TP-LINK®

User Guide

TD-W8960N

300Mbps Wireless N ADSL2+ Modem Router

Rev: 5.0.0
1910010662

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 © 2012 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.

National Restrictions

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

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

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

This device has been designed to operate with the antennas listed below, and having a maximum gain of 3 dBi. Antennas not included in this list or having a gain greater than 3 dBi are strictly prohibited for use with this device. The required antenna impedance is 50 ohms.

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

Industry Canada Statement:

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions:

(1)This device may not cause harmful interference, and

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

IMPORTANT NOTE:

Radiation Exposure Statement:

This equipment complies with Canada radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes:

(1) Le dispositif ne doit pas produire de brouillage préjudiciable, et

(2) Ce dispositif doit accepter tout brouillage reçu,y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

NOTE IMPORTANTE:

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

Korea Warning Statements:

당해 무선설비는 운용중 전파혼신 가능성이 있음.

NCC Notice:

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

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

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

DECLARATION OF CONFORMITY

For the following equipment:

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

Model No.: **TD-W8960N**

Trademark: **TP-LINK**

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

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

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

ETSI EN 300 328 V1.7.1: 2006

ETSI EN 301 489-1 V1.8.1:2008& ETSI EN 301 489-17 V2.1.1:2009

EN 55022:2010

EN 55024:2010

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

EN 61000-3-3:2008

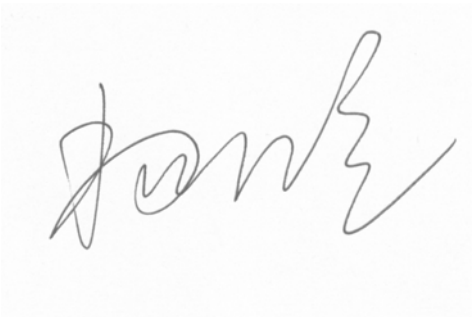
EN60950-1:2006+A11：2009+A1:2010+A12:2011

EN62311:2008

The product carries the CE Mark:

CE1588

Person is responsible for marking this declaration:



Yang Hongliang

Product Manager of International Business

Date of issue: 2012

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 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 Router **7**

2.1 System Requirements 7

2.2 Installation Environment Requirements 7

2.3 Connecting the Router 7

Chapter 3. Quick Installation Guide **9**

3.1 Configuring the PC 9

3.2 Quick Installation Guide 12

Chapter 4. Configuring the Router **16**

4.1 Login 16

4.2 Device Info 16

4.3 Quick Setup 17

4.4 Advanced Setup 17

4.4.1 Layer2 Interface 18

4.4.2 WAN Service 21

4.4.3 MAC Clone 29

4.4.4 LAN 30

4.4.5 NAT 31

4.4.6 Security 36

4.4.7 Parental Control 39

4.4.8 Quality of Service 41

4.4.9 Bandwidth Control 44

4.4.10 Routing 46

4.4.11 DNS 48

4.4.12 DSL 50

4.4.13 UPnP 51
4.4.14 Interface Grouping 52
4.4.15 IPSec 53
4.4.16 Multicast 56
4.5 Wireless 57
4.5.1 Basic 57
4.5.2 Security 58
4.5.3 MAC Filter 73
4.5.4 Wireless Bridge 73
4.5.5 Advanced 75
4.5.6 Station info 76
4.6 Diagnostics 77
4.7 Management 77
4.7.1 Settings 77
4.7.2 System Log 80
4.7.3 SNMP Agent 81
4.7.4 TR-069 client 82
4.7.5 Internet Time 83
4.7.6 Access Control 84
4.7.7 Update Firmware 85
4.7.8 Reboot 86
Appendix A: FAQ 87
Appendix B: Configuring the PC 90
Appendix C: Specifications 97
Appendix D: Glossary 98
Appendix E: Technical Support 102

Package Contents

The following contents should be found in your package:

- One TD-W8960N 300Mbps Wireless N ADSL2+ Modem Router
- One power Adapter for TD-W8960N 300Mbps Wireless N ADSL2+ Modem Router
- Quick Installation Guide
- One RJ45 cable
- Two RJ11 cables
- One ADSL splitter
- One Resource CD for TD-W8960N 300Mbps Wireless N ADSL2+ Modem Router, including:
  - This User Guide
  - Other Helpful Information

☞ **Note:**

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

Chapter 1. Product Overview

Thank you for choosing the **TD-W8960N 300Mbps Wireless N ADSL2+ Modem Router**.

1.1 Overview of the Router

The TD-W8960N 300Mbps Wireless N 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-W8960N 300Mbps Wireless N ADSL2+ Modem Router utilizes integrated ADSL2+ transceiver and high speed MIPS CPU. The Router supports full-rate ADSL2+ connectivity conforming to the ITU and ANSI specifications.

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

Incredible Speed

The 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 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.

Multiple Security Protections

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-W8960N 300Mbps Wireless N ADSL2+ Modem Router provides complete data privacy.

Flexible Access Control

The 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.

Simple Installation

Since the 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 Router, please look through this guide to know all the Router's functions.

1.2 Main Features

- Complies with IEEE 802.11n to provide a wireless data rate of up to 300Mbps
- One RJ11 LINE port, four 10/100M Auto-Negotiation RJ45 LAN ports, supporting Auto MDI/MDIX
- 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
- Adopts 300M wireless LAN transmission 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
- Supports WPS
- Built-in firewall supporting IP address filtering, MAC address filtering and parental control
- Built-in DHCP server

1.3 Panel Layout

1.3.1 The Front Panel

The Router's LEDs are located on the front panel.

Figure 1-1

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

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 function is disabled.
(WPS)	On	A wireless device has been successfully added to the network by WPS function.
	Flash	WPS handshaking is in process and will continue for about 2 minutes. Please press the WPS button on other wireless devices that you want to add to the network while the LED is flashing.
	Off	The WPS function is disabled or the wireless device fails to be added to the network in 2 minutes after WPS function is enabled. Please refer to 4.5.2.1 WPS Setup for more information.
(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 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

The Router's ports, where the cables are connected, and RESET button are located on the back panel.

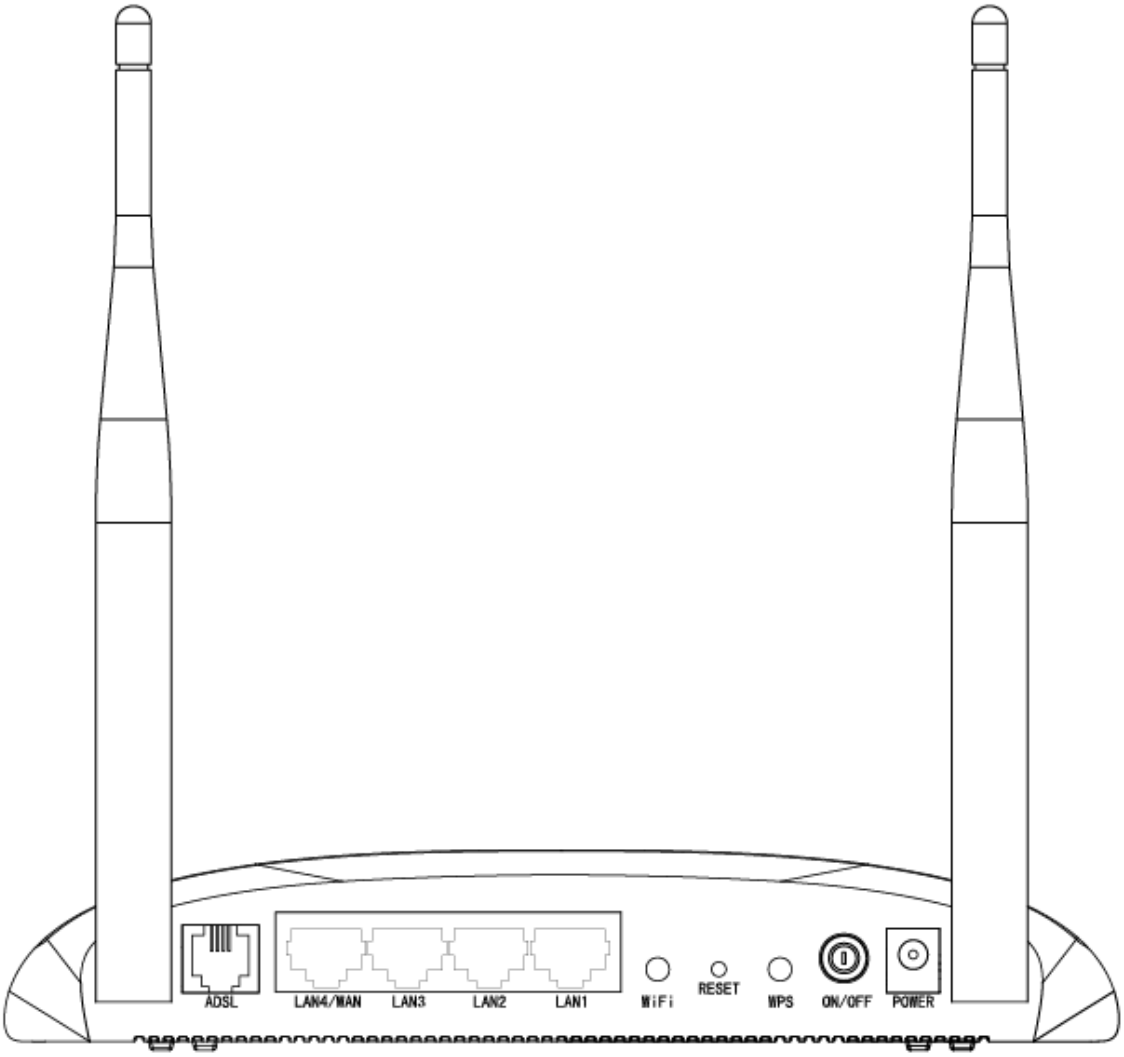


Figure 1-2

- **ADSL:** Connect to the Modem Port of Splitter or to the telephone line.
- **LAN1, LAN2, LAN3, LAN4/WAN:** Through these ports, you can connect the 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.
- **WiFi:** The switch for the WiFi function.
- **RESET:** There are two ways to reset the Router's factory defaults.

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

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

- **WPS:** The switch for the WPS function. For details, please refer to 4.5.2.1 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 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

- Place the Router in a well ventilated place far from any heater or heating vent
- Avoid direct irradiation of any strong light (such as sunlight)
- Keep at least 2 inches (5 cm) of clear space around the Router
- Operating temperature: 0℃~40℃ (32℉~104℉)
- Operating Humidity: 10% ~ 90% RH (non-condensing)

2.3 Connecting the Router

Back to LED Explanation

Before installing the Router, please make sure your broadband service provided by your ISP is available. If there is any problem, please contact your ISP. After that, please install the Router according to the following steps. Don't forget to pull out the power plug and keep your hands dry.

1. Locate an optimum location for the Router. The best place is usually at the center of your wireless network.
2. Adjust the direction of the antenna. Normally, upright is a good direction.
3. Connect your PC and Switch/Hub in your LAN to the LAN Ports of the Router. (If you have a wireless NIC and want to have wireless connection, please skip this step.)
4. Connect the telephone line to the Line port on the Router. Or you can access the Internet and make calls at the same time by using a separate splitter to divide the data and voice. The external splitter has three ports:
   - LINE: Connect to the wall jack
   - PHONE: Connect to the phone sets
   - MODEM: Connect to the ADSL LINE port of device

   Plug one end of the twisted-pair ADSL cable into the ADSL LINE port on the rear panel of device. Connect the other end to the MODEM port of the external splitter.
5. Connect the power adapter to the power plug of the Router, and the other end into an electrical outlet. The electrical outlet shall be installed near the device and shall be easily accessible.
6. Turn on the ON/OFF switch to power the device. It will start to work automatically.

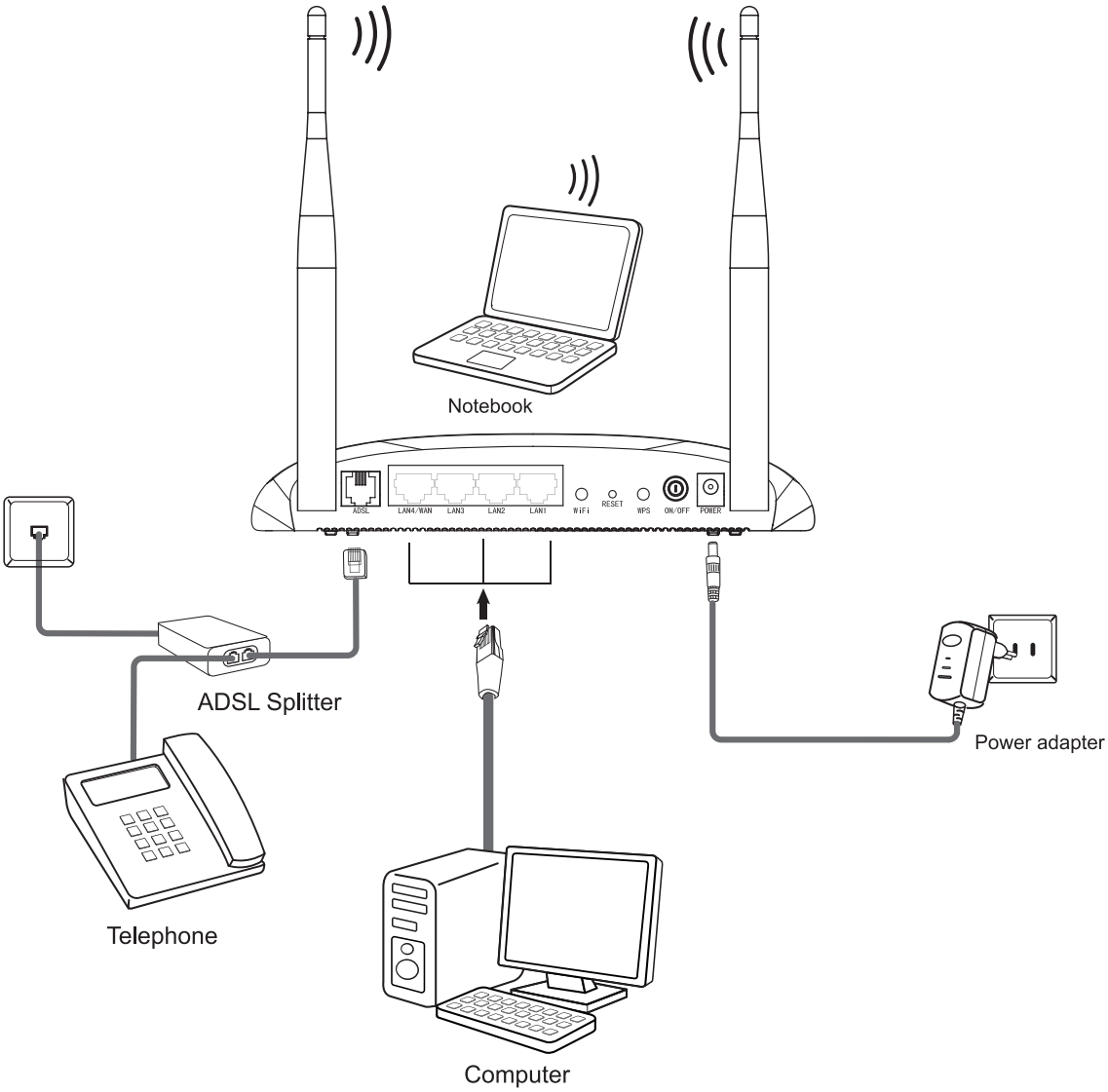

Notebook
ADSL
LAN4/WAN
LAN3
LAN2
LAN1
WiFi
RESET
WPS
ON/OFF
POWER
ADSL Splitter
Power adapter
Telephone
Computer

Figure 2-1

Chapter 3. Quick Installation Guide

This chapter will show you how to configure the basic functions of your **TD-W8960N 300Mbps Wireless N ADSL2+ Modem Router** using **Quick Setup Wizard** within minutes.

3.1 Configuring the PC

After you directly connect your PC to the **TD-W8960N** or connect your adapter to a Hub/Switch which has connected to the Router, you need to configure your PC's IP address. Follow the steps below to configure it. Here takes Windows XP for example. For more details, please refer to Appendix B.

Step 1: Click the **Start** menu on your desktop, right click **My Network Places**, and then select **Properties** (shown in Figure 3-1).

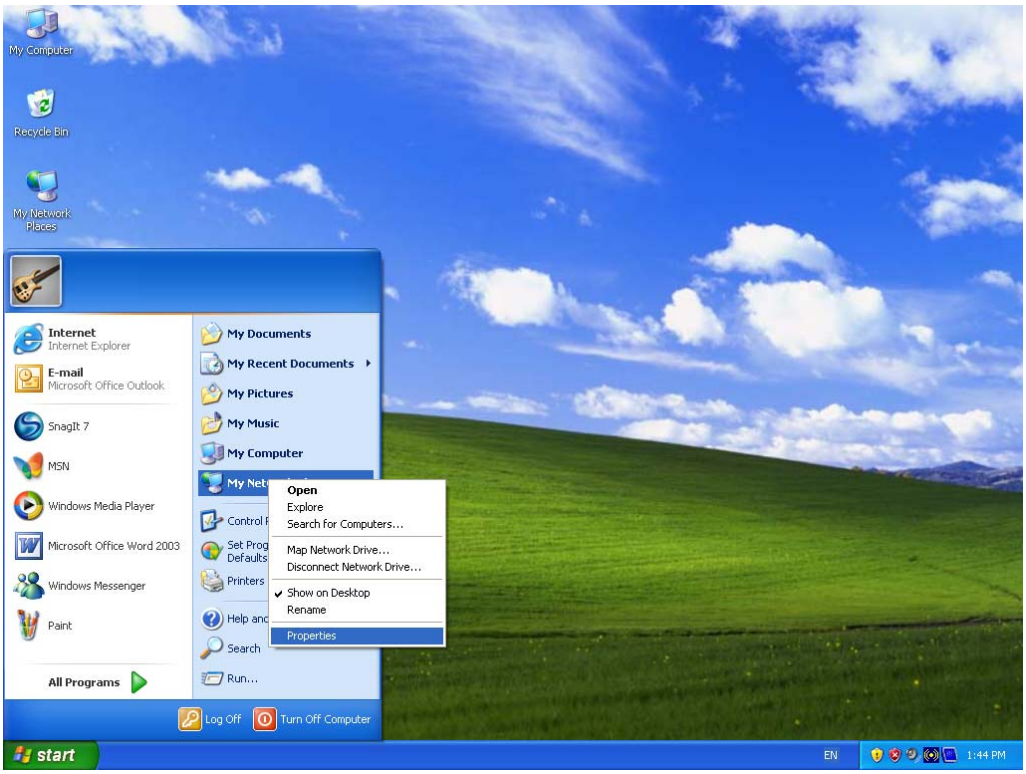


Figure 3-1

Step 2: Right click **Local Area Connection** (LAN), and then select **Properties**.

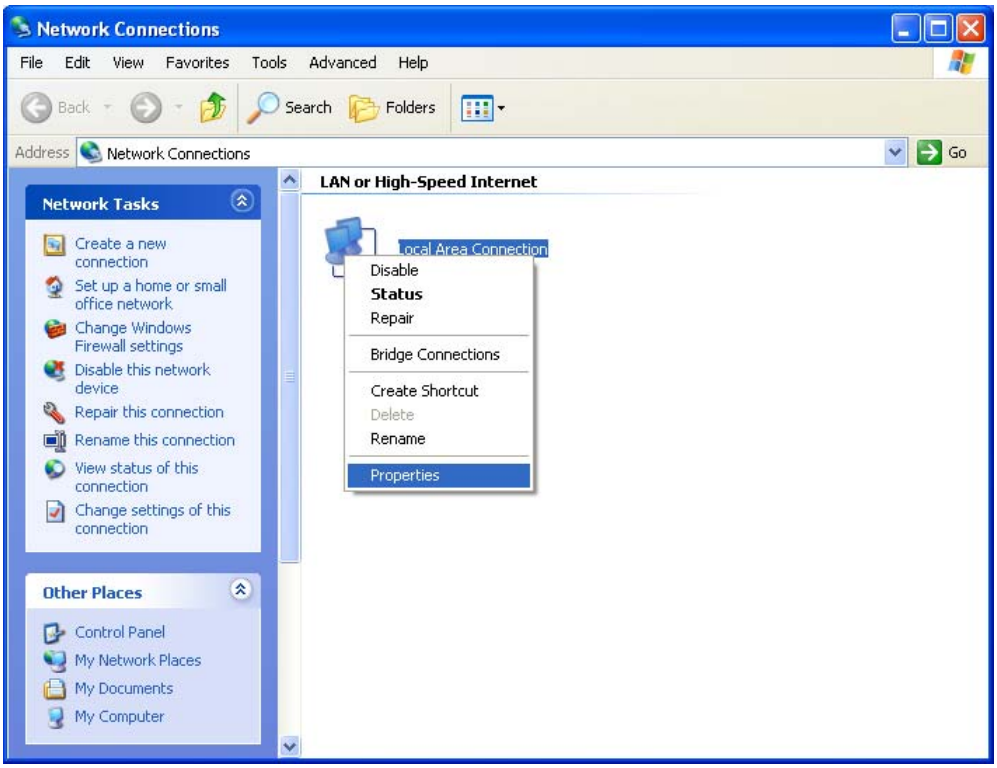


Figure 3-2

Step 3: Select **General** tab, highlight **Internet Protocol (TCP/IP)**, and then click the **Properties** button.

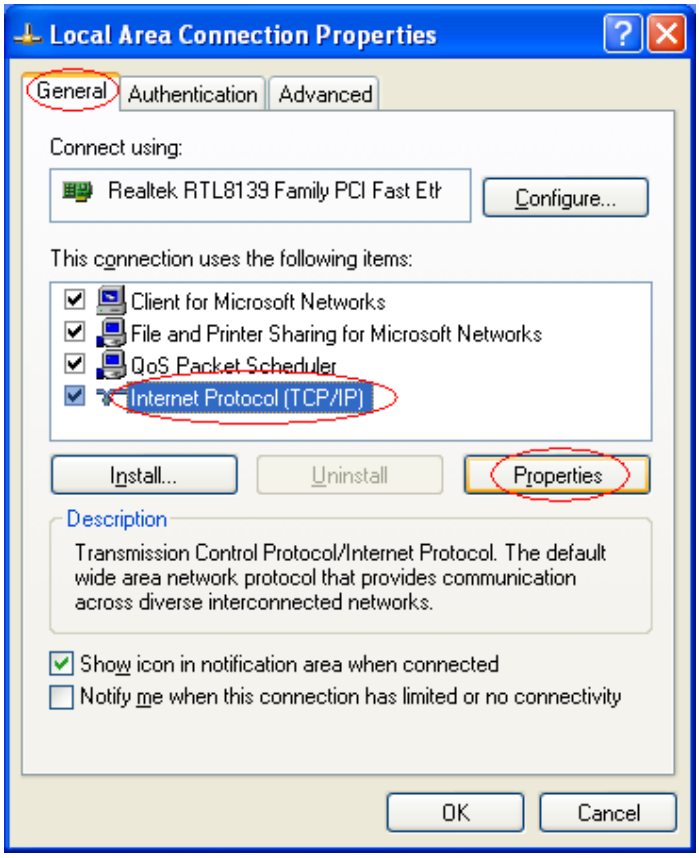


Figure 3-3

Step 4: Configure the IP address as Figure 3-4 shows. After that, click **OK**.

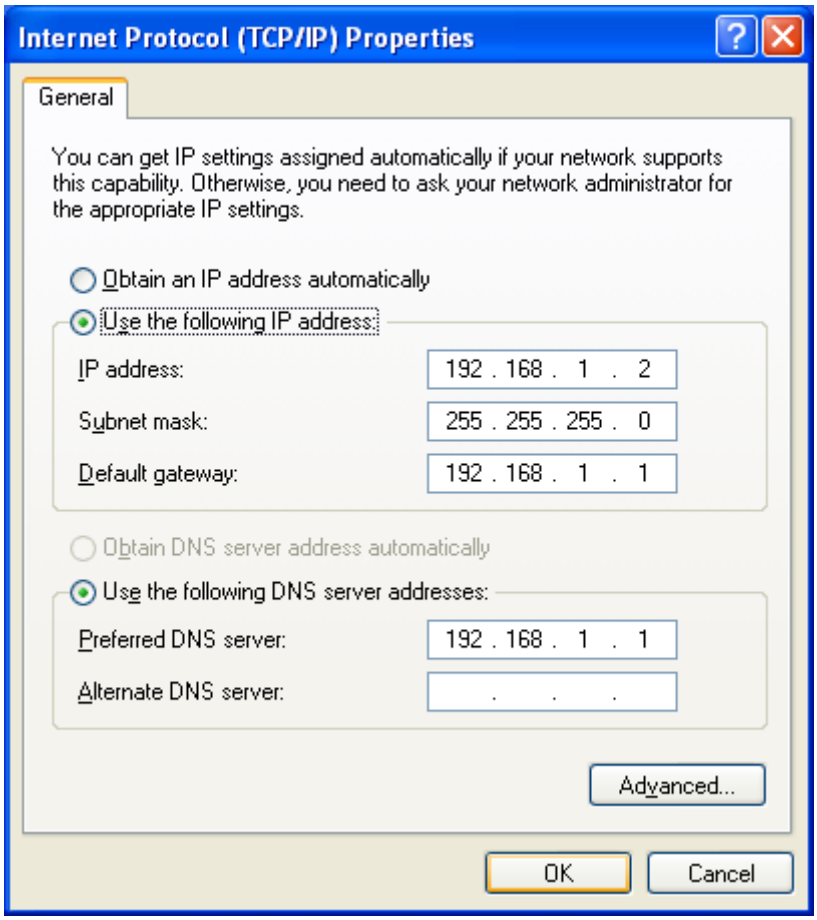


Figure 3-4

☞ **Note:**

You can configure the PC to get an IP address automatically, select “Obtain an IP address automatically” and “Obtain DNS server address automatically” in the screen above.

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

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

```
Pinging 192.168.1.1 with 32 bytes of data:

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

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

Figure 3-5

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

```
Pinging 192.168.1.1 with 32 bytes of data:

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

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

Figure 3-6

You can check it following the steps below:

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

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

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

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

3.2 Quick Installation Guide

With a Web-based utility, it is easy to configure and manage the TD-W8960N 300Mbps Wireless N 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.

1. To access the configuration utility, open a web-browser and type the default address http://192.168.1.1 in the address field of the browser.

Figure 3-7

After a moment, a login window will appear, similar to the Figure 3-8. Enter **admin** for the User Name and Password, both in lower case letters. Then click the **OK** button or press the **Enter** key.

Figure 3-8

☞ **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.

2. After your successful login, you will see the Login screen as shown in Figure 3-9. Click **Quick Setup** menu to access **Quick Setup Wizard**.

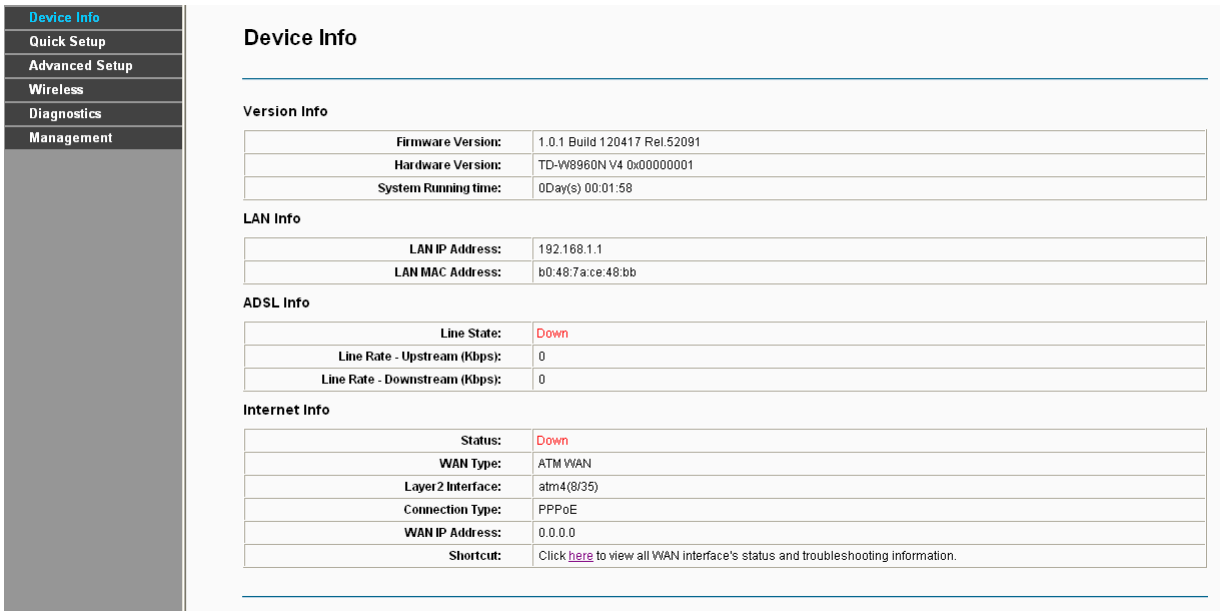


Figure 3-9

3. Change the VPI or VCI values which are used to define a unique path for your connection. If you have been given specific settings for this to configuration, type in the correct values assigned by your ISP. Here we select PPPoE ADSL WAN Link Type for example, enter the

PPP Username and **PPP Password** given by your ISP, and then click **Next**.

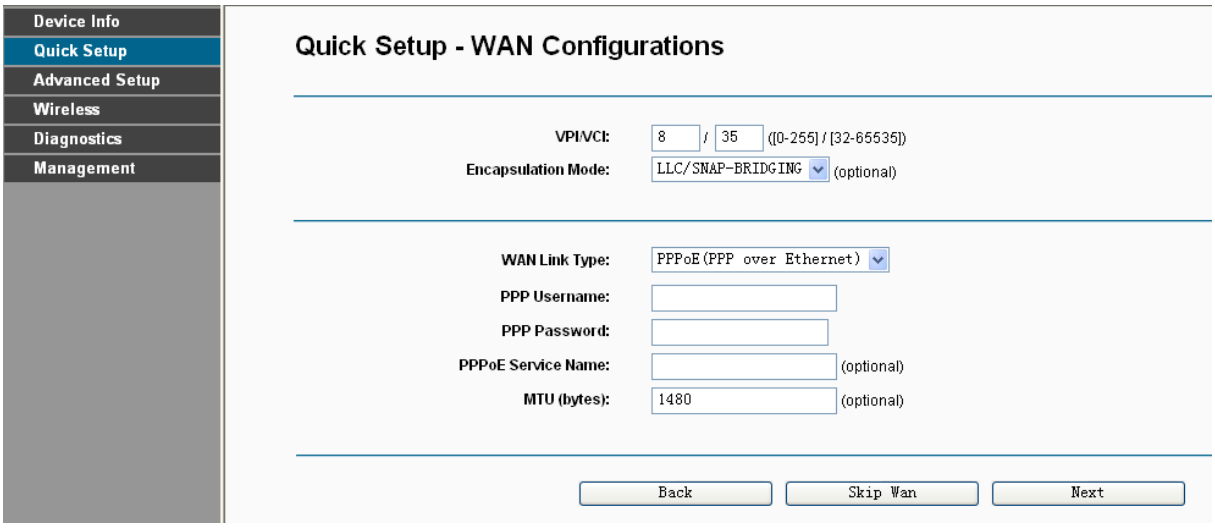


Figure 3-10

Note:

The Quick Setup Wizard will guide you to configure the WAN Service over ATM interface.

4. On the **Wireless Configurations** screen, we use the default SSID, select Network Authentication (take **Mixed WPA2/WPA-PSK Personal** for example), set a Pre-Shared Key, and then click **Save** to continue.

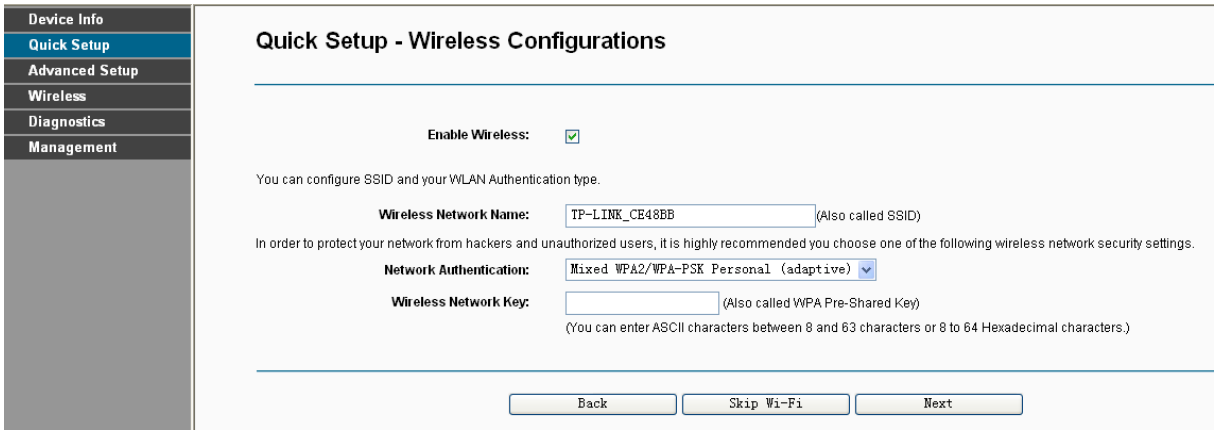


Figure 3-11

Note:

The default **ATM&WAN** service will be cleared after clicking the **Next** button on this Quick Setup page.

