TP-LINK®

User Guide

TD-W8968

300Mbps Wireless N USB ADSL2+ Modem Router

REV: 5.0.0
1910011586

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 © 2016 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

CE1588

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.

RF Exposure Information

This device meets the EU requirements (1999/5/EC Article 3.1a) on the limitation of exposure of the general public to electromagnetic fields by way of health protection.

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

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

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.
- Adapter shall be installed near the equipment and shall be easily accessible.
- The plug considered as disconnect device of adapter.
- Use only power supplies which are provided by manufacturer and in the original packing of this product. If you have any questions, please don't hesitate to contact us.

Explanation of the symbols on the product label

Symbol	Explanation
	RECYCLING This product bears the selective sorting symbol for Waste electrical and electronic equipment (WEEE). This means that this product must be handled pursuant to European directive 2012/19/EU in order to be recycled or dismantled to minimize its impact on the environment. User has the choice to give his product to a competent recycling organization or to the retailer when he buys a new electrical or electronic equipment.
	DC voltage

TP-LINK® TP-LINK TECHNOLOGIES CO., LTD

DECLARATION OF CONFORMITY

For the following equipment:

Product Description: 300Mbps Wireless N USB ADSL2+ Modem Router

Model No.: TD-W8968

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, Directive 2009 /125 /EC

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

EN 300328 V1.9.1

EN 301489-1 V1.9.2& EN 301489-17 V2.2.1

EN 55022: 2010+AC: 2011

EN 61000-3-2: 2014

EN 61000-3-3: 2013

EN 55024: 2010

EN 60950-1: 2006 + A11: 2009 + A1: 2010 + A12: 2011 +A2: 2013

EN 50385: 2002

EN 50581: 2012

(EC) No 278/2009

(EC) No 1275/2008

(EU) No 801/2013

The product carries the CE Mark:

CE1588

Person responsible for making this declaration:

Yang Hongliang

Product Manager of International Business

Date of issue: 2016-02-26

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 5

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

2.1 System Requirements 7

2.2 Installation Environment Requirements 7

2.3 Connecting the Modem Router 8

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 Device Info 14

4.3 Quick Setup 15

4.4 Operation Mode 15

4.5 Advanced Setup 16

4.5.1 Layer2 Interface 17

4.5.2 WAN Service 19

4.5.3 3G Settings 28

4.5.4 MAC Clone 31

4.5.5 LAN 31

4.5.6 NAT 35

4.5.7 Security 40

4.5.8 Parental Control 44

4.5.9 Quality of Service 46

4.5.10 Bandwidth Control 49

4.5.11 Routing 51

4.5.12 DNS 53
4.5.13 DSL 55
4.5.14 UPnP 56
4.5.15 Interface Grouping 56
4.5.16 IP Tunnel 58
4.5.17 IPSec 60
4.5.18 Multicast 63
4.6 IPTV 63
4.7 Wireless 64
4.7.1 Basic 64
4.7.2 Security 65
4.7.3 Wireless Schedule 78
4.7.4 MAC Filter 79
4.7.5 Wireless Bridge 81
4.7.6 Advanced 82
4.7.7 Station info 83
4.8 Guest Network 84
4.8.1 Basic 84
4.8.2 Station list 85
4.9 USB Settings 85
4.9.1 USB Mass Storage 86
4.9.2 User Accounts 86
4.9.3 Storage Sharing 87
4.9.4 FTP Server 89
4.9.5 Media Server 90
4.9.6 Print Server 91
4.10 Diagnostics 92
4.11 Management 92
4.11.1 Settings 93
4.11.2 System Log 95
4.11.3 SNMP Agent 96
4.11.4 TR-069 client 97
4.11.5 Internet Time 99
4.11.6 Access Control 99
4.11.7 Upgrade Firmware 101
4.11.8 Reboot 102

4.12Logout 102

Appendix A: Specifications 104

Appendix B: Troubleshooting 105

Package Contents

The following contents should be found in your package:

- One TD-W8968 300Mbps Wireless N USB ADSL2+ Modem Router
- One power Adapter for TD-W8968 300Mbps Wireless N USB ADSL2+ Modem Router
- Quick Installation Guide
- One RJ45 cable
- Two RJ11 cables
- One ADSL splitter

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 **TD-W8968 300Mbps Wireless** N USB ADSL2+ Modem Router.

1.1 Overview of the Modem Router

The TD-W8968 300Mbps Wireless N USB ADSL2+ Modem Router integrates 4-port Switch, Firewall, NAT-router and Wireless AP. Powered by 2x2 MIMO technology, the Wireless N 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 TD-W8968 300Mbps Wireless N USB ADSL2+ Modem Router utilizes integrated ADSL2+ transceiver and high speed MIPS CPU. The modem 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 wireless connection with other 802.11n 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 802.11n wireless modem router will give you the unexpected networking experience at speed 650% faster than 802.11g. It is also compatible with all IEEE 802.11g and IEEE 802.11b 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 TD-W8968 300Mbps Wireless N USB 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 staff. 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

- One RJ11 LINE port, four 10/100M Auto-Negotiation RJ45 LAN ports, supporting Auto MDI/MDIX
- Complies with IEEE 802.11n to provide a wireless data rate of up to 300Mbps
- Quick response semi-conductive surge protect circuit, reliable surge-protect function
- AFE to support Annex A and L deployments
- Provides external splitter
- Multi-user sharing a high-speed Internet connection
- Connecting the internet on demand and disconnecting from the Internet when idle for PPPoE
- Provides WPA/WPA2, WPA-PSK/WPA2-PSK data security, TKIP/AES encryption security
- Provides 64/128-bit WEP encryption security and wireless LAN ACL (Access Control List)
- Adopts Advanced DMT modulation and demodulation technology
- Supports access control, parents and network administrators can establish restricted access policies based on time of day for children or staff
- Supports Virtual Server, Port Triggering and DMZ host
- Supports UPnP, Dynamic DNS, Static Routing
- Supports bridge mode and router function
- Supports Web management
- Supports firmware upgrade
- Supports Flow Statistics
- Built-in firewall supporting IP address filtering, MAC address filtering and parental control
- Built-in DHCP server
- Supports USB Storage Sharing, Print Server, FTP Server, Media Server
- Supports IPv6
- Supports Guest Network
- Supports WPS

1.3 Panel Layout

1.3.1 The Front Panel

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

Figure 1-1

LED Explanation:

Name	Status	Indication
(Power)	On	The modem router is powered on.
	Off	The modem router is off. Please ensure that the power adapter is connected correctly.
(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.
(Internet)	On	The network is available with a successful Internet connection.
	Flash	There is data being transmitted or received via the Internet.
	Off	There is no successful Internet connection or the modem router is operating in Bridge mode. Please refer to **Note 2** for troubleshooting.
(WLAN)	On	Wireless is enabled but no data is being transmitted.
	Flash	The modem router is sending or receiving data over the wireless network.
	Off	Wireless is disabled.
(**WPS**)	On	A wireless device has been successfully added to the network by **WPS** function.
	Slow 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.
	Quick Flash	A wireless device has failed to be added to the network by WPS function. Please refer to 4.7.2.1 WPS Setup for more information.
(USB)	On	A storage device or printer has connected to the USB port.

	Flash	The modem router is sending or receiving data over this USB port.
	Off	No storage device or printer is plugged into the USB port.
(LAN1-4)	On	There is a device connected to this LAN port.
	Flash	The modem router is sending or receiving data over this LAN port.
	Off	There is no device connected to this LAN port.

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 if your Internet service is available now.
2. If the Internet LED is off, please check your ADSL LED first. If your ADSL LED is also off, please refer to **Note 1**. If your ADSL LED is GREEN 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. Refer to **4.2 Device Info** for more information.

1.3.2 The Back Panel

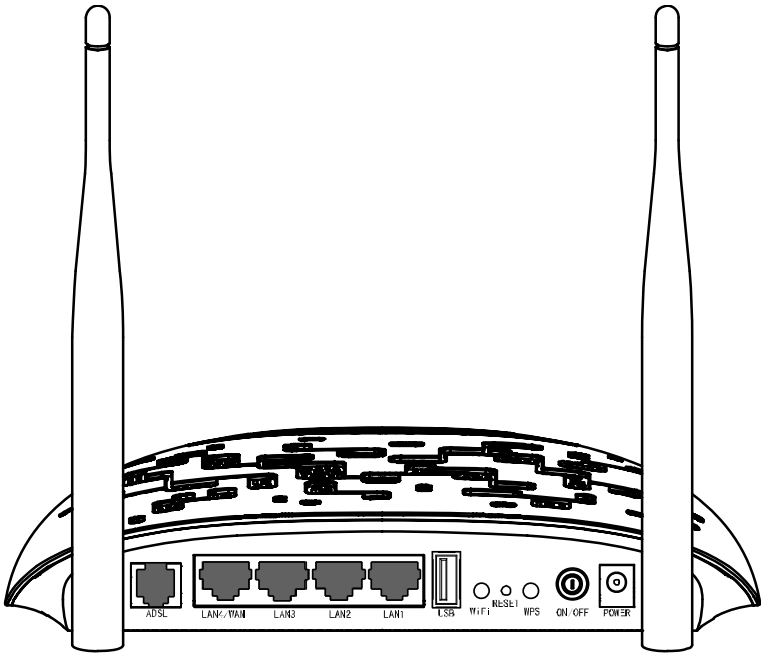


Figure 1-2

- **ADSL:** Connect to the Modem Port of Splitter or to the telephone line.
- **LAN4/WAN, LAN3, LAN2, LAN1:** Through these ports, you can connect the modem router to your PC or the other Ethernet network devices. Enable EWAN function and you will be able to connect to Cable/FTTH/VDSL/ADSL device.
- **USB**: The USB port connects to a USB storage device or a USB printer.
- **WiFi:** The switch for the WiFi function.

- **RESET:** There are two ways to reset the modem router's factory defaults.

1) Use the **Restore Default** function on **Management** -> **settings** -> **Restore Default** page in the modem router's Web-based Utility.

2) Use the Factory Default **RESET** button: With the modem router powered on, use a pin to press and hold the **RESET** button for at least 5 seconds. And the modem router will reboot to its factory default settings.

- **WPS:** The switch for the WPS function. For details, please refer to 4.7.2.1 WPS Setup.
- **ON/OFF:** The switch for the power.
- **POWER:** The Power plug is where you will connect the power adapter.
- **Wireless Antennas:** To receive and transmit the wireless data.

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 or 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.

Generally, **TD-W8968** is placed on a horizontal surface. The device also can be mounted on the wall as shown in Figure 2-1.

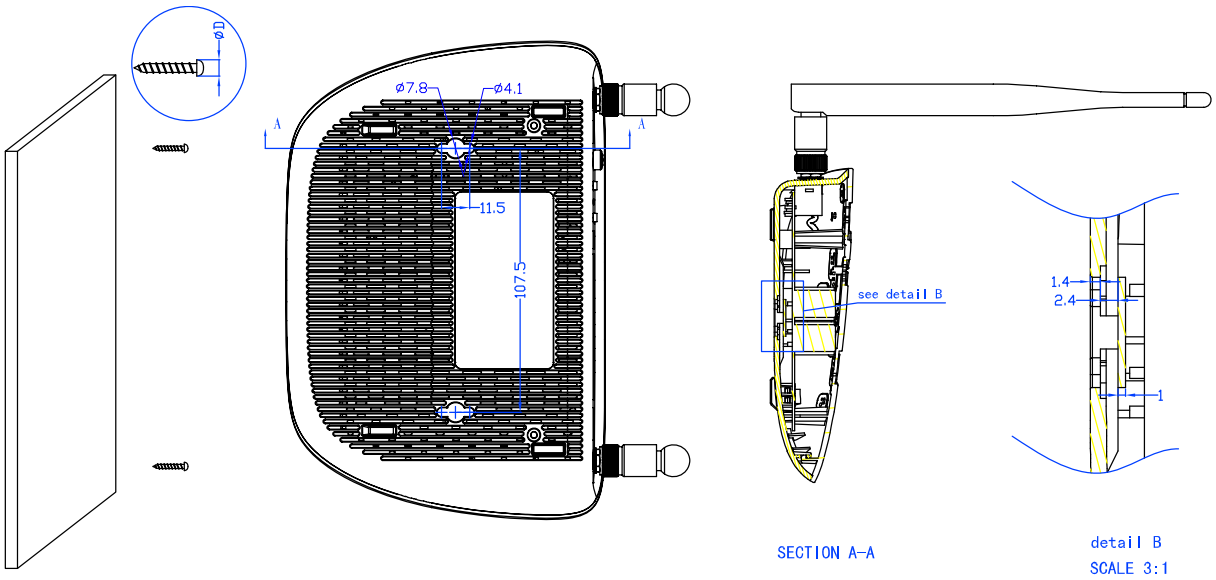


Figure 2-1 Wall-mount Install

Note:

The diameter of the screw, 4.1mm<D<7.8mm, and the distance of two screws is 107.5mm. The screw that project from the wall need around 4mm based, and the length of the screw need to be at least 20mm to withstand the weight of the product.

2.3 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 **TD-W8968**, 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 **TD-W8968**

Plug one end of the twisted-pair ADSL cable into the ADSL port on the rear panel of **TD-W8968**. 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 **TD-W8968**.

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.

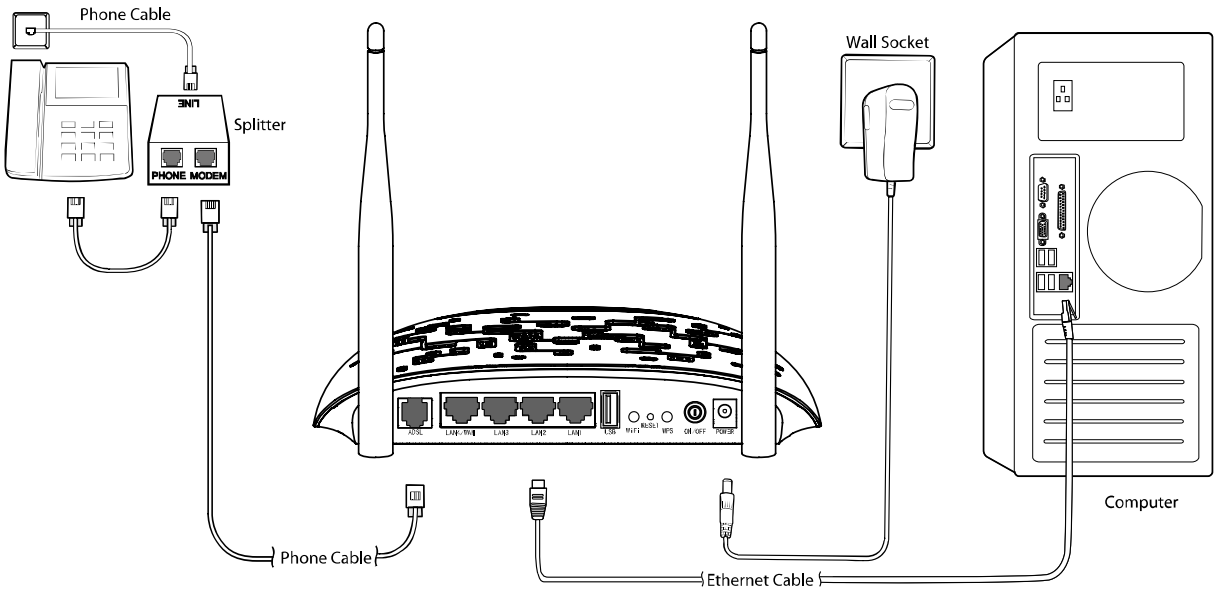


Figure 2-2

Chapter 3. Quick Installation Guide

This chapter will show you how to configure the basic functions of your TD-W8968 300Mbps Wireless N USB ADSL2+ Modem Router using Quick Setup Wizard within minutes.

3.1 TCP/IP Configuration

The default IP address of the TD-W8968 300Mbps Wireless N USB 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 the IP address for your PC in the following way.

- Obtain an IP address automatically

  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 modem router has been established.

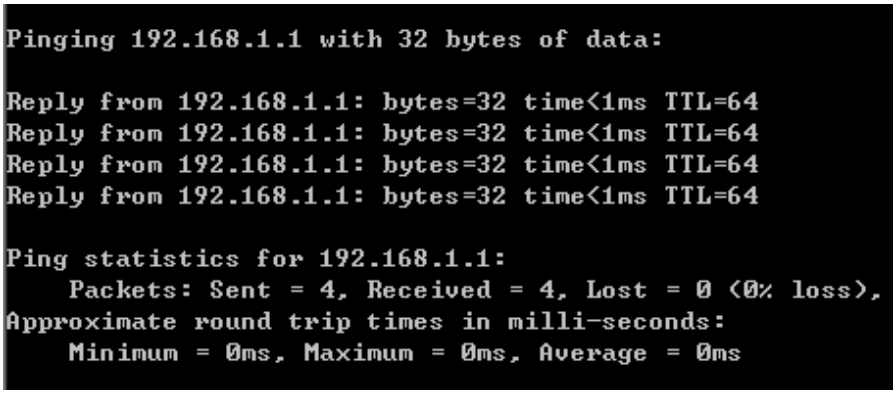


Figure 3-1

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

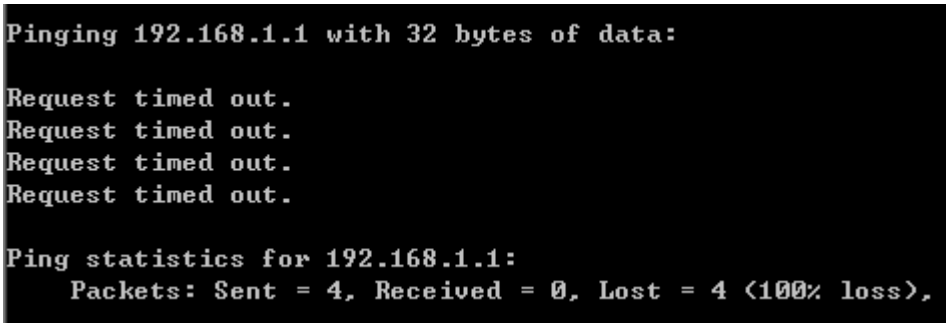


Figure 3-2

You can check it following the steps below:

1) **Is the connection between your PC and the modem 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 modem 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 TD-W8968 300Mbps Wireless N USB 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 3-3

After a moment, a login window will appear, similar to the Figure 3-4. Enter **admin** for the user name and password, both in lower case letters. Then click the **Login** button or press the **Enter** key.

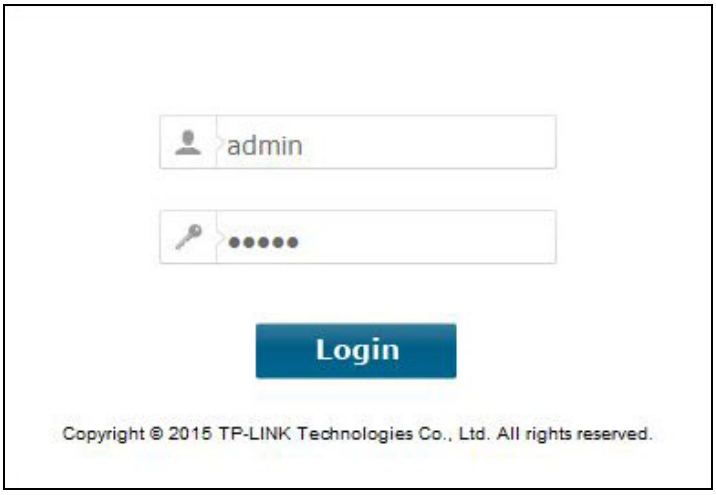


Figure 3-4

☞ **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 **Quick Setup Wizard**. Click **Next** to continue.

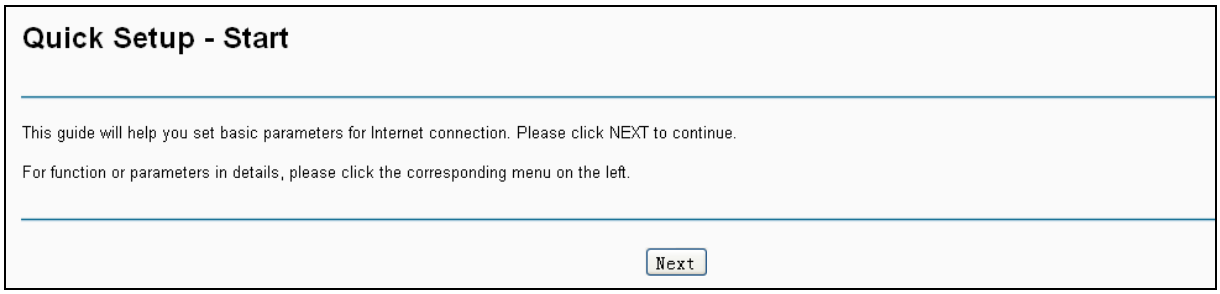


Figure 3-5

Step 3. Choose the **Operation Mode** for Internet access, and then click **Next**. For **ADSL Modem Router Mode** and **Wireless Router Mode**, **3G Router Mode** can be set as a backup internet access method. If you do not want to configure 3G settings now, just untick the option.

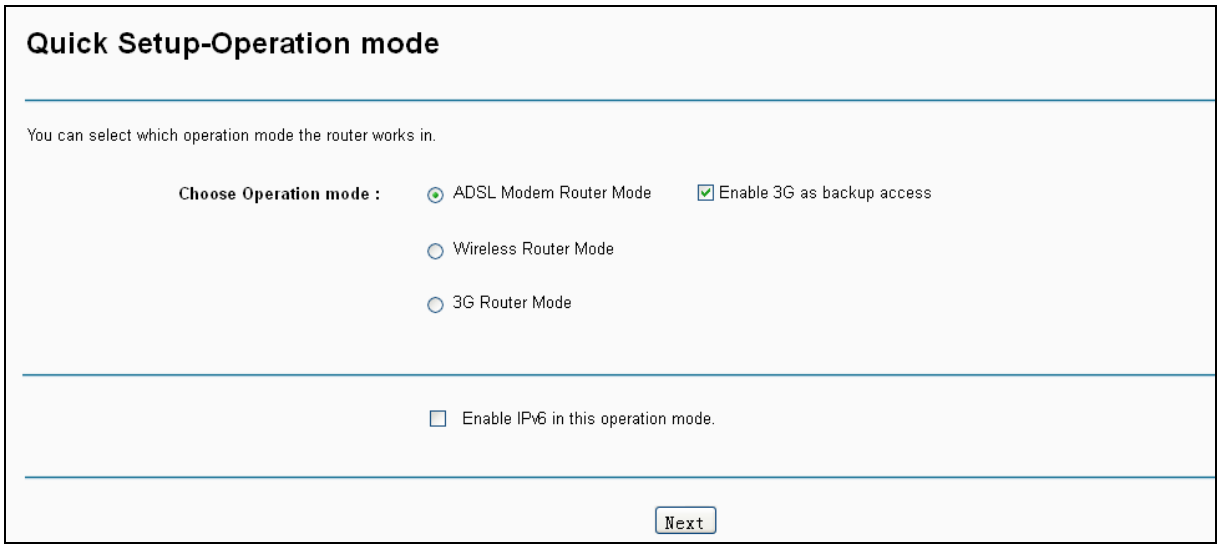


Figure 3-6

- **ADSL Modem Router Mode:** In this mode, the device enables multi-users to share Internet via ADSL using its ADSL port and share it wirelessly at 300Mbps wireless 802.11n speeds.
- **Wireless Router Mode:** In this mode, the device enables multi-users to share Internet via Ethernet WAN (EWAN) using its interchangeable LAN/WAN port and share it wirelessly at 300Mbps wireless 802.11n speeds.
- **3G Router Mode:** In this mode, the device allows multi-users to share a 3G mobile broadband connection via wired or wireless connection.

Note:

If you are unwilling to configure WAN Service now, you can click the **Skip WAN** button. Then you can configure WAN service referring to 4.5.1 Layer2 Interface.

Step 4. Configure parameters for WAN connection.

- If **ADSL Modem Router Mode** is chosen, please select your **Country** and **ISP** from the drop-down list, and enter related parameters provided by your ISP. Then click **Next**. Here we use **PPPoE** as an example.

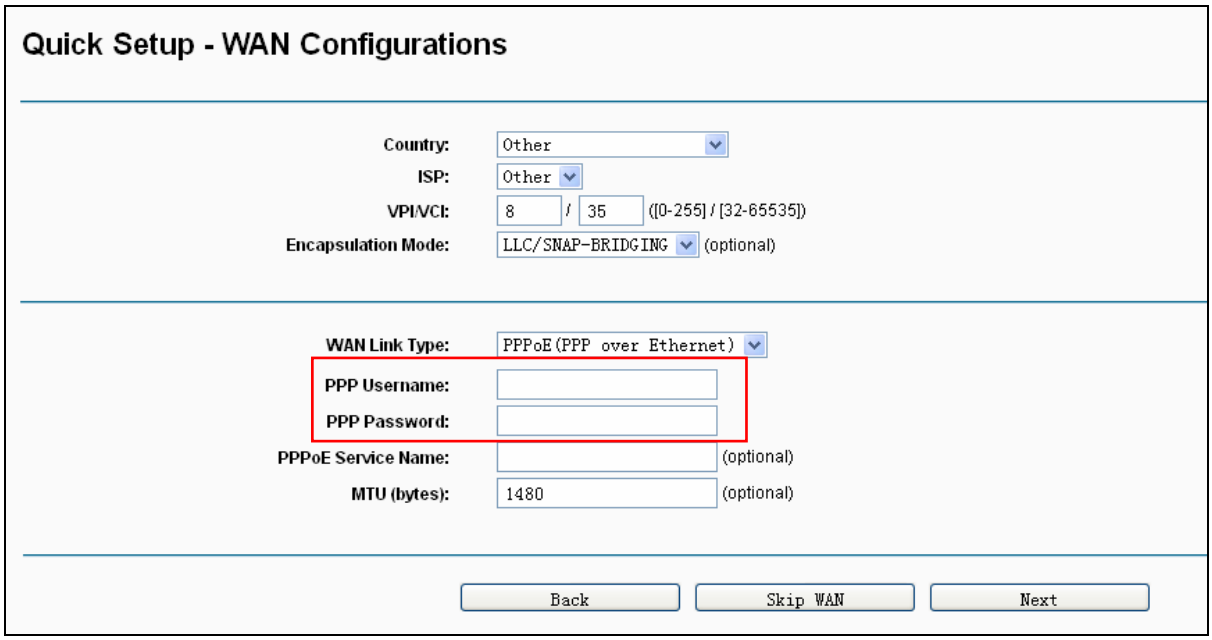


Figure 3-7

Note:

If your country or ISP is not listed, please select **Other**. Then you can manually enter the VPI/VCI values and select **Encapsulation Mode** provided by your ISP.

- If **Wireless Router Mode** is chosen, please select **WAN Link Type** provided by your ISP and enter the related parameters, then click **Next**. Here we use **PPPoE** as an example.

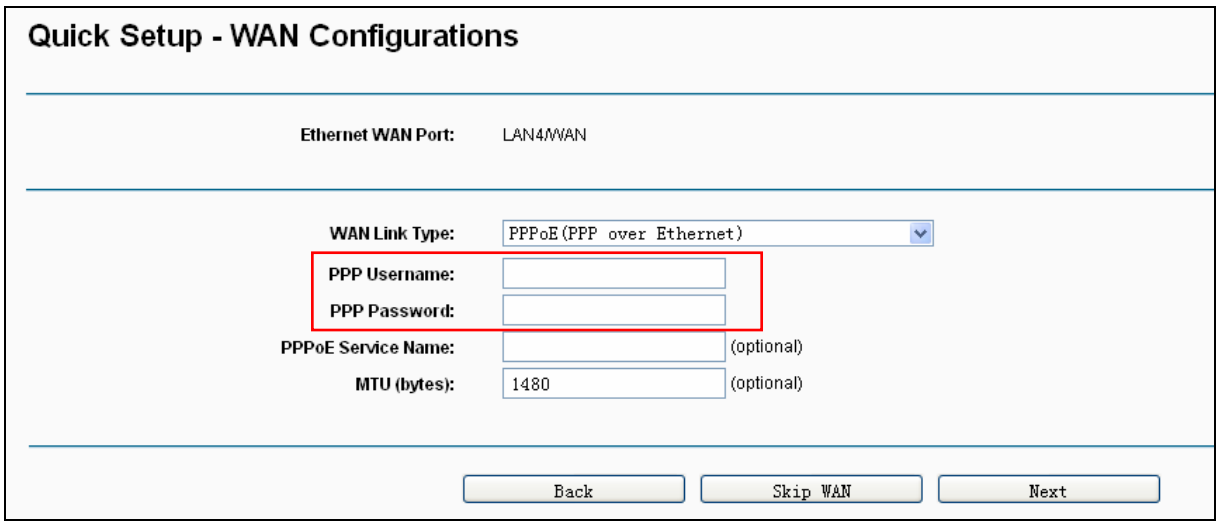


Figure 3-8

- If **3G Router Mode** is chosen, you should first insert your 3G USB modem on the USB port of the modem router. Then select your location and mobile ISP. Click **Save** to continue.

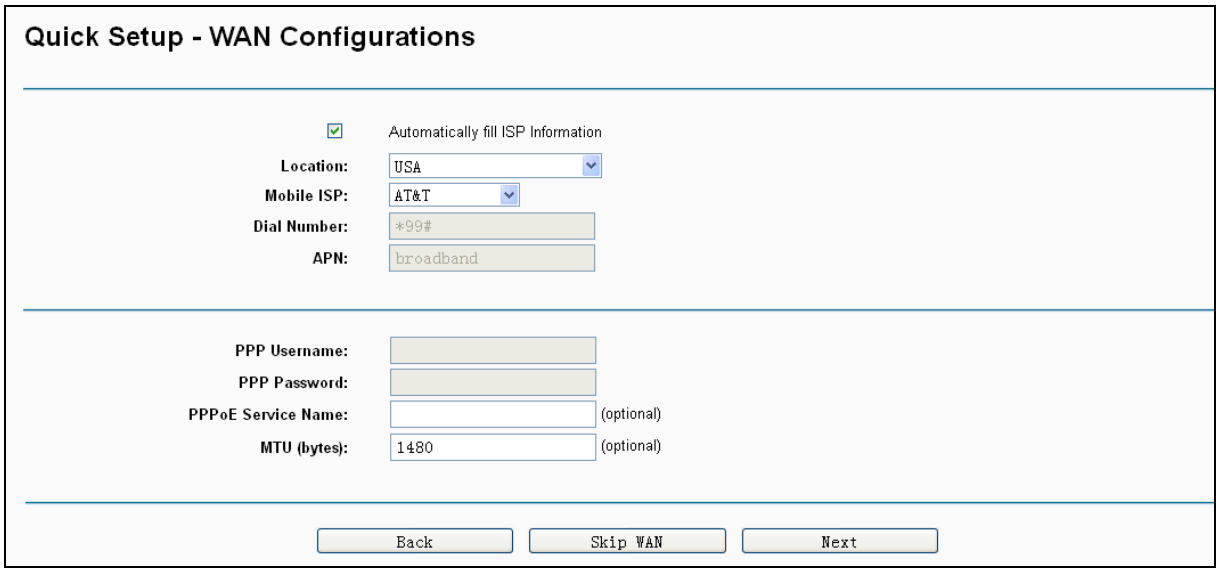


Figure 3-9

Step 5. The WLAN function is enabled by default. You can rename your wireless network name and create your own password in this page. The default wireless name is TP-LINK_XXXX, and the default wireless password, the same as the PIN code, is printed on the bottom label. Click **Next** to continue.

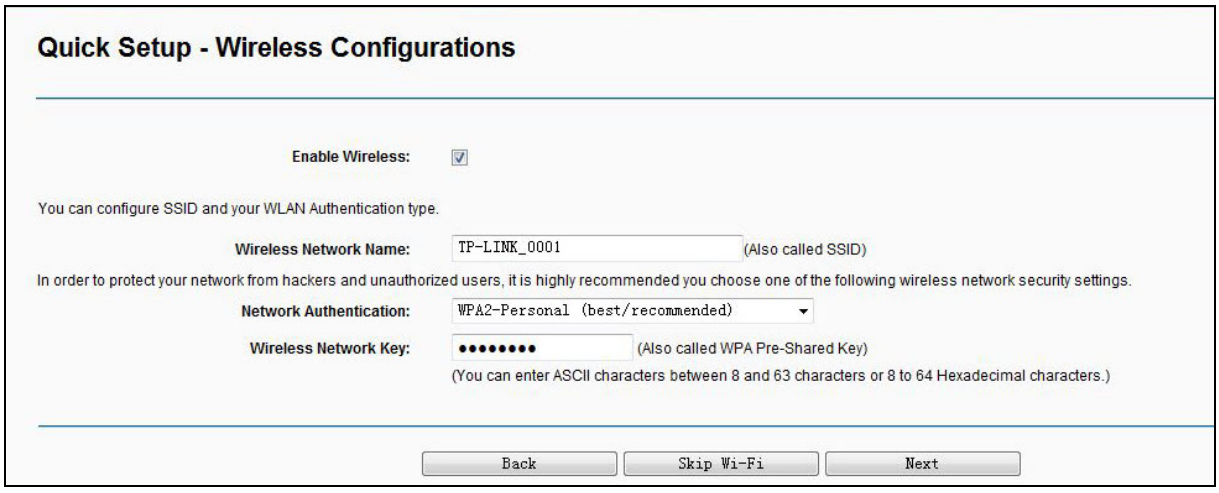


Figure 3-10

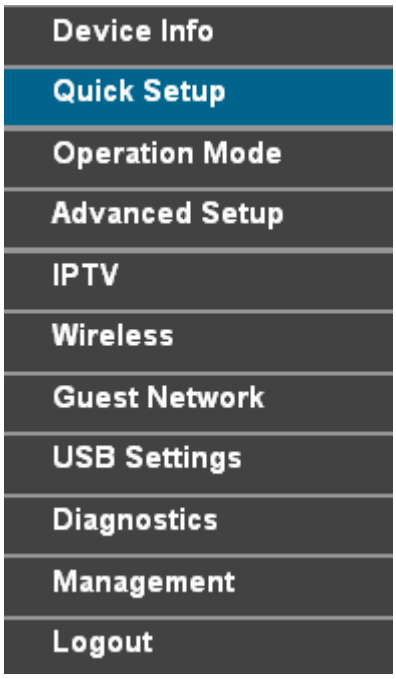
Step 6. You will see the **Summary** screen, click **Confirm** to make your settings take effect.

Chapter 4. Configuring the Modem Router

This chapter will show each Web page's key function and the configuration way.

4.1 Login

After your successful login, you will see the eleven 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 Device Info

Choose "**Device Info**" menu, there are six submenus under the main menu: **Summary**, **WAN**, **Statistics**, **Route**, **ARP** and **DHCP**. This Device Info section mainly introduces the elementary information about the modem router and its current settings in use. Click any of them, and you will be able to view the corresponding information.

Choose "**Device Info**"→"**Summary**", you will see the Summary screen (shown in Figure 4-1). The first table indicates the information about the version including Software and Hardware. The second table displays the current status of the Internet connection. This information will vary depending on the settings of the modem router configured on the Advanced Setup screen.

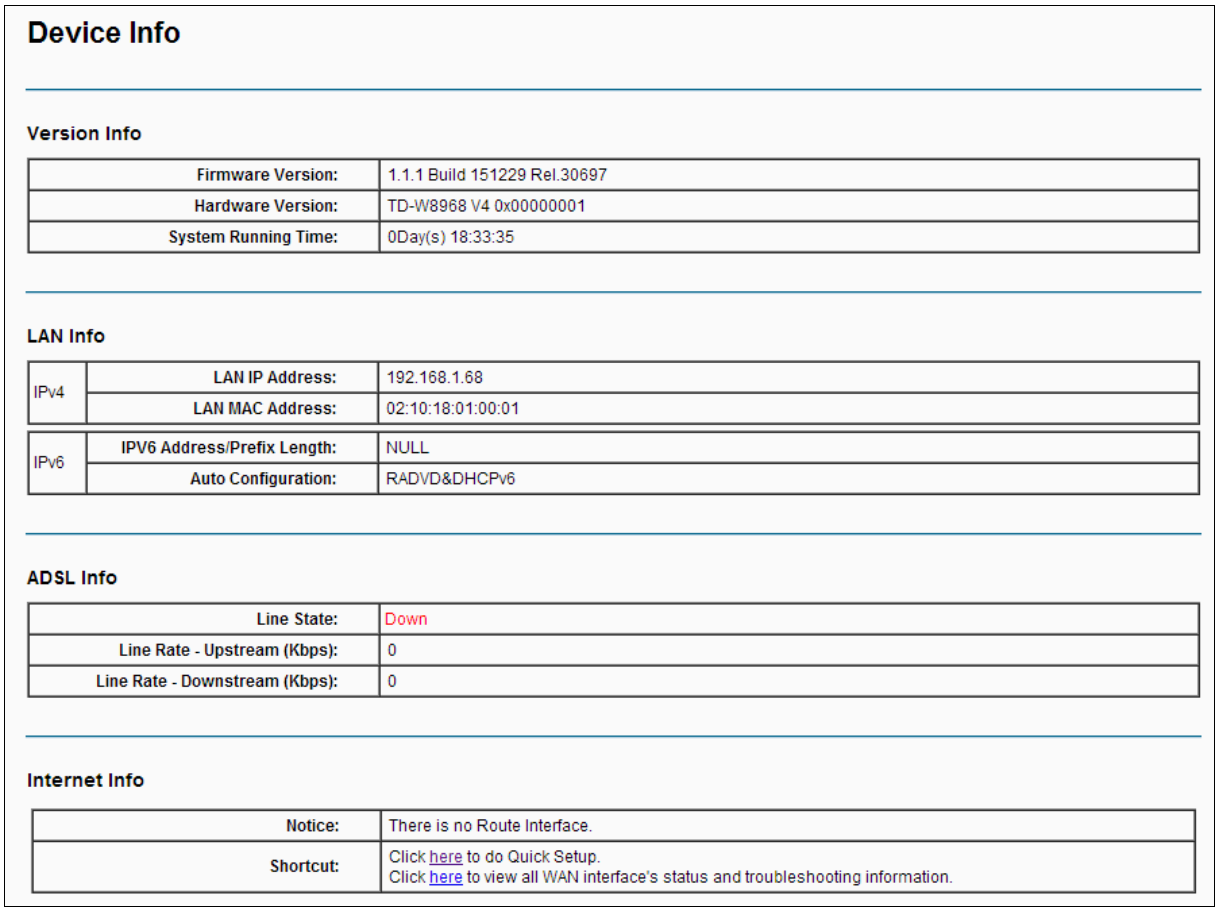


Figure 4-1

Note:

Click the other submenus under the main menu **Device Info**, and you will be able to view the corresponding information about **WAN**, **Statistics**, **Route**, **ARP** and **DHCP**.

4.3 Quick Setup

Please refer to Section 3.2 Quick Installation Guide.

4.4 Operation Mode

Choose "**Operation Mode**", and you will see the screen as shown in Figure 4-2. The modem router supports three operation mode types: **ADSL Modem Router Mode**, **Wireless Router Mode** and **3G Router Mode**. Select your desired mode and then click **Save/Apply**. Then the modem router will reboot. Please wait.

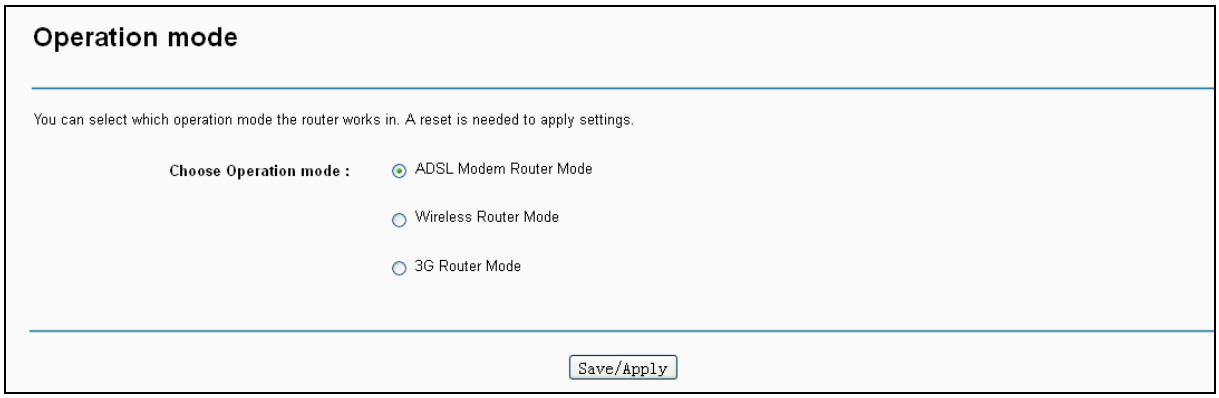


Figure 4-2

- **ADSL Modem Router Mode:** In this mode, the device enables multi-users to share Internet via ADSL using its ADSL port and share it wirelessly at 300Mbps wireless 802.11n speeds.
- **Wireless Router Mode:** In this mode, the device enables multi-users to share Internet via Ethernet WAN (EWAN) using its interchangeable LAN/WAN port and share it wirelessly at 300Mbps wireless 802.11n speeds.
- **3G Router Mode:** In this mode, the device allows multi-users to share a 3G mobile broadband connection via wired or wireless connection.

4.5 Advanced Setup

In **ADSL Modem Router Mode**, choose "**Advanced Setup**", there are many submenus under the main menu. Click any one of them, and you will be able to configure the corresponding function.

This Advanced Setup section mainly introduces how to configure the modem router for adequate use. The detailed explanations for each subsection are provided below.

☞ **Note:**

To completely configure the WAN Interface, you need to first select the Layer2 Interface (4.5.1 Layer2 Interface) according to the connection ISP provides for you, and then to select the type of the connection (4.5.2 WAN Service) for the further configuration.

4.5.1 Layer2 Interface

4.5.1.1 ATM Interface

Choose "**Advanced Setup**"→"**Layer2 Interface**"→"**ATM Interface**", you can Configure ATM interfaces on the screen below.

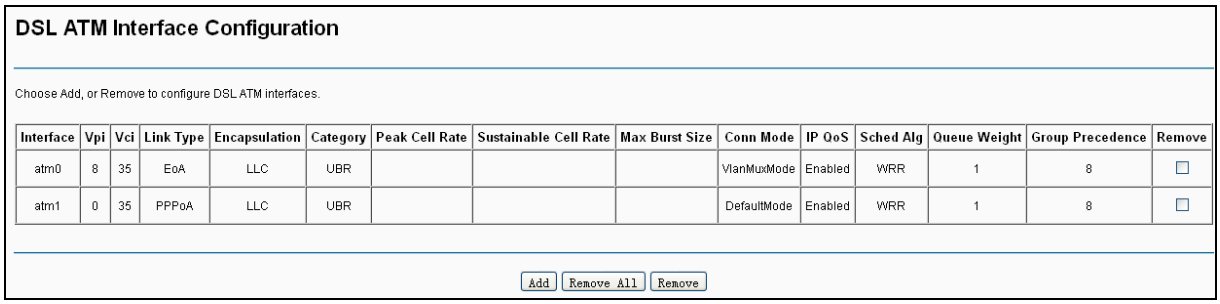


Figure 4-3

- **Remove**: Select the check box in the table on the screen above and then click the **Remove** button, the corresponding interface will be deleted in the table.

Note:

If the interface is used by the configuration of the 4.5.2 WAN Service, you need to remove the corresponding WAN Service entry first before you can remove it here.

- **Add**: Click the button, and you can add a new interface in the next screen.

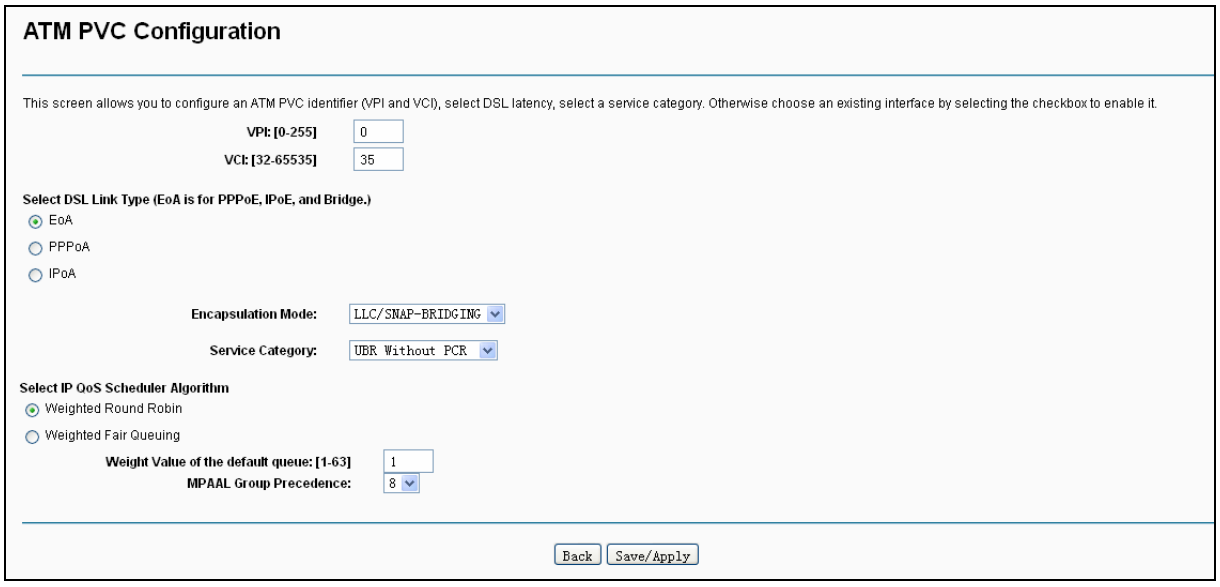


Figure 4-4

- **VPI/VCI**: the VPI and VCI values provided by your ISP. Do not change them unless it was required by your ISP.
- **DSL Link Type**: Select a DSL Link Type which is provided by your ISP. The options include **EoA** (it is for PPPoE, IPoE, and Bridge), **PPPoA** (PPP over ATM) and **IPoA** (IP over ATM).
- **Encapsulation Mode**: The mode of the data processing over the Link Type you have selected. Uses the default setting, if you are not sure.
- **Service Category**: Select the type of the service assigned by your ISP in the drop-down list. The default type is **UBR Without PCR**.

