SW200

User Manual

V1.0

Contents

1 Introduction

The device supports multiple line modes. It provides four 10/100 base-T Ethernet interfaces at the user end. The device provides high-speed ADSL2/2+ broadband connection to the Internet or Intranet for high-end users, such as net bars and office users. It provides high performance access to the Internet.
The device supports WLAN access, such as WLAN AP or WLAN device, to the Internet. It complies with IEEE 802.11, 802.11b/g/n specifications, WEP, WPA, and WPA2 security specifications.

1.1 Safety Precautions

Follow the following instructions to prevent the device from risks and damage caused by fire or electric power:

- Use volume labels to mark the type of power.
- Use the power adapter packed within the device package.
- Pay attention to the power load of the outlet or prolonged lines. An overburden power outlet or damaged lines and plugs may cause electric shock or fire accident. Check the power cords regularly. If you find any damage, replace it at once.
- Proper space left for heat dissipation is necessary to avoid damage caused by overheating to the device. The long and thin holes on the device are designed for heat dissipation to ensure that the device works normally. Do not cover these heat dissipation holes.
- Do not put this device close to a place where a heat source exists or high temperature occurs. Avoid the device from direct sunshine.
- Do not put this device close to a place where it is over damp or watery. Do not spill any fluid on this device.
- Do not connect this device to any PCs or electronic products, unless our customer engineer or your broadband provider instructs you to do this, because any wrong connection may cause power or fire risk.
- Do not place this device on an unstable surface or support.

1.2 LEDs and Interfaces

Front Panel

The following table describes the LEDs of the device.

LEDs	Status	Description
Power	On	The initialization of the device is successful.
	Off	The device is powered off.
DSL	On	DSL link up / link synchronized.
	Off	Link disconnection.
	Blinking	Link training / DSL link not synchronized.
INT	On	Successful PPP session.
	Blinking	Failure PPP session (1 minute after link up).
	Off	Before DSL link up.
WiFi	On	The WLAN connection has been activated.
	Off	The WLAN connection is not activated.
LAN1~4	On	The LAN connection is normal and activated.
	Off	The LAN interface is disconnected.
WPS	Blinking	WPS is triggered, and is waiting for client to negotiate.
	Off	WPS is idle.

Rear Panel

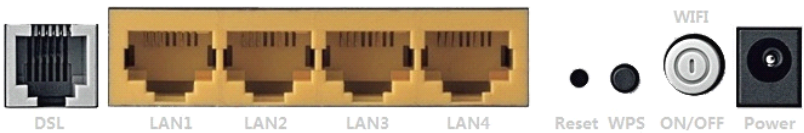


Figure 1

The following table describes the interfaces and buttons of the device:

Interface	Description
Reset	Reset to the factory default configuration. Keep the device powered on, and insert a needle into the hole for 3 seconds, then release it. The device is reset to the factory default configuration.
ON/OFF	Power switch, power on or power off the device.
Power	Power interface, for connecting to the power adapter of DC 12V, 0.5A.
LAN1~4	RJ45 interface, for connecting to the Ethernet interface of a PC or the Ethernet devices through an Ethernet cable.
DSL	RJ11 interface, for connecting to the ADSL interface or a splitter through a telephone cable.
WLAN/WPS	● Press the button between 1s and 5s to enable WLAN function. ● Press the button for more than 5s to enable WPS (Wi-Fi Protected Setup) function.

1.3 System Requirements

Recommended system requirements are as follows:

- Service subscriber
- 10 Base T/100 Base T Ethernet card
- Hub or switch (attached to several PCs through one of Ethernet interfaces on the device)
- Operating system: Windows 98 SE, Windows 2000, Windows ME, Windows XP, Windows Vista, Window 7
- Internet Explorer V5.0 or higher, Netscape V4.0 or higher, or FireFox 1.5 or higher

1.4 Features

The device supports the following features:

- Various line modes (line auto-negotiation)
- External PPPoE dial-up access
- Internal PPPoE/PPPoA dial-up access
- 1483B/1483R/MER access
- Multiple PVCs (eight at most)
- A single PVC with multiple sessions
- Multiple PVCs with multiple sessions
- Auto PVC
- DHCP server
- IPv4/IPv6
- NAT/NAPT
- ALG
- TR-069
- SNMP
- Static route
- Firmware upgrading through Web, TFTP, or FTP
- Resetting to the factory defaults through Reset button or Web
- DNS relay
- Virtual server
- Two-level passwords and usernames
- Web interface
- Telnet CLI
- System status display
- PPP session PAP/CHAP
- IP/Port filter
- Remote access control
- Line connection status test
- Remote management (Telnet; HTTP)
- Backup and restoration of configuration file
- IP quality of service (QoS)
- Universal plug and play (UPnP)

- WLAN with high-speed data transmission rate, compatible with IEEE 802.11b/g/n, 2.4 GHz compliant equipment

2 Hardware Installation

Step 1 Connect the **DSL** interface of the router and the **Modem** interface of the splitter through a telephone cable. Connect the phone to the **Phone** interface of the splitter through a cable. Connect the incoming line to the **Line** interface of the splitter.

The splitter has three interfaces:

- **Line**: Connect to a wall phone jack (RJ-11 jack)
- **Modem**: Connect to the ADSL jack of the device
- **Phone**: Connect to a telephone set.

Step 2 Connect the **LAN** interface of the modem with the network card of the PC through an Ethernet line (MDI/MDIX).

Note:

Use twisted-pair cables to connect with the hub or Switch.

Step 3 Plug the power adapter to the wall outlet and then connect the other end of it to the **Power** interface of the modem.

Connection 1

Figure1 displays the application diagram for the connection of the modem, PC, splitter, and telephone sets, when no telephone set is placed before a splitter. This type of connection is recommended.

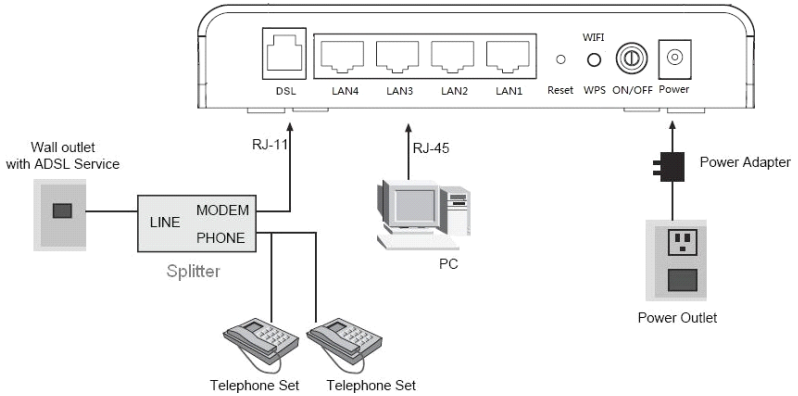


Figure 2 Connection diagram (no telephone set is placed before the splitter)

Connection 2

Figure 2 displays the connection when the telephone set is placed before a splitter.

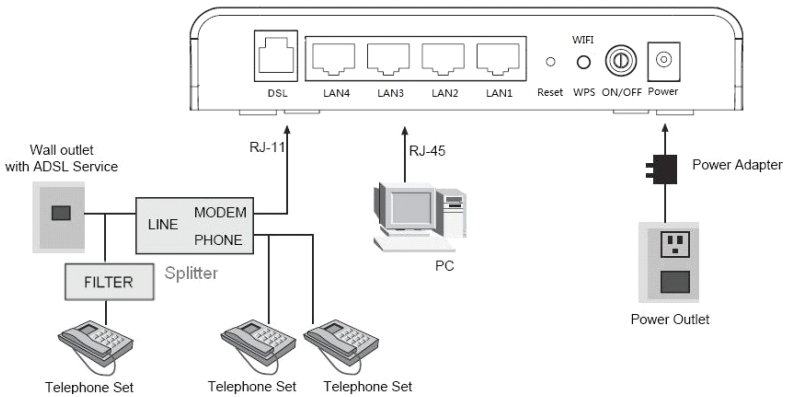


Figure 3 Connection diagram (a telephone set is placed before the splitter)

Note:

In actual application, it is recommended to following connection 1. When connection 2 is used, the filter must be installed close to the telephone cable. See Figure2. Do not use the splitter to replace the filter.

Installing a telephone directly before the splitter may lead to a failure of connection between the modem and the device of LAN side, or cannot access into the Internet, or slow the connection speed. If you really need to add a telephone set before the splitter, you have to add a micro filter before connecting to a telephone set. Do not connect several telephones before the splitter. Do not connect several telephones with the micro filter.

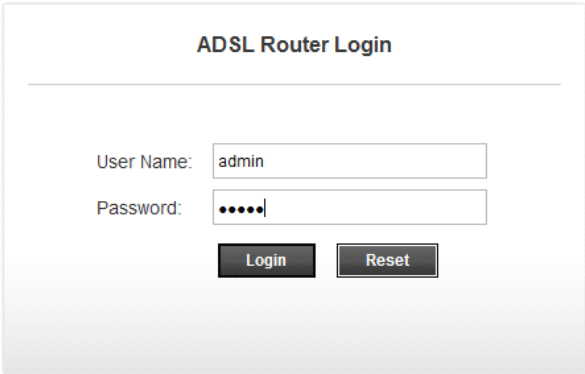
3 About the Web Configuration

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

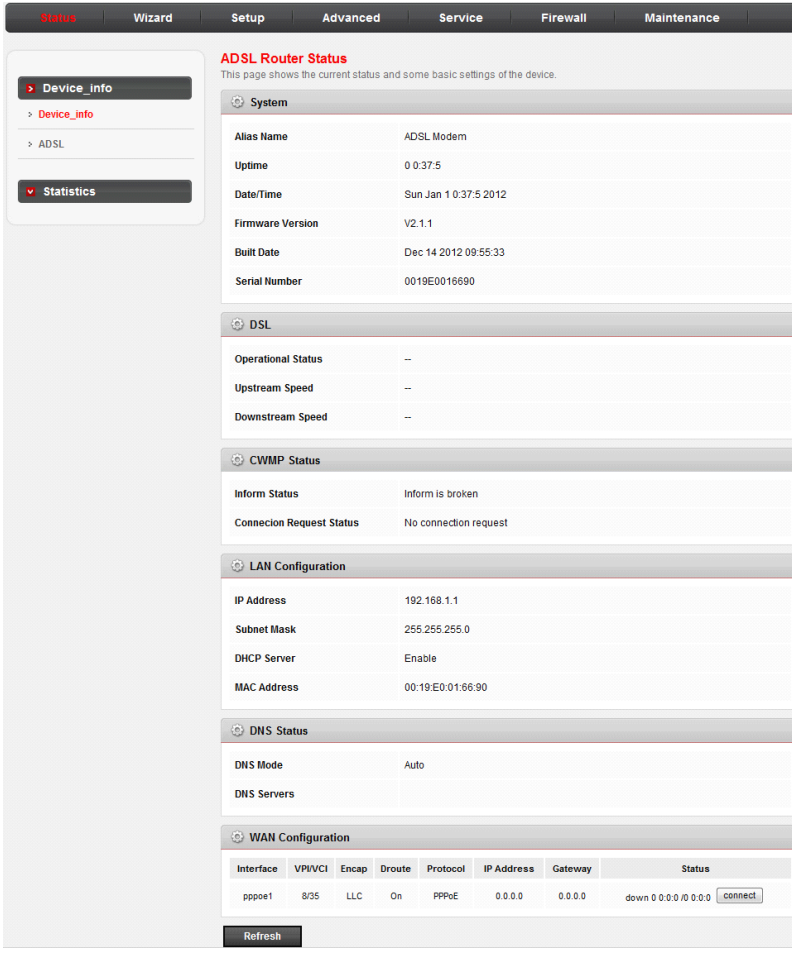
3.1 Access the Router

The following is the detailed description of accessing the router for the first time.
Configure the IP address of the PC as 192.168.1.X (2~254), Subnet Mask as 255. 255.255.0.
Open the Internet Explorer (IE) browser and enter **http://192.168.1.1**.In the **Login** page that is displayed, enter the username and password.

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

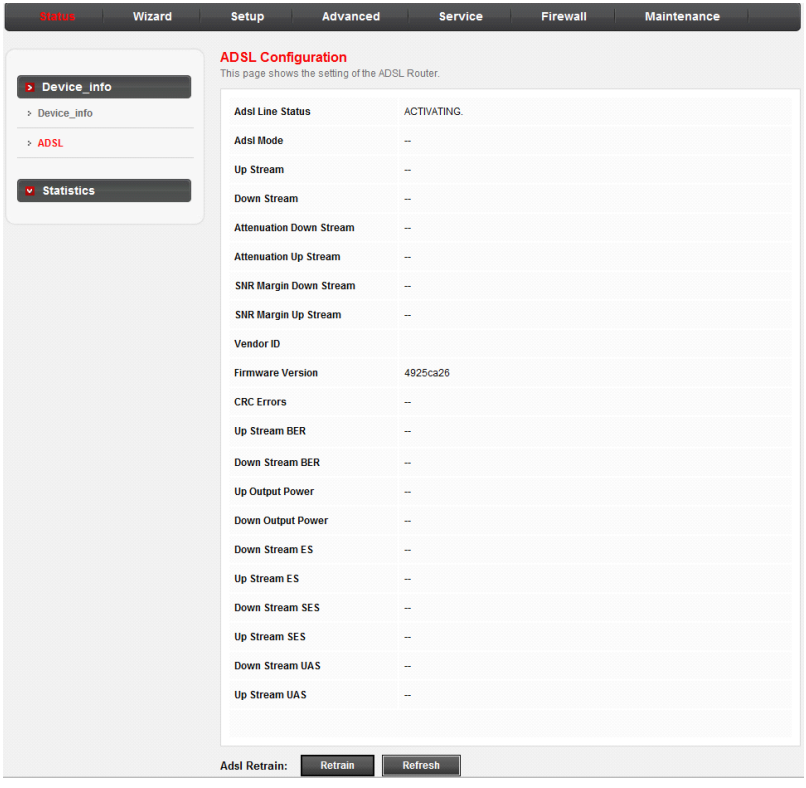


If you log in as a super user, you will see the **Device Info** page as shown below appears. You can check the basic settings of the modem, such as firmware version, upstream speed, downstream speed, LAN MAC address, LAN IP address, DHCP server status. You can also view the basic status of WAN and DNS server.

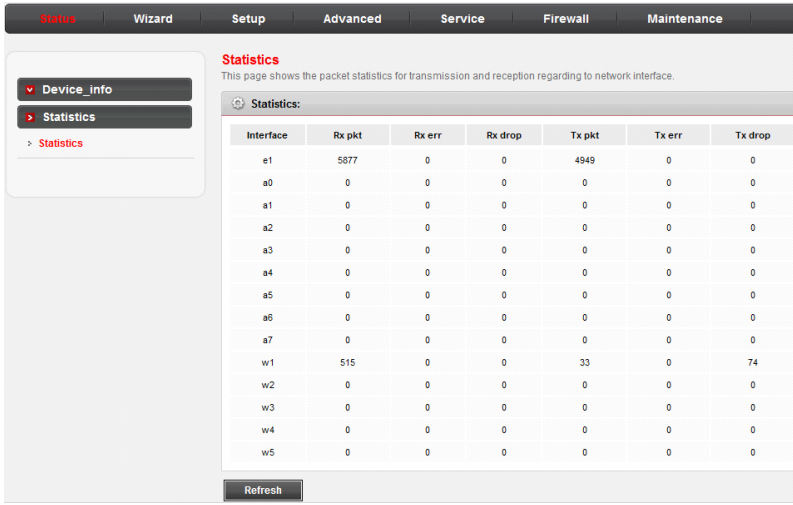

Status
Wizard
Setup
Advanced
Service
Firewall
Maintenance
Device_info
Device_info
ADSL
Statistics
ADSL Router Status
This page shows the current status and some basic settings of the device.
System
Alias Name
ADSL Modem
Uptime
0 0:37:5
Date/Time
Sun Jan 1 0:37:5 2012
Firmware Version
V2.1.1
Built Date
Dec 14 2012 09:55:33
Serial Number
0019E0016690
DSL
Operational Status
--
Upstream Speed
--
Downstream Speed
--
CWMP Status
Inform Status
Inform is broken
Connecion Request Status
No connection request
LAN Configuration
IP Address
192.168.1.1
Subnet Mask
255.255.255.0
DHCP Server
Enable
MAC Address
00:19:E0:01:66:90
DNS Status
DNS Mode
Auto
DNS Servers
WAN Configuration
Interface
VPI/VCI
Encap
Droute
Protocol
IP Address
Gateway
Status
pppoe1
8/35
LLC
On
PPPoE
0.0.0.0
0.0.0.0
down 0 0:0:0 /0 0:0:0
connect
Refresh

3.2 Status

The tab **Status** contains **Device Info** and **Statistics**. Click **Status** > **Device Info** > **ADSL**, the following page appears. You can see the router settings such as the Adsl Line Status, Vendor ID and Firmware Version.

