User Guide

300Mbps Wireless N ADSL2+ Modem Router

TD-W8961N

1910012832
REV 4.0.0

CONTENTS

About This Guide 1

Chapter 1 Introduction 2

1.1 Product Overview 2

1.2 Product Appearance 2

1.2.1 The Front Panel 2

1.2.2 The Back Panel 3

Chapter 2 Hardware Installation 5

2.1 Positioning the Modem Router 5

2.2 Connecting the Modem Router 6

Chapter 3 Quick Start 8

Chapter 4 Software Configuration 12

4.1 Status 12

4.1.1 Device Info 12

4.1.2 System Log 13

4.1.3 Statistics 14

4.2 Interface Setup 17

4.2.1 Internet 17

4.2.2 LAN 23

4.2.3 Wireless 28

4.2.4 6RD 38

4.2.5 Guest Network 39

4.3 Advanced Setup 40

4.3.1 Firewall 40

4.3.2 Routing 41

4.3.3 NAT 42

4.3.4 QoS 46

4.3.5 VLAN 48

4.3.6 ADSL 50

4.4 Access Management 51

4.4.1 ACL 51

4.4.2 Filter 52

4.4.3 SNMP 59

4.4.4 UPnP 59

4.4.5 DDNS 60

4.4.6 CWMP 60
4.5 Maintenance 61
4.5.1 Administration 61
4.5.2 Time Zone 62
4.5.3 Firmware 63
4.5.4 SysRestart 65
4.5.5 Diagnostics 66
4.6 Help 66
Appendix A: Configuring the PC 68
Appendix B: Troubleshooting 73

About This Guide

This guide is a complement to Quick Installation Guide. The Quick Installation Guide instructs you on quick Internet setup, and this guide provides details of each function and shows you the way to configure these functions appropriate to your needs.

Note that features available in the router may vary by model and software version. Router availability may also vary by region or ISP. All images, steps, and descriptions in this guide are only examples and may not reflect your actual Router experience.

Conventions

In this guide, the following conventions are used:

Convention	Description
Teal Underlined	Hyperlinks are teal underlined. You can click to redirect to a website or a specific section.
Teal	Contents to be emphasized and texts on the web page are in teal, including the menus, items, buttons, etc.
→	The menu structures to show the path to load the corresponding page. For example, Access Management → Filter means the Filtering function page is under the Access Management menu.
☞ Note	Ignoring this type of note might result in a malfunction or damage to the device.

More Info

The latest software, management app and utility can be found at the Download Center page at https://www.tp-link.com/support.

The Quick Installation Guide can be found where you find this guide or inside the package of the router.

Specifications can be found on the product page at https://www.tp-link.com.

TP-Link Community is provided for you to discuss our products and share knowledge at https://community.tp-link.com.

Our Technical Support contact information can be found at Contact Technical Support page at www.tp-link.com/support.

Chapter 1 Introduction

1.1 Product Overview

TP-Link's Modem Router is a combined wired/wireless network connection device with integrated wireless router and DSL modem, reducing hassle of configuration and saving space.

With ADSL and WAN, the modem router is compatible with ADSL connections and fiber/cable access.

With Ethernet ports and antennas, the modem router provides wired and wireless access for multiple computers and mobile devices.

With various features and functions, the modem router is the perfect hub of your home or business network.

1.2 Product Appearance

1.2.1 The Front Panel

The modem router's LEDs are located on the front panel (View from left to right).

LED Explanation:

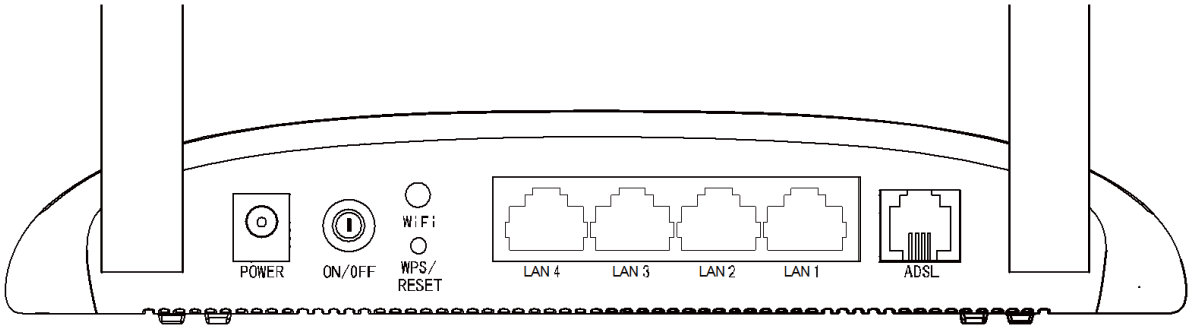
Name	Status	Indication
(Power)	On	System initialization completes.
	Flash	System initializing or firmware upgrading is in process. Do not disconnect or power off the modem router.
	Off	Power is off.
(ADSL)	On	ADSL synchronization is established.
	Flash	ADSL synchronization is in progress.
	Off	ADSL synchronization fails. Please refer to Note 1 for troubleshooting.
(Internet)	On	Internet connection is available.
	Flash	There is data being transmitted or received via the Internet.
	Off	No successful Internet connection is available or the modem router is operating in Bridge mode. Please refer to Note 2 for

Name	Status	Indication
		troubleshooting.
(Wireless)	On	The wireless function is enabled.
	Flash	The modem router is sending or receiving data over the wireless network.
	Off	The wireless function is disabled.
(WPS)	On	A wireless device has been successfully added to the network by WPS function.
	Flash	A wireless device is trying to connect to the network via WPS. This process may take up to 2 minutes.
	Off	The WPS function is disabled or the wireless device fails to be added to the network in 2 minutes after WPS function is enabled. Please refer to WPS Settings for more information.
(LAN1-4)	On	The corresponding LAN port is connected.
	Flash	The modem router is sending or receiving data over this LAN port.
	Off	The corresponding LAN port is not connected.

☞ Note:

1. If the ADSL LED is off, please check your Internet connection first. Refer to 2.2 Connecting the Modem Router for more information about how to make Internet connection correctly. If you have already made a right connection, please contact your ISP to make sure if your Internet service is available now.
2. If the Internet LED is off, please check your ADSL LED first. If your ADSL LED is also off, please refer to Note 1. If your ADSL LED is on, please check your Internet configuration. You may need to check this part of information with your ISP and make sure everything has been input correctly. Refer to 4.1.1 Device Info and 4.2.1 Internet for more information.

1.2.2 The Back Panel



Item	Description
POWER	For connecting the modem router to power socket via the provided power adapter.
ON/OFF	The switch for the power.
WiFi	The button for the wireless function.
WPS/RESET	The switch for the WPS and Reset function. Please refer to the note below for more information.
LAN 1, LAN 2, LAN 3, LAN 4	Through the port, you can connect the modem router to your PC or the other Ethernet network devices.
ADSL	Through the port, you can connect the modem router with the telephone. Or you can connect them by an external separate splitter. For details, please refer to 2.2 Connecting the Modem Router.
Antennas	Used for wireless operation and data transmit.

☞ Note:

If your client devices, such as wireless adapters, support Wi-Fi Protected Setup, then you can press this button for about two seconds to quickly establish a connection between the router and client devices and automatically configure wireless security for your wireless network. For details, please refer to WPS Settings.

If you press this button for about 8 seconds, you will enable the RESET function. Refer to Appendix B: Troubleshooting about how to reset the modem router to factory defaults.

Chapter 2 Hardware Installation

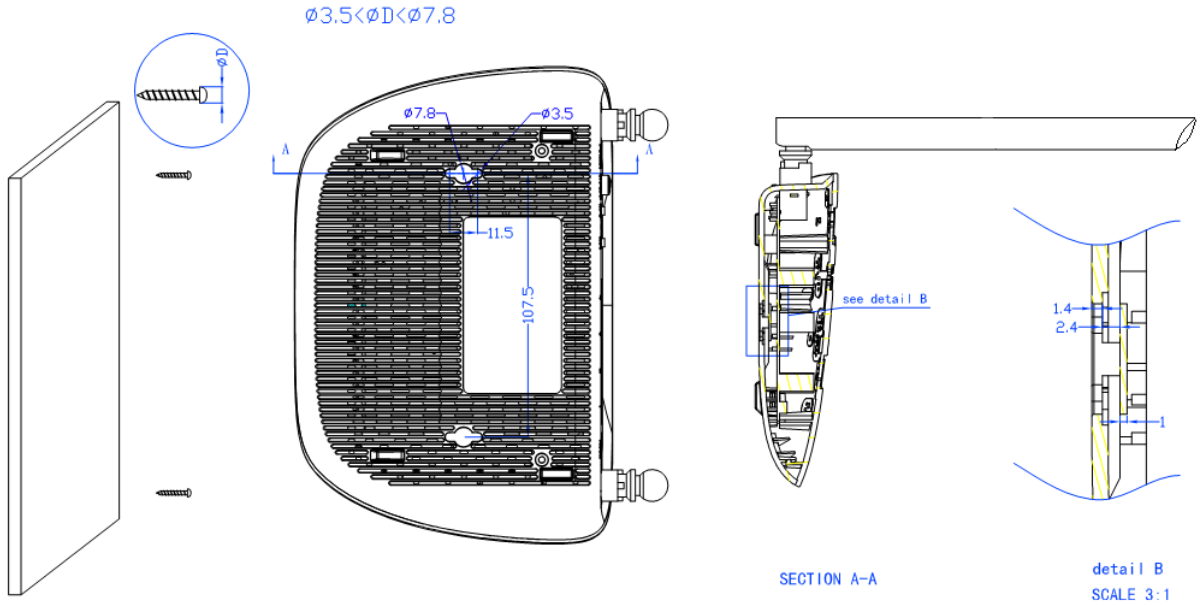
2.1 Positioning the Modem Router

With the modem router, you can access your network from anywhere within the wireless network coverage. However, the wireless signal strength and coverage vary depending on the actual environment of your modem router. Many obstacles may limit the range of the wireless signal, for example, concrete structures or thick walls.

For your security and best Wi-Fi performance, please:

- Do NOT locate the modem router in a place where it will be exposed to moisture or excessive heat.
- Keep away from the strong electromagnetic radiation and the device of electromagnetic sensitive.
- Place the modem router in a location where it can be connected to the various devices as well as to a power source.
- Make sure the cables and power cord are safely placed out of the way to avoid a tripping hazard.

Generally, the modem router is placed on a horizontal surface, such as on a shelf or desktop. The device also can be mounted on the wall as shown in the following figure.

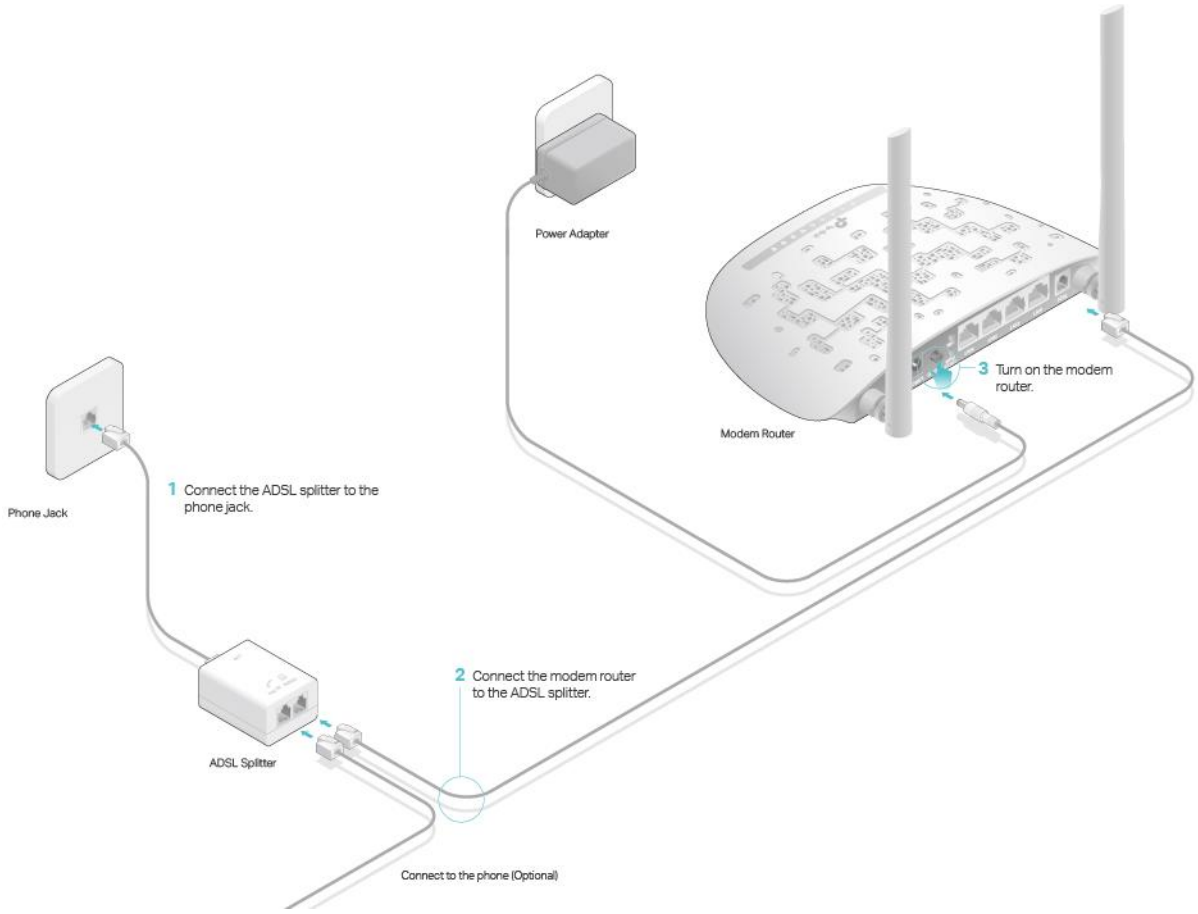


☞ Note:

The diameter of the screw, 3.5mm<D<7.8mm, and the distance of two screws is 107.5mm. The screw that project from the wall need around 4mm based, and the length of the screw need to be at least 20mm to withstand the weight of the product.

2.2 Connecting the Modem Router

Before installing the device, please make sure your broadband service provided by your ISP is available. If there is any problem, please contact your ISP. Before cable connection, cut off the power supply and keep your hands dry. You can follow the steps below to install it.



Step 1: Connect the ADSL Line.

Method One: Directly connect the modem router to the phone jack with the ADSL line.

Method Two: Connect the modem router to the phone jack via a separate splitter. External splitter can divide the data and voice, and then you can access the Internet and make calls at the same time. The external splitter has three ports:

- LINE: Connect to the wall jack
- PHONE: Connect to the phone sets
- MODEM: Connect to the ADSL port of the modem router

Step 2: Connect your computer to the modem router.

Method One: Wired

Connect the computer to a LAN port on your modem router with an Ethernet cable.

Method Two: Wireless

Click the network icon of your computer or go to Wi-Fi Setting of your smart device, then use the default SSID (Wireless Network Name) and Wireless Password printed on the product label of the modem router to join the network.

Method Three: Via the WPS button

Wireless devices that support WPS, including Android phones, tablets, most USB network cards, can be connected to your router through this method. (WPS is not supported by iOS devices.)

☞ Note:

The WPS function cannot be configured if the wireless function of the modem router is disabled. Also, the WPS function will be disabled if your wireless encryption is WEP. Please make sure the wireless function is enabled and is configured with the appropriate encryption before configuring the WPS.

1) Tap the WPS icon on the device's screen.
2) Immediately press the WPS button on your modem router.
3) The WPS LED flashes for about two minutes during the WPS process.
4) When the WPS LED is on, the client device has successfully connected to the modem router.

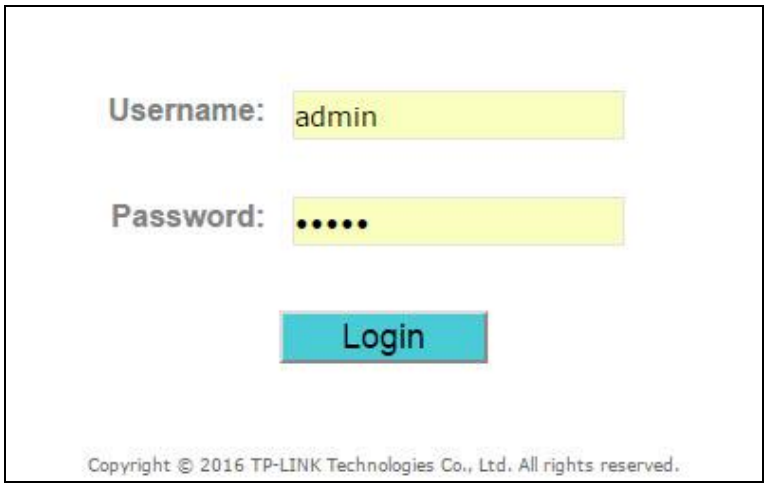
Step 3: Attach the power adapter. The electrical outlet shall be installed near the device and shall be easily accessible.

Chapter 3 Quick Start

This chapter will show you how to configure the basic functions of your modem router using Quick Setup Wizard within minutes.

1. If the TCP/IP Protocol on your computer is set to the static (fixed) IP address, you need to change it to obtain an IP address automatically. Please refer to Appendix A: Configuring the PC for more detailed instruction.
2. Once your host PC is properly configured, launch a web browser and go to http://tplinkmodem.net or 192.168.1.1.

3. Enter the default Username admin and the default Password admin, then click Login or press Enter to access to the Quick Setup.

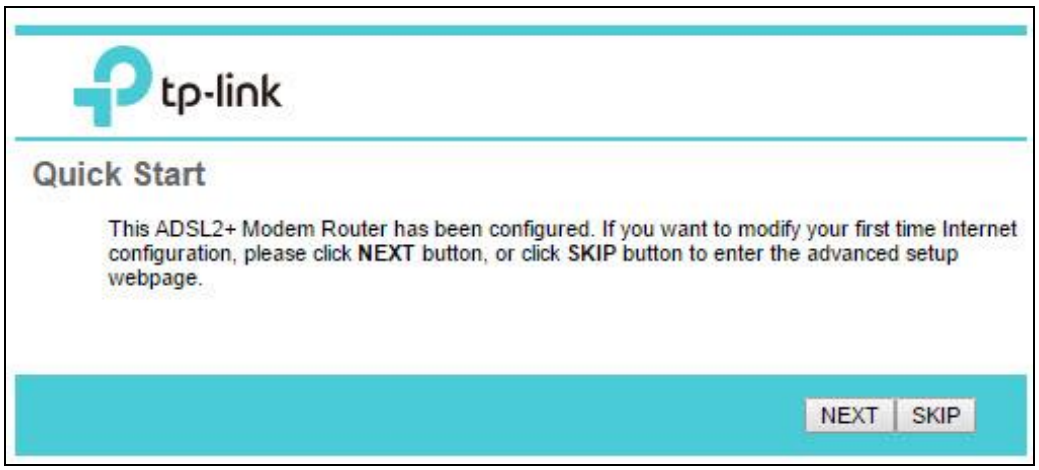


☞ Note:

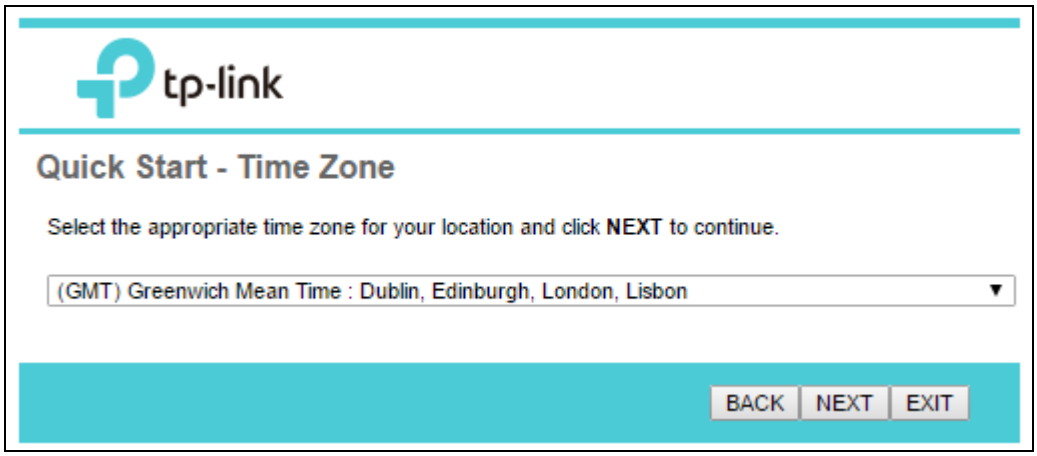
A Quick Setup window will pop up automatically when logging for the first time; otherwise, select Quick Start from the menu and click RUN WIZARD.

4. Follow the steps below to set up your modem router quickly.

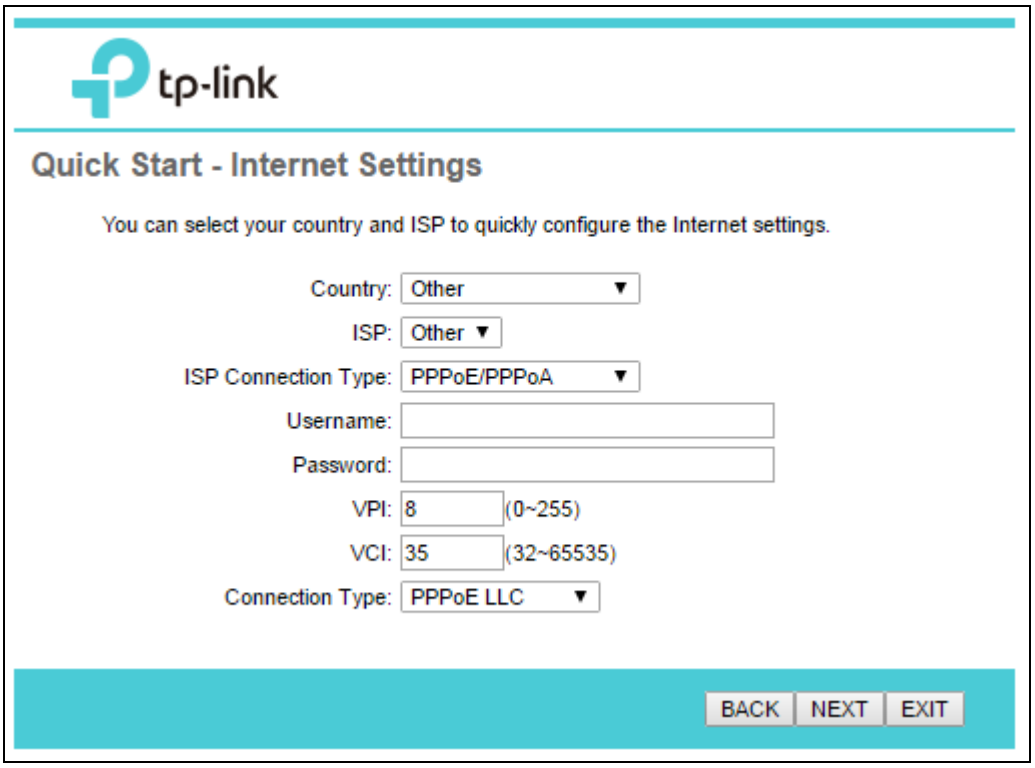
Step 1: Click NEXT to continue.



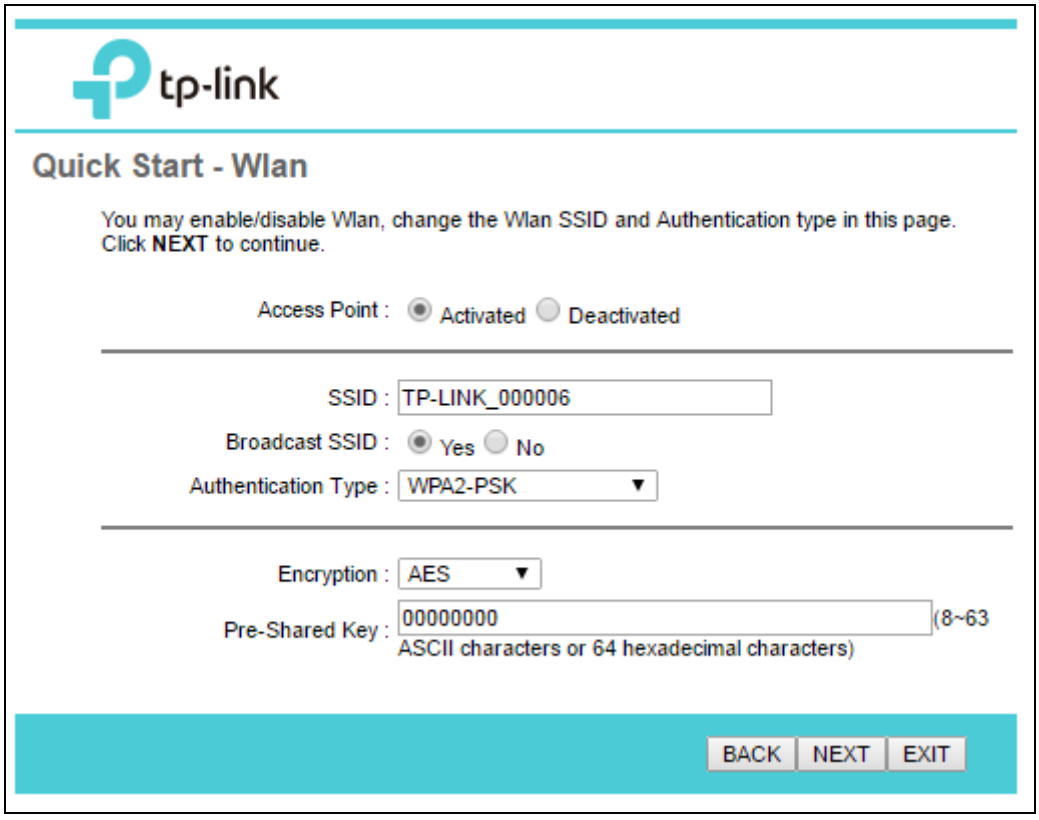
Step 2: Configure the time zone for the modem router, and then click NEXT.



Step 3: Select your country and ISP from the dropdown list. Then select your ISP Connection type and complete the corresponding settings with the information provided by your ISP and click NEXT. Here we take PPPoE/PPPoA mode for example.



