TP-LINK®

User Guide

Archer D2

AC750 Wireless Dual Band Gigabit ADSL2+ Modem Router

Rev: 1.0.0
1910011088

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 © 2014 TP-LINK TECHNOLOGIES CO., LTD. All rights reserved.

http://www.tp-link.com

FCC STATEMENT

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."

CE Mark Warning

CE 0700

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.

National Restrictions

This device is intended for home and office use in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

Country	Restriction	Reason/remark
Bulgaria	None	General authorization required for outdoor use and public service
France	Outdoor use limited to 10 mW e.i.r.p. within the band 2454-2483.5 MHz	Military Radiolocation use. Refarming of the 2.4 GHz band has been ongoing in recent years to allow current relaxed regulation. Full implementation planned 2012
Italy	None	If used outside of own premises, general authorization is required
Luxembourg	None	General authorization required for network and service supply(not for spectrum)
Norway	Implemented	This subsection does not apply for the geographical area within a radius of 20 km from the centre of Ny-Ålesund
Russian Federation	None	Only for indoor applications

Note: Please don't use the product outdoors in France.

Canadian Compliance Statement

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions:

(1)This device may not cause interference, and

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

Cet appareil est conforme aux norms CNR exemptes de licence d'Industrie Canada. Le fonctionnement est soumis aux deux conditions suivantes:

(1)cet appareil ne doit pas provoquer d'interférences et

(2)cet appareil doit accepter toute interférence, y compris celles susceptibles de provoquer un fonctionnement non souhaité de l'appareil.

This device has been designed to operate with the antennas listed below, and having a maximum gain of 5 dBi. Antennas not included in this list or having a gain greater than 5 dBi are strictly prohibited for use with this device. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that permitted for successful communication.

Industry Canada Statement

Complies with the Canadian ICES-003 Class B specifications.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

This device complies with RSS 210 of Industry Canada. This Class B device meets all the requirements of the Canadian interference-causing equipment regulations.

Cet appareil numérique de la Classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

Korea Warning Statements:

당해 무선설비는 운용중 전파혼신 가능성이 있음.

NCC Notice& BSMI Notice:

注意！

依據 低功率電波輻射性電機管理辦法

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性或功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通行；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信規定作業之無線電信。低功率射頻電機需忍受合法通信或工業、科學以及醫療用電波輻射性電機設備之干擾。

減少電磁波影響，請妥適使用。

安全諮詢及注意事項

●請使用原裝電源供應器或只能按照本產品注明的電源類型使用本產品。

●清潔本產品之前請先拔掉電源線。請勿使用液體、噴霧清潔劑或濕布進行清潔。

●注意防潮，請勿將水或其他液體潑灑到本產品上。 □

●插槽與開口供通風使用，以確保本產品的操作可靠並防止過熱，請勿堵塞或覆蓋開口。

●請勿將本產品置放於靠近熱源的地方。除非有正常的通風，否則不可放在密閉位置中。

●請不要私自打開機殼，不要嘗試自行維修本產品，請由授權的專業人士進行此項工作。

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

EAC

Safety Information

- When product has power button, the power button is one of the way to shut off the product; when there is no power button, the only way to completely shut off power is to disconnect the product or the power adapter from the power source.
- Don’t disassemble the product, or make repairs yourself. You run the risk of electric shock and voiding the limited warranty. If you need service, please contact us.
- Avoid water and wet locations.

This product can be used in the following countries:

AT	BG	BY	CA	CZ	DE	DK	EE
ES	FI	FR	GB	GR	HU	IE	IT
LT	LV	MT	NL	NO	PL	PT	RO
RU	SE	SK	TR	UA	US		

DECLARATION OF CONFORMITY

For the following equipment:

Product Description: AC750 Wireless Dual Band Gigabit ADSL2+ Modem Router

Model No.: **Archer D2**

Trademark: **TP-LINK**

We declare under our own responsibility that the above products satisfy all the technical regulations applicable to the product within the scope of Council Directives:

Directives 1999/5/EC, Directives 2004/108/EC, Directives 2006/95/EC, Directives 1999/519/EC, Directives 2011/65/EU

The above product is in conformity with the following standards or other normative documents

EN 300 328 V1.8.1

EN 301 489-1 V1.9.2 & EN 301 489-17 V2.2.1

EN 55022: 2010 + AC: 2011

EN 55024: 2010

EN 61000-3-2: 2006 + A1: 2009 + A2: 2009

EN 61000-3-3: 2013

EN 60950-1: 2006 + A11: 2009 + A1: 2010 + A12: 2011

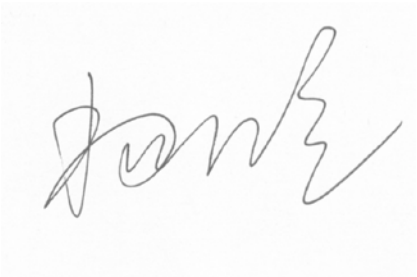
EN 50385: 2002

EN 301 893 V1.7.1

The product carries the CE Mark:

CE 0700 ⓘ

Person responsible for making this declaration:



Yang Hongliang

Product Manager of International Business

Date of issue: 2014

TP-LINK TECHNOLOGIES CO., LTD

Building 24 (floors 1, 3, 4, 5), and 28 (floors 1-4) Central Science and Technology Park, Shennan Rd, Nanshan, Shenzhen, China

CONTENTS

Package Contents **1**

Chapter 1. Product Overview **2**

1.1 Overview of the Modem Router 2

1.2 Main Features 3

1.3 Panel Layout 4

1.3.1 The Front Panel 4

1.3.2 The Back Panel 6

Chapter 2. Connecting the Modem Router **7**

2.1 System Requirements 7

2.2 Installation Environment Requirements 7

2.3 Connecting the Modem Router 7

Chapter 3. Quick Installation Guide **9**

3.1 TCP/IP Configuration 9

3.2 Quick Installation Guide 10

Chapter 4. Configuring the Modem Router **14**

4.1 Login 14

4.2 Status 15

4.3 Quick Setup 17

4.4 Operation Mode 17

4.5 Network 17

4.5.1 WAN Settings 18

4.5.2 Interface Grouping 27

4.5.3 LAN Settings 28

4.5.4 IPv6 LAN Settings 29

4.5.5 MAC Clone 31

4.5.6 ALG Settings 31

4.5.7 DSL Settings 32

4.5.8 IPSec VPN 32

4.6 IPTV 35

4.7 DHCP Server 36

4.7.1 DHCP Settings 36

4.7.2 Clients List 38
4.7.3 Address Reservation 38
4.7.4 Conditional Pool 39
4.8 Wireless 2.4GHz 41
4.8.1 Basic Settings 41
4.8.2 WPS Settings 42
4.8.3 Wireless Security 44
4.8.4 Wireless Schedule 46
4.8.5 Wireless MAC Filtering 47
4.8.6 Wireless Advanced 49
4.8.7 Wireless Status 50
4.9 Wireless 5GHz 51
4.9.1 Basic Settings 51
4.9.2 WPS Settings 52
4.9.3 Wireless Security 54
4.9.4 Wireless Schedule 56
4.9.5 Wireless MAC Filtering 57
4.9.6 Wireless Advanced 59
4.9.7 Wireless Status 61
4.10 Guest Network 61
4.10.1 Basic Settings 61
4.10.2 Guest Network Status 62
4.11 USB Settings 63
4.11.1 USB Mass Storage 63
4.11.2 User Accounts 64
4.11.3 Storage Sharing 65
4.11.4 FTP Server 66
4.11.5 Media Server 68
4.11.6 Print Server 69
4.12 Route Settings 69
4.12.1 Default Gateway 70
4.12.2 Static Route 70
4.12.3 RIP Settings 71
4.13 IPv6 Route Settings 71
4.13.1 IPv6 Default Gateway 71
4.13.2 IPv6 Static Route 72

4.14 Forwarding 73
4.14.1 Virtual Server 73
4.14.2 Port Triggering 75
4.14.3 DMZ 76
4.14.4 UPnP 77
4.15 Parental Control 78
4.16 Firewall 79
4.16.1 Rule 79
4.16.2 LAN Host 80
4.16.3 WAN Host 81
4.16.4 Schedule 83
4.17 IPv6 Firewall 84
4.17.1 IPv6 Rule 84
4.17.2 IPv6 LAN Host 85
4.17.3 IPv6 WAN Host 86
4.17.4 IPv6 Schedule 87
4.18 IPv6 Tunnel 88
4.19 Bandwidth Control 91
4.20 IP&MAC Binding 92
4.20.1 Binding Settings 92
4.20.2 ARP List 93
4.21 Dynamic DNS 94
4.22 Diagnostic 94
4.23 System Tools 95
4.23.1 System Log 95
4.23.2 Time Settings 96
4.23.3 Manage Control 97
4.23.4 CWMP Settings 98
4.23.5 SNMP Settings 99
4.23.6 Backup & Restore 100
4.23.7 Factory Defaults 100
4.23.8 Firmware Upgrade 101
4.23.9 Reboot 102
4.23.10 Statistics 102
4.24 Logout 104

Appendix A: Specifications **105**

Appendix B: Troubleshooting **106**

Appendix C: Technical Support **109**

Package Contents

The following contents should be found in your package:

- One Archer D2 AC750 Wireless Dual Band Gigabit ADSL2+ Modem Router
- One Power Adapter for Archer D2 AC750 Wireless Dual Band Gigabit ADSL2+ Modem Router
- Quick Installation Guide
- One RJ45 cable
- Two RJ11 cables
- One ADSL splitter
- One Resource CD for Archer D2 AC750 Wireless Dual Band Gigabit ADSL2+ Modem Router, including:
  - This User Guide
  - Other Helpful Information

☞ **Note:**

Make sure that the package contains the above items. If any of the listed items are damaged or missing, please contact your distributor.

Chapter 1. Product Overview

Thank you for choosing the **Archer D2 AC750 Wireless Dual Band Gigabit ADSL2+ Modem Router**.

1.1 Overview of the Modem Router

The Archer D2 AC750 Wireless Dual Band Gigabit ADSL2+ Modem Router integrates 4-port Switch, Firewall, NAT-Router and Wireless AP. The AC750 Wireless Dual Band Gigabit ADSL2+ Modem Router delivers exceptional range and speed, which can fully meet the need of Small Office/Home Office (SOHO) networks and the users demanding higher networking performance.

The Archer D2 AC750 Wireless Dual Band Gigabit ADSL2+ Modem Router utilizes integrated ADSL2+ transceiver and high speed MIPS CPU. The Router supports full-rate ADSL2+ connectivity conforming to the ITU and ANSI specifications.

In addition to the basic DMT physical layer functions, the ADSL2+ PHY supports dual latency ADSL2+ framing (fast and interleaved) and the I.432 ATM Physical Layer.

The modem router provides up to 300Mbps (2.4GHz) + 450Mbps (5GHz) wireless connection with other wireless clients. The incredible speed makes it ideal for handling multiple data streams at the same time, which ensures your network stable and smooth. The performance of this 802.11ac wireless modem router will give you the unexpected networking experience at speed much faster than 802.11n. It is also compatible with all IEEE 802.11a, IEEE 802.11b, IEEE 802.11g and IEEE 802.11n, products.

With multiple protection measures, including SSID broadcast control and wireless LAN 64/128 WEP encryption, Wi-Fi protected Access (WPA2-PSK, WPA-PSK), as well as advanced Firewall protections, the Archer D2 AC750 Wireless Dual Band Gigabit ADSL2+ Modem Router provides complete data privacy.

The modem router provides flexible access control, so that parents or network administrators can establish restricted access policies for children or staffs. It also supports Virtual Server and DMZ host for Port Triggering, and then the network administrators can manage and monitor the network in real time with the remote management function.

Since the modem router is compatible with virtually all the major operating systems, it is very easy to manage. Quick Setup Wizard is supported and detailed instructions are provided step by step in this user guide. Before installing the modem router, please look through this guide to know all the modem router's functions.

1.2 Main Features

- Complies with IEEE 802.11ac to provide a wireless data rate of up to 300Mbps (2.4GHz) + 450Mbps (5GHz).
- Four 10/100/1000Mbps Auto-Negotiation RJ45 LAN ports (Auto MDI/MDIX), one RJ11 port.
- Provides external splitter.
- Adopts Advanced DMT modulation and demodulation technology.
- Supports bridge mode and Router function.
- Multi-user sharing a high-speed Internet connection.
- Downstream data rates up to 24Mbps, upstream data rates up to 1Mbps.
- Supports long transfers, the max line length can reach to 6.5Km.
- Supports remote configuration and management through SNMP and CWMP.
- Supports PPPoE, which allows connecting to the Internet on demand and disconnecting from the Internet when idle.
- Provides reliable ESD and surge-protect function with quick response semi-conductive surge protection circuit.
- High speed and asymmetrical data transmit mode, provides safe and exclusive bandwidth.
- Compatible with all mainstreams DSLAM (CO).
- Provides integrated access of internet and route function which face to SOHO user.
- Real-time Configuration and device monitoring.
- Supports Multiple PVC (Permanent Virtual Circuit).
- Built-in DHCP server.
- Built-in firewall, supporting IP/MAC filter and URL filter.
- Supports Virtual Server, DMZ host and Port Triggering.
- Supports Dynamic DNS, UPnP and Static Routing.
- Supports system log and flow Statistics.
- Supports firmware upgrade and Web management.
- Provides WPA-PSK/WPA2-PSK data security, TKIP/AES encryption security.
- Provides 64/128-bit WEP encryption security and wireless LAN ACL (Access Control List).
- Supports USB Storage Sharing, Print Server, FTP Server, Media Server.
- Supports Ethernet WAN (EWAN).
- Supports Bandwidth Control.
- Supports IPv6.
- Supports Guest Network.

1.3 Panel Layout

1.3.1 The Front Panel

Figure 1-1

The modem router's LEDs are located on the top panel (View from top to bottom). They indicate the device's working status. For details, please refer to LED Explanation.

LED Explanation:

Name	Status	Indication
(WPS)	On	A wireless device has been successfully added to the network by WPS function.
	Flash	WPS handshaking is in process and will continue for about 2 minutes. Please press the WPS button on other wireless devices that you want to add to the network while the LED is flashing.
	Off	A wireless device has failed to be added to the network by WPS function. Please refer to 4.8.2 WPS Settings for more information.
(USB)	On	The USB device is identified and ready to use.
	Flash	The USB device is being identified.
	Off	No USB device is plugged into the USB port.

(LAN)	On	At least one LAN port is connected.
	Off	No LAN port is connected.
(Wireless)	On	The wireless 2.4GHz/5GHz band is working properly.
	Off	The wireless function is disabled.
(Internet)	On	The network is available with a successful Internet connection.
	Off	There is no successful Internet connection or the modem router is operating in Bridge mode. Please refer to **Note 2** for troubleshooting.
(ADSL)	On	ADSL line is synchronized and ready to use.
	Flash	The ADSL negotiation is in progress.
	Off	ADSL synchronization fails. Please refer to **Note 1** for troubleshooting.
(Power)	On	System start-up complete.
	Flash	System starting up or device updating.
	Off	Power is off. Please ensure that the power adapter is connected correctly.

Note:

1. If the ADSL LED is off, please check your Internet connection first. Refer to **2.3 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 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 have been input correctly.

1.3.2 The Back Panel

Figure 1-2

- **ADSL**: Through the port, you can connect the telephone to the modem router. Or you can connect them by an external separate splitter. For details, please refer to 2.3 Connecting the Modem Router.
- **USB**: The USB port connects to a USB storage device or a USB printer.
- **WPS**: The switch for the WPS function. For details, please refer to 4.8.2 WPS Settings.
- **WiFi ON/OFF**: The switch for the WiFi function. Press it to enable/disable the WiFi function.
- **RESET**: There are two ways to reset the modem router's factory defaults.

  Method one: With the modem router powered on, use a pin to press and hold the RESET button for at least 8-10 seconds. And the modem router will reboot to its factory default settings.

  Method two: Restore the default setting from 4.23.7 Factory Defaults of the modem router's Web-based Management.
- **LAN4/WAN, LAN3, LAN2, LAN1:** Through these ports, you can connect the modem router to your PC or other Ethernet network devices. In wireless router mode you will be able to connect to Cable/FTTH/VDSL/ADSL devices.
- **POWER ON/OFF**: The switch for the power.
- **POWER**: The Power plug is where you will connect the power adapter.
- **Antennas**: Used for wireless operation and data transmit.

Chapter 2. Connecting the Modem Router

2.1 System Requirements

- Broadband Internet Access Service (DSL/Cable/Ethernet).
- PCs with a working Ethernet Adapter and an Ethernet cable with RJ45 connectors.
- TCP/IP protocol on each PC.
- Web browser, such as Microsoft Internet Explorer, Mozilla Firefox and Apple Safari.

2.2 Installation Environment Requirements

- The Product should not be located where it will be exposed to moisture or excessive heat.
- 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 so they do not create a tripping hazard.
- The modem router can be placed on a shelf or desktop.
- Keep away from the strong electromagnetic radiation and the device of electromagnetic sensitive.

2.3 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: Plug one end of the twisted-pair ADSL cable into the ADSL port on the rear panel of Archer D2, and insert the other end into the wall socket.

Method two: You can use 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 Archer D2

Plug one end of the twisted-pair ADSL cable into the ADSL port on the rear panel of Archer D2. Connect the other end to the MODEM port of the external splitter.

Step 2: Connect the Ethernet cable. Attach one end of a network cable to your computer's Ethernet port or a regular hub/switch port, and the other end to the LAN port on the modem router Archer D2.

Step 3: Power on the computers and LAN devices.

Step 4: Attach the power adapter. Connect the power adapter to the power connector on the rear of the device and plug in the adapter to an electrical outlet or power extension. The electrical outlet shall be installed near the device and shall be easily accessible.

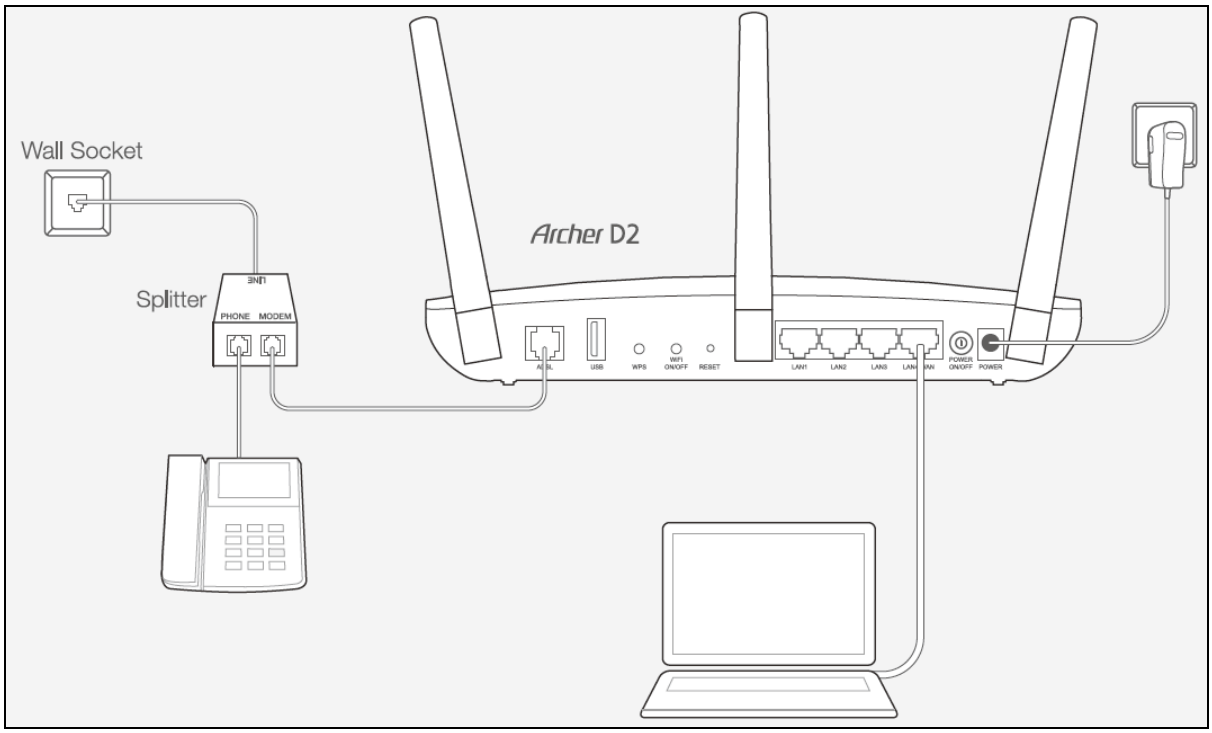

Wall Socket
Splitter
LINE
PHONE
MODEM
Archer D2
USB
WPS
WiFi ON/OFF
RESET
LAN1
LAN2
LAN3
POWER ON/OFF
POWER

Figure 2-1

Chapter 3. Quick Installation Guide

This chapter will show you how to configure the basic functions of your Archer D2 AC750 Wireless Dual Band Gigabit ADSL2+ Modem Router using **Quick Setup Wizard** within minutes.

3.1 TCP/IP Configuration

The default IP address of the Archer D2 AC750 Wireless Dual Band Gigabit ADSL2+ 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. In this guide, we use all the default values for description.

Connect the local PC to the LAN/WAN port of the modem router. And then you can configure your PC in the following way.

1) Set up the TCP/IP Protocol in "**Obtain an IP address automatically**" mode on your PC. If you need instructions as to how to do this, please refer to **T3** in Appendix B: Troubleshooting.

2) Then the built-in DHCP server will assign IP address for the PC.