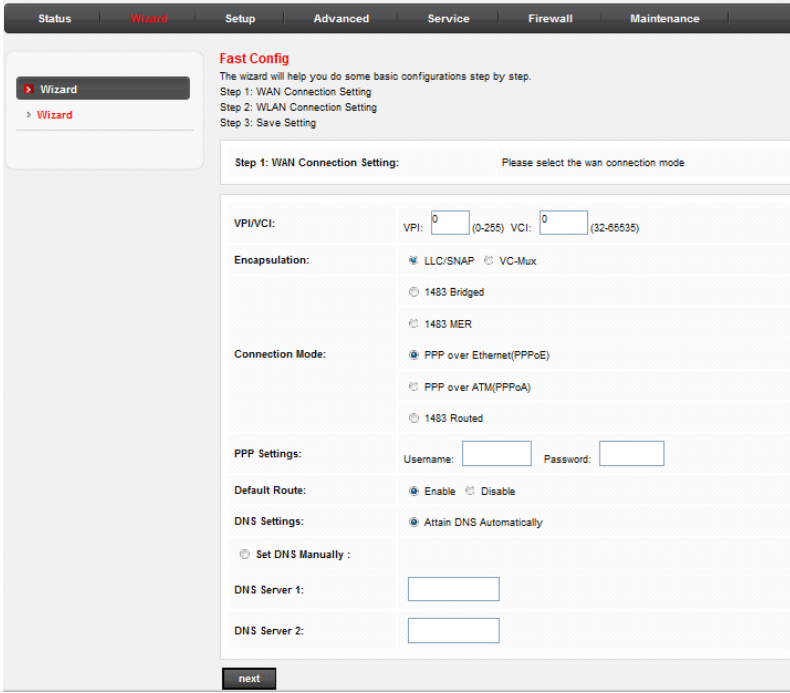


Click **Status** > **Statistics**, the following page appears. In this page, you can view the statistics of each network port.

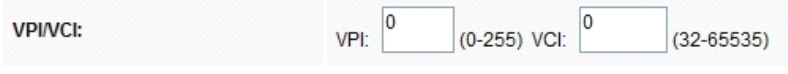


3.3 Wizard

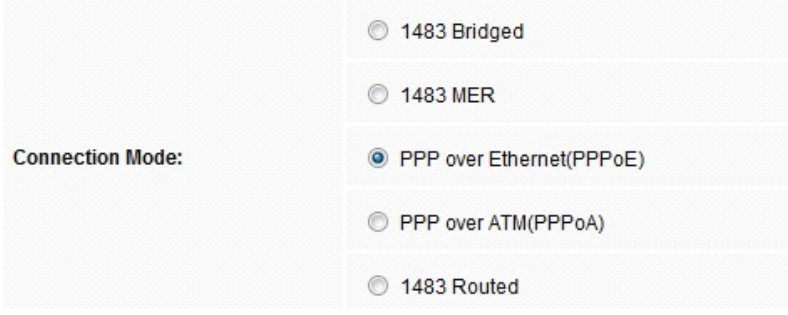
In the navigation bar, click **Wizard**. The tab **Wizard** only contains **Wizard.**



1) Change the VPI or VCI values which are used to define a unique path for your connection. If you have been given specific settings for this to configuration, type in the correct values assigned by your ISP.

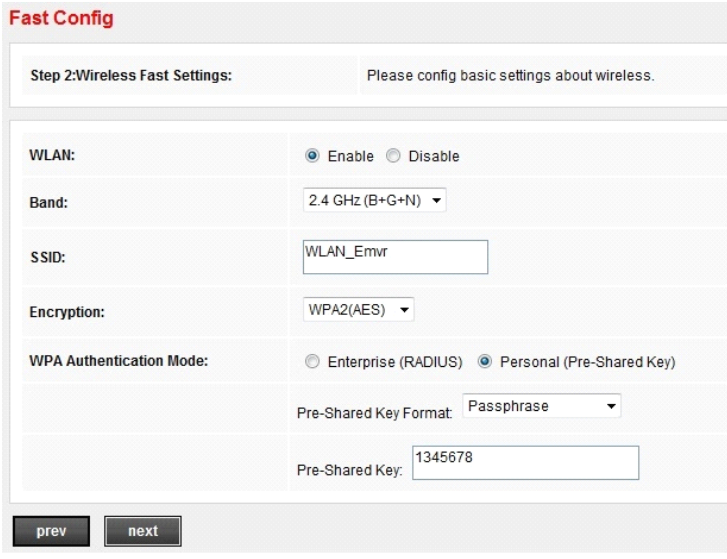


2) Please select the Connection Type given by your ISP.

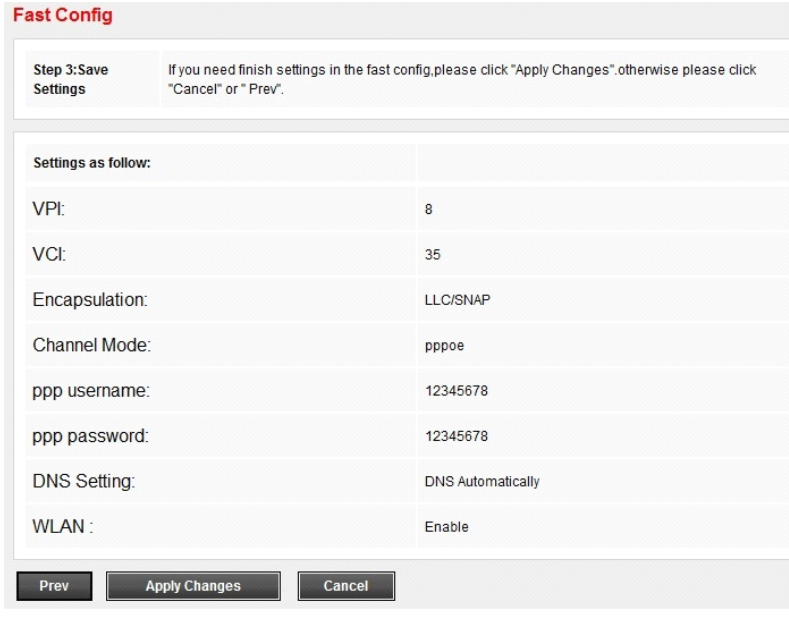


3) Here we use PPPoE as an example. Enter the Username, Password and Confirm Password given by your ISP, and then click Next.

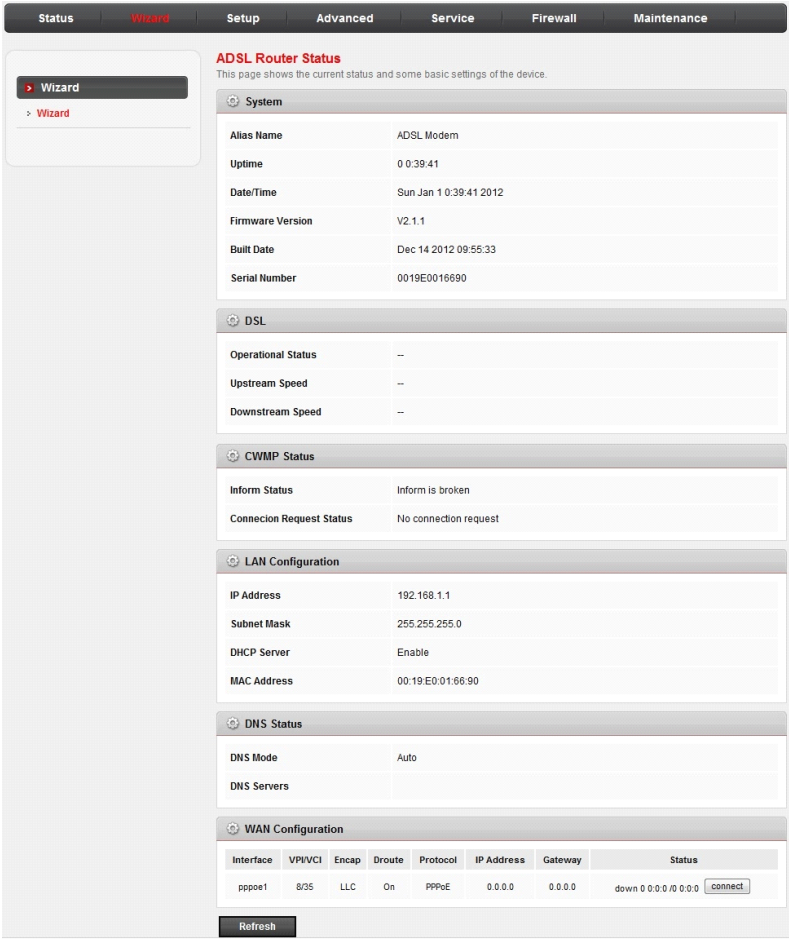
4) On the Wireless screen, we use the default SSID, select a Mode. Set a Password or select Disable Security(Disable Security is not recommended.), and then click **Next** to continue.



5) On this page, please confirm all parameters. Click **Prev** to modify or click the **Apply Changes** button to save your configuration.



6) You will see the Complete screen below.


Status
Wizard
Setup
Advanced
Service
Firewall
Maintenance
Wizard
Wizard
ADSL Router Status
This page shows the current status and some basic settings of the device.
System
Alias Name
ADSL Modem
Uptime
0 0:39:41
Date/Time
Sun Jan 1 0:39:41 2012
Firmware Version
V2.1.1
Built Date
Dec 14 2012 09:55:33
Serial Number
0019E0016690
DSL
Operational Status
--
Upstream Speed
--
Downstream Speed
--
CWMP Status
Inform Status
Inform is broken
Connecion Request Status
No connection request
LAN Configuration
IP Address
192.168.1.1
Subnet Mask
255.255.255.0
DHCP Server
Enable
MAC Address
00:19:E0:01:66:90
DNS Status
DNS Mode
Auto
DNS Servers
WAN Configuration
Interface
VPI/VCI
Encap
Droute
Protocol
IP Address
Gateway
Status
pppoe1
8/35
LLC
On
PPPoE
0.0.0.0
0.0.0.0
down 0 0:0:0 /0 0:0:0
connect
Refresh

3.4 Setup

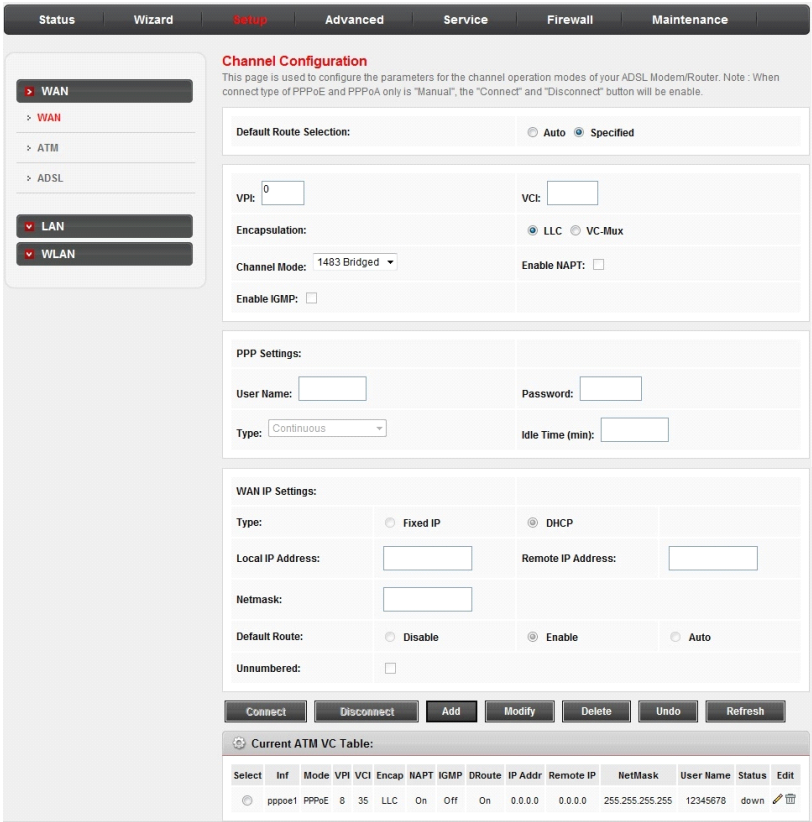
In the navigation bar, click **Setup**. The tab **Setup** contains **WAN, LAN** and **WLAN.**

3.4.1 WAN Configuration

3.4.1.1 WAN

Choose **Setup** > **WAN** > **WAN** and the page shown in the following figure appears.

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



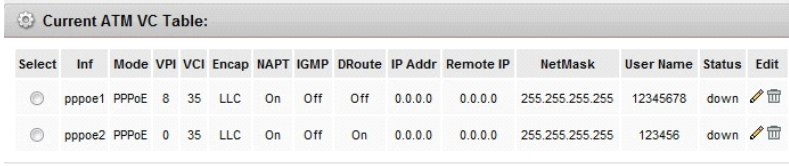
The following table describes the parameters of this page.

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.
VCI	The virtual channel between two points in an ATM network, ranging from 32 to 65535 (1 to

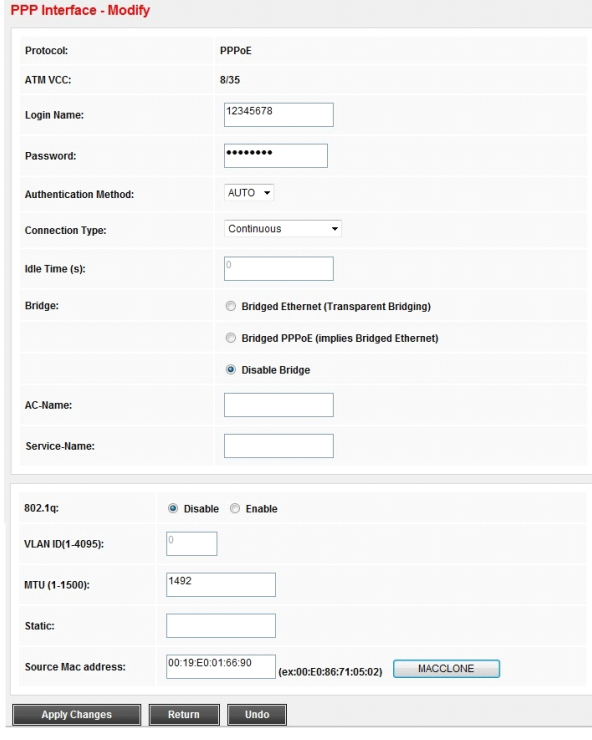
Field	Description
	31 are reserved for known protocols)
Encapsulation	You can choose **LLC** and **VC-Mux**.
Channel Mode	You can choose **1483 Bridged**, **1483 MER**, **PPPoE**, **PPPoA**, **1483 Routed** or **IPoA**.
Enable NAPT	Select it to enable Network Address Port Translation (NAPT) function. 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.
IP Protocol	Select this interface support ipv4/ipv6, ipv4 or ipv6.
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

Field	Description
	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.
IPv6 WAN Setting	Set ipv6 wan setting if this interface support ipv6
Address Mode	Select this interface support Slaac or Static to generate wan ipv6 addresses.
Enable DHCPv6 Client	Enable or disable dhcpv6 client on this interface, if enable, user can specify if the dhcpv6 client request Address or request Prefix.
Add	After configuring the parameters of this page, click it to add a new PVC into the **Current ATM VC Table**.
Modify	Select a PVC in the **Current ATM VC Table**, then modify the parameters of this PVC. After finishing, click it to apply the settings of this PVC.
Delete	Select a PVC in the Current ATM VC Table, and then click **Delete** to delete it
Current ATM VC 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.

