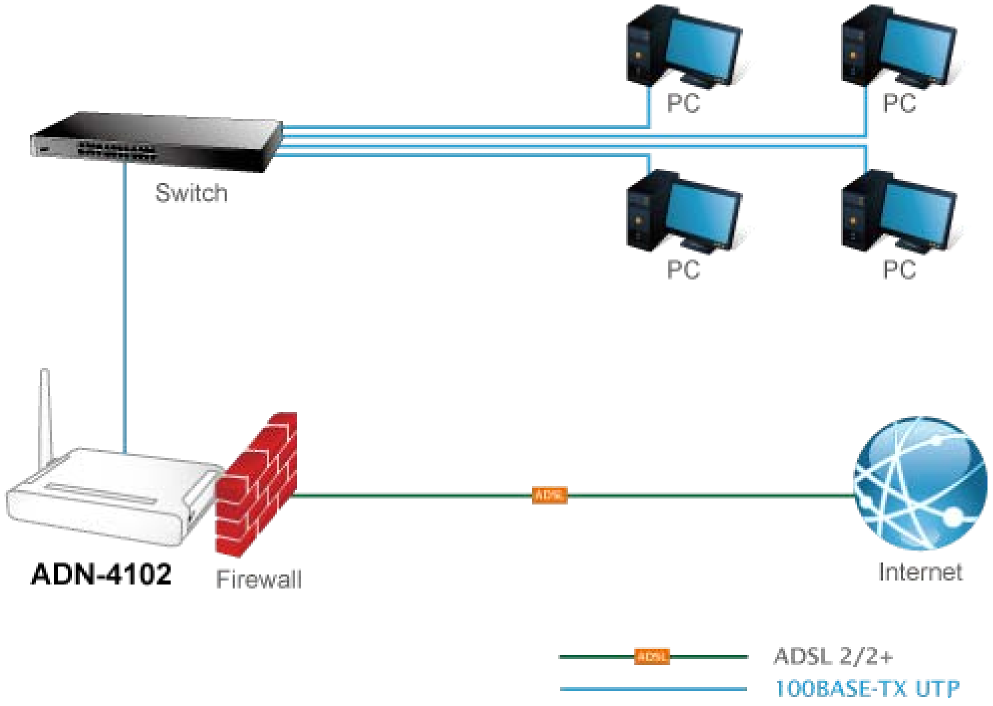
User’s Manual of 802.11n Wireless ADSL2/2+ Router
Model: ADN-4102
Rev: 1.0 (July 2015)
Part No. EM-ADN-4102_v1.0

Contents

Chapter 1. Overview

Built-in Firewall to Have Safe Internet Surfing

PLANET ADN-4102 is a Wireless ADSL 2/2+ Router compliant with 802.11n and features 1T1R MIMO antenna technology. The ADN-4102's built-in parental controls is to limit children's online time – be it computing or gaming, thus creating a safer computing environment for children. In Annex M mode, the ADN-4102 provides transmission rates up to 24Mbps downstream and 3.5Mbps upstream with ADSL 2+ support. Through integration with single chipset to reduce boot time, the ADN-4102 brings more powerful performance to users. The ADN-4102 also supports PPPoA (RFC 2364 -- PPP over ATM Adaptation Layer 5), RFC 2684 encapsulation over ATM (bridged or routed), PPP over Ethernet (RFC 2516), and IPoA (RFC1483) to establish a connection with ISP.



High-speed 802.11n Wireless Access

With built-in IEEE 802.11b/g and 802.11n wireless network capabilities, the ADN-4102 allows any computer and wireless-enabled network device to connect it without additional cabling. Smart phones also jump on the bandwagon of wireless networking. Its 802.11n wireless capability gives you a high-speed wireless transmission up to 150Mbps. With a compatible wireless LAN card installed in your PC, any file can be transferred at a very high speed. The radio coverage is also doubled than before, offering you the high-speed wireless connection, even in a spacious office or house.

One-touch Secure Wireless Connection

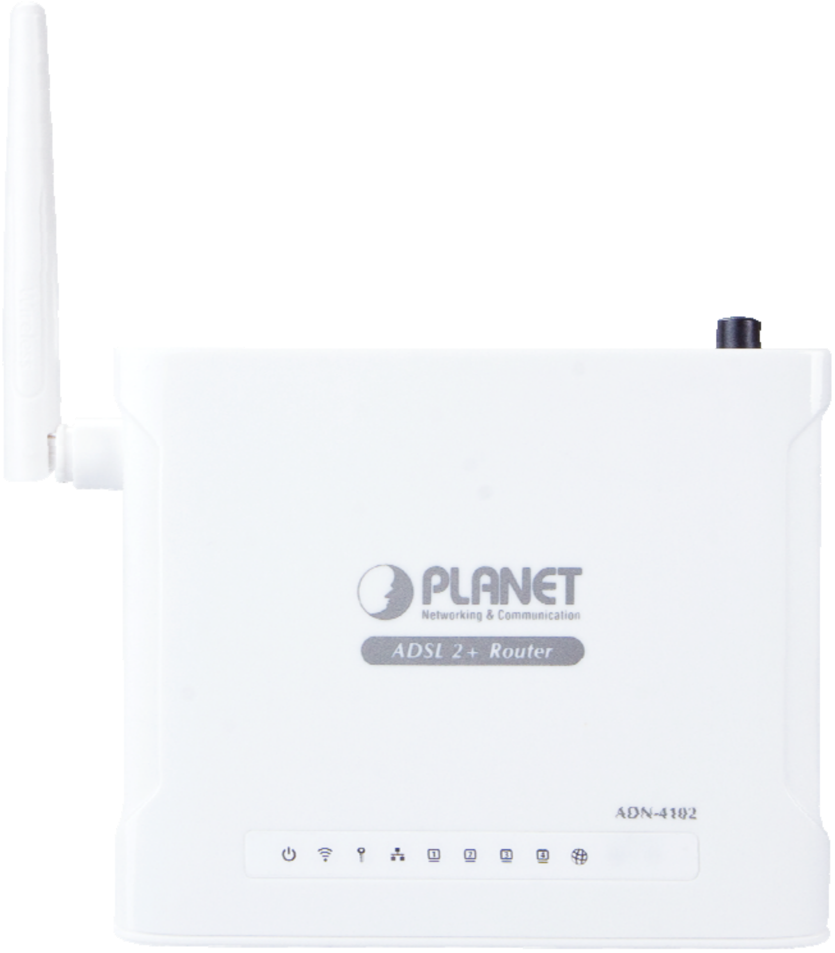
To secure the wireless communication, the ADN-4102 features the most up-to-date encryptions like WEP, WPA-PSK and WPA2-PSK. The ADN-4102 also supports WPS configuration with PBC/PIN type for users to easily connect to a secure wireless network with no need of complicated settings.

WPS (Wi-Fi Protected Setup)
Quick & Easy Wireless Connection
Step 1
WPS
Click
Step 2
Press
WPS Button
Step 3
Connected

4-in-1 (4 Multiple SSIDs) Wireless Networking Infrastructures

Up to four wireless networking with management can be established by the ADN-4102. This flexibility makes it the best choice for SOHO wireless networking in restaurants, hotels, bookstores and more.

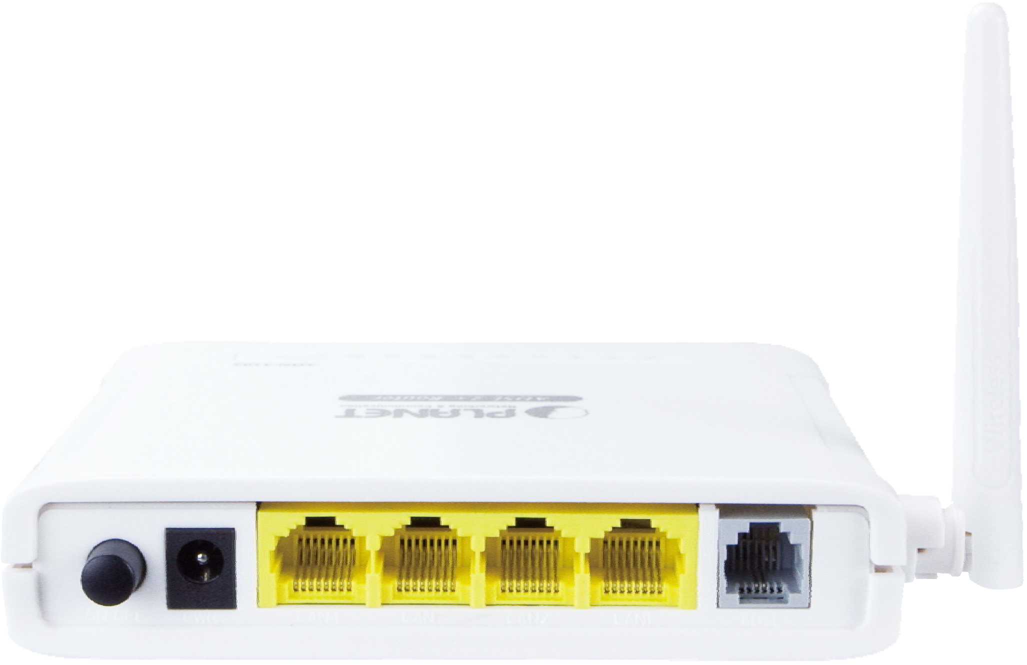
Front Panel

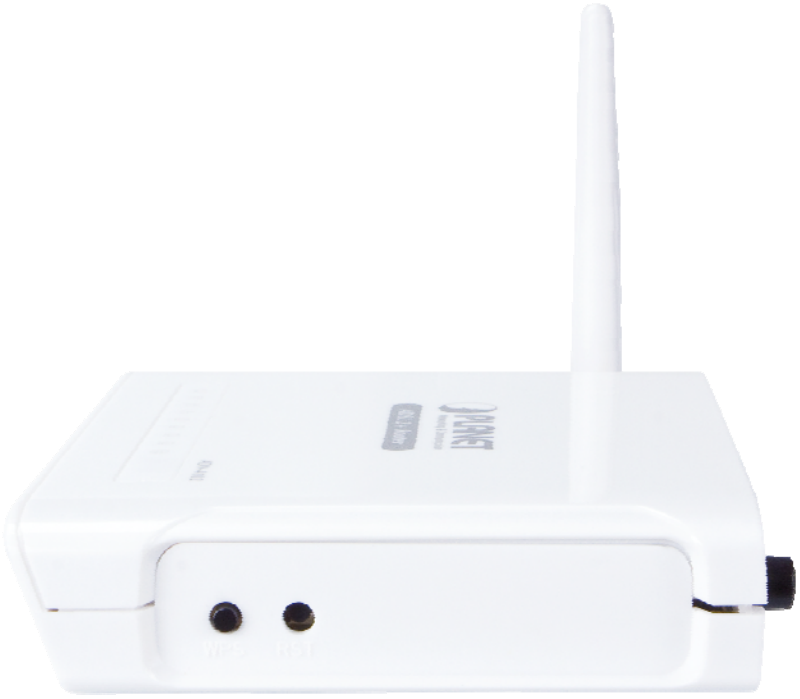


LED Indicator

LED	State	Description
PWR	Green	Indicates when the ADSL Router is powered on. The LED will remain on.
	Off	When the router is powered off
DSL	Green	When DSL port is connected by Ethernet cable, the LED remains ON.
	Flashing	Modem is trying to establish a connection to telecom’s network
Internet	Off	No Internet connection.
	Green	Indicates when the router is connected to a DSLAM. The LED will blink rapidly when Internet traffic is transmitted or received.
LAN 1-4	Green	Indicates when a networking device is connected to a wired port on the back of the ADN-4102. The LED will blink rapidly when wired data traffic is transmitted or received.
	Flashing	TX or RX activity
Wi-Fi	Green	Blinks rapidly when wireless data traffic is transmitted or received over the wireless network.
	Flashing	The wireless data is transmitting.
	Off	The wireless Interface is disabled.
WPS	Off	WPS service is not in use or WPS is set up successfully.
	Green	Wi-Fi Protected Setup activity. When the WPS mode is activated, the Power LED blinks as it awaits a connection

Rear Panel





Port and Button Definition

Connector	Description
POWER Button	The power button is for turning on or off the router.
WPS	Pressing for 5 seconds and then releasing it can enable the WPS function of the wireless clients. The ADN-4102 and clients will automatically configure the security key and connect directly.
RST	The reset button can restore the default settings of device. To restore factory defaults, keep the device powered on and push a paper clip into the hole. Press down the button for over 5 seconds and then release.
PWR	Power connector with 12V DC, 0.5A
LAN 1-4	Router is successfully connected to a device through the corresponding port (1, 2, 3, or 4). If the LED is flashing, the ADN-4102 is actively sending or receiving data over that port.
ADSL	The RJ11 connector allows data communication between the modem and the ADSL network through a twisted-pair phone wire.

1.1 System Requirements

Make sure first that you have prepared these following items to guarantee the router can work normally.

- Services subscriptions.
- An 10/100Mbps Ethernet card installed on your PC.
- Hub or Switch. (Attached to several PCs through one of Ethernet interfaces on the device).
- Operating system: Windows 7, Windows 2000, or Windows XP.
- Internet Explorer V8.0 or higher, or firefox v23 or higher.

1.2 Features

The device supports the following features:

Internet Access Features

- Shared Internet Access through a single external IP address
- Supports NAT (Network Address Translation)
- Built-in ADSL 2/2+ Modem for all common ADSL connections
- Various WAN connections - PPPoE, PPPoA, Direct Connection Supports Fixed and Dynamic IP Address

Advanced Internet Functions

- Supports Virtual Servers with quick and easy setup
- DMZ Support to allow unrestricted 2-way communication with servers or individual users on the Internet
- Simple firewall with NAT technology
- Provides options for access control from Internet like Telnet, FTP, TFTP, HTTP, and ICMP services
- Supports IP/ MAC/ Application/ URL filtering
- Universal Plug and Play (UPnP) to allow automatic discovery and configuration of the broadband router
- Dynamic DNS Support, allowing users to connect a server to the LAN by using a Domain Name even if you have a dynamic IP address
- Supports Planet Dynamic DNS service
- RIP v1/v2 Routing support

LAN Features

- 4-port 10/100BASE-TX switching
- DHCP (Dynamic Host Configuration Protocol) Server Support
- Supports IPv6/IPv4
- Optional NAT ALG, offering 9 items that can be selected from web UI, including VPN passthrough, SIP, H.323, ICQ, etc
- Parental Controls -- Limit specific PC with IP or MAC address to the time and programs available for internet connection

Wireless Features

- IEEE 802.11b/g/n Wireless Standard compliant
- Provides data rate up to 150Mbps via 802.11n technology

- WEP (Wired Equivalent Privacy) Support with key sizes of 64 bit and 128 bit
- WPS (Wi-Fi Protected Setup) Push Button Control for easy wireless connection without configurations
- WPA-PSK Support: WPA-PSK_TKIP and WAP-PSK_AES encryptions
- Wireless MAC Access Control to ensure that only trusted wireless stations can access your LAN

1.3 Specifications

Product		802.11n Wireless ADSL 2/2+ 4-port Router
Model		ADN-4102A
Hardware		
Standard		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,Multimode (ITU G.994.1) Capable of ADSL2 Standard - G.dmt.bis (ITU G.992.3) Capable of ADSL2+ Standard - G.dmt.bisplus (ITU G.992.5) - Reach Extended ADSL (RE ADSL) Supports Annex A, M, L
Protocol		RFC 2364 - PPP over ATM (LLC/VCMUX) RFC 2516 - PPP over Ethernet (LLC/VCMUX) RFC 1483 - Classic IP over ATM (LLC/VCMUX) RFC 2684 - Bridged IP over ATM (LLC/VCMUX) RFC 2684 - Routed IP over ATM (LLC/VCMUX)
AAL and ATM Support		Supports up to 8 PVCs ATM Forum UNI 3.1/4.0 PVC VC and LLC Multiplexing Integrated ATM AAL5 support (UBR,CBR,VBR-rt and VBR-nrt) 0~255 VPI plus 1~65535 VCI address range OAM F4 & F5 Segment end-to-end loop-back, AIS, and RDI OAM cells
Ports	**LAN**	4 x Ethernet (10/100Mbps, auto-negotiation, auto MDI/MDI-X)
	WLAN	1 x 802.11b/g/n Access Point with one 2dBi dipole antenna
	WAN	1 x RJ11
LED Indicators		PWR, Link, Data, LAN 1~4, WLAN, WPS
Button		Reset, WPS, Power
Max. Concurrent Sessions		2048
Wireless Standard		IEEE 802.11b, g and 802.11n
Wireless Frequency		2.4 to 2.4835GHz (Industrial Scientific Medical Band)
Wireless Channels		Maximum 14 channels, depending on regulatory authorities

Wireless Data Encryption	64 bit/128 bit WEP, WPA-PSK/WPA2-PSK and WPS PBC
Wireless Data Rate	Maximum up to 150 Mbps IEEE 802.11b: 1/2/5.5/11Mbps IEEE 802.11g: 6/9/12/18/24/36/48/54Mbps IEEE 802.11n: 14/29/43/58/87/116/130/144Mps in 20MHz 30/60/90/120/150Mbps in 40MHz
RF Modulation	IEEE 802.11b mode: DSSS (CCK,QPSK,BPSK) IEEE 802.11g mode: OFDM (BPSK,QPSK,16QAM,64QAM) HT20 and HT40: 64 QAM, 16QAM, QPSK, BPSK
Transmit Power	IEEE 802.11b: 16.5dBm ± 1.5dBm IEEE 802.11g: 14dBm ± 1.5dBm IEEE 802.11n HT20M:13dbm ± 1.5dBm IEEE 802.11n HT40M: 13dbm ± 1.5dBm
Receiver Sensitivity	IEEE 802.11b: < -80dBm IEEE 802.11g: < -68dBm IEEE 802.11n HT20M: < -64dbm IEEE 802.11n HT40M: < -61dbm
Software	
Protocols/Features	NAT supports multimedia applications NAT, Static Routing, and RIPv1/2 Transparent Bridging Dynamic Domain Name System (DDNS) SNTP DNS relay and IGMP proxy DMZ and Virtual Server Quality of Service (QoS) for Traffic Prioritization TR-069 Ready UPnP
Security	PPP over PAP (Password Authentication Protocol, RFC 1334) PPP over CHAP (Challenge Authentication Protocol, RFC 1994) DoS Protection Access Control ACL (Access Control) IP / MAC / URL Filter Stateful Packet Inspection (SPI) Firewall Password protection for system management
Management	Web-based configuration Embedded Telnet server for remote and local management Firmware upgraded and configuration data upload/download via Web Support DHCP Server/Client/Relay Built-in diagnostic tool TR-069
Environment Specifications	
Dimensions (W x D x H)	117 x 100 x 25 mm

Power	12V DC, 0.5A
Temperature and Humidity	Operating temperature: 0 ~ 50 degrees C Storage temperature: -10 ~ 70 degrees C Humidity: 10 ~ 95% non-condensing
Emission	FCC, CE

Chapter 2. Hardware Installation

Connect the **LINE** interface of the device and the **DSL** interface of the splitter with a telephone cable. Connect the phone set to the **Phone** interface of the splitter through a telephone cable. Connect the input cable to the **LINE** interface of the splitter.

The splitter has three interfaces:

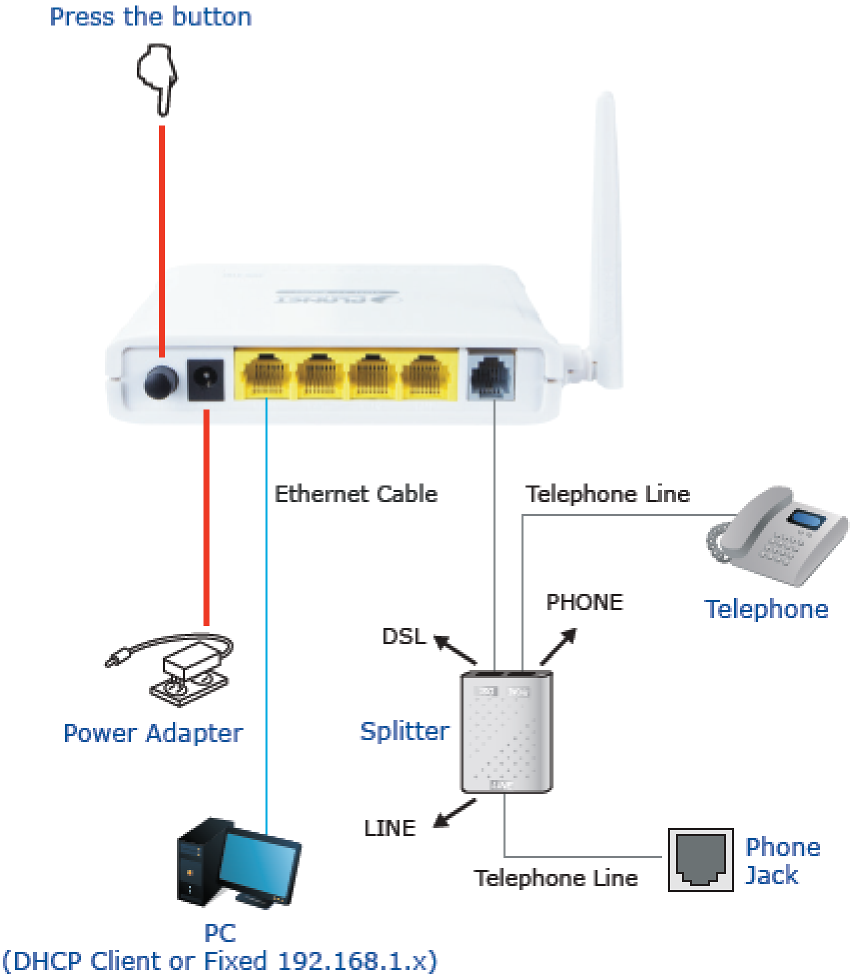
- **LINE**: Connect to a wall phone interface (RJ-11 jack).
- **DSL**: Connect to the DSL interface of the device.
- **Phone**: Connect to a telephone set.

Connect the **LAN** interface of the device to the network card of the PC through an Ethernet cable (MDI/MDIX).

Note	Use the twisted-pair cable to connect the hub or switch.

Insert one end of the power adapter to the wall outlet and connect the other end to the **POWER** interface of the device.

The following figure shows the application diagram for the connection of the router, PC, splitter and the telephone sets.



Chapter 3. Web Configuration

This chapter describes how to configure the device by using the Web-based configuration utility.

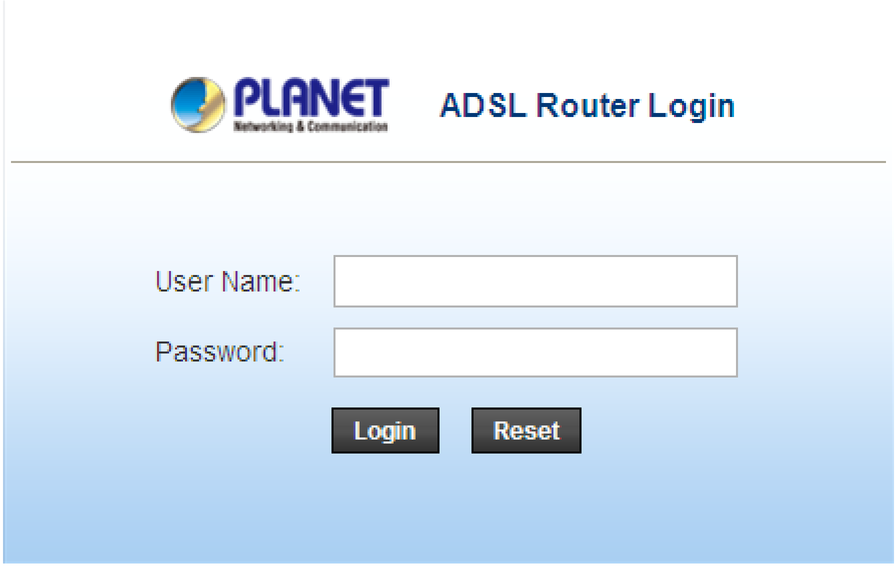
3.1 Accessing the Router

The following describes how to access the device for the first time in details.

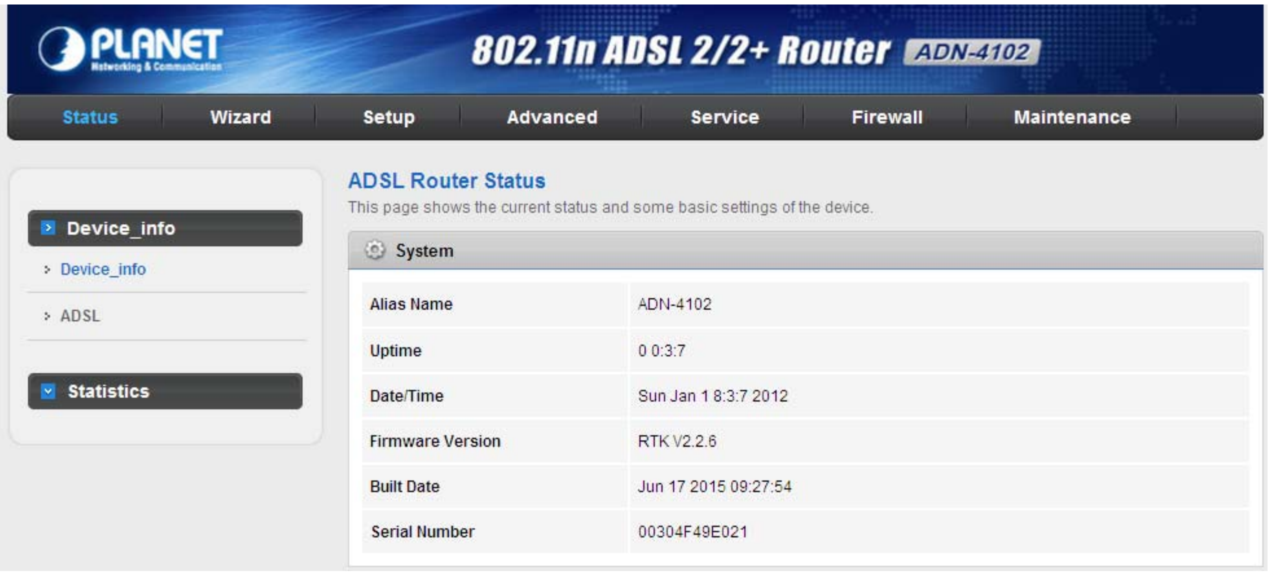
Step 1 Open the Internet Explorer (IE) browser and enter **http://192.168.1.1** in the address bar.

Step 2 On the **Login** page that is displayed, enter the username and password, and then click **OK**.

- The username and password of the super user are **admin** and **admin**.



After logging in, the page shown in the following figure appears. You can check, configure and modify all the settings.



ADSL Router Status

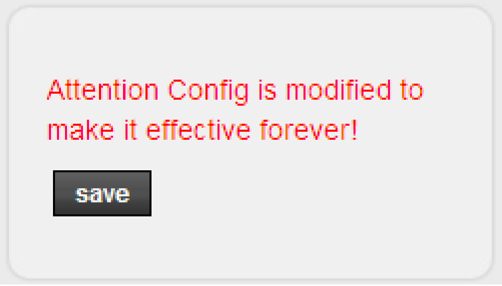
This page shows the current status and some basic settings of the device.

System

Alias Name	ADN-4102
Uptime	0 0:3:7
Date/Time	Sun Jan 1 8:3:7 2012
Firmware Version	RTK V2.2.6
Built Date	Jun 17 2015 09:27:54
Serial Number	00304F49E021

Note

On the Web configuration page, you can click **Apply Changes** to save the settings temporarily. If you want to save the settings on this page permanently, clicks "save" that appears at the bottom of the Web page after the configuration.



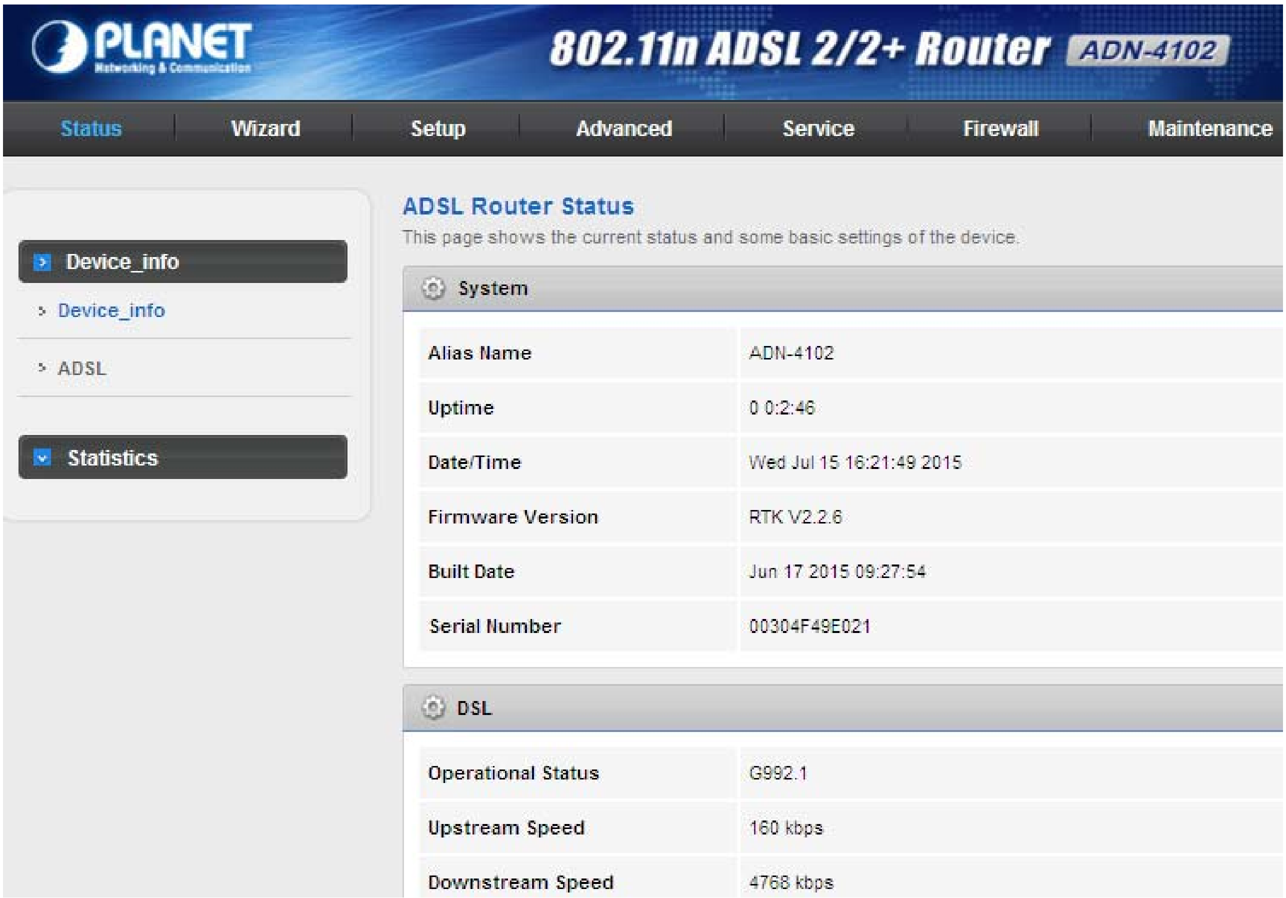
Attention Config is modified to make it effective forever!

3.2 Status

In the navigation bar, choose **Status**. On the **Status** page that is displayed contains: **Device Info**, **ADSL** and **Statistics**.

3.2.1 Device Information

Choose **Status** > **Device Info** and the page displayed shows the current status and some basic settings of the router, such as software version, DSP version, uptime, upstream speed, and downstream speed.



ADSL Router Status

This page shows the current status and some basic settings of the device.

System

Alias Name	ADN-4102
Uptime	0 0:2:46
Date/Time	Wed Jul 15 16:21:49 2015
Firmware Version	RTK V2.2.6
Built Date	Jun 17 2015 09:27:54
Serial Number	00304F49E021

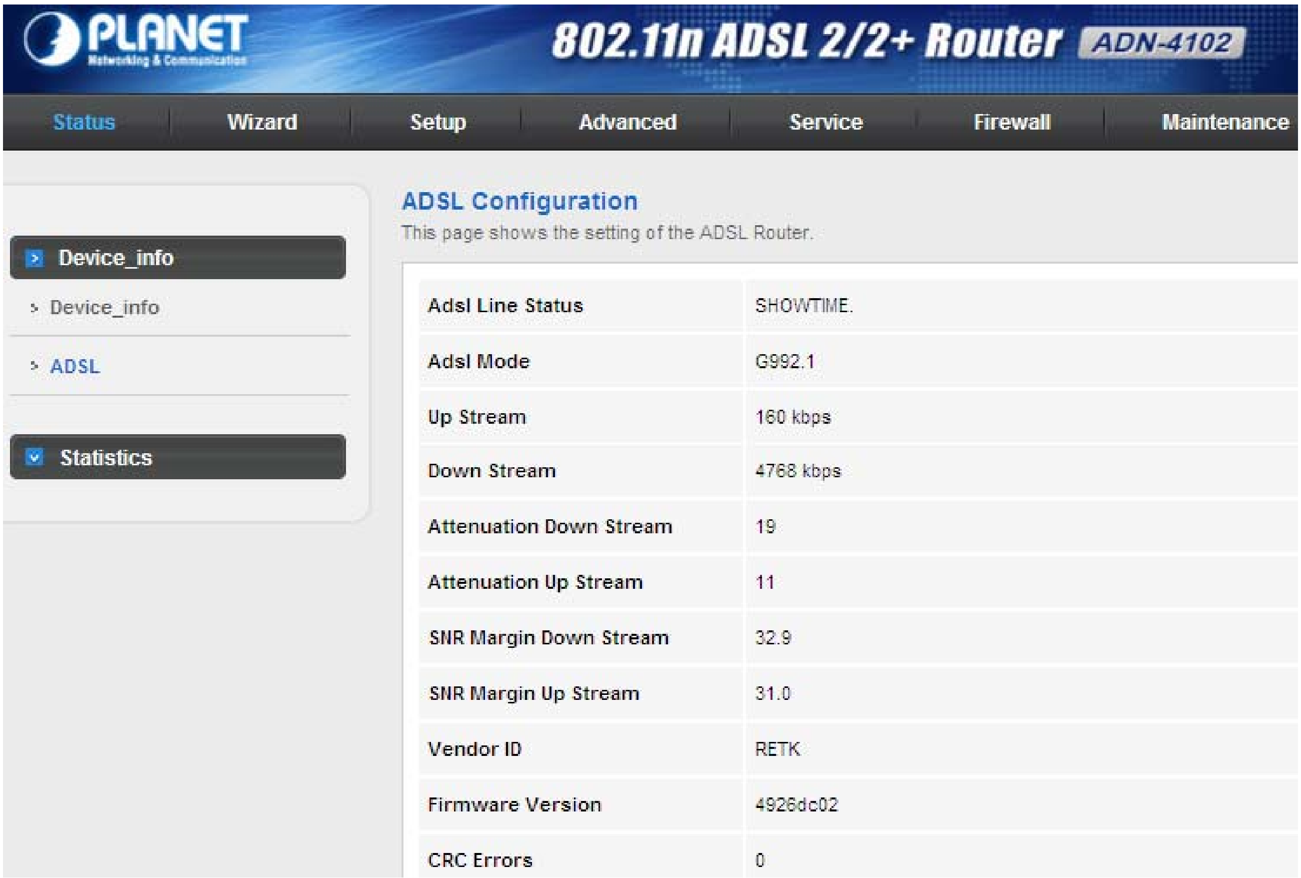
DSL

Operational Status	G992.1
Upstream Speed	160 kbps
Downstream Speed	4768 kbps

3.2.2 ADSL

Click **ADSL** in the left pane and the page shown in the following figure appears. On this page, you can view the ADSL line status, upstream rate, downstream rate and other information.

Choose **Status** > **LAN** and the page displayed shows some basic LAN settings of the router. On this page, you can view the LAN IP address, DHCP server status, MAC address, and DHCP client table.



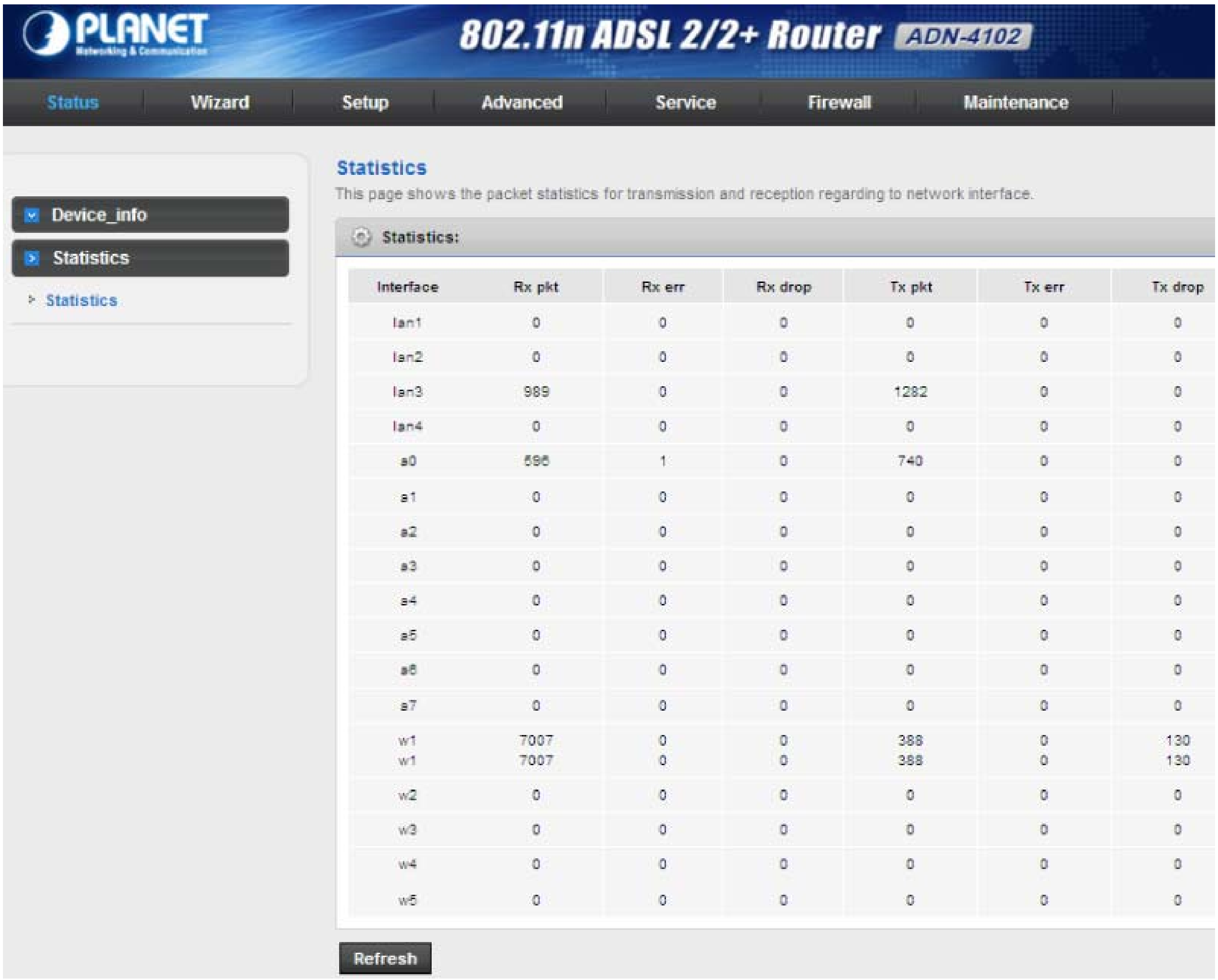
ADSL Configuration

This page shows the setting of the ADSL Router.

Adsl Line Status	SHOWTIME.
Adsl Mode	G992.1
Up Stream	160 kbps
Down Stream	4768 kbps
Attenuation Down Stream	19
Attenuation Up Stream	11
SNR Margin Down Stream	32.9
SNR Margin Up Stream	31.0
Vendor ID	RETK
Firmware Version	4926dc02
CRC Errors	0

3.2.3 Statistics

Choose **Status** > **Statistics.** Click **Statistics** in the left pane and the page shown in the following figure appears. On this page, you can view the statistics of each network port.



Statistics

This page shows the packet statistics for transmission and reception regarding to network interface.

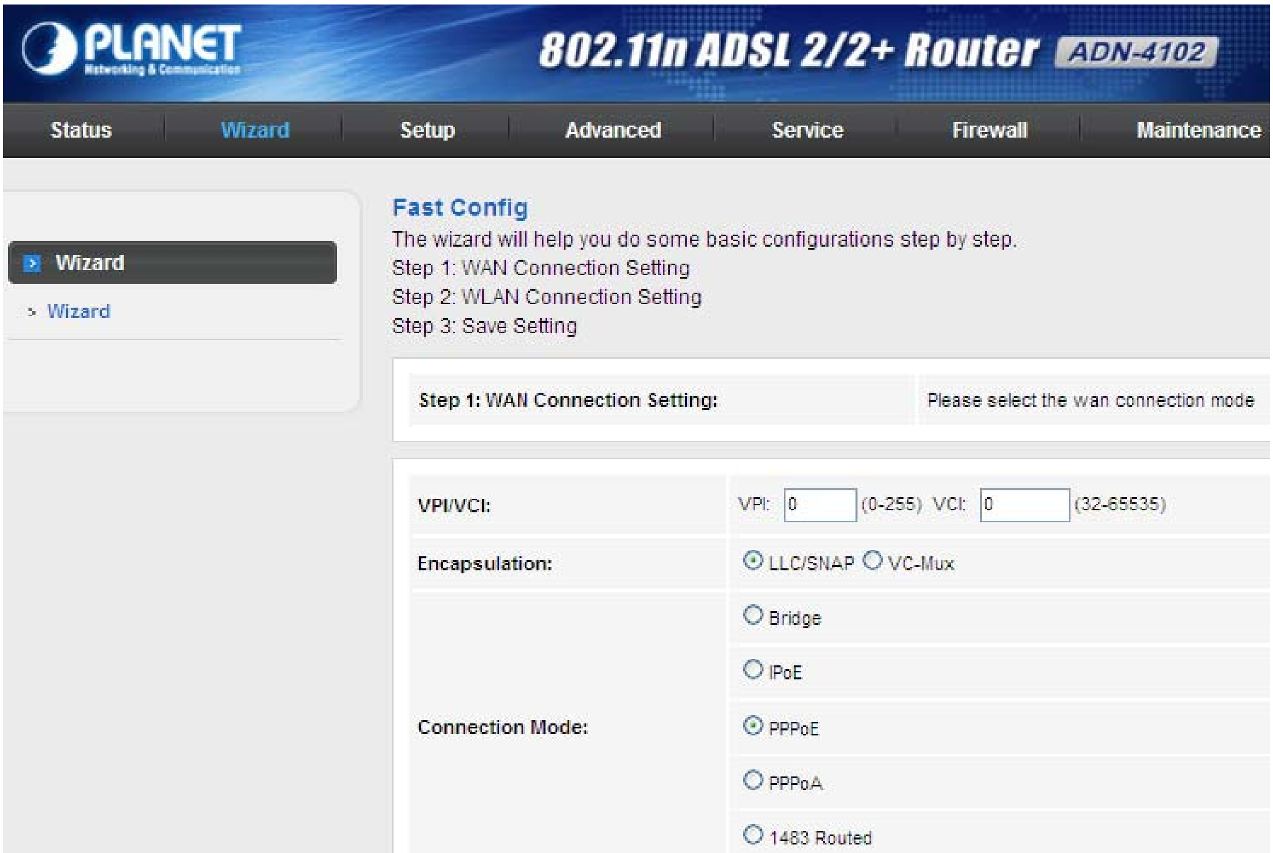
Statistics:

Interface	Rx pkt	Rx err	Rx drop	Tx pkt	Tx err	Tx drop
lan1	0	0	0	0	0	0
lan2	0	0	0	0	0	0
lan3	989	0	0	1282	0	0
lan4	0	0	0	0	0	0
a0	596	1	0	740	0	0
a1	0	0	0	0	0	0
a2	0	0	0	0	0	0
a3	0	0	0	0	0	0
a4	0	0	0	0	0	0
a5	0	0	0	0	0	0
a6	0	0	0	0	0	0
a7	0	0	0	0	0	0
w1 w1	7007 7007	0 0	0 0	388 388	0 0	130 130
w2	0	0	0	0	0	0
w3	0	0	0	0	0	0
w4	0	0	0	0	0	0
w5	0	0	0	0	0	0

3.3 Wizard

When subscribing to a broadband service, you should be aware of the method by which you are connected to the Internet. Your physical WAN device can be either PPP, ADSL, or both. The technical information about the properties of your Internet connection is provided by your Internet Service Provider (ISP). For example, your ISP should inform you whether you are connected to the Internet using a static or dynamic IP address, and the protocol that you use to communicate on the Internet.