5. You will see the **Summary** screen below, click **Confirm** to configure these settings.

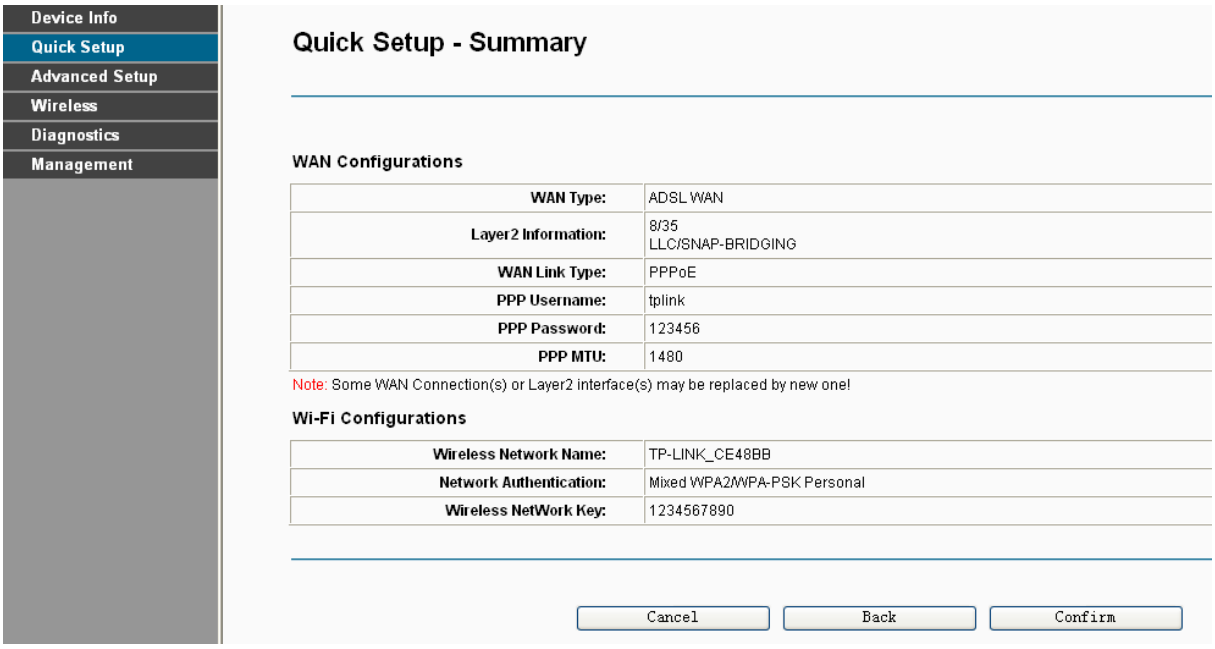

Device Info
Quick Setup
Advanced Setup
Wireless
Diagnostics
Management
Quick Setup - Summary
WAN Configurations
WAN Type: ADSL WAN
Layer2 Information: 8/35 LLC/SNAP-BRIDGING
WAN Link Type: PPPoE
PPP Username: tplink
PPP Password: 123456
PPP MTU: 1480
Note: Some WAN Connection(s) or Layer2 interface(s) may be replaced by new one!
Wi-Fi Configurations
Wireless Network Name: TP-LINK_CE48BB
Network Authentication: Mixed WPA2/WPA-PSK Personal
Wireless NetWork Key: 1234567890
Cancel
Back
Confirm

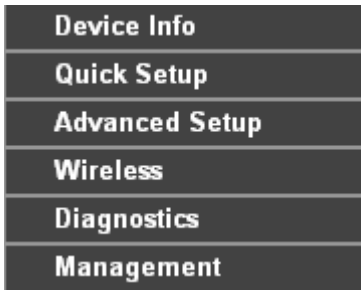
Figure 3-12

Chapter 4. Configuring the 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 six 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 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 TD-W8960N connection. This information will vary depending on the settings of the Router configured on the Advanced Setup screen.

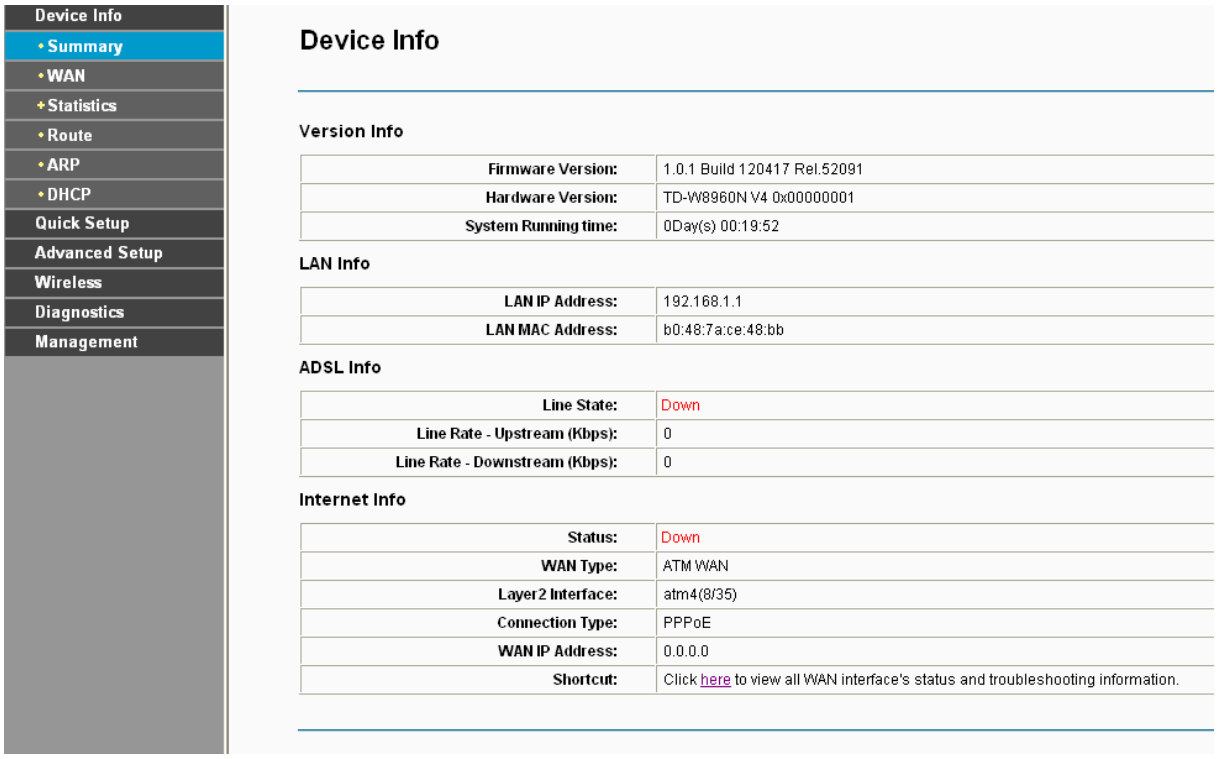


Figure 4-1

☞ **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 Advanced Setup

Choose "**Advanced Setup**", there are many submenus under the main menu. Among the submenus, **Layer2 Interface**, **WAN Service**, **LAN** etc. are default menus, while **NAT**, **IP/MAC filtering** of the **Security**, **Quality of Service** and **DNS** will appear only when you select some corresponding functions. 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 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 (4.4.1 Layer2 Interface) according to the connection ISP provides you, and then to select the type of the connection (4.4.2 WAN Service) for the further configuration.

4.4.1 Layer2 Interface

Choose "**Advanced Setup**"→"**Layer2 Interface**", and you can select WAN Service Interface (layer2 interface) over **ATM interface** or **ETH interface**.

- **ATM Interface:** Configure the Router to access Internet as an ADSL user. ISP provides you VPI (Virtual Path Identifier), VCI (Virtual Channel Identifier) settings and the DSL Interface with RJ11 connector. (Figure 2-1)
- **ETH Interface:** Configure the Router to access Internet as an Ethernet user. ISP provides you Broadband Internet Service and the Ethernet Interface with RJ45 connector.

4.4.1.1 ATM interface

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

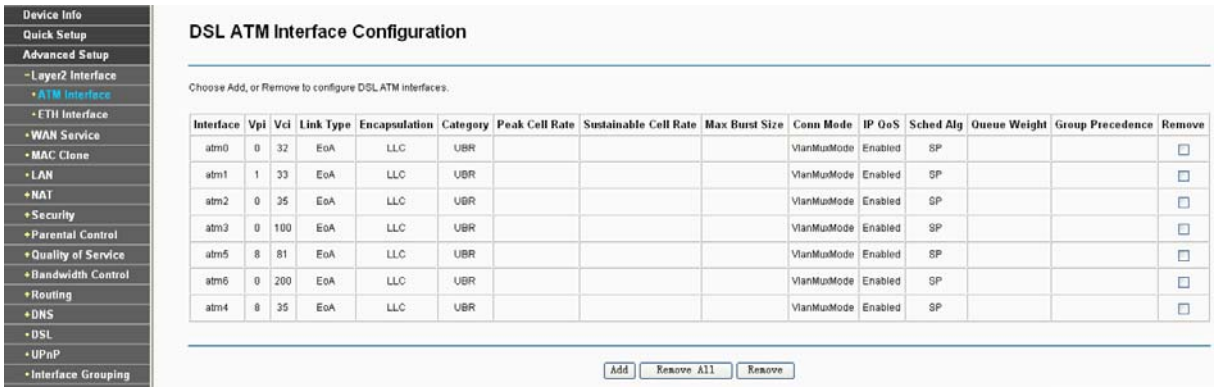


Figure 4-2

- **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 4.4.2 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.

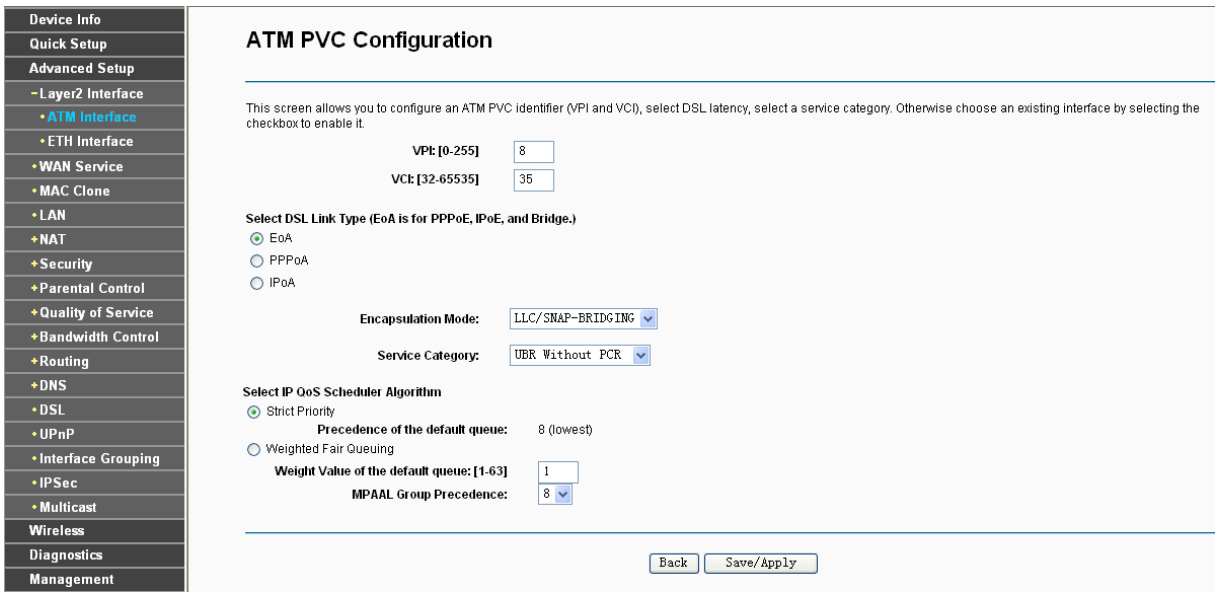


Figure 4-3

- **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 **4.4.8 Quality of Service**.

4.4.1.2 ETH interface

Choose "**Advanced Setup**"→"**Layer2 Interface→ETH Interface**", you can configure ETH WAN interfaces on the screen below.

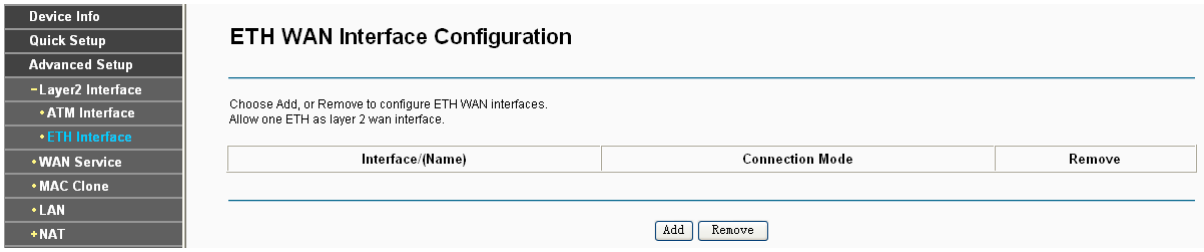


Figure 4-4

Note:

To make sure the ETH port available, you should first choose "**Advanced Setup**"→"**LAN Ports**" to enable the Virtual LAN Ports feature.

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

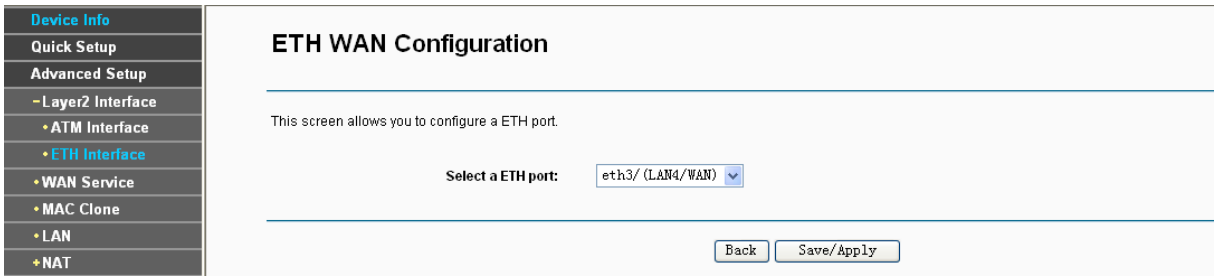


Figure 4-5

- **ETH port**: Select an ETH port to configure as the WAN port.

Click **Save/Apply** to save your settings and then you will see the screen similar to Figure 4-6.

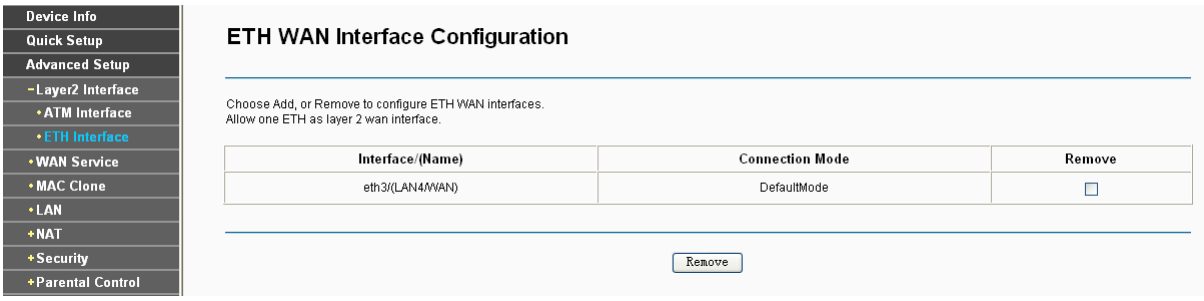


Figure 4-6

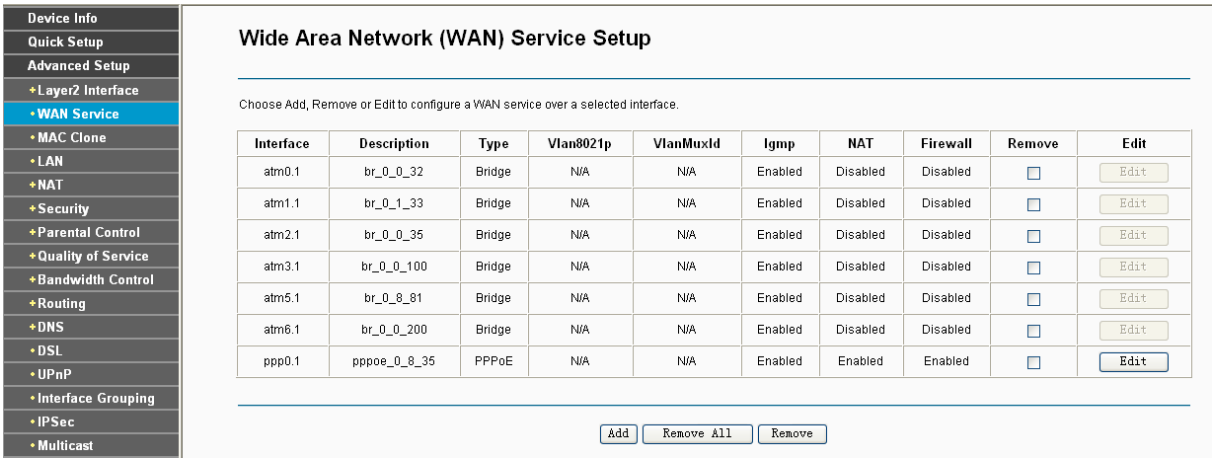
- **Remove:** Select the check box in the table on the screen above and then click the **Remove** button, the corresponding interface will be deleted in the table.

Note:

One ETH is allowed to configure as the layer 2 WAN Interface.

4.4.2 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.



Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	Remove	Edit
atm0.1	br_0_0_32	Bridge	N/A	N/A	Enabled	Disabled	Disabled	☐	Edit
atm1.1	br_0_1_33	Bridge	N/A	N/A	Enabled	Disabled	Disabled	☐	Edit
atm2.1	br_0_0_35	Bridge	N/A	N/A	Enabled	Disabled	Disabled	☐	Edit
atm3.1	br_0_0_100	Bridge	N/A	N/A	Enabled	Disabled	Disabled	☐	Edit
atm5.1	br_0_8_81	Bridge	N/A	N/A	Enabled	Disabled	Disabled	☐	Edit
atm6.1	br_0_0_200	Bridge	N/A	N/A	Enabled	Disabled	Disabled	☐	Edit
ppp0.1	pppoe_0_8_35	PPPoE	N/A	N/A	Enabled	Enabled	Enabled	☐	Edit

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 (4.4.1 Layer2 Interface) to configure them again.

4.4.2.1 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 (4.4.1.1 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**.

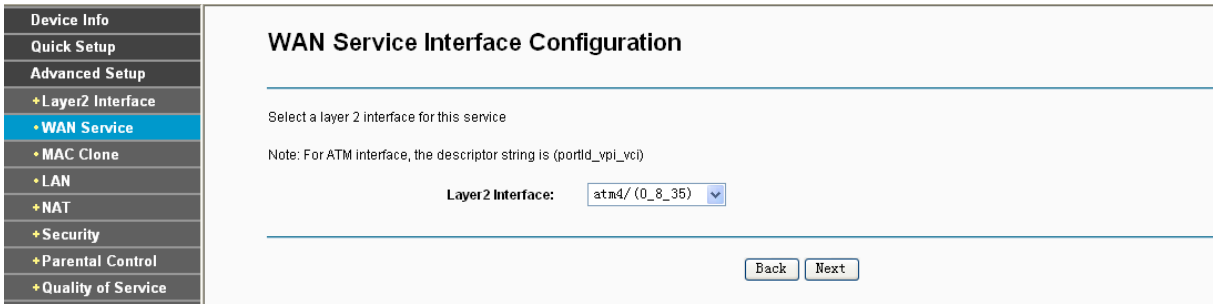


Figure 4-8

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**.

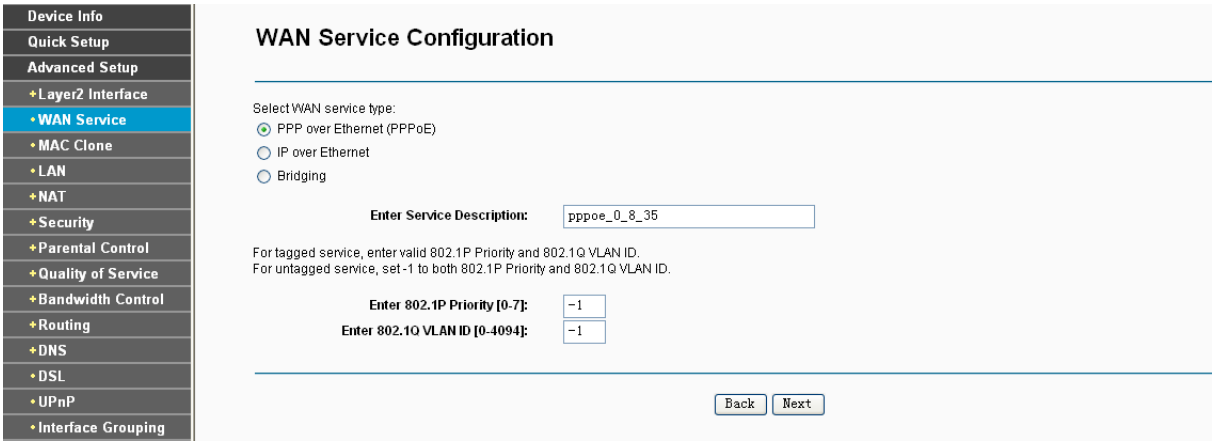


Figure 4-9

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

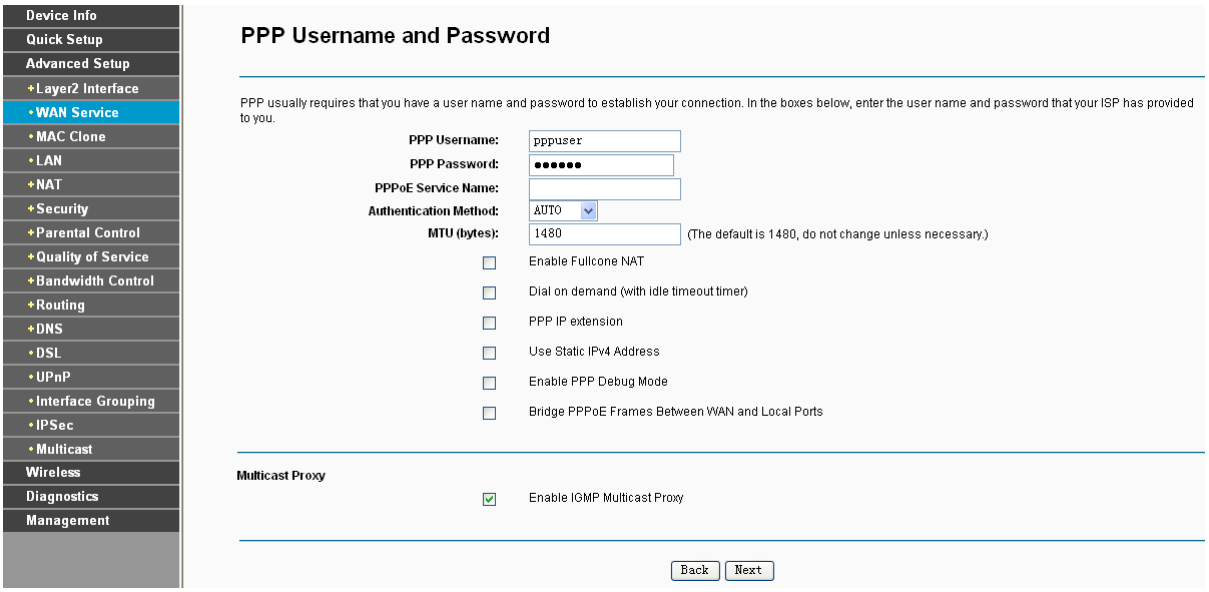


Figure 4-10

- **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 Fullcone NAT**: It is a type of NAT, if not enabled, the default NAT will act.
- **Dial on demand (with idle timeout timer)**: The 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 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 disabled, 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**.

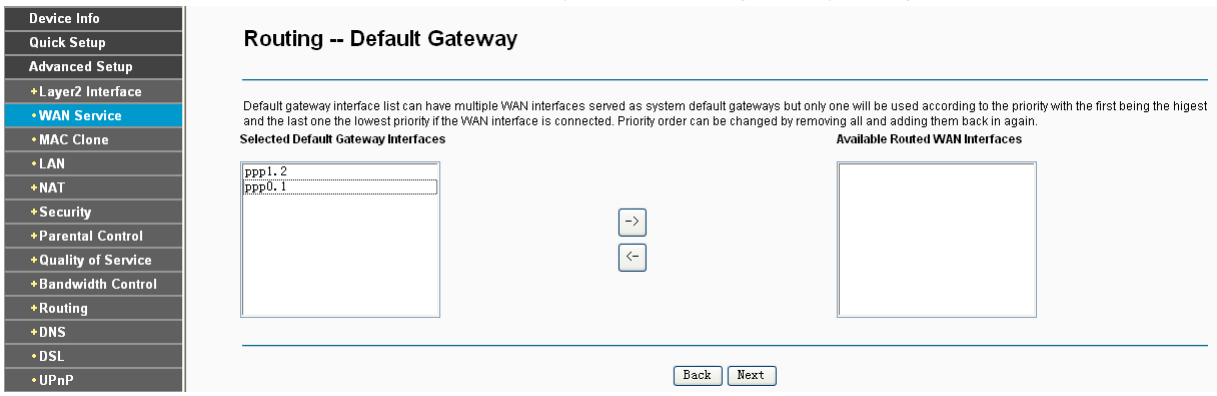


Figure 4-11

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

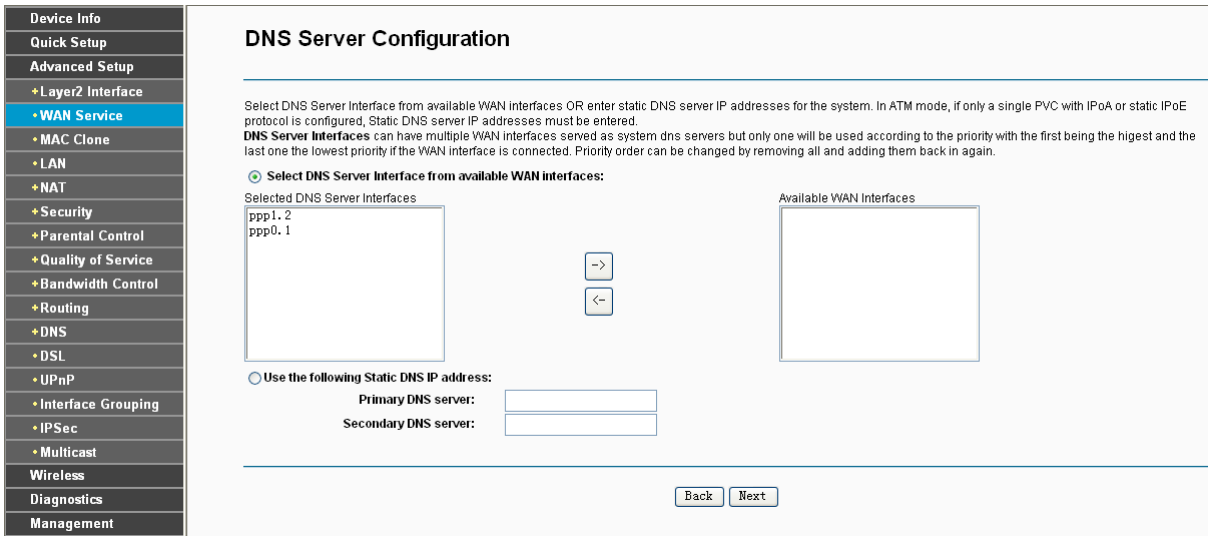


Figure 4-12

- **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.

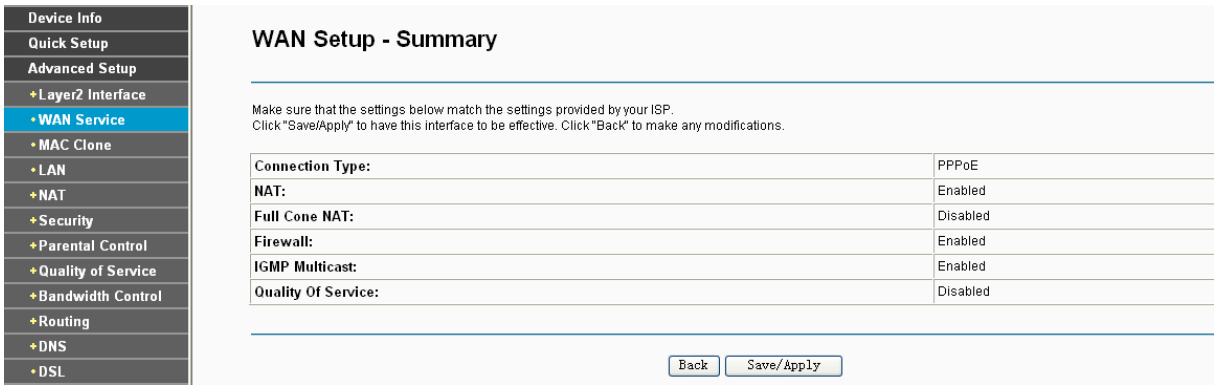


Figure 4-13

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

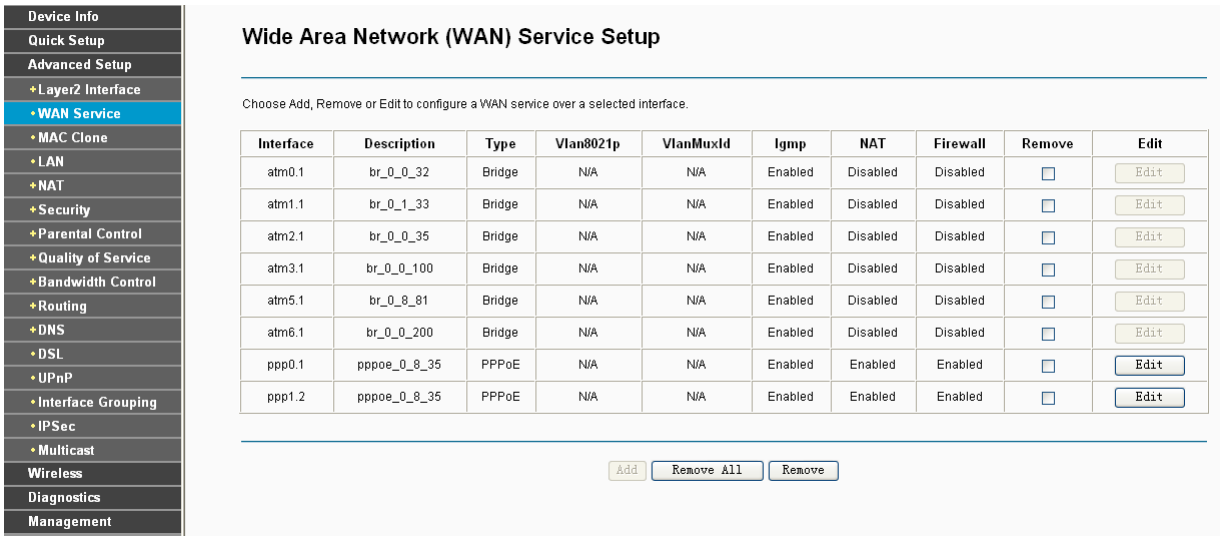


Figure 4-14

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

4.4.2.2 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 (4.4.1.1 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 **IPoE** 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**.

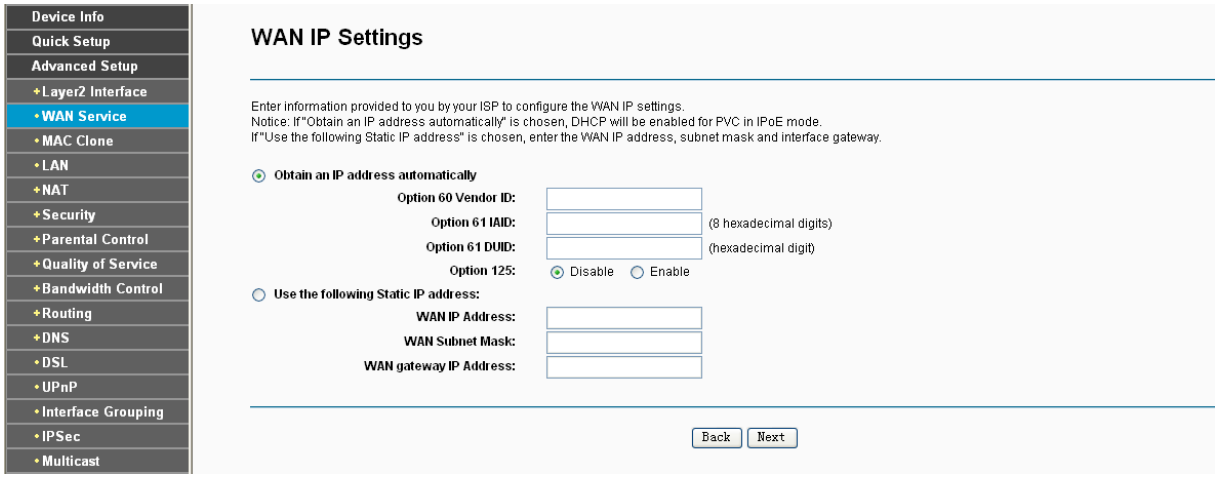


Figure 4-15

- **Obtain an IP address automatically:** Select this option, the 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 Router. The DHCP options include IP network information, and also the vendor-specific options. In some cases, the Router is implemented to perform user-defined operations (as shown below). You can implement your own treatment of all such options.

2) If the 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 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**.

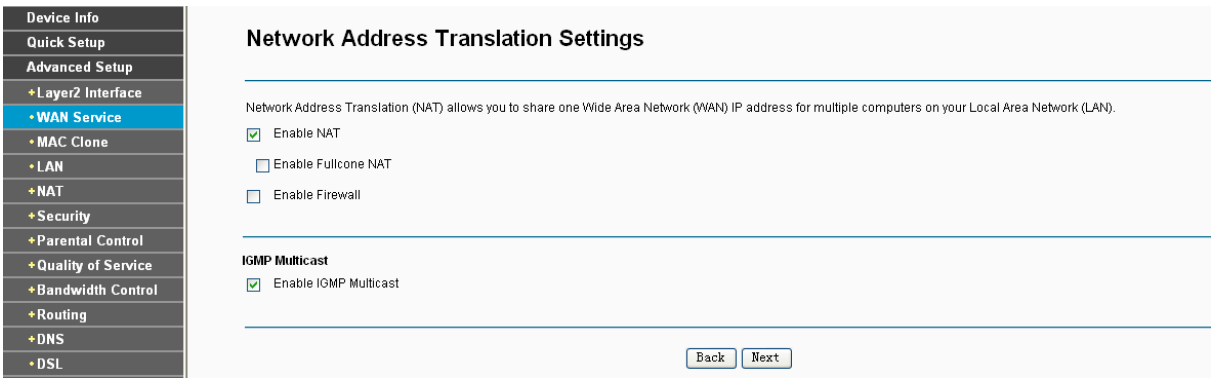


Figure 4-16

➢ **Enable NAT:** This technology translates the IP addresses of a local area network to a different IP address for the Internet. If this 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 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 4.4.5 NAT.