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 next 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.

```
Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

You can check it 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.

3.2 Quick Installation Guide

With a Web-based utility, it is easy to configure and manage the Archer D2 AC750 Wireless Dual Band Gigabit ADSL2+ Modem Router. The Web-based utility can be used on any Windows, Macintosh or UNIX OS with a Web browser, such as Microsoft Internet Explorer, Mozilla Firefox or Apple Safari.

Step 1. To access the configuration utility, open a web-browser and type the default address http://tplinkmodem.net/ in the address field of the browser.

Figure 3-1

After a moment, a login window will appear, similar to the Figure 3-2. Enter **admin** for the User Name and Password, both in lower case letters. Then click the **Login** button or press the **Enter** key.

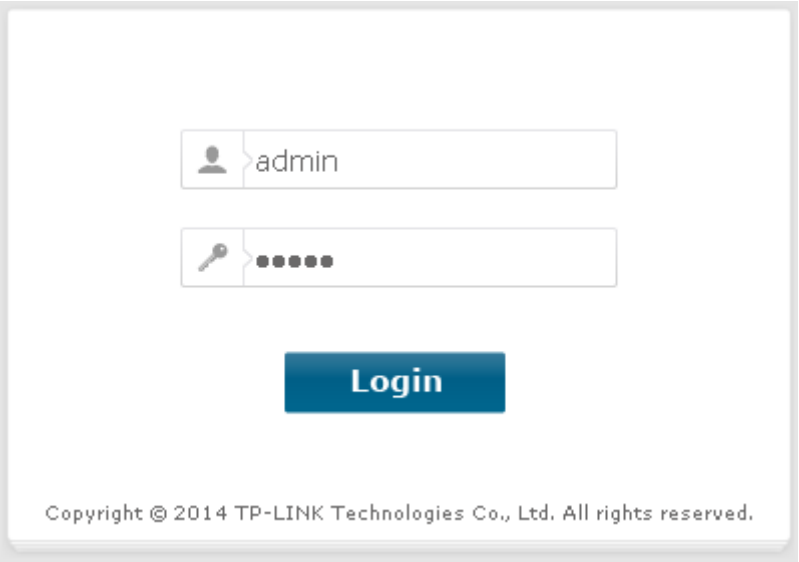


Figure 3-2

☞ **Note:**

1) Do not mix up the user name and password with your ADSL account user name and password which are needed for PPP connections.
2) If the above screen does not pop up, it means that your Web-browser has been set to a proxy. Go to **Tools** menu→**Internet Options**→**Connections**→**LAN Settings**, in the screen that appears, cancel the Using Proxy checkbox, and click **OK** to finish it.

Step 2. After your successful login, you will see the Login screen as shown in Figure 3-3. Click **Quick Setup** menu to access **Quick Setup Wizard**.

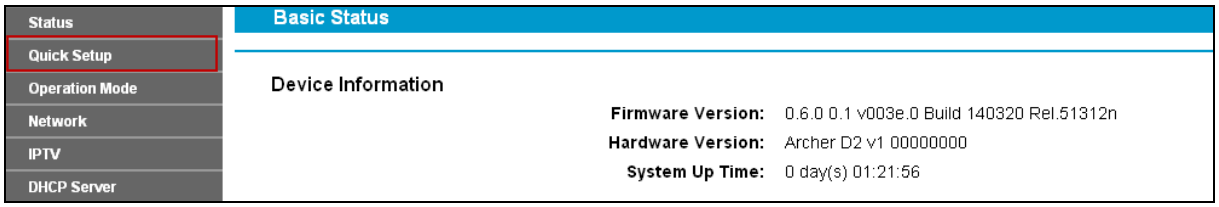


Figure 3-3

Step 3. The **Quick Setup** page will appear for you to quickly configure your modem router. Click **Next** to continue.

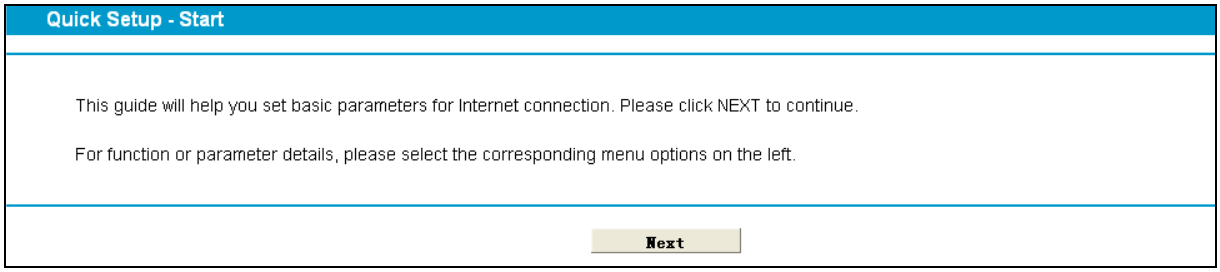


Figure 3-4

Step 4. Select the **Region** and the **Time Zone** from the drop-down list, and then click **Next**.

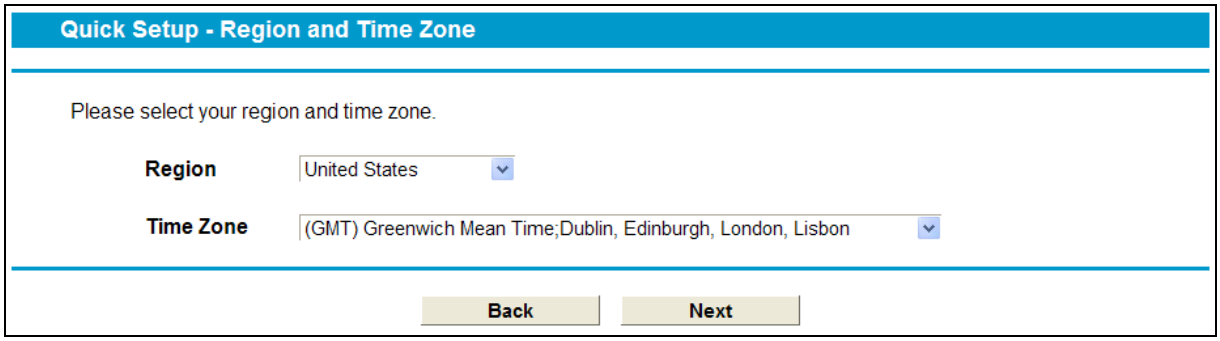


Figure 3-5

Step 5. Select **Yes** to auto detect your connection type and then click **Next**. It will take about two minutes, please wait.

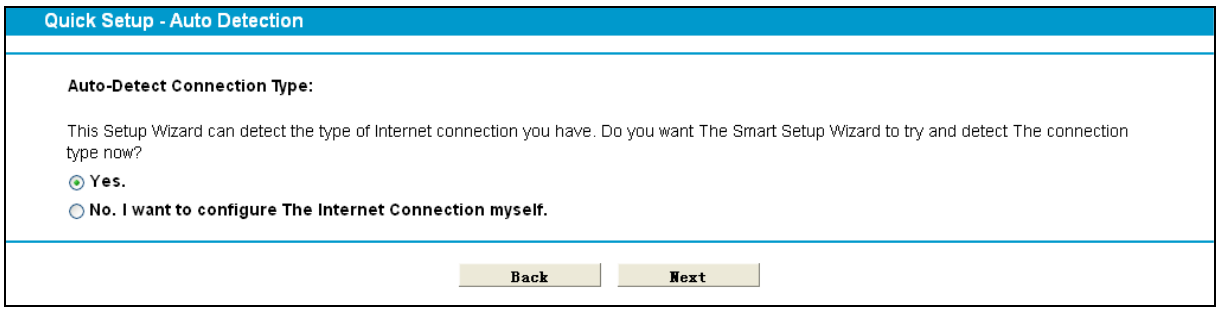


Figure 3-6

Step 6. Configure parameters for WAN connection. Here we take PPPoE as an example. Enter username and password provided by your ISP and click **Next** to continue.

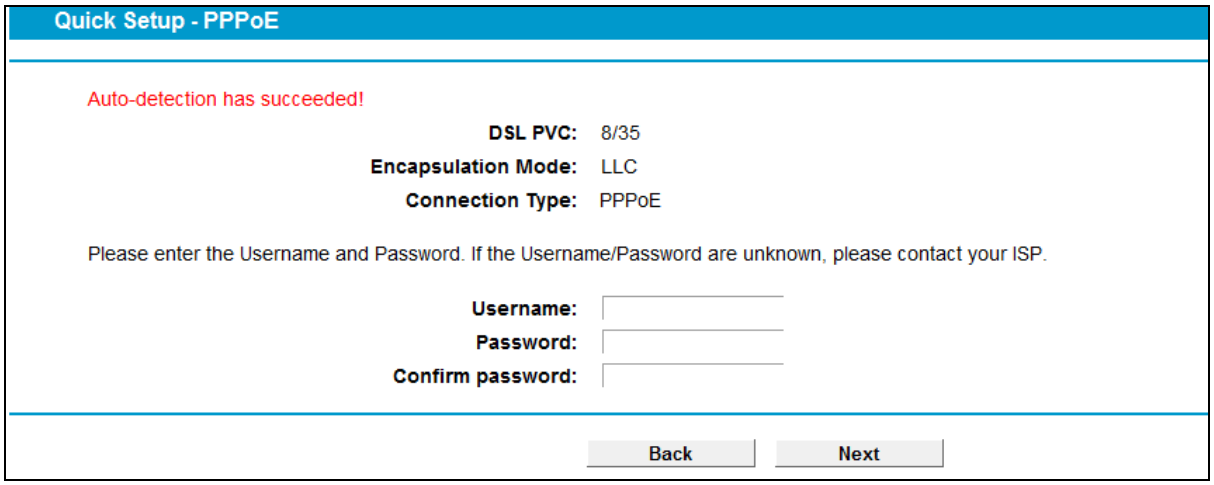


Figure 3-7

Step 7. Configure the basic parameters for 2.4GHz wireless network, and then click **Next**.

Figure 3-8

Step 8. Configure the basic parameters for 5GHz wireless network and then click **Next**.

Figure 3-9

Step 9. On this page, please confirm all parameters. Click **Save** and wait a moment for your settings taking effect.

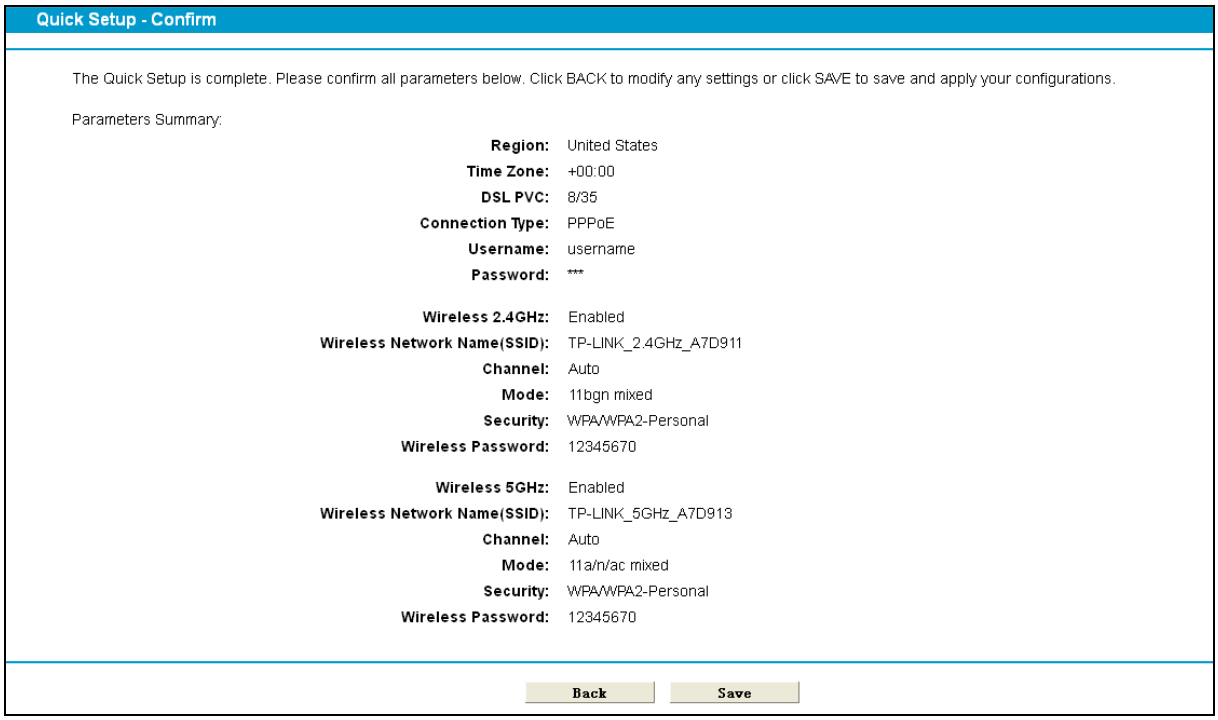


Figure 3-10

Step 10. You will see the **Complete** screen below. Click **Finish** to complete these settings.

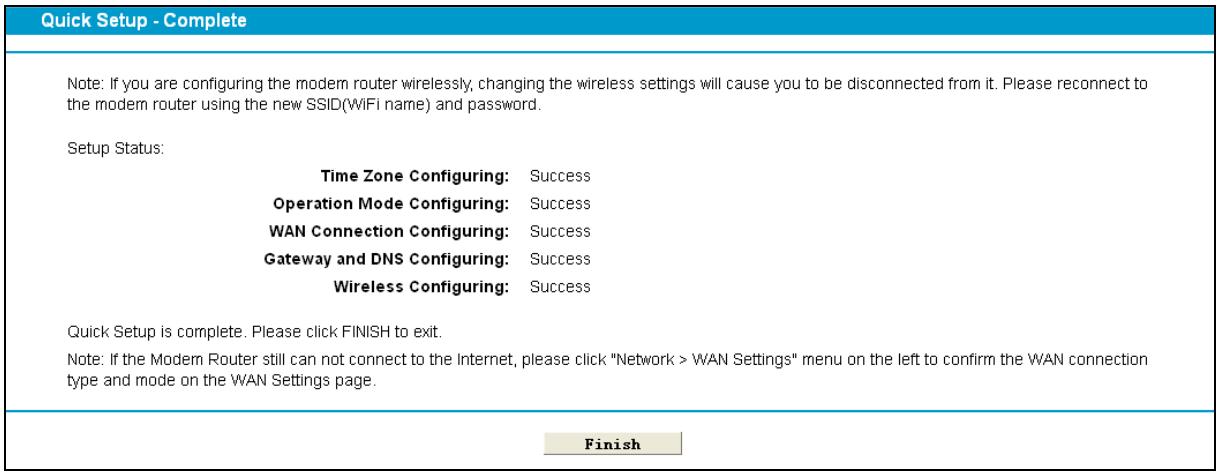


Figure 3-11

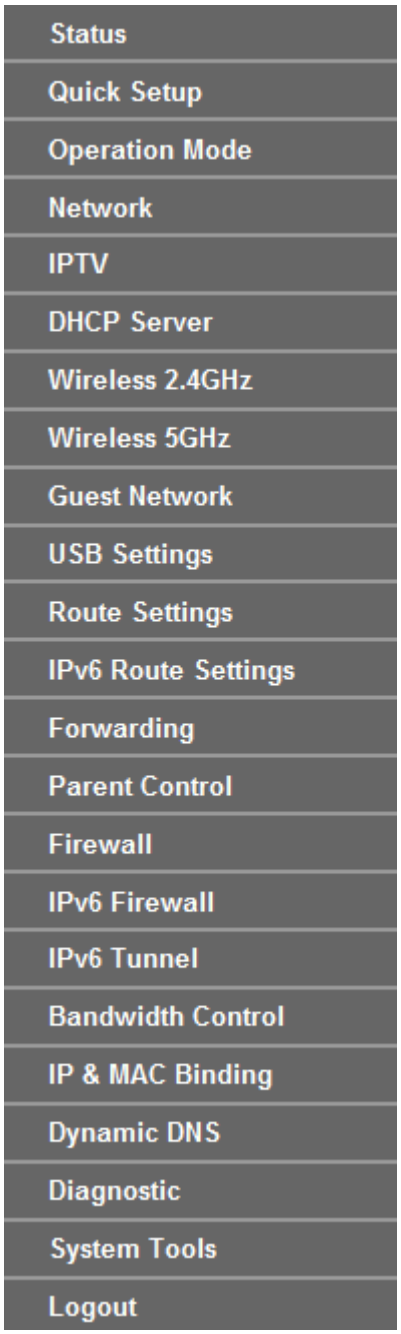
The basic settings for your modem router are completed. Please open the web browser and try to log on to http://www.tp-link.com to test your Internet connection.

Chapter 4. Configuring the Modem Router

This chapter will show configuration for the key functions on the Web-based management page.

4.1 Login

After your successful login, you will see the twenty-three main menus on the left of the Web-based utility. On the right, there are the corresponding explanations and instructions.



The detailed explanations for each Web page's key function are listed below.

4.2 Status

Choose “**Status**”, you can see the corresponding information about **Device Information**, **DSL**, **WAN**, **LAN** and **Wireless**.

Basic Status

Device Information

Firmware Version: 0.6.0 0.2 v003e.0 Build 140507 Rel.35898n
Hardware Version: Archer D2 v1 00000000
System Up Time: 0 day(s) 00:08:44

DSL

Line Status: Disconnected
DSL Modulation Type: Multimode
Annex Type: Annex A/L

	Upstream	Downstream
Current Rate (Kbps)	0	0
Max Rate (Kbps)	0	0
SNR Margin (dB)	0	0
Line Attenuation (dB)	0	0
Errors (Pkts)	0	0

WAN

Name	Connection Type	VPI/VCI	IP/Mask	Gateway	DNS	Status
br_8_35_0	Bridge	8/35	N/A	N/A	N/A	Disconnected

IPv6 WAN

Name	Connection Type	VPI/VCI	IPv6 Address/Prefix Length	Gateway	DNSv6	Status

LAN

MAC Address: 6E:D6:49:A3:92:D6
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
DHCP: Enabled

IPv6 LAN

IPv6 Address: N/A
Prefix Length: 64
Autoconfiguration Type: RADVD

Wireless 2.4GHz

Status: Enabled
Schedule: Disabled
SSID: TP-LINK_2.4GHz_130969
Channel: Auto(Channel 7)
Channel Width: Auto
Mode: 11bgn mixed
Security: WPA/WPA2-Personal
MAC Address: 00:0A:EB:13:09:69
Max Tx Rate: 300Mbps
WDS Status: Disabled

Wireless 5GHz

Status: Enabled
Schedule: Disabled
SSID: TP-LINK_5GHz_13096B
Channel: Auto(Channel 36)
Channel Width: Auto
Mode: 11a/n/ac mixed
Security: WPA/WPA2-Personal
MAC Address: 00:0A:EB:13:09:6B
Max Tx Rate: 433Mbps
WDS Status: Disabled

Figure 4-1

4.3 Quick Setup

Please refer to 3.2 Quick Installation Guide.

4.4 Operation Mode

Choose "**Operation Mode**", and you will see the screen as shown in Figure 4-2. Select your desired mode and then click **Save**.

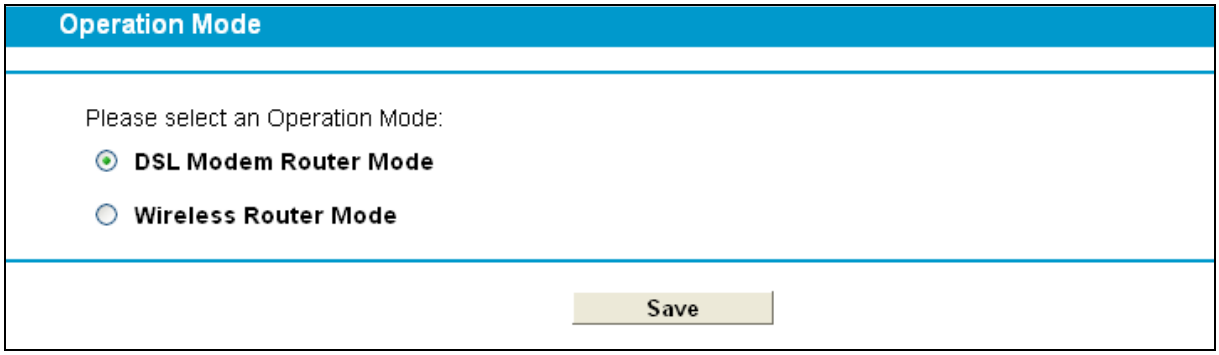
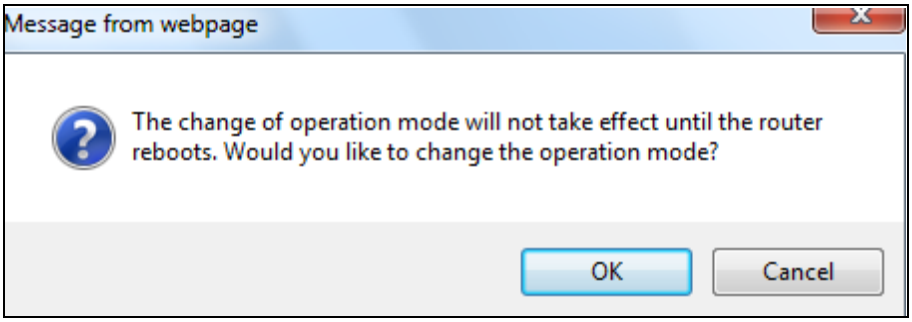


Figure 4-2

- **DSL Modem Router Mode:** The device enables multi-users to share Internet via ADSL using its ADSL port and share it wirelessly at 450Mbps wireless speeds over the crystal clear 5GHz band and 300Mbps over the 2.4GHz band.
- **Wireless Router Mode:** The device enables multi-users to share Internet via Ethernet WAN (EWAN) using its interchangeable LAN4/WAN port and share it wirelessly at 450Mbps wireless speeds over the crystal clear 5GHz band and 300Mbps over the 2.4GHz band.

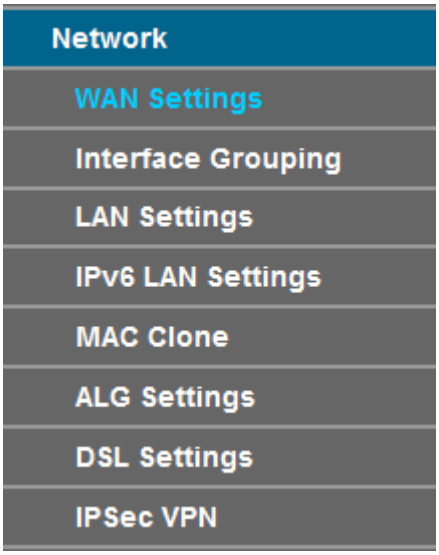
After you click the **Save** button, the Note Dialog will appear. Click **OK** and then the modem router will reboot. Please wait.



Note Dialog

4.5 Network

Choose "**Network**", there are many submenus under the main menu. Click any one of them, and you will be able to configure the corresponding function.



4.5.1 WAN Settings

Choose "**Network**"→"**WAN Settings**", and you will see the WAN Port Information Table in the screen similar to Figure 4-3. There are six different configurations for the connection types, which are Static IP, Dynamic IP, PPPoE, PPPoA, IPoA and Bridge. You can select the corresponding types according to your needs.

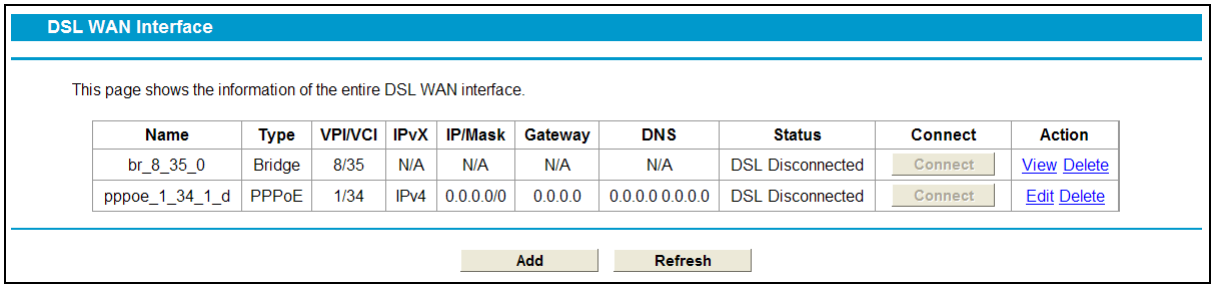


Figure 4-3

Click **Add** to add a new entry, you can configure the parameters for ATM and WAN Service in the next screen (shown in Figure 4-4).

Figure 4-4

4.5.1.1 Static IP

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.

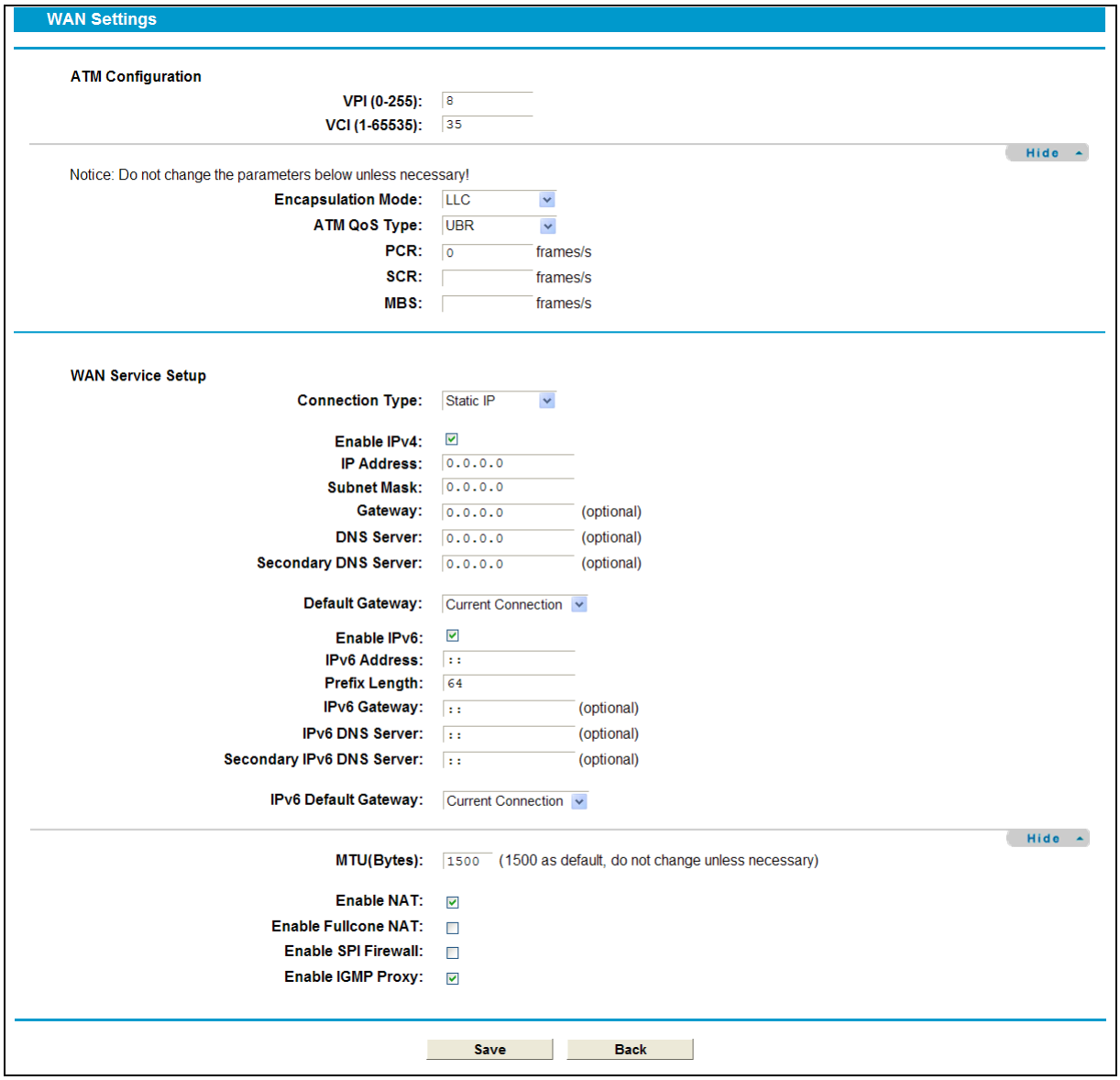


Figure 4-5

ATM Configuration:

- **VPI (0~255):** 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 (1~65535):** Identifies the virtual channel endpoints in an ATM network. The valid range is from 1 to 65535 (1 to 31 is reserved for well-known protocols). Please input the value provided by your ISP.

Click **Advance**, the advanced selections of ATM Configuration can be shown.

- **Encapsulation Mode:** Select the encapsulation mode for the Static IP Address. Here you can leave it by default.
- **ATM Qos Type:** Select ATM Qos Type provided by your ISP. The default type is UBR.

WAN Service Setup:

- **Enable IPv4:** Check the box to enable IPv4.
- **IP Address:** Enter the IP address in dotted-decimal notation provided by your ISP.
- **Subnet Mask:** Enter the subnet Mask provided by your ISP, which is usually 255.255.255.0.

- **Gateway** (Optional): Enter the gateway IP address in dotted-decimal notation provided by your ISP.
- **DNS Server/ Secondary DNS Server:** Here you can set DNS Server (at least one) manually. The modem router will use the first DNS Server for priority.
- **Default Gateway:** Select a WAN Interface from the drop-down list as the IPv4 default gateway.
- **Enable IPv6:** Check the box to enable IPv6.
- **IPv6 Address:** Enter the IPv6 address provided by your ISP.
- **Prefix Length:** Enter the prefix length of the IPv6 address. The default value is 64.
- **IPv6 Gateway:** Enter the gateway IPv6 address provided by your ISP.
- **IPv6 DNS Server / Secondary IPv6 DNS Server:** Here you can set IPv6 DNS Server (at least one) manually. The Route will use this IPv6 DNS Server for priority.
- **IPv6 Default Gateway:** Select a WAN Interface from the drop-down list as the IPv6 default gateway.

Click **Advance**, advanced selections of WAN Service Setup can be shown.

- **MTU (bytes)**: The default **MTU** (Maximum Transmission Unit) value is 1500 Bytes. Do not change the default value unless required by your ISP.
- **Enable NAT**: This technology translates the IP addresses of a local area network to a different IP address for the Internet. If this modem router is hosting your network's connection to the Internet, please select the check box.
- **Enable Fullcone NAT**: It is a type of NAT, if not enabled, the default NAT will act.
- **Enable SPI Firewal**l: The SPI firewall enhances network's security. Select the option to use a firewall, or else without a firewall.
- **Enable IGMP Proxy**: IGMP (Internet Group Management Protocol) is used to manage multicasting on TCP/IP networks. Some ISPs use IGMP to perform remote configuration for client devices, such as the modem router. It is enabled by default.

Click the **Save** button to save the settings.

4.5.1.2 Dynamic IP

Select **Dynamic IP** type if your ISP provides the DHCP service, and the modem router will automatically get IP parameters from your ISP.

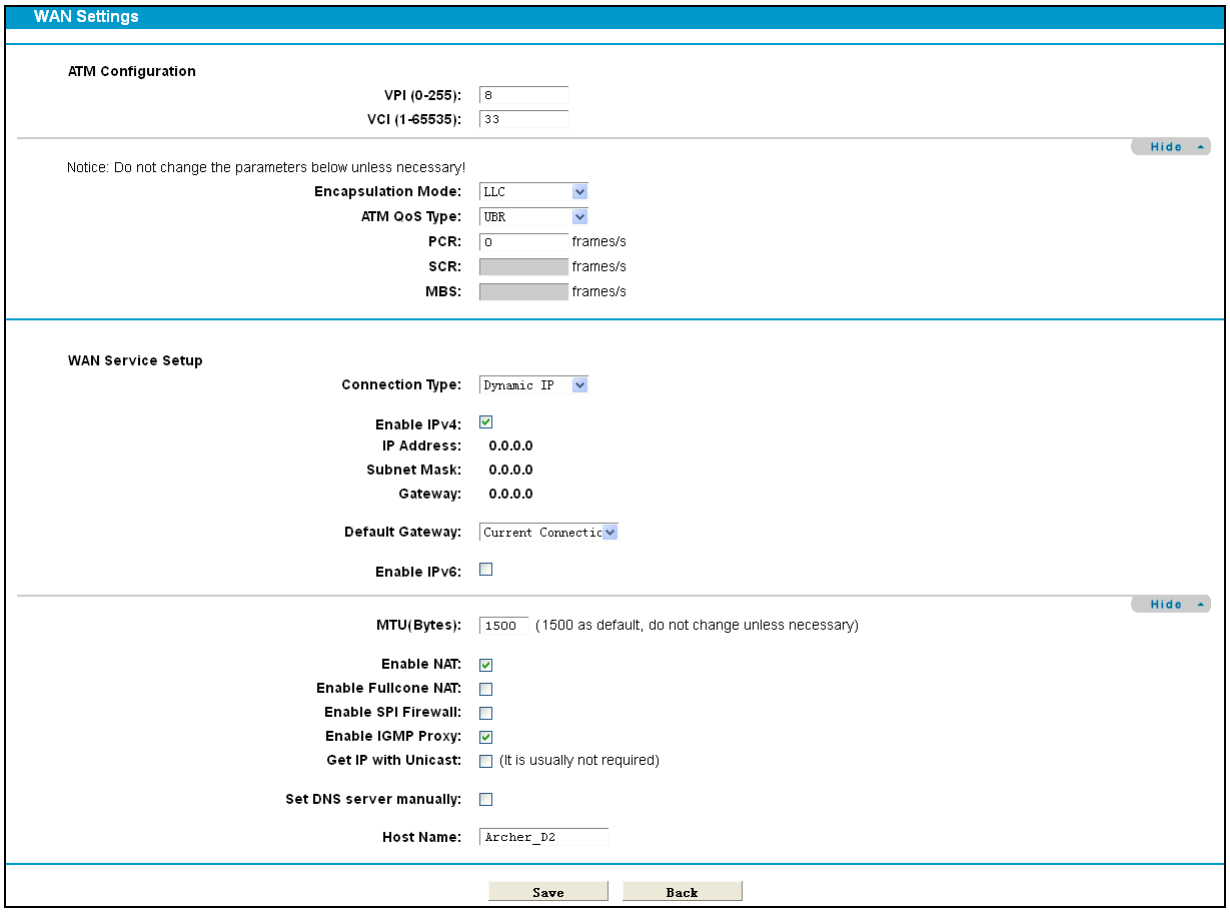


Figure 4-6

Click **Advance**, advanced selections for WAN Service Setup can be shown.

- **MTU (bytes):** The default **MTU** (Maximum Transmission Unit) value is 1500 Bytes. Do not change the default value unless required by your ISP.
- **Enable NAT:** This technology translates the IP addresses of a local area network to a different IP address for the Internet. If this modem router is hosting your network's connection to the Internet, please select the check box.
- **Enable Fullcone NAT**: It is a type of NAT, if not enabled, the default NAT will act.
- **Enable SPI Firewall:** The SPI firewall enhances network's security. Select the option to use a firewall, or else without a firewall.
- **Enable IGMP Proxy**: IGMP (Internet Group Management Protocol) is used to manage multicasting on TCP/IP networks. Some ISPs use IGMP to perform remote configuration for client devices, such as the modem router. It is enabled by default.
- **Get IP with Unicast:** It is disabled by default. A few ISPs' DHCP Servers do not support the broadcast applications. When the modem router cannot get the IP address normally, you can choose this option. (It is rarely required)
- **Set DNS Server manually:** Choose "Set DNS Server manually", you can set DNS Server manually here. The modem router will use this DNS Server for priority.
- **Get IPv6 Address with Unicast:** It is disabled by default. A few ISPs' DHCP Servers do not support the broadcast applications. When the modem router cannot get the IPv6 address normally, you can choose this option.(It is rarely required.)

- **Set IPv6 DNS Server manually:** Choose “Set IPv6 DNS Server manually”, you can set IPv6 DNS Server manually here. The modem router will use this IPv6 DNS Server for priority.
- **Host Name:** Here displays model number of your modem router.

Click the **Save** button to save the settings.

4.5.1.3 PPPoE

If your ISP provides a **PPPoE** connection and you need to use an ATM Interface, choose **PPPoE** in the drop-down list, and then the screen will be displayed as below.

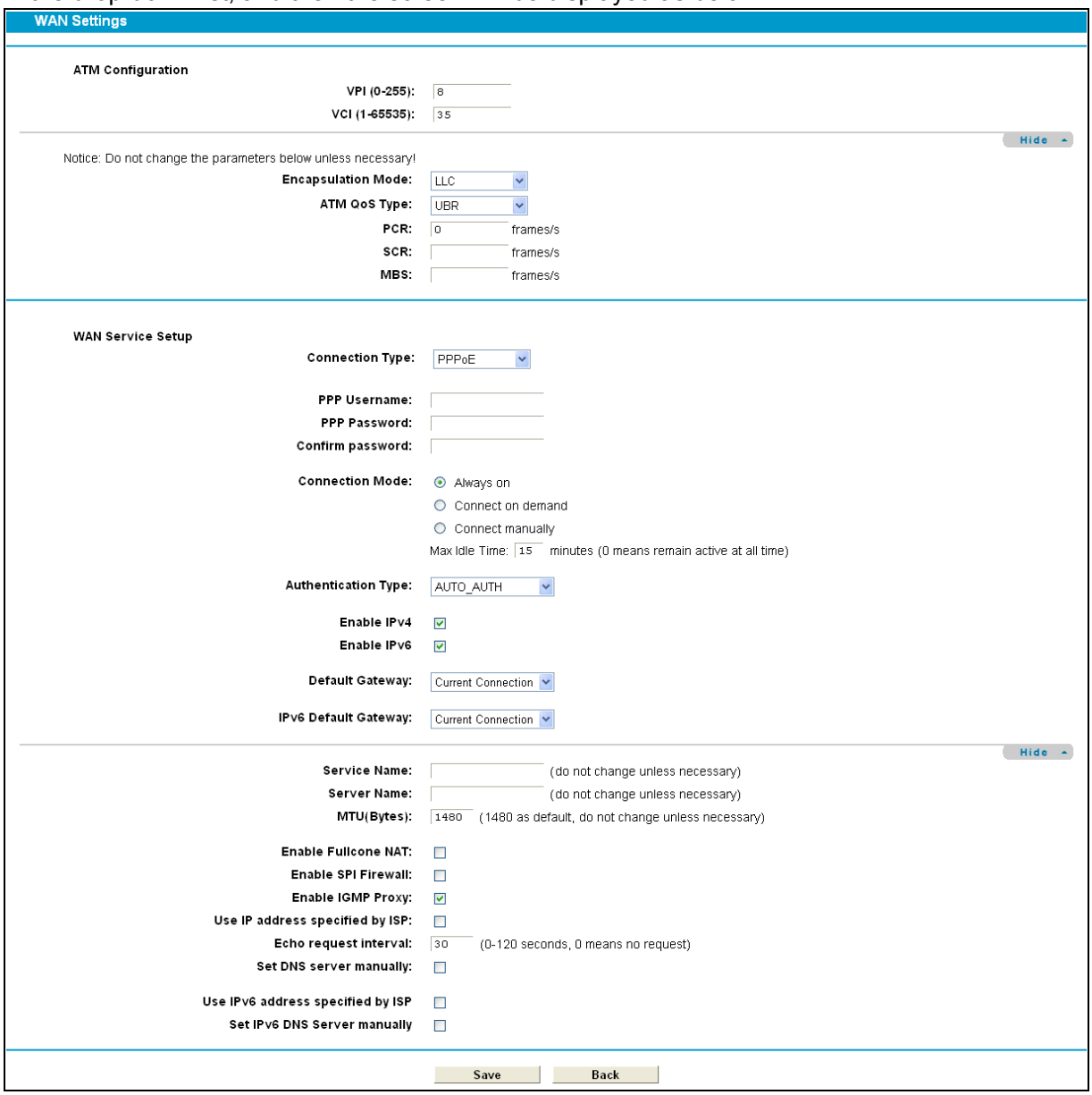


Figure 4-7

- **PPP Username/Password/Confirm Password**: Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Always on:** The connection can be re-established automatically when it is down.

- **Connect on demand:** This mode is dependent on the traffic. If there is no traffic (or **Idle**) for a pre-specified period of time (**MAX Idle Time**), the connection will drop down automatically. And once there is a request for Internet connection, it will be on automatically.
- **Connect Manually:** You can manually control the status of a connection. This mode also supports the **Max Idle Time** function as **Connect on Demand** mode. The Internet connection can be disconnected automatically after a specified inactivity period and re-established when you attempt to access the Internet again.
- **Authentication Type**: Select the **Authentication Type** from the drop-down list, the default method is **AUTO_AUTH**, and you can leave it as a default setting.
- **Enable IPv4:** Check this box to enable IPv4.
- **Enable IPv6:** Check this box to enable IPv6.
- **Default Gateway:** Select a WAN connection from the drop-down list as the IPv4 default gateway.
- **IPv6 Default Gateway:** Select a WAN connection from the drop-down list as the IPv6 default gateway.

Click **Advance**, advanced selections for WAN Service Setup can be shown.

- **Service Name/Server Name**: Enter the Service Name and Server Name if it was provided by your ISP. You can leave them blank, if the ISP doesn't provide them.
- **MTU (bytes):** The default **MTU** (Maximum Transmission Unit) value is 1480 Bytes. Do not change the default value unless required by your ISP.
- **Enable Fullcone NAT**: It is a type of NAT, if not enabled, the default NAT will act.
- **Enable SPI Firewall:** The SPI firewall enhances network's security. Select the option to use a firewall, or else without a firewall.
- **Enable IGMP Proxy**: IGMP (Internet Group Management Protocol) is used to manage multicasting on TCP/IP networks. Some ISPs use IGMP to perform remote configuration for client devices, such as the modem router. It is enabled by default.
- **Use IP address specified by ISP:** Select this option and enter the IP address provided by your ISP.
- **Set DNS Server manually:** Choose "Set DNS Server manually", you can set DNS Server manually here. The modem router will use this DNS Server for priority.
- **Use IPv6 address specified by ISP:** Choose "Use IPv6 address specified by ISP", you can enter the IPv6 address provided by your ISP.
- **Set IPv6 DNS Server manually:** Choose "Set IPv6 DNS Server manually", you can set IPv6 DNS Server manually here. The modem router will use this IPv6 DNS Server for priority.

Click the **Save** button to save the settings.

4.5.1.4 PPPoA

If your ISP provides a **PPPoA** connection and you need to use an ATM Interface, choose **PPPoA** in the drop-down list, and then the screen will be displayed as below.

The configuration is similar to **PPPoE**. Please refer to the section 4.5.1.3 PPPoE to configure this part.

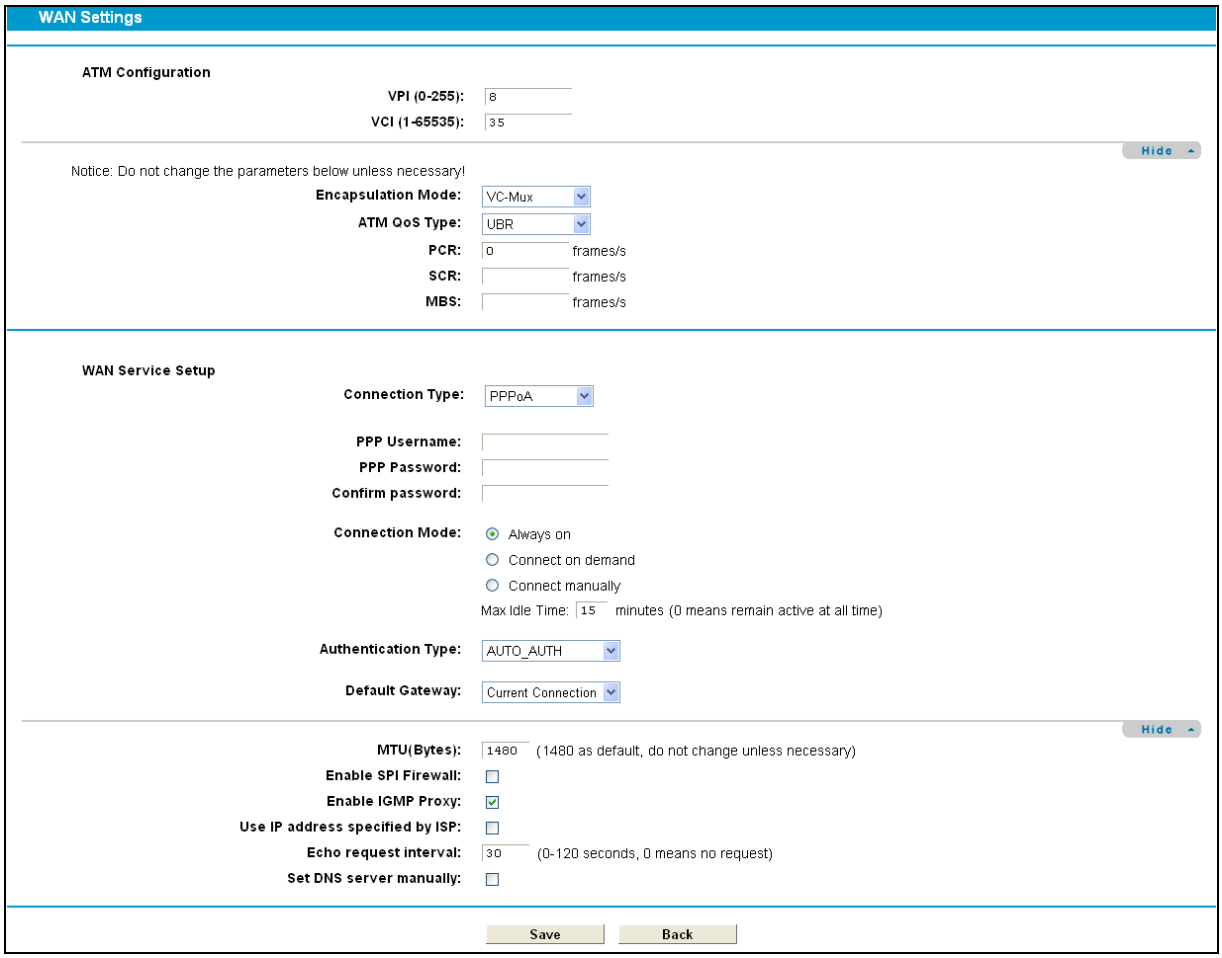


Figure 4-8

4.5.1.5 IPoA

If your ISP provides an IPoA connection, select **IPoA** option for the **Connection Type** on the screen.

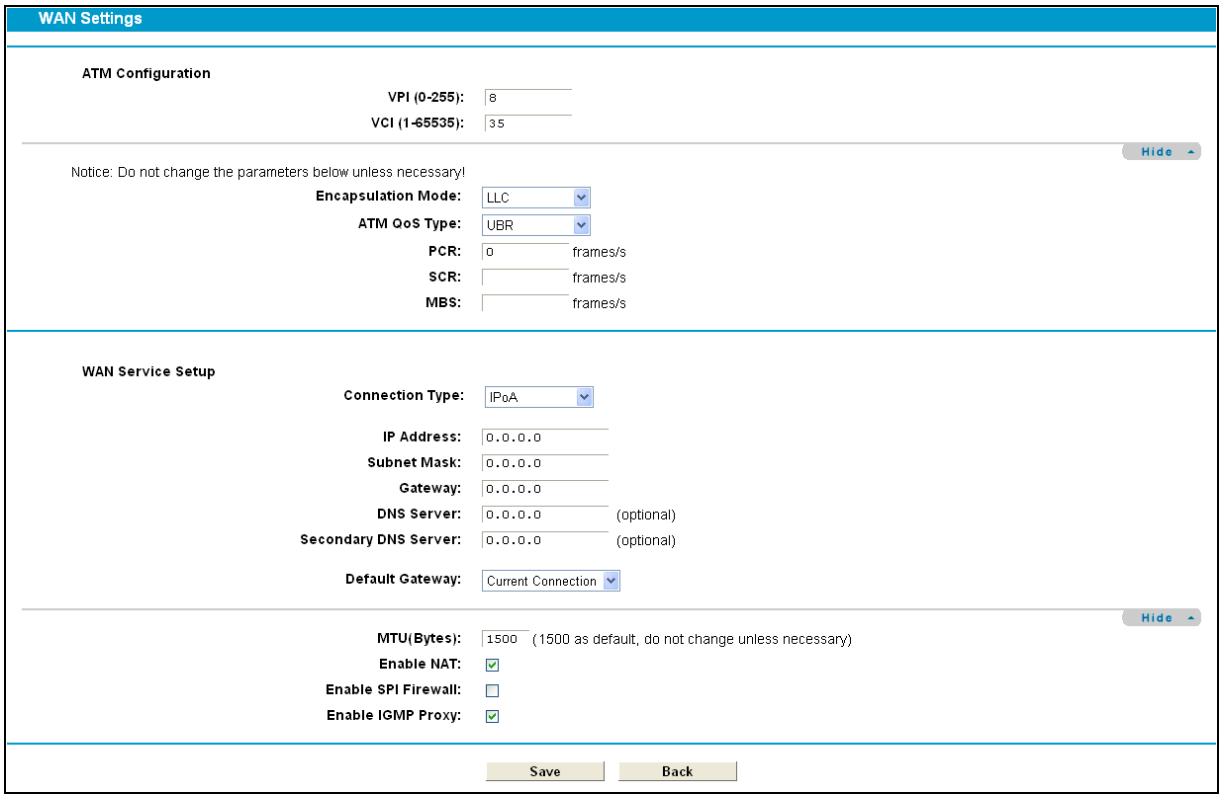


Figure 4-9

- **IP Address/Subnet Mask:** Enter the IP Address and Subnet Mask provided by ISP.
- **DNS Server/Secondary DNS Server:** Type in your preferred DNS server.
- **Default Gateway:** Select a WAN Interface from the drop-down list as the IPv4 default gateway.

4.5.1.6 Bridge

If you select this type of connection, the modem router 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.

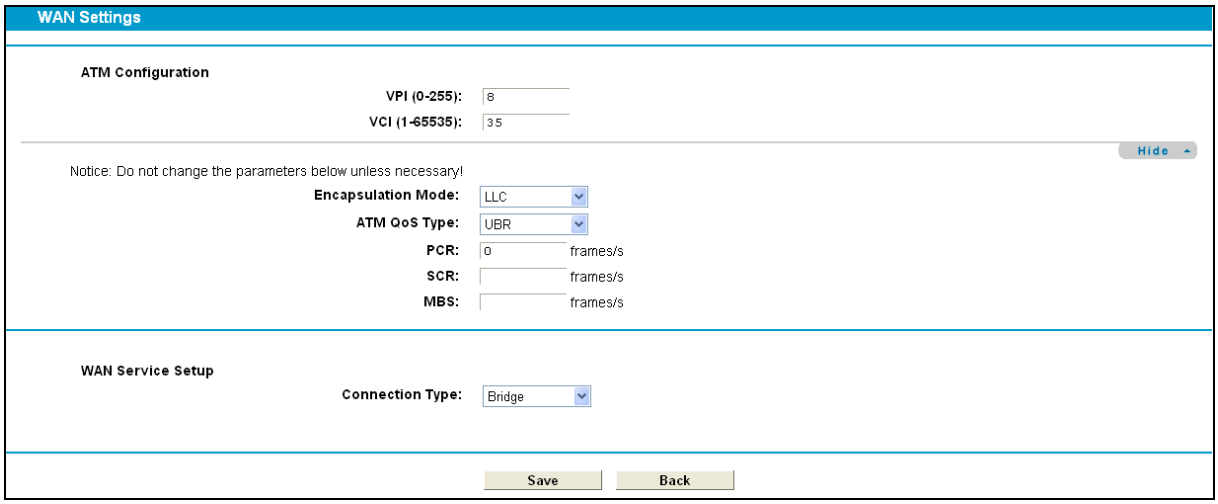


Figure 4-10

Note:

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

4.5.2 Interface Grouping

Choose "**Network**"→"**Interface Grouping**", you can view all the current groups on this page (shown in Figure 4-11).

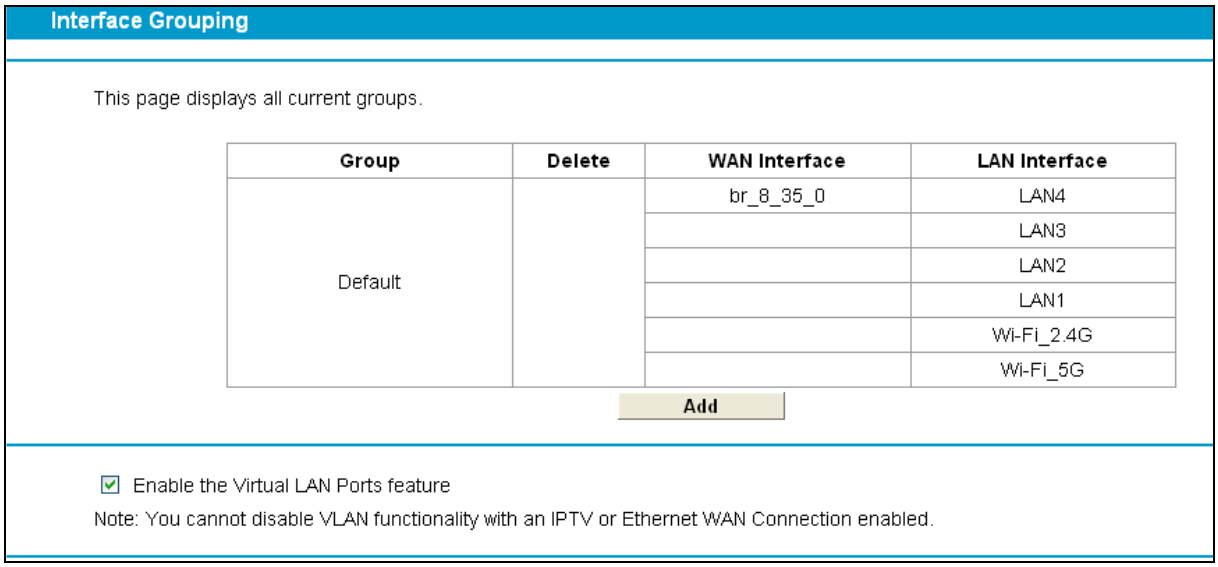


Figure 4-11

- **Enable the Virtual LAN Ports feature:** 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. Because VLANs are based on logical instead of physical connections, it is very flexible for user/host management, bandwidth allocation and resource optimization. If you want to active the Interface Grouping function, please check the box to enable the Virtual LAN Ports feature.

Note:

It is not allowed to disable the VLAN with Ethernet Connection enabled.

To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the **Add** button.

Click the **Add** button. You can add a new interface group in the next screen. For example, if you want LAN1 and LAN3 to be a group called Group 1 over br_8_35_0 WAN interface, you can refer to the following figure.

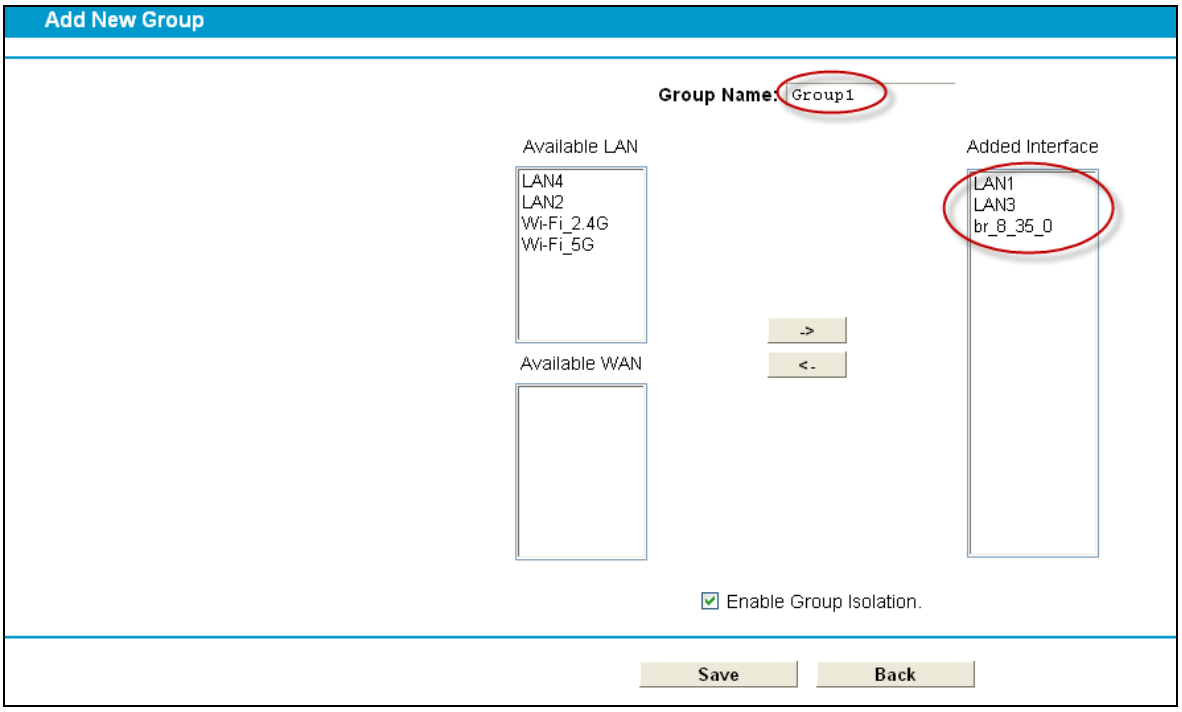


Figure 4-12

Click **Save** to make the entry effective immediately

4.5.3 LAN Settings

Choose "**Network**"→"**LAN Settings**" menu, and you will see the LAN screen (shown in Figure 4-13). Please configure the parameters for LAN ports according to the descriptions below.

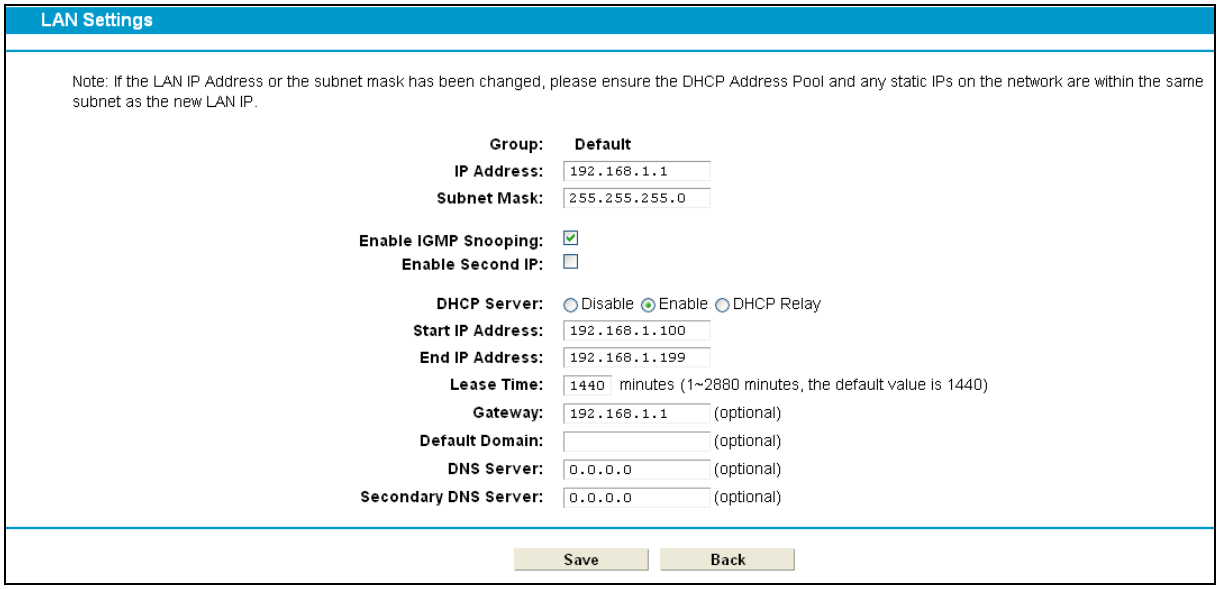


Figure 4-13

- **IP Address:** You can configure the modem router's IP Address and Subnet Mask for LAN Interface.
  - **IP Address:** Enter the modem router's local IP Address, then you can access to the Web-based Utility via the IP Address, the default value is 192.168.1.1.
  - **Subnet Mask:** Enter the modem router's Subnet Mask, the default value is 255.255.255.0.

- **Enable IGMP Snooping:** IGMP Snooping is the process of listening to IGMP (Internet Group Management Protocol) network traffic. The feature prevents hosts on a local network from receiving traffic for a multicast group they have not explicitly joined. It is enabled by default.
- **Enable Second IP:** You can configure the modem router's second IP Address and Subnet Mask for LAN Interface through which you can also access the Web-based Utility as the default IP Address and Subnet Mask.
- **DHCP Server:** The DHCP(Dynamic Host Configuration Protocol) server is enabled by default. DHCP service will supply IP settings to computers connected to the modem router though the Ethernet port which are configured to automatically obtain IP settings. When the modem router is set for DHCP, it becomes the default gateway for DHCP client connected to it. If you change the IP address of the modem router, you must change the range of IP addresses in the pool used for DHCP on the LAN.