Note:

Enabling packet level QoS for PVC improves performance for selected classes of applications. While QoS consumes system resources; therefore the number of PVC(s) will be reduced. Besides this, it cannot be set for the connection type of CBR and Real-time VBR. If you select the QoS

service, the Quality of Service menu will be added to the Web-based Utility, the detailed configuration will be described in **4.5.9 Quality of Service**.

4.5.1.2 ETH Interface

If your modem router works on **Wireless Router Mode**, choose "**Advanced Setup**"→"**Layer2 Interface→ETH Interface**", you can see ETH WAN interface on the screen below.

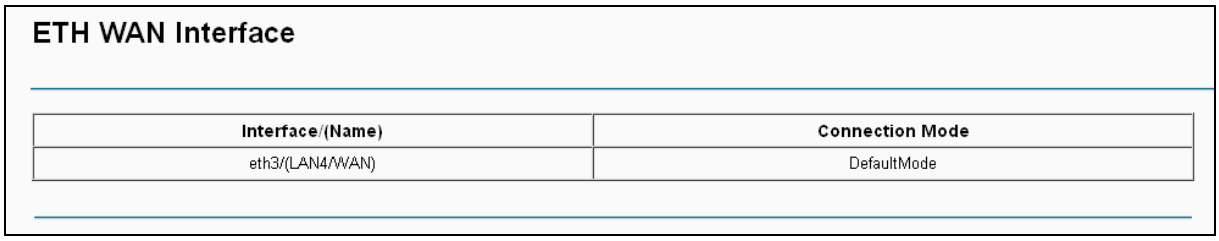


Figure 4-5

4.5.1.3 USB 3G Interface

If you enable 3G as backup access or your modem router works on **3G Router Mode**, choose "**Advanced Setup**"→"**Layer2 Interface**"→"**USB 3G Interface**", you can see USB 3G interface status on the screen below.

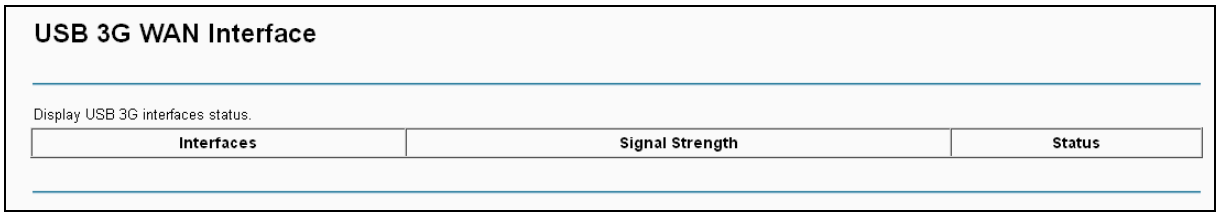


Figure 4-6

4.5.2 WAN Service

Choose "**Advanced Setup**"→"**WAN Service**", and you will see the WAN Port Information Table in the screen similar to Figure 4-7, which describes the WAN port settings and the relevant manipulation to each interface. After you add a new Lay2 Interface, please follow the instructions below to complete the further configuration of WAN Interface. There are five different configurations for the connection types, which are PPPoE, IPoE, Bridge, PPPoA, and IPoA. You can select the corresponding types according to your needs.

Note:

Bridge mode is not available under Wireless Router Mode.

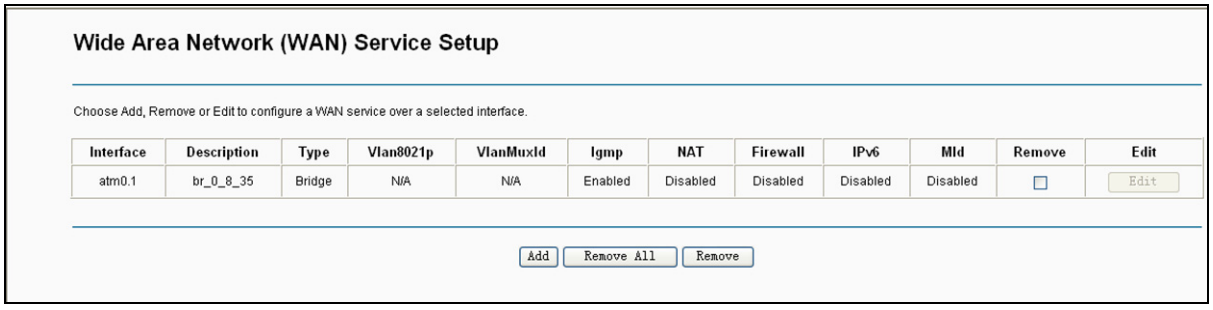


Figure 4-7

Note:

The following section adopts different VPI, VCI to introduce further configuration for the different connection types, if you need to change the configuration of ATM PVC (VPI/VCI), you should go to the previous section (4.5.1 Layer2 Interface) to configure them again.

4.5.2.1 ATM-EoA-PPPoE

If your ISP provides a **PPPoE** connection and you need to use an ATM Interface, follow the steps below to add a WAN service over a selected ATM interface:

1. Add a **new** ATM interface and select **EoA** option for DSL Link Type (4.5.1.1 ATM Interface).
2. Click the **Add** button on the screen Figure 4-7 and you will enter the next screen as shown in Figure 4-8. Click **Next**.

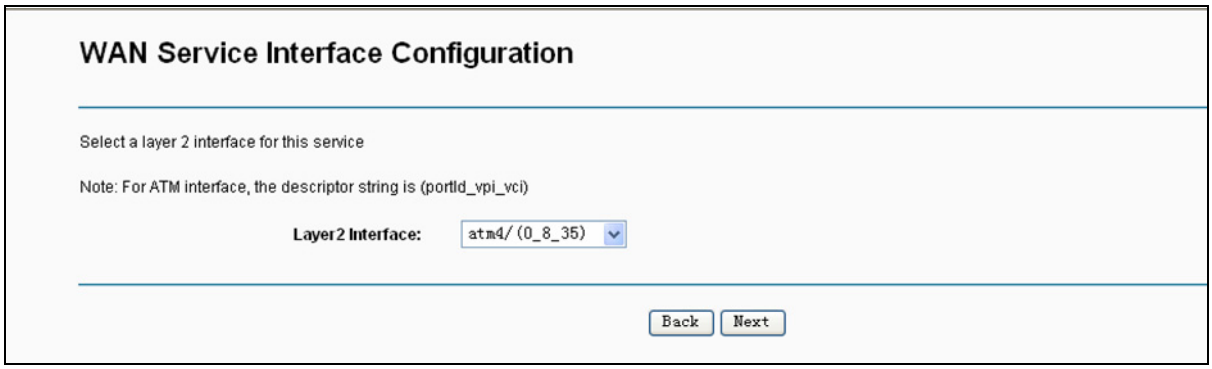


Figure 4-8

3. Select the **WAN service type** in Figure 4-9. If your ISP provides a PPPoE connection, select **PPPoE** option. You can create a service name for the **Service Description** or leave it the default name. Click **Next**.

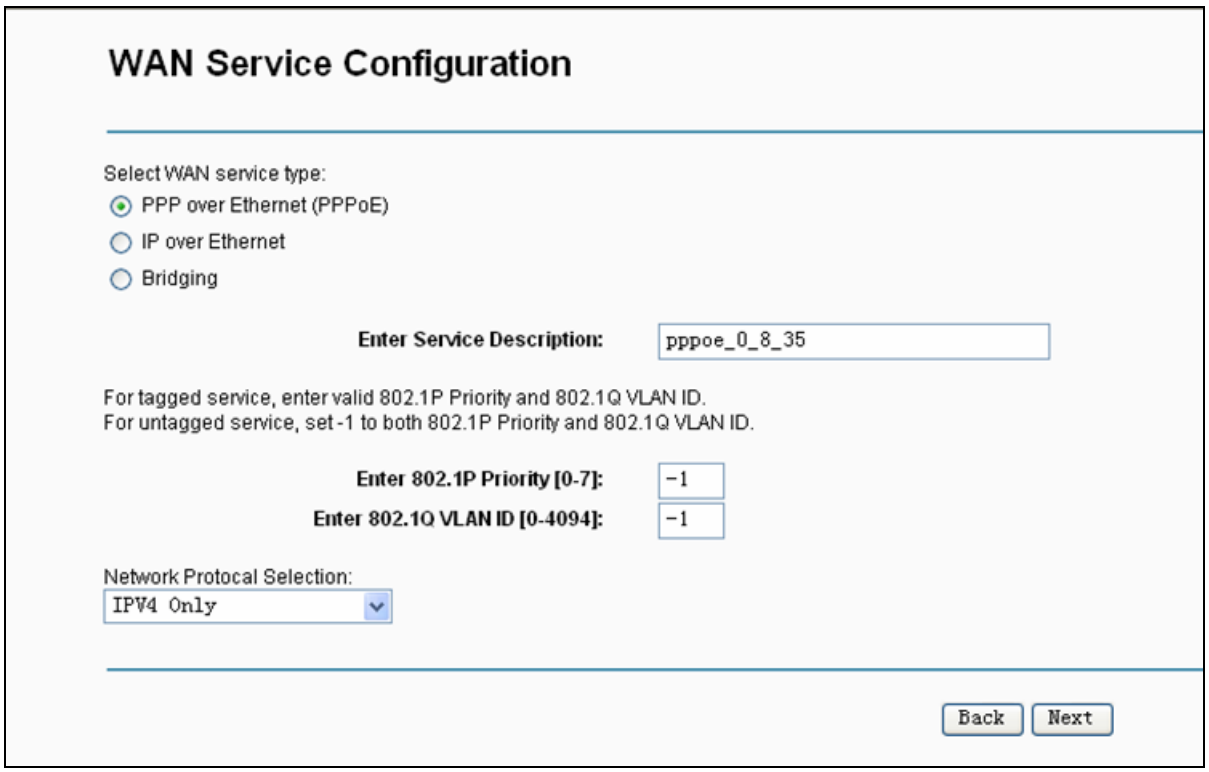


Figure 4-9

4. Enter the following parameters and then click **Next**.

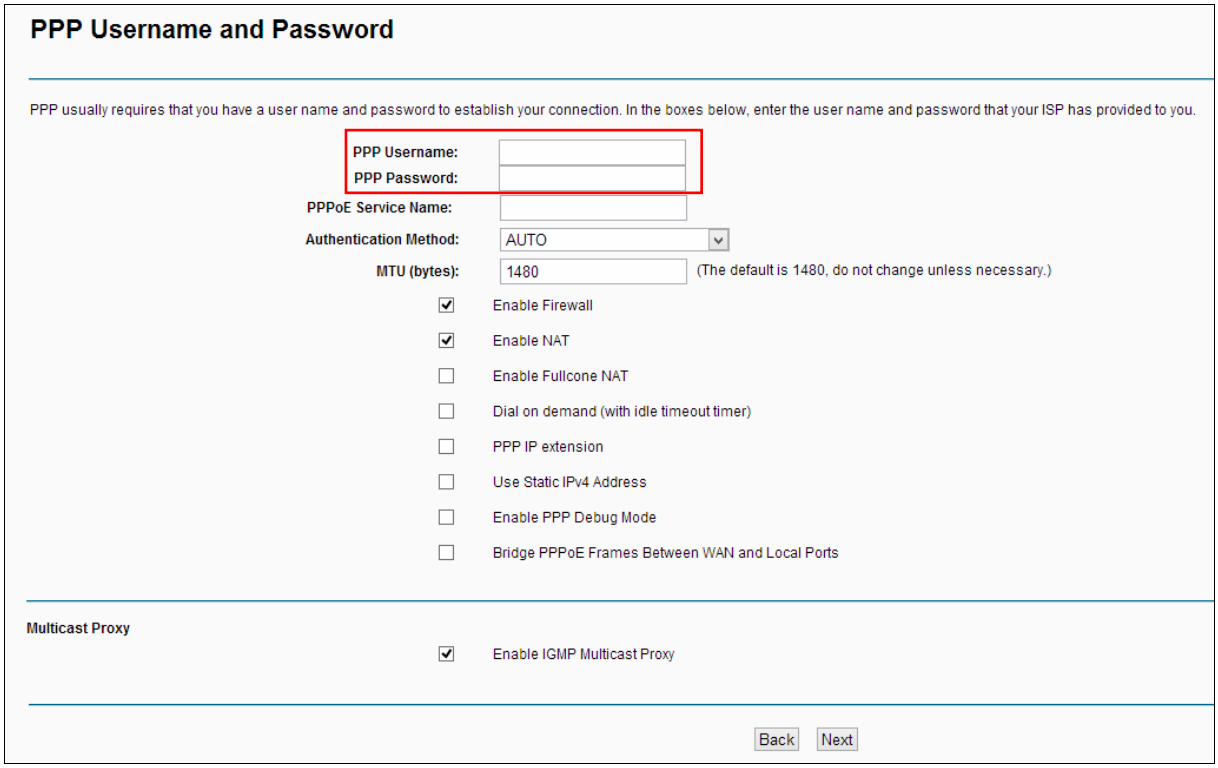


Figure 4-10

- **PPP Username/Password**: Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **PPPoE Service Name**: Enter the Service Name if it was provided by your ISP. If you leave it blank, the default name will be the same as the **Service Description** on the previous screen.
- **Authentication Method**: Select the **Authentication Method** from the drop-down list, the default method is **AUTO**, and you can leave it as a default setting.

Note:

If you are not sure about the **PPP IP extension** and **PPP Debug Mode** etc. below, please don't select these options.

- **MTU Size**: Maximum Transmission Unit Size. Check this box then you can change the MTU size. The default **MTU** value is 1480 Bytes. It is not recommended that you change the default value unless required by your ISP.
- **Enable Firewall:** A PPP Firewall enhances network's security. Select the Option to use the firewall.
- **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. If another router exists in your network, you don't need to select the option.
- **Enable Fullcone NAT:** It is a type of NAT, if not enabled, the default NAT will act.
- **Dial on demand (with idle timeout timer):** The modem router will cut off the Internet connection after it has been inactive for a specific period of time (idle timeout), and it will

automatically re-establish the connection as soon as you attempt to access the Internet again. If your Internet is charged by time you may want to select this option in order to save money.

- **PPP IP extension:** Select this option to get the public IP address from the PPP server to your PC, and the NAT and SPI Firewall will be closed. Sometimes you can think it as bridge while PPP dialing in the modem router. It's a special feature deployed by some ISP. Unless your ISP specifically requires this setup, do not select it.
- **Use Static IPv4 Address:** If your ISP gives you a static **WAN**, Gateway and **DNS** IP address, select this option to enter them manually.
- **Enable PPP Debug Mode: Select this option to debug the PPP function and you can see many PPP log information in the System Log. Only PPP has this debug Mode.**
- **Bridge PPPoE Frames Between WAN and Local Ports:** Select this option to start PPP connection in your local PC.
- **Enable IGMP Multicast 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 router. The default value is enabled, and if you are not sure, please contact your ISP or just leave it.

5. Select a preferred wan interface as the system default gateway in Figure 4-11 and click **Next**.

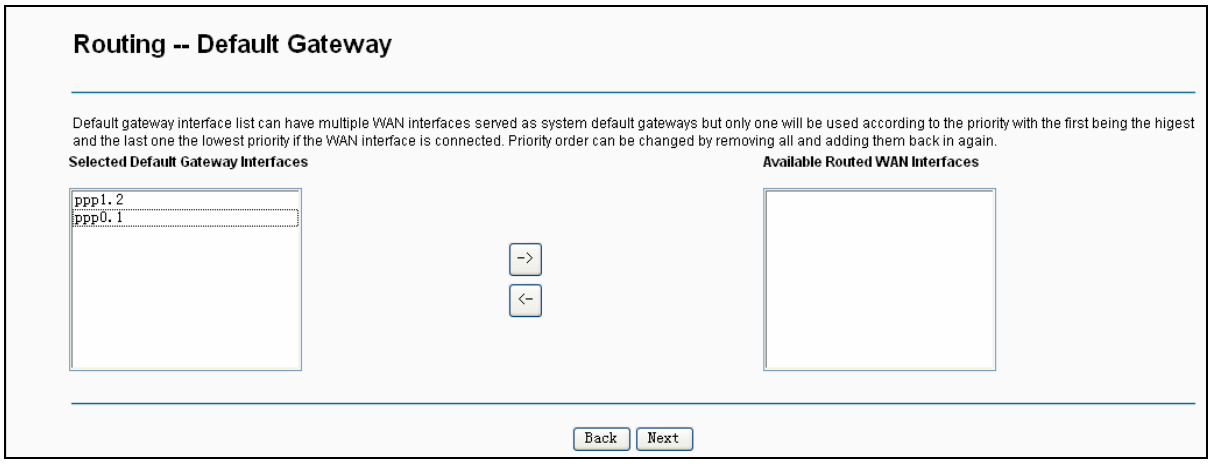


Figure 4-11

6. Configure the DNS Server Addresses on the screen below and click **Next**.

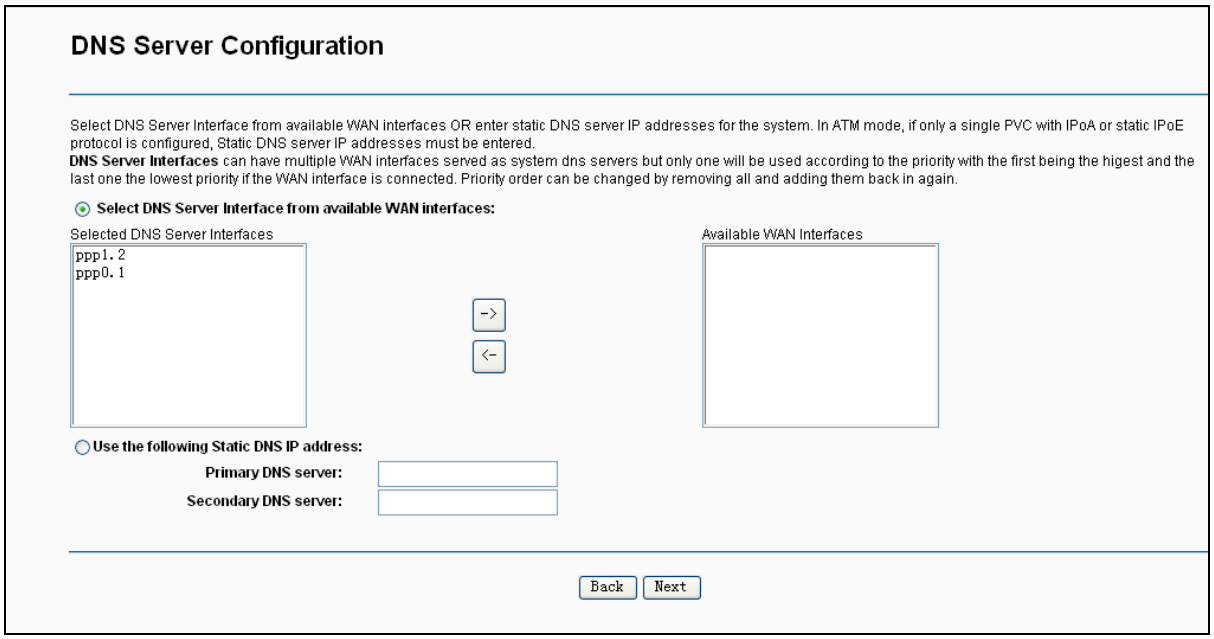


Figure 4-12

- **Select DNS Server Interface from available WAN Interfaces:** You can select this option to automatically get DNS server information from the selected WAN interface.
- **Use the following Static DNS IP Address:** You can select this option to manually enter the primary and /or optional secondary DNS server IP addresses provided by your ISP.

Note:

If only single PVC with IPoA is configured, you must enter static DNS server IP addresses.

7. On the next screen you will see the detailed settings you've made. Please click the **Save/Apply** button to save these settings.

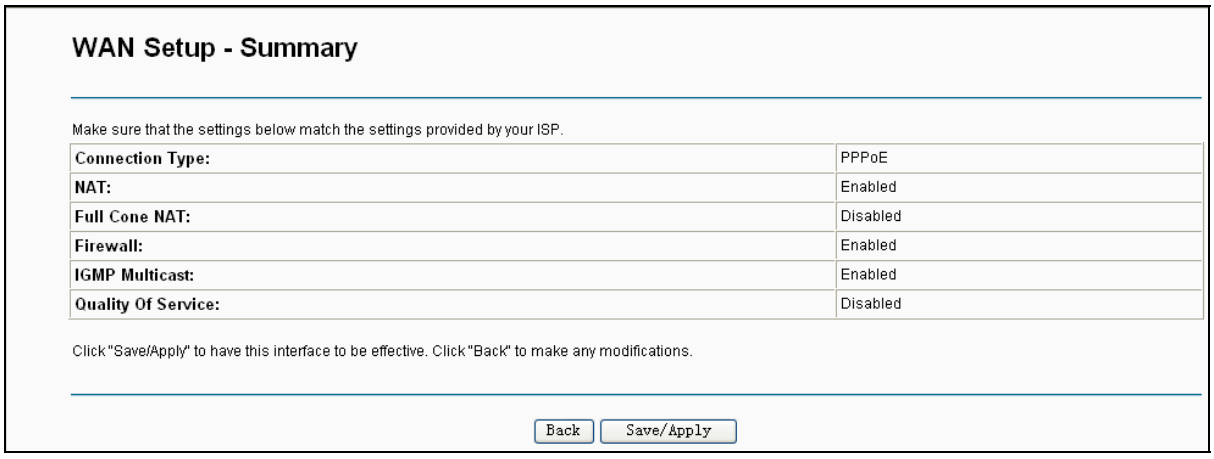


Figure 4-13

8. On the next screen you will see the WAN Port Information Table with the new configuration.

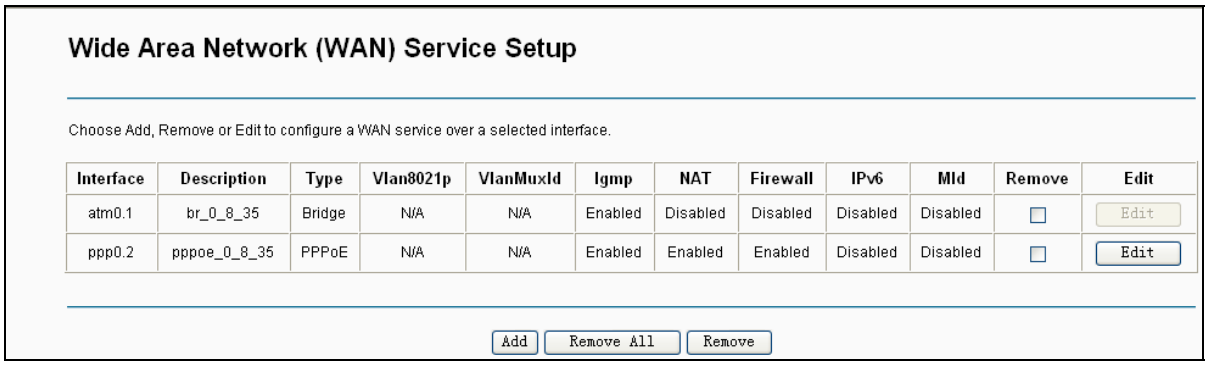


Figure 4-14

- **Remove All:** Click **Remove All**, then all the interface in the table will be deleted.
- **Remove:** Select the check box in the table above and then click **Remove**, the corresponding interface will be deleted in the table.

4.5.2.2 ATM-EoA-IPoE

If your ISP provides an **IPoE** connection and you need to use an ATM Interface, follow the steps below to add a WAN service over a selected ATM interface:

1. Add a **new** ATM interface and select **EoA** option for DSL Link Type (4.5.1.1 ATM Interface).
2. Click the **Add** button on the screen (as shown Figure 4-7). Select WAN Service Interface over ATM PVC on the next screen (as shown Figure 4-8).
3. If your ISP provides an IPoE connection, select **IP over Ethenet** option for the **WAN service type** on the screen (as shown Figure 4-9), and click **Next** button to continue.
4. Enter parameters in the following blanks to configure the WAN IP Address and click **Next**.

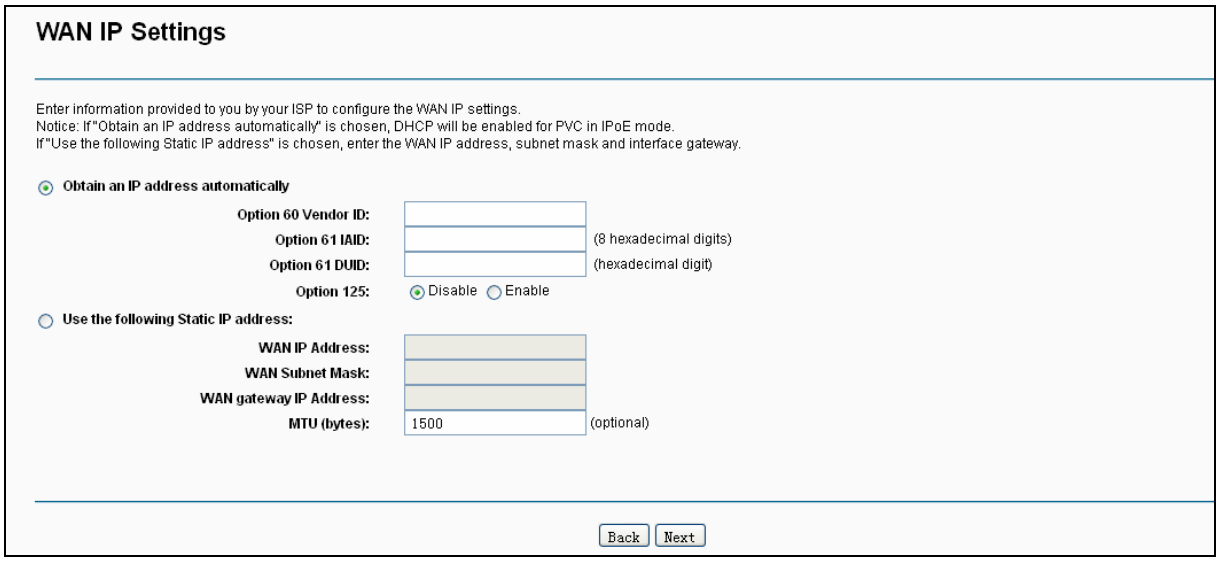


Figure 4-15

- **Obtain an IP address automatically:** Select this option, the modem router will be able to obtain IP network information dynamically from a DHCP server provided by your ISP.

Note:

1) The response message from a DHCP server typically contains a number of configuration parameters (DHCP options) for the modem router. The DHCP options include IP network

information, and also the vendor-specific options. In some cases, the modem router is implemented to perform user-defined operations (as shown below). You can implement your own treatment of all such options.

2) If the modem router is functioning as a DHCP client, it must identify itself in option 61 (client-identifier) in every DHCP message. DUID/IAID is portion of option 61.

- **Option 60 Vendor ID:** The option code 60 used to identify Vendor class.
- **Option 61 IAID:** IAID (Identity Association ID) assigns an Identity Association ID to individual interfaces. In cases where the device is functioning with a single DHCP client identity, it must use value 1 for IAID for all DHCP interactions. In cases where the device is functioning with multiple DHCP client identities, the values of IAID have to start at 1 for the first identity and be incremented for each subsequent identity. For example, the device may use IAID value 1 for the first physical interface and value 2 for the second. Alternatively, the device may use IAID value 1 for the virtual circuit corresponding to the first connection object in the data model and value 2 for the second connection object in the data model.
- **Option 61 DUID:** Specifies the name of the interface whose link-layer address the server is to use as its DUID (DHCP Unique Identifier). You must enter a value for this parameter or the server will not start. When the server starts, the DUID is written to the system log.
- **Option 125:** The option 125 allows DHCP server to be pre-configured with policy for handling classes of devices in a certain way without requiring DHCP server to be able to parse the unique format used in client-identifier option.

➢ **Use the following Static IP address**: If you are provided with a static IP/gateway Address, please select this option, and then enter the **WAN IP Address**, **WAN Subnet Mask** and **WAN gateway IP Address** manually.

5. You will see the next screen as below. You can enable the **NAT**, **SPI Firewall**, and **IGMP Multicast**, if you are not sure about the settings, just leave the default settings. Click **Next**.

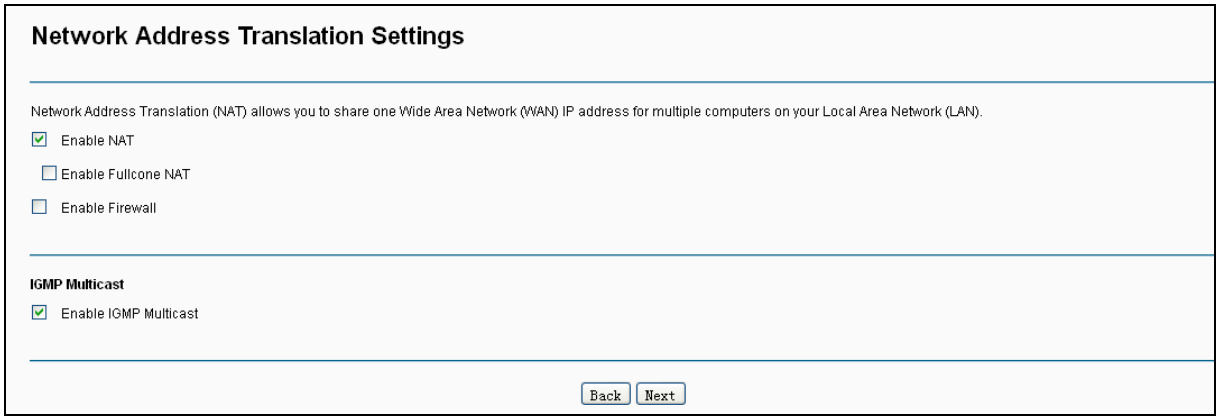


Figure 4-16

➢ **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. If another router exists in your network, you don't need to select the option.

➢ **Enable Fullcone NAT:** It is a type of NAT, if not enabled, the default NAT will act.

➢ **Enable Firewall:** A SPI firewall enhances network's security. Select the option to use a firewall, or else without a firewall.

- **Enable IGMP Multicast:** This is disabled by default. This setting will not allow IGMP (Internet Group Management Protocol) packets to be forwarded to the LAN. IGMP is used to manage multicasting on TCP/IP networks. Most users will not need to enable this. Some ISPs use IGMP to perform remote configuration for client devices, such as the router. If you are unsure, check with your ISP.

Note:

If you select the **Enable NAT** checkbox, the **NAT** menu will be added to the Web-based Utility. We will describe the detailed configuration in 4.5.6 NAT.

6. Select a preferred **WAN** interface as the system default gateway and click **Next**.

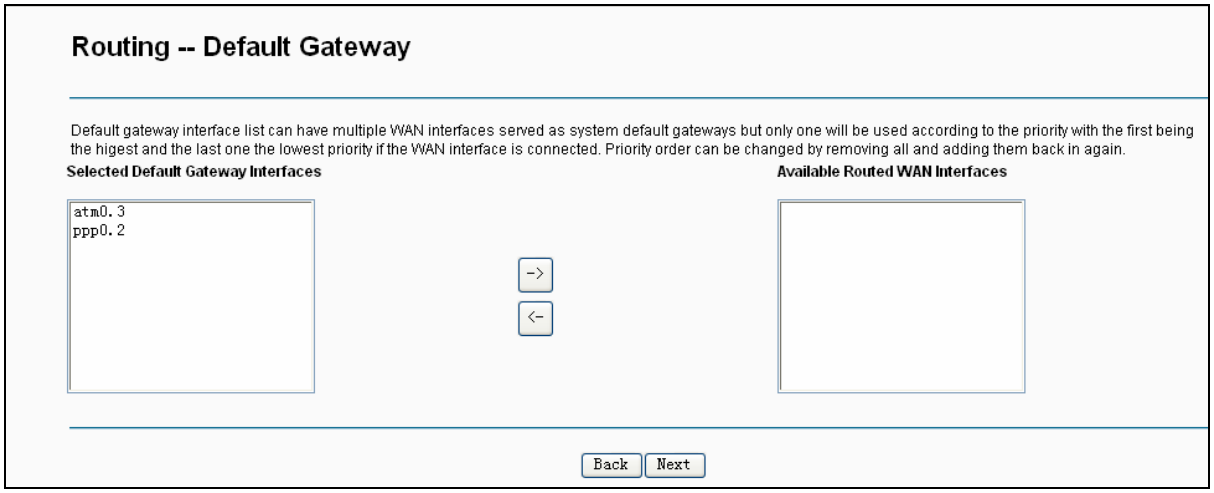


Figure 4-17

7. Configure the DNS Server Addresses on the screen as follows.

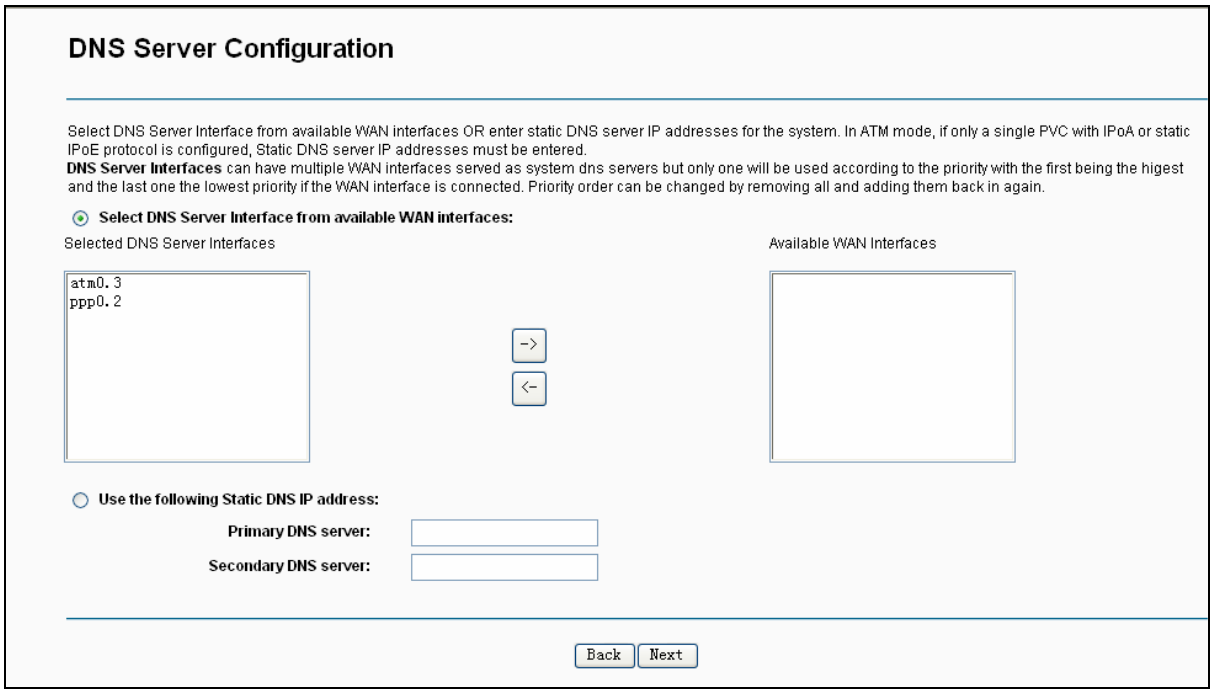


Figure 4-18

Note:

If only single PVC with IPoA is configured, you must enter static DNS server IP addresses.

8. On the next screen (as shown Figure 4-19) you will see the detailed settings you've made. Please click the **Apply/Save** button to save these settings.

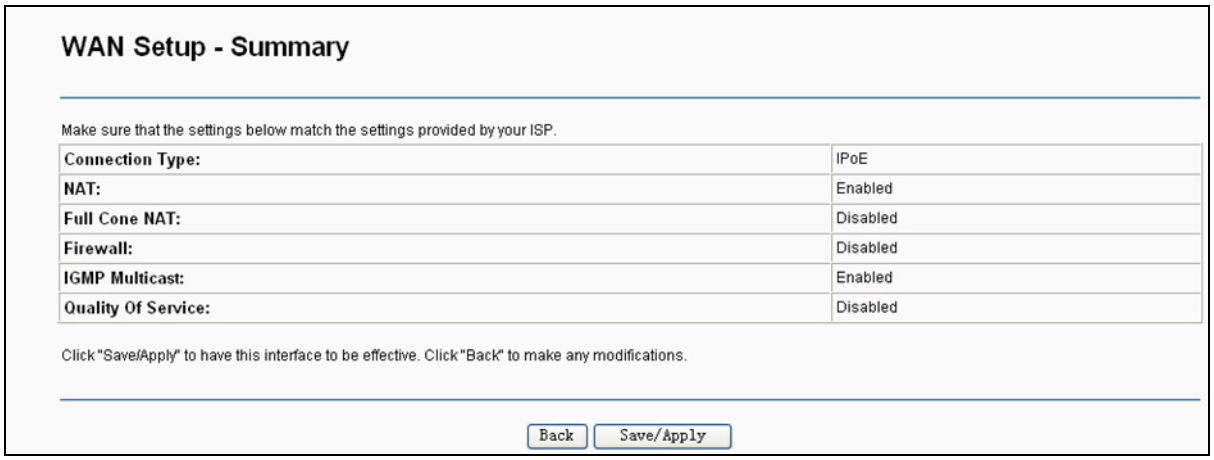


Figure 4-19

4.5.2.3 ATM-EoA-Bridging

If you want to adopt the **Bridge** service and you need to use an ATM Interface, follow the steps below to add a WAN service over a selected ATM interface:

1. Add a new ATM interface and select **EoA** option for DSL Link Type (see 4.5.1.1 ATM Interface).
2. Click the **Add** button on the screen Figure 4-7. Select WAN Service Interface over ATM PVC on the next screen (as shown Figure 4-8).
3. Select **Bridging** option for the **WAN service type** on the screen (as shown Figure 4-9), and click **Next** button to continue.
4. On the screen (as shown Figure 4-13) you will see the detailed settings you've made. Please click the **Apply/Save** button to save these settings.

4.5.2.4 ATM-PPPoA

If your ISP provides a **PPPoA** connection and you need to use an ATM Interface, follow the steps below to add a WAN service over a selected ATM interface:

1. Add a new ATM interface and select **PPPoA** option for DSL Link Type (see 4.5.1.1 ATM Interface).
2. Click the **Add** button on the screen Figure 4-7 and the next configuration is similar to **PPPoE**, (see section 4.5.2.1 ATM-EoA-PPPoE**)**. The difference is that you don't need to set the **PPPoE Service Name** and **Bridge PPPoE Frames Between WAN and Local Ports** on the screen of Figure 4-10.

4.5.2.5 ATM-IPoA

If your ISP provides an **IPoA** connection and you need to use an ATM Interface, follow the steps below to add a WAN service over a selected ATM interface.

1. Add a new ATM interface and select **IPoA** option for DSL Link Type (see 4.5.1.1 ATM Interface).

2. Click the **Add** button on the screen Figure 4-7 and the next configuration is similar to **IPoE** (see section 4.5.2.2 ATM-EoA-IPoE). The difference is that you have to manually set the Static IP Address on the screen of Figure 4-15, and the Static IP Address for DNS Server on the screen of Figure 4-18.

Note:

ETH and ATM service can not coexist. If the ATM Interface had configured, you cannot configure any other WAN service over the ETH Interface until the ATM Interface is deleted.

4.5.2.6 ETH-PPPoE

If your ISP provides a **PPPoE** connection, click the **Add** button on the screen Figure 4-7 and the following configuration is similar to **PPPoE** over ATM interface (see section 4.5.2.1 ATM-EoA-PPPoE).

4.5.2.7 ETH-IPoE

If your ISP provides an **IPoE** connection, click the **Add** button on the screen Figure 4-7 and the next configuration is similar to **IPoE** over ATM interface (see section 4.5.2.2 ATM-EoA-IPoE).

4.5.3 3G Settings

Choose menu "**Advanced Setup→3G Settings**", you can configure parameters for 3G function on the screen below. To use the 3G function, you should first insert your USB modem on the USB port of the modem router. There is already much 3G USB modem information embedded in the modem router. The USB modem parameters will be set automatically if the card is supported by the modem router. If your USB modem inserted is supported by the modem router, then "**Identify successfully**" will display in the USB 3G Modem field as shown in Figure 4-20.

Some 3G USB modem may not be supported by the modem router. For more information, please refer to **Compatibility List** on our website: www.tp-link.com. If your 3G USB modem is incompatible with our modem router, please feel free to contact our Technical Support.

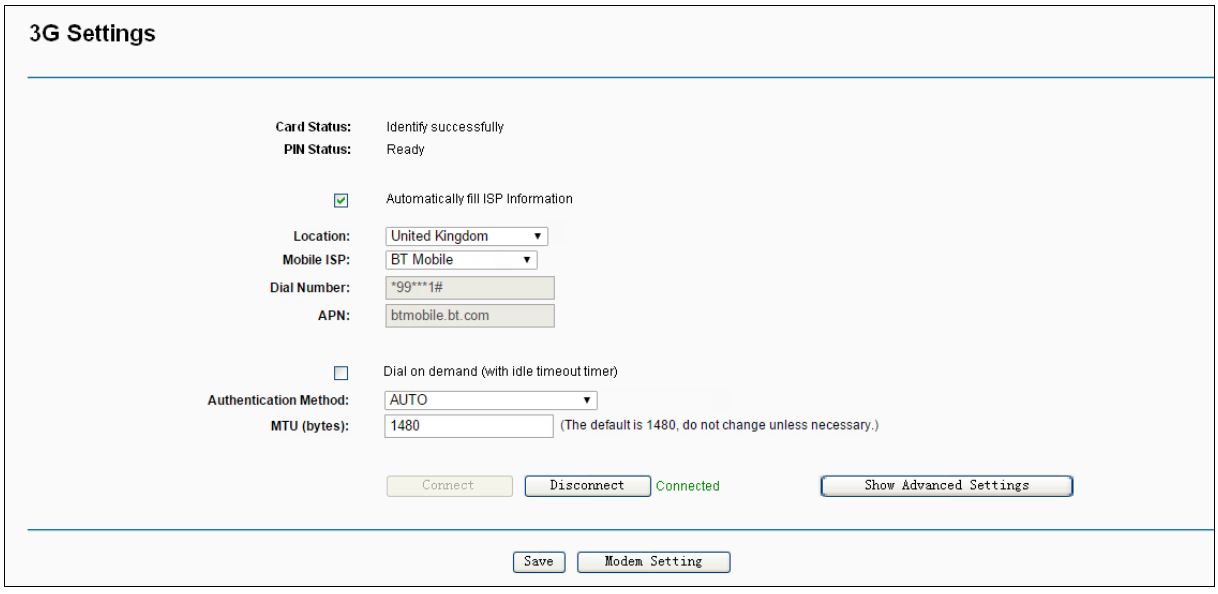


Figure 4-20

- **Location:** The location where you're enjoying the 3G card.

- **Mobile ISP:** The ISP (Internet Service Provider) you apply to for 3G service. The modem router will show the default Dial Number and APN of that ISP.

  Note:

  If your **Location** or **Mobile ISP** is not listed, please untick the box before **Automatically fill ISP Information**. Then fill the **Dial Number** and **APN** blanks below.

- **Dial on demand:** Dial on demand is dependent on the traffic. If there is no traffic (or **Idle**) for a pre-specified period of time **(Inactivity Timeout**), the connection will drop down automatically. And once there is traffic send or receive, the connection will be automatically on. If you want your Internet connection to remain active at all times, enter **0** in the **Inactivity Timeout** field.

  Note:

  Sometimes the connection cannot be disconnected although you specify a time to **Inactivity Timeout** because some applications visit the Internet continually in the background.

- **Connect/Disconnect:** You can click the **Connect/Disconnect** button to connect/disconnect connection immediately.
- **Authentication Method:** Some ISPs need a specific authentication type, please confirm it with your ISP or keep it Auto.
- **MTU size(in bytes):** The default MTU (Maximum Transmission Unit) size is 1480 bytes, which is usually fine. For some ISPs, you need modify the MTU. This should not be done unless you are sure it is necessary for your ISP.