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

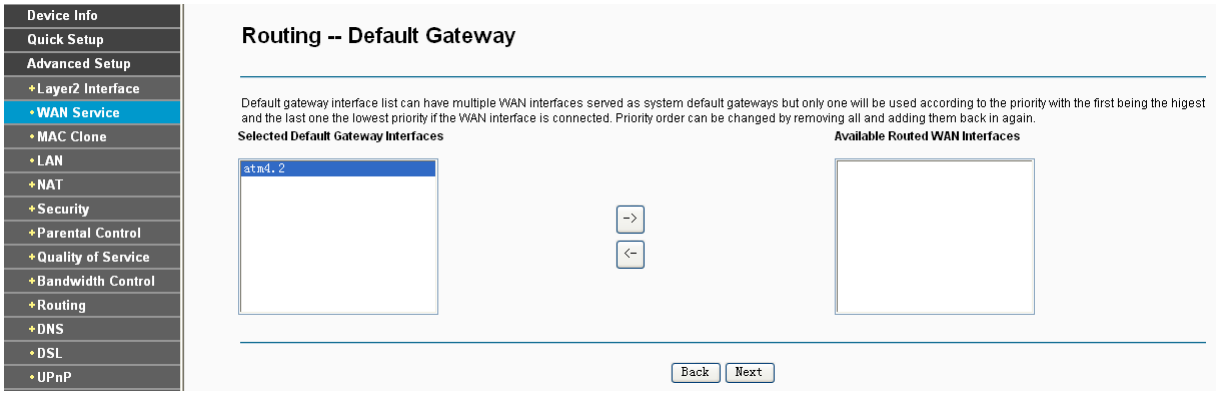


Figure 4-17

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

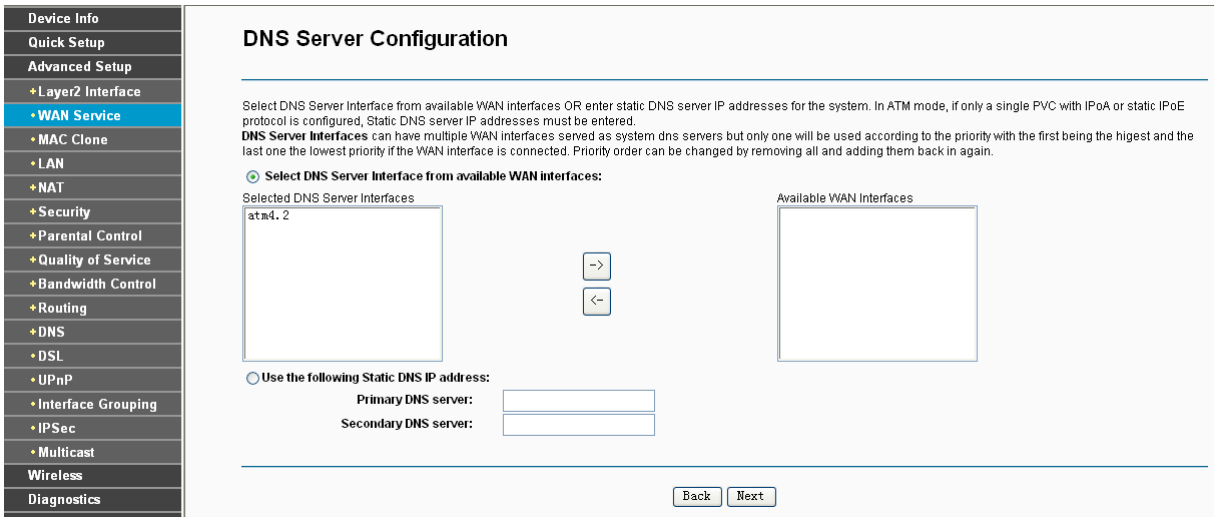


Figure 4-18

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.

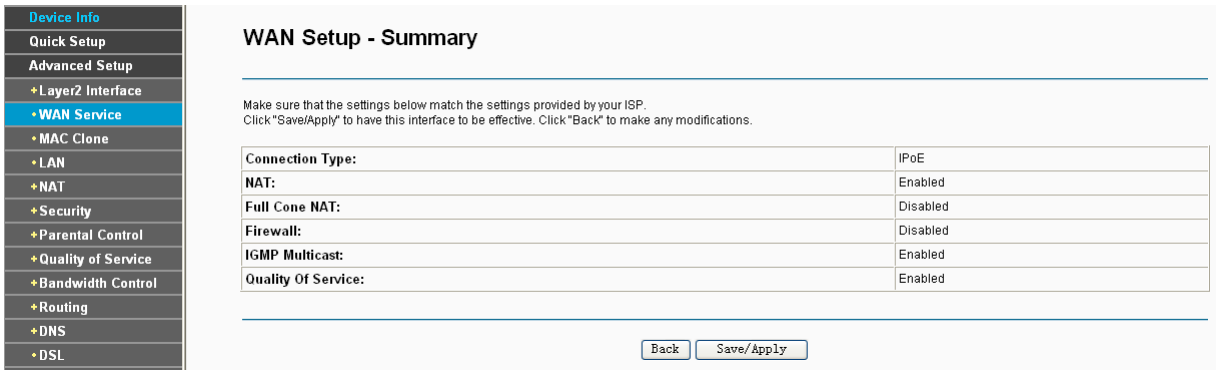


Figure 4-19

4.4.2.3 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 4.4.1.1 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.

4.4.2.4 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 4.4.1.1 ATM interface).
2. Click the **Add** button on the screen Figure 4-7 and the next configuration is similar to **PPPoE**, (see section 4.4.2.1 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.

4.4.2.5 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 4.4.1.1 ATM interface).
2. Click the **Add** button on the screen Figure 4-7 and the next configuration is similar to **IPoE** (see section 4.4.2.2 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.

4.4.2.6 ETH-PPPoE

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

1. Add a new **ETH** interface on the screen of 4.4.1.2 ETH interface.
2. Click the **Add** button on the screen Figure 4-7 and the following configuration is similar to **PPPoE** over ATM interface (see section 4.4.2.1 ATM-EoA-PPPoE).

4.4.2.7 ETH-IPoE

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

1. Add a new **ETH** interface on the screen of 4.4.1.2 ETH interface.
2. Click the **Add** button on the screen Figure 4-7 and the next configuration is similar to **IPoE** over ATM interface (see section 4.4.2.2 ATM-EoA-IPoE).

4.4.2.8 ETH-Bridge

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

1. Add a new **ETH** interface on the screen of 4.4.1.2 ETH interface.
2. Click the **Add** button on the screen Figure 4-7 and the next configuration is similar to **Bridge** over ATM interface (see section 4.4.2.3 ATM-EoA-Bridging).

4.4.3 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 4.4.1 Layer2 Interface and its default MAC Address. If you have not configured corresponding WAN Service for the interface on the section 4.4.2 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.

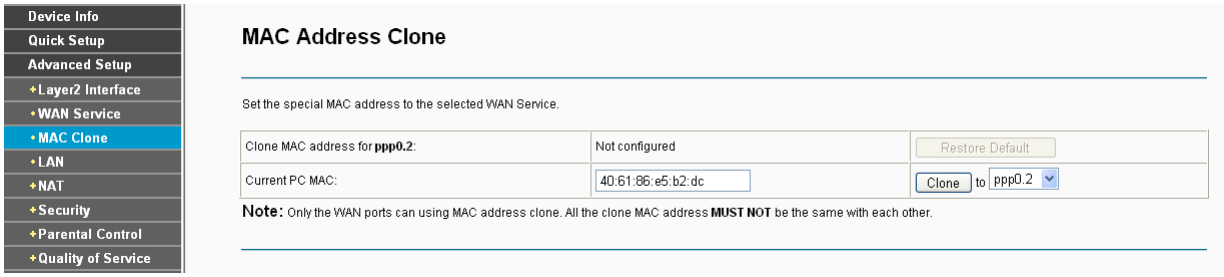


Figure 4-20

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.

4.4.4 LAN

Choose "**Advanced Setup**"→"**LAN**", and you will see the LAN screen (shown in Figure 4-21), the section allows you to configure the Router's LAN ports settings.

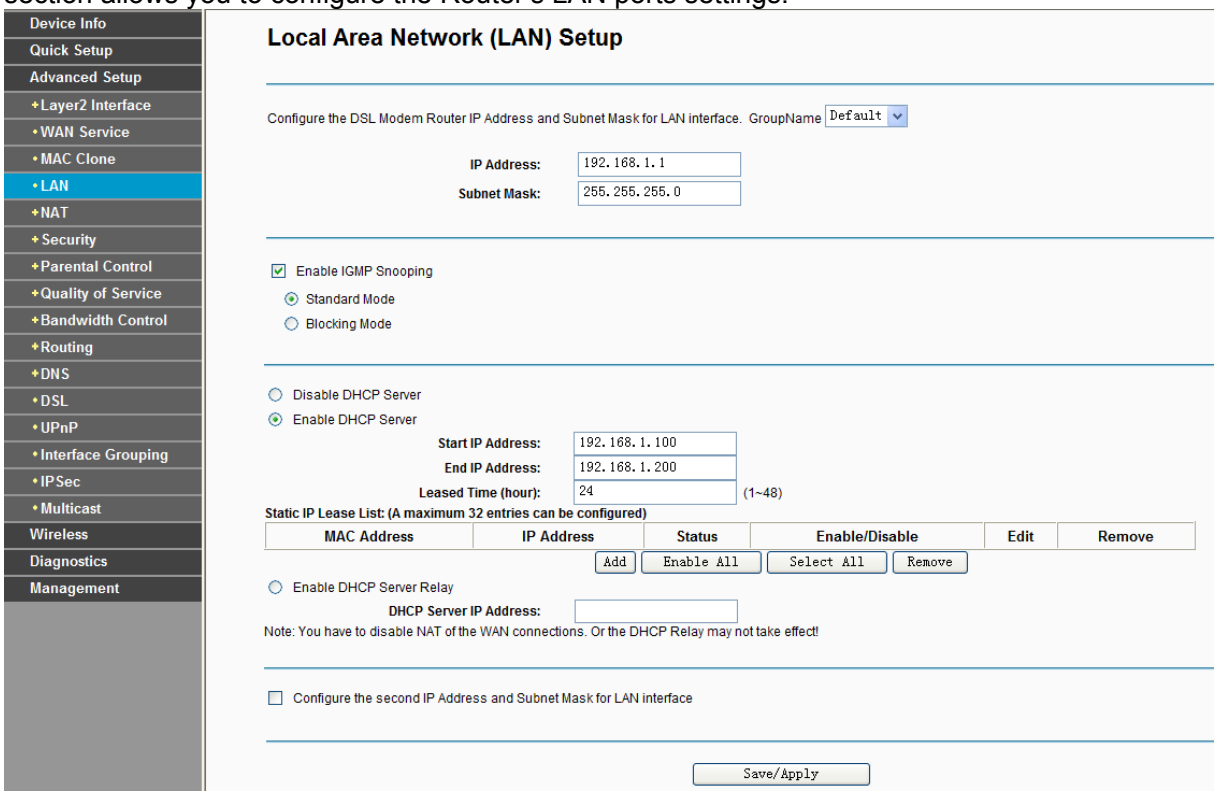


Figure 4-21

- **IP Address:** You can configure the Router's IP Address and Subnet Mask for LAN Interface.
  - **IP Address:** Enter the 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 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 Router's Dynamic Host Configuration Protocol (DHCP) server function. The DHCP server is enabled by default for the 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 Router though the Ethernet port. When the 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 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 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 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 Entries** button, and then you will set the rule in the screen as below.

Figure 4-22

- 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 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.

4.4.5 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 (4.4.2 WAN Service), you will see the **NAT** menu in the Web-based Utility (shown in Figure 4-24).

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.

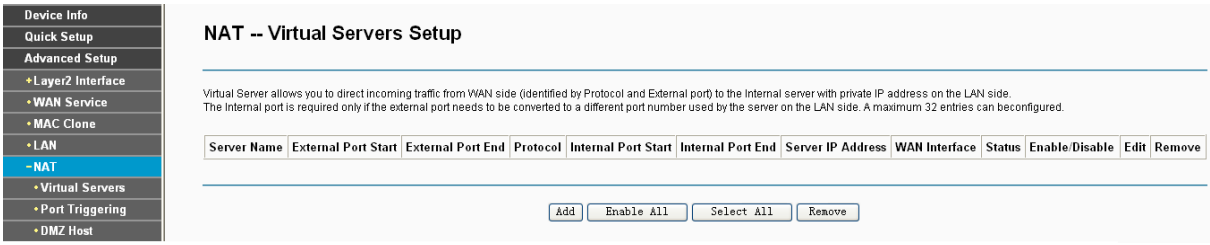


Figure 4-23

4.4.5.1 Virtual Servers

Choose "**Advanced Setup**"→"**NAT**"→"**Virtual Servers**", you can set up virtual servers on the screen below (shown in Figure 4-25).

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.

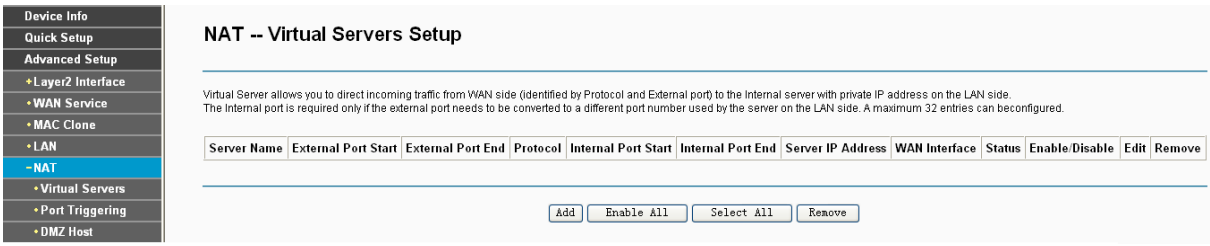


Figure 4-25

- **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 4-25) 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 4-25, and then you will see the new Virtual Server in the next screen as shown in Figure 4-26.

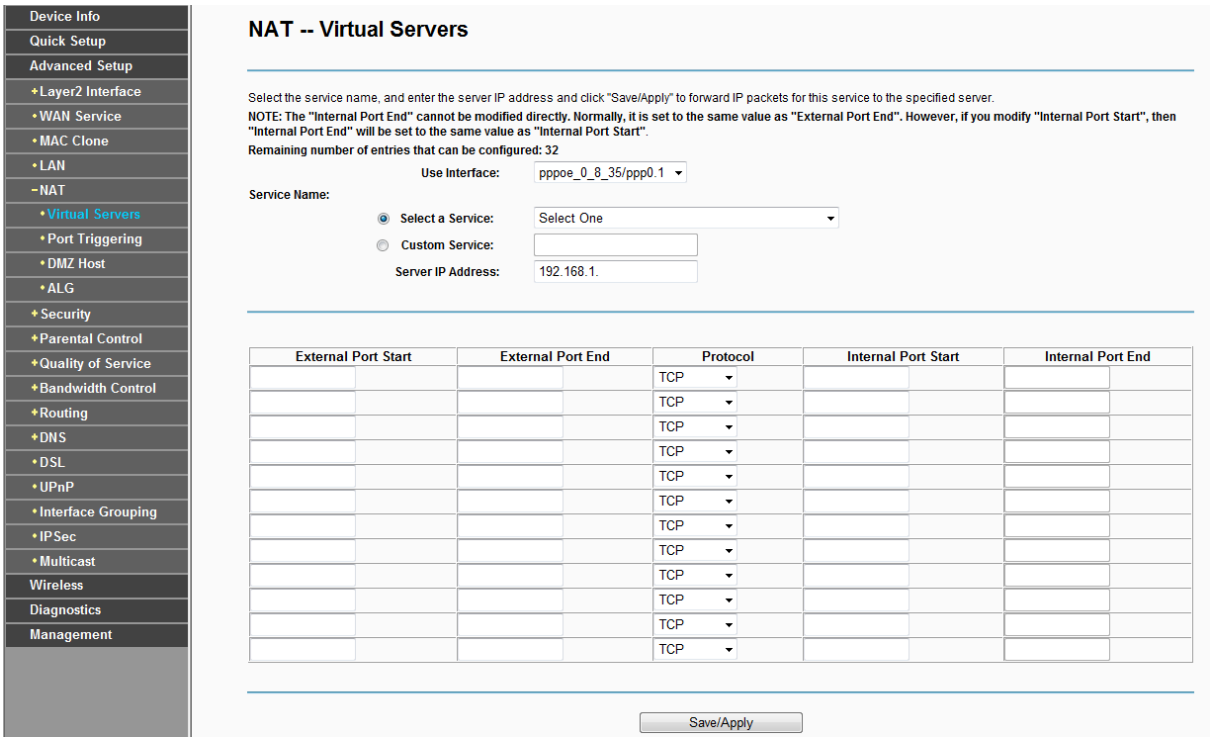


Figure 4-26

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 4-25.

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.

4.4.5.2 Port Triggering

Choose "**Advanced Setup**"→"**NAT**"→"**Port Triggering**", you can set Port Triggering on the screen (shown in Figure 4-27).

Some applications require that specific ports in the 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 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.

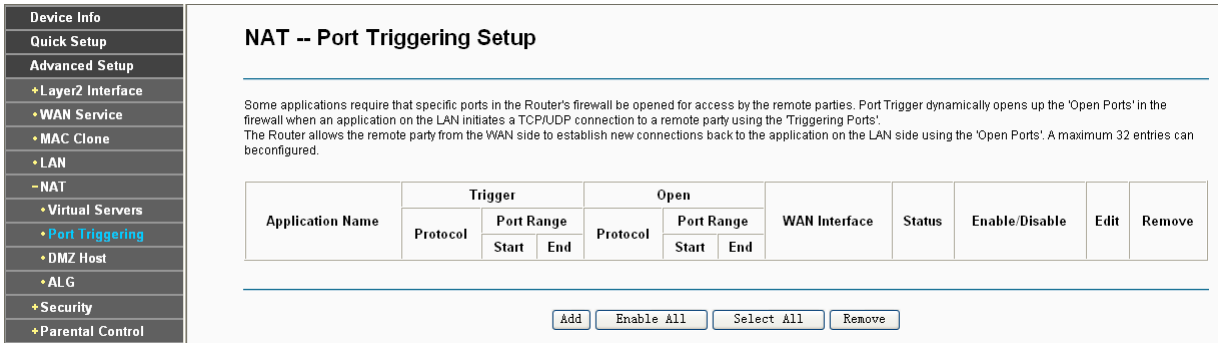


Figure 4-27

- **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 4-27) 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 4-27, and then you will see the new Port Triggering in the next screen as shown in Figure 4-28.

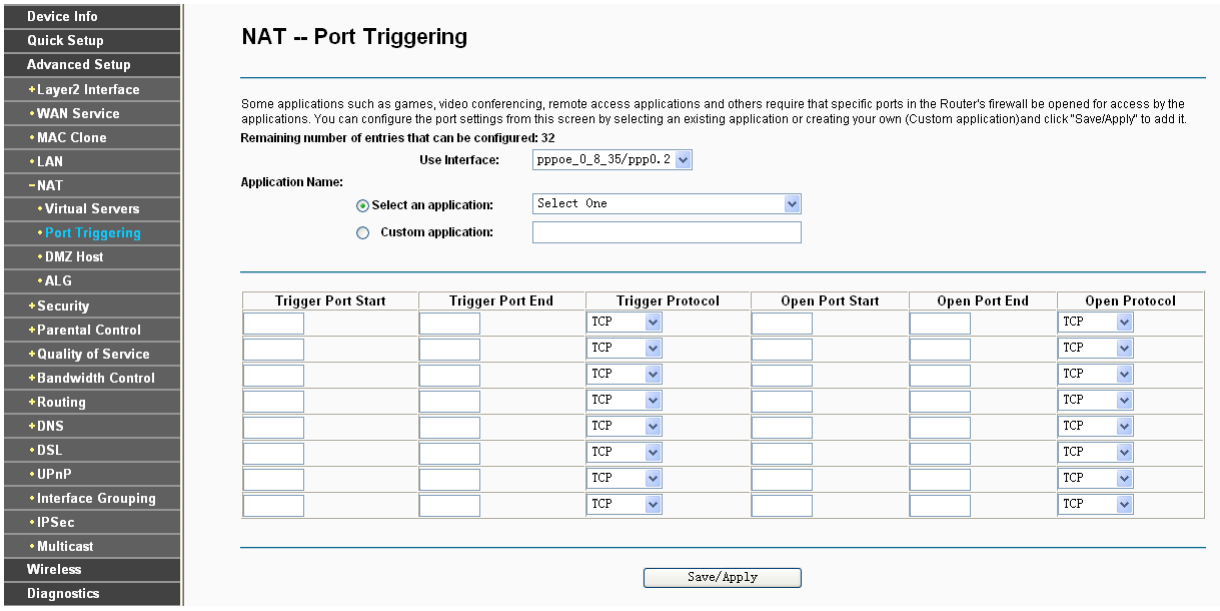


Figure 4-28

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 4-27.

☞ **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.

4.4.5.3 DMZ Host

Choose "**Advanced Setup**"→"**NAT**"→"**DMZ Host**", you can set up DMZ Host on the screen (shown in Figure 4-29).

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.

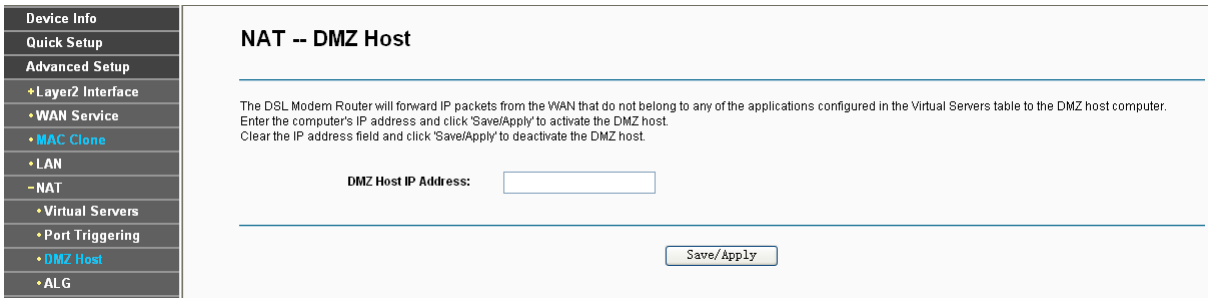


Figure 4-29

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.

4.4.5.4 ALG

Choose "**Advanced Setup**"→"**NAT**"→"**ALG**", and then you can configure the basic security in the screen as shown in Figure 4-29.

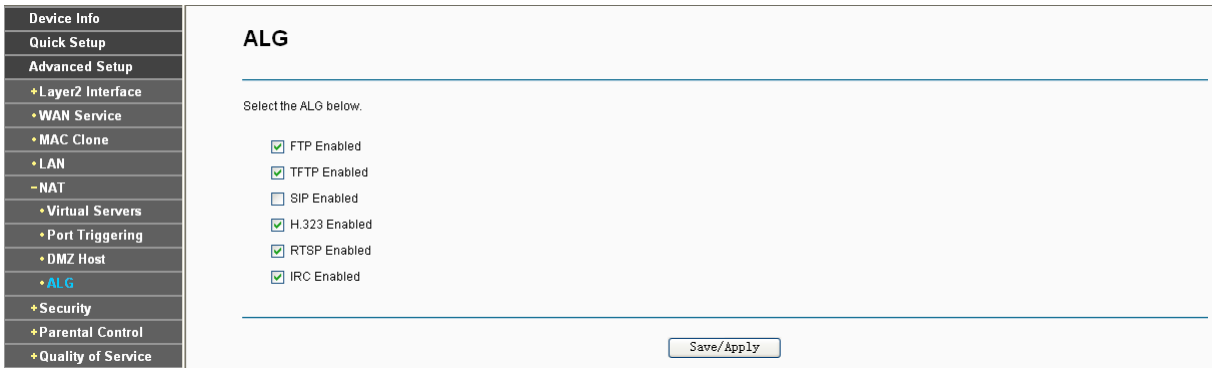


Figure 4-29

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

4.4.6 Security

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

Figure 4-30

4.4.6.1 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 includes **Outgoing** and **Incoming**, the detailed descriptions are provided below.

IP Filtering - Outgoing

Choose "**Advanced Setup**"→"**Security**"→"**IP Filtering**", you can configure Outgoing Filtering rules on the screen (shown in Figure 4-31).

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.

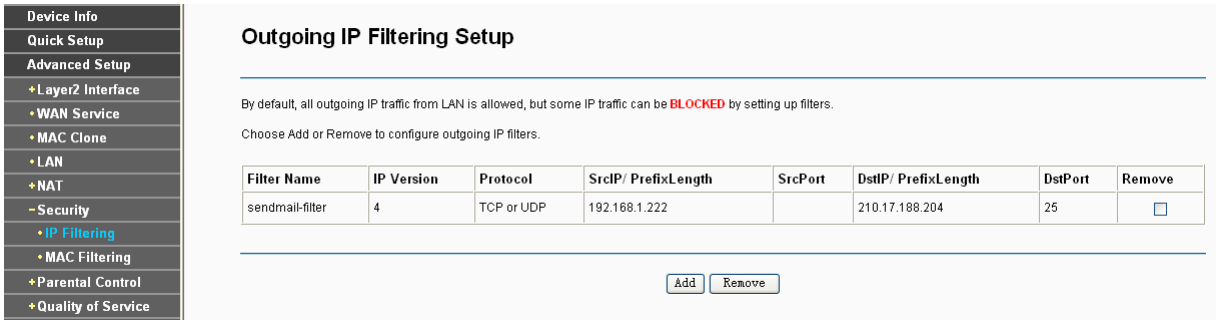


Figure 4-31

Set up an Outgoing IP Filtering rule:

1. Click the **Add** button in Figure 4-31, and you will see the next screen as shown in Figure 4-32.

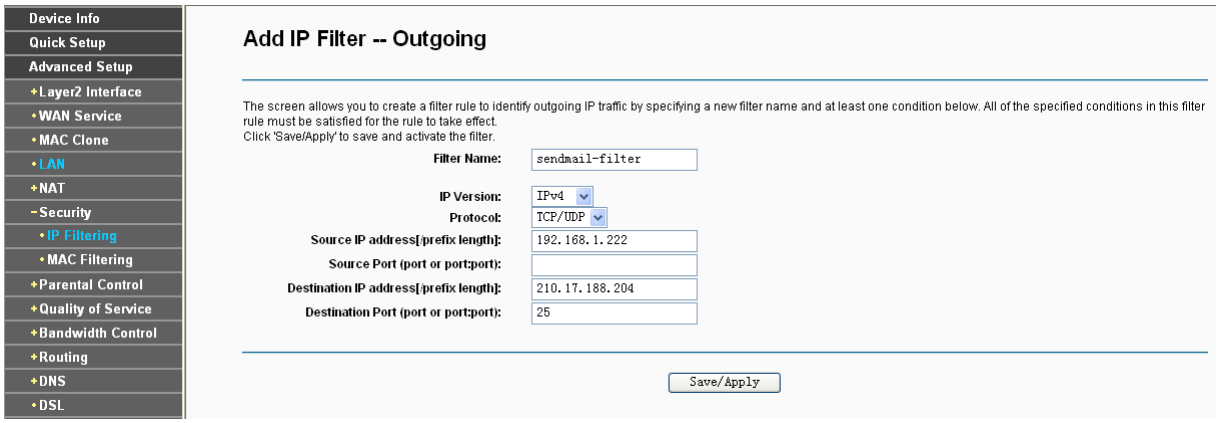


Figure 4-32

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.

4.4.6.2 MAC Filtering

Choose "**Advanced Setup**"→"**Security**"→"**MAC Filtering**", you can configure MAC Filtering rules on the screen as shown in Figure 4-35. 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.

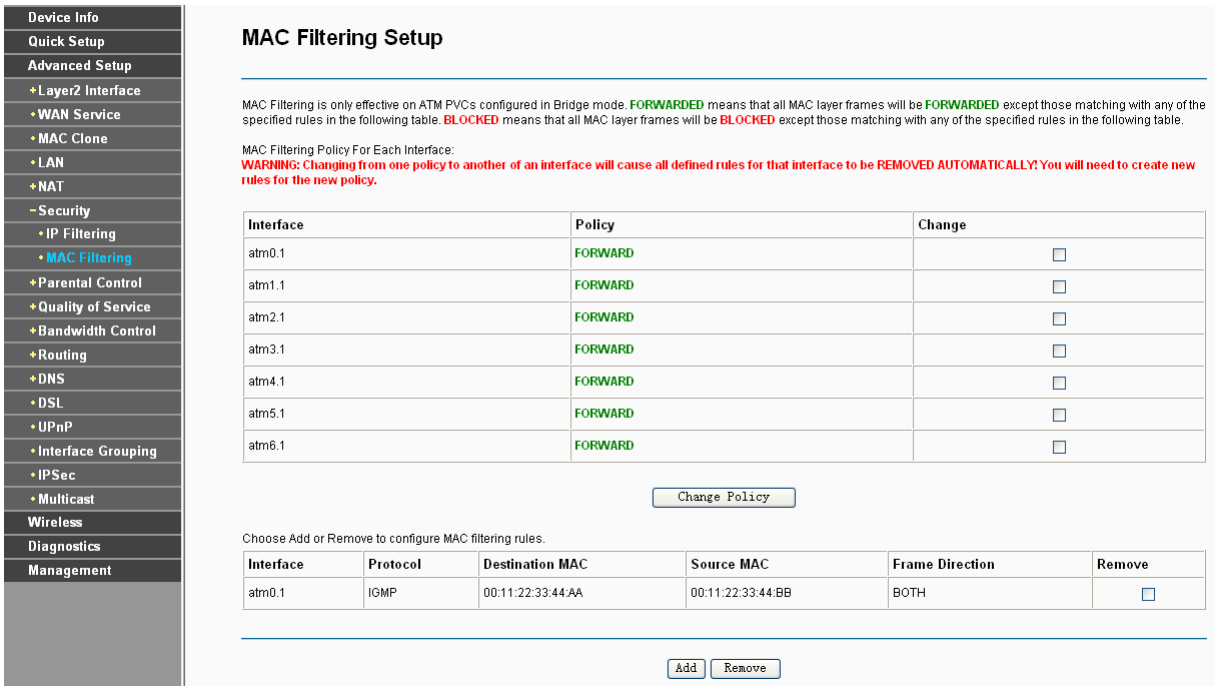


Figure 4-35

- **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 4-35). 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 4-35).
- **Remove:** Select the check box in the table (shown in Figure 4-35) 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 4-35, and you will see the next screen similar to in Figure 4-36.

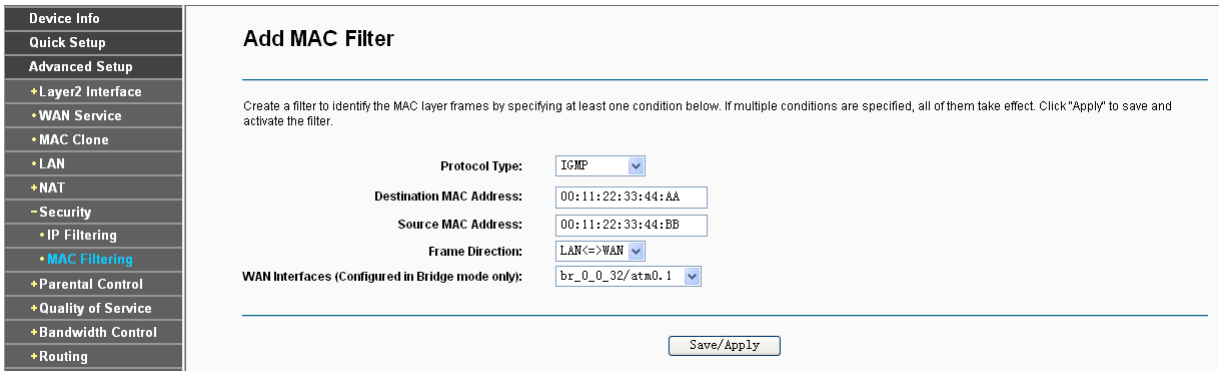


Figure 4-36

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 4-35.

4.4.7 Parental Control

Choose "**Advanced Setup**"→"**Parental Control**". You can configure the Parental Control on the screen as shown in Figure 4-37. 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 router to access certain websites. These two features work independently.