  - **Start IP Address:** Enter a value for the DHCP server to start with when issuing IP addresses. The default Start IP Address is **192.168.1.100**, and the Start IP Address must be 192.168.1.100 or greater, but smaller than 192.168.1.254.
  - **End IP Address:** Enter a value for the DHCP server to end with when issuing IP addresses. The End IP Address must be smaller than 192.168.1.254. The default End IP Address is **192.168.1.254**.
  - **Leased Time:** The Leased Time is duration in which a DHCP client can lease its current dynamic IP address assigned by the modem router. After the dynamic IP address has expired, the user will be automatically assigned to a new dynamic IP address. The default is **1440** minutes.

The detailed configuration about DHCP server, please refer to section 4.6 DHCP Server.

4.5.4 IPv6 LAN Settings

Choose menu "**Network**"→"**IPv6 LAN Settings**", you can configure LAN IPv6 interface for your modem router.

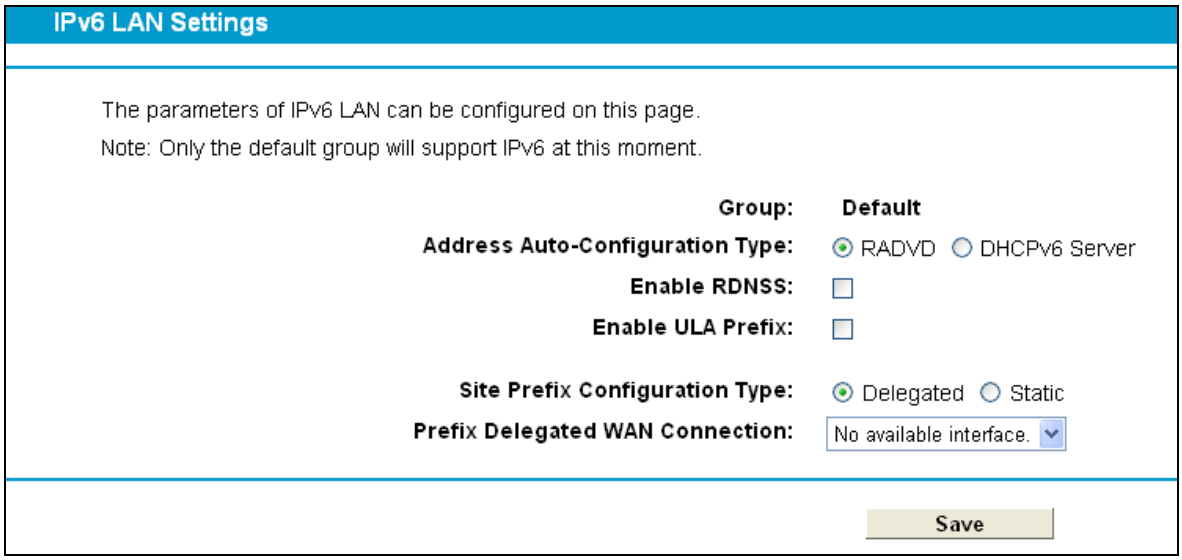


Figure 4-14

- **Address Auto-configuration Type:** Select a type to assign IPv6 addresses to the computers in your LAN. RADVD and DHCPv6 Server are provided.

  1) If RADVD is selected, it doesn't need to be configured.

2) If DHCPv6 Server is selected, please complete the following parameters.

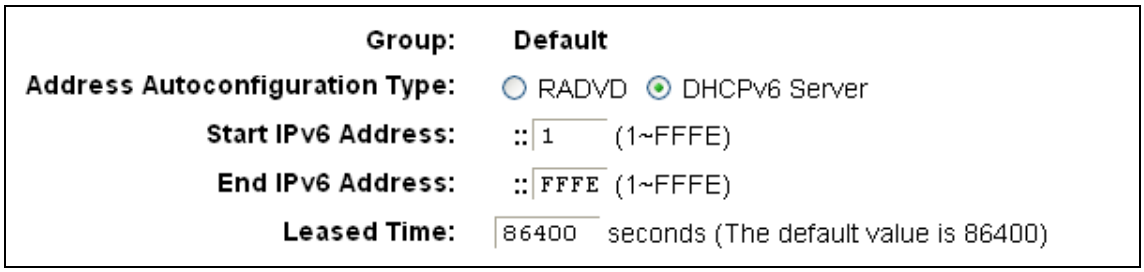


Figure 4-15

- **Start IPv6 Address:** Enter a value for the DHCPv6 server to start with when issuing IPv6 addresses.
- **End IPv6 Address:** Enter a value for the DHCPv6 server to end with when issuing IPv6 addresses.
- **Leased Time:** The Leased Time is the duration in which a DHCP client can lease its current dynamic IPv6 address assigned by the modem router. After the dynamic IPv6 address has expired, the user will be automatically assigned a new dynamic IPv6 address. The default is 86400 seconds.

➢ **Site Prefix Configuration Type:** Select a type to assign prefix to IPv6 addresses. Delegated and Static are provided.

1) If Delegated is selected, please complete the following parameters.

Figure 4-16

- **Prefix Delegated WAN Connection:** Select a WAN connection form the drop-down list to assign prefix.

2) If Static is selected, please complete the following parameters.

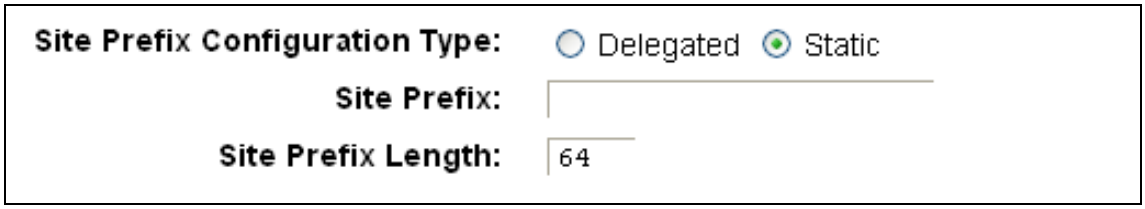


Figure 4-17

- **Site Prefix:** Enter a value for the site prefix.
- **Site Prefix Length:** Enter a value for the site prefix length.

Click the **Save** button to save the settings.

4.5.5 MAC Clone

Choose menu "**Network**"→"**MAC Clone**", you can configure the MAC address of the WAN Interface as shown below.

The WAN Interface List displays the WAN Interfaces you have configured on the section 4.5.1 WAN Settings and its default MAC Address. You can select the corresponding WAN Interface from the drop-down list and click **Clone MAC To** button to clone your current PC MAC, and then click **Save**.

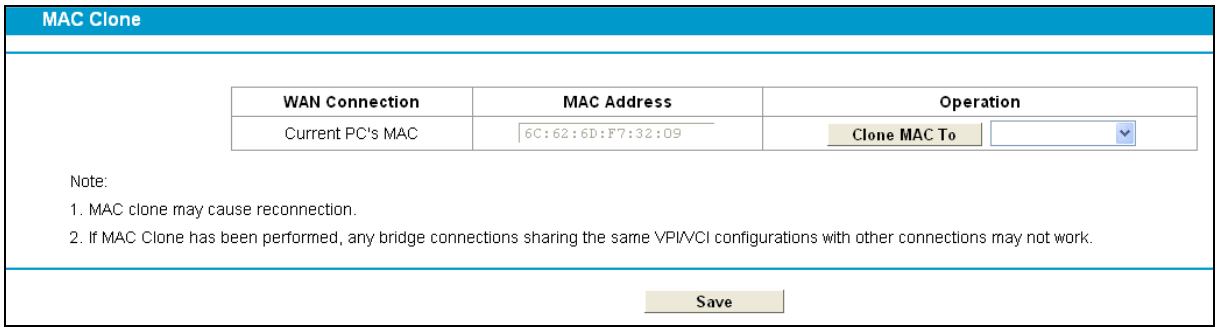


Figure 4-18

Note:

Only the WAN Ports can use MAC Address Clone function. All the clone MAC addresses must not be the same with each other.

4.5.6 ALG Settings

Choose menu "**Network**"→"**ALG Settings**", and then you can configure the basic security in the screen as shown in Figure 4-19.

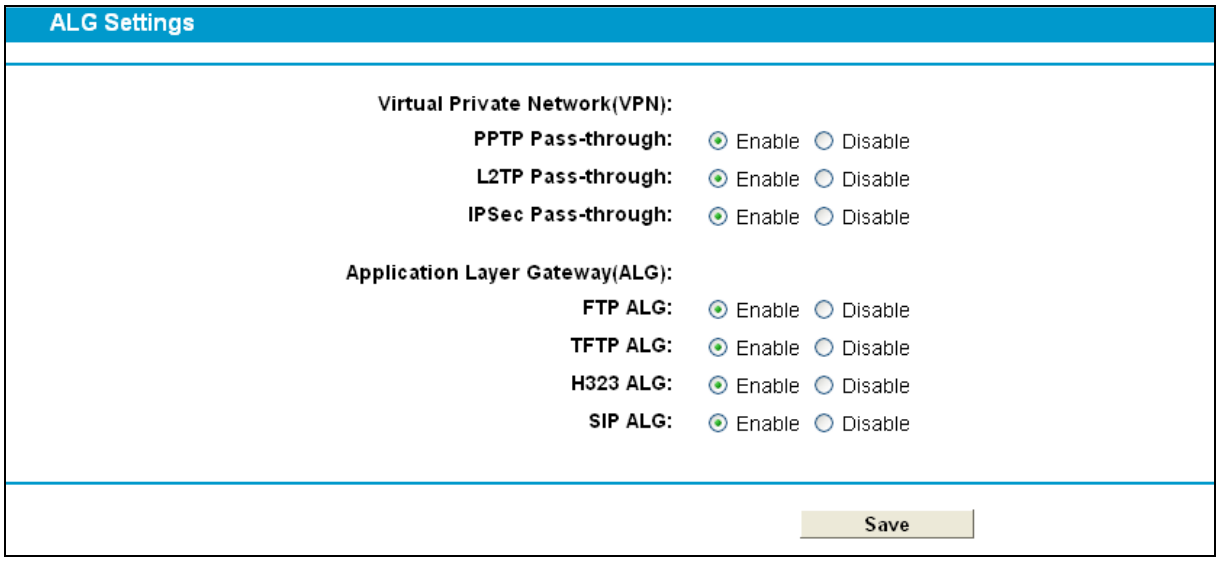


Figure 4-19

- **Virtual Private Network (VPN):** VPN Pass-through must be enabled if you want to allow VPN tunnels using VPN protocols to pass through the modem router.
  - **PPTP Pass-through:** PPTP (Point-to-Point Tunneling Protocol) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. To allow PPTP tunnels to pass through the modem router, click **Enable**.

- **L2TP Pass-through:** L2TP (Layer Two Tunneling Protocol) is the method used to enable Point-to-Point sessions via the Internet on the Layer Two level. To allow L2TP tunnels to pass through the modem router, click **Enable**.
- **IPSec Pass-through:** IPSec (Internet Protocol security) is a suite of protocols for ensuring private, secure communications over Internet Protocol (IP) networks, through the use of cryptographic security services. To allow IPSec tunnels to pass through the modem router, click **Enable**.

➢ **Application Layer Gateway (ALG):** It is recommended to enable ALG (Application Layer Gateway) because ALG allows customized Network Address Translation (NAT) traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols such as FTP, TFTP etc.

- **FTP ALG:** To allow FTP clients and servers to transfer data across NAT, click **Enable**.
- **TFTP ALG:** To allow TFTP clients and servers to transfer data across NAT, click **Enable**.
- **H323 ALG:** To allow H323 clients and servers to transfer data across NAT, click **Enable**.
- **SIP ALG:** To allow SIP clients and servers to transfer data across NAT, click **Enable**.

Click the **Save** button to save your settings.

4.5.7 DSL Settings

Choose "**Advanced Setup**"→"**DSL Settings**", you can select the DSL Modulation Type and the Annex Type in the next screen. The DSL settings can be changed when you meet the physical connection problem. Please check the proper settings with your Internet service provider.

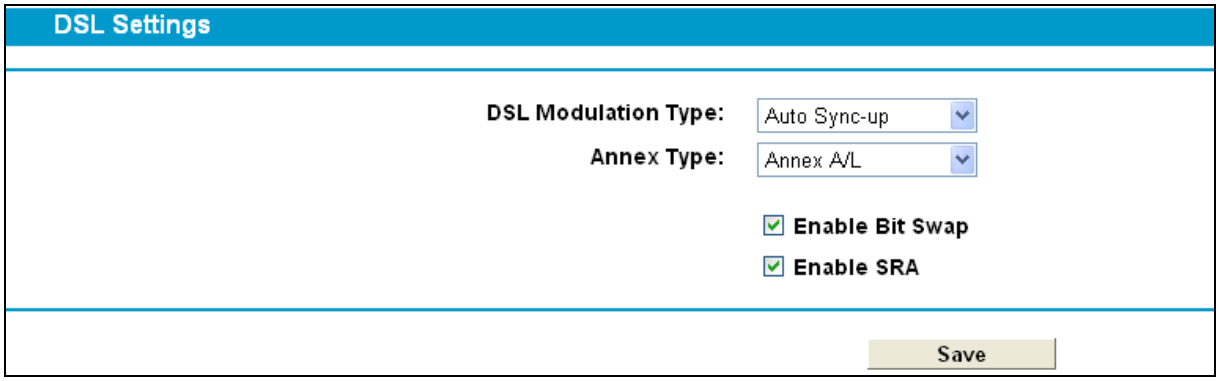


Figure 4-20

➢ **DSL Modulation Type:** Select the DSL operation Modulation Type which your DSL connection uses.
➢ **Annex Type:** Select the DSL operation Annex Type which your DSL connection uses.

Click the **Save** button to save your settings.

4.5.8 IPSec VPN

Choose "**Network**"→"**IPSec VPN**", you can Add/Remove or Enable/Disable the IPSec tunnel connections on the screen as shown in Figure 4-21.

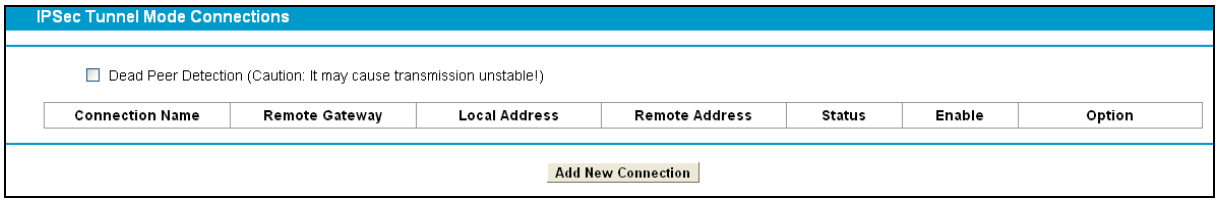
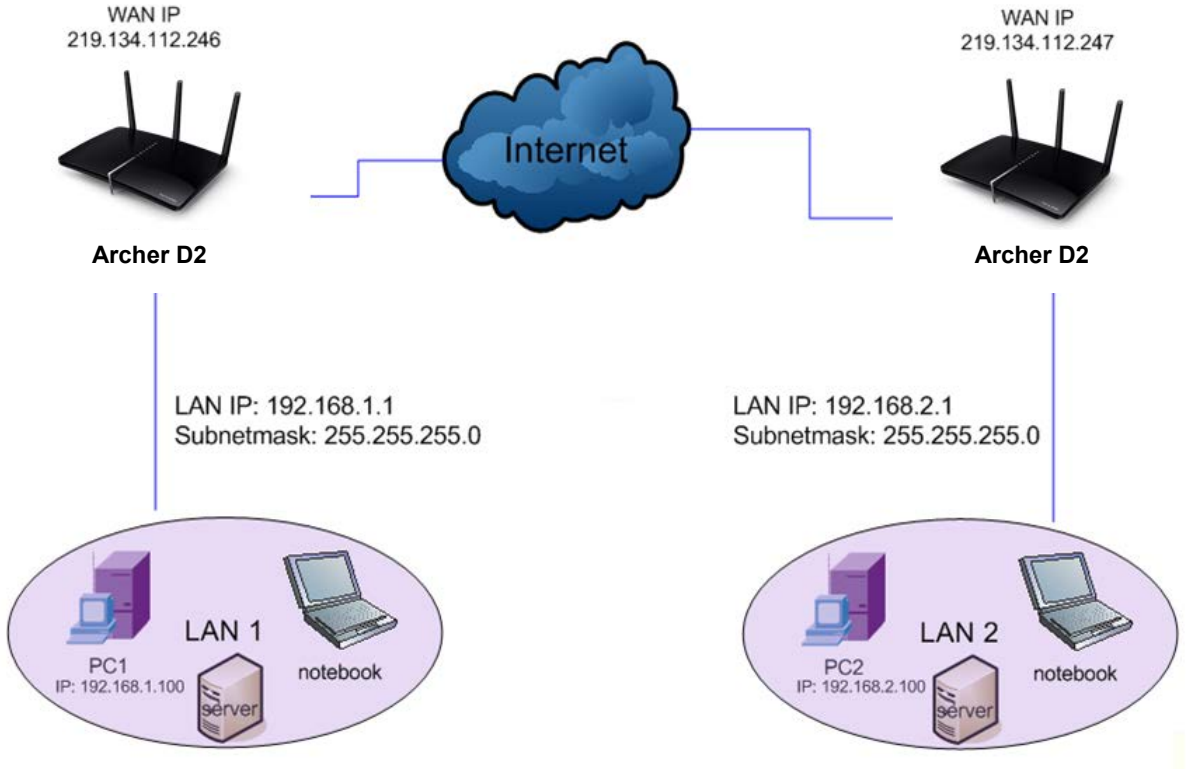


Figure 4-21

This section will guide you to configure a VPN tunnel between two Archer D2s. The topology is as follows.



Note:

You could also use other VPN Routers to set VPN tunnels with Archer D2. Archer D2 supports up to 10 VPN tunnels simultaneously.

Click **Add New Connection** in Figure 4-21 and then you will enter the screen shown in Figure 4-22.

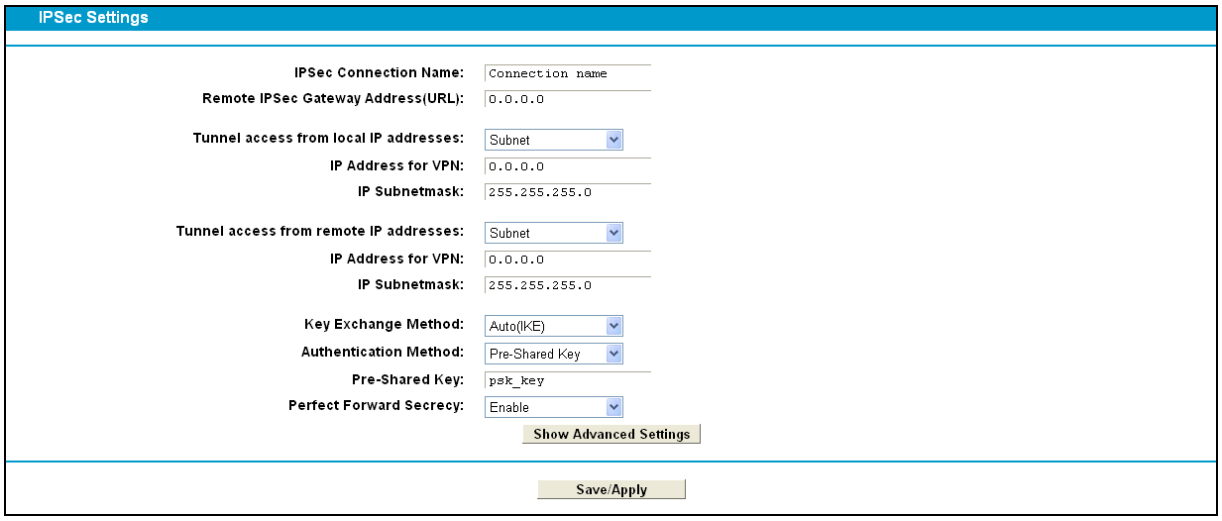


Figure 4-22

- **IPSec Connection Name:** Enter a name for your VPN.
- **Remote IPSec Gateway Address (URL):** Enter the destination gateway IP address which is the public WAN IP or Domain Name of the remote VPN server endpoint. (For example: Input **219.134.112.247** in **Device1**, Input **219.134.112.246** in **Device 2**)
- **Tunnel access from local IP addresses:** Choose Subnet if you want the Whole LAN to join the VPN network, or else choose Single Address if you want single IP to join the VPN network.
- **IP Address for VPN:** Enter the IP address of your LAN. (For example: Input **192.168.1.1** in **Device1**, Input **192.168.2.1** in **Device2**)
- **IP Subnetmask:** Enter the Subnet mask of your LAN. (For example: Input **255.255.255.0** in both **Device1** and **Device2**)
- **Tunnel access from remote IP addresses:** Choose Subnet if you want the Remote Whole LAN to join the VPN network, or else choose Single Address if you want single IP to join the VPN network.
- **IP Address for VPN:** Enter the IP address of the Remote LAN. (For example: Input **192.168.2.1** in **Device1**,Input **192.168.1.1** in **Device2**)
- **IP Subnetmask:** Enter the subnetmask of the remote LAN. (For example: Input **255.255.255.0** in both **Device1** and **Device2**)
- **Key Exchange Method:** Select **Auto (IKE)** or **Manual**.
- **Authentication Method:** Select **Pre-Shared Key** (recommended).
- **Pre-Shared Key:** Input the Pre-Shared key for Authentication. (For example: Input 12345678)
- **Perfect Forward Secrecy:** PFS is an additional security protocol.

After complete the basic settings and click Save/Apply in both **Device1** and **Device2**, PCs in LAN1 could communicate with PCs in remote LAN2. (For example: You can ping the IP address of PC2 which is 192.168.2.100 in PC1)

☞ **Note:**

The VPN Servers Endpoint from both ends must use the same pre-shared keys and Perfect Forward Secrecy settings.

Click **Show Advanced Settings** and then you can configure the Advanced Settings. **We recommend you leave the Advanced Settings as default value.**

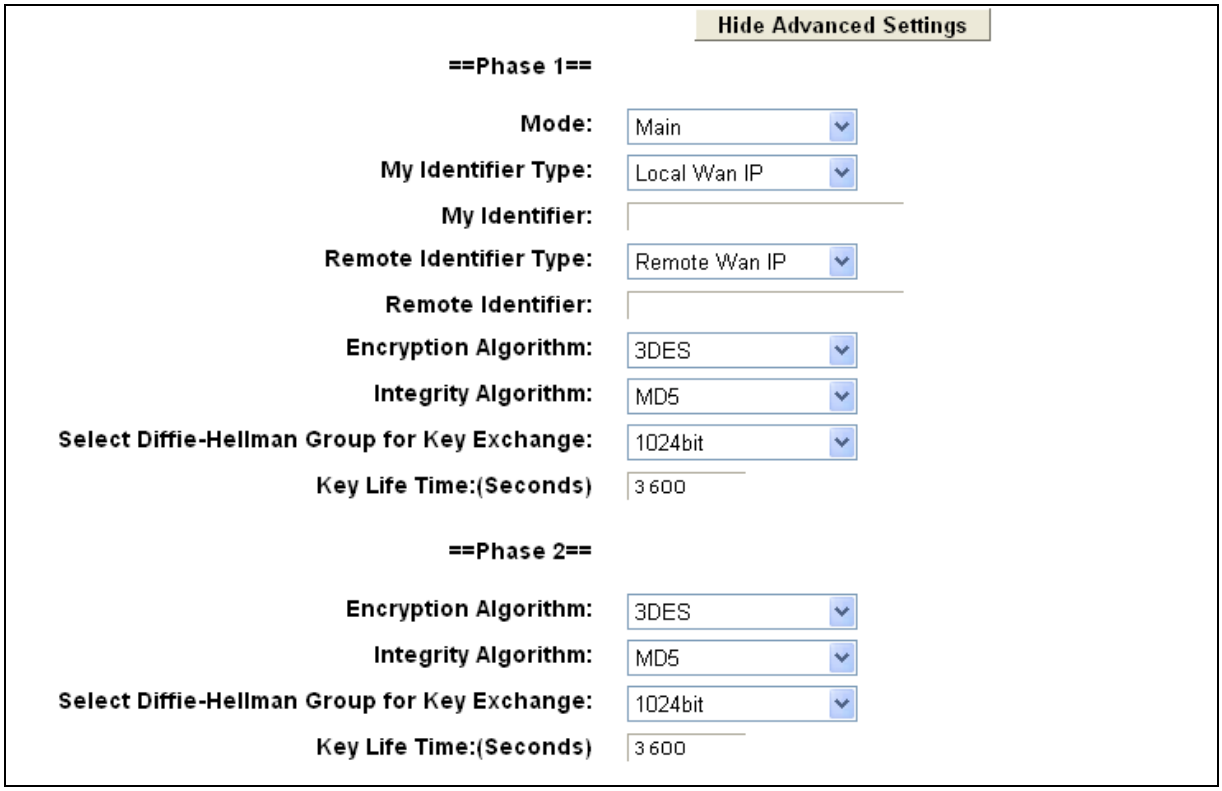


Figure 4-23

- **Mode:** Select **Main Mode** to configure the standard negotiation parameters for IKE phase1. Select **Aggressive Mode** to configure IKE phase1 of the VPN Tunnel to carry out negotiation in a shorter amount of time. (Not Recommended-Less Secure)

☞ **Note:**

The difference between the two modes is that aggressive mode will pass more information in fewer packets, with the benefit of slightly faster connection establishment, at the cost of transmitting the identities of the security firewall in the clear. When using aggressive mode, some configuration parameters such as Diffie-Hellman groups and PFS can not be negotiated, resulting in a greater importance of having "compatible" configuration on both ends.

- **Key Life Time:** Enter the number of seconds for the IPSec lifetime. It is the period of time to pass before establishing a new IPSec security association (SA) with the remote endpoint. The default value is 3600.

☞ **Note:**

If you want to change the default settings of **Advanced Settings**, please make sure that both VPN server endpoints use the same Encryption Algorithm, Integrity Algorithm, Diffie-Hellman Group and Key Life time in both **phase1** and **phase2**.

4.6 IPTV

Choose "**IPTV**", and you will see the screen as shown in Figure 4-24.

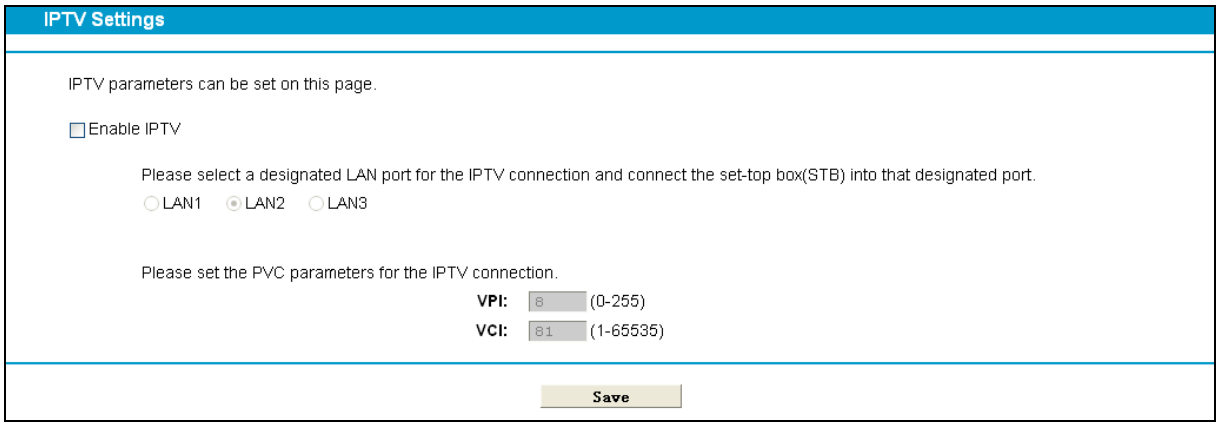


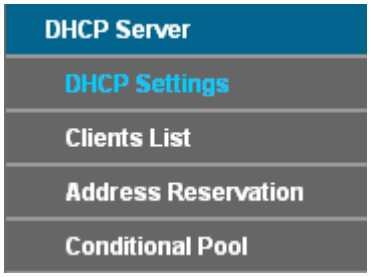
Figure 4-24

- **Enable IPTV:** Check the box to enable IPTV function.
- **VPI (0~255):** 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 (1~65535):** Identifies the virtual channel endpoints in an ATM network. The valid range is from 1 to 65535 (1 to 31 is reserved for well-known protocols). Please input the value provided by your ISP.

Click the **Save** button to save your settings.

4.7 DHCP Server

Choose "**DHCP Server**", you can see the next submenus:



Click any of them, and you will be able to configure the corresponding function.

4.7.1 DHCP Settings

Choose menu "**DHCP Server**"→"**DHCP Settings**", you can configure the DHCP Server on the page as shown in Figure 4-25.The modem router is set up by default as a DHCP (Dynamic Host Configuration Protocol) server, which provides the TCP/IP configuration for all the PC(s) that are connected to the modem router on the LAN.

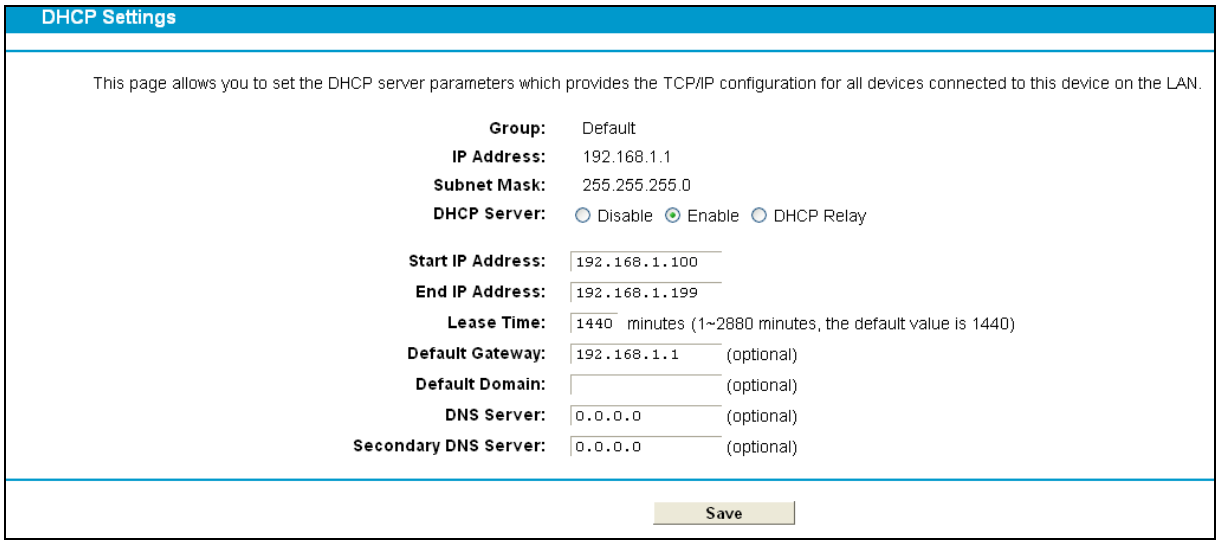
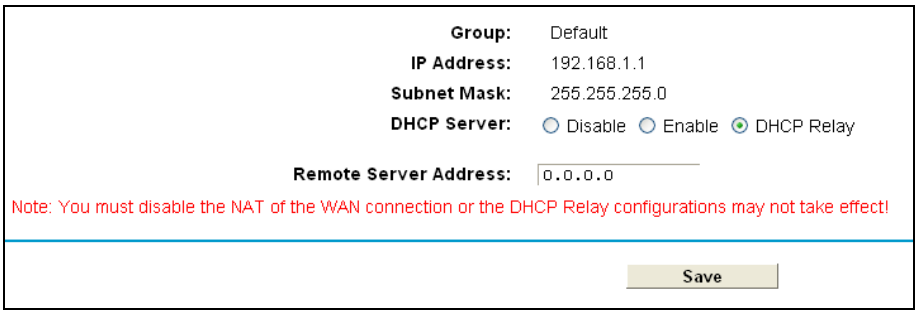


Figure 4-25

- **Group/ IP Address/ Subnet Mask:** Displays group name, IP address and subnet mask. The parameters can be configured on the Interface Grouping page and LAN Settings page.
- **DHCP Server:** If enabled, the modem router will work as a DHCP server, which provides the TCP/IP configuration for all the PC(s) that are connected to it on the LAN.
- **Start IP Address:** Enter a value for the DHCP server to start with when issuing IP addresses. Because the default IP address for the modem router is 192.168.1.1, the default Start IP Address is **192.168.1.100**, and the Start IP Address must be 192.168.1.100 or greater, but smaller than 192.168.1.254.
- **End IP Address:** Enter a value for the DHCP server to end with when issuing IP addresses. The End IP Address must be smaller than 192.168.1.254. The default End IP Address is **192.168.1.254**.
- **Lease Time:** The Leased Time is the amount of time in which a DHCP client can lease its current dynamic IP address assigned by the modem router. After the dynamic IP address has expired, the user will be automatically assigned a new dynamic IP address. The default is **1440** minutes.
- **Default Gateway** (Optional.)**:** It is suggested to input the IP address of the LAN port of the modem router. The default value is 192.168.1.1.
- **Default Domain** (Optional.)**:** Input the domain name of your network.
- **Primary DNS** (Optional.)**:** Input the DNS IP address provided by your ISP.
- **Secondary DNS** (Optional.)**:** Input the IP address of another DNS server if your ISP provides two DNS servers.
- **DHCP Relay:** Select **Relay**, then you will see the next 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.



Note:

1) To use the DHCP server function of the modem router, you must configure all computers on the LAN as "Obtain an IP Address automatically".
2) You have to disable NAT of the WAN connections, or the DHCP Relay may not take effect.
3) If you select **Disabled**, the DHCP function will not take effect.

Click the **Save** button to save your settings.

4.7.2 Clients List

Choose menu "**DHCP Server**"→"**Clients List**", you can view the information about the clients attached to the modem router in the screen as shown in Figure 4-26.

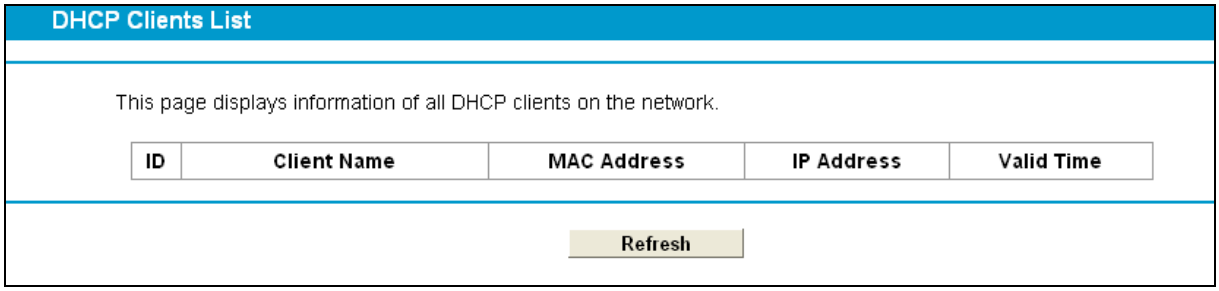


Figure 4-26

- **Client Name:** The name of the DHCP client.
- **MAC Address:** The MAC address of the DHCP client.
- **IP Address:** The IP address that the modem router has allocated to the DHCP client.
- **Valid Time:** The time of the DHCP client leased. After the dynamic IP address has expired, a new dynamic IP address will be automatically assigned to the user.

Click the **Refresh** button to update this page.

4.7.3 Address Reservation

Choose menu "**DHCP Server**"→"**Address Reservation**", you can view and add a reserved address for clients via the next screen (shown in Figure 4-27).When you specify a reserved IP address for a PC on the LAN, that PC will always receive the same IP address each time when it accesses the DHCP server. Reserved IP addresses should be assigned to the servers that require permanent IP settings.

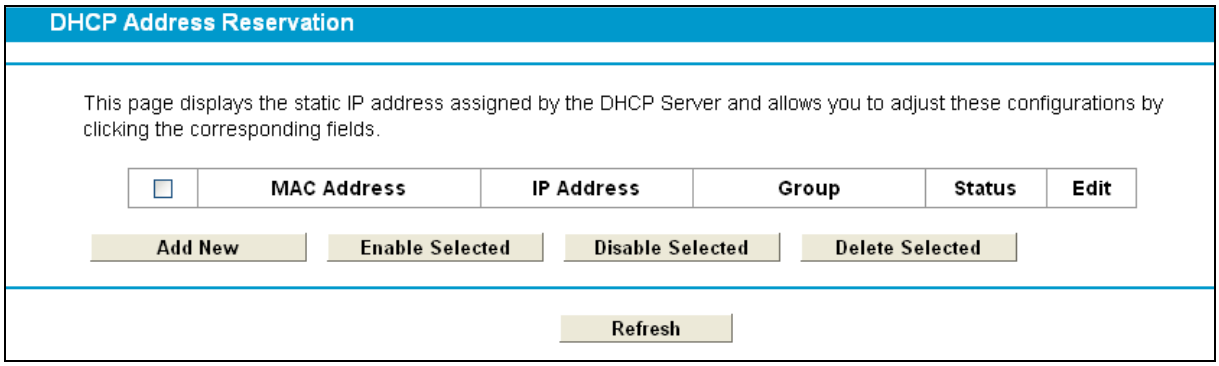


Figure 4-27

- **MAC Address:** The MAC address of the PC for which you want to reserve an IP address.
- **IP Address:** The IP address reserved for the PC by the modem router.
- **Status:** The status of this entry, either **Enabled** or **Disabled**.

To Reserve an IP address:

1. Click the **Add New** button. Then Figure 4-28 will pop up.
2. Enter the MAC address (in XX:XX:XX:XX:XX:XX format.) and IP address (in dotted-decimal notation) of the computer for which you want to reserve an IP address.
3. Click the **Save** button.

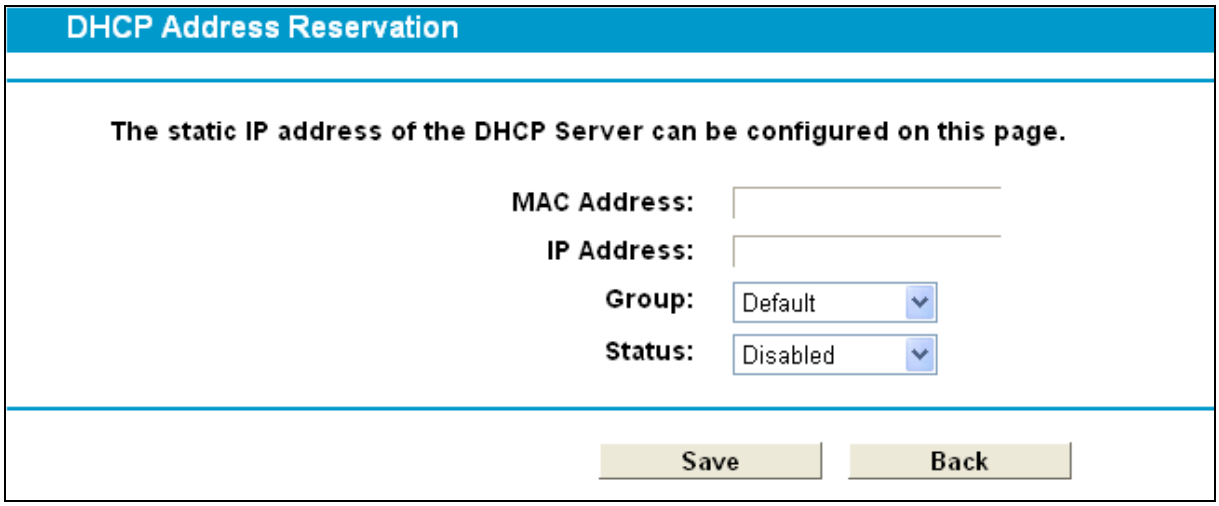


Figure 4-28

To modify or delete an existing entry:

1. Click **Edit** in the entry you want to modify the entry.
2. Modify the information.
3. Click the **Save** button.

Click the **Enable/Disable Selected** button to make selected entries enabled/disabled.
Click the **Delete Selected** button to delete the selected entries.

4.7.4 Conditional Pool

Choose menu "**DHCP Server**"→"**Conditional Pool**", you can see the next screen (shown in Figure 4-29). This page displays vendor class settings and allows you to set parameters for vendor class by clicking corresponding buttons.

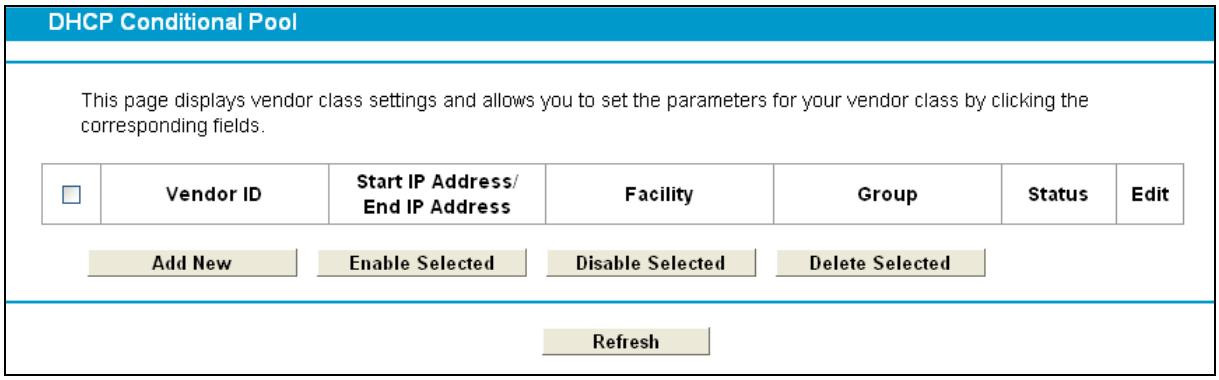


Figure 4-29

To add a vendor class:

1. Click the **Add New** button. Then Figure 4-30 will pop up.
2. Enter parameters for the vendor class.

Click the **Save** button.

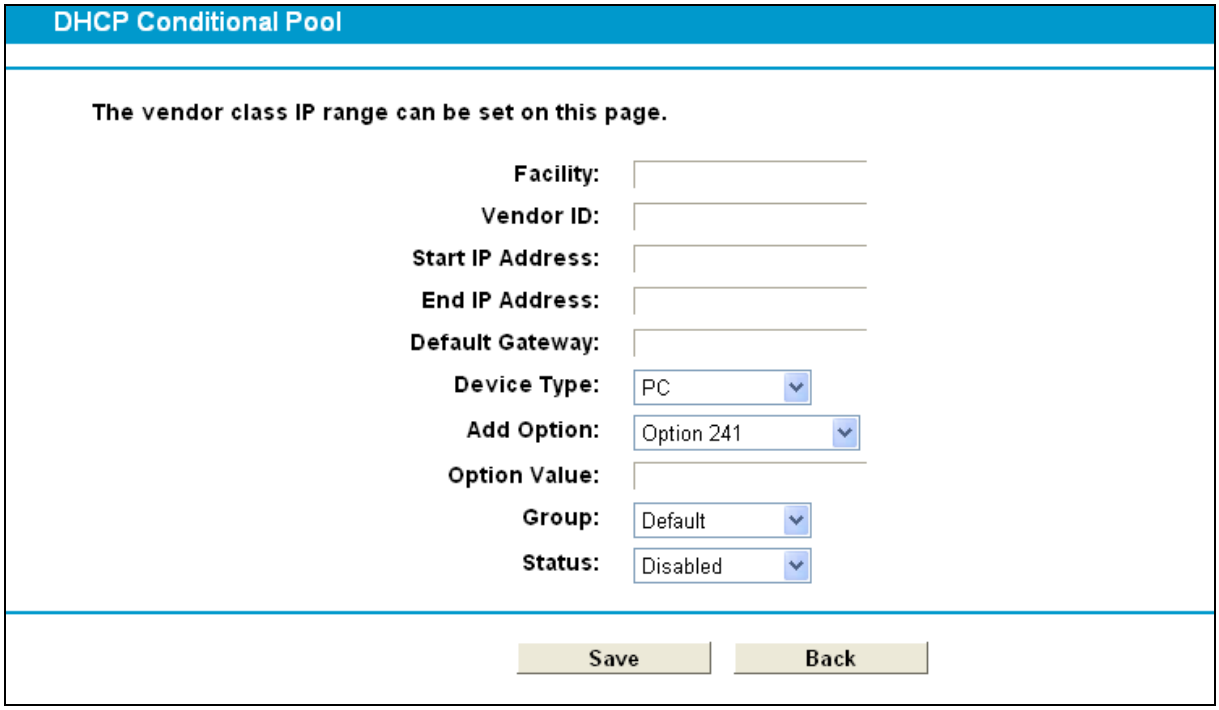


Figure 4-30

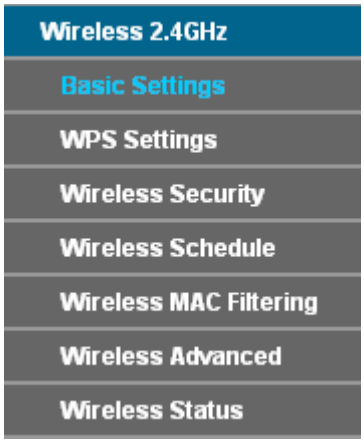
To modify or delete an existing entry:

1. Click **Edit** in the entry you want to modify the entry.
2. Modify the information.
3. Click the **Save** button.

Click the **Enable/Disable Selected** button to make selected entries enabled/disabled.

Click the **Delete Selected** button to delete the selected entries.

4.8 Wireless 2.4GHz



There are seven submenus under the Wireless 2.4 GHz menu: **Basic Settings**, **WPS Settings**, **Wireless Security**, **Wireless Schedule**, **Wireless MAC Filtering**, **Wireless Advanced** and **Wireless Status**. Click any of them, and you will be able to configure the corresponding function.

4.8.1 Basic Settings

Choose menu "**Wireless 2.4GHz**" → "**Basic Settings**", you can configure the basic settings for the wireless network of 2.4GHz on this page.

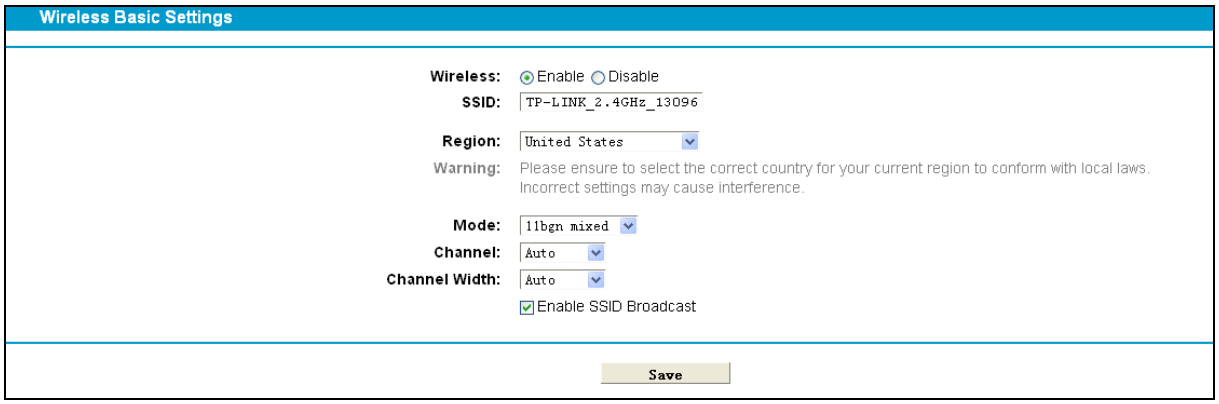


Figure 4-31

- **SSID:** Wireless network name. Enter a desired SSID which is case-sensitive and must not exceed 32 characters. The default SSID is TP-LINK_2.4GHz_XXXXXX (xx is the last six numbers of MAC address).
- **Region:** Select your region from the drop-down list. This field specifies the region where the wireless function of the modem router can be used. It may be illegal to use the wireless function of the modem router in a region other than one of those specified in this field. If your country or region is not listed, please contact your local government agency for assistance.

  ☞ **Note:**

  Limited by local law regulations, version for North America does not have region selection option.

- **Mode:** Select the desired mode.
  11b only: Select if all of your wireless clients are 802.11b.
  11g only: Select if all of your wireless clients are 802.11g.
  11n only: Select only if all of your wireless clients are 802.11n.

11bg mixed: Select if you are using both 802.11b and 802.11g wireless clients.

11bgn mixed: Select if you are using a mix of 802.11b, 11g, and 11n wireless clients.

When 802.11g mode is selected, only 802.11g wireless stations can be connected to the modem router. When 802.11n mode is selected, only 802.11n wireless stations can connect to the modem router. It is strongly recommended that you set the Mode to **802.11bgn mixed**, and all of 802.11b, 802.11g, and 802.11n wireless stations can connect to the modem router.

- **Channel:** Select the channel you want to use from the drop-down list. 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.
- **Channel Width:** Select the channel width from the drop-down list. The default setting is automatic, which can adjust the channel width for your clients automatically.

Note:

If **11b only**, **11g only**, or **11bg mixed** is selected in the **Mode** field, the **Channel Width** selecting field will turn grey and the value will become 20M, which is unable to be changed.

- **Enable SSID Broadcast:** When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the modem router. If this checkbox is selected, the wireless router will broadcast its name (SSID) on the air.

Click **Save** to save your settings.

4.8.2 WPS Settings

This section will guide you to add a new wireless device to an existing network quickly by **WPS** (also called **QSS**) function.