Note:

3G settings is unavailable when operation mode is not 3G Router Mode and the backup is not enabled. Please tick the box in the next screen to **enable 3G as a backup solution for Internet access** or change settings on Operation Mode if you want to use 3G.

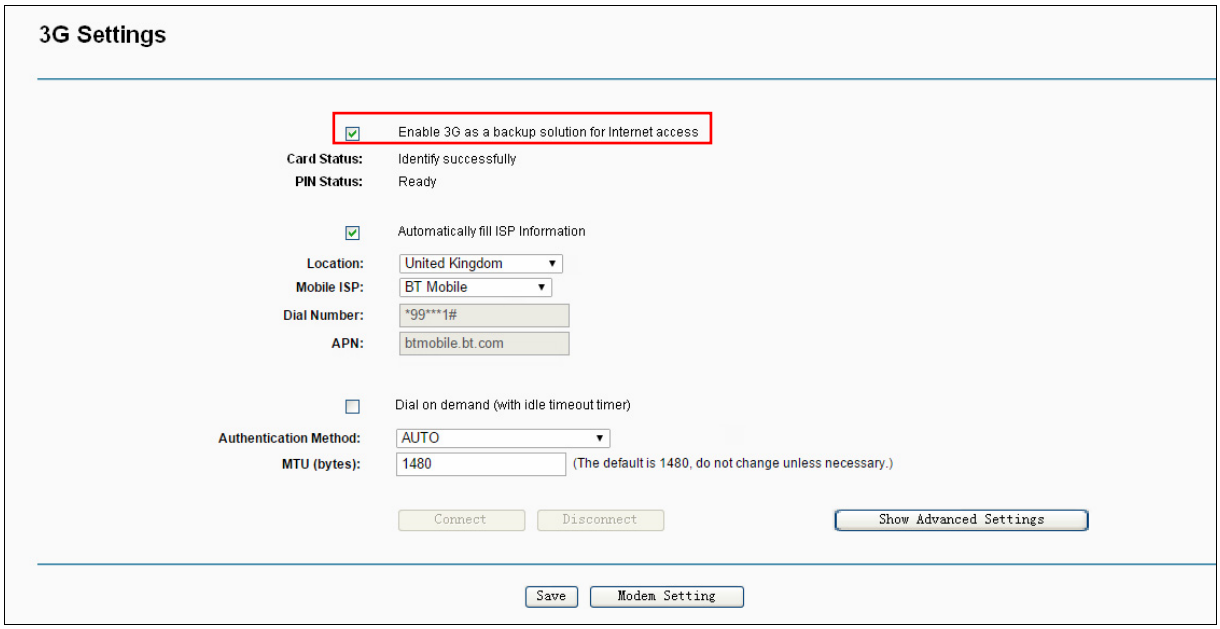


Figure 4-21

Click **Modem Settings** in Figure 4-20, 3G Modem settings can be shown as below.

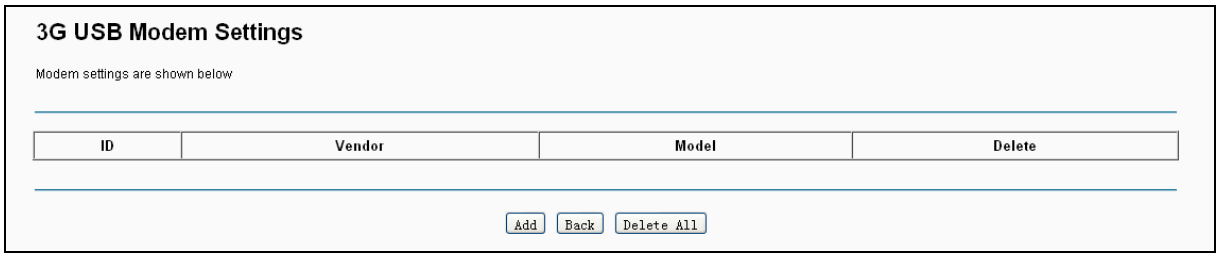


Figure 4-22

To upload 3G USB Modem Configuration File:

1. Click the **Add** button. Then Figure 4-23 will pop up.
2. Click the **Browse** button in Figure 4-23, and then select the right file from the drop-down list.

Click the **Upload Settings** button to upload the file.

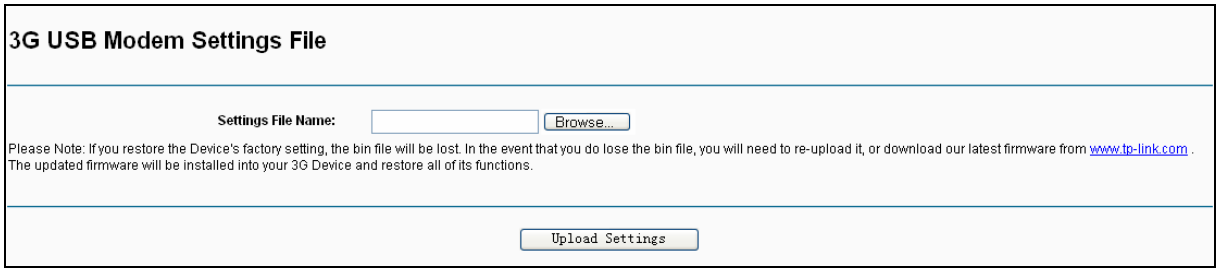


Figure 4-23

Click **Show Advanced Settings** in Figure 4-20, advanced settings can be shown as below.

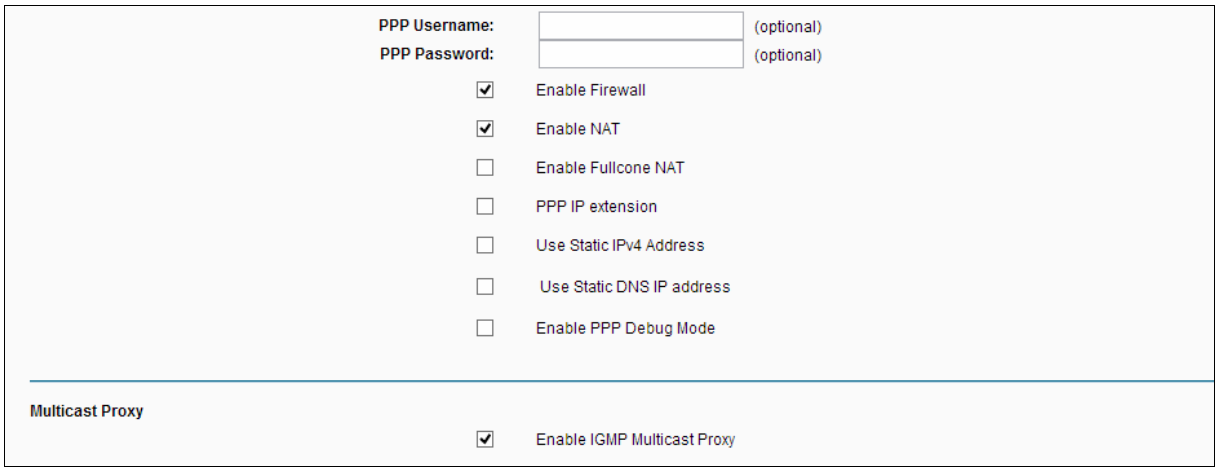


Figure 4-24

- **PPP Username/Password:** Enter the Username and Password provided by your ISP. These fields are case-sensitive.
- **Use Static IPv4 Address:** If your ISP specifies an IP address for you, click the checkbox and fill the Static IPv4 Address.
- **Use Static DNS IP Address:** If your ISP specifies a DNS IP address for you, click the checkbox and fill the **Primary DNS** and **Secondary DNS** blanks below. The Secondary DNS is optional. Otherwise, the DNS servers will be assigned dynamically from ISP.
- **Primary DNS:** Enter the DNS IP address in dotted-decimal notation provided by your ISP.

- **Secondary DNS:** (Optional) Enter another DNS IP address in dotted-decimal notation provided by your ISP.

Once the connection is successful, you will find the 3G screen is similar to Figure 4-20. Click menu "**Device Info**"→"**WAN**" and you will see the 3G status is similar to Figure 4-25.

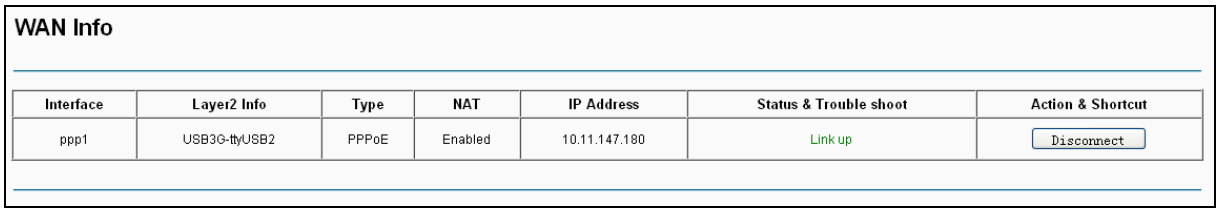


Figure 4-25

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

4.5.4 MAC Clone

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

The WAN Interface List displays the Lay2 Interfaces you have configured on the section 4.5.1 Layer2 Interface and its default MAC Address. If you have not configured corresponding WAN Service for the interface on the section 4.5.2 WAN Service, the blank for MAC Address will display "Need a corresponding WAN Service".

The last one of WAN Interface List displays your PC's current address.

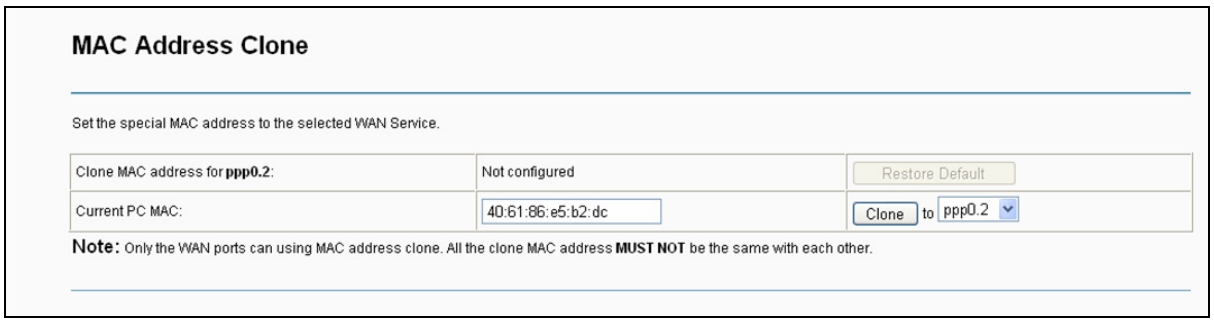


Figure 4-26

Type the new value for the WAN Interface who's MAC Address you want to change.

You can select corresponding WAN Interface from the drop-down list and click **Clone** button to clone your current PC MAC.

Click **Restore Default** button to restore the WAN Interface's default MAC Address.

Note:

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

4.5.5 LAN

Choose "**Advanced Setup**"→"**LAN**", and you will see the LAN screen including **IPv4 LAN Config** and **IPv6 LAN Config**. The section allows you to configure the modem router's LAN ports settings.

4.5.5.1 IPv4 LAN Config

Choose "**Advanced Setup**"→"**LAN**" →"**IPv4 LAN Config**", and you will see the LAN screen (shown in Figure 4-27), here you can configure LAN IPv4 interface for your modem router.

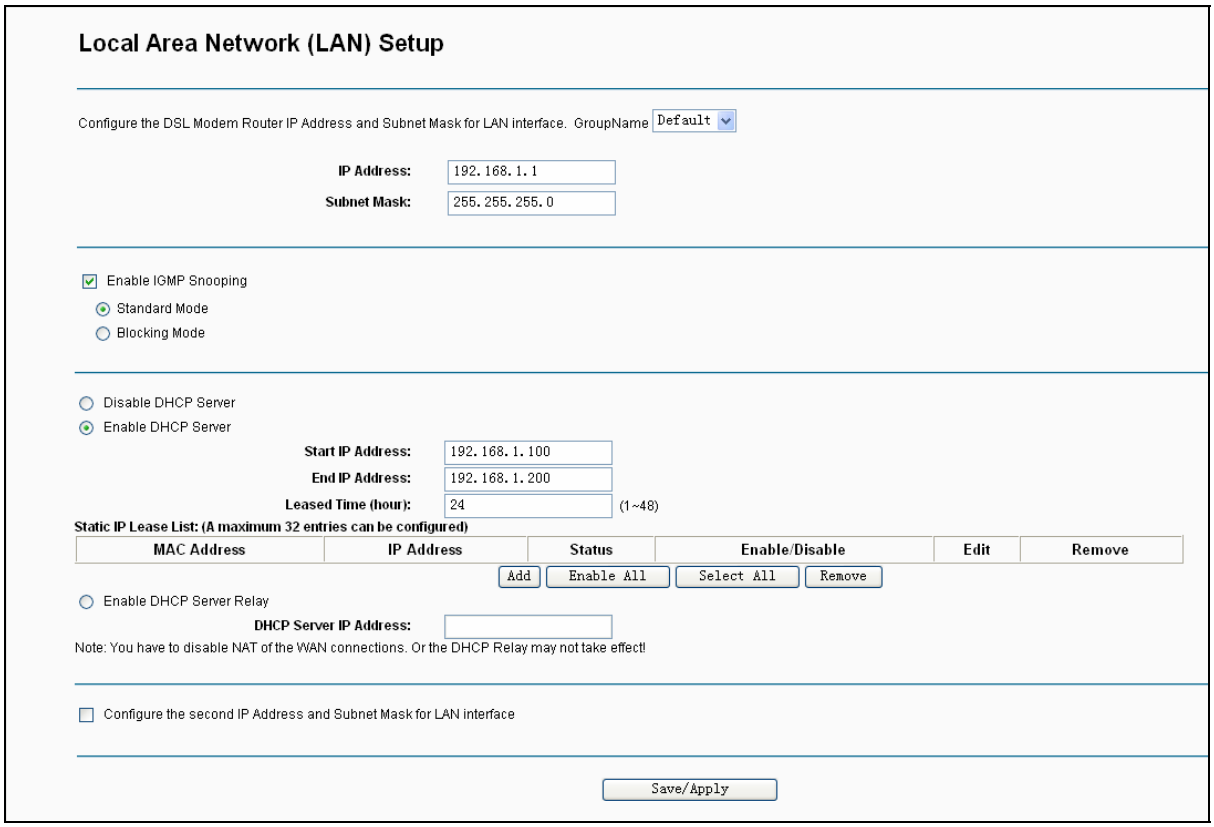


Figure 4-27

- **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:** If you select the option, please choose the IGMP Mode**:** Standard Mode or Blocking Mode.
- **DHCP Server:** These settings allow you to configure the modem router's Dynamic Host Configuration Protocol (DHCP) server function. The DHCP server is enabled by default for the modem router's Ethernet LAN interface. DHCP service will supply IP settings to computers which are configured to automatically obtain IP settings that are connected to the modem router though the Ethernet port. When the modem router is set for DHCP, it becomes the default gateway for DHCP client connected to it. Keep in mind that 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. Because the default IP address for the modem router is 192.168.1.1, the default Start IP Address is **192.168.1.2**, and the Start IP Address must be 192.168.1.2 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 (hour):** The Leased Time is the amount of time in which a network user will be allowed connection to the modem router with their current dynamic IP address. Enter the amount of time, in hours, then the user will be "leased" this dynamic IP address. After the dynamic IP address has expired, the user will be automatically assigned a new dynamic IP address. The default is **24** hours.

➢ **Static IP Lease List**: The function allows you to specify a reserved IP address for a PC on the LAN, that PC will always obtain the assigned IP address each time when it accesses the DHCP server. Reserved IP addresses should be assigned to servers that require permanent IP settings. Click the **Add** button in Figure 4-27, and then you will set the rule in the screen as below.

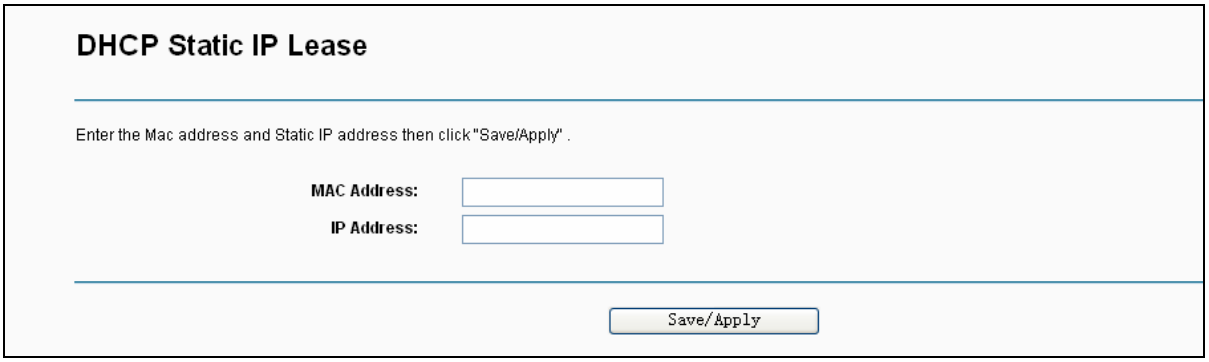


Figure 4-28

- MAC Address: The MAC address of the computer on the LAN which you want to reserve an IP.
- IP Address: The IP address you want to reserved to the computer.

➢ **Configure the second IP Address and Subnet Mask:** You can configure the modem router's second IP Address and Subnet Mask for LAN Interface through which you can also access to the Web-based Utility as the default IP Address and Subnet Mask.

4.5.5.2 IPv6 LAN Config

Choose "**Advanced Setup**"→"**LAN**" →"**IPv6 LAN Config**", and you will see the LAN screen (shown in Figure 4-29), here you can configure LAN IPv6 interface for your modem router.

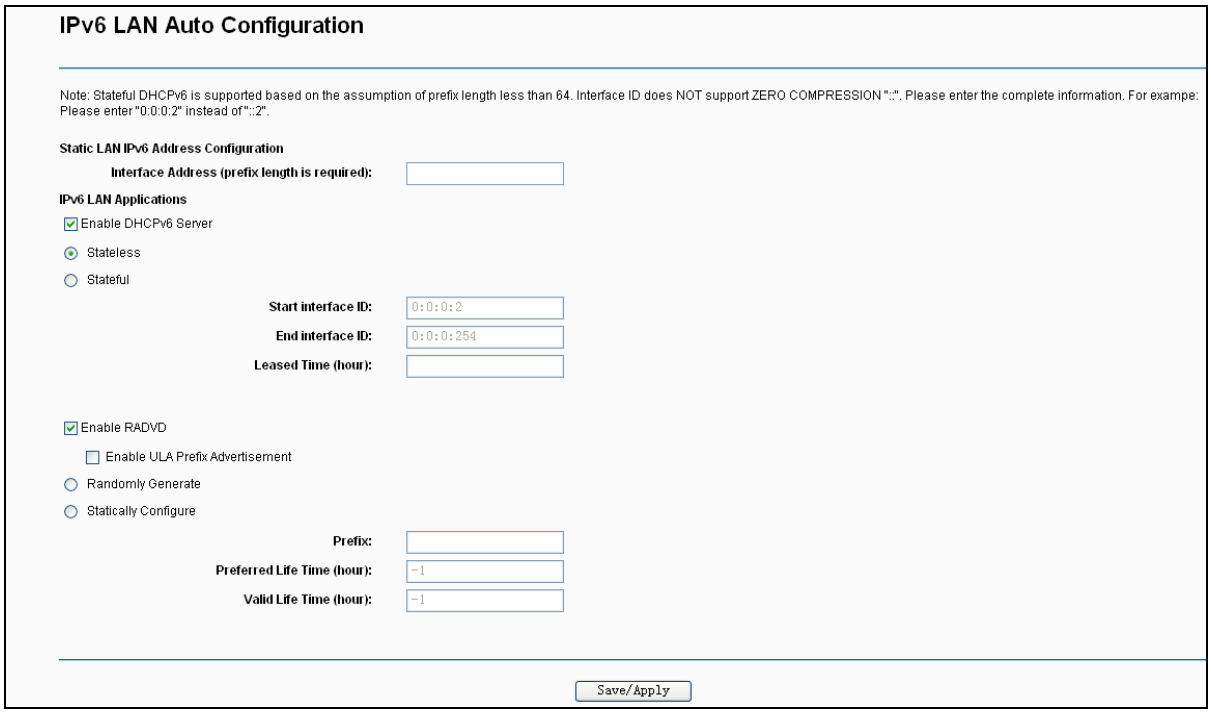


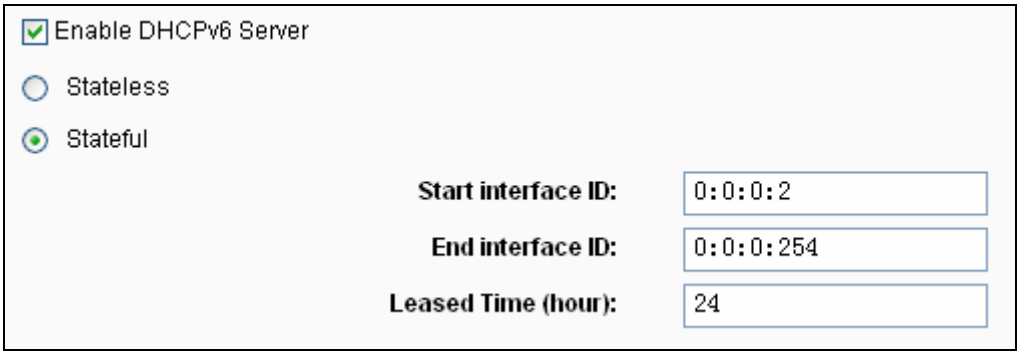
Figure 4-29

- **Interface Address (prefix length is required):** Here enter the prefix length of your interface address.
- **IPv6 LAN Applications:** Select a type to assign IPv6 addresses to the computers in your LAN. DHCPv6 Server and RADVD are provided.

  For DHCPv6 Server:

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

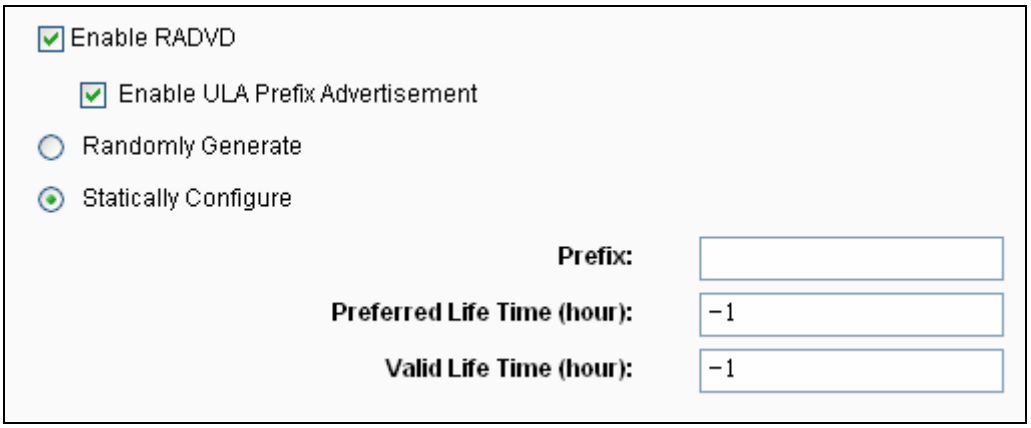
  2) If **Stateful** is selected, please complete the following parameters.



- **Start interface ID:** Enter a value for the DHCPv6 server to start with when issuing IPv6 addresses.
- **End interface ID:** Enter a value for the DHCPv6 server to end with when issuing IPv6 addresses.
- **Leased Time (hour):** The Leased Time is the amount of time in which a network user will be allowed to connect to the modem router with their current dynamic IPv6 address. Enter the amount of time, in hours, then the user will be "leased" this dynamic IPv6 address. After the dynamic IPv6 address has expired, the user will be automatically assigned a new dynamic IPv6 address. The default is 24 hours.

For RADVD:

1) If **Randomly Generate** is selected, it doesn't need to be configured.
2) If **Statically Configure** is selected, please complete the following parameters.



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

Click **Save/Apply** to make the configuration take effect.

4.5.6 NAT

NAT (Network Address Translation) allows you to share one WAN (Wide Area Network) IP address for multiple computers on your LAN (Local Area Network).

☞ **Note:**

When you select **PPPoA** or **PPPoE** for the WAN Setup, or when you select **Enable NAT** for the type of **IPoA** and **IPoE** connection (4.5.2 WAN Service), you will see the **NAT** menu in the Web-based Utility.

Choose "**Advanced Setup**"→"**NAT**", there are three submenus under the main menu**: Virtual Servers**, **Port Triggering, DMZ Host** and **ALG**. Click any of them, and you will be able to configure the corresponding function.

4.5.6.1 Virtual Servers

Choose "**Advanced Setup**"→"**NAT**"→"**Virtual Servers**", you can set up virtual servers on the screen below (shown in Figure 4-30).

Virtual servers can be used for setting up public services on your LAN, such as DNS, Email and FTP. A virtual server is defined as a service port, and all requests from the 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.

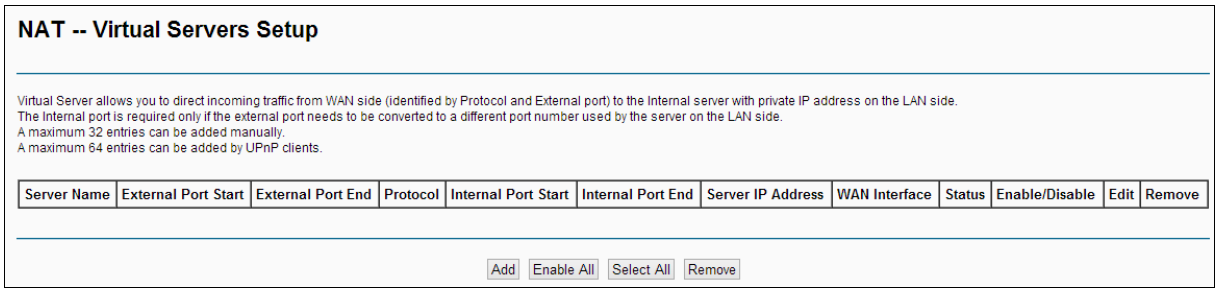


Figure 4-30

- **Virtual Server Table:** The table indicates the information about the Virtual Server entries.
  - **Server Name:** This is the name of the **Virtual Server**. It is exclusive and must be filled in.
  - **External Port Start:** The base number of External Ports. You can type a service port or leave it blank.
  - **External Port End:** The end number of External Ports. You can type a service port or leave it blank.
  - **Protocol:** The protocol used for this application, **TCP**, **UDP**, or **TCP/UDP**.
  - **Internal Port Start:** The base number of Internal Ports. You can type a service port or leave it blank.
  - **Internal Port End:** The end number of Internal Ports. You can type a service port or leave it blank.
  - **Server IP Address:** The IP Address of the PC providing the service application.
  - **WAN Interface:** The WAN Service Interface providing the service application.
- **Add:** Click the **Add** button to add a new entry.
- **Remove:** Select the check box in the table (shown in Figure 4-30) and then click the **Remove** button, then the corresponding entry will be deleted in the table.

To add a virtual server entry:

1. Click the **Add** button on the preceding screen Figure 4-30, and then you will see the new Virtual Server in the next screen as shown in Figure 4-31.

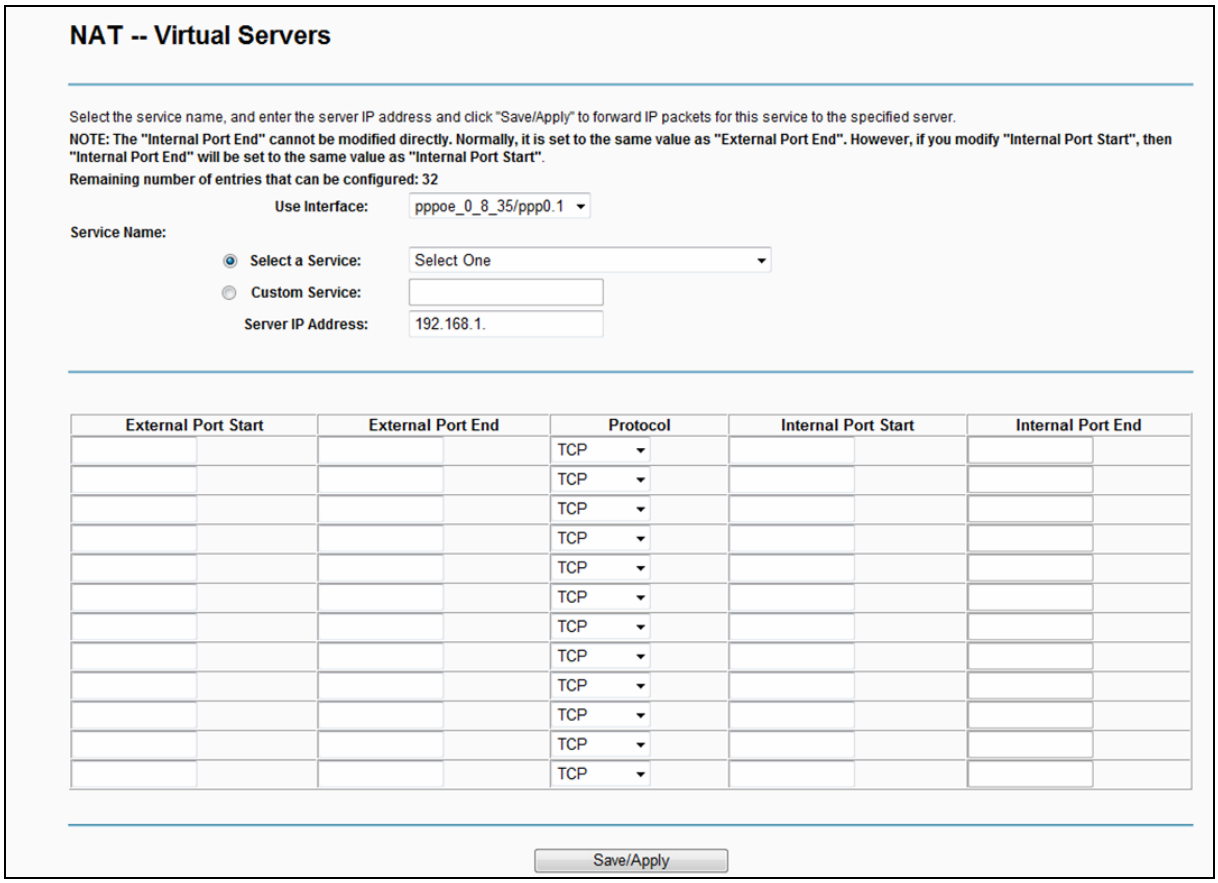


Figure 4-31

2. Select the Interface which you want to use from the drop-down list.
3. Select the service which you want to use from the drop-down list. If the list does not have the service you need, type the name of the custom service in the text box.
4. Type the IP Address of the computer in the **Server IP Address** text box.
5. Enter the External Port Start, External Port End, Internal Port Start and Internal Port End in the table, and then select the protocol used for this Virtual Server, **TCP**, **UDP** or **All**.
6. Click **Save/Apply** to enable virtual server and then you will see your setting as shown in Figure 4-30.

☞ **Note:**

If you select the service from the drop-down list, the External Port Start, External Port End, Internal Port Start, Internal Port End and the Protocol will be added in the table automatically. You only need to enter the Server IP Address for the Virtual Server.

4.5.6.2 Port Triggering

Choose "**Advanced Setup**"→"**NAT**"→"**Port Triggering**", you can set Port Triggering on the screen (shown in Figure 4-32).

Some applications require that specific ports in the modem router's firewall should be opened for access by remote devices. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote device using the triggering ports. The modem router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the open ports. A maximum 32 entries can be configured.

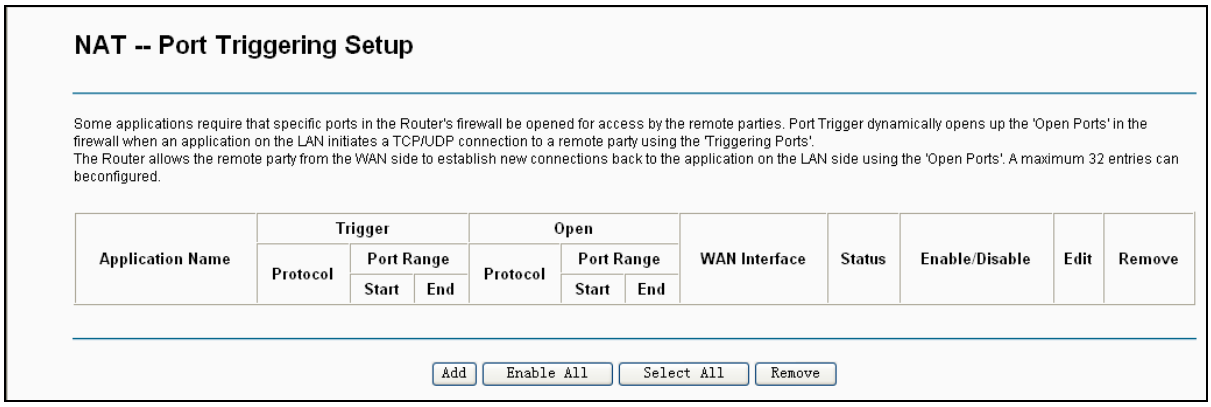


Figure 4-32

- **Port Triggering Table:** The table indicates the information about the Port Triggering entries.
  - **Application (Name):** This is the name of the **Port Triggering**. It is exclusive and must be filled.
  - **Trigger:** It includes the Protocol and the Start and End value of the Trigger Ports.
  - **Open:** It includes the Protocol and the Start and End value of the Open Ports.
  - **WAN Interface:** The WAN Service Interface setting the Port Triggering.
- **Add:** Click the button to add a new entry.
- **Remove:** Select the check box in the table (shown in Figure 4-32) and then click the **Remove** button, then the corresponding entry will be deleted in the table.

To add a new Port Triggering:

1. Click the **Add** button in Figure 4-32, and then you will see the new Port Triggering in the next screen as shown in Figure 4-33.

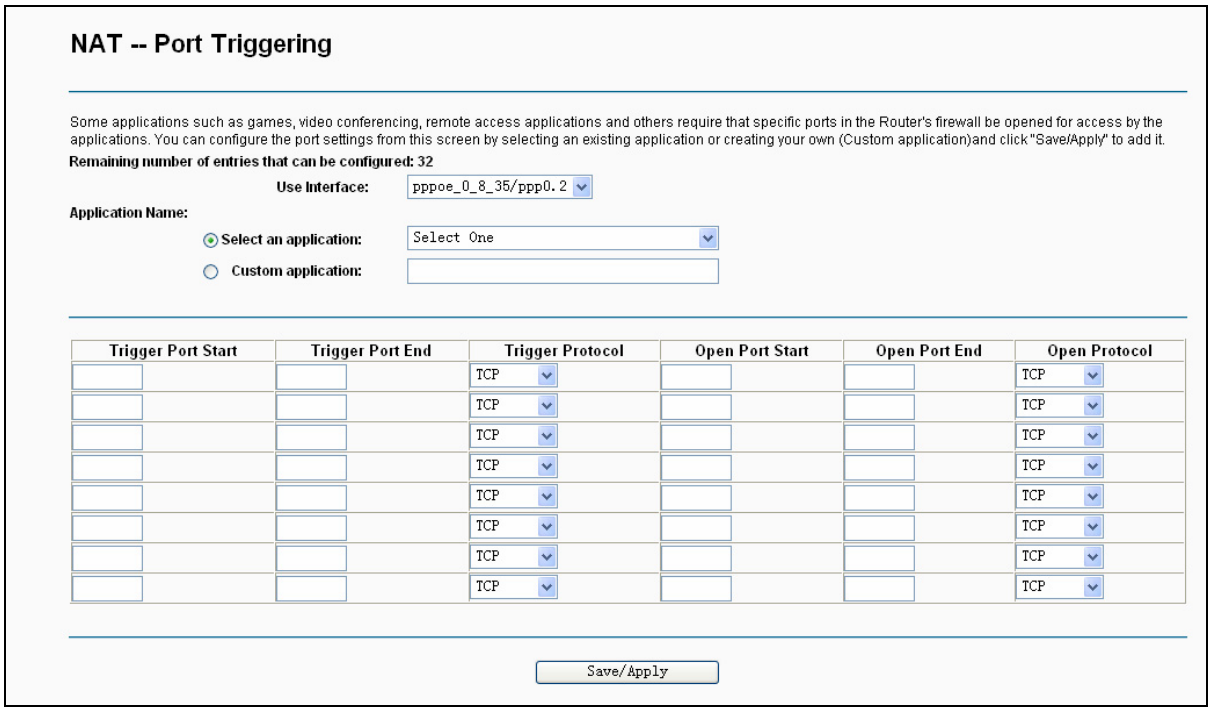


Figure 4-33

2. Select the application from the drop-down list. If the list does not have the application that you want, select the **Custom application** radio button, and type the name of the custom application in the text box.
3. Enter the **Trigger Port Start**, **Trigger Port End**, **Open Port Start** and **Open Port End** in the table, and then select the **Trigger protocol** and **Open protocol**, **TCP**, **UDP** or **All**.
4. Click **Save/Apply** to enable the settings and then you will see your settings as shown in Figure 4-32.

Note:

If you select the application from the drop-down list, the External Port Start, External Port End, Internal Port Start, Internal Port End and the Protocol will be added in the table automatically.

4.5.6.3 DMZ Host

Choose "**Advanced Setup**"→"**NAT**"→"**DMZ Host**", you can set up DMZ Host on the screen (shown in Figure 4-34).

The DMZ host feature can make a local host be exposed to the Internet for a special-purpose service, such as online gaming or video conferencing.

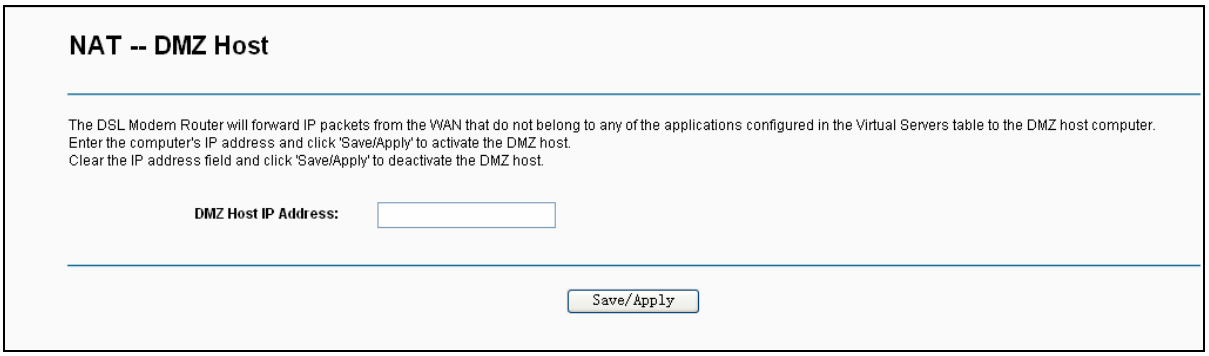


Figure 4-34

To add a new DMZ Host:

You can enter the computer's IP address and then click **Save/Apply** to activate the DMZ host you set on this page.

Note:

DMZ host forwards all the ports at the same time. 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 change while using the DHCP function.

4.5.6.4 ALG

Choose "**Advanced Setup**"→"**NAT**"→"**ALG**", and then you can configure the basic security in the screen as shown in Figure 4-35.

Figure 4-35

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

4.5.7 Security

Choose "**Advanced Setup**"→"**Security**", and you will see the security screen including **IP Filtering** and **MAC Filtering** (only effective in Bridging mode) submenus.

4.5.7.1 IP Filtering

The IP address filtering feature makes it possible for administrators to control user's access to the Internet, which is based on user's IP. The IP address filtering here means **Outgoing**, the detailed descriptions are provided below.

Choose "**Advanced Setup**"→"**Security**"→"**IP Filtering**", you can configure Outgoing Filtering rules on the screen (shown in Figure 4-36).

The Outgoing IP Filtering feature allows you to control some IP traffic from LAN to access to some specifically addresses. By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters.

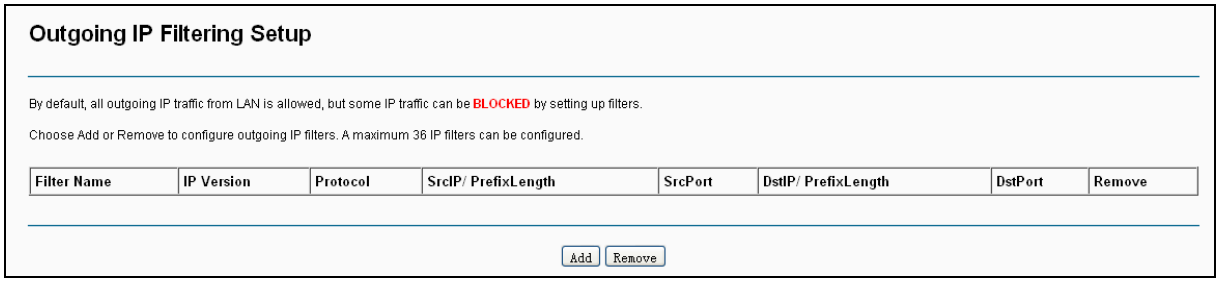


Figure 4-36

Set up an Outgoing IP Filtering rule:

1. Click the **Add** button in Figure 4-36, and you will see the next screen as shown in Figure 4-37.

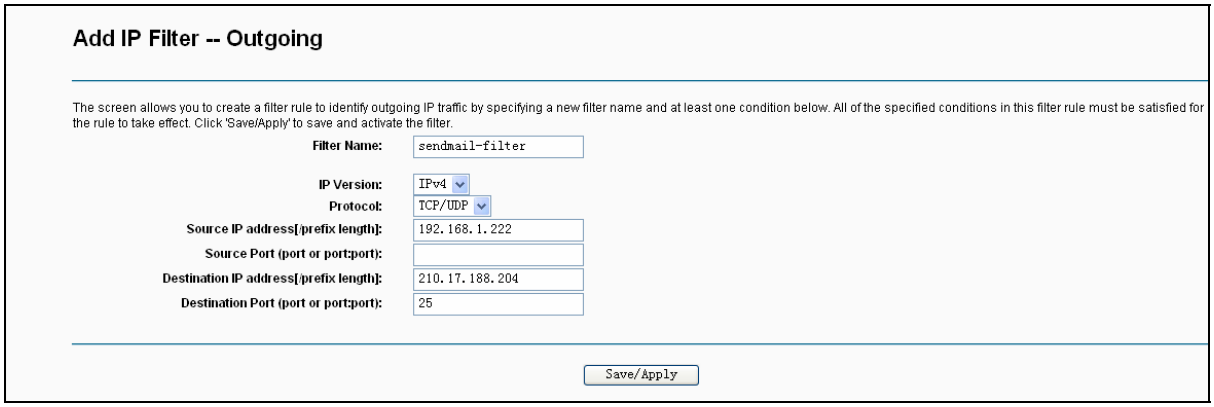


Figure 4-37

2. Enter the **Filter name** for the rule, it is exclusive and must be filled.
3. Select the **protocol: TCP/UDP**, **TCP**, **UDP** or **ICMP** in the drop-down list for the connection between the Source IP address and Destination IP address.
4. Enter a **Source IP Address** in dotted-decimal notation format and then type **Source Port** (port or port**:** port) in the text boxes separately.
5. Enter a **Destination IP Address** in dotted-decimal notation format and then type **Destination Port** (port or port**:** port) in the text boxes separately.
6. Click **Save/Apply** to save this entry.

Note:

When you add an Outgoing IP Filtering entry, you must configure at least one condition on the preceding screen except the Filter name. If you leave the Protocol blank, it means that the rule is effective to all protocols, if you leave the Source IP Address and/or Destination IP Address blank, it suggests that all Source IP Addresses and/or Destination IP Addresses are controlled by the rule, if you leave the Source Port and/or Destination Port blank, it suggests that all Source Ports and/or Destination Ports are controlled by the rule.

4.5.7.2 MAC Filtering

Choose "**Advanced Setup**"→"**Security**"→"**MAC Filtering**", you can configure MAC Filtering rules on the screen as shown in Figure 4-38. The section allows you to control access to the Internet by users on your local network based on their MAC Address.

Note:

MAC Filtering is only effective on ATM PVC(s) configured in Bridging mode.