In the navigation bar, choose **Wizard**. The page shown in the following figure appears. The **Wizard** page guides fast and accurate configuration of the Internet connection and other important parameters. The following sections describe these various configuration parameters. Whether you configure these parameters or use the default ones, click **NEXT** to enable your Internet connection.


PLANET Networking & Communication
802.11n ADSL 2/2+ Router ADN-4102
Status
Wizard
Setup
Advanced
Service
Firewall
Maintenance
Wizard
Wizard

Fast Config

The wizard will help you do some basic configurations step by step.
Step 1: WAN Connection Setting
Step 2: WLAN Connection Setting
Step 3: Save Setting

Step 1: WAN Connection Setting:	Please select the wan connection mode

VPI/VCI:	VPI: 0 (0-255) VCI: 0 (32-65535)
Encapsulation:	● LLC/SNAP ○ VC-Mux
Connection Mode:	○ Bridge ○ IPoE ● PPPoE ○ PPPoA ○ 1483 Routed

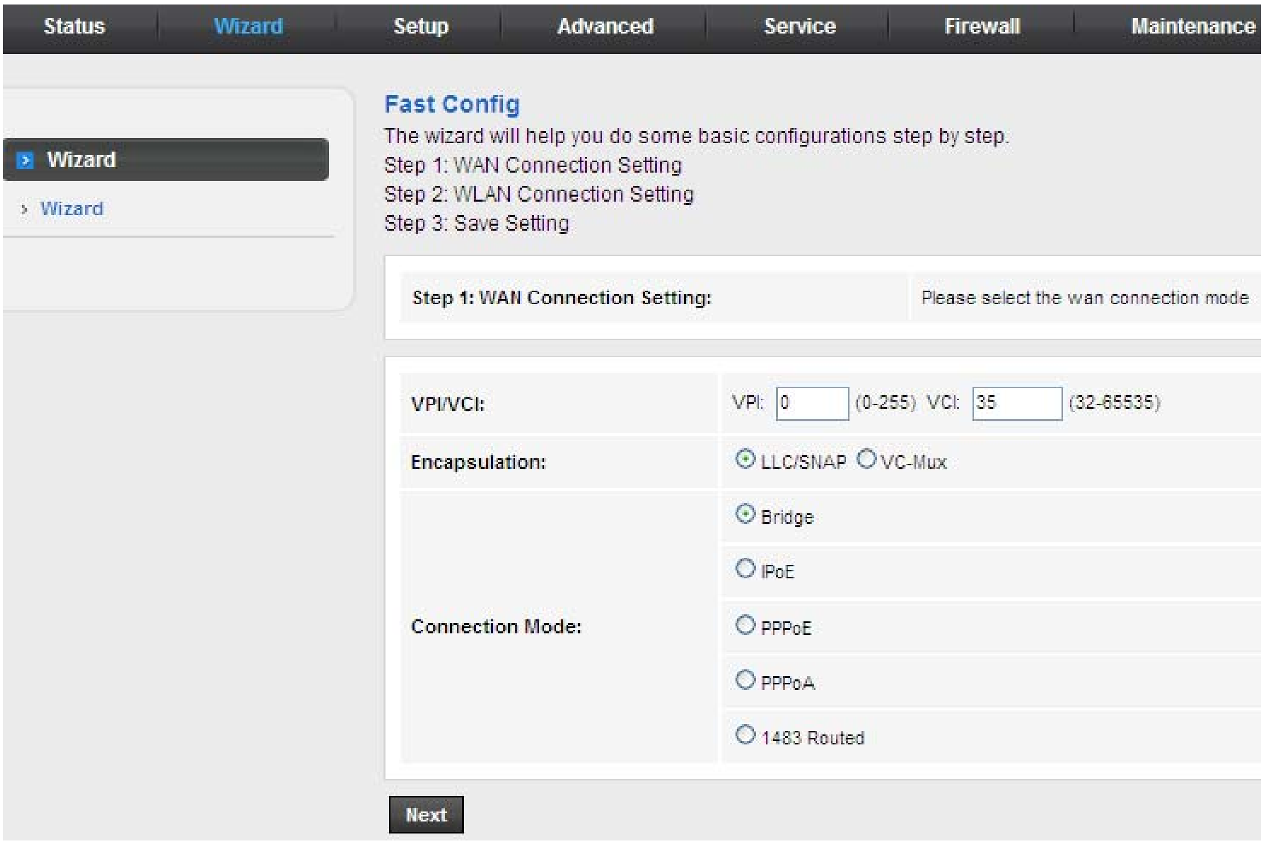
The following table describes the parameters on this page:

Field	Description
VPI	Virtual path identifier (VPI) is the virtual path between two points in an ATM network. Its valid value is in the range of 0 to 255. Enter the correct VPI provided by your ISP. By default, VPI is set to **0**.
VCI	Virtual channel identifier (VCI) is the virtual channel between two points in an ATM network. Its valid value is in the range of 32 to 65535. (0 to 31 is reserved for local management of ATM traffic) Enter the correct VCI provided by your ISP. By default, VCI is set to **0**.

There are five WAN connection types: **Bridged, IPoE (MER), PPP over Ethernet (PPPoE), PPP over ATM (PPPoA)**, **1483 Routed**, and. The following describes them respectively.

Bridge

After setting, click **Next** and the page as shown in the following figure appears.

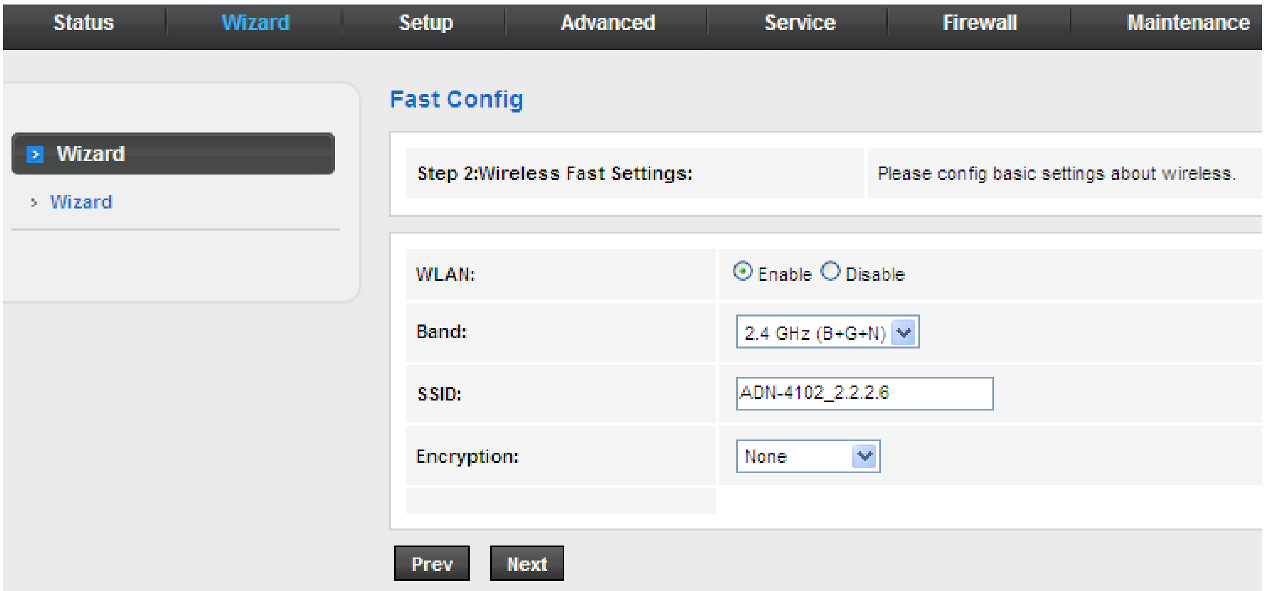


Fast Config

The wizard will help you do some basic configurations step by step.
Step 1: WAN Connection Setting
Step 2: WLAN Connection Setting
Step 3: Save Setting

Step 1: WAN Connection Setting:	Please select the wan connection mode

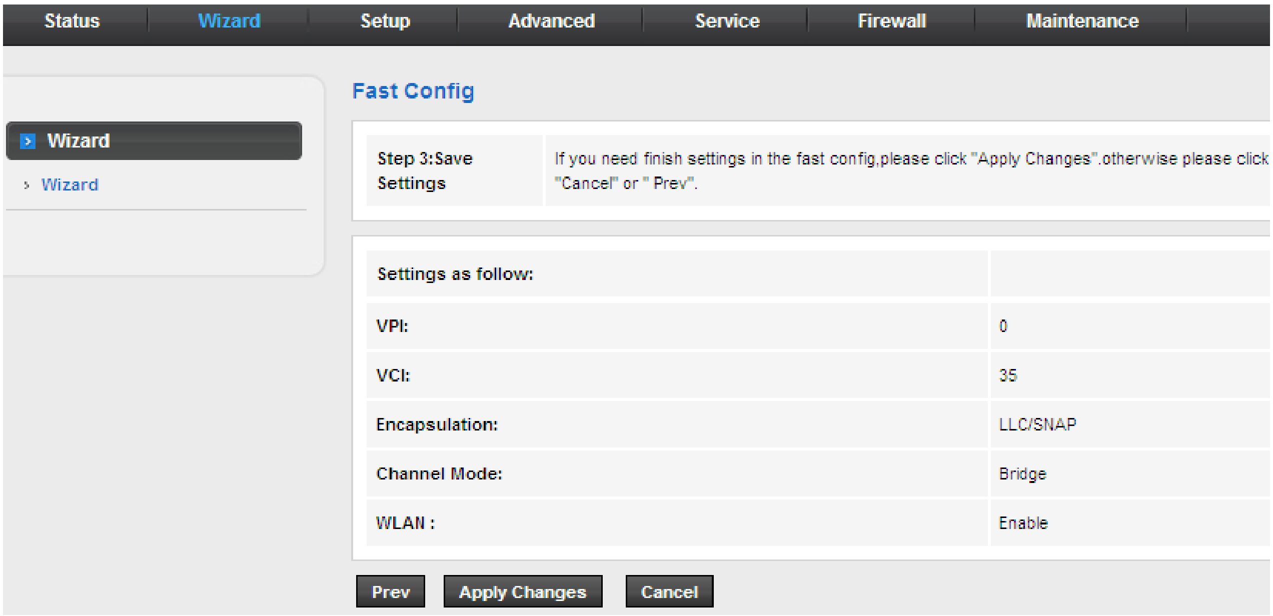
VPI/VCI:	VPI: 0 (0-255) VCI: 35 (32-65535)
Encapsulation:	● LLC/SNAP ○ VC-Mux
Connection Mode:	● Bridge
	○ IPoE
	○ PPPoE
	○ PPPoA
	○ 1483 Routed



Fast Config

Step 2:Wireless Fast Settings:	Please config basic settings about wireless.

WLAN:	● Enable ○ Disable
Band:	2.4 GHz (B+G+N)
SSID:	ADN-4102_2.2.2.6
Encryption:	None



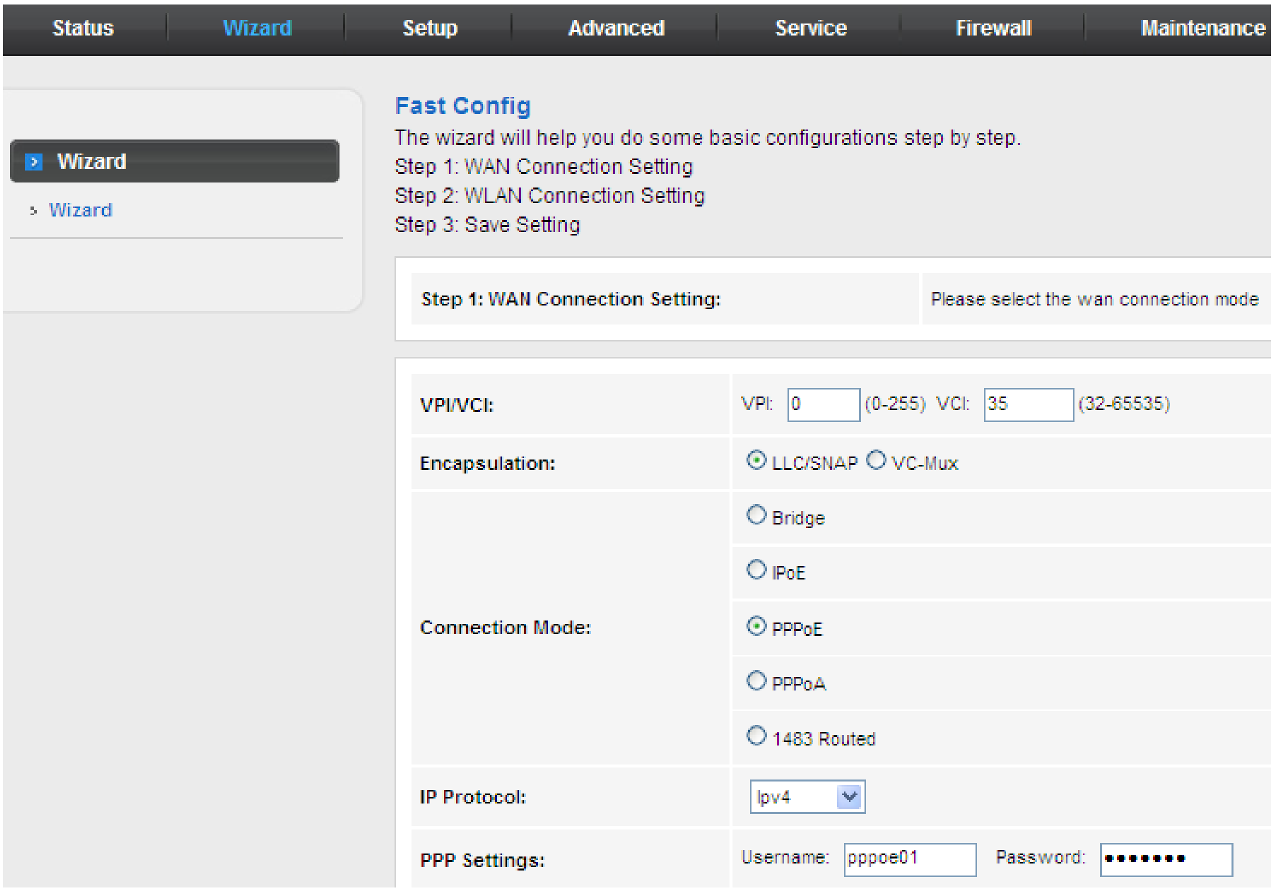
Fast Config

Step 3:Save Settings	If you need finish settings in the fast config,please click "Apply Changes".otherwise please click "Cancel" or " Prev".

Settings as follow:	
VPI:	0
VCI:	35
Encapsulation:	LLC/SNAP
Channel Mode:	Bridge
WLAN :	Enable

PPPoE/PPPoA

On the **Connection Mode** page, set the WAN connection type to **PPP over Ethernet (PPPoE)**, and the encapsulation mode to **LLC/SNAP**.



Fast Config

The wizard will help you do some basic configurations step by step.
Step 1: WAN Connection Setting
Step 2: WLAN Connection Setting
Step 3: Save Setting

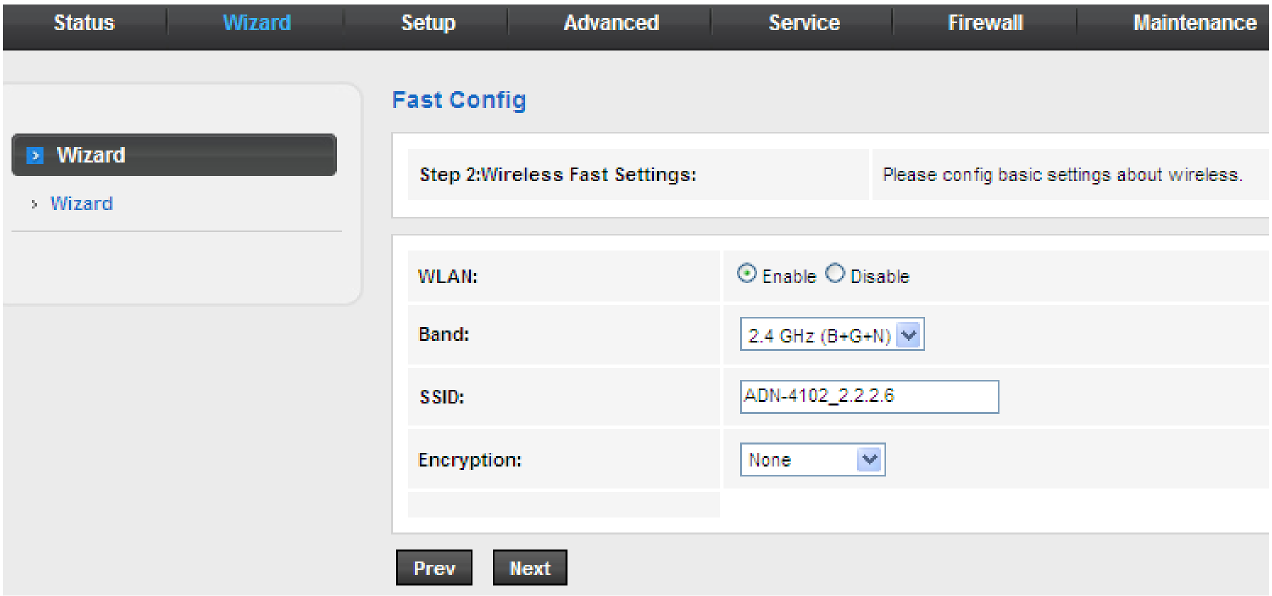
Step 1: WAN Connection Setting:	Please select the wan connection mode

VPI/VCI:	VPI: 0 (0-255) VCI: 35 (32-65535)
Encapsulation:	● LLC/SNAP ○ VC-Mux
Connection Mode:	○ Bridge ○ IPoE ● PPPoE ○ PPPoA ○ 1483 Routed
IP Protocol:	Ipv4
PPP Settings:	Username: pppoe01 Password: ●●●●●●●

Field	**Description**
PPP Username	Enter the username for PPPoE dial-up, which is provided by your ISP.

Field	Description
PPP Password	Enter the password for PPPoE dial-up, which is provided by your ISP.

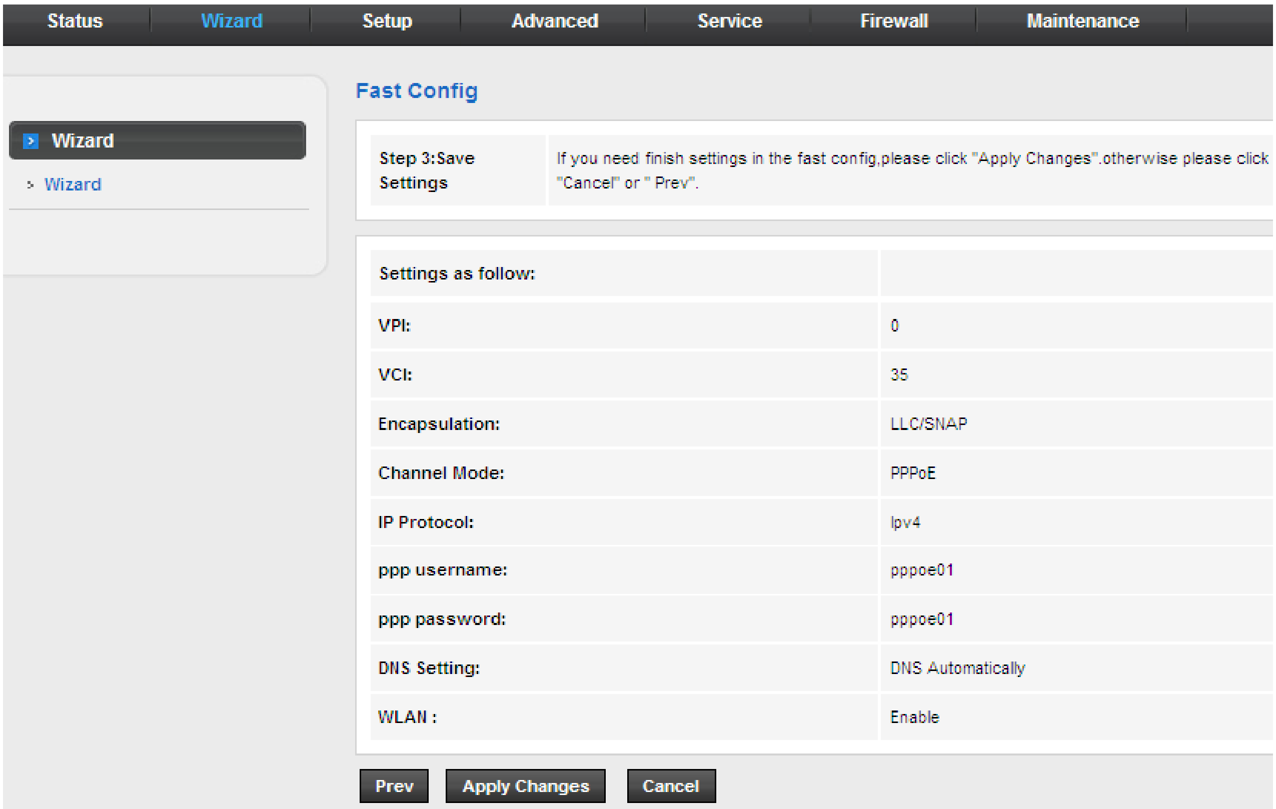
After setting, click **Next** and the page as shown in the following figure appears.



Fast Config

Step 2:Wireless Fast Settings:	Please config basic settings about wireless.

WLAN:	● Enable ○ Disable
Band:	2.4 GHz (B+G+N)
SSID:	ADN-4102_2.2.2.6
Encryption:	None



Fast Config

Step 3:Save Settings	If you need finish settings in the fast config,please click "Apply Changes".otherwise please click "Cancel" or " Prev".

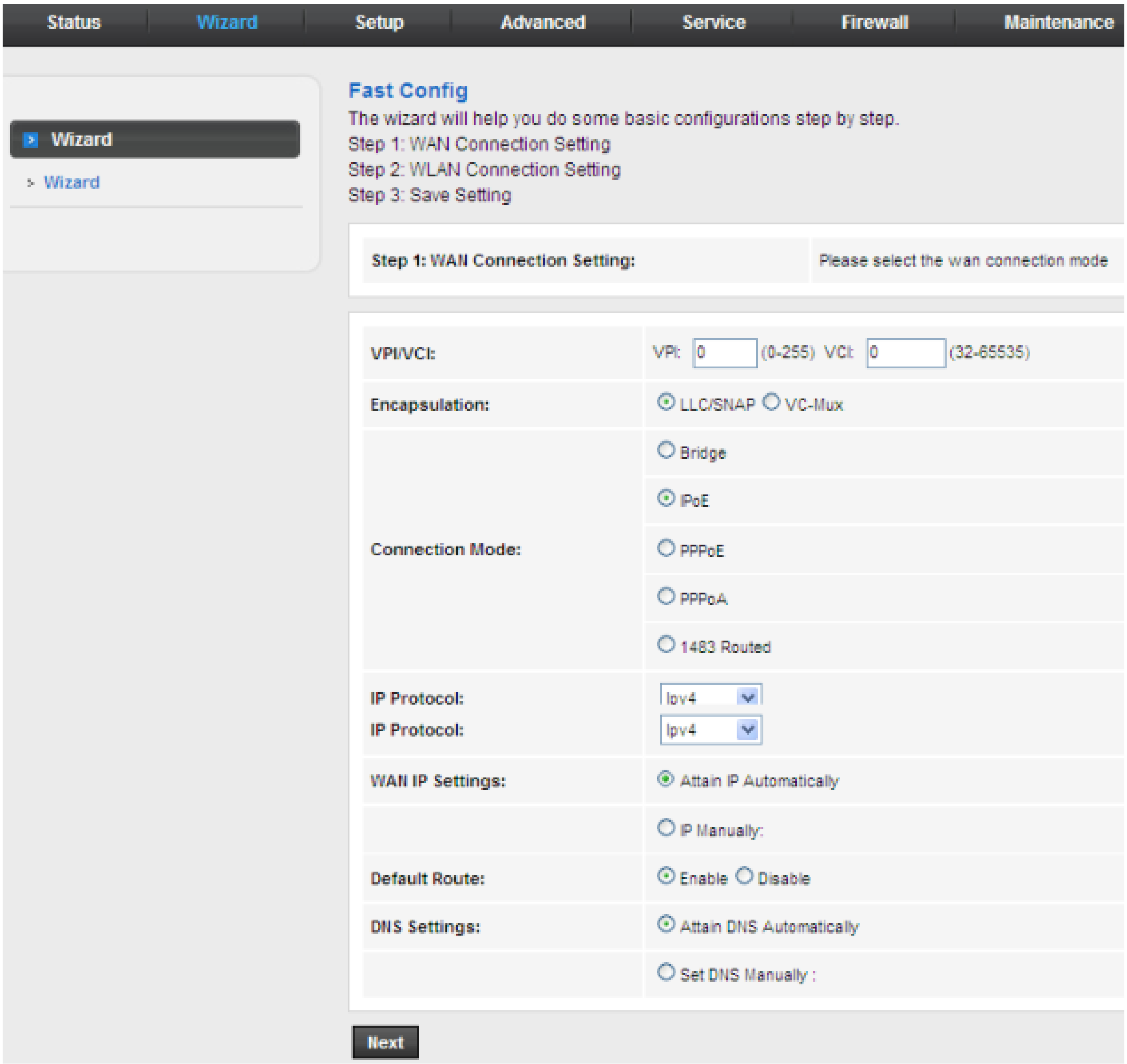
Settings as follow:	
VPI:	0
VCI:	35
Encapsulation:	LLC/SNAP
Channel Mode:	PPPoE
IP Protocol:	Ipv4
ppp username:	pppoe01
ppp password:	pppoe01
DNS Setting:	DNS Automatically
WLAN :	Enable

Note

If the WAN connection type is set to **PPPoA**, the parameters of the WAN connection type are the same as those of **PPPoE**. For the parameters on these pages, refer to the parameter description of **PPPoE**.

IPoE (MER)/1483 Routed

On the **Connection Mode** page, set the WAN connection type to **IPoE,** and the encapsulation mode to **LLC/SNAP**.



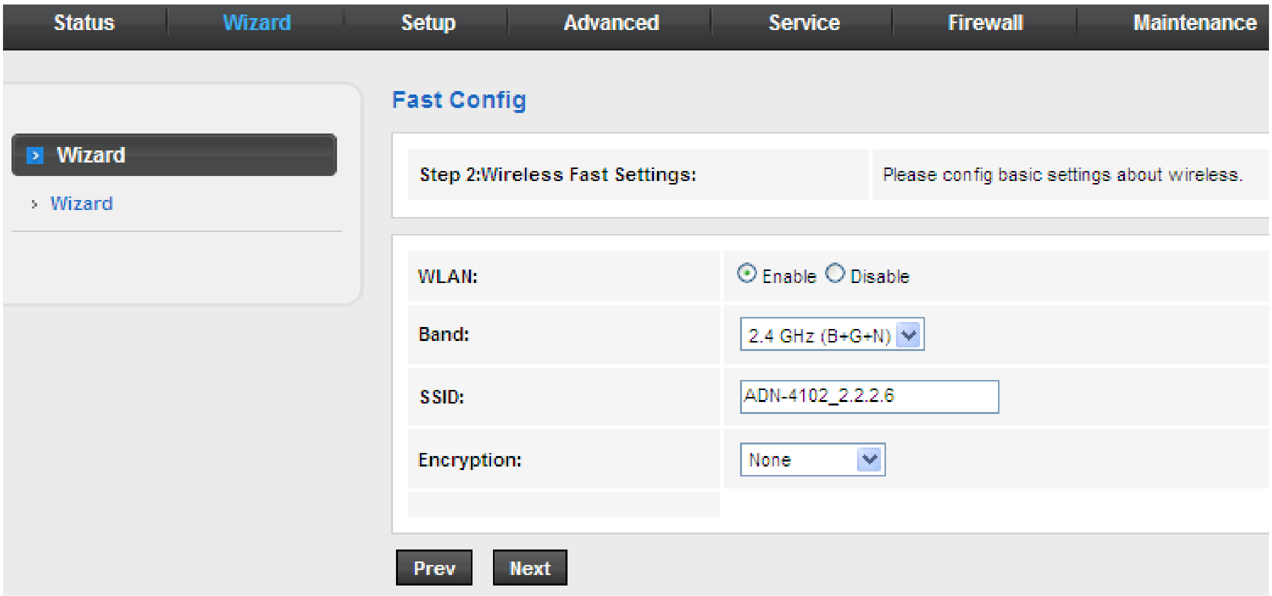
Fast Config

The wizard will help you do some basic configurations step by step.
Step 1: WAN Connection Setting
Step 2: WLAN Connection Setting
Step 3: Save Setting

Step 1: WAN Connection Setting:	Please select the wan connection mode

VPI/VCI:	VPI: 0 (0-255) VCI: 0 (32-65535)
Encapsulation:	● LLC/SNAP ○ VC-Mux
Connection Mode:	○ Bridge ● IPoE ○ PPPoE ○ PPPoA ○ 1483 Routed
IP Protocol: IP Protocol:	Ipv4 Ipv4
WAN IP Settings:	● Attain IP Automatically ○ IP Manually:
Default Route:	● Enable ○ Disable
DNS Settings:	● Attain DNS Automatically ○ Set DNS Manually :

Field	Description
Attain IP Automatically	Select it and DHCP automatically assigns the IP address for WAN connection.
IP Manually	When selecting it, you need to manually enter the IP address, subnet mask, and default gateway for WAN connection, which are provided by your ISP.
Attain DNS Automatically	Select it and DHCP automatically assigns DNS server address.
Set DNS Manually	Select it to manually enter the primary DNS server address and secondary DNS server address.

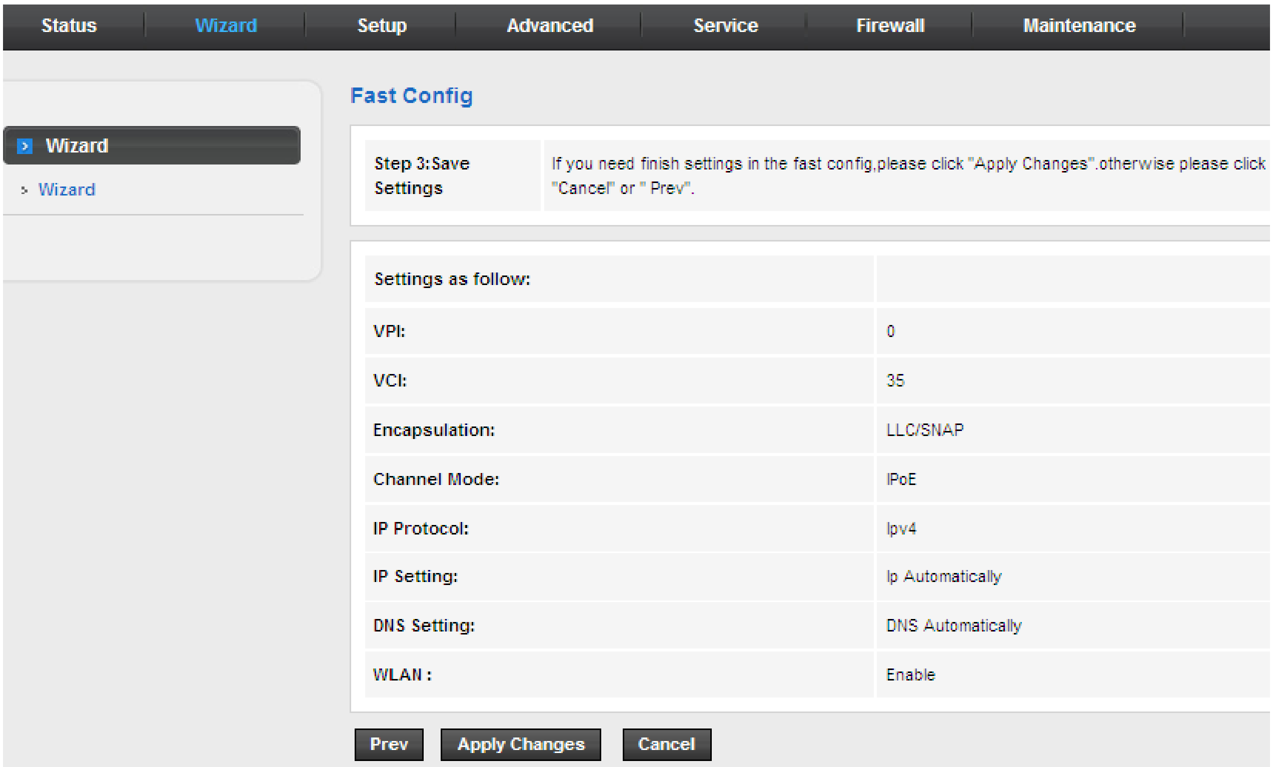


Fast Config

Step 2:Wireless Fast Settings:	Please config basic settings about wireless.

WLAN:	● Enable ○ Disable
Band:	2.4 GHz (B+G+N)
SSID:	ADN-4102_2.2.2.6
Encryption:	None

After setting, click **Next** and the page as shown in the following figure appears.



Fast Config

Step 3:Save Settings	If you need finish settings in the fast config,please click "Apply Changes".otherwise please click "Cancel" or " Prev".

Settings as follow:	
VPI:	0
VCI:	35
Encapsulation:	LLC/SNAP
Channel Mode:	IPoE
IP Protocol:	Ipv4
IP Setting:	Ip Automatically
DNS Setting:	DNS Automatically
WLAN :	Enable

For subsequent configuration, refer to the description in the above section **PPPoE/PPPoA**.

Note

If the WAN connection type is set to **1483 Routed**, the parameters of the WAN connection type are the same as those of **IPoE**. For the parameters on these pages, refer to the parameter description of **IPoE**.

3.4 Setup

In the navigation bar, click Setup. The Setup page that is displayed contains WAN and LAN.

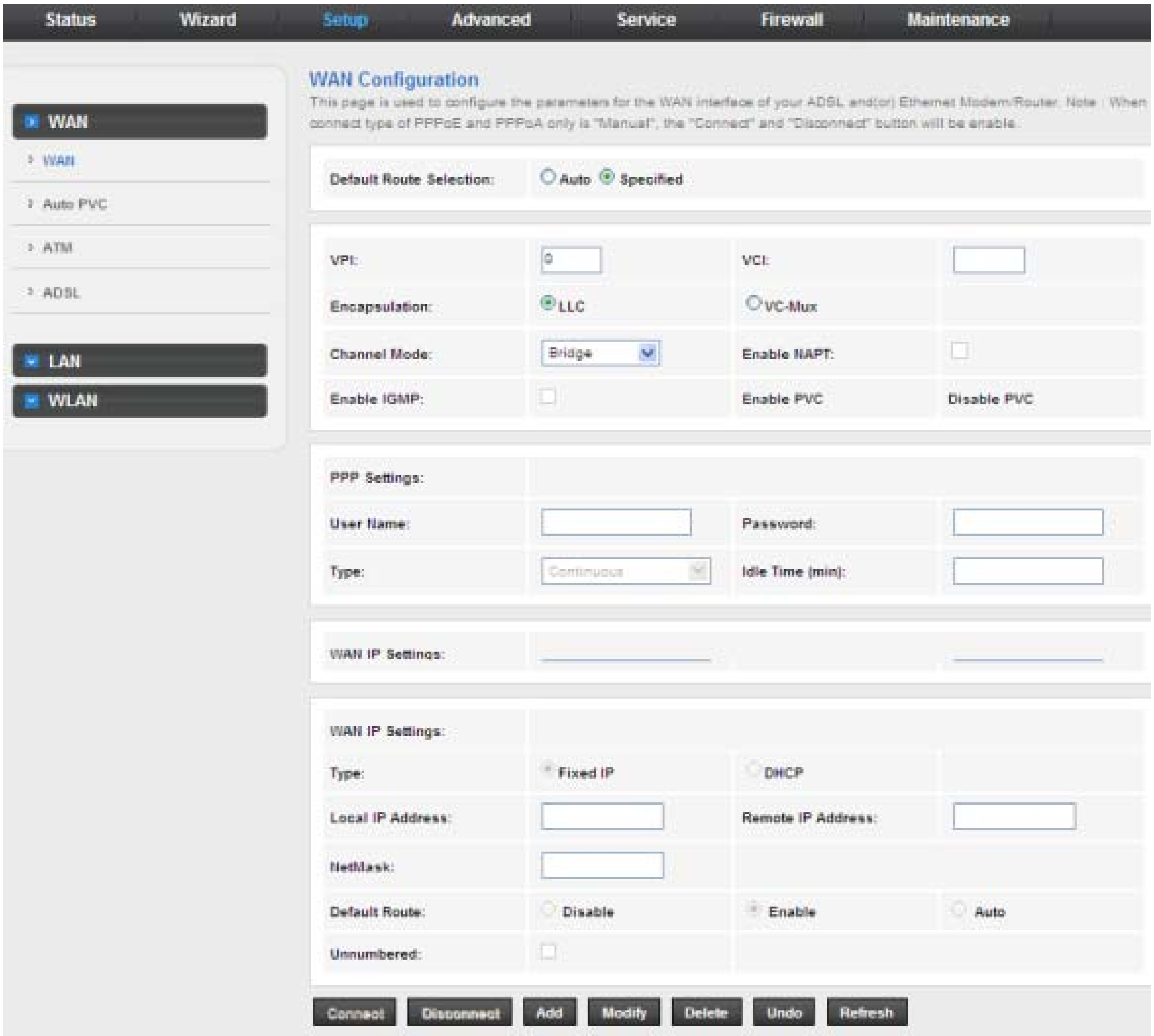
3.4.1 WAN

Choose **Setup** > **WAN**. The **WAN** page that is displayed contains **WAN**, **Auto PVC, ATM** and **ADSL**.

3.4.1.1 WAN Setting

Click **WAN** in the left pane and the page shown in the following figure appears.

On this page, you can configure WAN interface of your router.



WAN Configuration

This page is used to configure the parameters for the WAN interface of your ADSL and(or) Ethernet Modem/Router. Note : When connect type of PPPoE and PPPoA only is "Manual", the "Connect" and "Disconnect" button will be enable.

Default Route Selection:	○ Auto ● Specified		
VPI:	0	VCI:	
Encapsulation:	● LLC	○ VC-Mux	
Channel Mode:	Bridge	Enable NAPT:	□
Enable IGMP:	□	Enable PVC	Disable PVC
PPP Settings:			
User Name:		Password:	
Type:	Continuous	Idle Time (min):	
WAN IP Settings:			
WAN IP Settings:			
Type:	● Fixed IP	○ DHCP	
Local IP Address:		Remote IP Address:	
NetMask:			
Default Route:	○ Disable	● Enable	○ Auto
Unnumbered:	□		

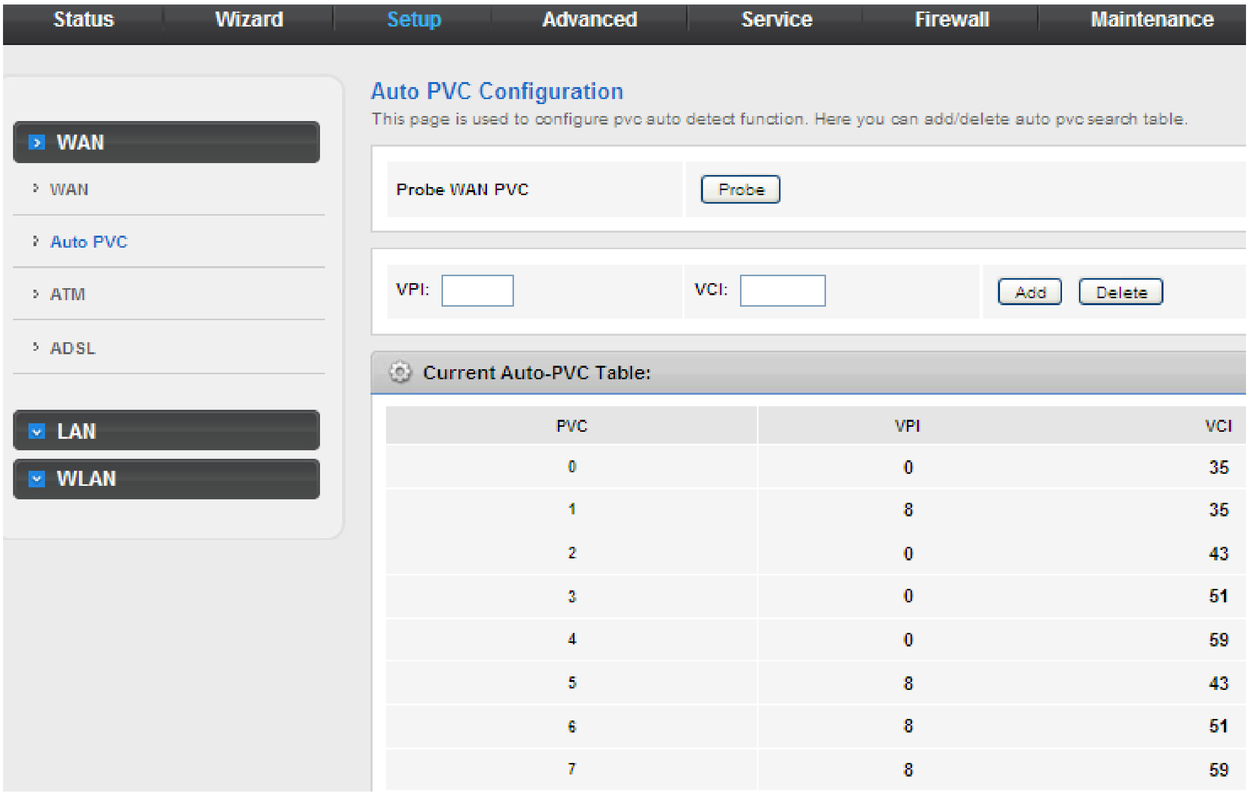
The following table describes the parameters:

Field	Description
Default Route Selection	You can select **Auto** or **Specified**.
VPI	The virtual path between two points in an ATM network, ranging from 0 to 255.