After proper settings, click Add and the following page appears.



Click in the **PPPoE** mode, the page shown in the following figure appears. In this page, you can configure parameters of this PPPoE PVC.

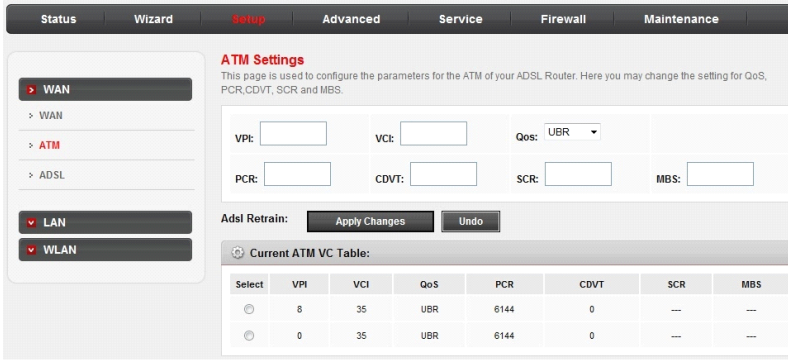


The following table describes the parameters and buttons of this page.

Field	Description
Protocol	It displays the protocol type used for this WAN connection.
ATM VCC	The ATM virtual circuit connection assigned for this PPP interface (VPI/VCI).
Login Name	The user name provided by your ISP.
Password	The password provided by your ISP.
Authentication Method	You can choose **AUTO**, **PAP** or **CHAP**.
Connection Type	You can choose **Continuous**, **Connect on Demand** or **Manual**.
Idle Time (s)	If choose **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.
Bridge	You can select **Bridged Ethernet**, **Bridged PPPoE** or **Disable Bridge**.
AC-Name	The accessed equipment type.
Service-Name	The service name.
802.1q	You can select **Disable** or **Enable**. After enable it, you need to enter the VLAN ID. The value ranges from 1 to 4095.
Apply Changes	Click it to save the settings of this page temporarily.
Return	Click it to return to the **Channel Configuration** page.
Reset	Click it to refresh this page.
Source Mac address	The MAC address you want to clone.
MAC Clone	Click it to enable the MAC Clone function with the MAC address that is configured.

3.4.1.2 ATM Setting

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



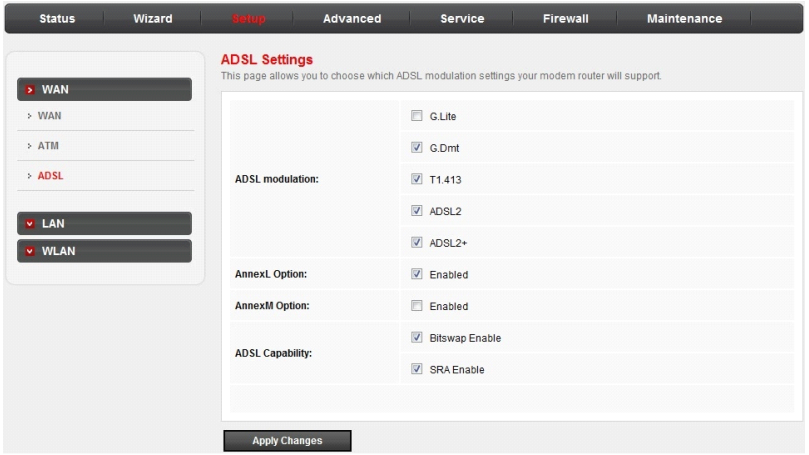
The following table describes the parameters of this page.

Field	Description
VPI	The virtual path identifier of the ATM PVC.
VCI	The virtual channel identifier of the ATM PVC.
QoS	The QoS category of the PVC. You can choose **UBR**, **CBR**, **rt-VBR** or **nrt-VBR**.
PCR	Peak cell rate (PCR) is the maximum rate at which cells can be transmitted along a connection in the ATM network. Its value ranges from 1 to 65535.
CDVT	Cell delay variation tolerance (CDVT) is the amount of delay permitted between ATM cells (in microseconds). Its value ranges from 0 to 4294967295.
SCR	Sustain cell rate (SCR) is the maximum rate that traffic can pass over a PVC without the risk of cell loss. Its value ranges from 0 to 65535.

Field	Description
MBS	Maximum burst size (MBS) is the maximum number of cells that can be transmitted at the PCR. Its value ranges from 0 to 65535.

3.4.1.3 ADSL Setting

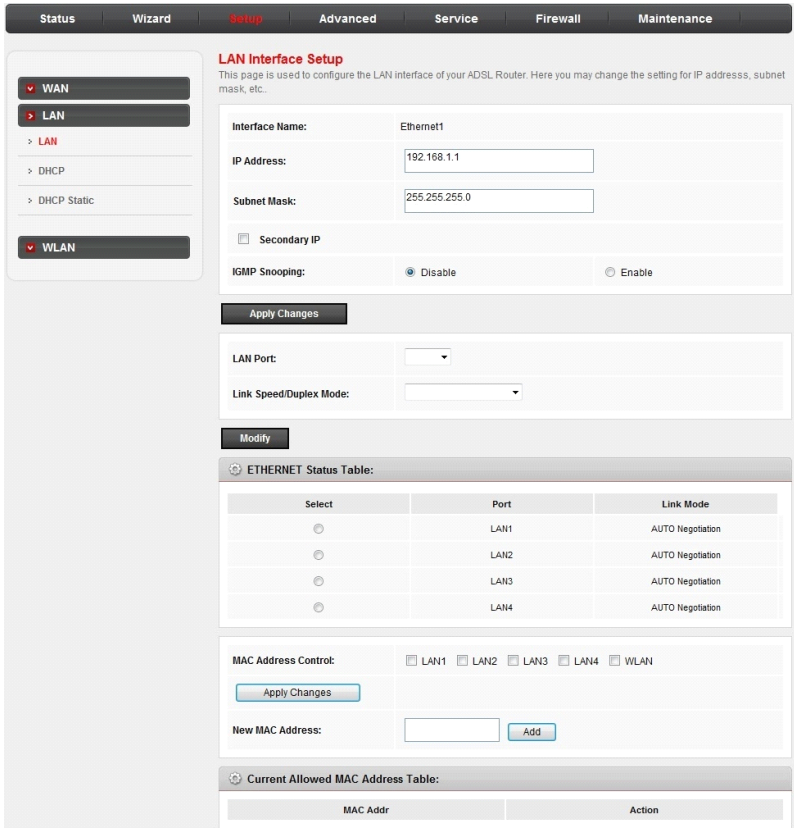
Click **ADSL** in the left pane, the page shown in the following figure appears. In this page, you can select the DSL modulation. Generally you need to remain this factory default settings. The router negotiates the modulation modes with the DSLAM.



3.4.2 LAN

3.4.2.1 LAN

Click **LAN** in the left pane, the page shown in the following figure appears.
In 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.



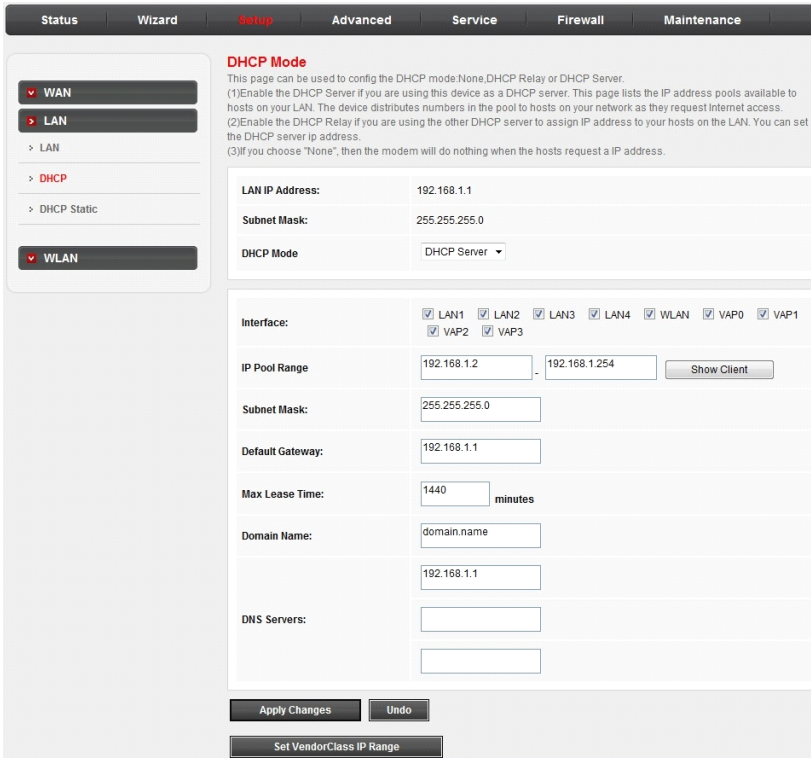
The following table describes the parameters of this page.

Field	Description
IP Address	Enter the IP address of LAN interface. It is recommended to use an address from a block that is reserved for private use. This address block is 192.168.1.1- 192.168.255.254.
Subnet Mask	Enter the subnet mask of LAN interface. The range

Field	Description
	of subnet mask is from 255.255.0.0-255.255.255.254.
Secondary IP	Select it to enable the secondary LAN IP address. The two LAN IP addresses must be in the different network.
LAN Port	You can choose the LAN interface you want to configure.
Link Speed/Duplex Mode	You can select the following modes from the drop-downlist:**100Mbps/FullDuplex**,**100Mbps/Half Duplex**,**10Mbps/FullDuplex**,**10Mbps/Half Duplex** and **Auto Negotiation**.
Modify	Select the index from Ethernet status table, and then click **modify**.
Ethernet Status Table	It shows the current Ethernet status list.
MAC Address Control	Select the LAN interface on which you want to run MAC Address Control.
New MAC Address	A MAC address to be added.
Current Allowed MAC Address Table	It shows the current allowed MAC address list.

3.4.2.2 DHCP

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

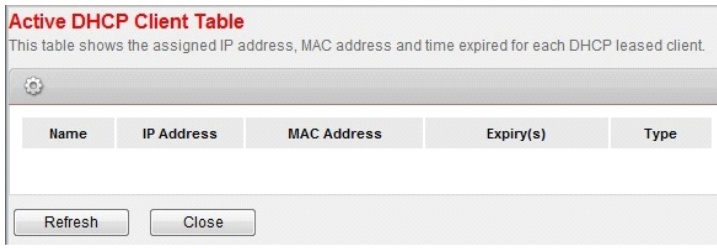


The following table describes the parameters of this page.

Field	Description
DHCP Mode	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 operation systems that support the DHCP client.
IP Pool Range	It specifies the first IP address in the IP address pool. The router assigns IP address that base on the IP

Field	Description
	pool range to the host.
Pool Size	It allows the size machines that can be set up
Show Client	Click it, the **Active DHCP Client Table** appears. It shows IP addresses assigned to clients.
Default Gateway	Enter the default gateway of the IP address pool.
Max Lease Time	The lease time determines the period that the host retains the assigned IP addresses before the IP addresses change.
Domain Name	Enter the domain name if you know. If you leave this blank, the domain name obtained by DHCP from the ISP is used. You must enter host name (system name) on each individual PC. The domain name can be assigned from the router through the DHCP server.
DNS Servers	You can configure the DNS server ip addresses for DNS Relay.
Set VendorClass IP Range	Click it, the **Device IP Range Table** page appears. You can configure the IP address range based on the device type.

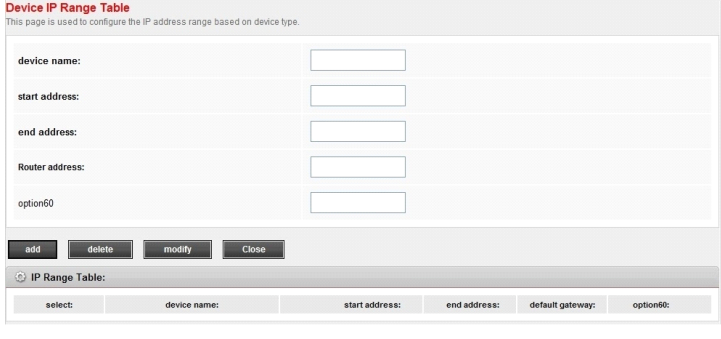
Click **Show Client** in the **DHCP Mode** page, the page shown in the following figure appears. You can view the IP address assigned to each DHCP client.



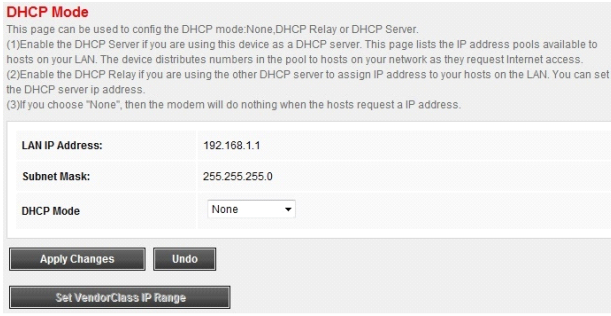
The following table describes the parameters and buttons in this page.

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-A0-C5-00-02-12.
Expiry (s)	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.

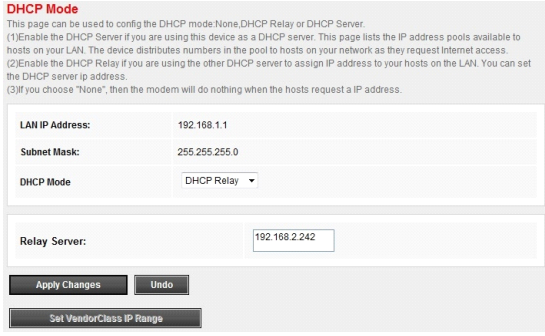
Click **Set Vendor Class IP Range** in the **DHCP Mode** page, the page as shown in the following figure appears. In this page, you can configure the IP address range based on the device type.



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



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

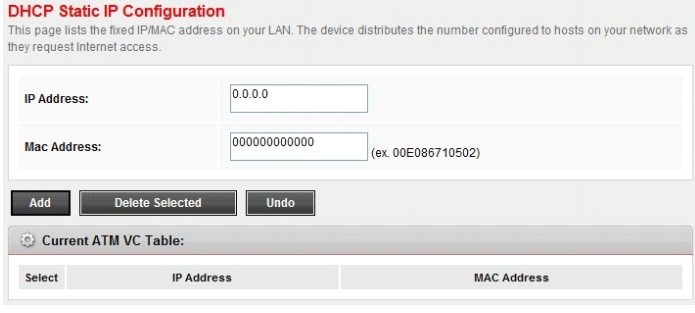


The following table describes the parameters and buttons of this page.

Field	Description
DHCP Mode	If set to **DHCP Relay**, the router acts a surrogate DHCP Server and relays the DHCP requests and reponses 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 of this page.
Undo	Click it to refresh this page.

3.4.2.3 DHCP Static

Click **DHCP Static** in the left pane, 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.



The following table describes the parameters and buttons of this page.

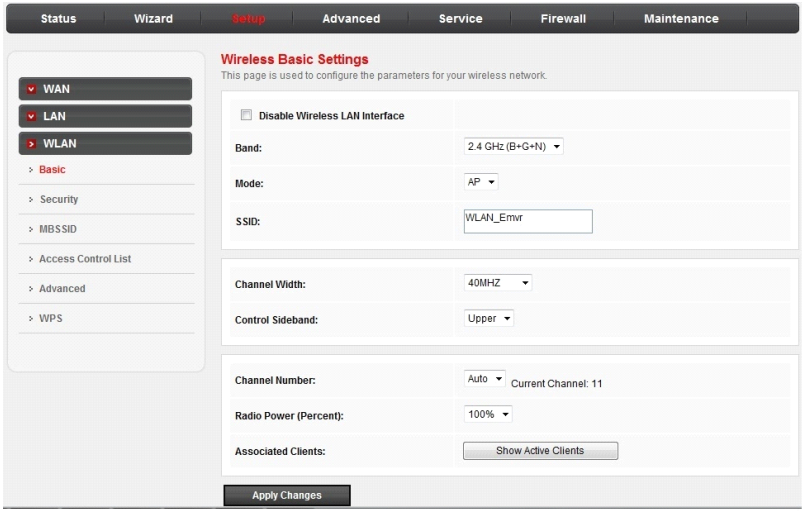
Field	Description
IP Address	Enter the specified IP address in the IP pool range, which is assigned to the host.
MAC Address	Enter the MAC address of a host on the LAN.
Add	After entering the IP address and MAC address, click it. A row will be added in the **DHCP Static IP Table**.
Delete Selected	Select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

3.4.3 WLAN

Choose **Setup** > **WLAN**. The WLAN page that is displayed contains **Basic**, **Security**, **MBSSID**, **Access Control**, **Advanced** and **WPS**.