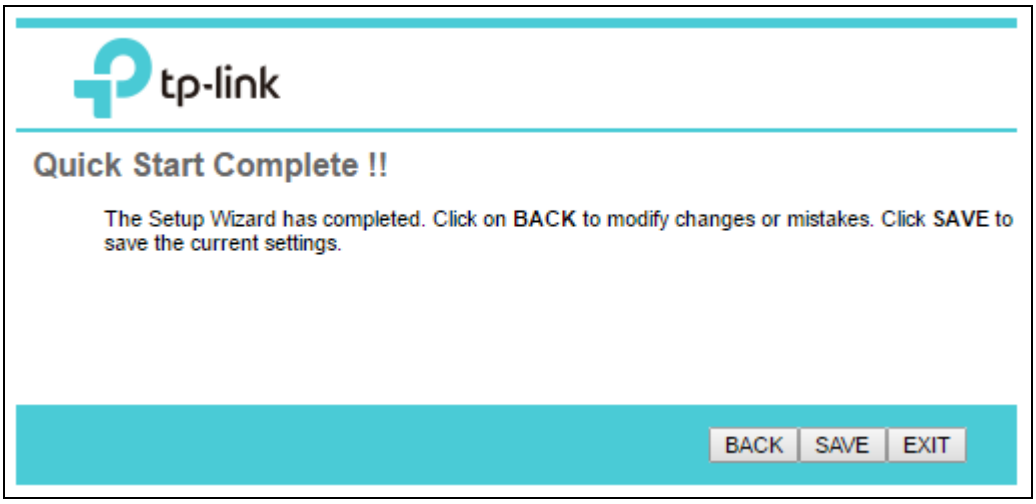
Step 4: Configure the rules for the Wlan, and click NEXT.



☞ Note:

If the Access Point is activated, the wireless function will be available even without the external antenna because of an additional printed antenna. To adopt the wireless security protection measures, please refer to section 4.2.3 Wireless.

Step 5: Click SAVE to finish the Quick Start.



Chapter 4 Software Configuration

This User Guide recommends using the Quick Installation Guide for first-time installation. For advanced users, if you want to know more about this device and make use of its functions adequately, maybe you will get help from this chapter to configure the advanced settings through the web management page to configure and manage the device.

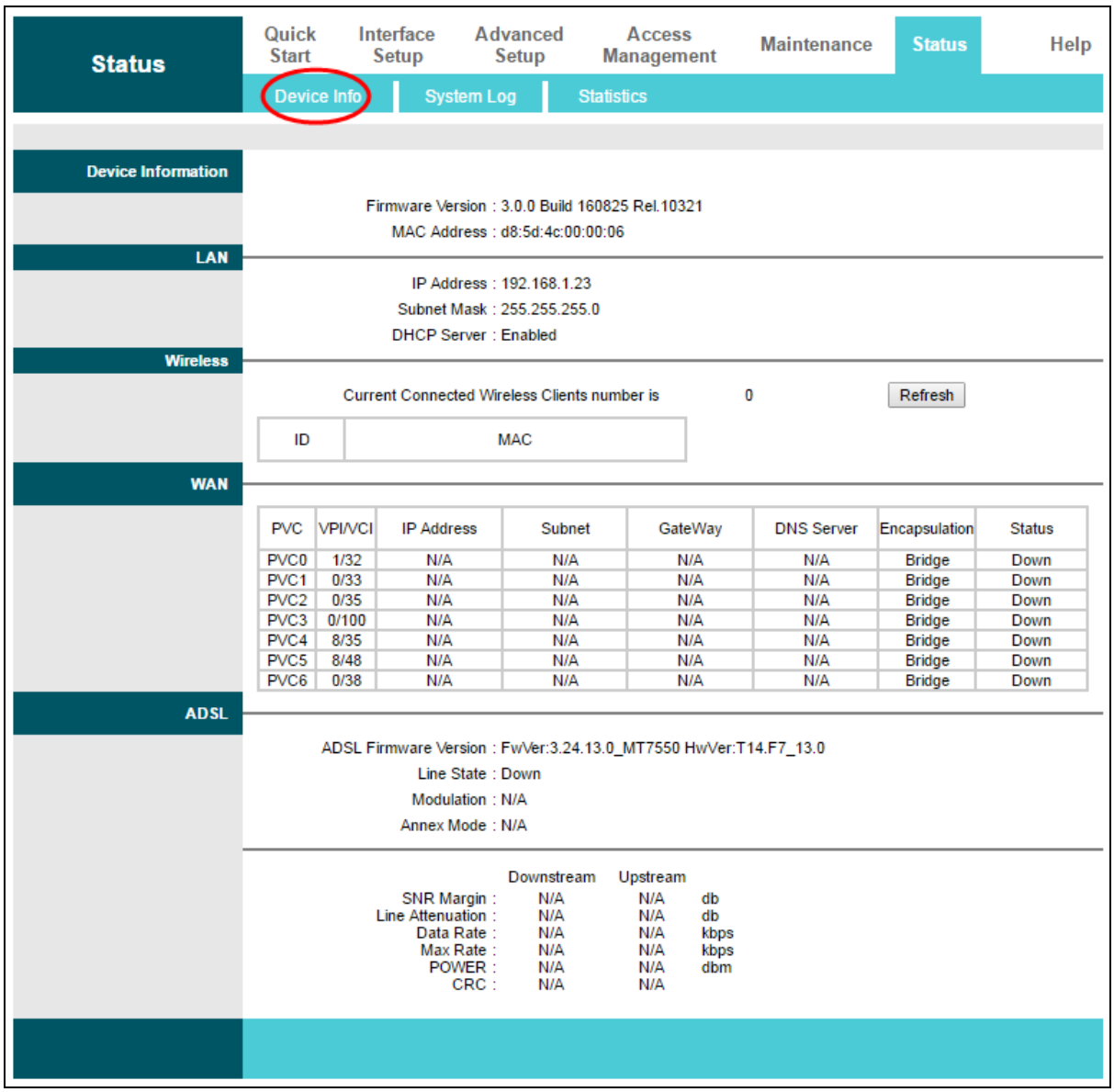
After your successful login, you will see the main menus of the web management page and submenus with detailed configurations or status information will be available after you click one of the main menus. To apply any settings you have altered on the page, please click SAVE to make the settings take effect.

4.1 Status

Choose Status, and you will see the following submenus: Device Info, System Log and Statistics. Click any of them, and you can configure the corresponding function.

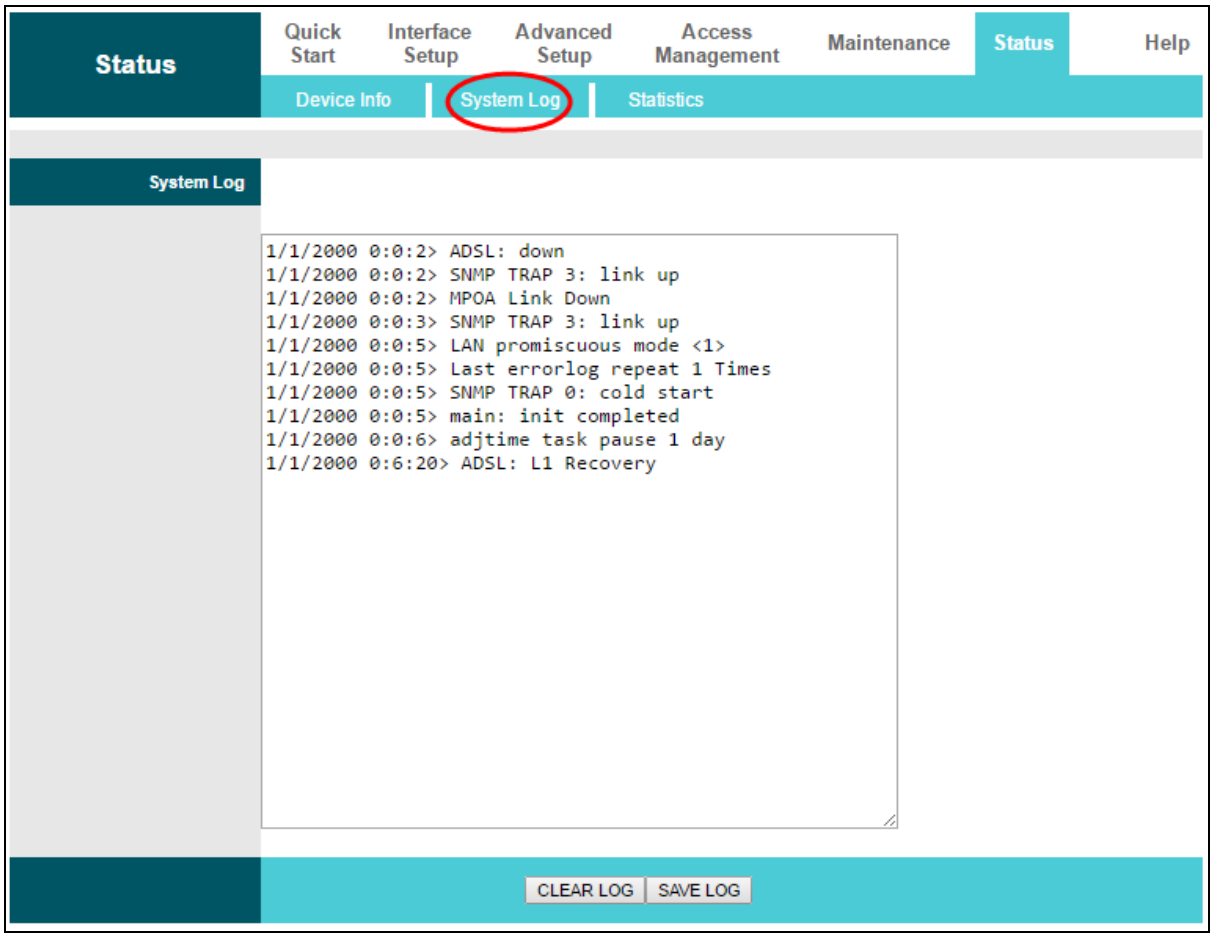
4.1.1 Device Info

Go to Status → Device Info, and you can view the device information, including LAN, Wireless, WAN and ADSL. The information will vary depending on the settings of the modem router configured on the Interface Setup screen.



4.1.2 System Log

Go to Status → System Log, and you can query the logs of the modem router.



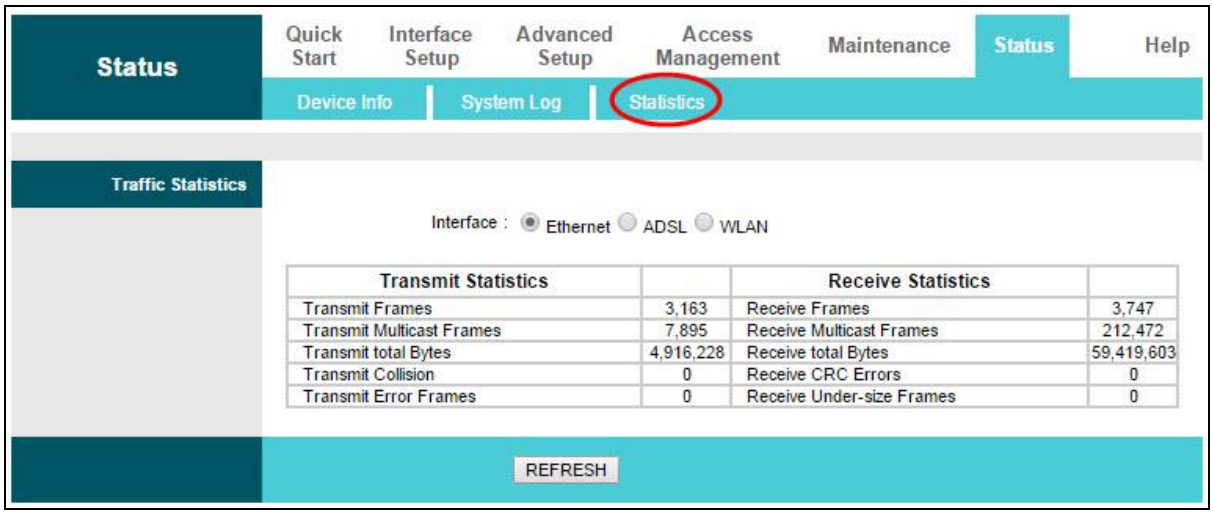
The modem router can keep logs of all traffic. You can query the logs to find what happened to your modem router.

Click CLEAR LOG to clear the logs.

Click SAVE LOG to save the logs.

4.1.3 Statistics

Go to Status → Statistics, and you can view the network traffic over Ethernet, ADSL and WLAN.



➢ **Interface:** You can select Ethernet, ADSL or WLAN to view the corresponding network traffic over different ports.

- Select Ethernet, and you will see the statistics table as below.

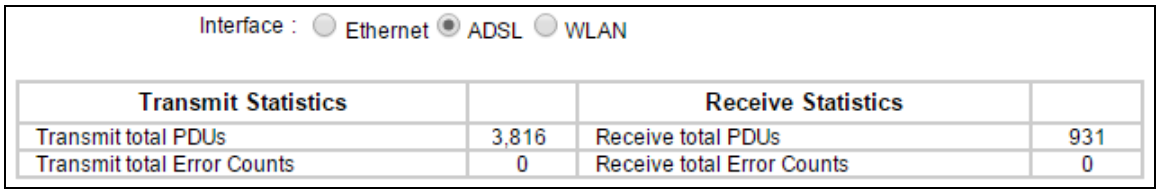
Interface : Ethernet ADSL WLAN

Transmit Statistics		Receive Statistics	
Transmit Frames	3,237	Receive Frames	3,816
Transmit Multicast Frames	7,931	Receive Multicast Frames	213,354
Transmit total Bytes	4,968,824	Receive total Bytes	59,682,544
Transmit Collision	0	Receive CRC Errors	0
Transmit Error Frames	0	Receive Under-size Frames	0

Statistics Table:

Transmit Statistics	**Transmit Frames**	The frames transmitted over the Ethernet port.
	Transmit Multicast Frames	The multicast frames transmitted over the Ethernet port.
	Transmit total Bytes	The total bytes transmitted over the Ethernet port.
	Transmit Collision	The collision occurred over the Ethernet port when data is being transmitted.
	Transmit Error Frames	The error frames over the Ethernet port when data is being transmitted.
Receive Statistics	**Receive Frames**	The frames received over the Ethernet port.
	Receive Multicast Frames	The multicast frames received over the Ethernet port.
	Receive total Bytes	The total bytes received over the Ethernet port.
	Receive CRC Errors	The CRC errors occurred over the Ethernet port when data is being received.
	Receive Under-size Frames	The Under-size frames received over the Ethernet port.

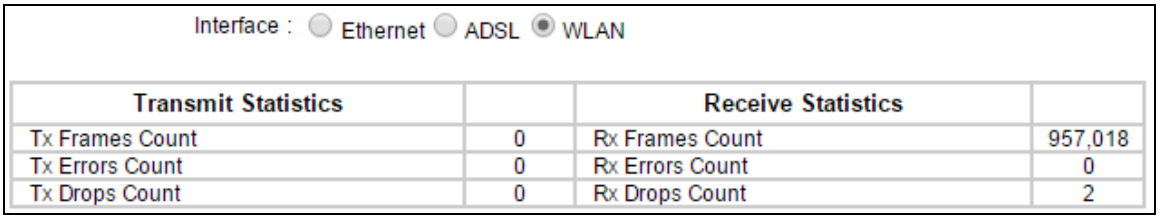
- Select ADSL, and you will see the statistics table as below.



Statistics Table:

Transmit Statistics	**Transmit total PDUs**	The total PDUs transmitted over the ADSL port.
	Transmit total Error Counts	The total errors occurred over the ADSL port when data is being transmitted.
Receive Statistics	**Receive total PDUs**	The total PDUs transmitted over the ADSL port.
	Receive total Error Counts	The total errors occurred over the ADSL port when data is being received.

- Select WLAN, and you will see the statistics table as below.



Statistics Table:

Transmit Statistics	**Tx Frames Count**	The frames transmitted over the WLAN when wireless data is being transmitted.
	Tx Errors Count	The errors occurred over the WLAN when wireless data is being transmitted.
	Tx Drops Count	The drops occurred over the WLAN when wireless data is being transmitted.
Receive Statistics	**Rx Frames Count**	The frames received over the WLAN when wireless data is being transmitted.
	Rx Errors Count	The errors occurred over the WLAN when wireless data is being received.
	Rx Drops Count	The drops occurred over the WLAN when wireless data is being received.

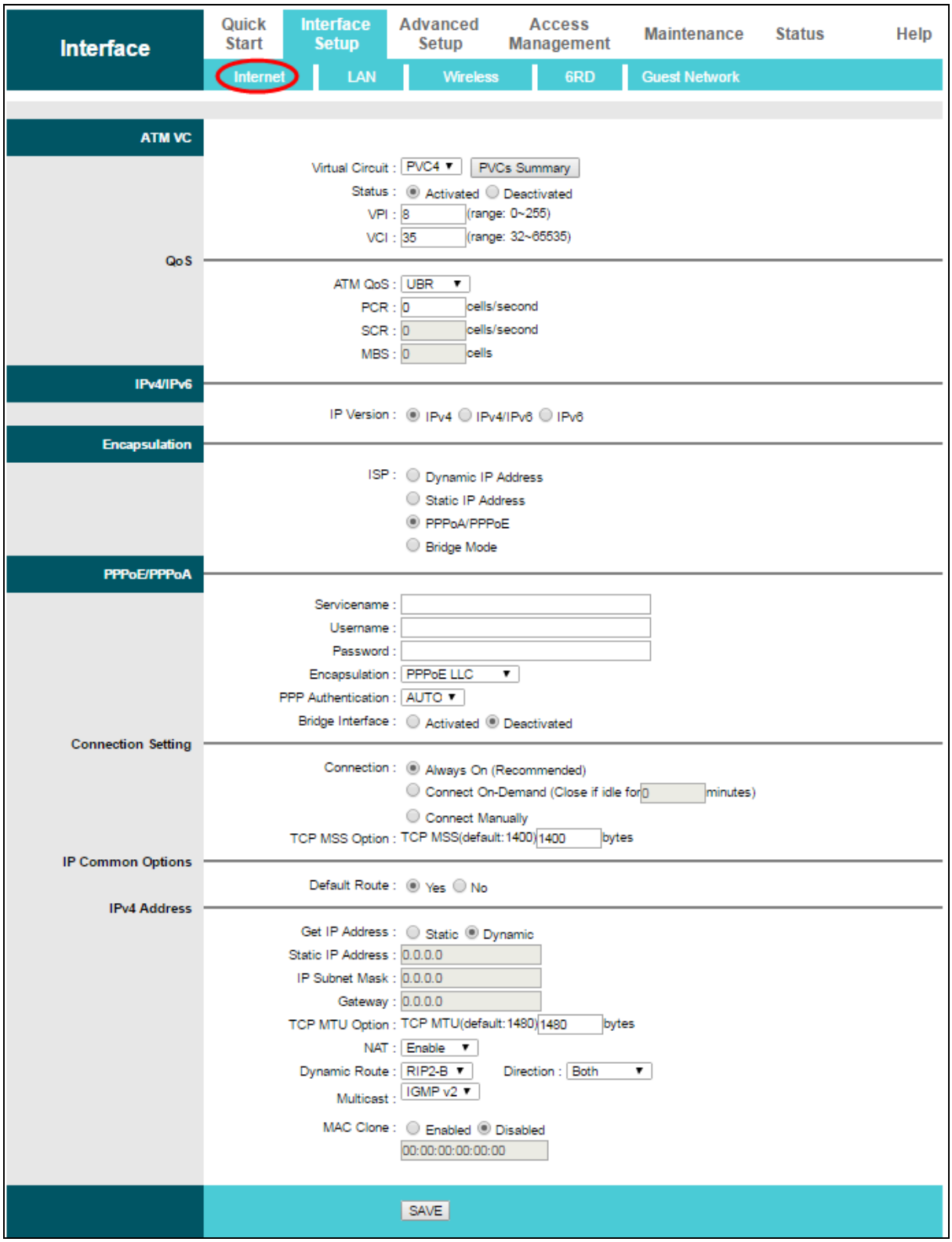
Click REFRESH to refresh immediately.

4.2 Interface Setup

Choose Interface Setup, and you will see the following submenus: Internet, LAN, Wireless, 6RD, Guest Network. Click any of them, and you can configure the corresponding function.

4.2.1 Internet

Go to Interface Setup → Internet, and you can configure the parameters for WAN ports in the following screen.



➢ **ATM VC:** ATM settings are used to connect to your ISP. Your ISP provides VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) settings to you. In this device, you can totally set up 8 VCs on different encapsulations. If you apply 8 different virtual circuits from your ISP, you need to activate the VC to take effect. For PVCs management, you can use ATM QoS to setup each PVC traffic line's priority.

- **Virtual Circuit:** Select the VC number you want to setup, PVC0~PVC7.

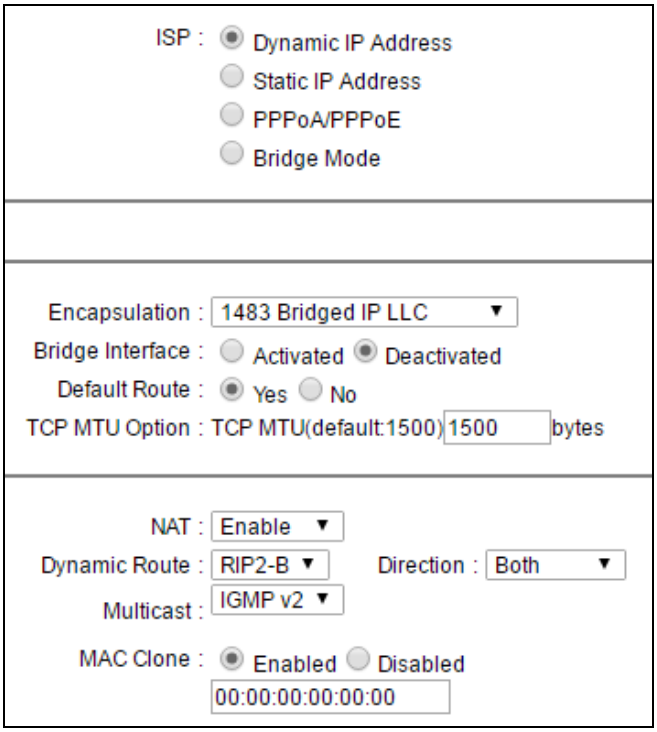
- **PVCs Summary:** Click the button, and you can view the summary information about the PVCs.
- **Status:** If you want to use a designed VC, you should activate it.
- **VPI:** Identifies the virtual path between endpoints in an ATM network. The valid range is from 0 to 255. Please input the value provided by your ISP.
- **VCI:** Identifies the virtual channel endpoints in an ATM network. The valid range is from 32 to 65535 (1 to 31 is reserved for well-known protocols). Please input the value provided by your ISP.
- **ATM QoS:** Select the Quality of Service types for this Virtual Circuit, including CBR (Constant Bit Rate), UBR (Unspecified Bit Rate) and VBR (Variable Bit Rate). These QoS types are all controlled by the parameters specified below, including PCR (Peak Cell Rate), SCR (Sustained Cell Rate) and MBS (Maximum Burst Size). Please configure them according to your needs.

➢ **IPv4/IPv6:** Select the version of IP.

➢ **Encapsulation:** There are four connection types: Dynamic IP Address, Static IP Address, PPPoA/PPPoE and Bridge Mode. Please choose the designed type that you want to use. After that, you should follow the configuration below to proceed.

1) Dynamic IP Address

Select this option if your ISP provides you an IP address automatically. This option is typically used for Cable services. Please enter the Dynamic IP information accordingly.

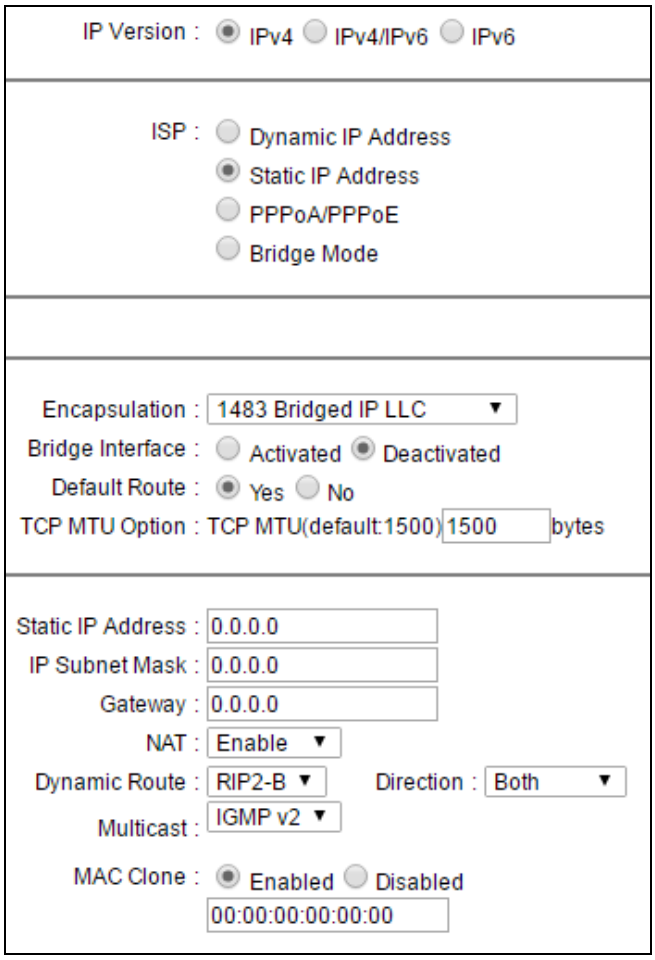


- **Encapsulation:** Select the encapsulation mode for the Dynamic IP Address. You can leave it default.
- **Bridge Interface:** Activate the option, and the modem router can also work in Bridge mode.

- **Default Route:** If enable this function, the current PVC will be considered as the default gateway to internet from this device.
- **TCP MTU Option:** Enter the TCP MTU as your desire.
- **NAT:** Select this option to Enable/Disable the NAT (Network Address Translation) function for this VC. The NAT function can be activated or deactivated per PVC basis.
- **Dynamic Route:** Select this option to specify the RIP (Routing Information protocol) version for WAN interface, including RIP1, RIP2-B and RIP2-M. RIP2-B and RIP2-M are both sent in RIP2 format. The difference is that RIP2-M using Multicast, while RIP2-B using Broadcast format.
- **Direction:** Select this option to specify the RIP direction. None is for disabling the RIP function. Both means the ADSL modem router will periodically send routing information and accept routing information, and then incorporate them into routing table. IN only means the ADSL modem router will only accept but will not send RIP packet. OUT only means the ADSL modem router will only send but will not accept RIP packet.
- **Multicast:** Select IGMP version, or disable the function. IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a multicast group. The ADSL ATU-R supports both IGMP version 1 (IGMP v1), IGMP v2 and IGMP v3. Select Disabled to disable it.
- **Mac Clone:** ISP just permits only one computer with the authenticated MAC address to access the Internet. In this case, you can enable MAC Clone function to allow more computers to access the Internet via the same account.

2) Static IP Address

Select this option if your ISP provides static IP information to you. You should set Static IP Address, IP Subnet Mask, and Gateway address in the screen below.