Field	Description
VCI	The virtual channel between two points in an ATM network, ranging from 32 to 65535 (1 to 31 are reserved for known protocols)
Encapsulation	You can choose **LLC** and **VC-Mux**.
Channel Mode	You can choose **Bridge**, **IPoE**, **PPPoE**, **PPPoA**, **1483 Routed** or **IPoA**.
Enable NAPT	Select it to enable Network Address Port Translation (NAPT) function. If you do not select it and you want to access the Internet normally, you must add a route on the uplink equipment. Otherwise, the access to the Internet fails. Normally, it is enabled.
Enable IGMP	You can enable or disable Internet Group Management Protocol (IGMP) function.
PPP Settings	
User Name	Enter the correct user name for PPP dial-up, which is provided by your ISP.
Password	Enter the correct password for PPP dial-up, which is provided by your ISP.
Type	You can choose **Continuous**, **Connect on Demand**, or **Manual**.
Idle Time (min)	If set the type to **Connect on Demand**, you need to enter the idle timeout time. Within the preset minutes, if the router does not detect the flow of the user continuously, the router automatically disconnects the PPPoE connection.
WAN IP Settings	
Type	You can choose **Fixed IP** or **DHCP**. ● If select **Fixed IP**, you should enter the local IP address, remote IP address and subnet mask. ● If select **DHCP**, the router is a DHCP client, the WAN IP address is assigned by the remote DHCP server.
Local IP Address	Enter the IP address of WAN interface provided by your ISP.
Netmask	Enter the subnet mask of the local IP address.
Unnumbered	Select this checkbox to enable IP unnumbered function.
Add	After configuring the parameters of this page, click it to add new PVC into the **Current ATM VC Table**.
Modify	Select PVC in the **Current ATM VC Table**, and modify the parameters of this PVC. After finishing, click it to apply the settings of this PVC.
WAN Interfaces Table	This table shows the existed PVCs. It shows the interface name, channel mode, VPI/VCI, encapsulation mode, local IP address, remote IP address and other information. The maximum item of this table is eight.

3.4.1.2 Auto PVC

Click **Auto PVC** in the left pane and the page shown in the following figure appears. On this page, you can get a PVC automatically through detecting function, and add or delete the PVC that you do not want.



Auto PVC Configuration

This page is used to configure pvc auto detect function. Here you can add/delete auto pvc search table.

Probe WAN PVC

VPI:

VCI:

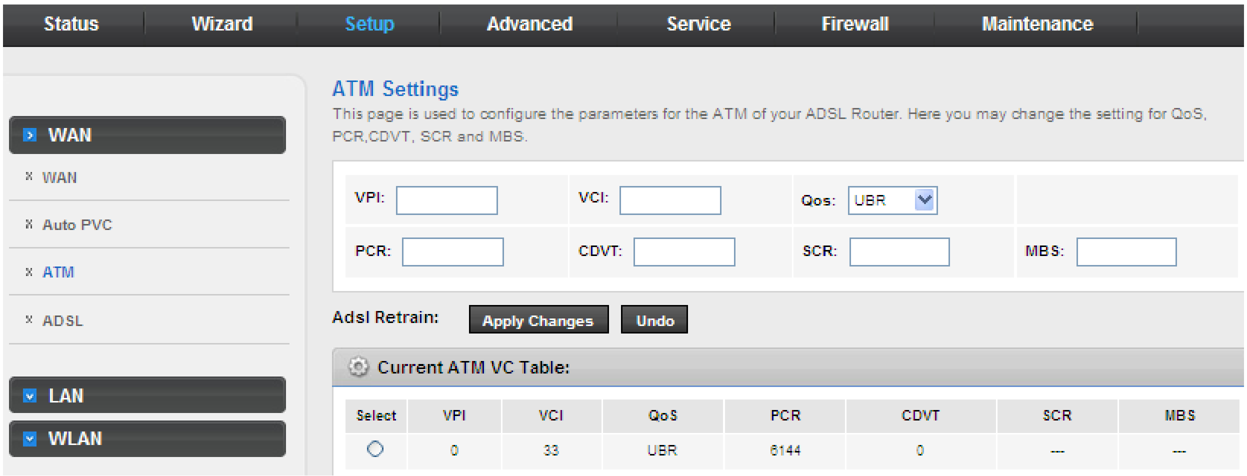
Current Auto-PVC Table:

PVC	VPI	VCI
0	0	35
1	8	35
2	0	43
3	0	51
4	0	59
5	8	43
6	8	51
7	8	59

Field	Description
Probe WAN PVC	Click Probe to display WAN Permanent virtual circuit.
VPI	Virtual Path Identifier. This is read-only field and is selected on the Select column of the Current ATM VC Table.
VCI	Virtual Channel Identifier. This is read-only field and is selected on the Select column in the Current ATM VC Table. The VCI, together with VPI, is used to identify the next destination of a cell as it passes through the ATM switch.

3.4.1.3 ATM

Click **ATM** in the left pane and the page shown in the following figure appears. On this page, you can configure the parameters of the ATM, including QoS, PCR, CDVT, SCR and MBS.



ATM Settings

This page is used to configure the parameters for the ATM of your ADSL Router. Here you may change the setting for QoS, PCR,CDVT, SCR and MBS.

VPI: VCI: Qos: UBR

PCR: CDVT: SCR: MBS:

Adsl Retrain:

Current ATM VC Table:

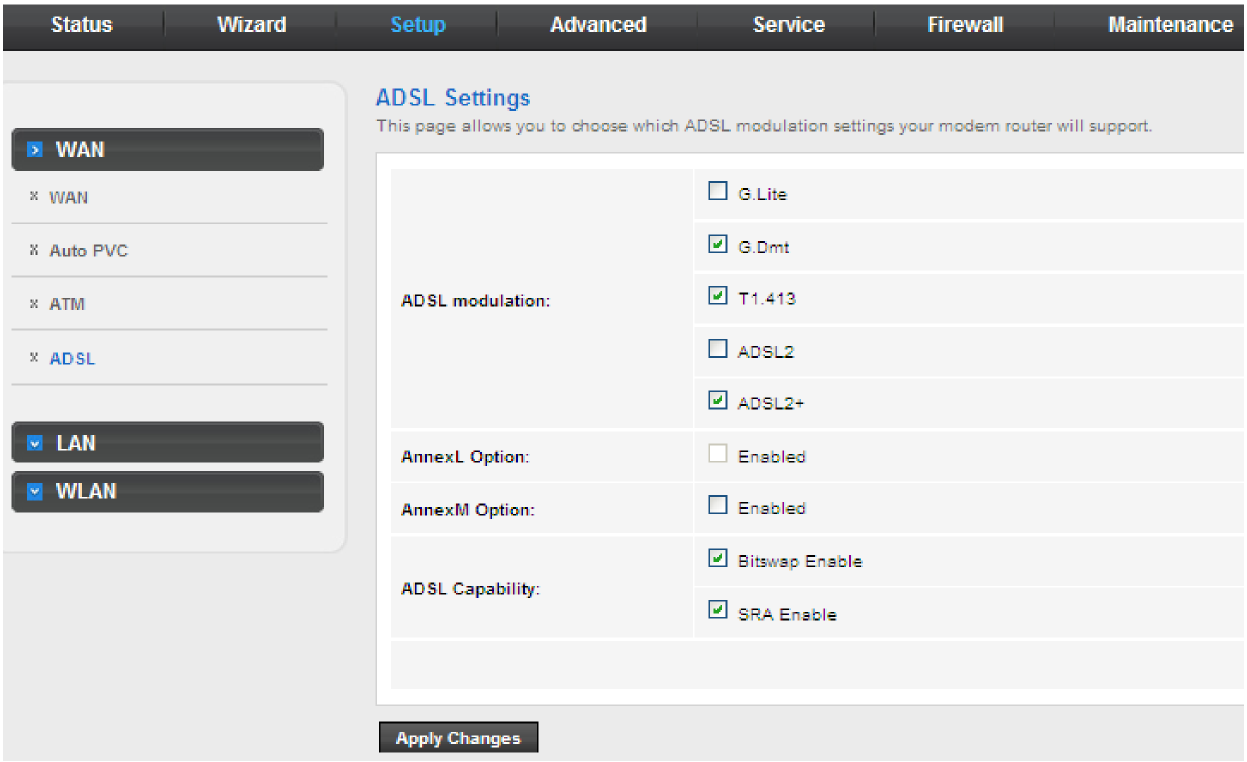
Select	VPI	VCI	QoS	PCR	CDVT	SCR	MBS
○	0	33	UBR	6144	0	---	---

The following table describes the parameters:

Field	Description
VPI	Virtual Path Identifier. This is read-only field and is selected on the Select column in the Current ATM VC Table.
VCI	Virtual Channel Identifier. This is read-only field and is selected on the Select column in the Current ATM VC Table. The VCI, together with VPI, is used to identify the next destination of a cell as it passes through the ATM switch.
QoS	Quality of Server, a characteristic of data transmission that measures how accurately and how quickly a message or data is transferred from a source host to a destination host over a network. The four QoS options are ■ UBR (Unspecified Bit Rate): When UBR is selected; the SCR and MBS fields are disabled. ■ CBR (Constant Bit Rate): When CBR is selected; the SCR and MBS fields are disabled. ■ nrt-VBR (non-real-time Variable Bit Rate): When nrt-VBR is selected, the SCR and MBS fields are enabled. ■ rt-VBR (real-time Variable Bit Rate): When rt-VBR is selected, the SCR and MBS fields are enabled.
PCR	Peak Cell Rate, measured in cells/sec., is the cell rate which the source may never exceed.
SCR	Sustained Cell Rate, measured in cells/sec., is the average cell rate over the duration of the connection.
MBS	Maximum Burst Size, a traffic parameter that specifies the maximum number of cells that can be transmitted at the peak cell rate.
CDVT	Cell delay variation tolerance (CDVT) is the amount of delay permitted between ATM cells (in microseconds).

3.4.1.4 ADSL

Click **ADSL** in the left pane and the page shown in the following figure appears. On this page, you can select the DSL modulation. This factory default setting is mostly used . The router supports these modulations: **G.Lite**, **G.Dmt**, **T1.413**, **ADSL2** and **ADSL2+**. The router negotiates the modulation modes with the DSLAM.



ADSL Settings

This page allows you to choose which ADSL modulation settings your modem router will support.

ADSL modulation: □ G.Lite ☑ G.Dmt ☑ T1.413 □ ADSL2 ☑ ADSL2+

AnnexL Option: □ Enabled

AnnexM Option: □ Enabled

ADSL Capability: ☑ Bitswap Enable ☑ SRA Enable

The following table describes the parameters:

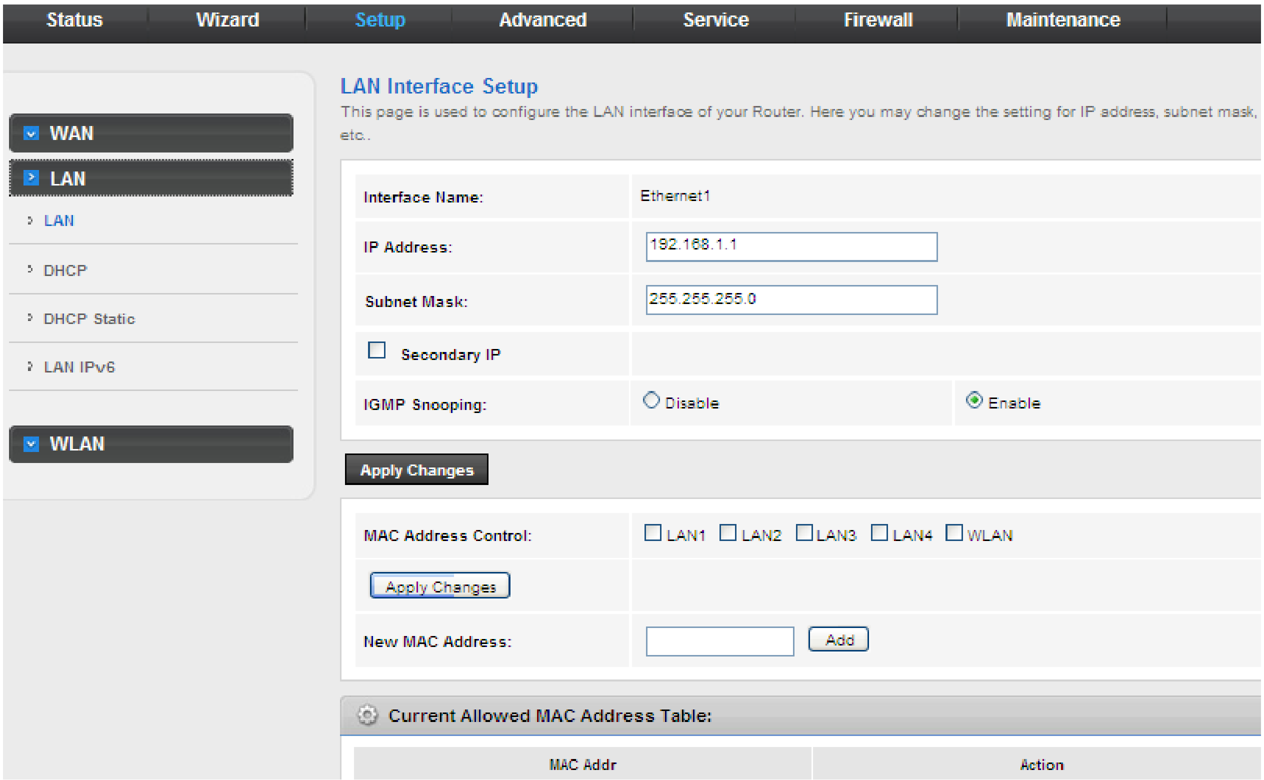
Field	Description
ADSL modulation	Choose preferred xdsl standard protocols. G.lite : G.992.2 Annex A G.Dmt : G.992.1 Annex A T1.413 : T1.413 issue #2 ADSL2 : G.992.3 Annex A ADSL2+ : G.992.5 Annex A
AnnexL Option	Enable/Disable ADSL2/ADSL2+ Annex L capability.
AnnexM Option	Enable/Disable ADSL2/ADSL2+ Annex M capability.
ADSL Capability	"Bitswap Enable": Enable/Disable bitswap capability. "SRA Enable": Enable/Disable SRA (seamless rate adaptation) capability.

3.4.2 LAN

Choose Setup > **LAN**. The **LAN** page that is displayed contains **LAN, DHCP, DHCP Static and LAN IPv6**.

3.4.2.1 LAN Setting

Click **LAN** in the left pane and the page shown in the following figure appears. On this page, you can change IP address of the router. The default IP address is **192.168.1.1**, which is the private IP address of the router.



LAN Interface Setup

This page is used to configure the LAN interface of your Router. Here you may change the setting for IP address, subnet mask, etc..

Interface Name: Ethernet1

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

□ Secondary IP

IGMP Snooping: ○ Disable ● Enable

Apply Changes

MAC Address Control: □ LAN1 □ LAN2 □ LAN3 □ LAN4 □ WLAN

Apply Changes

New MAC Address: Add

Current Allowed MAC Address Table:

MAC Addr	Action

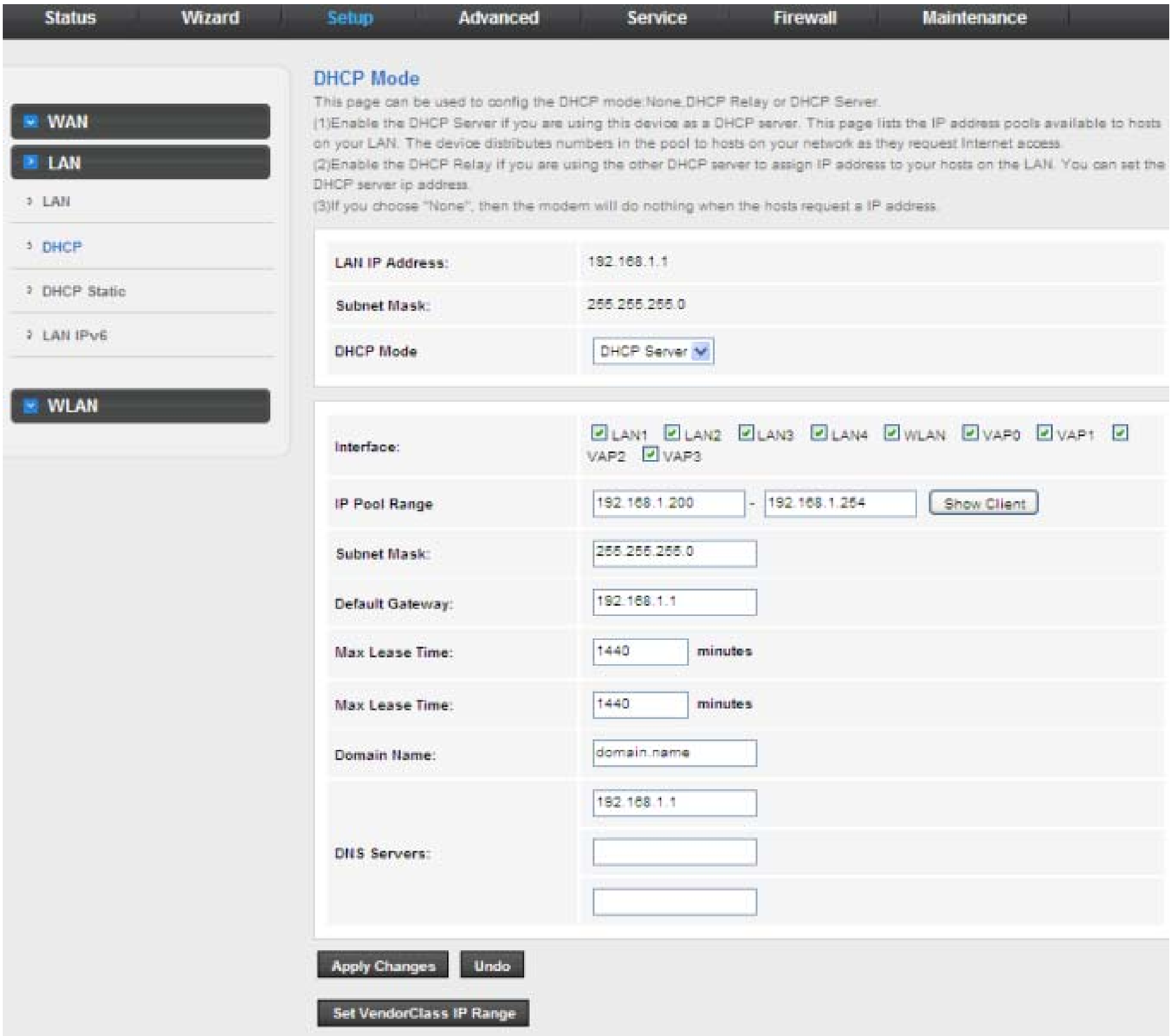
The following table describes the parameters:

Field	Description
IP Address	The IP address of your LAN hosts used to identify the device's LAN port.
Subnet Mask	Enter the subnet mask of LAN interface. The range of subnet mask is from 255.255.0.0 to 255.255.255.254
Secondary IP	Select it to enable/disable a secondary LAN IP address. The two LAN IP addresses must be in the different network.
IGMP Snooping	Enable/disable the IGMP snooping function for the multiple bridged LAN ports.
MAC Address Control	It is the access control based on MAC address. Select LAN1, LAN2, LAN3, LAN4, WLAN and the host whose MAC address listed in the Currently Allowed MAC Address Table can access the device. Then click "Apply Changes" to save the new settings.
New MAC Address	Enter MAC address and then click Add to add a new MAC address.

3.4.2.2 DHCP

Dynamic Host Configuration Protocol (DHCP) allows the individual PC to obtain the TCP/IP configuration from the centralized DHCP server. You can configure this router as a DHCP server or disable it. The DHCP server can assign IP address, IP default gateway, and DNS server to DHCP clients. This router can also act as a surrogate DHCP server (DHCP Relay) where it relays IP address assignment from an actual real DHCP server to clients. You can enable or disable DHCP server.

Click **DHCP** in the left pane and the page shown in the following figure appears.



DHCP Mode

This page can be used to config the DHCP mode:None,DHCP Relay or DHCP Server.
(1)Enable the DHCP Server if you are using this device as a DHCP server. This page lists the IP address pools available to hosts on your LAN. The device distributes numbers in the pool to hosts on your network as they request Internet access.
(2)Enable the DHCP Relay if you are using the other DHCP server to assign IP address to your hosts on the LAN. You can set the DHCP server ip address.
(3)If you choose "None", then the modem will do nothing when the hosts request a IP address.

LAN IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
DHCP Mode	DHCP Server

Interface:	☑ LAN1 ☑ LAN2 ☑ LAN3 ☑ LAN4 ☑ WLAN ☑ VAP0 ☑ VAP1 ☑ VAP2 ☑ VAP3
IP Pool Range	192.168.1.200 - 192.168.1.254 Show Client
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.1.1
Max Lease Time:	1440 minutes
Max Lease Time:	1440 minutes
Domain Name:	domain.name
DNS Servers:	192.168.1.1

Apply Changes   Undo

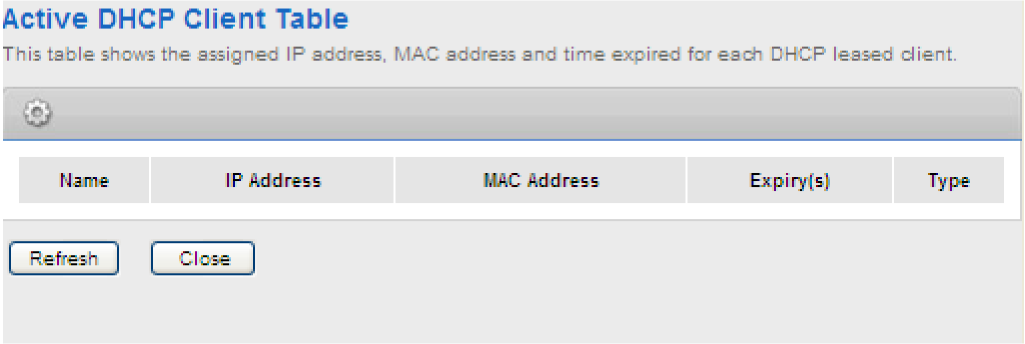
Set VendorClass IP Range

The following table describes the parameters:

Field	Description
DHCP Mode	You can choose None, DHCP Relay and DHCP Server. If set to DHCP Server, the router can assign IP addresses, IP default gateway and DNS Servers to the host in Windows95, Windows NT and other operating systems that support the DHCP client.
Interface	By default, all ports are selected; click it to unselect and those ports cannot function with the IP address.
IP Pool Range	Specify the lowest and highest addresses in the pool. It specifies the first IP address in the IP address pool. The router assigns IP address based on the IP pool range to the host.
Show Client	Click it and the Active DHCP Client Table appears. It shows IP addresses assigned to clients.

Field	Description
Subnet Mask	Enter the subnet mask.
Default Gateway	Enter the default gateway of the IP address pool.
Max. Lease Time	The Lease Time is the amount of time that a network user is allowed to maintain a network connection to the device using the current dynamic IP address. At the end of the Lease Time, the lease is either renewed or a new IP is issued by the DHCP server. The amount of time is in units of seconds. The default value is 1440 minutes (1 day).
Domain Name	Domain Name is the most recognized system for assigning addresses to Internet web servers.
DNS Servers	You can configure the DNS server IP addresses for DNS Relay.

Click **Show Client** on the **DHCP Mode** page and the page shown in the following figure appears. You can view the IP address assigned to each DHCP client.



Active DHCP Client Table

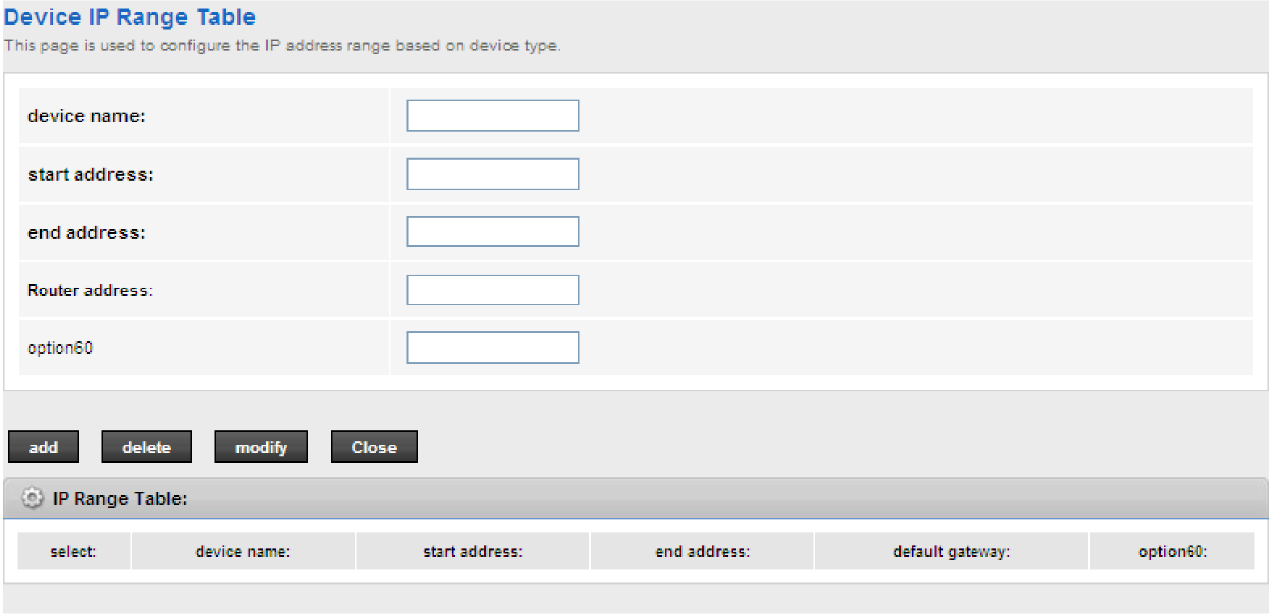
This table shows the assigned IP address, MAC address and time expired for each DHCP leased client.

Name	IP Address	MAC Address	Expiry(s)	Type

The following table describes the parameters:

Field	Description
IP Address	It displays the IP address assigned to the DHCP client from the router.
MAC Address	It displays the MAC address of the DHCP client. Each Ethernet device has a unique MAC address. The MAC address is assigned at the factory and it consists of six pairs of hexadecimal character, for example, 00-30-4F-00-02-12.
Expiry	It displays the lease time. The lease time determines the period that the host retains the assigned IP addresses before the IP addresses change.
Refresh	Click it to refresh this page.
Close	Click it to close this page.

Click **Set Vendor Class IP Range** on the **DHCP Mode** page and the page as shown in the following figure appears. On this page, you can configure the IP address range based on the device type.



Device IP Range Table

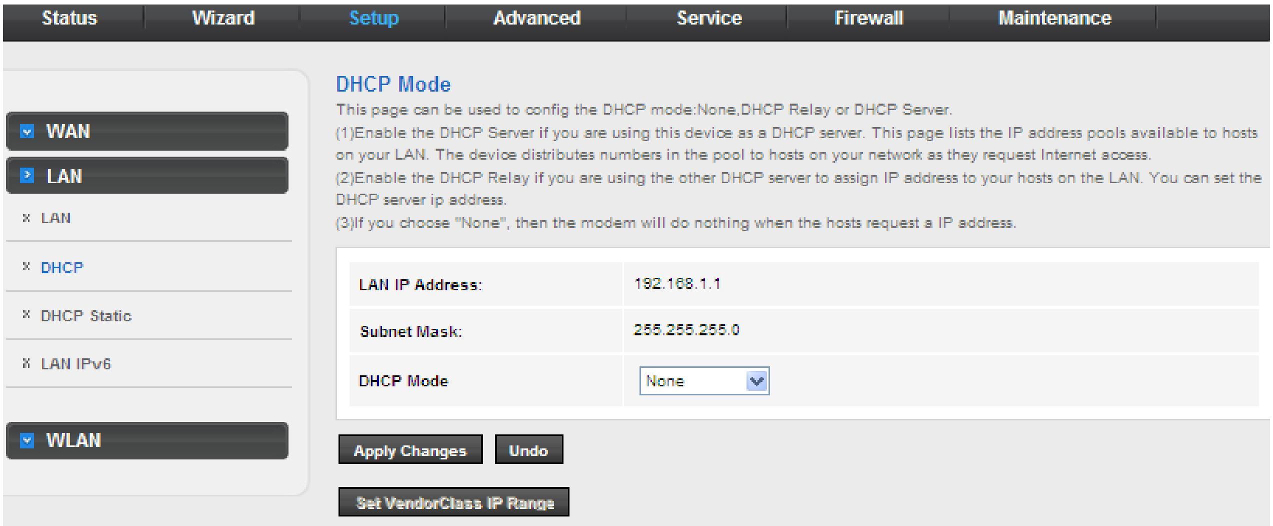
This page is used to configure the IP address range based on device type.

device name:	
start address:	
end address:	
Router address:	
option60	

IP Range Table:

select:	device name:	start address:	end address:	default gateway:	option60:

In the **DHCP Mode** field, choose **None** and the page shown in the following figure appears.

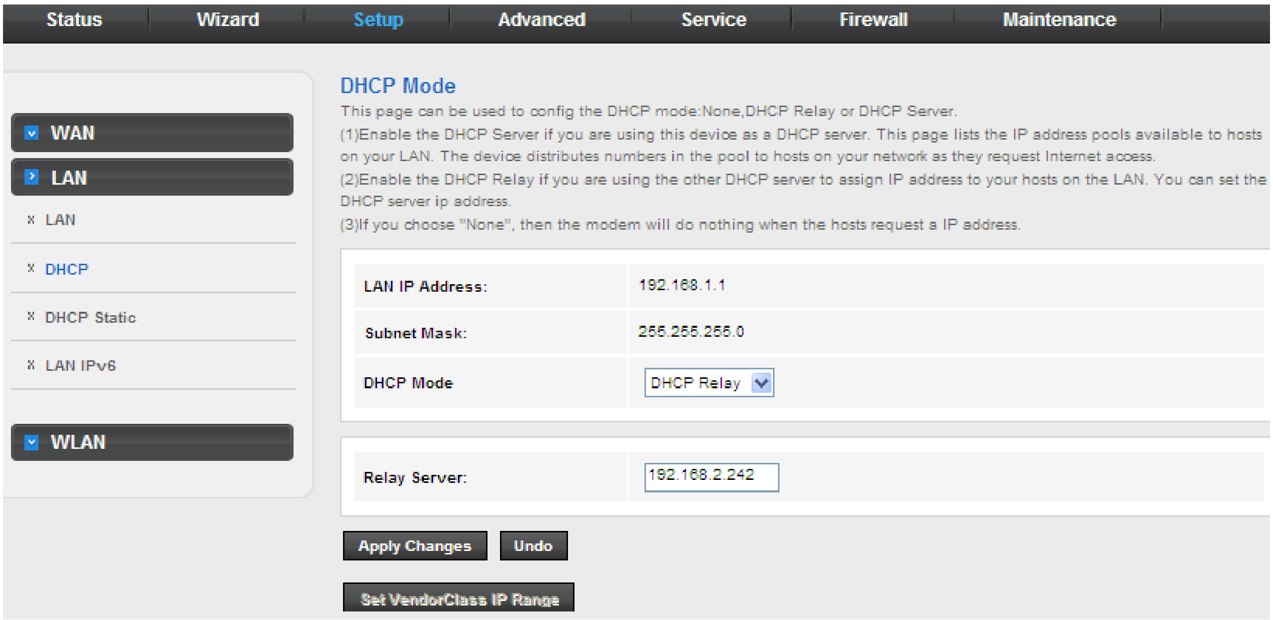


DHCP Mode

This page can be used to config the DHCP mode:None,DHCP Relay or DHCP Server.
(1)Enable the DHCP Server if you are using this device as a DHCP server. This page lists the IP address pools available to hosts on your LAN. The device distributes numbers in the pool to hosts on your network as they request Internet access.
(2)Enable the DHCP Relay if you are using the other DHCP server to assign IP address to your hosts on the LAN. You can set the DHCP server ip address.
(3)If you choose "None", then the modem will do nothing when the hosts request a IP address.

LAN IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
DHCP Mode	None

In the **DHCP Mode** field, choose **DHCP Relay** and the page shown in the following figure appears.



DHCP Mode

This page can be used to config the DHCP mode:None,DHCP Relay or DHCP Server.
(1)Enable the DHCP Server if you are using this device as a DHCP server. This page lists the IP address pools available to hosts on your LAN. The device distributes numbers in the pool to hosts on your network as they request Internet access.
(2)Enable the DHCP Relay if you are using the other DHCP server to assign IP address to your hosts on the LAN. You can set the DHCP server ip address.
(3)If you choose "None", then the modem will do nothing when the hosts request a IP address.

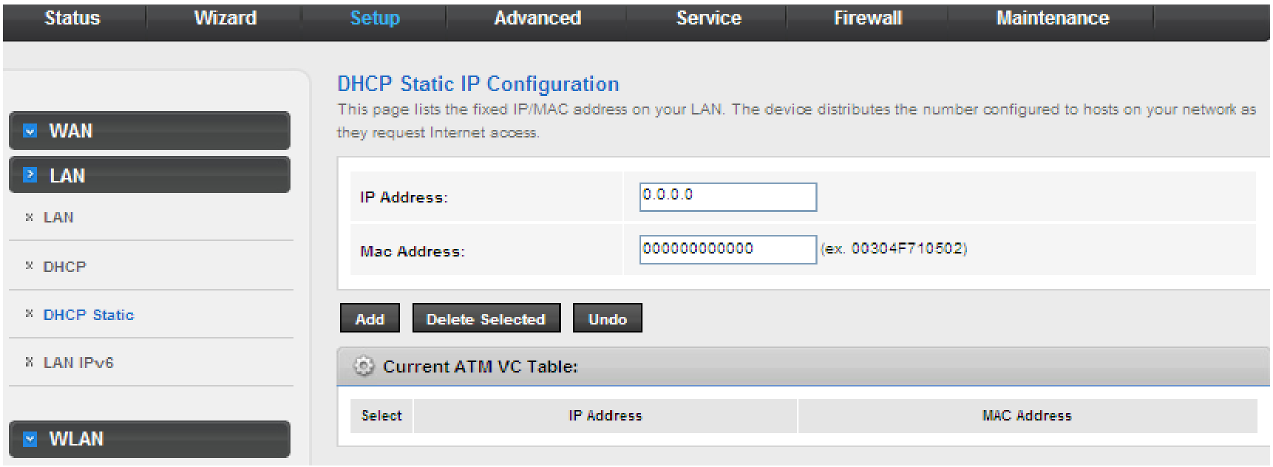
LAN IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
DHCP Mode	DHCP Relay
Relay Server:	192.168.2.242

The following table describes the parameters:

Field	Description
DHCP Mode	If set to **DHCP Relay**, the router acts as a surrogate DHCP Server and relays the DHCP requests and responses between the remote server and the client.
Relay Server	Enter the DHCP server address provided by your ISP.
Apply Changes	Click it to save the settings on this page.
Undo	Click it to refresh this page.

3.4.2.3 DHCP Static IP

Click **DHCP Static IP** in the left pane and the page shown in the following figure appears. You can assign the IP addresses on the LAN to the specific individual PCs based on their MAC address.



DHCP Static IP Configuration

This page lists the fixed IP/MAC address on your LAN. The device distributes the number configured to hosts on your network as they request Internet access.

IP Address:	0.0.0.0
Mac Address:	000000000000 (ex. 00304F710502)

Current ATM VC Table:

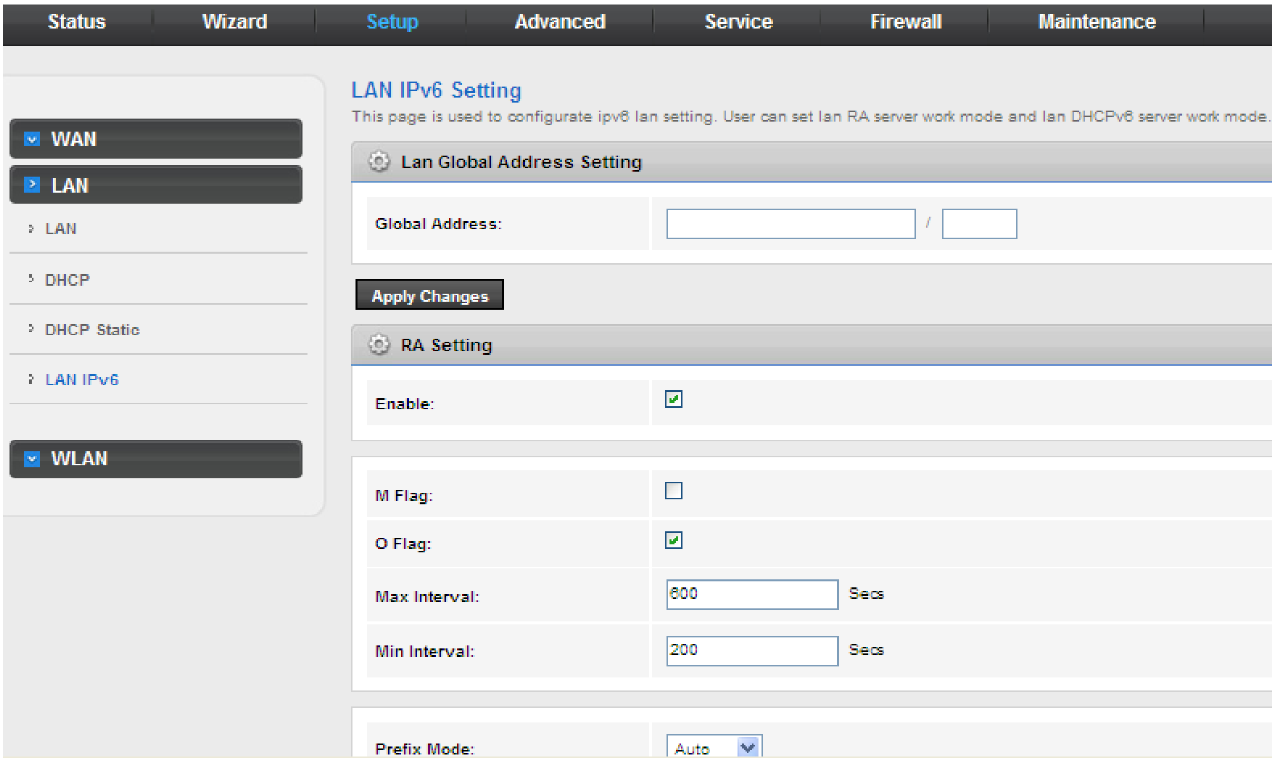
Select	IP Address	MAC Address

The following table describes the parameters:

Field	Description
IP Address	Enter the specified IP address in the IP pool range, which is assigned to the host.
MAC Address	Enter the MAC address of a host on the LAN.
Add	After entering the IP address and MAC address, click it. A row will be added in the **DHCP Static IP Table**.
Delete Selected	Select a row in the **DHCP Static IP Table**; then click it and this row is deleted.
Undo	Click it to refresh this page.
Current ATM VC Table	It shows the assigned IP address based on the MAC address.

3.4.2.4 LAN IPv6

On this page, you can configure the LAN IPv6. Choose **Setup** > **LAN** > **LAN IPv6**. The **IPv6 LAN setting** page as shown in the following figure appears:



LAN IPv6 Setting

This page is used to configurate ipv6 lan setting. User can set lan RA server work mode and lan DHCPv6 server work mode.

Lan Global Address Setting

Global Address: [ ] / [ ]

RA Setting

Enable: ☑

M Flag: □

O Flag: ☑

Max Interval: 600 Secs

Min Interval: 200 Secs

Prefix Mode: Auto

The following table describes the parameters:

LAN Global Address Setting

Field	Description
Global Address	Specify the LAN global IPv6 address; may be assigned by ISP.

RA Settings

Field	Description
Enable	Enable or disable the Router Advertisement feature.

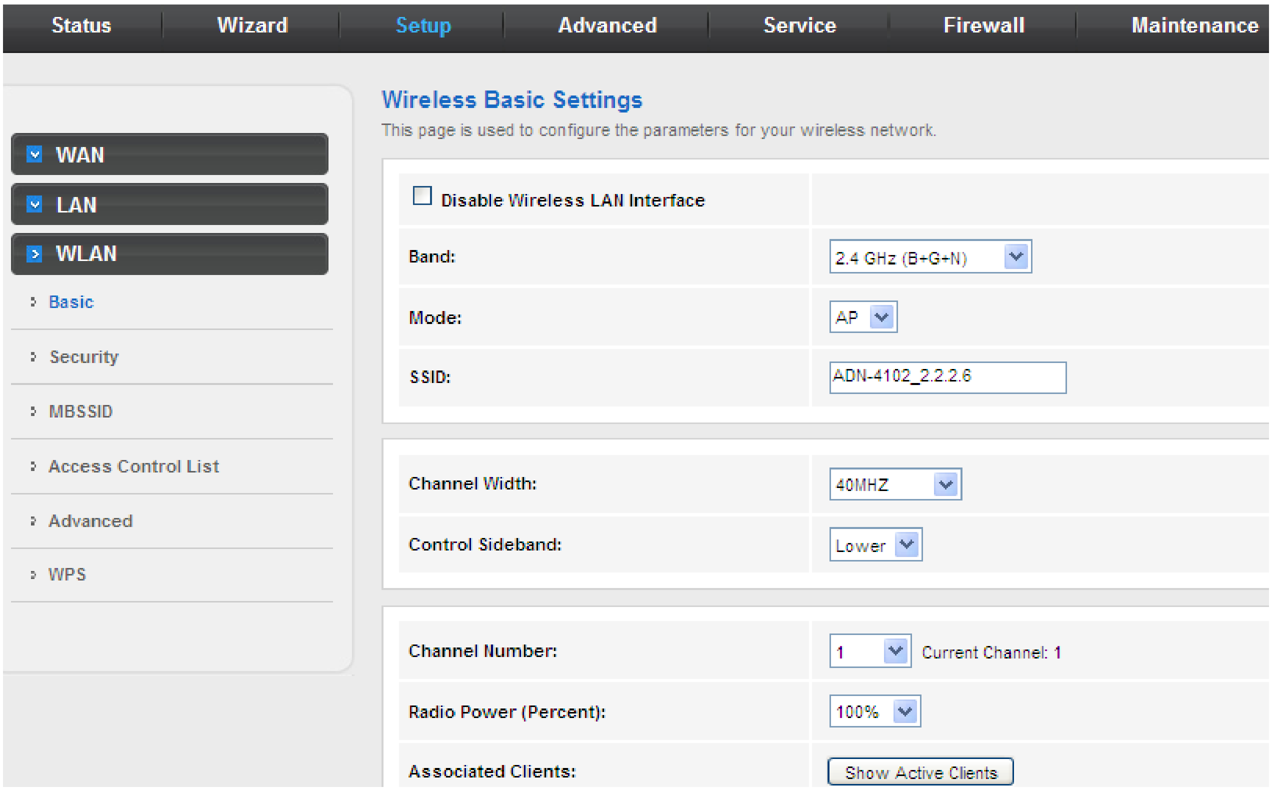
Field	Description
M Flag	Enable or disable the “Managed address configuration” flag in RA packet.
O Flag	Enable or disable the “Other configuration” flag in RA packet.
Max. Interval	Maximum sending time interval.
Min. Interval	Minimum sending time interval.
Prefix Mode	Specify the RA feature prefix mode **Auto:** The RA prefix will use WAN dhcp-pd prefix **Manual:** User will specify the prefix Address, Length, Preferred time and Valid time.
ULA	Unique Local Address. Enable/Disable the feature to access.
RA DNS Enable	Enable/Disable the feature to access.