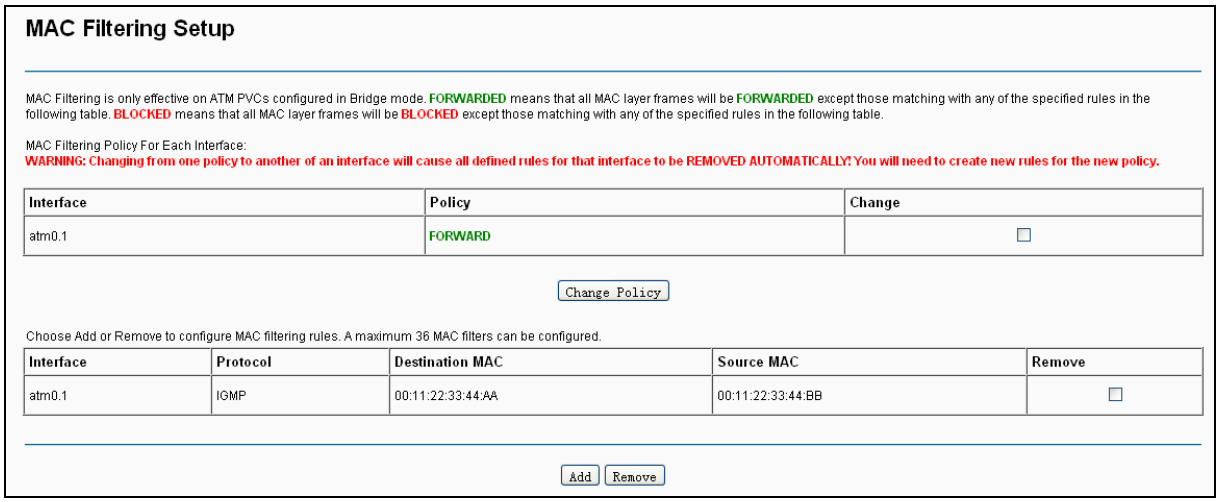


Figure 4-38

- **Change Policy:** There are two policies for the MAC filters**: FORWARDED** and **BLOCKED**. Select the **Change** checkbox and click the **Change Policy** button to change from one policy to another. When you set **FORWARDED**, it means that all MAC layer frames will be **forwarded** except those matching with any of the specified rules in the table (shown in Figure 4-38). While **BLOCKED** means that all MAC layer frames will be **blocked** except those matching with any of the specified rules in the preceding table.
- **Add:** Click the **Add** button, and then you can add a new MAC Filter in the next screen (shown in Figure 4-38).
- **Remove:** Select the check box in the table (shown in Figure 4-38) and then click the **Remove** button, and then the corresponding entry will be deleted in the table.

To add a MAC Filtering rule:

1. Click the **Add** button in Figure 4-38, and you will see the next screen similar to in Figure 4-39.

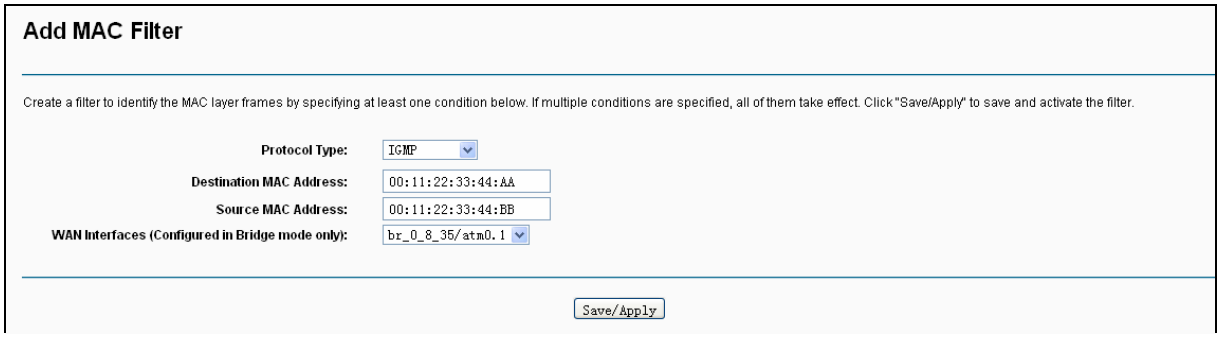


Figure 4-39

2. Select **Protocol Type** in the drop-down list for the rule.

3. Enter **Destination MAC Address** and **Source MAC Address** in the text box.
4. Select **Frame Direction** in the drop-down list for the rule.
5. Select the **WAN interfaces** from the drop-down list.
6. Click **Save/Apply** to save this entry and then you will see your settings as shown in Figure 4-38.

4.5.7.3 ARP Binding

Choose "**Advanced Setup**"→"**Security**"→"**ARP Binding**", and you will see the ARP Binding screen. This function allows you to bind network device's IP address to its MAC address, and prevents ARP spoofing and other ARP attacks.

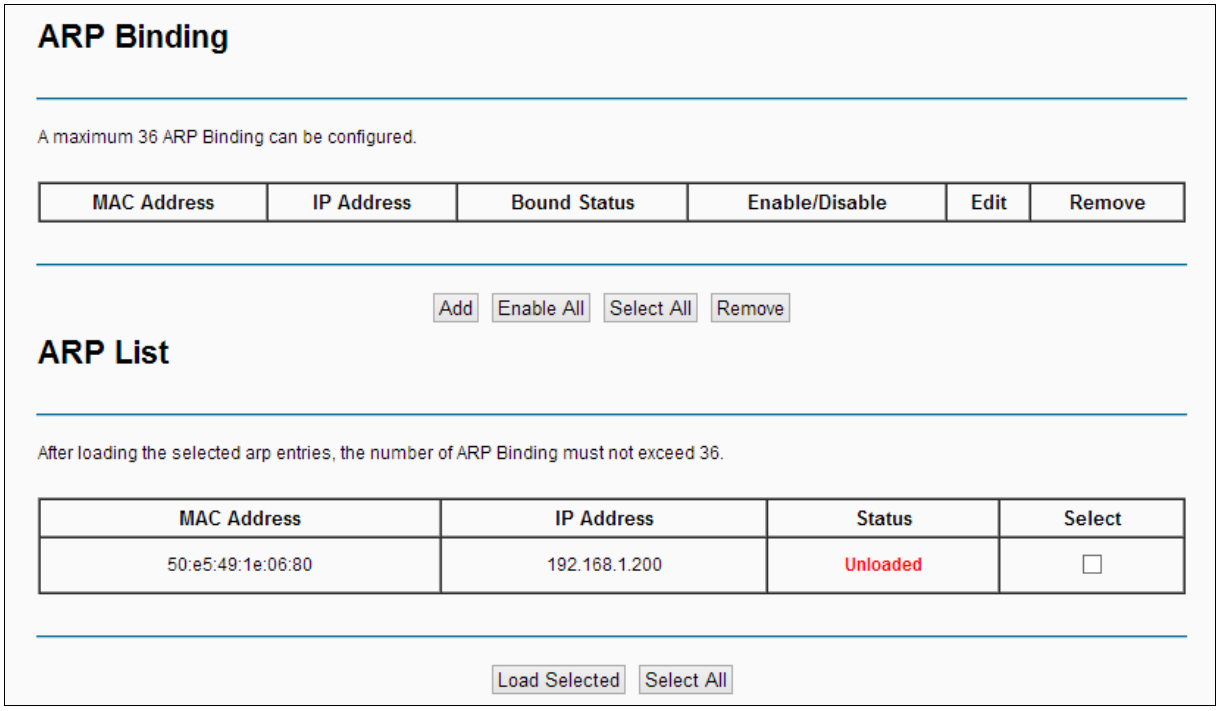


Figure 4-40

To bind a connected network device's IP address and MAC address:

1. Select the entry of the connected device's MAC Address and IP Address in ARP List as shown in Figure 4-41.

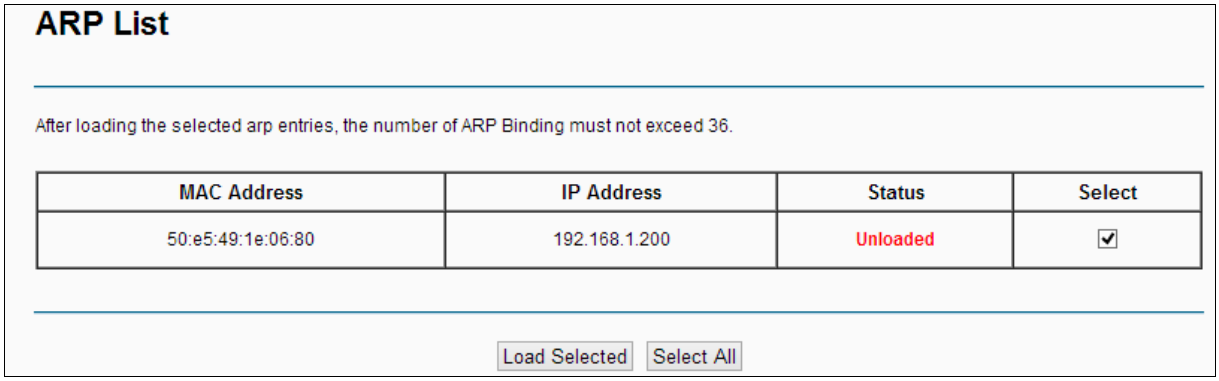


Figure 4-41

2. Click **Load Selected** and the device's information will appear on the ARP Binding table as shown in Figure 4-42.

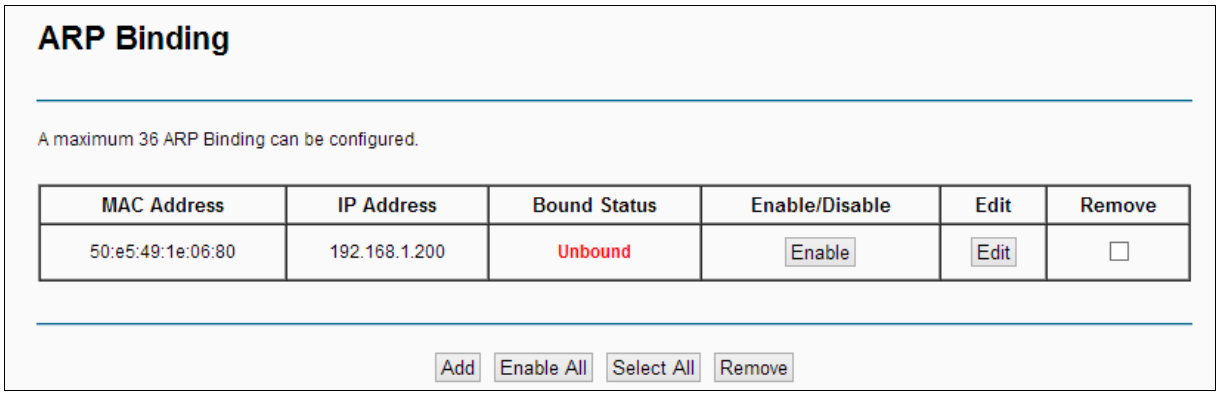


Figure 4-42

3. Click **Enable** to bind the device's MAC address to its IP address.

To manually bind a network device's IP address and MAC address:

1. Click the **Add** button in Figure 4-40, and then you will see the next screen as shown in Figure 4-43.

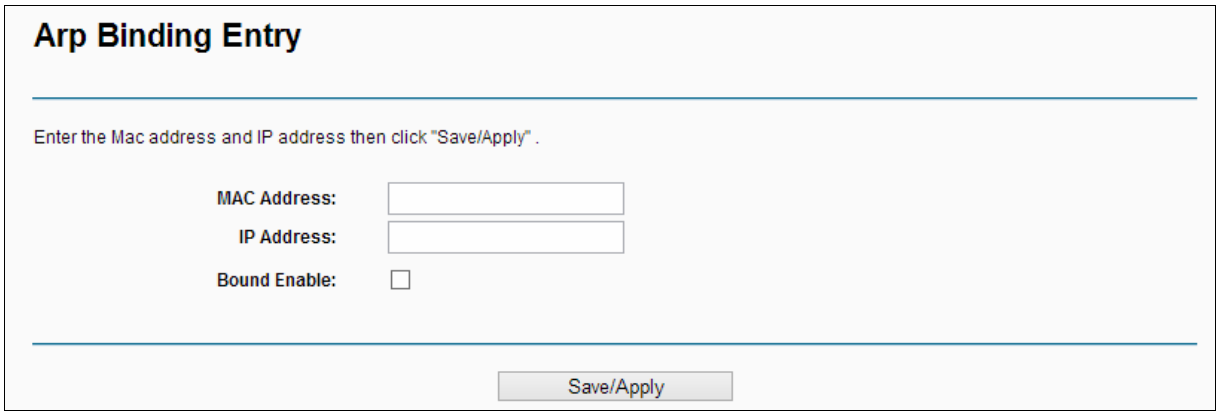


Figure 4-43

2. Enter the **MAC Address** and **IP Address** of the network device.
3. Tick **Bound Enable** to enable this entry.
4. Click **Save/Apply** to save this entry and then you will see your settings as shown in Figure 4-40.

4.5.8 Parental Control

Choose "**Advanced Setup**"→"**Parental Control**", and you will see the Parental Control screen including Time Restriction and URL Filter. Time Restriction allows you to control the Internet activities of the child by restricting the time of surfing. URL Filter limits every computer connected to the modem router to access certain websites. These two features work independently.

4.5.8.1 Time Restriction

This feature allows you add time of day restriction to a special LAN device connected to the modem router.

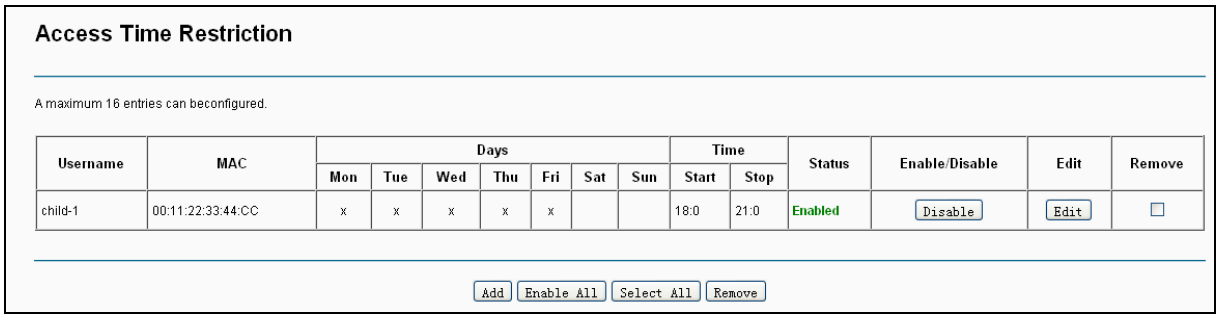


Figure 4-44

To add a Time Restriction entry:

1. Click the **Add** button in Figure 4-44, and then you will see the next screen as shown in Figure 4-45.

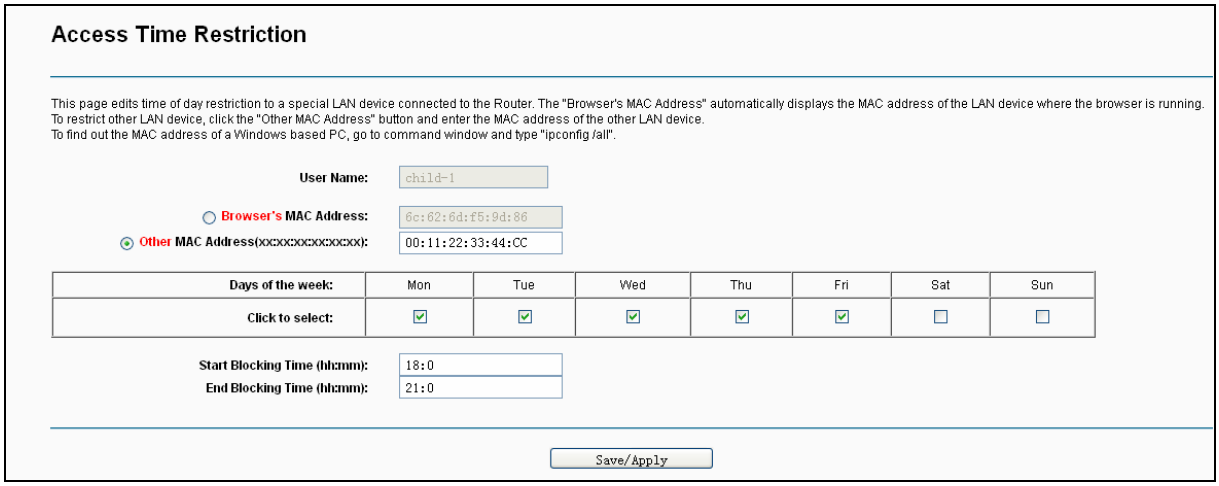


Figure 4-45

2. Enter the **User Name** of the LAN device connected to the modem router.
3. To restrict the device where the browser is running, select the **Browser's MAC Address** radio button. The MAC Address has been automatically displayed in the text box. To restrict other LAN devices, click **Other MAC Address** radio button and enter the MAC address of the other LAN device.
4. Select the day to allow the rule to take effect in the table.
5. Enter the **Start Blocking Time** and **End Blocking Time** in the text box separately, and then the device controlled will then be unable to connect to the internet during that time.
6. Click **Save/Apply** to save this entry and then you will see your settings as shown in Figure 4-44.

Note:

The Time Restriction will not work correctly before the time of the device is set in "**Management → Internet Time**".

4.5.8.2 URL Filter

This feature allows you to configure the filter rules based on URL to control all the computers in the LAN to access the specified port, and it is independent with Time Restriction feature.

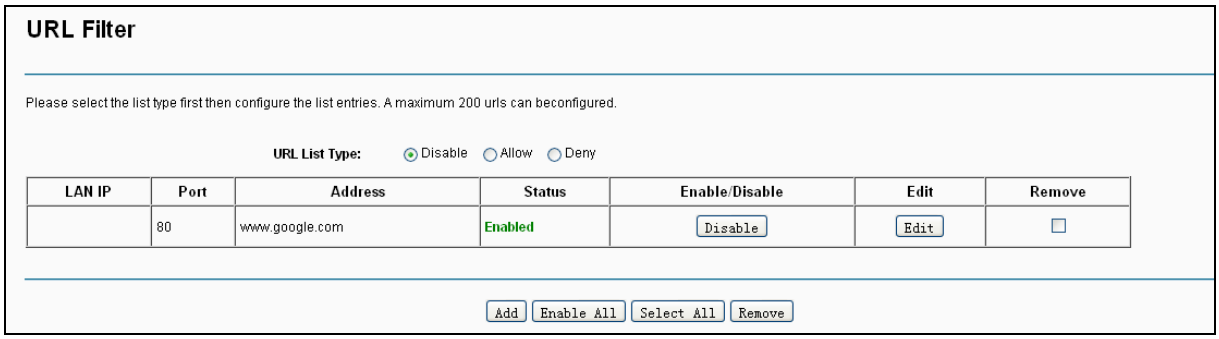


Figure 4-46

There are three policies for the URL Filter.

- **Disable**: URL Filter function will not take effect.
- **Allow**: Only allow the PCs to access the specified URL.
- **Deny**: Block the PCs to access the specified URL.

To add a URL Filter entry:

1. Check the **Deny** or **Allow** radio button. Here we take **Deny** for example.
2. Click the **Add** button in Figure 4-46 and then you will see the next screen as shown in Figure 4-47. Enter the URL Address and Port Number.

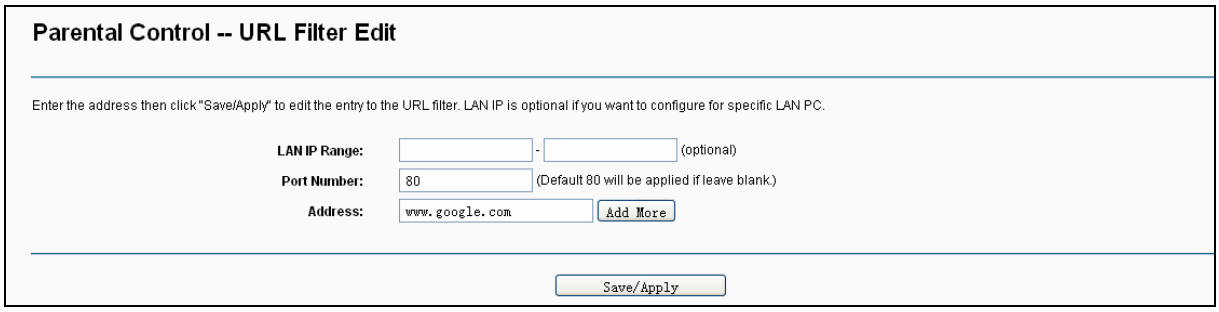


Figure 4-47

3. Click **Save/Apply** to save this entry and then you will see your settings as shown in Figure 4-46. Every computer connected to the modem router will not access this URL address on the port.

4.5.9 Quality of Service

Choose "**Advanced Setup**"→"**Quality of Service**", you can enable QoS (Quality of Service) on the screen shown in Figure 4-48. QoS helps to prioritize data as it enters your modem router. By attaching special identification marks or headers to incoming packets, QoS determines which queue the packets enter, based priority. This is useful when there are certain types of data you want to give higher priority, such as voice data packets give higher priority than Web data packets. This option will provide better service of selected network traffic over various technologies.

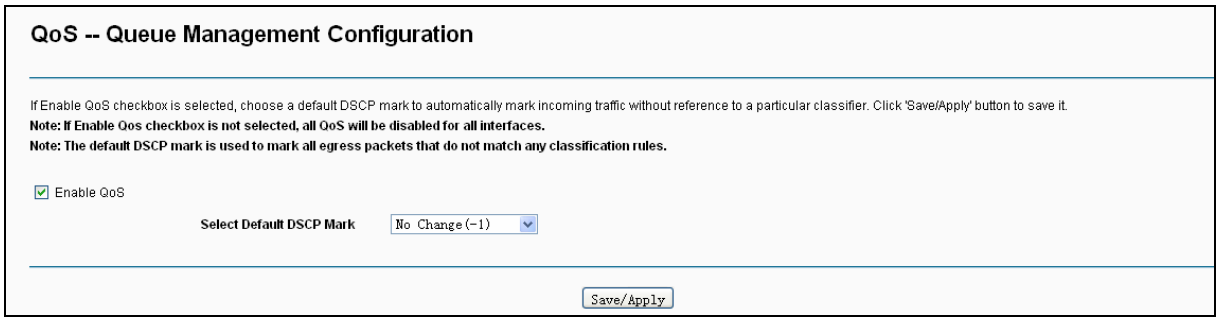


Figure 4-48

Select the **Enable QoS** checkbox to enable all QoS for all interfaces.

Select a **Default DSCP Mark** from drop-down list to automatically mark incoming traffic without reference to a particular classifier.

Click **Save/Apply** to save the current configuration.

Note:

The default DSCP mark is used to mark all egress packets that do not match any classification rules.

4.5.9.1 Queue Config

Choose "**Advanced Setup**"→"**Quality of Service**"→"**Queue Config**", you can set up virtual servers on the screen below.

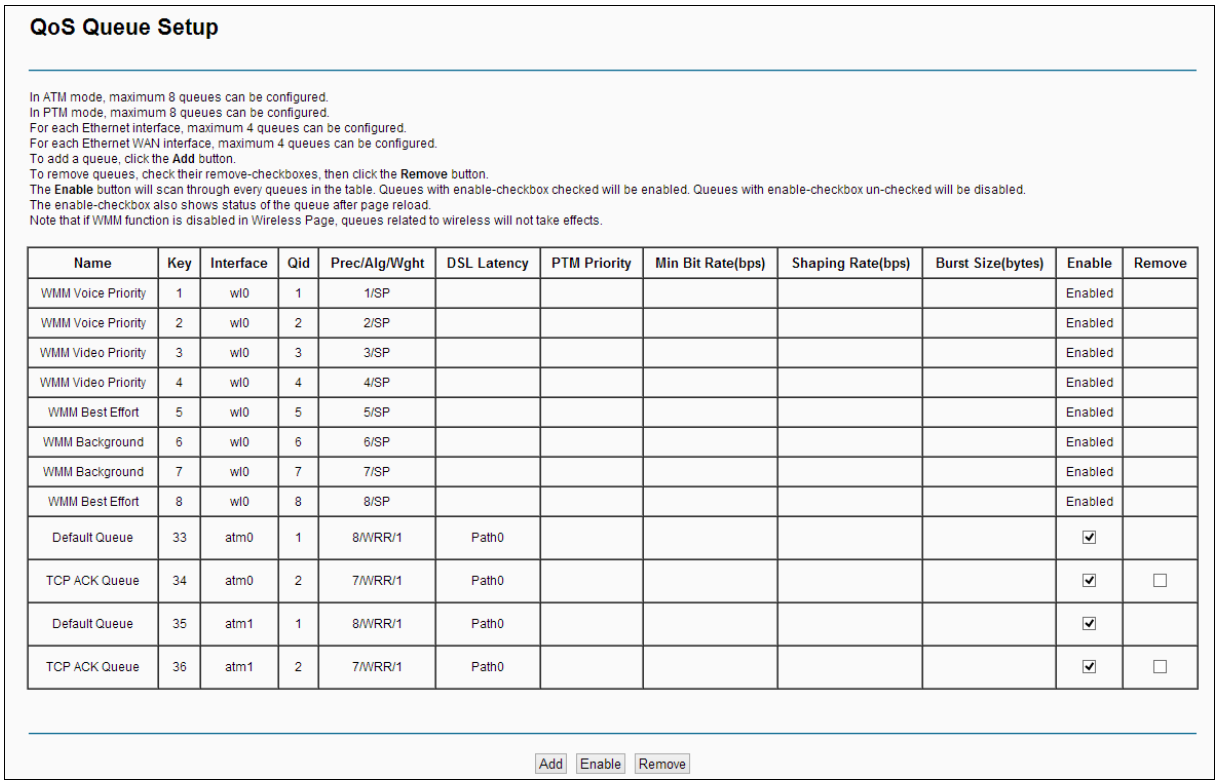


Figure 4-49

Click the **Add** button in Figure 4-49, and you can configure the QoS queue entry on the next screen as shown in Figure 4-50.

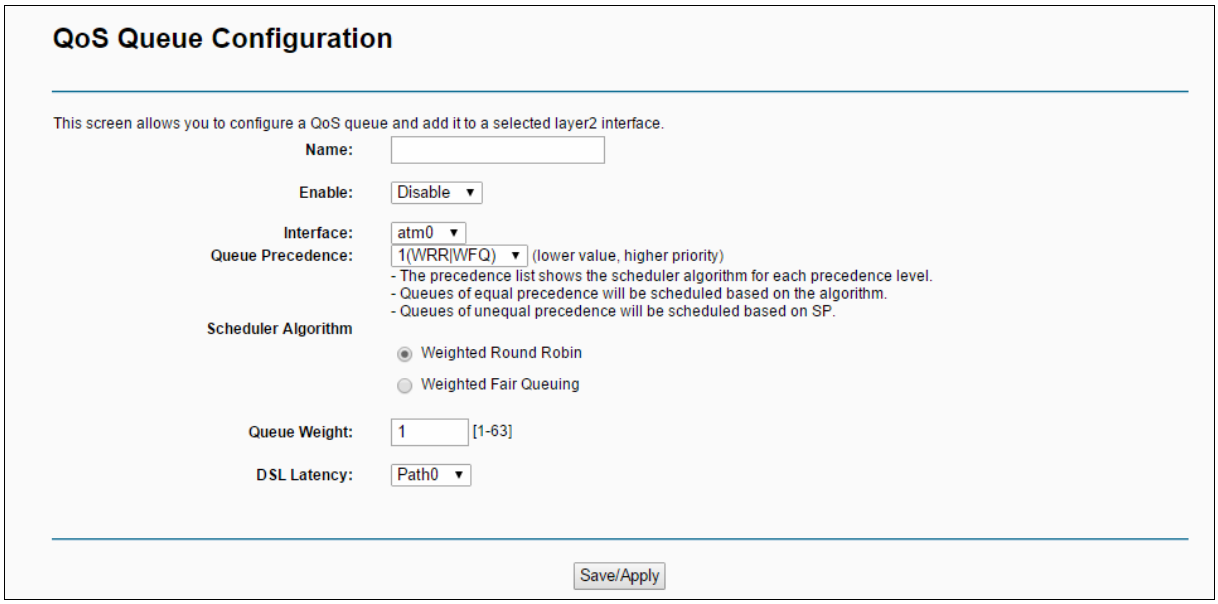


Figure 4-50

- **Name**: Set a name for the entry.
- **Enable**: Select Enable option to take this entry effect.
- **Interface**: Assigned a specific Wan Service for this QoS queue entry.
- **Queue Precedence**: Specify precedence for this QoS queue entry.
- **DSL Latency**: Select latency path for the type of data transmission, only Path0 is available for this modem router.

After you specify the condition, click **Save/Apply** to save the entry and then you will see you settings as shown in Figure 4-49.

Note:

1) Lower integer values for precedence imply higher priority for this queue relative to others.
2) The queue entry configured here will be used by the classifier to place ingress packets appropriately.

4.5.9.2 QoS Classification

This section will guide you to create a traffic class rule to classify the upstream traffic, assign queue which defines the precedence and the interface and optionally overwrite the IP header DSCP byte.

A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect.

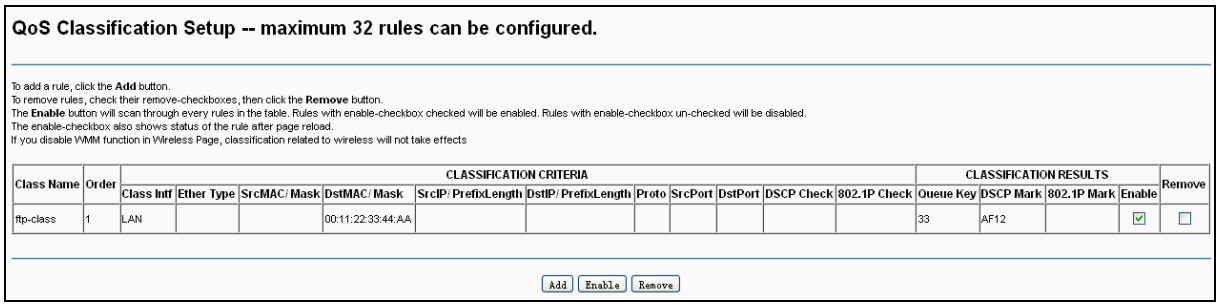


Figure 4-51

Click the **Add** button in Figure 4-51, and you can configure the QoS on the next screen.

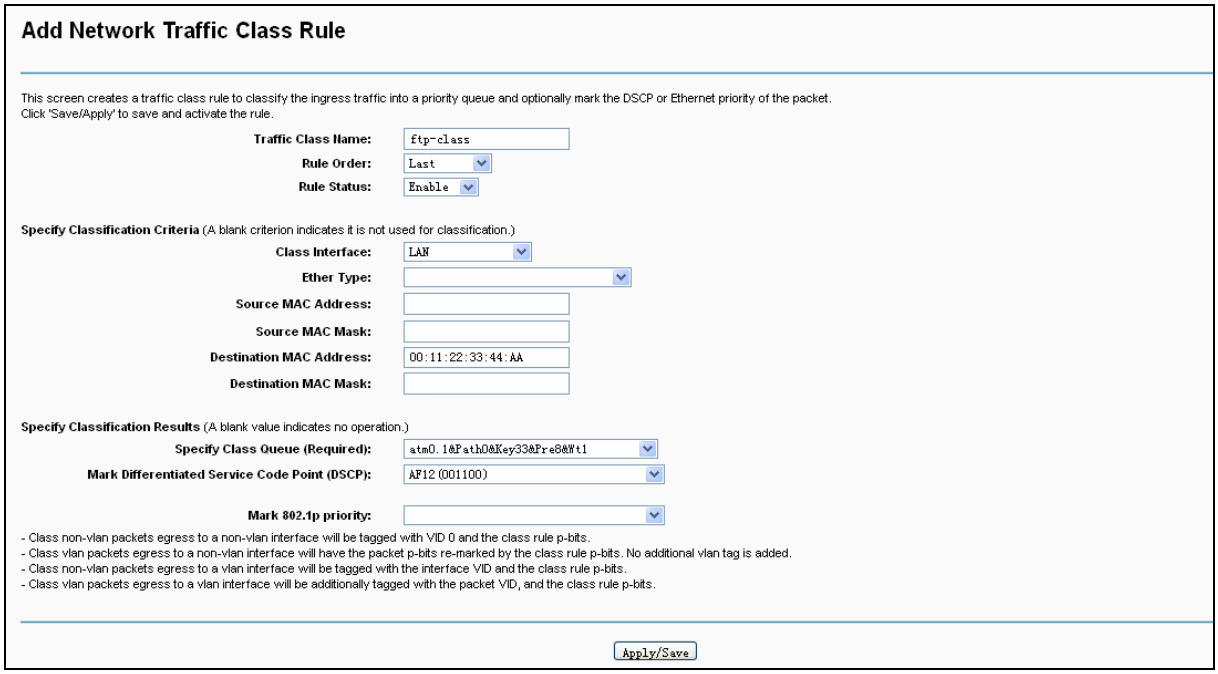


Figure 4-52

After you specify the condition, click **Save/Apply** to save the entry.

4.5.10 Bandwidth Control

Choose "**Advanced Setup**"→"**Bandwidth Control**" and then you will see the screen as shown in Figure 4-53. This page allows you to enable this function and to configure the value of Total Upstream/Downstream Bandwidth.

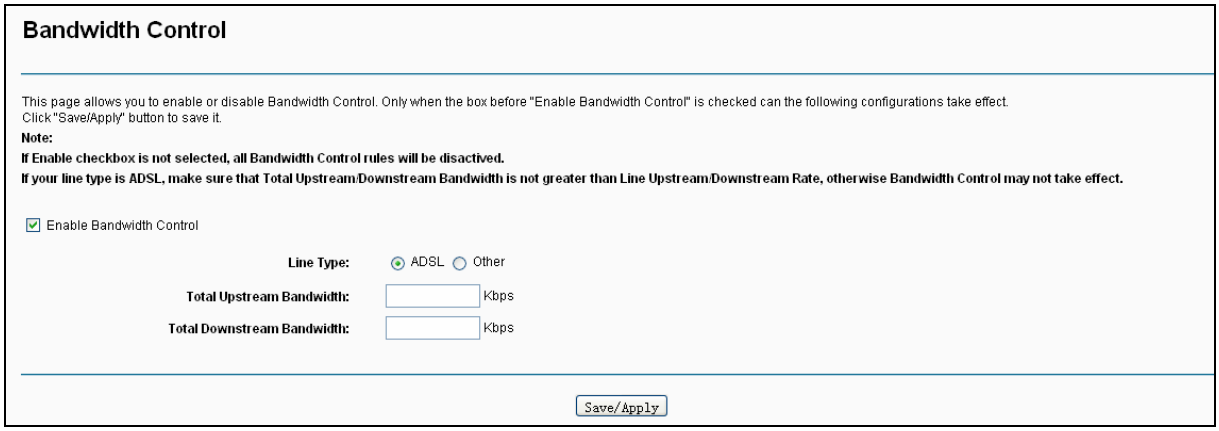


Figure 4-53

- **Enable Bandwidth Control**: Check this box to enable the Bandwidth Control function.
- **Total Upstream Bandwidth (Kbps)**: Enter the upload speed through the WAN port.
- **Total Downstream Bandwidth (Kbps)**: Enter the download speed through the WAN port.
- **Save/Apply**: Click this button to make the configuration take effect.

Note:

The Total Upstream Bandwidth and Total Downstream Bandwidth are required to be configured.

4.5.10.1 Rules List

Choose "**Advanced Setup**"→"**Bandwidth Control**" →"**Rules List**" and then you will see the screen as shown in Figure 4-54. This page allows you to view and configure TC rules.

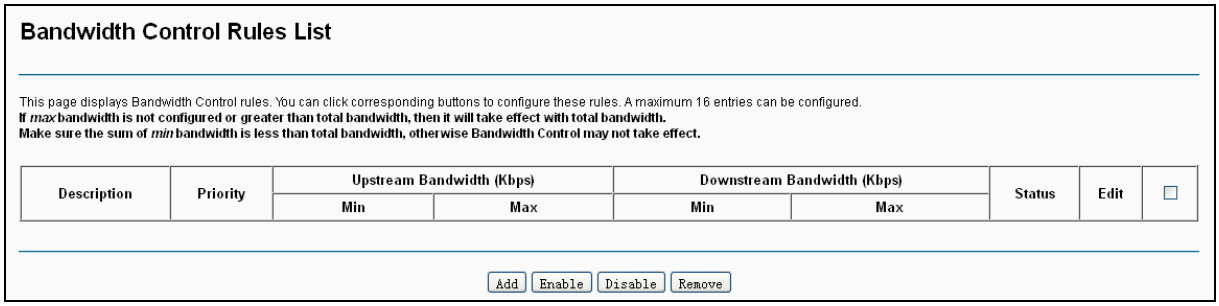


Figure 4-54

To add a TC rule, click the **Add** button and you can configure it in the screen as shown in Figure 4-55.

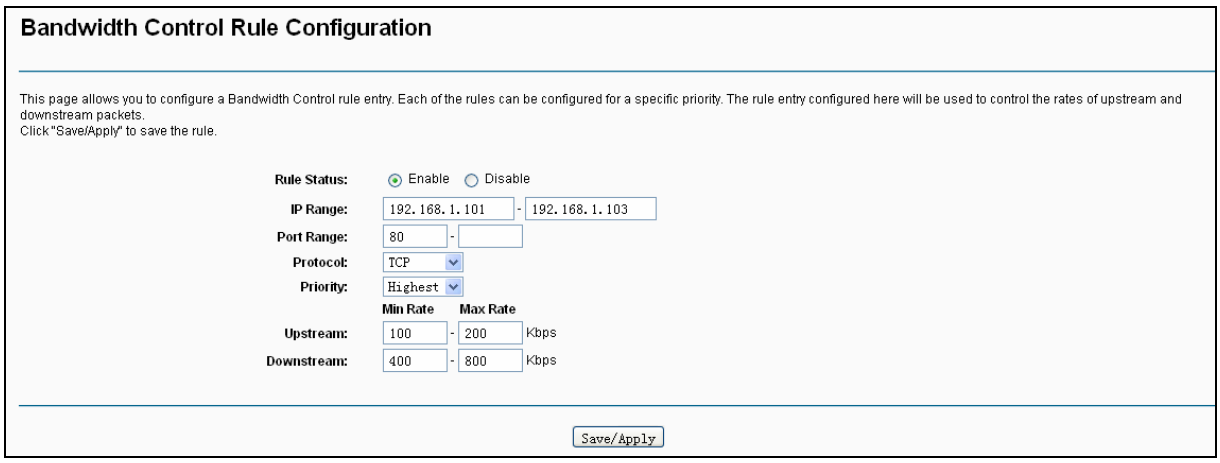


Figure 4-55

- **Rule Status**: Select the status of the rule from the drop-down list to enable or disable the rule.
- **IP Range**: Enter a single IP address or a range of IP addresses.
- **Port Range**: Enter a single port or a range of ports.
- **Protocol**: Select a protocol type from the drop-down list. TCP, UDP and ALL are available here.

- **Priority**: Select priority form the drop-down list. There are five options: Highest, 1, 2, 3, 4, 5, 6 and Lowest. The default precedence of the rule is 4.
- **Upstream**: Enter the min and max upload speed through the WAN port.
- **Downstream**: Enter the min and max download speed through the WAN port.

After completing the above configuration, click the **Save/Apply** button to make it take effect and then you will see the following list as shown in Figure 4-56. If you want to modify the rule, click the **Edit** button. If you want to delete the rule, check the **Remove** box first and then click the **Remove** button.

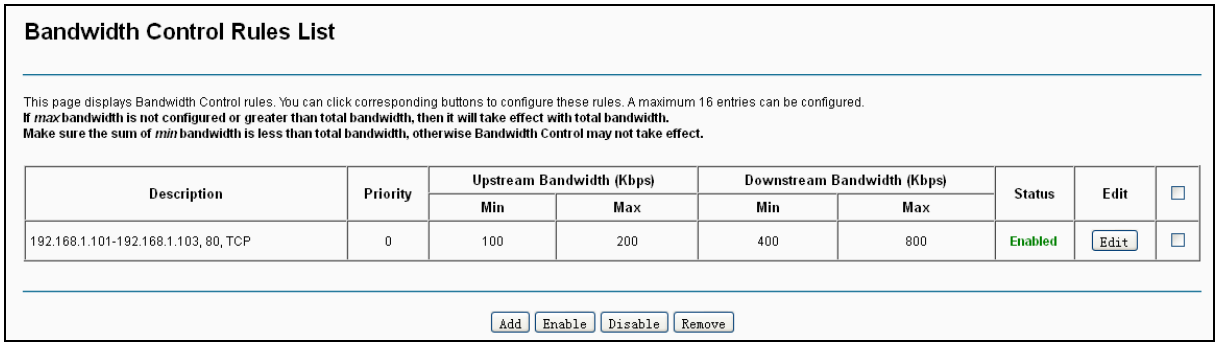


Figure 4-56

Note:

The priority, max upstream/downstream rate and min upstream/downstream rate work on allocation of surplus upload/download bandwidth. For rules with different priority, the surplus bandwidth is firstly allocated to the rule with the highest priority according to its max upstream/downstream rate. If there still has surplus bandwidth, it is allocated to the rule with hypo-high priority. For rules with the same priority, the surplus bandwidth is allocated to them according to their min upstream/downstream rate. The greater a rule's min upstream/downstream rate is, the more bandwidth it gets.

4.5.11 Routing

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

4.5.11.1 Default Gateway

Choose "**Advanced Setup**"→"**Routing**"→"**Default Gateway**", you can see the Default Gateway screen.

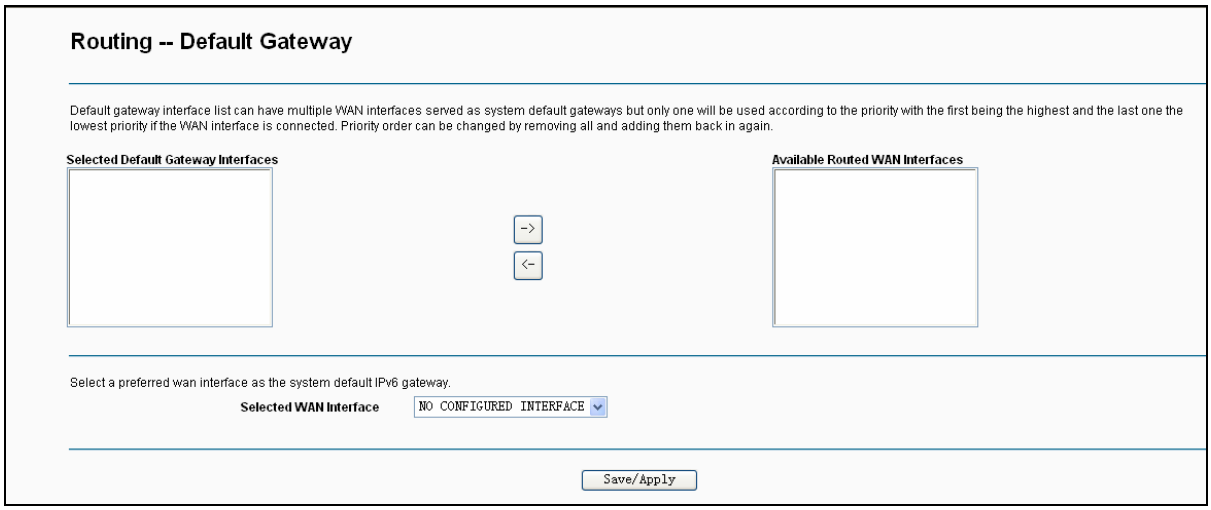


Figure 4-57

4.5.11.2 Static Route

Choose "**Advanced Setup**"→"**Routing**"→"**Static Route**". You can see the Static Route screen, this screen allows you to configure the static routes (shown in Figure 4-58). A static route is a pre-determined path that network information must travel to reach a specific host or network.

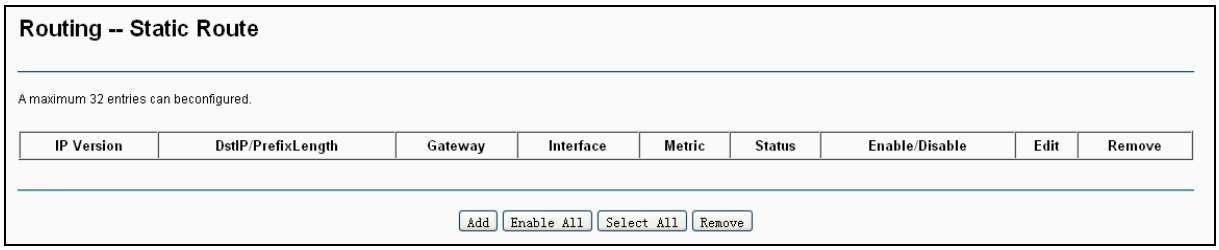


Figure 4-58

To add static routing entries:

1. Click the **Add** button in Figure 4-58, and you will see the screen as shown in Figure 4-59.

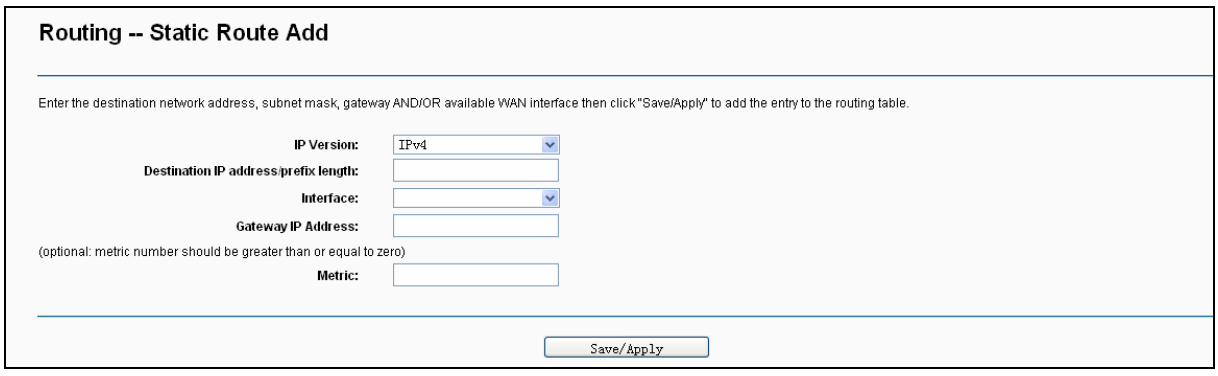


Figure 4-59

2. Enter the following data:

- **IP Version:** Select the version of IP.
- **Destination IP Address/prefix length:** The **Destination IP Address** is the address of the network or host that you want to assign to a static route.