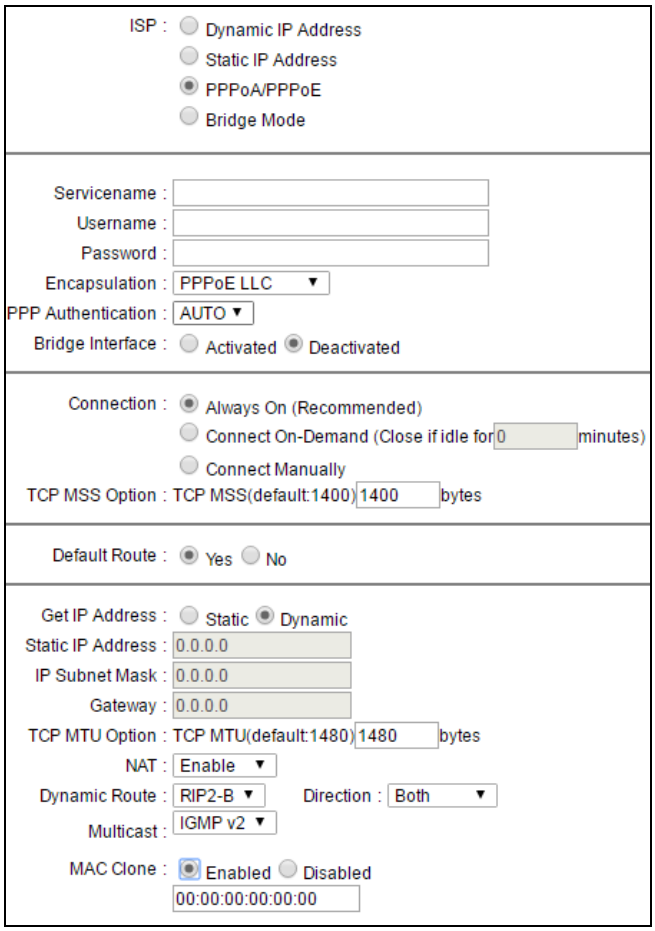


☞ Note:

Each IP address entered in the fields must be in the appropriate IP form, which is four IP octets separated by a dot (x.x.x.x), such as 192.168.1.100. The modem router will not accept the IP address if it is not in this format.

3) PPPoA/PPPoE

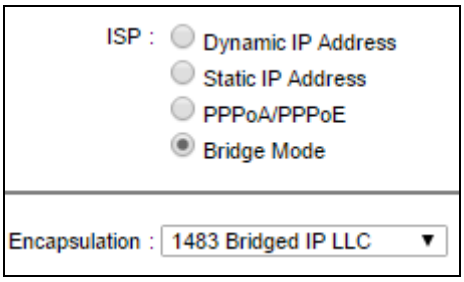
Select this option if your ISP requires you to use a PPPoE connection. This option is typically used for DSL services. Select Dynamic PPPoE to obtain an IP address automatically for your PPPoE connection. Select Static PPPoE to use a static IP address for your PPPoE connection. Please enter the information accordingly.



- **Servicename:** Enter a name to mark current connection, or you can leave it blank.
- **Username:** Enter your username for your PPPoA/PPPoE connection.
- **Password:** Enter your password for your PPPoA/PPPoE connection.
- **Encapsulation:** For both PPPoA and PPPoE connection, you need to specify the type of Multiplexing, either LLC or VC Mux.
- **Bridge Interface:** Activate the option, and the modem router can also work in Bridge mode.
- **Connection:** For PPPoA/PPPoE connection, you can select Always On or Connect On-Demand or Connect Manually. Connect On-Demand is dependent on the traffic. If there is no traffic (or Idle) for a pre-specified period of time, the connection will tear down automatically. And once there is traffic send or receive, the connection will be automatically on.
- **TCP MSS Option:** Enter the TCP MSS as your desire.
- **Default Route:** You should select Yes to configure the PVC as the default gateway to internet from this device.
- **Get IP Address:** Select Static or Dynamic. For PPPoA/PPPoE connection, you need to specify the public IP address for this ADSL modem router. The IP address can be either dynamically (via DHCP) or given IP address provided by your ISP. For Static IP, you need to specify the IP address, Subnet Mask and Gateway IP address.

4) Bridge Mode

If you select this type of connection, the modem can be configured to act as a bridging device between your LAN and your ISP. Bridges are devices that enable two or more networks to communicate as if they are two segments of the same physical LAN.

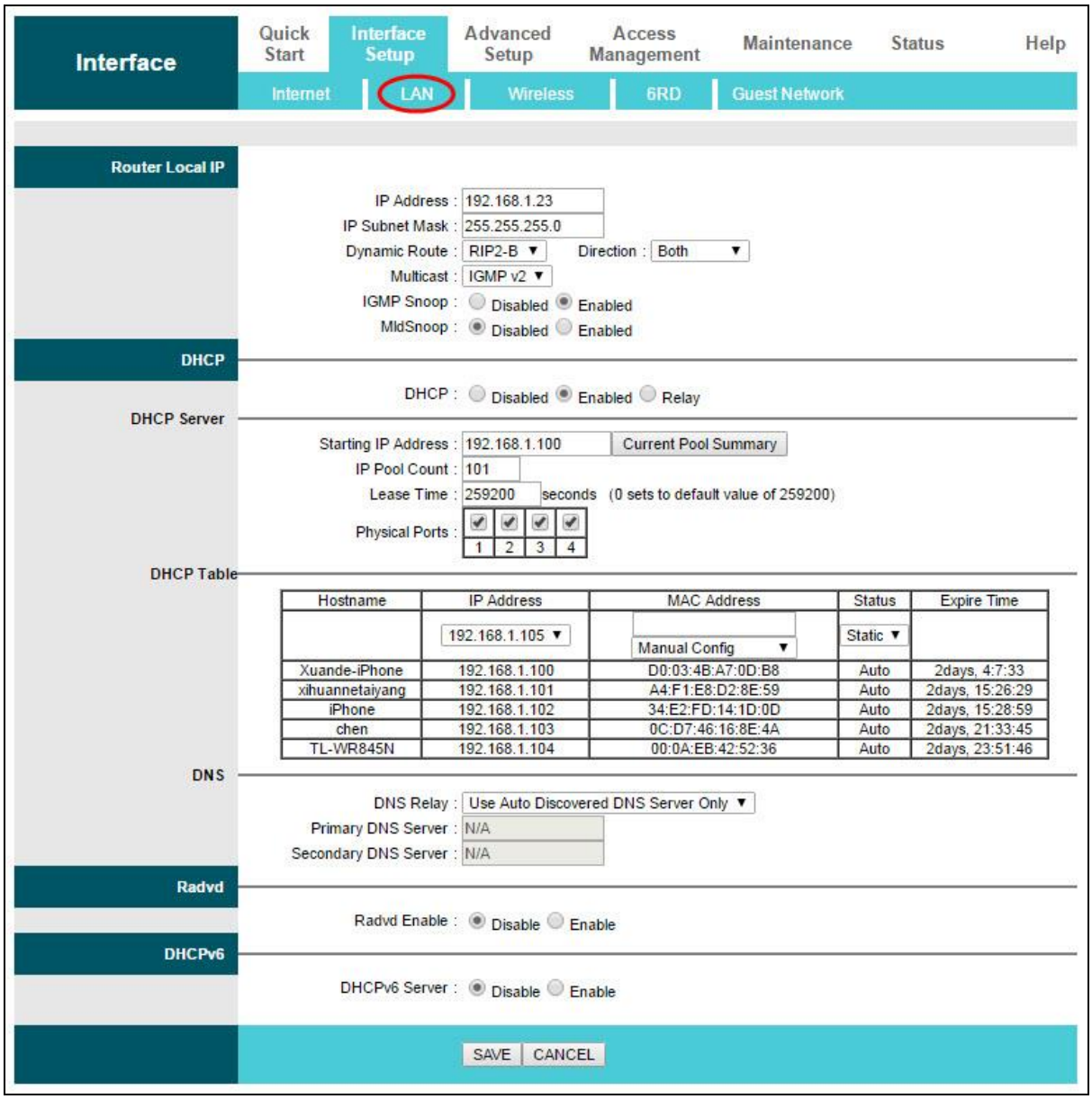


☞ Note:

After you finish the Internet configuration, please click SAVE to make the settings take effect.

4.2.2 LAN

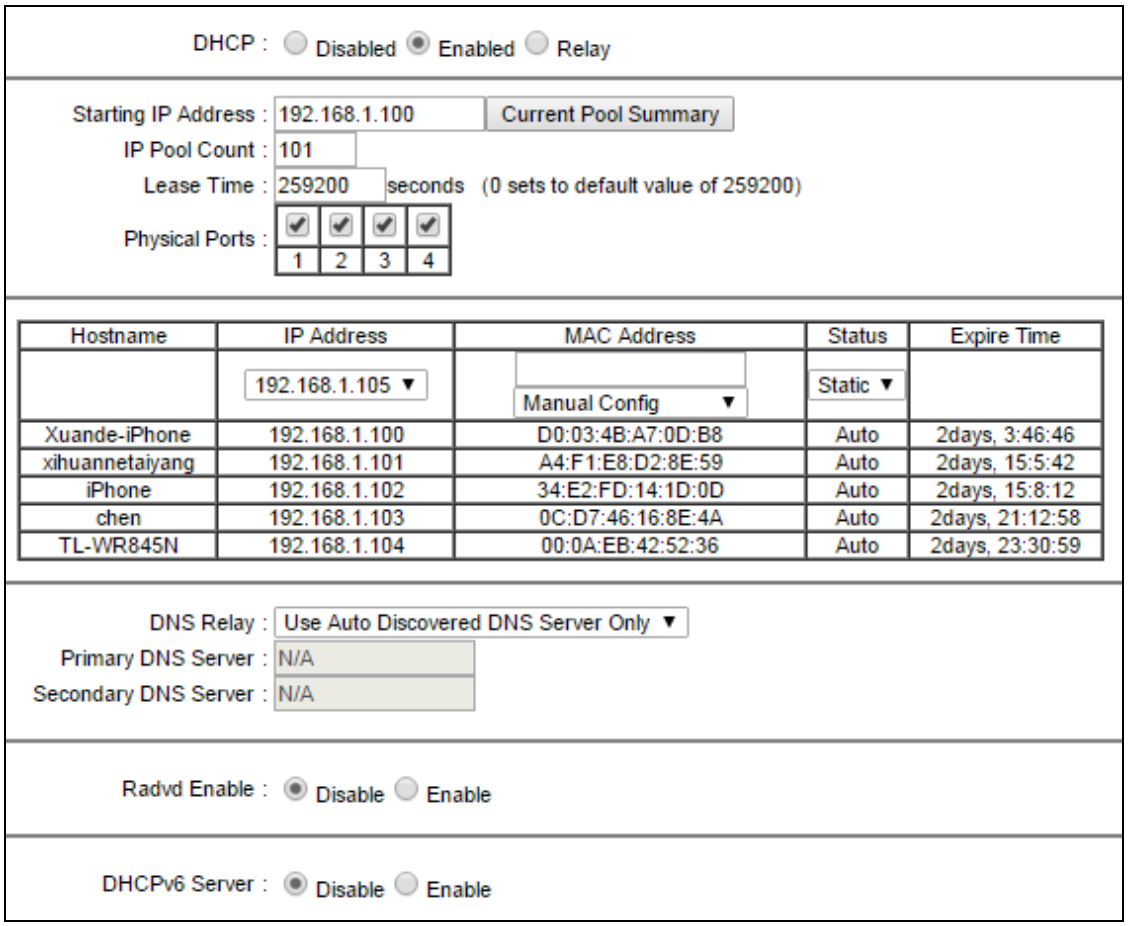
Go to Interface Setup → LAN, and you will see the LAN screen. Please configure the parameters for LAN ports according to the descriptions below.



- **Router Local IP:** These are the IP settings of the LAN interface for the device. These settings may be referred to as Private settings. You may change the LAN IP address if needed. The LAN IP address is private to your internal network and cannot be seen on the Internet.
  - **IP Address:** Enter the modem router's local IP Address, then you can access to the Web management page via the IP Address. The default value is 192.168.1.1.
  - **IP Subnet Mask:** Enter the modem router's Subnet Mask. The default value is 255.255.255.0.
  - **Dynamic Route:** Select this option to specify the RIP (Routing Information protocol) version for LAN interface, including RIP1, RIP2-B and RIP2-M. RIP2-B and RIP2-M are both sent in RIP2 format, the difference is that RIP2-M using Multicast, while RIP2-B using Broadcast format.

- **Direction:** Select this option to specify the RIP direction. None is for disabling the RIP function. Both means the ADSL modem router will periodically send routing information and accept routing information, and then incorporate them into routing table. IN only means the ADSL modem router will only accept but will not send RIP packet. OUT only means the ADSL modem router will only send but will not accept RIP packet.
- **Multicast:** Select IGMP version, or disable the function. IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a multicast group. The ADSL ATU-R supports both IGMP version 1 (IGMP v1), IGMP v2 and IGMP v3. Select Disabled to disable it.
- **IGMP Snoop:** Enable the IGMP Snoop function if you need.
- **Mld Snoop:** Enable the Mld Snoop function if you need.

➢ **DHCP:** Select Enabled, then you will see the screen below. The modem router will work as a DHCP Server; it becomes the default gateway for DHCP client connected to it. DHCP stands for Dynamic Host Control Protocol. The DHCP Server gives out IP addresses when a device is booting up and request an IP address to be logged on to the network. That device must be set as a DHCP client to obtain the IP address automatically. By default, the DHCP Server is enabled. The DHCP address pool contains the range of the IP address that will automatically be assigned to the clients on the network.



- **Starting IP Address:** Enter the starting IP address for the DHCP server's IP assignment. Because the default IP address for the modem router is 192.168.1.1, the default Start IP Address is 192.168.1.100.
- **IP Pool Count:** The max user pool size.
- **Lease Time:** The length of time for the IP lease. After the dynamic IP address has expired, the user will be automatically assigned a new dynamic IP address. The default is 259200 seconds.
- **Physical Ports:** If a physical port is unchecked, the client connected to that port will not be able to obtain IP address automatically although the DHCP function is enabled. All ports are checked by default.

➢ **DHCP Table**: The information of the DHCP clients will be displayed here

Hostname	IP Address	MAC Address	Status	Expire Time
	192.168.1.105 ▼	Manual Config ▼	Static ▼	
Xuande-iPhone	192.168.1.100	D0:03:4B:A7:0D:B8	Auto	2days, 3:17:59
xihuannetaiyang	192.168.1.101	A4:F1:E8:D2:8E:59	Auto	2days, 14:36:55
iPhone	192.168.1.102	34:E2:FD:14:1D:0D	Auto	2days, 14:39:25
chen	192.168.1.103	0C:D7:46:16:8E:4A	Auto	2days, 20:44:11
TL-WR845N	192.168.1.104	00:0A:EB:42:52:36	Auto	2days, 23:2:12

- **Hostname:** Display the name of the DHCP client.
- **IP Address:** Display the IP Address of the DHCP client.
- **MAC Address:** Display the MAC Address of the DHCP client.
- **Status:** Display the status of the assigned IP Address, either Static or Auto. Static indicates that the IP Address is bounded to the MAC Address, while Auto indicates that the IP Address is assigned to the MAC Address automatically.

How to assign a static IP address to the client?

1). Select an IP Address from the drop-down list.

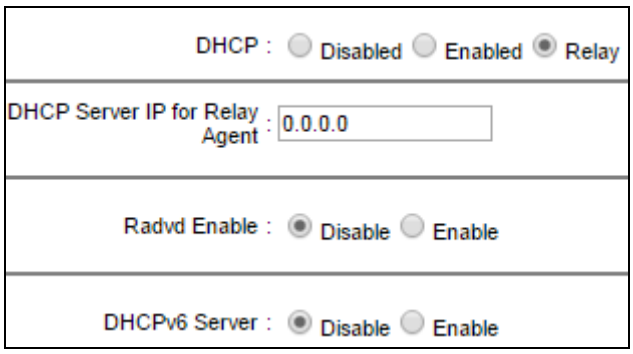
2). Enter the MAC Address of the client in the table.

- **DNS Relay:** If you want to disable this feature, you just need to set both Primary and secondary DNS IP to 0.0.0.0. If you want to use DNS relay, you can setup DNS server IP to 192.168.1.1 on their Computer. If not, the device will perform as no DNS relay.
- **Primary DNS Server:** Type in your preferred DNS server.
- **Secondary DNS Server:** Type in your preferred DNS server.

☞ Note:

If Use Auto Discovered DNS Server Only is selected in DNS Relay, this modem router will accept the first received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment. If Use User Discovered DNS Server Only is selected in DNS Relay, it is necessary for you to enter the primary and optional secondary DNS server IP addresses. After type in the address, click SAVE to save it and invoke it.

➢ **DHCP Relay:** Select Relay, then you will see the following screen, and the modem router will work as a DHCP Relay. A DHCP relay is a computer that forwards DHCP data between computers that request IP addresses and the DHCP server that assigns the addresses. Each of the device's interfaces can be configured as a DHCP relay. If it is enabled, the DHCP requests from local PCs will forward to the DHCP server runs on WAN side. To have this function working properly, please run on router mode only, disable the DHCP server on the LAN port, and make sure the routing table has the correct routing entry.



- **DHCP Server IP for Relay Agent:** Enter the DHCP server IP Address runs on WAN side.

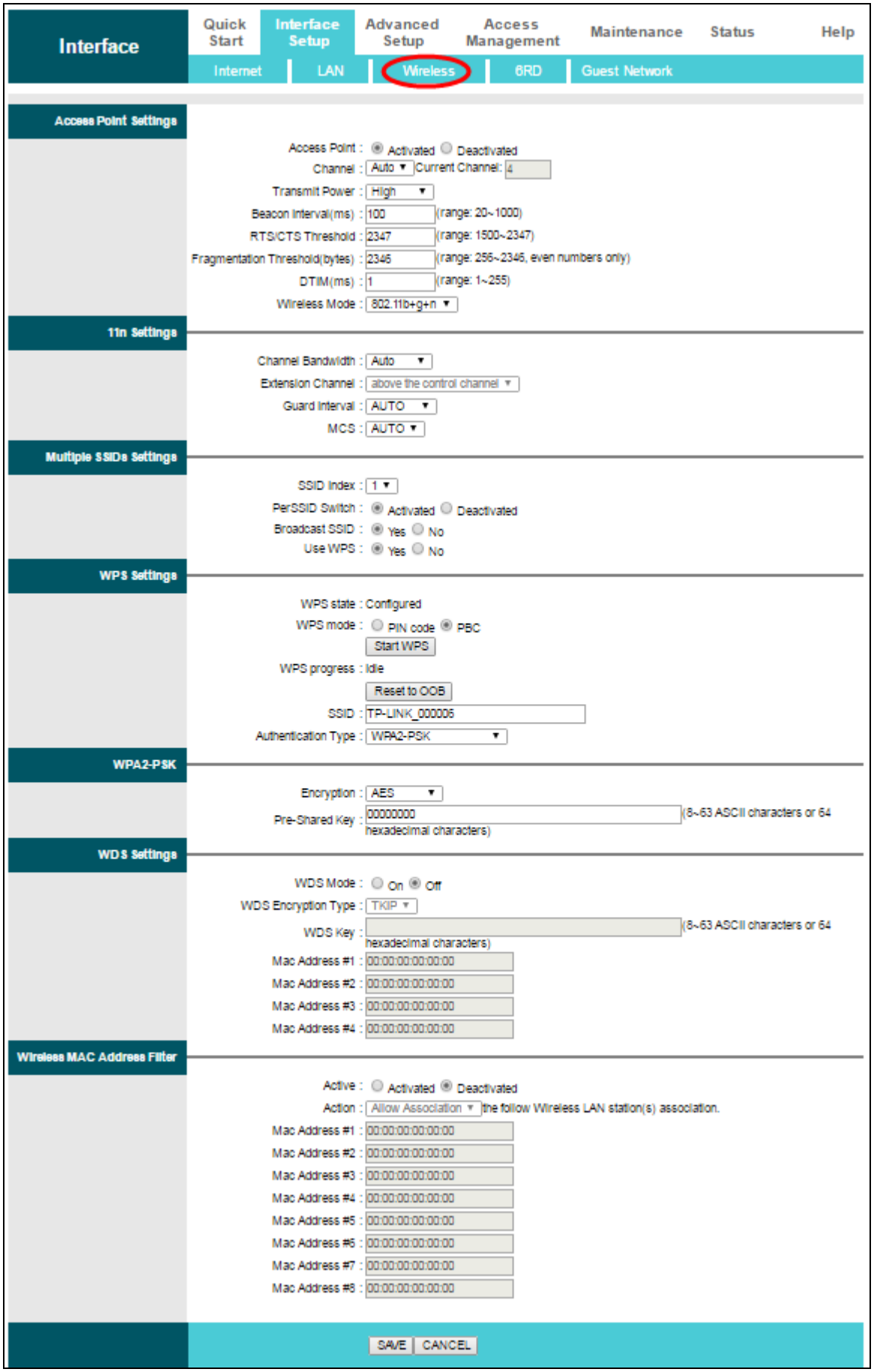
☞ Note:

If you select Disabled, the DHCP function will not take effect.

- **Radvd Enable:** Enable or Disable the auto configuration of radvd.
- **DHVCPv6 Server:** Enable or Disable the modem router working as a DHCPv6 Server.

4.2.3 Wireless

Go to Interface Setup → Wireless, and you will see the Wireless screen. Please configure the parameters for wireless according to the descriptions below.


Interface
Quick Start
Interface Setup
Advanced Setup
Access Management
Maintenance
Status
Help
Internet
LAN
Wireless
6RD
Guest Network
Access Point Settings
Access Point : Activated Deactivated
Channel : Auto Current Channel: 4
Transmit Power : High
Beacon Interval(ms) : 100 (range: 20~1000)
RTS/CTS Threshold : 2347 (range: 1500~2347)
Fragmentation Threshold(bytes) : 2346 (range: 256~2346, even numbers only)
DTIM(ms) : 1 (range: 1~255)
Wireless Mode : 802.11b+g+n
11n Settings
Channel Bandwidth : Auto
Extension Channel : above the control channel
Guard Interval : AUTO
MCS : AUTO
Multiple SSIDs Settings
SSID Index : 1
PerSSID Switch : Activated Deactivated
Broadcast SSID : Yes No
Use WPS : Yes No
WPS Settings
WPS state : Configured
WPS mode : PIN code PBC
Start WPS
WPS progress : Idle
Reset to OOB
SSID : TP-LINK_000006
Authentication Type : WPA2-PSK
WPA2-PSK
Encryption : AES
Pre-Shared Key : 00000000 (8~63 ASCII characters or 64 hexadecimal characters)
WDS Settings
WDS Mode : On Off
WDS Encryption Type : TKIP
WDS Key : (8~63 ASCII characters or 64 hexadecimal characters)
Mac Address #1 : 00:00:00:00:00:00
Mac Address #2 : 00:00:00:00:00:00
Mac Address #3 : 00:00:00:00:00:00
Mac Address #4 : 00:00:00:00:00:00
Wireless MAC Address Filter
Active : Activated Deactivated
Action : Allow Association the follow Wireless LAN station(s) association.
Mac Address #1 : 00:00:00:00:00:00
Mac Address #2 : 00:00:00:00:00:00
Mac Address #3 : 00:00:00:00:00:00
Mac Address #4 : 00:00:00:00:00:00
Mac Address #5 : 00:00:00:00:00:00
Mac Address #6 : 00:00:00:00:00:00
Mac Address #7 : 00:00:00:00:00:00
Mac Address #8 : 00:00:00:00:00:00
SAVE
CANCEL

- **Access Point Settings:** These are the settings of the access point. You can configure the rules to allow wireless-equipped computers and other devices to communicate with a wireless network.
  - **Access Point:** Select Activated to allow wireless station to associate with the access point.
  - **Channel:** Select the channel you want to use from the drop-down List of Channel. This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
  - **Transmit Power:** Here you can specify the transmit power of modem router. You can select High, Medium or Low which you would like. High is the default setting and is recommended.
  - **Beacon Interval:** Enter a value between 20-1000 milliseconds. The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the modem router to synchronize the wireless network. The default value is 100.
  - **RTS/CTS Threshold:** Should you encounter inconsistent data flow, only minor reduction of the default value 2347 is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The modem router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. In most cases, keep its default value of 2347.
  - **Fragmentation Threshold:** This value specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor reduction of the default value is recommended. In most cases, it should remain at its default value of 2346.
  - **DTIM:** This value, between 1 and 255, indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the modem router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages. The default value is 1.
  - **Wireless Mode:** In the drop-down list you can select 802.11b, 802.11g, 802.11n, 802.11b+g, 802.11g+n and 802.11b+g+n. 802.11b+g+n allows both 802.11b, 802.11g and 802.11n wireless stations to connect to the modem router.
- **11n Settings:** These are the settings of the 11n parameters. If 802.11n, 802.11g+n or 802.11b+g+n is selected for Wireless mode, these settings will be displayed.

- **Channel Bandwidth:** Select the Bandwidth you want to use from the drop-down List. There are three options, Auto, 20 MHz and 40 MHz. If bigger bandwidth is selected, device could transmit and receive data with higher speed.
- **Extension Channel:** If Auto or 40 MHz is selected, this option will be displayed.
- **Guard Interval:** If 20MHz is selected, this option will be displayed. And then you can select the guard interval you want from the drop-down list.
- **MCS:** Select the wireless transmission rate from the drop-down list. By default, the option is AUTO.

➢ **Multiple SSIDs Settings:** These are the settings of the SSID.

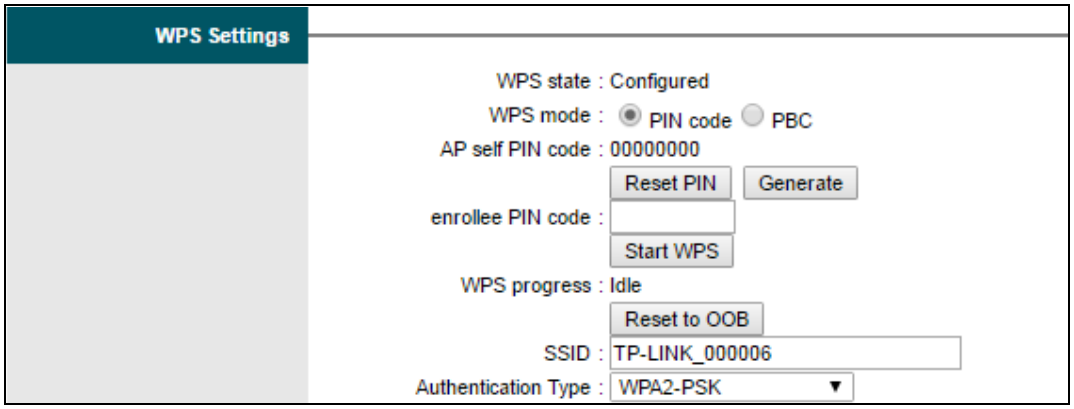
- **SSID Index:** The index of the SSID, and in this model, you can only leave it as a default value of 1.
- **PerSSID Switch:** Select Activated to allow switch of per SSID.
- **Broadcast SSID:** When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the modem router. To broadcast the modem router's SSID, keep the default setting. If you don't want to broadcast the modem router's SSID, select No.
- **Use WPS:** Use WPS (Wi-Fi Protected Setup) function, you can add a new wireless device to an existing network quickly. To use WPS, keep the default setting, and configure the parameters in WPS Settings. If you don't want to Use WPS, select No.

➢ **WPS Settings:** WPS can help you to add a new wireless device to an existing network quickly.

- **WPS state:** Display the current WPS state.
- **WPS mode:** If the wireless adapter supports Wi-Fi Protected Setup (WPS), you can establish a wireless connection between wireless adapter and modem router using either PIN method or Push Button Configuration (PBC) method, please select the one you want.