DHCPv6 Settings

Field	Description
DHCPv6 Mode	Select the Mode to None or Manual Mode or Auto Mode.
IPv6 Address Suffix Pool	Enter the IPv6 address.
IPv6 DNS Mode	Select the Mode to Auto or Manual.

3.5 WLAN

This page contains all the wireless basic settings. Most users will be able to configure the wireless portion and get it working properly using the setting on this screen.



Wireless Basic Settings

This page is used to configure the parameters for your wireless network.

☐ Disable Wireless LAN Interface

Band: 2.4 GHz (B+G+N)

Mode: AP

SSID: ADN-4102_2.2.2.6

Channel Width: 40MHZ

Control Sideband: Lower

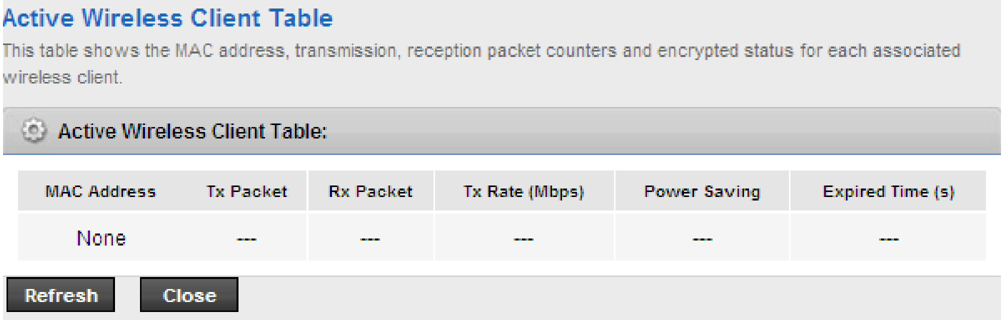
Channel Number: 1 Current Channel: 1

Radio Power (Percent): 100%

Associated Clients:

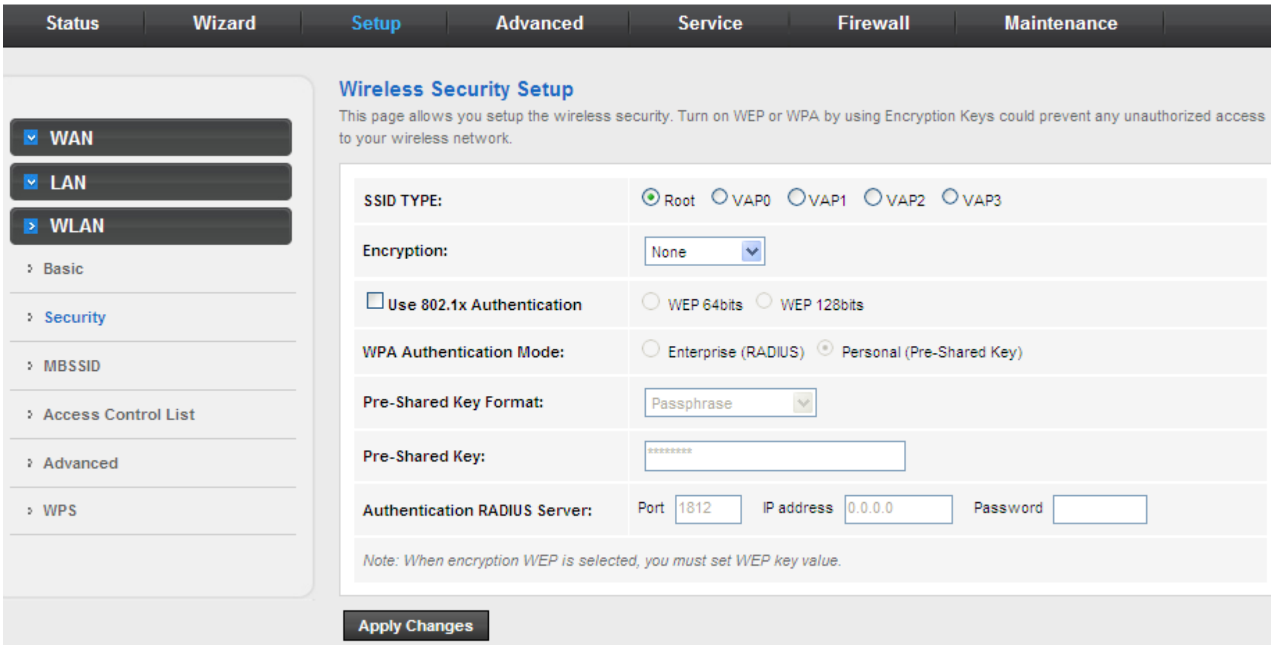
The following table describes the parameters:

Fields	Description
Disable Wireless LAN Interface	Enable/Disable the wireless function for ADSL modem.
Band	Select the appropriate band from the list provided to correspond with your network setting.
Mode	Select AP Mode.
SSID	The Service Set Identifier (SSID) or network name. It is case sensitive and must not exceed 32 characters, which may be any keyboard character. The mobile wireless stations will select the same SSID to be able to communicate with your ADSL modem (or AP).
Channel Width	Select channel width to 20MHz, 40MHz or 20/40MHz.
Control Sideband	Select upper or lower sideband.
Channel Number	Select the appropriate channel from the list provided to correspond with your network settings. You will assign a different channel for each AP to avoid signal interference.
Radio Power (Percent)	100%, 80%, 50%, 25%, 10%.
Associated	Click it to see the clients currently associated with the ADSL modem.

Fields	Description
Clients	 Active Wireless Client Table This table shows the MAC address, transmission, reception packet counters and encrypted status for each associated wireless client. Active Wireless Client Table: MAC Address | Tx Packet | Rx Packet | Tx Rate (Mbps) | Power Saving | Expired Time (s) None | --- | --- | --- | --- | ---

3.5.1 Security

This screen allows you to set up the wireless security. Turn on WEP or WPA by using encryption keys that could prevent any unauthorized access to your WLAN.



Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

SSID TYPE:	● Root ○ VAP0 ○ VAP1 ○ VAP2 ○ VAP3
Encryption:	None
□ Use 802.1x Authentication	○ WEP 64bits ○ WEP 128bits
WPA Authentication Mode:	○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)
Pre-Shared Key Format:	Passphrase
Pre-Shared Key:	********
Authentication RADIUS Server:	Port 1812 IP address 0.0.0.0 Password

Note: When encryption WEP is selected, you must set WEP key value.

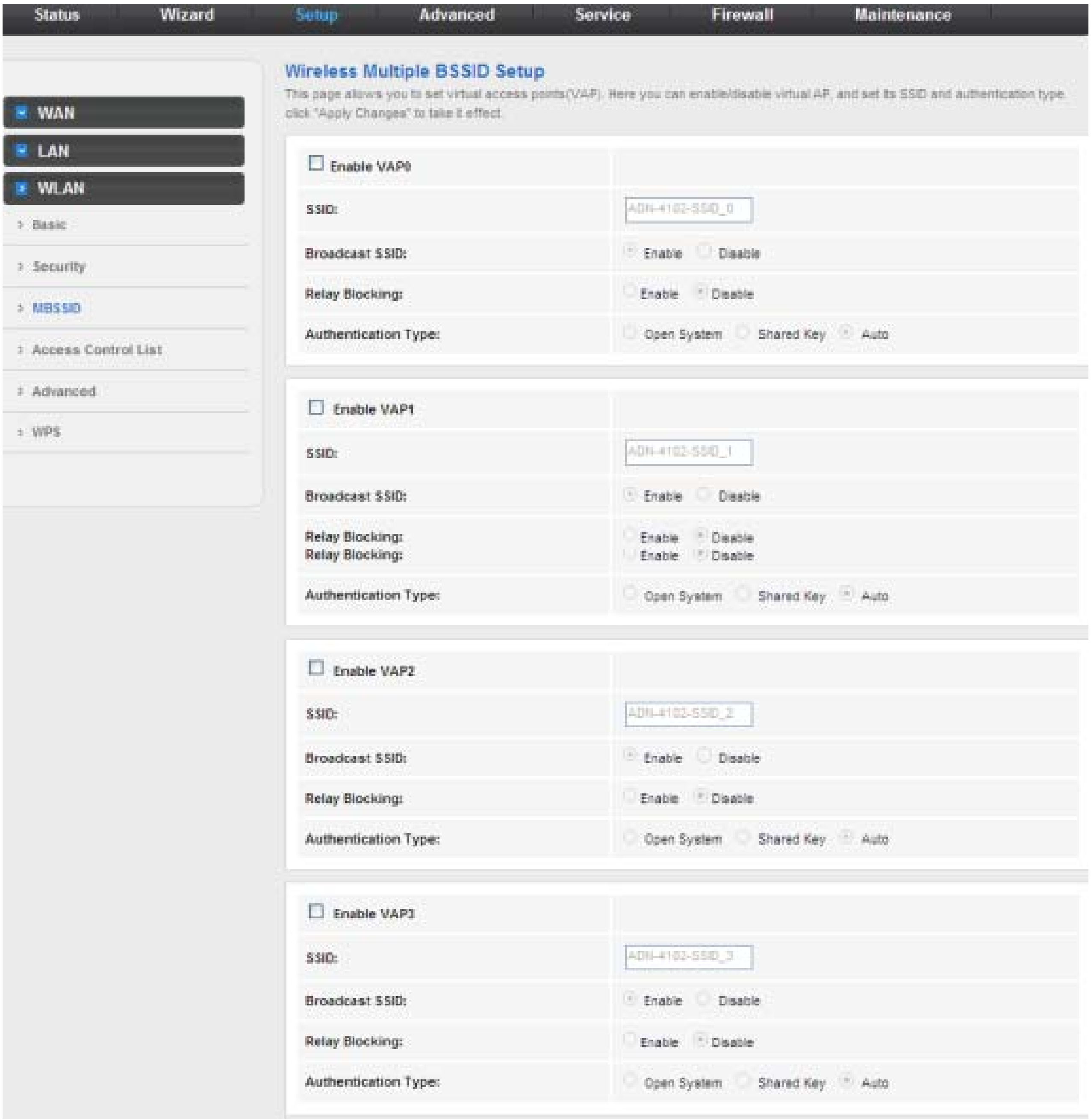
The following table describes the parameters:

Fields	Description
SSID Type	Select the SSID Type.

Fields	Description
Encryption	There are 4 types of security to be selected. To secure your WLAN, it's strongly recommended to enable this feature. **WEP:** Make sure that all wireless devices on your network are using the same encryption level and key. **WPA/WPA2 (TKIP):** WPA/WPA2 uses Temporal Key Integrity Protocol (TKIP) for data encryption. TKIP utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers. **WPA/WPA2 (AES):** WPA/WPA2, also known as 802.11i, uses Advanced Encryption Standard (AES) for data encryption. AES utilizes a symmetric 128-bit block data encryption. **WPA2 Mixed:** The AP supports WPA (TKIP) and WPA2 (AES) for data encryption. The actual selection of the encryption methods will depend on the clients.
Use 802.1x Authentication	Check it to enable 802.1x authentication. This option is selected only when the "Encryption" is chosen to either None or WEP. If the "Encryption" is WEP, you need to further select the WEP key length to be either WEP 64 character or WEP 128 character.
WPA Authentication Mode	There are 2 types of authentication mode for WPA. **WPA-RADIUS:** WPA RADIUS uses an external RADIUS server to perform user authentication. To use WPA RADIUS, enter the IP address of the RADIUS server, the RADIUS port (default is 1812) and the shared secret from the RADIUS server. **Pre-Shared Key:** Pre-Shared Key authentication is based on a shared secret that is known only by the parties involved. To use WPA Pre-Shared Key, select key format and enter a password in the "Pre-Shared Key Format" and "Pre-Shared Key" setting respectively.
Pre-Shared Key Format	**Passphrase:** Select this to enter the Pre-Shared Key secret as user-friendly textual secret. **Hex (64 characters):** Select this to enter the Pre-Shared Key secret as hexadecimal secret.
Pre-Shared Key	Specify the shared secret used by this Pre-Shared Key. If the "Pre-Shared Key Format" is specified as PassPhrase, then it indicates a passphrase of 8 to 64 character long or 64-hexadecimal number.
Authentication RADIUS Server	If the WPA-RADIUS is selected in "WPA Authentication Mode", the port (default is 1812), IP address and password of external RADIUS server are specified here.

3.5.2 MBSSIDs

This screen allows you to do the wireless multiple MBSSIDs setup.



Wireless Multiple BSSID Setup

This page allows you to set virtual access points(VAP). Here you can enable/disable virtual AF, and set its SSID and authentication type. click "Apply Changes" to take it effect.

□ Enable VAP0	
SSID:	ADN-4102-SSID_0
Broadcast SSID:	● Enable ○ Disable
Relay Blocking:	○ Enable ● Disable
Authentication Type:	○ Open System ○ Shared Key ● Auto

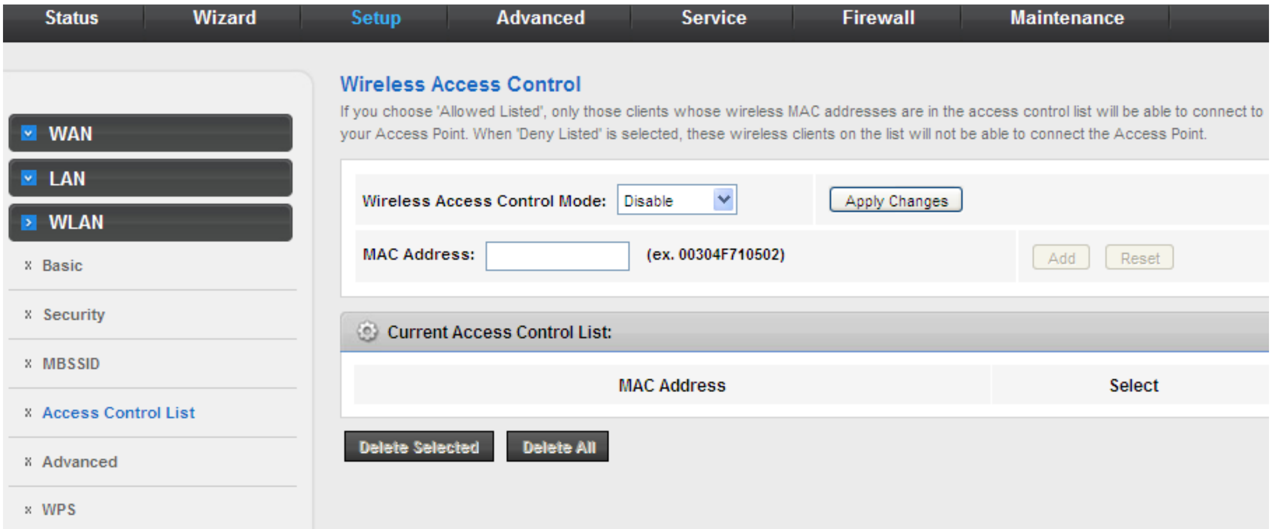
□ Enable VAP1	
SSID:	ADN-4102-SSID_1
Broadcast SSID:	● Enable ○ Disable
Relay Blocking: Relay Blocking:	○ Enable ● Disable ○ Enable ● Disable
Authentication Type:	○ Open System ○ Shared Key ● Auto

□ Enable VAP2	
SSID:	ADN-4102-SSID_2
Broadcast SSID:	● Enable ○ Disable
Relay Blocking:	○ Enable ● Disable
Authentication Type:	○ Open System ○ Shared Key ● Auto

□ Enable VAP3	
SSID:	ADN-4102-SSID_3
Broadcast SSID:	● Enable ○ Disable
Relay Blocking:	○ Enable ● Disable
Authentication Type:	○ Open System ○ Shared Key ● Auto

3.5.3 Access Control

This page allows administrator to have access control by entering MAC address of client stations. When this function is enabled, MAC address can be added to access control list and only those clients whose wireless MAC address are in the access control list will be able to connect to your DSL device (or AP).



Wireless Access Control

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

Wireless Access Control Mode: Disable

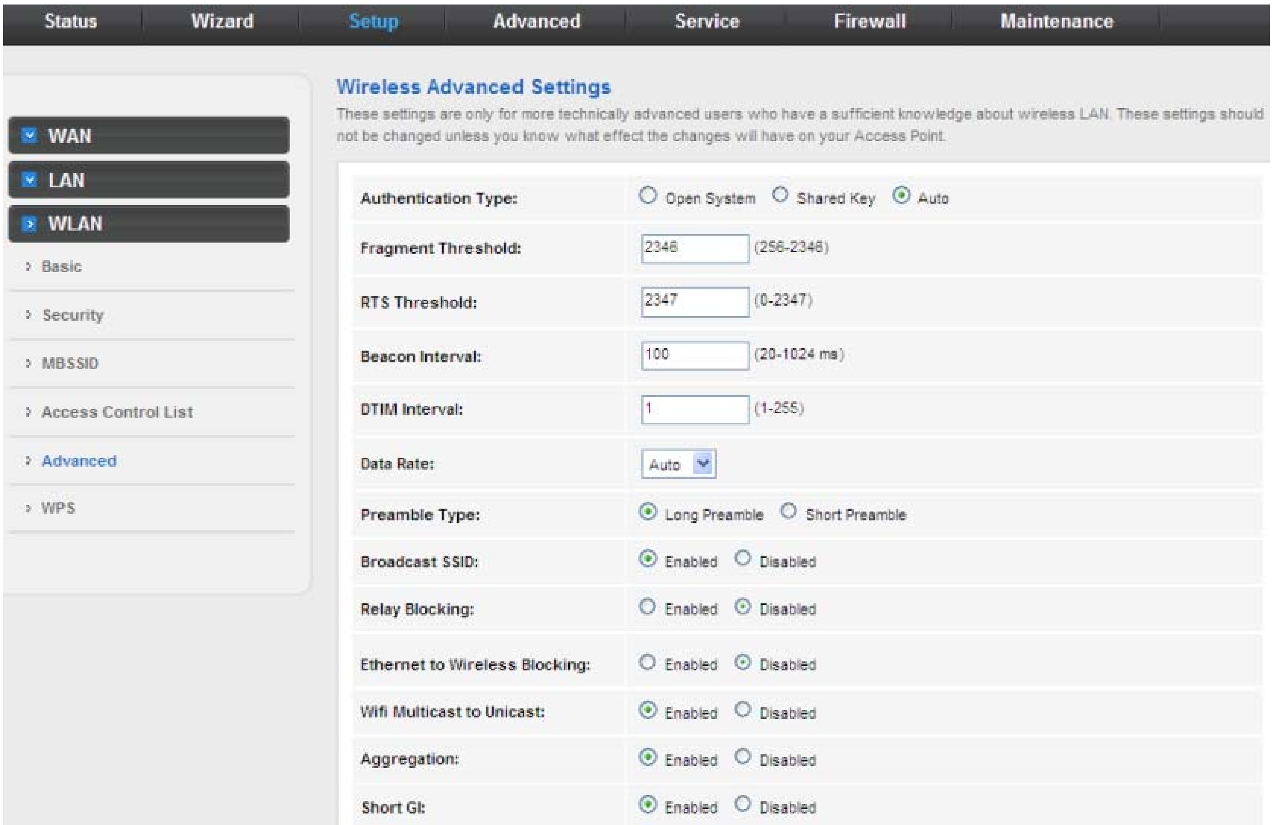
MAC Address: (ex. 00304F710502)

Current Access Control List:

MAC Address	Select

Field	Description
Wireless Access Control Mode	The Selections are: **Disable:** Disable the wireless ACL feature. **Allow Listed:** When this option is selected, no wireless clients except those whose MAC addresses are in the current access control list will be able to connect (to this device). **Deny Listed:** When this option is selected, all wireless clients except those whose MAC addresses are in the current access control list will not be able to connect (to this device).
MAC Address	Enter client MAC address.
Apply Changes	Click Apply Changes to add new settings; then it restarts.
Add	Click to add MAC address to the Current Access Control List.
Reset	Clear the settings.
Delete Selected	Select the rows to be deleted from Current Access Control List.
Delete All	Flush the list.

3.5.4 Advanced Settings



Wireless Advanced Settings

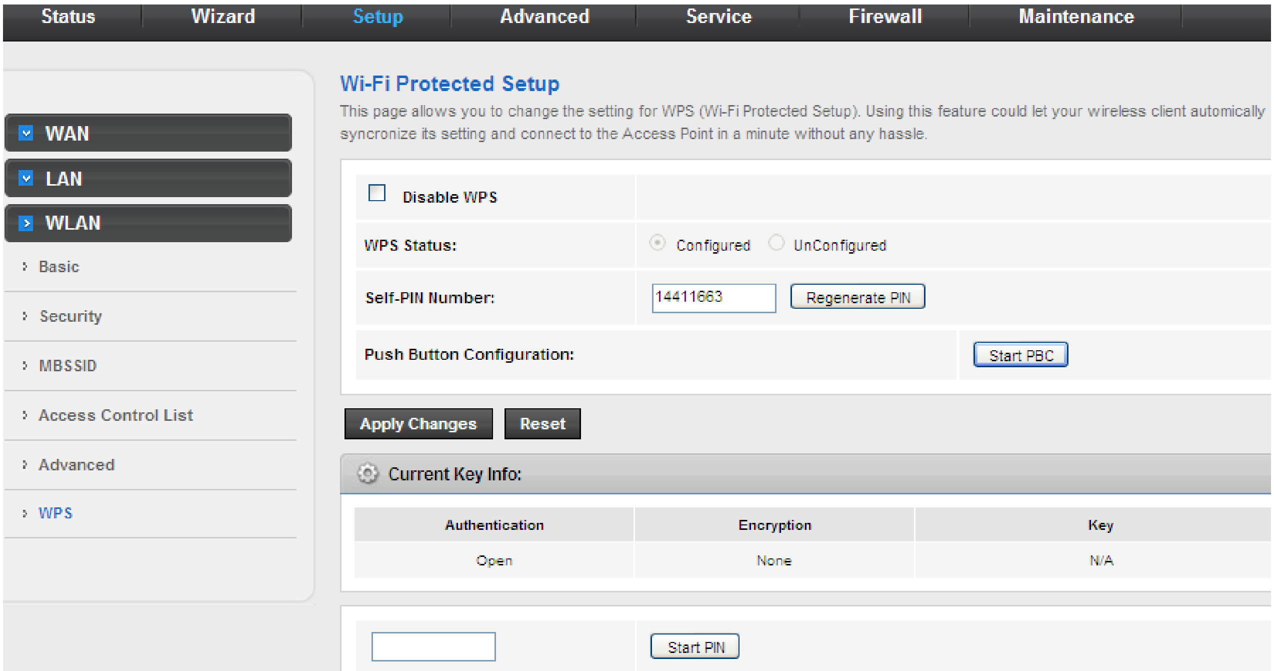
These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.

Authentication Type:	○ Open System ○ Shared Key ● Auto
Fragment Threshold:	2346 (256-2346)
RTS Threshold:	2347 (0-2347)
Beacon Interval:	100 (20-1024 ms)
DTIM Interval:	1 (1-255)
Data Rate:	Auto
Preamble Type:	● Long Preamble ○ Short Preamble
Broadcast SSID:	● Enabled ○ Disabled
Relay Blocking:	○ Enabled ● Disabled
Ethernet to Wireless Blocking:	○ Enabled ● Disabled
Wifi Multicast to Unicast:	● Enabled ○ Disabled
Aggregation:	● Enabled ○ Disabled
Short GI:	● Enabled ○ Disabled

This page allows advanced users who have sufficient knowledge of wireless LAN. These settings will not be changed unless you know exactly what will happen for the changes you made on your DSL device.

3.5.5 WPS

Wi-Fi Protected Setup (WPS) is a push-button or pin to simplify a secure network set-up.



Wi-Fi Protected Setup

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automically syncronize its setting and connect to the Access Point in a minute without any hassle.

☐ Disable WPS

WPS Status: ● Configured ○ UnConfigured

Self-PIN Number: 14411663

Push Button Configuration:

Current Key Info:

Authentication	Encryption	Key
Open	None	N/A

The following table describes the parameters:

Field	Description
Disable WPS	Enable/Disable the WPS function.
Self-Pin Number	Click Regenerate Pin to reset automatically to obtain an 8-digit number.
Push Button Configuration	Click Start PBC button to connect from Wi-Fi dongle to device automatically.
Start Pin	Enter the Pin number to connect from device to Wi-Fi dongle.

3.6 Advanced

In the navigation bar, click **Advanced**. On the **Advanced** page that is displayed contains **Route**, **NAT**, **QoS**, **CWMP** (**TR-069**), **Port Mappings** and **Others**.

3.6.1 Route

The Routing page enables you to define specific route for your Internet and network data. Most users do not need to define routes. On a typical small home or office LAN, the existing routes that set up the default gateways for your LAN hosts and for the DSL device provide the most appropriate path for all your Internet traffic.

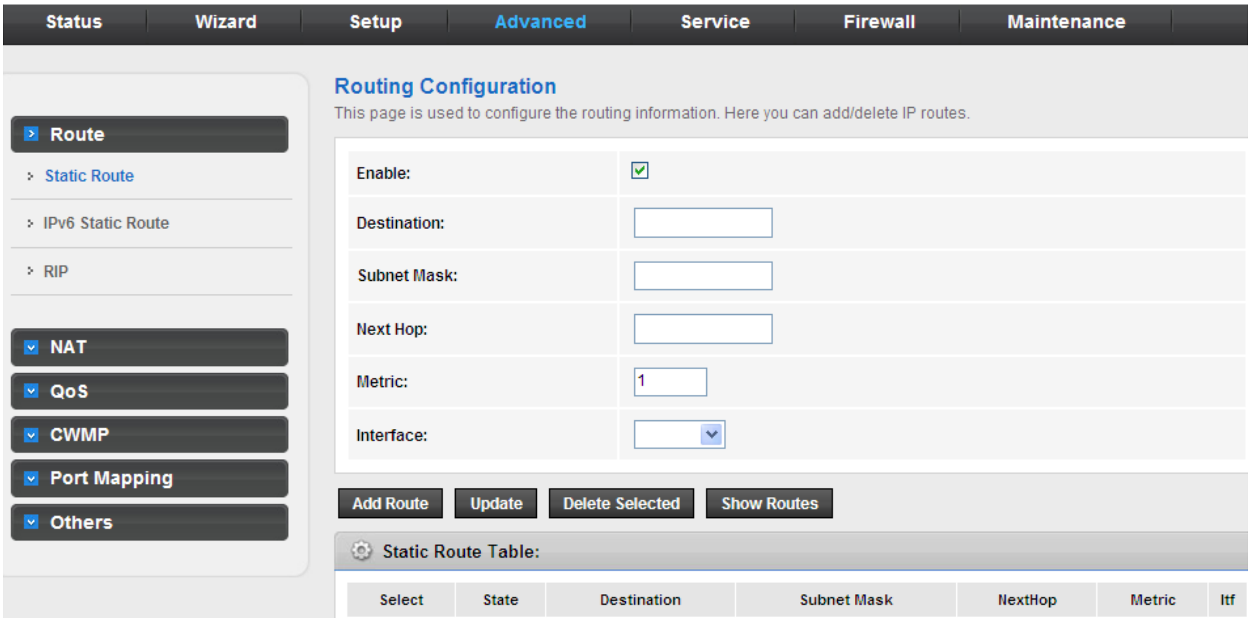
- On your LAN hosts, a default gateway directs all Internet traffic to the LAN port(s) on the DSL device. Your LAN hosts know their default gateway either because you assigned it to them when you modified your TCP/IP properties, or because you configured them to receive the information dynamically from a server whenever they access the Internet.

➢ On the DSL device itself, a default gateway is defined to direct all outbound Internet traffic to a route at your ISP. The default gateway is assigned either automatically by your ISP whenever the device negotiates an Internet access, or manually by user to set up through the configuration.

You may need to define routes if your home setup includes two or more networks or subnets, if you connect to two or more ISP services, or if you connect to a remote corporate LAN.

3.6.1.1 Static Route

Click **Static Route** in the left pane and the page shown in the following figure appears. This page is used to configure the routing information. You can add or delete IP routes.



Routing Configuration

This page is used to configure the routing information. Here you can add/delete IP routes.

Enable: ☑
Destination:
Subnet Mask:
Next Hop:
Metric: 1
Interface:

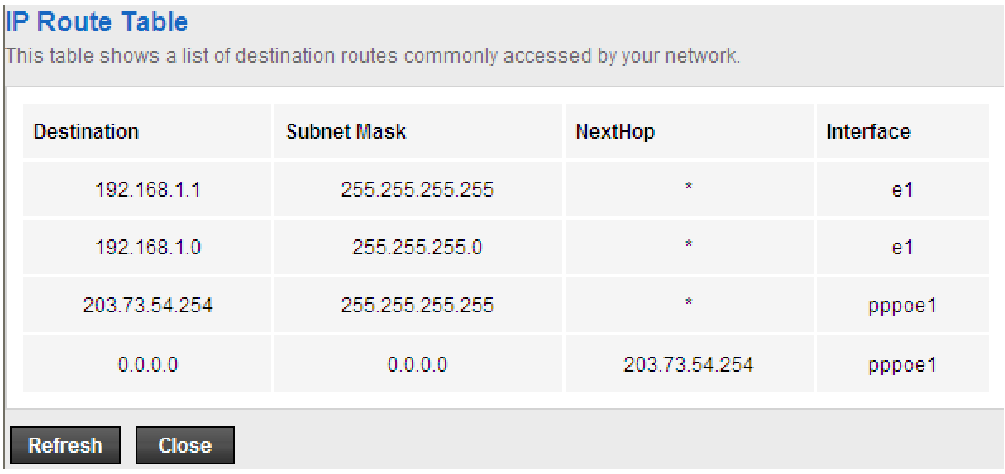
Static Route Table:

Select	State	Destination	Subnet Mask	NextHop	Metric	Itf

The following table describes the parameters:

Field	Description
Enable	Click it to enable/disable the selected route or route to be added.
Destination	The network IP address of the subnet. The destination can be specified as the IP address of a subnet or a specific host in the subnet. It can also be specified as all zeros to indicate that this route should be used for all destinations for which no other route is defined (this is the route that creates the default gateway).
Subnet Mask	The network mask of the destination subnet. The default gateway uses a mask of 0.0.0.0.
Next Hop	The IP address of the next hop through which traffic will flow towards the destination subnet.
Metric	Defines the number of hops between network nodes that data packets travel. The

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>default value is 0, which means that the subnet is directly one hop away on the local LAN network.</td></tr>
<tr><td>Interface</td><td>The WAN interface to which a static routing subnet is to be applied.</td></tr>
<tr><td>Add Route</td><td>Add a user-defined destination route.</td></tr>
<tr><td>Update</td><td>Update the selected destination route on the Static Route Table.</td></tr>
<tr><td>Delete Selected</td><td>Delete a selected destination route on the Static Route Table.</td></tr>
<tr><td>Show Routes</td><td>
Click this button to view the DSL device’s routing table. The IP Route Table displays, as shown in Figure.

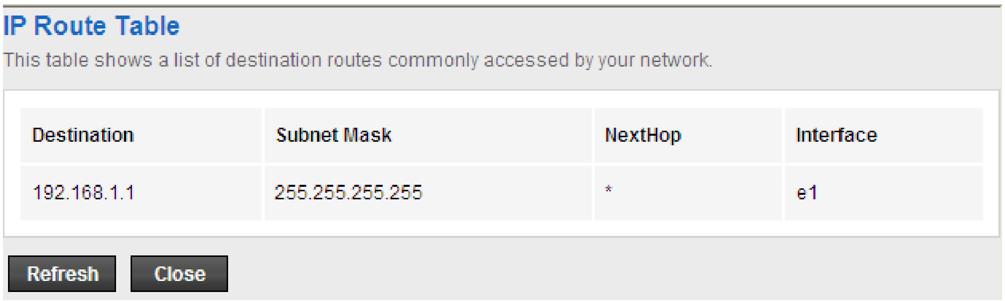


IP Route Table

This table shows a list of destination routes commonly accessed by your network.

<table>
<tr><th>Destination</th><th>Subnet Mask</th><th>NextHop</th><th>Interface</th></tr>
<tr><td>192.168.1.1</td><td>255.255.255.255</td><td>*</td><td>e1</td></tr>
<tr><td>192.168.1.0</td><td>255.255.255.0</td><td>*</td><td>e1</td></tr>
<tr><td>203.73.54.254</td><td>255.255.255.255</td><td>*</td><td>pppoe1</td></tr>
<tr><td>0.0.0.0</td><td>0.0.0.0</td><td>203.73.54.254</td><td>pppoe1</td></tr>
</table>

Click Show Routes and the page shown in the following figure appears. The table shows a list of destination routes commonly accessed by your network.



IP Route Table

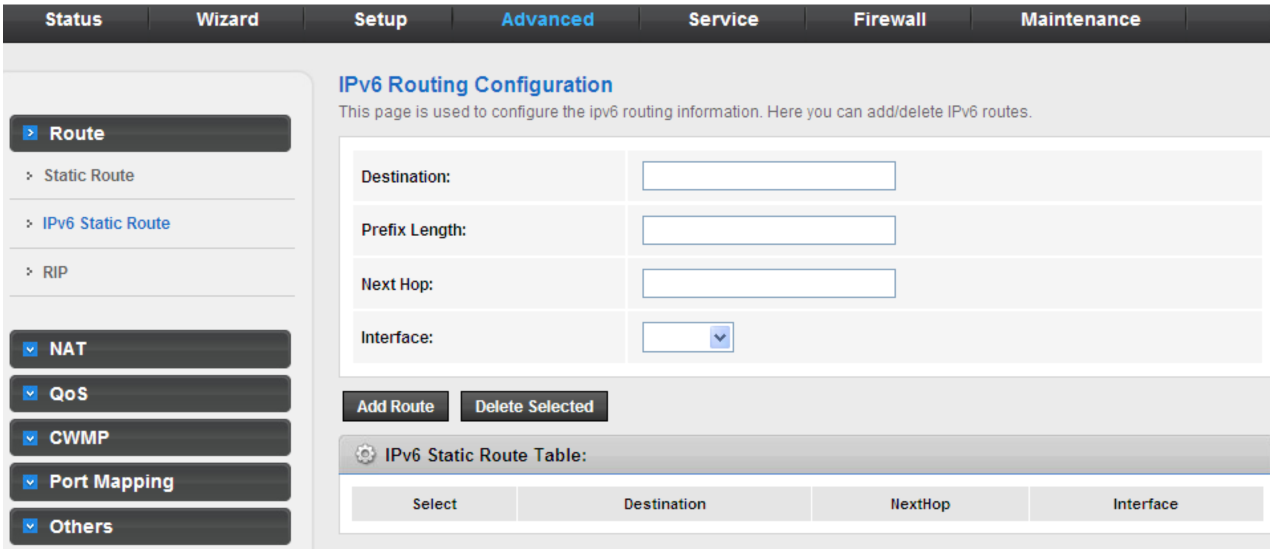
This table shows a list of destination routes commonly accessed by your network.

<table>
<tr><th>Destination</th><th>Subnet Mask</th><th>NextHop</th><th>Interface</th></tr>
<tr><td>192.168.1.1</td><td>255.255.255.255</td><td>*</td><td>e1</td></tr>
</table>

</td></tr>
</table>

3.6.1.2 IPv6 Static Route

Click **IPv6 Static Route** in the left pane and the page shown in the following figure appears. This page is used to configure the routing information. You can add or delete IP routes.



IPv6 Routing Configuration

This page is used to configure the ipv6 routing information. Here you can add/delete IPv6 routes.

Destination:	
Prefix Length:	
Next Hop:	
Interface:	

IPv6 Static Route Table:

Select	Destination	NextHop	Interface

The following table describes the parameters:

Fields	Description
Destination	Enter the IPv6 address of the destination device.
Prefix Length	Enter the prefix length of the IPV6 address.
Next Hop	Enter the IPv6 address of the next hop in the IPv6 route to the destination address.
Interface	The interface for the specified route.
Add Route	Click it to add the new static route to the IPv6 Static Route Table.
Delete the Selected	Select a row in the IPv6 Static Route Table and click it to delete the row.

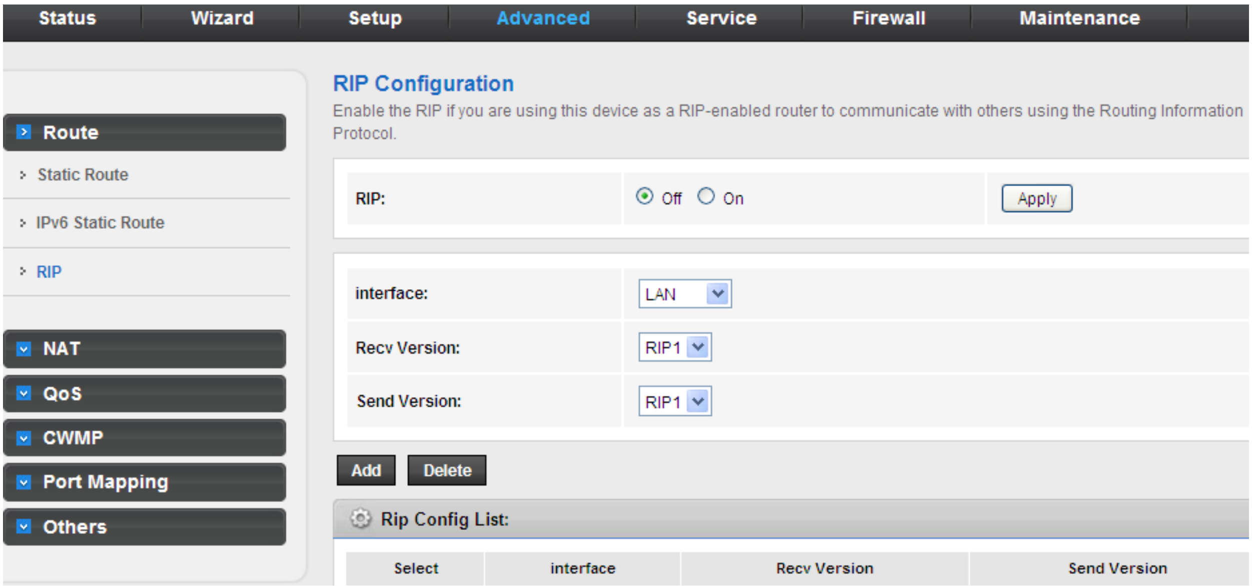
3.6.1.3 RIP

RIP is an Internet protocol you can set up to share routing table information with other routing devices on your LAN, at your ISP's location, or on remote networks connected to your network via the ADSL line. Most small home or office networks do not need to use RIP; they have only one router, such as the ADSL Router, and one path to an ISP. In these cases, there is no need to share routes, because all Internet data from the network is sent to the same ISP gateway. You may want to configure RIP if any of the following circumstances apply to your network:

- Your home network setup includes an additional router or RIP-enabled PC (other than the ADSL Router). The ADSL Router and the router will need to communicate via RIP to share their routing tables.
- Your network connects via the ADSL line to a remote network, such as a corporate network. In order

for your LAN to learn the routes used within your corporate network, they should both be configured with RIP.

➢ Your ISP requests that you run RIP for communication with devices on their network.



RIP Configuration

Enable the RIP if you are using this device as a RIP-enabled router to communicate with others using the Routing Information Protocol.

RIP: ● Off ○ On

interface: LAN

Recv Version: RIP1

Send Version: RIP1

Rip Config List:

Select	interface	Recv Version	Send Version

The following table describes the parameters:

Field	Description
RIP	You can select **OFF** or **ON**. In this example, **OFF** is selected.
Apply	Click it to save the settings on this page.
Interface	Choose the router interface that uses RIP.
Recv Version	Choose the interface version that receives RIP messages. You can choose **RIP1**, **RIP2**, or **Both**. ● Choose **RIP1** to indicate the router receives RIP v1 messages. ● Choose **RIP2** to indicate the router receives RIP v2 messages. ● Choose **Both** to indicate the router receives RIP v1 and RIP v2 messages.
Send Version	The working mode for sending RIP messages. You can choose **RIP1** or **RIP2**. ● Choose **RIP1** to indicate the router broadcasts RIP1 messages only. ● Choose **RIP2** to indicate the router multicasts RIP2 messages only.
Add	Click it to add the RIP interface to the **Rip Config List**.
Delete	Select a row in the **Rip Config List** and click it to delete the row.

3.6.2 NAT

Choose **Advanced** > **NAT** and the page shown in the following figure appears. The page displayed contains **DMZ**, **Virtual Server**, **ALG**, **NAT Exclude IP**, **Port Trigger**, **FTP ALG Port**, and **NAT IP Mapping**.