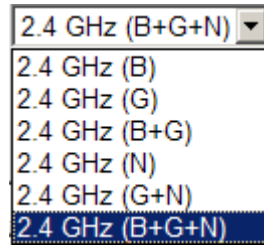
3.4.3.1 Basic Settings

Choose **WLAN** > **Basic**, and the following page appears. In this page, you can configure the parameters for wireless LAN clients that may connect to the modem.



The following table describes the parameters of this page.

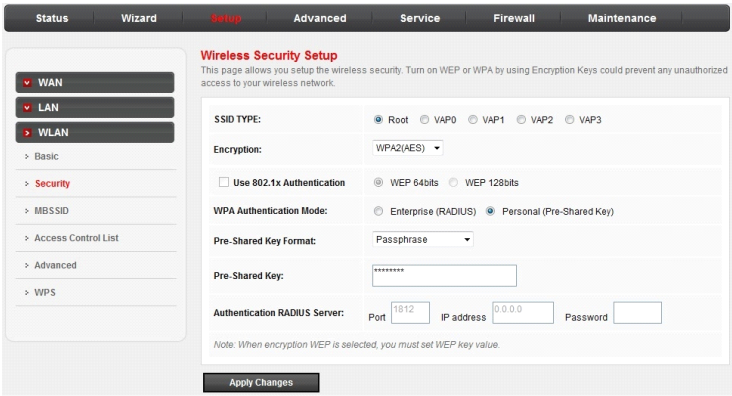
Field	Description
Band	Choose the working mode of the modem. You can choose from drop-down list.

Field	Description
	
Mode	Choose the network model of the modem, which is varied according to the software. By default, the network model of the modem is **AP**.
SSID	The service set identification (SSID) is a unique name to identify the modem in the wireless LAN. Wireless stations associating to the modem must have the same SSID. Enter a descriptive name that is used when the wireless client connecting to the modem.
Broadcast SSID	Enable or disable this function.
Channel Width	You can choose **20MHZ**, **40MHZ** or **20/40MHZ**.
Control Sideband	You can choose Upper or Lower.
Country/Area	Select the country from the drop-down list.
Channel Number	A channel is the radio frequency used by 802.11b/g/n wireless devices. You should use a different channel from an adjacent AP to reduce the interference. Interference and degrading performance occurs when radio signal from different APs overlap. Choose a channel from the drop-down list box.
Radio Power	You can choose the transmission power of the radio signal. The default one is **100%**. It is recommended to choose the default value**100%**.
Show Active Clients	Click it to view the information of the wireless

Field	Description
	clients that are connected to the modem.
Apply Changes	Click it to apply the settings temporarily. If you want to save the settings of this page permanently, click **Save** in the lower left corner.

3.4.3.2 Security

Choose **WLAN** > **Security**, and the following page appears.

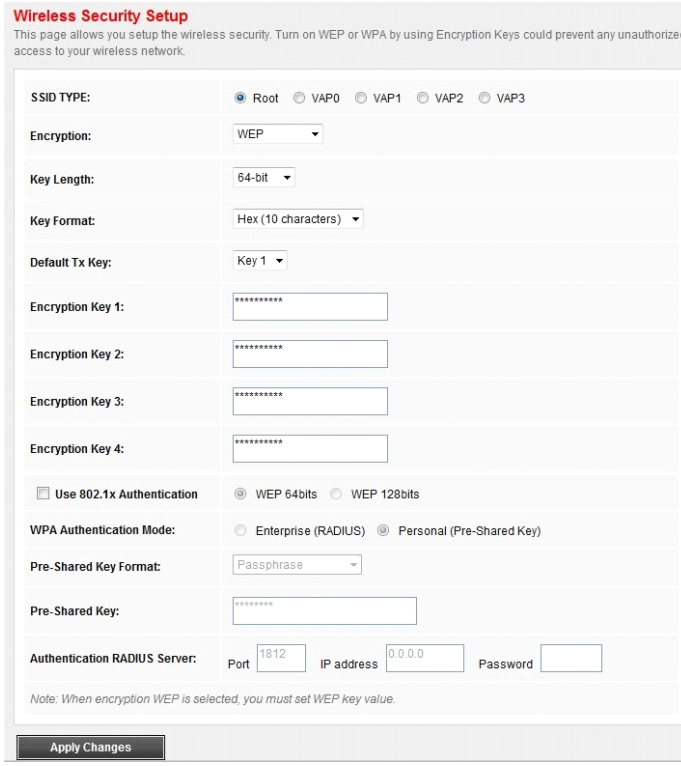


The following table describes the parameters of this page.

Field	Description
SSID Type	Service Set Identifier, is a name of a local area network
Encryption	Configure the wireless encryption mode. You can choose **None**, **WEP**, **WPA (TKIP)**, **WPA (AES)**, **WPA2 (AES)**, **WPA2 (TKIP)** or **WPA2 Mixed**. ● Wired equivalent privacy0 (WEP) encrypts data frames before transmitting over the wireless network. ● Wi-Fi protected access (WPA) is a subset of

Field	Description
	the IEEE802.11i security specification draft. ● WPA2 Mixed is the collection of WPA and WPA2 encryption modes. The wireless client establishes the connection between the modem through WPA or WPA2. Key differences between WPA and WEP are user authentication and improved data encryption.
Set WEP Key	It is available when you set the encryption mode to **WEP**. Click it, the **Wireless WEP Key Setup** page appears.
WPA Authentication Mode	● Select **Personal (Pre-Shared Key)**, enter the pre-shared key in the **Pre-Shared Key** field. ● Select **Enterprise (RADIUS)**, enter the port, IP address, and password of the Radius server. You need to enter the username and password provided by the Radius server when the wireless client connects the modem. If the encryption is set to **WEP**, the modem uses 802.1 X authentication, which is Radius authentication.

Click **Set WEP Key**, and the following page appears.



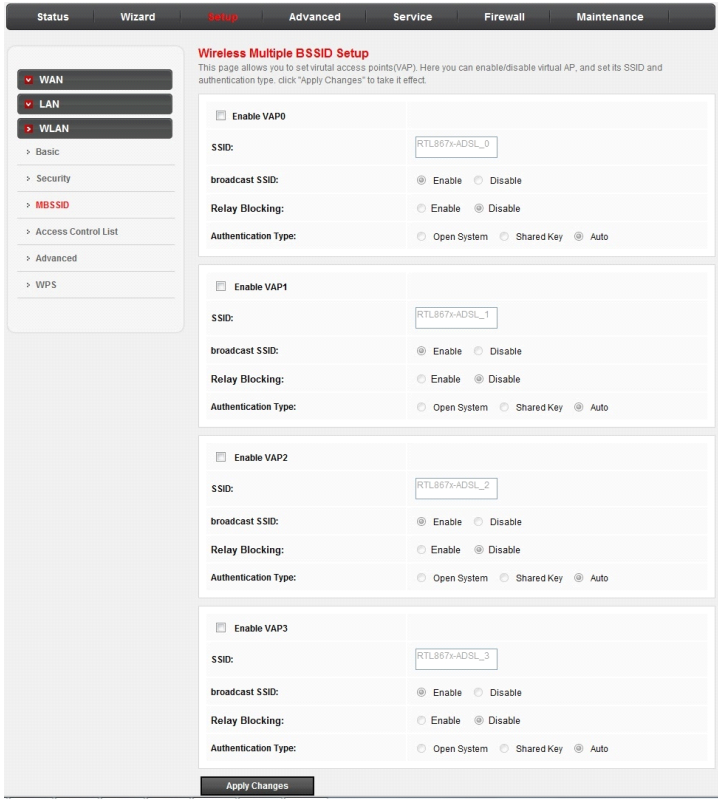
The following describes the parameters of this page.

Field	Description
Key Length	Choose the WEP key length. You can Choose **64-bit** or **128-bit**.
Key Format	● If you choose **64-bit**, you can choose ASCII (5 characters) or Hex (10 characters). ● If you choose **128-bit**, you can choose ASCII (13 characters) or Hex (26 characters).
Default Tx Key	Choose the index of WEP Key. You can choose **Key**

Field	Description
	1, **Key 2**, **Key 3** or **Key 4**.
Encryption Key 1 to 4	The Encryption keys are used to encrypt the data. Both the modem and wireless stations must use the same encryption key for data transmission. ● If you choose **64-bit** and **ASCII (5 characters)**, enter any 5 ASCII characters. ● If you choose **64-bit** and **Hex (10 characters)**, enter any 10 hexadecimal characters. ● If you choose **128-bit** and **ASCII (13 characters)**, enter any 13 ASCII characters. ● If you choose **128-bit** and **Hex (26 characters)**, enter any 26 hexadecimal characters.
Apply Changes	Click it to apply the settings temporarily. If you want to save the settings of this page permanently, click **Save** in the lower left corner.

3.4.3.3 Multi-BSSID

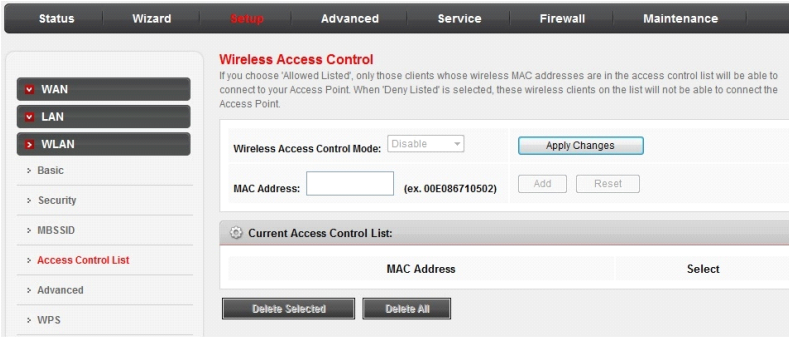
Choose **WLAN** > **MBSSID**, and the following page appears. In this page, you can configure the multi-BSSID of the wireless clients.



It supports 4 virtual access points (VAPs).It is a unique name to identify the modem in the wireless LAN. Wireless stations associating to the modem must have the same name. Enter a descriptive name that is used when the wireless client connecting to the modem.

3.4.3.4 Access Control

Choose **WLAN** > **Access Control List**, and the following page appears. In this page, you can configure the access control of the wireless clients.



Choose **Allow Listed** as the access control mode to enable white list function. Only the devices whose MAC addresses are listed in the **Current Access Control List** can access the modem.

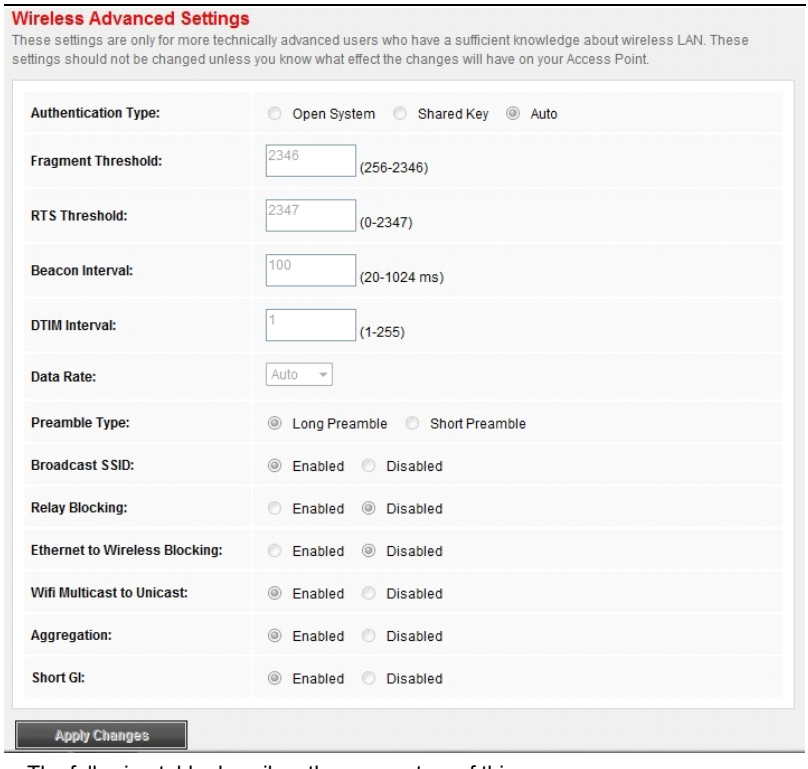
Choose **Deny Listed** as the access control mode to to enable black list function. The devices whose MAC addresses are listed in the **Current Access Control List** are denied to access the modem.

3.4.3.5 Advanced

Choose **Wireless** > **Advanced**, and the following page appears. In this page, you can configure the wireless advanced parameters. It is recommended to use the default parameters.

Note:

The parameters in the **Advanced** are modified by the professional personnel, it is recommended to keep the default values.



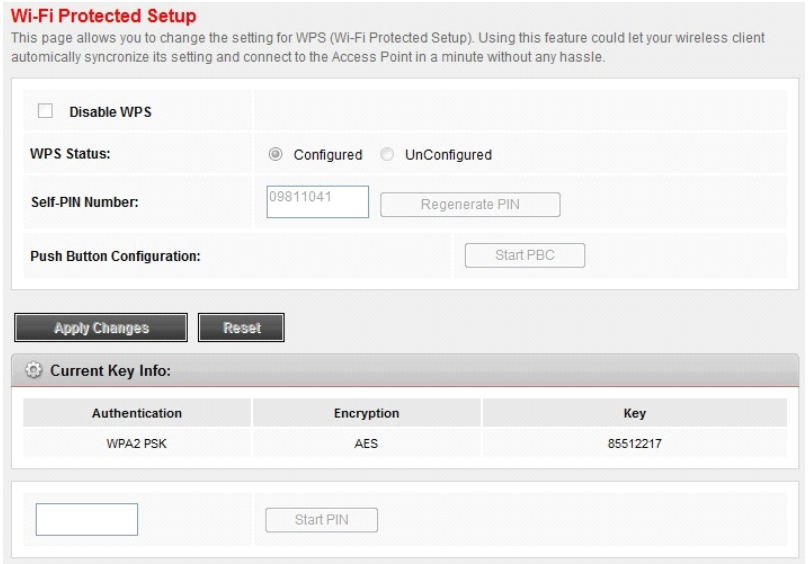
The following table describes the parameters of this page.

Field	Description
Authentication	Select the modem operating in the open system or encryption authentication. You can choose **Open System, Shared Key** or **Auto**. ● In the open system, the wireless client can directly connect to the device ● In the encryption authentication, the wireless client connects to the modem through the shared key.

Field	Description
Data Rate	Choose the transmission rate of the wireless data. You can choose **Auto**, **1 M**, **2 M**, **5.5 M**, **11 M**, **6 M**, **9 M**, **12 M**, **18 M**, **24 M**, **36 M**, **48 M**, **54M, MSC0 ~ MSC7.**
Preamble Type	● **Long Preamble**: It means this card always use long preamble. ● **Short Preamble**: It means this card can support short preamble capability.
Broadcast SSID	Select whether the modem broadcasts SSID or not. You can select **Enable** or **Disable**. ● Select **Enable**, the wireless client searches the modem through broadcasting SSID. ● Select **Disable** to hide SSID, the wireless clients can not find the SSID.
Relay Blocking	Wireless isolation. Select **Enable**, the wireless clients that are connected to the modem can not intercommunication.
Ethernet to Wireless Blocking	Whether the wireless network can communicate with the Ethernet network or not.
Wifi Multicast to Unicast	Enable it to using unicast to transmit multicast packet
Aggregation	It is applied when the destination end of all MPDU are for one STA.
Short GI	It is not recommended to enable GI in obvious environment of Multi-path effect.
Apply Changes	Click it to apply the settings temporarily. If you want to save the settings of this page permanently, click **Save** in the lower left corner.