- **Interface:** Select the Interface name in the text box, or else, the default Use Interface will be adopted for the Static Route.
- **Gateway IP Address:** If you select the IPoE or IPoA mode for **Interface**, the screen above will display this item, you should type the Gateway address correctly, and the other option for **Interface** will adopt the default Gateway address for the Static Route.

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

Note:

Gateway IP address should be correctly configured if IP based Interface (IPoE, IPoA) is selected.

4.5.11.3 RIP

Choose "**Advanced Setup**"→"**Routing**"→"**RIP**", you can see the screen as shown in Figure 4-60.

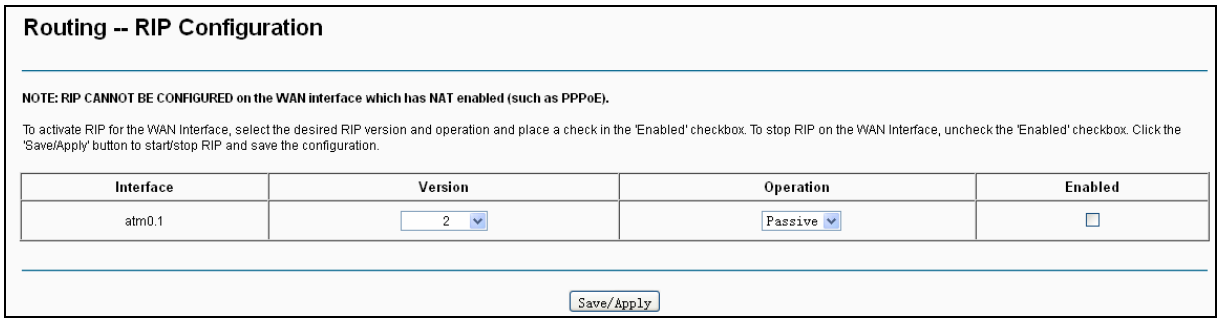


Figure 4-60

Note:

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

4.5.12 DNS

When you select the connection type **PPPoE**, **PPPoA** or **IPoA** for WAN configuration, you will see the **DNS** menu which includes **DNS Server** and **Dynamic DNS** submenus.

4.5.12.1 DNS Server

Choose "**Advanced Setup**"→"**DNS**"→"**DNS Server**", and you can see the **DNS Server Configuration** screen as shown in Figure 4-61.

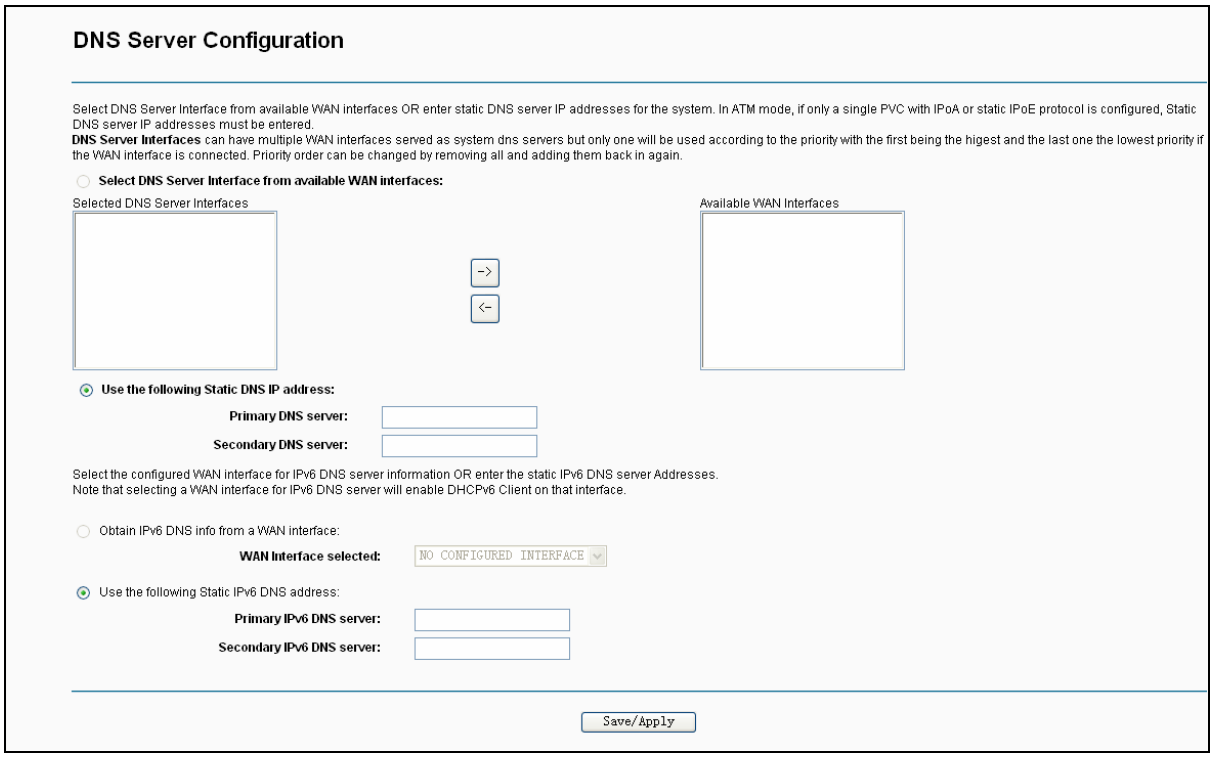


Figure 4-61

For PPPoA, PPPoE enabled PVC(s), please select the **Select DNS Server Interface from available WAN interfaces** checkbox, this modem router will accept automatically the first received DNS assignment from the selected configured WAN interface during the connection establishment.

For single PVC with IPoA, static IPoE protocol, please select the **Use the following Static DNS IP address** checkbox, and enter the primary and /or optional secondary DNS server IP addresses provided by your ISP.

Here you can also select a configured WAN interface for IPv6 DNS server or enter the static IPv6 DNS server Addresses provided by your ISP.

Click the **Save/ Apply** button to save the new configuration.

4.5.12.2 Dynamic DNS

Choose "**Advanced Setup**"→"**DNS**"→"**Dynamic DNS**", you can see the **Dynamic DNS** screen, this screen allows you to configure the Dynamic DNS (shown in Figure 4-62).

The modem router offers a Dynamic Domain Name System (**DDNS**) feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP Address. The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your modem router to be more easily accessed from various locations on the Internet.

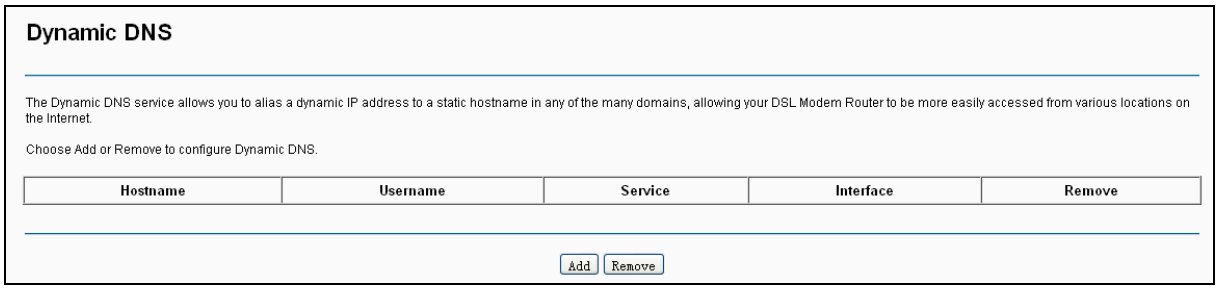


Figure 4-62

To add a DDNS entry:

1. Click the **Add** button (pop-up after Figure 4-62), and then you will set the DDNS in the next screen (shown in Figure 4-63).

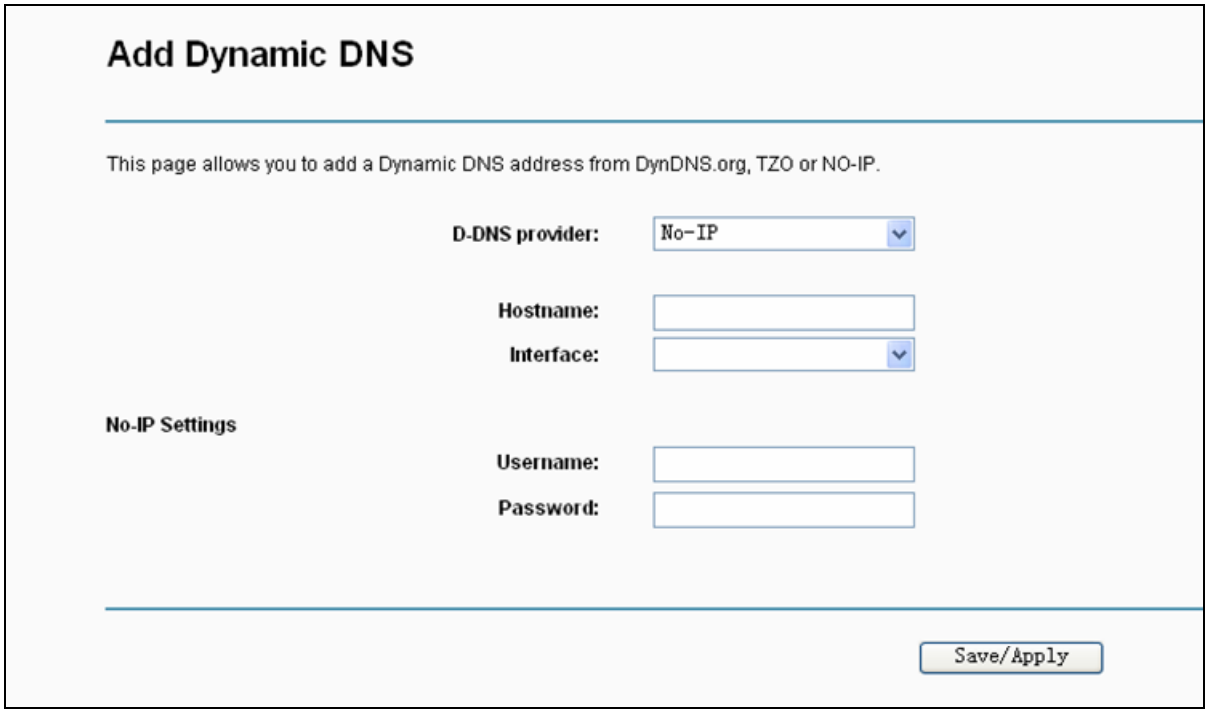


Figure 4-63

2. Select **D-DNS provider** in the drop-down list.
3. Enter the **Hostname** of the DNS Server, and select the corresponding **Interface** for the DDNS, you can leave it default.
4. Type the **User Name** and **Password** for your DDNS account.

Click **Save/Apply** to save your settings.

4.5.13 DSL

Choose "**Advanced Setup**"→"**DSL**", you can see the DSL Settings screen, this screen allows you to configure the DSL (shown in Figure 4-64).

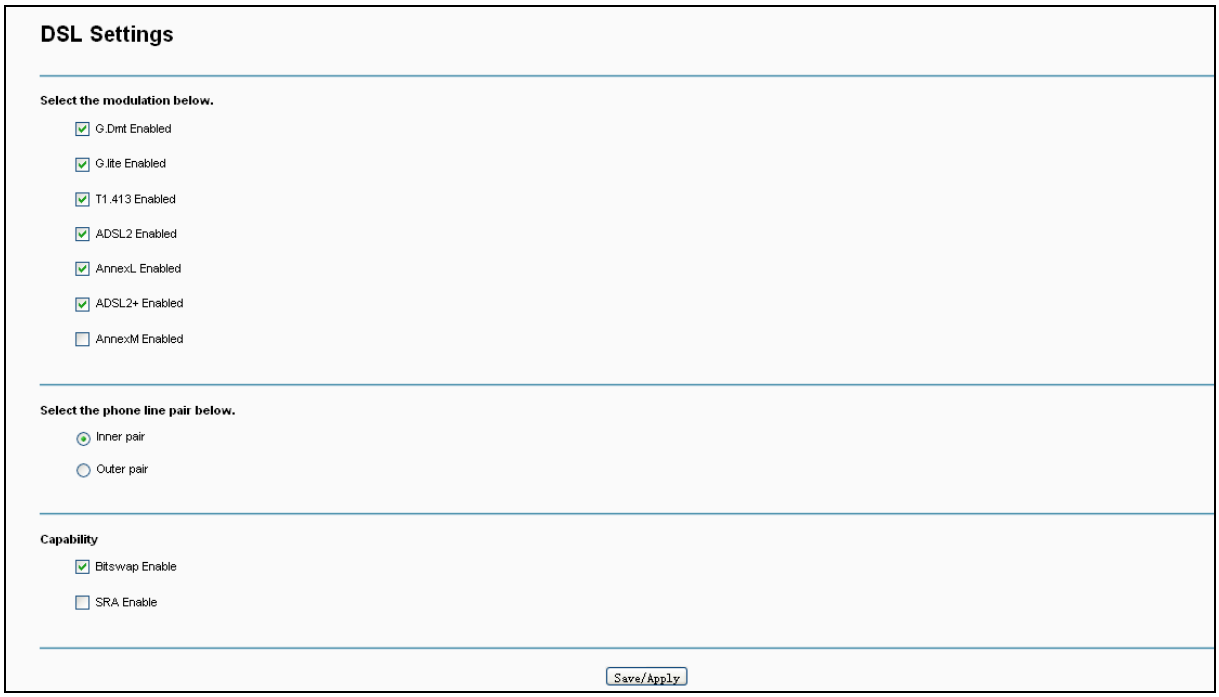


Figure 4-64

You can select the modulation type, phone line pair and the capability of Bitswap or SRA. After you set them up, click **Save/Apply** to save the configurations.

4.5.14 UPnP

Choose "**Advanced Setup**"→"**UPnP**", you can Enable or Disable the UPnP (Universal Plug and Play) protocol on the screen.

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

Figure 4-65

Select the checkbox and click **Save/Apply** to enable the UPnP function.

4.5.15 Interface Grouping

Choose "**Advanced Setup**"→"**Interface Grouping**", you can configure multiple ports to PVC and bridging groups to perform as an independent network.

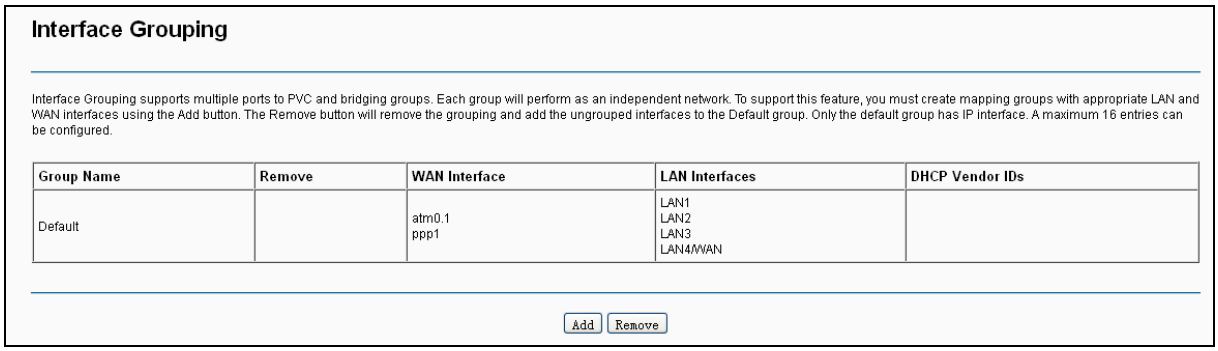


Figure 4-66

To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the **Add** button. The **Remove** button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

To create a new interface group:

1. Click the **Add** button. You can add a new interface group in the next screen.

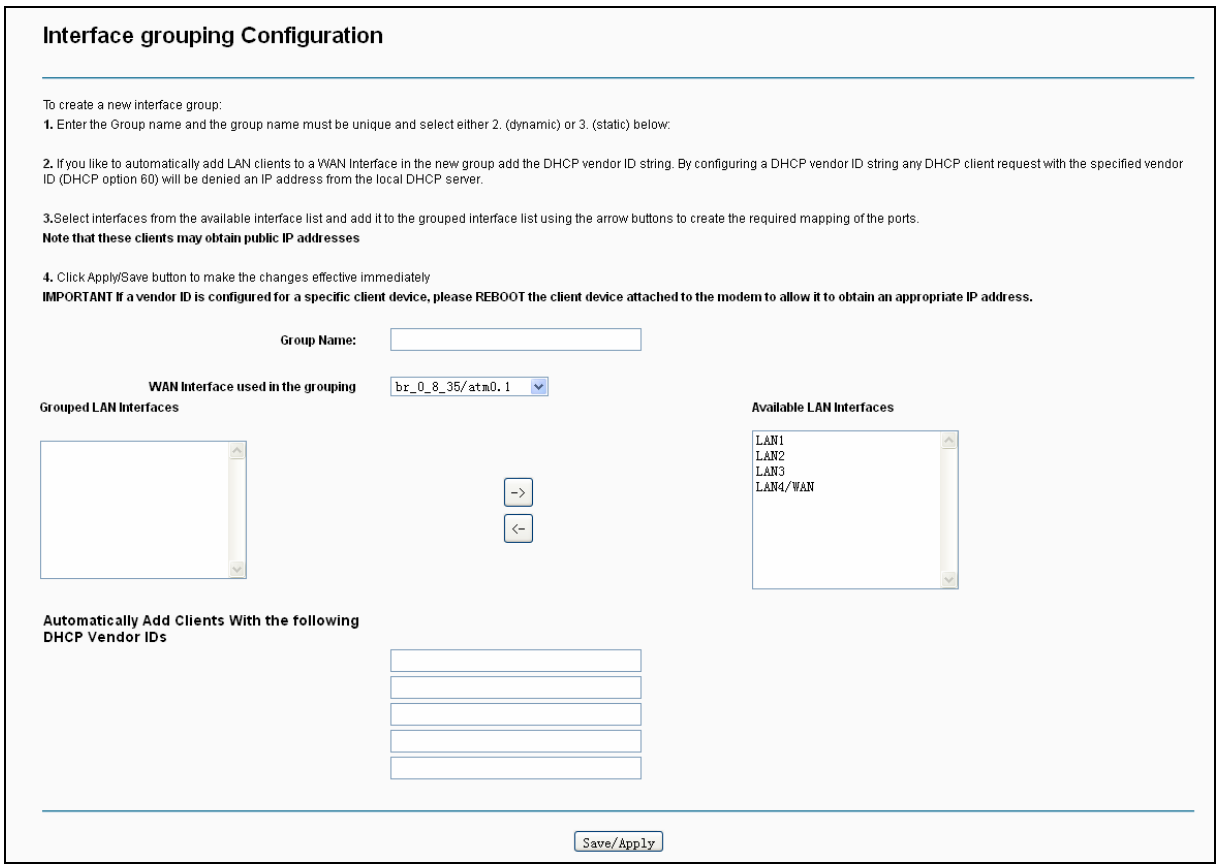


Figure 4-67

2. Enter a unique name for Group.
3. Select the Interface which you want to use from the drop-down list.

Note:

If you like to automatically add LAN clients to a WAN Interface in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the

specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.

4. Select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports.

☞ **Note:**

These clients may obtain public IP addresses.

5. Click **Save/Apply** to make the entry effective immediately.

☞ **Note:**

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

4.5.16 IP 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 "**Advanced Setup**"→"**IP Tunnel**", it includes two menus**: IPv6inIPV4 and IPv4inIPv6**, The detailed descriptions are provided below.

4.5.16.1 IPv6inIPv4

Choose "**Advanced Setup**"→""**IP Tunnel**"→"**IPv6inIPv4**", you can see the 6in4 tunnel configuration screen. This screen allows you to configure the static routes (shown in Figure 4-68).

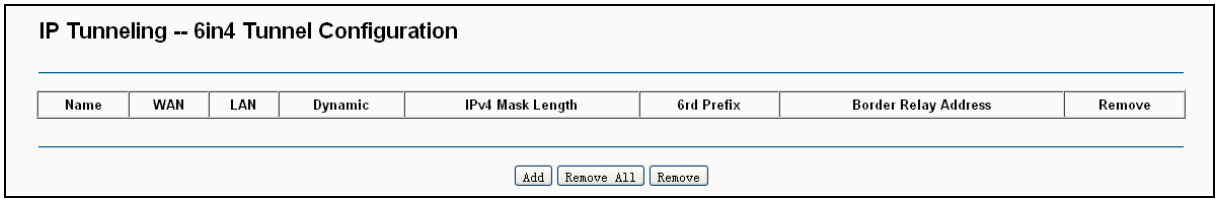


Figure 4-68

Click the **Add** button in Figure 4-68, and you can configure the 6in4 tunnel on the next screen as shown in Figure 4-69.

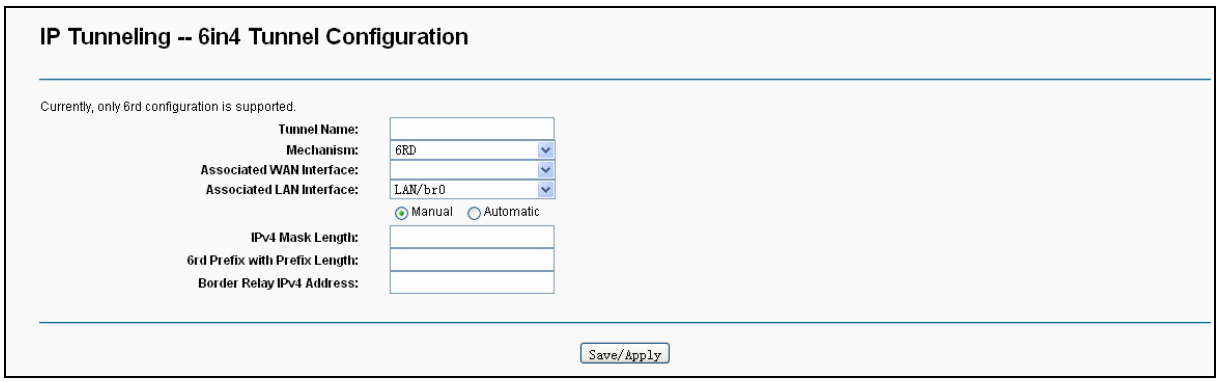


Figure 4-69

- **Mechanism:** 6RD, this type is used in the situation that your WAN connection is IPv4 while LAN connection is IPv6.

- **Associated WAN Interface:** Select a WAN connection from the drop-down list. Only the connected WAN connections can be shown in the drop-down list.
- **Associated LAN Interface:** Select a LAN connection from the drop-down list. Only the connected LAN connections can be shown in the drop-down list.
- **IPv4 Mask Length:** The length of the selected WAN connection's IPv4 mask.
- **6rd Prefix with Prefix Length:** The length of the 6rd prefix.
- **Border Relay IPv4 Address:** The IPv4 address of the border relay router of 6RD tunnel.

Click **Save/Apply** to make the configuration take effect.

Note:

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

4.5.16.2 IPv4inIPv6

Choose "**Advanced Setup**"→""**IP Tunnel**"→"**IPv4inIPv6**". You can see the 4in6 tunnel configuration screen, this screen allows you to configure the static routes (shown in Figure 4-70).

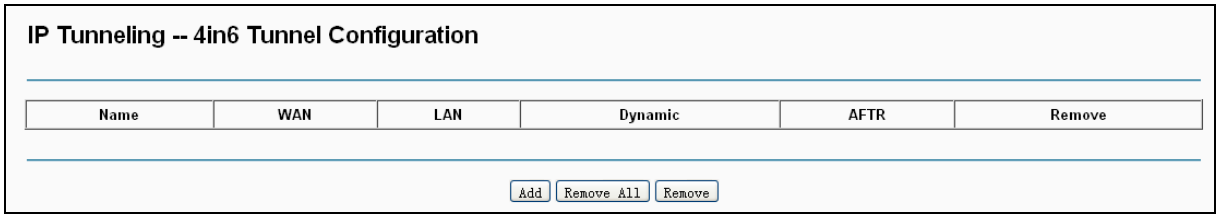


Figure 4-70

Click the **Add** button in Figure 4-70, and you can configure the 6in4 tunnel on the next screen as shown in Figure 4-71.

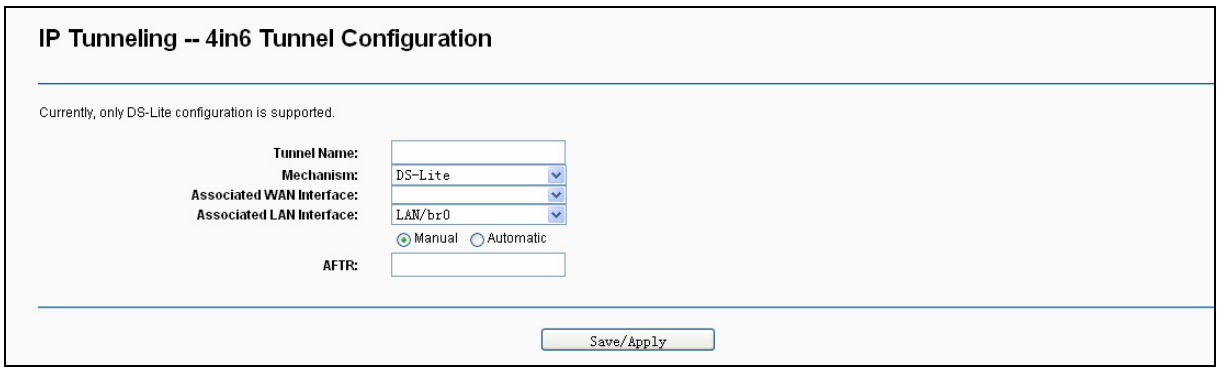


Figure 4-71

- **Mechanism:** DS-Lite, this type is used in the situation that your WAN connection is IPv6 while LAN connection is IPv4.
- **Associated WAN Interface:** Select a WAN connection from the drop-down list. Only the connected WAN connections can be shown in the drop-down list.
- **Associated LAN Interface:** Select a LAN connection from the drop-down list. Only the connected LAN connections can be shown in the drop-down list.
- **AFTR:** Enter the IPv6 address of the remote node.

Click **Save/Apply** to make the configuration take effect.

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.

4.5.17 IPSec

Choose "**Advanced Setup**"→"**IPSec**", you can Add/Remove or Enable/Disable the IPSec tunnel connections on the screen as shown in Figure 4-72.

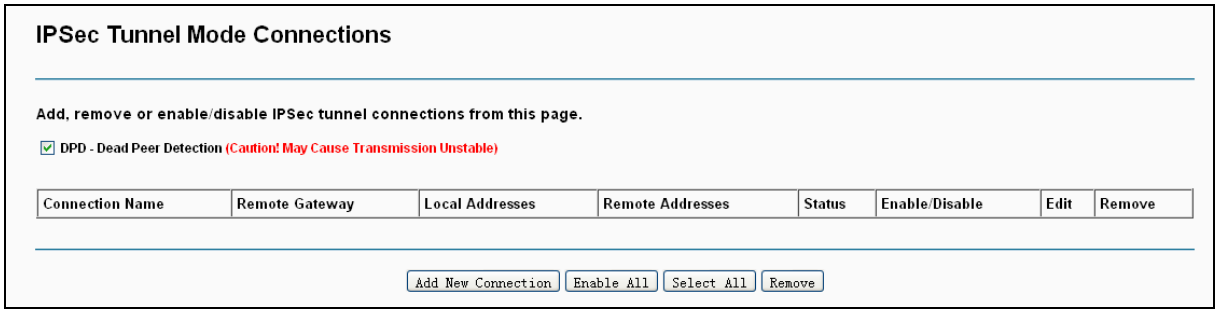
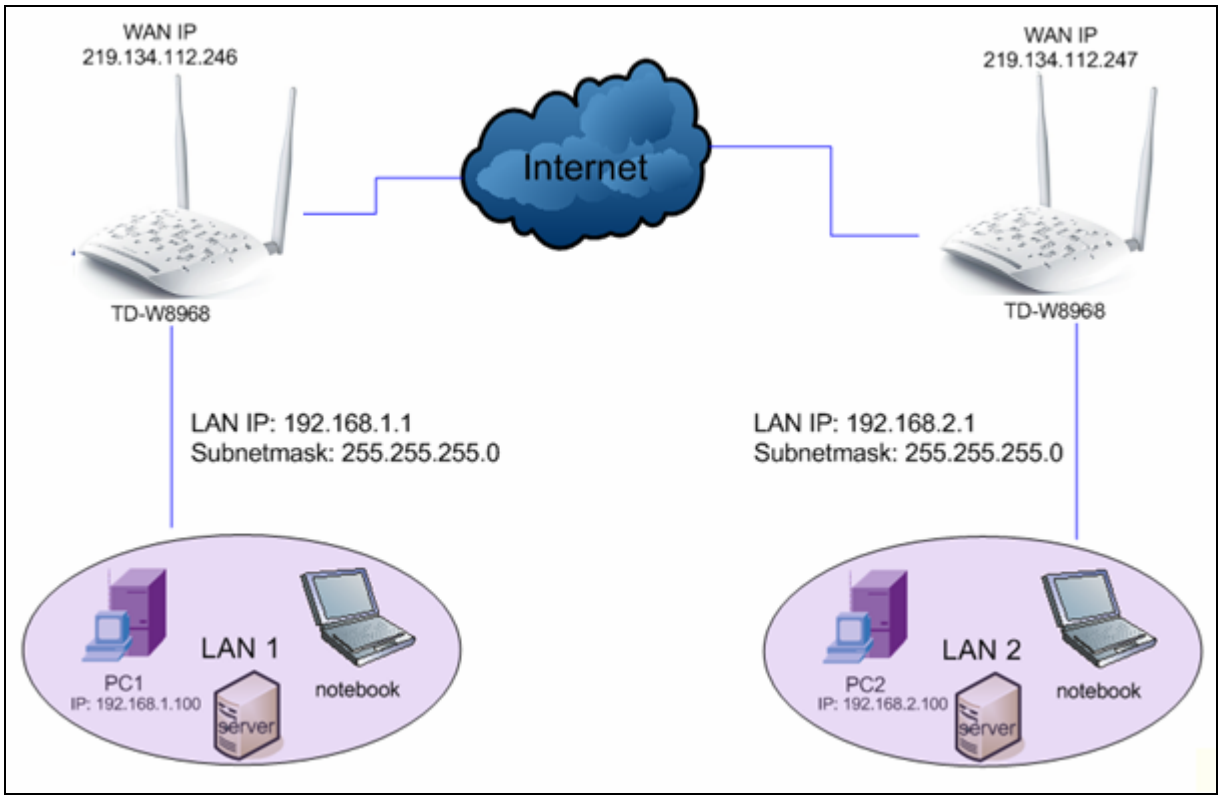


Figure 4-72

This section will guide you to configure a VPN tunnel between two TD-W8968s. The topology is as follows.



Note:

You could also use other VPN routers to set VPN tunnels with TD-W8968. TD-W8968 supports up to 10 VPN tunnels simultaneously.

Click **Add New Connection** in Figure 4-72 and then you will enter the screen shown in Figure 4-73.

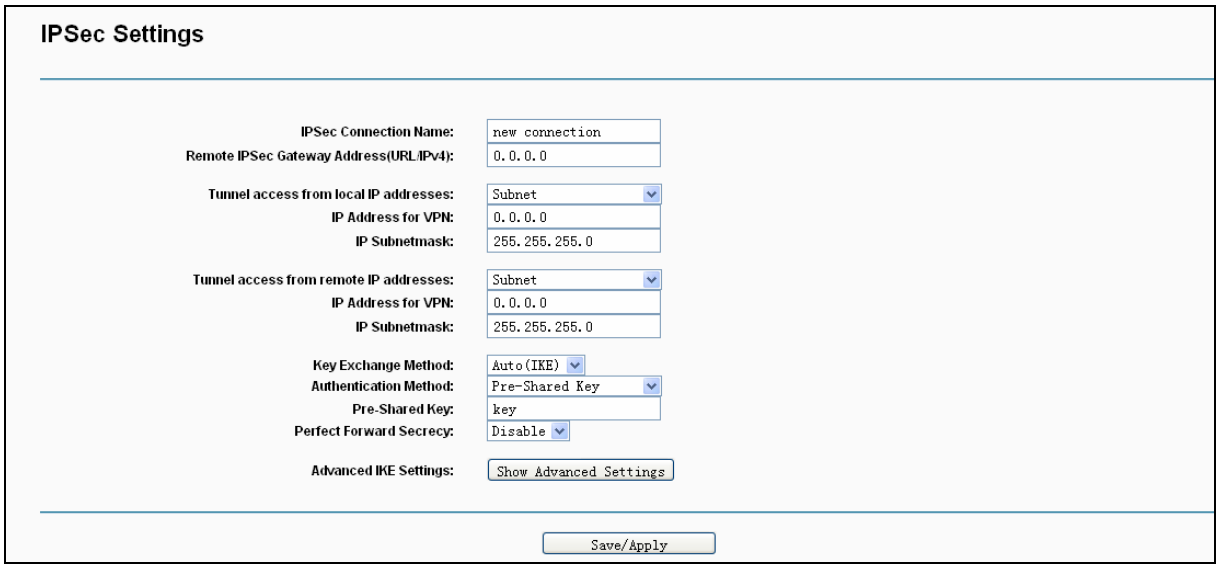


Figure 4-73

- **IPSec Connection Name:** Enter a name for your VPN.
- **Remote IPSec Gateway Address (IP or Domain Name):** Enter the destination gateway IP address in the box 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.

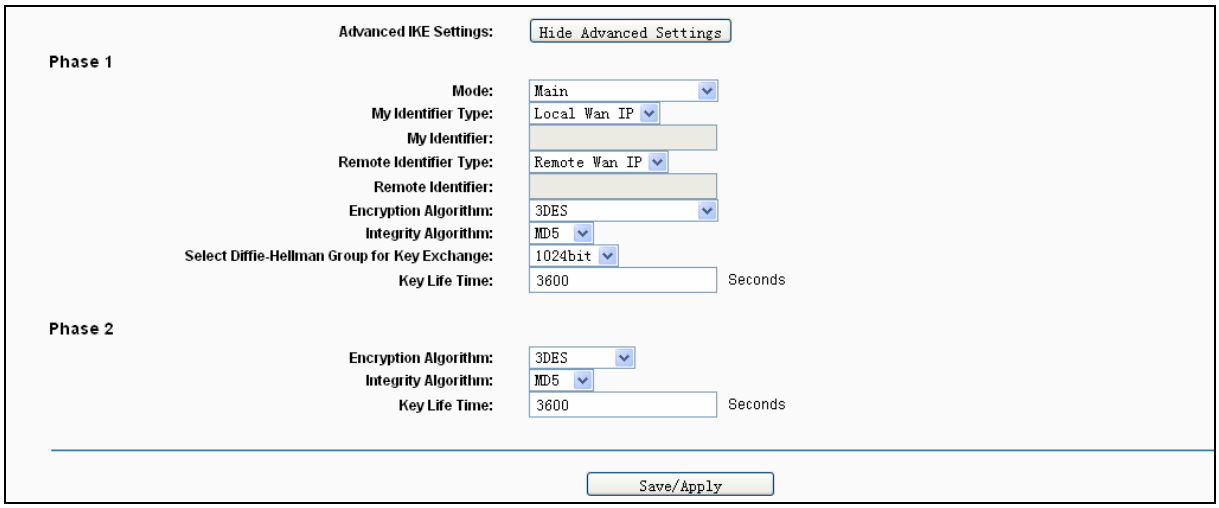
We recommend you leave the Advanced Settings as default value.

After complete the basic settings and click Save/Apply in both **Device1** and **Device2**, PCs in LAN1 could conmmunicate 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.



- **Main Mode:** Select Main Mode to configure the standard negotiation parameters for IKE phase1.
- **Aggressive Mode:** 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 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**.

4.5.18 Multicast

Choose "**Advanced Setup**"→"**Multicast**", you can configure the IGMP protocol on the screen.

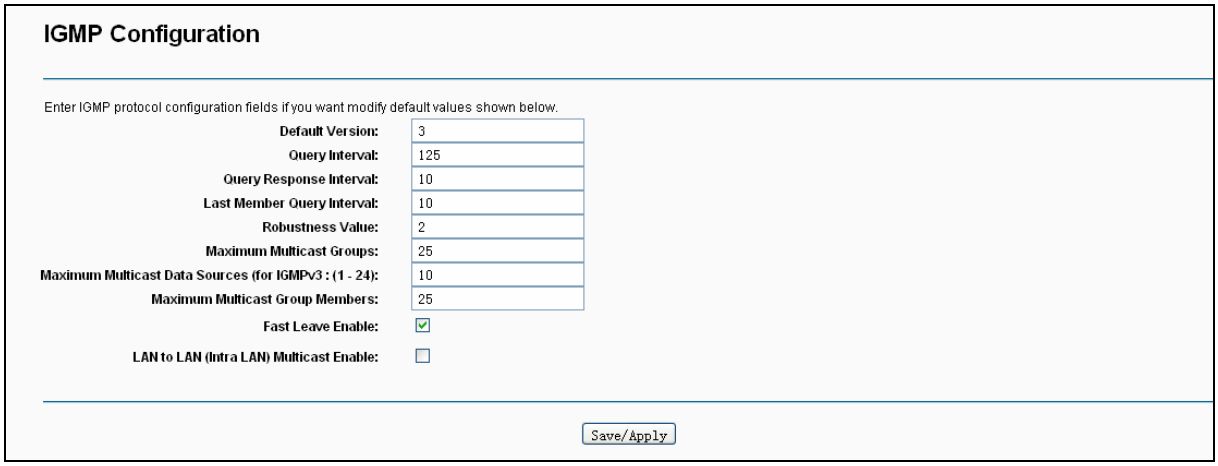


Figure 4-74

Click **Apply/Save** to save your settings.

4.6 IPTV

Choose "**IPTV**", and you will see the screen as shown in Figure 4-75.

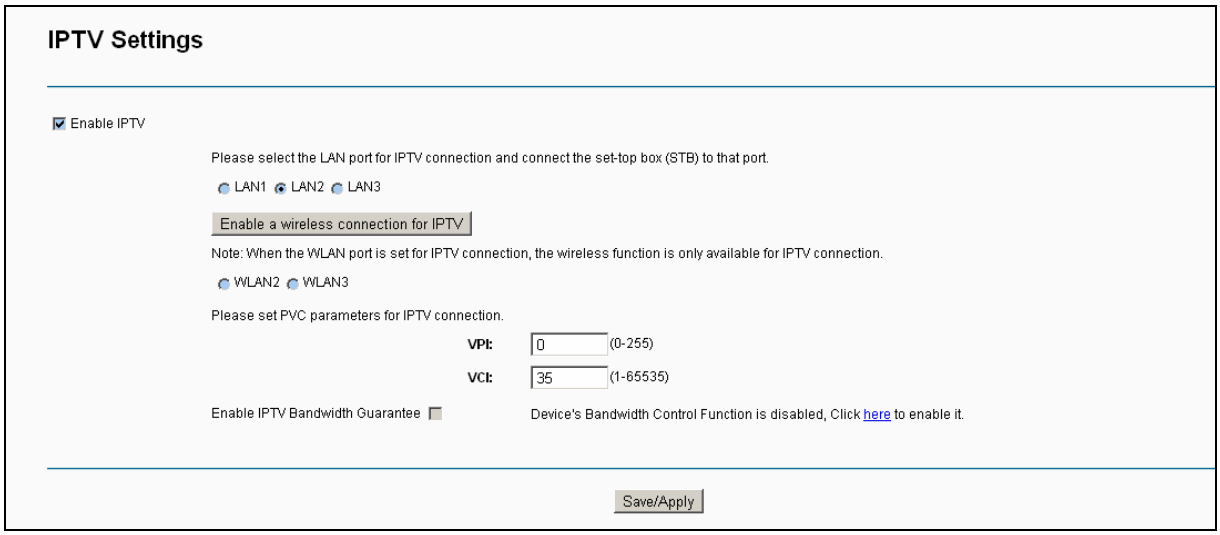


Figure 4-75

- **Enable IPTV:** Check this box to enable IPTV. If this checkbox is selected, please set the following parameters as shown in the figure below. Make sure the following settings are correct.
- **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/Apply** button to save your settings.

To add a wireless connection for IPTV:

1. Click the **Enable a wireless connection for IPTV** button. Then Figure 4-76 will pop up.
2. Configure the settings please refer to Section 4.7.1 Basic.

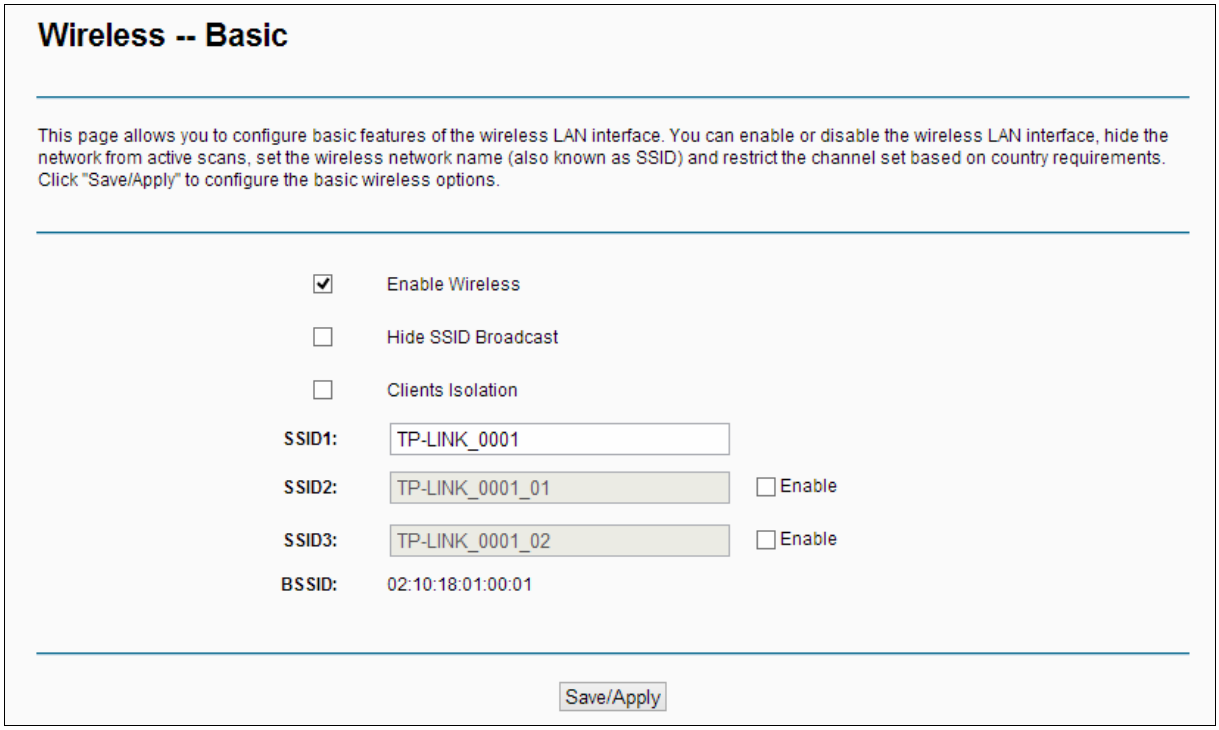


Figure 4-76

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

4.7 Wireless

Choose "**Wireless**", there are six submenus to configure Wireless LAN settings. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.7.1 Basic

Choose "**Wireless**"→"**Basic**", you will see the screen of **Wireless--Basic** settings shown as below. The basic settings for wireless networking are set on this screen.