a). Choose menu "**WPS Settings**", and you will see the next screen (shown in Figure 4-32).

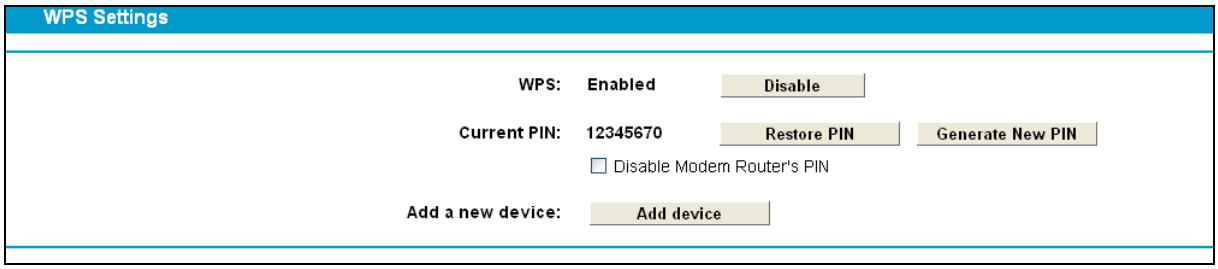


Figure 4-32

- **WPS:** Enable or disable the WPS function here.
- **Current PIN:** The current value of the modem router's PIN is displayed here.
- **Restore PIN:** Restore the PIN of the modem router to its default.
- **Generate New PIN:** Click this button to get a new random PIN code. You can ensure the network security by generating a new PIN.
- **Add device:** You can add a new device to the existing network manually by clicking this button.

b). To add a new device:

If the wireless adapter supports Wi-Fi Protected Setup (WPS), you can establish a wireless connection between wireless adapter and modem router using either Push Button Configuration (PBC) method or PIN method.

Note:

To build a successful connection by WPS, you should also do the corresponding configuration of the new device for WPS function meanwhile.

I. Use the Wi-Fi Protected Setup Button

Use this method if your client device has a Wi-Fi Protected Setup button.

Step 1: Press the WPS button on the back panel of the modem router, as shown in the following figure.

You can also keep the default WPS Status as **Enabled** and click the **Add device** button in Figure 4-32, then Choose "**Press the WPS button of the new device within the next two minutes**" and click **Connect**. (Shown in the following figure)

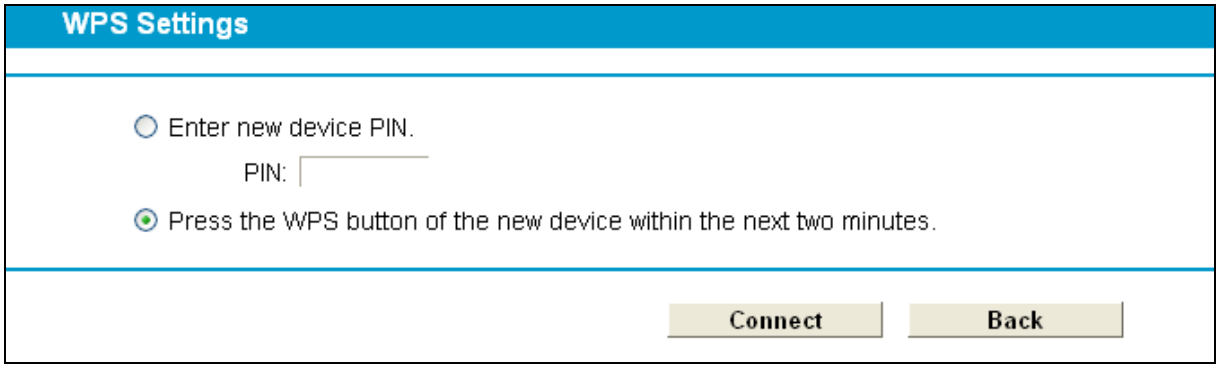


Figure 4-33

Step 2: Press and hold the WPS button of the client device directly.

Step 3: The Wi-Fi Protected Setup LED flashes for two minutes during the Wi-Fi Protected Setup process.

Step 4: When the WPS LED is on, the client device has successfully connected to the modem router.

Refer back to your client device or its documentation for further instructions.

II. Enter the client device's PIN on the modem router

Use this method if your client device has a Wi-Fi Protected Setup PIN number.

Step 1: Keep the default WPS Status as **Enabled** and click the **Add device** button in Figure 4-32, then the following screen will appear.

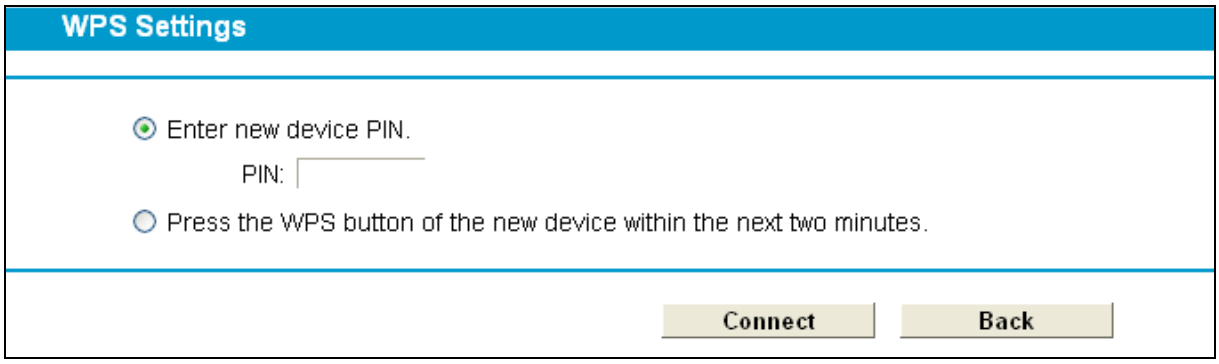


Figure 4-34

Step 2: Enter the PIN number from the client device in the field on the above WPS screen. Then click **Connect** button.

Step 3: "**Connect successfully**" will appear on the screen of Figure 4-34, which means the client device has successfully connected to the modem router.

III. Enter the modem router's PIN on your client device

Use this method if your client device asks for the modem router's PIN number.

Step 1: On the client device, enter the PIN number listed on the modem router's Wi-Fi Protected Setup screen. (It is also labeled on the bottom of the modem router.)

Step 2: The Wi-Fi Protected Setup LED flashes for two minutes during the Wi-Fi Protected Setup process.

Step 3: When the WPS LED is on, the client device has successfully connected to the modem router.

Step 4: Refer back to your client device or its documentation for further instructions.

☞ **Note:**

1) The WPS LED on the modem router will light green for five minutes if the device has been successfully added to the network.

2) The WPS function cannot be configured if the Wireless Function of the modem router is disabled. Please make sure the Wireless Function is enabled before configuring the WPS.

4.8.3 Wireless Security

Choose menu "**Wireless 2.4GHz**"→" **Wireless Security**", you can configure the security settings of your wireless network.

There are three wireless security modes supported by the modem router: WPA/WPA2 – Personal, WPA/WPA2 – Enterprise, WEP (Wired Equivalent Privacy).

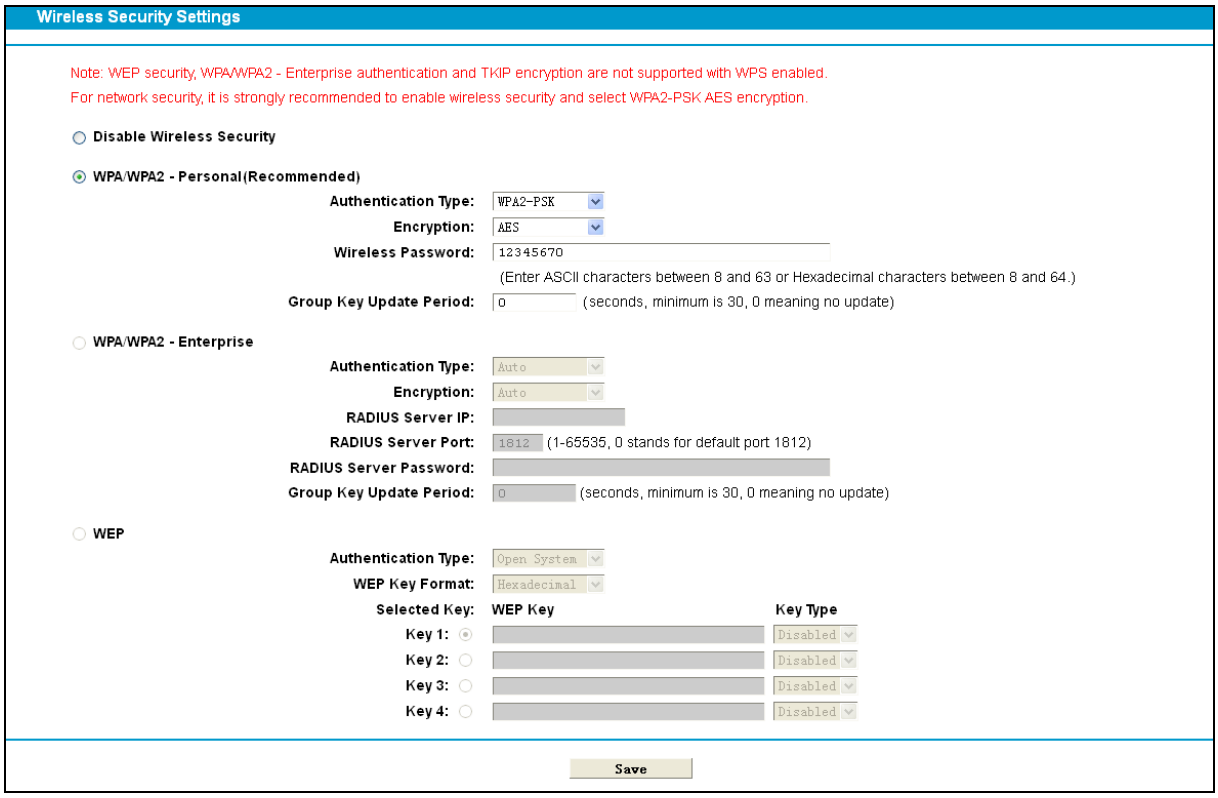
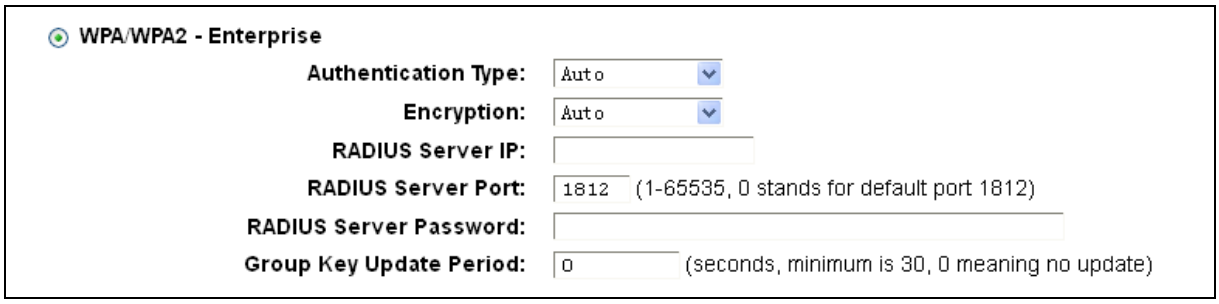


Figure 4-35

- **Disable Wireless Security:** If you do not want to use wireless security, check this radio button. But it's strongly recommended to choose one of the below modes to ensure security.
- **WPA/WPA2-Personal:** It's the WPA/WPA2 authentication type based on pre-shared passphrase. It is chosen by default.
  - **Authentication Type:** You can choose the type for the WPA/WPA2-Personal security from the drop-down list. The default setting is **WAP2-PSK**.
  - **Encryption:** You can select **Auto**, **TKIP** or **AES** as Encryption.
  - **Wireless Password:** You can enter ASCII characters between 8 and 63 characters or 8 to 64 Hexadecimal characters. The default password is the same with the default PIN code, which is labeled on the bottom of the modem router or can be found in Figure 4-32.
  - **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.
- **WPA/WPA2 – Enterprise:** It's based on Radius Server.

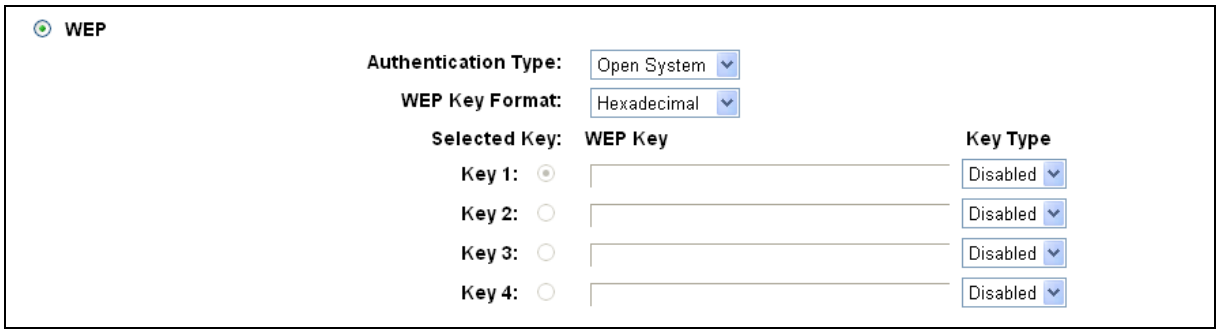


  - **Authentication Type:** You can choose the type for the WPA/WPA2-Enterprise security from the drop-down list. The default setting is **Auto**, which can select **WPA** or **WPA2** as

authentication type automatically based on the wireless station's capability and request.

- **Encryption:** You can select **Auto**, **TKIP** or **AES** as Encryption.
- **RADIUS Server IP:** Enter the IP address of the Radius Server.
- **RADIUS Server Port:** Enter the port that radius service used.
- **RADIUS Server Password:** Enter the password for the Radius Server.
- **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.

➢ **WEP:** It is based on the IEEE 802.11 standard.



- **Authentication Type:** You can choose the type for the WEP security from the drop-down list. The default setting is **Open System**.
- **WEP Key Format: Hexadecimal** and **ASCII** formats are provided here. **Hexadecimal** format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length. **ASCII** format stands for any combination of keyboard characters in the specified length.
- **WEP Key:** Select which of the four keys will be used and enter the matching WEP key that you create. Make sure these values are identical on all wireless stations in your network.
- **Key Type:** You can select the WEP key length (64-bit, or 128-bit.) for encryption. "Disabled" means this WEP key entry is invalid.

  64-bit: You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not promoted) or 5 ASCII characters.

  128-bit: You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not promoted) or 13 ASCII characters.

Be sure to click the **Save** button to save your settings on this page.

4.8.4 Wireless Schedule

Choose menu "**Wireless 2.4GHz**"→"**Wireless Schedule**", you can configure the Task Schedule as shown below.

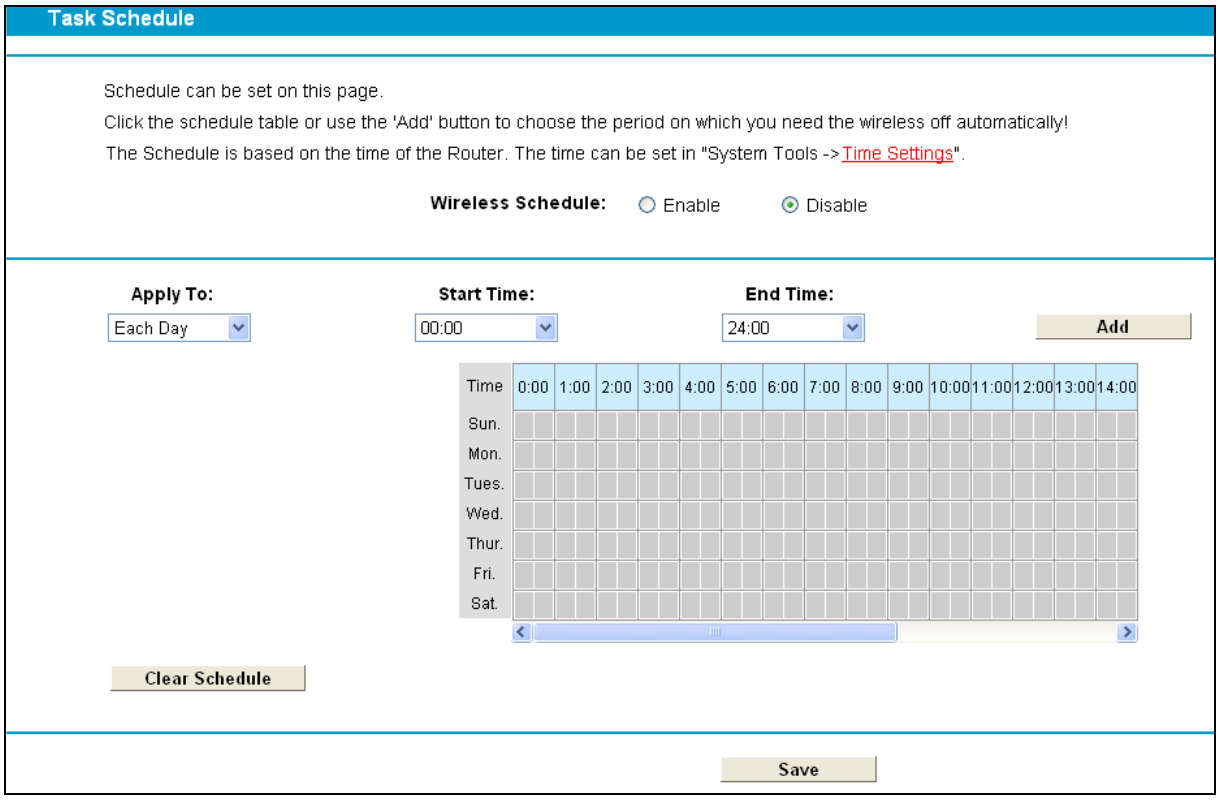


Figure 4-36

☞ Note:

The time you set is the period you need the wireless off.

Before configure the wireless schedule, please set system time first which refer to 4.23.2 Time Settings, then you can enable or disable Wireless Schedule.

- **Apply To:** Select the day or days you want to switch the wireless off.
- **Start Time, End Time:** You can select all day-24 hours or you may enter the **Start Time** and **End Time** in the corresponding field.
- **Add:** Click this button to add your selected time to the below table.

Click the **Clear Schedule** button to clear your settings in the table.

Click **Save** to complete the settings.

4.8.5 Wireless MAC Filtering

Choose menu "**Wireless 2.4GHz**" → "**Wireless MAC Filtering**", you can control the wireless access by configuring the **Wireless MAC Filtering** function, shown in Figure 4-37.

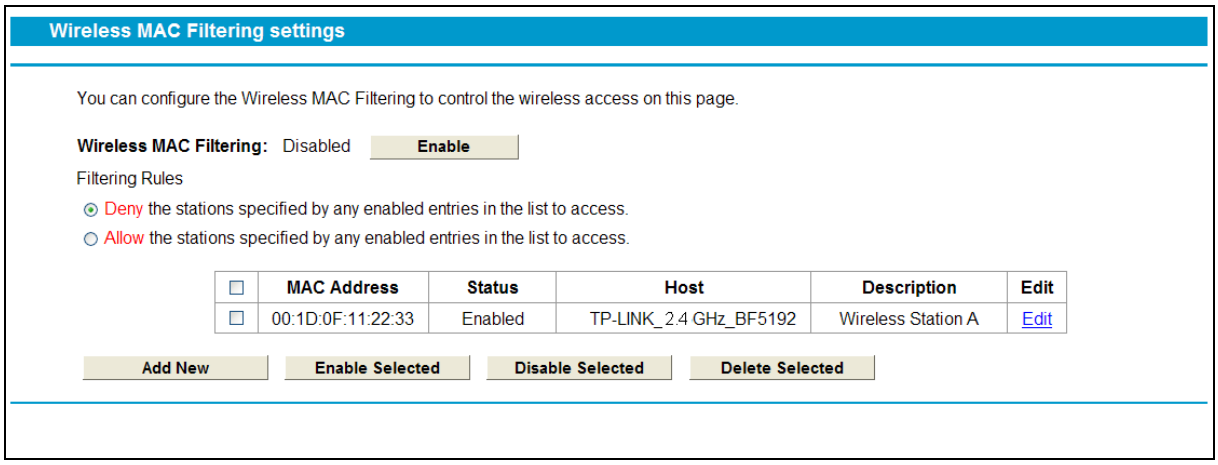


Figure 4-37

To filter wireless users by MAC Address, click **Enable**. The default setting is **Disabled**.

- **MAC Address:** The wireless station's MAC address that you want to filter.
- **Status:** The status of this entry, either **Enabled** or **Disabled**.
- **Host:** The wireless network name (SSID).
- **Description:** A simple description of the wireless station.

To Add a Wireless MAC Address filtering entry, click the **Add New** button. The following page will appear, shown in Figure 4-38:

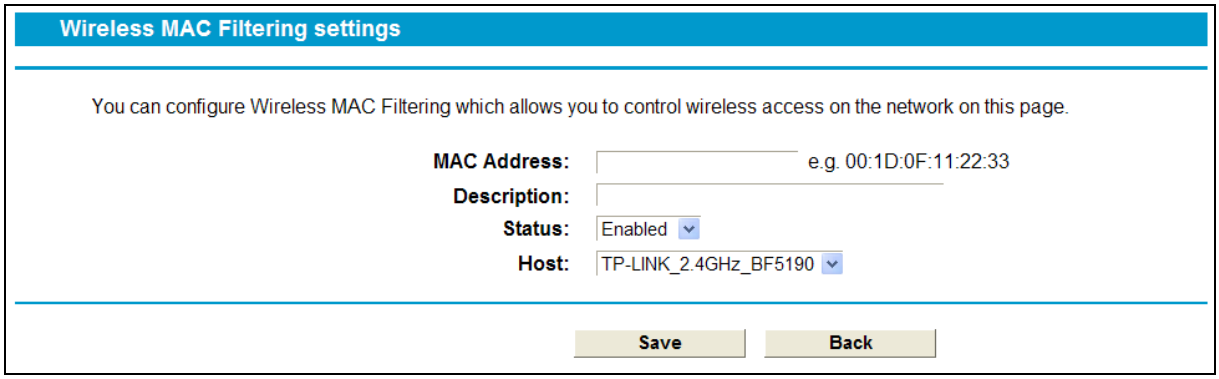


Figure 4-38

To add or modify a MAC Address Filtering entry, follow these instructions:

1. Enter the appropriate MAC Address into the **MAC Address** field. The format of the MAC Address is XX:XX:XX:XX:XX:XX (X is any hexadecimal digit). For example: 00:1D:0F:11:22:33.
2. Give a simple description for the wireless station in the **Description** field. For example: Wireless station A.
3. Select **Enabled** or **Disabled** for this entry from the **Status** drop-down list.
4. Select **Host** from the drop-down list.
5. Click the **Save** button to save this entry.

To edit or delete an existing entry:

1. Click the **Edit** in the entry you want to modify.

2. Modify the information.
3. Click the **Save** button.

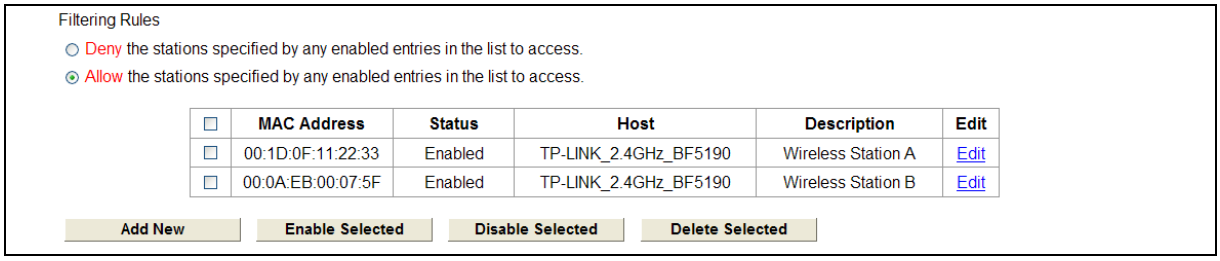
Click the **Enable/ Disabled Selected** button to make selected entries enabled or disabled.

Click the **Delete Selected** button to delete the selected entries.

For example: If you desire that the wireless station A with MAC address 00:1D:0F:11:22:33 and the wireless station B with MAC address 00:0A:EB:00:07:5F are able to access the modem router, but all the other wireless stations cannot access the Modem router, you can configure the **Wireless MAC Address Filtering** list by following these steps:

1. Click the **Enable** button to enable this function.
2. Select the radio button "**Allow the stations specified by any enabled entries in the list to access**" for **Filtering Rules**.
3. Delete all or disable all entries if there are any entries already.
4. Click the **Add New** button.
   1) Enter the MAC address 00:1D:0F:11:22:33/00:0A:EB:00:07:5F in the **MAC Address** field.
   2) Enter wireless station A/B in the **Description** field.
   3) Select **Enabled** in the **Status** drop-down list.
   4) Select **TP-LINK_2.4GHz** for the **Host**.
   5) Click the **Save** button.

The filtering rules that configured should be similar to the following list:



4.8.6 Wireless Advanced

Choose menu "**Wireless 2.4GHz**"→"**Wireless Advanced**", you can configure the advanced settings of your wireless network.

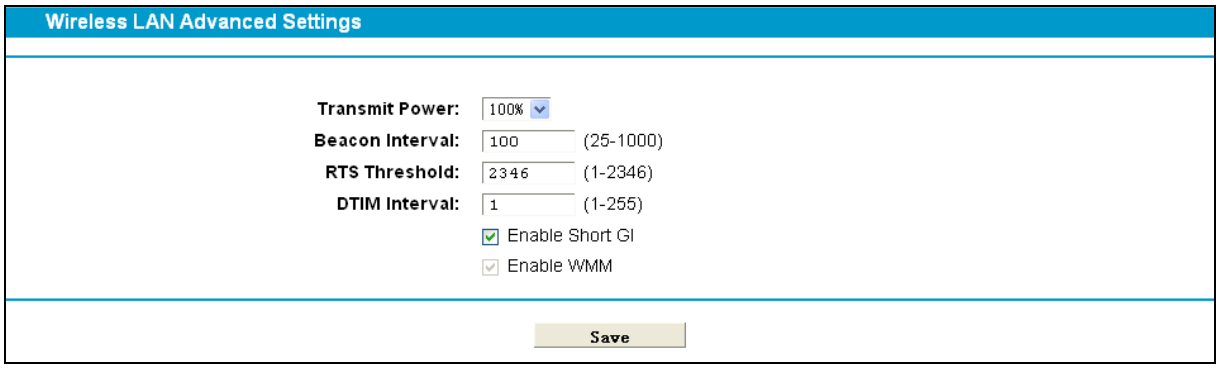


Figure 4-39

- **Transmit Power:** Here you can specify the transmit power of the modem router. You can select 100%, 50% or 25%. 100% is the default setting and is recommended.

- **Beacon Interval:** Enter a value between 25-1000 milliseconds for Beacon Interval here. The beacons are the packets sent by the modem router to synchronize a wireless network. Beacon Interval value determines the time interval of the beacons. The default value is 100.
- **RTS Threshold:** Here you can specify the RTS (Request to Send) Threshold. If the packet is larger than the specified RTS Threshold size, the modem router will send RTS frames to a particular receiving station and negotiate the sending of a data frame. The default value is 2346.
- **DTIM Interval:** This value determines 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. You can specify the value between 1-255 Beacon Intervals. The default value is 1, which indicates the DTIM Interval is the same as Beacon Interval.
- **Enable Short GI:** It is recommended to Enable Short GI, which will increase the data capacity by reducing the guard interval time.
- **Enable WMM:** This function guarantee the packets with high-priority messages being transmitted preferentially. It is strongly recommended to enable WMM.

☞ **Note:**

If you are not familiar with the setting items in this page, it's strongly recommended to keep the provided default values; otherwise it may result in lower wireless network performance.

4.8.7 Wireless Status

Choose menu "**Wireless 2.4GHz**"→"**Wireless Status**", you can see the MAC Address, Current Status, Received Packets and Sent Packets for each connected wireless station.

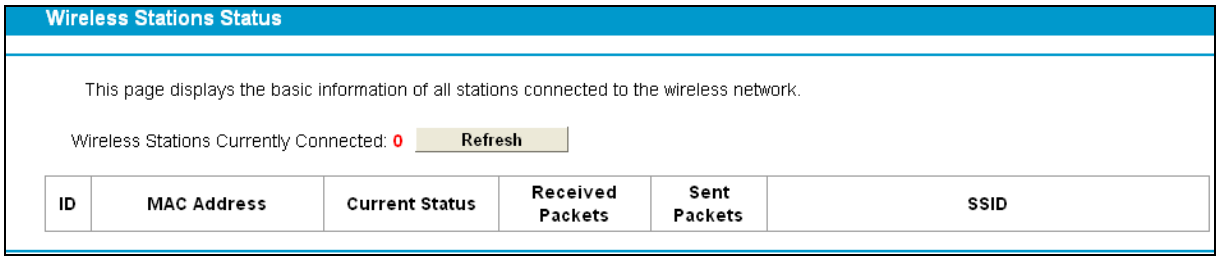
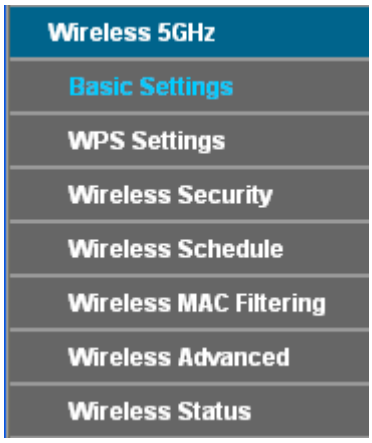


Figure 4-40

- **MAC Address:** The connected wireless station's MAC address.
- **Current Status:** The connected wireless station's running status.
- **Received Packets:** Packets received by the station.
- **Sent Packets:** Packets sent by the station.
- **SSID:** The wireless network name.

Click on the **Refresh** button to update this page.

4.9 Wireless 5GHz



There are seven submenus under the Wireless 5GHz menu: **Basic Settings**, **WPS Settings**, **Wireless Security**, **Wireless Schedule**, **Wireless MAC Filtering**, **Wireless Advanced** and **Wireless Status**. Click any of them, and you will be able to configure the corresponding function.

4.9.1 Basic Settings

Choose menu "**Wireless 5GHz**" → "**Basic Settings**", you can configure the basic settings for the wireless network of 5GHz on this page.

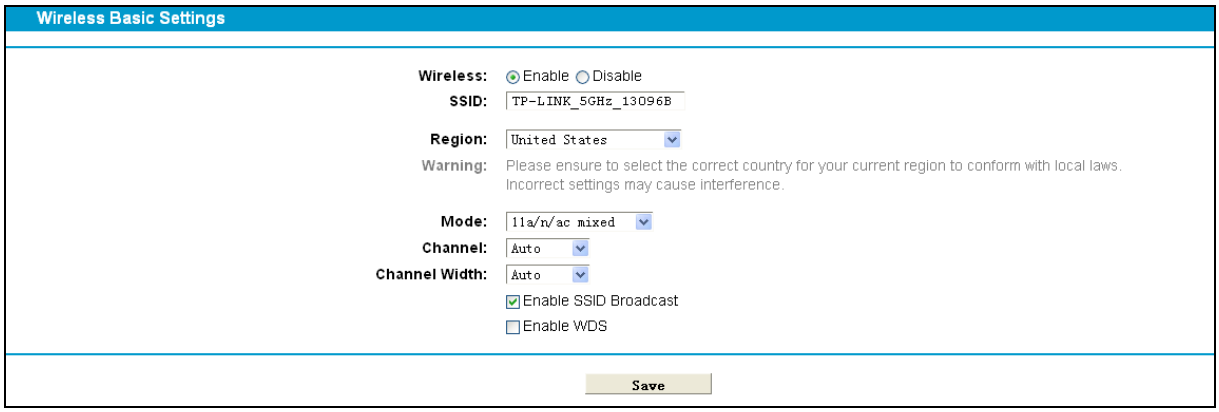


Figure 4-41

- **SSID:** Wireless network name. Enter a desired SSID which is case-sensitive and must not exceed 32 characters.
- **Region:** Select your region from the drop-down list. This field specifies the region where the wireless function of the modem router can be used. It may be illegal to use the wireless function of the modem router in a region other than one of those specified in this field. If your country or region is not listed, please contact your local government agency for assistance.

  ☞ **Note:**

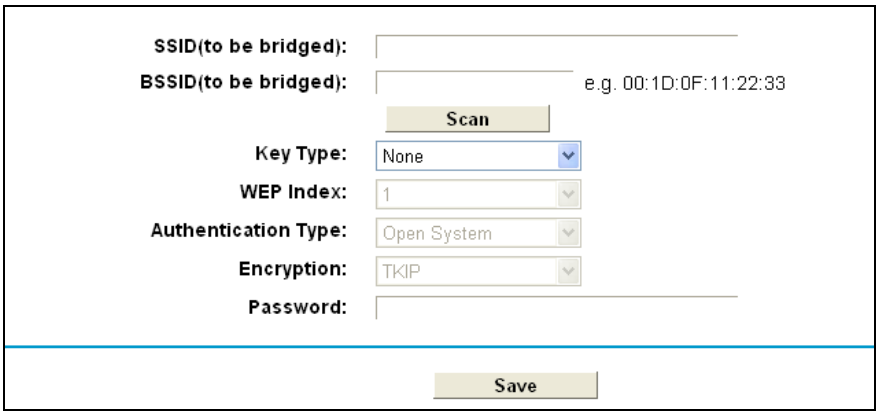
  Limited by local law regulations, version for North America does not have region selection option.

- **Mode:** Select the desired mode.

  11an mixed - Select if you are using both 802.11a and 802.11n wireless clients.

  11a/n/ac mixed - Select if you are using a mix of 802.11a, 802.11n and 802.11ac wireless clients. It is strongly recommended that you set the Mode 11a/n/ac mixed.

- **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.
- **Channel Width:** Select the channel width from the drop-down list. The default setting is auto, which can adjust the channel width for your clients automatically.
- **Enable SSID Broadcast:** When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the modem router. If this checkbox is selected, the wireless router will broadcast its name (SSID) on the air.
- **Enable WDS:** With this function, the modem router can bridge two or more Wlans. If this checkbox is selected, you will need to set the following parameters as shown in the figure below. Make sure the following settings are correct.



- **SSID (to be bridged):** The SSID of the AP your modem router is going to connect to as a client. You can also use the search function to select the SSID to join.
- **BSSID (to be bridged):** The BSSID of the AP your modem router is going to connect to as a client. You can also use the search function to select the BSSID to join.
- **Scan:** Click this button to search the AP which runs in the current channel.
- **Key type**: This option should be chosen according to the AP's security configuration. It is recommended that the security type is the same as your AP's security type
- **WEP Index**: This option should be chosen if the key type is WEP(ASCII) or WEP(HEX). It indicates the index of the WEP key.
- **Authentication Type**: This option should be chosen if the key type is WEP(ASCII) or WEP(HEX). It indicates the authorization type of the Root AP.
- **Password:** If the AP your modem router is going to connect needs password, you need to fill the password in this blank.

Click **Save** to save your settings.

4.9.2 WPS Settings

This section will guide you to add a new wireless device to an existing network quickly by **WPS** (also called **QSS**) function.

a). Choose menu "**WPS Settings**", and you will see the next screen (shown in Figure 4-42).

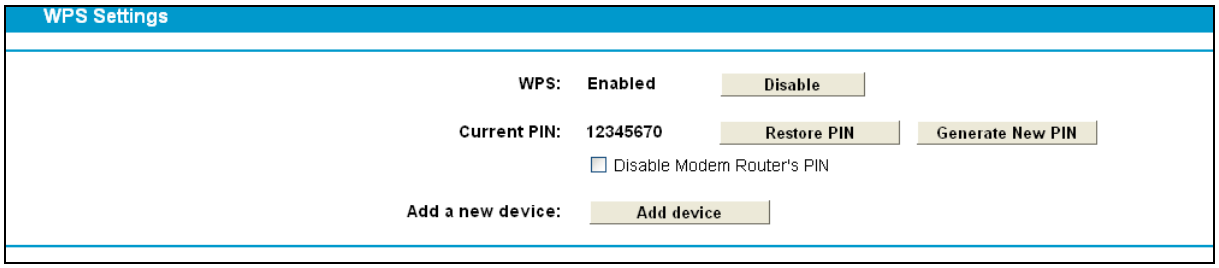


Figure 4-42

- **WPS:** Enable or disable the WPS function here.
- **Current PIN:** The current value of the modem router's PIN is displayed here.
- **Restore PIN:** Restore the PIN of the modem router to its default.
- **Generate New PIN:** Click this button to get a new random PIN code. You can ensure the network security by generating a new PIN.
- **Add device:** You can add a new device to the existing network manually by clicking this button.

b). To add a new device:

If the wireless adapter supports Wi-Fi Protected Setup (WPS), you can establish a wireless connection between wireless adapter and modem router using either Push Button Configuration (PBC) method or PIN method.

Note:

To build a successful connection by WPS, you should also do the corresponding configuration of the new device for WPS function meanwhile.

I. Use the Wi-Fi Protected Setup Button

Use this method if your client device has a Wi-Fi Protected Setup button.

Step 1: Press the WPS button on the back panel of the modem router, as shown in the following figure.

You can also keep the default WPS Status as **Enabled** and click the **Add device** button in Figure 4-42, then Choose "**Press the WPS button of the new device within the next two minutes**" and click **Connect**. (Shown in the following figure)

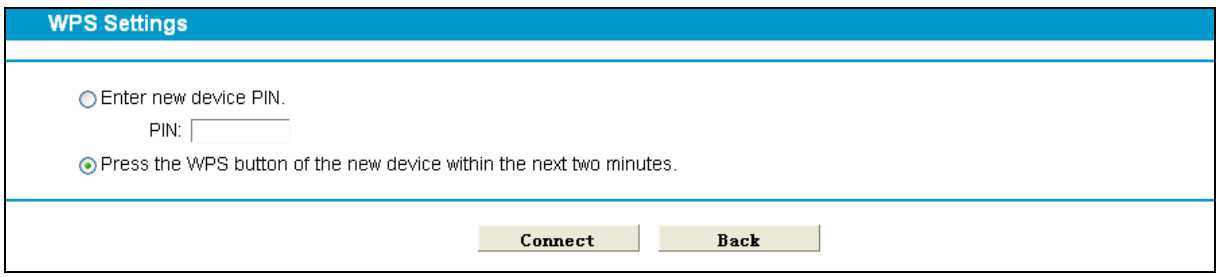


Figure 4-43

Step 2: Press and hold the WPS button of the client device directly.

Step 3: The Wi-Fi Protected Setup LED flashes for two minutes during the Wi-Fi Protected Setup process.

Step 4: When the WPS LED is on, the client device has successfully connected to the modem router.

Refer back to your client device or its documentation for further instructions.

II. Enter the client device's PIN on the modem router

Use this method if your client device has a Wi-Fi Protected Setup PIN number.

Step 1: Keep the default WPS Status as **Enabled** and click the **Add device** button in Figure 4-42, then the following screen will appear.

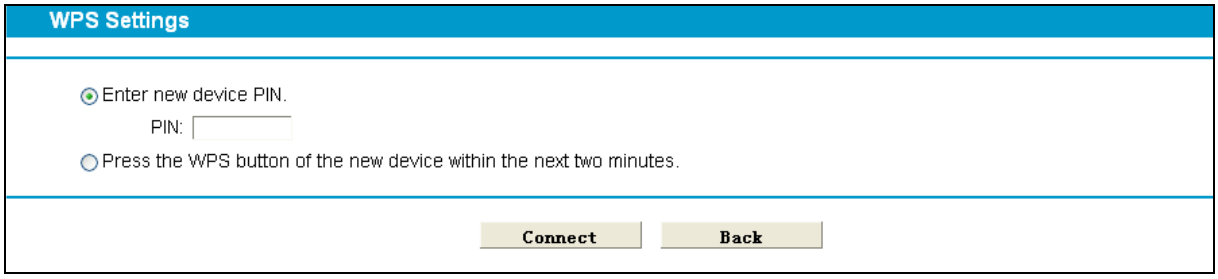


Figure 4-44

Step 2: Enter the PIN number from the client device in the field on the above WPS screen. Then click **Connect** button.

Step 3: "**Connect successfully**" will appear on the screen of Figure 4-44, which means the client device has successfully connected to the modem router.

III. Enter the modem router's PIN on your client device

Use this method if your client device asks for the modem router's PIN number.

Step 1: On the client device, enter the PIN number listed on the modem router's Wi-Fi Protected Setup screen. (It is also labeled on the bottom of the modem router.)