3.4.3.6 WPS

Choose **WLAN** > **WPS** and the following page appears.



There are two ways for the wireless client to establish the connection with the modem through WPS. The modem generates PIN, see the above figure. Click **Regenerate PIN** to generate a new PIN, and then click **Start PBC**, In the wireless client tool, enter the PIN which is generated by the modem, start connection. The client will automatically establish the connection with the modem through the encryption mode, and you need not to enter the key. The other way is the wireless client generates PIN. In the above figure, enter PIN of the wireless client in the **Client PIN Number** field, then click **Start PIN** to establish the connection.

Note:

The wireless client establishes the connection with the modem through WPS negotiation.The wireless client must support WPS

3.5 Advanced

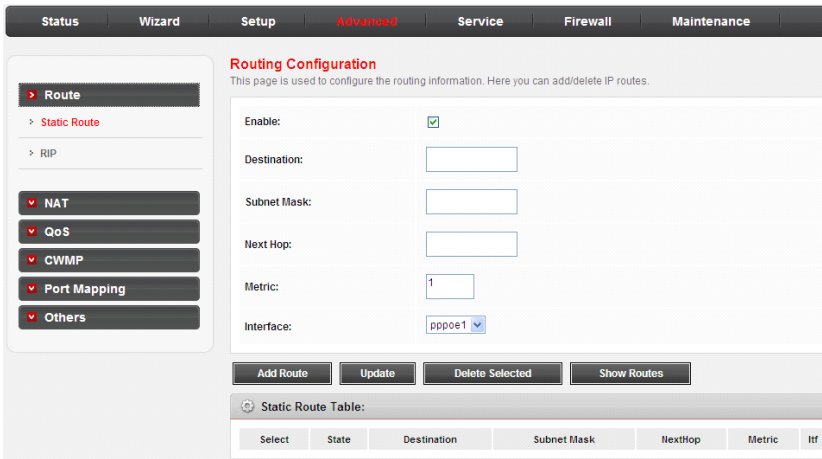
In the navigation bar, click **Advanced**. The tab **Advanced** contains **Route**, **NAT**, **QoS**, **CWMP**, **Port Mapping** and **Others**.

3.5.1 Route

Choose **Advanced** > **Route**, the page shown in the following figure appears. The page that is displayed contains **Static Route**, **RIP.**

3.5.1.1 Static Route

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



The following table describes the parameters and buttons of this page.

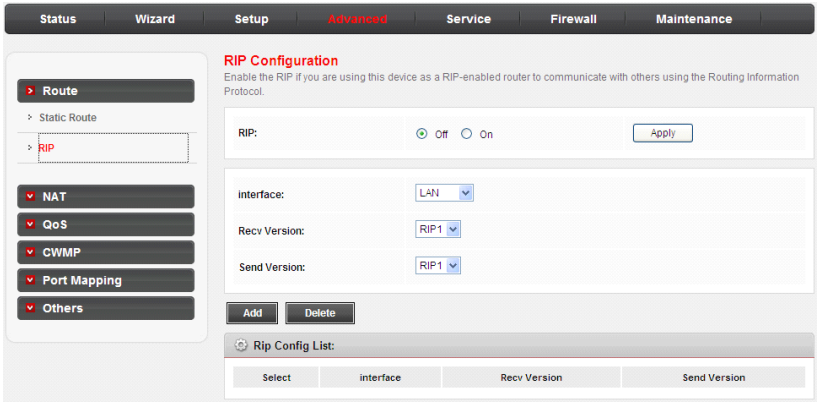
Field	Description
Enable	Select it to use static IP routes.

Field	Description
Destination	Enter the IP address of the destination device.
Subnet Mask	Enter the subnet mask of the destination device.
Next Hop	Enter the IP address of the next hop in the IP route to the destination device.
Metric	The metric cost for the destination.
Interface	The interface for the specified route.
Add Route	Click it to add the new static route to the **Static Route Table**.
Update	Select a row in the **Static Route Table** and modify the parameters. Then click it to save the settings temporarily.
Delete Selected	Select a row in the **Static Route Table** and click it to delete the row.
Show Routes	Click it, the **IP Route Table** appears. You can view a list of destination routes commonly accessed by your network.
Static Route Table	A list of the previously configured static IP routes.

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

3.5.1.2 RIP

Click **RIP** in the left pane, the page shown in the following figure appears. If you are using this device as a RIP-enabled router to communicate with others using Routing Information Protocol (RIP), enable RIP. This page is used to select the interfaces on your devices that use RIP, and the version of the protocol used.



The following table describes the parameters and buttons of this page.

Field	Description
RIP	Select **On**, the router communicates with other RIP-enabled devices.
Apply	Click it to save the settings of 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** indicates the router receives RIP v1 messages. ● Choose **RIP2** indicates the router receives RIP v2 messages. ● Choose **Both** indicates 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** indicates the router broadcasts RIP1 messages only. ● Choose **RIP2** indicates the router multicasts

Field	Description
	RIP2 messages only.
Add	Click it to add the RIP interface to the **Rip Configuration List**.
Delete	Select a row in the **Rip Configuration List** and click it to delete the row.

3.5.2 NAT

3.5.2.1 DMZ

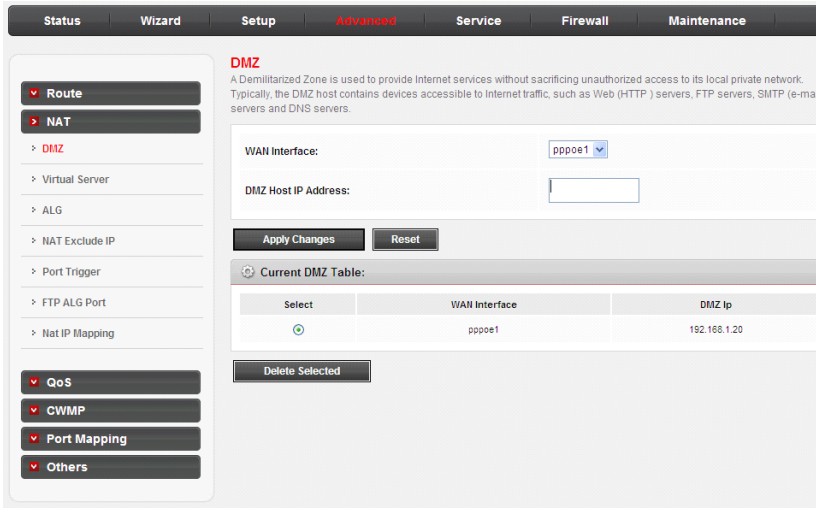
Demilitarized Zone (DMZ) is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

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

Step 1 Select **WAN Interface**.

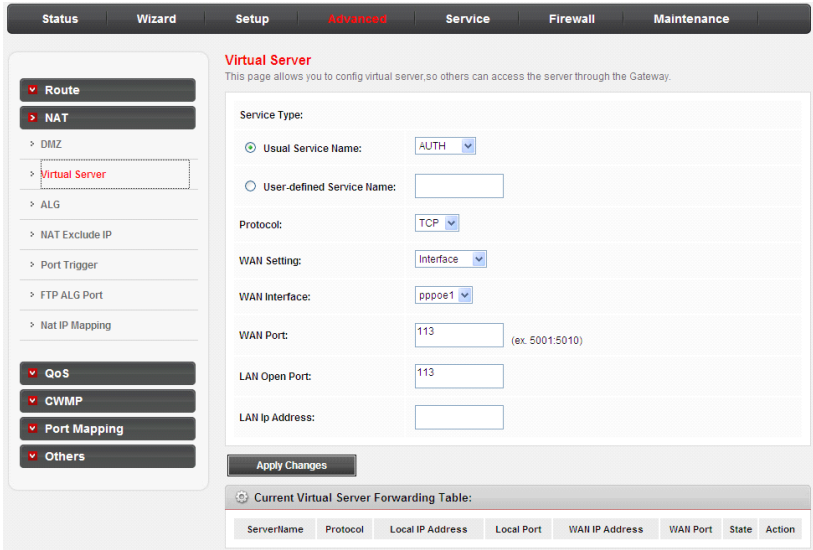
Step 4 Enter an IP address of the DMZ host.

Step 5 Click **Apply Changes** to save the settings of this page temporarily.



3.5.2.2 Virtual Server

Click **Virtual Server** in the left pane, the page shown in the following figure appears.



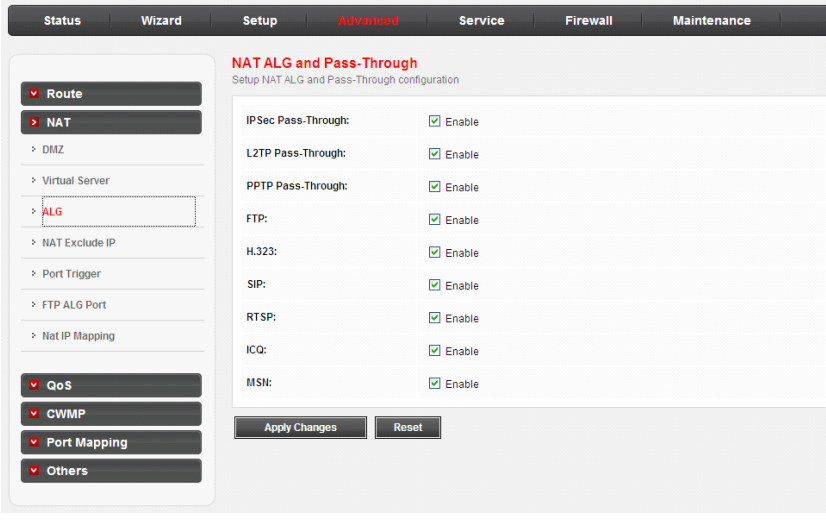
The following table describes the parameters of this page.

Field	Description
Service Type	You can select the common service type, for example, **AUTH**, **DNS**,**FTP** or **POP3**. 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.

Field	Description
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.

3.5.2.3 ALG

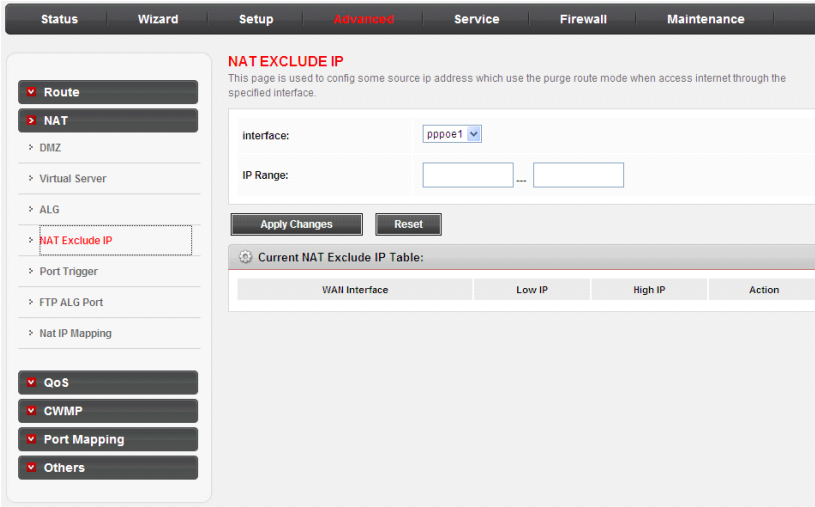
Click **ALG** in the left pane, the page shown in the following figure appears. Choose the NAT ALG and Pass-Through options, and then click **Apply Changes**.



3.5.2.4 NAT Exclude IP

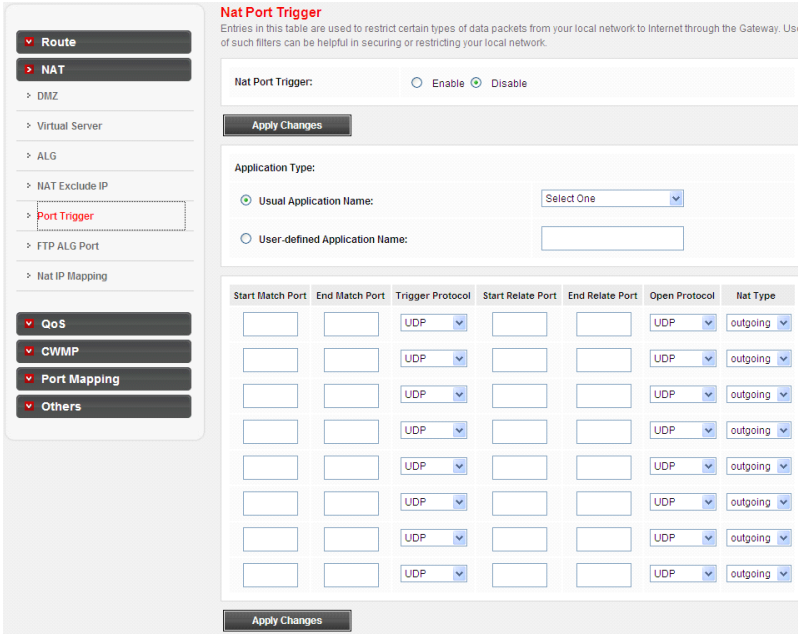
Click **NAT Exclude IP** in the left pane, the page shown in the following figure appears.

In the page, you can configure some source IP addresses which use the purge route mode when accessing internet through the specified interface.



3.5.2.5 Port Trigger

Click **Port Trigger** in the left pane, the page shown in the following figure appears.



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.

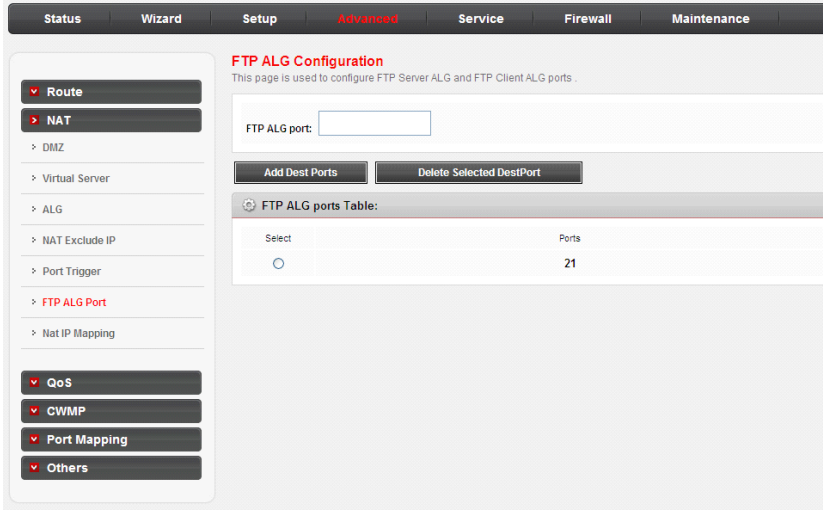
If the application you want to setup isn't listed, click the **User-defined Application Name** radio button and type in a name for the trigger in the Custom application field. Configure the **Start Match Port**, **End Match Port**, **Trigger Protocol**, **Start Relate Port**, **End Relate Port, Open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

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

3.5.2.6 FTP ALG PORT

Click **FTP ALG PORT** in the left pane, the page shown in the following figure appears.

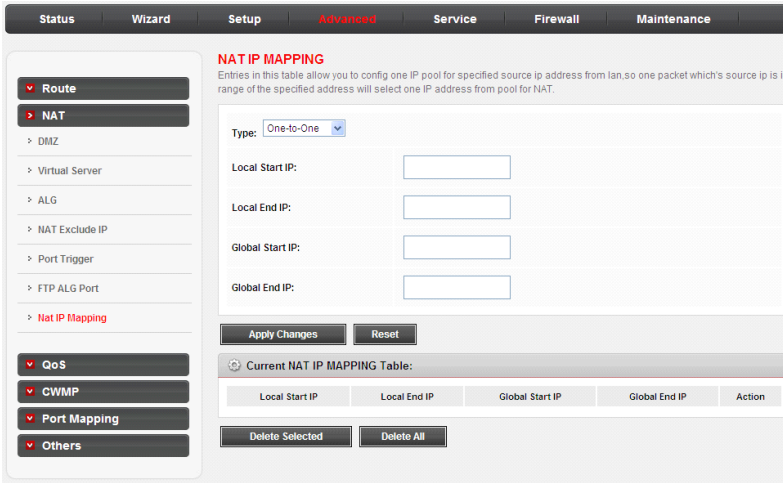
This page is used to configure FTP Server ALG and FTP Client ALG ports .