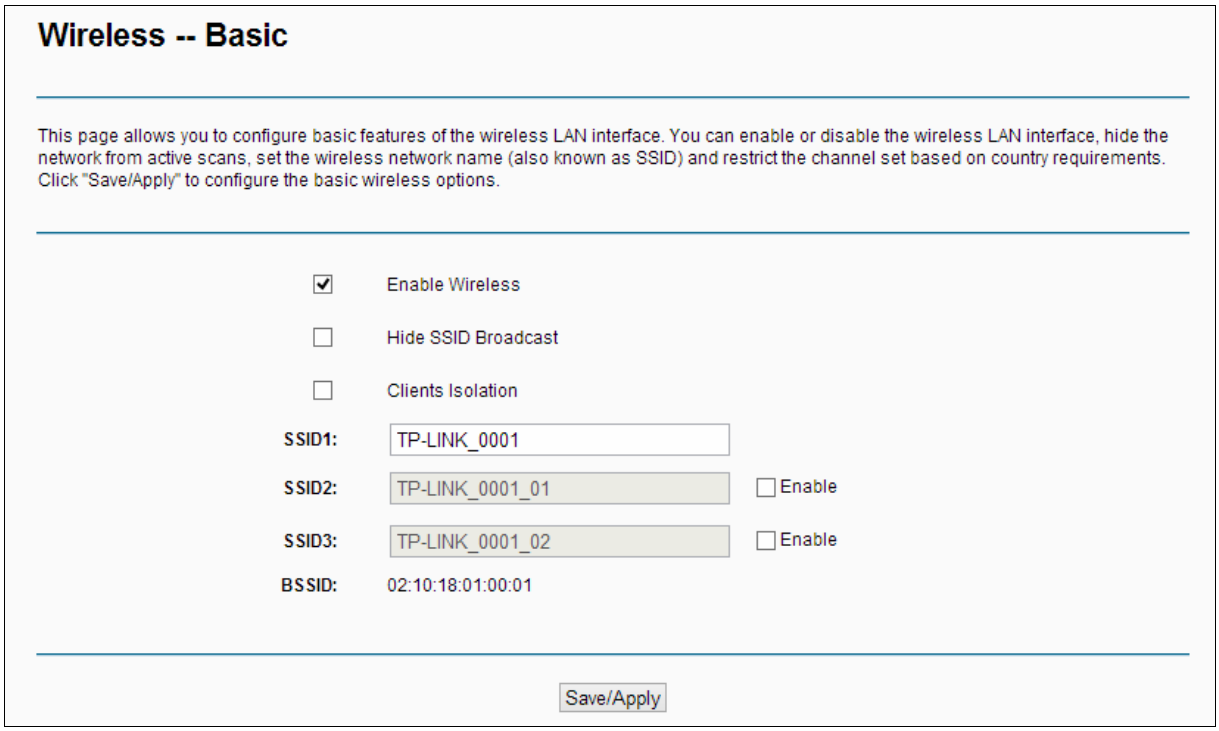


Figure 4-77

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on Region requirements.

- **Enable Wireless:** If you want to use wireless features, you must select “Enable Wireless”. If you deselect “Enable Wireless” option, all the Wireless settings below will be disabled.
- **Hide SSID Broadcast:** When wireless clients survey the local area for wireless networks to associate with, you can select this option to avoided being surveyed.
- **Clients Isolation:** Select this option to enable AP isolation function so that stations associated to the AP will not be able to communicate with each other.
- **SSID1:** Wireless network name. Enter a desired SSID which is case-sensitive and must not exceed 32 characters. The SSID is shared among all points in a wireless network and it must be identical for all devices in the wireless network. Make sure this setting is the same for all stations in your wireless network. Type the desired SSID in the space provided.
- **SSID2/3:** The modem router can broadcast three SSIDs at most. Tick the box to enable SSID2 or SSID3 as needed.
- **BSSID:** Show the MAC address of the modem router.

Click **Apply/Save** to save your settings.

4.7.2 Security

Choose “**Wireless**”→”**Security**”, you will see the screen of **Wireless--Security** settings shown as below. You can configure security features of the wireless LAN interface by manually setting the network authentication or through **WPS** (Wi-Fi Protected Setup) method.

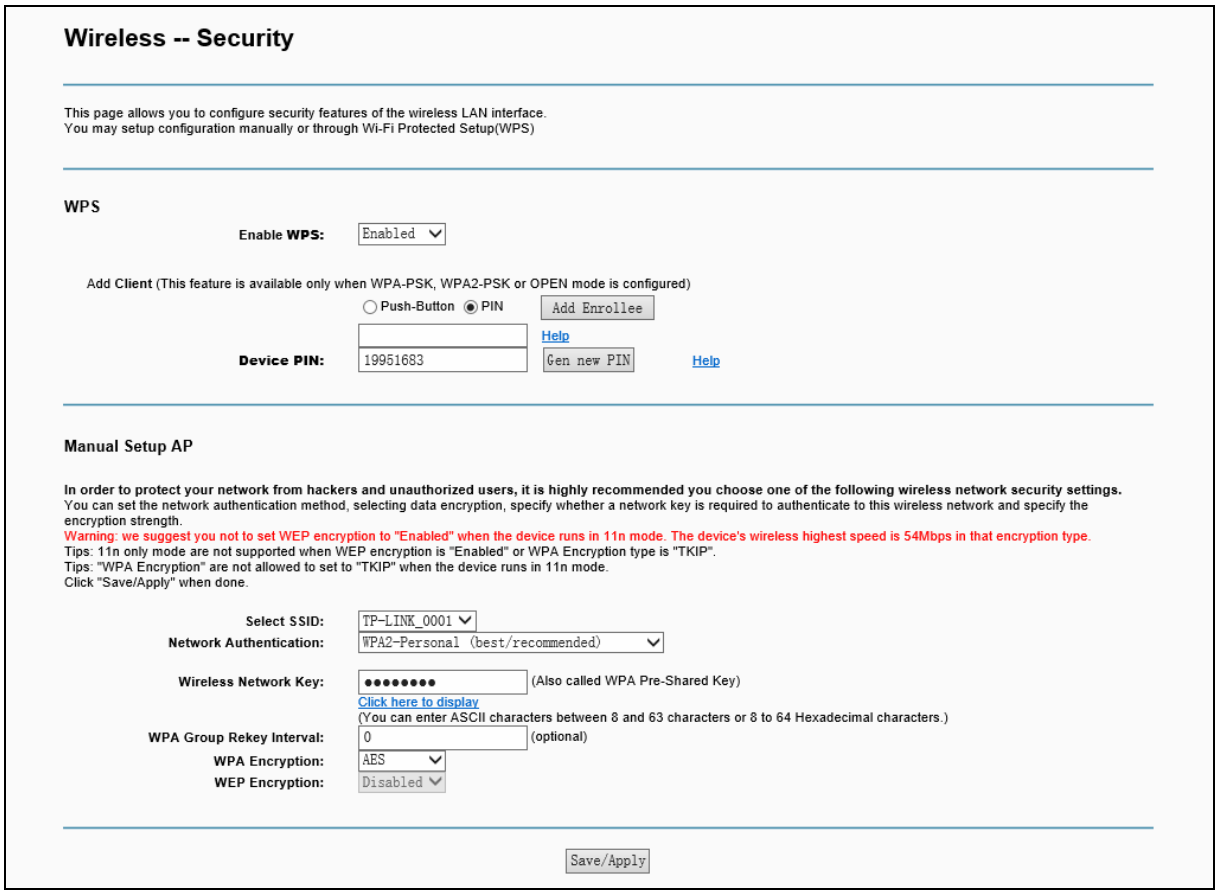


Figure 4-78

4.7.2.1 WPS Setup

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

Note:

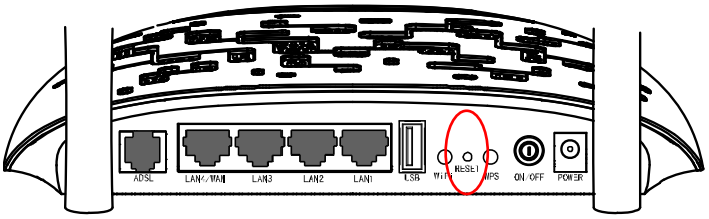
1) This feature is available only when OPEN, WPA-PSK, WPA2-PSK or Mixed WPA2/WPA-PSK mode is configured.
2) To build a successful connection by WPS, you should also do the corresponding configuration of the new device for WPS function meanwhile.

I. By PBC

There are two ways to add the wireless adapter to the network by PCB.

Method One: Hardware push button.

Step 1: Press the WPS button on the back panel of the modem router.



Step 2: Press and hold the WPS button of the wireless adapter (if it has one) for 2 or 3 seconds.

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

Figure 4-79

Method Two: Software push button.

Step 1: Click **Push-Button** on Figure 4-78, you will see the screen as shown below. Then click **Add Enrollee**.

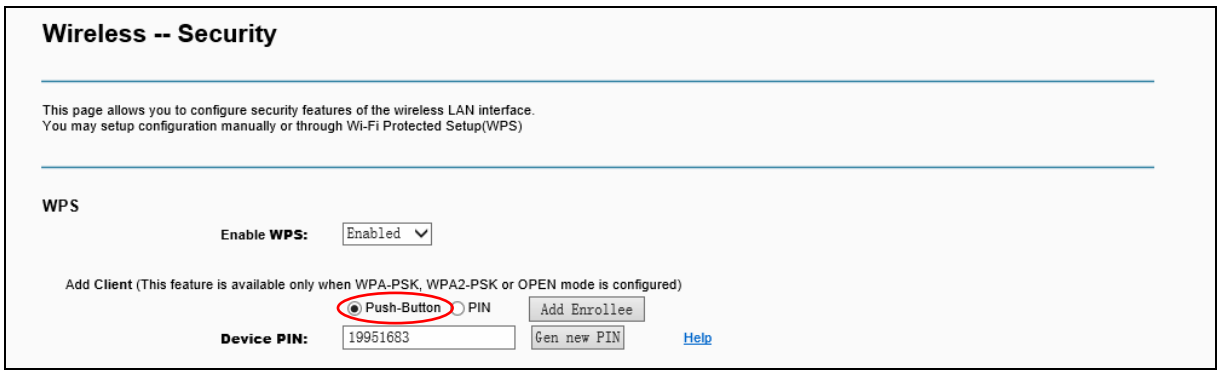


Figure 4-80

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

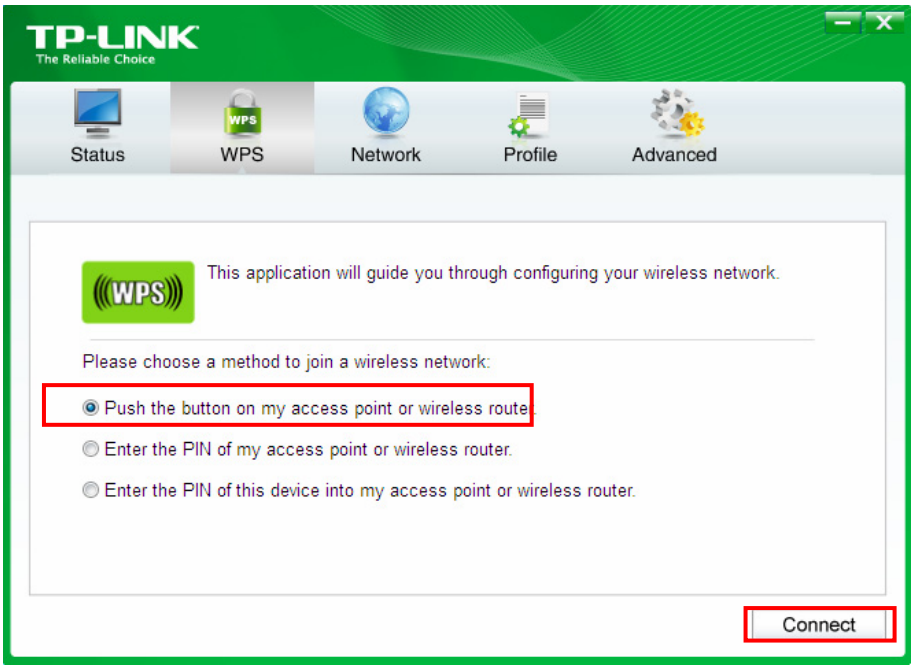


Figure 4-81

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

Figure 4-82

II. By PIN

If the new device supports Quick Security Setup and the PIN method, you can add it to the network by PIN with the following two methods.

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

Step 1: Select the **PIN** checkbox and enter the PIN code of the wireless adapter in the field under as shown below. Then click **Add Enrollee**.

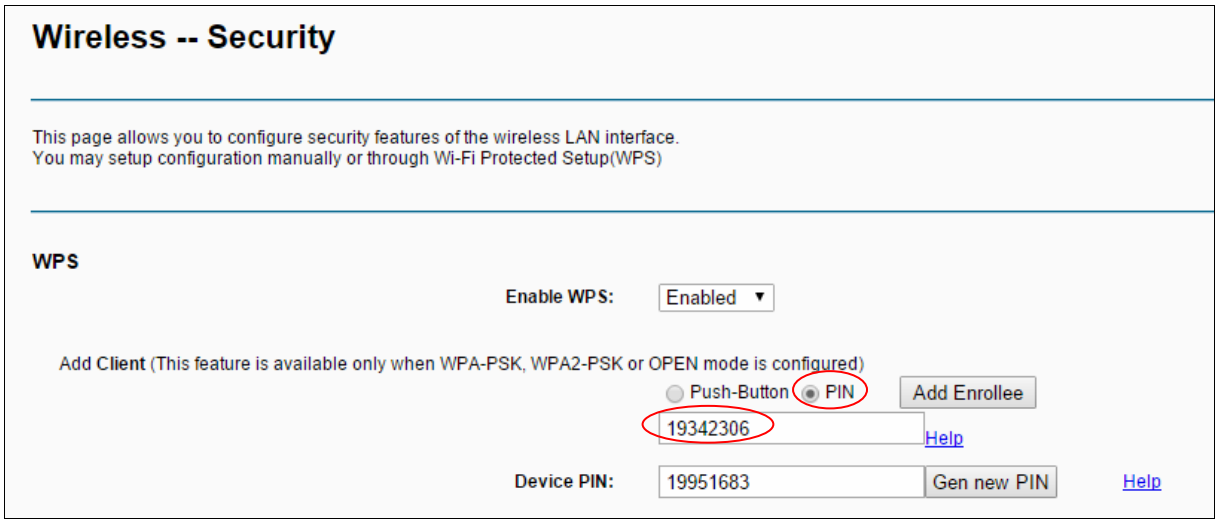


Figure 4-83

Note:

The PIN code of the adapter is always displayed on the WPS configuration screen.

Step 2: For the configuration of the wireless adapter, please choose "**Enter the PIN of this device into my access point or wireless router.**" in the configuration utility of the WPS as below, and click **Connect**.

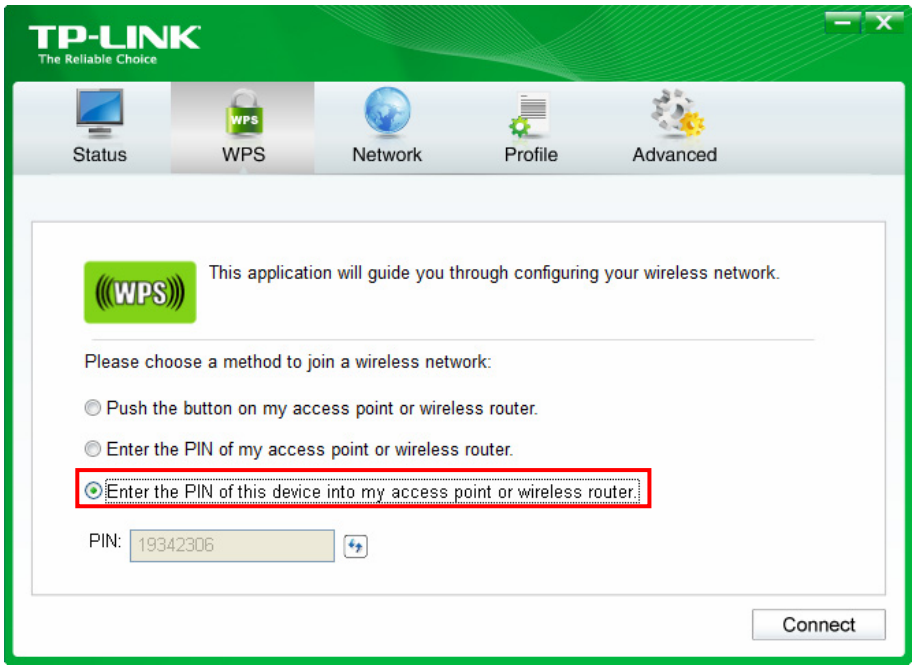


Figure 4-84

Note:

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

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

Step 1: Get the Current PIN code generated by the modem router as shown below. You can click **Gen New PIN** to get a new PIN code for modem router.

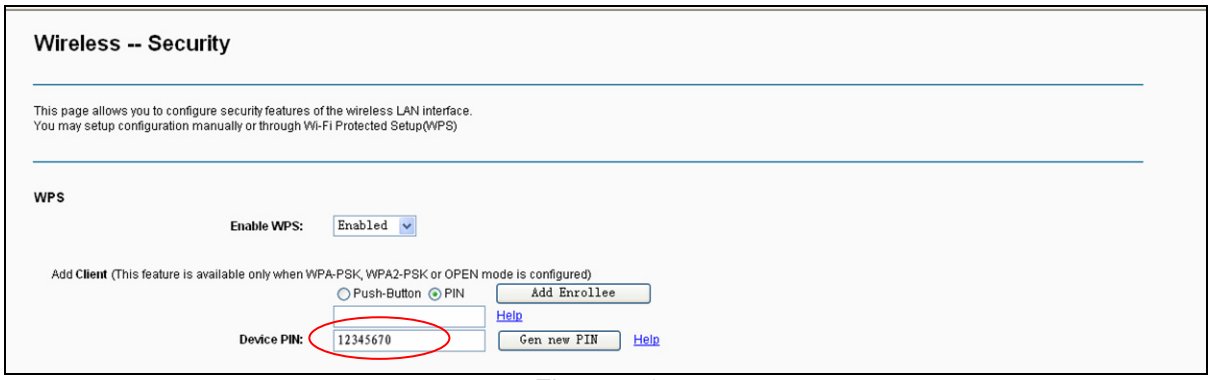


Figure 4-85

Step 2: For the configuration of the wireless adapter, please choose "**Enter the PIN of my access point or wireless router**" in the configuration utility of the WPS as below, and enter the PIN code of the modem router into the field after "**PIN**". Then click **Connect**.

Figure 4-86

4.7.2.2 Manual Setup AP

Follow the instructions below to configure security features of the wireless LAN interface manually. You can set the network authentication method, select data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.

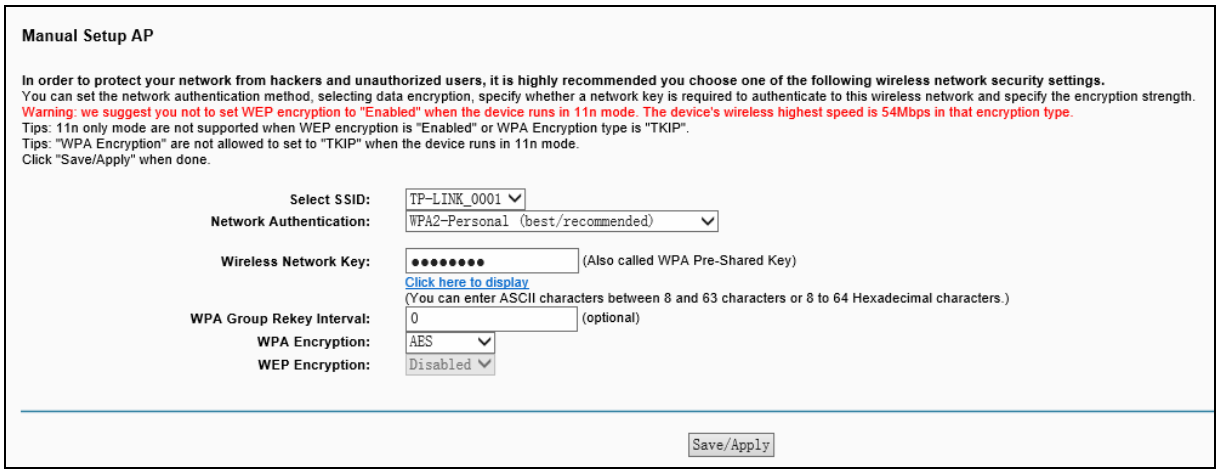


Figure 4-87

- **Select SSID:** Select the SSID from the drop-down list.
- **Network Authentication:** Select an authentication type from the drop-down list.

Note:

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

1. WEP

WEP is a basic encryption method offering two levels of encryption, 64-bit and 128-bit encryption. To configure the WEP encryption, there are two ways.

- Keep the Network Authentication of **Open (insecurity)** and select **Enabled** from the WEP Encryption drop-down list, as shown in Figure 4-88. **Open (insecurity)** with WEP encryption disable allows any wireless station to associate with the access point.
- Select **Shared (good)** from the Network Authentication drop-down list, as shown in Figure 4-89. **Shared (good)** must enable WEP encryption. Network using Open or Shared authentication with WEP encryption only allows stations using the same network key encryption to associate with it. Follow the instructions below to configure the Shared Keys.

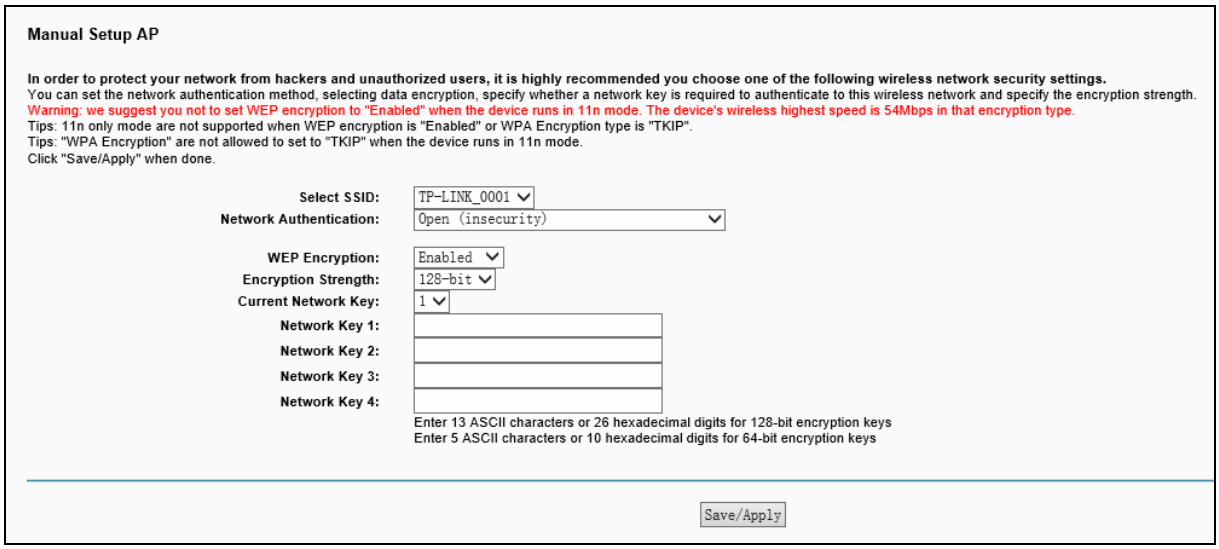


Figure 4-88

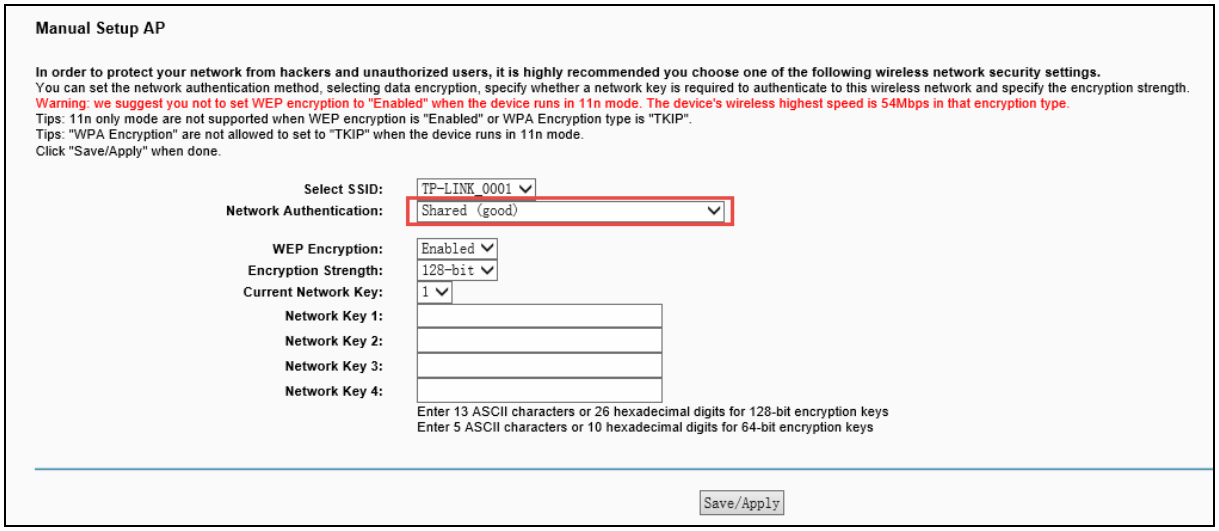


Figure 4-89

- **Encryption Strength:** Select the appropriate level of encryption, 64-bit or 128-bit.
- **Current Network Key:** To indicate which WEP key to use, select a transmission key number.
- **Network Key 1-4:** If you want to manually enter the WEP keys, then enter them in the network Key 1-4 fields.

Configure WEP Settings

1. Select the SSID from the **Select SSID** drop-down list.
2. Select **Shared (good)** from the **Network Authentication** drop-down list. The menu will change to offer the appropriate settings.
3. Select **64-bit** from the **WEP Encryption** drop-down list.
4. Select "**1**" from **Current Network Key** drop-down list.
5. Type in the password in the **Network Key 1** field.
6. Click **Save/Apply** to save the new configuration.

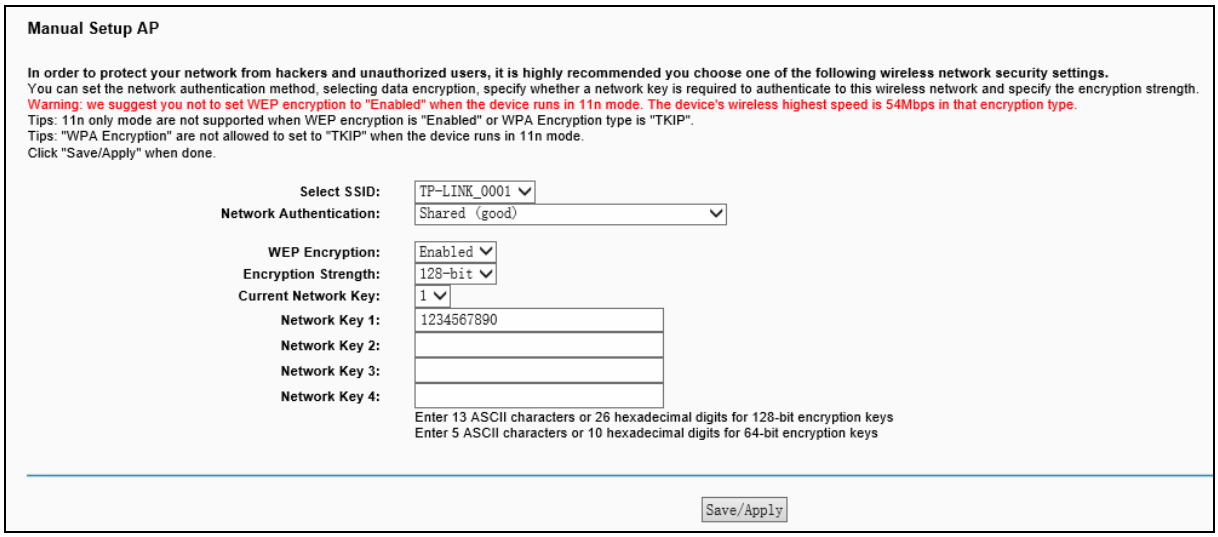


Figure 4-90

Note:

We use **Network Authentication** Shared (good), **Encryption Strength** 64-bit, **Current Network Key** “1” and enter 10 hexadecimal digits”1234567890” in the **Network Key 1** for example, as shown in Figure 4-90 above.

2. WPA-Enterprise

WPA security for wireless communication has been developed to overcome some of the shortcomings of WEP. WPA combines the key generation with the authentication services of a RADIUS server.

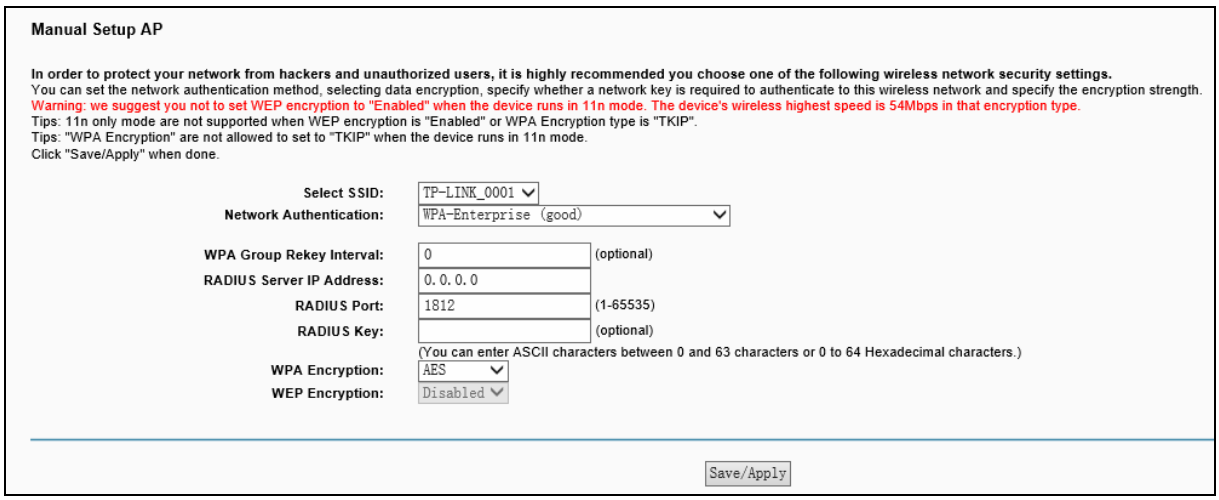


Figure 4-91

- **WPA Group ReKey Interval:** Enter the Key Renewal period, which tells the modem router how often it should change encryption keys.
- **RADIUS Server IP Address:** The IP address of the RADIUS server.
- **RADIUS Port:** The port of the RADIUS server. The default number is 1812.
- **RADIUS Key:** The password of the RADIUS Server.
- **WPA Encryption:** Select the encryption you want to use: TKIP+ AES or AES (AES is an encryption method stronger than TKIP).

Configure WPA settings

1. Select the SSID from the **Select SSID** drop-down list.
2. Select **WPA** from the **Network Authentication** drop-down list. The menu will change to offer the appropriate settings.
3. Change the **WPA Group Rekey Interval** as desired.
4. Type in the IP address of the RADIUS server used in the **RADIUS Server IP Address** field.
5. Change the **RADIUS Port** if necessary.
6. Type in the password in the **RADIUS Key** field.
7. Use the default setting **AES** of WPA Encryption.
8. Click **Save/Apply** to save the new configuration.

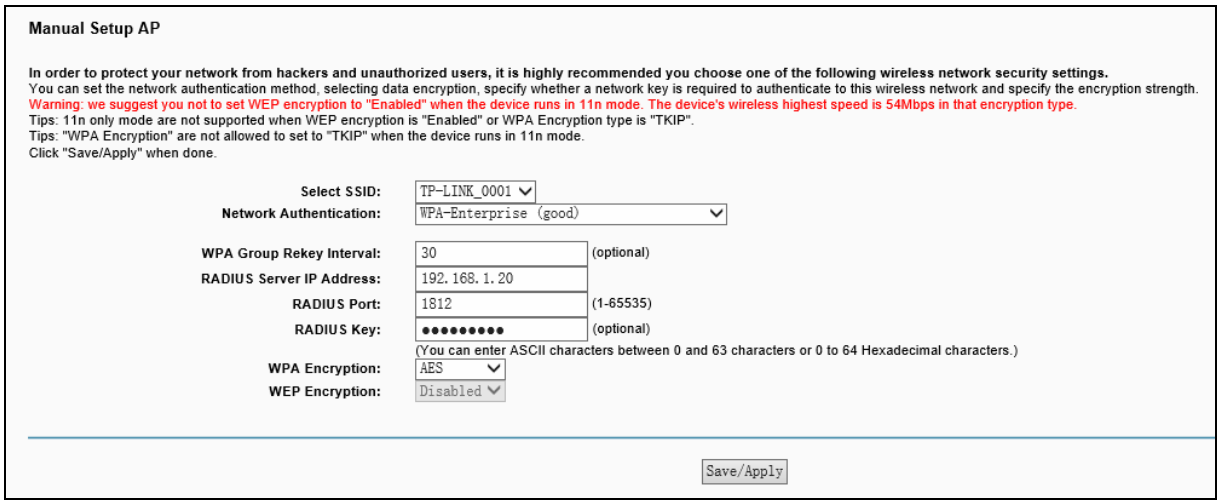


Figure 4-92

3. WPA-Personal

WPA-Personal requires a shared key and does not use a separate server for authentication. PSK keys can be ASCII or Hex type.

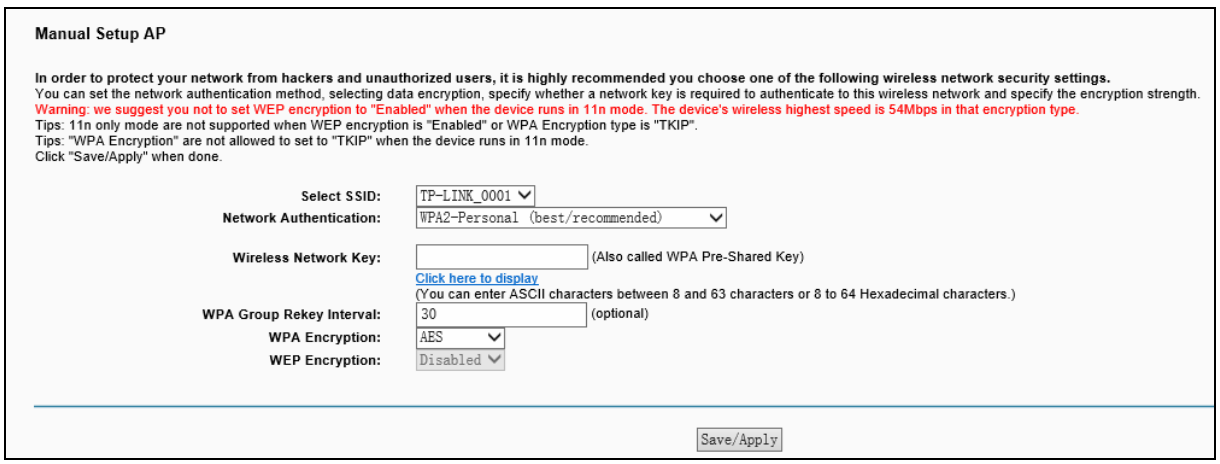


Figure 4-93

- **Wireless Network Key:** Enter the key shared by the modem router and your other network devices. It must have 8-63 ASCII characters or 8-64 Hexadecimal digits.
- **Click here to display:** Click it to show you the WPA Pre-Shared Key.

Configure WPA-Personal settings

1. Select the SSID from the **Select SSID** drop-down list.
2. Select **WPA-Personal**. The menu will change to offer the appropriate settings as the picture show above.
3. WPA-Personal requires a shared key. Type the key in the space provided. PSK keys can be ASCII or Hex type.
4. Change the Group Key Interval as desired or use the default setting.
5. Click **Save/Apply** to save the new configuration.

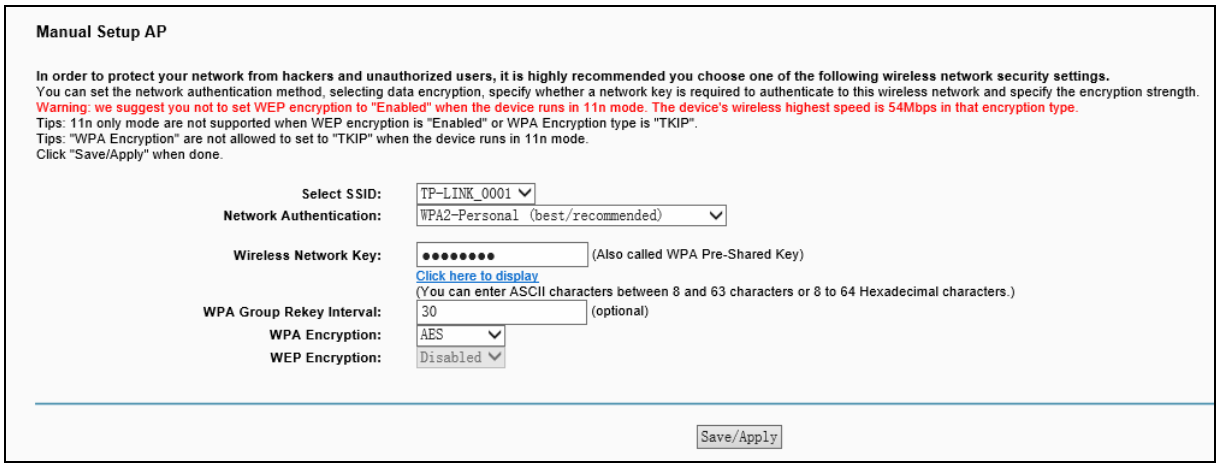


Figure 4-94

Note:

If you click the option “Click here to display”, the Figure 4-95 will pop-up, and it shows the password you have set. In addition, it won't show the blank characters in both ends of the password phrase.

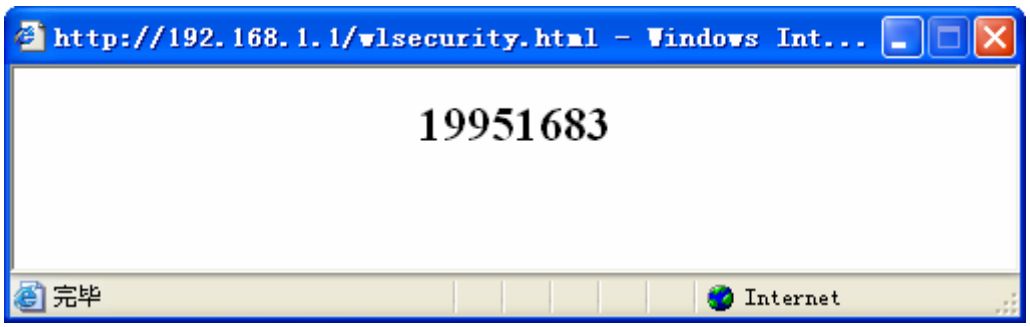


Figure 4-95

4. WPA2-Enterprise

To configure WPA2-Enterprise settings, select the WPA2-Enterprise option from the drop-down list. The menu will change to offer the appropriate settings. The steps of these settings are similar to WPA settings.

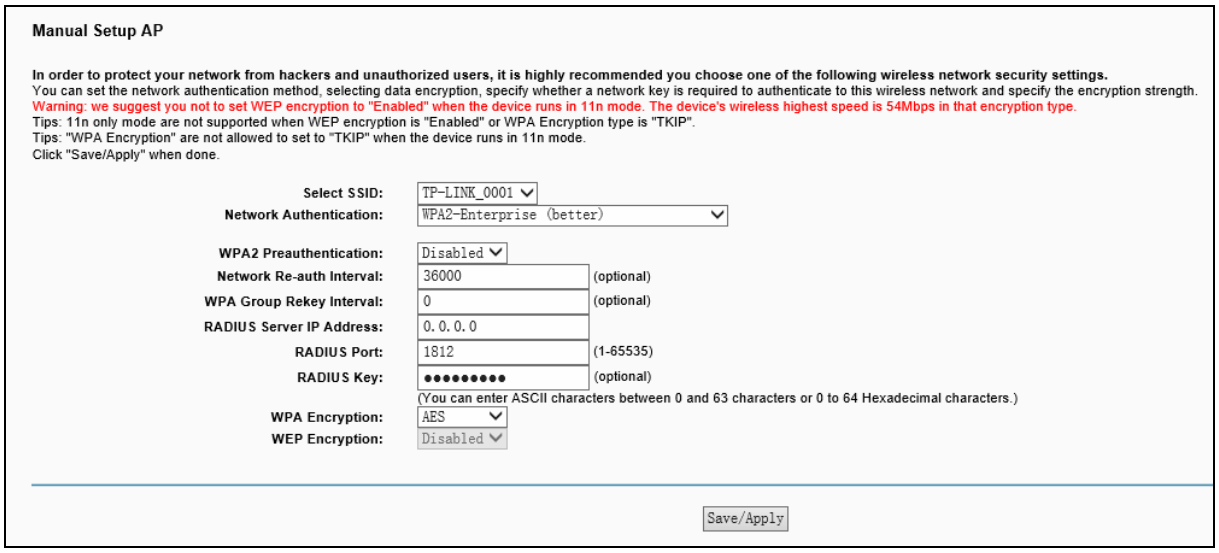


Figure 4-96

- **WPA2 Preauthentication:** Select Enable from the drop-down list, Stations will authenticate with the AP during the scanning process, and once association is required, the station has been already authenticated.
- **Network Re-auth Interval:** Enter a value in seconds as the frequency interval to enable periodic Network Re-authentication function, while leave it blank or enter “0” to disable it.

5. WPA2-Personal

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

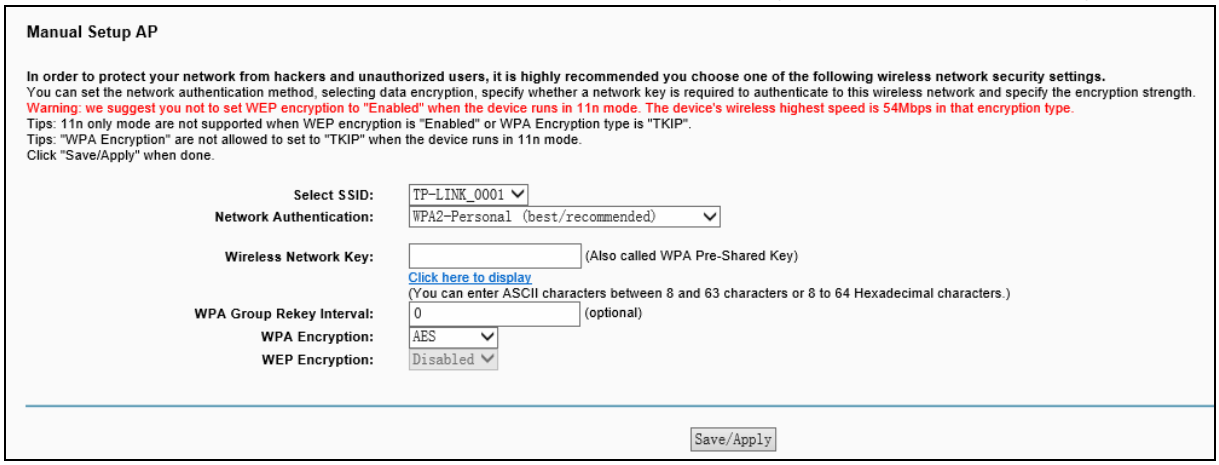


Figure 4-97

6. Mixed WPA2/WPA Enterprise

To configure Mixed WPA2/WPA Enterprise settings, select the Mixed WPA2/WPA Enterprise option from the drop-down list. The menu will change to offer the appropriate settings. The steps to these settings are similar to those for WPA-PSK.

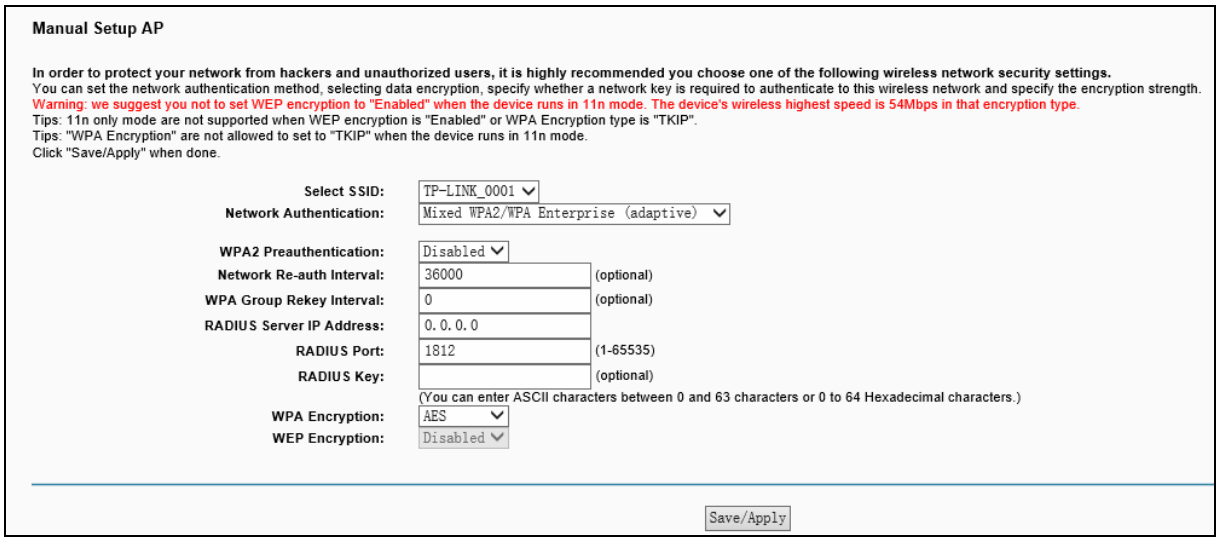


Figure 4-98

7. Mixed WPA2/WPA Personal

To configure Mixed WPA2/WPA-Personal settings, select the Mixed WPA2/WPA Personal option from the drop-down list. The menu will change to offer the appropriate settings. The steps of this setting are the same with WPA-PSK.