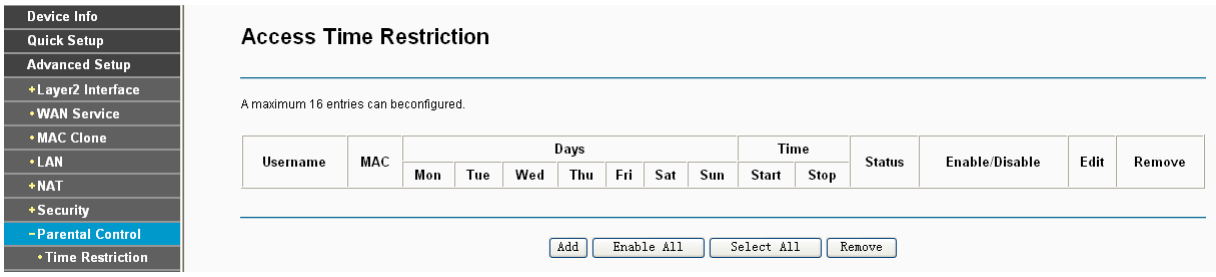


Figure 4-37

4.4.7.1 Time Restriction

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

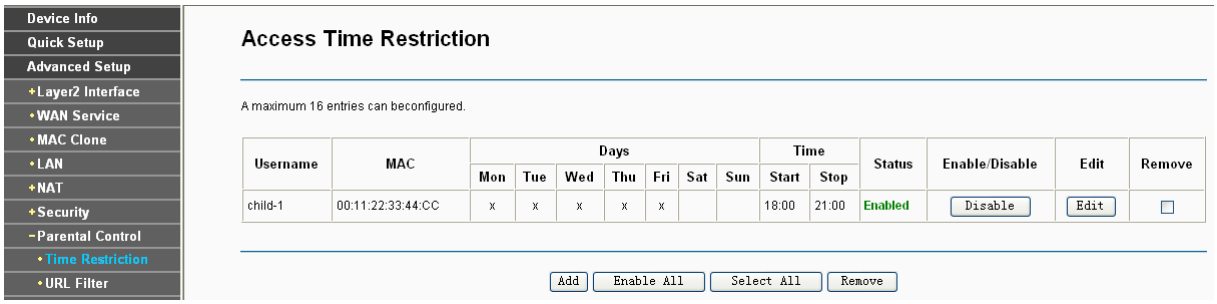


Figure 4-38

To add a Time Restriction entry:

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

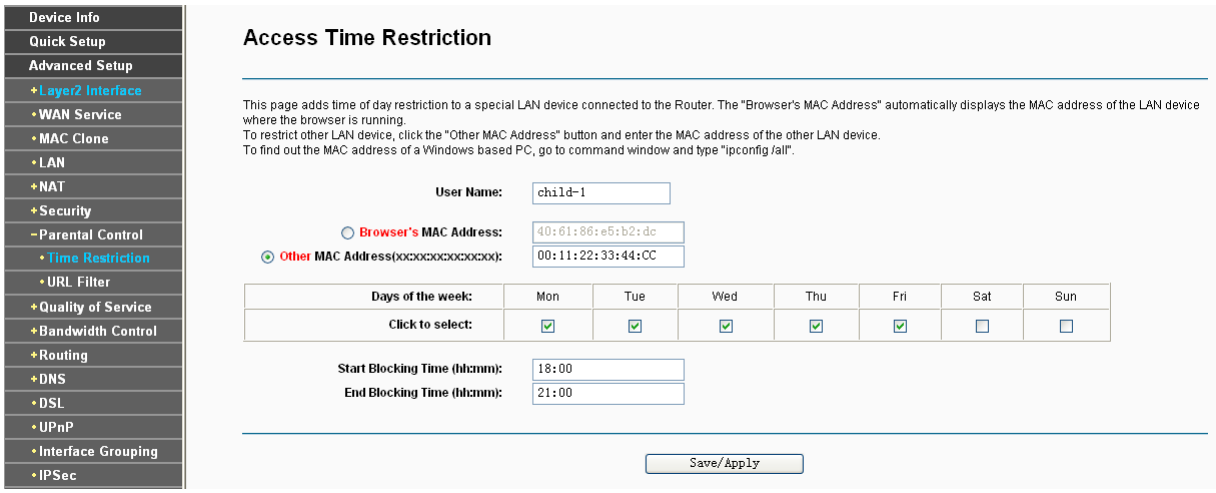


Figure 4-39

2. Enter the **User Name** of the LAN device connected to the 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 4-38.

☞ **Note:**

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

4.4.7.2 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.

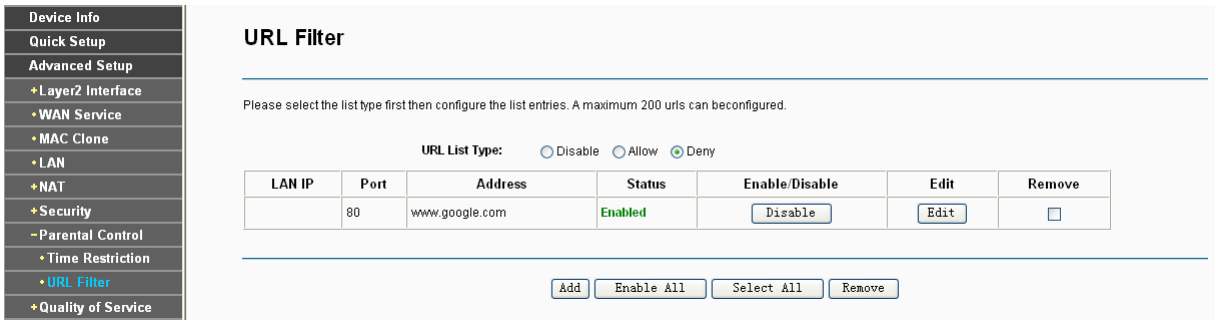


Figure 4-40

There are two 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 4-40 and then you will see the next screen as shown in Figure 4-41. Enter the URL Address and Port Number.

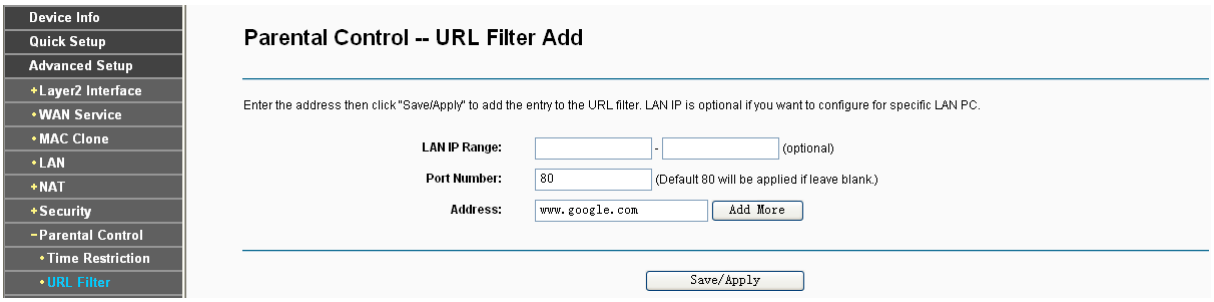


Figure 4-41

3. Click **Save/Apply** to save this entry and then you will see your settings as shown in Figure 4-40. Every computer connected to the router will not access this URL address on the port.

4.4.8 Quality of Service

Choose "**Advanced Setup**"→"**Quality of Service**", you can enable QoS (Quality of Service) on the screen shown in Figure 4-42. QoS helps to prioritize data as it enters your 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.

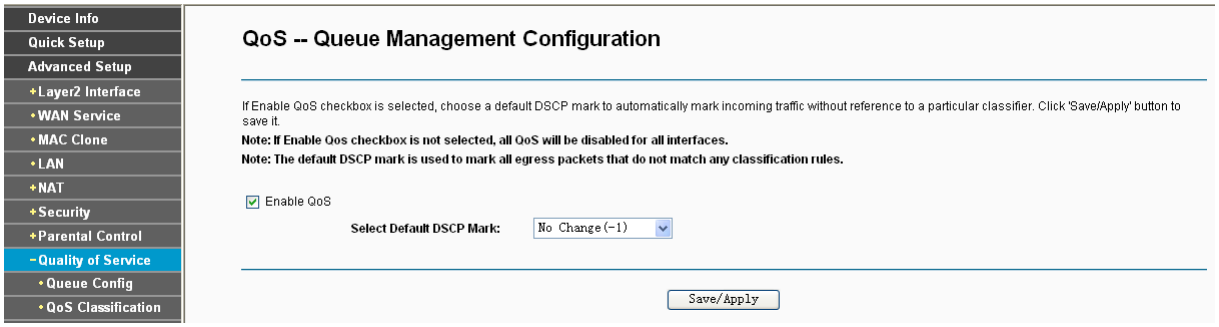


Figure 4-42

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

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

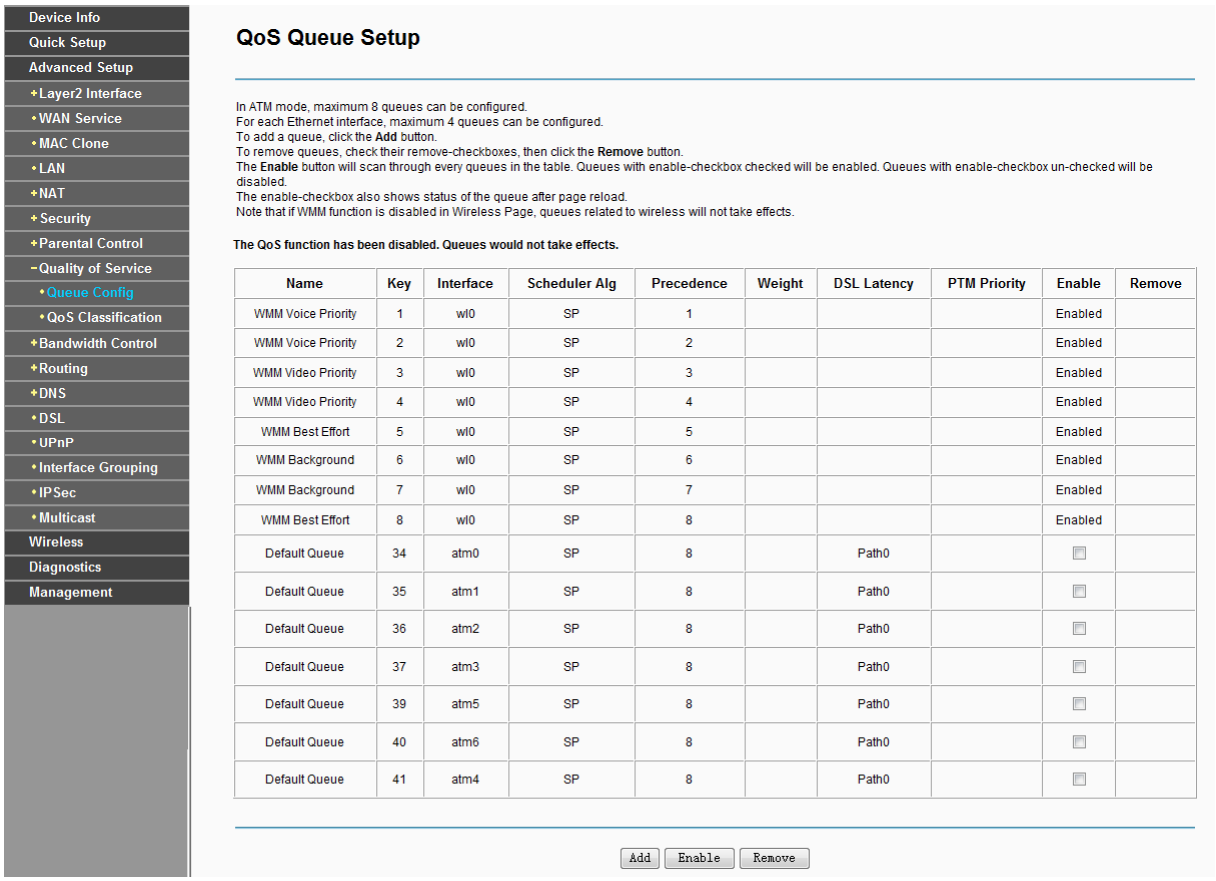
Click **Save/Apply** to save the current configuration.

☞ **Note:**

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

4.4.8.1 Queue Config

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



Name	Key	Interface	Scheduler Alg	Precedence	Weight	DSL Latency	PTM Priority	Enable	Remove
WMM Voice Priority	1	wl0	SP	1				Enabled	
WMM Voice Priority	2	wl0	SP	2				Enabled	
WMM Video Priority	3	wl0	SP	3				Enabled	
WMM Video Priority	4	wl0	SP	4				Enabled	
WMM Best Effort	5	wl0	SP	5				Enabled	
WMM Background	6	wl0	SP	6				Enabled	
WMM Background	7	wl0	SP	7				Enabled	
WMM Best Effort	8	wl0	SP	8				Enabled	
Default Queue	34	atm0	SP	8		Path0			
Default Queue	35	atm1	SP	8		Path0			
Default Queue	36	atm2	SP	8		Path0			
Default Queue	37	atm3	SP	8		Path0			
Default Queue	39	atm5	SP	8		Path0			
Default Queue	40	atm6	SP	8		Path0			
Default Queue	41	atm4	SP	8		Path0			

Figure 4-43

Click the **Add** button in Figure 4-43, and you can configure the QoS queue entry on the next screen as shown in Figure 4-44.

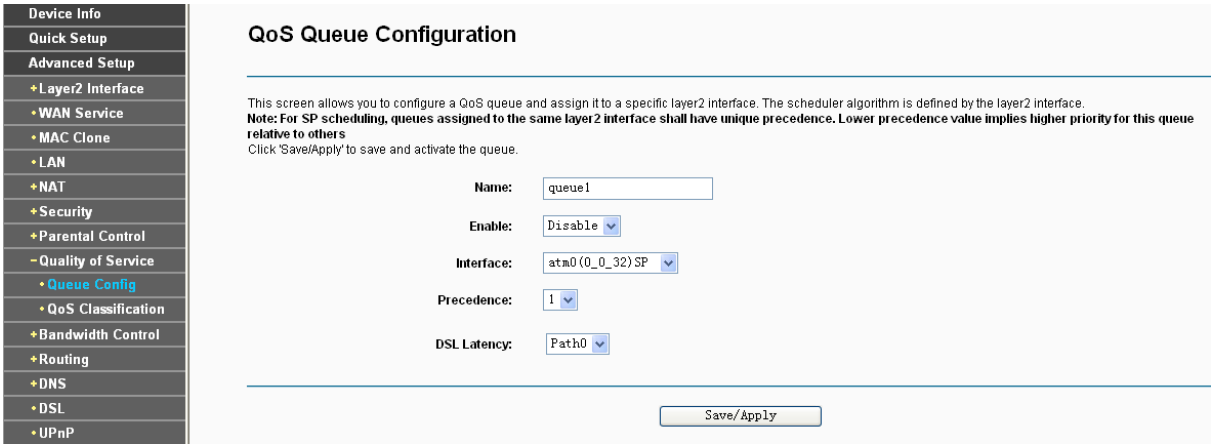


Figure 4-44

- **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.

- **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 Router.

After you specify the condition, click **Save/Apply** to save the entry and then you will see you settings as shown in Figure 4-43.

☞ **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.

4.4.8.2 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.

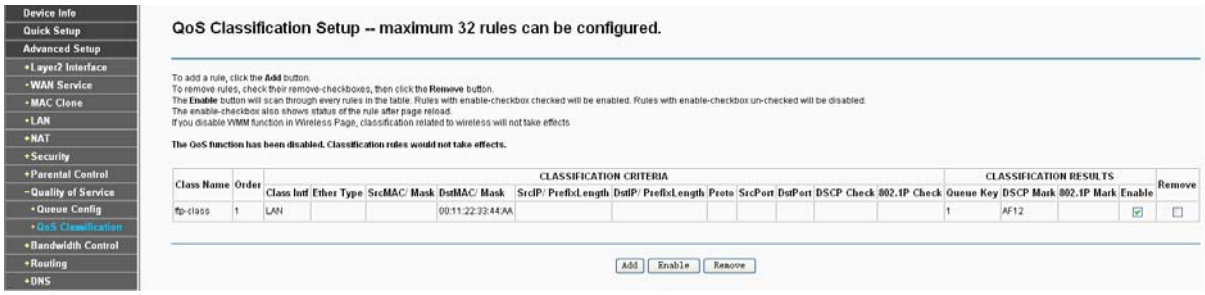


Figure 4-45

Click the **Add** button Figure 4-45, and you can configure the QoS on the next screen.

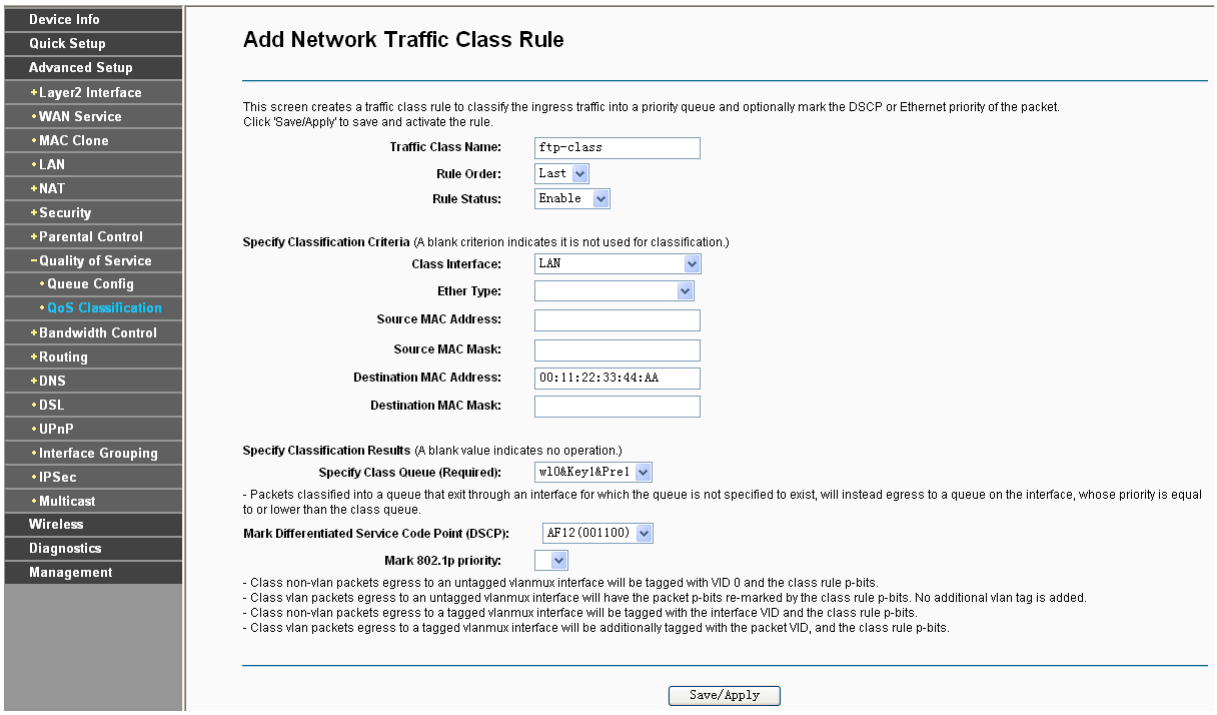


Figure 4-46

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

4.4.9 Bandwidth Control

Choose "**Advanced Setup**"→"**Bandwidth Control**" and then you will see the screen as shown in Figure 4-47. This page allows you to enable this function and to configure the value of Total Upstream/Downstream Bandwidth.

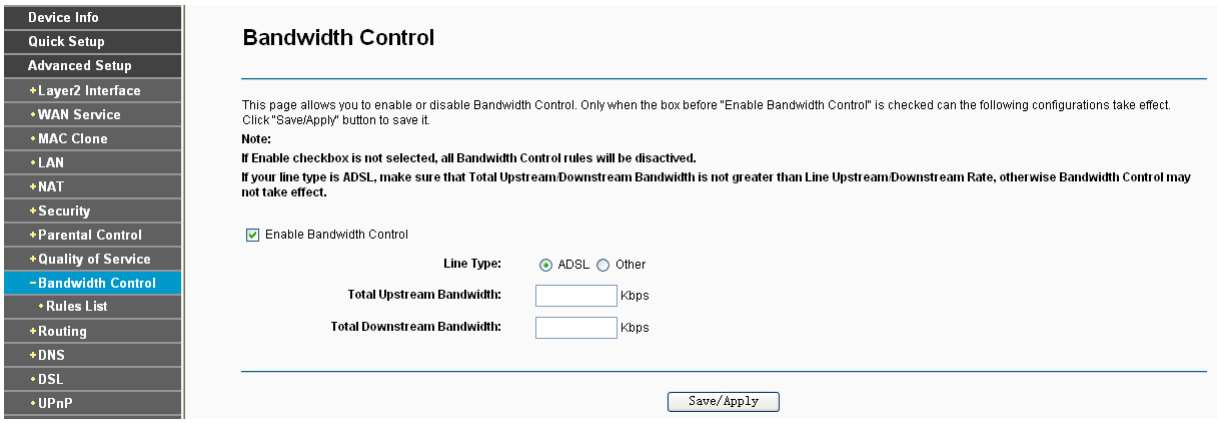


Figure 4-47

- **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.

4.4.9.1 Traffic Control Rule

Choose "**Advanced Setup**"→"**Traffic Control**" →"**Traffic Control Rule**" and then you will see the screen as shown in Figure 4-48. This page allows you to view and configure TC rules.

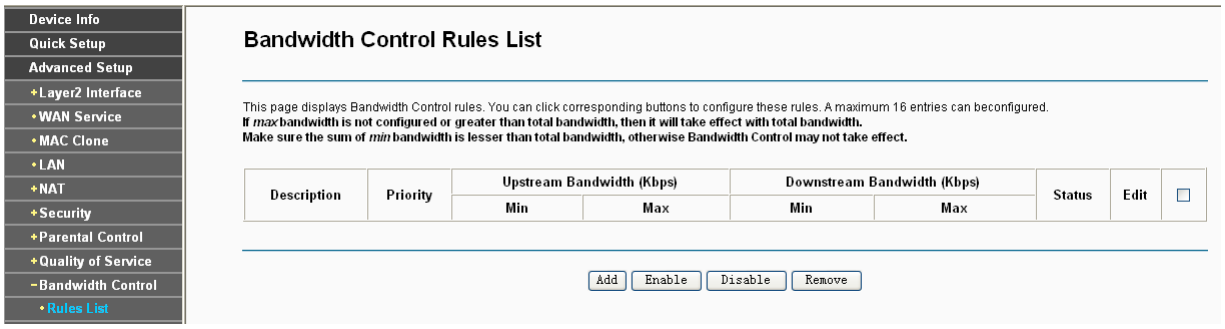


Figure 4-48

To add a TC rule, click the **Add** button and you can configure it in the screen as shown in Figure 4-49.

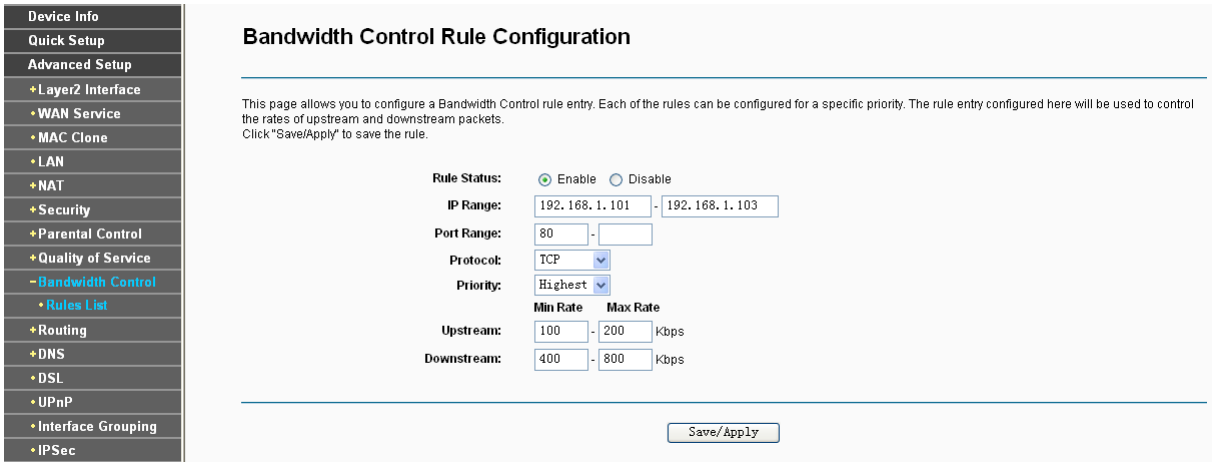


Figure 4-49

- **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 4-50. 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 4-50

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.

4.4.10 Routing

Choose "**Advanced Setup**"→"**Routing**", it includes three menus**: Default Gateway**, **Static Route and RIP** (shown in Figure 4-51). The detailed descriptions are provided below.

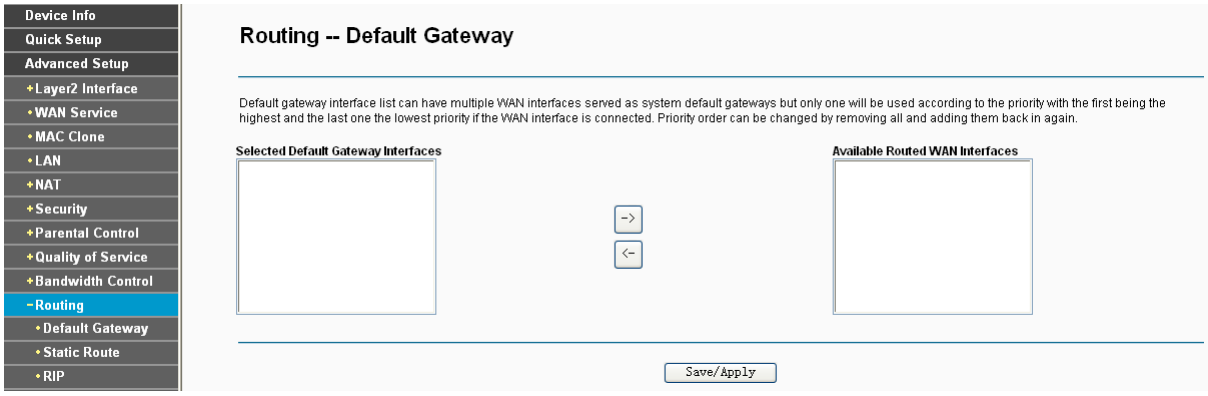


Figure 4-51

4.4.10.1 Default Gateway

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

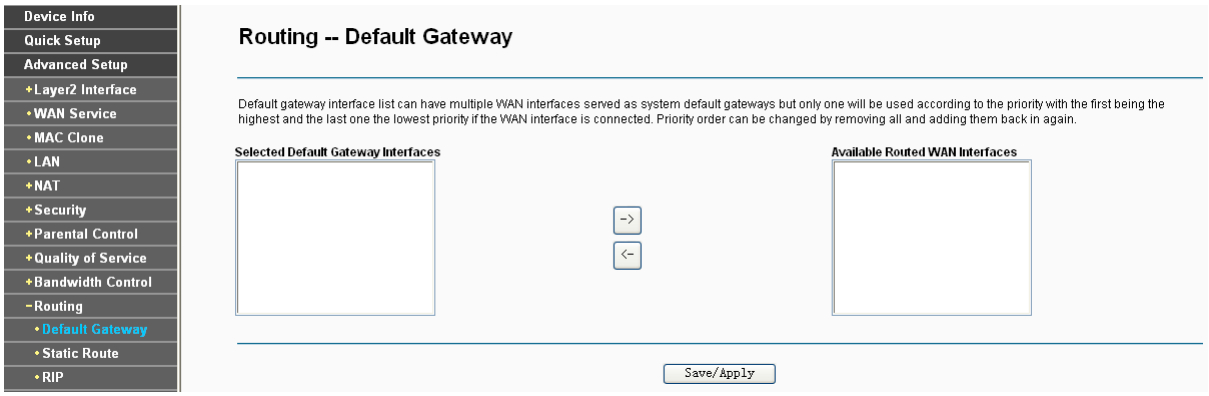


Figure 4-52

4.4.10.2 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 4-53). A static route is a pre-determined path that network information must travel to reach a specific host or network.

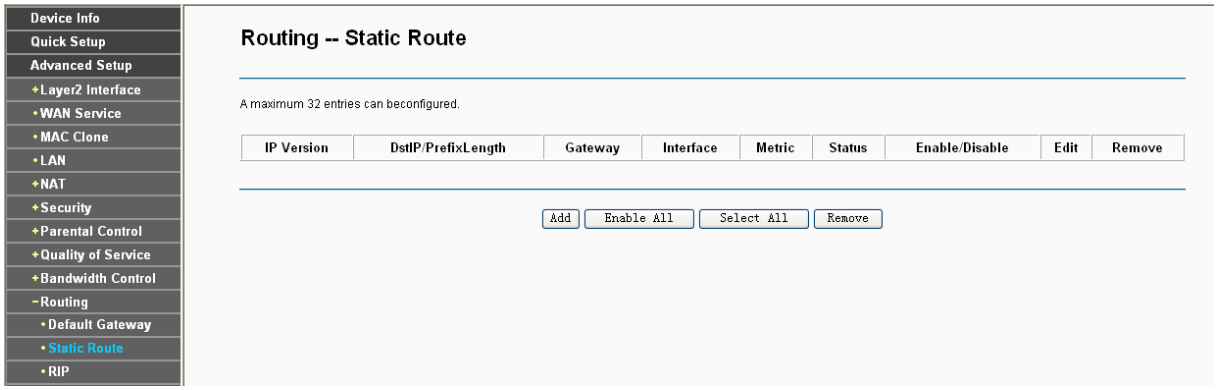


Figure 4-53

To add static routing entries:

1. Click the **Add** button in Figure 4-53, and you will see the screen as shown in Figure 4-54.

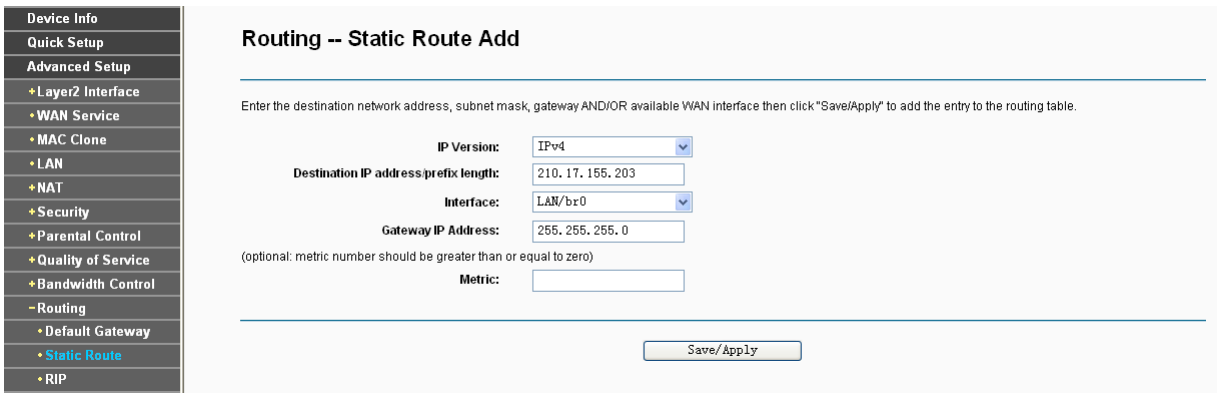


Figure 4-54

2. Enter the following data:

➢ **IP Version:** Select the version of IP.

- **Destination IP Address:** 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 and then you will see you settings as shown in Figure 4-53.

To remove a static routing entry:

1. Select the **Remove** check box according to the entry in the Figure 4-53.
2. Click the **Remove** button, and the entry will be deleted.

☞ **Note:**

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

4.4.10.3 RIP

Choose "**Advanced Setup**"→"**Routing**"→"**RIP**", you can see the RIP (Routing Information Protocol) screen which allows you to configure the RIP (shown in Figure 4-55).

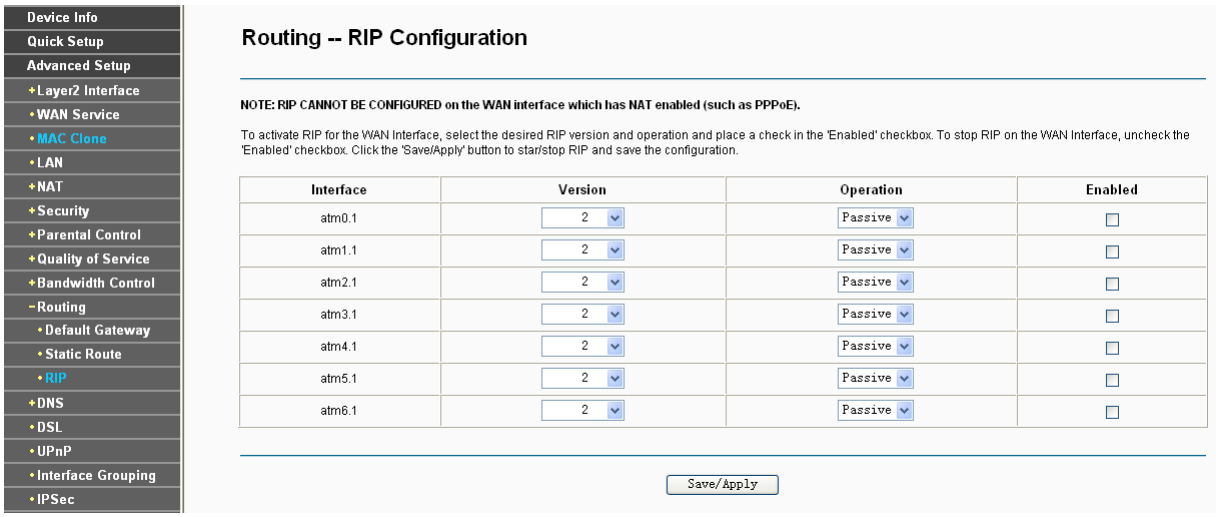


Figure 4-55

☞ **Note:**

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

To activate RIP for the device, configure an individual interface, select the desired RIP version and operation, and select **Enabled** checkbox for the interface.

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

4.4.11 DNS

When you select the connection type **PPPoE**, **PPPoA** or **IPoA** for WAN configuration, you will see the **DNS** menu in the Web-based Utility (shown in Figure 4-56). It includes **DNS Server** and **Dynamic DNS** submenus.