Step 2: The Wi-Fi Protected Setup LED flashes for two minutes during the Wi-Fi Protected Setup process.

Step 3: When the WPS LED is on, the client device has successfully connected to the modem router.

Step 4: Refer back to your client device or its documentation for further instructions.

☞ **Note:**

1) The WPS LED on the modem router will light green for five minutes if the device has been successfully added to the network.

2) The WPS function cannot be configured if the Wireless Function of the modem router is disabled. Please make sure the Wireless Function is enabled before configuring the WPS.

4.9.3 Wireless Security

Choose menu "**Wireless 5GHz**"→" **Wireless Security**", you can configure the security settings of your wireless network.

There are three wireless security modes supported by the modem router: WPA/WPA2 – Personal, WPA/WPA2 – Enterprise, WEP (Wired Equivalent Privacy).

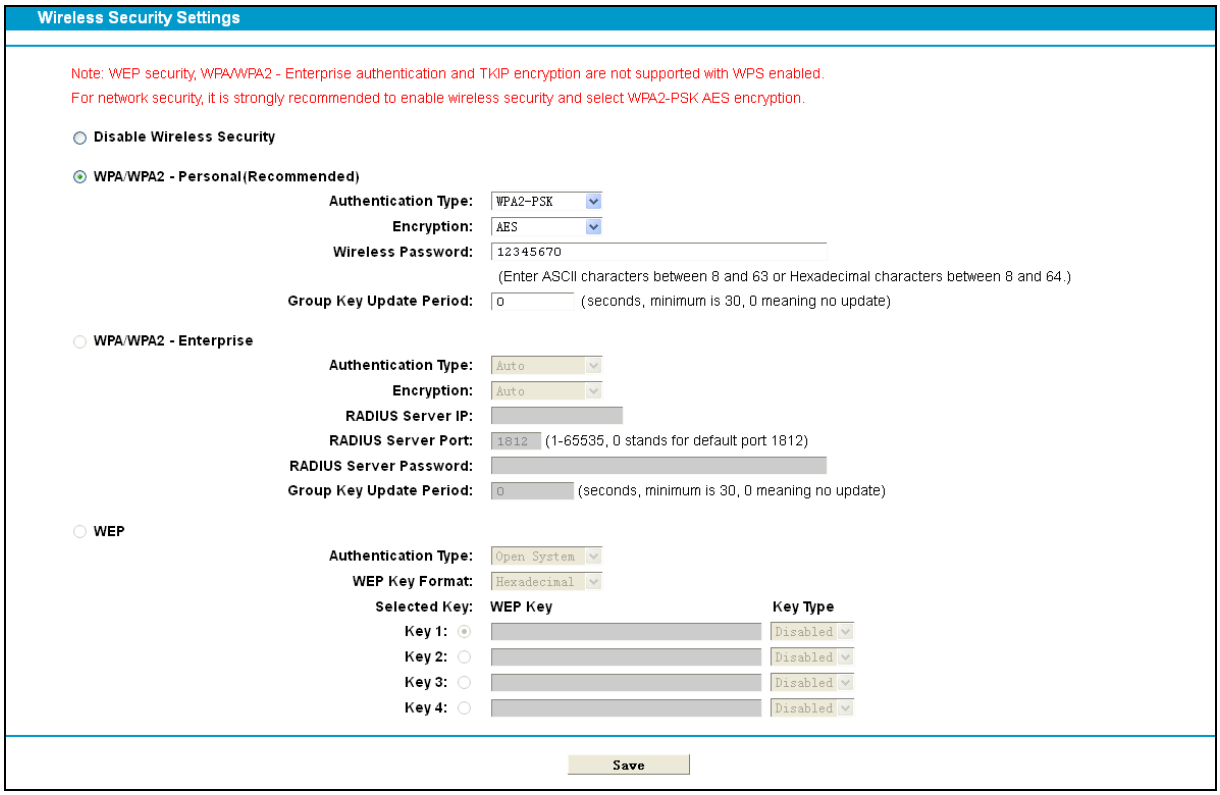
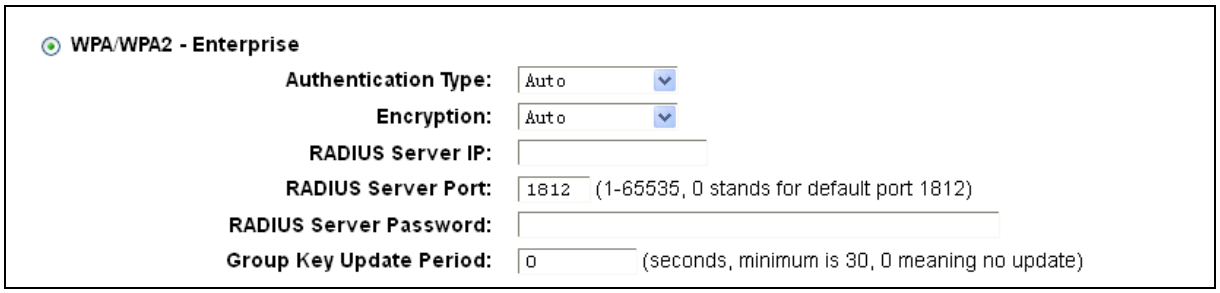


Figure 4-45

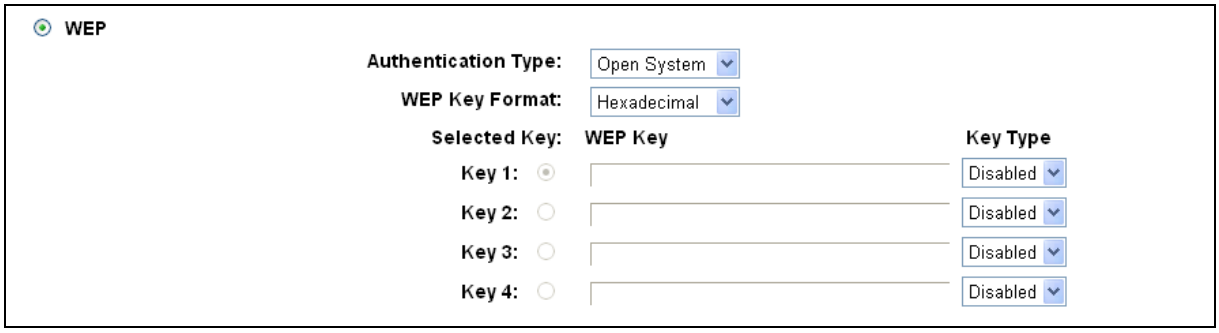
- **Disable Wireless Security:** If you do not want to use wireless security, check this radio button. But it's strongly recommended to choose one of the below modes to ensure security.
- **WPA/WPA2-Personal -** It's the WPA/WPA2 authentication type based on pre-shared passphrase. It is chosen by default.
  - **Authentication Type:** You can choose the type for the WPA/WPA2-Personal security from the drop-down list. The default setting is **WPA-PSK**.
  - **Encryption:** You can select **Auto**, **TKIP** or **AES** as Encryption.
  - **Wireless Password:** You can enter ASCII characters between 8 and 63 characters or 8 to 64 Hexadecimal characters. The default password is the same with the default PIN code, which is labeled on the bottom of the modem router or can be found in Figure 4-32.
  - **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.
- **WPA/WPA2 – Enterprise:** It's based on Radius Server.



- **Authentication Type:** You can choose the type for the WPA/WPA2-Enterprise security from the drop-down list. The default setting is **Auto**, which can select **WPA** or **WPA2** as authentication type automatically based on the wireless station's capability and request.

- **Encryption:** You can select **Auto**, **TKIP** or **AES** as Encryption.
- **RADIUS Server IP:** Enter the IP address of the Radius Server.
- **RADIUS Server Port:** Enter the port that radius service used.
- **RADIUS Server Password:** Enter the password for the Radius Server.
- **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.

➢ **WEP:** It is based on the IEEE 802.11 standard.



- **Authentication Type:** You can choose the type for the WEP security from the drop-down list. The default setting is **Open System**.
- **WEP Key Format: Hexadecimal** and **ASCII** formats are provided here. **Hexadecimal** format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length. **ASCII** format stands for any combination of keyboard characters in the specified length.
- **WEP Key:** Select which of the four keys will be used and enter the matching WEP key that you create. Make sure these values are identical on all wireless stations in your network.
- **Key Type:** You can select the WEP key length (64-bit, or 128-bit.) for encryption. "Disabled" means this WEP key entry is invalid.

  64-bit: You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not promoted) or 5 ASCII characters.

  128-bit: You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not promoted) or 13 ASCII characters.

Be sure to click the **Save** button to save your settings on this page.

4.9.4 Wireless Schedule

Choose menu "**Wireless 5GHz**"→"**Wireless Schedule**", you can configure the Task Schedule as shown below.

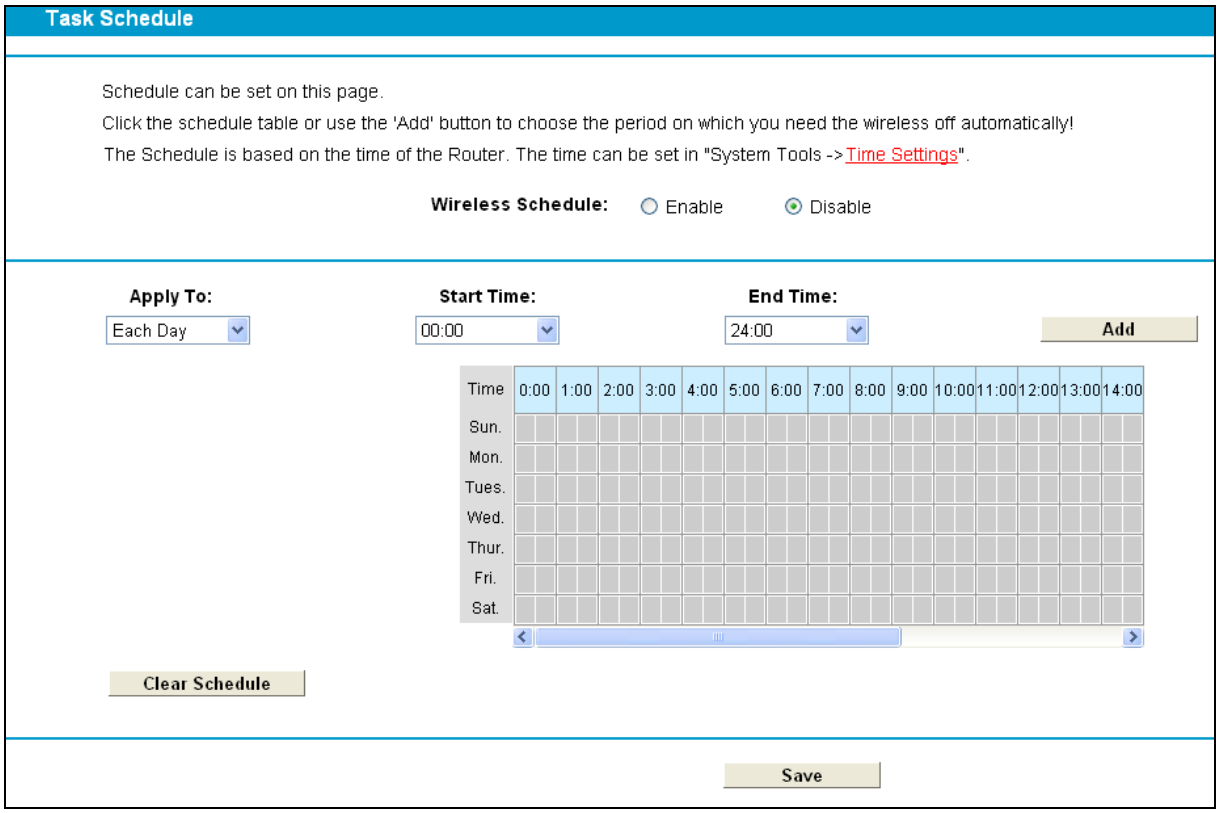


Figure 4-46

☞ Note:

The time you set is the period you need the wireless off.

Before configure the wireless schedule, please set system time first which refer to 4.23.2 Time Settings, then you can enable or disable Wireless Schedule.

- **Apply To:** Select the day or days you want to switch the wireless off.
- **Start Time, End Time:** You can select all day-24 hours or you may enter the **Start Time** and **End Time** in the corresponding field.
- **Add:** Click this button to add your selected time to the below table.

Click the **Clear Schedule** button to clear your settings in the table.
Click **Save** to complete the settings.

4.9.5 Wireless MAC Filtering

Choose menu "**Wireless 5GHz**" → "**Wireless MAC Filtering**", you can control the wireless access by configuring the **Wireless MAC Filtering** function, shown in Figure 4-37.

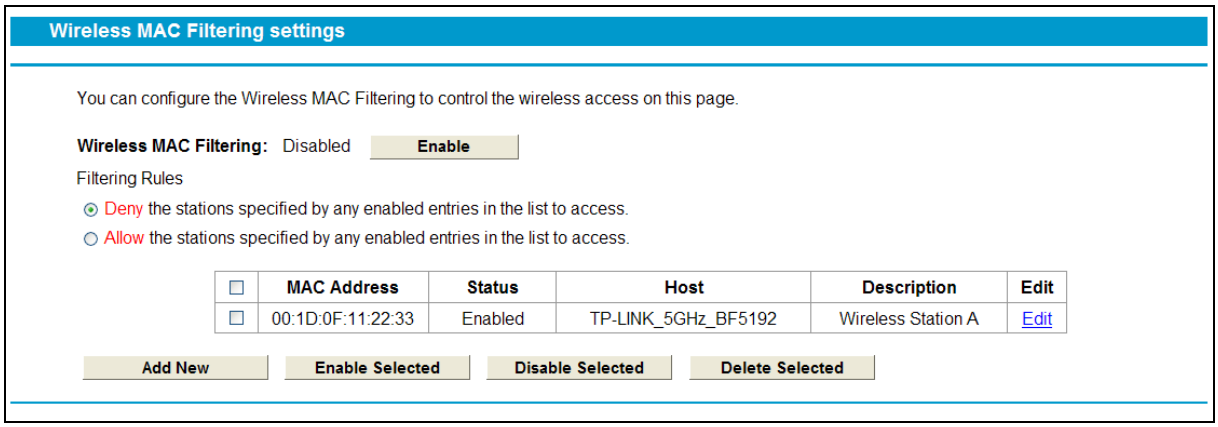


Figure 4-47

To filter wireless users by MAC Address, click **Enable**. The default setting is **Disabled**.

- **MAC Address:** The wireless station's MAC address that you want to filter.
- **Status:** The status of this entry either **Enabled** or **Disabled**.
- **Host:** The wireless network name (SSID).
- **Description:** A simple description of the wireless station.

To Add a Wireless MAC Address filtering entry, click the **Add New** button. The following page will appear, shown in Figure 4-38:

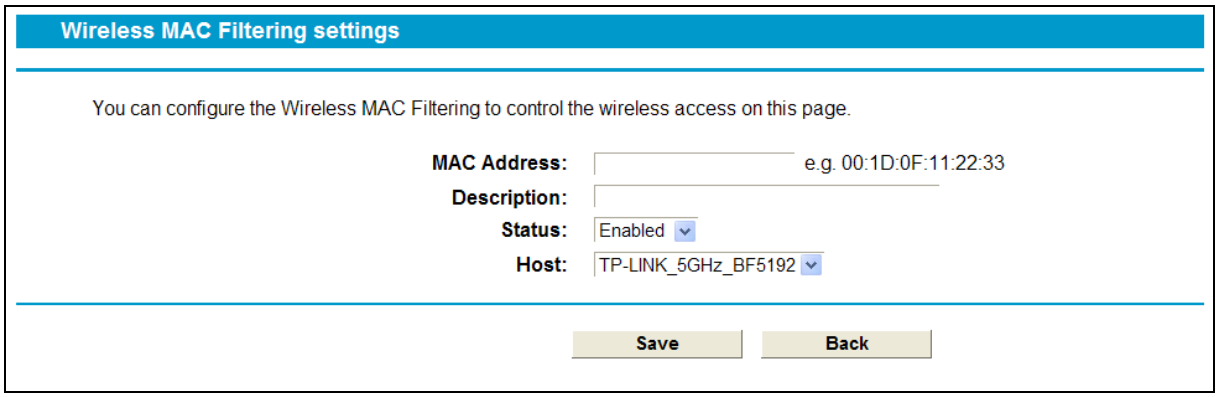


Figure 4-48

To add or modify a MAC Address Filtering entry, follow these instructions:

1. Enter the appropriate MAC Address into the **MAC Address** field. The format of the MAC Address is XX:XX:XX:XX:XX:XX (X is any hexadecimal digit). For example: 00:1D:0F:11:22:33.
2. Give a simple description for the wireless station in the **Description** field. For example: Wireless station A.
3. Select **Enabled** or **Disabled** for this entry from the **Status** drop-down list.
4. Select **Host** from the drop-down list.
5. Click the **Save** button to save this entry.

To edit or delete an existing entry:

1. Click the **Edit** in the entry you want to modify.
2. Modify the information.

3. Click the **Save** button.

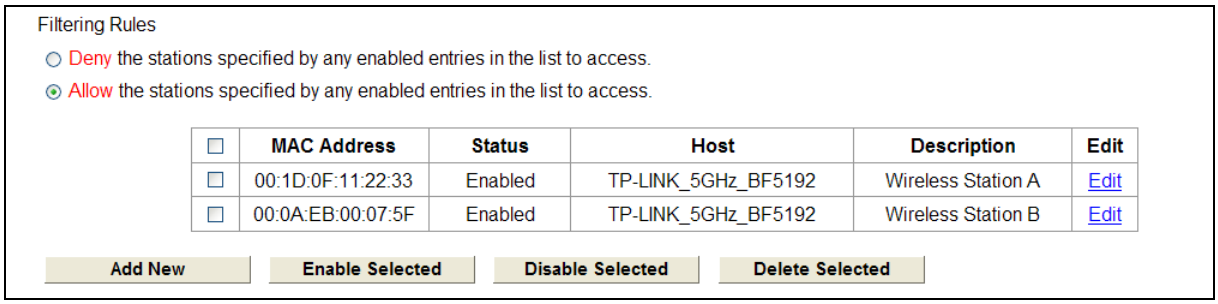
Click the **Enable/ Disabled Selected** button to make selected entries enabled or disabled.

Click the **Delete Selected** button to delete the selected entries.

For example: If you desire that the wireless station A with MAC address 00:1D:0F:11:22:33 and the wireless station B with MAC address 00:0A:EB:00:07:5F are able to access the modem router, but all the other wireless stations cannot access the Modem router, you can configure the **Wireless MAC Address Filtering** list by following these steps:

1. Click the **Enable** button to enable this function.
2. Select the radio button "**Allow the stations specified by any enabled entries in the list to access**" for **Filtering Rules**.
3. Delete all or disable all entries if there are any entries already.
4. Click the **Add New** button.
   1) Enter the MAC address 00:1D:0F:11:22:33/00:0A:EB:00:07:5F in the **MAC Address** field.
   2) Enter wireless station A/B in the **Description** field.
   3) Select **Enabled** in the **Status** drop-down list.
   4) Select **TP-LINK_5GHz** for the **Host**.
   5) Click the **Save** button.

The filtering rules that configured should be similar to the following list:



4.9.6 Wireless Advanced

Choose menu "**Wireless 5GHz**"→"**Wireless Advanced**", you can configure the advanced settings of your wireless network.

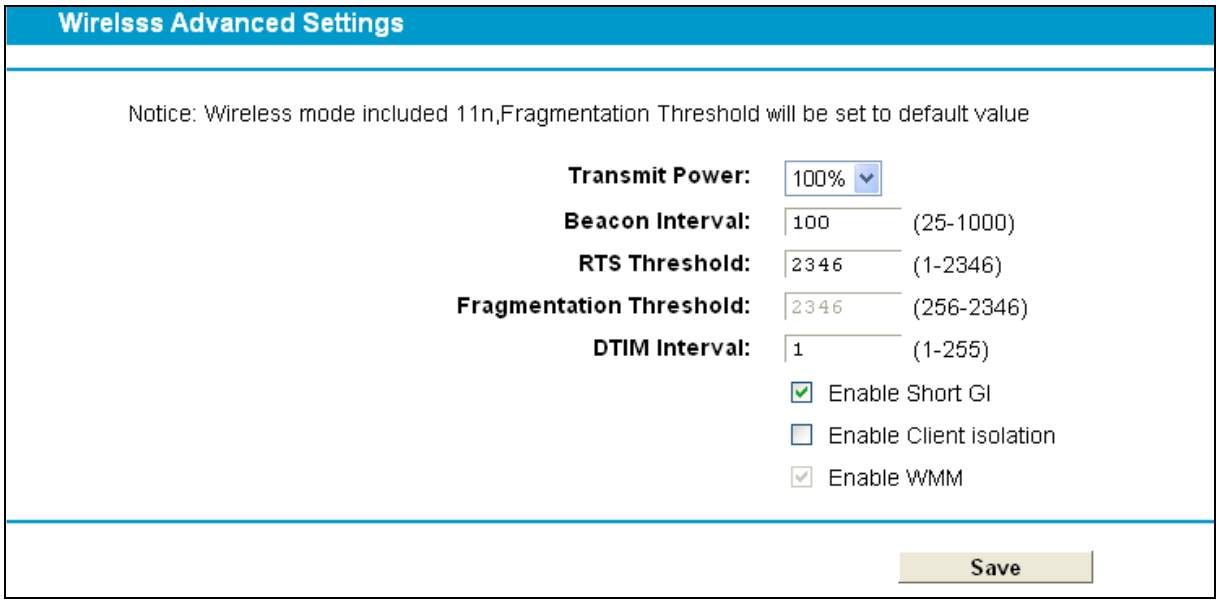


Figure 4-49

- **Transmit Power:** Here you can specify the transmit power of the modem router. You can select 100%, 50% or 25%. 100% is the default setting and is recommended.
- **Beacon Interval:** Enter a value between 25-1000 milliseconds for Beacon Interval here. The beacons are the packets sent by the modem router to synchronize a wireless network. Beacon Interval value determines the time interval of the beacons. The default value is 100.
- **RTS Threshold:** Here you can specify the RTS (Request to Send) Threshold. If the packet is larger than the specified RTS Threshold size, the modem router will send RTS frames to a particular receiving station and negotiate the sending of a data frame. The default value is 2346.
- **Fragmentation Threshold:** This value is the maximum size determining whether packets will be fragmented. Setting the Fragmentation Threshold too low may result in poor network performance because of excessive packets. 2346 is the default setting and is recommended.
- **DTIM Interval:** This value determines 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. You can specify the value between 1-255 Beacon Intervals. The default value is 1, which indicates the DTIM Interval is the same as Beacon Interval.
- **Enable Short GI:** It is recommended to Enable Short GI, which will increase the data capacity by reducing the guard interval time.
- **Enabled Client Isolation:** This function can isolate wireless stations on your network from each other. Wireless devices will be able to communicate with the modem router but not with each other. Client isolation is disabled by default.
- **Enable WMM:** This function guarantee the packets with high-priority messages being transmitted preferentially. It is strongly recommended to enable WMM.

☞ **Note:**

If you are not familiar with the setting items in this page, it's strongly recommended to keep the provided default values; otherwise it may result in lower wireless network performance.

4.9.7 Wireless Status

Choose menu "**Wireless 5GHz**"→"**Wireless Status**", you can see the MAC Address, Current Status, Received Packets and Sent Packets for each connected wireless station.

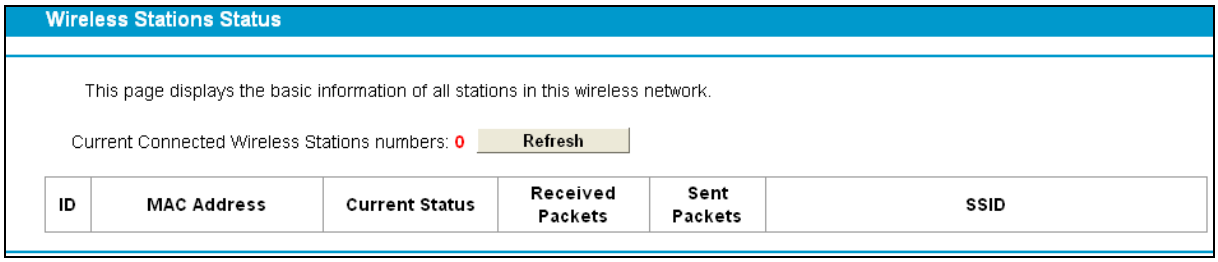
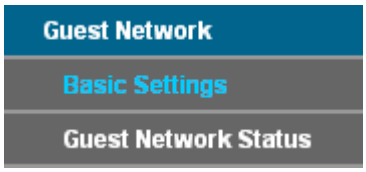


Figure 4-50

- **MAC Address:** The connected wireless station's MAC address
- **Current Status:** The connected wireless station's running status, one of **STA-AUTH/ STA-ASSOC/ STA-JOINED/ WPA/ WPA-PSK/ WPA2/ WPA2-PSK/ AP-UP/ AP-DOWN/ Disconnected**
- **Received Packets:** Packets received by the station
- **Sent Packets:** Packets sent by the station

Click on the **Refresh** button to update this page.

4.10 Guest Network



There are two submenus under the Guest Network menu: **Basic Settings** and **Guest Network Status**. Click any of them, and you will be able to scan or configure the corresponding function. The detailed explanations for each submenu are provided below.

4.10.1 Basic Settings

Choose menu "**Guest Network**"→"**Basic Settings**", and you will see the screen as shown in Figure 4-51. 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.

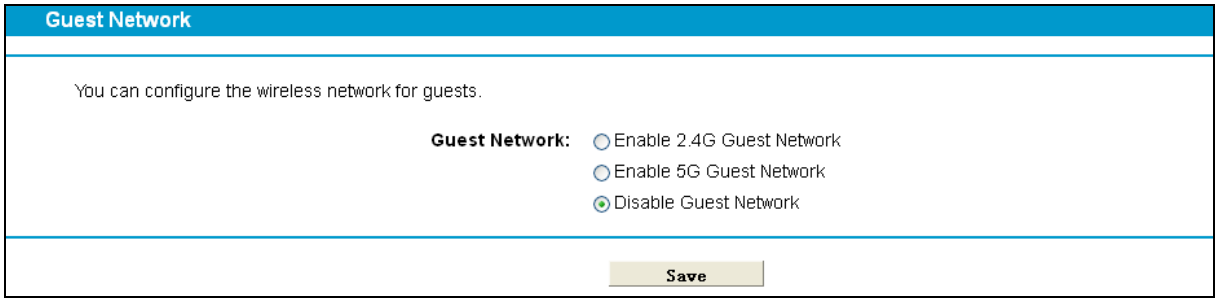


Figure 4-51

- **Enable 2.4G Guest Network:** Check this box to enable 2.4G Guest Network. And you can set wireless parameters for 2.4G guest network as shown in Figure 4-52.

- **Enable 5G Guest Network:** Check this box to enable 5G Guest Network. And you can set wireless parameters for 5G guest network similar to Figure 4-52.

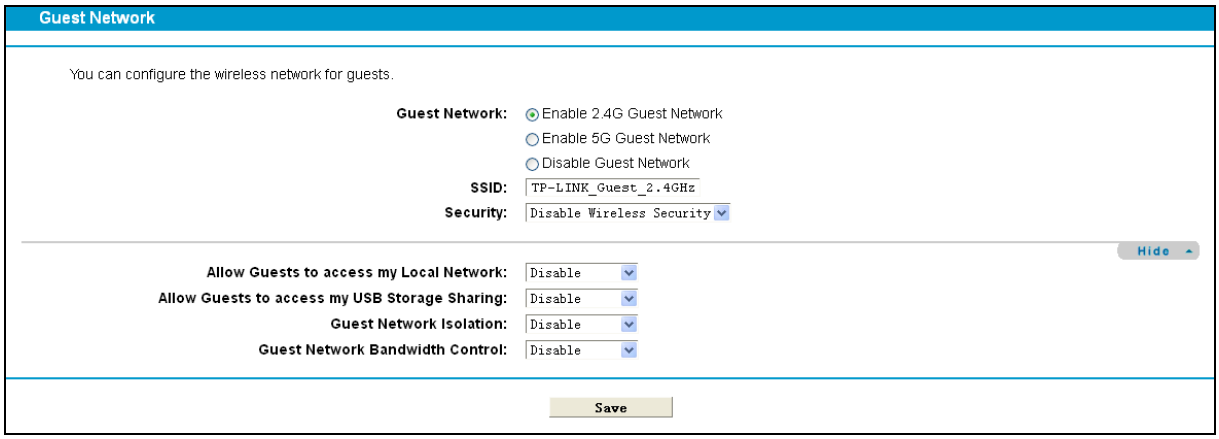


Figure 4-52

- **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. The default name is TP-LINK Guest_XGHz.
- **Security:** It's strongly recommended to enable WPA/WPA2-Personal.
- **Allow Guests to access my Local Network**: The guests have access to your Local Network, but can not login the modem router's web-management page.
- **Allow Guests to access my USB Storage Sharing:** The guests can access the specified files on the USB storage device via the function of USB Storage Sharing, but the function of FTP Server, Media Server and Print Server are not available in Guest Network. For more details please refer to 4.11.3 Storage Sharing.
- **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 /Downstream Bandwidth for guest network.

Click **Save** to save your settings.

4.10.2 Guest Network Status

Choose menu "**Guest Network**"→"**Guest Network Status**", you can see the MAC Address, Current Status, Received Packets and Sent Packets for each connected wireless station.

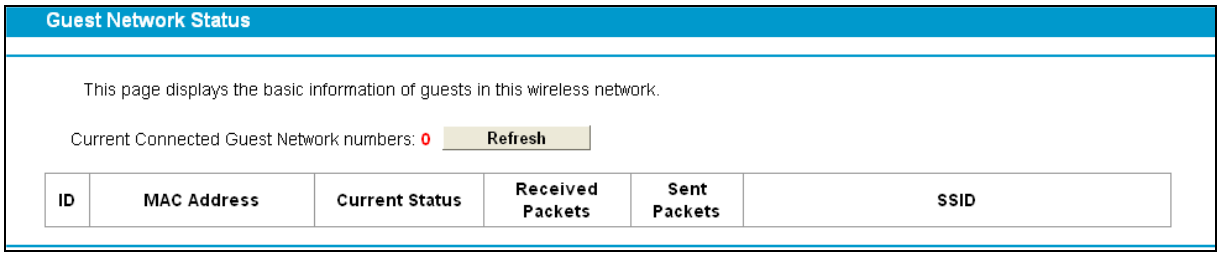


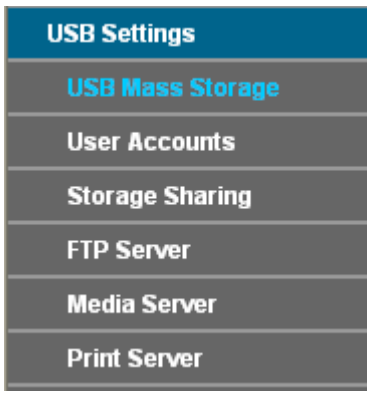
Figure 4-53

- **MAC Address:** The connected wireless station's MAC address.
- **Current Status:** The connected wireless station's running status.

- **Received Packets:** Packets received by the station.
- **Sent Packets:** Packets sent by the station.

Click on the **Refresh** button to update this page.

4.11 USB Settings



There are six submenus under the USB Settings menu, **USB Mass Storage**, **User Accounts**, **Storage Sharing**, **FTP Server**, **Media Server** and **Print Server**. Click any of them, and you will be able to configure the corresponding function.

4.11.1 USB Mass Storage

Choose menu "**USB Settings**" → "**USB Mass Storage**", you can configure a USB disk drive attached to the modem router and view volume and share properties such as share name, capacity, status, and action, on this page as shown below.

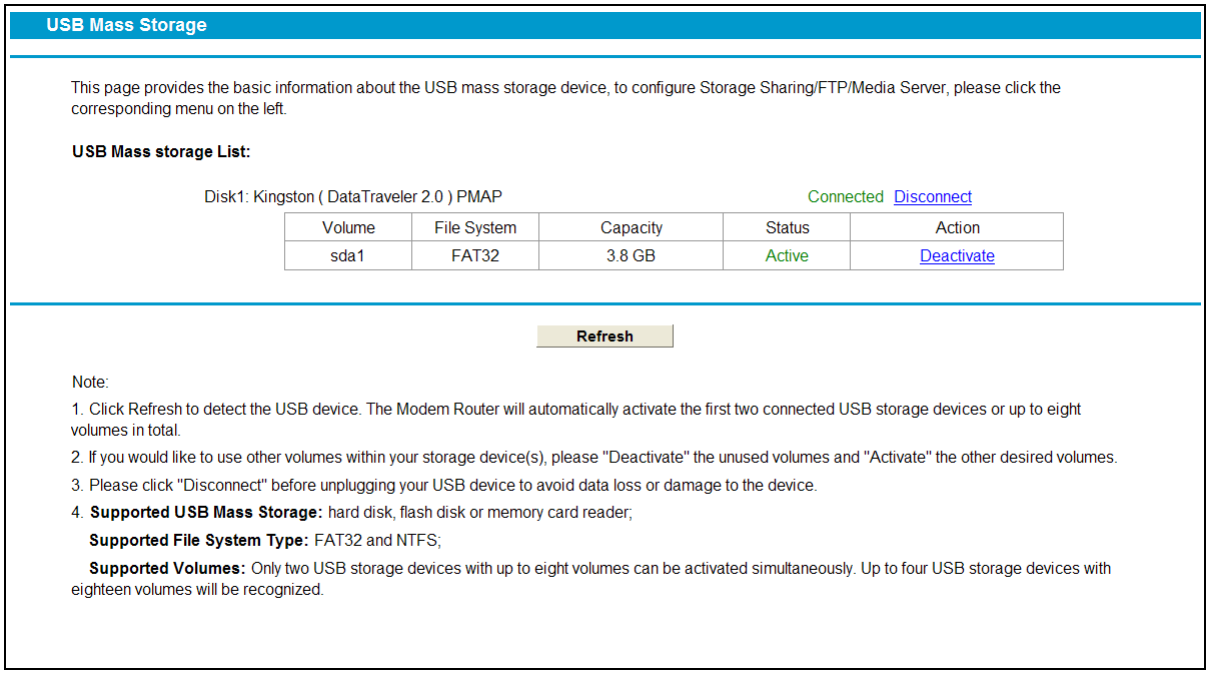


Figure 4-54

- **Volume:** The volume name of the USB drive the users have access to.
- **File System:** The system of the USB drive.
- **Capacity:** The storage capacity of the USB driver.

- **Status:** Indicates the shared or non-shared status of the volume. **Active** means volume can be shared, while **Inactive** means volume can not be shared. If **Inactive** in Action field is enabled, **Active** will be displayed in the Status field, which means volume can not be shared.
- **Action:** When the volume is shared, you can click the **Deactivate** to stop sharing the volume; when volume is non-shared, you can click the **Activate** button to share the volume.

Click **Disconnect** to safely remove the USB storage device that is connected to USB port.

Note:

Before removing the USB storage device, you should click "Disconnect" to make sure that all your data have been saved completely. Removing device directly may cause your USB storage device crashed.

4.11.2 User Accounts

You can specify the user name and password for Storage Sharing and FTP Server users on this page. Storage Sharing users can access the folders by entering the following URL into the address field of your browser or Windows Explorer, such as. \\192.168.1.1. FTP Server users can log into the FTP Server via FTP Client.

You can set up five users and control their access to the USB mass storage by Storage Sharing or FTP on this page. The Super User has the right to read and write to Storage Sharing and FTP Server.

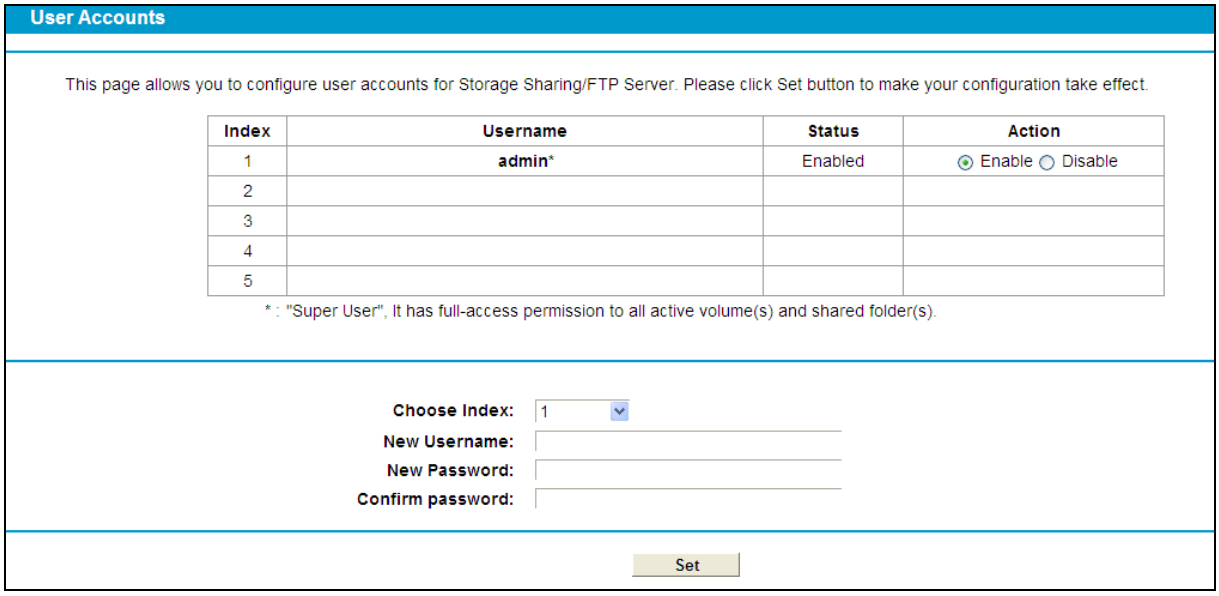


Figure 4-55

To add a new user account, please follow the steps below:

1. Choose the index from the drop-down list of **Choose Index**.
2. Self-define a **New Username**.
3. Enter the password in the **New Password** field.
4. Re-enter the password in the **Confirm password** field.
5. Click the **Set** button, and then a new entry will be added in the table.

To delete an existing user account, please click **Delete** in the **Action** column.

4.11.3 Storage Sharing

Choose menu "**USB Settings**" → "**Storage Sharing**", you can configure a USB disk drive attached to the modem router and view volume and share properties on this page as shown below.

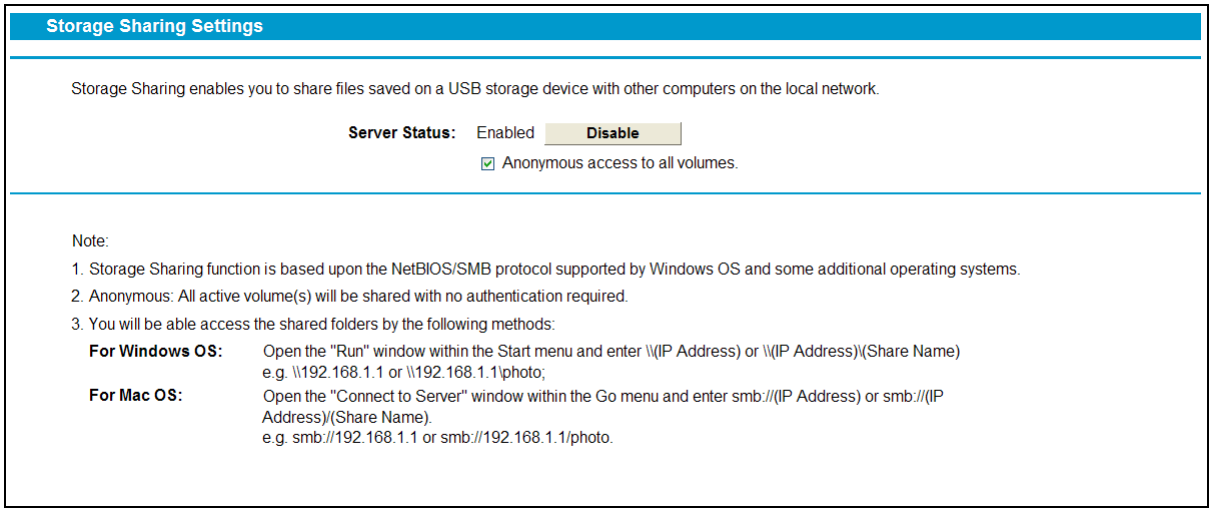
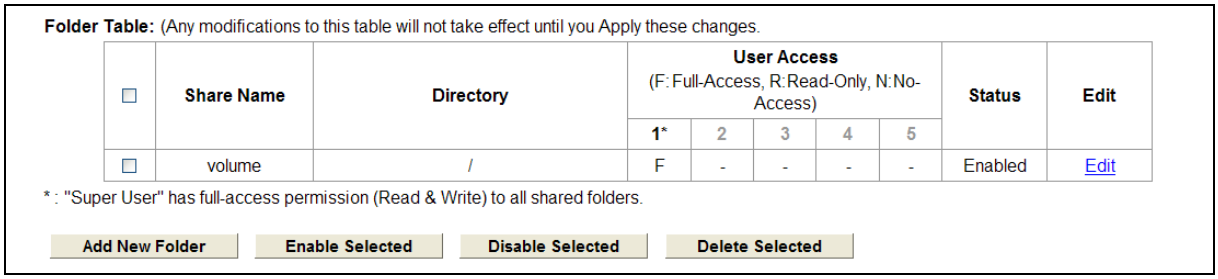


Figure 4-56

- **Server Status:** Indicates the Storage Sharing's current status.
- **Anonymous access to all the volumes:** This function is enabled by default, so that users can access to all activated volumes without authentication. If you want to add a shared folder which does not allow anonymous login, uncheck the box. Then **Folder Table** will be displayed as shown below.



- **Share Name:** This folder's display name.
- **Directory:** The real full path of the specified folder.
- **User Access:** The authorization of users. * users mean Super Users who have the full-access permission to all activated volumes and share folders. F stands for fully access, R stands for read-only and N stands for no-access.
- **Status:** The status of the entry is enabled or disabled.
- **Edit:** Click **Edit** in the table, and then you can modify the entry.

To add a new folder, follow the instructions below.

1. Click **Add New Folder**.

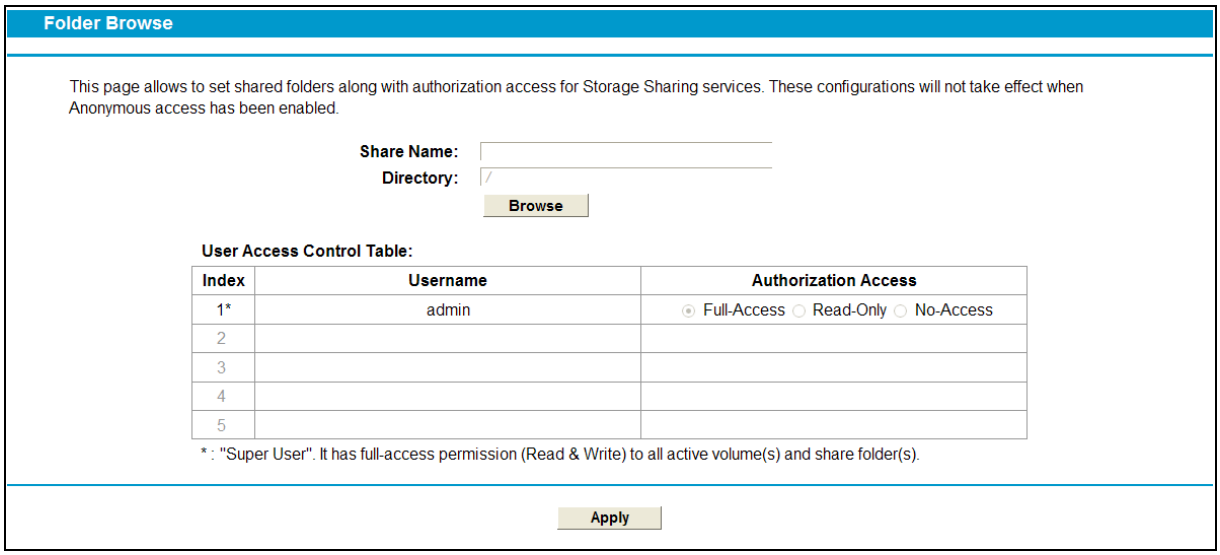


Figure 4-57

2. Click the **Browse** button, and then select the **Select Volume** from the drop-down list.
3. Enter the display name of the share folder in **Share Name** filed.
4. Click the **Apply** button to apply the settings.

You can click the **upper** button to go to the upper folder

Click the **Enable/Disable Selected** button to enable or disable the selected entries.

Click the **Delete Selected** button to delete the selected entries.

Note:

1. The max share folders number is 10. If you want to share a new folder when the number has reached 10, you can delete an existing share folder and then add a new one.
2. If you want to change the Storage Sharing settings, you can click the Apply button to make the changes take effect.

4.11.4 FTP Server

Choose menu "**USB Settings**"→ "**FTP Server**", you can create an FTP server that can be accessed from the Internet or your local network.

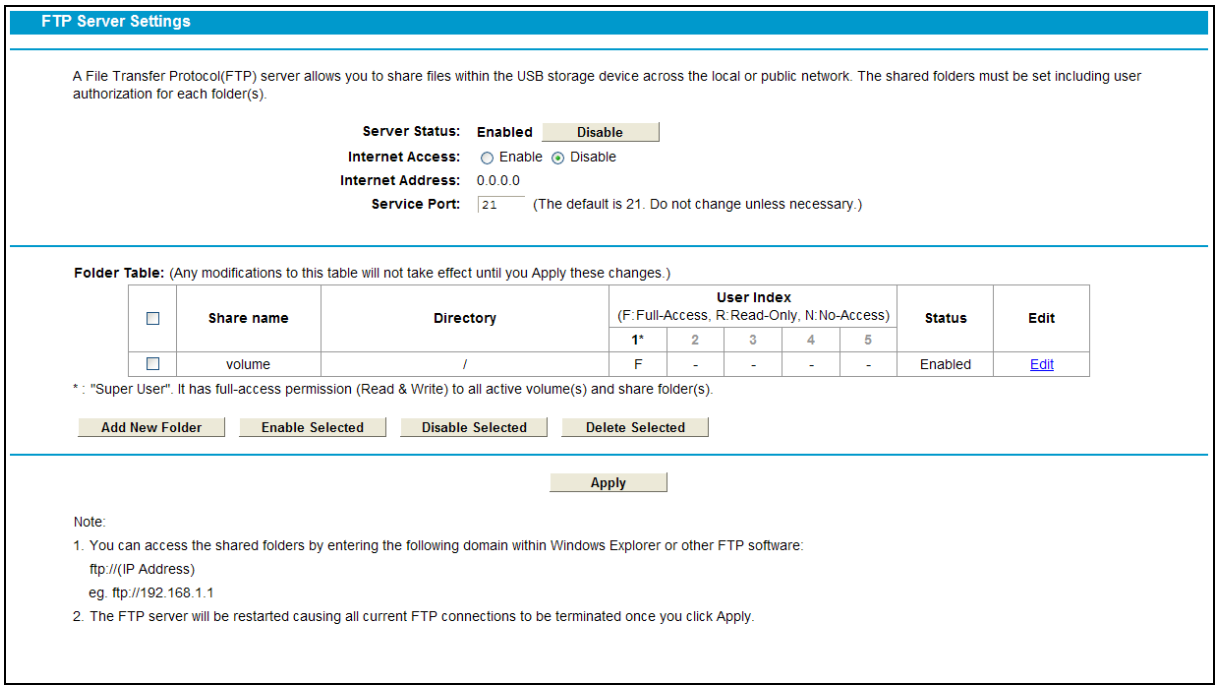


Figure 4-58

- **Server Status:** Indicates the FTP Server's current status.
- **Internet Access:** If **Internet Access** is enabled, user(s) in public network can access FTP server via Internet Address.
- **Internet Address:** If Internet Access is enabled, WAN IP will be displayed here.
- **Service Port:** Enter the FTP Port number to use. The default is 21.
- **Share Name:** This folder's display name.
- **Directory:** The real full path of the specified folder.
- **User Index:** The authorization of the user is displayed.
- **Status:** The status of the entry is enabled or disabled.
- **Edit:** Click **Edit** to modify the entry.

To add a new folder, follow the instructions below.

1. Click **Add New Folder** in Figure 4-58.

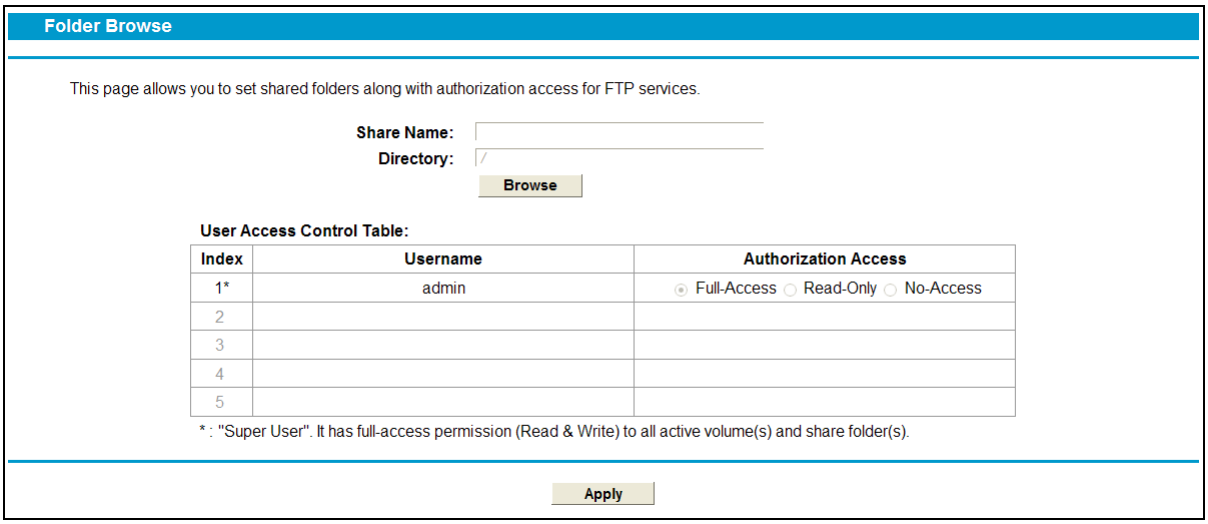


Figure 4-59

2. Click the **Browse** button, and then select the **Select Volume** from the drop-down list.
3. Enter display name of the share folder in **Share Name** filed.
4. Click the **Apply** button to apply the settings.

You can click the **upper** button to go to the upper folder.

Click the **Enable/Disable Selected** button to enable or disable the selected entries.