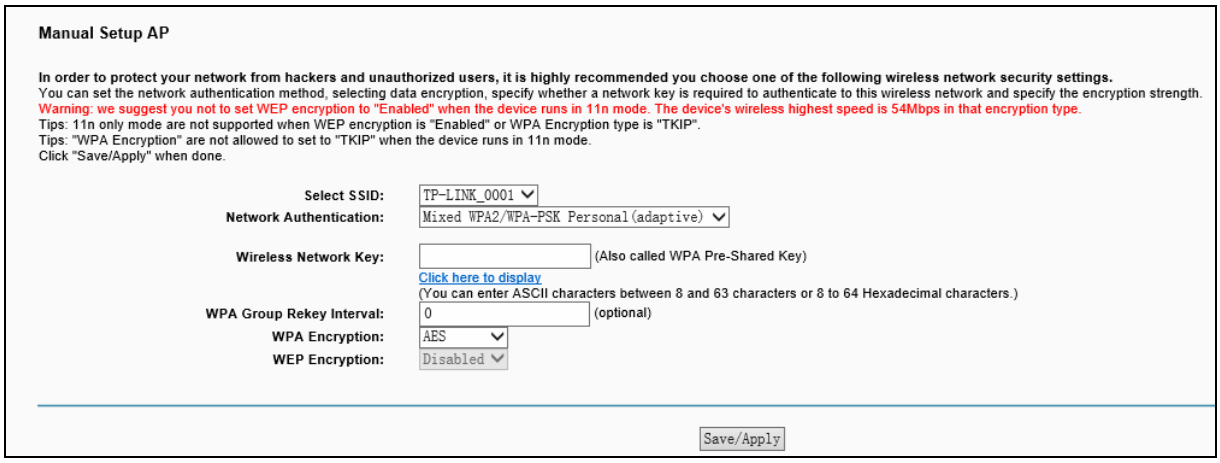


Figure 4-99

4.7.3 Wireless Schedule

Choose menu “**Wireless**”→“**Wireless Schedule**”, you can configure the Task Schedule as shown below. Please set the modem router’s system time first.

Figure 4-100

☞ 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 4.11.5 Internet Time, then you can enable or disable Wireless Schedule.

- **Apply To:** Select the day or days you need 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 the **Save/Apply** button to complete the settings.

4.7.4 MAC Filter

Choose "**Wireless**"→"**MAC Filter**", you will see the screen of **Wireless--MAC Filter** settings shown as below.

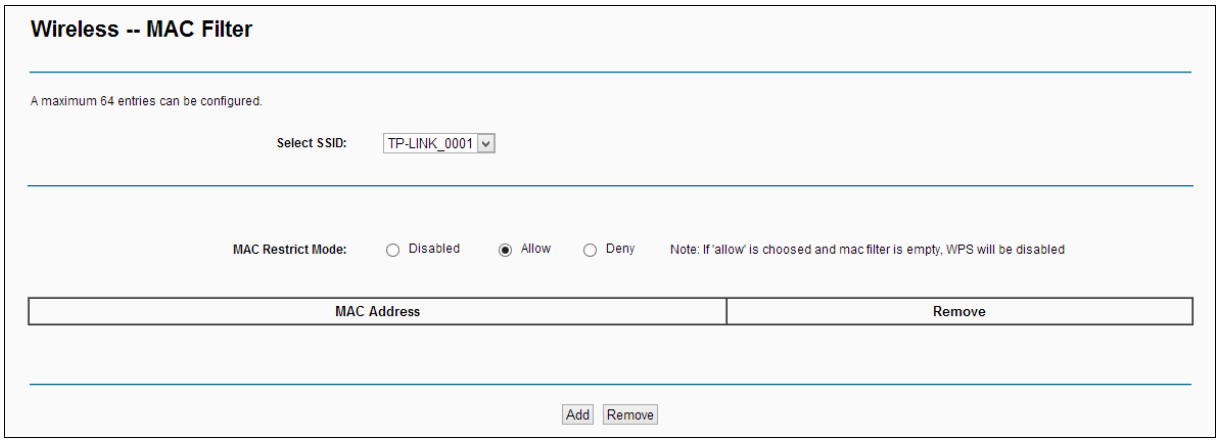


Figure 4-101

Wireless access can be filtered by using the MAC addresses of the wireless devices transmitting within your network's RADIUS. To filter wireless users by MAC Address, either permitting or blocking access. If you do not wish to filter users by MAC Address, select Disabled.

- **Select SSID:** Select the SSID of the wireless network in which you want to use the MAC Filter function.
- **Disabled:** Select this option to disable MAC Filter function.
- **Allow:** Select this option to enable MAC Filter function that allow wireless access by the devices listed on this screen.
- **Deny:** Select this option to enable MAC Filter function that block wireless access from the devices listed on this screen.
- **Add:** Click this button to add the MAC Address.
- **Remove:** Select the item of the MAC Address and click this button to remove it.

When you click the **Add** button, the pop-up picture shown below, and then you can type the MAC Address in the **MAC Address** field.

☞ **Note:**

The form of MAC Address must be "**xx:xx:xx:xx:xx:xx**", like "**00:13:0A:55:FF:09**".

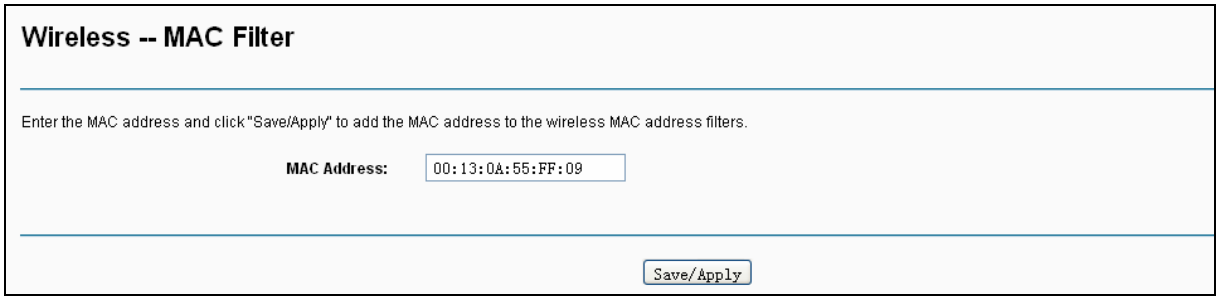


Figure 4-102

When you finished making changes to the MAC Filter List screen, click **Save/Apply** to save the changes.

4.7.5 Wireless Bridge

Choose "**Wireless**"→"**Wireless Bridge**", you will see the screen of **Wireless--Bridge** settings shown as below. You can configure wireless bridge features of the wireless LAN interface and click **Apply/Save** button to save the current configuration.

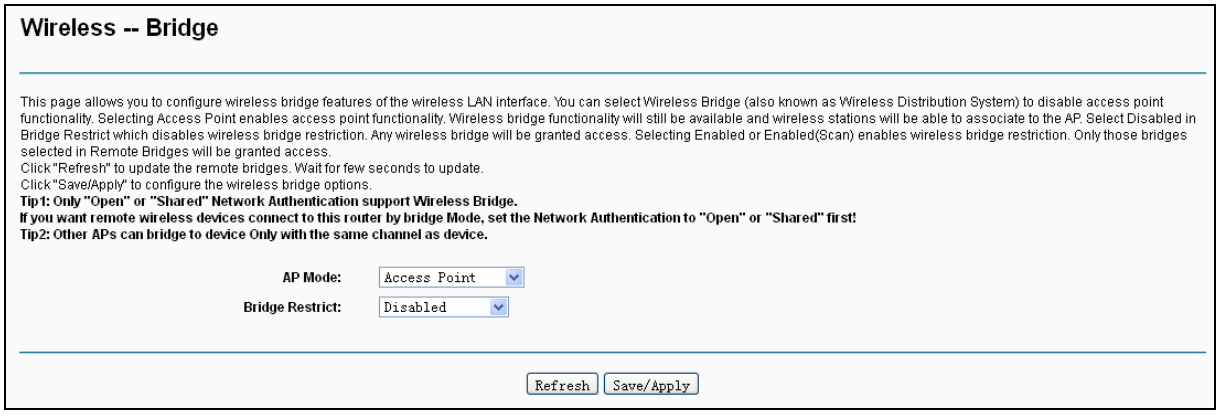


Figure 4-103

- **AP Mode**: Select an AP Mode from the drop-down list. Options available are: Access Point and Wireless Bridge.
  - **Access Point**: Select this option to allow wireless stations including AP clients to access.
  - **Wireless Bridge**: Also known as WDS (Wireless Distribution System), it will bridges the wireless stations which also in bridge mode to connect two or more remote LANs.
- **Bridge Restrict**:
  - **Disabled**: Select this option to disables wireless bridge restriction, that any wireless bridge will be granted access.
  - **Enabled**: Select this option (as shown below) to enables wireless bridge restriction, please enter the MAC address of the Remote Bridges that you want to connect with, and only these Remote Bridges are granted access.

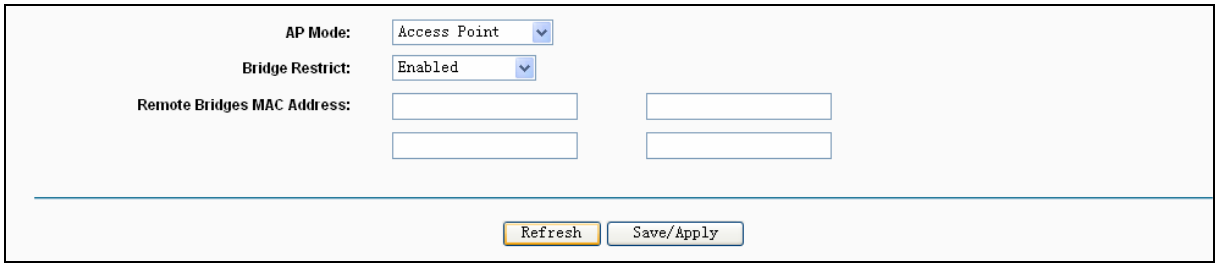


Figure 4-104

- **Enabled (Scan)**: Select this option to enables wireless bridge restriction, and it will scan the environment for APs that exist around the device. Only those selected AP will be granted access.
- **Refresh:** Click this button to scan and display the APs.

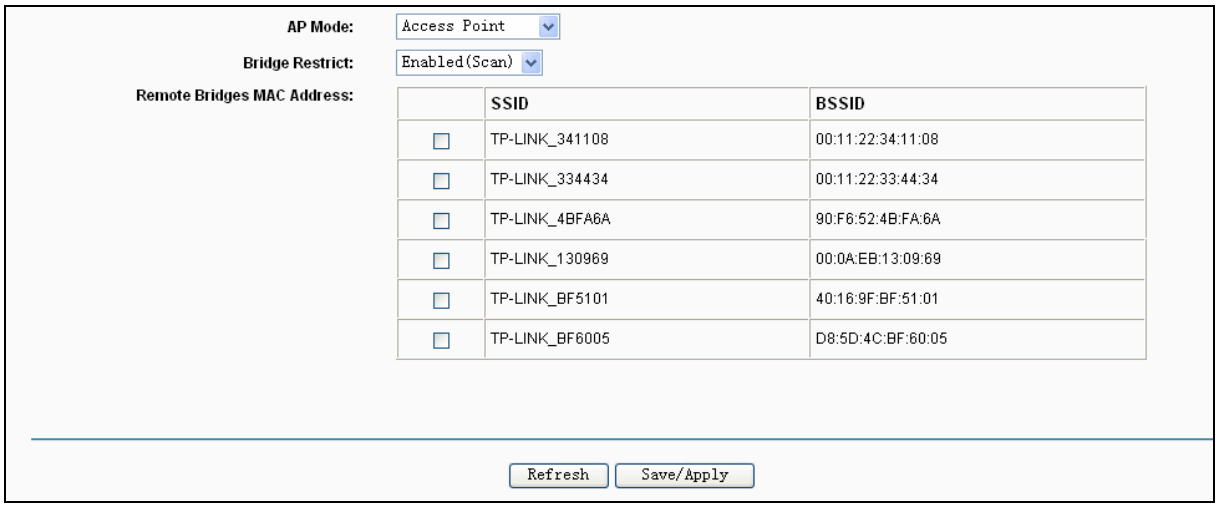


Figure 4-105

Note:

Only Open or Shared authentication method support wireless bridge, you should choose "**Wireless**"→"**Security**" to change authentication method to "open" or "shared" mode first.

4.7.6 Advanced

Choose "**Wireless**"→"**Advanced**", you will see the screen of **Wireless--Advanced** settings shown as below.

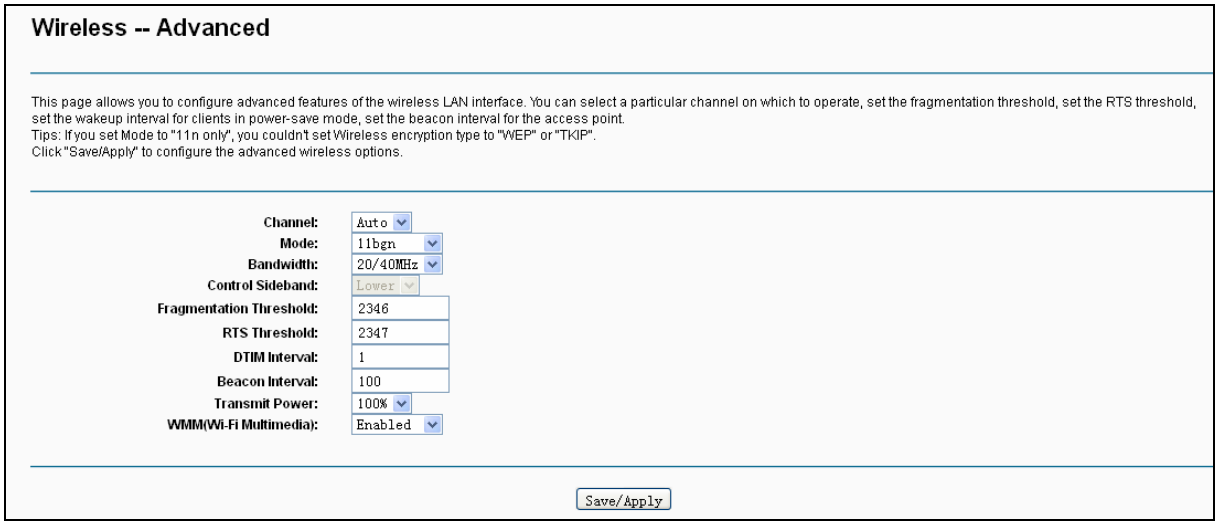


Figure 4-106

- **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.
- **Mode**: In the drop-down list you can select "11b", "11bg", "11bgn" and "11n only". "11bgn" allows both 802.11b, 802.11g and 802.11n wireless stations to connect to the modem router.
- **Bandwidth**: Select the Bandwidth you want to use from the drop-down List. If bigger bandwidth is selected, device could transmit and receive data with higher speed.

- **Control Sideband**: If bigger bandwidth is selected, this option will allow you select the Control Sideband you want.
- **Fragmentation Threshold:** This value specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor reduction of the default value is recommended. In most cases, it should remain at its default value of 2346.
- **RTS Threshold:** Should you encounter inconsistent data flow, only minor reduction of the default value 2347 is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The modem router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. This mechanism can provide you a quiet communication channel by notifying other stations not to send packet for a period of time. In most cases, keep its default value of 2347.
- **DTIM Interval:** This value, between 1 and 255, indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. The countdown unit is measured by the amounts of beacon frames received. When the modem router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages. The default value is 1.
- **Beacon Interval:** Enter a value between 20-1000 milliseconds. The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the modem router to synchronize the wireless network. The default value is 100.
- **Transmit Power:** This option will allow you to configure the wireless transmit power. High transmit power will extend the wireless signal range of the device and make the signal transmit more legible. Low transmit power with the smaller wireless signal range that will decrease the probability of interrupt by other Wi-Fi device.
- **WMM (Wi-Fi Multimedia):** This function can guarantee the packets with high-priority messages being transmitted preferentially. It is strongly recommended.

4.7.7 Station info

Choose "**Wireless**"→" **Station Info**", you will see the screen of **Wireless--Authenticated Stations** setting shown as below.

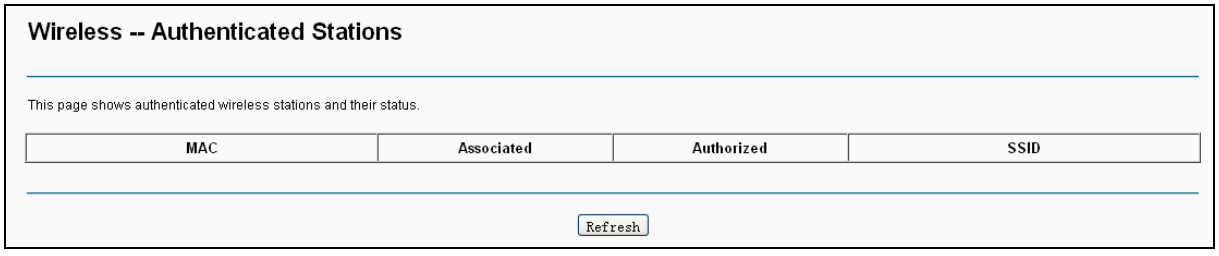


Figure 4-107

This page shows authenticated wireless stations and their status.

- **MAC**: Displays the connected wireless station's MAC address.

- **Associated**: Displays whether the wireless station has associated with the access point.
- **Authorized**: Displays the information of Authentication.
- **SSID**: Displays the connected wireless station's SSID.

You cannot change any of the values on this page. To update this page and to show the current connected wireless stations, click on the **Refresh** button.

4.8 Guest Network

There are two submenus under the Guest Network menu: **Basic** and **Station 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.

4.8.1 Basic

Choose menu "**Guest Network**"→"**Basic**", and you will see the screen as shown in Figure 4-108. 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.

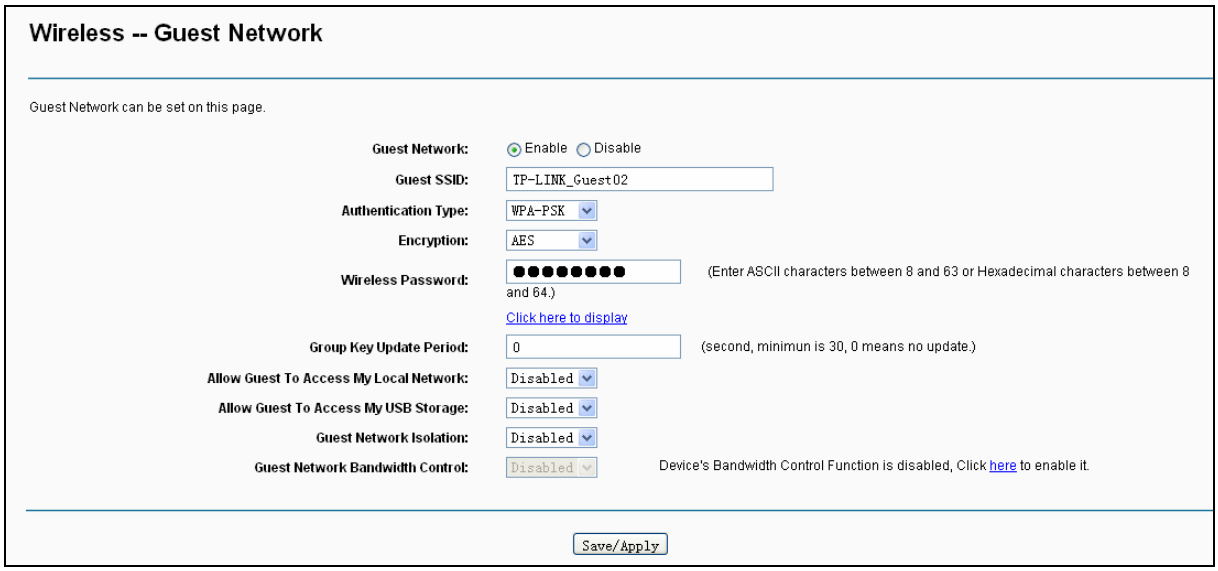


Figure 4-108

You can enable or disable Guest Network. When you enable this function, you could set wireless parameters for Guest Network.

- **Guest SSID:** The guest network name. When setting up a Guest network, it is strongly recommended to use a name that easily distinguishes it from your primary network.
- **Authentication Type:** Select the Authentication Type from the drop-down list.
- **Encryption:** You can select either **AES** or **AES+TKIP.**
- **Wireless Password:** Here display the default wireless password, you can click **Click here to display** to see the default wireless password, and you can also enter ASCII characters

between 8 and 63 characters or 8 to 64 Hexadecimal characters to create a new password.

- **Group Key Update Period:** Specify the group key update interval in seconds. The value should be 30 or above. Enter 0 to disable the update.
- **Allow Guest to Access my Local Network**: The guests have access to your Local Network, but can not login the modem router's web management interface.
- **Allow Guest to Access my USB Storage:** 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 4.9.3 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 Bandwidth and Downstream Bandwidth for guest network.

Click **Save/Apply** to save your settings.

4.8.2 Station list

Choose menu "**Guest Network**"→"**Station list**", you can see the MAC Address, Associated, Authorized, SSID and Interface.

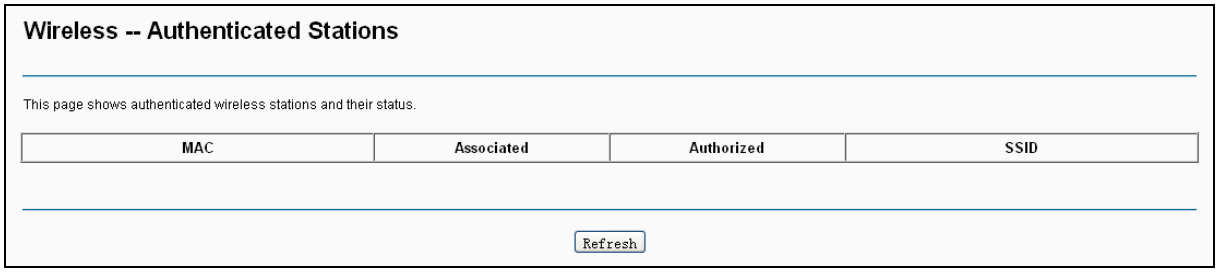
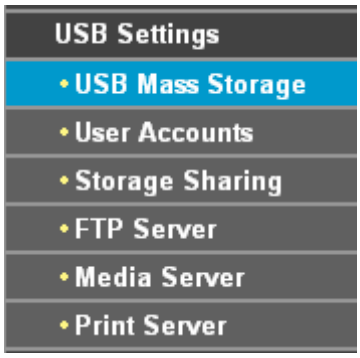


Figure 4-109

- **MAC:** Displays the connected wireless station's MAC address.
- **Associated**: Displays whether the wireless station has associated with the access point.
- **Authorized**: Displays the information of Authentication.
- **SSID**: Displays the connected wireless station's SSID.

You cannot change any of the values on this page. To update this page and to show the current connected wireless stations, click on the **Refresh** button.

4.9 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.

4.9.1 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, etc on this page as shown below.

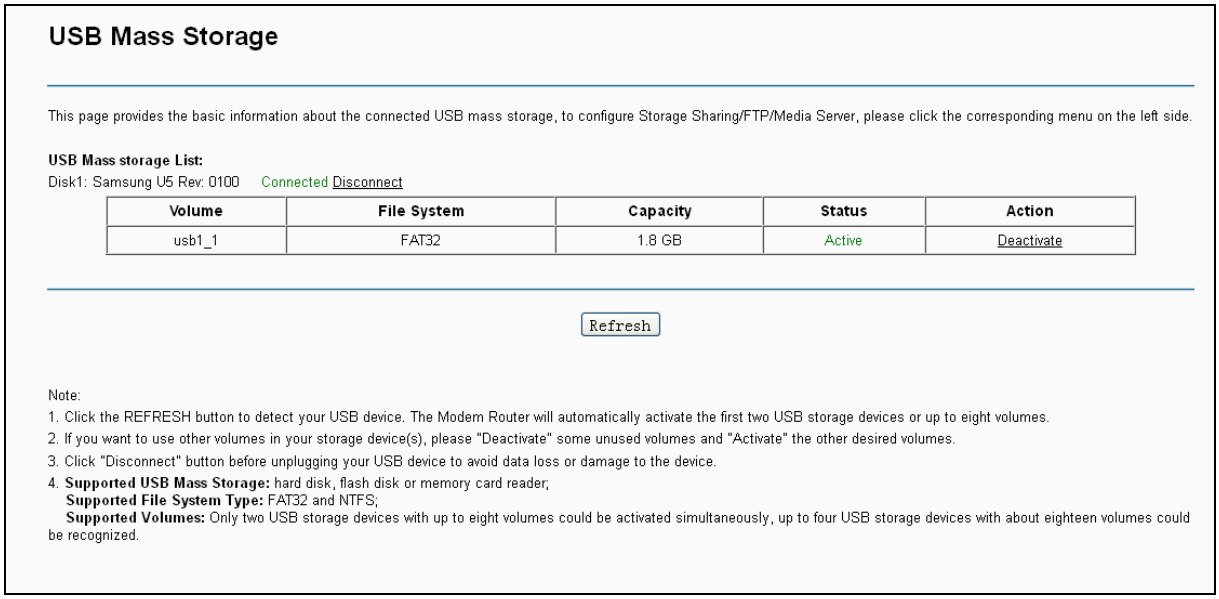


Figure 4-110

- **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..
- **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.

4.9.2 User Accounts

You can specify the user name and password for Storage Sharing and FTP Server users on this page. There are five users here, which provide means to control the access to the USB mass storage by Storage Sharing or FTP. The Super User has the right to read and write to Storage Sharing and FTP Server.

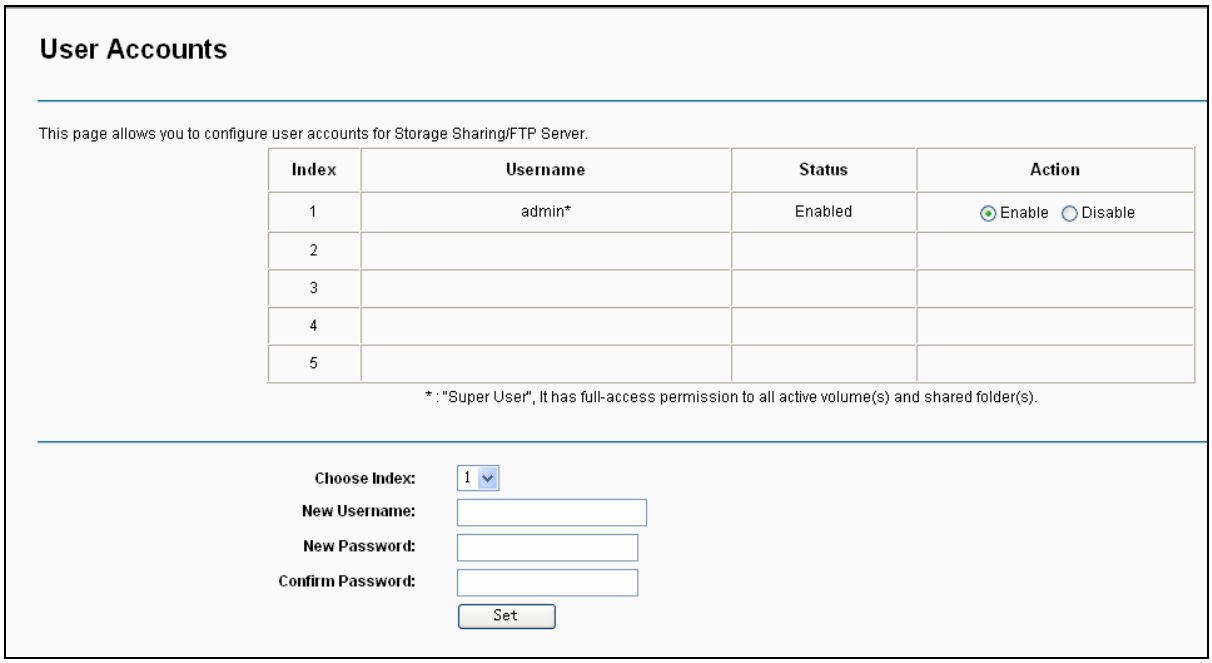


Figure 4-111

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.

Click the **Set** button, and then a new entry will be added in the table.

4.9.3 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.

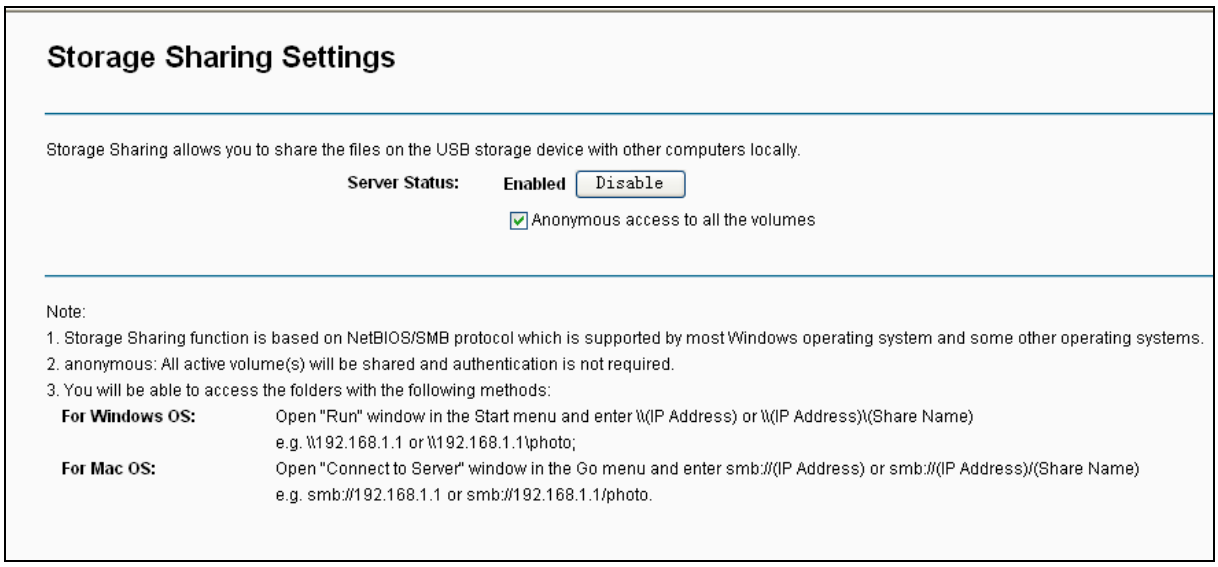


Figure 4-112

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

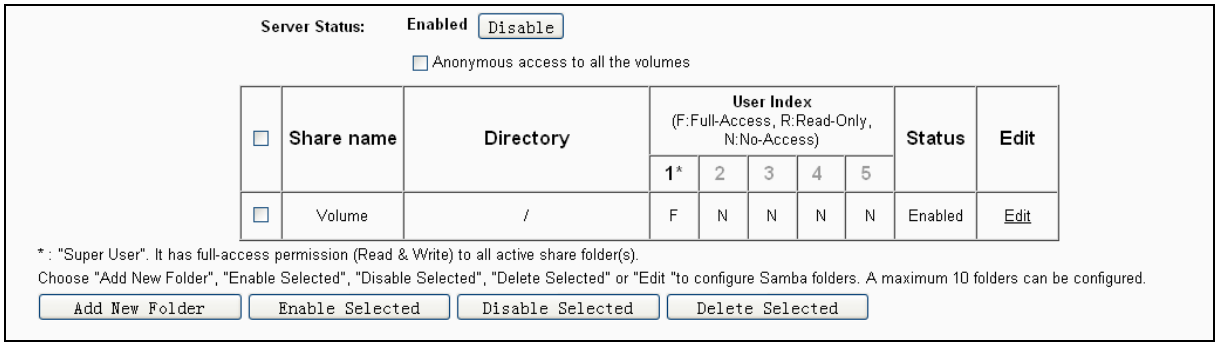


Figure 4-113

- **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. * users mean Super Users who have the full-access permission to all activated volumes and share folders. Grey users mean the users who have no right to use this function. Others are common users.
- **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** in Figure 4-113.

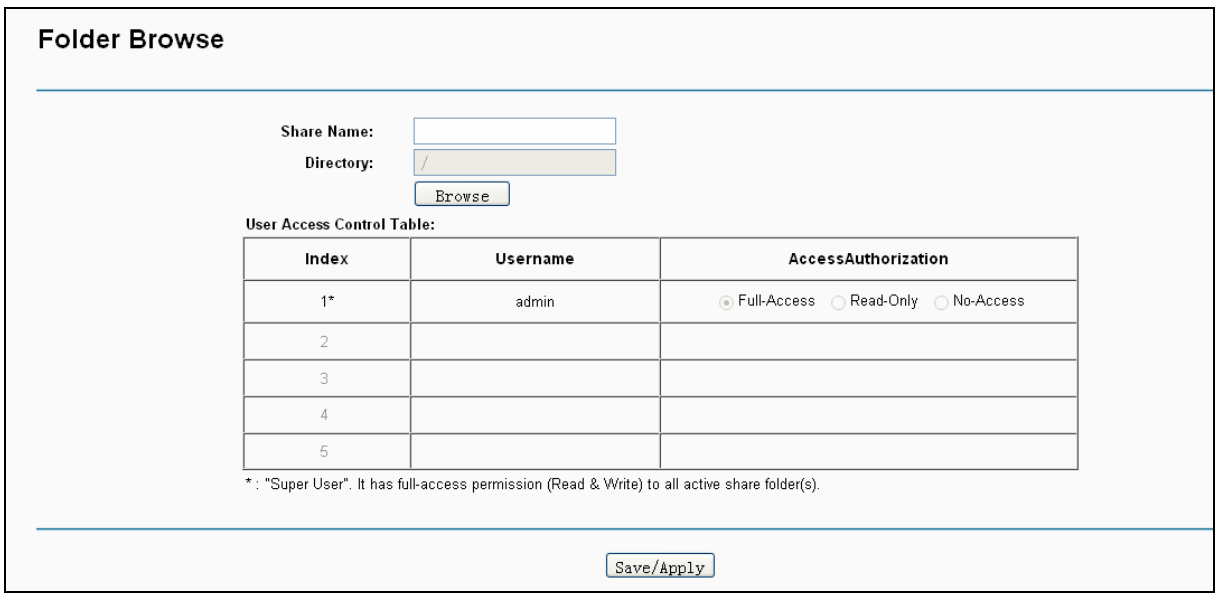


Figure 4-114

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 **Save/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.

4.9.4 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.

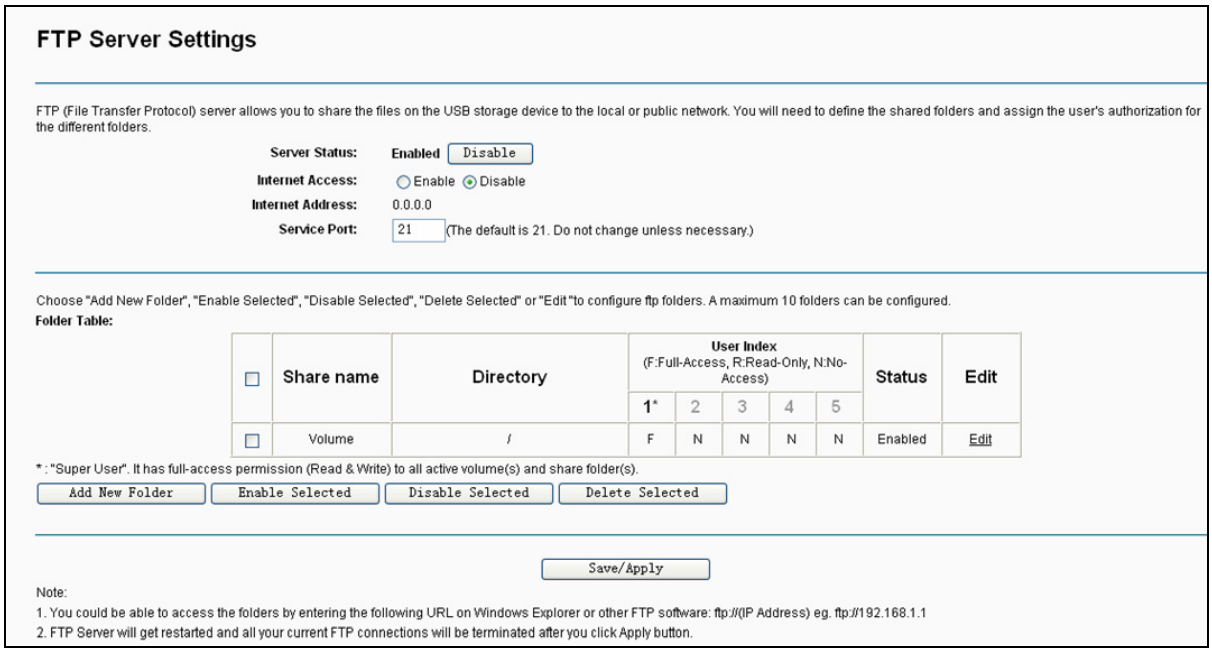


Figure 4-115

- **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** in the table, and then you can modify the entry.

To add a new folder, follow the instructions below.

1. Click **Add New Folder** in Figure 4-115.

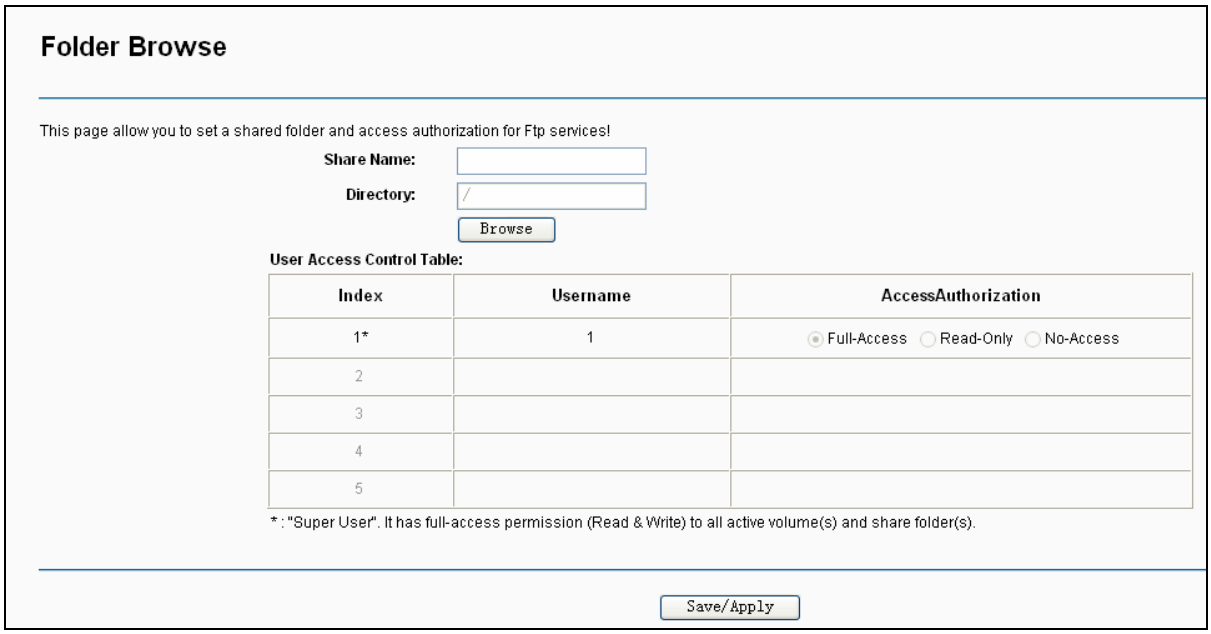


Figure 4-116

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 **Save/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.

4.9.5 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.

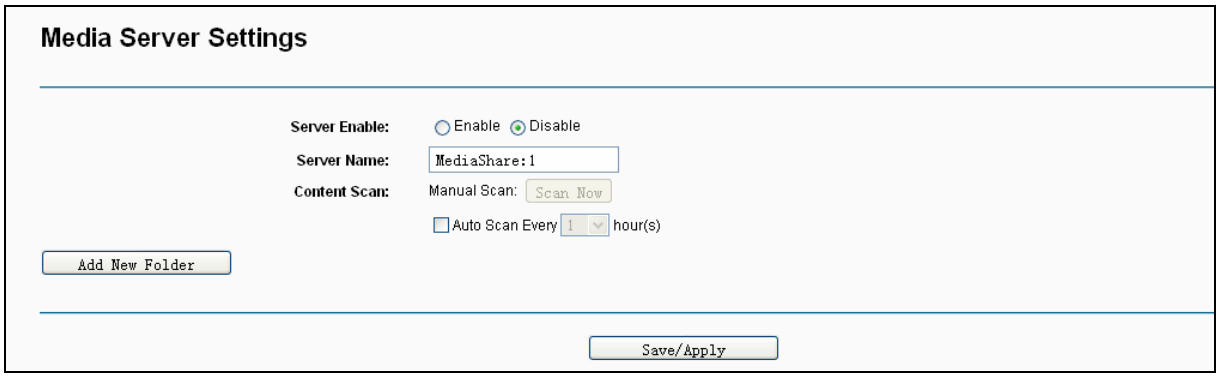


Figure 4-117

- **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 4-118.

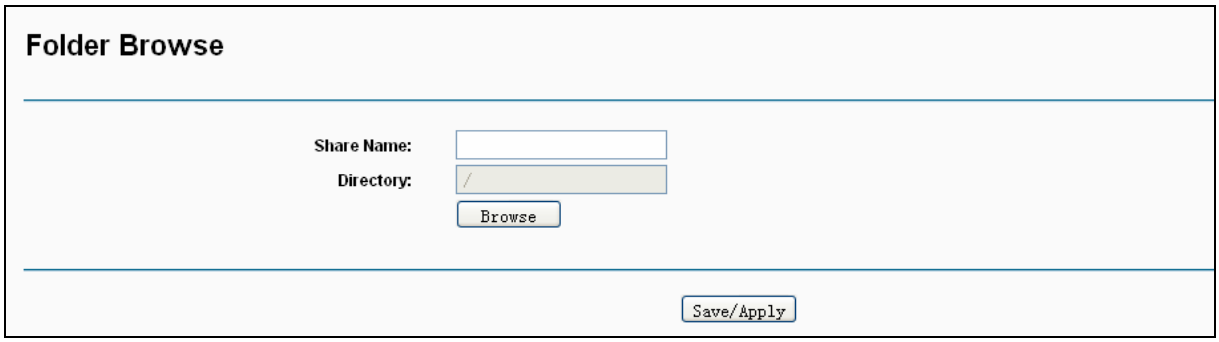


Figure 4-118

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

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

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

4.9.6 Print Server

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

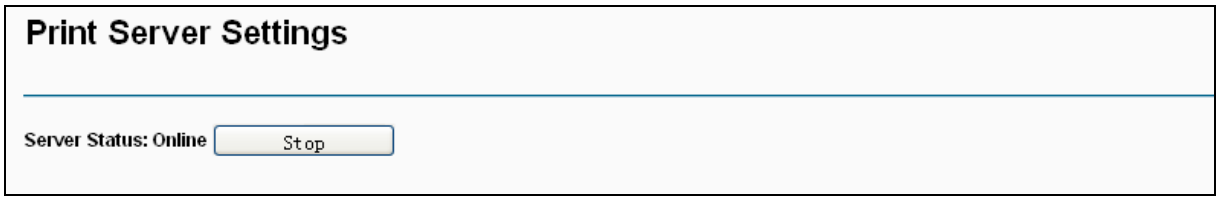


Figure 4-119

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

- **Online:** Indicates the print service 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 has been turned on, but at this moment other users are using print services.

4.10 Diagnostics

Choose "**Diagnostics**", you will see the Diagnostics screen. This section describes the result of the test for the ENET (Ethernet) Connection, Wireless Connection and ADSL Synchronization. You can refer to the **Help** menu to get more information about the corresponding test.