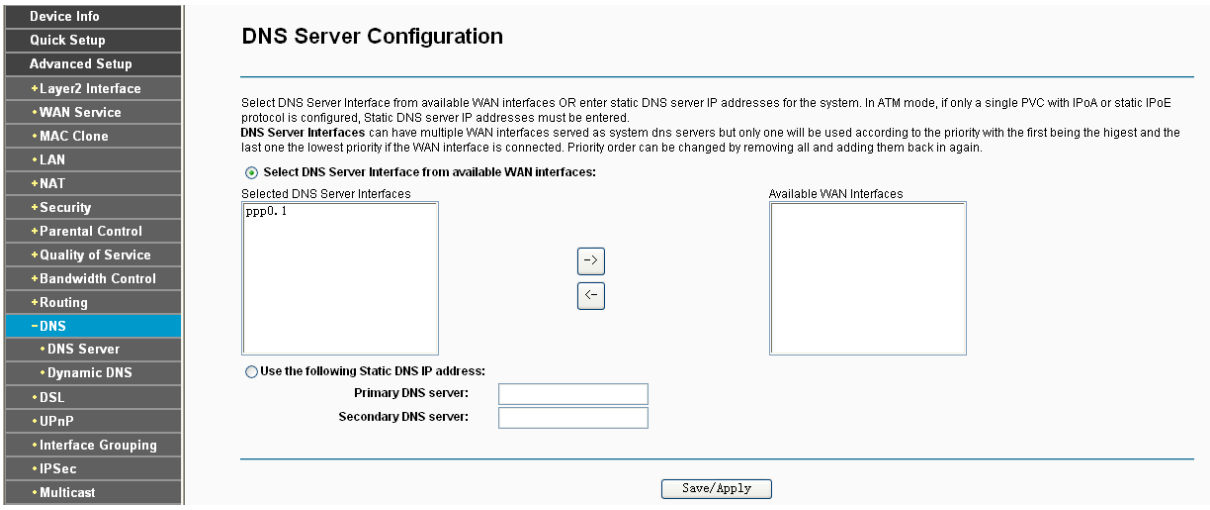


Figure 4-56

4.4.11.1 DNS Server

Choose "**Advanced Setup**"→"**DNS**"→"**DNS Server**", and you can see the **DNS Server Configuration** screen. Deselect the checkbox before **Auto DNS Server**, and then you will be able to manually configure the DNS Server Addresses as shown in Figure 4-57.

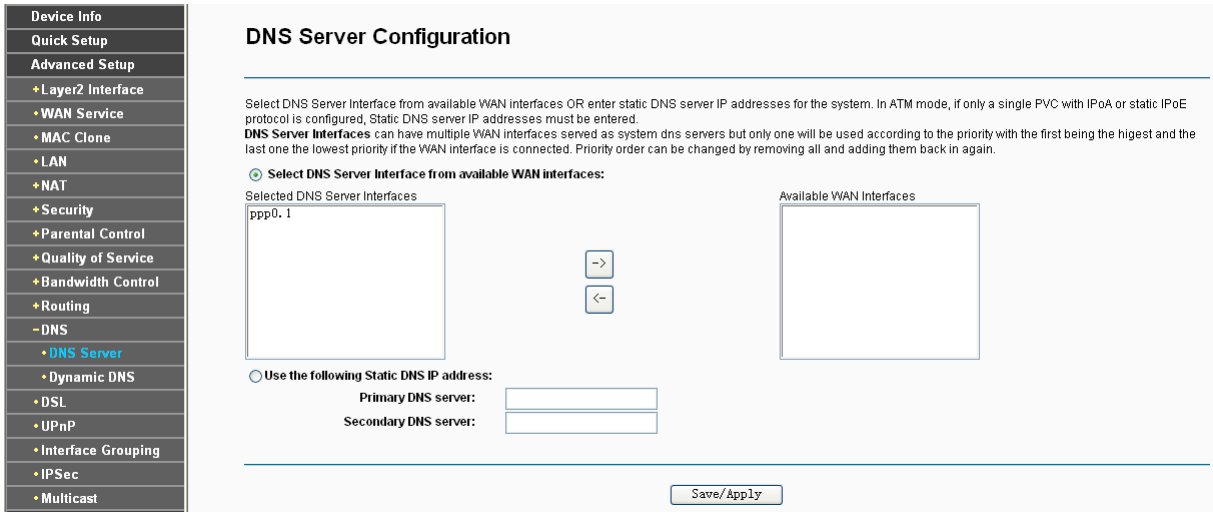


Figure 4-57

For PPPoA, PPPoE enabled PVC(s), please select the **Obtain DNS info from a WAN interface** checkbox, this 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.

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

4.4.11.2 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 4-58).

The 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 Router to be more easily accessed from various locations on the Internet.

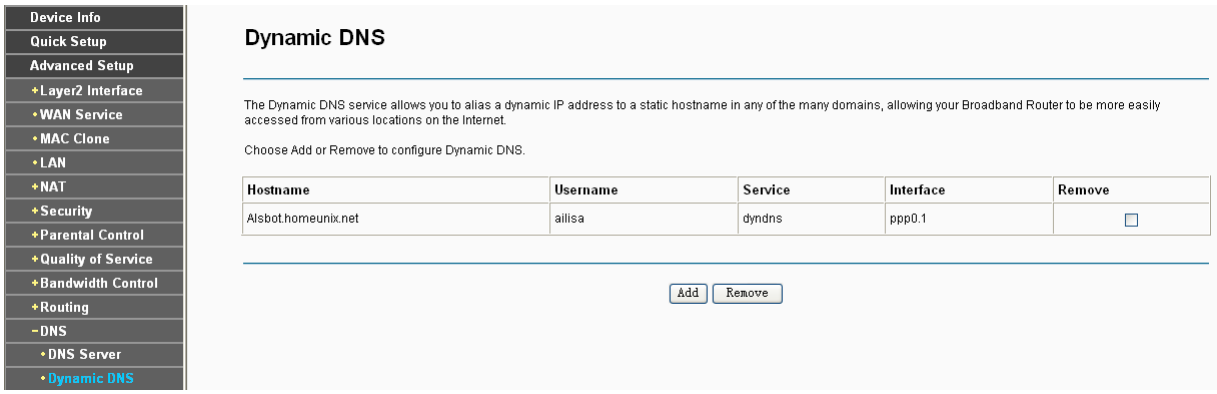


Figure 4-58

To add a DDNS entry:

1. Click the **Add** button (pop-up Figure 4-58), and then you will set the DDNS in the next screen (shown in Figure 4-59).

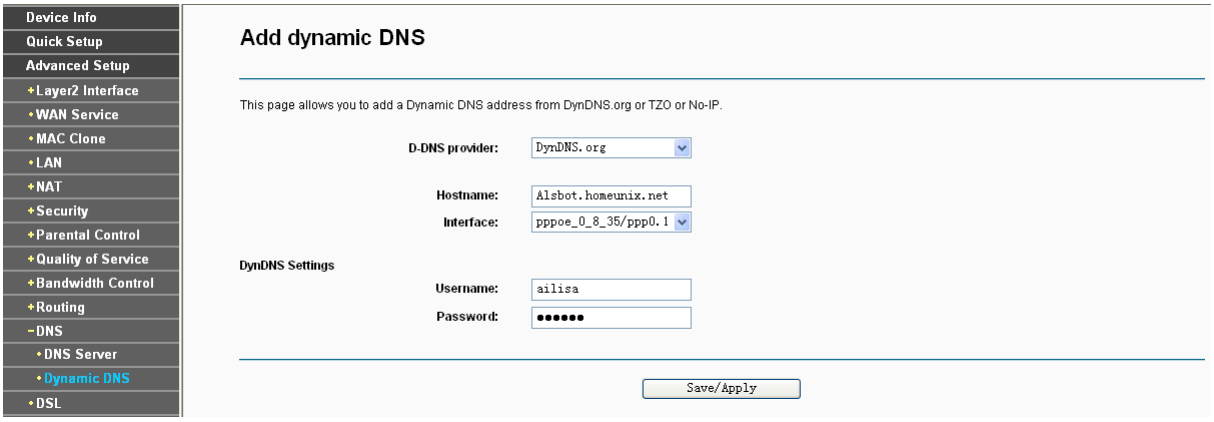


Figure 4-59

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.
5. Click **Save/Apply** to save the entry and then you will see your settings as shown in Figure 4-58.

4.4.12 DSL

Choose "**Advanced Setup**"→"**DSL**", you can see the DSL Settings screen, this screen allows you to configure the DSL (shown in Figure 4-60).

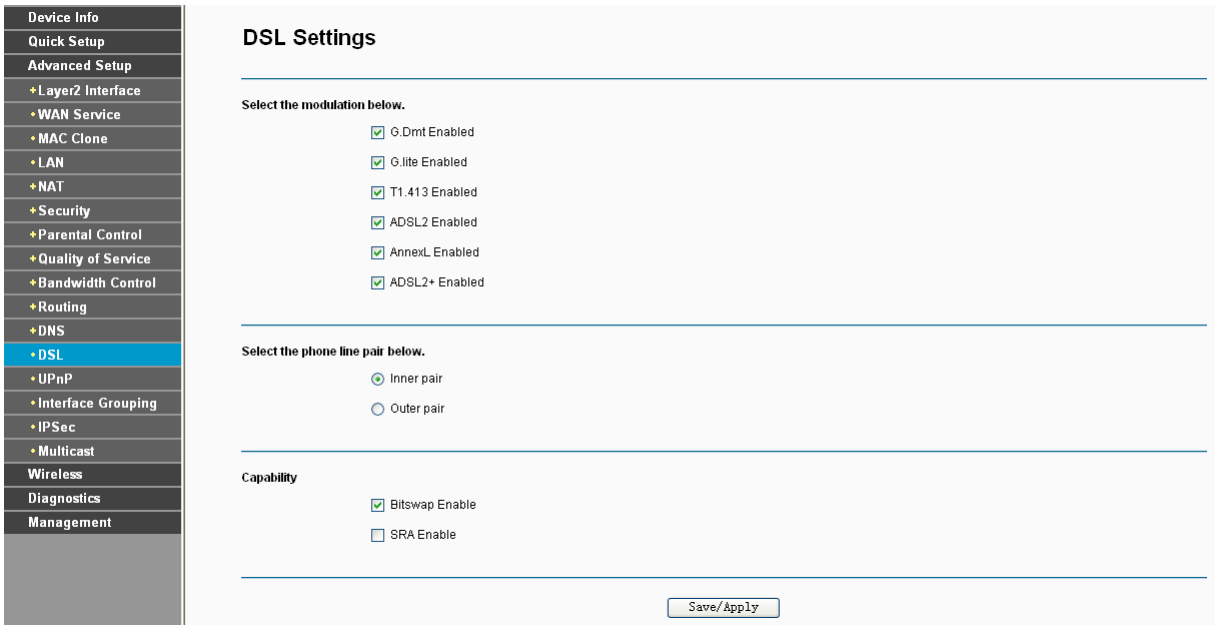


Figure 4-60

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.

4.4.13 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.

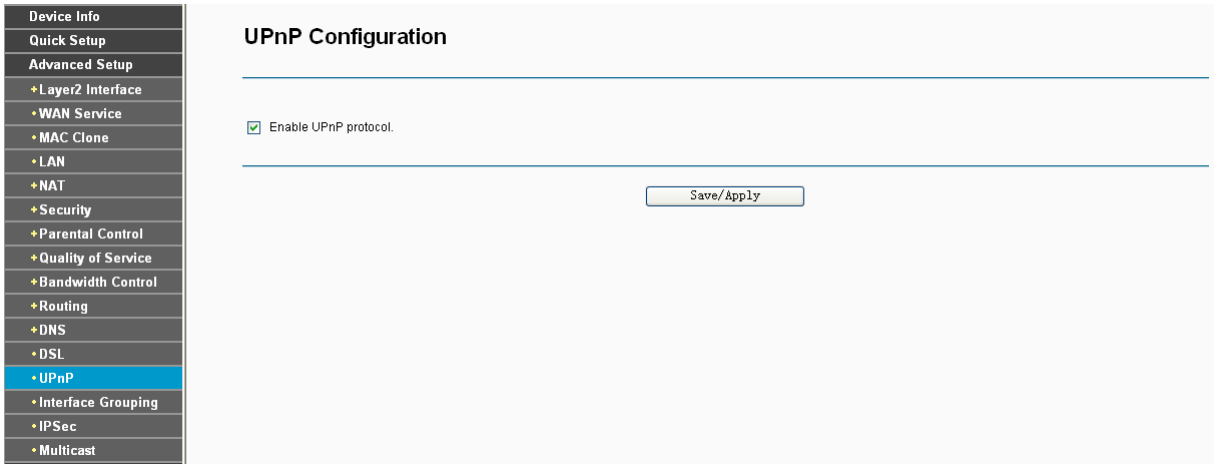


Figure 4-61

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

4.4.14 Interface Grouping

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

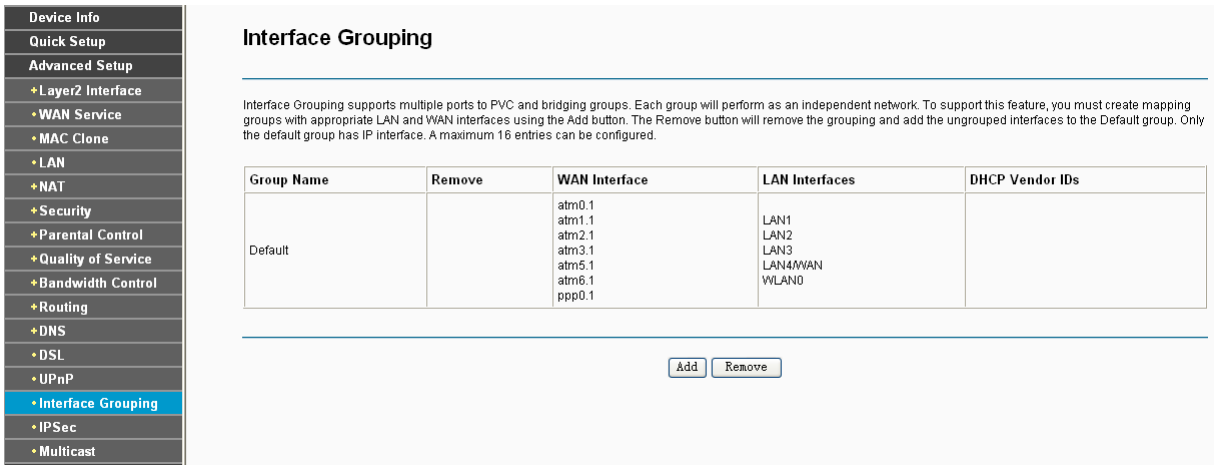


Figure 4-62

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.

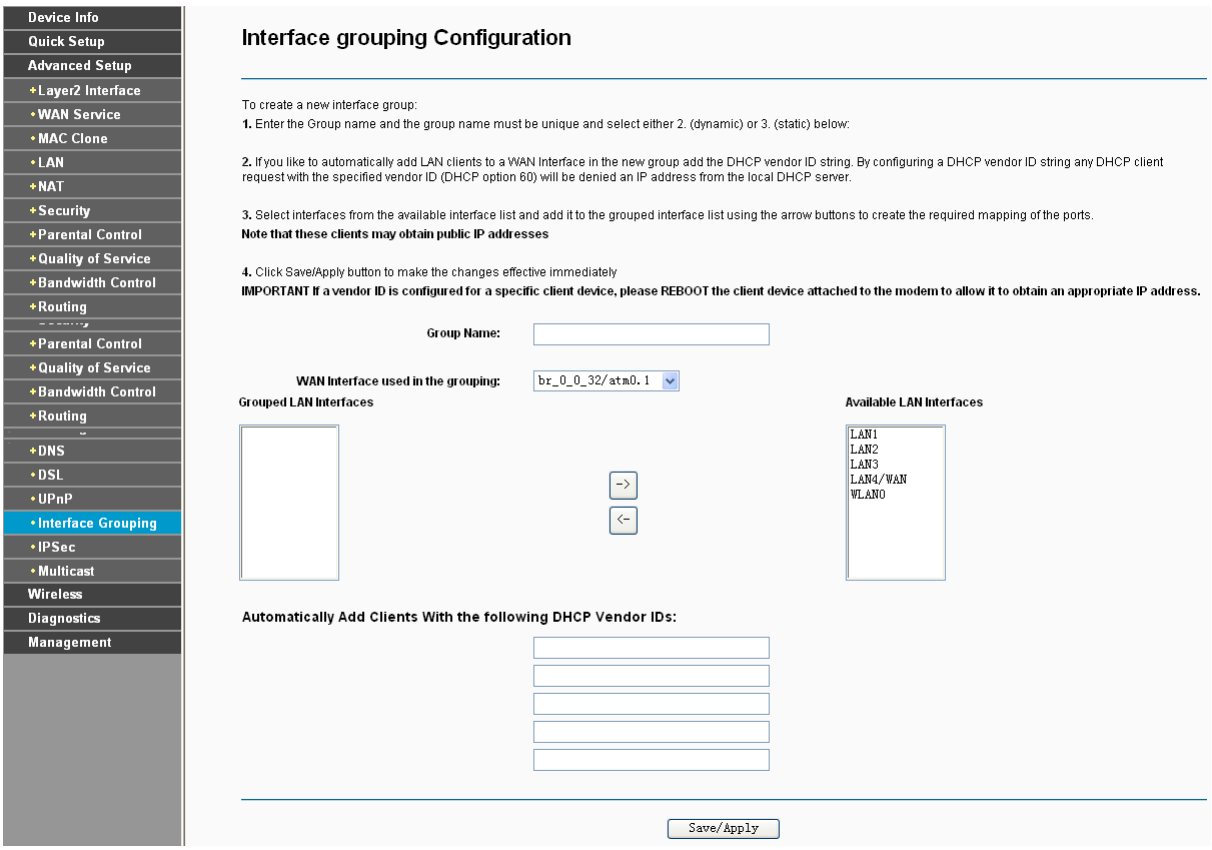


Figure 4-63

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.

4.4.15 IPSec

Choose "**Advanced Setup**"→"**IPSec**", you can Add/Remove or Enable/Disable the IPSec tunnel connections on the screen as shown in Figure 4-65.

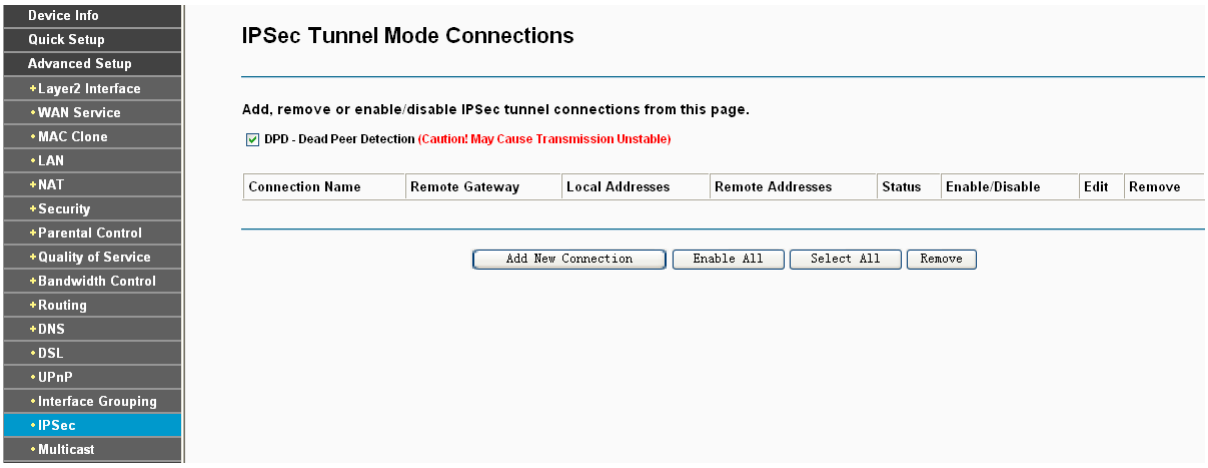
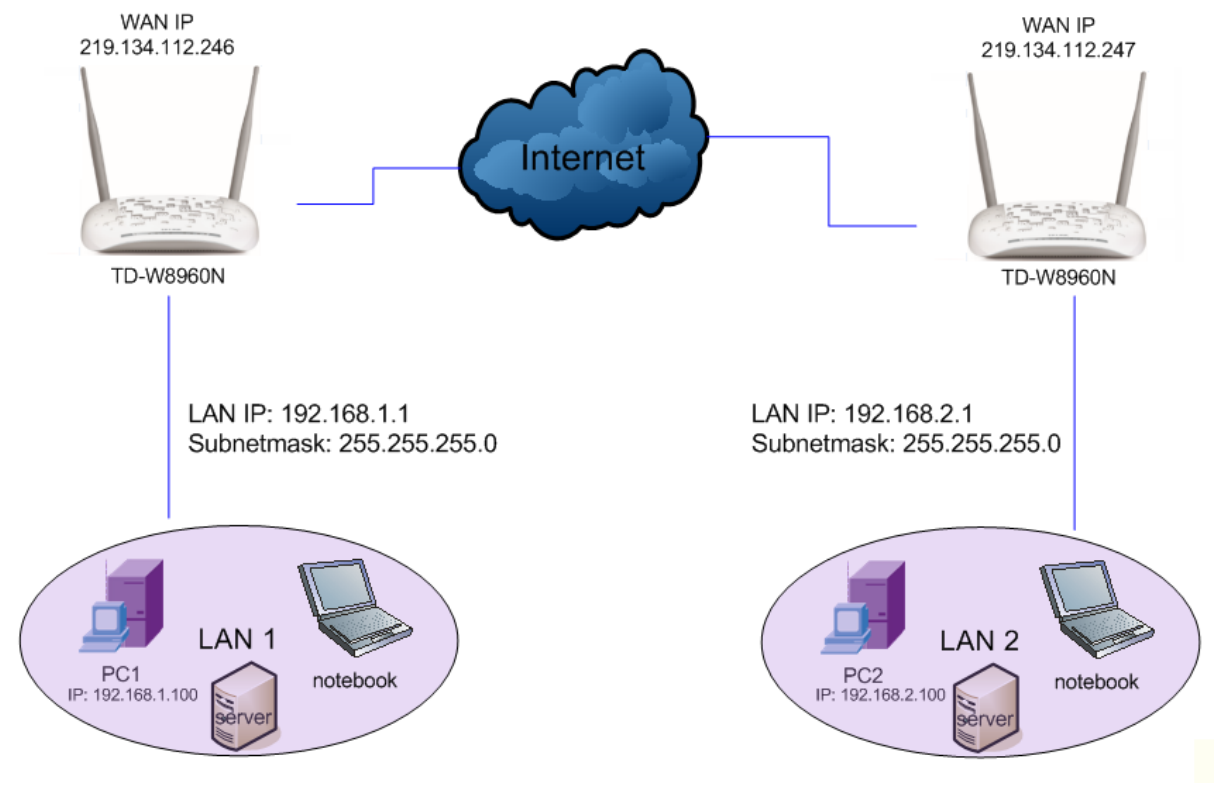


Figure 4-65

This section will guide you to configure a VPN tunnel between two TD-W8960Ns. The topology is as follows.



Note:

You could also use other VPN Routers to set VPN tunnels with TD-W8960N. TD-W8960N supports up to 10 VPN tunnels simultaneously.

Click **Add New Connection** in Figure 4-65 and then you will enter the screen shown in Figure 4-66.

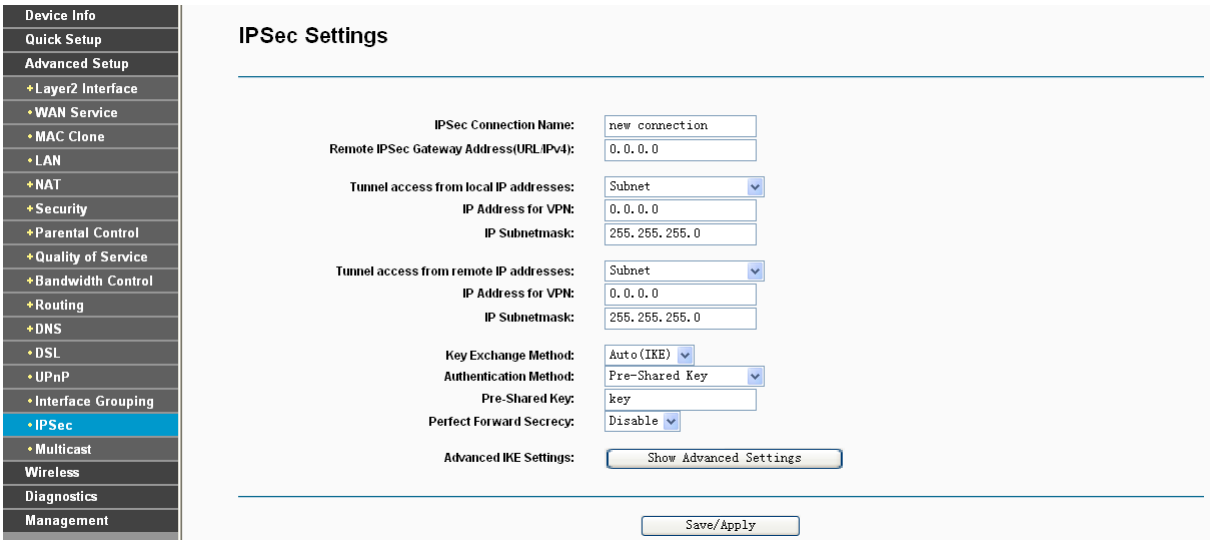


Figure 4-66

- **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.

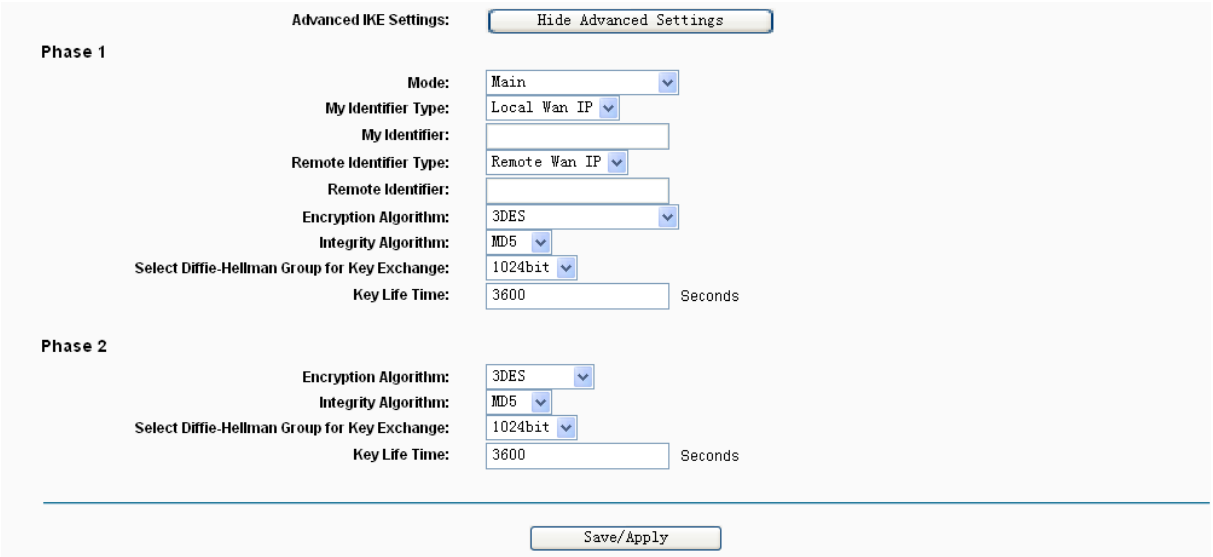
We recommend you leave the Advanced Settings as default value.

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**.

4.4.16 Multicast

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

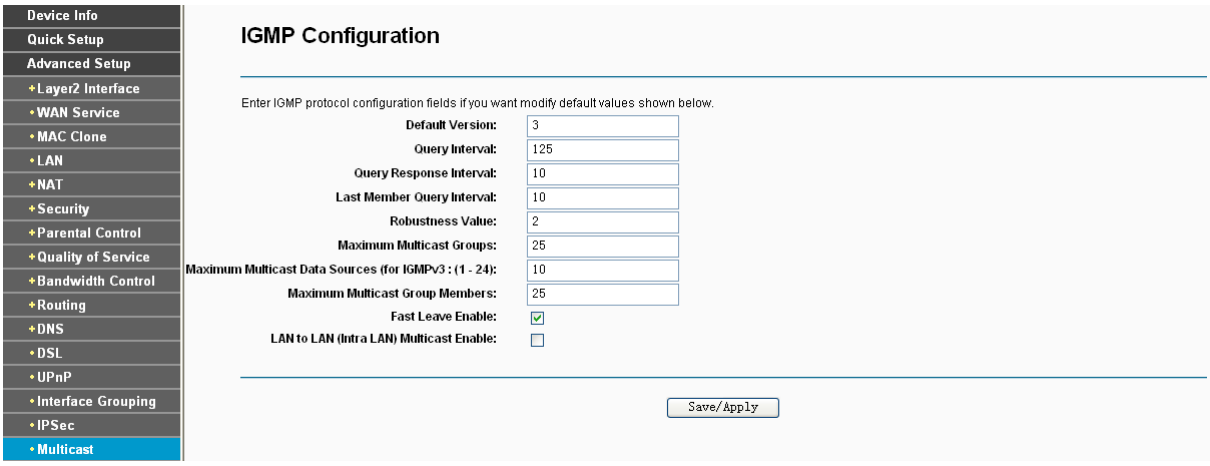
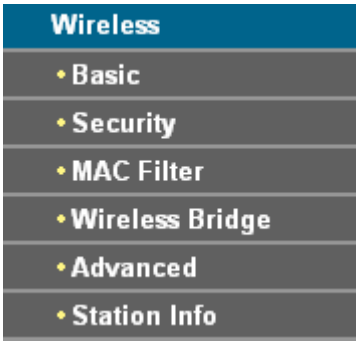


Figure 4-64

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

4.5 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.



4.5.1 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.

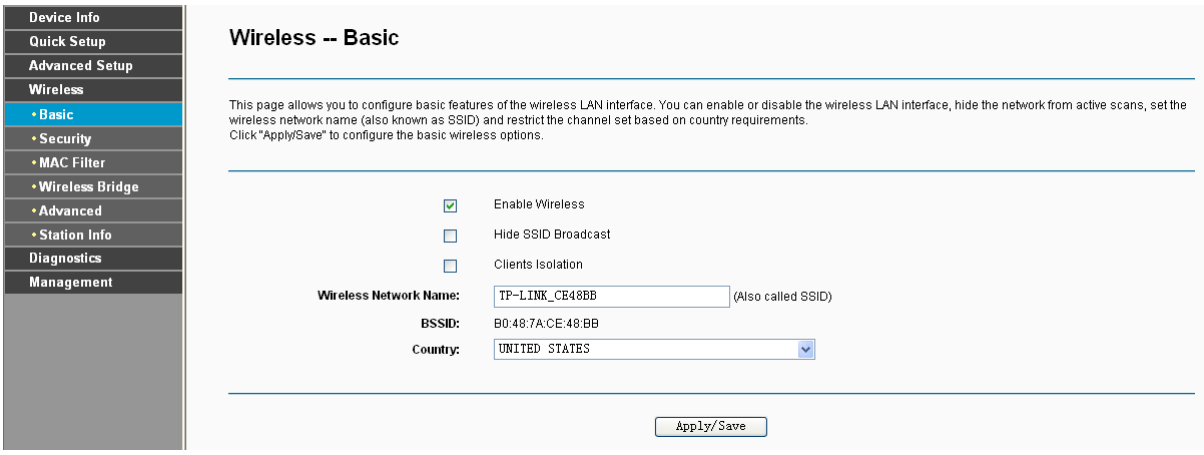


Figure 4-67

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.
- **SSID:** Wireless network name shared among all points in a wireless network. The SSID must be identical for all devices in the wireless network. It is case-sensitive and must not exceed 32 characters (use any of the characters on the keyboard). Make sure this setting is the same for all stations in your wireless network. Type the desired SSID in the space provided.
- **BSSID:** Show the MAC address of the Router.

➢ **Country:** Restrict the channel set and transmit power.

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

4.5.2 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.

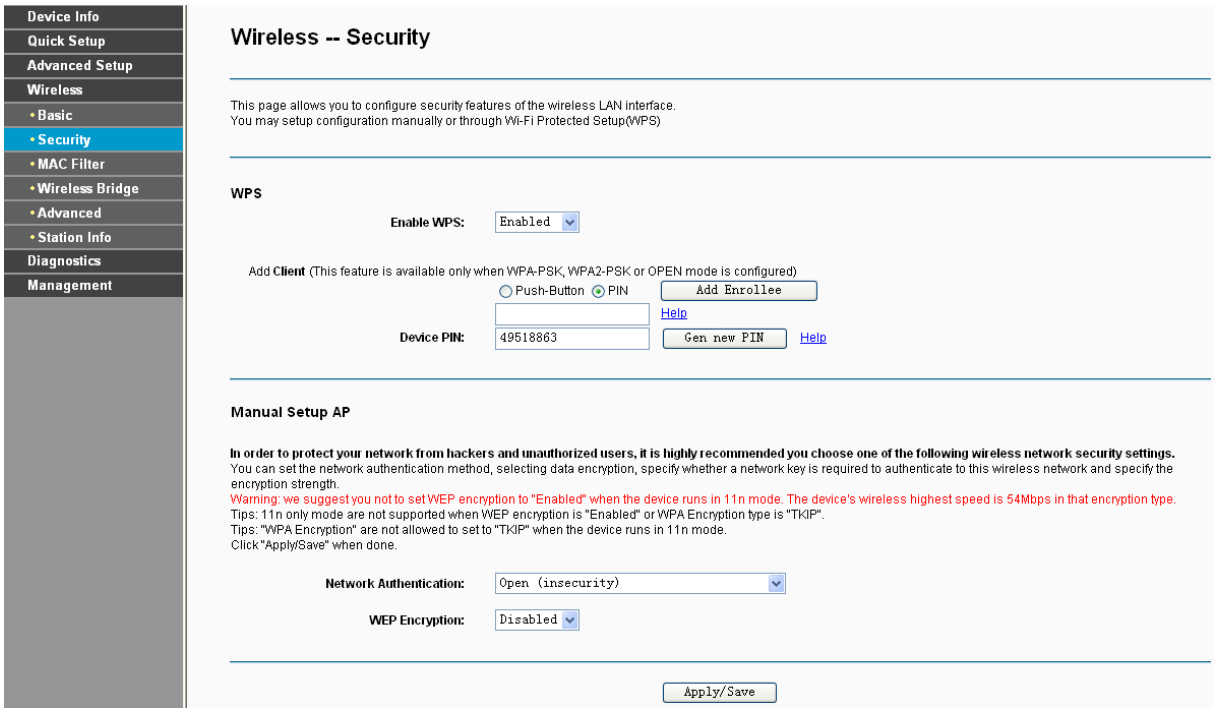


Figure 4-68

4.5.2.1 WPS Setup

Back to LED Explanation

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

If the wireless adapter supports WPS and the Push Button Configuration (PBC) method, you can add it to the network by PBC with the following two methods. Click **Push-Button**, you will see the screen as shown below.