3.6.2.1 DMZ

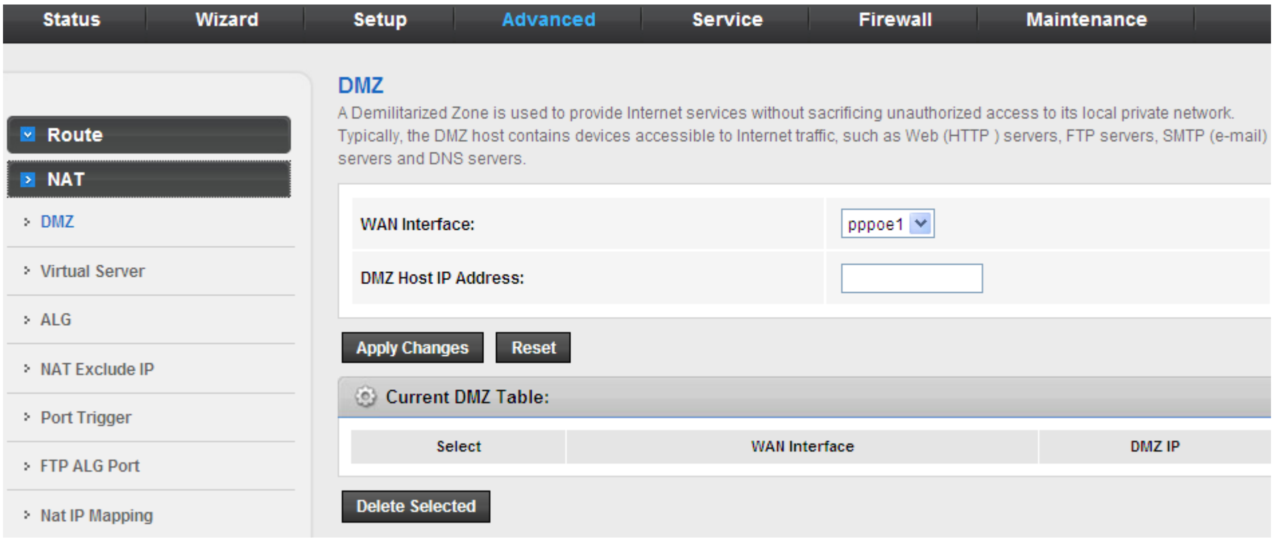
Demilitarized Zone (DMZ) is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

Click **DMZ** in the left pane and the page shown in the following figure appears. The following describes how to configure manual DMZ.

Select **Enable DMZ** to enable this function.

Enter an IP address of the DMZ host.

Click **Apply Changes** to save the settings on this page temporarily.



DMZ

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

WAN Interface: pppoe1

DMZ Host IP Address:

Current DMZ Table:

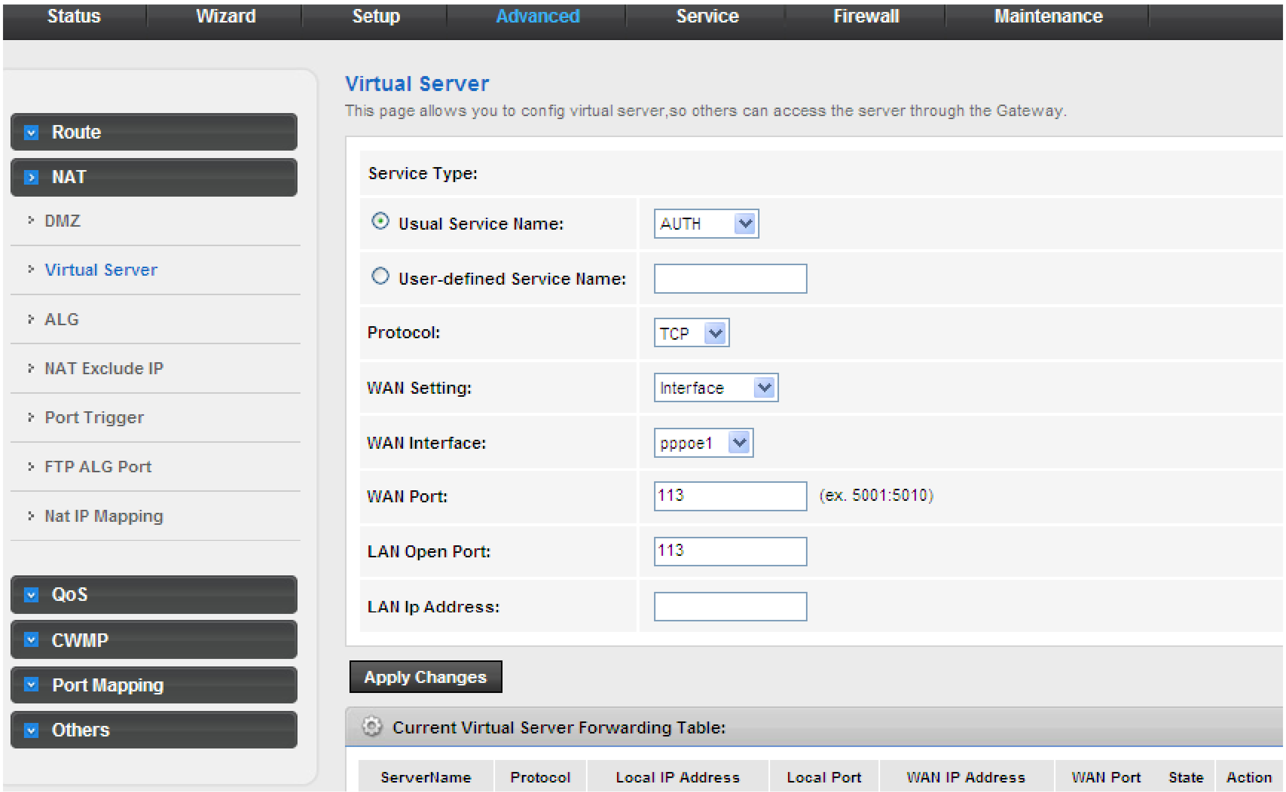
Select	WAN Interface	DMZ IP

The following table describes the parameters:

Field	Description
WAN Interface	Choose a WAN Interface.
DMZ Host IP Address	Enter an IP address of the DMZ host.
Current DMZ Table	A list of the previously configured DMZ information.
Apply Changes	Click Apply Changes to add new settings.
Reset	Clear the settings.
Delete the Selected	Select the number of rows from the Current DMZ Table to be deleted.

3.6.2.2 Virtual Server

Internet users would not be able to access a server on your LAN because of native NAT protection.The "virtual server" feature solves these problems and allows internet users to connect to your servers.



Virtual Server

This page allows you to config virtual server,so others can access the server through the Gateway.

Service Type:

● Usual Service Name: AUTH

○ User-defined Service Name:

Protocol: TCP

WAN Setting: Interface

WAN Interface: pppoe1

WAN Port: 113 (ex. 5001:5010)

LAN Open Port: 113

LAN Ip Address:

Current Virtual Server Forwarding Table:

ServerName	Protocol	Local IP Address	Local Port	WAN IP Address	WAN Port	State	Action

The following table describes the parameters:

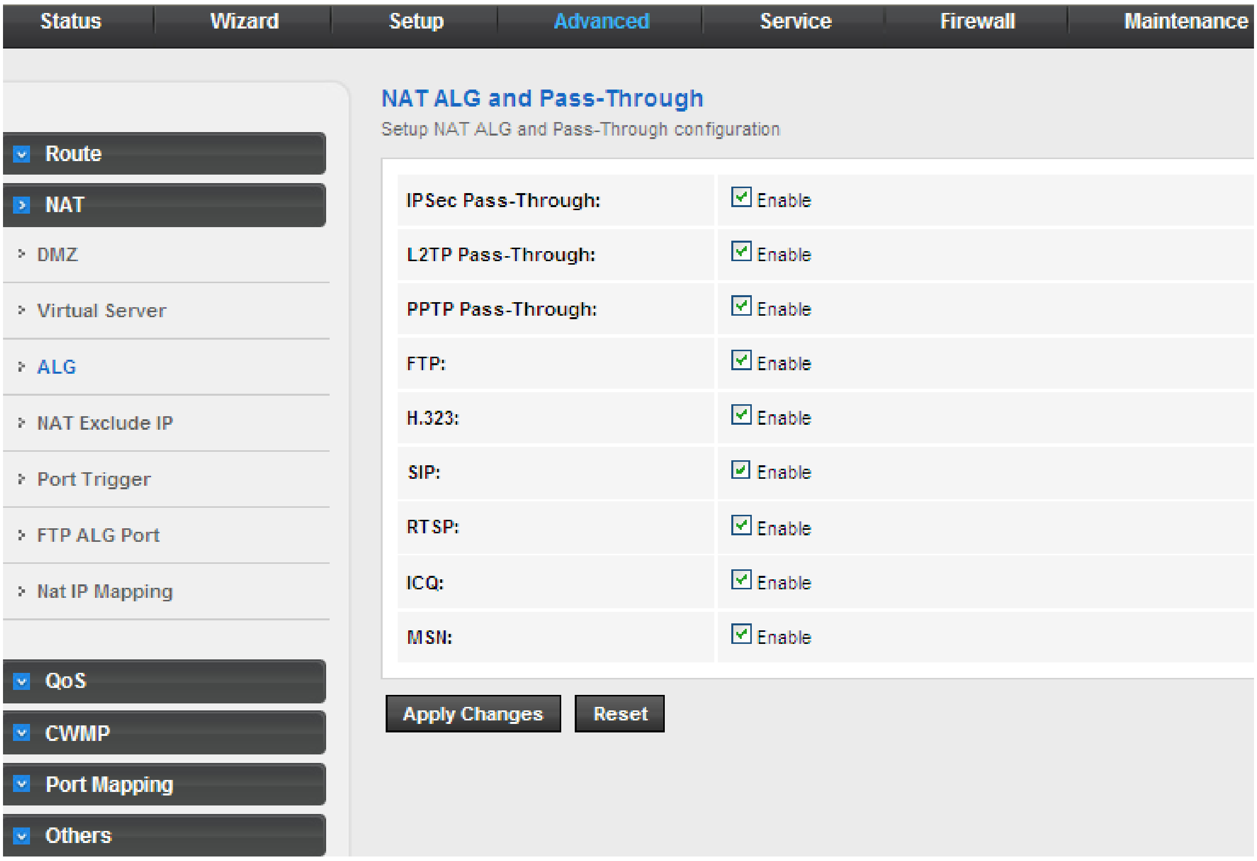
Field	Description
Service Type	You can select the common service type, for example, **AUTH**, **DNS** or **FTP**. You can also define a service name. ● If you select **Usual Service Name**, the corresponding parameter has the default settings. ● If you select **User-defined Service Name**, you need to enter the corresponding parameters.
Protocol	Choose the transport layer protocol that the service type uses. You can choose **TCP** or **UDP**.
WAN Setting	You can choose **Interface** or **IP Address**.
WAN Interface	Choose the WAN interface that will apply virtual server.
WAN Port	Choose the access port on the WAN.
LAN Open Port	Enter the port number of the specified service type.
LAN IP Address	Enter the IP address of the virtual server. It is in the same network segment with LAN IP address of the router.

3.6.2.3 ALG

An application layer gateway (ALG) is a feature on ScreenOS gateways that enables the gateway to parse application layer payloads and take decisions on them. ALGs are typically employed to support applications that use the application layer payload to communicate the dynamic Transmission Control Protocol (TCP) or

User Datagram Protocol (UDP) ports on which the applications open data connections. Such applications include the File Transfer Protocol (FTP) and various IP telephony protocols.

ALG consists of a security component that augments a firewall or NAT employed in a computer network. It allows customized NAT traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols such as FTP, SIP, RTSP, file transfer in IM applications, etc. In order for these protocols to work through NAT or a firewall, either the application has to know about an address/port number combination that allows incoming packets, or the NAT has to monitor the control traffic and open up port mappings (*firewall pinhole*) dynamically as required. Legitimate application data can thus be passed through the security checks of the firewall or NAT that would have otherwise restricted the traffic for not meeting its limited filter criteria.



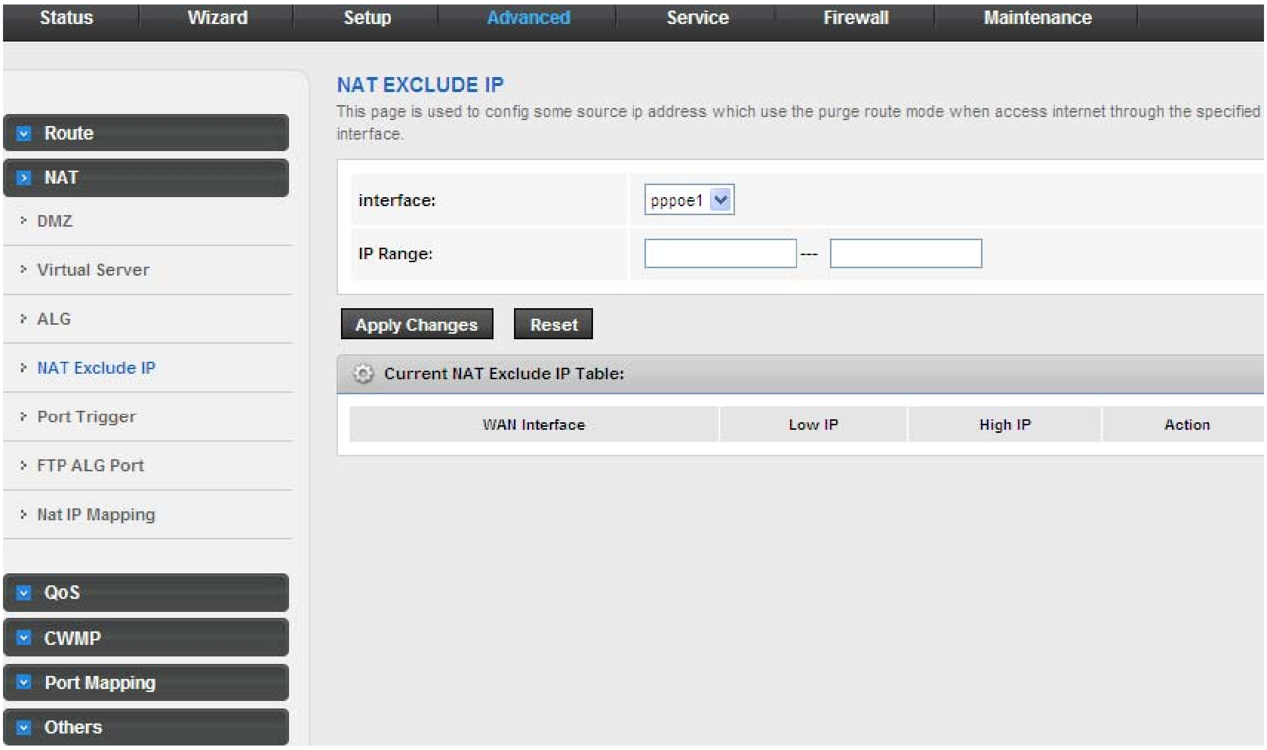
NAT ALG and Pass-Through

Setup NAT ALG and Pass-Through configuration

IPSec Pass-Through:	☑ Enable
L2TP Pass-Through:	☑ Enable
PPTP Pass-Through:	☑ Enable
FTP:	☑ Enable
H.323:	☑ Enable
SIP:	☑ Enable
RTSP:	☑ Enable
ICQ:	☑ Enable
MSN:	☑ Enable

3.6.2.4 NAT excluding IP

NAT improves network security in effect by hiding the private network behind one global and visible IP address. NAT address mapping can also be used to link two IP domains via a LAN-to-LAN connection. Network Address Translation (NAT) is the method by which the Router shares the single IP address assigned by your ISP with the other computers on your network. This function should only be used if your ISP assigns you multiple IP addresses or you need NAT disabled for an advanced system configuration. If you have a single IP address and you turn NAT off, the computers on your network will not be able to access the Internet. Other problems may also occur. Turning off NAT will disable your firewall functions.



NAT EXCLUDE IP

This page is used to config some source ip address which use the purge route mode when access internet through the specified interface.

interface: pppoe1

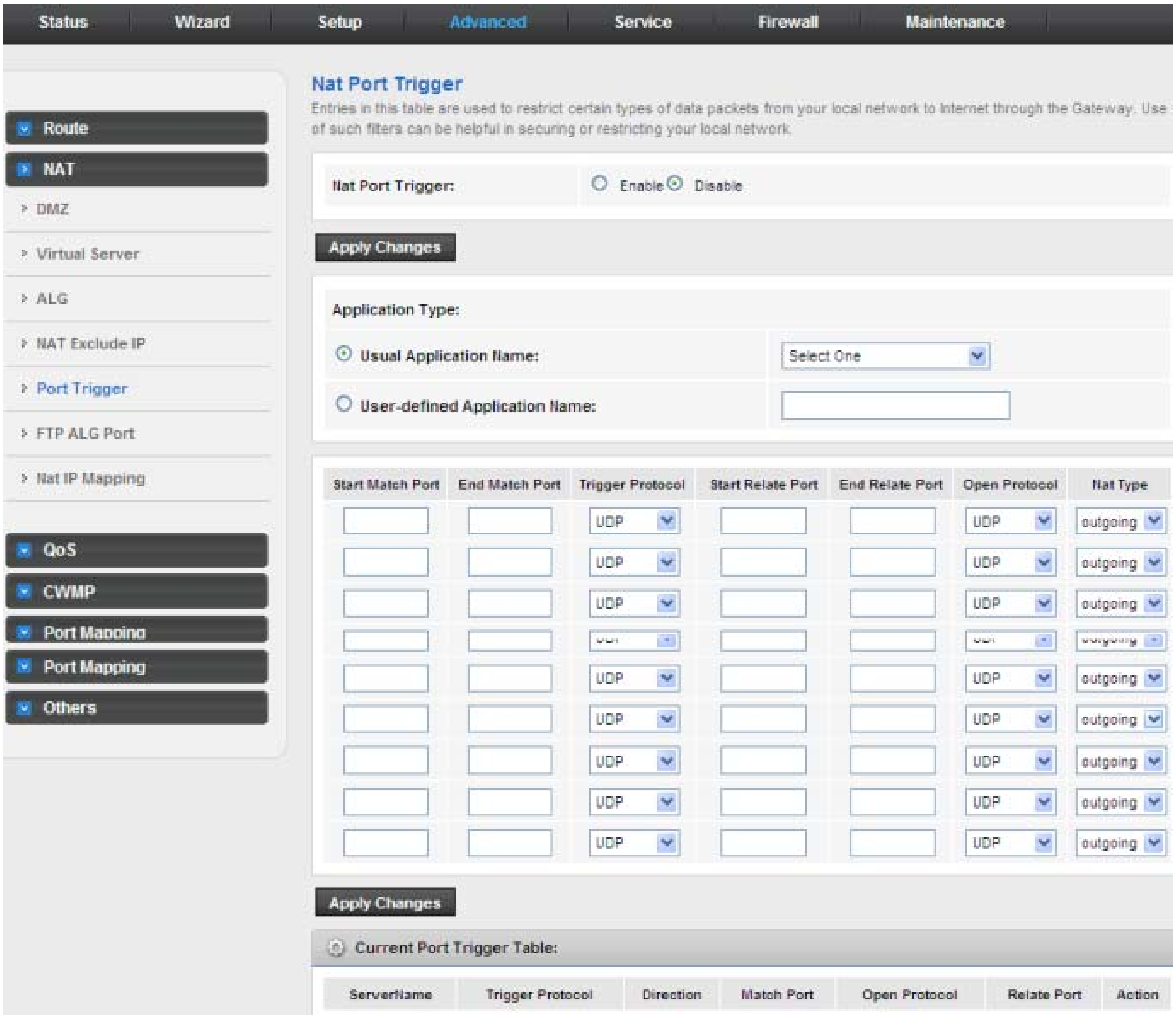
IP Range: ___ --- ___

Current NAT Exclude IP Table:

WAN Interface	Low IP	High IP	Action

3.6.2.5 Port Trigger

Port triggering is a configuration option on a NAT-enabled router that allows a host machine to dynamically and automatically forward a specific port back to itself. Port triggering opens an incoming port when your computer is using a specified outgoing port for specific traffic. Port triggering does not require that you know the computer's IP address in advance. The IP address is captured automatically. Port triggering requires specific outbound traffic to open the inbound ports, and the triggered ports are closed after a period of no activity.



Nat Port Trigger

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Nat Port Trigger: ○ Enable ● Disable

Apply Changes

Application Type:

● Usual Application Name: Select One

○ User-defined Application Name:

Start Match Port	End Match Port	Trigger Protocol	Start Relate Port	End Relate Port	Open Protocol	Nat Type
		UDP			UDP	outgoing
		UDP			UDP	outgoing
		UDP			UDP	outgoing
		UDP			UDP	outgoing
		UDP			UDP	outgoing
		UDP			UDP	outgoing
		UDP			UDP	outgoing
		UDP			UDP	outgoing
		UDP			UDP	outgoing

Apply Changes

Current Port Trigger Table:

ServerName	Trigger Protocol	Direction	Match Port	Open Protocol	Relate Port	Action

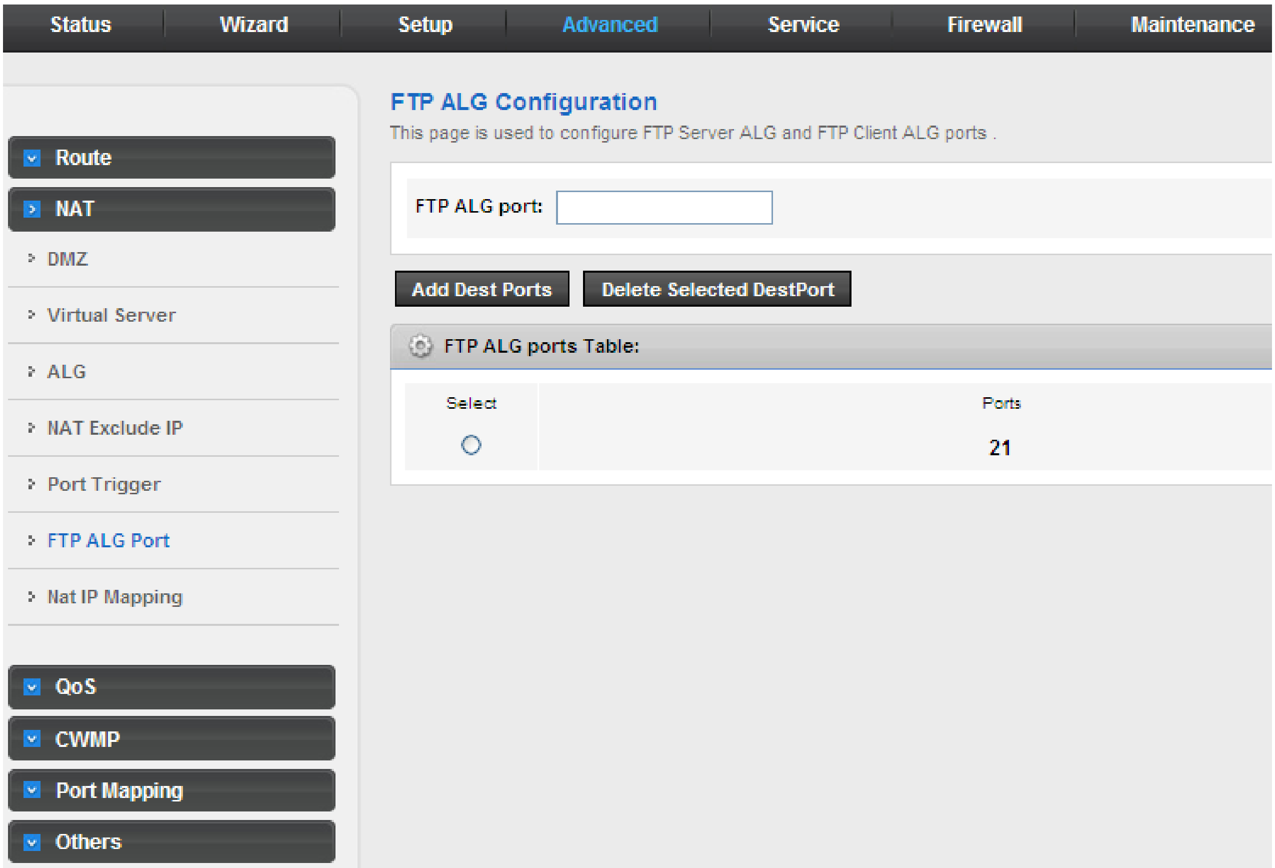
Click the **Usual Application Name** drop-down menu to choose the application you want to setup for port triggering. When you have chosen an application the default Trigger settings will populate the table below.

If the application you want to set up isn't listed, click the **User-defined Application Name** radio button and type in a name for the trigger in the Custom application field. Configure the **Start Match Port**, **End Match Port**, **Trigger Protocol**, **Start Relate Port**, **End Relate Port, Open Protocol** and **Nat type** settings for the port trigger you want to configure.

When you have finished, click the **Apply changes** button.

3.6.2.6 FTP ALG Port

FTP uses two communication channels, one for control commands and one for the actual files being transferred. When an FTP session is opened, the FTP client establishes a TCP connection (the control channel) to (usually) port 21 on the FTP server. What happens after this point depends on the mode of FTP being used.



FTP ALG Configuration

This page is used to configure FTP Server ALG and FTP Client ALG ports .

FTP ALG port:

FTP ALG ports Table:

Select	Ports
○	21

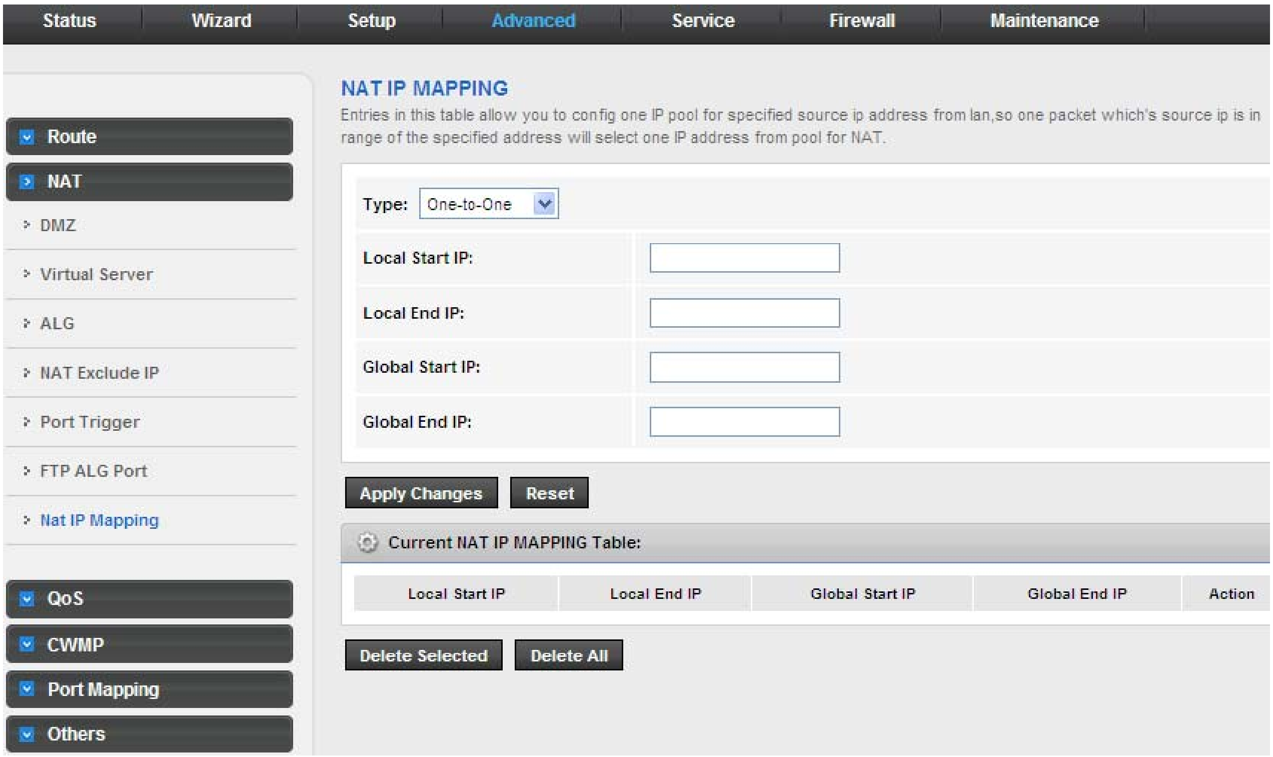
The following table describes the parameters:

Field	Description
FTP ALG port	Set an FTP ALG port.
Add Dest. Ports	Add a port configuration.
Delete Selected Dest. Port	Delete a selected port configuration from the list.

3.6.2.7 NAT IP Mapping

NAT is short for Network Address Translation. The Network Address Translation Settings window allows you to share one WAN IP address for multiple computers on your LAN. Click **NAT IP Mapping** in the left pane and the page shown in the following figure appears.

Entries in this table allow you to configure one IP pool for specified source IP address from LAN, so one packet whose source IP is in range of the specified address will select one IP address from the pool for NAT.



NAT IP MAPPING

Entries in this table allow you to config one IP pool for specified source ip address from lan,so one packet which's source ip is in range of the specified address will select one IP address from pool for NAT.

Type: One-to-One

Local Start IP:

Local End IP:

Global Start IP:

Global End IP:

Current NAT IP MAPPING Table:

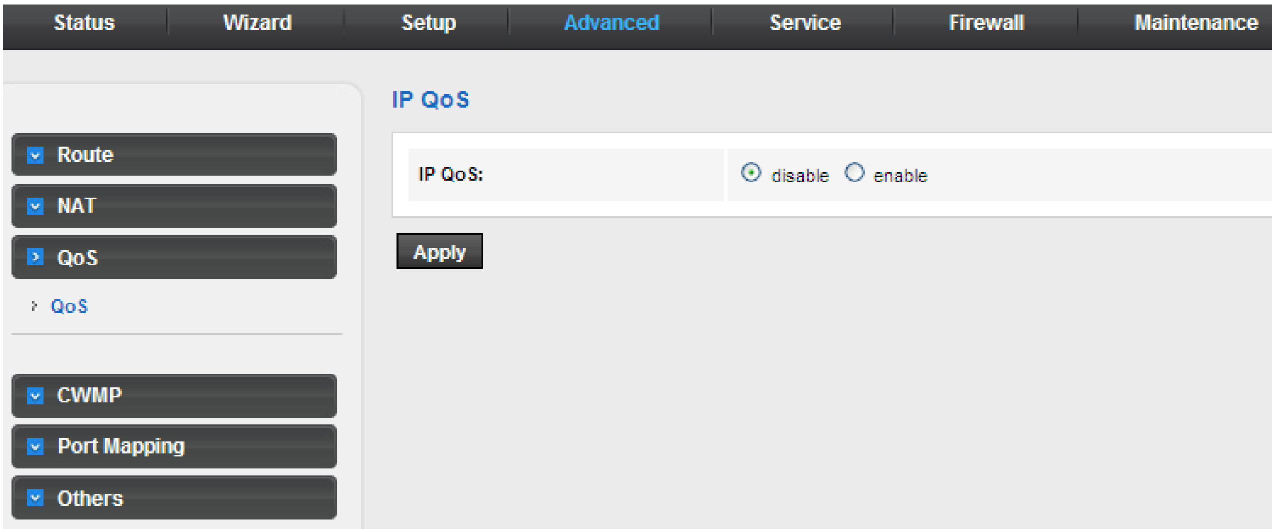
Local Start IP	Local End IP	Global Start IP	Global End IP	Action

The following table describes the parameters:

Fields	Description
Type	There are four types: one-to-one, Many-to-One, Many-to-Many, Many-to-one.
Local Start & End IP	Enter the local IP Address you plan to map to. Local Start IP is the starting local IP address and Local End IP is the ending local IP address. If the rule is for all local IPs, then the Start IP is 0.0.0.0 and the End IP is 255.255.255.255
Global Start & End IP	Enter the Globe IP Address you want to do NAT. Global Start IP is the starting global IP address and Global End IP is the ending global IP address. If you have a dynamic IP, enter 0.0.0.0 as the global Start IP.
NAT IP Mapping Table	This displays the information about the Mapping addresses.

3.6.3 QoS

The DSL device provides a control mechanism that can provide different priority to different users or data flows. The QoS is enforced by the QoS rules in the QoS table. A QoS rule contains two configuration blocks: **Traffic Classification** and **Action**. The Traffic Classification enables you to classify packets on the basis of various fields in the packet and perhaps the physical ingress port. The Action enables you to assign the strictly priority level for and mark some fields in the packet that matches the Traffic Classification rule. You can configure any or all field as needed in these two QoS blocks for a QoS rule.



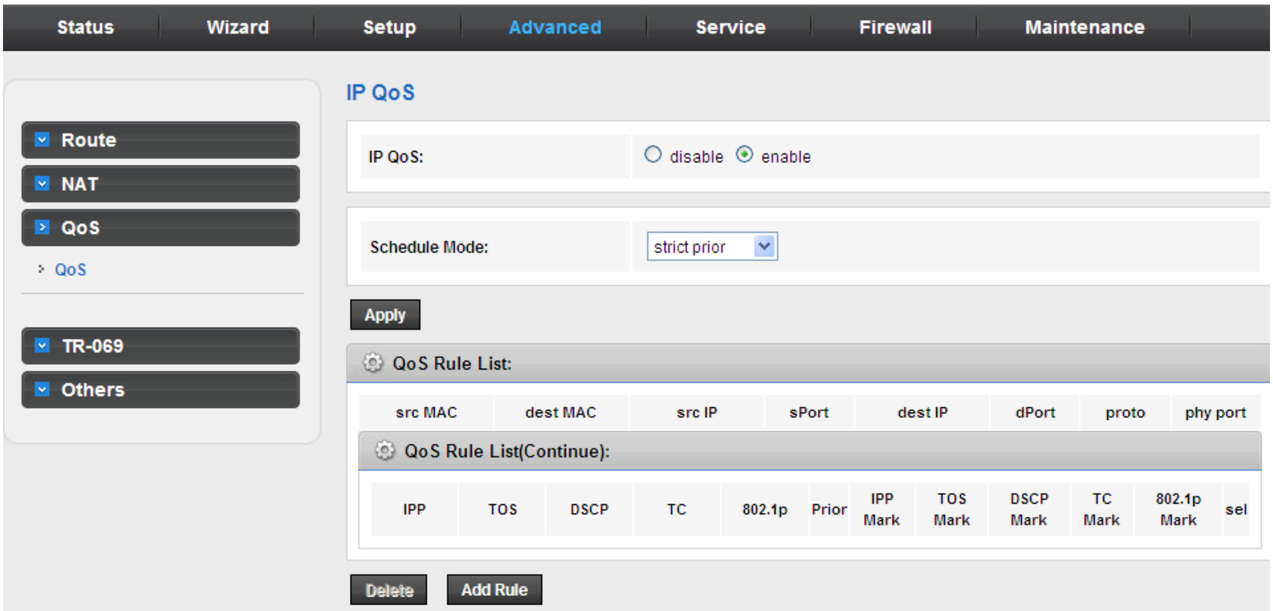
IP QoS

IP QoS: ● disable ○ enable

Enable QoS and click **Apply** to enable IP QoS function.

Click **add rule** to add a new IP QoS rule.

The page shown in the following figure appears.



IP QoS

IP QoS: ○ disable ● enable

Schedule Mode: strict prior

QoS Rule List:

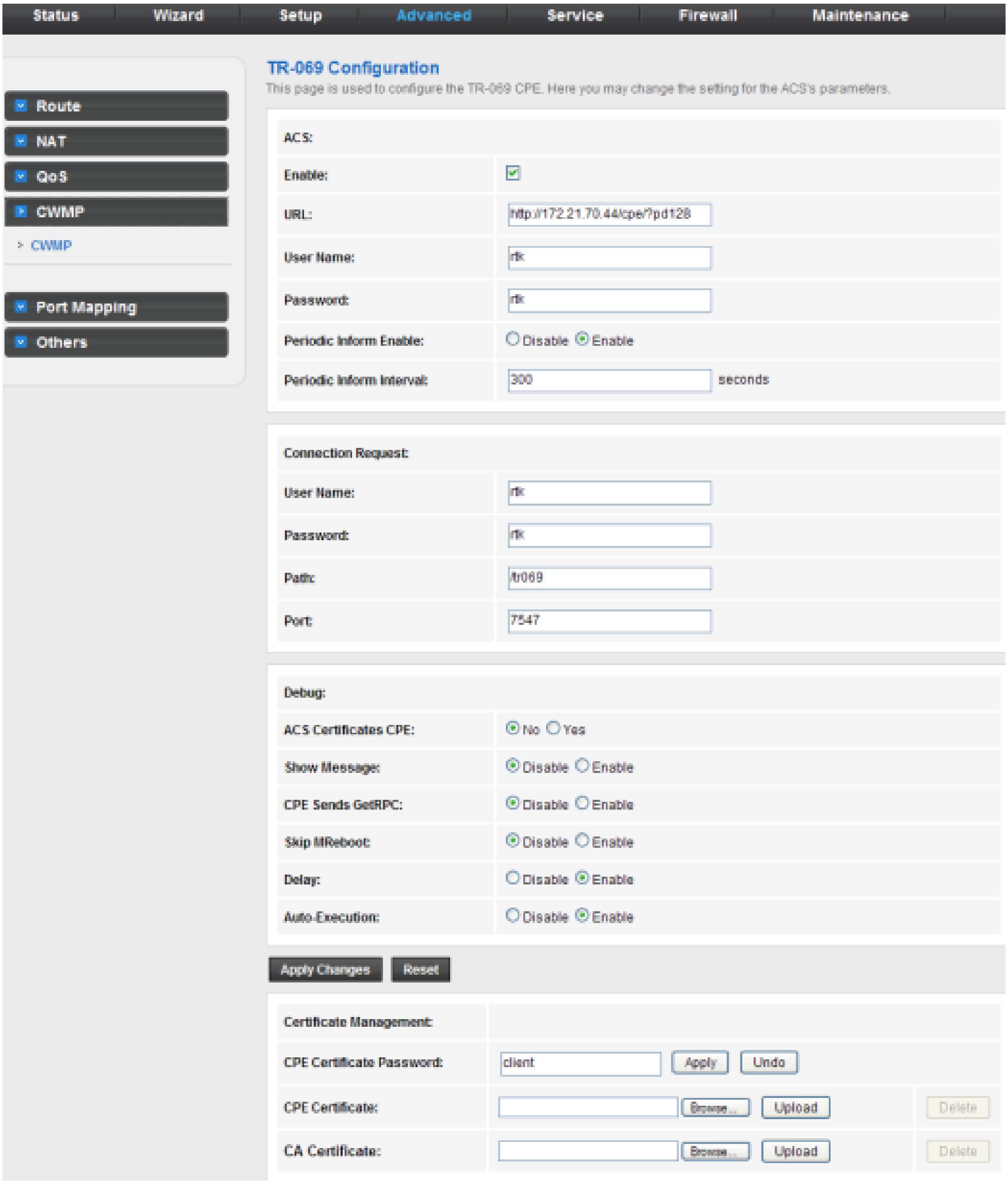
src MAC	dest MAC	src IP	sPort	dest IP	dPort	proto	phy port

QoS Rule List(Continue):

IPP	TOS	DSCP	TC	802.1p	Prior	IPP Mark	TOS Mark	DSCP Mark	TC Mark	802.1p Mark	sel

3.6.4 CWMP (TR-069)

Choose **Advanced** > **CWMP** and the page shown in the following page appears. On this page, you can configure the TR-069 CPE.



TR-069 Configuration

This page is used to configure the TR-069 CPE. Here you may change the setting for the ACS's parameters.

ACS:

Enable: ☑

URL: http://172.21.70.44/cpe/?pd128

User Name: rtk

Password: rtk

Periodic Inform Enable: ○ Disable ● Enable

Periodic Inform Interval: 300 seconds

Connection Request:

User Name: rtk

Password: rtk

Path: /tr069

Port: 7547

Debug:

ACS Certificates CPE: ● No ○ Yes

Show Message: ● Disable ○ Enable

CPE Sends GetRPC: ● Disable ○ Enable

Skip MReboot: ● Disable ○ Enable

Delay: ○ Disable ● Enable

Auto-Execution: ○ Disable ● Enable

Certificate Management:

CPE Certificate Password: client

CPE Certificate:

CA Certificate:

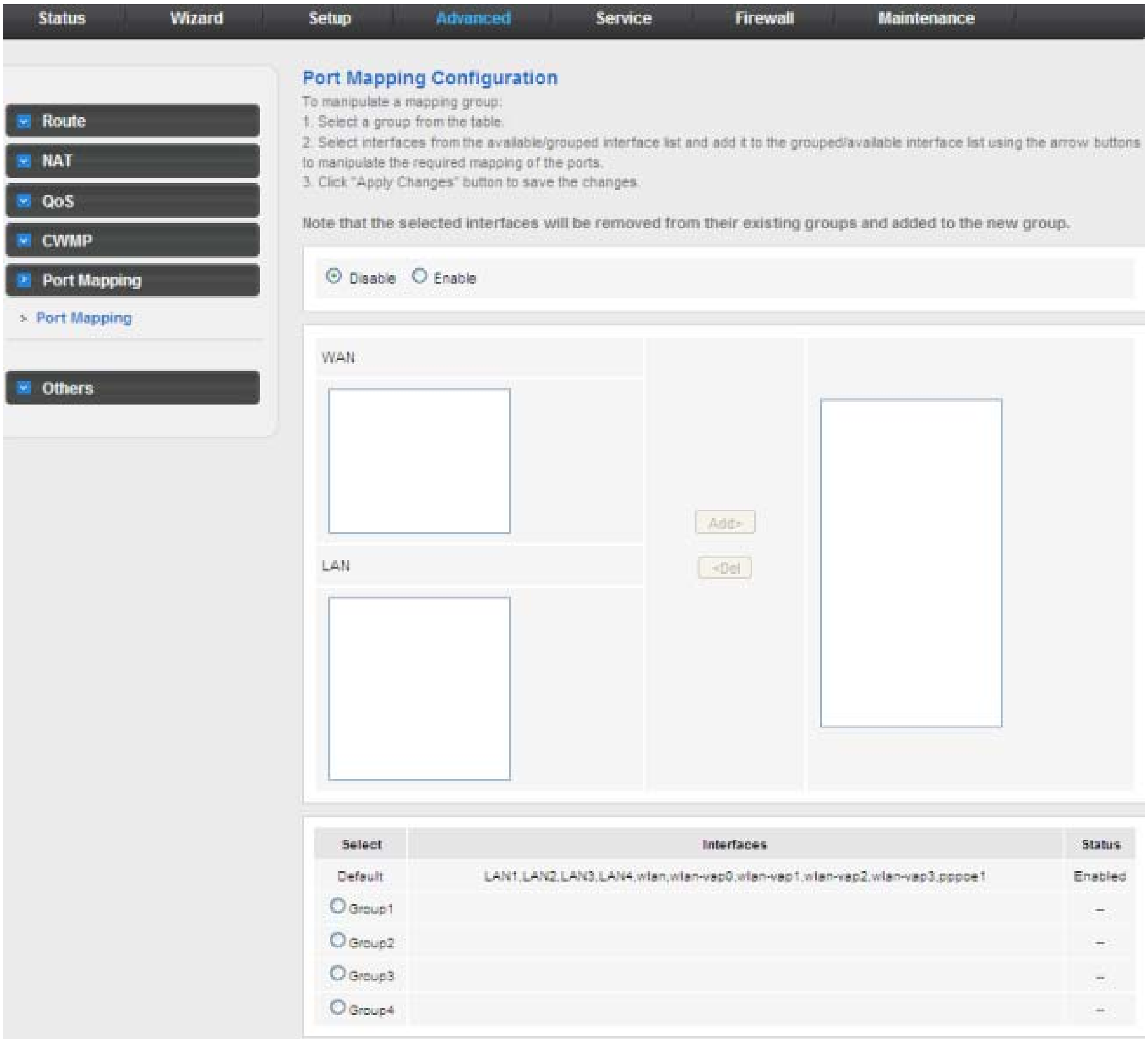
The following table describes the parameters:

Field	Description
ACS	
Enable	Enable/Disable the function to access.