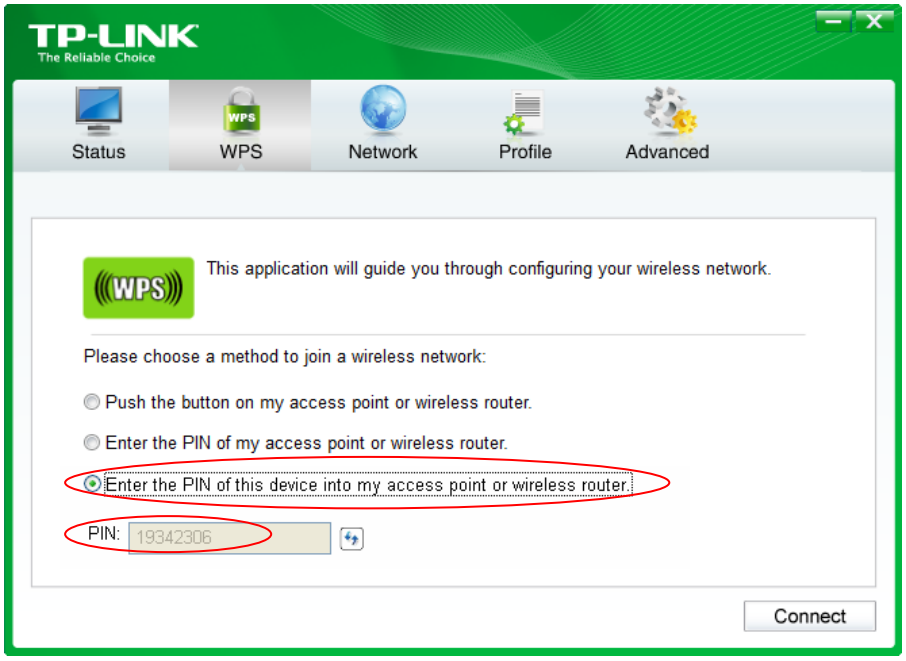
1) By PIN

If the wireless adapter supports Wi-Fi Protected Setup and the PIN method, you can add it to the network by PIN with the following two methods. Select PIN code, you will see the following screen.



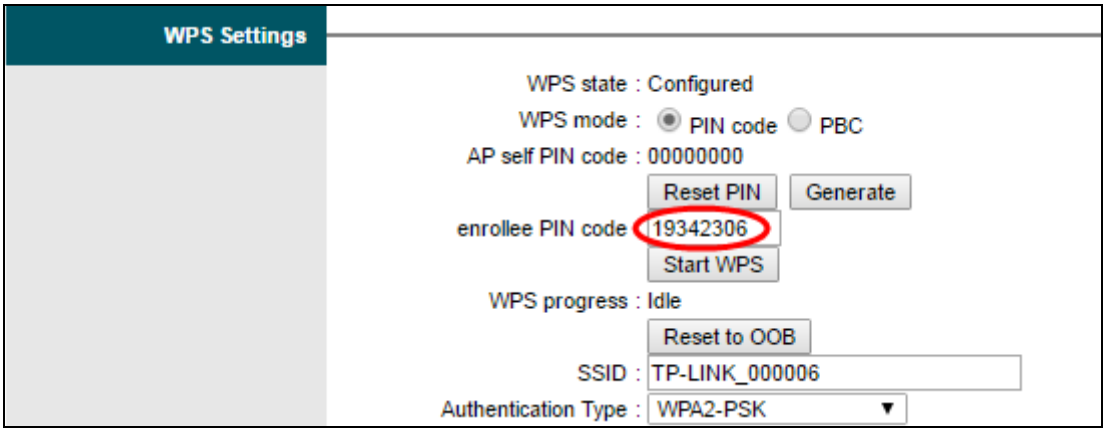
Method One: Enter the PIN of wireless adapter into my modem router

Step 1: For the configuration of the wireless adapter, please choose Enter the PIN of this device into my access point or wireless router in the configuration utility, and get the PIN code on the screen as below, then click Connect.



The WPS Configuration Screen of Wireless Adapter

Step 2: For the modem router, keep PIN code selected and enter the PIN code of the wireless adapter in the field next to enrollee PIN code as shown below. Then click Start WPS.

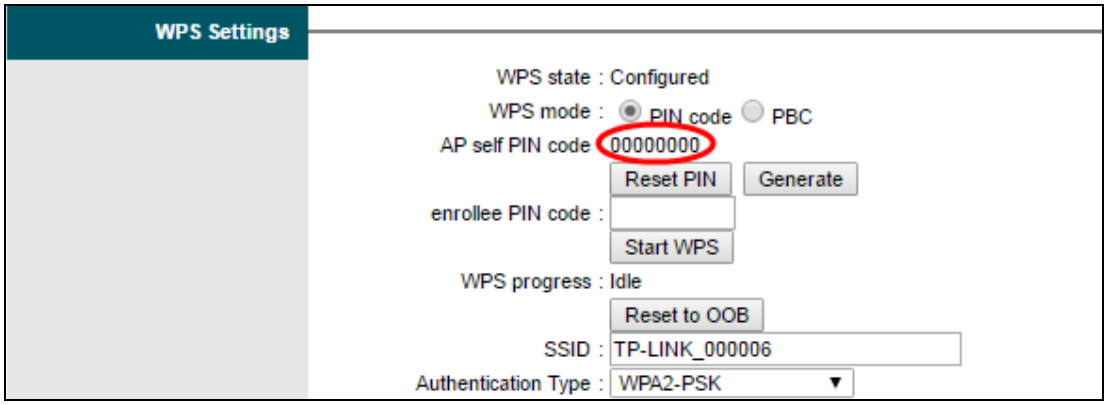


☞ Note:

In this example, the default PIN code of this adapter is 19342306 as the preceding figure shown.

Method Two: Enter the PIN from your Router or AP device

Step 1: Get the Current PIN code of your modem router from AP self PIN code (each modem router has its unique PIN code. Here takes the PIN code 00000000 of this modem router for example).



Step 2: For the configuration of the wireless adapter, please choose Enter the PIN of my access point or wireless router in the configuration utility, and enter the PIN code of the modem router into the field next to PIN. Then click Connect.

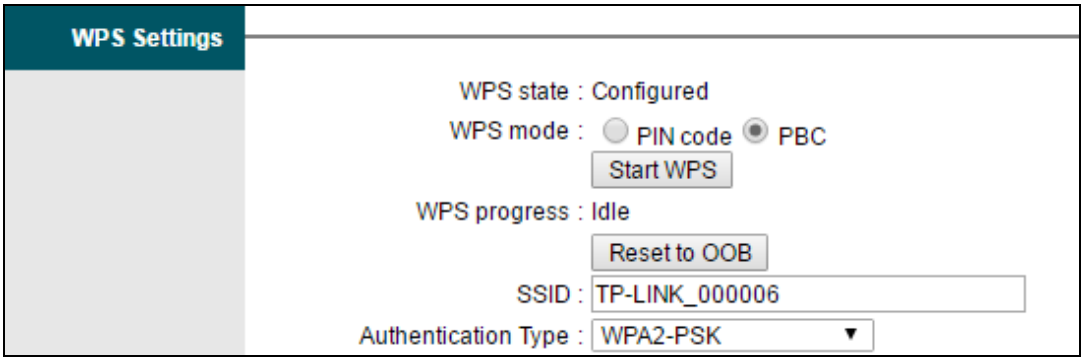
The WPS Configuration Screen of Wireless Adapter

☞ Note:

The default PIN code of the modem router can be found on its label or the WPS screen in its web configuration page.

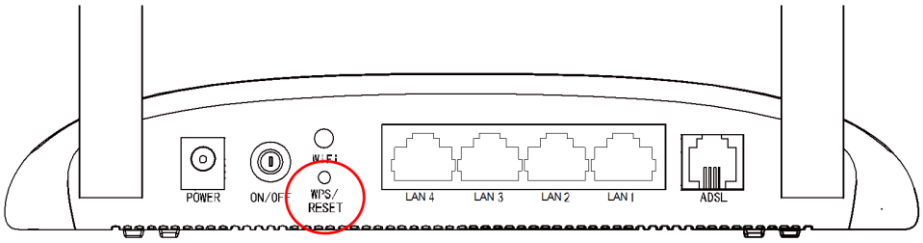
2) PBC

If the wireless adapter supports Wi-Fi Protected Setup and the Push Button Configuration (PBC) method, you can add it to the network by PBC with the following two methods. Select PBC, you will see the following screen.



Method One: Hardware push button

Step 1: Press the WPS/RESET button on your modem router for about 2 seconds or click the Start WPS button on the screen.



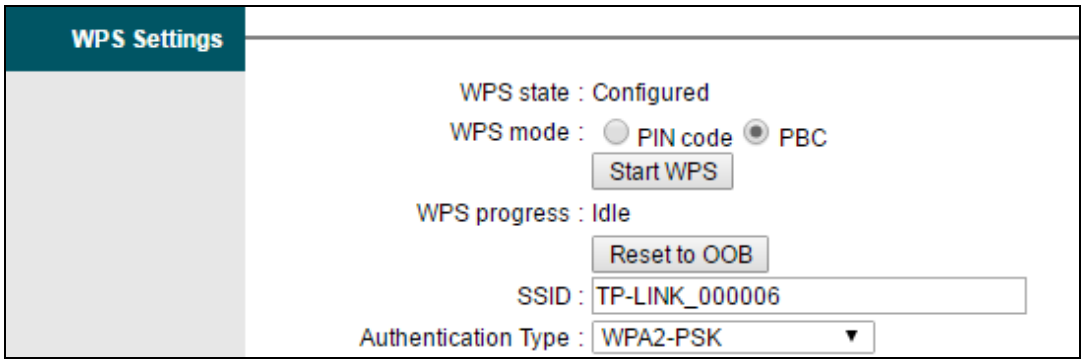
Step 2: Press and hold the WPS button of the adapter directly for about 2 seconds.

Step 3: Wait until the following screen appears. Click OK to complete the WPS configuration.

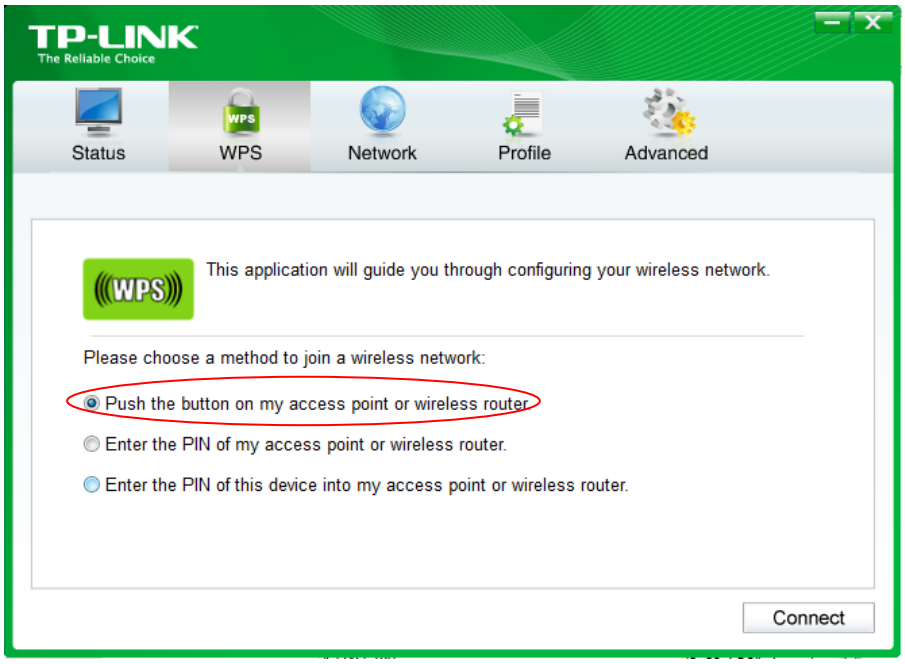
The WPS Configuration Screen of Wireless Adapter

Method Two: Software push button

Step 1: Click Start WPS button on the screen.



Step 2: For the configuration of the wireless adapter, please choose Push the button on my access point or wireless router in the configuration utility as below, and click Connect.



The WPS Configuration Screen of Wireless Adapter

Step 3: Wait for a while until the following screen appears. Click OK to complete the WPS configuration.

The WPS Configuration Screen of Wireless Adapter

- **WPS progress:** Show the current WPS progress.
- **Reset to OOB:** Reset WPS AP to the OOB (out-of-box) configuration.
- **SSID:** Wireless network name shared among all points in a wireless network. The SSID must be identical for all devices in the wireless network. It is case-sensitive and must not exceed 32 characters (use any of the characters on the keyboard). Make sure this setting is the same for all stations in your wireless network. Type the desired SSID in the space provided.
- **Authentication Type:** Select an authentication type from the drop-down list, which allows you to configure security features of the wireless LAN interface. Options available are: Disabled, WEP-64Bits, WEP-128Bits, WPA-PSK, WPA2-PSK, and WPA-PSK/ WPA2-PSK.

WEP- 64Bits

To configure WEP-64Bits settings, select the WEP-64Bits option from the drop-down list. The menu will change to offer the appropriate settings. WEP-64Bits is a data privacy mechanism based on a 64-bit shared key algorithm, as described in the IEEE 802.11g standard.

WEP-128Bits

To configure WEP-128Bits settings, select the WEP-128Bits option from the drop-down list. The menu will change to offer the appropriate settings. 128-bit is stronger than 64-bit.

WPA-PSK

To configure WPA-PSK settings, select the WPA-PSK option from the drop-down list. The menu will change to offer the appropriate settings. WPA-PSK requires a shared key and does not use a separate server for authentication. PSK keys can be ASCII or Hex type.

- **Encryption:** Select the encryption you want to use: TKIP/AES, TKIP or AES (AES is an encryption method stronger than TKIP).
  - ✓ **TKIP** (Temporal Key Integrity Protocol) - a wireless encryption protocol that provides dynamic encryption keys for each packet transmitted.
  - ✓ **AES** (Advanced Encryption Standard) - A security method that uses symmetric 128-bit block data encryption.
- **Pre-Shared Key:** Enter the key shared by the modem router and your other network devices.

WPA2-PSK

To configure WPA2-PSK settings, select the WPA2-PSK option from the drop-down list. The menu will change to offer the appropriate settings. WPA2-PSK requires a shared key and does not use a separate server for authentication. PSK keys can be ASCII or Hex type.

WPA-PSK/WPA2-PSK

To configure WPA-PSK/WPA2-PSK settings, select the WPA-PSK/WPA2-PSK option from the drop-down list. The menu will change to offer the appropriate settings. WPA-PSK/WPA2-PSK requires a shared key and does not use a separate server for authentication. PSK keys can be ASCII or Hex type. WPA-PSK/WPA2-PSK is more flexible than WPA-PSK or WPA2-PSK.

➢ **WDS Settings:** With this function enabled, the modem router can bridge two or more WLANs.

- **WDS Mode:** Select On/Off to enable/disable WDS.
- **WDS Encryption Type:** You can select either AES or TKIP.
- **WDS Key:** Create a key for the router.
- **MAC Address:** Enter the MAC Address you wish to bridge in the field.

- **Wireless MAC Address Filter:** Wireless access can be filtered by using the MAC addresses of the wireless devices transmitting within your network's RADIUS.
  - **Active:** If you wish to filter users by MAC Address, select Activated, and Deactived for don't.
  - **Action:** To filter wireless users by MAC Address, select Allow Association or Deny Association the follow Wireless LAN station(s) association.
  - **MAC Address:** Enter the MAC Address you wish to filter in the field.

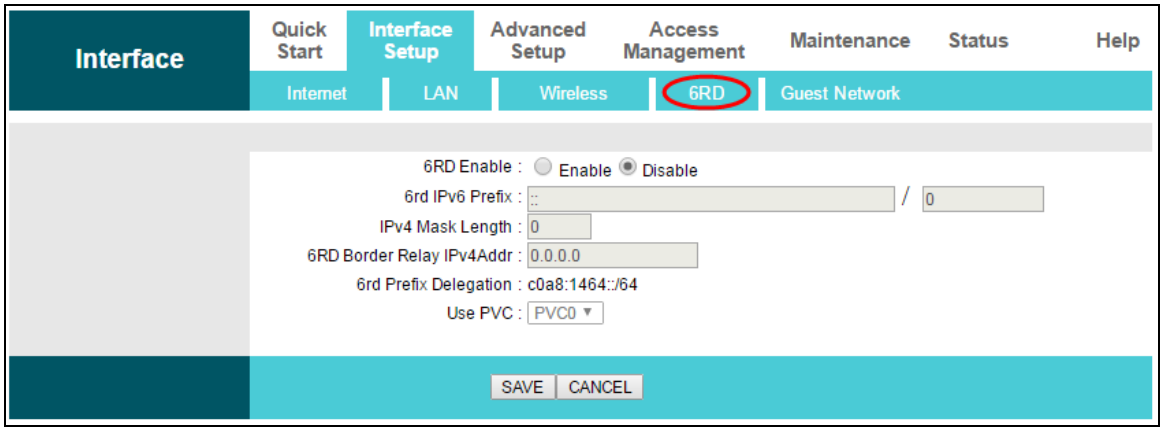
☞ Note:

For most users, it is recommended to use the default Wireless LAN Performance settings. Any changes made to these settings may adversely affect your wireless network. Under certain circumstances, changes may benefit performance. Carefully consider and evaluate any changes to these wireless settings.

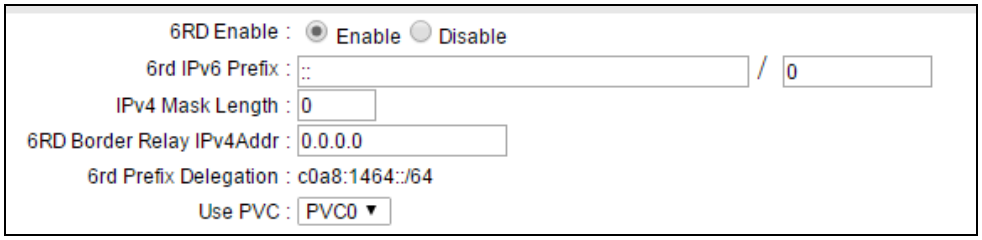
4.2.4 6RD

IPv6 tunnel is a kind of transition mechanism to enable IPv6-only hosts to reach IPv4 services, and to allow isolated IPv6 hosts and networks to reach each-other over IPv4-only infrastructure before IPv6 completely supplants IPv4. It is a temporary solution for networks that do not support native dual-stack, where both IPv6 and IPv4 run independently.

As a type of IPv6 tunnel, 6RD is used in the situation that your WAN connection is IPv4 while LAN connection is IPv6. Go to Interface Setup → 6RD.



- **6RD Enable:** The default setting is disabled. Select Enable when your WAN connection is IPv4 while LAN connection is IPv6.



- **6rd IPv6 Prefix:** Enter the prefix of the IPv6.

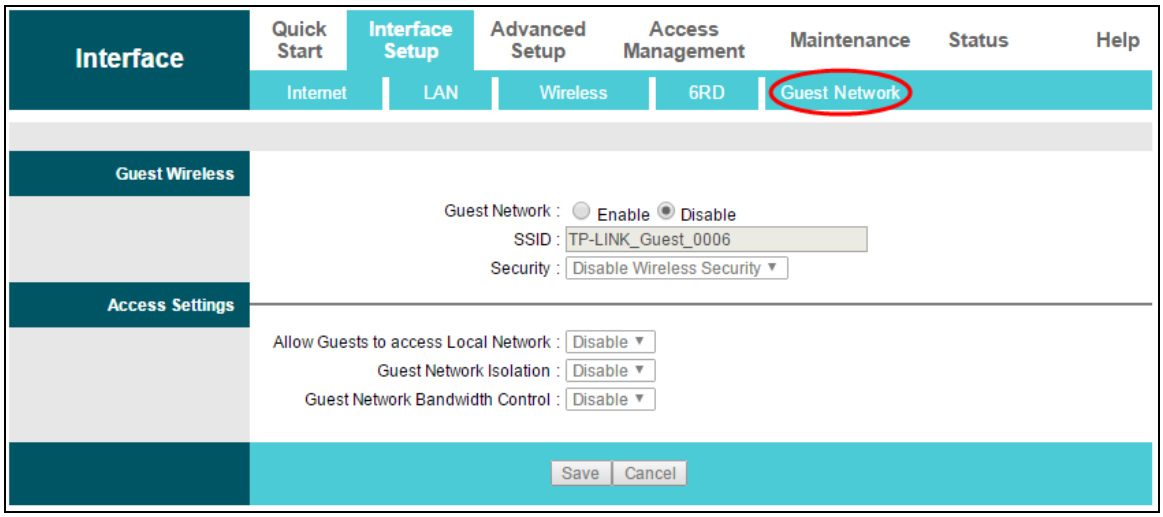
- **IPv4 Mask Length:** The length of the selected WAN connection's IPv4 mask.
- **6RD Border Relay IPv4Addr:** The IPv4 address of the border relay router of 6RD tunnel.
- **Use PVC:** Select the PVC from the drop-down list.

☞ Note:

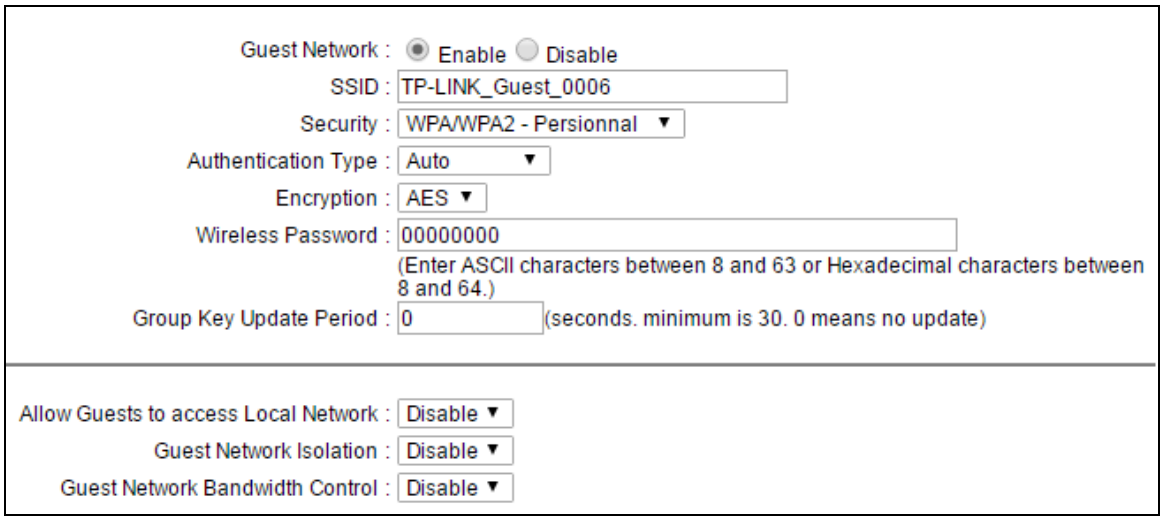
To enable the function, there should not be any IPv6 WAN connections.

4.2.5 Guest Network

Go to Interface Setup → Guest Network, and you will see the Guest Network screen. This feature allows you to create a separate network for your guests without allowing them to access your main network and the computers connected to it.



You can enable or disable Guest Network. The default setting is disabled. When you enable this function, you could set wireless parameters for Guest Network.



- **SSID:** The guest network name. When setting up a Guest network, it is strongly recommended to use a name that easily distinguishes it from your primary network.

- **Authentication Type:** Select the Authentication Type from the drop-down list.
- **Encryption:** You can select either AUTO, AES or TKIP.
- **Wireless Password:** You may personalize your guest network password by entering a new password.
- **Group Key Update Period:** Specify the group key update interval in seconds. The value should be 30 or above. Enter 0 to disable the update.
- **Allow Guests to access Local Network**: The guests have access to your local Network, but cannot login the modem router's web management interface.
- **Guest Network Isolation:** This function can isolate wireless clients on your guest network from each other. Client isolation is disabled by default.
- **Guest Network Bandwidth Control:** With this function, you can configure the Upstream Bandwidth and Downstream Bandwidth for guest network.

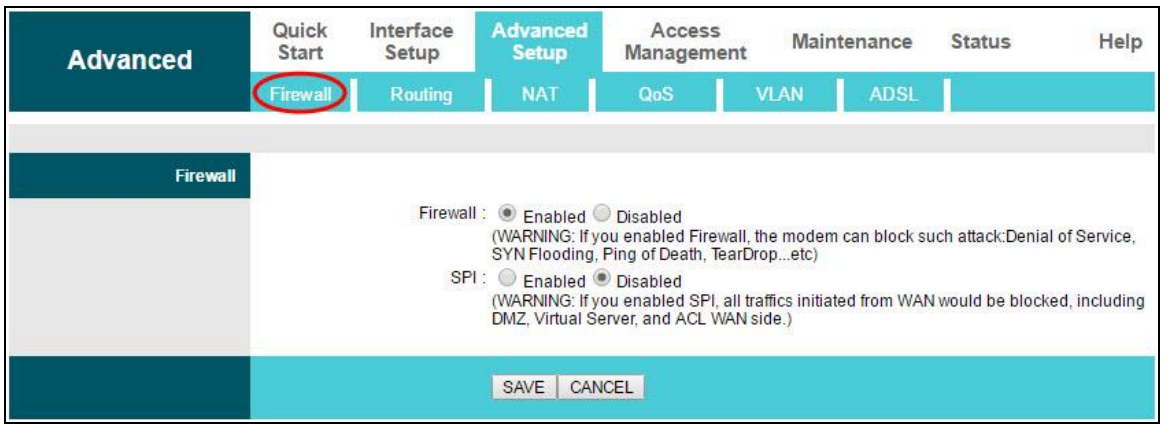
Click Save to save your settings.

4.3 Advanced Setup

Choose Advanced Setup, and you will see the following submenus. Click any of them, and you can configure the corresponding function.

4.3.1 Firewall

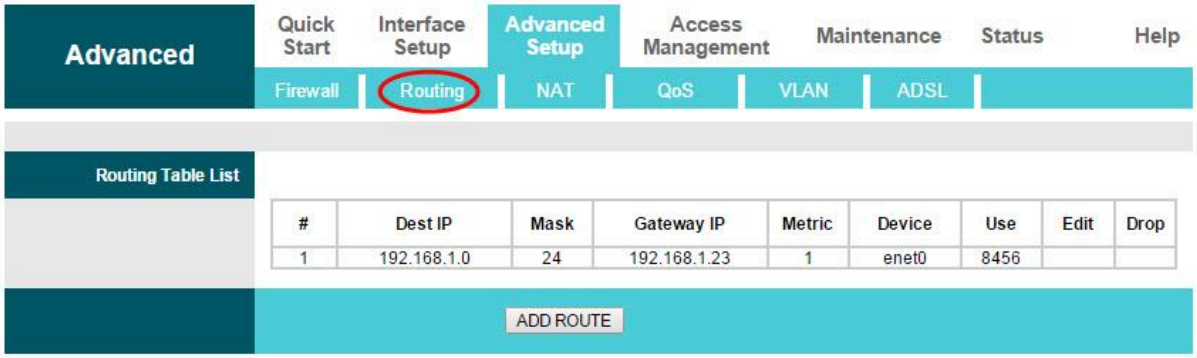
Go to Advanced Setup → Firewall, and you will see the following screen.