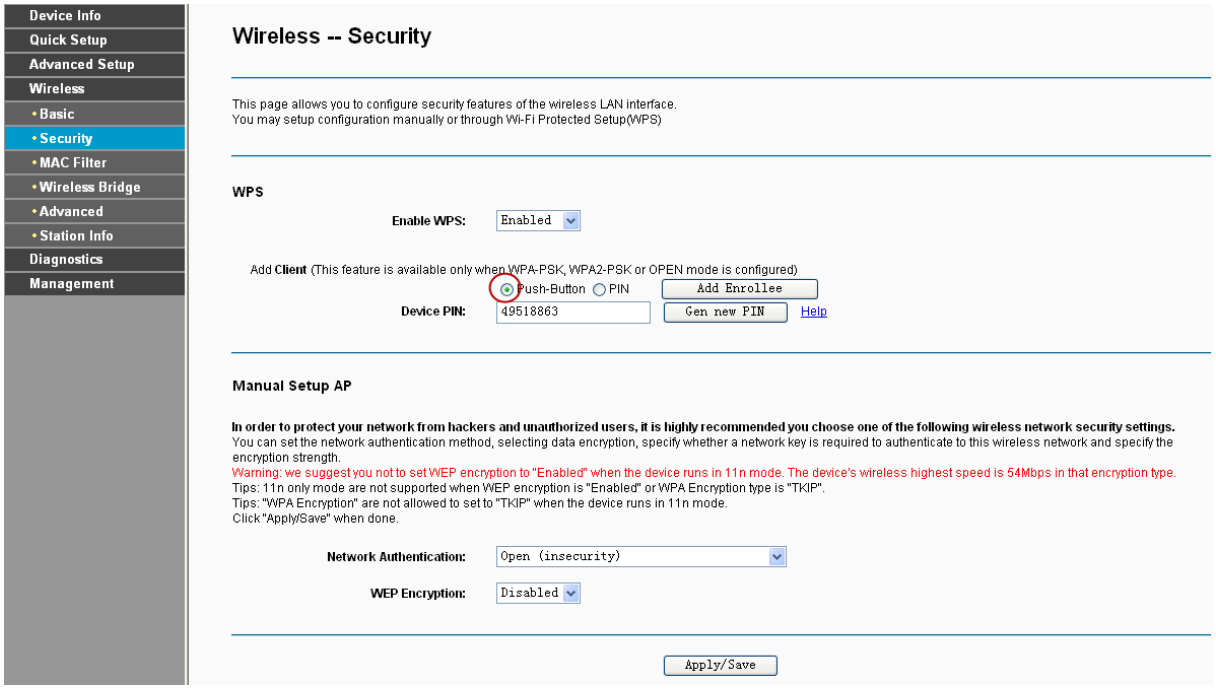
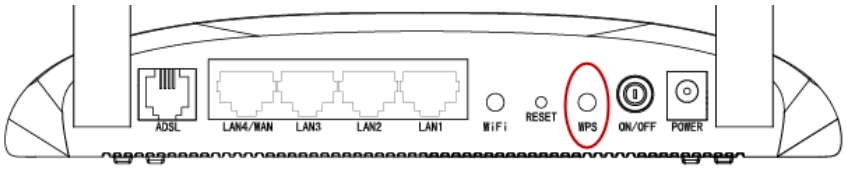


Figure 4-69

Method One: Hardware push button.

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



Step 2: Press and hold the WPS button of the adapter directly for 2 or 3 seconds.

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

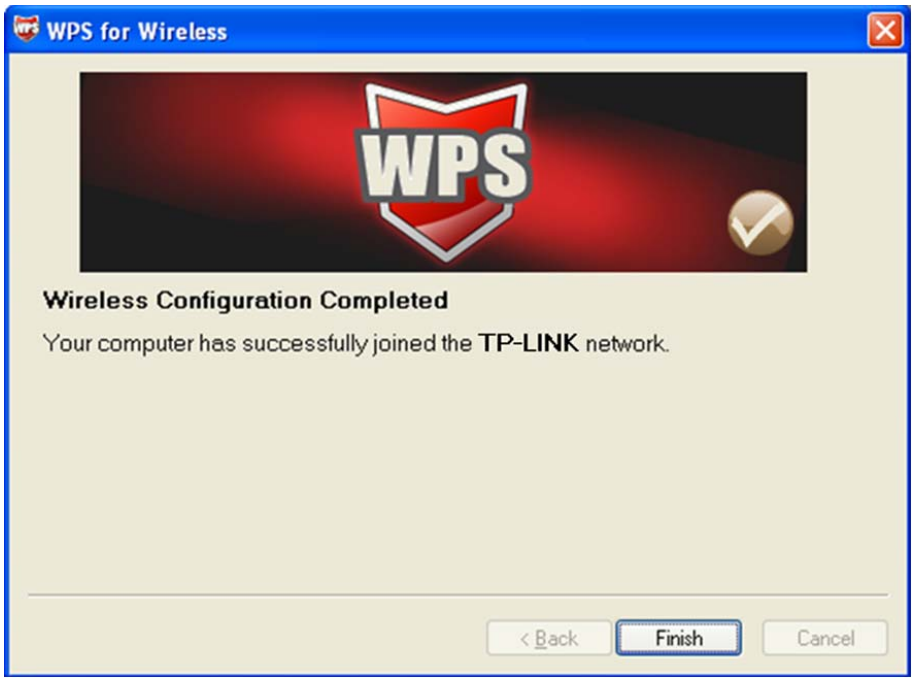
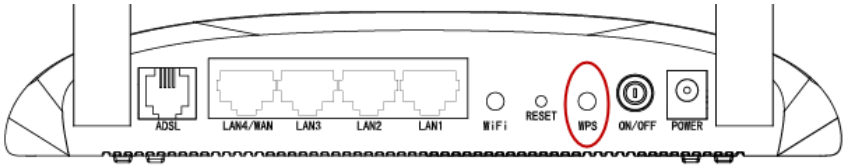


Figure 4-70

Method Two:

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



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

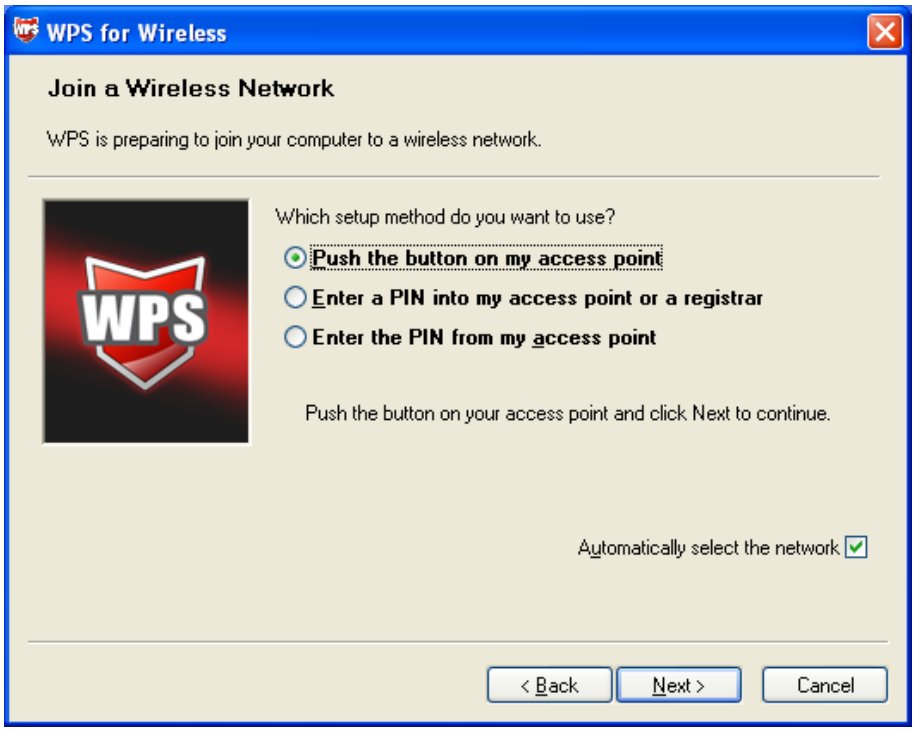


Figure 4-71

Step 3: Wait for a while until the next screen appears. Click **Finish** to complete the WPS configuration.

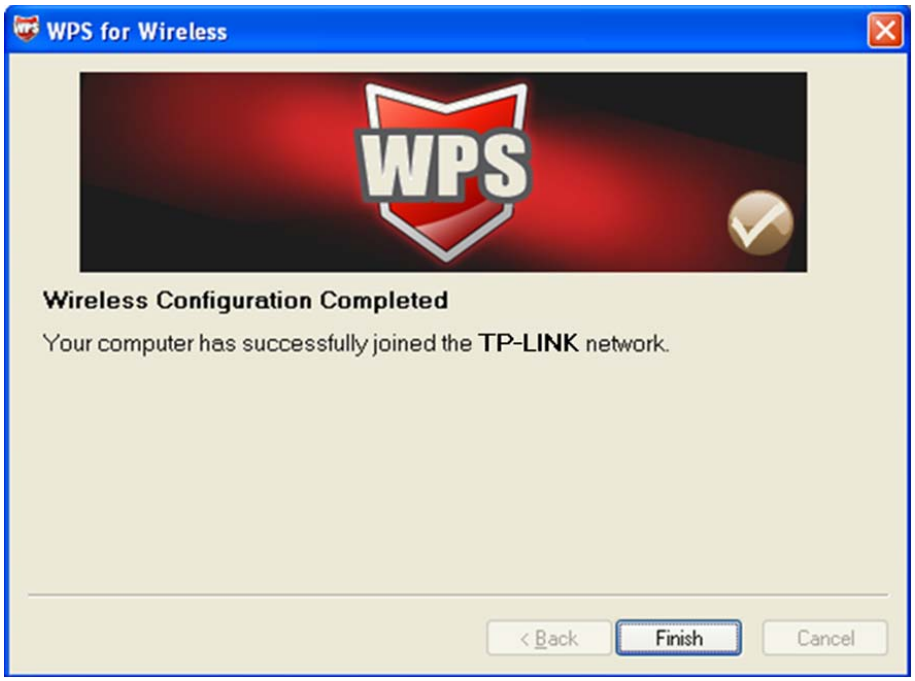


Figure 4-72

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 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**.

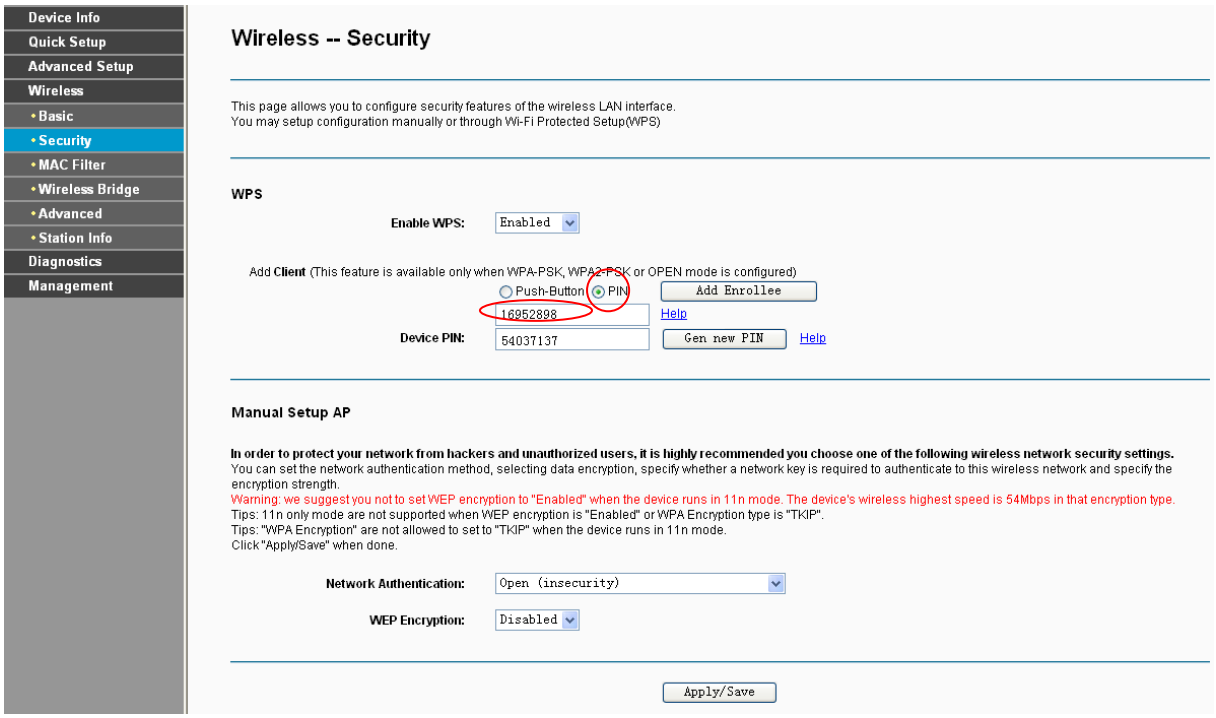


Figure 4-73

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 a PIN into my access point or a registrar**" in the configuration utility of the WPS as below, and click **Next**.

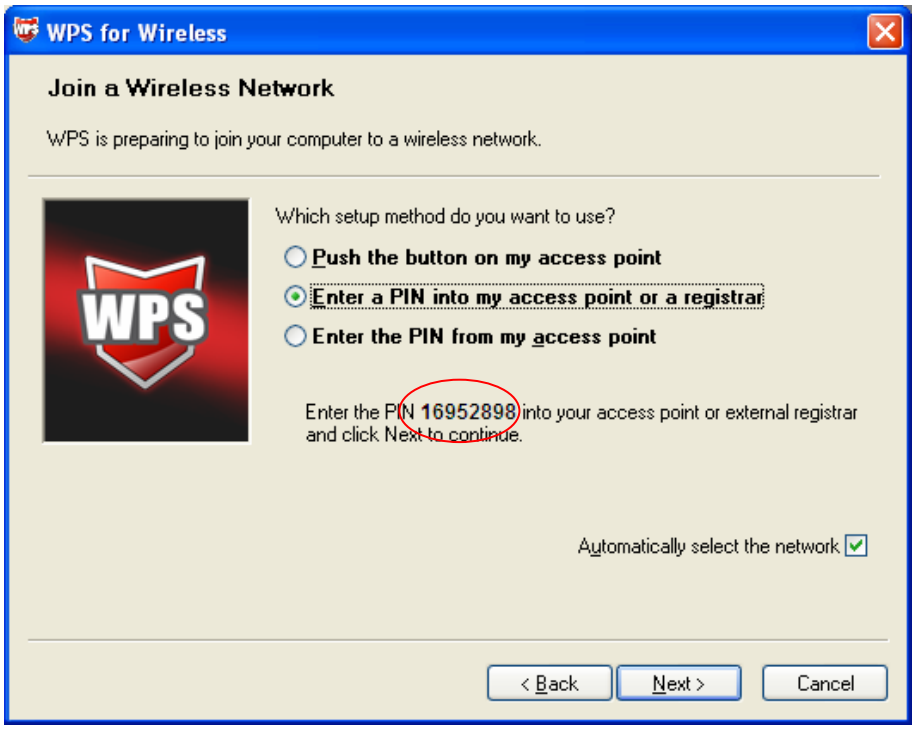


Figure 4-74

Note:

In this example, the default PIN code of this adapter is 16952898 as the preceding figure shown.

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

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

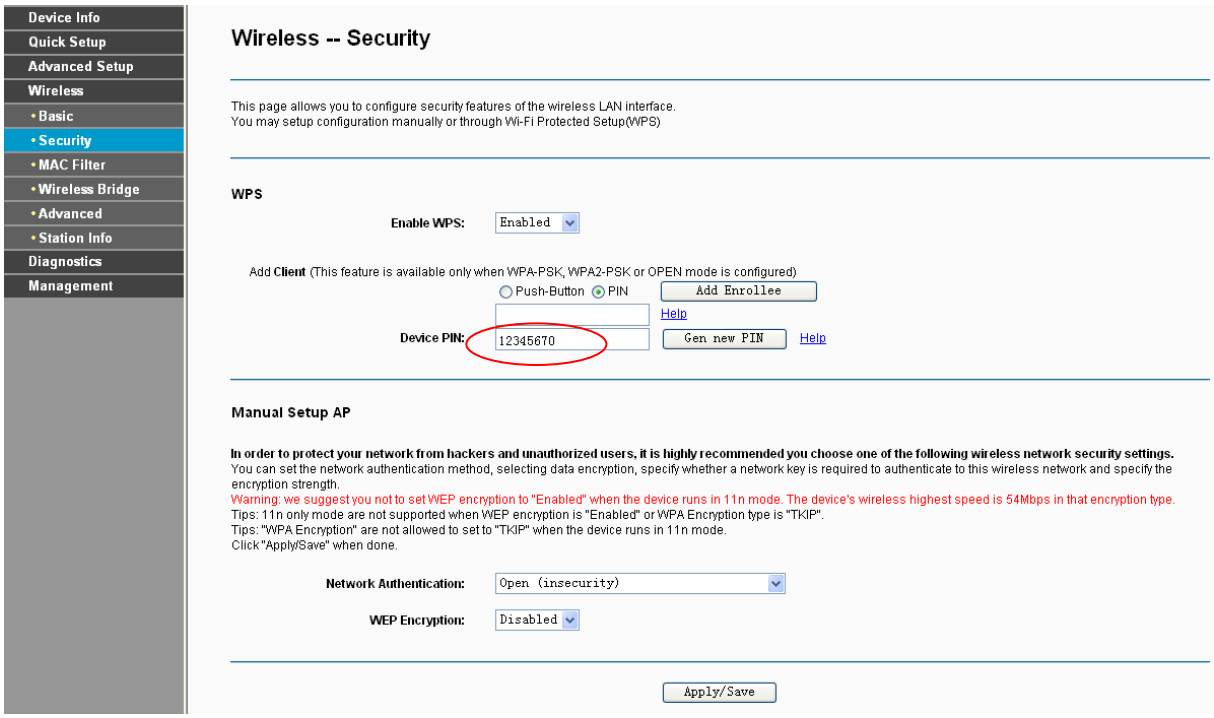


Figure 4-75

Step 2: For the configuration of the wireless adapter, please choose "**Enter a PIN from my access point**" in the configuration utility of the WPS as below, and enter the PIN code of the Router into the field after "**Access Point PIN**". Then click **Next**.

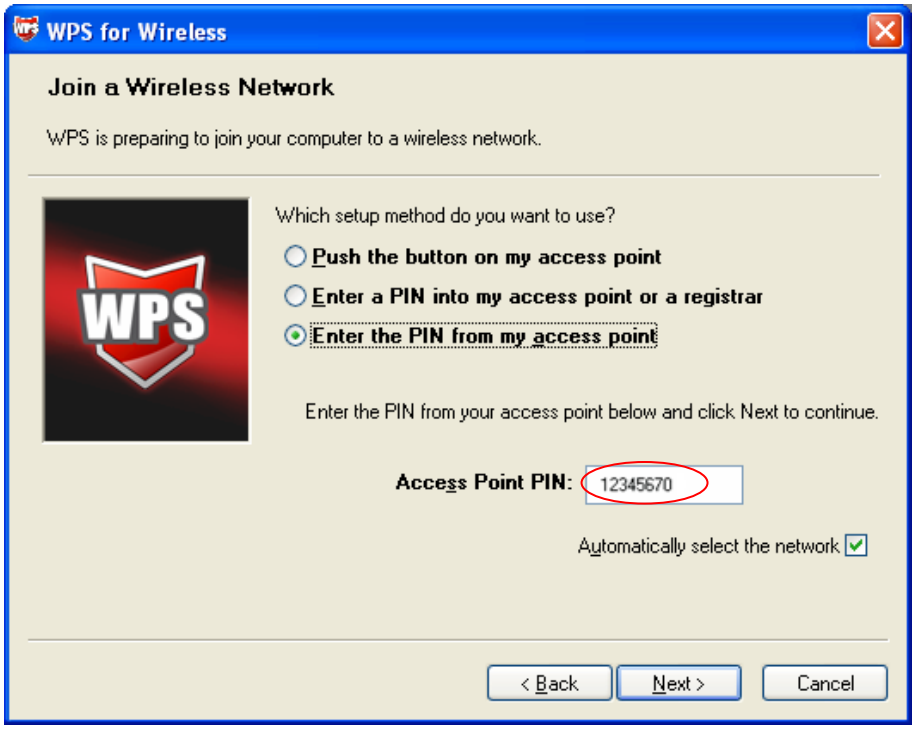


Figure 4-76

4.5.2.2 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.

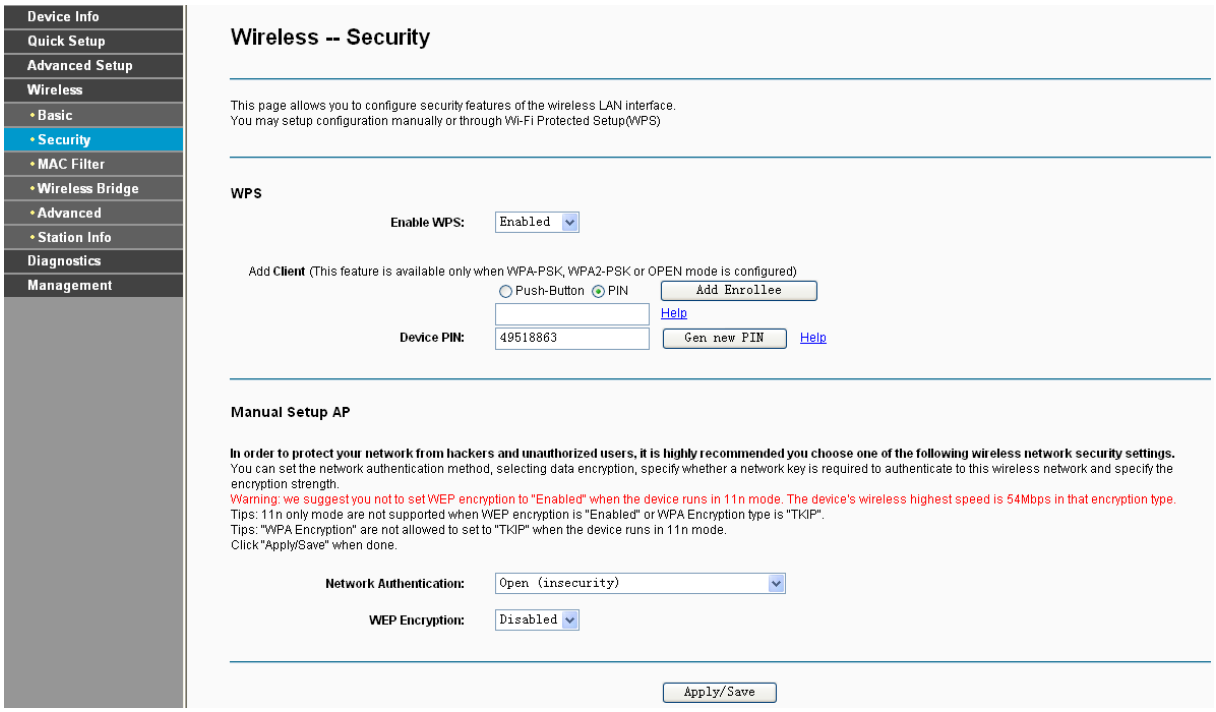


Figure 4-75

➢ **Network Authentication:** Select an authentication type from the drop-down list. Options available are: Open, Shared, WPA, WPA-PSK, WPA2, WPA2-PSK, Mixed WPA2/WPA, and Mixed WPA2/WPA-PSK.

☞ **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 4-78. **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 4-79. **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.

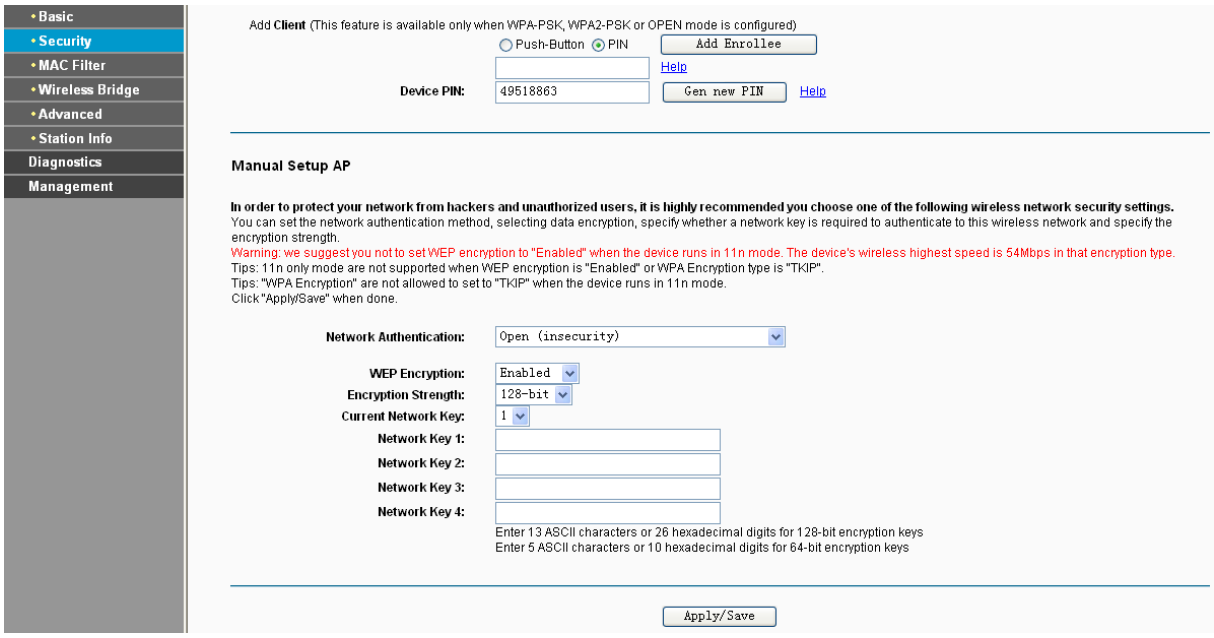


Figure 4-78

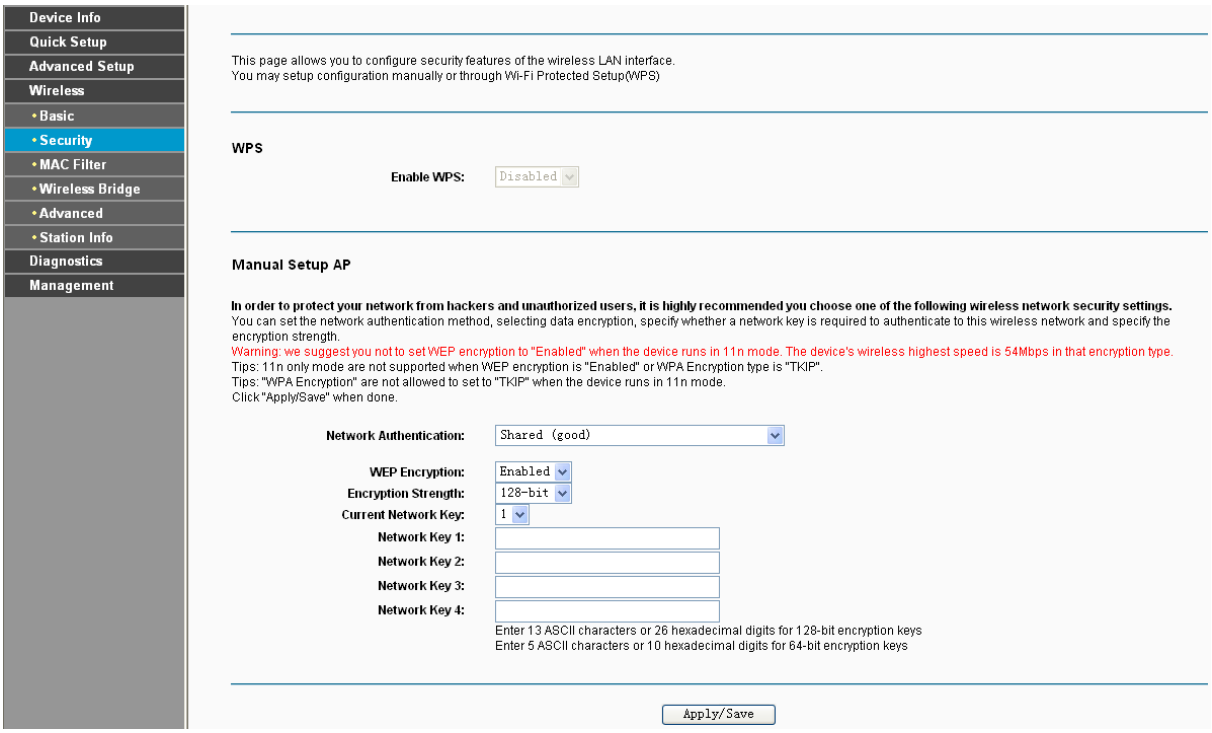


Figure 4-79

- **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 **Shared (good)** from the **Network Authentication** drop-down list. The menu will change to offer the appropriate settings.
2. Select **64-bit** from the **WEP Encryption** drop-down list.

3. Select “**1**” from **Current Network Key** drop-down list.
4. Type in the password in the **Network Key 1** field.
5. Click **Save/Apply** to save the new configuration.

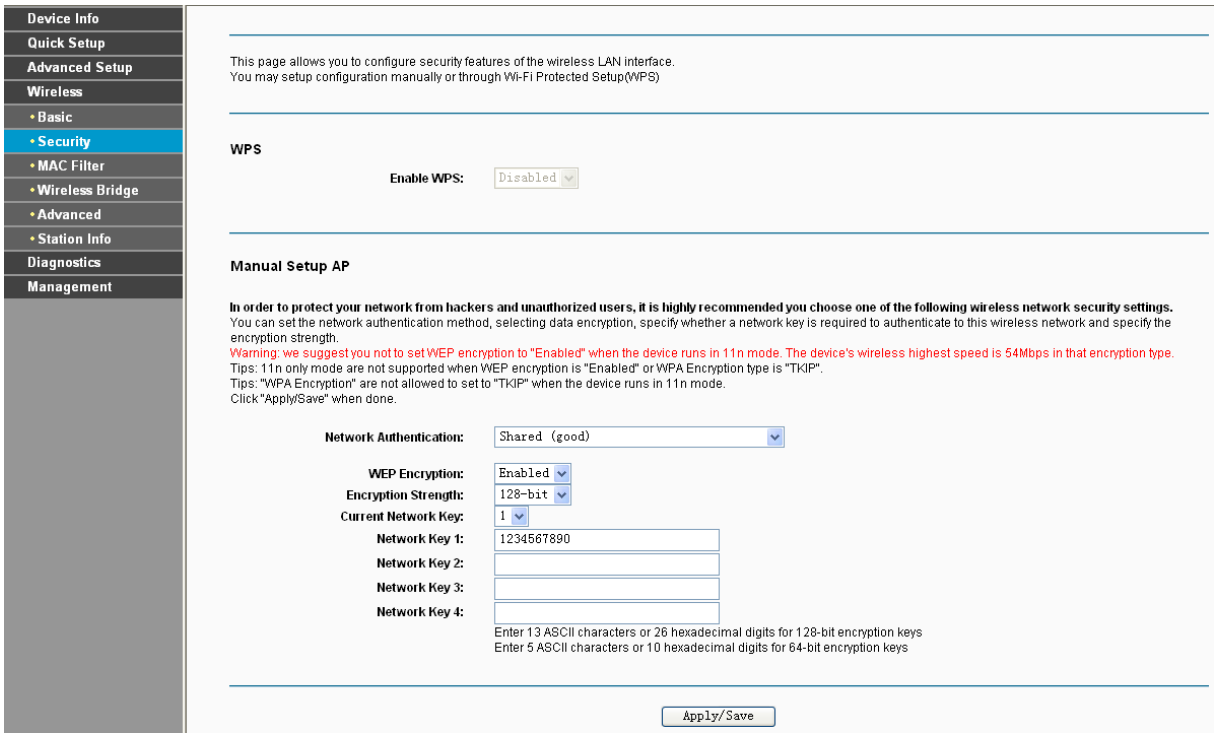


Figure 4-80

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 4-80 above.

2. WPA

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.

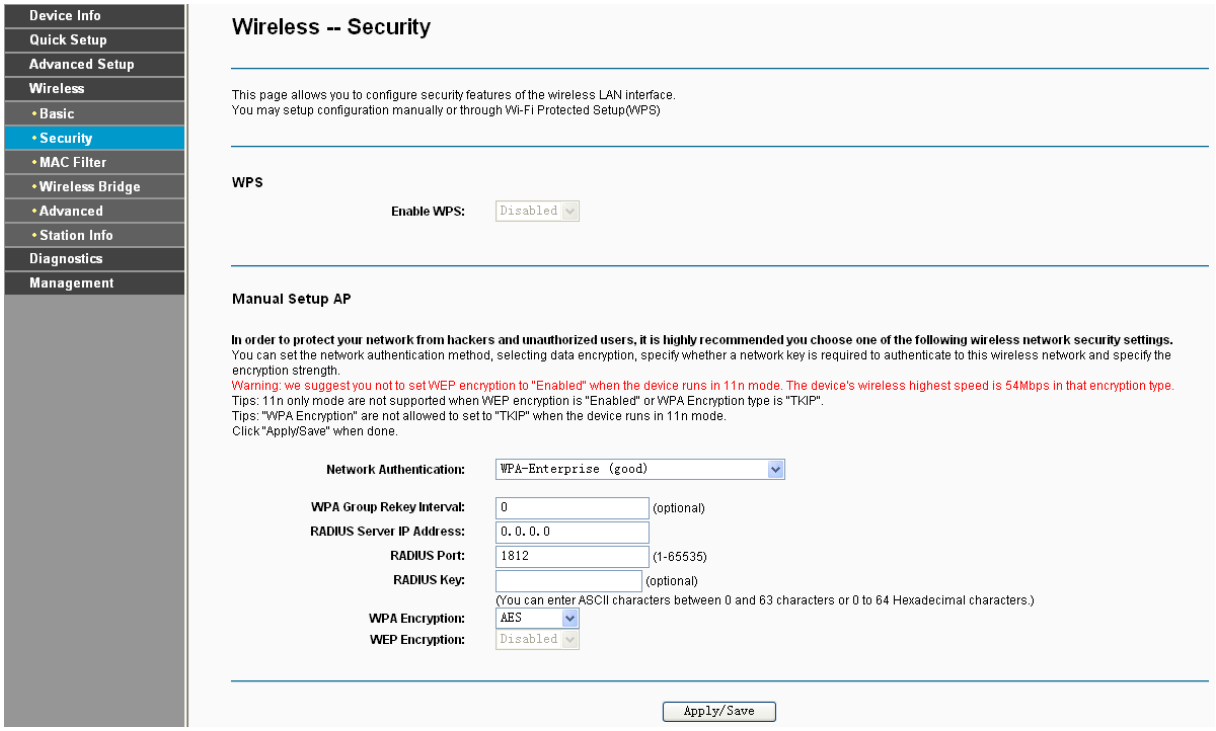


Figure 4-81

- **WPA Group ReKey Interval:** Enter the Key Renewal period, which tells the 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 or AES (AES is an encryption method stronger than TKIP).