Click the **Delete Selected** button to delete the selected entries.

Note:

1. The max share folders number is 10. If you want to share a new folder when the number has reached 10, you can delete an existing share folder and then add a new one.
2. If you want to change the FTP settings, you can click the Apply button to make the changes take effect.

4.11.5 Media Server

Choose menu "**USB Settings**"→ "**Media Server**", you can create media server that allows you to share stored content with other computers and devices on your home network and on the Internet.

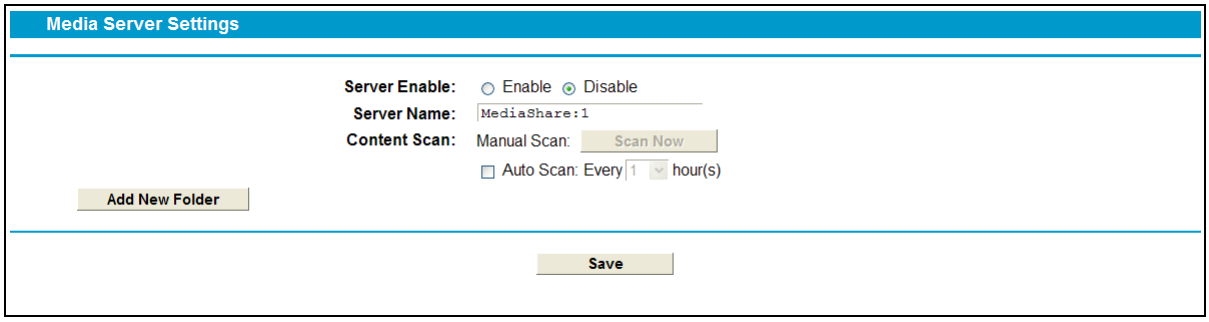


Figure 4-60

- **Server Enable**: Select this box to enable this function.
- **Server Name**: The name of this Media Server.

To add a new share folder for your media server, please follow the instructions below:

a) Click **Add New Folder** button, and you will see the screen as shown in Figure 4-61.

b) Enter the name of the share folder in **Share Name** field.

c) Click the **Apply** button to apply the configuration.

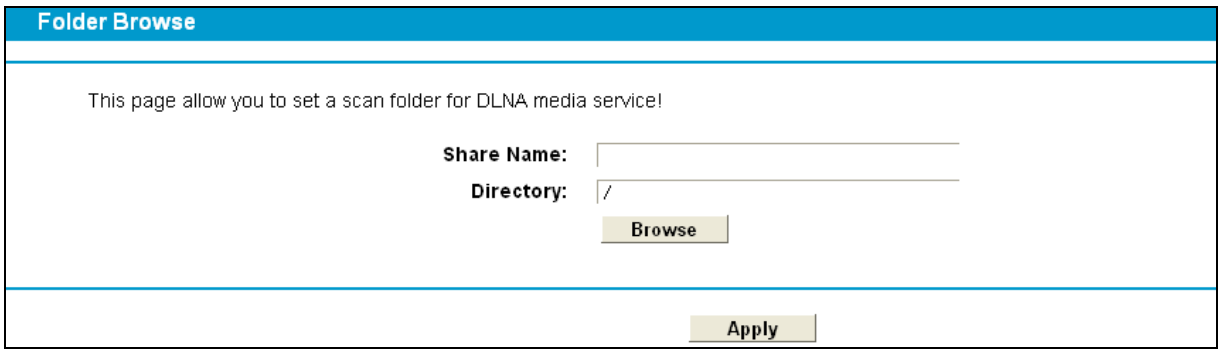


Figure 4-61

Click the **Scan now** to scan all the share folders immediately. You can also select the **Auto-scan**, and, at the same time, select an auto scan interval time from the drop-down list. In this case, the media server will automatically scan the share folders.

Note:

The max share folders number is 6. If you want share a new folder when the numbers has been reached to be 6, you can delete a share folder and then add a new one.

4.11.6 Print Server

Choose menu "**USB Settings**"→ "**Print Server**", you can configure print server on this page as shown below.

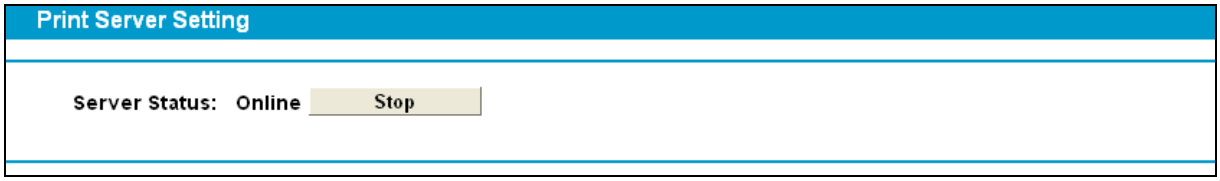


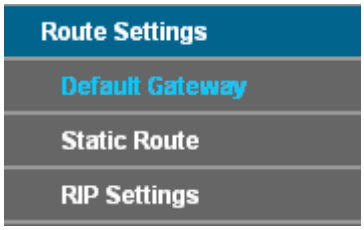
Figure 4-62

There are three states of the print server, they are as follows:

- **Online:** Indicates the print server has been turned on, and no user is using the print services at present. You can click the **Stop** button to stop the print service.
- **Offline:** Indicates the print service feature is disabled. You can click **Start** button to start the print service.
- **Busy:** Indicates the print service is occupied by other users at this moment.

4.12 Route Settings

Choose "**Route Settings**", it includes three menus**: Default Gateway**, **Static Route and RIP Settings**. The detailed descriptions are provided below.



4.12.1 Default Gateway

Choose "**Route Settings**"→"**Default Gateway**", you can see the Default Gateway screen. You can select a WAN Interface from the drop-down list as the system default gateway.

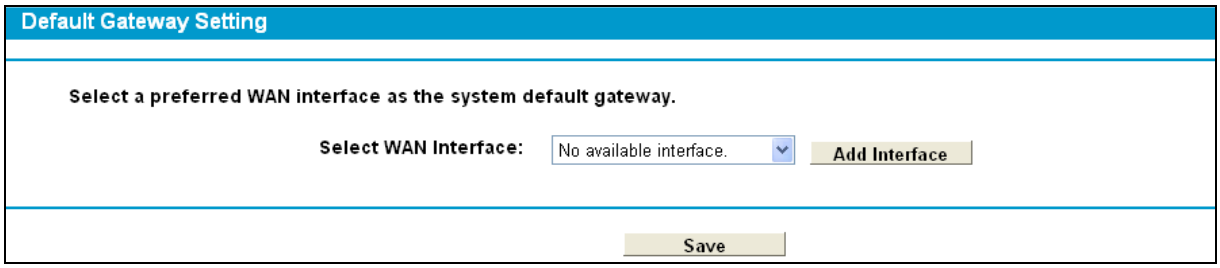


Figure 4-63

Click the **Add Interface** button, you can add WAN Interfaces.

Click the **Save** button to save your settings.

4.12.2 Static Route

Choose "**Route Settings**"→ "**Static Route**". You can see the Static Route screen, this screen allows you to configure the static routes (shown in Figure 4-64). A static route is a pre-determined path that network information must travel to reach a specific host or network.

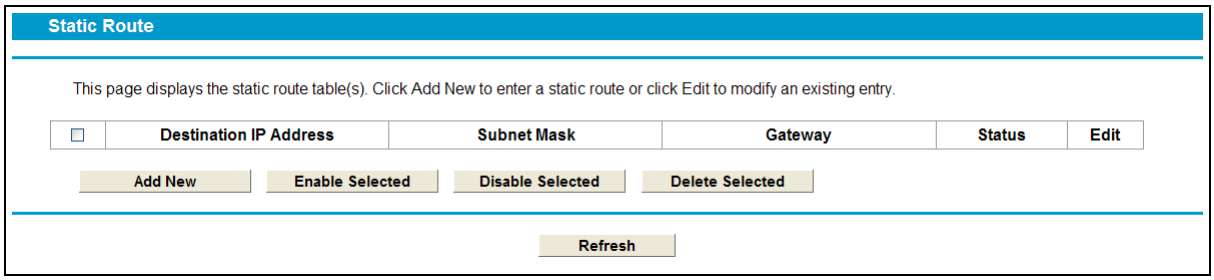


Figure 4-64

To add static routing entries:

1. Click the **Add New** button in Figure 4-64, and you will see the screen as shown in Figure 4-65.

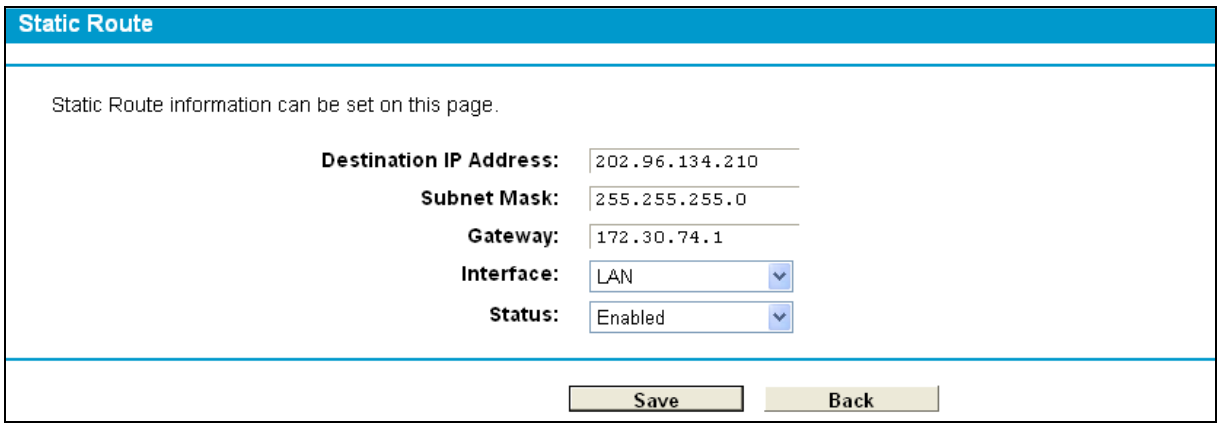


Figure 4-65

2. Enter the following data:

- **Destination IP Address:** The address of the network or host that you want to assign to a static route.
- **Subnet Mask:** It determines which portion of an IP Address is the network portion, and which portion is the host portion.
- **Gateway:** Type in the correct gateway address for the static route.
- **Interface:** Select the Interface from the drop-down list.
- **Status:** Select **Enabled** or **Disabled** from the drop-down list**.**

3. Click **Save** to save your settings as shown in Figure 4-65.

To modify or delete an existing entry:

1 Find the desired entry in the table.

2 Click **Edit** as desired on the **Edit** column.

Click the **Enable/ Disabled Selected** button to make selected entries enabled/ disabled.

Click the **Delete Selected** button to delete the selected entries.

4.12.3 RIP Settings

Choose "**Route Settings**"→"**RIP Settings**", you can see the RIP (Routing Information Protocol) screen which allows you to configure the RIP.

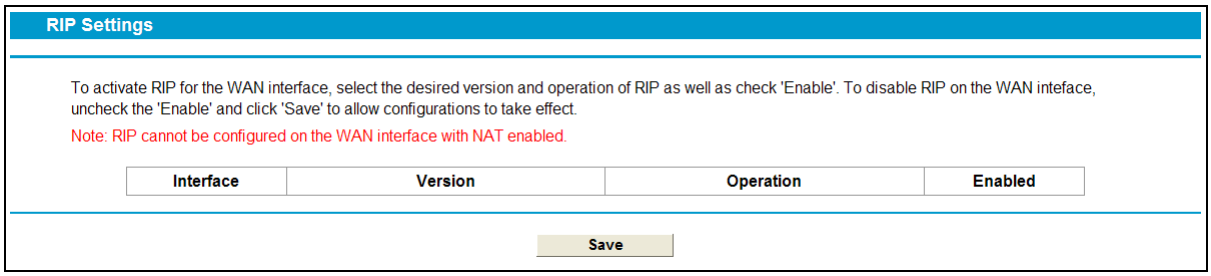


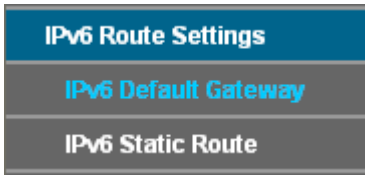
Figure 4-66

Note:

RIP cannot be configured on the WAN Interface which has NAT enabled (such as PPPoE).

4.13 IPv6 Route Settings

Choose "**IPv6 Route Settings**", it includes two menus**: IPv6 Default Gateway and IPv6 Static Route**. The detailed descriptions are provided below.



4.13.1 IPv6 Default Gateway

Choose "**IPv6 Route Settings**"→"**IPv6 Default Gateway**", you can see the Default Gateway screen. You can select a WAN Interface from the drop-down list as the system default gateway.

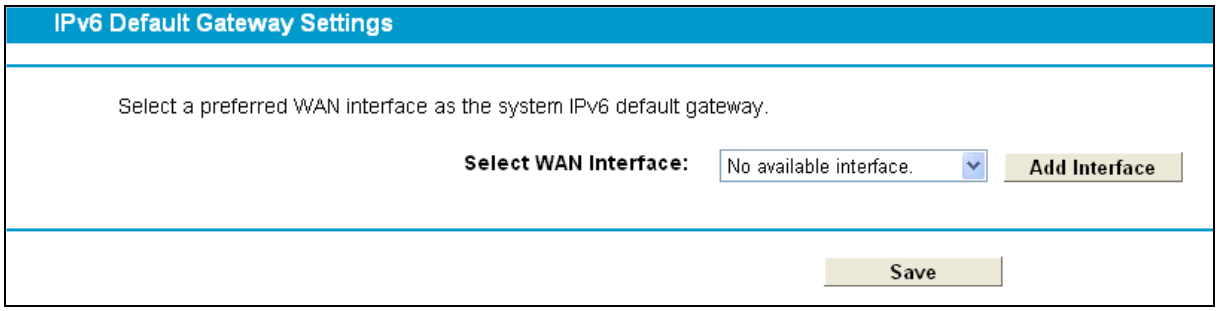


Figure 4-67

Click the **Add Interface** button, you can add WAN Interfaces.

Click the **Save** button to save your settings.

4.13.2 IPv6 Static Route

Choose "**IPv6 Route Settings**"→ "**IPv6 Static Route**". You can see the IPv6 Static Route screen. This screen allows you to configure the IPv6 static routes (shown in Figure 4-68). An IPv6 static route is a pre-determined path that network information must travel to reach a specific host or network.

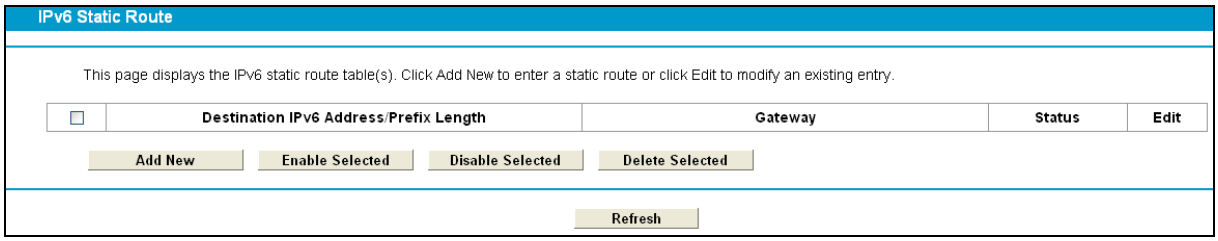


Figure 4-68

To add a new entry, follow the instructions below.

1. Click the **Add New** button in Figure 4-68, and you will see the screen as shown in Figure 4-69.

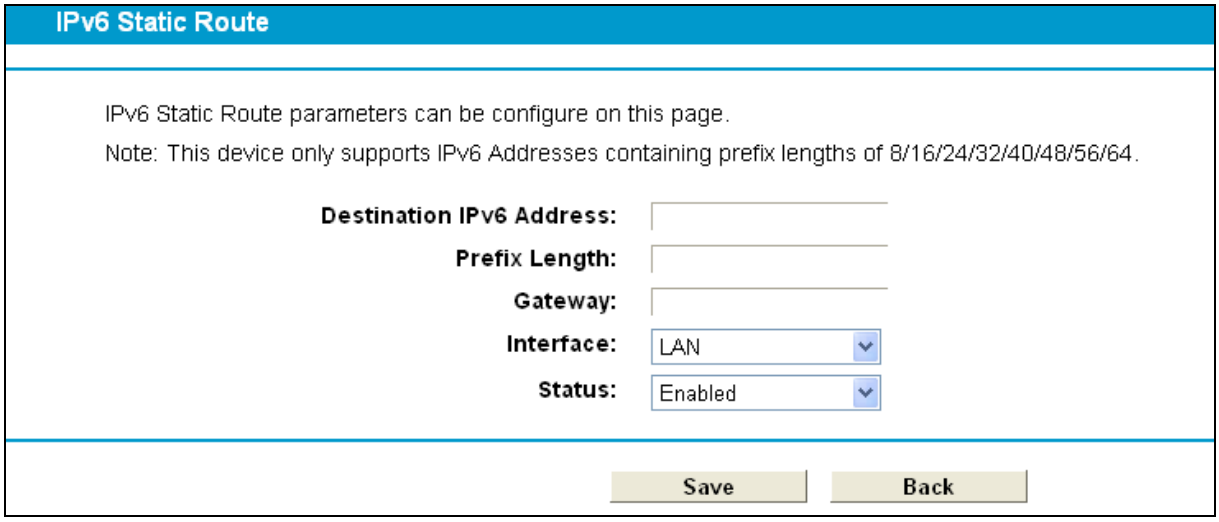


Figure 4-69

2. Enter the following data:

➢ **Destination IPv6 Address:** The IPv6 address of the network or host that you want to assign to a static route.

- **Prefix Length:** The prefix length of the destination IPv6 address.
- **Gateway:** Type in the correct IPv6 Gateway address for the IPv6 Static Route.
- **Interface:** Select the Interface from the drop-down list.
- **Status:** Select **Enabled** or **Disabled** from the drop-down list**.**

3. Click **Save** to save your settings.

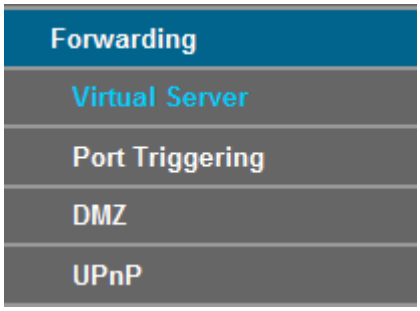
To modify or delete an existing entry:

1. Find the desired entry in the table.
2. Click **Edit** as desired on the **Edit** column.

Click the **Enable/ Disabled Selected** button to make selected entries enabled/ disabled.

Click the **Delete Selected** button to delete the selected entries.

4.14 Forwarding



There are four submenus under the Forwarding menu: **Virtual Server**, **Port Triggering**, **DMZ** and **UPnP**. Click any of them, and you will be able to configure the corresponding function.

4.14.1 Virtual Server

Choose menu "**Forwarding**" → "**Virtual Server**", and then you can view and add virtual servers in the next screen (shown in Figure 4-70). Virtual servers can be used for setting up public services on your LAN. A virtual server is defined as a service port, and all requests from Internet to this service port will be redirected to the computer specified by the server IP. Any PC that was used for a virtual server must have a static or reserved IP address because its IP address may change when using the DHCP function.

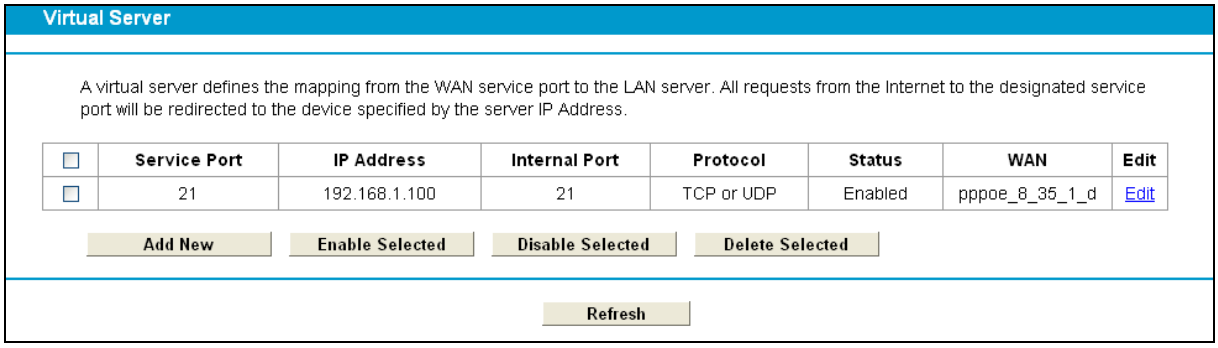


Figure 4-70

- **Service Port:** The numbers of External Service Ports. You can enter a service port or a range of service ports (the format is XX – YY; XX is the Start port and YY is the End port).

- **IP Address**: The IP address of the PC running the service application.
- **Protocol**: The protocol used for this application. The options are **TCP**, **UDP**, or **All** (all protocols supported by the modem router).
- **Status**: The status of this entry, "Enabled" means the virtual server entry is enabled.
- **Edit**: To modify or delete an existing entry.

To set up a virtual server entry:

1. Click the **Add New** button. (shown in Figure 4-71)
2. Select the service you want to use from the **Common Service Port** list. If the **Common Service Port** menu does not list the service that you want to use, enter the number of the service port or service port range in the **Service Port** field.
3. Enter the IP address of the computer running the service application in the **IP Address** field.
4. Select the protocol used for this application in the **Protocol** drop-down list.
5. Select the **Enabled** option in the **Status** drop-down list.

Click the **Save** button.

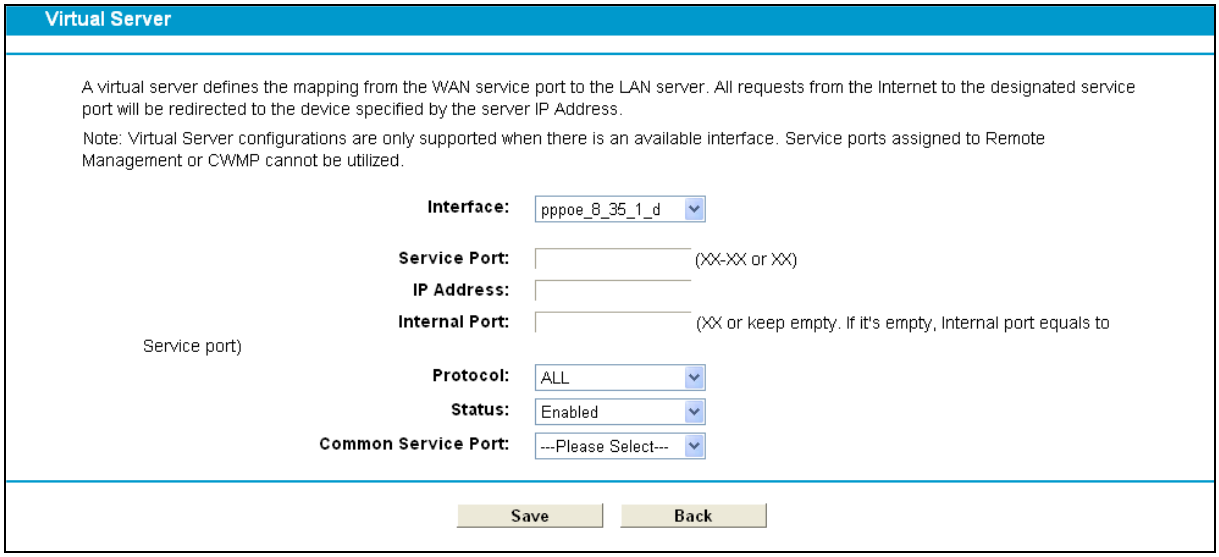


Figure 4-71

Note:

It is possible that you have a computer or server that has more than one type of available service. If so, select another service, and type the same IP address for that computer or server.

To modify or delete an existing entry:

1. Find the desired entry in the table.
2. Click **Edit** as desired on the **Edit** column.

Click the **Enable/ Disabled Selected** button to make selected entries enabled/ disabled.

Click the **Delete Selected** button to delete the selected entries.

Note:

If you set the service port of the virtual server as 80, you must set the Web management port on **System Tools –> Manage Control** page to be any other value except 80 such as 8080.

Otherwise there will be a conflict to disable the virtual server.

4.14.2 Port Triggering

Choose menu "**Forwarding**"→ "**Port Triggering**", you can view and add port triggering in the next screen (shown in Figure 4-72). Some applications require multiple connections, such as Internet games, video conferencing, Internet telephoning and so on. Port Triggering is used for those applications that cannot work with a pure NAT modem router.

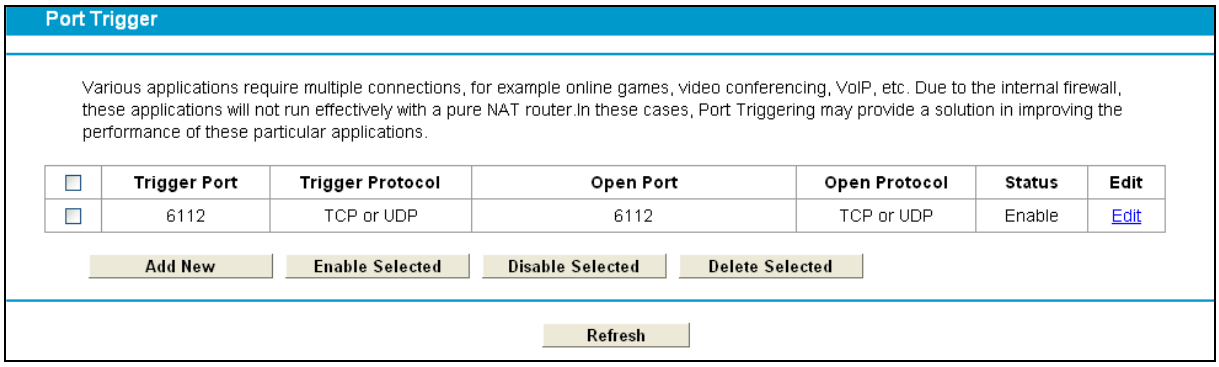


Figure 4-72

To add a new rule, follow the steps below.

1. Click the **Add New** button, the next screen will pop-up as shown in Figure 4-73.
2. Select a common application from the **Common Service Port** drop-down list, then both the **Trigger Port** field and the **Open Ports** field will be automatically filled. If the **Common Service Port** does not have the application you need, enter the **Trigger Port** and the **Open Ports** manually.
3. Select the protocol used for Trigger Port from the **Trigger Protocol** drop-down list. The options are **TCP**, **UDP**, or **All**.
4. Select the protocol used for Incoming Ports from the **Open Protocol** drop-down list. The options are **TCP**, **UDP**, or **All**. **.**
5. Select **Enable** in **Status** field.
6. Click the **Save** button to save the new rule.

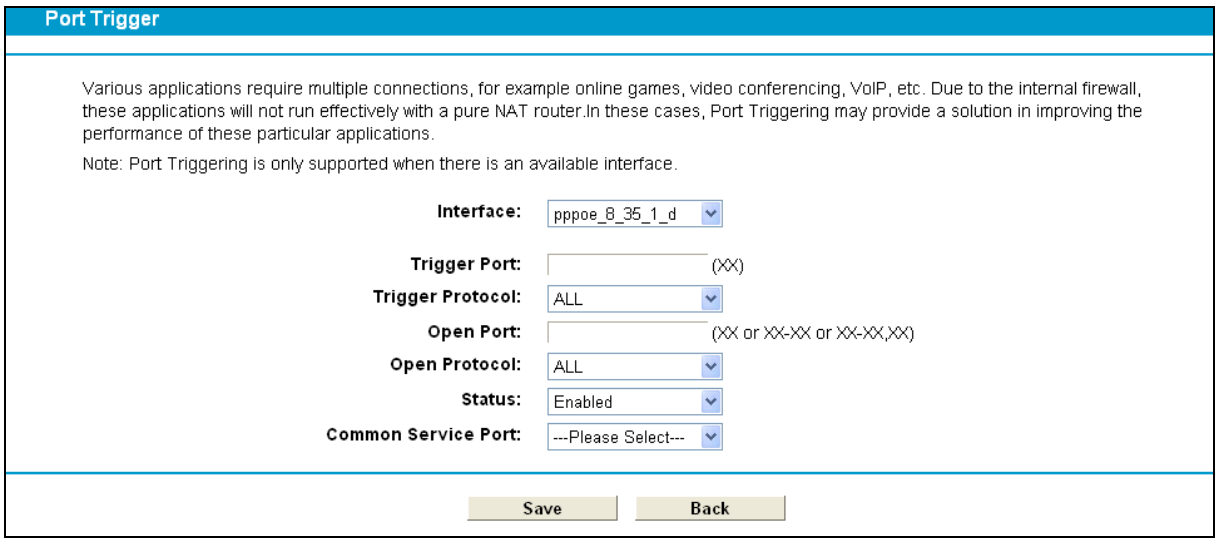


Figure 4-73

- **Interface**: Display the default gateway you have set in 4.5.1 WAN Settings.
- **Trigger Port**: The port for outgoing traffic. An outgoing connection using this port will trigger this rule.
- **Trigger Protocol**: The protocol used for Trigger Ports. The options are **TCP**, **UDP**, or **All** (all protocols supported by the modem router). .
- **Open Port**: The port or port range used by the remote system when it responds to the outgoing request. A response using one of these ports will be forwarded to the PC which triggered this rule. You can input at most 5 groups of ports (or port sections).
- **Open Protocol**: The protocol used for Open Port. The options are **TCP**, **UDP**, or **All** (all protocols supported by the modem router).
- **Status**: The status of this entry, Enabled means the Port Triggering entry is enabled.
- **Common Service Port**: Some popular applications already listed in the drop-down list of **Open Protocol**.

To modify or delete an existing entry:

1. Find the desired entry in the table.
2. Click **Edit** as desired on the **Edit** column.

Click the **Enable/ Disabled Selected** button to make selected entries enabled/ disabled.

Click the **Delete Selected** button to delete the selected entries.

Once the modem router is configured, the operation is as follows:

1. A local host makes an outgoing connection to an external host using a destination port number defined in the **Trigger Port** field.
2. The modem router records this connection, opens the incoming port or ports associated with this entry in the **Port Triggering** table, and associates them with the local host.
3. When necessary, the external host will be able to connect to the local host using one of the ports defined in the **Open Ports** field.

☞ **Note:**

1. When the trigger connection is released, the corresponding opened ports will be closed.
2. Each rule can only be used by one host on the LAN at a time. The trigger connection of other hosts on the LAN will be refused.
3. **Open Ports** ranges cannot overlap each other.

4.14.3 DMZ

Choose menu "**Forwarding→DMZ**", and then you can view and configure the DMZ host in the screen (shown in Figure 4-74).The DMZ host feature allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or video-conferencing. The modem router forwards packets of all services to the DMZ host. Any PC whose port is being forwarded must have its DHCP client function disabled and should have a new static IP Address assigned to it because its IP Address may be changed when using the DHCP function.

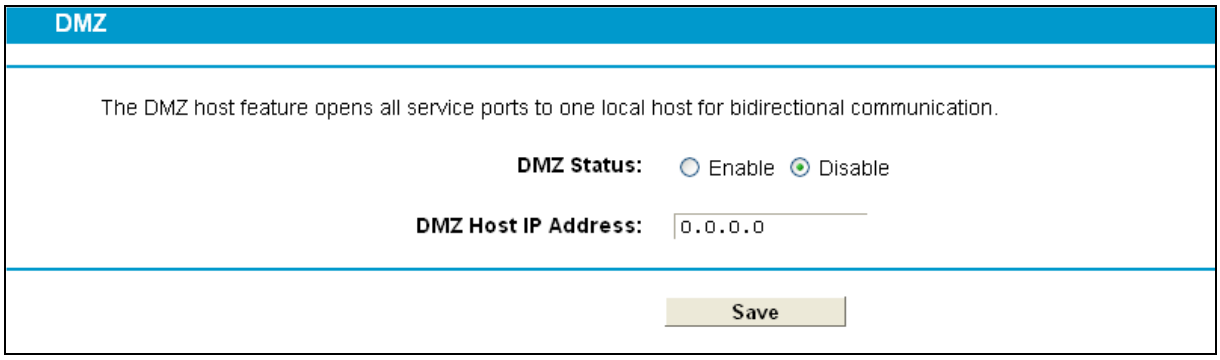


Figure 4-74

To assign a computer or server to be a DMZ server:

1. Click the **Enable** button.
2. Enter the IP address of a local PC that is set to be DMZ host in the **DMZ Host IP Address** field.
3. Click the **Save** button.

4.14.4 UPnP

Choose menu "**Forwarding→UPnP**", and then you can view the information about **UPnP** in the screen (shown in Figure 4-75). The **Universal Plug and Play (UPnP)** feature allows the devices, such as Internet computers, to access the local host resources or devices as needed. UPnP devices can be automatically discovered by the UPnP service application on the LAN.

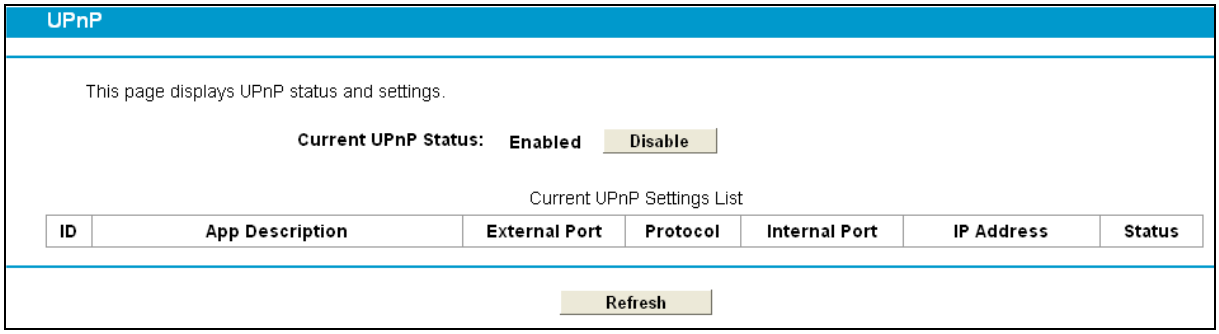


Figure 4-75

- **Current UPnP Status:** UPnP can be enabled or disabled by clicking the **Enable** or **Disable** button. This feature is enabled by default.
- **Current UPnP Settings List:** This table displays the current UPnP information.
  - **App Description**: The description about the application which initiates the UPnP request.
  - **External Port**: The port which the modem router opens for the application.
  - **Protocol**: The type of protocol which is opened.
  - **Internal Port**: The port which the modem router opened for local host.
  - **IP Address**: The IP address of the local host which initiates the UPnP request.

- **Status**: Either Enabled or Disabled. "Enabled" means that the port is still active; otherwise, the port is inactive.

Click the **Enable** button to enable UPnP.
Click the **Disable** button to disable UPnP.
Click the **Refresh** button to update the Current UPnP Settings List.

4.15 Parental Control

Choose menu "**Parental Control**", and you can configure the parental control in the screen as shown in Figure 4-76. The Parental Control function can be used to control Internet activities of the child, limit the child to access certain websites and restrict the time of surfing.

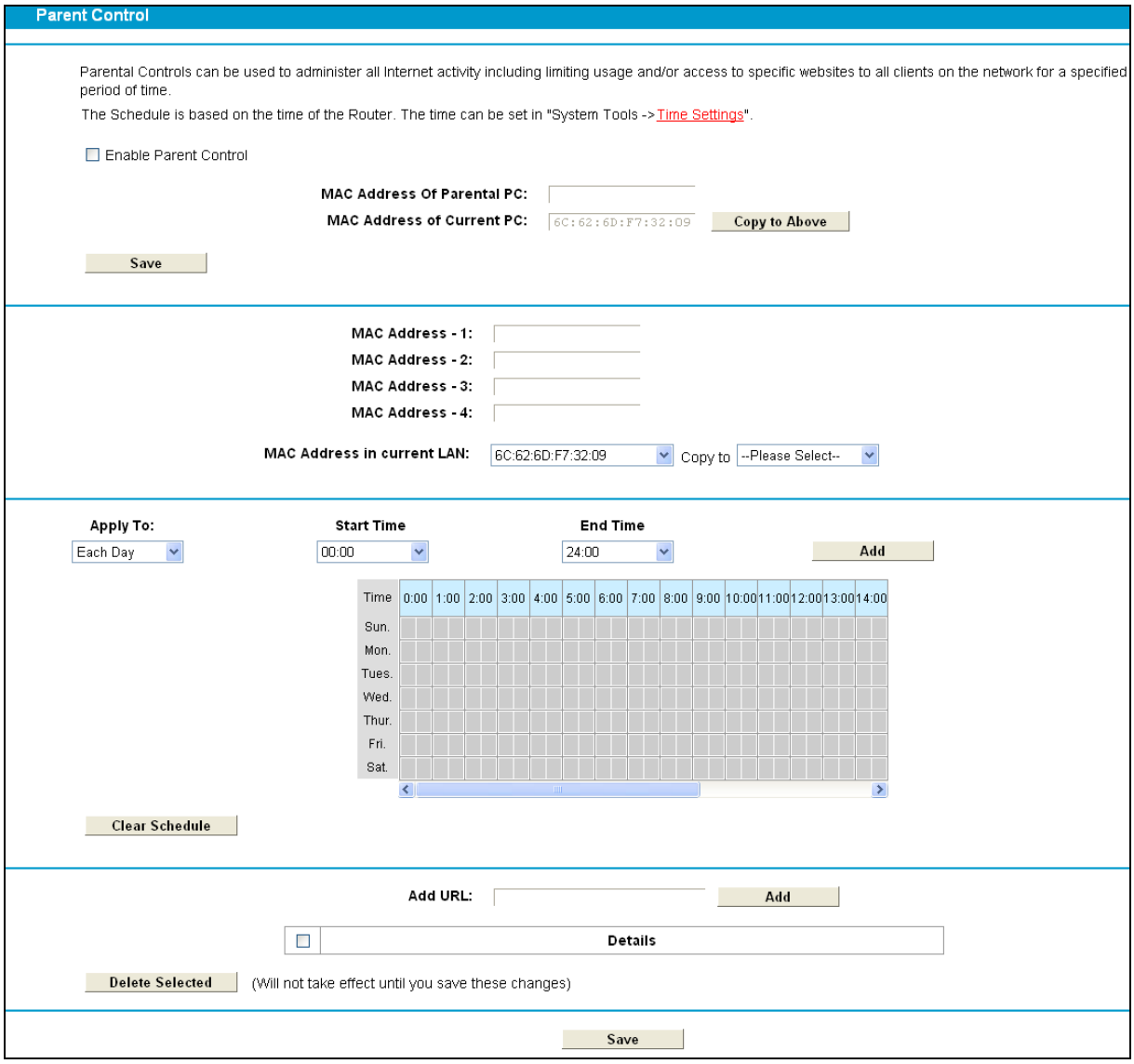


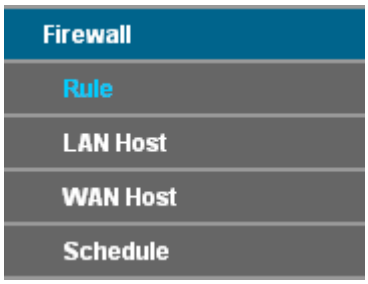
Figure 4-76

- **Enable Parental Control:** Check the box if you want this function to take effect. This function is disabled by default.
- **MAC Address of Parental PC:** In this field, enter the MAC address of the controlling PC, or you can make use of the **Copy To Above** button below.

- **MAC Address of Current PC:** This field displays the MAC address of the PC that is managing this modem router. If the MAC Address of your adapter is registered, you can click the Copy To Above button to fill this address to the MAC Address of Parental PC field above.
- **Add URL:** Here you can input the net addresses which the child is allowed to access.

Click the **Save** button to save your settings.

4.16 Firewall



There are four submenus under the Firewall menu: **Rule**, **LAN Host**, **WAN Host** and **Schedule**. Click any of them, and you will be able to configure the corresponding function.

4.16.1 Rule

Choose menu "**Firewall**" → "**Rule**", and then you can view and set access control rules in the screen as shown in Figure 4-77.

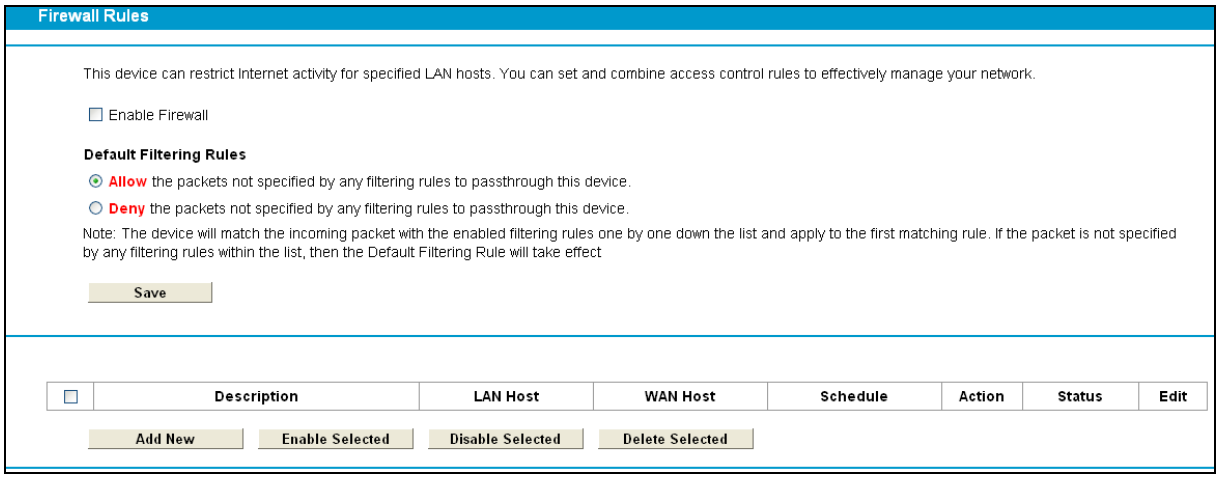


Figure 4-77

- **Enable Firewall:** Select the check box to enable the Firewall function, so the Default Filtering Rules can take effect.
- **Default Filtering Rules:** Select your desired filtering rule and click the **Save** button to save the rule.
- **Description:** Here displays the description of the rule and this name is unique.
- **LAN Host:** Here displays the LAN host selected in the corresponding rule.
- **WAN Host:** Here displays the WAN host selected in the corresponding rule.
- **Schedule:** Here displays the schedule selected in the corresponding rule.
- **Action：** Here displays the action selected in the corresponding rule.

- **Status:** Here displays the status of the rule, enabled or not.
- **Edit:** Here you can edit or delete an existing rule.

Click the **Enable /Disable Selected** button to enable or disable the selected rules in the list.

Click the **Delete Selected** button to delete the selected entries in the table.

The methods to add a new rule:

1. Click the **Add New** button and the next screen will pop up as shown in Figure 4-78.
2. Give a name (e.g. Rule_1) for the rule in the **Description** field.
3. Select a host from the **LAN Host** drop-down list or choose "**Add LAN Host**".
4. Select a target from the **WAN Host** drop-sown list or choose "**Add WAN Host**".
5. Select a schedule from the **Schedule** drop-down list or choose "**Add Schedule**".
6. In the **Action** field, select **Deny** or **Allow** to deny or allow your entry.
7. In the **Status** field, select **Enabled** or **Disabled** to enable or disable your entry.
8. In the **Direction** field, select **IN** or **OUT** from the drop-down list for the direction.
9. In the **Protocol** field, there are four options: All, TCP, UDP, and ICMP. Select one of them from the drop-down list for the target.
10. Click the **Save** button.

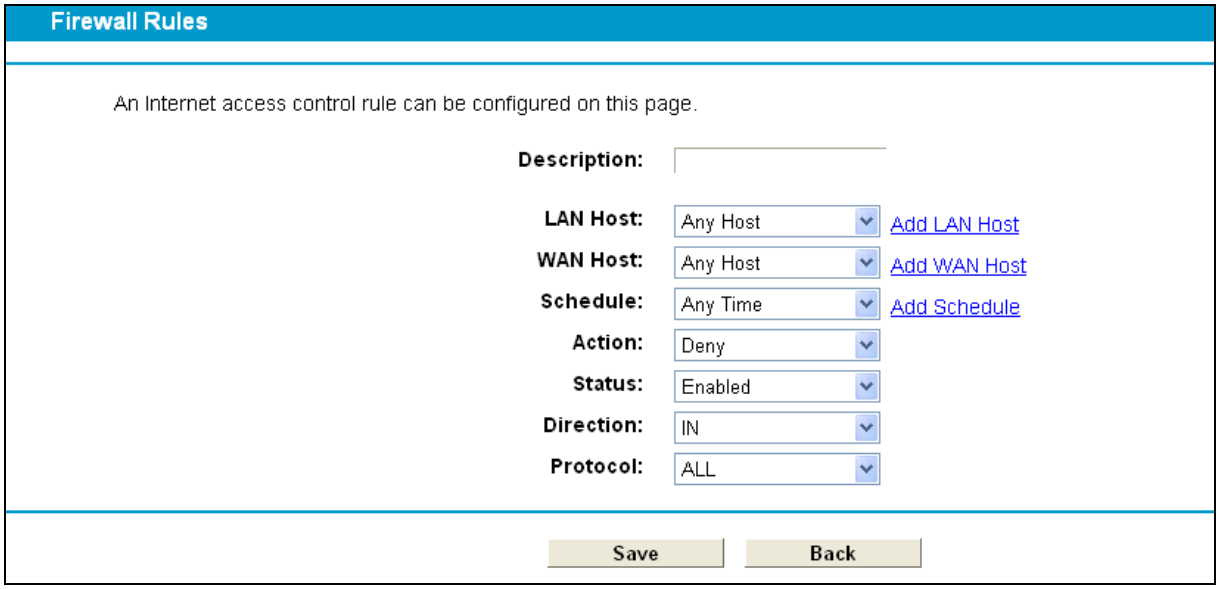


Figure 4-78

4.16.2 LAN Host

Choose menu "**Firewall**" → "**LAN Host**", and then you can view and set a Host list in the screen as shown in Figure 4-79.