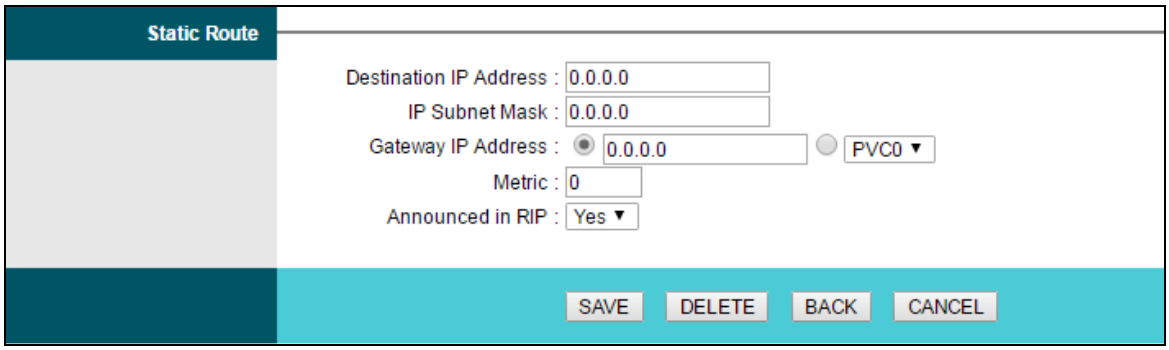
- **Firewall:** Select this option can automatically detect and block Denial of Service (DoS) attacks, such as Ping of Death, SYN Flood, Port Scan and Land Attack.
- **SPI:** If you enable SPI, all traffics initiated from WAN would be blocked, including DMZ, Virtual Server, and ACL WAN side.

4.3.2 Routing

Go to Advanced Setup → Routing, and you will see the routing information in the following screen.



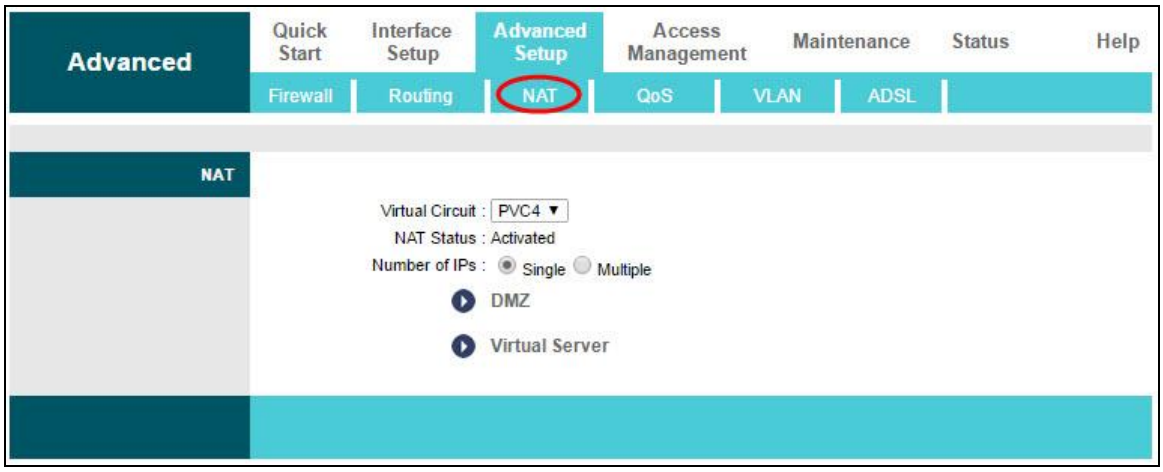
Click ADD ROUTE to add a new route in the following screen.



- **Destination IP Address:** This parameter specifies the IP network address of the final destination.
- **IP Subnet Mask:** Enter the subnet mask for this destination.
- **Gateway IP Address:** Enter the IP address of the gateway. The gateway is an immediate neighbor of your ADSL modem router that will forward the packet to the destination. On the LAN, the gateway must be a modem router on the same segment as your modem router; over Internet (WAN), the gateway must be the IP address of one of the remote nodes.
- **Metric:** Metric represents the "cost" of transmission for routing purposes. IP Routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not to be precise, but it must between 1 and 15. In practice, 2 or 3 is usually a good number.
- **Announced in RIP:** This parameter determines if the ADSL modem router will include the route to this remote node in its RIP broadcasts. If set to Yes, the route to this remote node will be propagated to other hosts through RIP broadcasts. If No, this route is kept private and is not included in RIP broadcasts.

4.3.3 NAT

Go to Advanced Setup → NAT, you can setup the NAT (Network Address Translation) function for the Modem router.



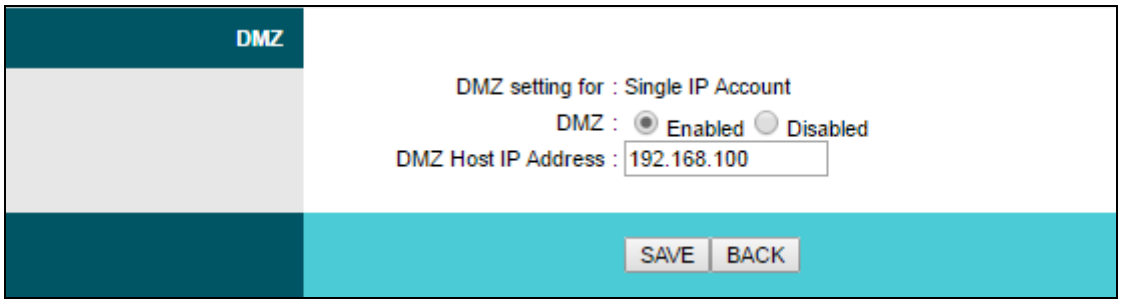
- **Virtual Circuit:** Enter Virtual Circuit Index that you plan to setup for the NAT function.
- **NAT Status:** This field shows the current status of the NAT function for the current VC. You can go to the previous screen to activate the function.

☞ Note:

For VCs with single IP, they share the same DMZ and Virtual servers; for VCs with multiple IPs, each VC can set DMZ and Virtual servers. Furthermore, for VCs with multiple IPs, they can define the Address Mapping rules; for VCs with single IP, since they have only one IP, there is no need to individually define the Address Mapping rule.

4.3.3.1 DMZ

Go to Advanced Setup → NAT → DMZ, you can configure the DMZ host in the following screen. A DMZ (demilitarized zone) is a host between a private local network and the outside public network. It prevents outside users from getting direct access to a server that has company data. Users of the public network outside the company can access to the DMZ host.

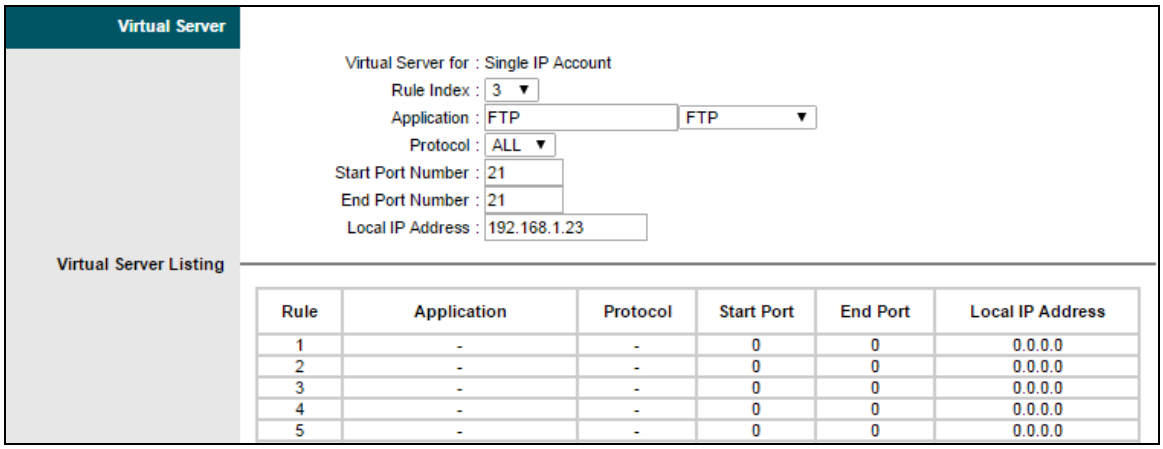


- **DMZ Host IP Address:** Enter the specified IP address for DMZ host on the LAN side.

4.3.3.2 Virtual Server

Go to Advanced Setup → NAT → Virtual Server, you can configure the Virtual Server in the following screen.

The Virtual Server is the server or server(s) behind NAT (on the LAN), for example, Web server or FTP server, which you can make visible to the outside world even though NAT makes your whole inside network appear as a single machine to the outside world.



- **Rule Index:** The Virtual server rule index for this VC. You can specify 10 rules in maximum. All the VCs with single IP will use the same Virtual Server rules.
- **Application:** The Virtual servers can be used for setting up public services on your LAN.
- **Protocol:** The protocol used for this application.
- **Start & End port number:** Enter the specific Start and End Port number you want to forward. If it is one port only, you can enter the End port number the same as Start port number. For example, if you want to set the FTP Virtual server, you can set the start and end port number to 21.
- **Local IP Address:** Enter the IP Address for the Virtual Server in LAN side.
- **Virtual Server Listing:** This displays the information about the Virtual Servers you establish.

To add a virtual server entry:

Step 1: Select Virtual Circuit and select Virtual Server.

Step 2: Select the Rule index for the rule.

Step 3: Select the application you want from drop-down list, then the protocol and port number will be added to the corresponding field automatically. You only need to configure the IP address for the virtual server. If the application list does not contain the service that you want, please configure the Port number, IP Address and Protocol manually.

Step 4: After that, click SAVE to make the entry take effect.

☞ Note:

For VCs with single IP, select Single; For VCs with multiple IPs, select Multiple for the option.

Other operations for the entries:

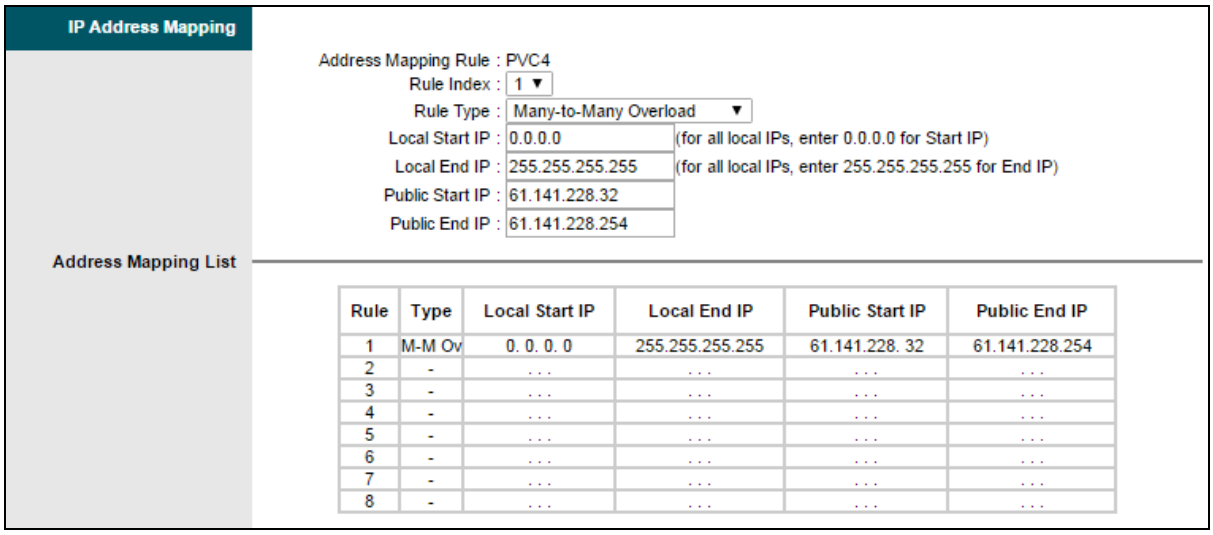
Enter the index of assigned entry, and click DELETE to delete the entry.

Click BACK to return to the previous screen.

Click CANCEL to cancel the configuration which is made just now.

4.3.3.3 IP Address Mapping

Select Multiple for numbers of IPs, and go to Advanced Setup → NAT → IP Address Mapping (for Multiple IP Service). You can configure the Address Mapping Rule in the following screen. The IP Address Mapping is for those VCs that configured with multiple IPs. The IP Address Mapping rule is per-VC based (only for Multiple IPs' VCs).



- **Rule Index:** Select the Virtual server rule index for this VC. You can specify 8 rules in maximum.
- **Rule Type:** There are four types: one-to-one, Many-to-One, Many-to-Many Overload and Many-to-Many No-overload.
- **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.
- **Public Start & End IP:** Enter the public IP Address you want to do NAT. Public Start IP is the starting public IP address and Public End IP is the ending public IP address. If you have a dynamic IP, enter 0.0.0.0 as the Public Start IP.
- **Address Mapping List:** This displays the information about the Mapping addresses.

To add a mapping rule:

Step 1: Select Virtual Circuit and Multiple for Number of IPs. Then select the tab IP Address Mapping.

Step 2: Select Rule Index for the rule.

Step 3: Select Rule Type you want from the drop-down list.

Step 4: Enter the local and public IP addresses in the corresponding fields.

Step 5: After that, click SAVE to make the entry take effect.

☞ Note:

IP Address Mapping is only available for VCs with Multiple IPs.

Other operations for the entries:

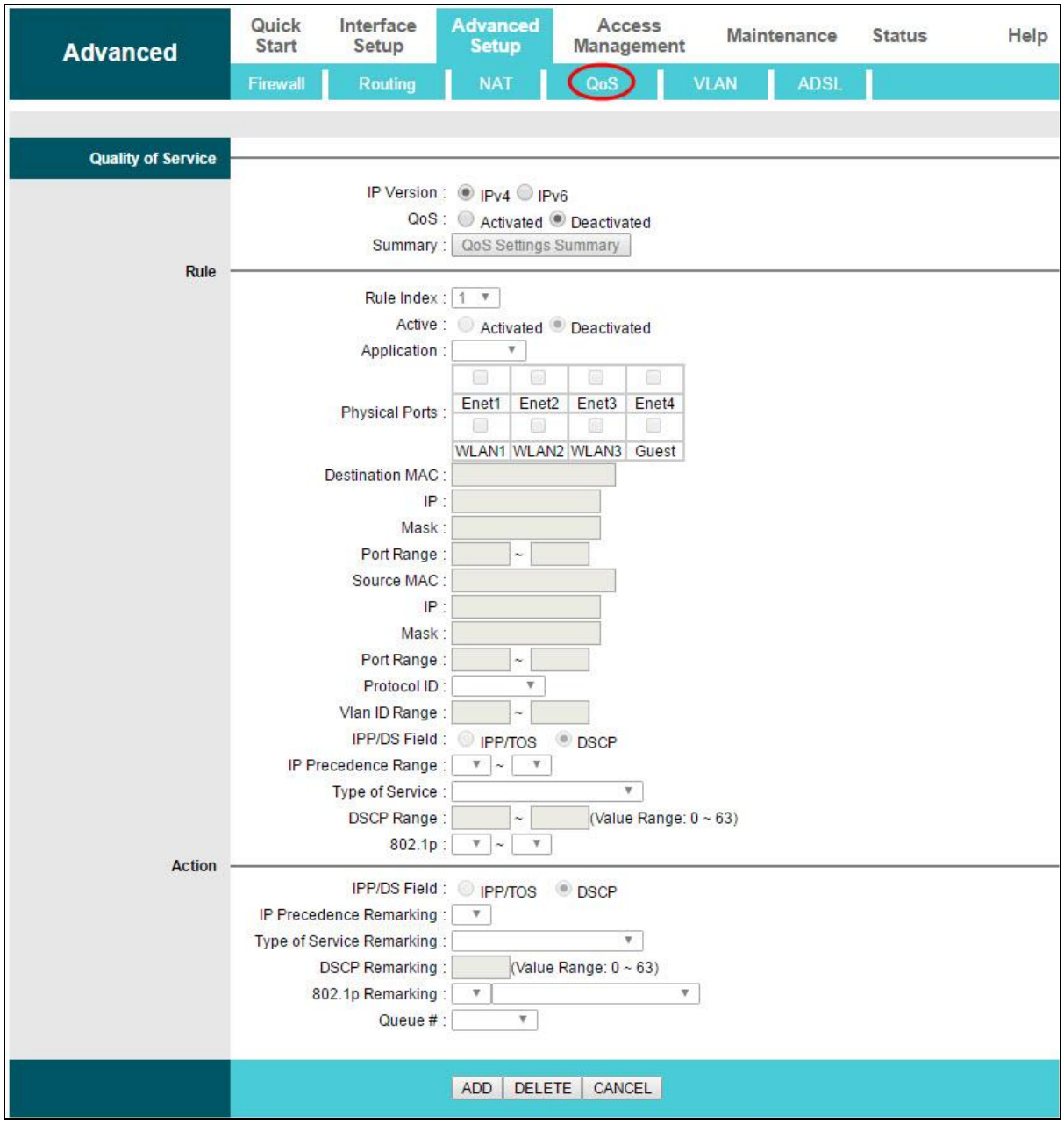
Select the index of assigned entry, and click DELETE to delete the entry.

Click BACK to return to the previous screen.

Click CANCEL to cancel the configuration which is made just now.

4.3.4 QoS

Go to Advanced Setup → QoS, you can configure the QoS in the following screen. QoS helps to prioritize data as it enters your modem router. By attaching special identification marks or headers to incoming packets, QoS determines which queue the packets enter, based priority. This is useful when there are certain types of data you want to give higher priority, such as voice data packets give higher priority than Web data packets. This option will provide better service of selected network traffic over various technologies.



- **IP Version：** Select your IP version.

- **QoS:** Select this option to Activate/Deactivate the IP QoS on different types (IP ToS and DiffServ).
- **Summary:** Click the button to view the configurations of QoS.

➢ **Rule:** Configure the rules for QoS. If the traffic complies with the rule, then the modem router will take the corresponding action to deal with it.

- **Rule Index:** Select the index for the rule you want to configure.
- **Active:** Activate the rule. The rule can take effect only when it is activated.
- **Application:** Select the application that the rule aimed at.
- **Physical Ports:** Select the port whose traffic flow are controlled by the rule.
- **Destination MAC & IP & Mask & Port Range:** Enter the IP information about the Destination host for the rule.
- **Source MAC & IP & Mask & Port Range:** Enter the IP information about the Source host for the rule.
- **Protocol ID:** Select one among TCP/UDP, TCP, UDP, ICMP or IGMP protocols for the application.
- **Vlan ID Range:** Enter the Vlan range, and the rule will be effective to the selected Vlans.
- **IPP/DS Field:** Select the type of the action to assign the priority.

When you select IPP/TOS, you can assign the priority via IP information. IP QoS function is intended to deliver guaranteed as well as differentiated Internet services by giving network resource and usage control to the Network operator.

- **IP Precedence Range:** Enter the IP precedence range that the modem router takes to differentiate the traffic.
- **Type of Service:** Select the type of service that the modem router takes to deal with the traffic.
- **802.1p:** Select the priority range for the rule.

When you select DSCP, you can assign the priority via DHCP (the header of IP group). It maps the IP group into corresponding service class.

- **DSCP Range:** Enter the DSCP range to differentiate the traffic.

➢ **Action:** Configure the action that the modem router takes to deal with the traffic which accord with the rule.

- **IPP/DS Field:** Select the type for the action.
- **IP Precedence Remarking:** Select the number to remark the priority for IP precedence.
- **Type of Service Remarking:** Select the type to remark the service.
- **DSCP Remarking:** Enter the number to remark the DSCP priority.
- **802.1p Remarking:** Select the type to remark the 802.1p priority.
- **Queue:** Select the priority type for the action.

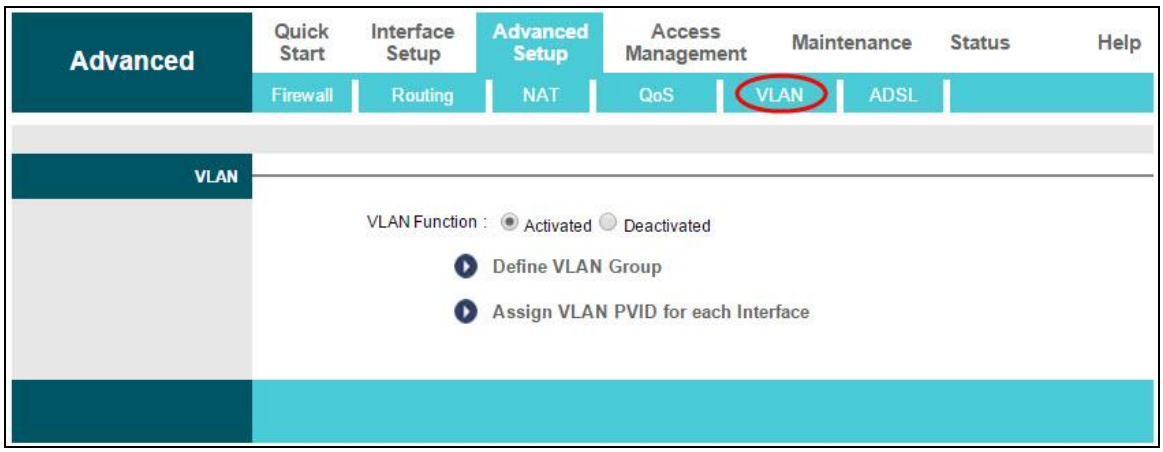
4.3.5 VLAN

Go to Advanced Setup → VLAN, you can activate the VLAN function in the following screen.

Virtual LAN (VLAN) is a group of devices on one or more LANs that are configured so that they can communicate as if they were attached to the same LAN, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, it is very flexible for user/host management, bandwidth allocation and resource optimization. There are two types of VLAN as follows:

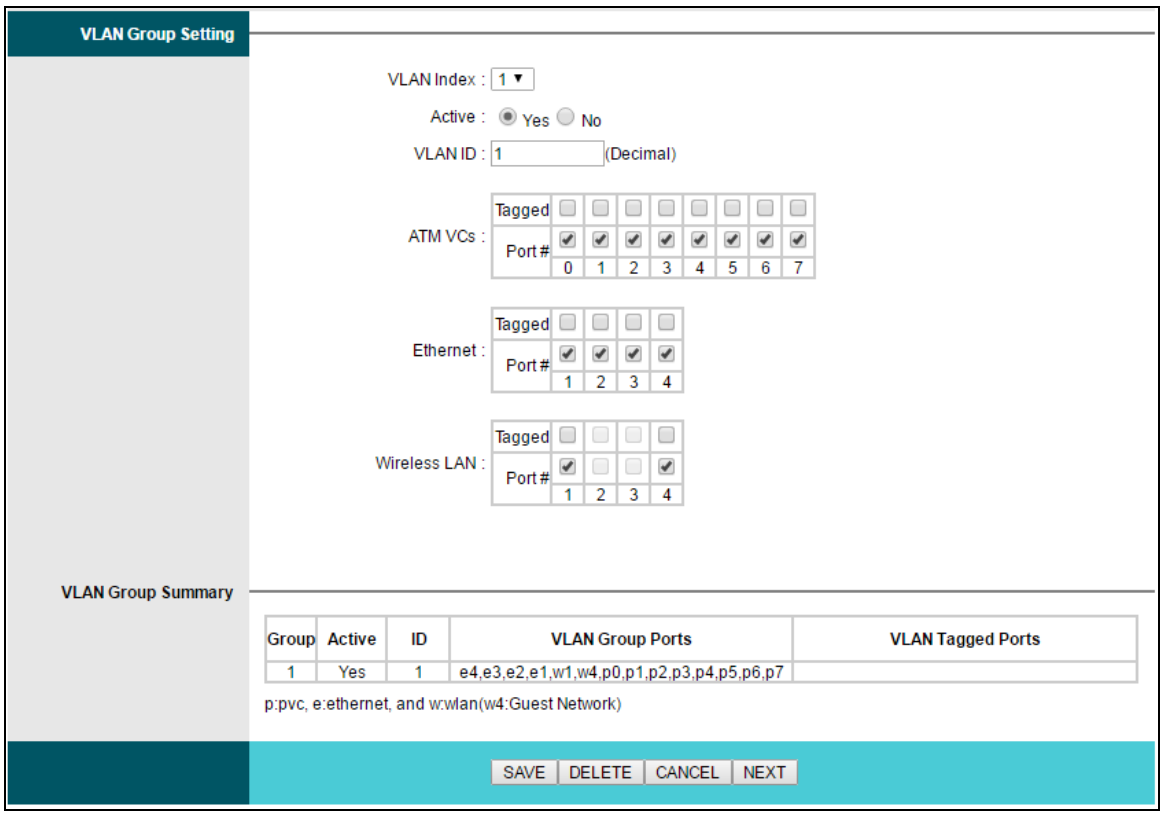
Port-Based VLAN: Each physical switch port is configured with an access list specifying membership in a set of VLANs.

ATM VLAN: Using LAN Emulation (LANE) protocol to map Ethernet packets into ATM cells and deliver them to their destination by converting an Ethernet MAC address into an ATM address.



1) Define VLAN Group

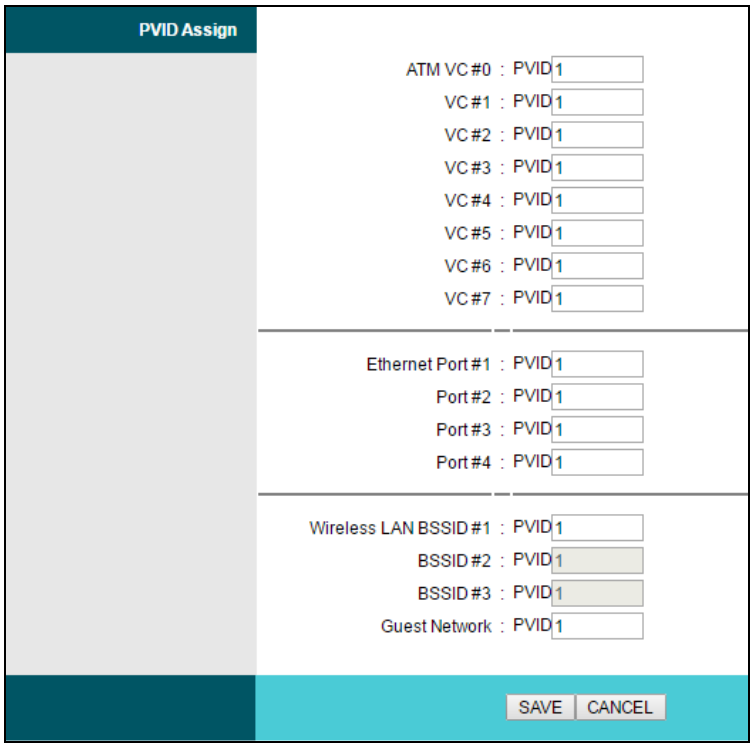
Click Define VLAN Group, you can define VLAN groups in the following screen.