3.5.2.7 Nat IP Mapping

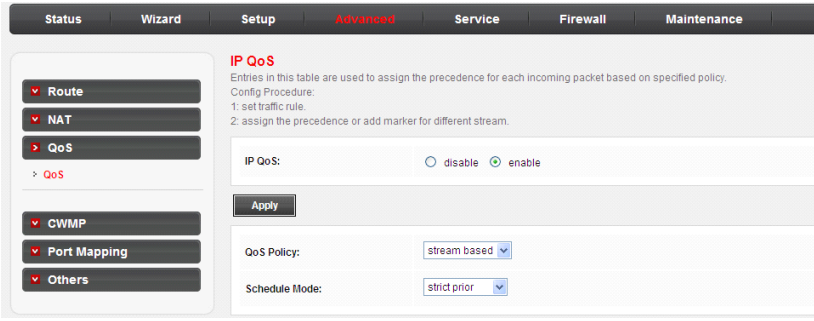
Click **Nat IP Mapping** in the left pane, the page shown in the following figure appears.

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.



3.5.3 QoS

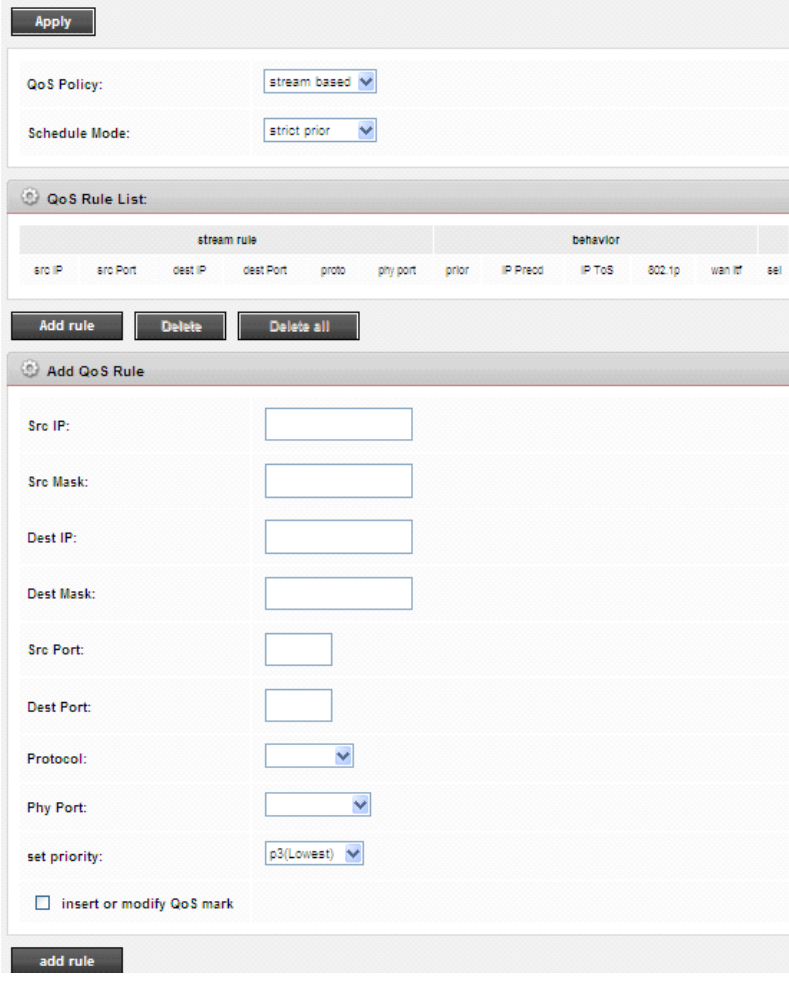
Choose **Advanced** > **QoS**, the page shown in the following figure appears. Entries in the **QoS Rule List** are used to assign the precedence for each incoming packet based on physical LAN port, TCP/UDP port number, source IP address, destination IP address and other information.



Step 1 Enable IP QoS and click **Apply** to enable IP QoS function.

Step 6 Click **add rule** to add a new IP QoS rule.

The page shown in the following figure appears.


IP QoS:
disable
enable
Apply
QoS Policy:
stream based
Schedule Mode:
strict prior
QoS Rule List:
stream rule
behavior
src IP
src Port
dest IP
dest Port
proto
phy port
prior
IP Precd
IP ToS
802.1p
wan if
sel
Add rule
Delete
Delete all
Add QoS Rule
Src IP:
Src Mask:
Dest IP:
Dest Mask:
Src Port:
Dest Port:
Protocol:
Phy Port:
set priority:
p3(Lowest)
insert or modify QoS mark
add rule

The following table describes the parameters and buttons of this page.

Field	Description
IP QoS	Select to enable or disable IP QoS function. You need to enable IP QoS if you want to configure the parameters of this page.
QoS Policy	You can choose **stream based**, **802.1p based** or **DSCP based**.
Schedule Mode	You can choose **strict prior** or **WFQ (4:3:2:1)**.
Source IP	The IP address of the source data packet.
Source Mask	The subnet mask of the source IP address.
Destination IP	The IP address of the destination data packet.
Destination Mask	The subnet mask of the destination IP address.
Source Port	The port of the source data packet.
Destination Port	The port of the destination data packet.
Protocol	The protocol responds to the IP QoS rules. You can choose **TCP**, **UDP**, **ICMP** or **TCP/UDP**.
Physical Port	The LAN interface responds to the IP QoS rules.
Set priority	The priority of the IP QoS rules. P0 is the highest priority and P3 is the lowest.
802.1p	You can choose from 0 to 7.
delete	Select a row in the **QoS Rule list** and click it to delete the row.
delete all	Select all the rows in the **QoS Rule list** and click it to delete the rows.

3.5.4 CWMP

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

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

Apply Changes | Reset

Certificate Management:

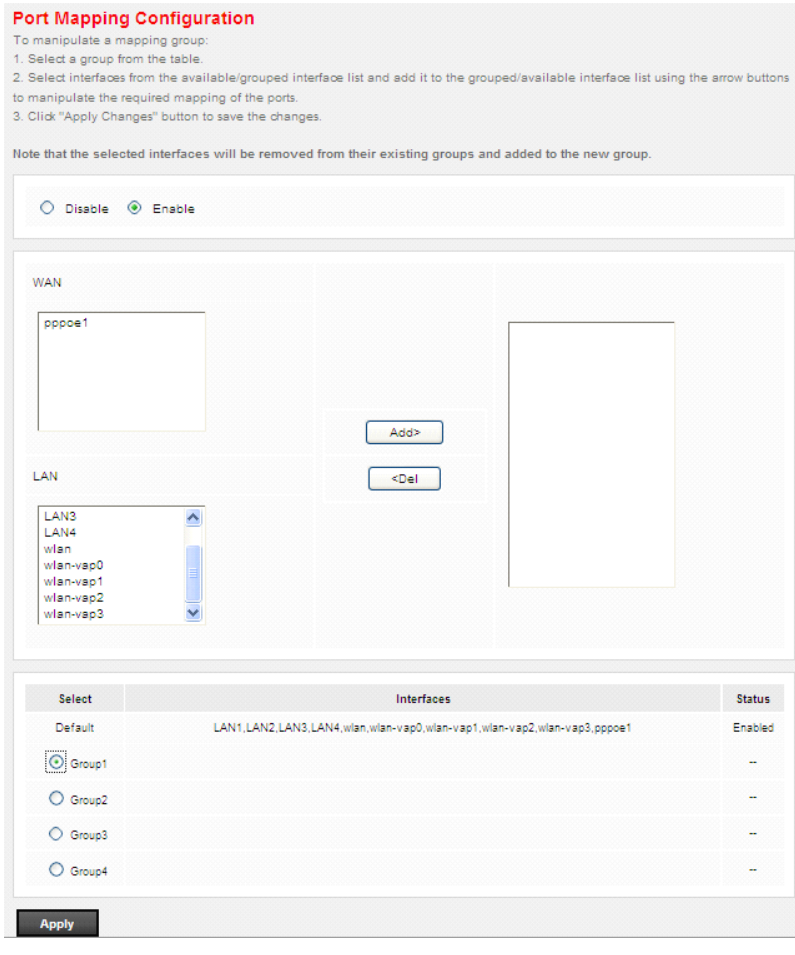
CPE Certificate Password:	client	Apply	Undo	
CPE Certificate:		浏览...	Upload	Delete
CA Certificate:		浏览...	Upload	Delete

The following table describes the parameters of this page:

Field	Description
ACS	
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.

3.5.5 Port Mapping

Choose **Advanced** > **Port Mapping**, the page shown in the following page appears.



Create four rules through Group1 to Group4. The procedure is as follows:

Step 1 Select **Enable** to enable port mapping.

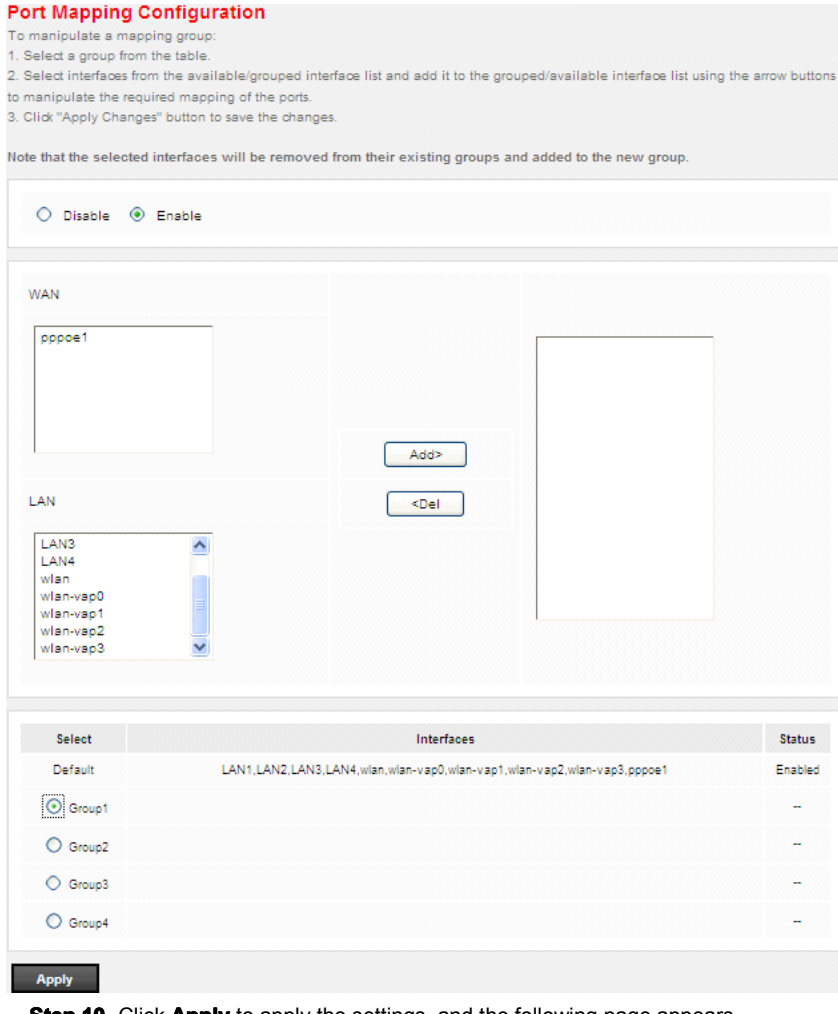
Step 7 Select Group1. Then the interfaces are added in the WAN and LAN table.

The following page appears.

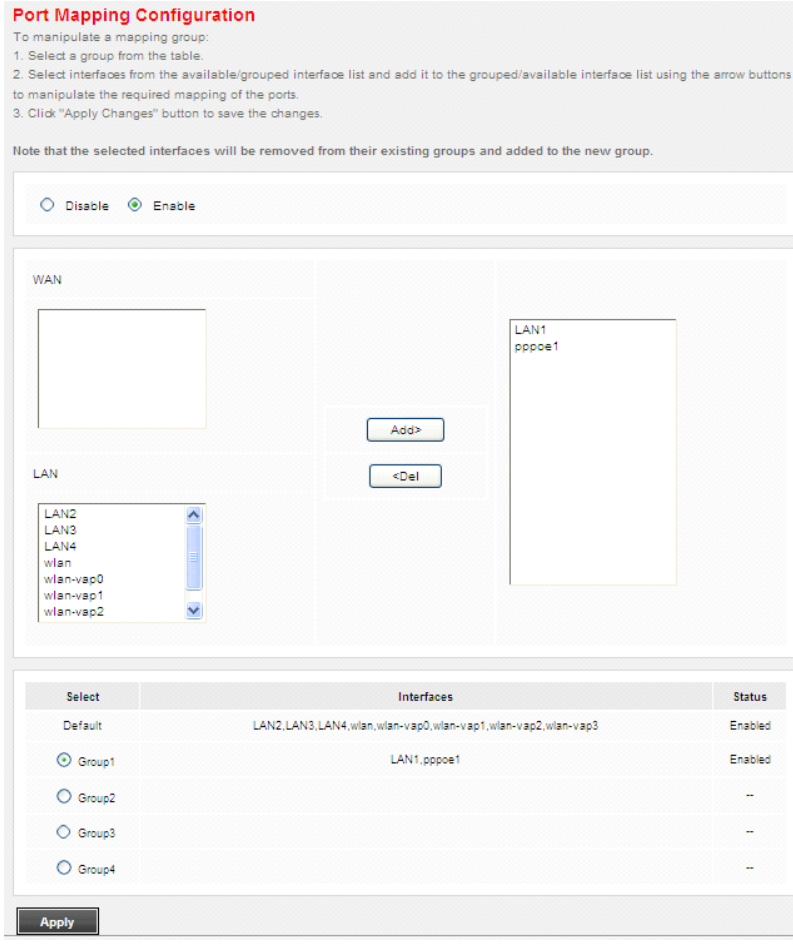
Step 8 Select the interfaces that are respectively added to WAN and LAN. Press **Ctrl** while selecting multiple interfaces.

Step 9 Click **Add** to add the interface to the rule.

The following page appears.



Step 10 Click **Apply** to apply the settings, and the following page appears.



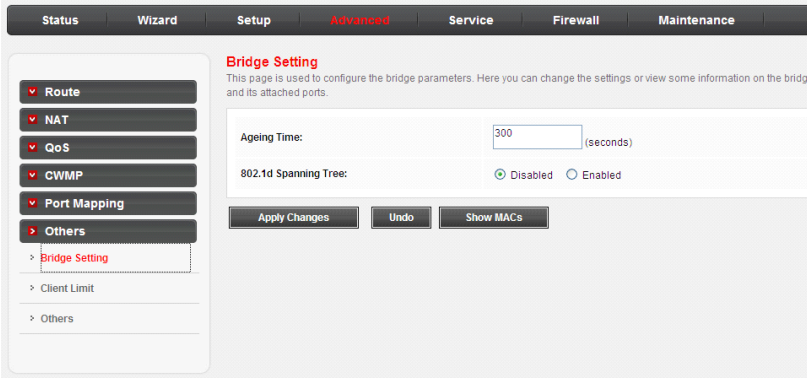
In this example, only interfaces of pppoe1 and LAN1 can communicate with each other. That is, only LAN1 can access the Internet through pppoe1 interface.

3.5.6 Others

Choose **Advanced** > **Others**. The page that is displayed contains **Bridge Setting**, **Client Limit**, **Tunnel** and **Others**.

3.5.6.1 Bridge Setting

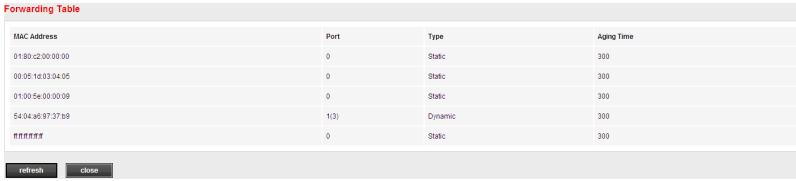
Choose **Bridge Setting** in the left pane, the page shown in the following figure appears. This page is used to configure the bridge parameters. You can change the settings or view some information on the bridge and its attached ports.