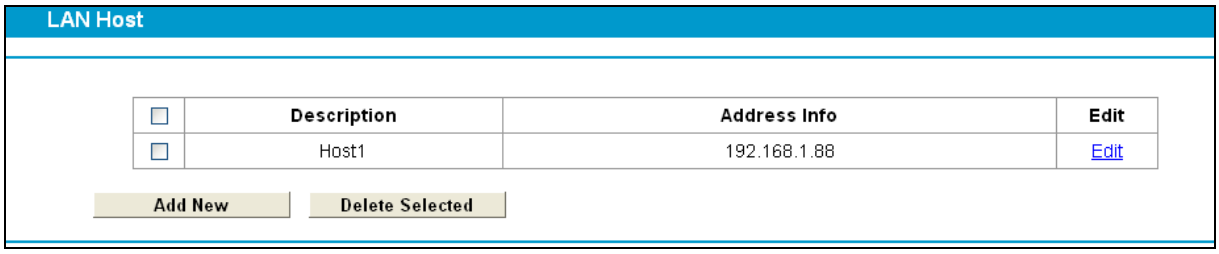


Figure 4-79

- **Description:** Here displays the description of the host and this description is unique.
- **Address Info:** Here displays the information about the host. It can be IP or MAC.
- **Edit:** To modify an existing entry.

To add a new entry, please follow the steps below.

1. Click the **Add New** button.
2. In the **Mode** field, select IP Address or MAC Address.
   - If you select IP Address, please follow the steps below:
     1) In **Description** field, create a unique description for the host (e.g. Host_1).
     2) In **IP Address** field, enter the IP address.
   - If you select MAC Address, please follow the steps below:
     1) In **Description** field, create a unique description for the host (e.g. Host_1).
     2) In **MAC Address** field, enter the MAC address.
3. Click the **Save** button to complete the settings.

Click the **Delete Selected** button to delete the selected entries in the table.

4.16.3 WAN Host

Choose menu "**Firewall**" → "**WAN Host**", and then you can view and set a Host list in the screen as shown in Figure 4-80.

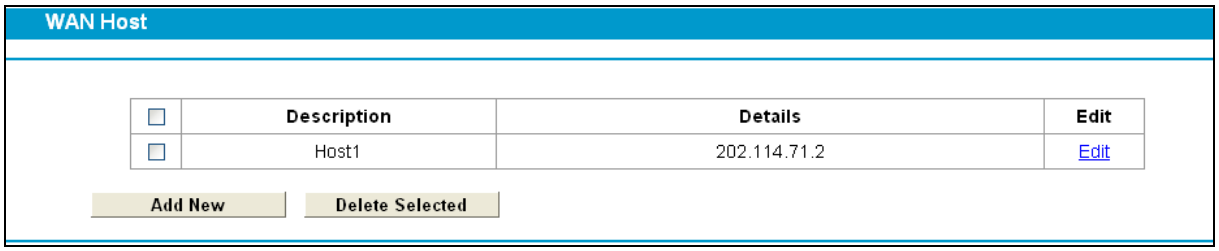


Figure 4-80

- **Description:** Here displays the description about the WAN and this description is unique.
- **Details:** The details can be IP address, port, or domain name.
- **Edit:** To modify an existing entry.

To add a new entry, please follow the steps below.

1. Click the **Add New** button.
2. In Mode field, select **IP Address**, **MAC Address** or **URL Address**.

If you select **IP Address**, the screen shown is Figure 4-81.

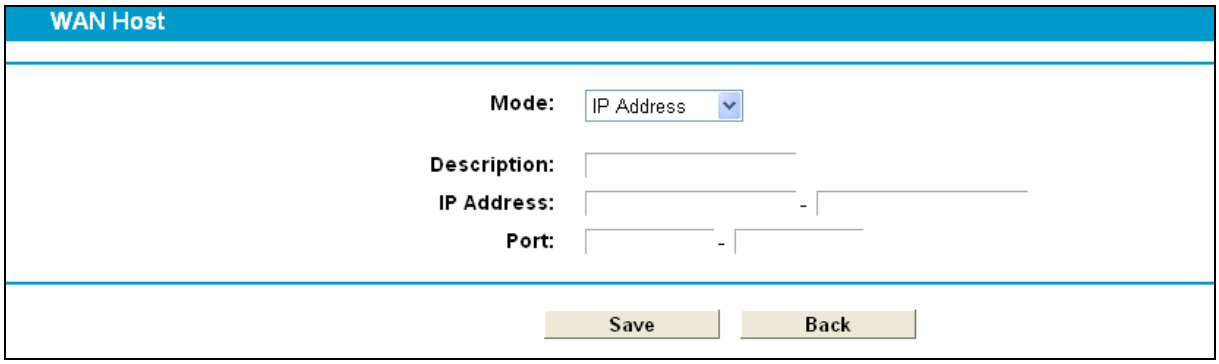


Figure 4-81

1) In **Description** field, create a unique description for the host (e.g. Host_1).

2) In **IP Address** field, enter the IP address.

If you select **MAC Address**, the screen shown is Figure 4-82.

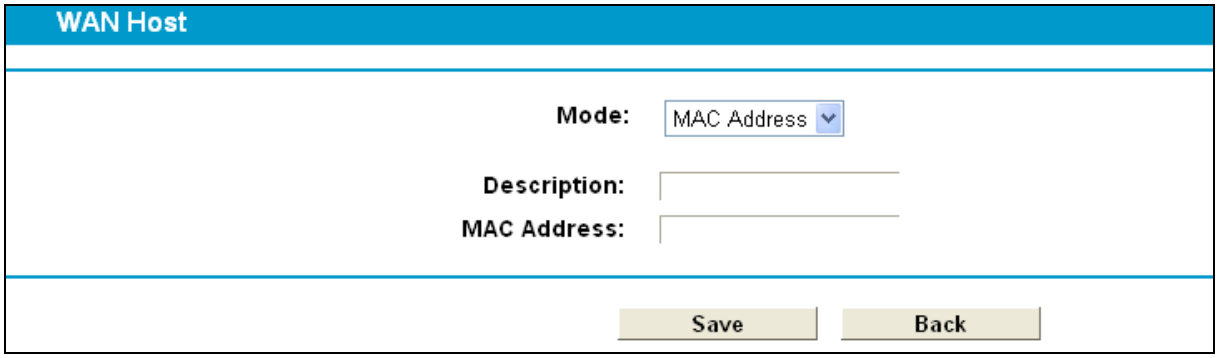


Figure 4-82

1) In **Description** field, create a unique description for the host (e.g. Host_1).
2) In **MAC Address** field, enter the MAC address.

If you select **URL Address**, the screen shown is Figure 4-83.

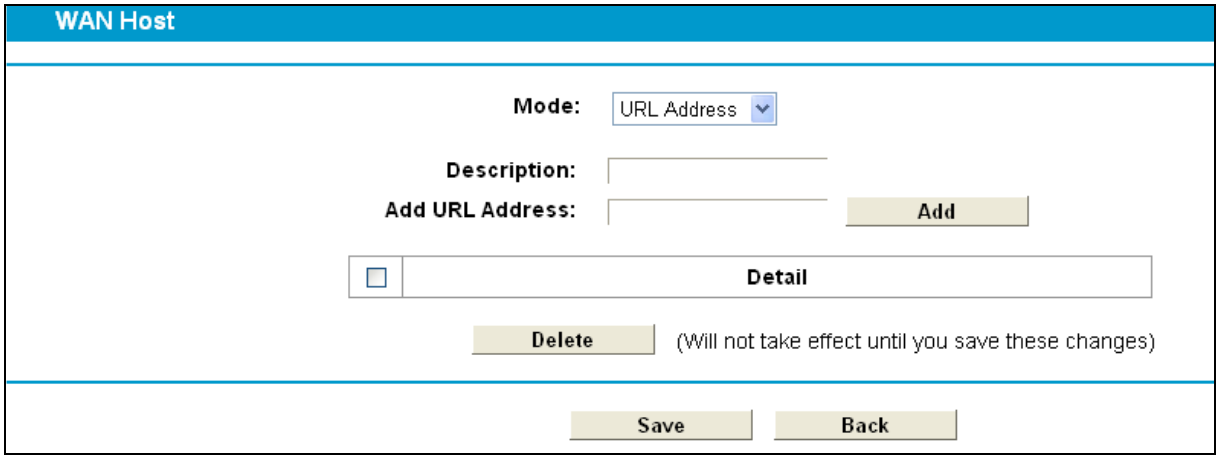


Figure 4-83

1) In **Description** field, create a unique description for the host (e.g. Host_1).

2) Enter the URL address in the **Add URL Address** field, and then click the **Add** button. The URL address will be shown in the **Detail** table. If you click the **Delete** button, the chosen URL address in the **Detail** table can be deleted.

3. Click the **Save** button to complete the settings.

4.16.4 Schedule

Choose menu "**Firewall**" → "**Schedule**", and then you can view and set a Schedule list in the next screen as shown in Figure 4-84.

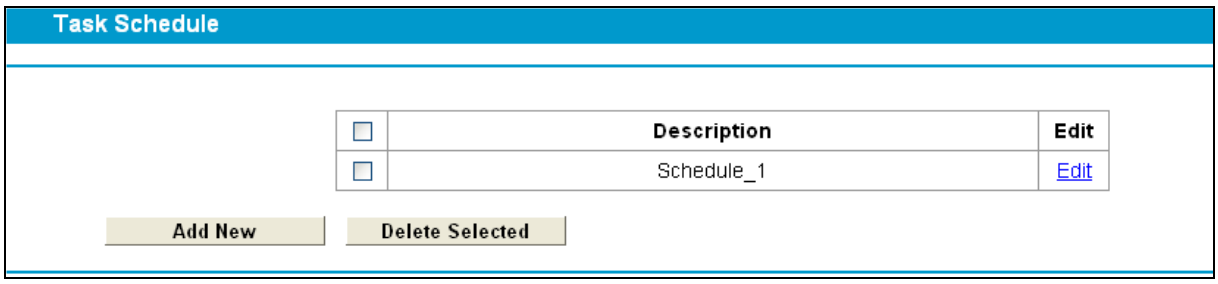


Figure 4-84

- **Description**: Here displays the description of the schedule and this description is unique.
- **Edit**: Here you can modify an existing schedule.

To add a new schedule, follow the steps below:

1. Click **Add New** button and the next screen will pop-up as shown in Figure 4-85.
2. In **Description** field, create a unique description for the schedule (e.g. Schedule_1).
3. In **Apply To** field, select the day or days you need.
4. In time field, you can select all day-24 hours or you may enter the **Start Time** and **End Time** in the corresponding field.
5. Click **Save** to complete the settings.

Click the **Clear Schedule** button to clear your settings in the table.

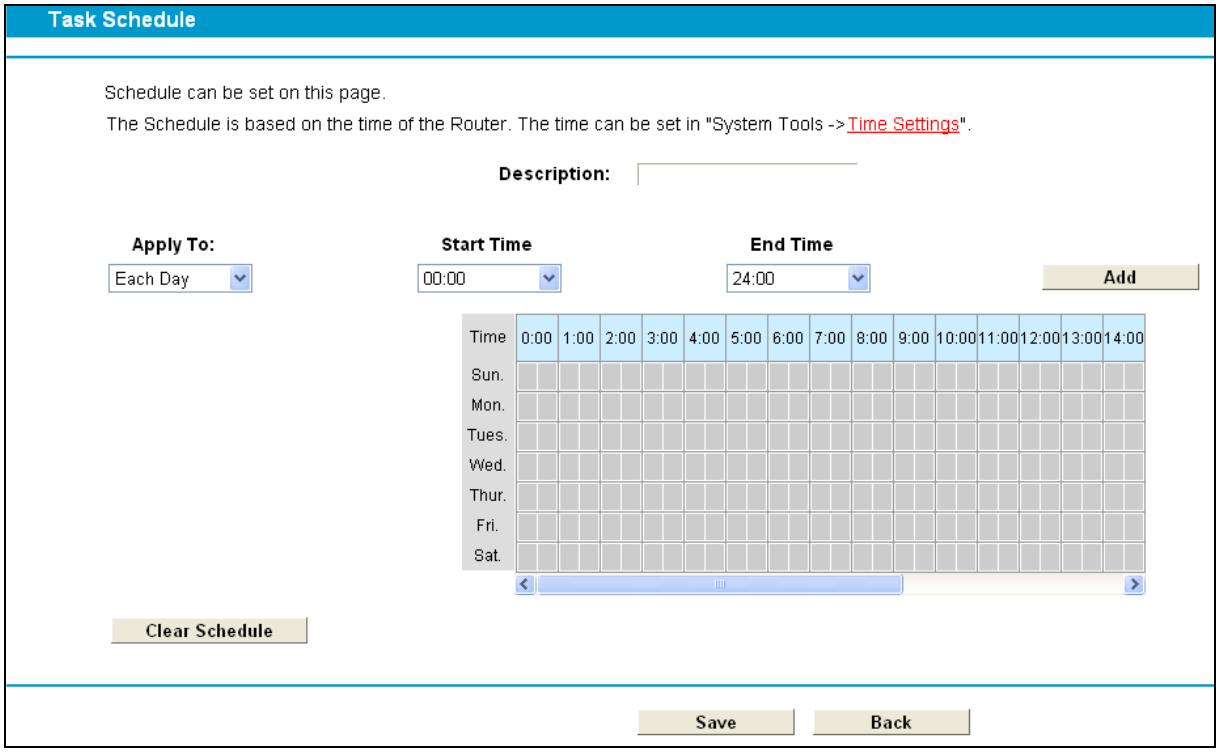
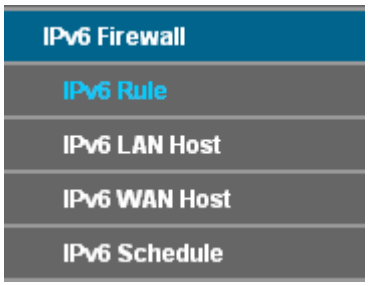


Figure 4-85

Click the **Delete Selected** button to delete the selected entries in the table.

4.17 IPv6 Firewall



There are four submenus under the IPv6 Firewall menu: **IPv6 Rule**, **IPv6 LAN Host**, **IPv6 WAN Host** and **IPv6 Schedule**. Click any of them, and you will be able to configure the corresponding function.

4.17.1 IPv6 Rule

Choose menu "**IPv6 Firewall**" → "**IPv6 Rule**", and then you can view and set access control rules in the screen as shown in Figure 4-86.

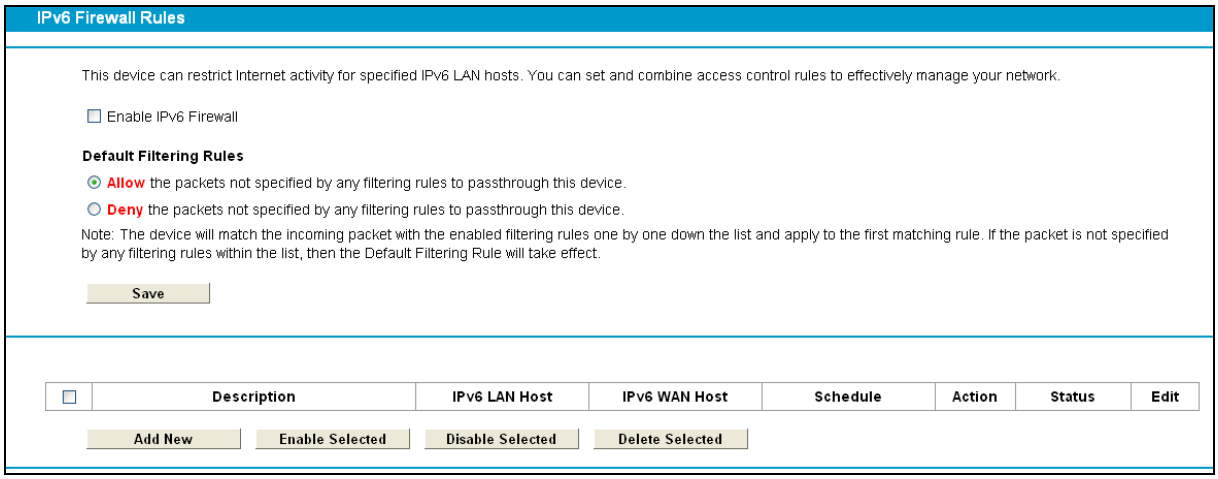


Figure 4-86

- **Enable IPv6 Firewall:** Select the check box to enable the IPv6 Firewall function, so the Default Filtering Rules can take effect.
- **Description:** Here displays the description of the IPv6 rule and this name is unique.
- **IPv6 LAN Host:** Here displays the LAN host selected in the corresponding rule.
- **IPv6 WAN Host:** Here displays the WAN host selected in the corresponding rule.
- **Schedule:** Here displays the schedule selected in the corresponding rule.
- **Action：** Here displays the action selected in the corresponding rule.
- **Status:** Here displays the status of the rule, either enabled or disabled.
- **Edit:** Here you can edit or delete an existing rule.

To add a new IPv6 rule:

1. Click the **Add New** button, and you will see the screen as shown in Figure 4-87.

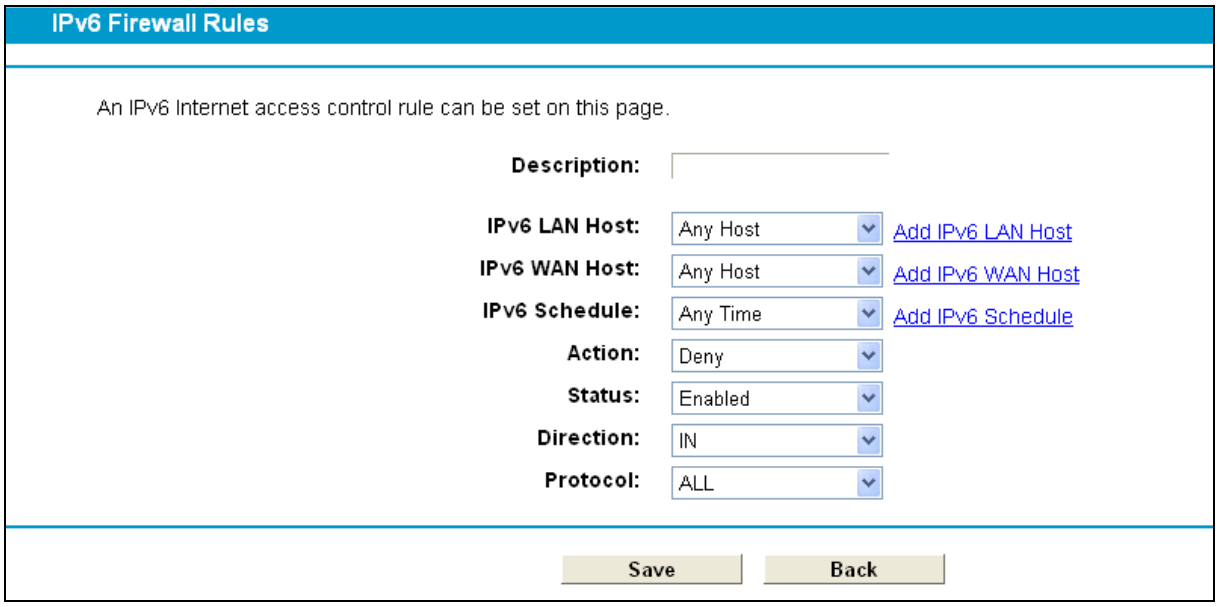


Figure 4-87

2. Give a name (e.g. Rule_1) for the rule in the **Description** field.
3. Select a host from the **IPv6 LAN Host** drop-down list or choose "**Add IPv6 LAN Host**".
4. Select a host from the **IPv6 WAN Host** drop-sown list or choose "**Add IPv6 WAN Host**".
5. Select a schedule from the **IPv6 Schedule** drop-down list or choose "**Add IPv6 Schedule**".
6. In the **Action** field, select **Deny** or **Allow** to deny or allow your entry.
7. In the **Status** field, select **Enabled** or **Disabled** to enable or disable your entry.
8. In the **Direction** field, select **IN** or **OUT** from the drop-down list for the direction.
9. In the **Protocol** field, here are four options, All, TCP, UDP, and ICMPv6. Select one of them from the drop-down list for the target.
10. Click the **Save** button to save the settings.

Click the **Enable/ Disable Selected** button to make selected entries enabled or disabled.

Click the **Delete Selected** button to delete the selected entries.

4.17.2 IPv6 LAN Host

Choose menu "**IPv6 Firewall**" → "**IPv6 LAN Host**", and then you can view and set a Host list in the screen as shown in Figure 4-88.

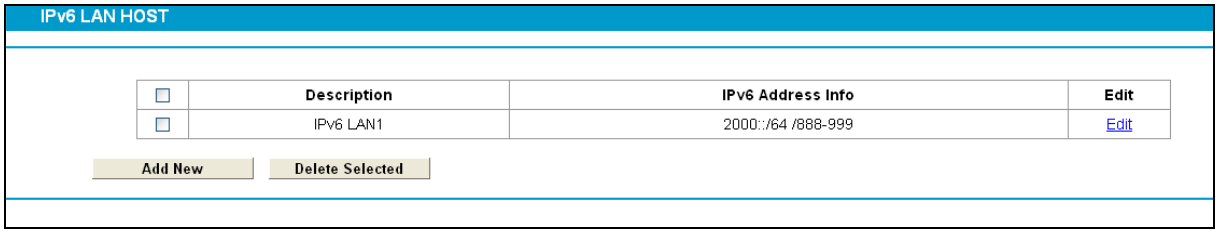


Figure 4-88

- **Description:** Here displays the description of the host and this description is unique.
- **IPv6 Address Info:** Here displays the information about the host.

➢ **Edit:** To modify an existing entry.

To add a new entry, please follow the steps below.

1. Click the **Add New** button, and you will see the screen as shown in Figure 4-89.

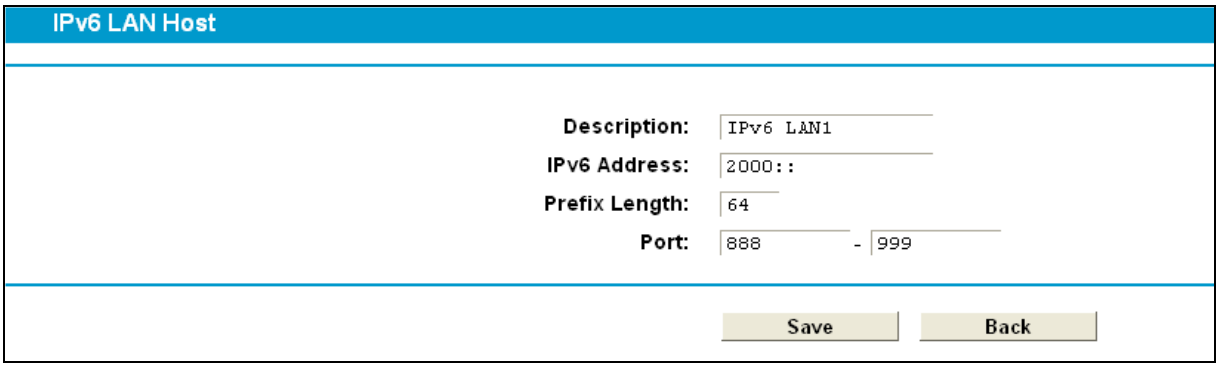


Figure 4-89

2. Create a unique name for the host (e.g. Host_1) in the **Description** field.
3. Enter an IPv6 address in the **IPv6 Address** field.
4. Enter the prefix length of the IPv6 address in the **Prefix Length** field.
5. Click the **Save** button to save the settings.

Click the **Delete Selected** button to delete the selected entries.

4.17.3 IPv6 WAN Host

Choose menu "**IPv6 Firewall**" → "**IPv6 WAN Host**", and then you can view and set a Host list in the screen as shown in Figure 4-90.

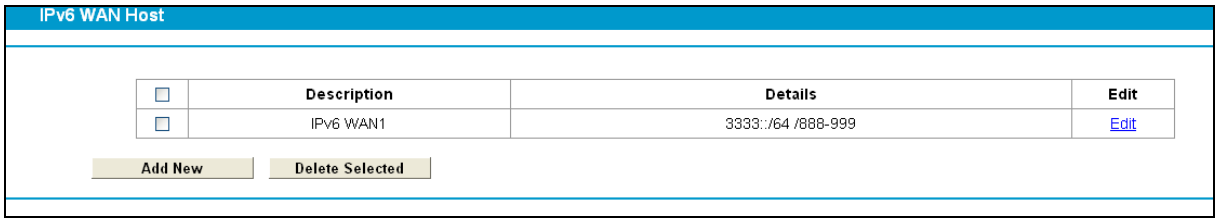


Figure 4-90

➢ **Description:** Here displays the description about the WAN and this description is unique.

➢ **Details:** The details can be IPv6 address, prefix length or port.

➢ **Edit:** To modify an existing entry.

To add a new entry, please follow the steps below.

1. Click the **Add New** button, and you will see the screen as shown in Figure 4-91.

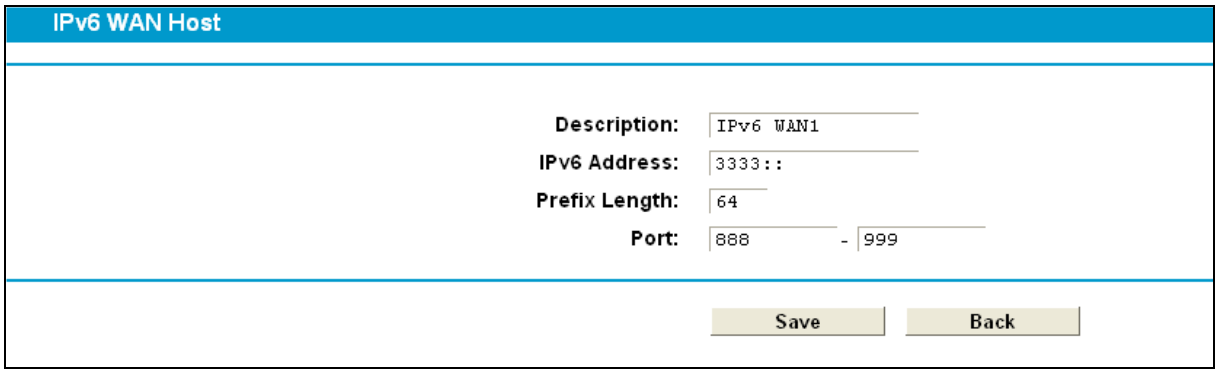


Figure 4-91

2. Create a unique description for the host (e.g. Host_1) in the **Description** field.
3. Enter an IPv6 address in the **IPv6 Address** field.
4. Enter the prefix length of the IPv6 address in the **Prefix Length** field.
5. Click the **Save** button to save the settings.

Click the **Delete Selected** button to delete the selected entries.

4.17.4 IPv6 Schedule

Choose menu "**IPv6 Firewall**" → "**IPv6 Schedule**", and then you can view and set a Schedule list in the next screen as shown in Figure 4-92.

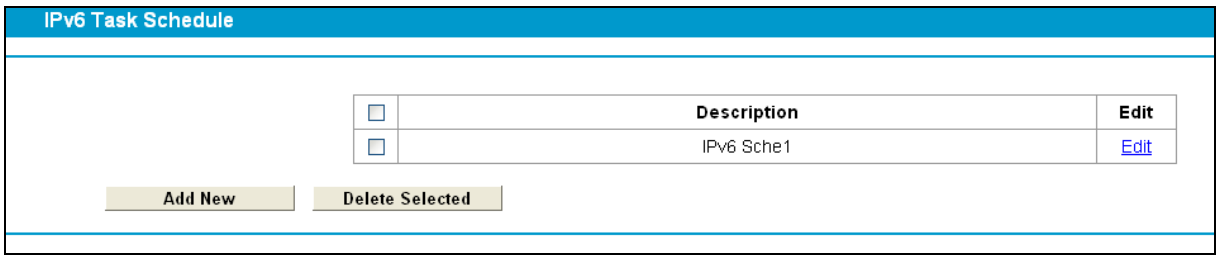


Figure 4-92

- **Description**: Here displays the description of the schedule and this description is unique.
- **Edit**: Here you can modify an existing schedule.

To add a new schedule, follow the steps below:

1. Click **Add New** button and you will see the screen as shown in Figure 4-93.

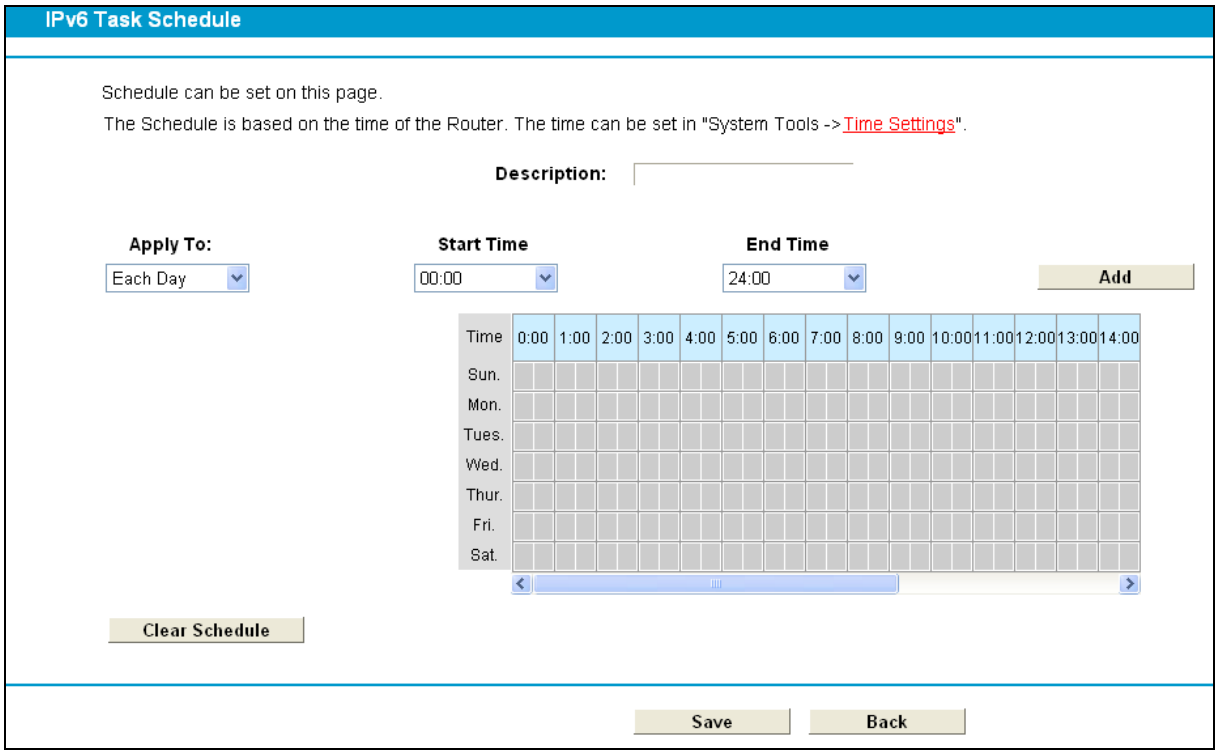


Figure 4-93

2. Create a unique description for the schedule (e.g. Schedule_1) in **Description** field.
3. Select the day or days you need in **Apply To** field.
4. In time field, you can select all day-24 hours or you may enter the **Start Time** and **End Time** in the corresponding field.
5. Click **Save** to save the settings.

Click the **Clear Schedule** button to clear your settings in the table.

Click the **Delete Selected** button to delete the selected entries.

4.18 IPv6 Tunnel

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.

Choose menu "**IPv6 Tunnel**", and you will see the screen as shown in Figure 4-94.

Figure 4-94

- **Enable:** Check the box to enable IPv6 Tunnel function. It is disabled by default.
- **Mechanism:** Select a type for IPv6 tunnel from the drop-down list. DS-Lite, 6RD and 6to4 are supported.

1) DS-Lite

This type is used in the situation that your WAN connection is IPv6 while LAN connection is IPv4. Select DS-Lite, and you will see the screen as shown in Figure 4-95.

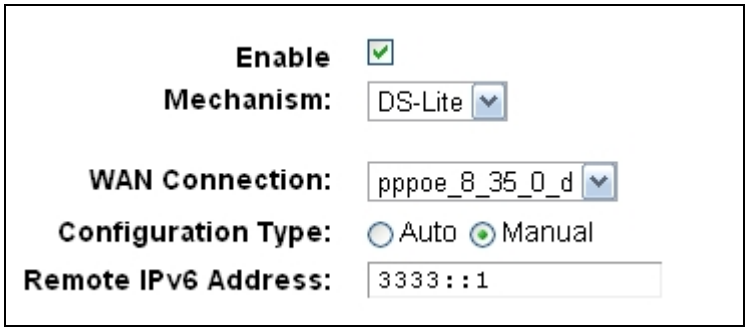


Figure 4-95

- **WAN Connection:** Select a WAN connection from the drop-down list. Only the connected WAN connections can be shown in the drop-down list.
- **Configuration Type:** Select a configuration type for this tunnel. **Auto** means to obtain the Remote IPv6 Address automatically while **Manual** means you set it manually.
- **Remote IPv6 Address:** Enter the IPv6 address of the remote node.

Note:

In this type, there should not have any IPv4 WAN connections. If there are IPv4 WAN connections, the page will prompt you to delete all the IPv4 WAN connections.

2) 6RD

This type is used in the situation that your WAN connection is IPv4 while LAN connection is IPv6. Select 6RD, and you will see the screen as shown in Figure 4-96.

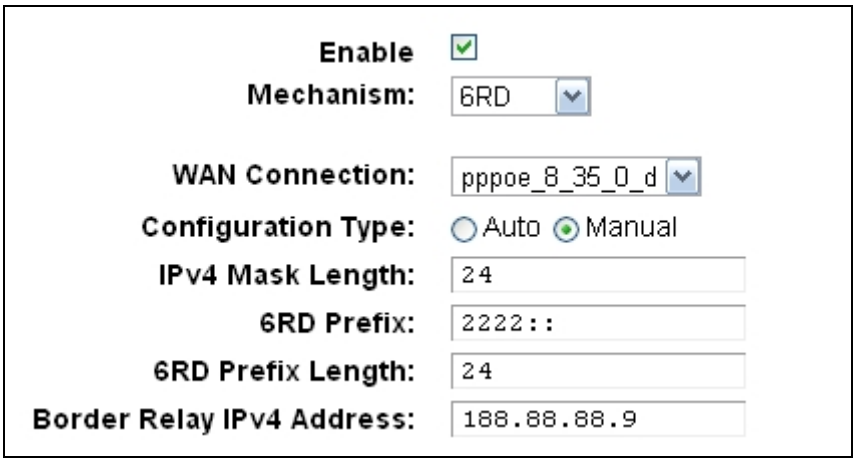


Figure 4-96

- **WAN Connection:** Select a WAN connection from the drop-down list. Only the connected WAN connections can be shown in the drop-down list.
- **Configuration Type:** Select a configuration type for this tunnel. Auto means to obtain the following parameters automatically while Manual means you set them up manually. If Auto is selected, only Dynamic IP WAN connection can be selected from the drop-down list.
- **IPv4 Mask Length:** The length of the selected WAN connection's IPv4 mask.
- **6RD Prefix:** The prefix of the 6RD tunnel.
- **6RD Prefix Length:** The length of the 6RD prefix.
- **Border Relay IPv4 Address:** The IPv4 address of the border relay router of 6RD tunnel.

Note:

In this type, there should not be any IPv6 WAN connections. If there are IPv6 WAN connections, the page will advise you to delete all the IPv6 WAN connections.

3) 6to4

This type is used in the situation that your WAN connection is IPv4 while LAN connection is IPv6. Select 6to4, and you will see the screen as shown in Figure 4-97.

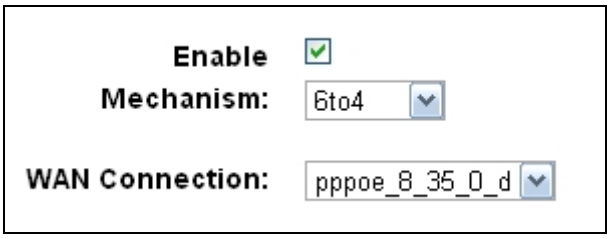


Figure 4-97

- **WAN Connection:** Select a WAN connection from the drop-down list. Only the connected WAN connections can be shown in the drop-down list.

Note:

In this type, there should not be any IPv6 WAN connections. If there are IPv6 WAN connections, the page will prompt you to delete all the IPv6 WAN connections.

4.19 Bandwidth Control

Choose menu "**Bandwidth Control**", and then you can configure the Upstream Bandwidth and Downstream Bandwidth in the next screen. The values you configure should be less than 1000000Kbps. For optimal control of the bandwidth, please select the right Line Type and consult your ISP for the total bandwidth of the egress and ingress.

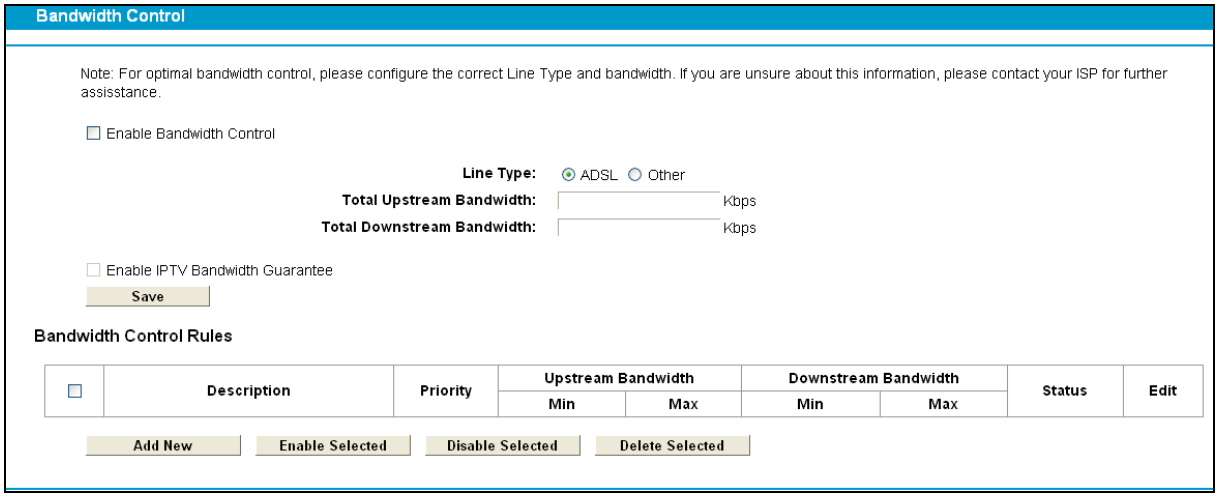


Figure 4-98

- **Enable Bandwidth Control:** Check this box to make the Bandwidth Control settings take effect. The bandwidth control rules won't take effect if bandwidth control is disabled.
- **Total Upstream Bandwidth:** The upload speed through the WAN port.
- **Total Downstream Bandwidth:** The download speed through the WAN port.
- **Enable IPTV Bandwidth Guarantee:** Check the box to enable IPTV bandwidth control.
- **Description:** This is the information about the rules such as address range.
- **Priority:** The priority of Bandwidth Control rules. '1' stands for the highest priority while '8' stands for the lowest priority. The total Upstream/ Downstream Bandwidth is first allocated to guarantee all the Min Rate of Bandwidth Control rules. If there is any bandwidth left, it is first allocated to the rule with the highest priority, then to the rule with the second highest priority, and so on.
- **Upstream bandwidth:** This field displays the max and min upload bandwidth through the WAN port.
- **Downstream bandwidth:** This field displays the max and min download bandwidth through the WAN port.
- **Status:** The status of this rule, either Enabled or Disabled.
- **Edit:** Click **Edit** to modify the rule.

To add/modify a Bandwidth Control rule, follow the steps below.

1. Click **Add New** shown in Figure 4-98, you will see a new screen shown in Figure 4-99.
2. Enter the information as the screen shown below.

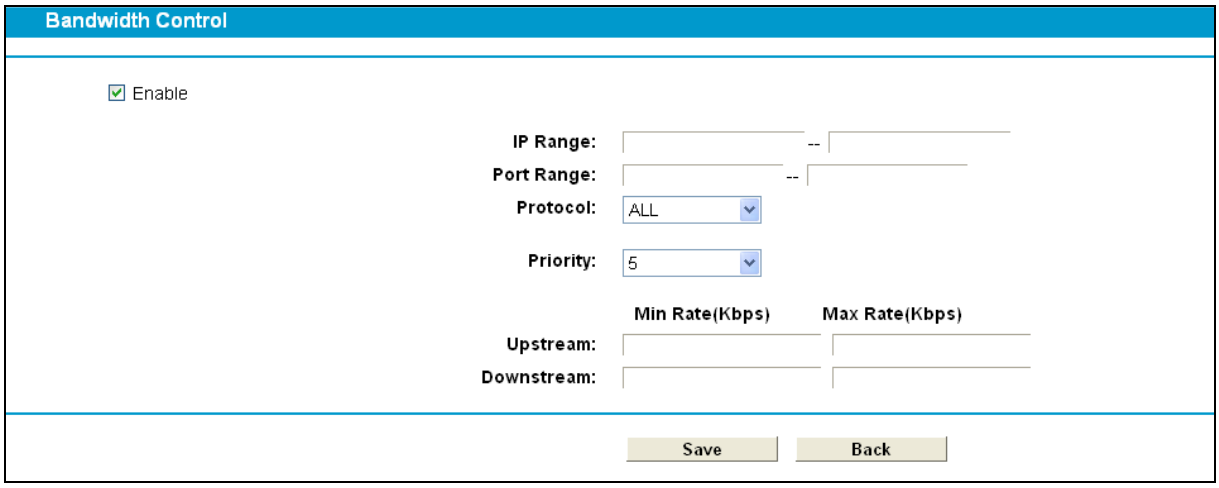


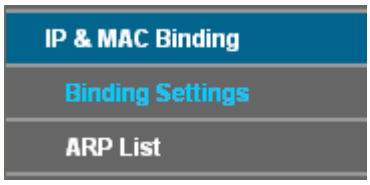
Figure 4-99

3. Click the **Save** button.

Click the **Enable/ Disable Selected** button to make selected entries enabled or disabled.

Click the **Delete Selected** button to delete the selected entries.

4.20 IP&MAC Binding



There are two submenus under the IP &MAC Binding menu: **Binding Settings** and **ARP List**. Click any of them, and you will be able to scan or configure the corresponding function. The detailed explanations for each submenu are provided below.

4.20.1 Binding Settings

This page displays the **IP & MAC Binding Setting** table; you can operate it in accord with your desire (shown in Figure 4-100).

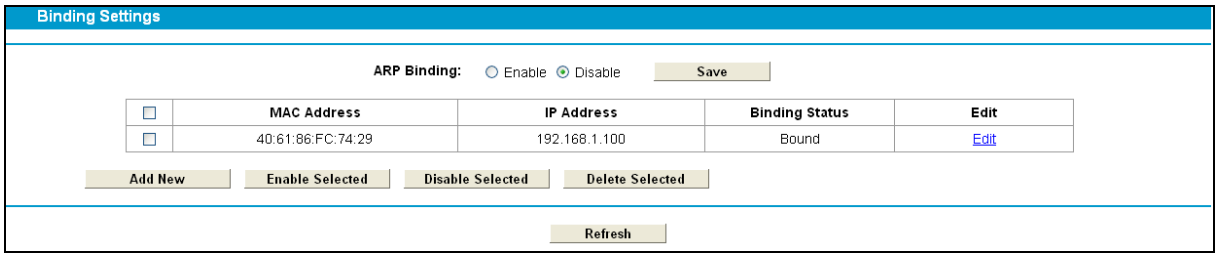


Figure 4-100

- **MAC Address:** The MAC address of the controlled computer in the LAN.
- **IP Address:** The assigned IP address of the controlled computer in the LAN.
- **Binding Status:** Indicates whether or not the MAC address and IP address are bound.
- **Edit:** To modify or delete an existing entry.

When you want to add or modify an IP & MAC Binding entry, you can click the **Add New** button or **Edit** button, and then you will go to the next page. This page is used for adding or modifying an IP & MAC Binding entry (shown in Figure 4-101.)

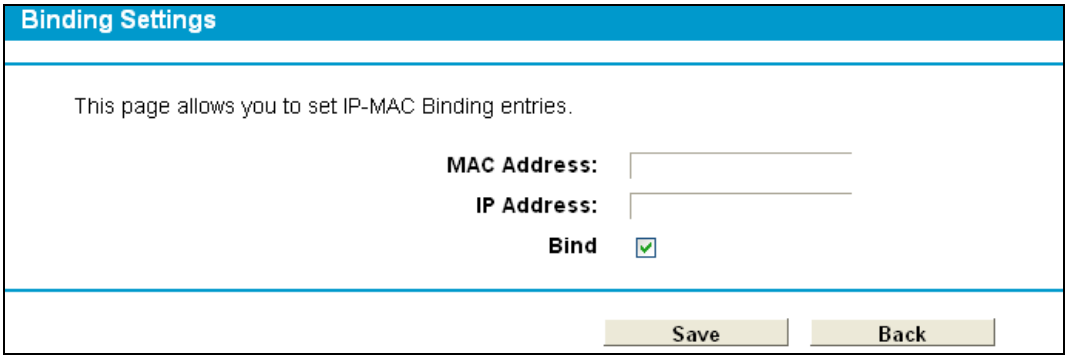


Figure 4-101

To add IP & MAC Binding entries, follow the steps below.

1. Click the **Add New** button as shown in Figure 4-100.
2. Enter the MAC Address and IP Address.
3. Select the Bind checkbox.
4. Click the **Save** button to save it.

To modify or delete an existing entry, follow the steps below.

1. Find the desired entry in the table.
2. Click **Edit** as desired on the **Edit** column.

Click the **Enable/ Disable Selected** button to make selected entries enabled or disabled.

Click the **Delete Selected** button to delete the selected entries.

4.20.2 ARP List

To manage the computer, you could observe the computers in the LAN by checking the relationship of MAC address and IP address on the ARP list, and you could also configure the items on the ARP list. This page displays the ARP List and shows all the existing IP & MAC Binding entries (shown in Figure 4-102).

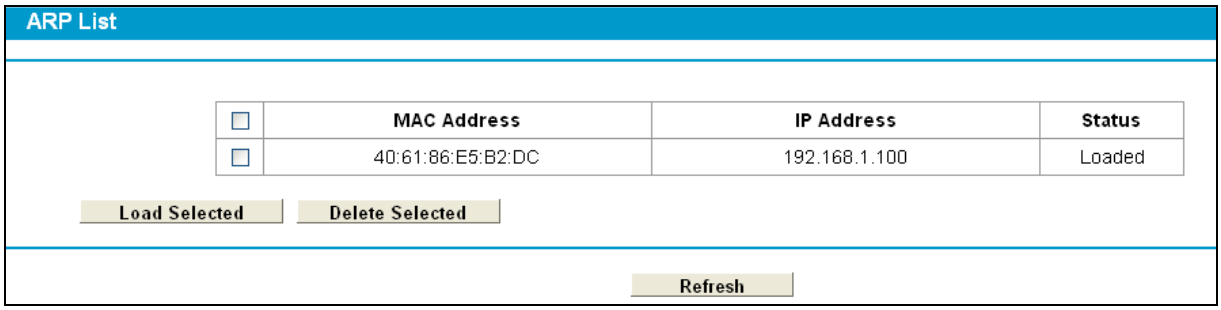


Figure 4-102

- **MAC Address:** The MAC address of the controlled computer in the LAN.
- **IP Address:** The assigned IP address of the controlled computer in the LAN.
- **Status:** Indicates whether or not the MAC and IP addresses are bound.

Click the **Load Selected** button to load selected items to the IP & MAC Binding list.

Click the **Delete Selected** button to delete the selected entries.

Click the **Refresh** button to refresh all items.

4.21 Dynamic DNS

Choose menu "**Dynamic DNS**", and you can configure the Dynamic DNS function.

The modem router offers the **DDNS** (Dynamic Domain Name System) feature, which allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (named by yourself) and a dynamic IP address, then your friends can connect to your server by entering your domain name no matter what your IP address is. Before using this feature, you need to sign up for DDNS service providers such as www.no-ip.com. The Dynamic DNS client service provider will give you a password or key.

Figure 4-103

- **Service Provider:** This field displays the service provider of DDNS.
- **Domain Name:** Enter the Domain name you received from the DDNS service provider.
- **Username & Password:** Type in the "User Name" and "Password" for your DDNS account.
- **Enable DDNS:** Check to activate the DDNS function.
- **Login/ Logout:** Log in to or log out of the DDNS service.

4.22 Diagnostic

Choose "**Diagnostic**", 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. Select your desired type and click the start button.

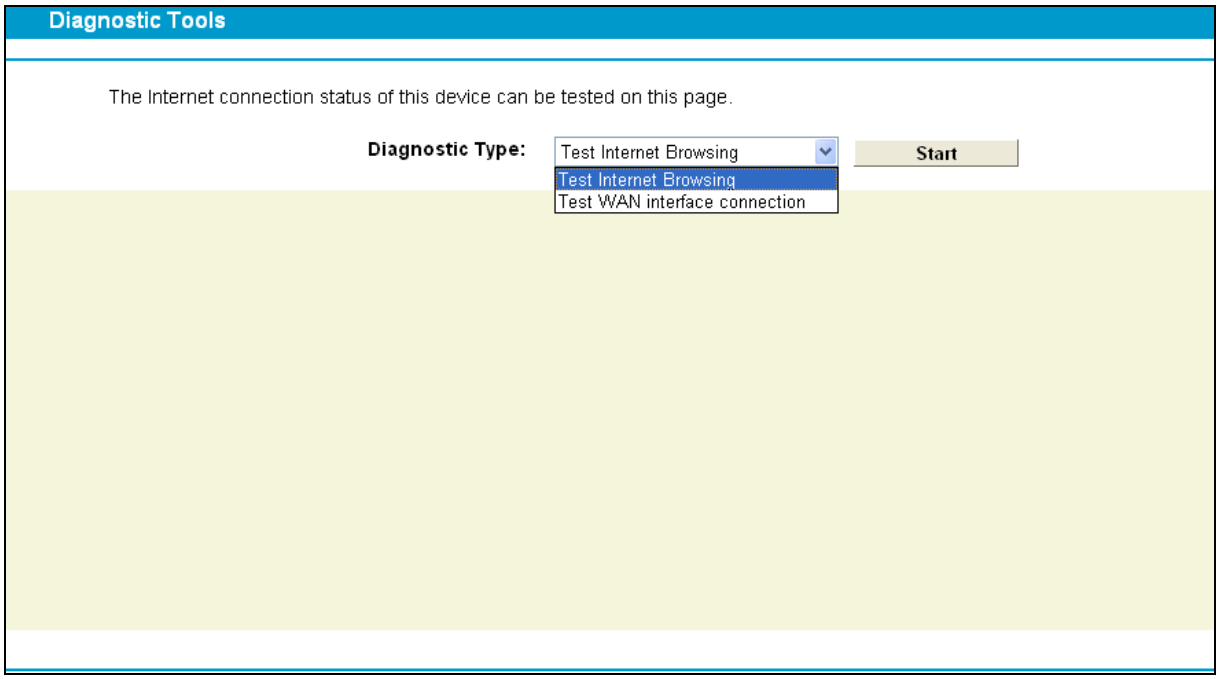


Figure 4-104

4.23 System Tools

Choose menu "**System Tools**", and you can see the submenus under the main menu: **System Log**, **Time Settings**, **Manage Control**, **CWMP Settings**, **SNMP Settings**, **Backup & Restore**, **Factory Defaults**, **Firmware Upgrade**, **Reboot** and **Statistics.** Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.23.1 System Log

Choose menu "**System Tools**" → "**System Log**", and then you can view the logs of the modem router.

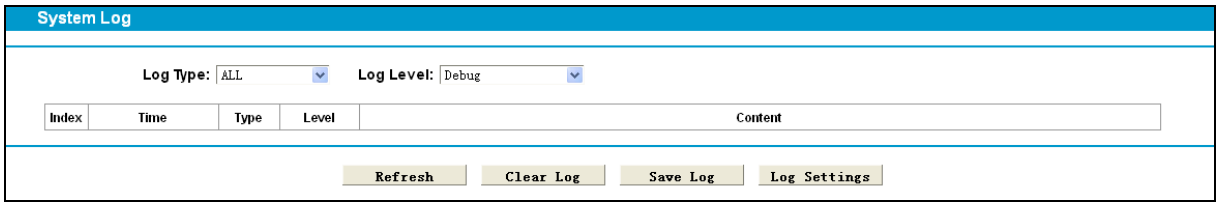


Figure 4-105

- **Log Type:** Select the log type to be displayed.
- **Log Level:** Select the log level to be displayed.
- **Refresh:** Refresh the page to show the latest log list.
- **Clear Log:** All the logs will be deleted from the modem router permanently, not just from the page.
- **Save Log:** Click to save all the logs in a txt file.