- **VLAN Index:** Select VLAN Index for this VC. You can specify 8 groups in maximum.
- **VLAN ID:** This indicates the VLAN group.
- **ATM VCs:** Select ATM VCs as members of VLAN, and if you leave the Tagged blank, the tag in frames will be deleted when transmitted from the VC.
- **Ethernet:** Select the Ethernet port as a member of VLAN.
- **Wireless LAN:** Select the wireless LAN port as a member of VLAN, and if you leave the Tagged blank, the tag in frames will be deleted when transmitted from the port.
- **VLAN Group Summary:** This displays the information about the VLAN Groups.

2) Assign VLAN PVID for each Interface

Click Assign VLAN PVID for each Interface, you can assign the PVID for each interface in the following screen.



- **PVID:** Each physical port has a default VID called PVID (Port VID). PVID is assigned to untagged frames or priority tagged frames (frames with null (0) VID) received on this port.

4.3.6 ADSL

Go to Advanced Setup → ADSL, and you can select ADSL Mode and ADSL Type in the following screen. The ADSL feature can be selected when you meet the physical connection problem. Please check the proper settings with your ISP.

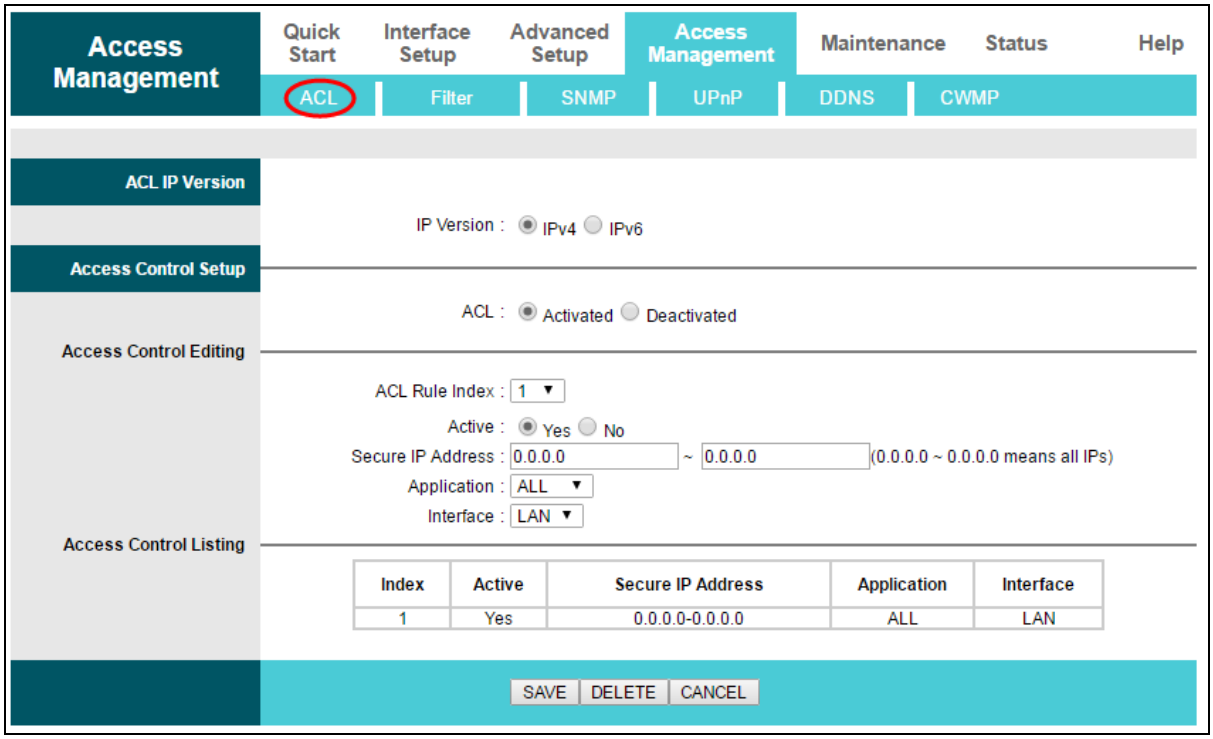
- **ADSL Mode:** Select the ADSL operation mode which your ADSL connection uses.
- **ADSL Type:** Select the ADSL operation type which your ADSL connection uses.

4.4 Access Management

Choose Access Management, and you will see the following submenus. Click any of them, and you can configure the corresponding function.

4.4.1 ACL

Go to Access Management → ACL, you will see the following screen. You can specify the client to access the ADSL modem router once setting his IP as a Secure IP Address through selected applications.



- **ACL:** If Activated, the IP addresses which are contained in the Access Control List can access to the modem router. If Deactivated, all IP addresses can access to the modem router.
- **ACL Rule Index:** Select the ACL rule index for the entry.
- **Active:** Select Yes to enable the ACL rule.
- **Secure IP Address:** Select the IP addresses which are permitted to access to the modem router remotely. With the default IP 0.0.0.0, any client would be allowed to remotely access the ADSL modem router.
- **Application:** Select the application for the ACL rule, and then you can access the modem router through it.
- **Interface:** Select the interface for access: LAN, WAN or Both.

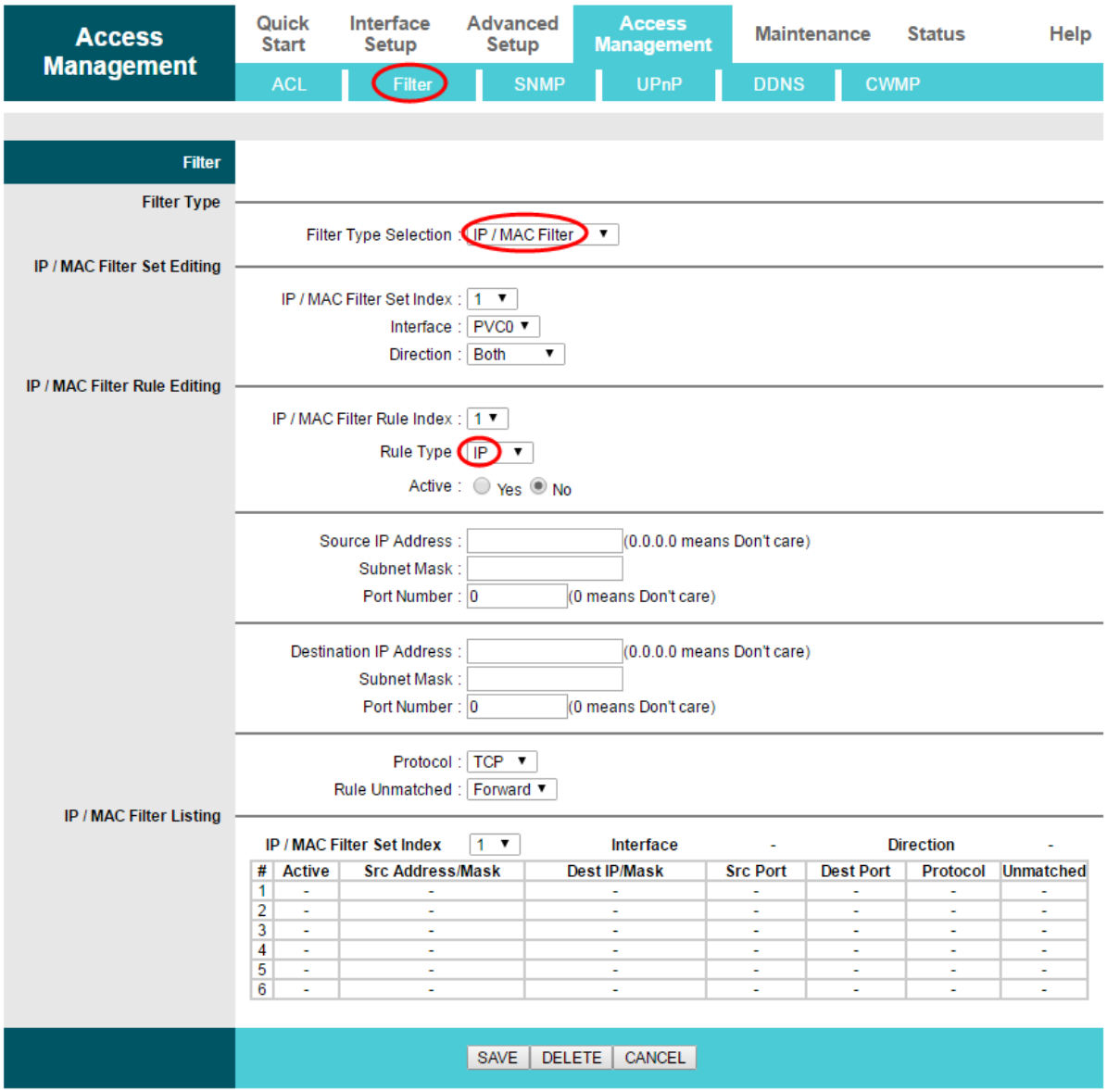
➢ **Access Control Listing:** This displays the information about the ACL Rules.

4.4.2 Filter

Go to Access Management → Filter, you will see the Filter screen (the default is IP/MAC Filter screen). The filtering feature includes IP/MAC Filter, Application Filter, and URL Filter. The feature makes it possible for administrators to control users' access to the Internet and protect the networks.

4.4.2.1 IP Filter

Select IP/MAC Filter as the Filter type, and select IP as the Rule type, then you can configure the filter rules based on IP address. The filtering includes Outgoing and Incoming, and the detailed descriptions are provided below.



➢ **Filter Type Selection:** Select the filter type for the configuration below.

- **IP/MAC Filter Set Index:** Select the Set index for the IP Filter entry. This index can match with six IP / MAC Filter Rule Indexes.
- **Interface:** Select the interface for the entry.

☞ Note:

If select PVC0~PVC7 as an interface, the filter will match the IP traffic of WAN port with specified IPs (Source IP Address and Destination IP Address). If select LAN as an interface, the filter will match the IP traffic of LAN port with specified IPs.

- **Direction:** Select the direction for this IP Filter rule. There are three filtering directions: Both, Incoming and Outgoing.

☞ Note:

Incoming means that IP traffic which is coming into the modem router, and the Outgoing means that IP traffic which is going out the modem router.

- **IP/MAC Filter Rule Index:** Select the Rule index for the IP Filter entry.

☞ Note:

You should set IP/MAC Filter Set Index and IP/MAC Filter Rule Index together to appoint the address (shown in the Filter List) for the IP Filter rule. For example, (1, 2), it means the rule will be shown in the row 2 IP/MAC Filter Set Index 1.

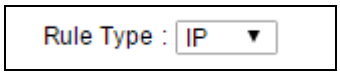
- **Rule Type:** For IP Filter, please select IP here.
- **Active:** Select Yes to make the rule to take effect.
- **Source IP Address:** Enter the source IP address for the rule. You can enter 0.0.0.0; it means that all IP addresses are controlled by the rule.
- **Destination IP Address:** Enter the destination IP address for the rule. You can enter 0.0.0.0, which means that all IP addresses are controlled by the rule. The set of Subnet Mask and Port Number are same as Source IP Address.
- **Subnet Mask:** Enter the Subnet Mask for the rule.
- **Port Number:** Enter the Port Number for the rule. You can enter 0, which means that all ports are controlled by the rule.
- **Protocol:** Select the protocol: TCP, UDP or ICMP for the filter rule.
- **Rule Unmatched:** If the current rule can not match, and you select Forward, the modem router will skip the rule and transmit directly. If you select Next, the modem router will find the next filter rule (show in Filter list) to match.
- **IP/MAC Filter Listing:** This displays the information about the IP Filter rules.

To add an IP Address filtering entry:

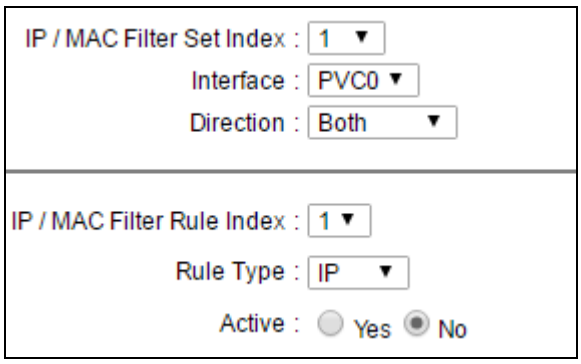
For example: If you desire to block E-mail received and sent by the IP address 192.168.1.7 on your local network and wish to make the PCs with IP address 192.168.1.8 unable to visit the website of IP address 202.96.134.12, while other PCs have no limit, you can configure the rules as follows. Presume the rules are both aimed at the interface PVC0, and their indexes are (1, 1), (1, 2) and (1, 3).

Step 1: Select IP/MAC Filter as the Filter Type Selection.

Select IP as the Rule Type on the Filter screen, then you can configure the specific rule for the example.



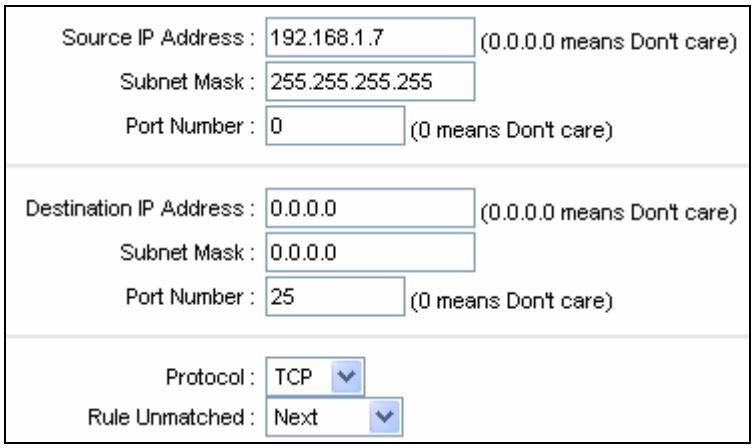
Step 2: Select IP/MAC Filter Set Index and IP/MAC Filter Rule Index for the rule, then select the Interface PVC0, and select the Direction Both for the first rule.



☞ Note:

If you want to make the rule take effect, please select Yes to active the rule.

Step 3: Enter the Source IP Address, Destination IP Address, Subnet Mask and Port Number in the corresponding field.



Step 4: Select the Protocol as TCP and select the Unmatched rule as Next.

Step 5: Finally, click SAVE to save the entry.

Step 6: Go to Step 2 to configure the next two rules: Block E-mail received by the IP address 192.168.1.7 on your local network; Make the PC with IP address 192.168.1.8 unable to visit the website of IP address 202.96.134.12.

☞ Note:

After you complete the IP filter rules for the example, the Filter list will show as follows. You can enter the IP / MAC Filter Set Index to view the information about the rule.

#	Active	Src Address/Mask	Dest IP/Mask	Src Port	Dest Port	Protocol	Unmatched
1	Yes	192.168.1.7/ 255.255.255.255	0.0.0.0/ 0.0.0.0	0	25	TCP	Next
2	Yes	192.168.1.7/ 255.255.255.255	0.0.0.0/ 0.0.0.0	0	110	TCP	Forward
3	Yes	192.168.1.8/ 255.255.255.255	202.96.134.12/ 255.255.255.255	0	0	TCP	Forward

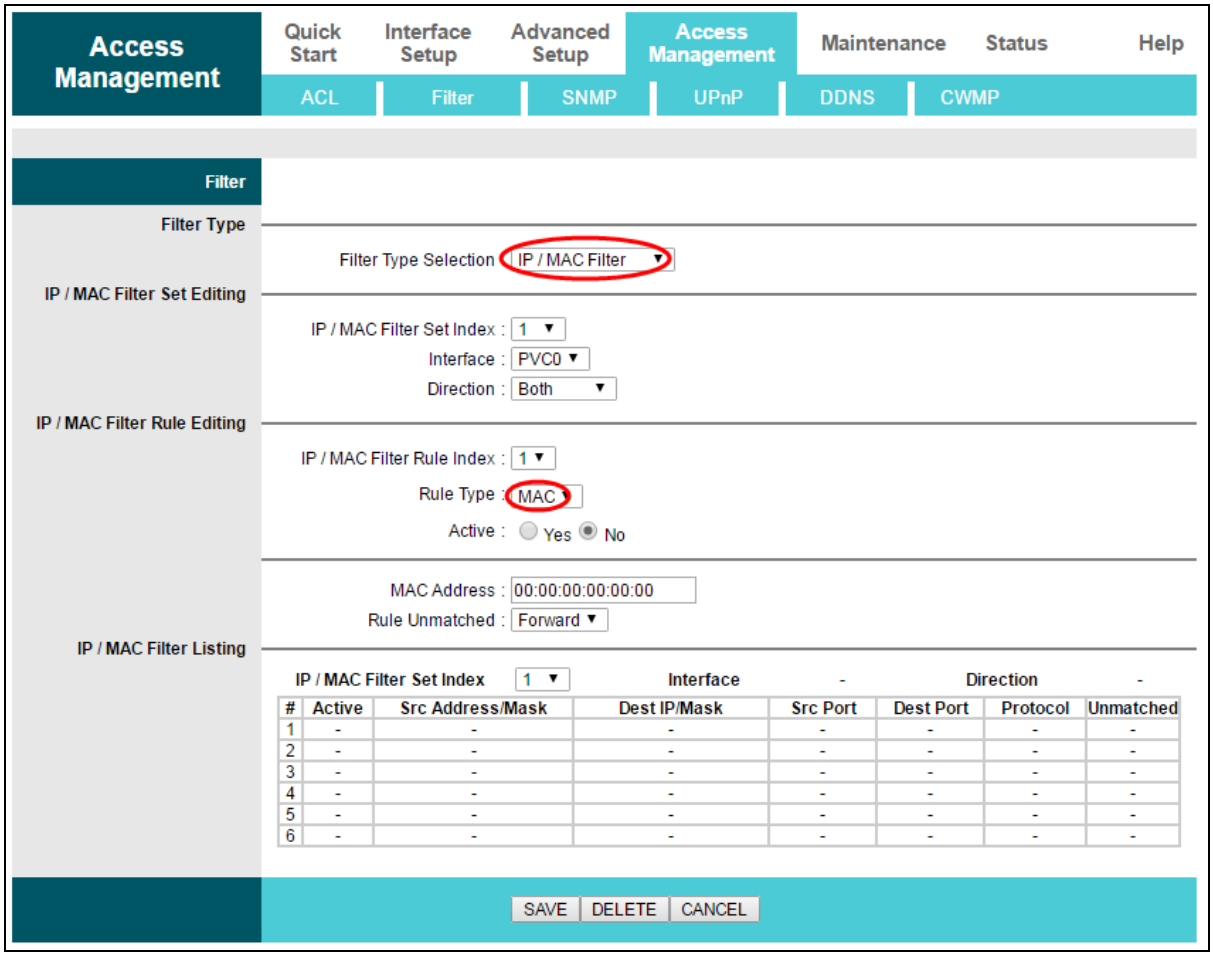
Other operations for the entries:

Select IP/MAC Filter Set Index and IP/MAC Filter Rule Index to view or modify the entry.

Select IP/MAC Filter Set Index and IP/MAC Filter Rule Index to locate the specific rule, and then click DELETE to delete the entry.

4.4.2.2 MAC Filter

Select IP/MAC Filter as the Filter type, and select MAC as the Rule type, and then you can configure the filter rules based on MAC address.



- **Rule Type:** Select MAC for the MAC Filter rule.
- **Active:** Select Yes to make the rule to take effect.
- **MAC Address:** Enter the MAC address for the rule.

- **Rule Unmatched:** If the current rule can not match, and you select Forward, the modem router will skip the rule and transmit directly. If you select Next, the modem router will find the next filter rule (show in Filter list) to match.
- **IP/MAC Filter Listing:** This displays the information about the MAC Filter rules.

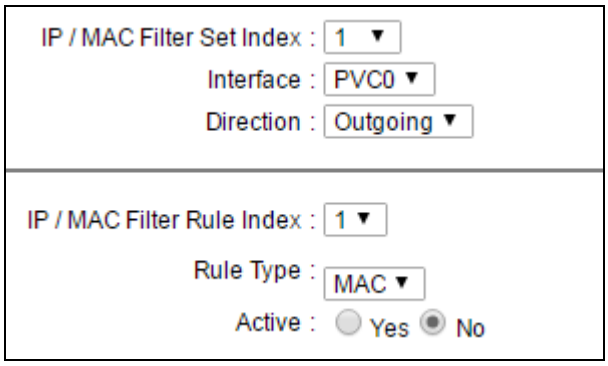
To add a MAC Address filtering entry:

For example: If you want to block the PCs with MAC addresses 00:0A:EB:00:07:BE and 00:0A:EB:00:07:5F to access the Internet, you can configure as follows. Presume the rules are both aimed at the interface PVC0, and their indexes are (1, 1) and (1, 2).

Step 1: Select IP/MAC Filter as the Filter Type Selection.

Select the MAC as the Rule Type on the Filter screen, then you can configure the specific rule for the example.

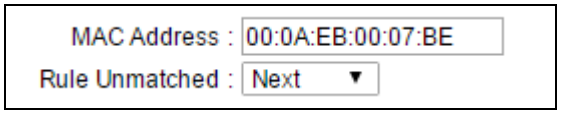
Step 2: Select the IP/MAC Filter Set Index and IP/MAC Filter Rule Index for the rule, then select the Interface PVC0, and select the Direction Outgoing for the first rule.



☞ Note:

If you want to make the rule take effect, please select Yes to active the rule.

Step 3: Enter the MAC Address and select the Unmatched rule as Next.



Step 4: Finally, click SAVE to save the entry.

Step 5: Go to Step 2 to configure the next rule: Block the PC with MAC address 00:0A:EB:00:07:BE to access the Internet.

☞ Note:

After you complete the MAC filter rules for the example, the Filter list will show as follows. You can enter the IP / MAC Filter Set Index to view the information about the rule.

#	Active	Src Address/Mask	Dest IP/Mask	Src Port	Dest Port	Protocol	Unmatched
1	Yes	00:0a:eb:00:07:be	-	-	-	-	Next
2	Yes	00:0a:eb:00:07:5f	-	-	-	-	Forward

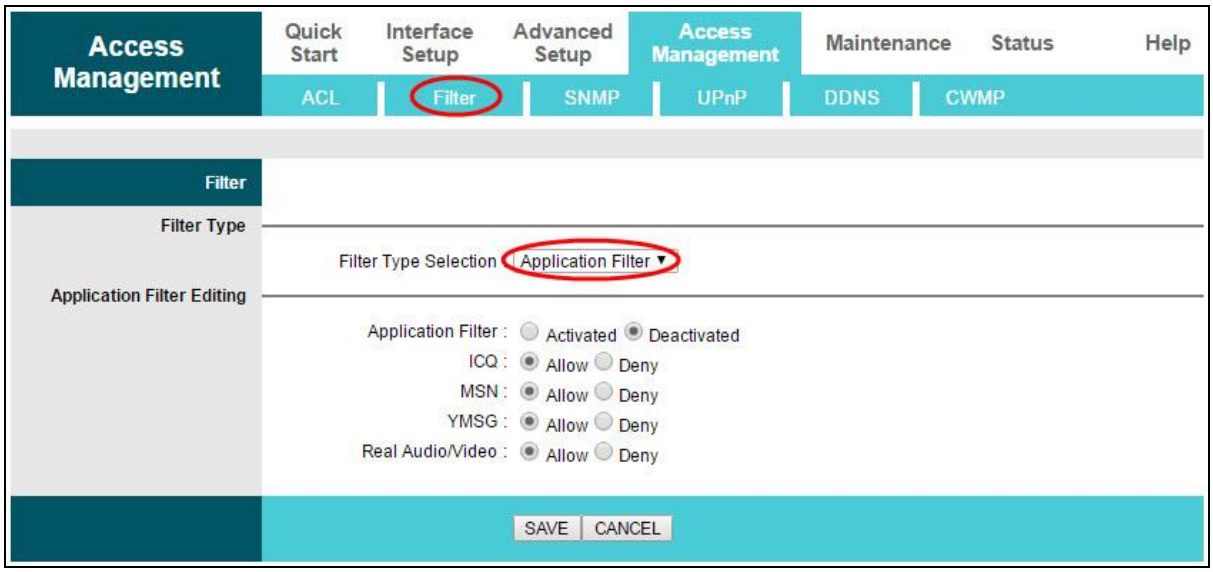
Other operations for the entries:

Select IP / MAC Filter Set Index and IP/MAC Filter Rule Index to view or modify the entry.

Select IP / MAC Filter Set Index and IP/MAC Filter Rule Index to locate the specific rule, and then click DELETE to delete the entry.

4.4.2.3 Application Filter

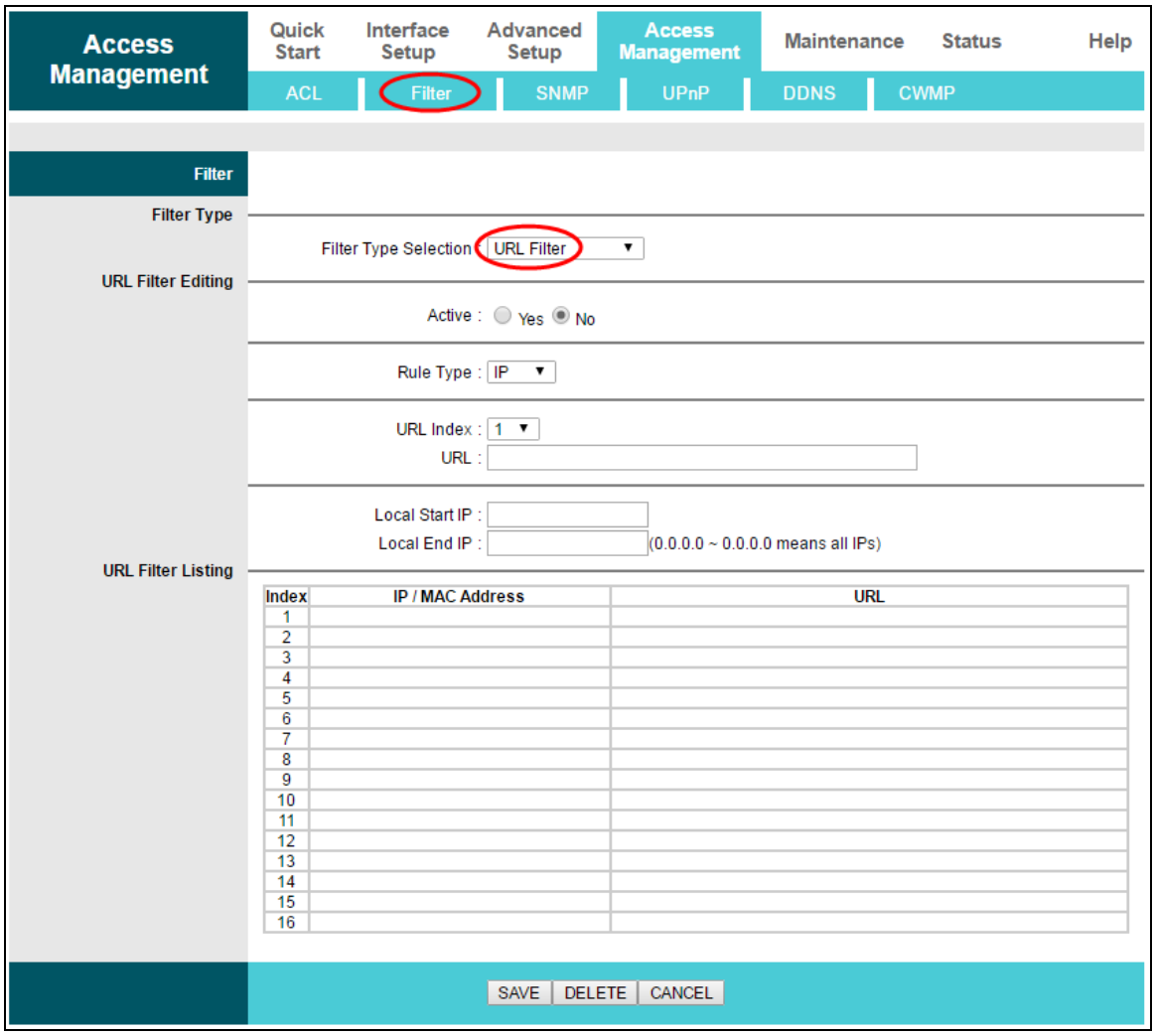
Select Application Filter as the Filter type, and then you can configure the filter rules based on application.