Field	Description
URL	The URL of the auto-configuration server to connect to.
User Name	The user name for logging in to the ACS.
Password	The password for logging in to the ACS.
Periodic Inform Enable	Select **Enable** to periodically connect to the ACS to check whether the configuration updates.
Periodic Inform Interval	Specify the amount of time between connections to ACS.
Connection Request	
User Name	The connection username provided by TR-069 service.
Password	The connection password provided by TR-069 service.
Debug	
Show Message	Select **Enable** to display ACS SOAP messages on the serial console.
CPE sends GetRPC	Select **Enable**, the router contacts the ACS to obtain configuration updates.
Skip MReboot	Specify whether to send an MReboot event code in the inform message.
Delay	Specify whether to start the TR-069 program after a short delay.
Auto-Execution	Specify whether to automatically start the TR-069 after the router is powered on.

3.6.5 Port Mapping

The ADSL device provides multiple interface groups. Up to five interface groups are supported including one default group. The LAN and WAN interfaces could be included. Traffic coming from one interface of a group can only be flowed to the interfaces in the same interface group. Thus, the DSL device can isolate traffic from group to group for some application. By default, all the interfaces (LAN and WAN) belong to the default group, and the other four groups are all empty. It is possible to assign any interface to any group but only one group.



Port Mapping Configuration

To manipulate a mapping group:

1. Select a group from the table.
2. Select interfaces from the available/grouped interface list and add it to the grouped/available interface list using the arrow buttons to manipulate the required mapping of the ports.
3. Click "Apply Changes" button to save the changes.

Note that the selected interfaces will be removed from their existing groups and added to the new group.

● Disable ○ Enable

Select	Interfaces	Status
Default	LAN1,LAN2,LAN3,LAN4,wlan,wlan-vap0,wlan-vap1,wlan-vap2,wlan-vap3,pppoe1	Enabled
○ Group1		--
○ Group2		--
○ Group3		--
○ Group4		--

The following table describes the parameters:

Fields	Description
Enabled/Disabled	Click radio button to enable/disable the interface group feature. If disabled, all interfaces belong to the default group.

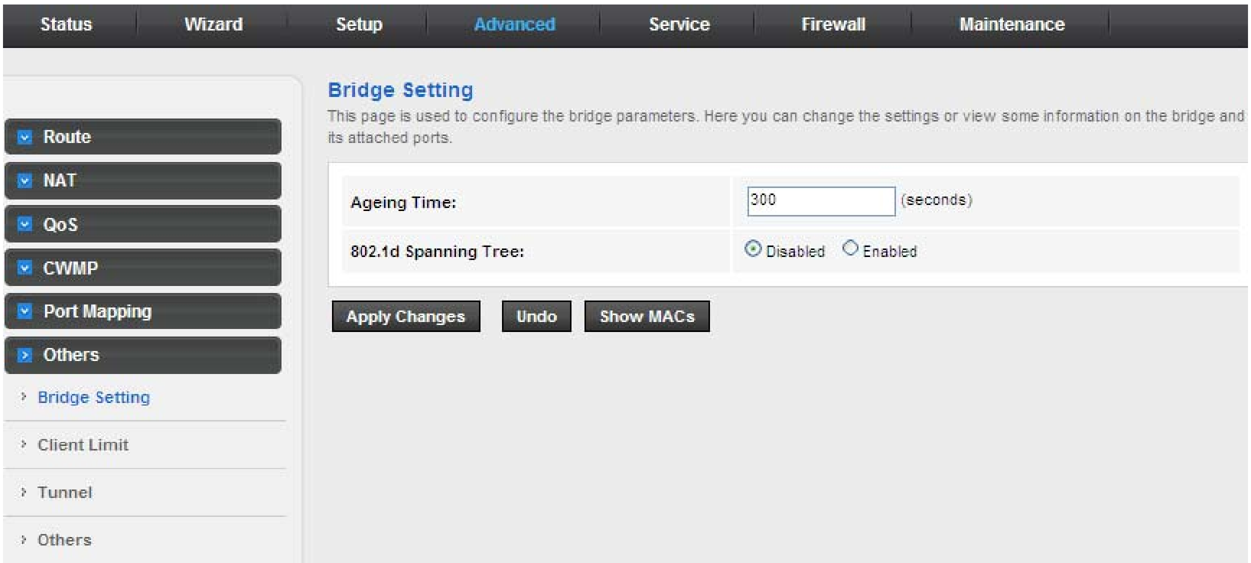
Interface groups	To manipulate a mapping group: 1. Select a group from the table. 2. Select interfaces from the available/grouped interface list and add it to the grouped/available interface list using the arrow buttons to manipulate the required mapping of the ports.

3.6.6. Others

Choose **Advance > Others** and the page shown in the following figure appears. The page displayed contains **Bridge Setting**, **Client Limit**, **Tunnel** and **Others**.

3.6.6.1 Bridge Setting

Choose **Advance** > **Others** > **Bridge Setting** and the page shown in the following figure appears. This page is used to configure the bridge parameters. You can change the settings or view some information on the bridge and its attached ports.



Bridge Setting

This page is used to configure the bridge parameters. Here you can change the settings or view some information on the bridge and its attached ports.

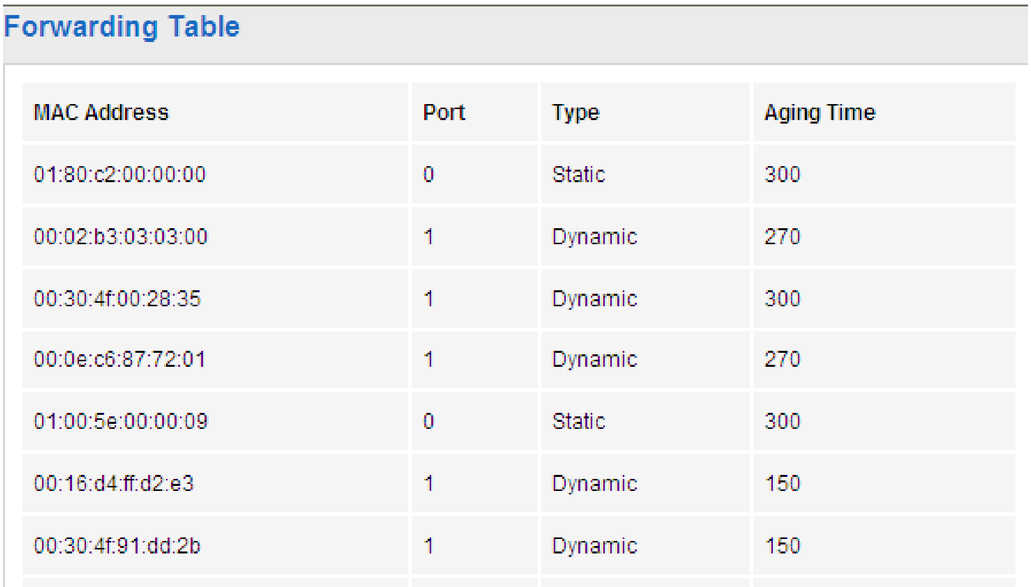
Ageing Time: 300 (seconds)

802.1d Spanning Tree: ● Disabled ○ Enabled

The following table describes the parameters:

Field	Description
Aging Time	If the host is idle for 300 seconds (default value), its entry is deleted from the bridge table.
802.1d Spanning Tree	You can select **Disable** or **Enable**. Select **Enable** to provide path redundancy while preventing undesirable loops in your network.
Show MACs	Click it to show a list of the learned MAC addresses for the bridge.

Click **Show MACs** and the page shown in the following figure appears. This table shows a list of learned MAC addresses for this bridge.

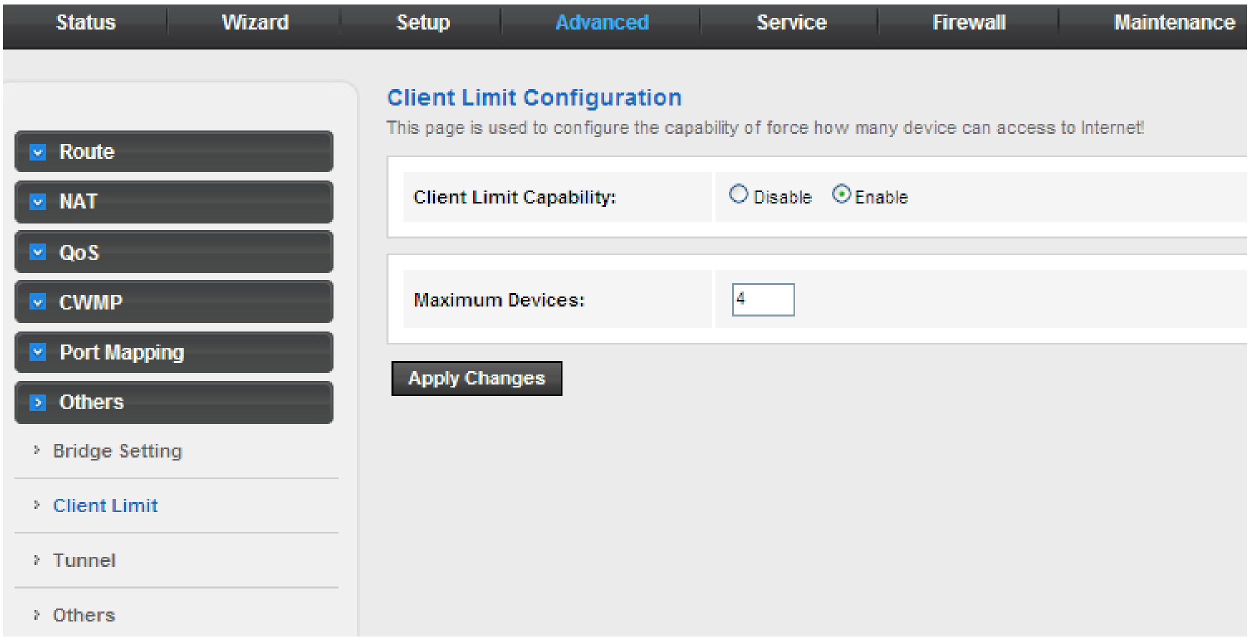


Forwarding Table

MAC Address	Port	Type	Aging Time
01:80:c2:00:00:00	0	Static	300
00:02:b3:03:03:00	1	Dynamic	270
00:30:4f:00:28:35	1	Dynamic	300
00:0e:c6:87:72:01	1	Dynamic	270
01:00:5e:00:00:09	0	Static	300
00:16:d4:ff:d2:e3	1	Dynamic	150
00:30:4f:91:dd:2b	1	Dynamic	150

3.6.6.2 Client Limit

Choose **Advance** > **Others** > **Client Limit** and the page shown in the following figure appears. This page is used to configure the capability of forcing how many devices can access the Internet.



Client Limit Configuration

This page is used to configure the capability of force how many device can access to Internet!

Client Limit Capability: ○ Disable ● Enable

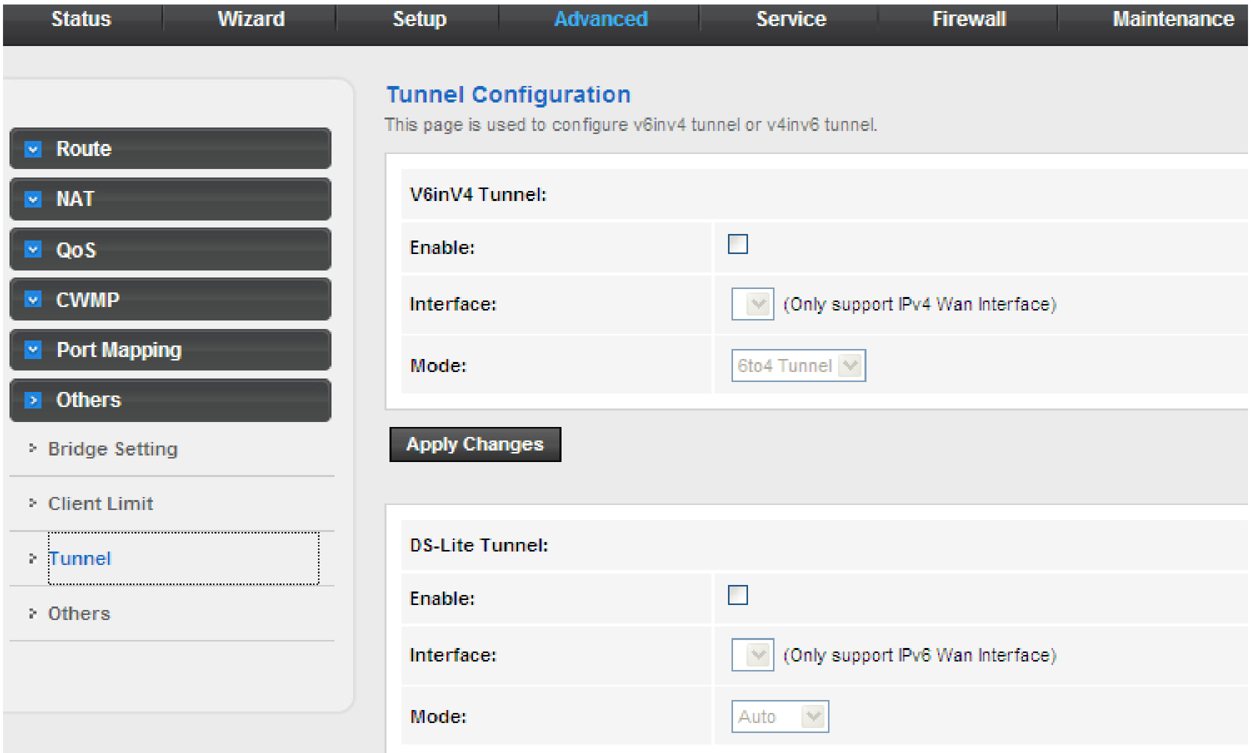
Maximum Devices: 4

Apply Changes

Fields	Description
Client Limit Capability	Enable/Disable the function to access If enabled, maximum devices would be 32; default is 4.

3.6.6.3 Tunnel

Choose **Advanced** > **Others** > **Tunnel** and the page shown in the following figure appears. This page is used to configure the IPv6 with LAN to transfer to IPv4.



Tunnel Configuration

This page is used to configure v6inv4 tunnel or v4inv6 tunnel.

V6inV4 Tunnel:

Enable: □

Interface: (Only support IPv4 Wan Interface)

Mode: 6to4 Tunnel

DS-Lite Tunnel:

Enable: □

Interface: (Only support IPv6 Wan Interface)

Mode: Auto

The following table describes the parameters:

V6inV4 Tunnel

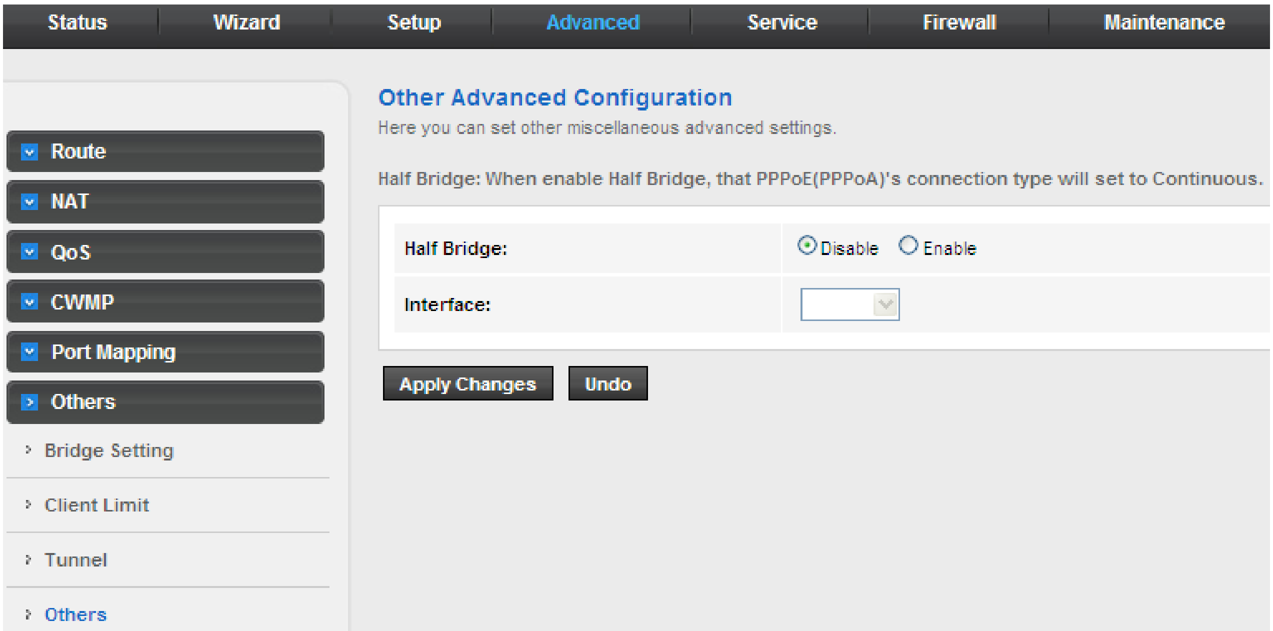
Field	Description
Enable	Enable or Disable the V6inV4 Tunnel.
Interface Name	Select the current WAN interface used as tunnel interface.
Mode	6to4 Tunnel or 6rd Tunnel.

DS-Lite Tunnel

Field	Description
Enable	Enable or disable the DS-Lite tunnel.
Interface	Select the current WAN interface used as tunnel interface.
Mode	Auto or manual.

3.6.6.4 Others

Choose **Advanced > Others > Others** in the left pane and the page shown in the following figure appears. You can enable half bridge so that the PPPoE or PPPoA connection will set to Continuous.



Other Advanced Configuration

Here you can set other miscellaneous advanced settings.

Half Bridge: When enable Half Bridge, that PPPoE(PPPoA)'s connection type will set to Continuous.

Half Bridge:	● Disable ○ Enable
Interface:	

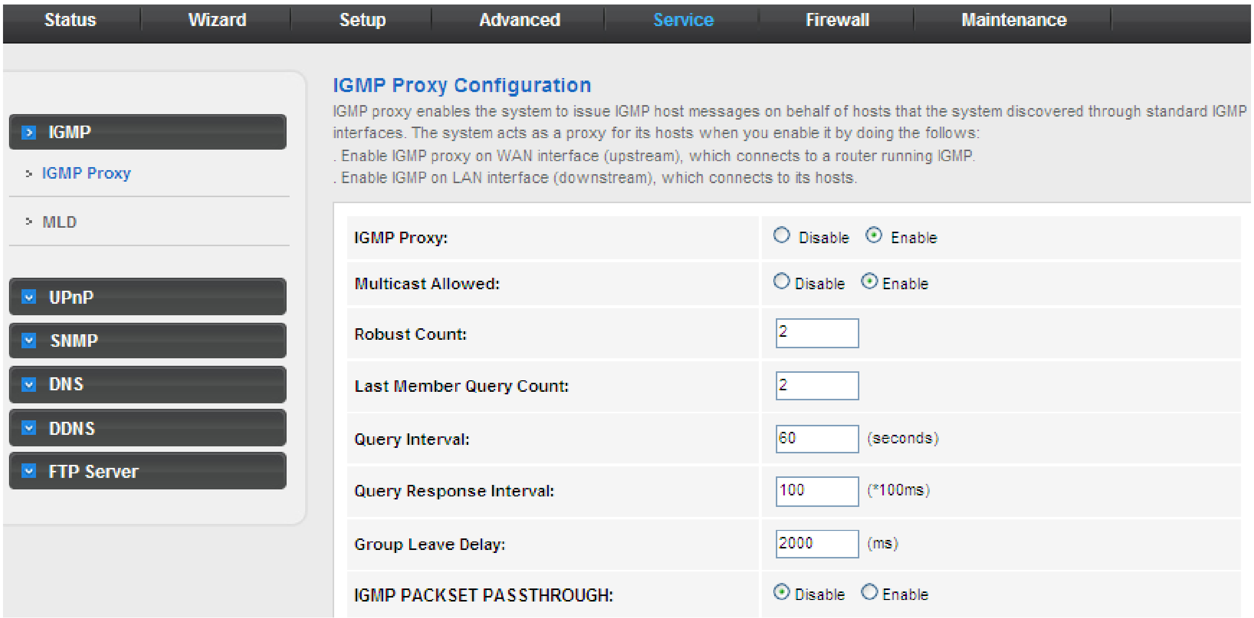
3.7 Service

In the navigation bar, click **Service**. On the **Service** page that is displayed contains **IGMP**, **UPnP**, **SNMP DNS** and **DDNS**.

3.7.1 IGMP

3.7.1.1 IGMP Proxy

Choose **Service** > **IGMP** and the page shown in the following figure appears. IGMP proxy enables the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. The system acts as a proxy for its hosts after you enable it.



IGMP Proxy Configuration

IGMP proxy enables the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. The system acts as a proxy for its hosts when you enable it by doing the follows:
. Enable IGMP proxy on WAN interface (upstream), which connects to a router running IGMP.
. Enable IGMP on LAN interface (downstream), which connects to its hosts.

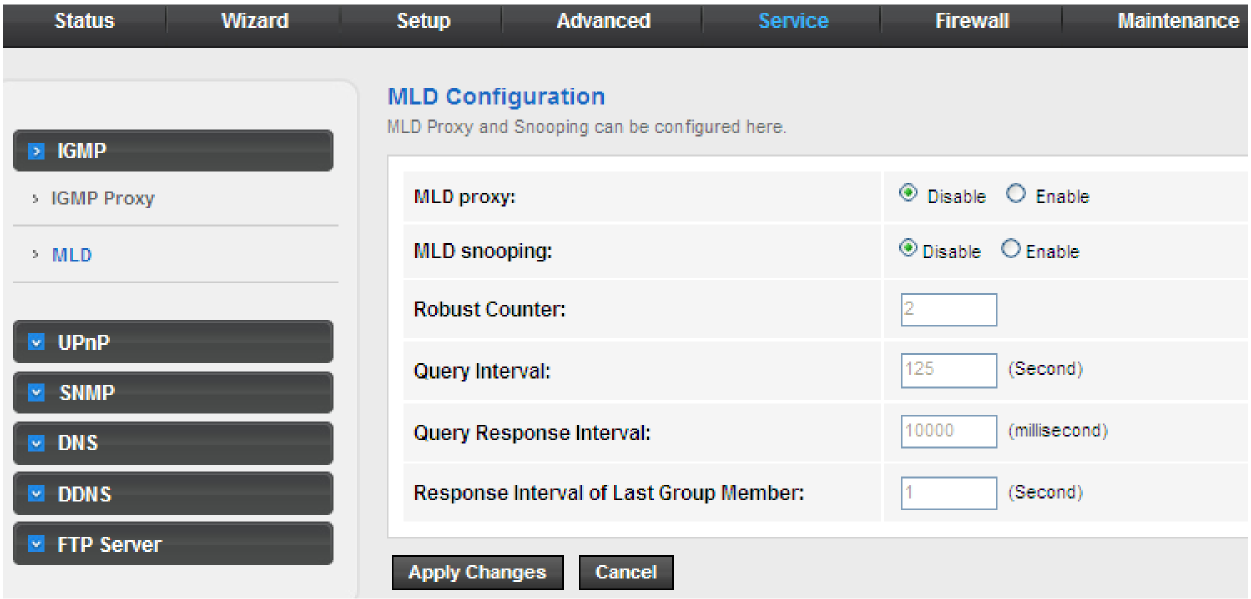
IGMP Proxy:	○ Disable ● Enable
Multicast Allowed:	○ Disable ● Enable
Robust Count:	2
Last Member Query Count:	2
Query Interval:	60 (seconds)
Query Response Interval:	100 (*100ms)
Group Leave Delay:	2000 (ms)
IGMP PACKSET PASSTHROUGH:	● Disable ○ Enable

The following table describes the parameters:

Field	Description
IGMP Proxy	The Internet Group Management Protocol**.** Enable/Disable the function to access.
Multicast Allowed	Enable/Disable the function to access.
Robust Count	Robust factor of the IGMP Proxy Counter.
Last Member Query Count	The last-member query interval is the maximum amount of time between group-specific query messages, including those sent in response to leave-group messages. You can configure this interval to change the amount of time it takes a routing device to detect the loss of the last member of a group.
Query Interval	The amount of time between IGMP General Query messages sent by the router (if the router is a querier on this subnet).
Query Response Interval	The maximum amount of time in seconds that the IGMP router waits to receive a response to a General Query message. The query response interval is the Maximum Response Time field in the IGMP v2 Host Membership Query message header. The default query response interval is 10 seconds and must be less than the query interval.
Group Leave Delay	The amount of time in seconds that the IGMP router waits to receive a response to a Group-Specific Query message. The last member query interval is also the amount of time in seconds between successive Group-Specific Query messages.

3.7.1.2 MLD

MLD means Multicast Listener Discovery; its component of the IPv6. MLD is used by IPv6 routers for discovering multicast listeners on a directly-attached link, much like IGMP being used in IPv4.



MLD Configuration

MLD Proxy and Snooping can be configured here.

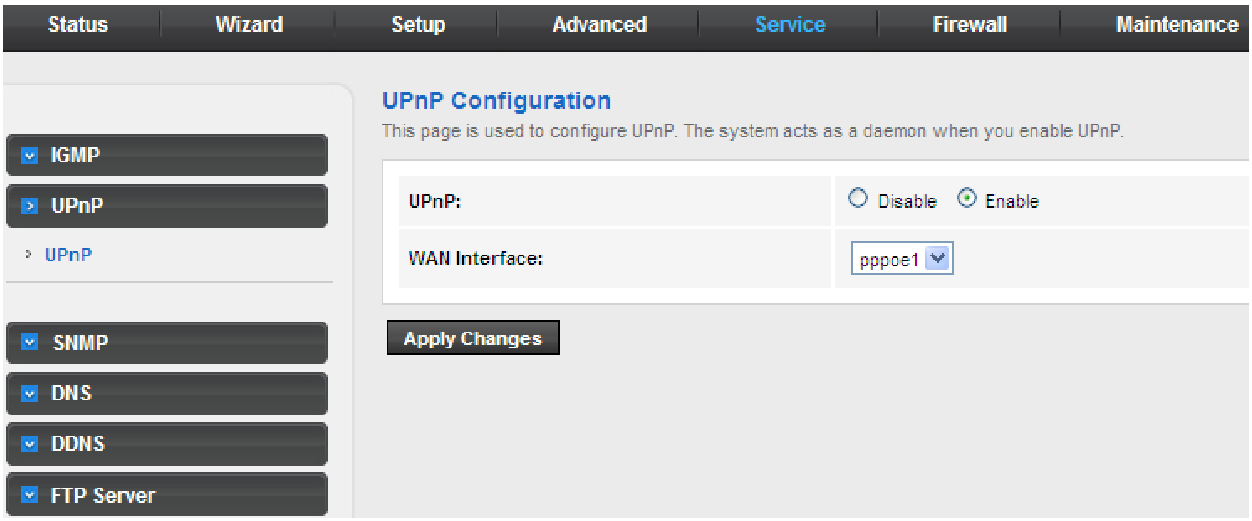
MLD proxy:	● Disable ○ Enable
MLD snooping:	● Disable ○ Enable
Robust Counter:	2
Query Interval:	125 (Second)
Query Response Interval:	10000 (millisecond)
Response Interval of Last Group Member:	1 (Second)

The following table describes the parameters:

Field	Description
MLD Proxy	MLD Proxy can be used to support IPv6 multicast data. Enable/Disable the function to access.
MLD Snooping	Snooping is an IPv6 multicast constraining mechanism that runs on Layer 2 devices to manage and control IPv6 multicast groups. By analyzing received MLD messages, a Layer 2 device running MLD Snooping establishes mappings between ports and multicast MAC addresses and forwards IPv6 multicast data based on these mappings. Multicast Listener Discovery Snooping (MLD). Enable/Disable the function to access.
Robust Counter	Robust factor of the MLD Counter.
Query Interval	The amount of time between IGMP General Query messages sent by the router (if the router is a querier on this subnet).
Query Response Interval	The maximum amount of time in seconds that the IGMP router waits to receive a response to a General Query message. The query response interval is the Maximum Response Time field in the IGMP v2 Host Membership Query message header. The default query response interval is 10 seconds and must be less than the query interval.
Response Interval of Last Group Member	The amount of time in seconds that the IGMP router waits to receive a response to a Group-Specific Query message. The last member query interval is also the amount of time in seconds between successive Group-Specific Query messages.

3.7.2 UPNP

Choose **Service** > **UPnP** and the page shown in the following figure appears. This page is used to configure UPnP. The system acts as a daemon after you enable it.



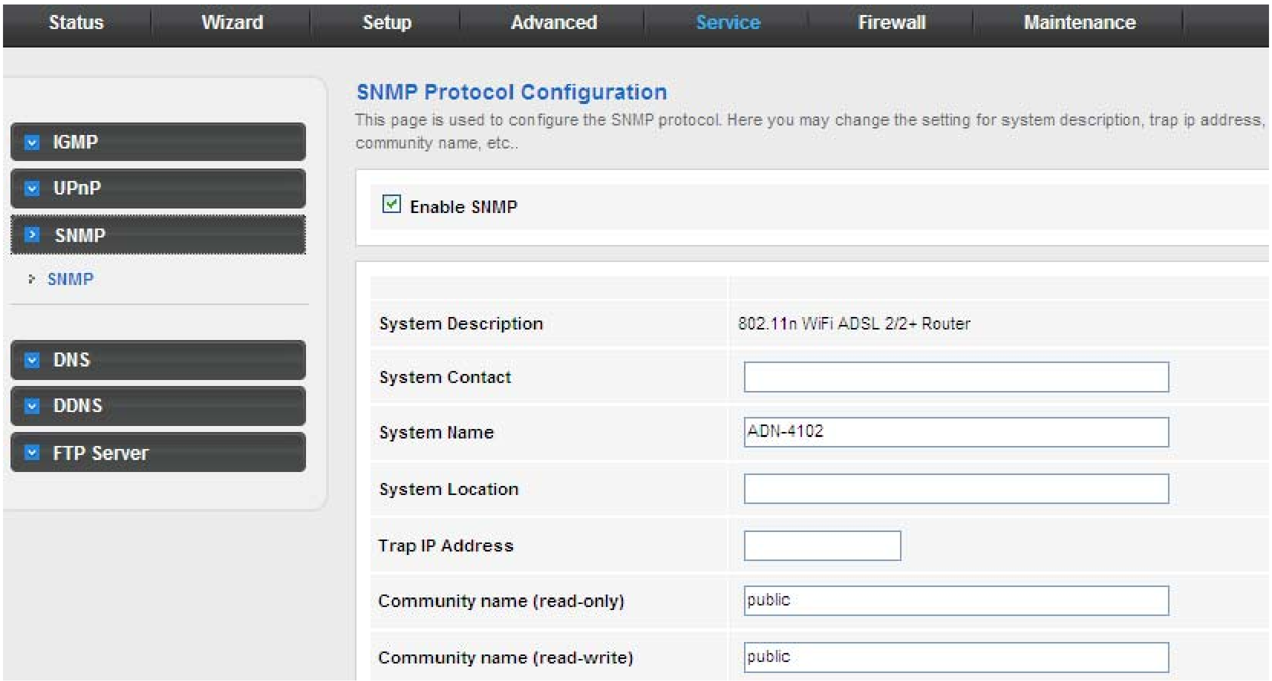
UPnP Configuration

This page is used to configure UPnP. The system acts as a daemon when you enable UPnP.

UPnP:	○ Disable ● Enable
WAN Interface:	pppoe1

3.7.3 SNMP

Choose **Service** > **SNMP**, click **Enable SNMP** and the page shown in the following figure appears. You can configure the SNMP parameters.



SNMP Protocol Configuration

This page is used to configure the SNMP protocol. Here you may change the setting for system description, trap ip address, community name, etc..

☑ Enable SNMP

System Description	802.11n WiFi ADSL 2/2+ Router
System Contact	
System Name	ADN-4102
System Location	
Trap IP Address	
Community name (read-only)	public
Community name (read-write)	public

The following table describes the parameters:

Field	Description
Enable SNMP	Select it to enable SNMP function. You need to enable SNMP, and then you can configure the parameters of this page.

Field	Description
Trap IP Address	Enter the trap IP address. The trap information is sent to the corresponding host.
Community Name (Read-only)	The network administrators must use this password to read the information of this router.
Community Name (Read-Write)	The network administrators must use this password to configure the information of the router.

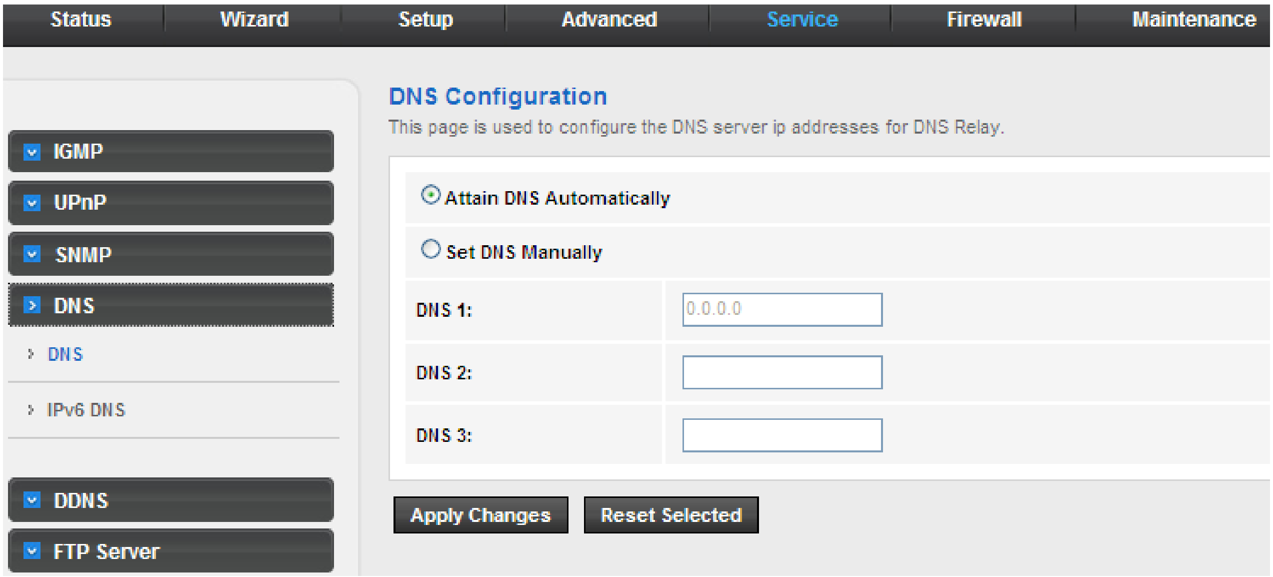
3.7.4 DNS

Domain Name System (DNS) is an Internet service that translates the domain name into IP address. Because the domain name is alphabetic, it is easier to remember. The Internet, however, is based on IP addresses. Every time you use a domain name, DNS translates the name into the corresponding IP address. For example, the domain name www.example.com might be translated to 198.105.232.4. The DNS has its own network. If one DNS server does not know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

Choose **Service** > **DNS**. The **DNS** page that is displayed contains **DNS** and **IPv6 DNS**.

3.7.4.1 DNS

Click **DNS** in the left pane and the page shown in the following figure appears.



DNS Configuration

This page is used to configure the DNS server ip addresses for DNS Relay.

● Attain DNS Automatically

○ Set DNS Manually

DNS 1: 0.0.0.0

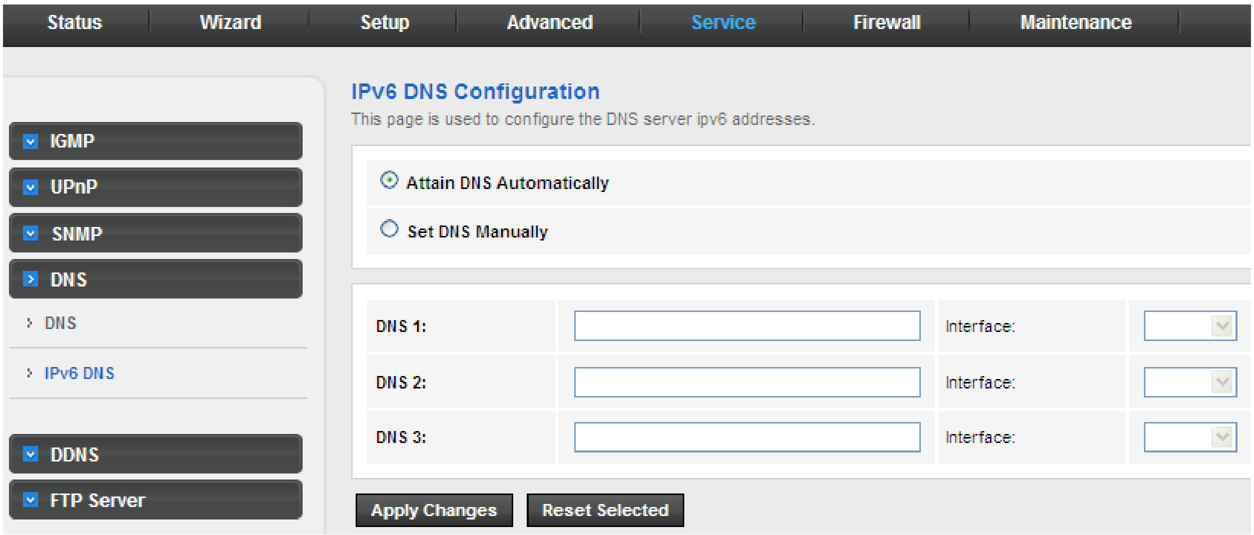
DNS 2:

DNS 3:

The following table describes the parameters:

Fields	Description
Attain DNS Automatically	Select it, and the router accepts the first received DNS assignment from one of the PPPoA, PPPoE or MER enabled PVC(s) during the connection establishment.
Set DNS Manually	Select it to enter the IP addresses of the DNS 1, DNS 2, DNS 3, servers manually.

3.7.4.2 IPv6 DNS



IPv6 DNS Configuration

This page is used to configure the DNS server ipv6 addresses.

● Attain DNS Automatically

○ Set DNS Manually

DNS 1: Interface:

DNS 2: Interface:

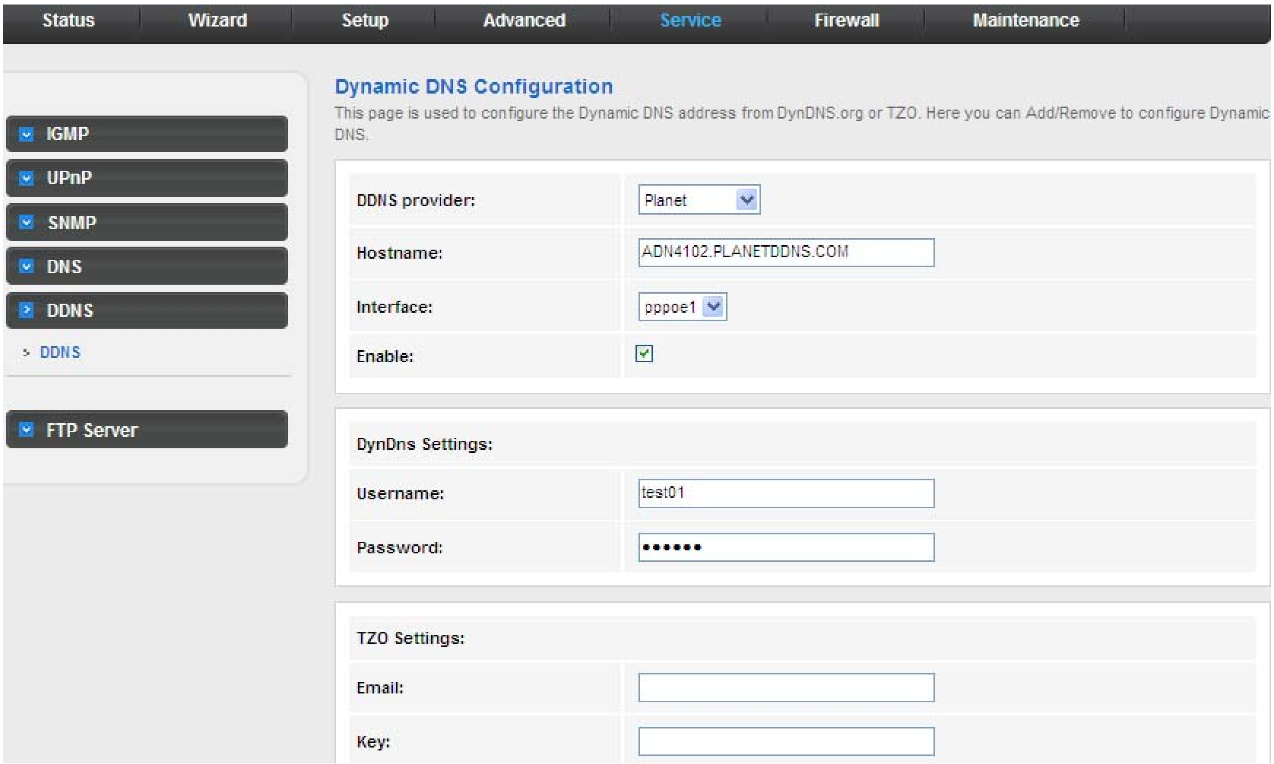
DNS 3: Interface:

The following table describes the parameters:

Field	Description
Attain DNS Automatically	Select it and the router accepts the first received DNS assignment from one of the PPPoA, PPPoE or MER enabled PVC(s) during the connection establishment.
Set DNS Manually	Select it and enter the IP addresses of the primary and secondary DNS server.

3.7.5 DDNS

Click **DDNS** in the left pane and the page shown in the following figure appears. This page is used to configure the dynamic DNS address from DynDNS.org, TZO, PHDNS or Planet. You can add or remove to configure dynamic DNS. The Planet DDNS is free for customers.



Dynamic DNS Configuration

This page is used to configure the Dynamic DNS address from DynDNS.org or TZO. Here you can Add/Remove to configure Dynamic DNS.