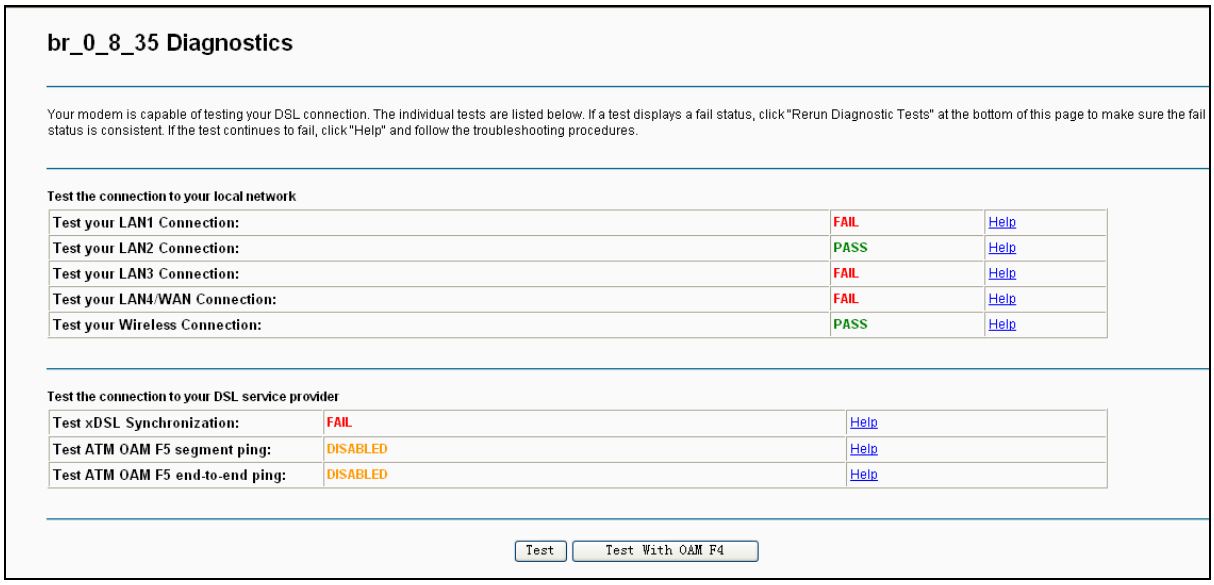
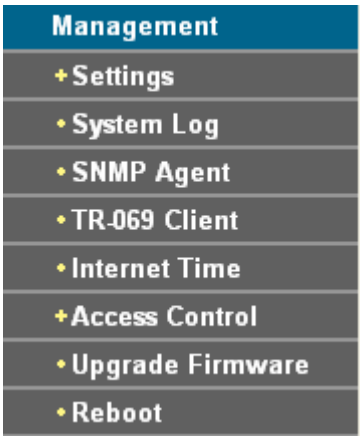


Figure 4-120

4.11 Management

Choose "**Management**", there are eight submenus under the main menu. They are **Settings**, **System Log**, **SNMP Agent**, **TR-069 Client**, **Internet Time**, **Access Control**, **Update Firmware** and **Reboot**. Click any of them, and you will be able to configure the corresponding function.



4.11.1 Settings

This section provides three important functions for managing the modem router: **Export** (Backup), **Import** (Update) and **Restore Default**. The detailed manipulations are described below.

4.11.1.1 Export

Choose "**Management**"→"**Settings**"→"**Export**", you can see the **Export** screen, this screen (shown in Figure 4-121) allows you to save the current configuration of the modem router as a backup file.

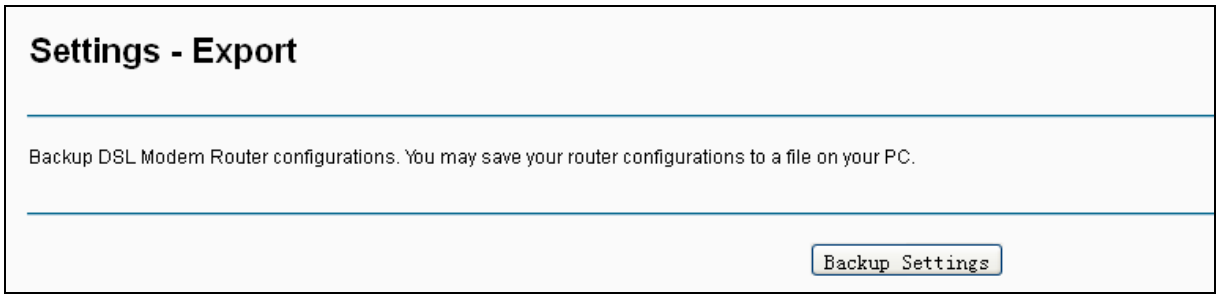


Figure 4-121

To back up the modem router's current settings:

1. Click the **Backup Settings** button on the preceding screen (pop-up Figure 4-121), the following screen will then appear (shown in Figure 4-122).

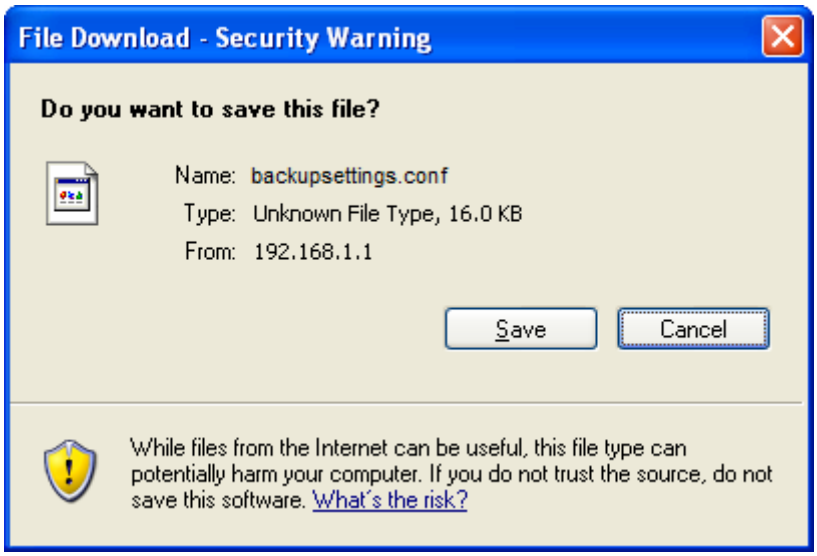


Figure 4-122

2. Click the **Save** button, and save the file as the appointed file (shown in Figure 4-123).

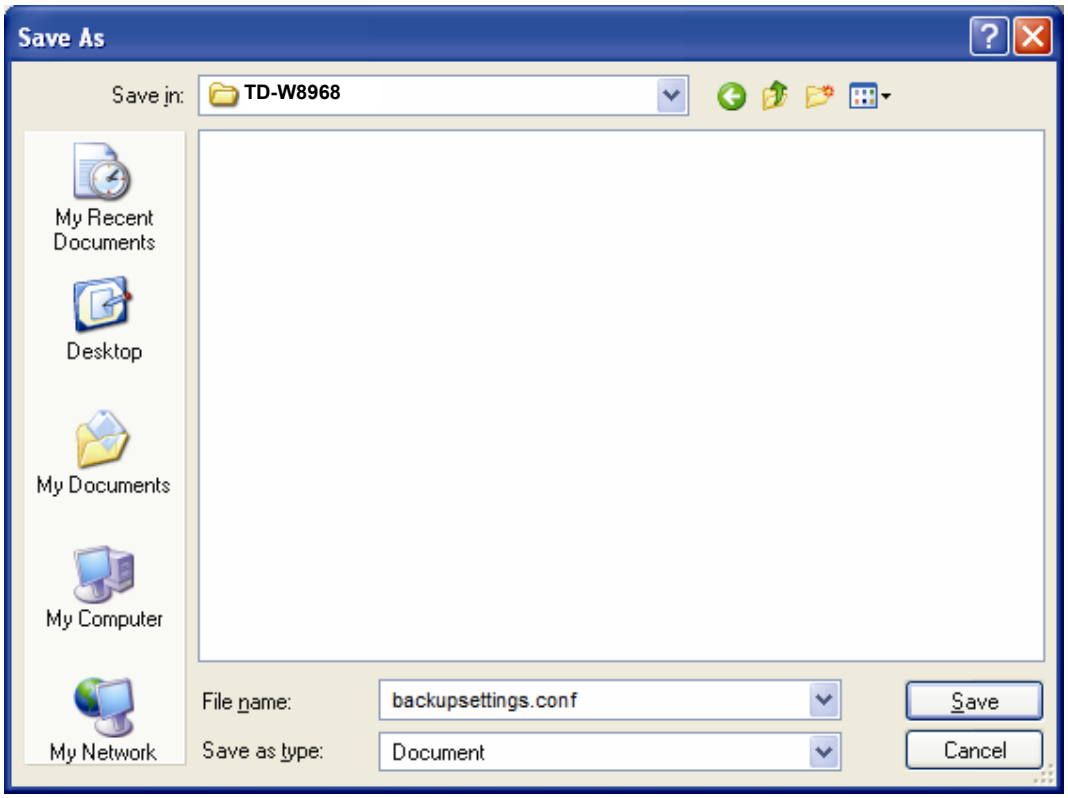


Figure 4-123

4.11.1.2 Import

Choose "**Management**"→"**Settings**"→"**Import**", you can see the **Import** screen, this screen (shown in Figure 4-124) allows you to update the modem router's settings.

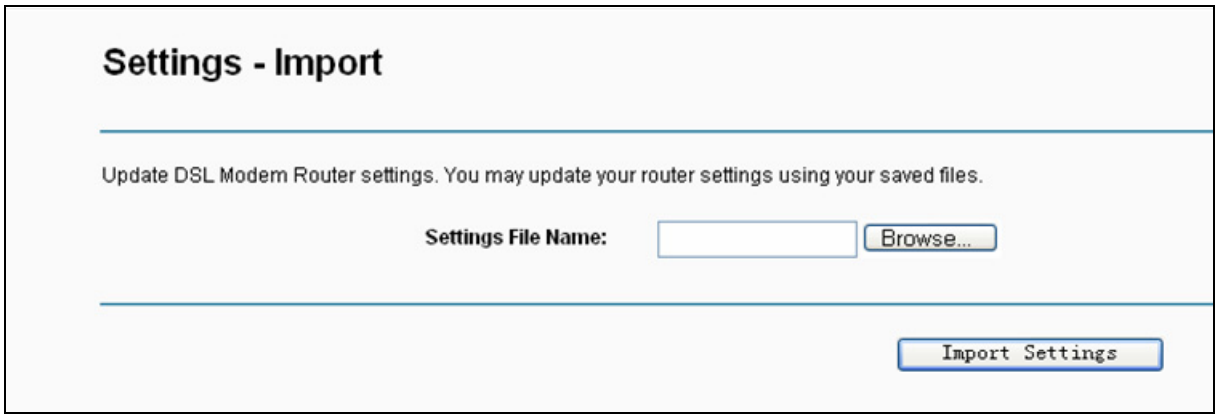


Figure 4-124

To update the modem router's settings:

1. Click the **Browse** button to locate the update file for the device, and you can also enter the exact path to the Setting file in the text box.
2. After you have selected the file for updating the settings, click the **Import Settings** button.

☞ **Note:**

The modem router will reboot upon completion. This process will take a while, don't turn off the modem router or press the **Reset** button while processing.

4.11.1.3 Restore Default

Choose "**Management**"→"**Settings**"→"**Restore Default**", you can see the **Restore Default** screen, this screen (shown in Figure 4-125) allows you to restore the modem router's configuration to the factory defaults on the screen.

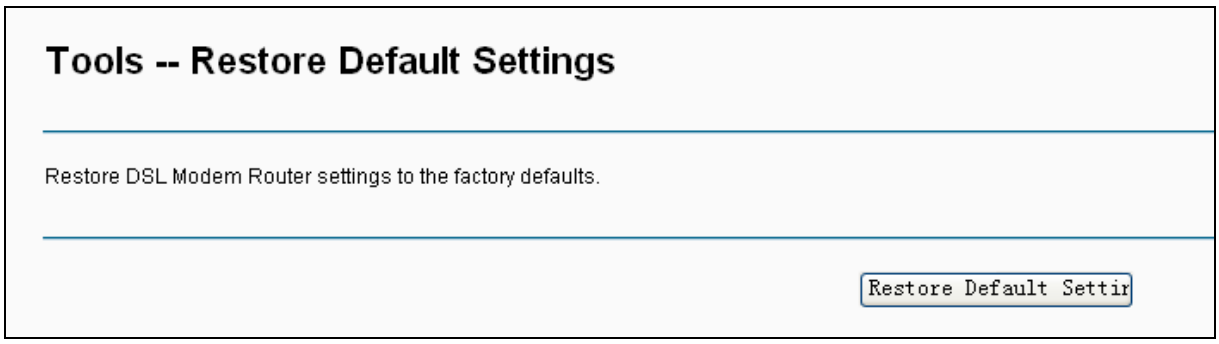


Figure 4-125

- **Restore Default Settings:** Click this button to restore the modem router's configuration to the factory defaults, and then follow the on-screen instructions to complete it.
- **Account and Password:** The default **user name** and its **password** are both **admin**.
- The default **IP Address:** 192.168.1.1.
- The default **Subnet Mask:** 255.255.255.0.

4.11.2 System Log

Choose "**Management**"→"**System Log**", you can see the **System Log** screen, this screen (shown in Figure 4-126) allows you to view the system log and configure the system log options.

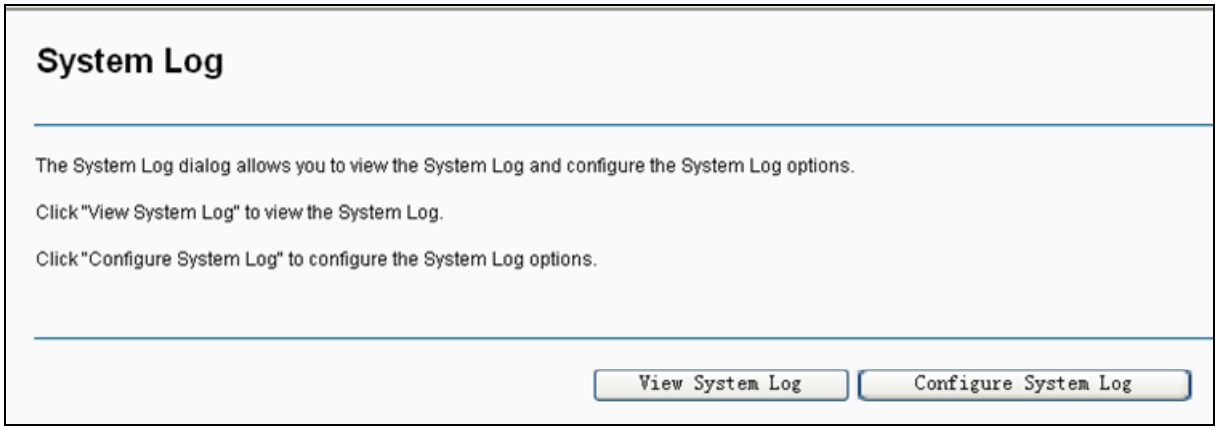


Figure 4-126

To view the System Log:

Click the **View System Log** button, you will see the screen (shown in Figure 4-127) which displays the modem router's recent logs.

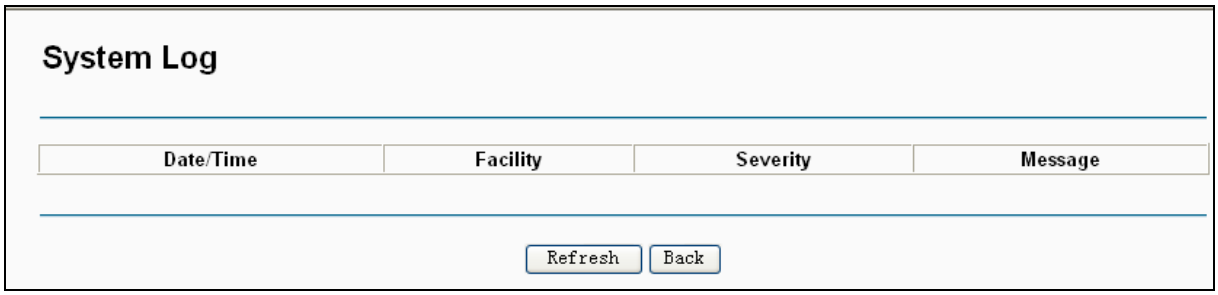


Figure 4-127

- **Refresh:** Click the button, the information in the table will be updated.
- **Back:** Click the button, the screen will back to the previous page.

To configure the System Log settings:

Click the **Configure System Log** button (shown in Figure 4-126), you will see the screen below (shown in Figure 4-128).

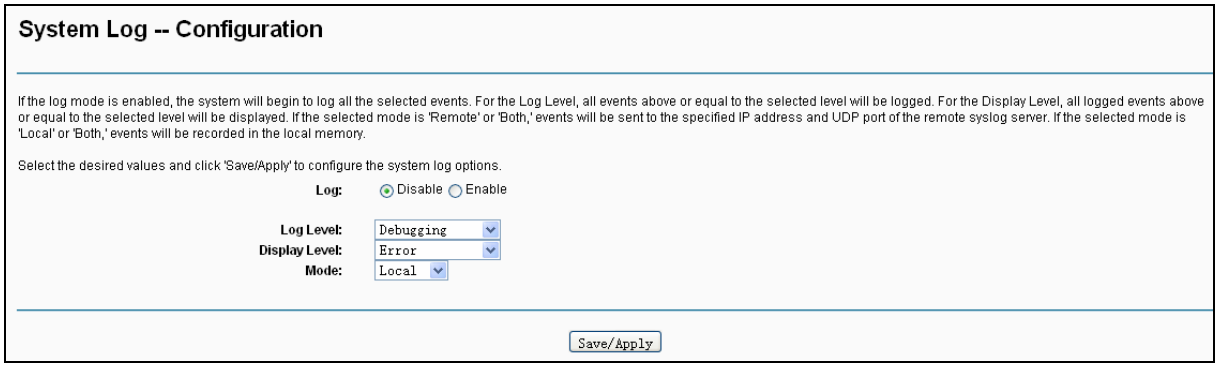


Figure 4-128

- **Disable/Enable:** Select the **Enable** to log the events, if you don't want to log these events, please select **Disable**.
- **Log Level:** Select the Log level in the drop-down list, for the Log level, all events above or equal to the selected level will be logged.
- **Display Level:** Select the Display level in the drop-down list, for the Display Level, all logged events above or equal to the selected level will be displayed.
- **Mode:** Select the mode to record the events. If the selected mode is **Local,** events will be recorded in the local memory. If the selected mode is **Remote**, events will be sent to the specified IP address and UDP port of the remote system log server. If the selected mode is **Both**, events will be sent to the local memory and the remote system log server.

4.11.3 SNMP Agent

Choose "**Management**"→"**SNMP Agent**", 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 any 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.

An **SNMP Agent** is an application running on the 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.

An **SNMP Manager** or SNMP Service is an application that performs the operational roles of generating SNMP messages/requests to modify and retrieve management information, and receiving the requested information and trap-event reports that are generated by the SNMP agent. SNMP Manager is the third-party management system. Monitor one is an SNMP Manager.

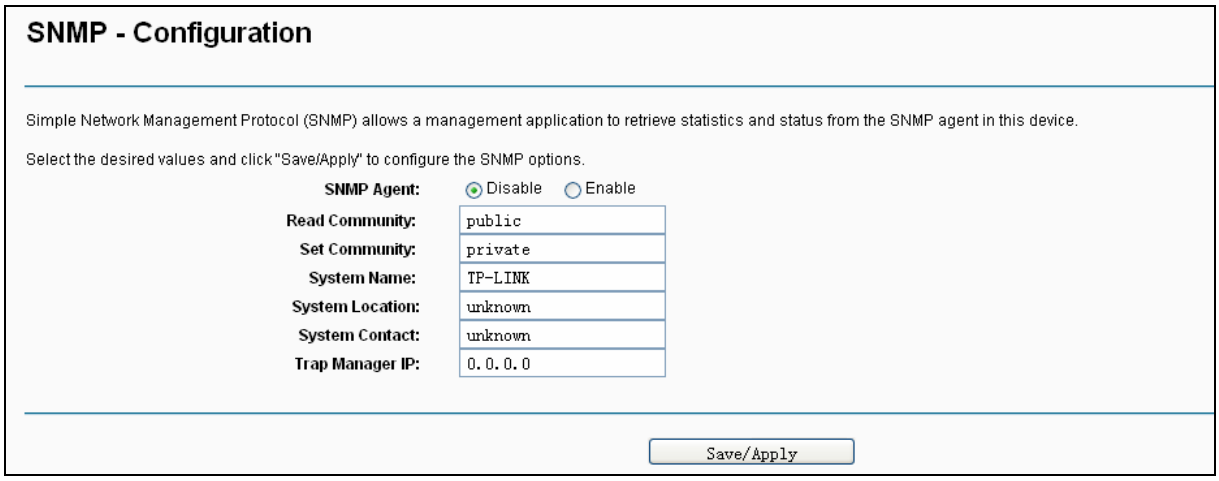


Figure 4-129

- **SNMP Agent:** You can select the checkbox to disable or enable the function.

Note:

SNMP Community string provides a simple method of authentication between the router (SNMP Agent) and a remote network manager (SNMP Manager). You can specify the community string as the password to authenticate the management station to the router.

- **Read Community:** This field allows you to specify the SNMP Community string which provides read-only access to the router that the community is only permitted to read the device configuration. The default value is “public”.
- **Set Community:** This field allows you to specify the SNMP Community string which provides read and write access to the router that the community has the authority to read and change the device configuration. The default value is “private”.
- **System Name:** Enter alphanumeric string to specify an SNMP community string name. Your router (SNMP agents) will expose management data on the managed systems as this "system name".
- **System Location:** The person to notify when problems occur.
- **System Contact:** The location of the person that is identified as the system contact.
- **Trap Manager IP:** Enter the IP address of the SNMP Manager，where the SNMP Agent forwards trap notifications.

Select the desired values and click **Save/Apply** to configure the SNMP options.

4.11.4 TR-069 client

Choose “**Management**”→“**TR-069 client**”, you can see the TR-069 client - Configuration screen as shown below.

TR-069（WAN Management Protocol）allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

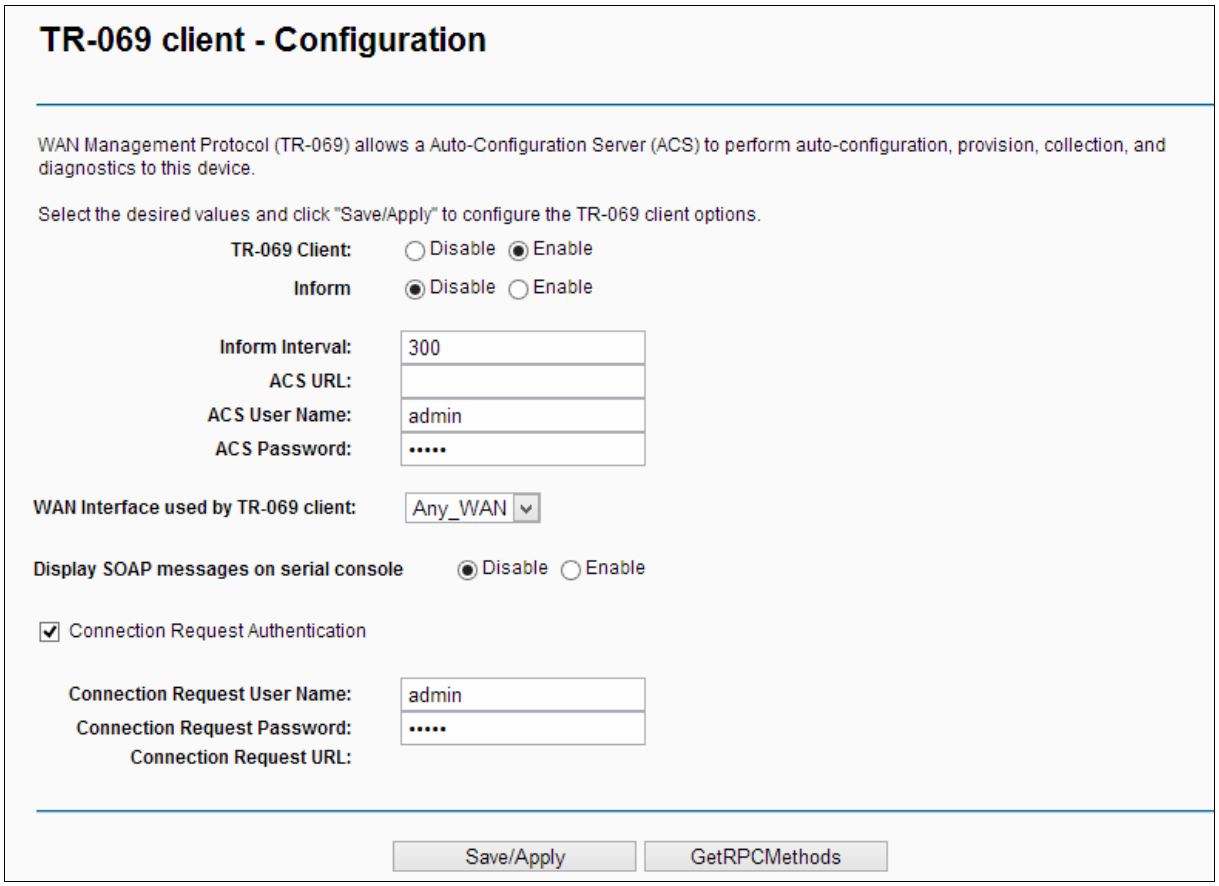


Figure 4-130

- **TR-069 Client:** You can select the checkbox to disable or enable the TR-69 Client function.
- **Inform:** You can select the checkbox to disable or enable the **Inform Interval.**
- **Inform Interval:** Type the interval time of your modem router contact with the **ACS**.
- **ACS URL:** Please accept this information from your ISP. And through **ACS** (Auto-Configuration Server) you can perform auto-configuration, provision, collection, and diagnostics to this modem router.
- **ACS User Name:** Please accept this User Name information from your ISP.
- **ACS Password:** Please accept the Password information from your ISP.

☞ **Note:**

If you want to log on the **ACS**, you must own the **ACS User Name** and **ACS Password**.

- **WAN Interface used by TR-069 Client**: Please select the WAN Interface from the drop-down list to perform this function.
- **Connection Request User Name:** Type the Connection Request User Name, set it yourself.
- **Connection Request Password:** Type the Connection Request Password, set it yourself.

☞ **Note:**

The Connection Request User Name and Connection Request Password used for **ACS** log on the router and manage it.

Select the desired values and click **Save/Apply** to configure the TR-069 client options.

4.11.5 Internet Time

Choose "**Management**"→"**Internet Time**", you can see the Time settings screen as shown below. Here you can configure the time of the modem router.

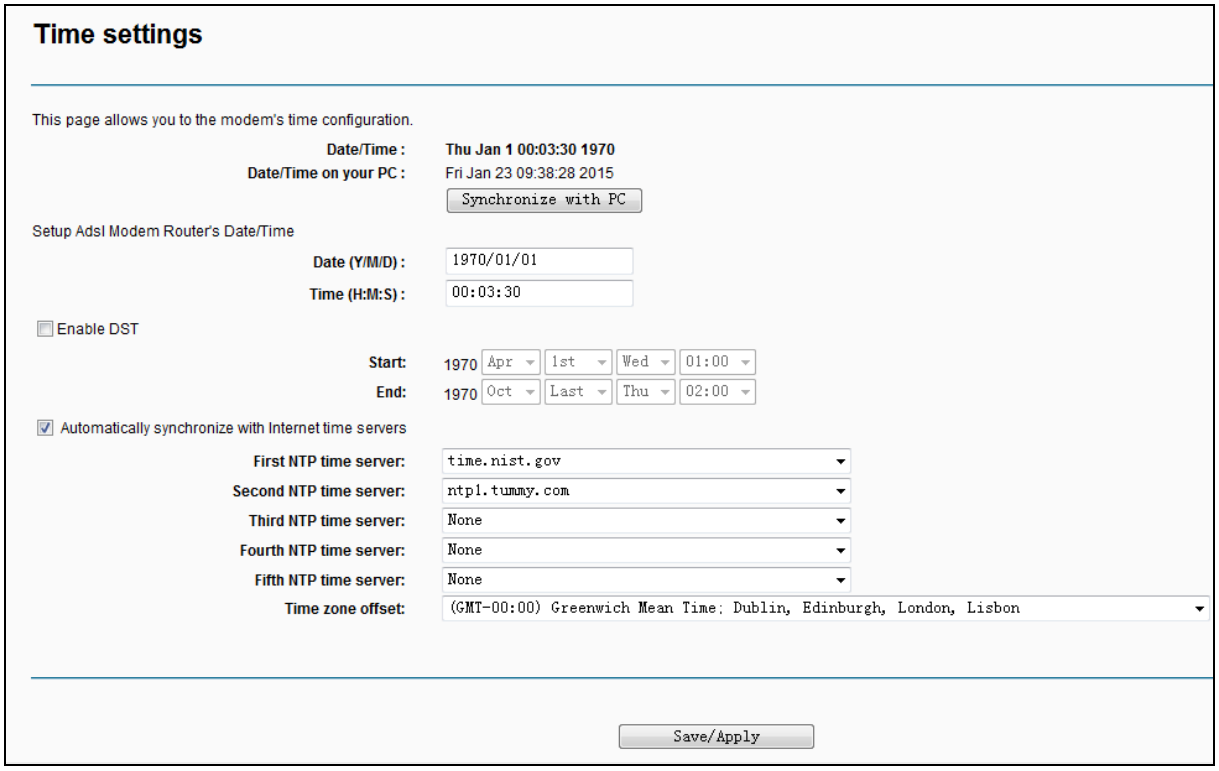


Figure 4-131

- **Enable DST:** Select the checkbox to enable daylight saving function.

4.11.6 Access Control

There are two submenus under the Access Control menu: **Passwords** and **Remote Access**. The detailed explanations for each submenu are provided below.

4.11.6.1 Passwords

Choose "**Management**"→"**Access Control**"→"**Passwords**", you can see the screen (shown in Figure 4-132) which allows you to change the factory default password of the modem router. The default password is the same as the user name, which is admin/admin, support/support, and user/user respectively.

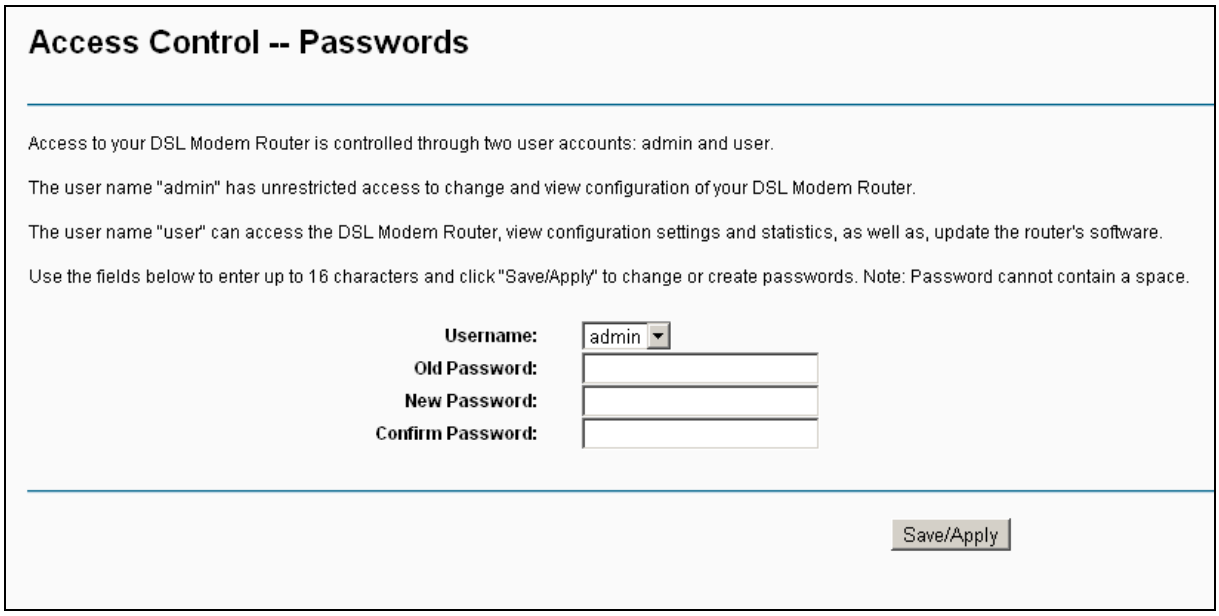


Figure 4-132

To change the password:

1. Select the **Username** whose password you want to change.
2. Enter the **Old Password** in the text box.
3. Enter the **New Password** and **Confirm Password**. The Confirm Password should be the same as the New Password.
4. Click **Save/Apply** to make your change take effect.

☞ **Note:**

1) Access to your DSL modem router is controlled through two user accounts: admin and user. The user name "admin" has unrestricted access to change and view configuration of your DSL modem router. The user name "user" can access the DSL modem router, view configuration settings and statistics, as well as, update the modem router's software.
2) Admin accounts can do remote management. For security reasons, please change the default password for this account when remote access function is enabled.
3) The password cannot contain a space, and its maximum length is 16 characters.

4.11.6.2 Remote Access

Choose "**Management**"→"**Access Control**"→"**Remote Access**", you can see the screen (shown in Figure 4-133) which allows you to change the factory default password of the modem router.

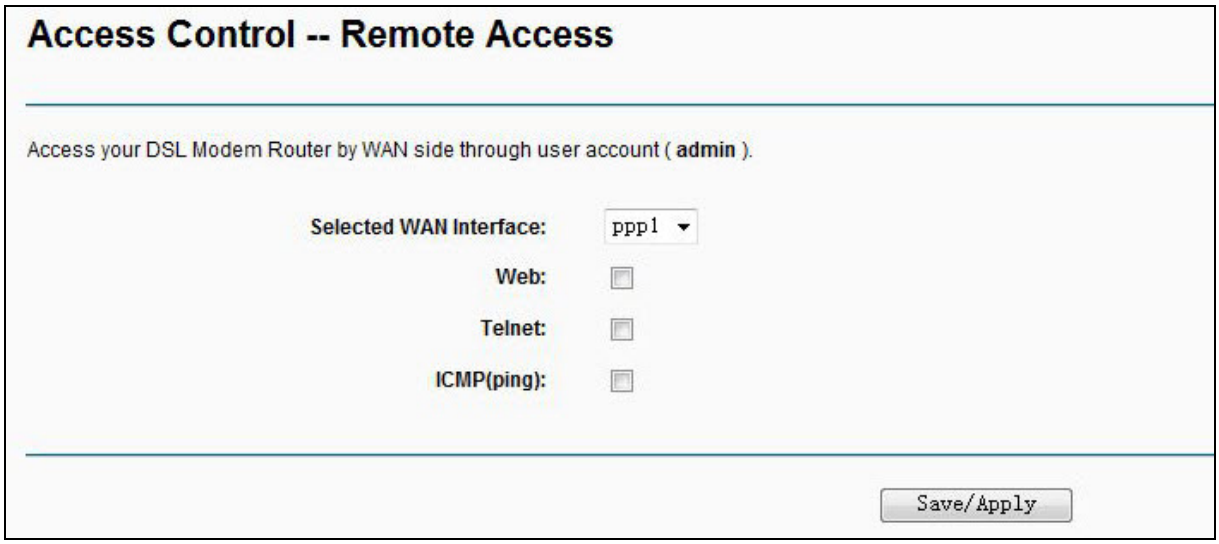


Figure 4-133

- **Web**：Select this box, you can access your modem router via web.
- **Telnet:** Select this box, you can access your modem router via command line.
- **ICMP(ping):** Select this box, PC in public network can ping the WAN address of the modem router.

Click **Save/Apply** to make your change take effect.

4.11.7 Upgrade Firmware

Choose "**Management**"→"**Upgrade Firmware**", you can see the screen (shown in Figure 4-134) which allows you to upgrade the latest version software to keep the modem router up to date.

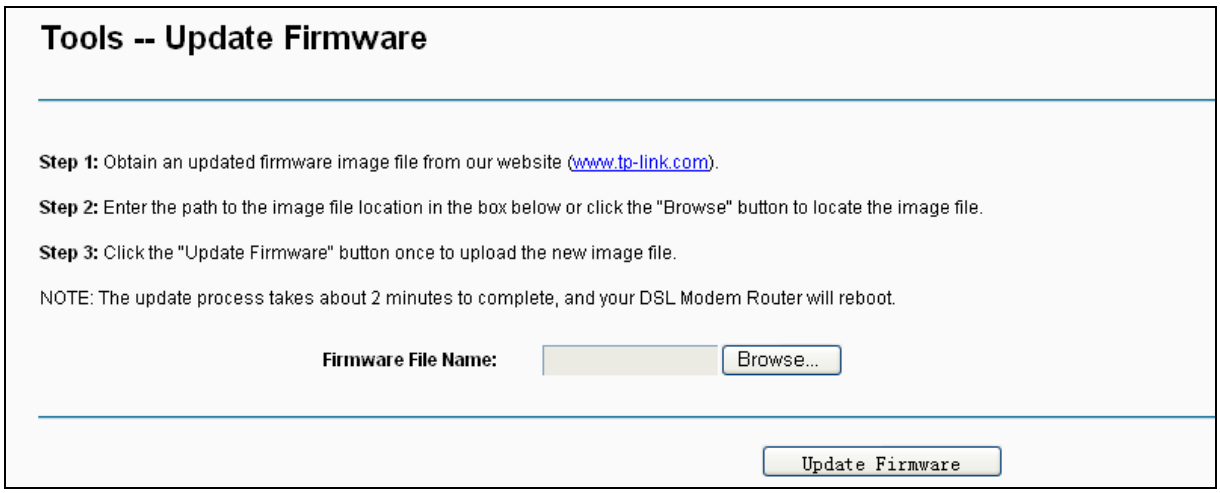


Figure 4-134

- **Browse:** Click the button to locate the latest software for the device.
- **Update Firmware:** After you have selected the latest software, click the button.

To update the modem router's software:

1. Download the latest software upgrade file from the **TP-LINK** website (http://www.tp-link.com).

2. Click **Browse** to view the folders and select the image file or enter the exact path to the image file location in the text box.
3. Click the **Update Firmware** button.

☞ **Note:**

1) There is no need to upgrade the firmware unless the new firmware has a new feature you want to use. However, when experiencing problems caused by the modem router itself, you can try to upgrade the firmware.
2) Do NOT revert to a previous version of firmware.
3) Before upgrading the modem router's firmware, you should write down some of your customized settings to avoid losing important configuration settings of the modem router.
4) Do not turn off the modem router or press the RESET button while the software is being updated.
5) The modem router will reboot after the Upgrading is finished.

4.11.8 Reboot

Choose "**Management**"→"**Reboot**", you can see the screen (shown in Figure 4-135) which allows you to reboot the modem router.

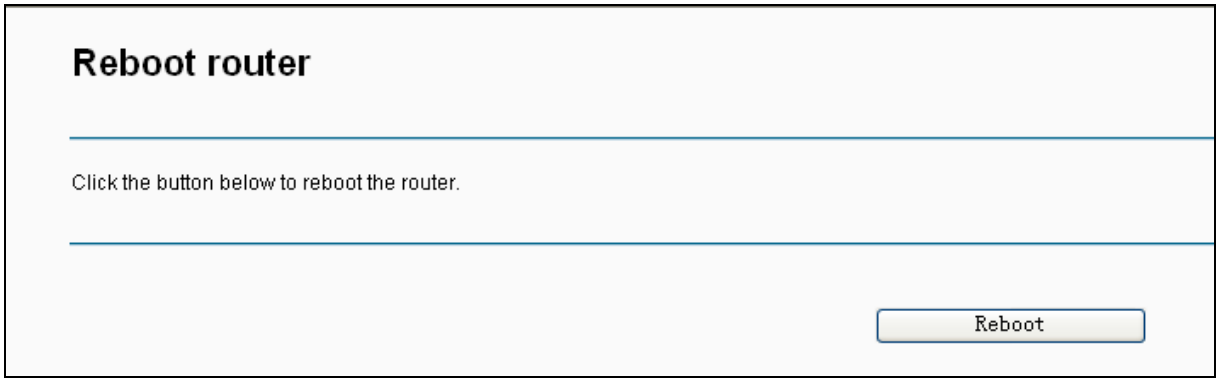


Figure 4-135

☞ **Note:**

1) After you clicked the **Reboot** button, please wait for a while before reopening your web browser.
2) Do not turn off the modem router or press the **RESET** button while the modem router is rebooting.
3) If necessary, reconfigure your PC's IP address to match your new configuration.

4.12 Logout

Choose "**Logout**", and you will back to the login screen as shown in Figure 4-136.

TP-LINK
300Mbps Wireless N USB ADSL2+ Modem Router
Model No. TD-W8968
Login
Copyright © 2015 TP-LINK Technologies Co., Ltd. All rights reserved.

Figure 4-136

Appendix A: Specifications

General	
Standards and Protocols	ANSI T1.413, ITU G.992.1, ITU G.992.2, ITU G.992.3, ITU G.992.5, IEEE 802.3, IEEE 802.3u, IEEE 802.11b , IEEE 802.11g , 802.11n TCP/IP, IPoA , PPPoA , PPPoE, SNTP, HTTP, DHCP, ICMP, NAT
Safety & Emissions	FCC, CE
Ports	Four 10/100M Auto-Negotiation RJ45 ports（Auto MDI/MDIX) One RJ11 port One USB 2.0 port
LEDs	Power, ADSL, Internet, WLAN, **WPS**, USB, 1,2,3,4(LAN),
Network Medium	10Base-T: UTP category 3, 4, 5 cable 100Base-TX: UTP category-5 Max line length: 6.5Km
Data Rates	Downstream: Up to 24Mbps Upstream: Up to 3.5Mbps（With Annex M enabled）
System Requirement	Internet Explorer 5.0 or later, Netscape Navigator 6.0 or later Win 9x/ ME/ 2000/ XP/ Vista/ 7/ 8/ 8.1/10
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. What can I do if I don't know or forget my password?

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

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

T2. 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.

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

- Click the **Apple** icon on the upper left corner of the screen.
- Go to "**System Preferences** -> **Network**".
- Select **Airport** on the left menu bar, and then click **Advanced** for wireless configuration; or select **Ethernet** for wired configuration.
- In the **Con-figure IPv4** box under **TCP/IP**, select **Using DHCP**.
- Click **Apply** to save the settings.

For Windows 7

- Click "**Start** -> **Control Panel** -> **Network and Internet** -> **View network status** -> **Change adapter settings**".
- Right-click **Wireless Network Connection** (or **Local Area Connection**), and then click **Properties**.
- Select **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
- Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Then click **OK**.

For Windows XP

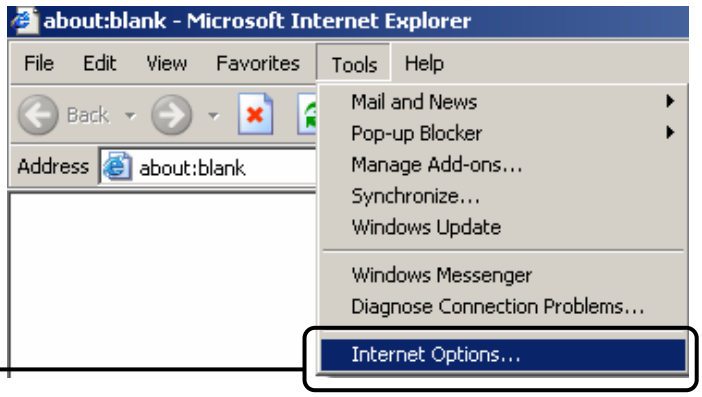
- Click "**Start** -> **Control Panel** -> **Network and Internet Connections** -> **Network Connections**".
- Right-click **Wireless Network Connection** (or **Local Area Connection**), and then click **Properties**.
- Select **Internet Protocol (TCP/IP)**, and then click **Properties**.
- Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Then click **OK**.

For Windows 8

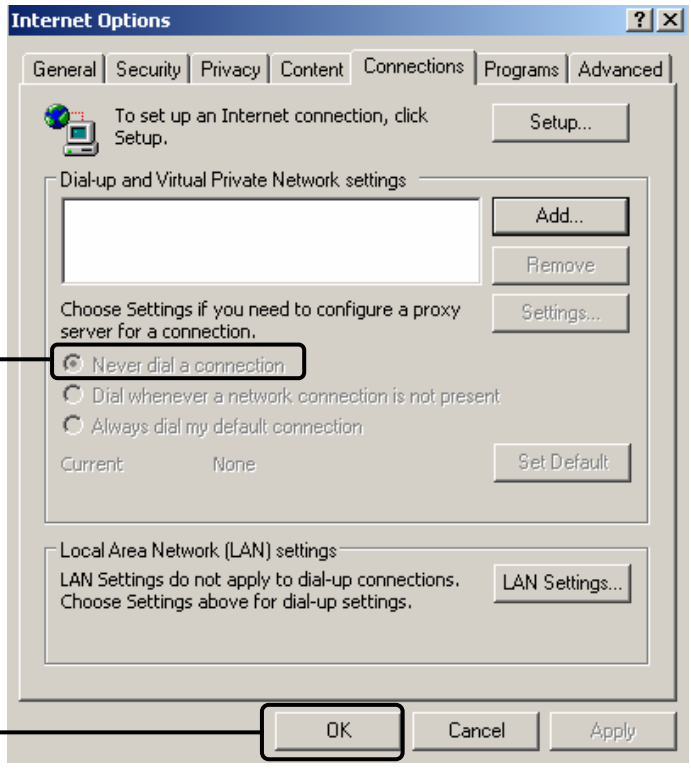
- Move your mouse to the lower right corner and you will see **Search** icon in the Popups. Go to " -> **Apps**". Type **Control Panel** in the search box and press **Enter**, then you will go to **Control Panel**.
- Click "**View network status and tasks** > **Change adapter settings**".
- Right-click "**Ethernet**" and then select **Properties**.
- 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** 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 feel free to contact our Technical Support if the problem still exists.

T5. How can I configure the USB features?

Please refer to our Application Guides. They can be found on the web: http://www.tp-link.com/app/usb.

☞ **Note:**

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