- **Filter Type Selection:** Select the Application Filter for the next configuration.
- **Application Filter:** Activate or deactivate the function.
- **ICQ & MSN & YMSG & Real Audio/Video:** Select Allow or Deny for these applications. If you select Allow, the modem router will accept the application; if you select Deny, the modem router will forbid the application.

4.4.2.4 URL Filter

Select URL Filter as the Filter type, and then you can configure the filter rules based on URL.



- **Filter Type Selection:** Select the URL Filter for the next configuration.
- **Active:** Select Yes to make the rule to take effect.
- **URL Index:** Select the index for the URL Filter entry.
- **URL:** Enter the URL for this URL Filter.
- **URL Filter Listing:** This displays the information about the URL Filter rules.

To add a URL filter entry:

For example: If you want to forbid the user to access the website: www.yahoo.com. Presume the rule is aimed at the interface PVC0, and its index is 1.

Step 1: Select URL Filter as the Filter Type Selection.

Step 2: Select Index for the rule, and then enter the website in the URL field.

Step 3: Finally, select Yes to active the rule, and then click SAVE to save the entry.

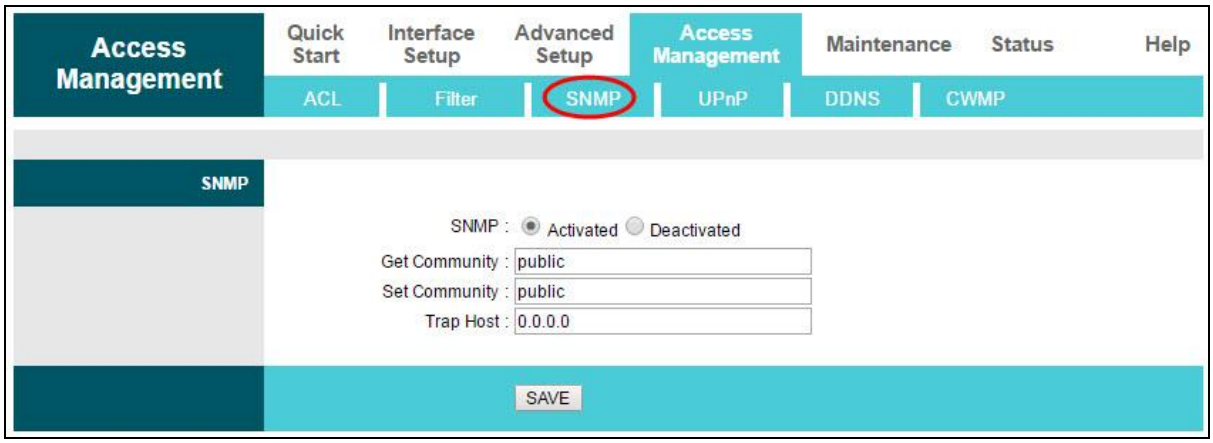
Other operations for the entries:

Select URL Index to view or modify the entry.

Select URL Index to locate the specific rule, and then click DELETE to delete the entry.

4.4.3 SNMP

Go to Access Management → SNMP, you will see the SNMP screen. The Simple Network Management Protocol (SNMP) is used for exchanging information between network devices.

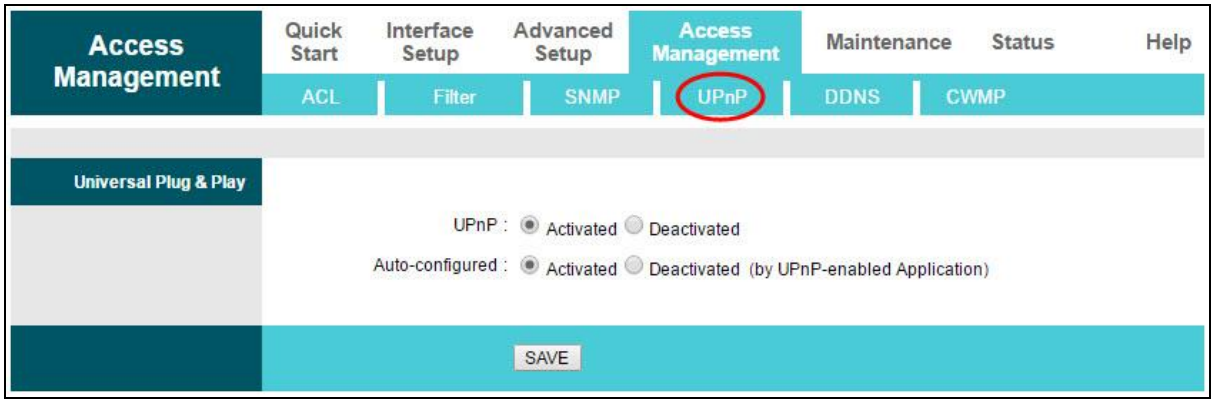


- **Get Community:** Set the password for the incoming Get and Get next requests from the management station.
- **Set Community:** Set the password for incoming Set requests from the management station.

4.4.4 UPnP

Go to Access Management → UPnP, you can configure the UPnP in the screen.

UPnP (Universal Plug and Play) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. An UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use. UPnP broadcasts are only allowed on the LAN.

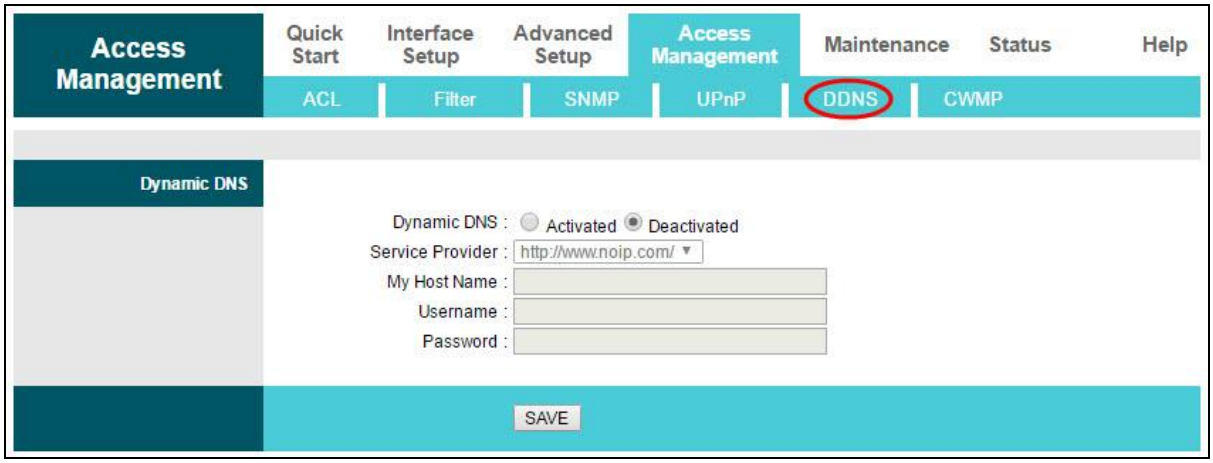


- **UPnP:** Activate or deactivate the UPnP function. Only when the function is activated can the UPnP take effect.
- **Auto-configured:** If you activate the function, the UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions.

4.4.5 DDNS

Go to Access Management → DDNS, you can configure the DDNS function in the screen.

The modem router offers a Dynamic Domain Name System (DDNS) feature. The feature lets you use a static host name with a dynamic IP address. User should type the host name, username and password assigned to your ADSL modem router by your Dynamic DNS provider.

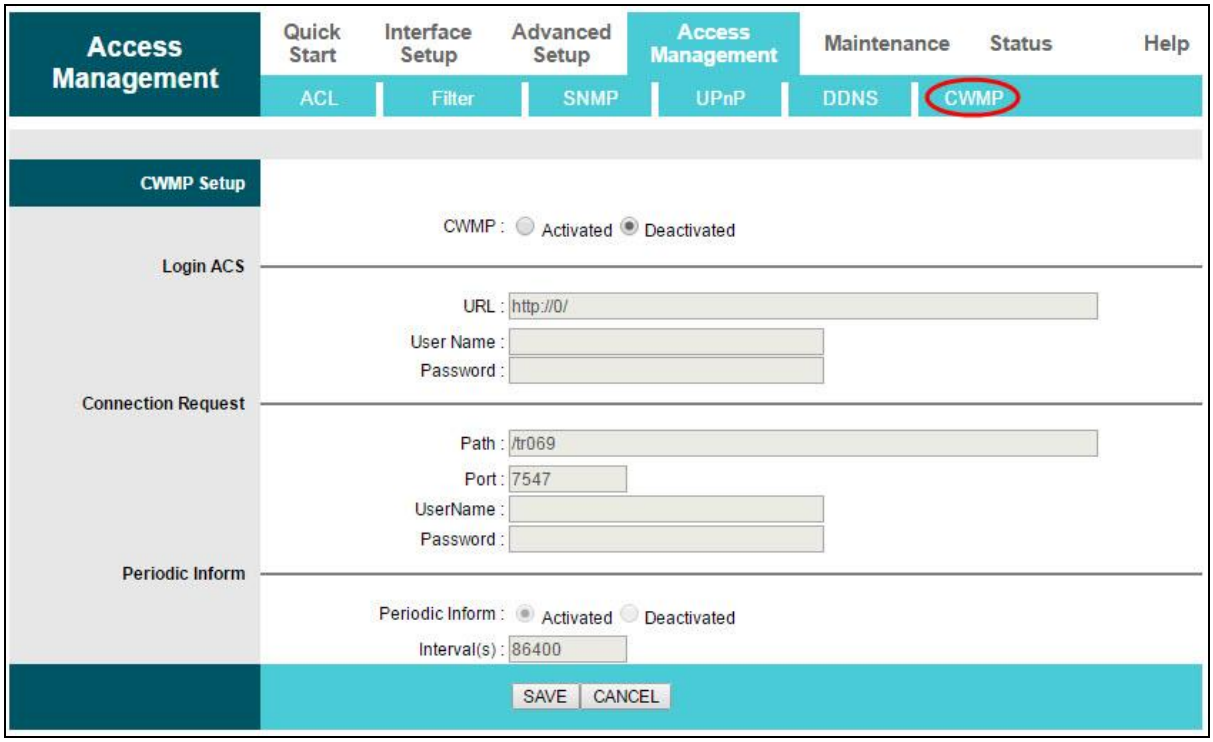


- **Dynamic DNS:** Activate the DDNS function or not.
- **Service Provider:** This field displays the service provider of DDNS.
- **My Host Name:** Enter your host name here.
- **Username & Password:** Type the Username and Password for your DDNS account.

4.4.6 CWMP

Go to Access Management → CWMP, you can configure the CWMP function in the screen.

The modem router offers CWMP feature. The function supports TR-069 protocol which collects information, diagnoses the devices and configures the devices automatically via ACS (Auto-Configuration Server).



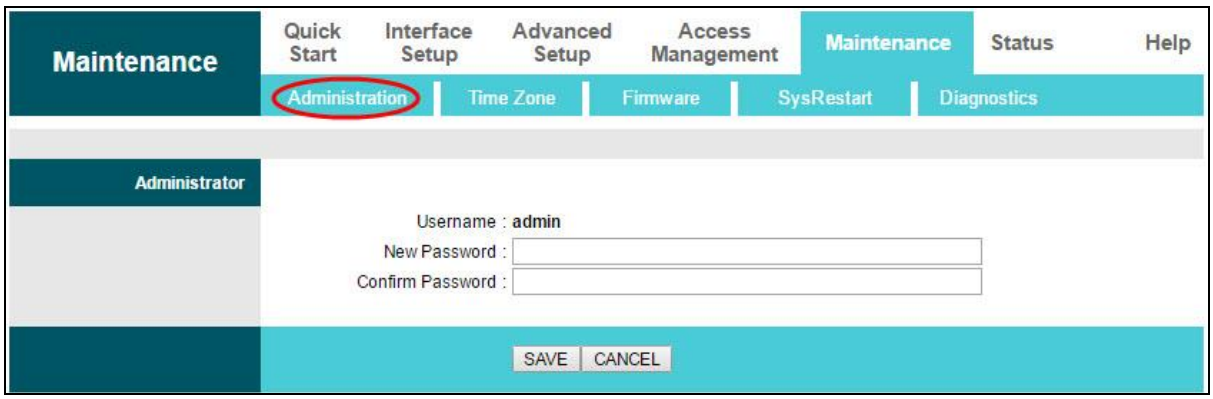
- **CWMP:** Activate the CWMP function or not.
- **URL:** Enter the website of ACS which is provided by your ISP.
- **User Name/Password:** Enter the username and password to login the ACS server.
- **Path:** Enter the path that connects to the ACS server.
- **Port:** Enter the port that connects to the ACS server.
- **UserName/Password:** Enter the username and password that provided the ACS server to login the modem router.
- **Periodic Inform:** Activate or deactivate the function. If activated, the information will be informed to ACS server periodically.
- **Interval:** Enter the interval time here.

4.5 Maintenance

Choose Maintenance, and you will see the following submenus. Click any of them, and you can configure the corresponding function.

4.5.1 Administration

Go to Maintenance → Administration, and you can set new password for admin in the screen.



☞ Note:

1) There is only one account that can access web management page. The default account is admin, and the password is admin. Admin has read/write access privilege.
2) When you change the password, you should enter the new password twice, and then click SAVE to make the new password take effect.

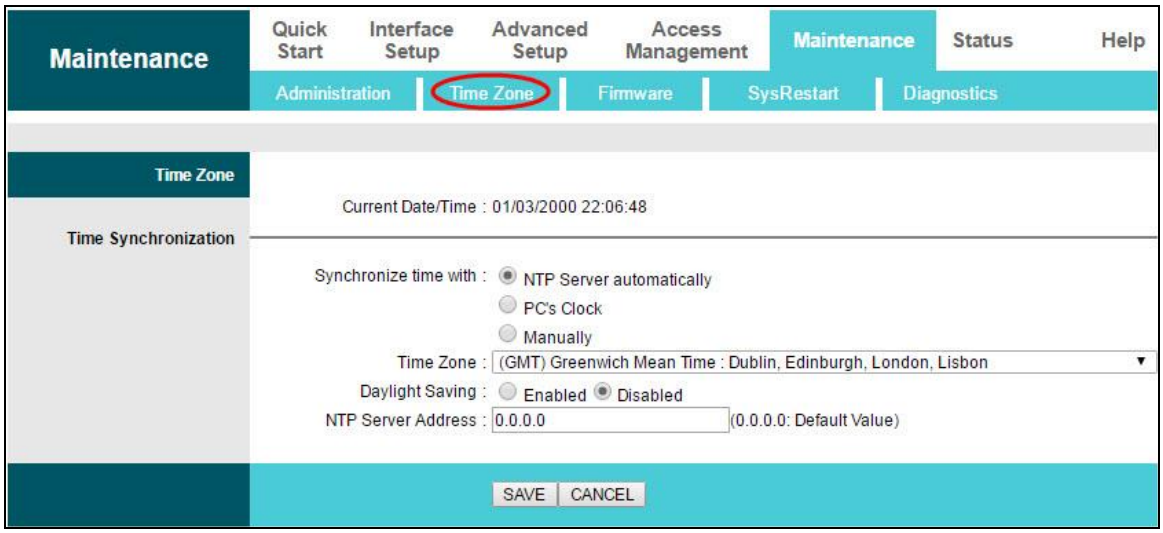
4.5.2 Time Zone

Go to Maintenance → Time Zone, and you can configure the system time in the screen.

The system time is the time used by the device for scheduling services. There are three methods to configure the time. You can manually set the time or connect to a NTP (Network Time Protocol) server. If a NTP server is set, you will only need to set the time zone. If you manually set the time, you may also set Daylight Saving dates and the system time will automatically adjust on those dates.

1) NTP Server automatically

Select NTP Server automatically as the Synchronize time, then you only need to set the time zone.

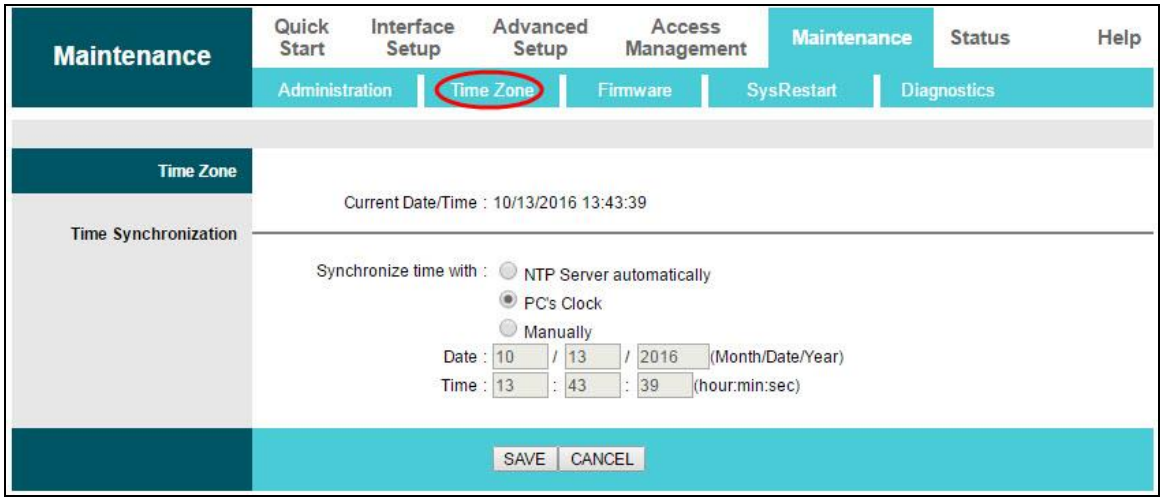


☞ Note:

The ADSL modem router is built-in some NTP Servers. When the modem router connects to the Internet, the modem router will get the system time automatically from the NTP Server. You can also configure the NTP Server address manually, and then the modem router will get the time from the specific Server firstly.

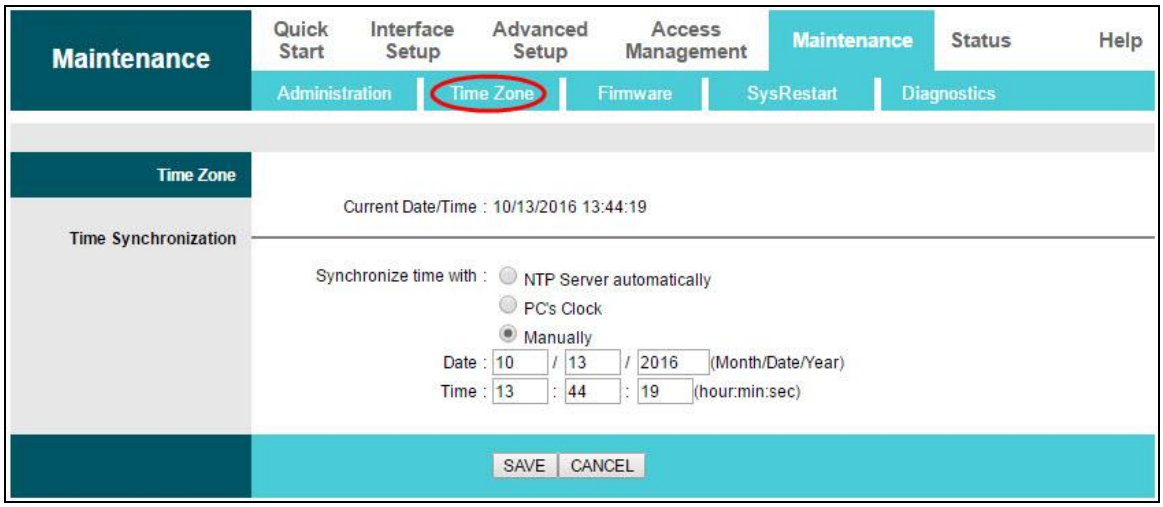
2) PC's Clock

Select PC's Clock as the Synchronize time, and you don't need to set any items.



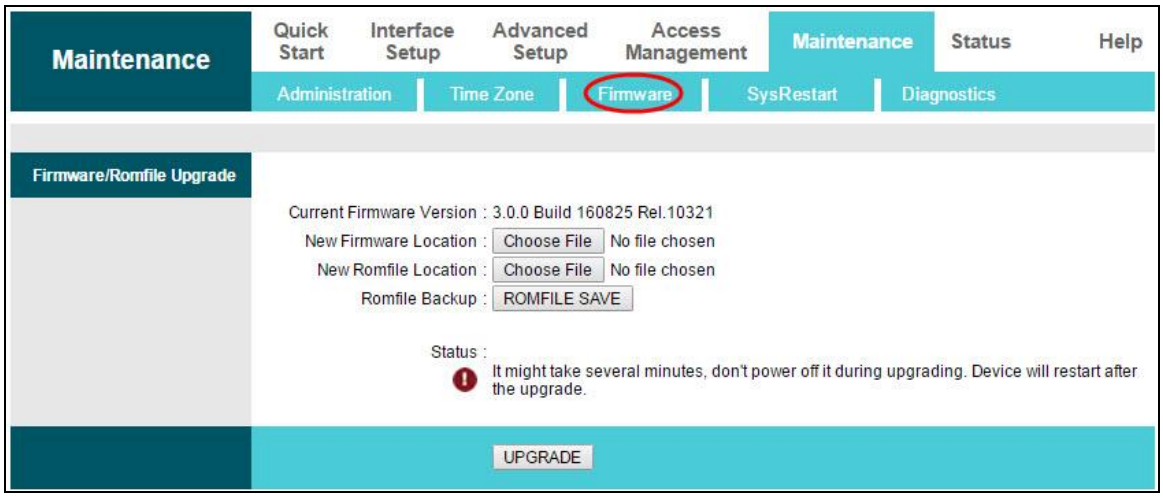
3) Manually

Select Manually as the Synchronize time, and you need to set the date and time corresponding to the current time.



4.5.3 Firmware

Go to Maintenance → Firmware, and you can upgrade the firmware of the modem router in the screen. Make sure the firmware or romfile you want to use is on the local hard drive of the computer. Click Choose File to find the local hard drive and locate the firmware or romfile to be used for upgrade.



To upgrade the modem router's firmware, follow these instructions below:

Step 1: Click Choose File of New Firmware Location to locate the update file.

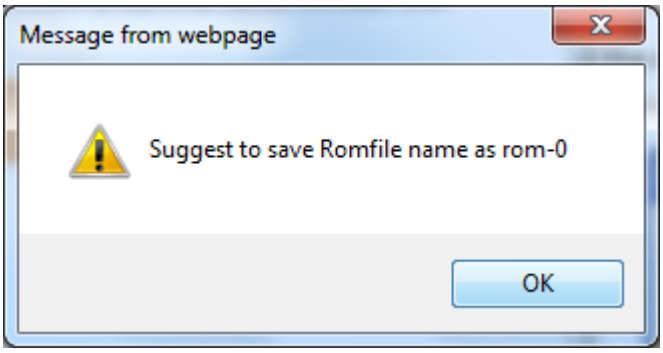
Step 2: Click UPGRADE.

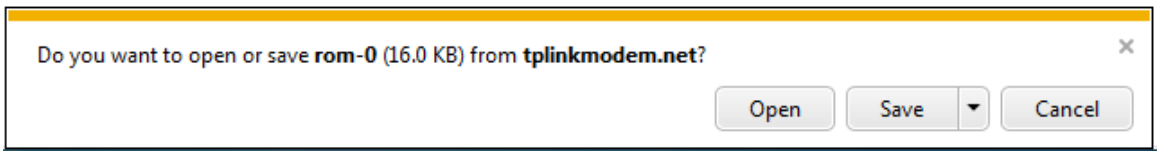
☞ Note:

1) When you upgrade the modem router's firmware, you may lose its current configurations, so please back up the modem router's current settings before you upgrade its firmware.
2) Do not turn off the modem router or press the WPS/Reset button while the firmware is being upgraded.
3) The modem router will reboot after the upgrading has been finished.

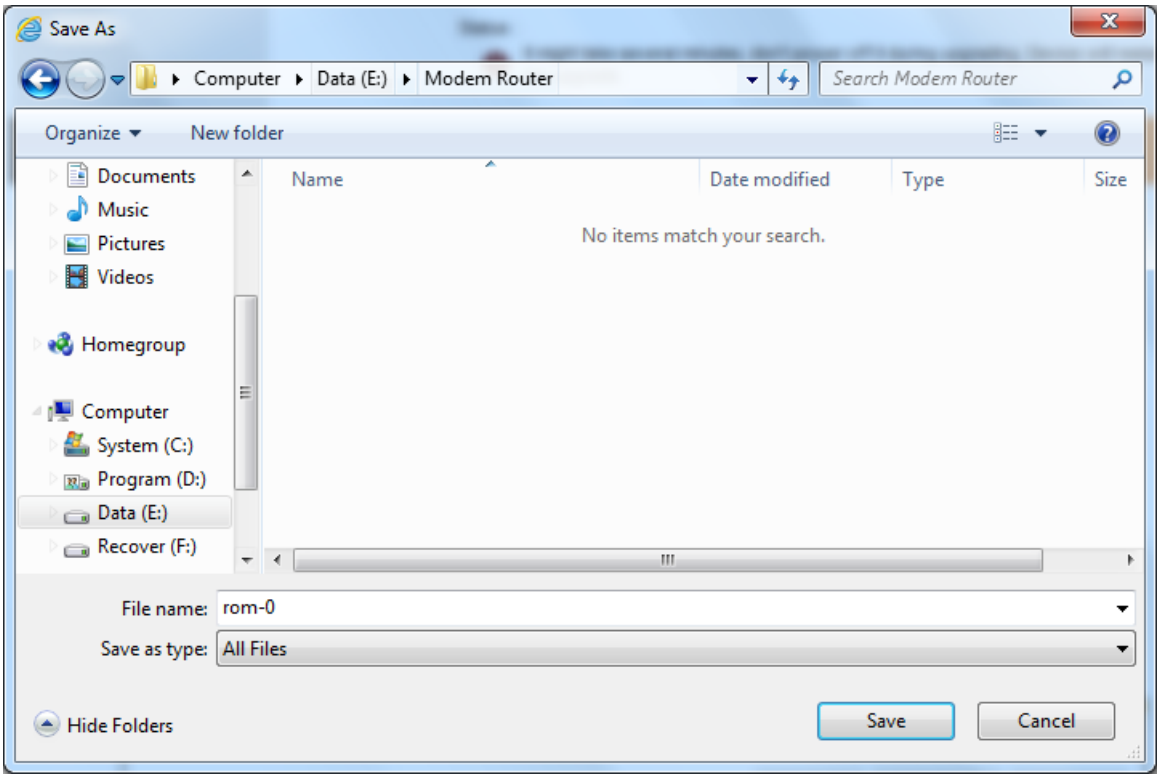
To back up the modem router's current settings:

Step 1: Click ROMFILE SAVE, click OK and then click Save in the following screens to proceed.