DDNS provider:	Planet
Hostname:	ADN4102.PLANETDDNS.COM
Interface:	pppoe1
Enable:	☑

DynDns Settings:

Username:	test01
Password:	••••••

TZO Settings:

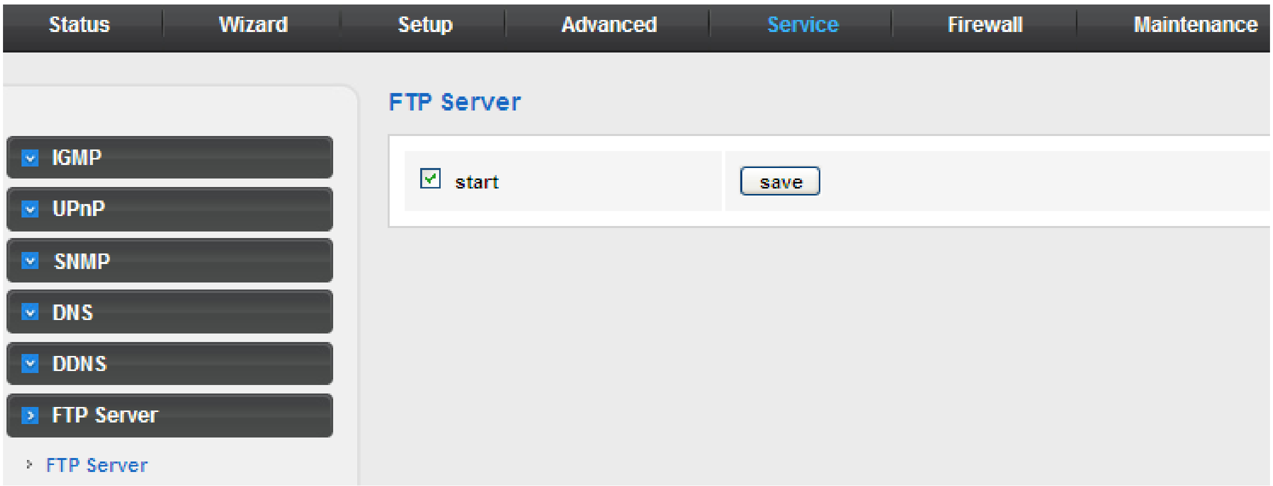
Email:	
Key:	

The following table describes the parameters:

Field	Description
DDNS provider	Choose the DDNS provider name. You can choose **DynDNS.org, TZO** or **Planet**.
Host Name	The DDNS identifier.
Interface	The WAN interface of the router.
Enable	Enable or disable DDNS function.
Username	The name provided by DDNS provider.
Password	The password provided by DDNS provider.
Email	The email provided by DDNS provider.
Key	The key provided by DDNS provider.

3.7.6 FTP Server

The File Transfer Protocol (FTP) is a standard network protocol used to transfer computer files from one host to another host over a TCP-based network. It’s built on a client-server architecture and uses separate control and data connections between the client and the server. FTP users may authenticate themselves using a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it.



FTP Server

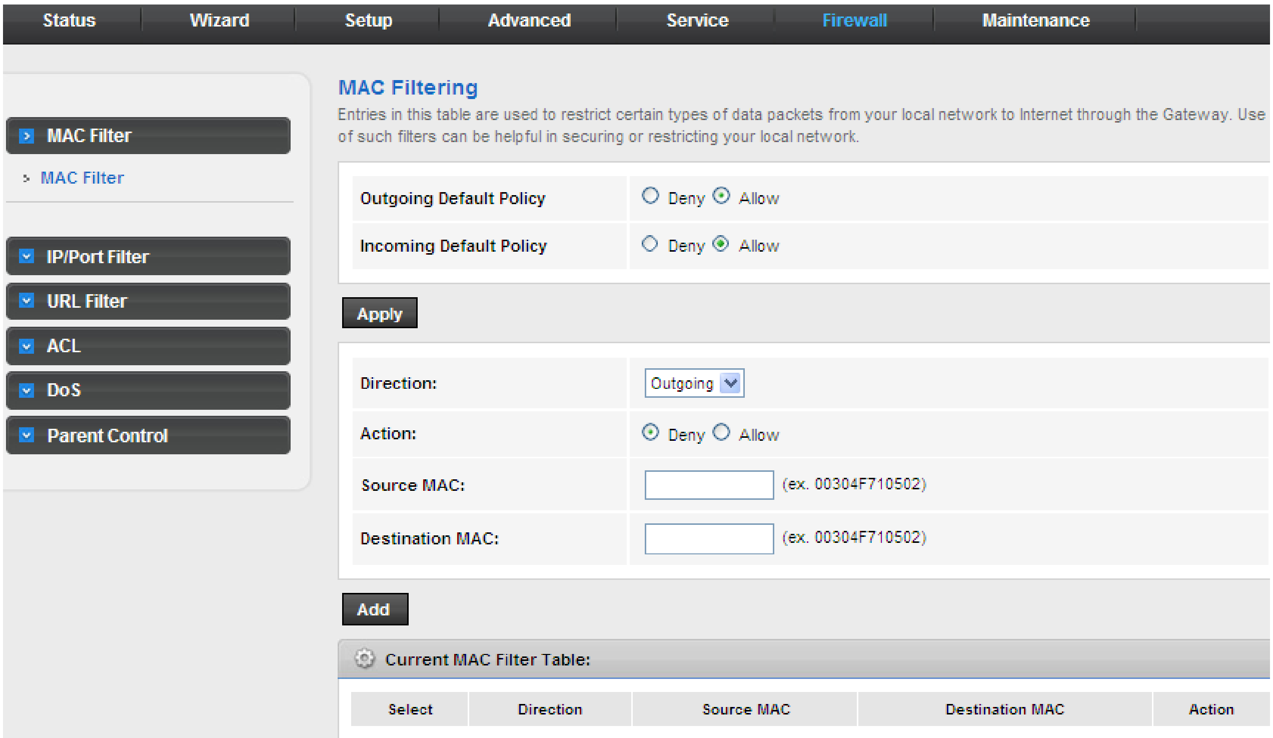
☑ start

3.8 Firewall

Choose Service > **Firewall** and the Firewall page that is displayed contains **MAC Filter**, **IP/Port Filter**, **URL Filter**, **ACL, DoS** and **Parent Control**.

3.8.1 MAC Filter

Click **MAC Filter** in the left pane and the page shown in the following figure appears. Entries in the table are used to restrict certain types of data packets from your local network to Internet through the gateway. These filters are helpful in securing or restricting your local network.



MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Outgoing Default Policy	○ Deny ● Allow
Incoming Default Policy	○ Deny ● Allow

Direction:	Outgoing
Action:	● Deny ○ Allow
Source MAC:	(ex. 00304F710502)
Destination MAC:	(ex. 00304F710502)

Current MAC Filter Table:

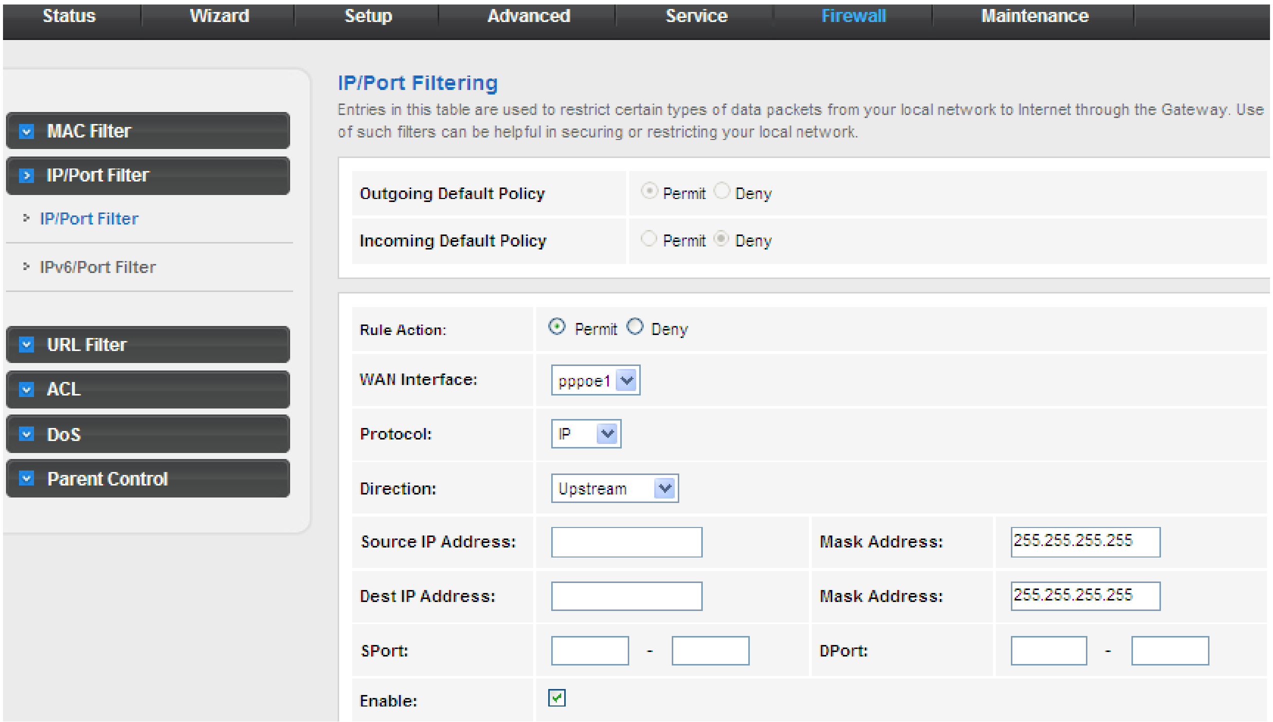
Select	Direction	Source MAC	Destination MAC	Action

Field	Description
Outgoing Default Policy	Specify the default action on the LAN to WAN bridging/forwarding path.
Incoming Default Policy	Specify the default action on the WAN to LAN bridging/forwarding path.
Direction	Traffic bridging/forwarding direction.
Action	Deny or allow traffic when matching this rule.
Src MAC Address	The source MAC address must be xxxxxxxxxxxx format.
Dst MAC Address	The destination MAC address must be xxxxxxxxxxxx format.

3.8.2 IP/Port Filter

3.8.2.1 IP/Port Filter

Click **IP/Port Filter** in the left pane and the page shown in the following figure appears. Entries in the table are used to restrict certain types of data packets through the gateway. These filters are helpful in securing or restricting your local network.



IP/Port Filtering

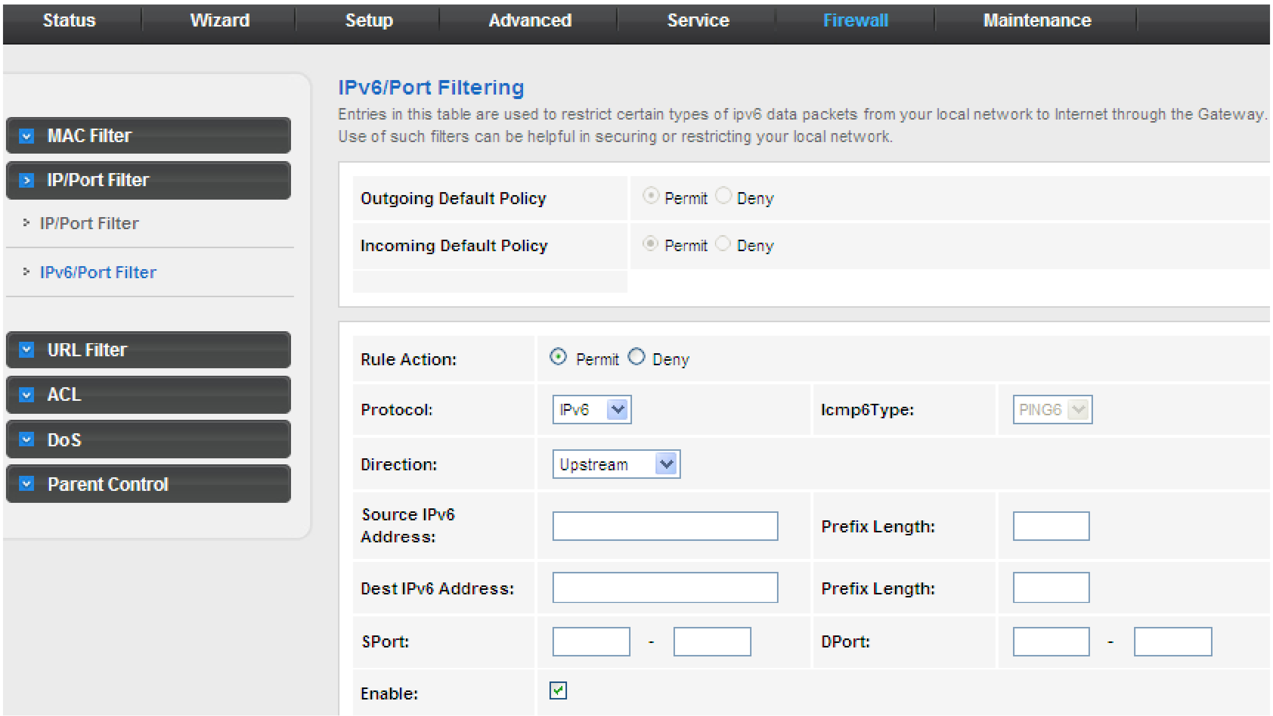
Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Outgoing Default Policy	● Permit ○ Deny
Incoming Default Policy	○ Permit ● Deny

Rule Action:	● Permit ○ Deny		
WAN Interface:	pppoe1		
Protocol:	IP		
Direction:	Upstream		
Source IP Address:		Mask Address:	255.255.255.255
Dest IP Address:		Mask Address:	255.255.255.255
SPort:	-	DPort:	-
Enable:	☑		

Field	Description
Outgoing Default Policy	Specify the default action on the LAN to WAN forwarding path.
Incoming Default Policy	Specify the default action on the WAN to LAN forwarding path.

3.8.2.2 IPv6/Port Filter



IPv6/Port Filtering

Entries in this table are used to restrict certain types of ipv6 data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Outgoing Default Policy	● Permit ○ Deny
Incoming Default Policy	● Permit ○ Deny

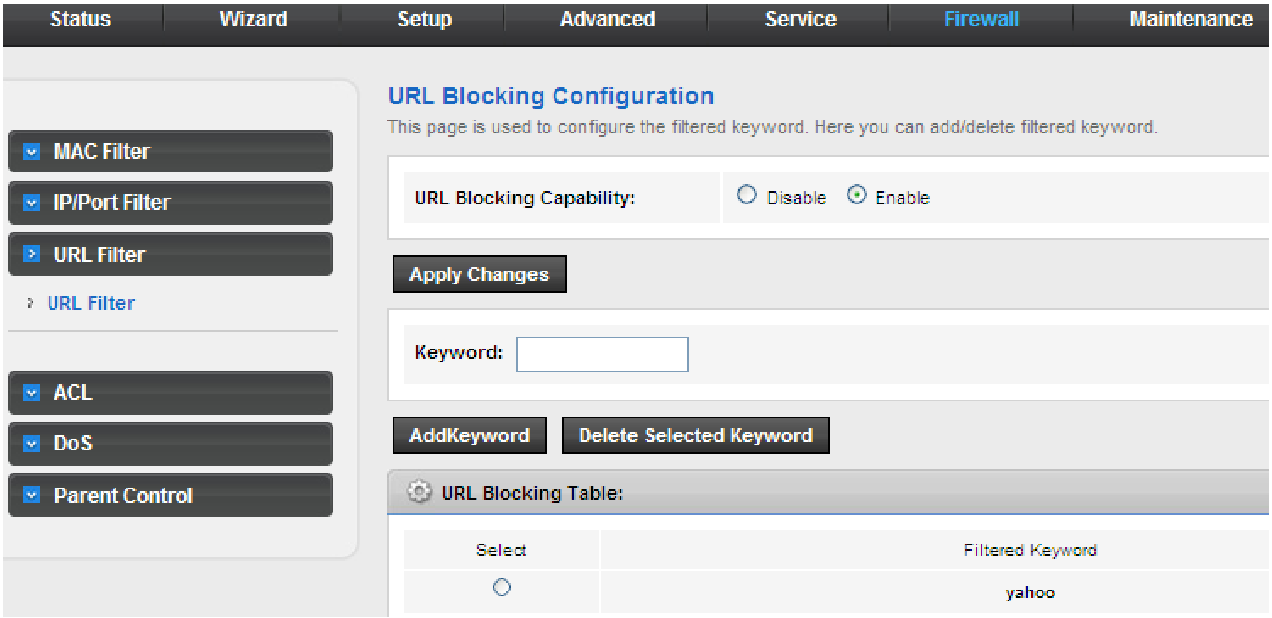
Rule Action:	● Permit ○ Deny		
Protocol:	IPv6	Icmp6Type:	PING6
Direction:	Upstream		
Source IPv6 Address:		Prefix Length:	
Dest IPv6 Address:		Prefix Length:	
SPort:	-	DPort:	-
Enable:	☑		

Fields on the second setting block:

Field	Description
Rule Action	Permit or deny traffic when matching this rule.
Direction	Traffic forwarding direction.
Protocol	There are 4 options available: IP, TCP, UDP and ICMP.
Src IP Address	The source IP address assigned to the traffic on which filtering is applied.
Src Subnet Mask	Subnet-mask of the source IP.
Src Port	Starting and ending source port numbers.
Dst IP Address	The destination IP address assigned to the traffic on which filtering is applied.
Dst Subnet Mask	Subnet-mask of the destination IP.
Dst Port	Starting and ending destination port numbers.
Enable	Enable/Disable the function to access.

3.8.3 URL Filter

Click **URL Filter** in the left pane and the page shown in the following figure appears. This page is used to block a fully qualified domain name, such as tw.yahoo.com and filtered keyword (yahoo). You can add or delete FQDN and filtered keyword.



URL Blocking Configuration

This page is used to configure the filtered keyword. Here you can add/delete filtered keyword.

URL Blocking Capability: ○ Disable ● Enable

Keyword:

URL Blocking Table:

Select	Filtered Keyword
○	yahoo

The following table describes the parameters:

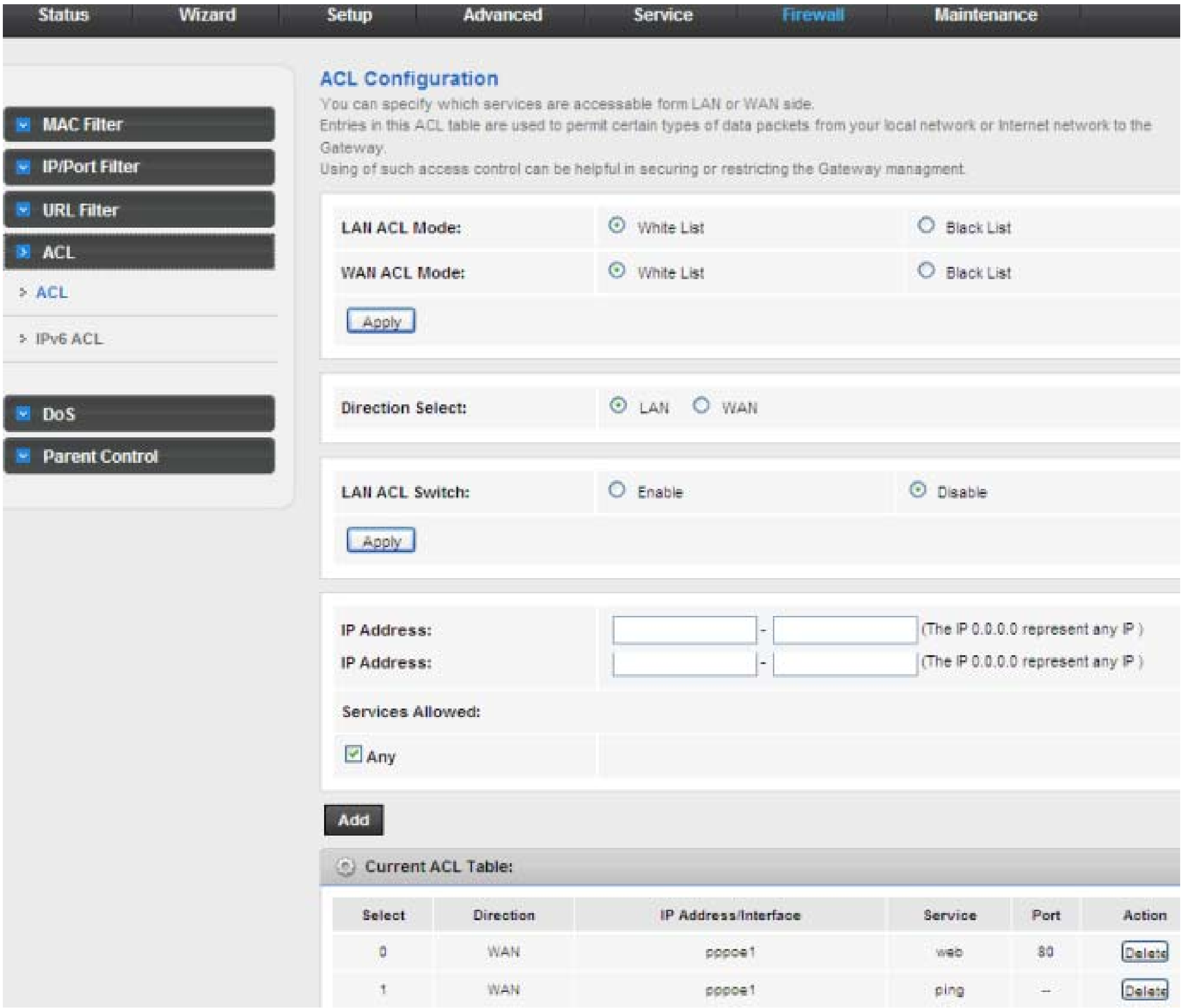
Field	Description
URL Blocking Capability	You can choose **Disable** or **Enable**. ● Select **Disable** to disable URL/KEYWORD blocking function and keyword filtering function. ● Select **Enable** to block access to the URLs and keywords specified in the **URL Blocking Table**.
Keyword	Enter the keyword to block.
Add Keyword	Click it to add a URL/keyword to the **URL Blocking Table**.
Delete Selected Keyword	Select a row in the **URL Blocking Table** and click it to delete the row.
URL Blocking Table	A list of the URLs to which access is blocked.

3.8.4 ACL

3.8.4.1 ACL

Choose **Service** > **ACL** and the page shown in the following figure appears. On this page, you can permit the data packets from LAN or WAN to access the router. You can configure the IP address for Access Control List (ACL). If ACL is enabled, only the effective IP address in the ACL can access the router.

Note	If you select **Enable** in ACL capability, ensure that your host IP address is in ACL list before it takes effect.



ACL Configuration

You can specify which services are accessable form LAN or WAN side.
Entries in this ACL table are used to permit certain types of data packets from your local network or Internet network to the Gateway.
Using of such access control can be helpful in securing or restricting the Gateway managment.

LAN ACL Mode: ● White List ○ Black List

WAN ACL Mode: ● White List ○ Black List

Apply

Direction Select: ● LAN ○ WAN

LAN ACL Switch: ○ Enable ● Disable

Apply

IP Address: [ ] - [ ] (The IP 0.0.0.0 represent any IP)

IP Address: [ ] - [ ] (The IP 0.0.0.0 represent any IP)

Services Allowed:

☑ Any

Add

Current ACL Table:

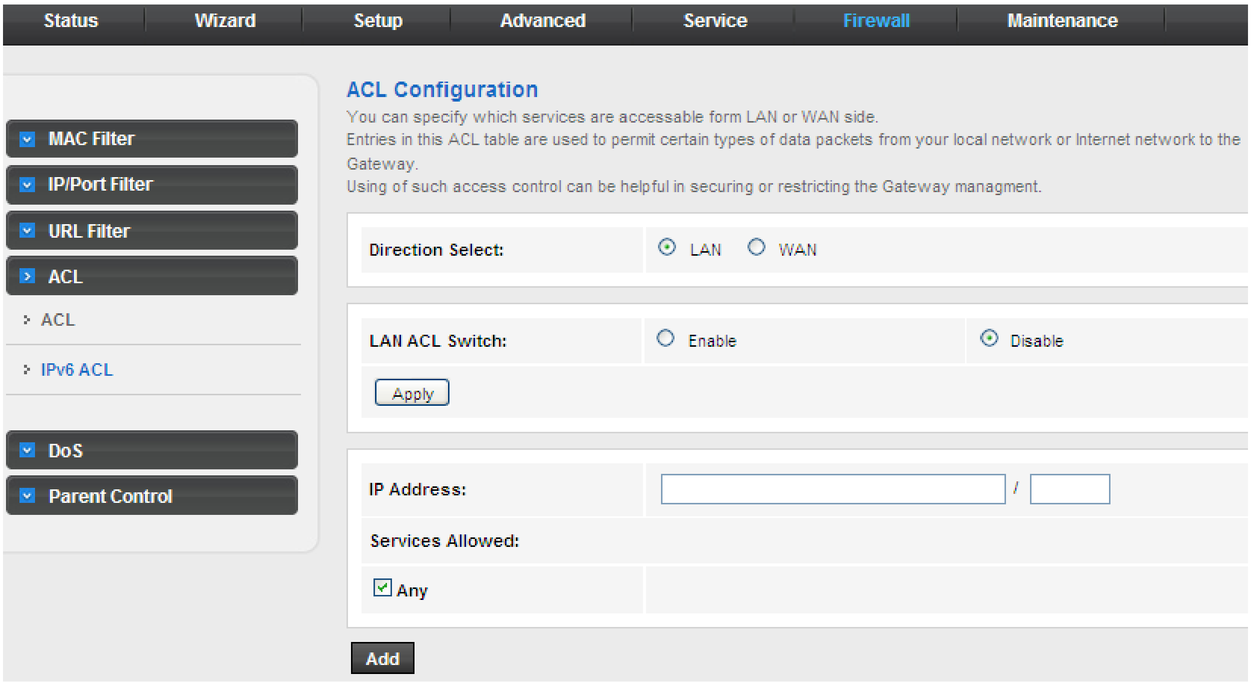
Select	Direction	IP Address/Interface	Service	Port	Action
0	WAN	pppoe1	web	80	Delete
1	WAN	pppoe1	ping	--	Delete

The following table describes the parameters:

Field	Description
LAN ACL Mode	• When you click White List, only the devices whose IP addresses are listed in the Current ACL Table can access the router. • When you click Black List, the devices whose IP addresses are listed in the Current ACL Table are denied to access the router.
WAN ACL Mode	• When you click White List, only the devices whose IP addresses are listed in the Current ACL Table can access the router. • When you click Black List, the devices whose IP addresses are listed in the Current ACL Table are denied to access the router.
Direction Select	Select the router interface. You can select **LAN** or **WAN**. In this example, **LAN** is selected.
LAN ACL Switch	Select it to enable or disable ACL function.
IP Address	Enter the IP address of the specified interface. Only the IP address that is in the same network segment with the IP address of the specified interface can access the router.
Services Allowed	You can choose the following services from LAN: **Web**, **Telnet**, **SSH**,

Field	Description
	FTP, **TFTP**, **SNMP**, or **PING**. You can also choose all the services.
Add	After setting the parameters, click it to add an entry to the **Current ACL Table**.

3.8.4.2 IPv6 ACL



ACL Configuration

You can specify which services are accessable form LAN or WAN side.
Entries in this ACL table are used to permit certain types of data packets from your local network or Internet network to the Gateway.
Using of such access control can be helpful in securing or restricting the Gateway managment.

Direction Select: ● LAN ○ WAN

LAN ACL Switch: ○ Enable ● Disable

Apply

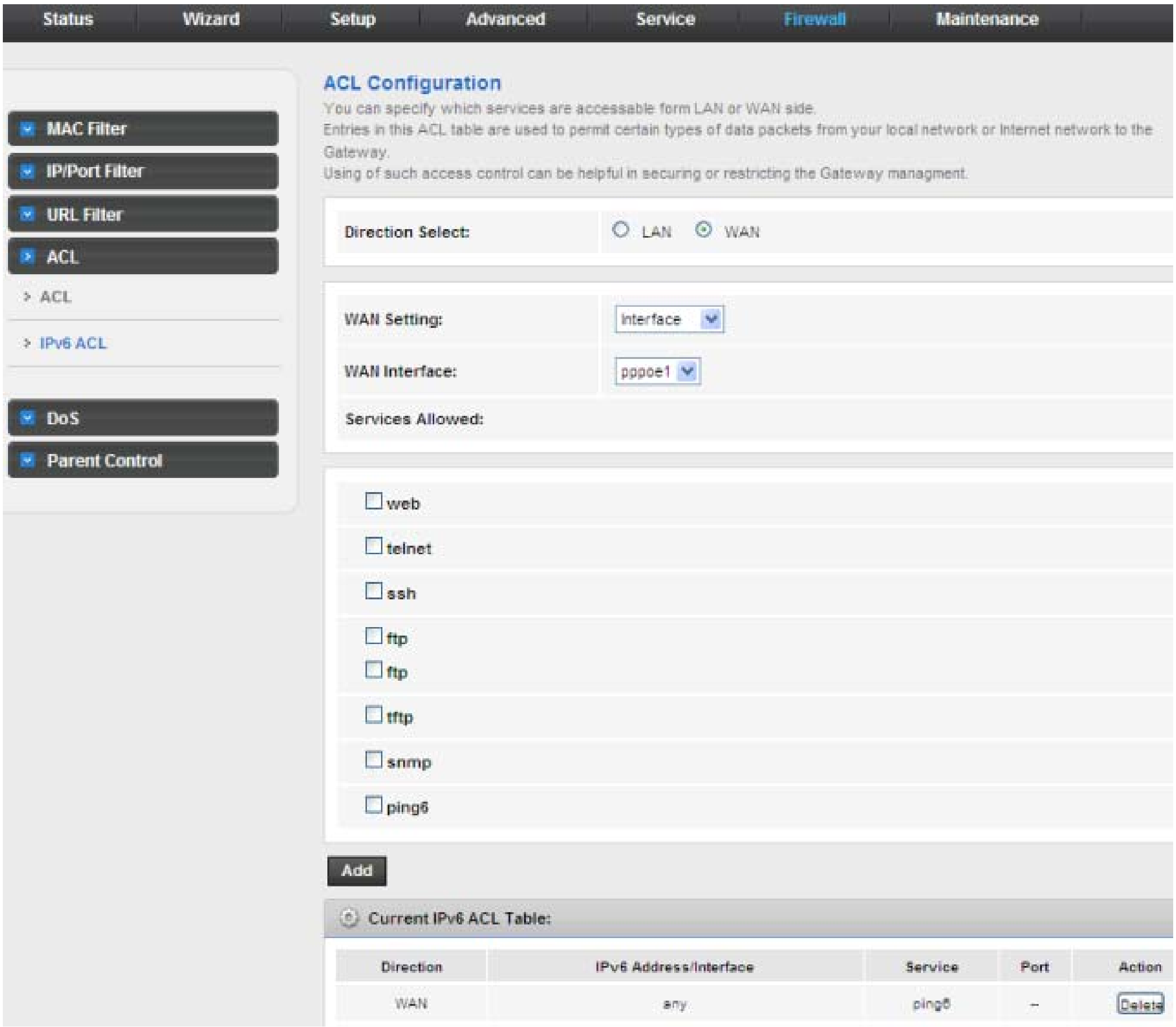
IP Address: /

Services Allowed:

☑ Any

Add

If **WAN** is selected in the field of **Direction Select**, the page is shown as the following figure.



ACL Configuration

You can specify which services are accessable form LAN or WAN side.
Entries in this ACL table are used to permit certain types of data packets from your local network or Internet network to the Gateway.
Using of such access control can be helpful in securing or restricting the Gateway managment.

Direction Select: ○ LAN ● WAN

WAN Setting: Interface

WAN Interface: pppoe1

Services Allowed:

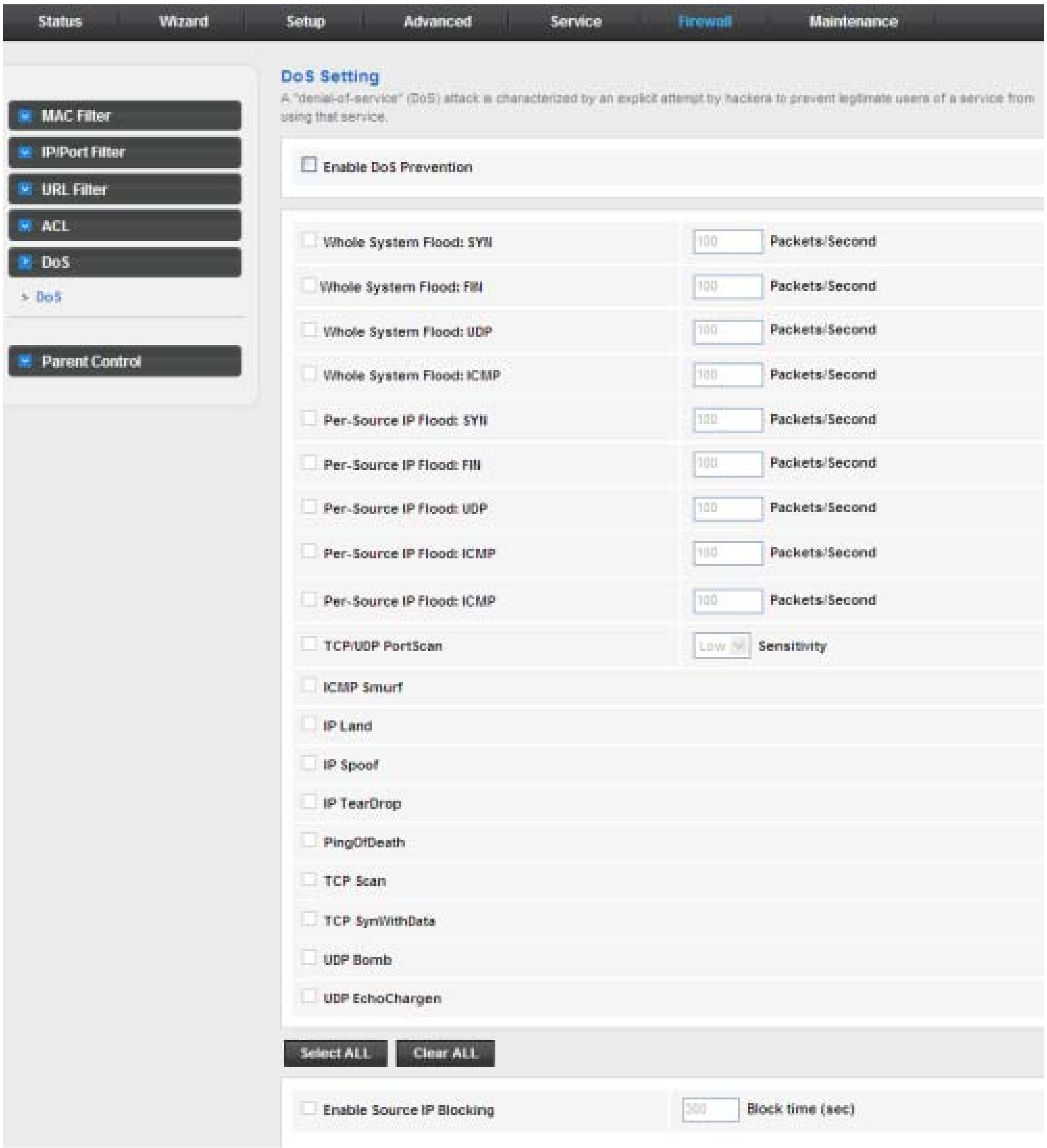
□ web
□ telnet
□ ssh
□ ftp
□ ftp
□ tftp
□ snmp
□ ping6

Current IPv6 ACL Table:

Direction	IPv6 Address/Interface	Service	Port	Action
WAN	any	ping6	–	Delete

3.8.5 DoS

Denial-of-Service Attack (DoS attack) is a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic.



DoS Setting

A "denial-of-service" (DoS) attack is characterized by an explicit attempt by hackers to prevent legitimate users of a service from using that service.

□ Enable DoS Prevention

□ Whole System Flood: SYN	100	Packets/Second
□ Whole System Flood: FIN	100	Packets/Second
□ Whole System Flood: UDP	100	Packets/Second
□ Whole System Flood: ICMP	100	Packets/Second
□ Per-Source IP Flood: SYN	100	Packets/Second
□ Per-Source IP Flood: FIN	100	Packets/Second
□ Per-Source IP Flood: UDP	100	Packets/Second
□ Per-Source IP Flood: ICMP	100	Packets/Second
□ Per-Source IP Flood: ICMP	100	Packets/Second
□ TCP/UDP PortScan	Low	Sensitivity
□ ICMP Smurf		
□ IP Land		
□ IP Spoof		
□ IP TearDrop		
□ PingOfDeath		
□ TCP Scan		
□ TCP SynWithData		
□ UDP Bomb		
□ UDP EchoChargen		

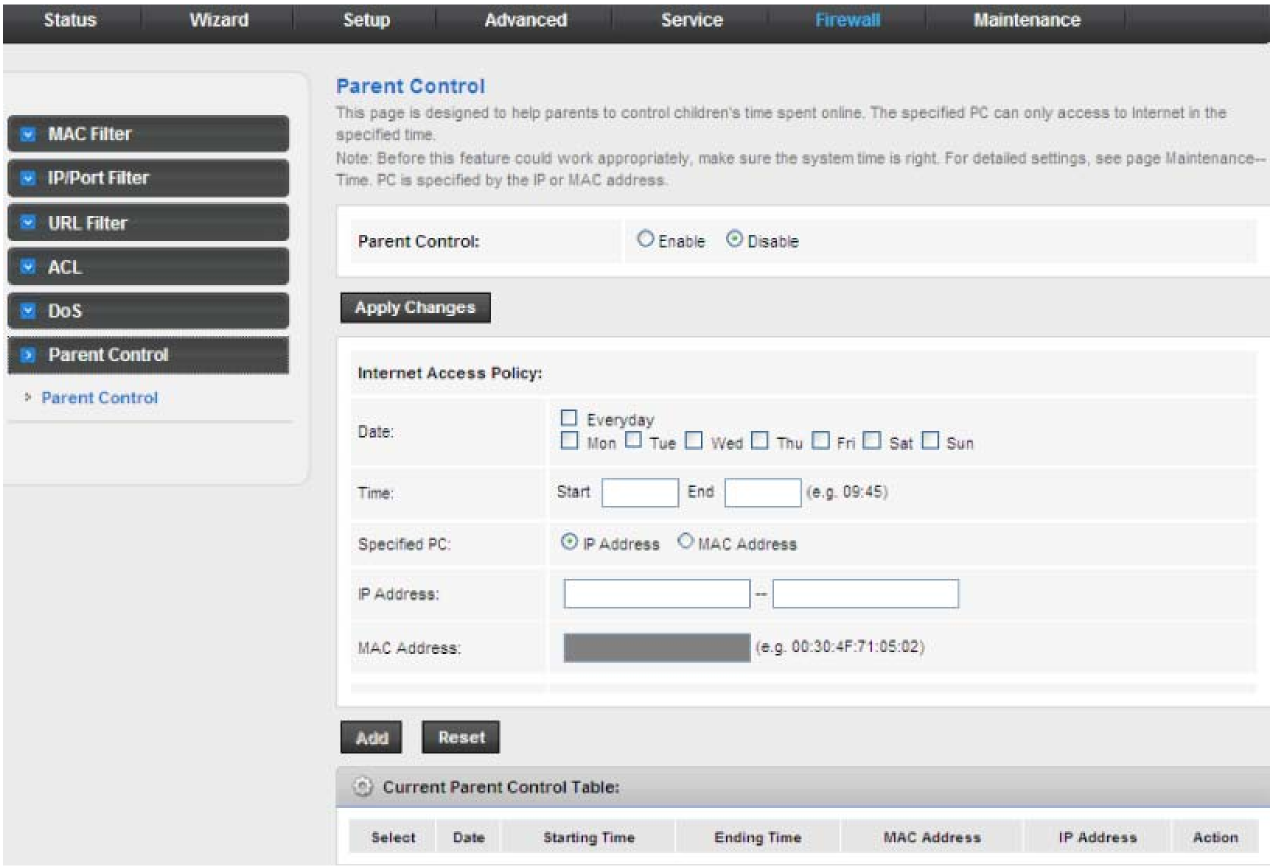
□ Enable Source IP Blocking 300 Block time (sec)

The following table describes the parameters:

Fields	Description
Enable DoS Prevention	Enable denial-of-service feature to access.
Enable Source IP Blocking	Enable the function to block IP Source and set the time in seconds.

3.8.6 Parental Control

Choose **Advance > Parental Control** and the page shown in the following figure appears. This page is used to control children's online time. The PC with specified MAC or IP address can only surf the internet within the specified period of time



Parent Control

This page is designed to help parents to control children's time spent online. The specified PC can only access to Internet in the specified time.

Note: Before this feature could work appropriately, make sure the system time is right. For detailed settings, see page Maintenance--Time. PC is specified by the IP or MAC address.

Parent Control: ○ Enable ● Disable

Internet Access Policy:

Date: □ Everyday
□ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun

Time: Start ____ End ____ (e.g. 09:45)

Specified PC: ● IP Address ○ MAC Address

IP Address: ____ -- ____

MAC Address: ____ (e.g. 00:30:4F:71:05:02)

Current Parent Control Table:

Select	Date	Starting Time	Ending Time	MAC Address	IP Address	Action

The following table describes the parameters:

Field	Description
Parental Control	Select it to enable Parental Control function. You need to enable Parental Control to configure the parameters on this page. Parental Control is used to control children's online time. If enabled, the PC with specified MAC or IP address can only surf the internet within the specified period of time.
Date	Select one or more days you want to control
Time	The specified period of time you want to control
Specify PC	Select IP or MAC
IP Address	The IP Address of the PC you want to control
MAC Address	The MAC Address of the PC you want to control
Add Rule	Add the Parental Control rule
Reset	Reset the page
Current Parental Control Table	Show Parental Control rules
Delete All	Delete all Parental Control rules

3.9 Maintenance

In the navigation bar, click Maintenance. The Maintenance page displayed contains Update, Password, Reboot, Time Log and Diagnostics.

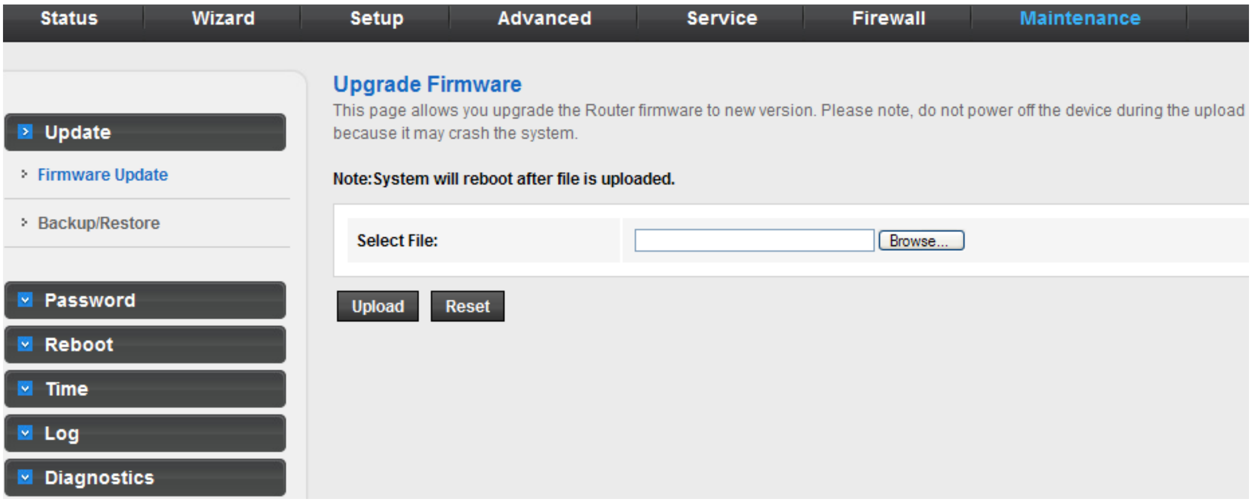
3.9.1 Update

Choose **Maintenance** > **Update**. The **Update** page displayed contains **Upgrade Firmware** and **Backup/Restore**.