Configure WPA settings

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

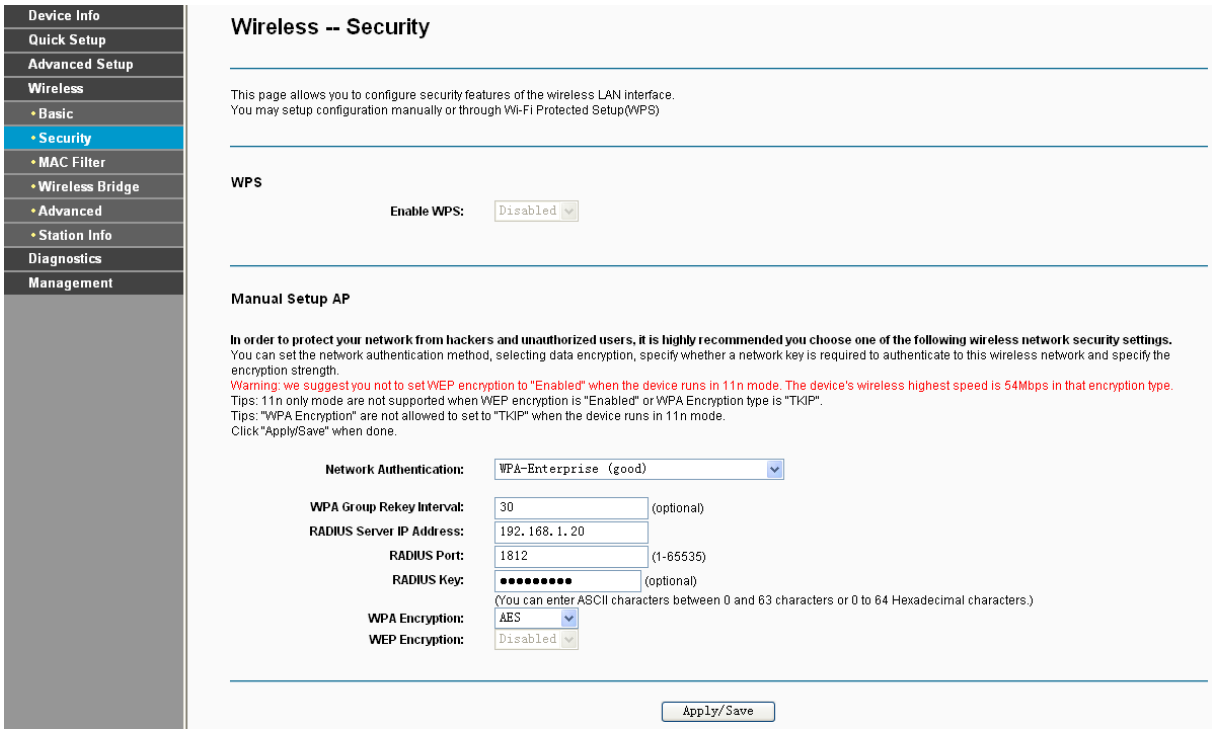


Figure 4-82

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.

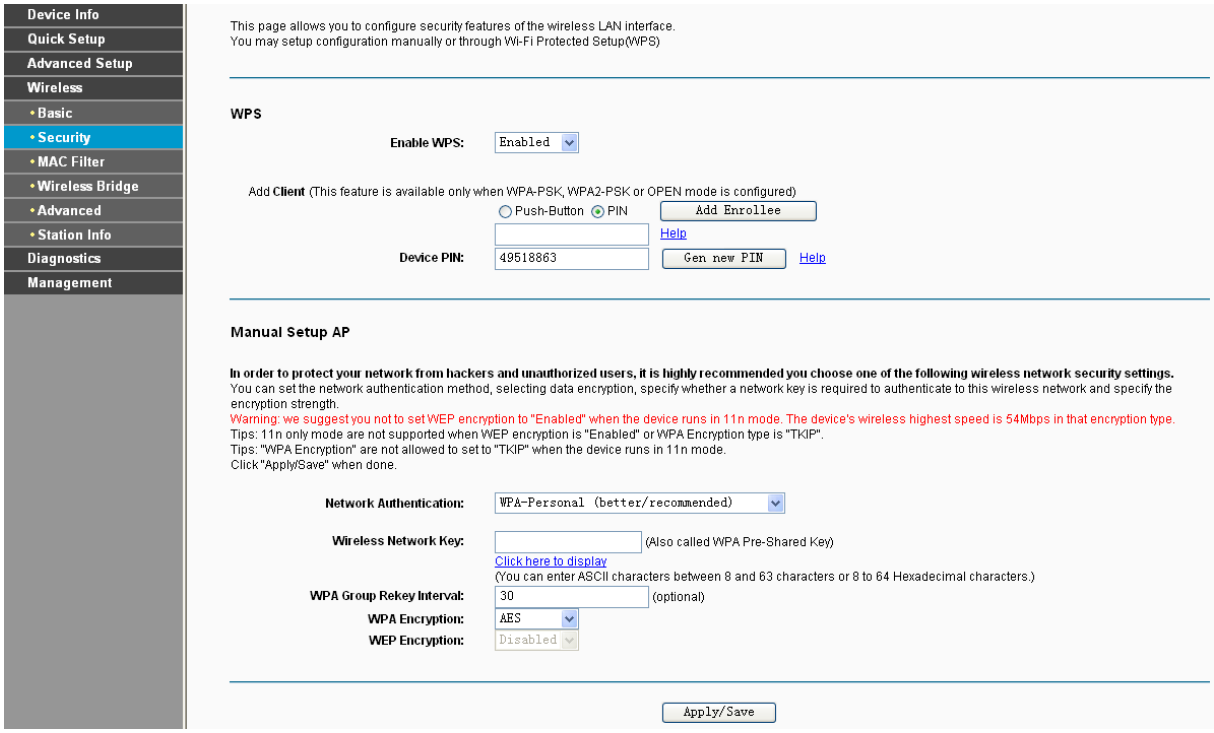


Figure 4-83

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

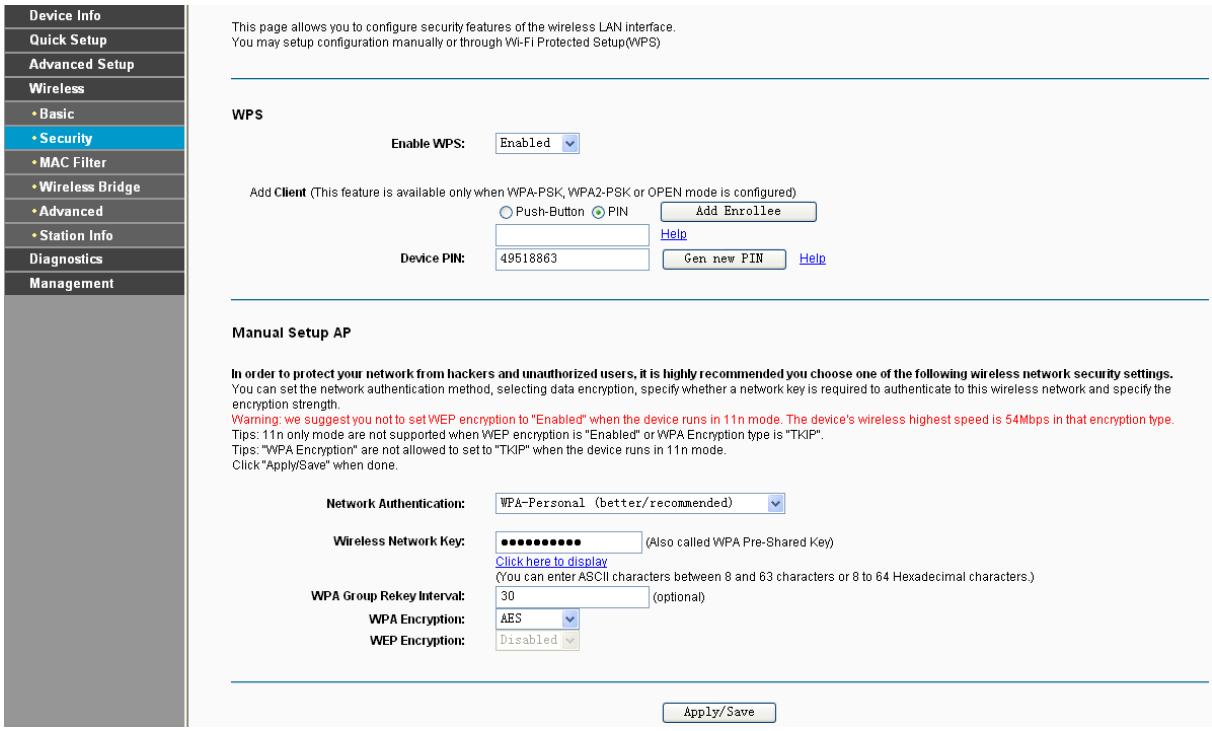


Figure 4-84

Note:

If you click the option “Click here to display”, the Figure 4-85 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.

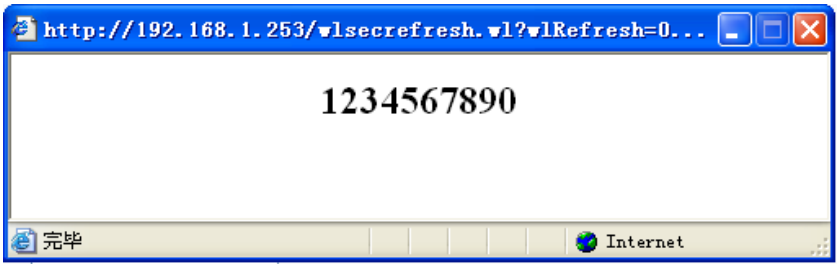


Figure 4-85

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.

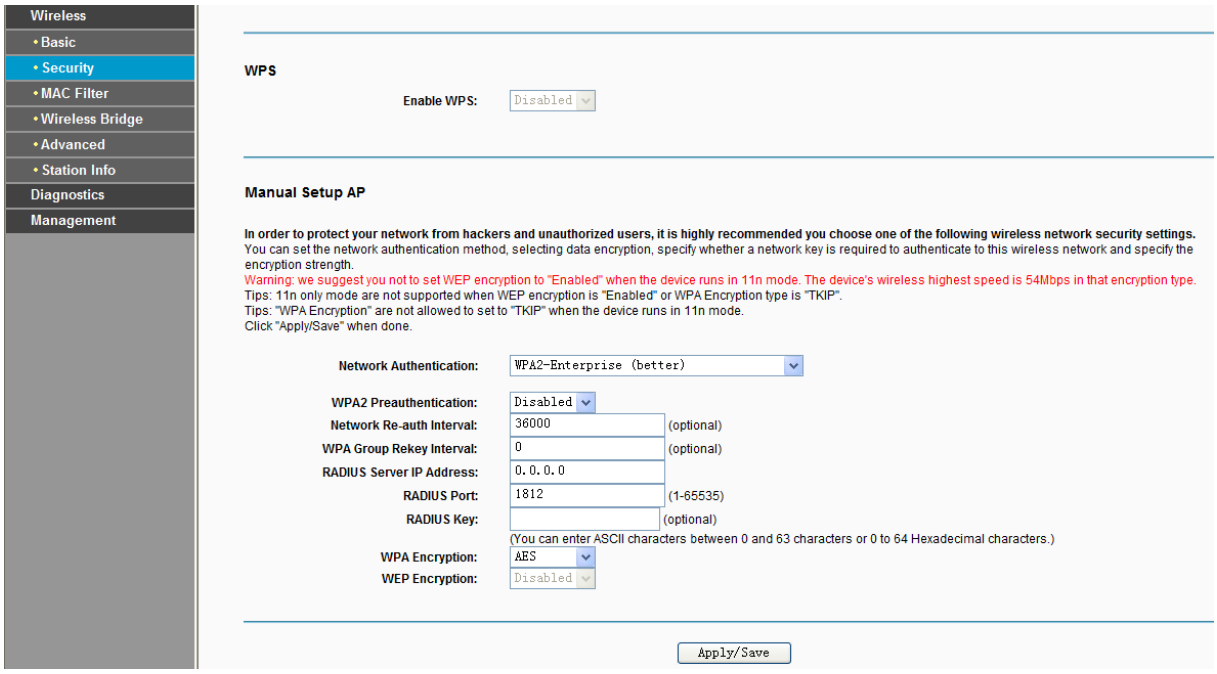


Figure 4-86

- **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.

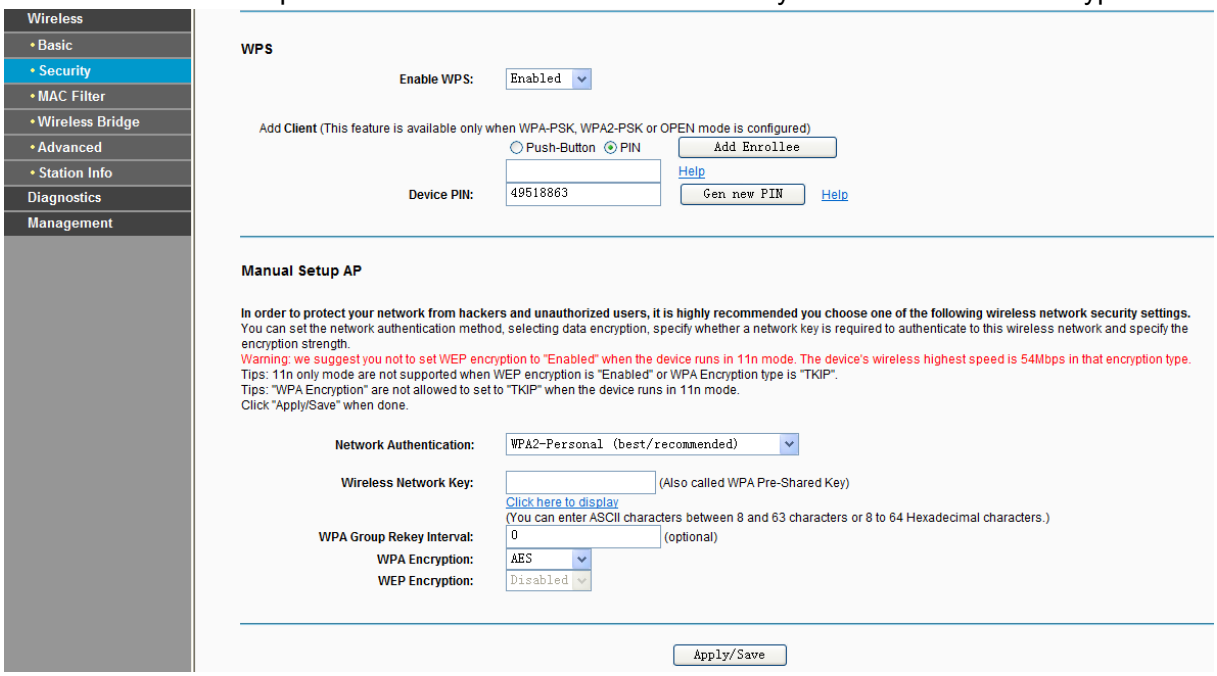


Figure 4-87

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.

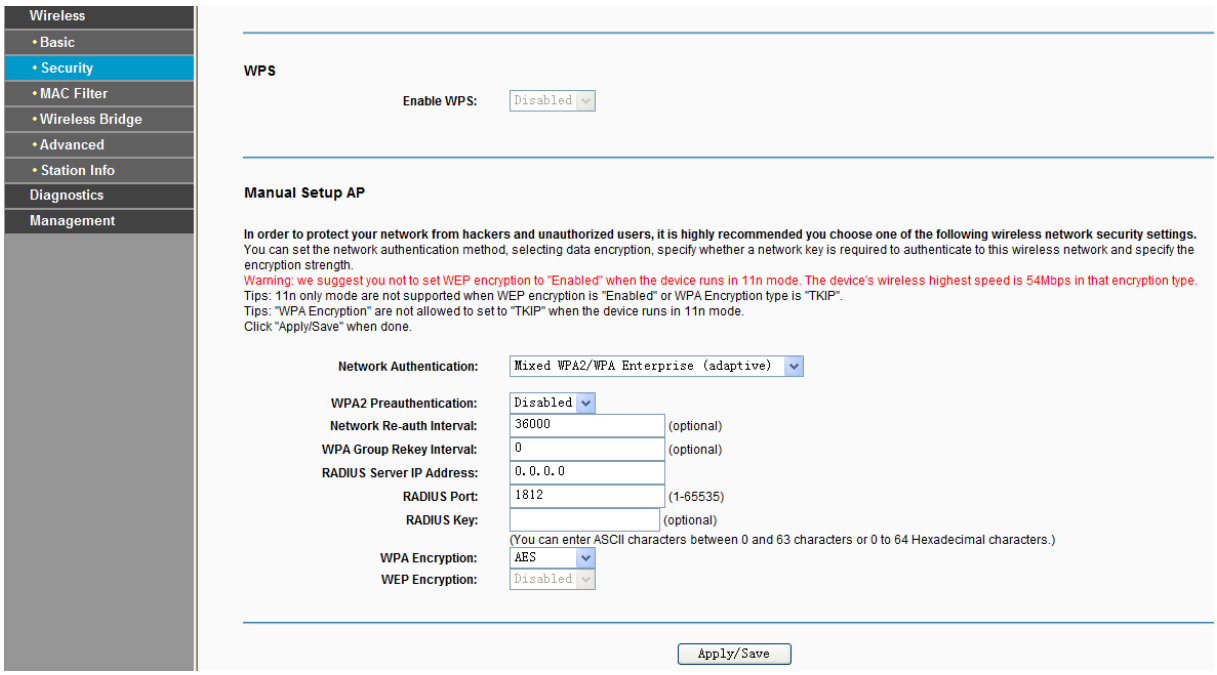


Figure 4-88

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.

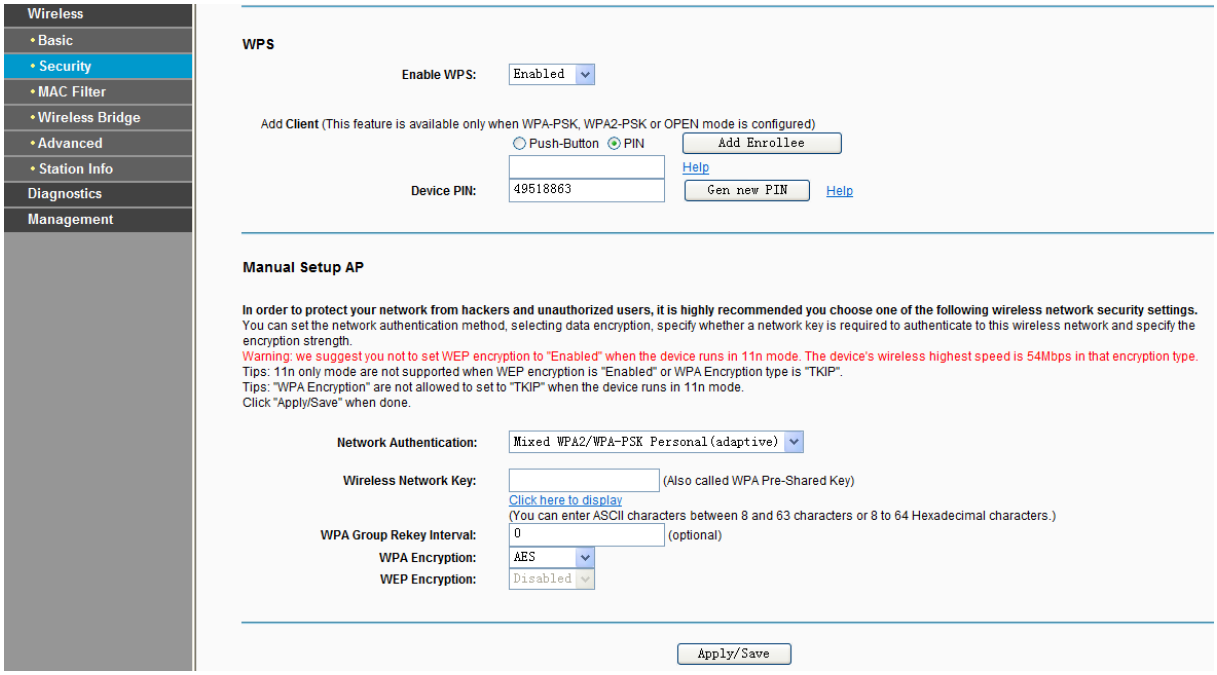


Figure 4-89

4.5.3 MAC Filter

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

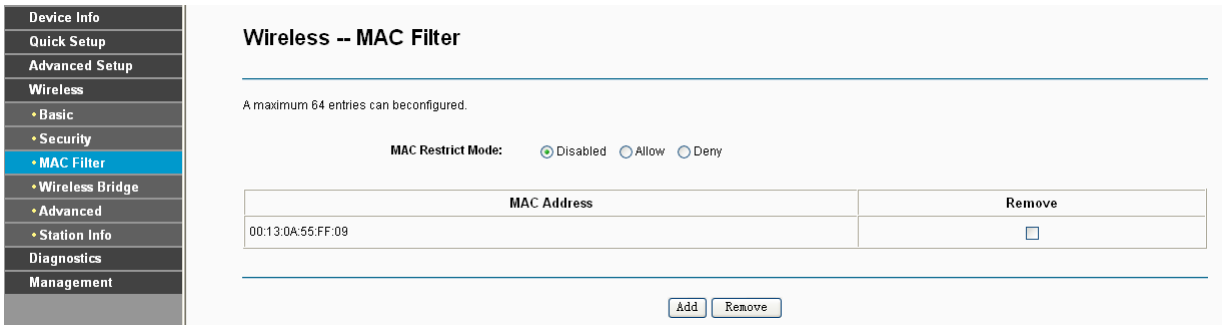


Figure 4-90

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.

- **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**".

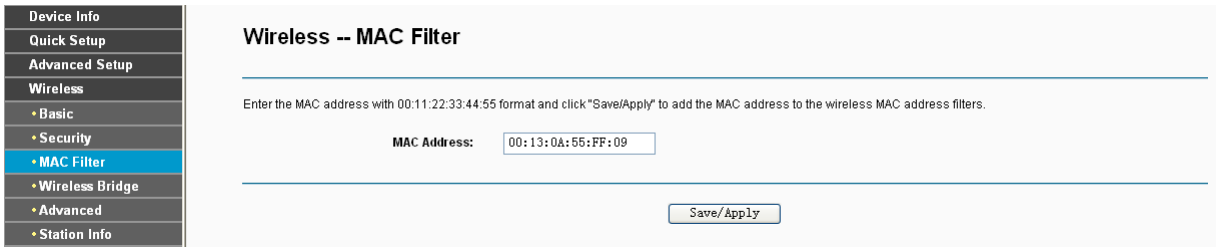


Figure 4-91

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

4.5.4 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.

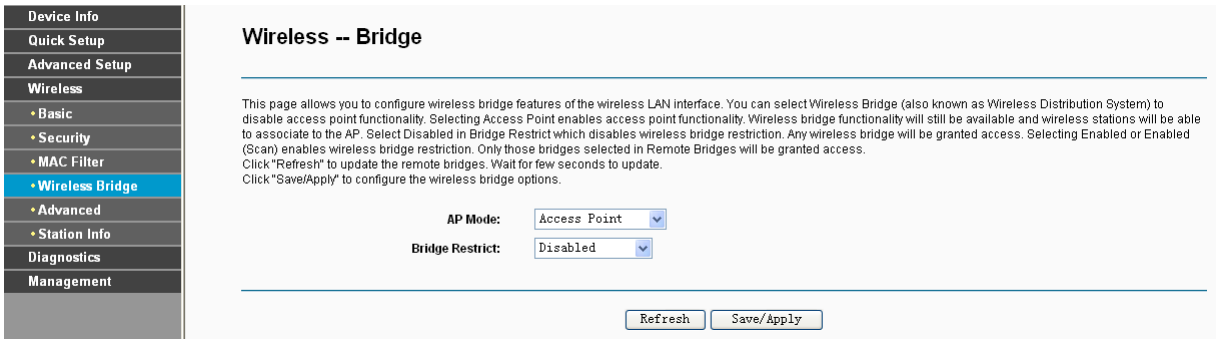


Figure 4-92

- **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.

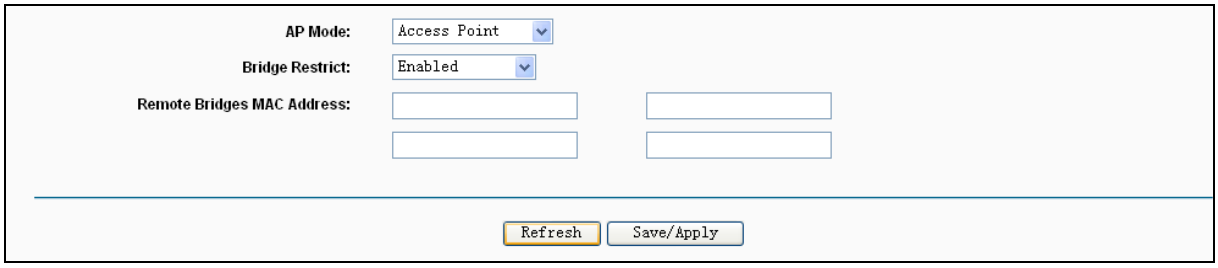


Figure 4-93

- **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.

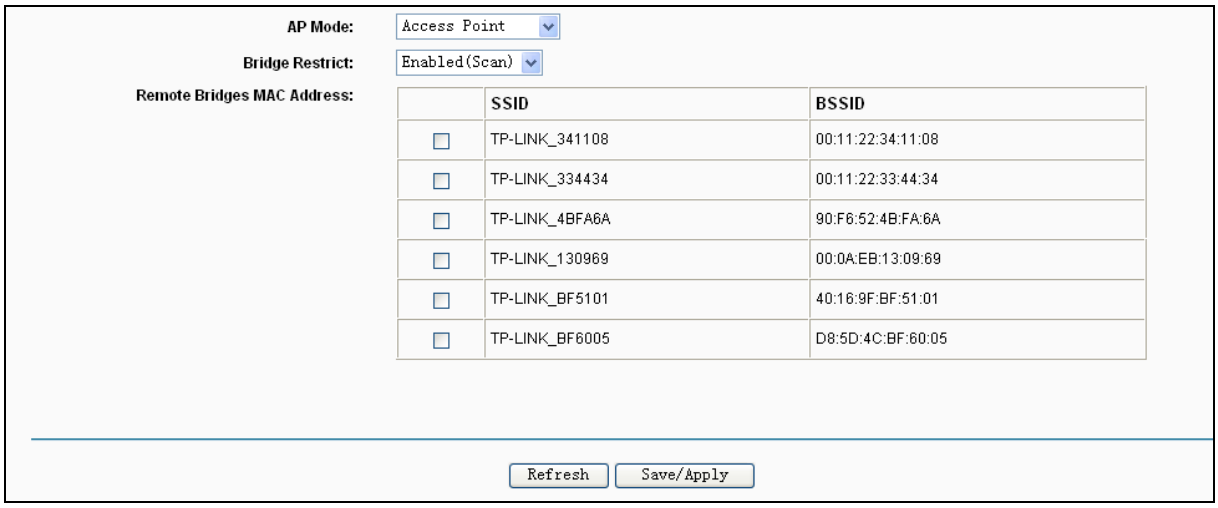


Figure 4-94

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.

4.5.5 Advanced

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

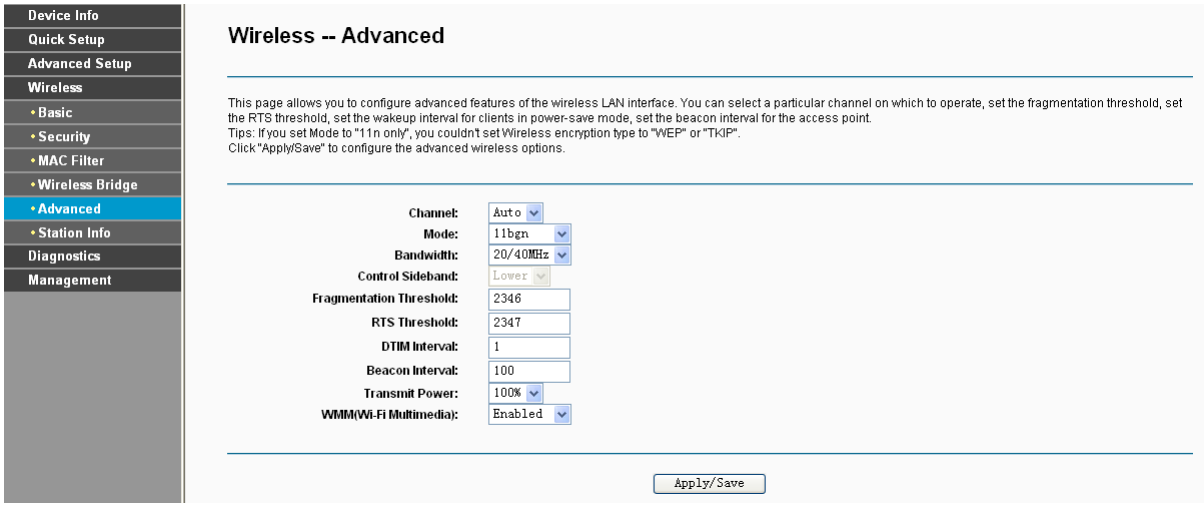


Figure 4-95

- **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 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 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 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 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.

4.5.6 Station info

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

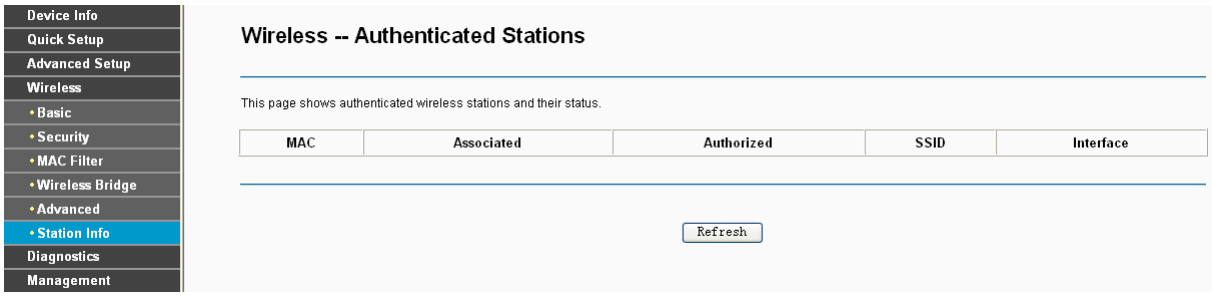


Figure 4-96

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.
- **Interface**: Displays the connected wireless station's Interface mode.

4.6 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.

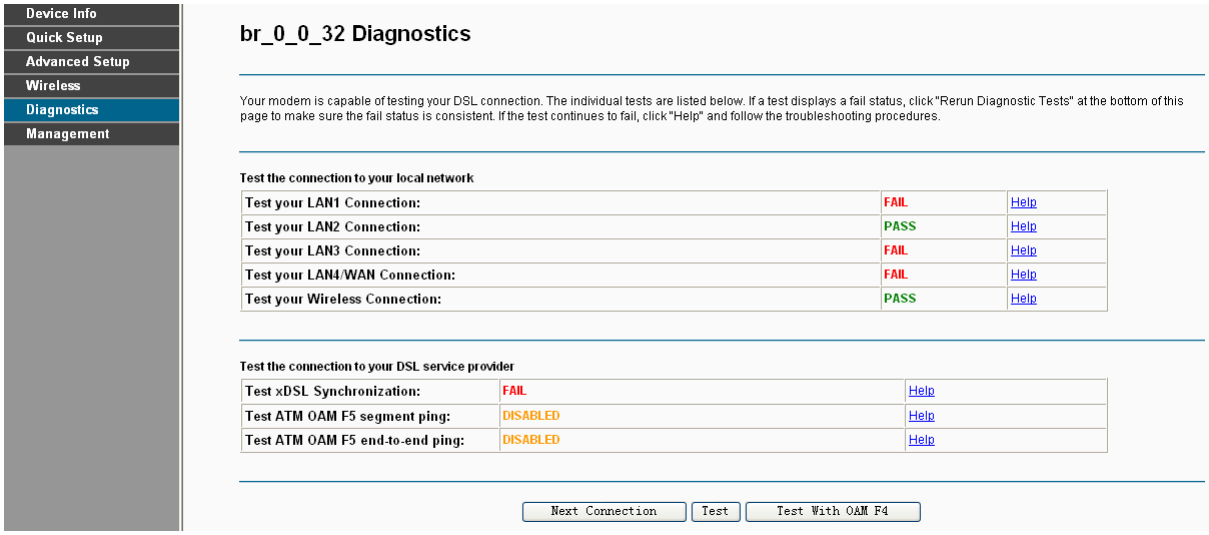
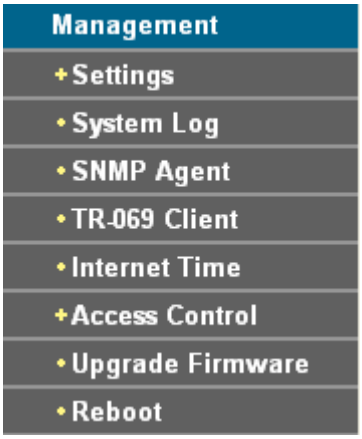


Figure 4-97

4.7 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.