- **Log Settings:** Click to set the logs in the screen (shown in Figure 4-106).

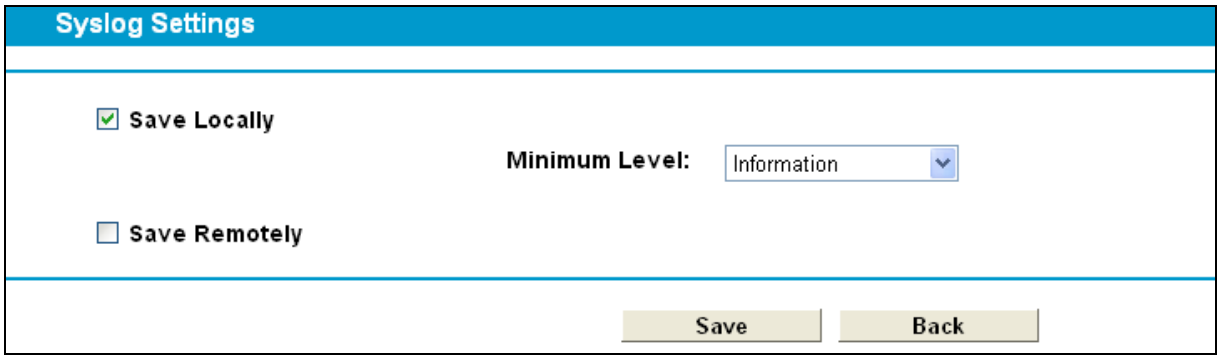


Figure 4-106

- **Save Locally:** If **Save Locally** is selected**,** events will be recorded in the local memory.
- **Minimum Level:** Select the Minimum level in the drop-down list, and then all logged events above or equal to the selected level will be displayed.
- **Save Remotely:** If **Save Remotely** is selected**,** events will be sent to the specified IP address and UDP port of the remote system log server.

Click the **Save** button to save your settings.

4.23.2 Time Settings

Choose menu "**System Tools**" → "**Time Settings**", and then you can configure the time on the following screen.

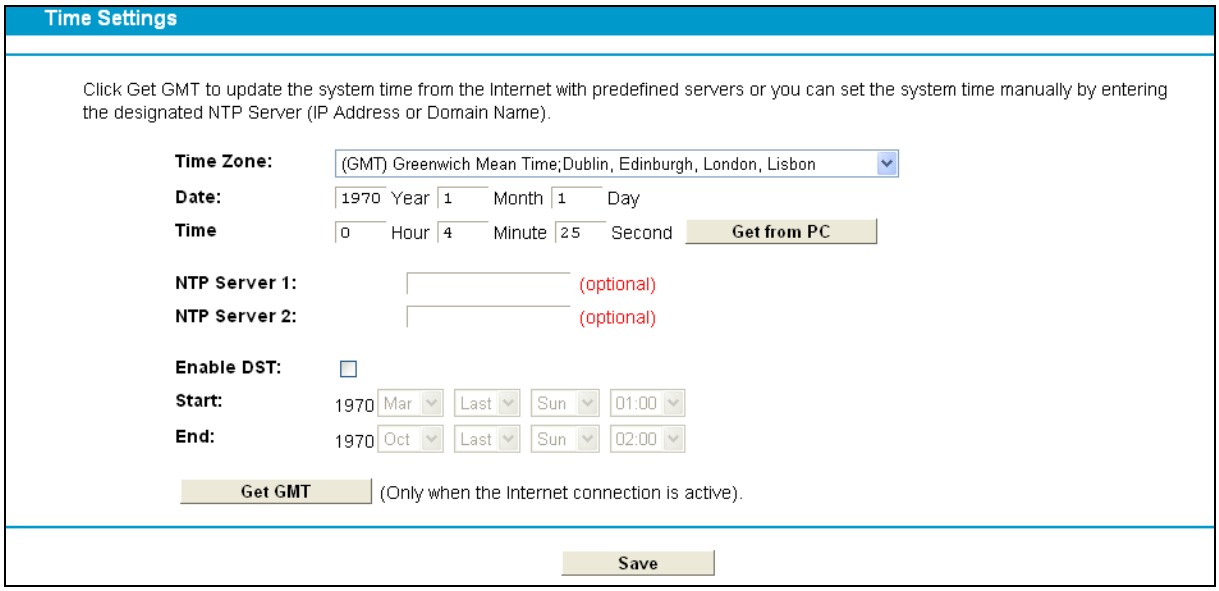


Figure 4-107

- **Time Zone:** Select your local time zone from this drop-down list.
- **Date:** Enter your local date in MM/DD/YY into the right blanks.
- **Time:** Enter your local time in HH/MM/SS into the right blanks.
- **NTP Server 1 / NTP Server 2:** Enter the address or domain of the **NTP Server 1** or **NTP Server 2**, and then the modem router will get the time from the NTP Server preferentially. In addition, the modem router has some common NTP Servers built in, so it can get time automatically once it connects the Internet.
- **Enable DST:** Select the checkbox to enable daylight saving function.
- **Start/End:** Select the correct Start time and End time.

To set time manually:

1. Select your local time zone.
2. Enter the **Date** in Year/Month/Day format.
3. Enter the **Time** in Hour/Minute/Second format.
4. Click **Save**.

To set time automatically:

1. Select your local time zone.
2. Enter the address or domain of the **NTP Server 1** or **NTP Server 2**.
3. Click the **Get GMT** button to get system time from Internet if you have connected to the Internet.

4.23.3 Manage Control

Choose "**System Tools**" → "**Manage Control**", you can see the screen (shown in Figure 4-108)

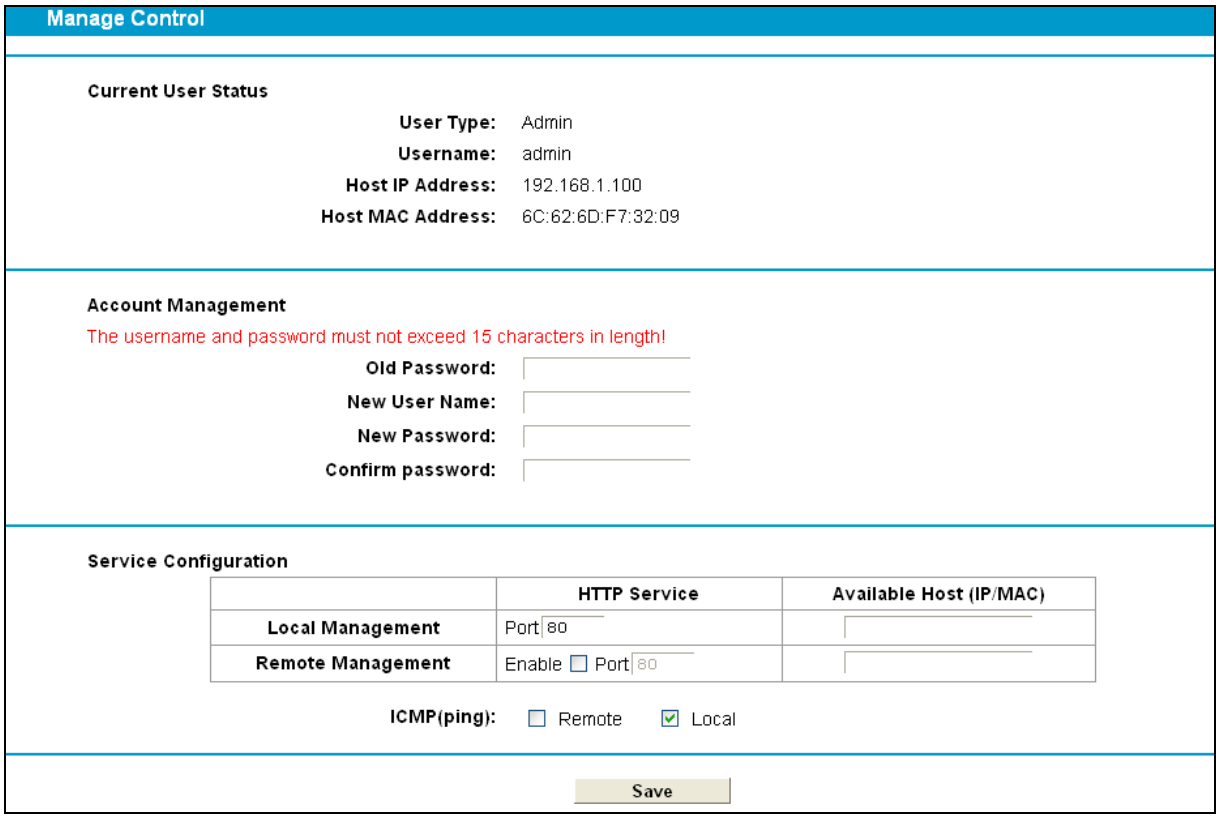


Figure 4-108

- **Current User Status:** This box displays the information about **User Type**, **User Name**, **Host IP Address and Host MAC Address**.
- **Account Management:** Here you can set the account user information about **New User Name** and **New Password**.
- **Service Configuration:** Here you can modify the port of the modem router's web management interface and limit the hosts which can log into this modem router's web management interface.
- **ICMP(ping):** If you select **Remote**, PCs in public network can ping the WAN address of the modem router. If you select **Local**, PCs in private network can ping the LAN address of the modem router.

4.23.4 CWMP Settings

Choose "**System Tools**" → "**CWMP Settings**", 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).

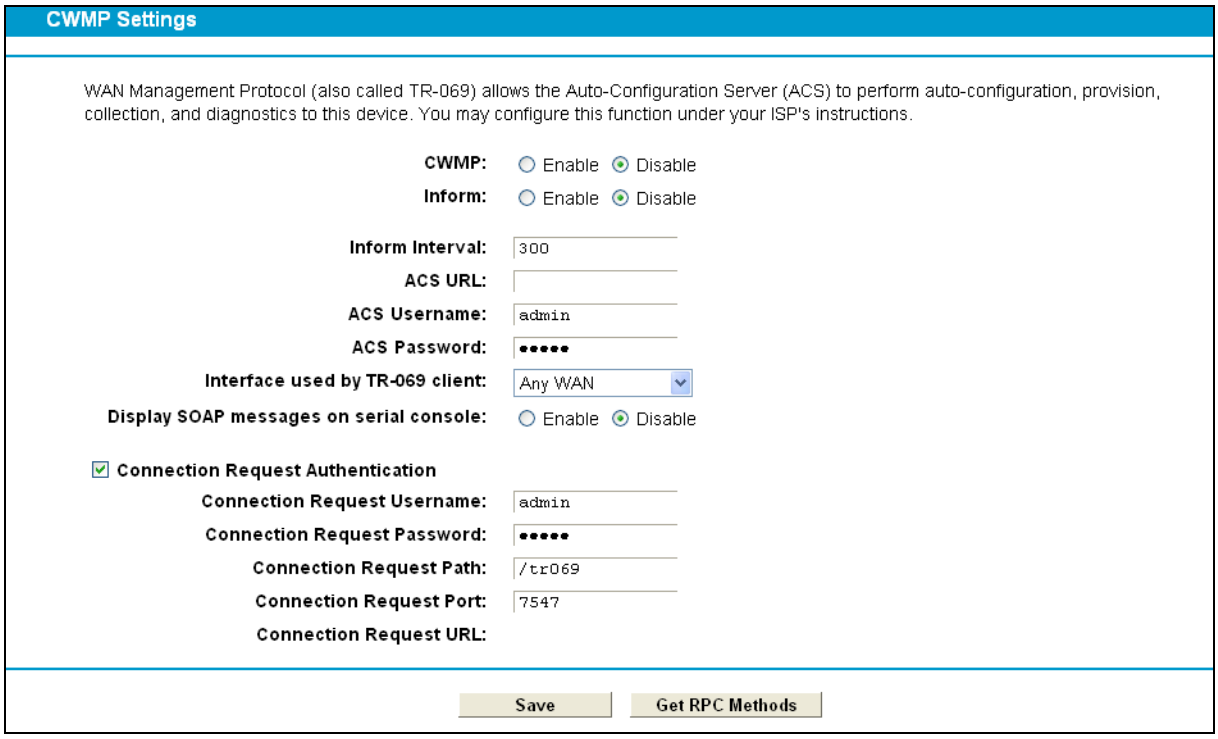


Figure 4-109

- **CWMP:** Select **Enable** to enable the CWMP function.
- **Inform:** If enabled, the information will be informed to ACS server periodically.
- **Inform Interval:** Enter the interval time here.
- **ACS URL:** Enter the website of ACS which is provided by your ISP.
- **ACS User Name/Password:** Enter the User Name and password to log in the ACS server.
- **Interface used by TR-069 client:** Select the interface used by the TR-069 client.
- **Display SOAP messages on serial console:** Enable or disable this function.
- **Connection Request User Name/Password:** Enter the User Name and Password for the ACS server to log in the modem router.
- **Connection Request Path:** Enter the path that connects to the ACS server.
- **Connection Request Port:** Enter the port that connects to the ACS server.
- **Connection Request URL:** Enter the URL that connects to the ACS server.

4.23.5 SNMP Settings

Choose "**System Tools**"→"**SNMP Settings**", you can see the SNMP-Configuration screen as shown below.

SNMP (Simple Network Management Protocol) has been widely applied in the computer networks currently, which is used for ensuring the transmission of the management information between two nodes. In this way, network administrators can easily search and modify the information on any node on the network. Meanwhile, they can locate faults promptly and implement the fault diagnosis, capacity planning and report generating.

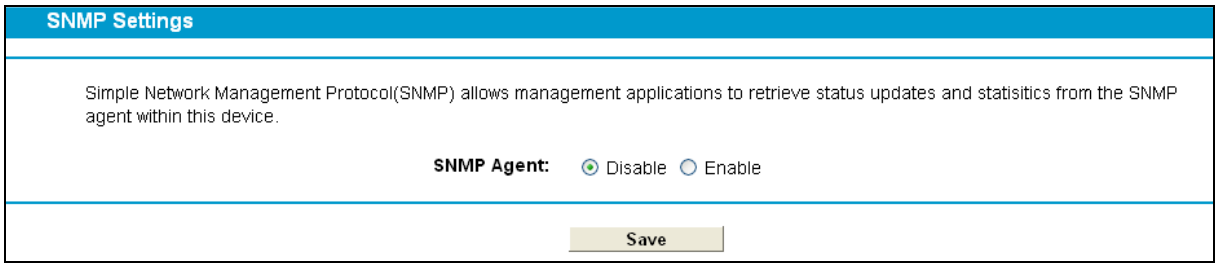


Figure 4-110

An **SNMP Agent** is an application running on the modem router that performs the operational role of receiving and processing SNMP messages, sending responses to the SNMP manager, and sending traps when an event occurs. So a router contains SNMP "agent" software can be monitored and/or controlled by SNMP Manager using SNMP messages.

4.23.6 Backup & Restore

Choose menu "**System Tools**" → "**Backup & Restore**", and then you can save the current configuration of the modem router as a backup file and restore the configuration via a backup file as shown in Figure 4-111.

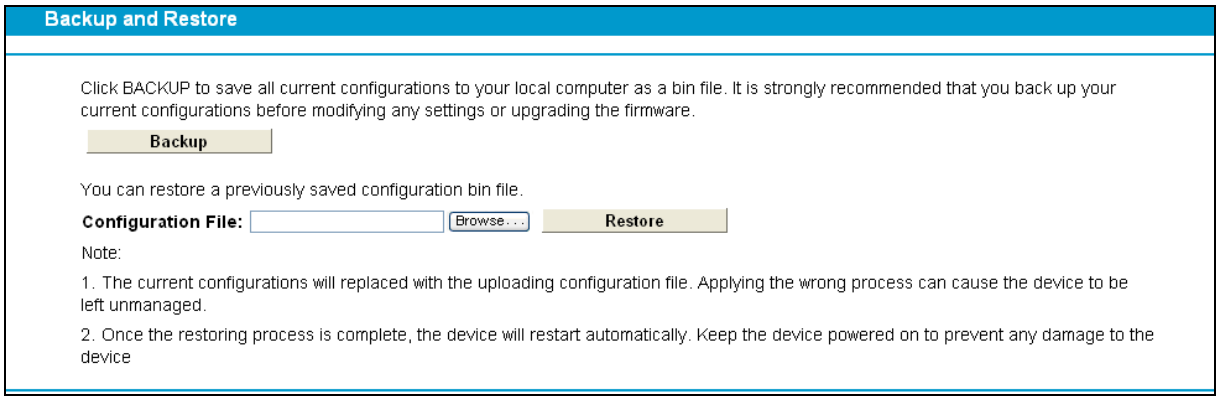


Figure 4-111

Click the **Backup** button to save all configuration settings as a backup file in your local computer.

To upgrade the modem router's configuration, follow these instructions.

1. Click the **Browse** button to find the configuration file which you want to restore.
2. Click the **Restore** button to update the configuration with the file.

Note:

The current configuration will be covered with the uploading configuration file. Wrong process will lead the device to be unmanaged. The restoring process lasts for 20 seconds and then the modem router will restart automatically. Keep the power of the modem router on during the process, in case of any damage.

4.23.7 Factory Defaults

Choose menu "**System Tools** → **Factory Defaults**", and then you can restore the configurations of the modem router to its factory defaults on the following screen

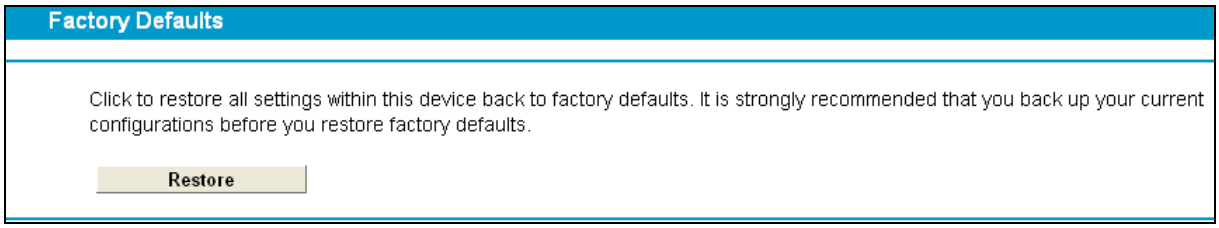


Figure 4-112

Click the **Restore** button to reset all configuration settings to their default values.

- The default **User Name**: admin
- The default **Password**: admin
- The default **Subnet Mask**: 255.255.255.0

Note:

All changed settings will be lost when factory defaults are restored.

4.23.8 Firmware Upgrade

Choose menu "**System Tools → Firmware Upgrade**", and then you can update the latest version of firmware for the modem router on the following screen.

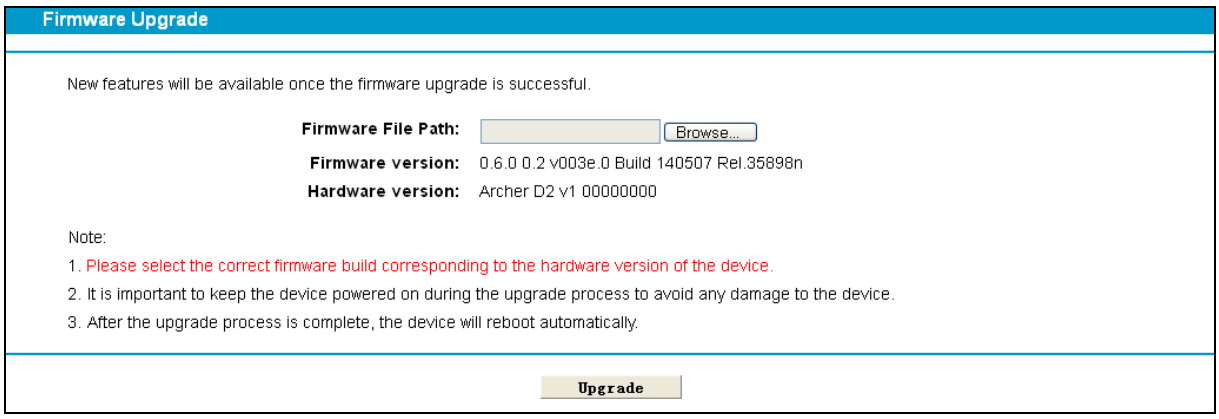


Figure 4-113

- **Firmware Version:** Displays the current firmware version.
- **Hardware Version:** Displays the current hardware version. The hardware version of the upgrade file must accord with the modem router's current hardware version.

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

1) Download a most recent firmware upgrade file from our website: www.tp-link.com.
2) Click the **Browse** button to find the upgrade file on the computer.
3) Click the **Upgrade** button.

Note:

1) New firmware versions are posted at http://www.tp-link.com and can be downloaded for free. There is no need to upgrade the firmware unless the new firmware has a new feature you want to use.

2) When upgrade the modem router's firmware, you may lose its current configurations, so please write down some of your customized settings before upgrading the firmware.

3) Do not turn off the modem router or press the Reset button while the firmware is being upgraded. Loss of power during the upgrade could damage the modem router.

4) The firmware version must correspond to the hardware.

5) The upgrade process takes a few moments and the modem router restarts automatically when the upgrade is complete.

4.23.9 Reboot

Choose menu "**System Tools**" → "**Reboot**", and then you can click the **Reboot** button to reboot the modem router via the next screen.

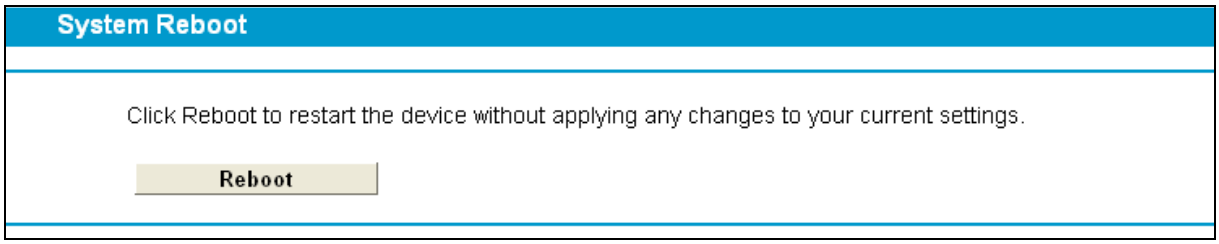


Figure 4-114

Some settings of the modem router will take effect only after rebooting, which include

- Change the LAN IP Address (system will reboot automatically).
- Change the DHCP Settings.
- Change the Wireless configurations.
- Change the Web Management Port.
- Upgrade the firmware of the modem router (system will reboot automatically).
- Restore the modem router's settings to factory defaults (system will reboot automatically).
- Update the configuration with the file (system will reboot automatically).

4.23.10 Statistics

Choose menu "**System Tools**" → "**Statistics**", and then you can view the statistics of the modem router, including total traffic and current traffic of the last Packets Statistic Interval.

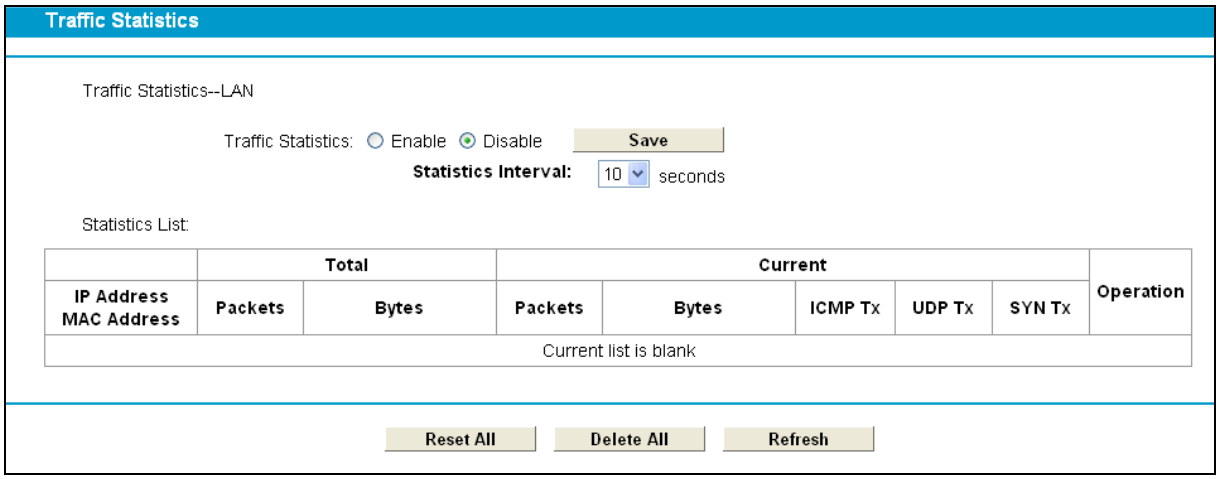


Figure 4-115

- **Traffic Statistics:** If it is disabled, the function of DoS protection in Security settings will be disabled. The default value is disabled. To enable it, click the **Enable**.
- **Statistics Interval (5-60):** Indicates the time section of the packets statistic. The default value is 10. Select a value between 5 and 60 seconds in the drop-down list.

Click **Reset All** to reset the values of all the entries to zero.

Click **Delete All** to delete all entries in the table.

Click the **Refresh** button to refresh immediately.

Statistics Table:

IP/MAC Address		The IP and MAC address are displayed with related statistics.
Total	**Packets**	The total number of packets received and transmitted by the modem router.
	Bytes	The total number of bytes received and transmitted by the modem router.
Current	**Packets**	The total number of packets received and transmitted in the last Packets Statistic interval seconds.
	Bytes	The total number of bytes received and transmitted in the last Packets Statistic interval seconds.
	ICMP Tx	The number of the ICMP packets transmitted to WAN per second at the specified Packets Statistics interval. It is shown like “current transmitting rate / Max transmitting rate”.
	UDP Tx	The number of UDP packets transmitted to the WAN per second at the specified Packets Statistics interval. It is shown like “current transmitting rate / Max transmitting rate”.
	SYN Tx	The number of TCP SYN packets transmitted to the WAN per second at the specified Packets Statistics interval. It is shown like “current transmitting rate / Max transmitting rate”.

Operation	**Reset**	Reset the value of the entry to zero.
	Delete	Delete the existing entry in the table.

4.24 Logout

Choose "**Logout**", and you will back to the login screen as shown in Figure 4-116.

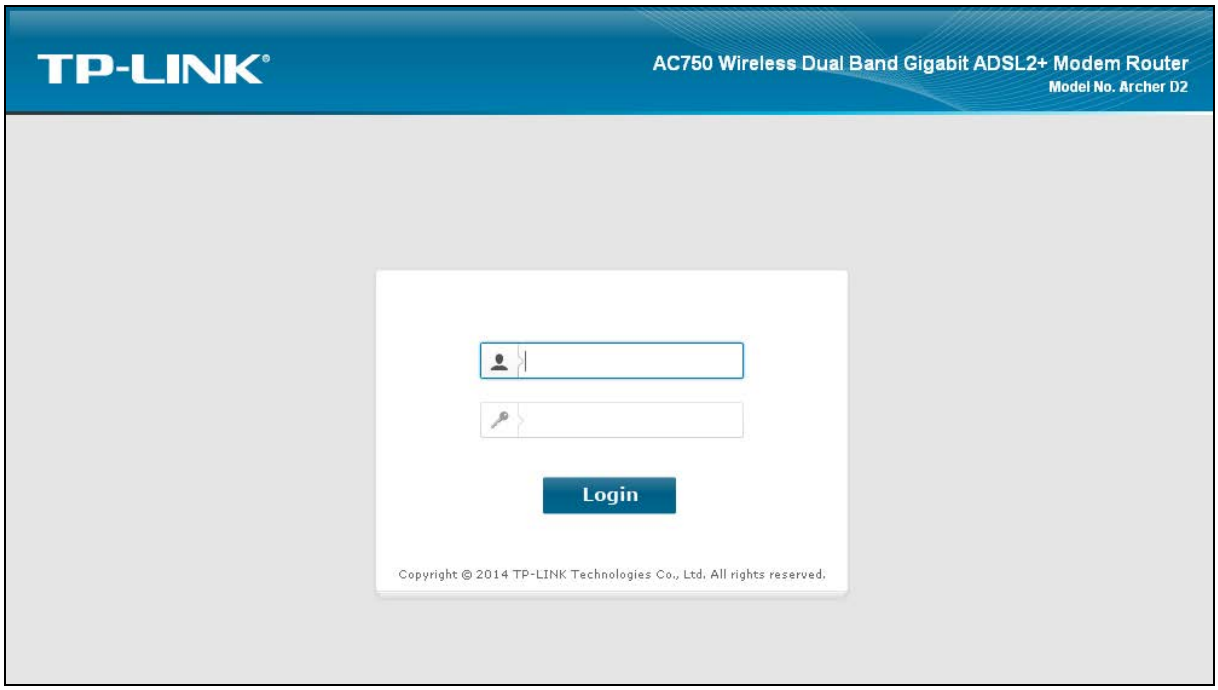


Figure 4-116

Appendix A: Specifications

General	
Standards and Protocols	ANSI T1.413, ITU G.992.1, ITU G.992.3, ITU G.992.5, IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, IEEE 802.3, IEEE 802.3u, IEEE802.3ab, TCP/IP, PPPoA, PPPoE, SNTP, HTTP, DHCP, ICMP, NAT
Safety & Emission	FCC, CE
Ports	Four 10/100/1000M Auto-Negotiation RJ45 ports（Auto MDI/MDIX) One RJ11 port One USB 2.0 port
LEDs	WPS, USB, (LAN), Wireless, Internet, ADSL, Power
Network Medium	10Base-T: UTP category 3, 4, 5 cable 100Base-TX: UTP category-5, 5e cable 1000Base-TX: UTP category-5, 5e cable Max line length: 6.5Km
Data Rates	Downstream: Up to 24Mbps Upstream: Up to 1Mbps
System Requirement	Windows 8/7/Vista/XP or Mac OS or Linux-based operating system Microsoft Internet Explorer, Firefox, Chrome or Safari browser for web-based configuration
Physical and Environment	
Working Temperature	0℃ ~ 40℃
Working Humidity	10% ~ 90% RH (non-condensing)
Storage Temperature	-40℃ ~ 70℃
Storage Humidity	5% ~ 90% RH (non-condensing)

Appendix B: Troubleshooting

T1. How do I restore my modem router's configuration to its factory default settings?

With the modem router powered on, press and hold the **RESET** button on the rear panel for 8 to 10 seconds before releasing it.

☞ **Note**:

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

T2. What can I do if I don't know or forget my password?

1) Restore the modem router's configuration to its factory default settings. If you don't know how to do that, please refer to **T1**.
2) Use the default user name and password: **admin**, **admin**.
3) Try to configure your modem router once again by following the instructions in 3.2 Quick Installation Guide.

T3. What can I do if I cannot access the web-based configuration page?

1) Configure your computer's IP Address.

For Mac OS X

1） Click the **Apple** icon on the upper left corner of the screen.

2） Go to "**System Preferences** -> **Network**".

3） Select **Airport** on the left menu bar, and then click **Advanced** for wireless configuration; or select **Ethernet** for wired configuration.

4） In the **Configure IPv4** box under **TCP/IP**, select **Using DHCP**.

5） Click **Apply** to save the settings.

For Windows 7

1） Click "**Start** -> **Control Panel** -> **Network and Internet** -> **View network status** -> **Change adapter settings**".

2） Right-click **Wireless Network Connection** (or **Local Area Connection**), and then click **Properties**.

3） Select **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.

4） Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Then click **OK**.

For Windows XP

1） Click "**Start** -> **Control Panel** -> **Network and Internet Connections** -> **Network Connections**".

2） Right-click **Wireless Network Connection** (or **Local Area Connection**), and then click **Properties**.

3） Select **Internet Protocol (TCP/IP)**, and then click **Properties**.

4） Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Then click **OK**.

For Windows 8

1） Move your mouse to the lower right corner and you will see **Search** icon in the Popups. Go to " -> **Apps**". Type **Control Panel** in the search box and press **Enter**, then you will go to **Control Panel**.

2） Click "**View network status and tasks** > **Change adapter settings**".

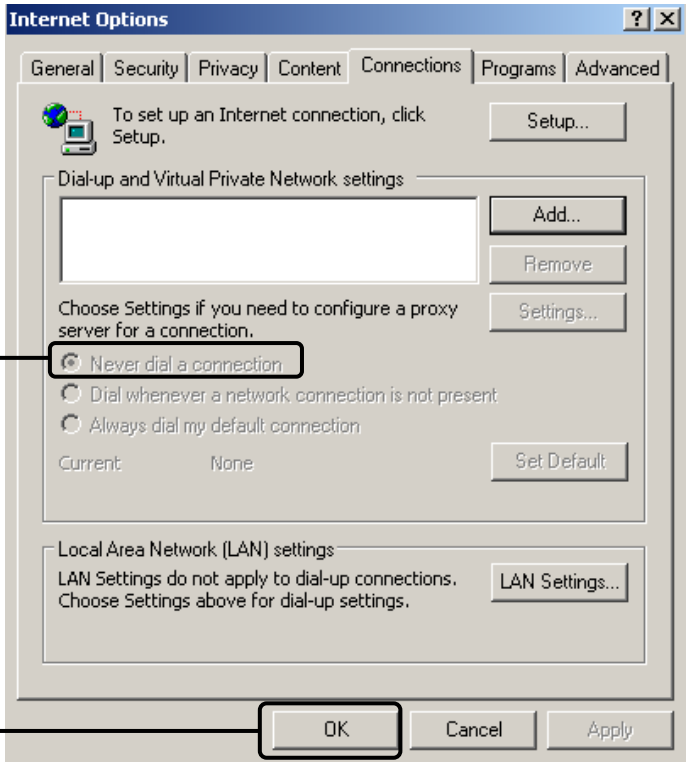
3） Right-click "**Ethernet**" and then select **Properties**.

4） Double-click **Internet Protocol Version 4 (TCP/IPv4)**. Select **Obtain an IP address automatically**, choose **Obtain DNS server address automatically** and then click **OK**.

2) Configure your IE browser

Open your IE browser, click **Tools** tab and you will see the following screen.

Click **Internet Options**



Select **Never dial a connection**

Click **OK**

Now, try to log on to the Web-based configuration page again after the above settings have been configured. If you still cannot access the configuration page, please restore your modem router's factory default settings and reconfigure your modem router following the instructions in 3.2 Quick Installation Guide. Please feel free to contact our Technical Support if the problem still exists.

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** and 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 3.2 Quick Installation Guide.
5) Please contact our Technical Support if the problem still exists.

☞ **Note:**

For more details about Troubleshooting and Technical Support contact information, please log on to our Technical Support Website: **http://www.tp-link.com/en/support**

Appendix C: Technical Support

Technical Support

- For more troubleshooting help, go to:
  http://www.tp-link.com/en/support/faq
- To download the latest Firmware, Driver, Utility and User Guide, go to:
  http://www.tp-link.com/en/support/download
- For all other technical support, please contact us by using the following details:

Global
Tel: +86 755 2650 4400
Fee: Depending on rate of different carriers, IDD.
E-mail: support@tp-link.com
Service time: 24hrs, 7 days a week

USA/Canada
Toll Free: +1 866 225 8139
E-mail: support.usa@tp-link.com (USA)
support.ca@tp-link.com (Canada)
Service time: 24hrs, 7 days a week

Turkey
Tel: 0850 7244 488 (Turkish Service)
Fee: Depending on rate of different carriers.
E-mail: support.tr@tp-link.com
Service time: 09:00 to 21:00, 7 days a week

Ukraine
Tel: 0800 505 508
Fee: Free for Landline; Mobile: Depending on rate of different carriers
E-mail: support.ua@tp-link.com
Service time: Monday to Friday, 10:00 to 22:00

Brazil
Toll Free: 0800 608 9799 (Portuguese Service)
E-mail: suporte.br@tp-link.com
Service time: Monday to Friday, 09:00 to 20:00; Saturday, 09:00 to 15:00

Indonesia
Tel: (+62) 021 6386 1936
Fee: Depending on rate of different carriers.
E-mail: support.id@tp-link.com
Service time: Monday to Friday, 09:00 to 18:00,
*Except public holidays

Australia/New Zealand
Tel: NZ 0800 87 5465 (Toll Free)
AU 1300 87 5465 (Depending on 1300 policy.)
E-mail: support.au@tp-link.com (Australia)
support.nz@tp-link.com (New Zealand)
Service time: 24hrs, 7 days a week

Germany/Austria
Tel: +49 1805 875 465 (German Service)
+49 1805 TPLINK
+43 820 820 360
Fee: Landline from Germany: 0.14EUR/min.
Landline from Austria: 0.20EUR/min.
E-mail: support.de@tp-link.com
Service time: Monday to Friday, 09:00 to 12:30 and 13:30 to 18:00. GMT+1 or GMT+2 (DST in Germany) *Except bank holidays in Hesse

Singapore
Tel: +65 6284 0493
Fee: Depending on rate of different carriers.
E-mail: support.sg@tp-link.com
Service time: 24hrs, 7 days a week

UK
Tel: +44 (0) 845 147 0017
Fee: Landline: 1p-10.5p/min, depending on the time of day. Mobile: 15p-40p/min, depending on your mobile network.
E-mail: support.uk@tp-link.com
Service time: 24hrs, 7 days a week

Italy
Tel: +39 023 051 9020
Fee: Depending on rate of different carriers.
E-mail: support.it@tp-link.com
Service time: Monday to Friday, 09:00 to 13:00; 14:00 to 18:00

Malaysia
Toll Free: 1300 88 875 465
Email: support.my@tp-link.com
Service time: 24hrs, 7 days a week

Poland
Tel: +48 (0) 801 080 618
+48 223 606 363 (if calls from mobile phone)
Fee: Depending on rate of different carriers.
E-mail: support.pl@tp-link.com
Service time: Monday to Friday, 09:00 to 17:00. GMT+1 or GMT+2 (DST)

France
Tel: 0820 800 860 (French service)
Fee: 0.118 EUR/min from France
Email: support.fr@tp-link.com
Service time: Monday to Friday, 09:00 to 18:00 *Except French Bank holidays

Switzerland
Tel: +41 (0) 848 800 998 (German Service)
Fee: 4-8 Rp/min, depending on rate of different time.
E-mail: support.ch@tp-link.com
Service time: Monday to Friday, 09:00 to 12:30 and 13:30 to 18:00. GMT+1 or GMT+2 (DST)

Russian Federation
Tel: 8 (499) 754 5560 (Moscow NO.)
8 (800) 250 5560 (Toll-free within RF)
E-mail: support.ru@tp-link.com
Service time: From 09:00 to 21:00 (Moscow time) *Except weekends and holidays in RF