Caution	Do not turn off the router or press the Reset button while the procedure is in progress.

3.9.1.1 Firmware Update

Click **Firmware** Update in the left pane and the page shown in the following figure appears. On this page, you can upgrade the firmware of the router.



Upgrade Firmware

This page allows you upgrade the Router firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

Note:System will reboot after file is uploaded.

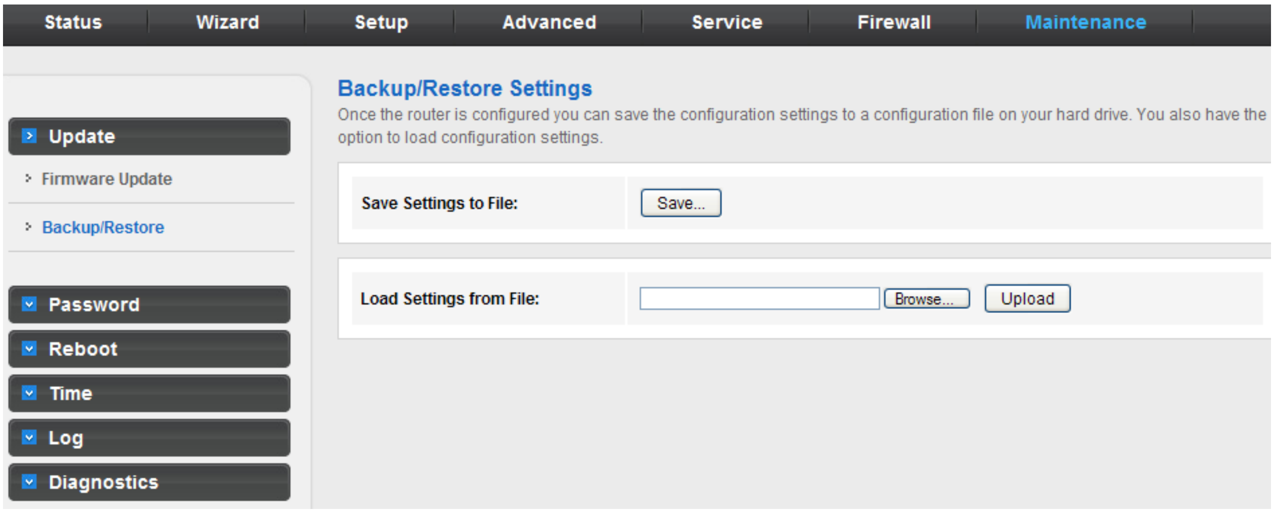
Select File:

The following table describes the parameters:

Field	Description
Select File	Click **Browse** to select the firmware file.
Upload	After selecting the firmware file, click **Upload** to start upgrading the firmware file.
Reset	Click it to start selecting the firmware file.

3.9.1.2 Backup/Restore

Click **Backup/Restore** in the left pane and the page shown in the following figure appears. You can back up the current settings to a file and restore the settings from the file that was saved previously.



Backup/Restore Settings

Once the router is configured you can save the configuration settings to a configuration file on your hard drive. You also have the option to load configuration settings.

Save Settings to File:

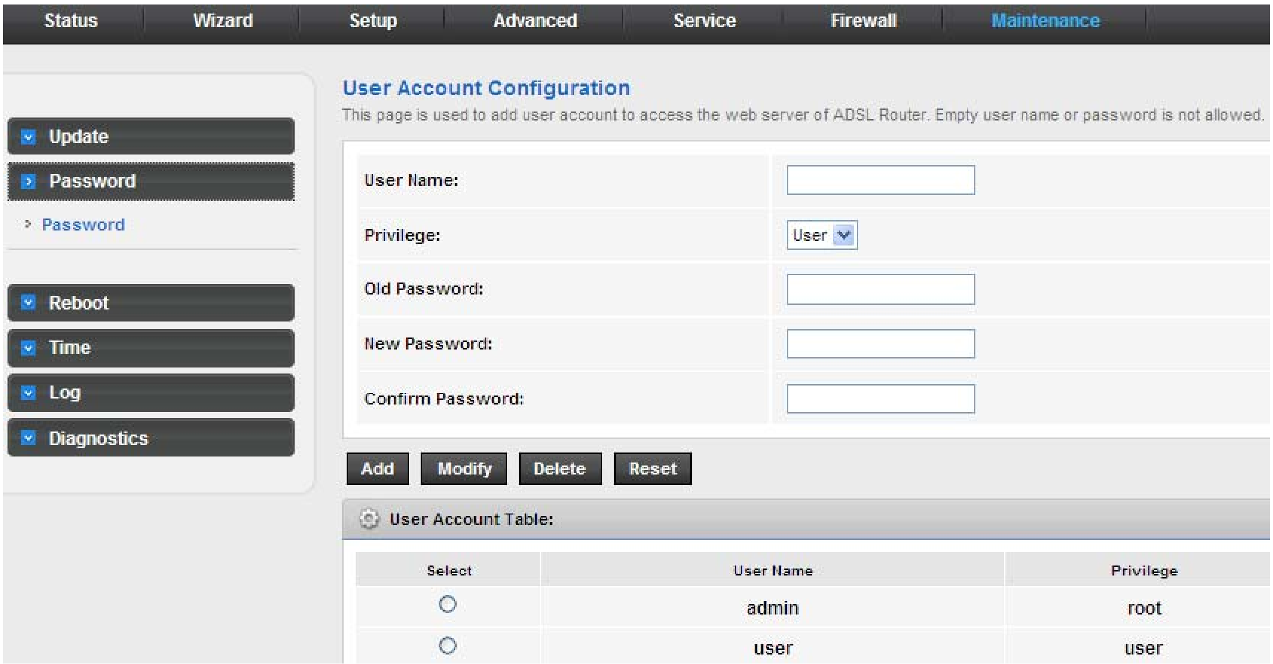
Load Settings from File:

The following table describes the parameters:

Field	Description
Save Settings to File	Click it and select the path. Then you can save the configuration file of the router.
Load Settings from File	Click **Browse** to select the configuration file.
Upload	After selecting the configuration file of the router, click **Upload** to start uploading the configuration file of the router.

3.9.2 Password

Choose **Maintenance** > **Password** and the page shown in the following figure appears. By default, the user name and password of the administrator are **admin** and **admin** respectively. The user name and password of the common user are **user** and **user** respectively.



User Account Configuration

This page is used to add user account to access the web server of ADSL Router. Empty user name or password is not allowed.

User Name:	
Privilege:	User
Old Password:	
New Password:	
Confirm Password:	

User Account Table:

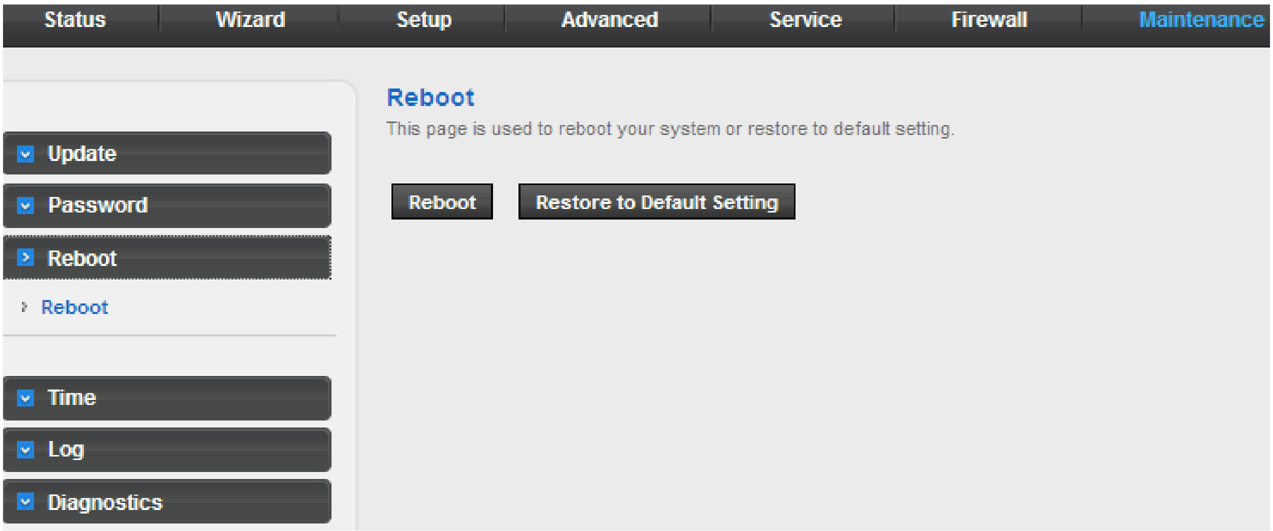
Select	User Name	Privilege
○	admin	root
○	user	user

The following table describes the parameters:

Field	Description
User Name	Choose the user name for accessing the router. You can choose **admin** or **user**.
Privilege	Choose the privilege for the account.
Old Password	Enter the old password
New Password	Enter your new password to which you want to change.
Confirmed Password	For confirmation, enter the new password again.

3.9.3 Reboot

Choose **Maintenance** > **Reboot** and the page shown in the following figure appears. You can set the router reset to the default settings or set the router to commit the current settings.



This page is used to reboot your system or restore to default setting.

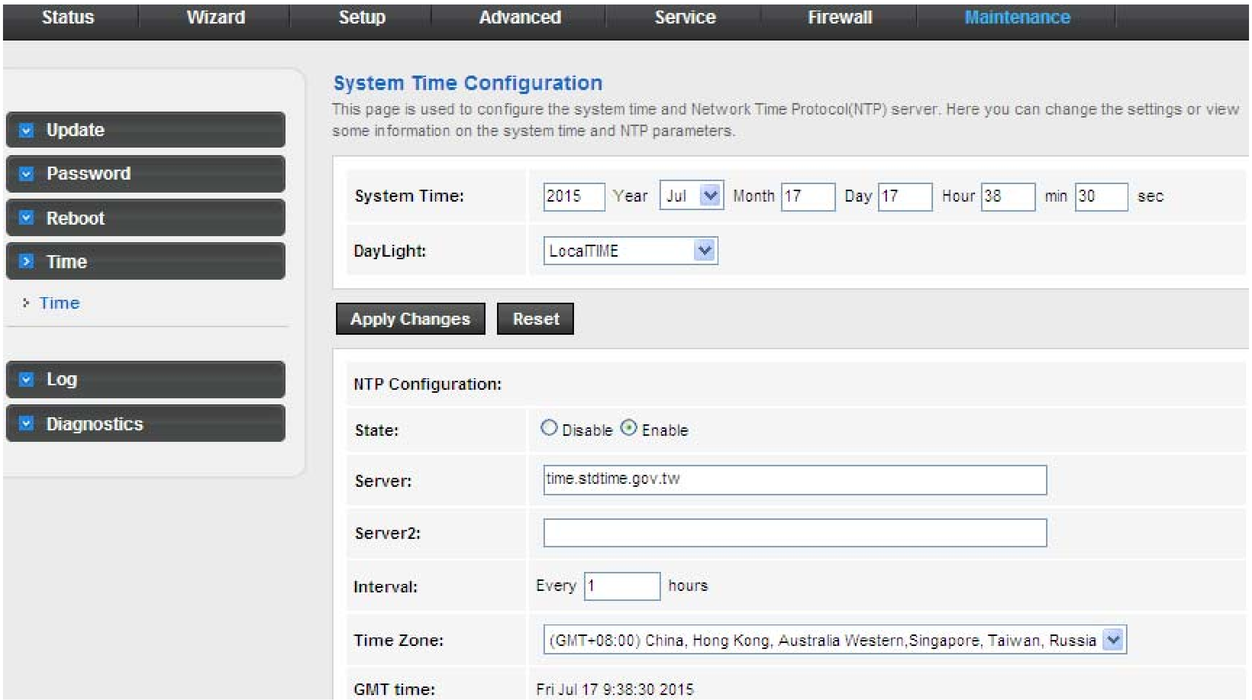
The following table describes the parameters:

Field	Description
Reboot	It takes around 30 seconds to reboot the device and then again login User name and Password.
Restore to Default Setting	It helps to change to default settings. It takes around 30 seconds to restart the device and then again login User name and Password.

Note	Do not turn off your modem or press the reset button while this procedure is in progress.

3.9.4. Time

Choose **Maintenance** > **Time** and the page shown in the following figure appears. You can configure the system time manually or get the system time from the time server.



System Time Configuration

This page is used to configure the system time and Network Time Protocol(NTP) server. Here you can change the settings or view some information on the system time and NTP parameters.

System Time: 2015 Year Jul Month 17 Day 17 Hour 38 min 30 sec

DayLight: LocalTIME

NTP Configuration:

State: ○ Disable ● Enable

Server: time.stdtime.gov.tw

Server2:

Interval: Every 1 hours

Time Zone: (GMT+08:00) China, Hong Kong, Australia Western,Singapore, Taiwan, Russia

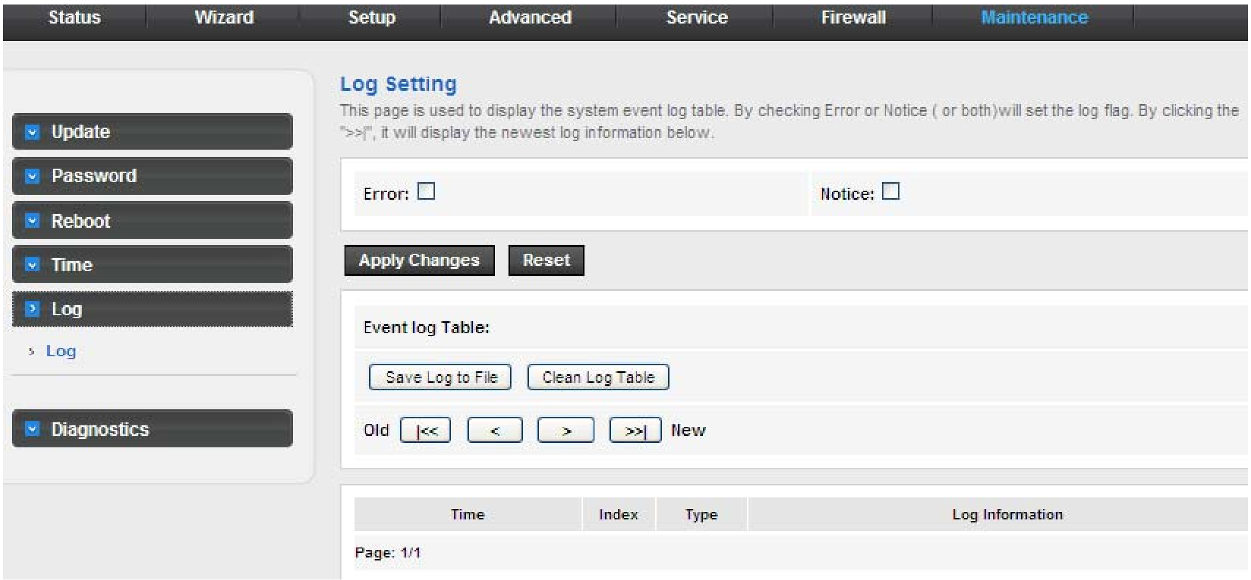
GMT time: Fri Jul 17 9:38:30 2015

The following table describes the parameters:

Fields	Description
System Time	Configure the system time manually.
Day Light	Daylight Saving Time.
State	Enable the option to update the system clock automatically. Disable the option to update the system clock manually.
Server	Configure the primary NTP server manually.
Server2	Configure the secondary NTP server manually.
Interval	NTP updating time interval.
Time Zone	Choose the time zone of your country from the drop-down list.
GMT Time	Greenwich Mean time.

3.9.5 Log

Choose **Maintenance** > **Log** and the page shown in the following figure appears. On this page, you can enable or disable system log function and view the system log.



Log Setting

This page is used to display the system event log table. By checking Error or Notice (or both)will set the log flag. By clicking the ">>|", it will display the newest log information below.

Error: □ Notice: □

Apply Changes | Reset

Event log Table:

Save Log to File | Clean Log Table

Old |<< < > >>| New

Time	Index	Type	Log Information

Page: 1/1

The following table describes the parameters:

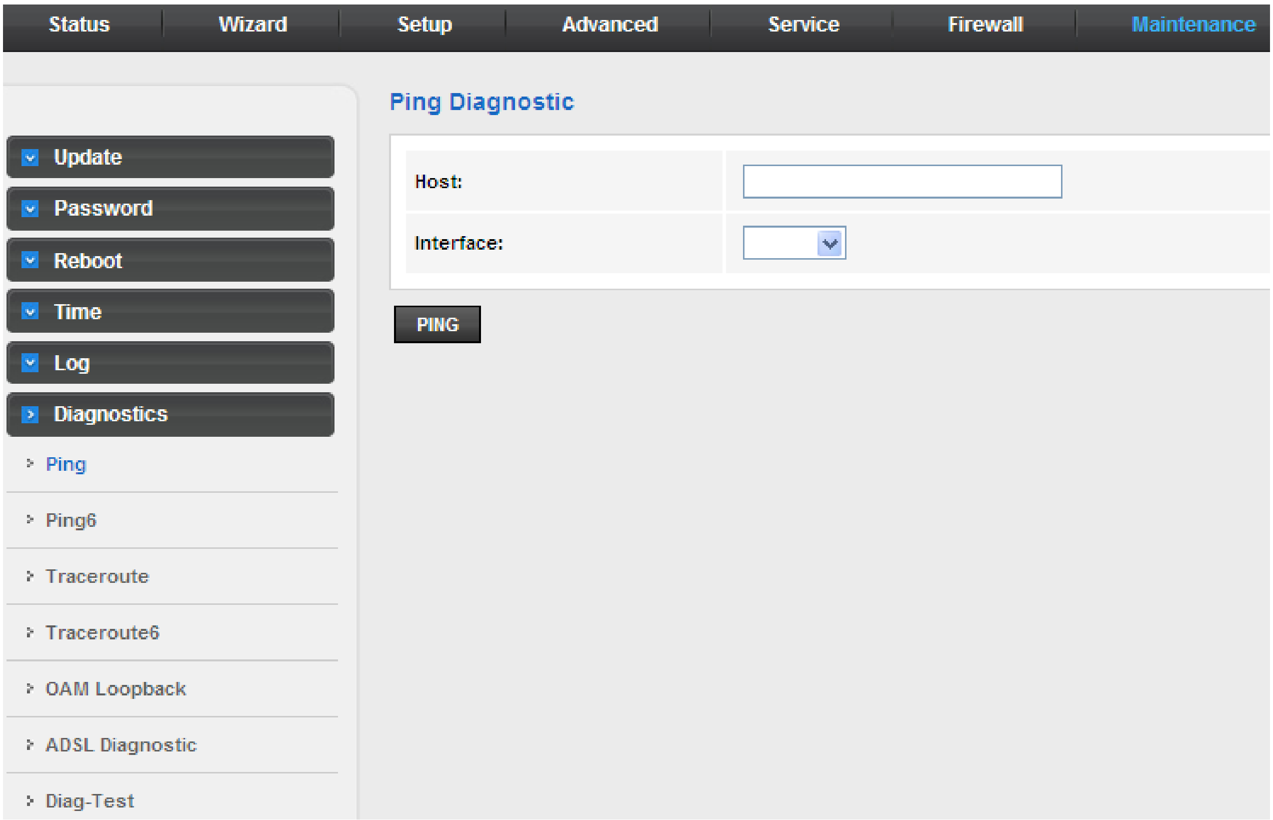
Fields	Description
Error	Enable/Disable the function to display the Error.
Notice	Enable/Disable the function to notify the Error.

3.9.6 Diagnostic

In the navigation bar, click **Diagnostic**. The **Diagnostic** page displayed contains **Ping**, **Ping6**, **Traceroute**, **Traceroute6**, **OAM Loopback**, **ADSL Statistics** and **Diag-Test**.

3.9.6.1 Ping

Choose **Diagnostic** > **Ping** and the page shown in the following figure appears.

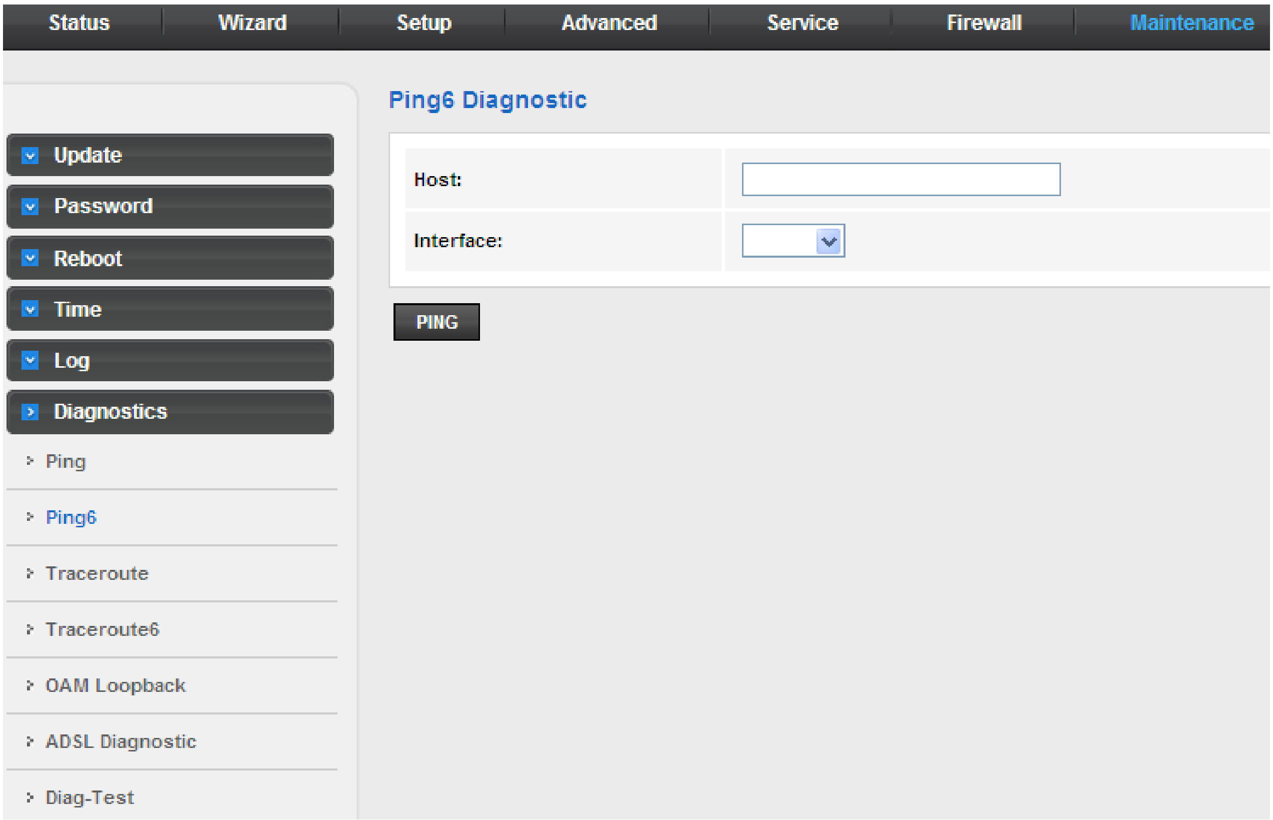


The following table describes the parameter:

Field	Description
Host Address	Enter IP address you want to ping.
Interface	Choose a WAN interface.

3.9.6.2 Ping6

Choose **Diagnostic** > **Ping6** and the page shown in the following figure appears.



Ping6 Diagnostic

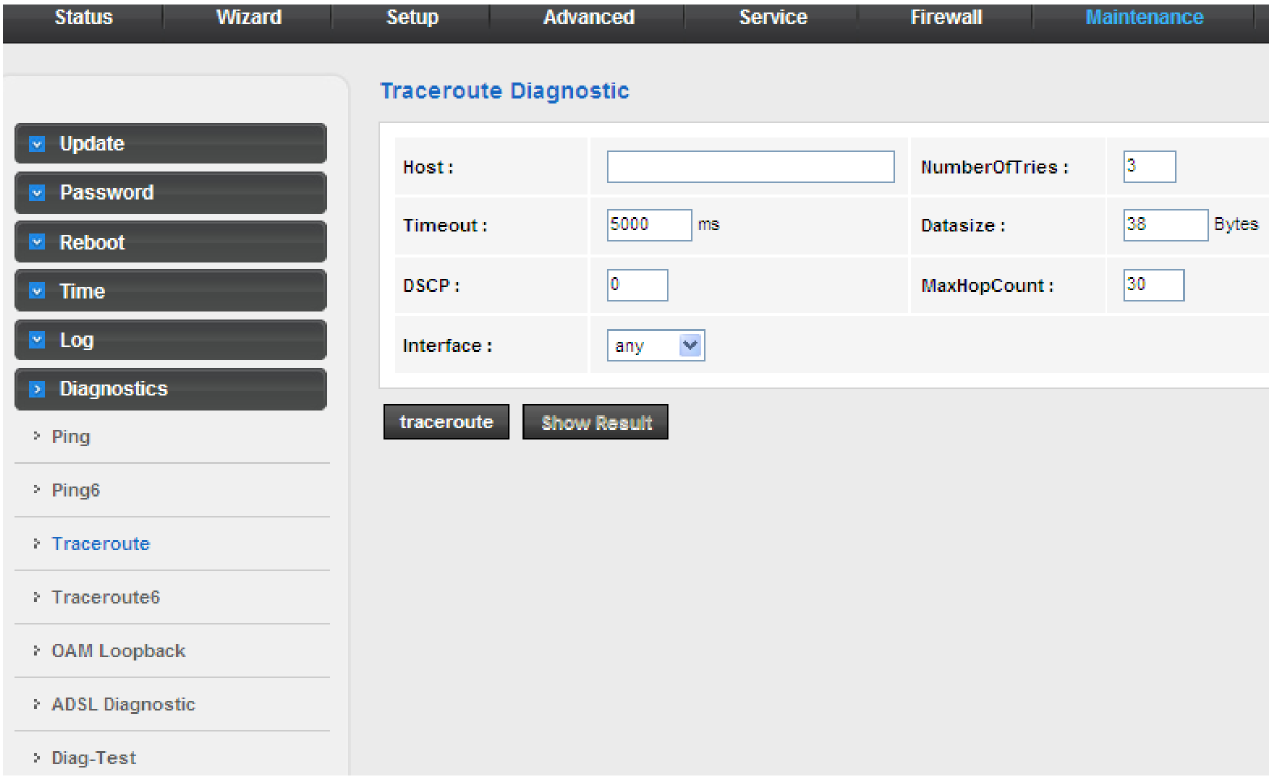
Host:

Interface:

Field	Description
Host Address	Enter IPv6 address you want to ping.
Interface	Choose a WAN interface.

3.9.6.3 Traceroute

Choose **Diagnostic** >**Traceroute** and the following page appears. By Traceroute Diagnostic, you can track the route path through the information which is from your computer to the Internet other side host.



Traceroute Diagnostic

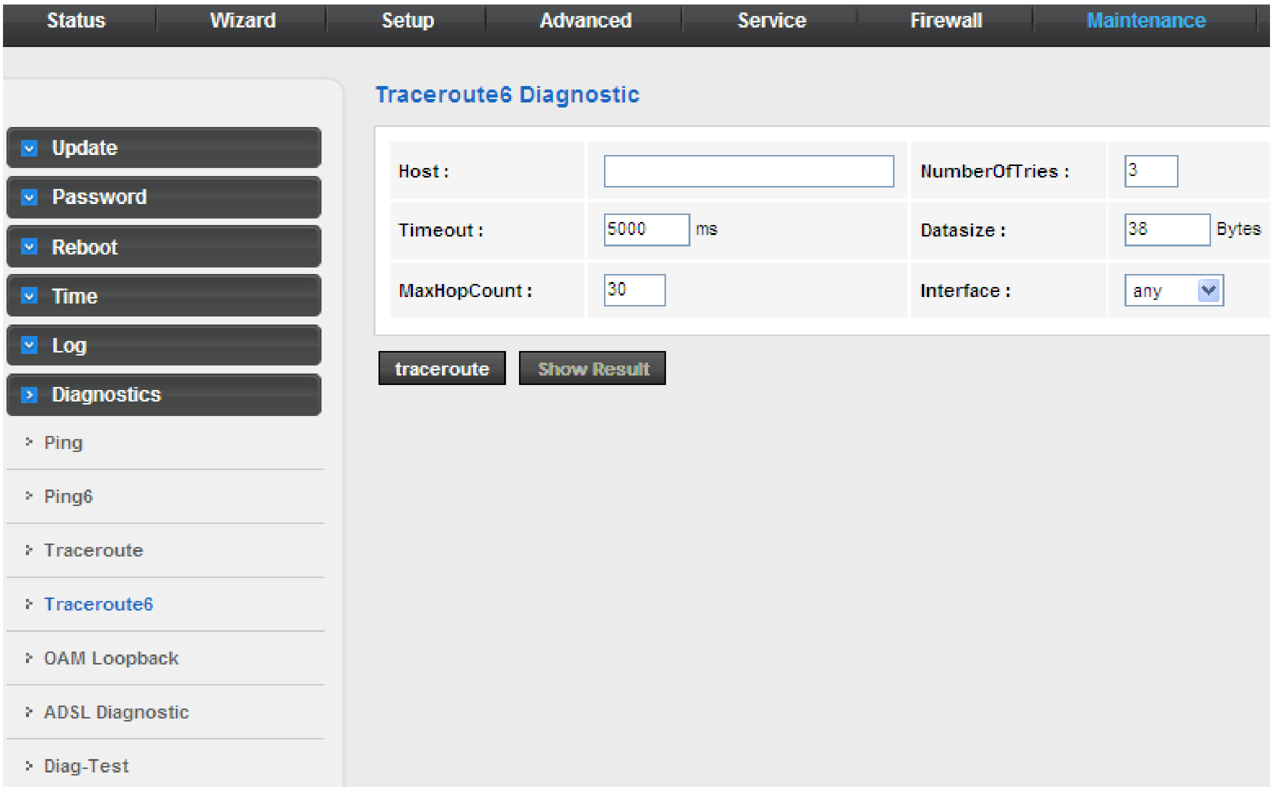
Host :		NumberOfTries :	3
Timeout :	5000 ms	Datasize :	38 Bytes
DSCP :	0	MaxHopCount :	30
Interface :	any		

The following table describes the parameters:

Field	Description
Host	Enter the destination host address for diagnosis.
NumberOfTries	Number of repetitions.
Timeout	Put in the timeout value.
Datasize	Packet size.
DSCP	Differentiated Services Code Point, You should set a value between 0-63.
MaxHopCount	Maximum number of routes.
Interface	Select the interface.

3.9.6.4 Traceroute6

Choose Diagnostic >Traceroute6 and the following page appears. By Traceroute Diagnostic, you can track the route path through the information which is from your computer to the Internet other side host.



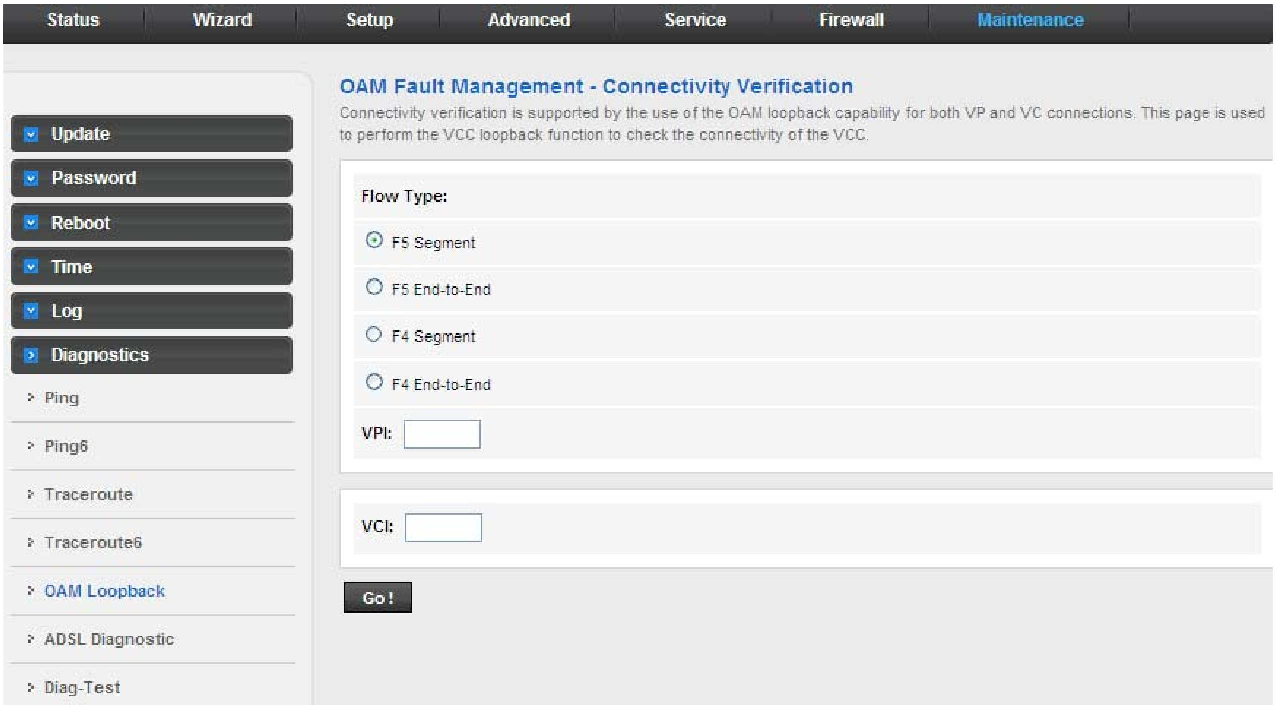
Traceroute6 Diagnostic

Host :		NumberOfTries :	3
Timeout :	5000 ms	Datasize :	38 Bytes
MaxHopCount :	30	Interface :	any

Fields	Description
Host	The address of a destination host to be diagnosed.
Number of Tries	Repeat times.
Timeout	Timeout duration.
Data size	Data packet size.
Max. Hop Count	Maximum number of routes.
Interface	Select the interface.

3.9.6.5 OAM Loopback

Choose **Diagnostic** > **OAM Loopback** and the page shown in the following figure appears. On this page, you can use VCC loopback function to check the connectivity of the VCC. The ATM loopback test is useful for troubleshooting problems with the DSLAM and ATM network.



OAM Fault Management - Connectivity Verification

Connectivity verification is supported by the use of the OAM loopback capability for both VP and VC connections. This page is used to perform the VCC loopback function to check the connectivity of the VCC.

Flow Type:

● F5 Segment

○ F5 End-to-End

○ F4 Segment

○ F4 End-to-End

VPI:

VCI:

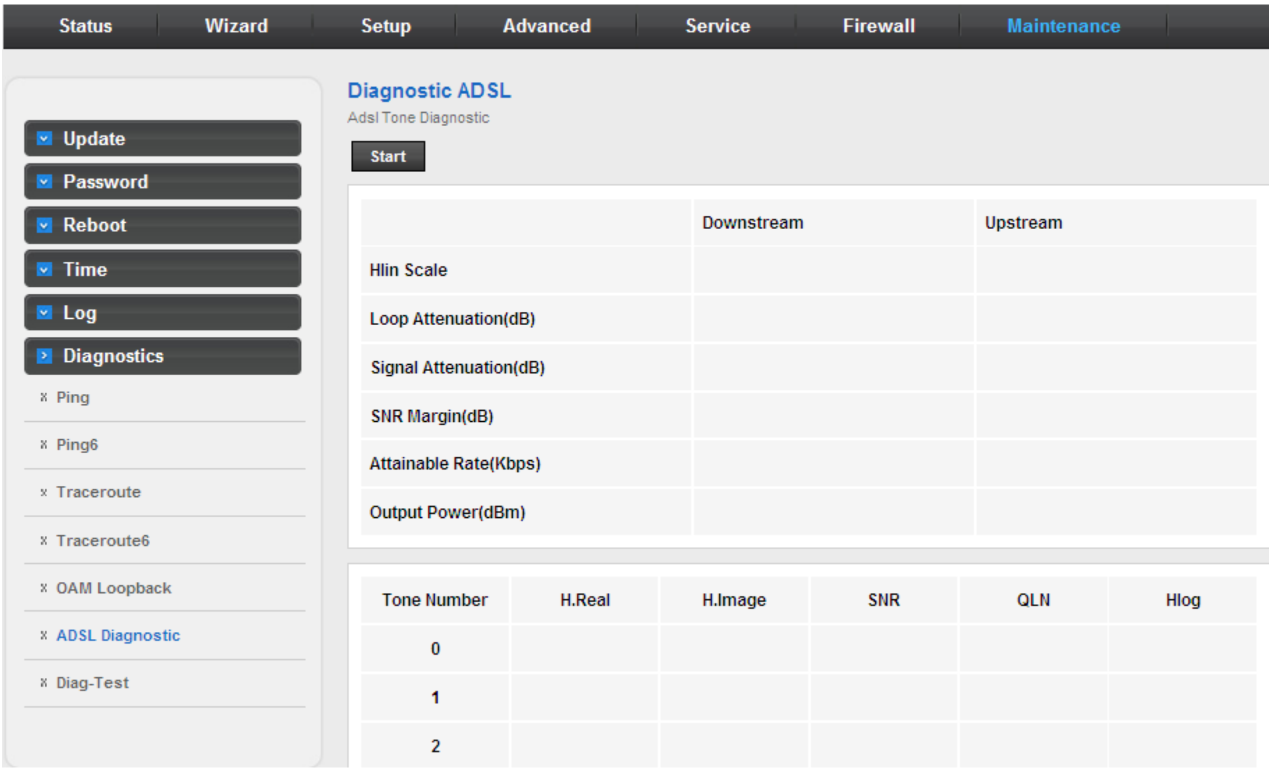
Go !

Click **Go!** to start testing.

Fields	Description
Flow Type	There are 4 flow types. The selection can be F5 Segment, F5 End-to-End, F4 Segment and F4 End-to-End
VPI	Virtual Path Identifier
VCI	Virtual Circuit Identifier.

3.9.6.6 ADSL Diagnostic

Choose **Diagnostic** > **ADSL Diagnostic** and the page shown in the following figure appears. It is used for ADSL tone diagnostics.



Diagnostic ADSL

Adsl Tone Diagnostic

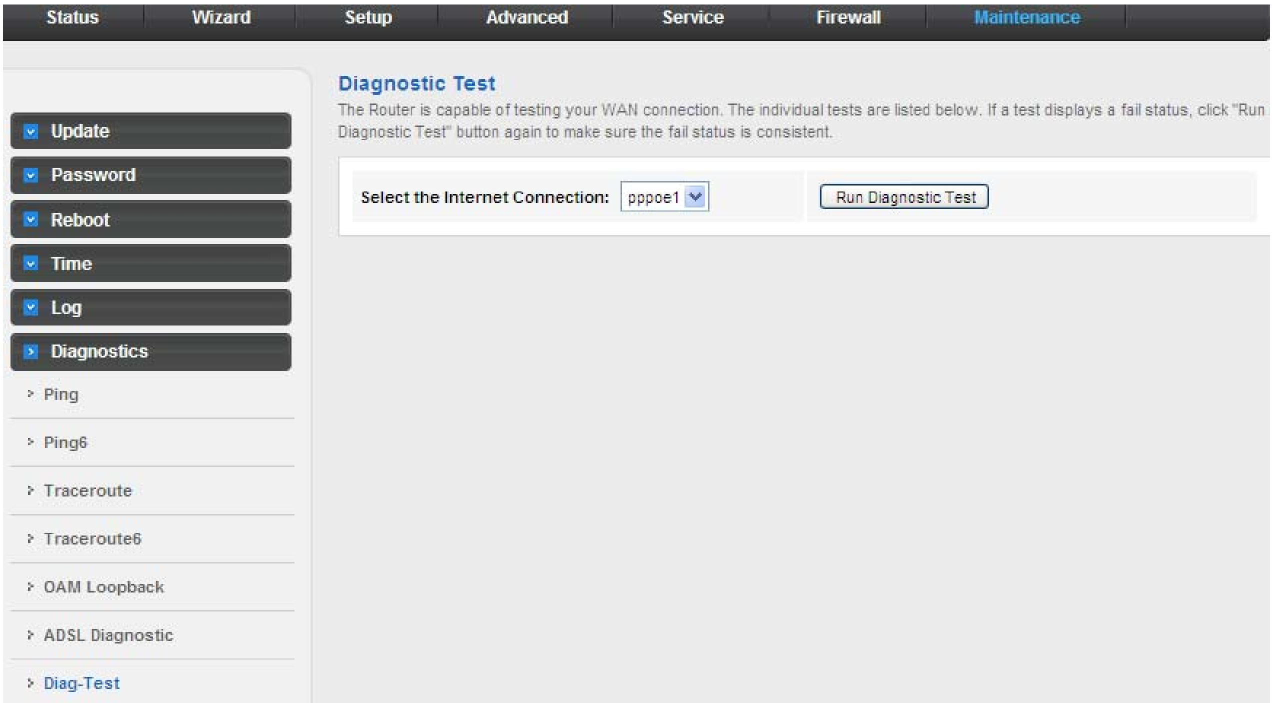
	Downstream	Upstream
Hlin Scale		
Loop Attenuation(dB)		
Signal Attenuation(dB)		
SNR Margin(dB)		
Attainable Rate(Kbps)		
Output Power(dBm)		

Tone Number	H.Real	H.Image	SNR	QLN	Hlog
0					
1					
2					

Click **Start** to start ADSL tone diagnostics.

3.9.6.7 Diag-Test

Choose **Diagnostics** > **Diag-Test** and the page shown in the following figure appears. On this page, you can test the DSL connection. You can also view the LAN status connection and ADSL connection.



Diagnostic Test

The Router is capable of testing your WAN connection. The individual tests are listed below. If a test displays a fail status, click "Run Diagnostic Test" button again to make sure the fail status is consistent.

Select the Internet Connection: pppoe1

Click **Run Diagnostic Test** to start testing.

Chapter 4. Q&A

Question	Answer
Why are all the indicators off?	● Check the connection between the power adapter and the power socket. ● Check whether the power switch is turned on.
Why is the **LAN** indicator not on?	Check the following: ● The connection between the device and the PC, the hub, or the switch ● The running status of the computer, hub, or switch
Why is the **Link** indicator not on?	Check the connection between the **Line** interface of the device and the socket.
Why does the Internet access fail when the **Link** indicator is on?	Ensure that the following information is entered correctly. ● VPI and VCI ● User name and password
Why does the web configuration page of the device fail to be accessed?	Choose **Start** > **Run** from the desktop. Enter **Ping 192.168.1.1** (the default IP address of the device) in the DOS window. If the web configuration page still cannot be accessed, check the following configurations. ● The connection between the device and the computer ● The TCP/IP properties of the network card of the computer
How to restore the default configuration after incorrect configuration?	Keep the device powered on and press the **Reset** button for 5 seconds. The device automatically reboots and is restored to the factory default configuration. The default configurations of the device are as follows: ● IP address: **192.168.1.1** ● Subnet mask: **255.255.255.0**. ● For an administrator user, use admin for both user name and password.