The following table describes the parameters and button of this page:

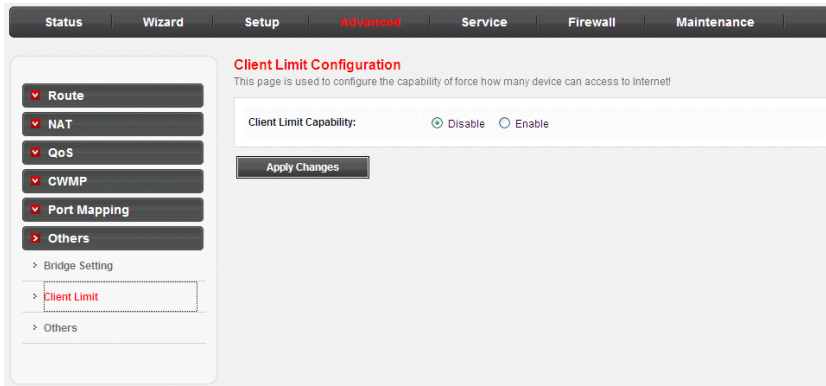
Field	Description
Ageing Time	If the host is idle for 300 seconds (default value), its entry is deleted from the bridge table.
Show MACs	Click it to show a list of the learned MAC addresses for the bridge.

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



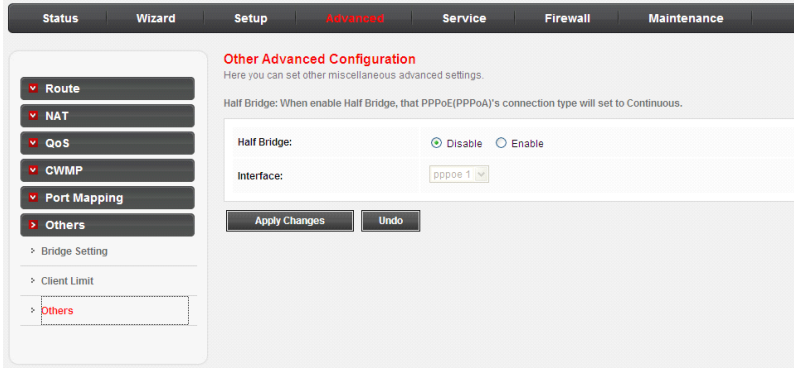
3.5.6.2 Client Limit

Choose **Client Limit** in the left pane, the page shown in the following figure appears. This page is used to configure the capability of forcing how many devices can access to the Internet.



3.5.6.3 Others

Choose **Others** in the left pane, the page shown in the following figure appears.



3.6 Service

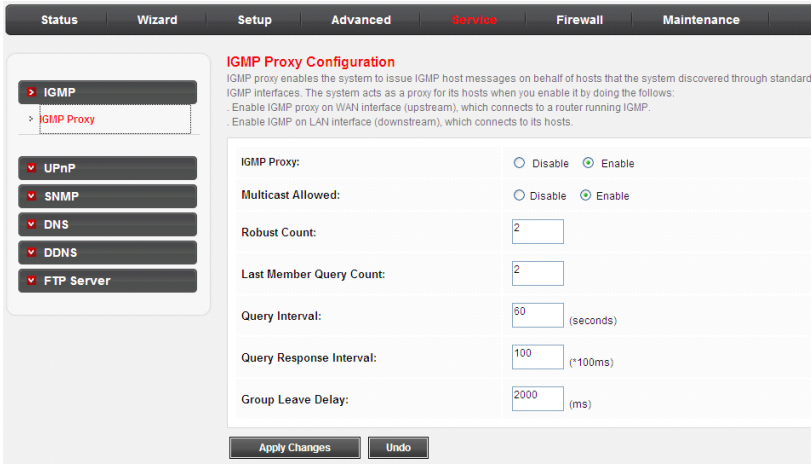
In the navigation bar, click **Service**. The tab **Service** contains **IGMP**, **UPnP**, **SNMP**, **DNS** and **DDNS.**

3.6.1 IGMP

Choose **Service** > **IGMP**, and the following page appears. The page that is displayed contains **IGMP Proxy**.

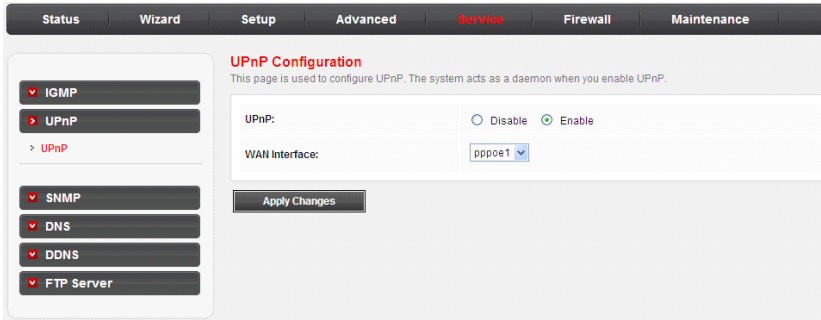
3.6.1.1 IGMP Proxy

Click **IGMP Proxy** in the left pane, the page shown in the following figure appears. In this page, you can enable or disable IGMP proxy. If you disable IGMP proxy, the modem will discard all the received multicast data packets.



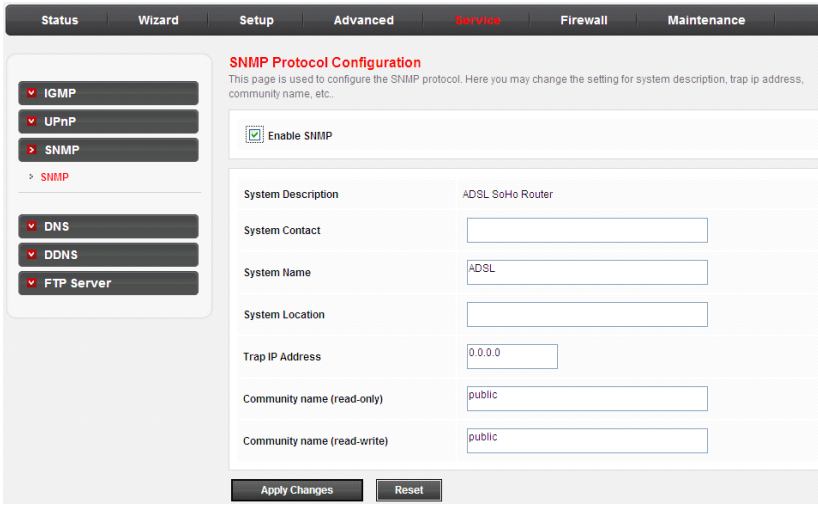
3.6.2 UPnP

Click **UPnP** in the left pane, the page shown in the following figure appears. The system acts as a daemon after you enable UPnP.



3.6.3 SNMP

Click **SNMP** in the left pane, the page shown in the following figure appears. You can configure the SNMP 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.
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.

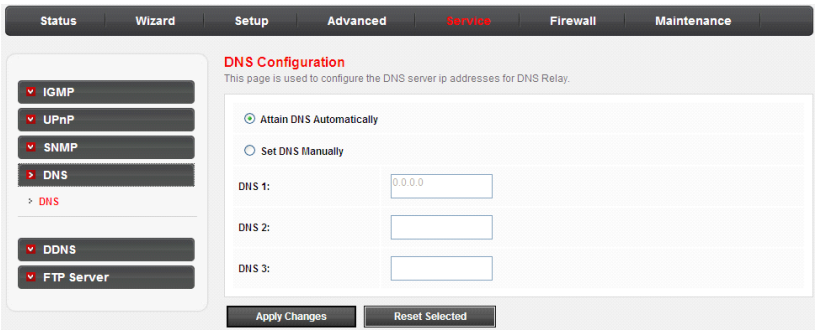
3.6.4 DNS

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**.

3.6.4.1 DNS

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



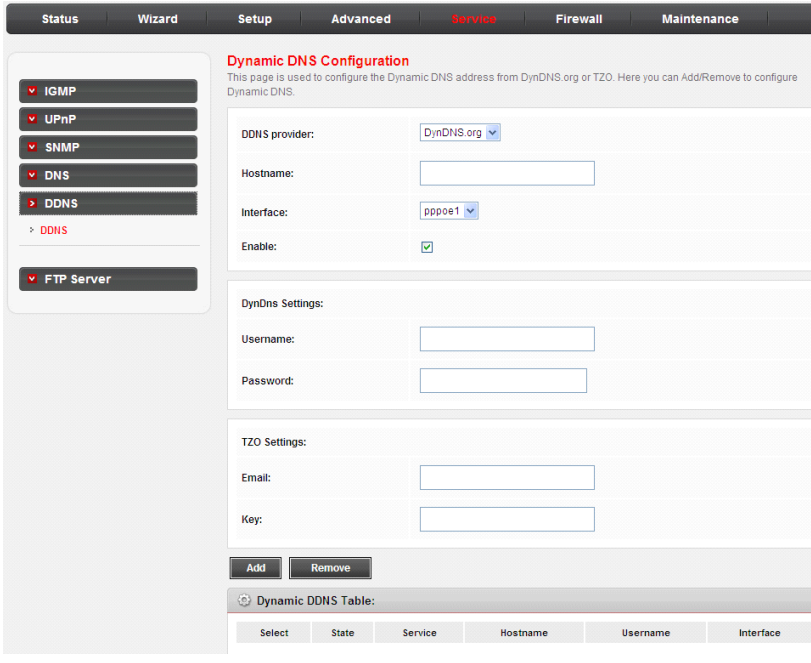
The following table describes the parameters and buttons of this page.

Field	Description
Attain DNS Automatically	Select it, 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, enter the IP addresses of the primary and secondary DNS server.
Apply Changes	Click it to save the settings of this page.

Field	Description
Reset Selected	Click it to start configuring the parameters in this page.

3.6.5 DDNS

Choose **Service** > **DDNS**, the page shown in the following figure appears. This page is used to configure the dynamic DNS address from DynDNS.org or TZO. You can add or remove to configure dynamic DNS.



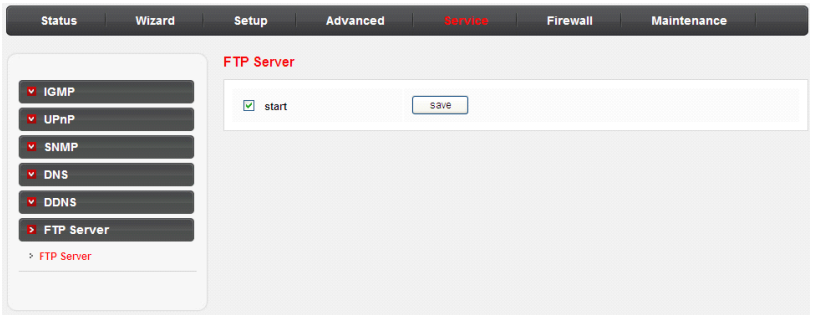
The following table describes the parameters of this page.

Field	Description
DDNS provider	Choose the DDNS provider name. You can choose **DynDNS.org** or **TZO**.

Field	Description
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.

3.6.6 FTP Server

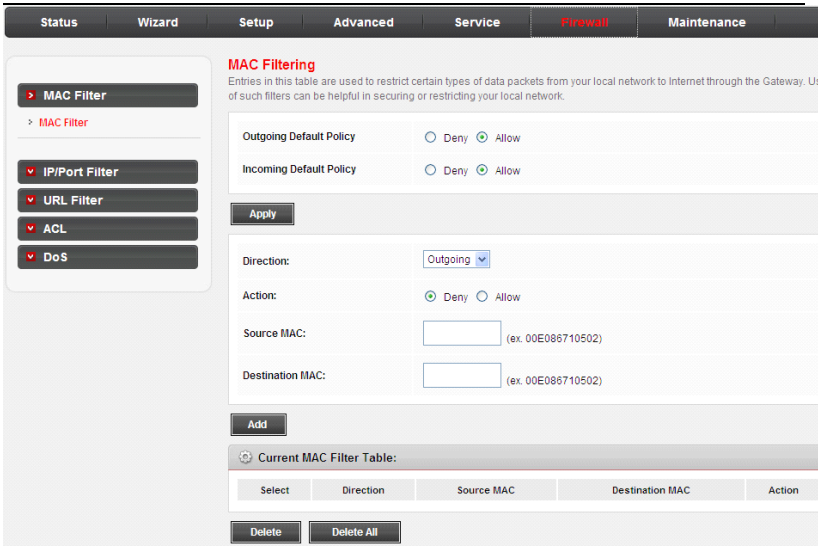
Choose **Service** > **FTP Server**, the page shown in the following figure appears. This page is used to start the FTP Server.



3.7 Firewall

3.7.1 MAC Filter

Click **MAC Filter** in the left pane, 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.

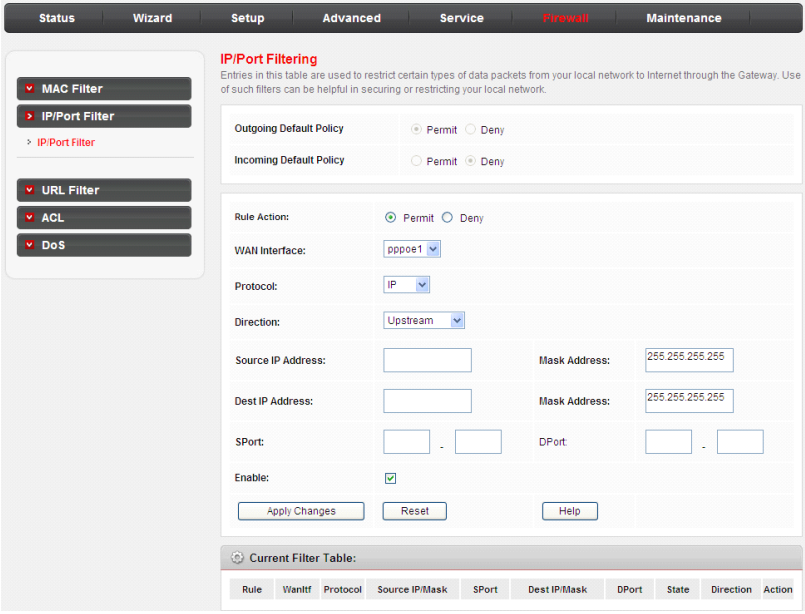


3.7.2 IP/Port Filter

Choose **Firewall** > **IP/Port Filter**, the page shown in the following figure appears. The page that is displayed contains **IP/Port Filter**.

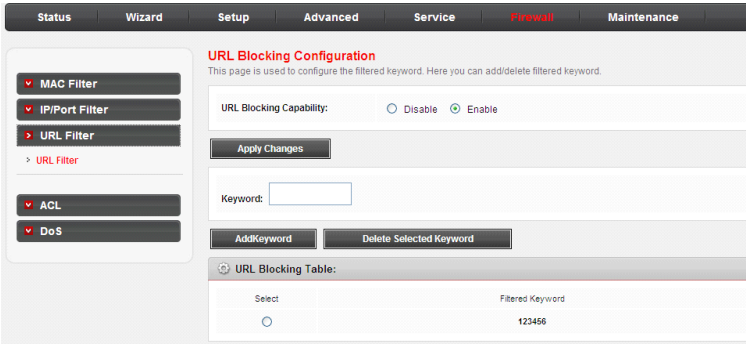
3.7.2.1 IP/Port Filter

Click **IP/Port Filter** in the left pane, 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.