Step 2: Save the file as the appointed file.



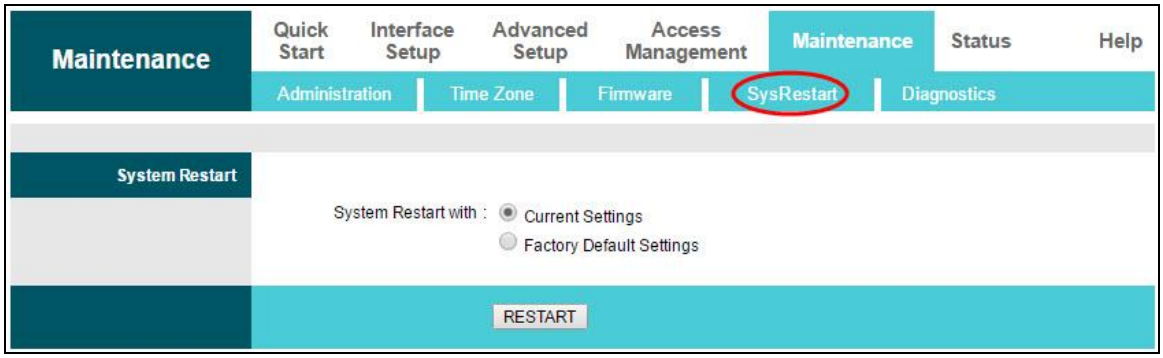
To restore the modem router's settings:

Step 1: Click Choose File of New Roomfile Location to locate the update file for the device.

Step 2: Click UPGRADE to complete.

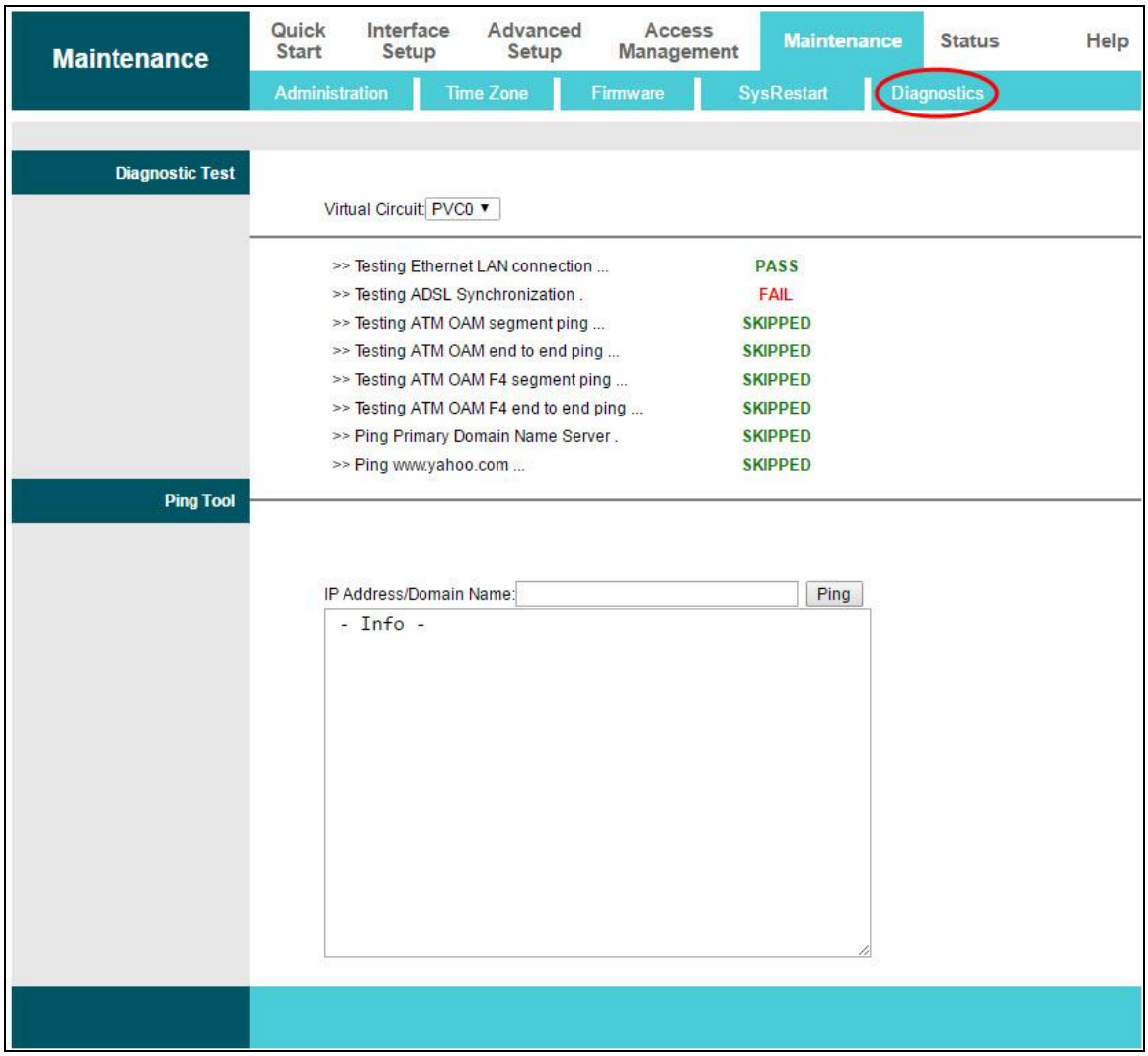
4.5.4 SysRestart

Go to Maintenance → SysRestart, and you can select to restart the device with current settings or restore to factory default settings in the screen.



4.5.5 Diagnostics

Go to Maintenance → Diagnostics, and you can view the test results for the connectivity of the physical layer and protocol layer for both LAN and WAN sides in the screen.



4.6 Help

Choose Help, and you can view the help information for configuration of any function.

☞ Note:

Click the tab, and you can get the corresponding information.

Appendix A: Configuring the PC

We'll introduce how to install and configure the TCP/IP correctly on your computer. First make sure your Ethernet Adapter is working, refer to the adapter's manual if necessary.

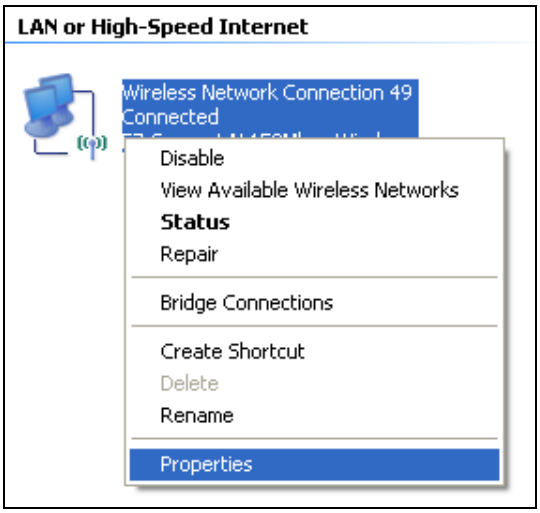
The default IP address of the modem router is 192.168.1.1. And the default Subnet Mask is 255.255.255.0. These values can be changed as you desire. Here we use all the default values for description and take Windows XP as example.

1. Configure TCP/IP component

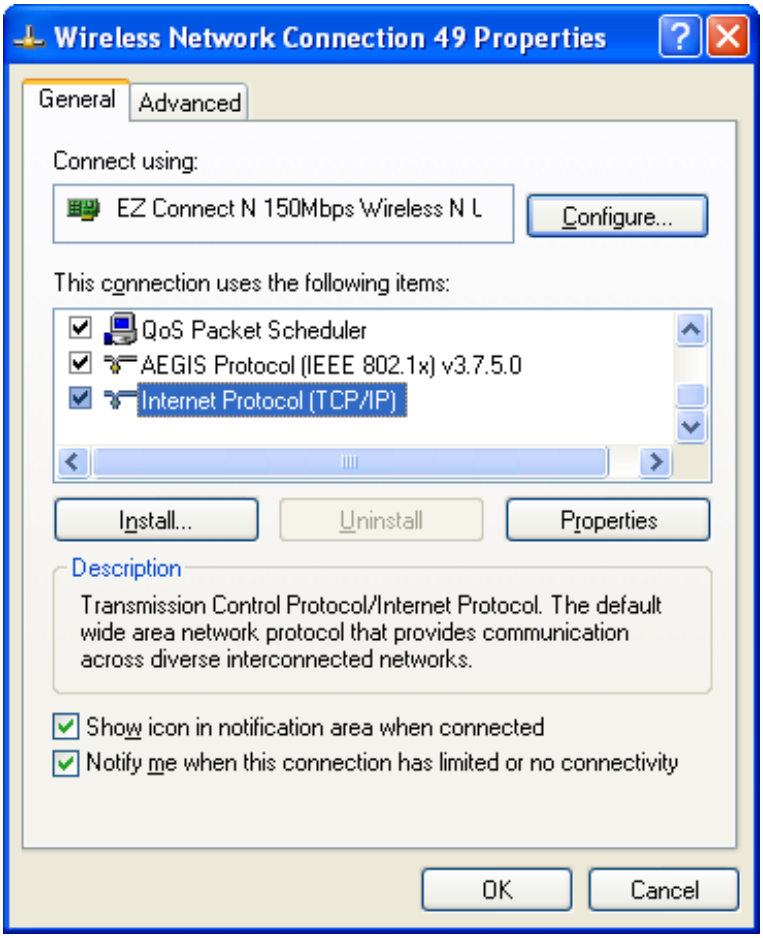
1) On the Windows taskbar, click Start, and then click Control Panel.

2) Click the Network and Internet Connections icon, and then click on the Network Connections tab in the appearing window.

3) Right click the icon that showed below, then select Properties on the prompt page.



4) In the prompt page that showed below, double click on the Internet Protocol (TCP/IP).

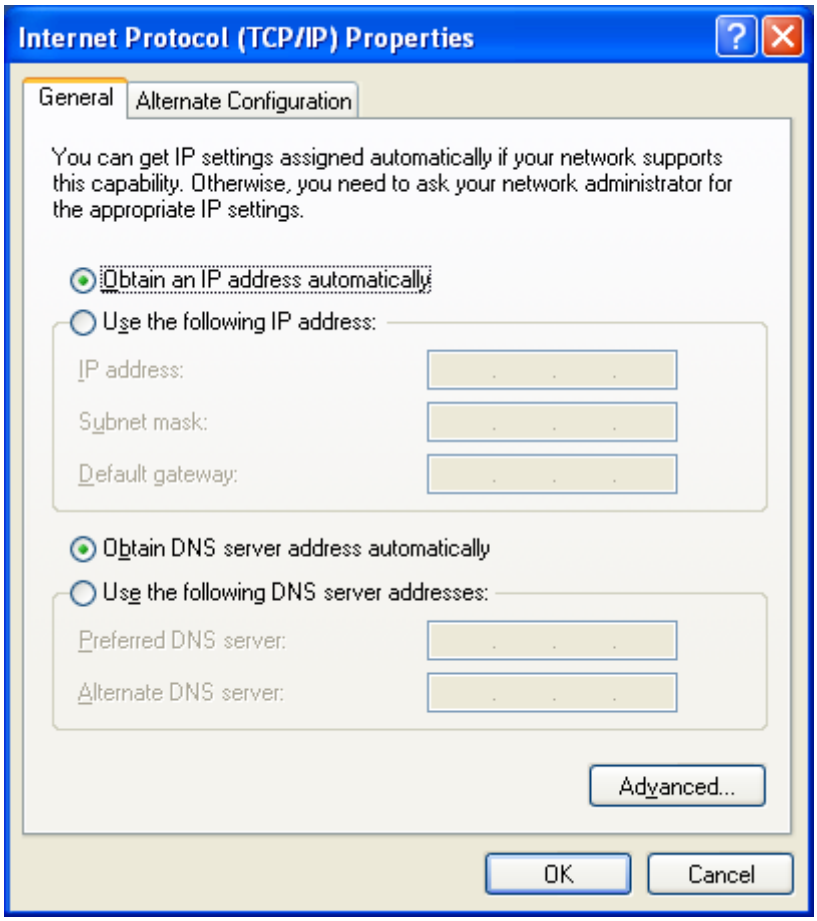


5) The following TCP/IP Properties window will display and the IP Address tab is open on this window by default.

Now you have two ways to configure the TCP/IP protocol below:

➢ **Setting IP address automatically**

Select Obtain an IP address automatically, and choose Obtain DNS server automatically, as shown in the Figure below:



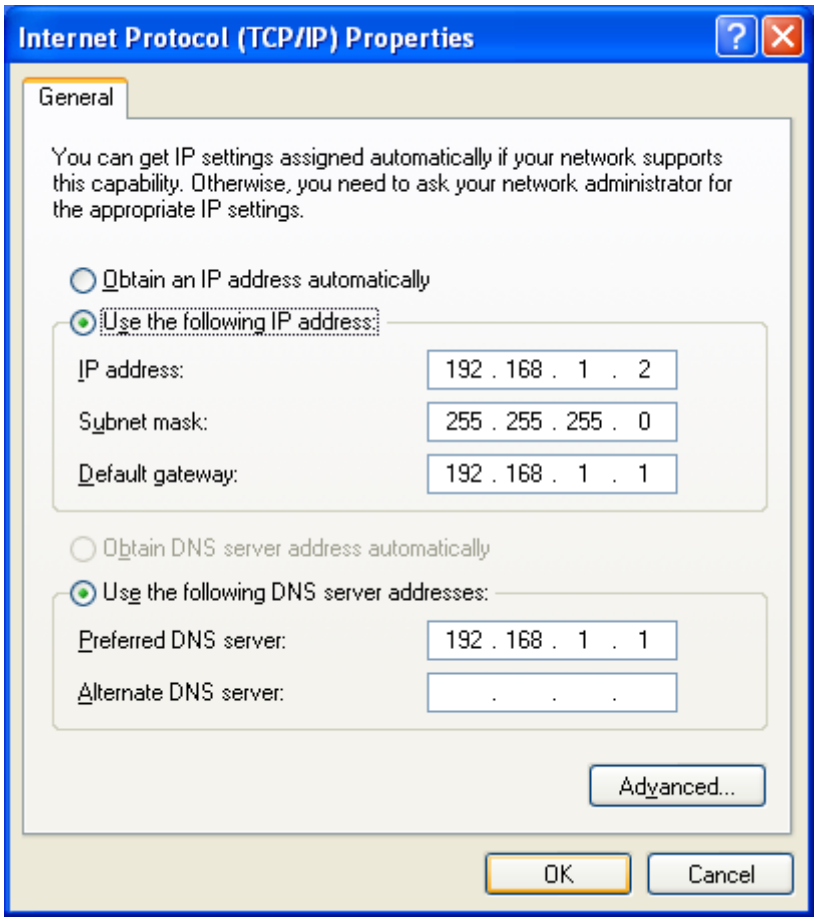
➢ **Setting IP address manually**

1) Select Use the following IP address radio button. And the following items available

2) If the modem router's LAN IP address is 192.168.1.1, specify the IP address as 192.168.1.x (x is from 2 to 254), and the Subnet mask as 255.255.255.0.

3) Type the modem router's LAN IP address (the default IP is 192.168.1.1) into the Default gateway field.

4) Select Use the following DNS server addresses. In the Preferred DNS Server field you can enter the same value as the Default gateway or type the local DNS server IP address.



Now: Click OK to keep your settings.

2. Verify the network connection

Now, you can run the Ping command in the command prompt to verify the network connection. Please click the Start menu on your desktop, select run tab, type cmd or command in the field and press Enter. Type *ping 192.168.1.1* on the following screen, and then press Enter.

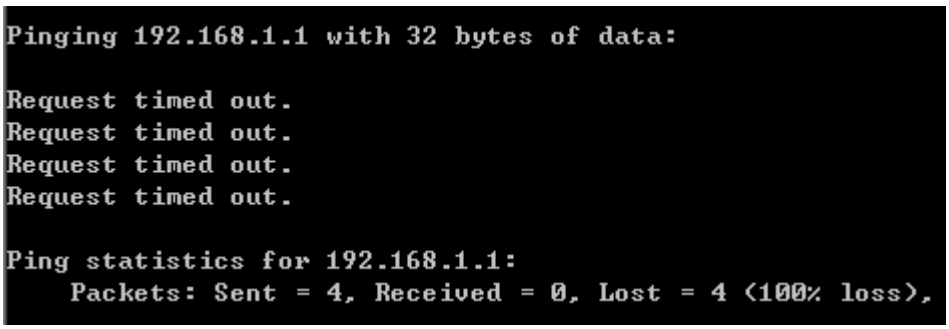
- If the result displayed is similar to the screen below, the connection between your PC and the router has been established.

```
Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

- If the result displayed is similar to the screen shown below, it means that your PC has not connected to the router.



You can check it by following the steps below:

1) Is the connection between your PC and the router correct?

The LEDs of LAN port which you link to the device and the LEDs on your PC's adapter should be lit.

2) Is the TCP/IP configuration for your PC correct?

If the router's IP address is 192.168.1.1, your PC's IP address must be within the range of 192.168.1.2 ~ 192.168.1.254.

Appendix B: Troubleshooting

T1. What can I do if I don't know or forget my password?

1) For default wireless password: Please refer to the Wireless Password/PIN labeled on the bottom of the modem router.

2) For the web management page password: Reset the modem router first and then use the default username and password: admin/admin.

T2. How do I restore my modem router's configuration to its factory default settings?

Method one: With the modem router powered on, press and hold down the WPS/RESET button for about 8 seconds until all LEDs turn off momentarily, then release the button.

Method two: Restore the default setting from Maintenance → SysRestart of the modem router's web management page.

☞ Note:

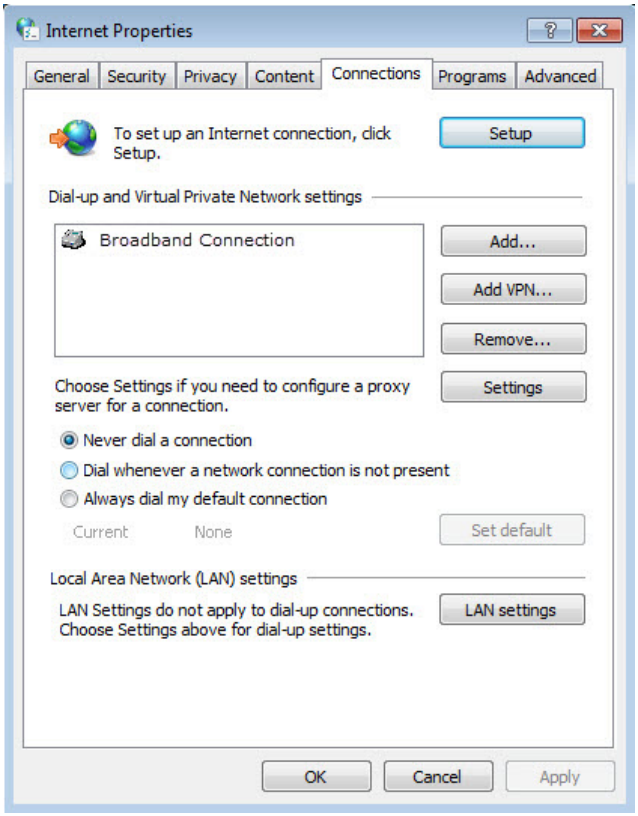
Once the modem router is reset, the current configuration settings will be lost and you will need to re-configure the router.

T3. What can I do if I cannot access the web management page?

- Make sure the modem router connects to the computer correctly and the corresponding LED indicator(s) light up.
- Make sure the IP address of your computer is configured to obtain an IP address automatically and obtain DNS server address automatically.
- Make sure the default access you input is right.
- Check your computer's settings:

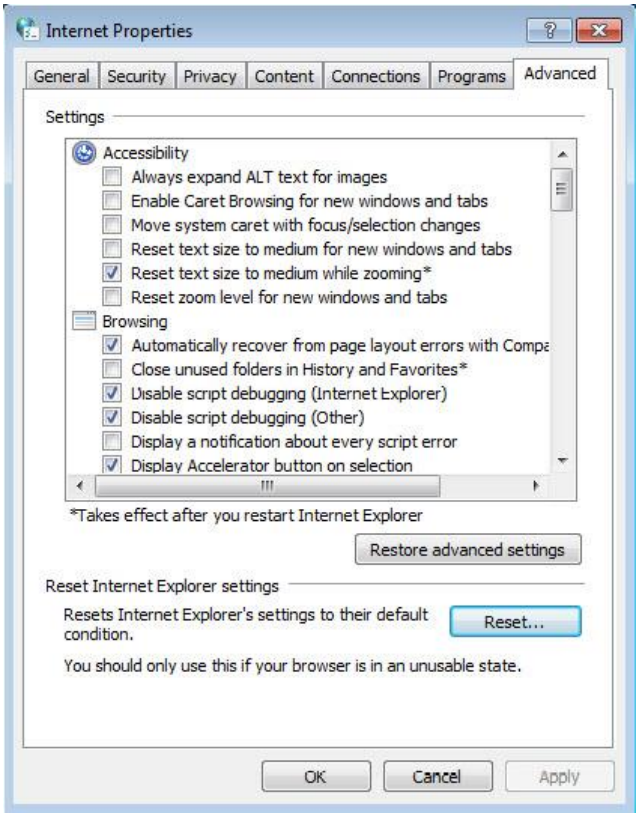
Go to Start → Control Panel → Network and Internet, and click View network status and tasks;

1) Click Internet Options on the bottom left;
2) Click Connections, and select Never dial a connection;



3) Click LAN settings, deselect the following three options and click OK;

4) Go to Advanced → Restore advanced settings, and click OK to save the settings.



- Change a web browser or computer and log in again.
- Reset the modem router to factory default settings.

☞ Note:

You'll need to reconfigure the modem router to surf the Internet once the modem router is reset.

- Open a web browser and log in again. If login fails, please contact the technical support.

T4. What can I do if I cannot access the Internet?

1) Check to see if all the connectors are connected well, including the telephone line, Ethernet cables and power adapter.
2) Check to see if you can log on to the web management page of the modem router. If you can, try the following steps. If you cannot, please set your computer referring to **T3** then try to see if you can access the Internet. If the problem persists, please go to the next step.
3) Consult your ISP and make sure all the VPI/VCI, Connection Type, account username and password are correct. If there are any mistakes, please correct the settings and try again.
4) If you still cannot access the Internet, please restore your modem router to its factory default settings and reconfigure your modem router by following the instructions in Chapter 3 Quick Start.
5) Please feel free to contact our Technical Support if the problem still exists.

☞ Note:

For more details about Troubleshooting and Technical Support contact information, please refer to the support page at www.tp-link.com.

COPYRIGHT & TRADEMARKS

Specifications are subject to change without notice. TP-Link is a registered trademark of TP-Link Technologies Co., Ltd. Other brands and product names are trademarks or registered trademarks of their respective holders.

No part of the specifications may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from TP-Link Technologies Co., Ltd. Copyright © 2020 TP-Link Technologies Co., Ltd. All rights reserved.

https://www.tp-link.com

FCC compliance information statement

Product Name: 300Mbps Wireless N ADSL2+ Modem Router

Model Number: TD-W8961N

Component Name	Model
I.T.E. Power	T090060-2B1

Responsible party:

TP-Link USA Corporation, d/b/a TP-Link North America, Inc.

Address: 145 South State College Blvd. Suite 400, Brea, CA 92821

Website: http://www.tp-link.com/us/

Tel: +1 626 333 0234

Fax: +1 909 527 6803

E-mail: sales.usa@tp-link.com

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the 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:

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

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.

2) This device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Note: The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user's authority to operate the equipment.

FCC RF Radiation Exposure Statement:

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

"To comply with FCC RF exposure compliance requirements, this grant is applicable to only Mobile Configurations. The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter."

We, **TP-Link USA Corporation**, has determined that the equipment shown as above has been shown to comply with the applicable technical standards, FCC part 15. There is no unauthorized change is made in the equipment and the equipment is properly maintained and operated.

Issue Date: 2020-06-08

FCC compliance information statement

Product Name: I.T.E. Power

Model Number: T090060-2B1

Responsible party:

TP-Link USA Corporation, d/b/a TP-Link North America, Inc.

Address: 145 South State College Blvd. Suite 400, Brea, CA 92821

Website: http://www.tp-link.com/us/

Tel: +1 626 333 0234

Fax: +1 909 527 6803

E-mail: sales.usa@tp-link.com

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the 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:

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

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

3) This device may not cause harmful interference.
4) This device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

We, **TP-Link USA Corporation**, has determined that the equipment shown as above has been shown to comply with the applicable technical standards, FCC part 15. There is no unauthorized change is made in the equipment and the equipment is properly maintained and operated.

Issue Date: 2020-06-08

CE Mark Warning

CE

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.

OPERATING FREQUENCY(the maximum transmitted power)

2400 MHz -2483.5 MHz(20dBm)

RF Exposure Information

This device meets the EU requirements (2014/53/EU Article 3.1a) on the limitation of exposure

of the general public to electromagnetic fields by way of health protection.

The device complies with RF specifications when the device used at 20 cm from your body.

EU declaration of conformity

TP-Link hereby declares that the device is in compliance with the essential requirements and other relevant provisions of directives 2014/30/EU, 2014/35/EU, 2009/125/EC, 2011/65/EU and (EU)2015/863.

The original EU declaration of conformity may be found at https://www.tp-link.com/en/ce

Продукт сертифіковано згідно с правилами системи УкрСЕПРО на відповідність вимогам нормативних документів та вимогам, що передбачені чинними законодавчими актами України.

Safety Information

- Keep the device away from water, fire, humidity or hot environments.
- Do not attempt to disassemble, repair, or modify the device. If you need service, please contact us
- Do not use damaged charger or USB cable to charge the device.
- Do not use any other chargers than those recommended
- Do not use the device where wireless devices are not allowed.
- Adapter shall be installed near the equipment and shall be easily accessible.
- Use only power supplies which are provided by manufacturer and in the original packing of this product. If you have any questions, please don't hesitate to contact us.

Explanation of the symbols on the product label

Symbol	Explanation
⎓	DC voltage

	Indoor use only
	Class II equipment
	Energy efficiency Marking
	Polarity of d.c. power connector
	Operator's manual
	RECYCLING This product bears the selective sorting symbol for Waste electrical and electronic equipment (WEEE). This means that this product must be handled pursuant to European directive 2012/19/EU in order to be recycled or dismantled to minimize its impact on the environment. User has the choice to give his product to a competent recycling organization or to the retailer when he buys a new electrical or electronic equipment.