3.7.3 URL Filter

Choose **Firewall** > **URL Filter**, the page shown in the following figure appears. This page is used to configure the filtered keyword. Here you can add/delete filtered keyword



3.7.4 ACL

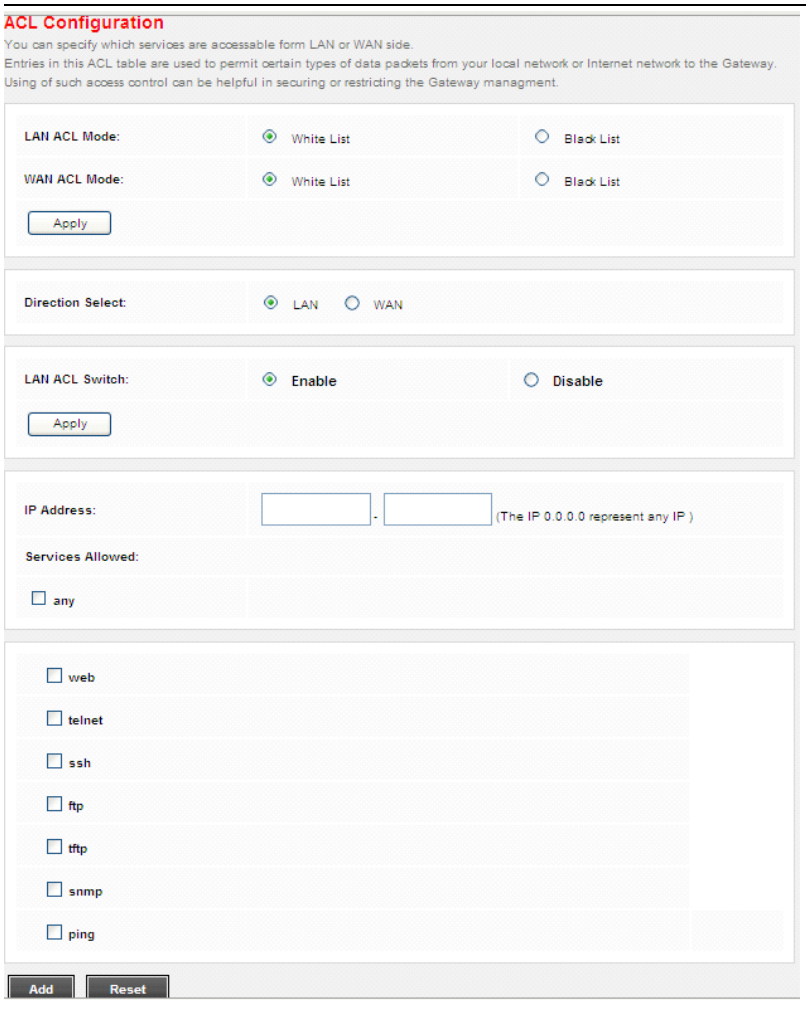
Choose **Firewall** > **ACL**, the page shown in the following figure appears. The page that is displayed contains **ACL.**

3.7.4.1 ACL

Click **ACL** in the left pane, the page shown in the following figure appears. In 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:

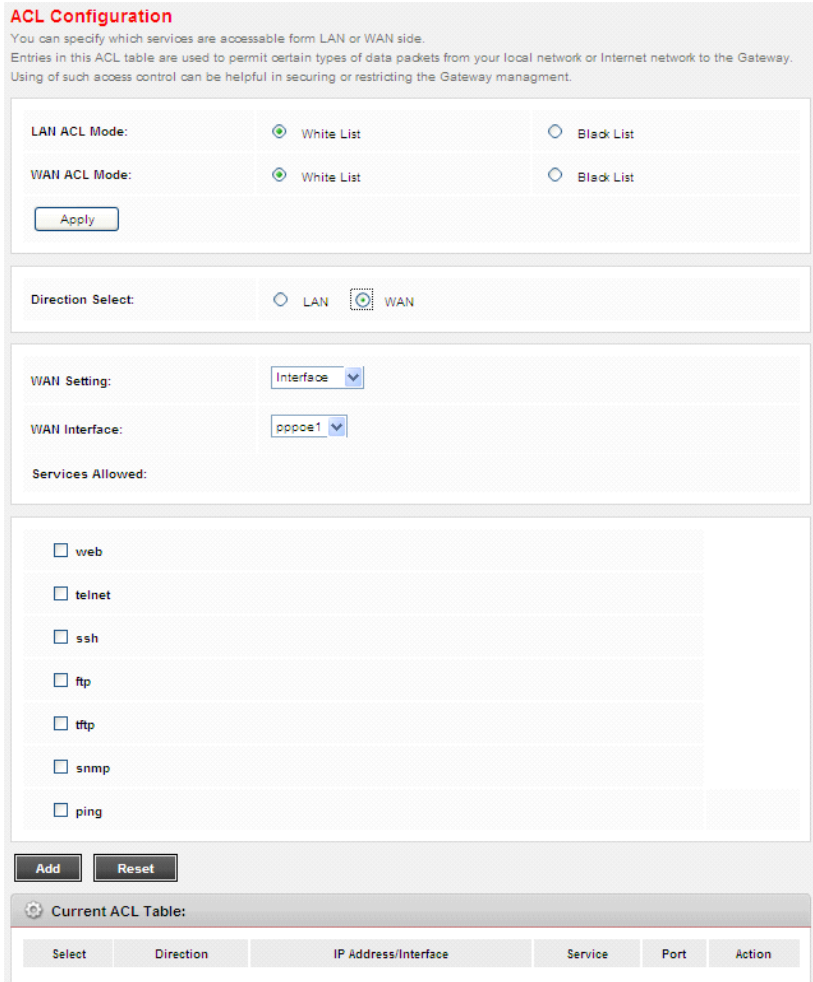
If you select **Enable** in ACL capability, ensure that your host IP address is in ACL list before it takes effect.



The following table describes the parameters and buttons of this page.

Field	Description
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**, **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**.
Reset	Click it to refresh this page.

Set direction of the data packets to **WAN**, the page shown in the following figure appears.



The following table describes the parameters and buttons of this page.

Field	Description
Direction Select	Select the router interface. You can select **LAN** or **WAN**. In this example, **WAN** is selected.
WAN Setting	You can choose **Interface** or **IP Address**.
WAN Interface	Choose the interface that permits data packets from WAN to access the router.
IP Address	Enter the IP address on the WAN. Only the IP address that is in the same network segment with the IP address on the WAN can access the router.
Services Allowed	You can choose the following services from WAN: **Web**, **Telnet**, **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**.
Reset	Click it to refresh this page.

3.7.5 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. Choose **Firewall** > **DoS**, the page shown in the following figure appears. In this page, you can prevent DoS attacks.

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
TCP/UDP PortScan	Low	Sensitivity
ICMP Smurf		
IP Land		
IP Spoof		
IP TearDrop		
PingOfDeath		
TCP Scan		
TCP SynWithData		
UDP Bomb		
UDP EchoChargen		

Select ALL | Clear ALL

Enable Source IP Blocking 300 Block time (sec)

Apply Changes

3.8 Maintenance

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

3.8.1 Update

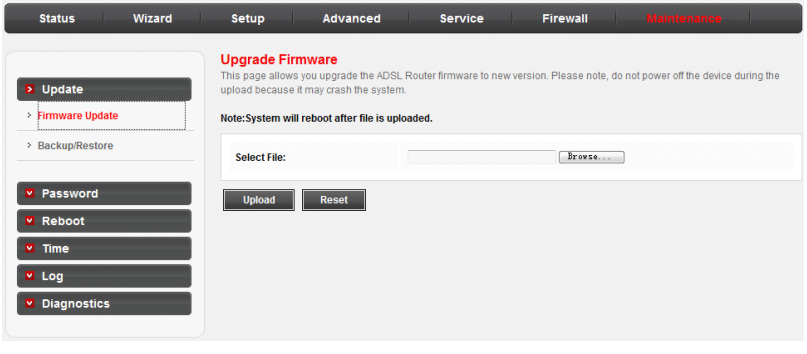
Choose **Maintenance** > **Update**. The **Update** page that is displayed contains **Firmware Update** and **Backup/Restore**.

Caution:

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

3.8.1.1 Firmware Update

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

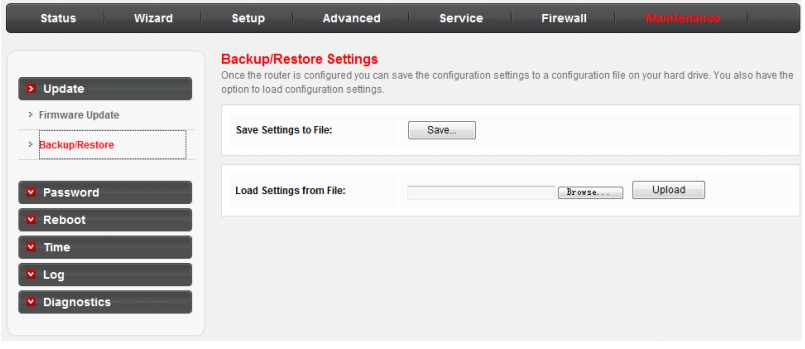


The following table describes the parameters and button of this page.

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

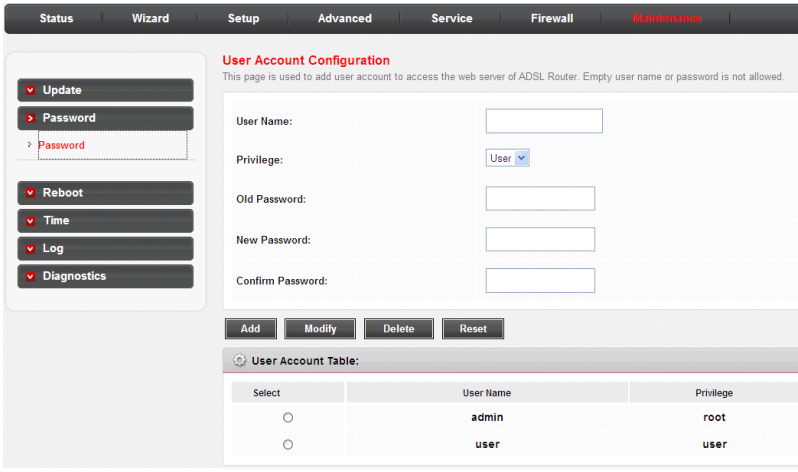
3.8.1.2 Backup/Restore

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



3.8.2 Password

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

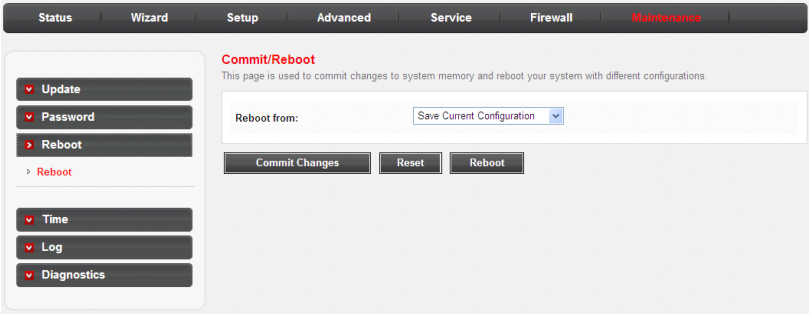


The following table describes the parameters of this page.

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 the password to which you want to change the old password.
Confirm Password	Enter the new password again.

3.8.3 Reboot

Choose **Maintenance** > **Reboot**, 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.

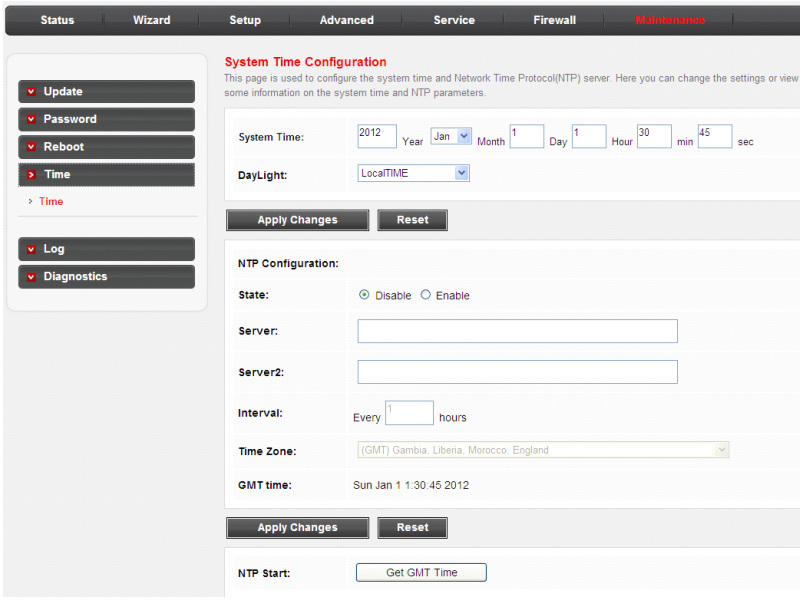


The following table describes the parameters and button of this page.

Field	Description
Reboot from	You can choose **Save Current Configuration** or **Factory Default Configuration**. Click **Reboot** to reboot the router. ● **Save Current Configuration**: Save the current settings, and then reboot the router. ● **Factory Default Configuration**: Reset to the factory default settings, and then reboot the the router.

3.8.4 Time

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

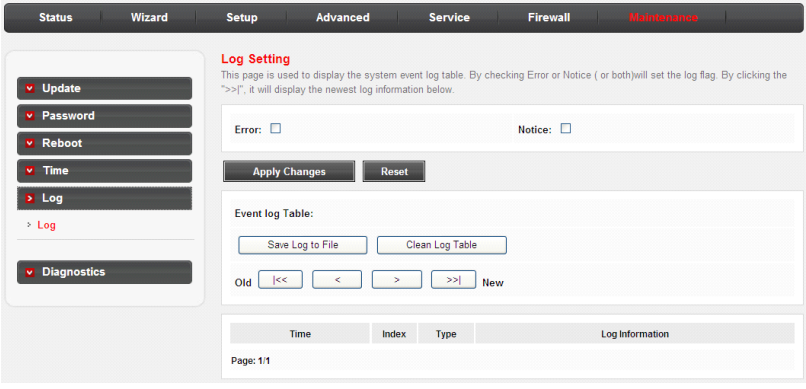


The following table describes the parameters of this page.

Field	Description
System Time	Set the system time manually.
NTP Configuration	
State	Select enable or disable NTP function. You need to enable NTP if you want to configure the parameters of NTP.
Server	Set the primary NTP server manually.
Server2	Set the secondary NTP server manually.
Time Zone	Choose the time zone in which area you are from the drop down list.

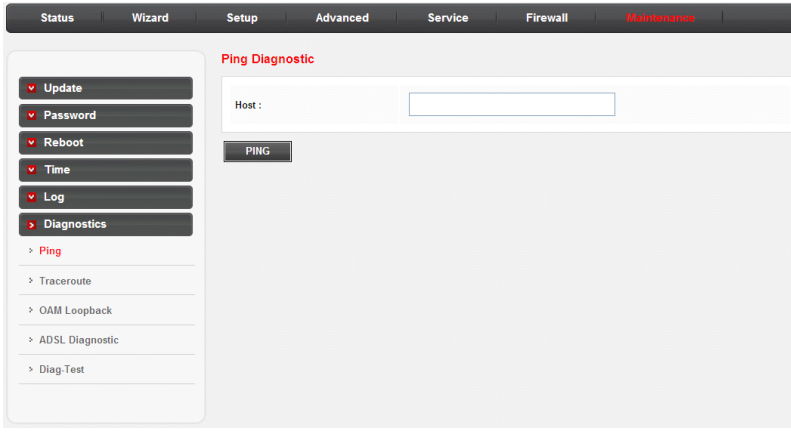
3.8.5 Log

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



3.8.6 Diagnostics

Choose **Maintenance** > **Diagnostics**, the page shown in the following page appears. The page that is displayed contains **Ping**, **Tracert**, **OAM Loopback**, **ADSL Diagnostic** and **Diag-test**. Select the option that you want to run diagnostics.


Status
Wizard
Setup
Advanced
Service
Firewall
Maintenance
Update
Password
Reboot
Time
Log
Diagnostics
Ping
Traceroute
OAM Loopback
ADSL Diagnostic
Diag-Test
Ping Diagnostic
Host :
PING

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 **DSL** indicator not on?	Check the connection between the **DSL** interface of the device and the socket.
Why does the Internet access fail when the **DSL** 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 configuration: ● The type of the network cable ● 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 3 seconds. Then, 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

Question	Answer
	● Subnet mask: 255.255.255.0. ● The user name and password of super user are **admin** and **admin** respectively. ● The user name and password of common user are **user** and **user** respectively.