4.7.1 Settings

This section provides three important functions for managing the Router; they are **Backup**, **Update** and **Restore Default** (shown in Figure 4-98). The detailed manipulations are described below.

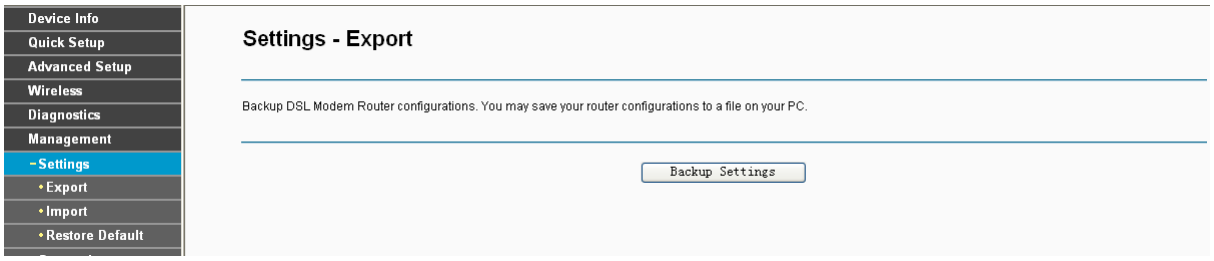


Figure 4-98

4.7.1.1 Export

Choose "**Management**"→"**Settings**"→"**Export**", you can see the **Export** screen, this screen (shown in Figure 4-99) allows you to save the current configuration of the Router as a backup file.

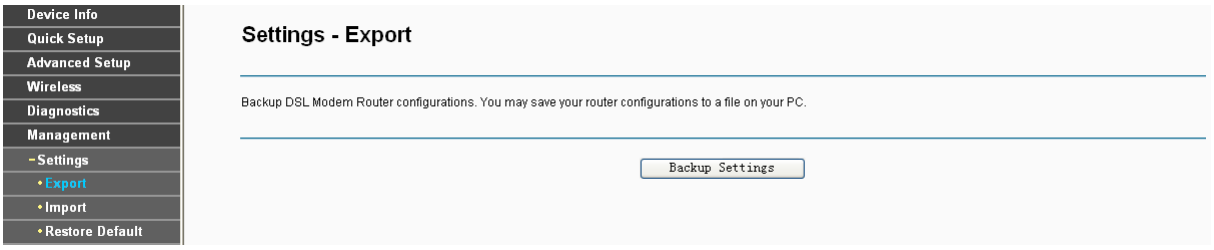


Figure 4-99

To back up the Router's current settings:

1. Click the **Export Settings** button on the preceding screen (pop-up Figure 4-99), the following screen will then appear (shown in Figure 4-100).

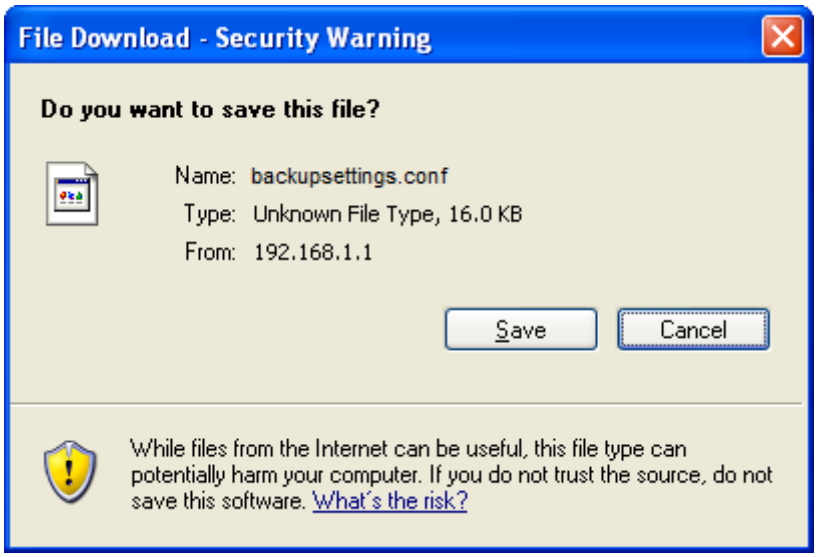


Figure 4-100

2. Click the **Save** button, and save the file as the appointed file (shown in Figure 4-101).

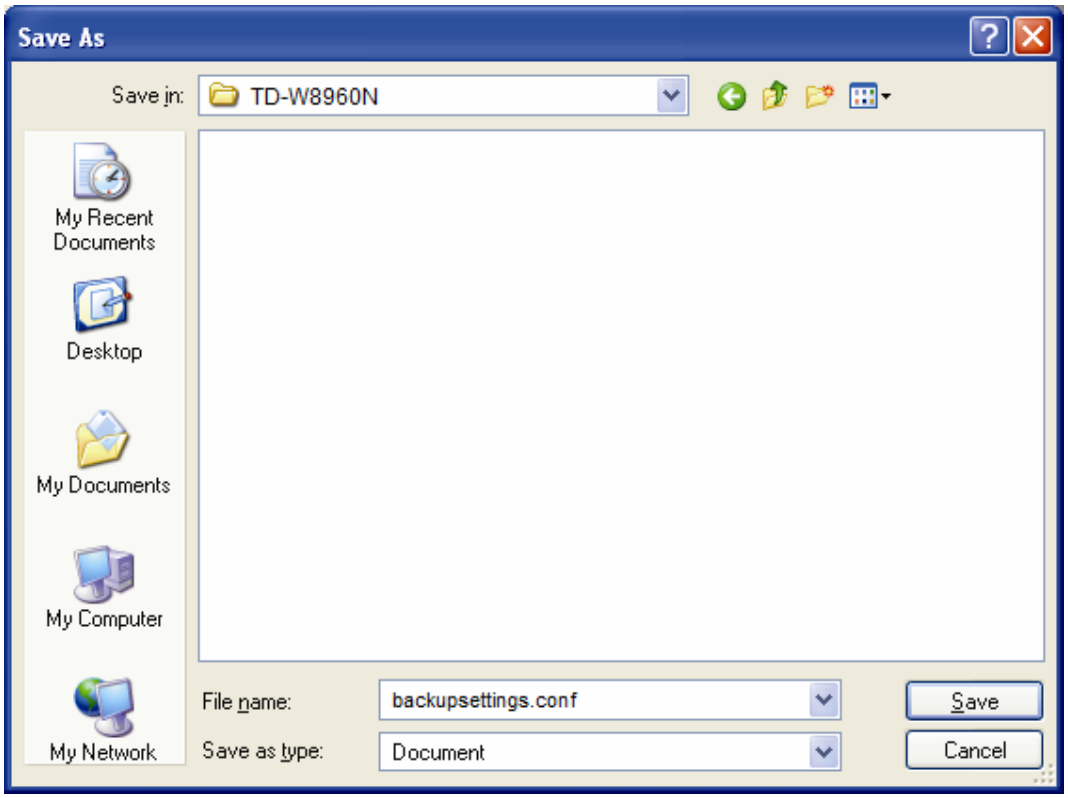


Figure 4-101

4.7.1.2 Import

Choose "**Management**"→"**Settings**"→"**Import**", you can see the **Import** screen, this screen (shown in Figure 4-102) allows you to update the Router's settings.

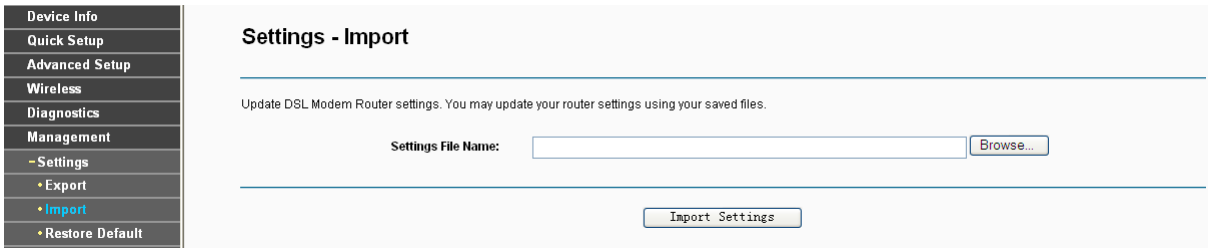


Figure 4-102

To update the 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 Router will reboot upon completion. This process will take a while, don't turn off the Router or press the **Reset** button while processing.

4.7.1.3 Restore Default

Choose "**Management**"→"**Settings**"→"**Restore Default**", you can see the **Restore Default** screen, this screen (shown in Figure 4-103) allows you to restore the Router's configuration to the factory defaults on the screen.

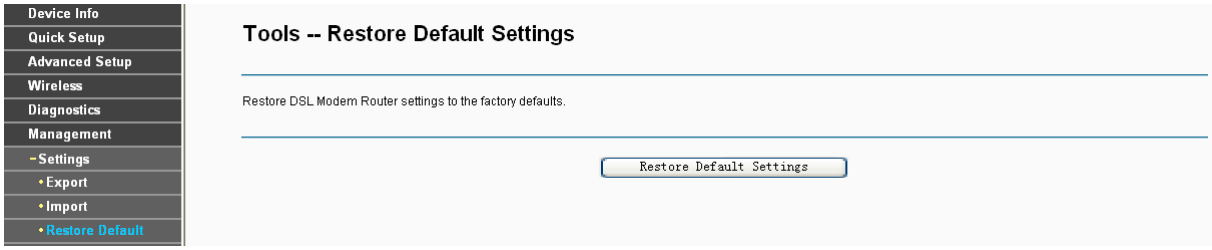


Figure 4-103

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

4.7.2 System Log

Choose "**Management**"→"**System Log**", you can see the **System Log** screen, this screen (shown in Figure 4-104) allows you to view the system log and configure the system log options.

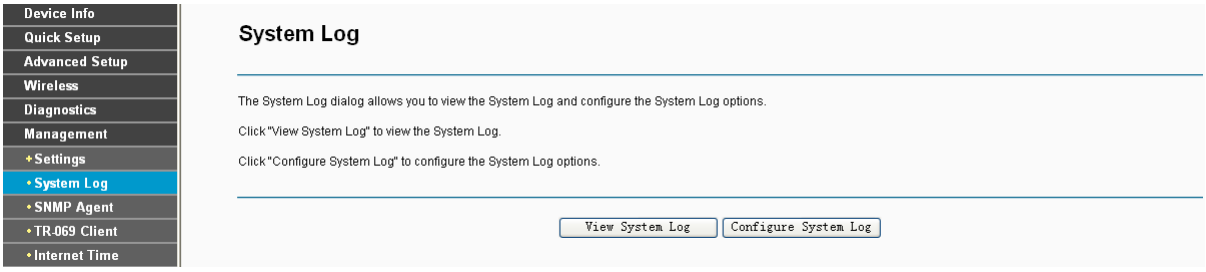


Figure 4-104

To View the System Log:

Click the **View System Log** button, you will see the screen (shown in Figure 4-105) which displays the Router's recent logs.

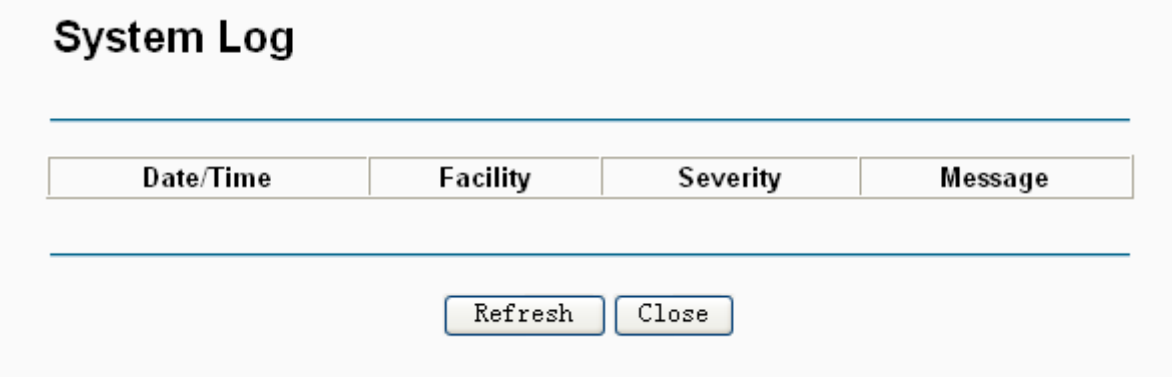


Figure 4-105

- **Refresh:** Click the button, the information in the table will be updated.
- **Close:** Click the button, the screen will be closed.

To Configure the System Log Settings:

Click the **Configure System Log** button (shown in Figure 4-104), you will see the screen below (shown in Figure 4-106).

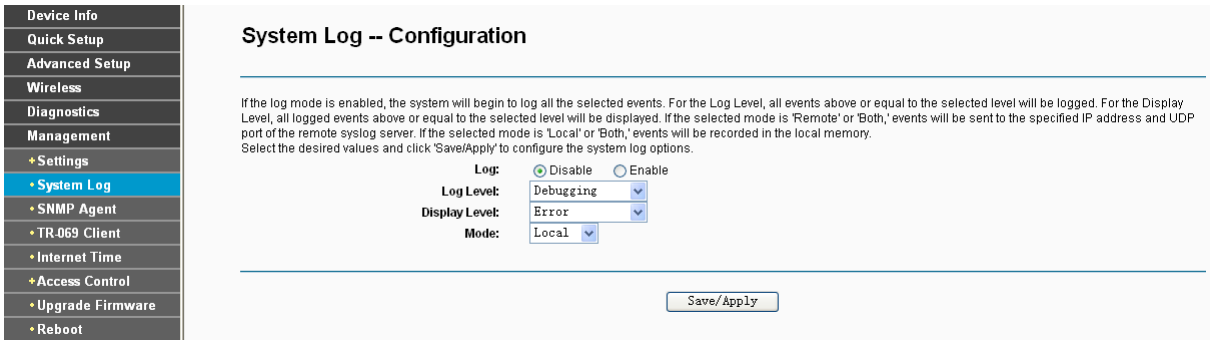


Figure 4-106

- **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.
- **Server IP Address:** Type the address of the server you want to record the events.
- **Server UDP Port:** Type the UDP Port of the server.

4.7.3 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.

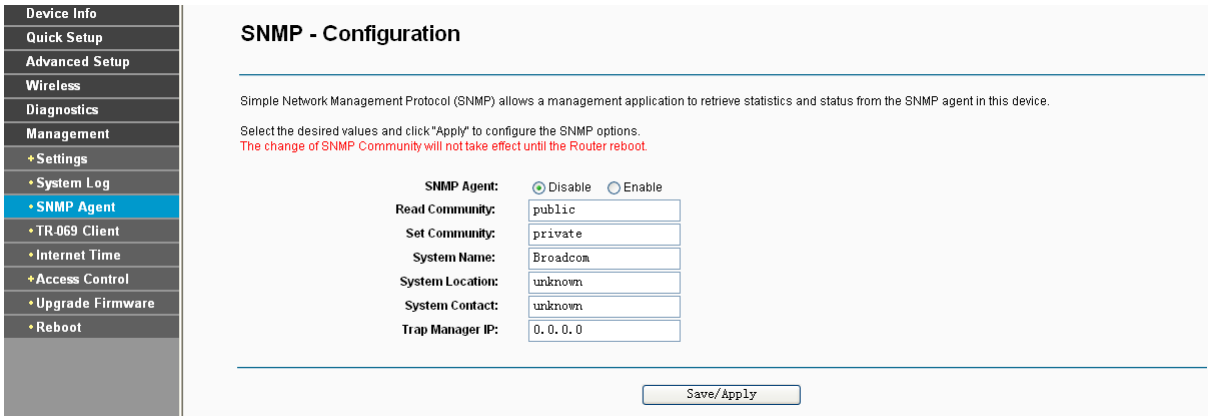


Figure 4-107

- **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 “public”.
- **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.

4.7.4 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.

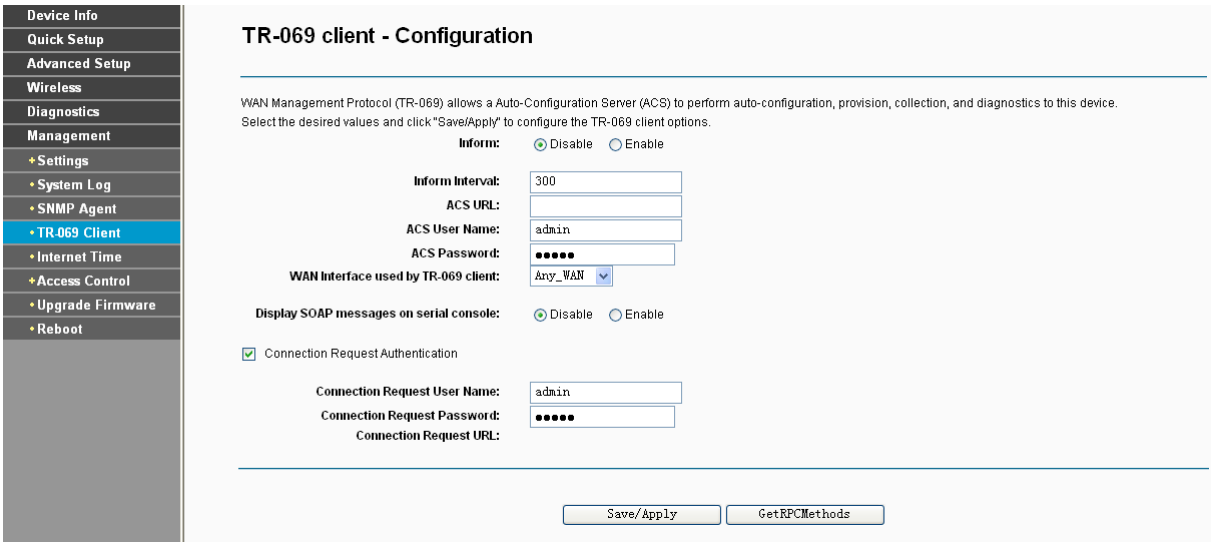


Figure 4-107

- **Inform:** You can select the checkbox to disable or enable the **Inform Interval.**
- **Inform Interval:** Type the interval time of your 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 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.

4.7.5 Internet Time

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

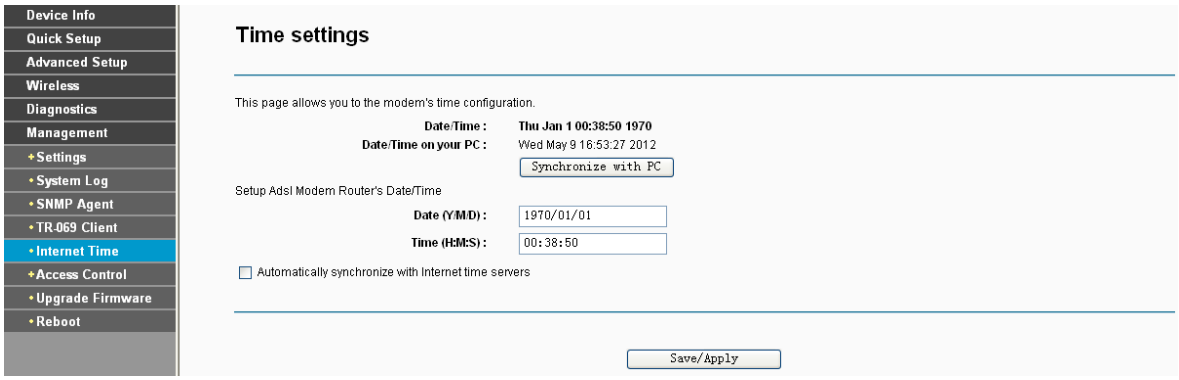


Figure 4-108

4.7.6 Access Control

Choose "**Management**"→"**Access Control**"→"**Password**", you can see the screen (shown in Figure 4-109) which allows you to change the factory default password of the Router. The default password is the same as the user name, which is admin/admin, support/support, and user/user respectively.

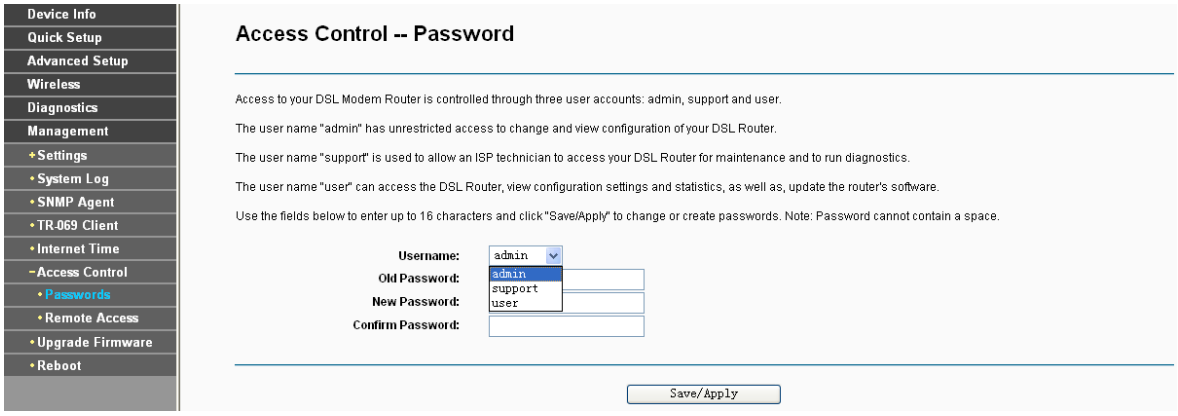


Figure 4-109

To change the password:

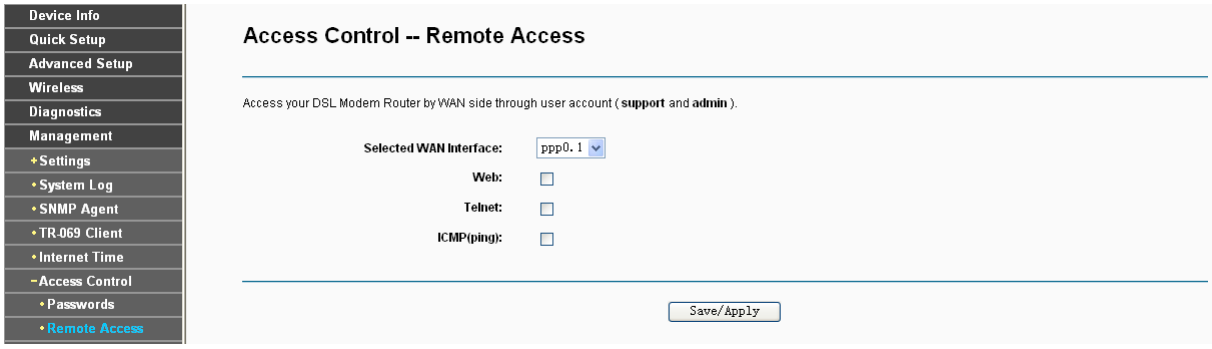
1. Select the **Username** whose password you want to change.
2. Enter the **Old Password** in the text box.
3. Enter the **New Password** and **Confirm Password**. The Confirm Password should be the same as the New Password.
4. Click **Save/Apply** to make your change take effect.

☞ **Note:**

1) Access to your DSL Modem Router is controlled through three user accounts: admin, support, and user. The user name "admin" has unrestricted access to change and view configuration of your DSL Modem Router. The user name "support" is used to allow an ISP technician to access your DSL Modem Router for maintenance and to run diagnostics. The user name "user" can access the DSL Modem Router, view configuration settings and statistics, as well as, update the Router's software.

2) Both of admin and support accounts can do remote management. For security reasons, please change the default password for these two accounts when remote access function is enabled.

3) The password cannot contain a space, and its maximum length is 16 characters.



4.7.7 Update Firmware

Choose "**Management**"→"**Update Firmware**", you can see the screen (shown in Figure 4-110) which allows you to upgrade the latest version software to keep the Router up to date.

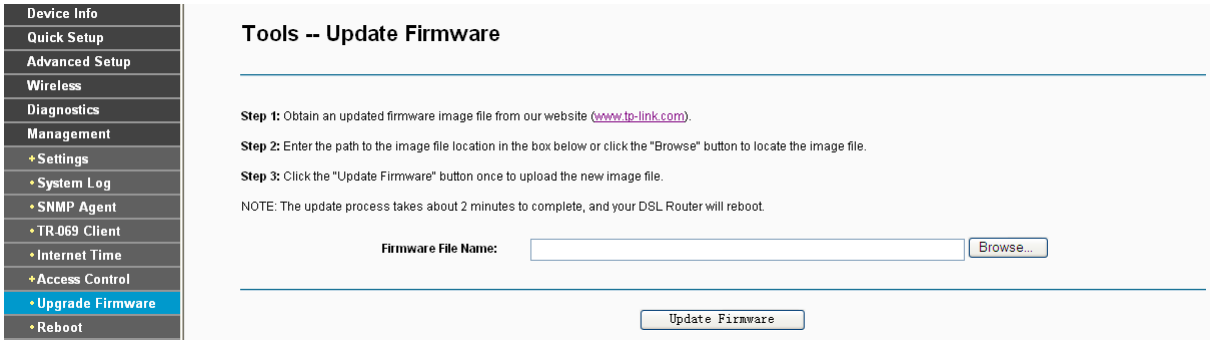


Figure 4-110

- **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 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 Router itself, you can try to upgrade the firmware.

2) Before upgrading the Router's firmware, you should write down some of your customized settings to avoid losing important configuration settings of the Router.

3) Do not turn off the Router or press the **RESET** button while the software is being updated.

4) The Router will reboot after the Upgrading is finished.

4.7.8 Reboot

Choose "**Management**"→"**Reboot**", you can see the screen (shown in Figure 4-111) which allows you to reboot the Router.

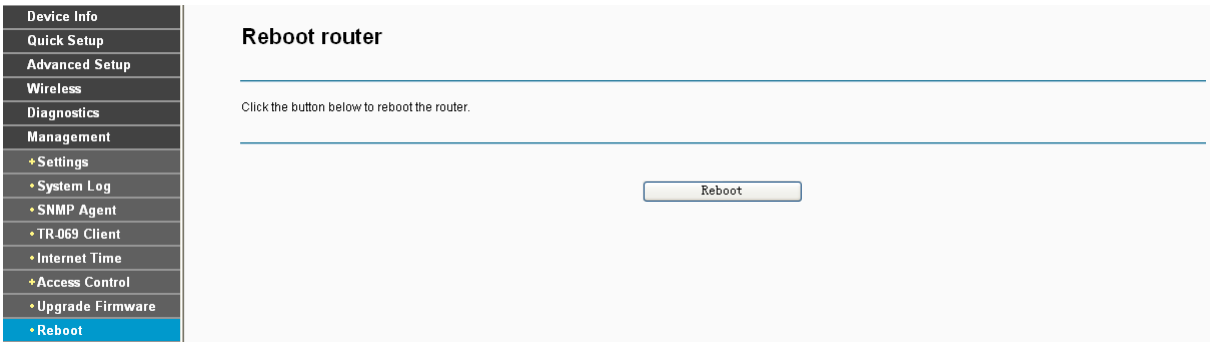


Figure 4-111

Note:

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

Appendix A: FAQ

1. How do I configure the Router to access Internet by ADSL users?

1) First, configure the ADSL Modem configured in RFC1483 bridge model.

2) Connect the Ethernet cable from your ADSL Modem to the WAN port on the Router. The telephone cord plugs into the Line port of the ADSL Modem.

3) Log in to the Router, and configure the WAN connection type as PPPoE connection mode. The detailed steps please refer to section 4.4.2.1 ATM-EoA-PPPoE.

4) If your ADSL lease is in “pay-according-time” mode, select “Dial on Demand” for Internet connection mode on the screen of Figure 4-10.

☞ **Note:**

If you are a Cable user, please configure the Router following the above steps.

2. How do I configure the Router to access Internet by Ethernet users?

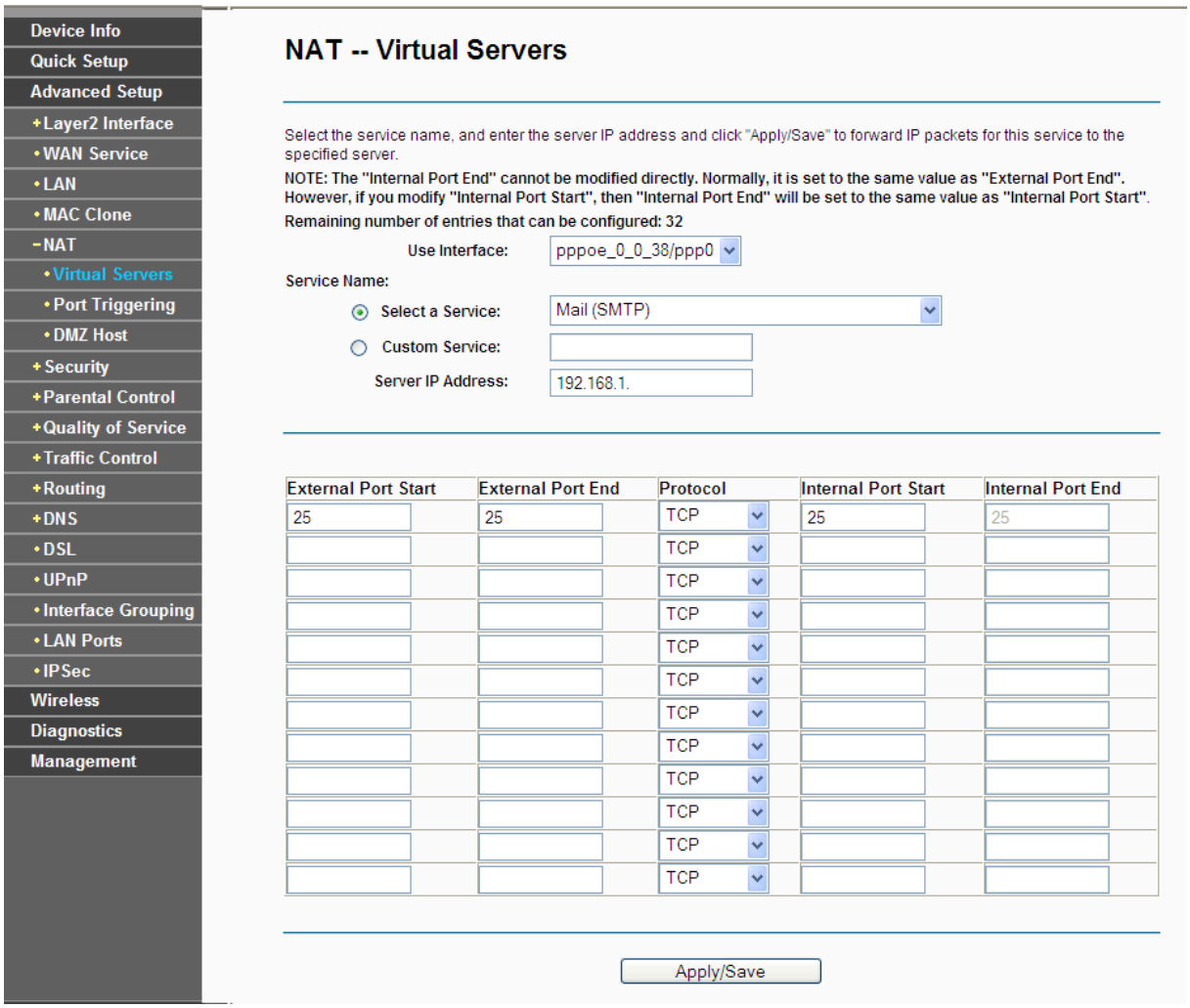
Log in to the Router, and configure the WAN connection type as IPoE connection mode. The detailed steps please refer to section 4.4.2.2 ATM-EoA-IPoE.

3. I want to use NetMeeting, what do I need to do?

1) If you start NetMeeting as a sponsor, you don’t need to do anything with the Router.

2) If you start as a response, you need to configure Virtual Server or DMZ Host.

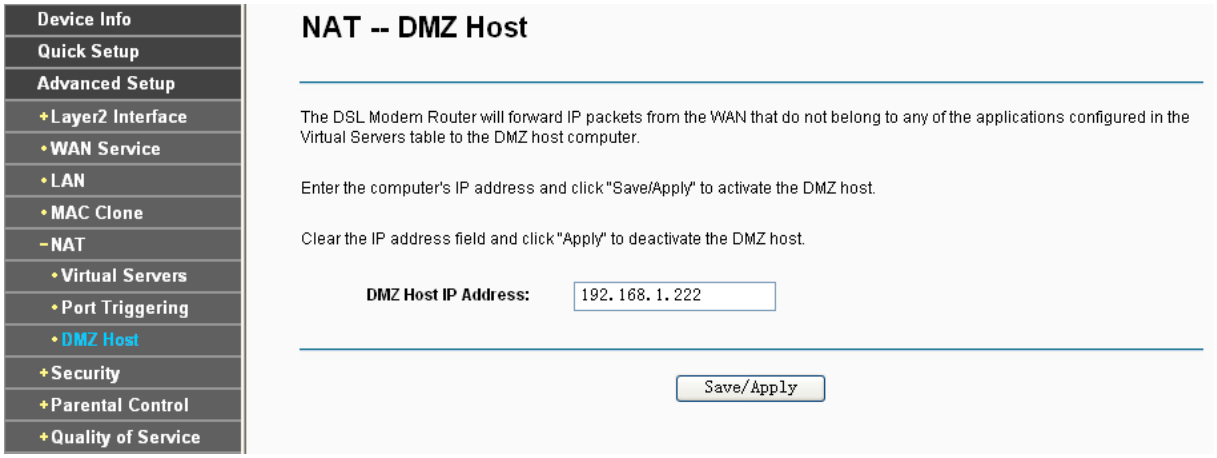
3) How to configure Virtual Server: Log in to the Router, click the “**Advanced Setup-NAT**” menu on the left of your browser, and click "**Virtual Servers**" submenu. On the "**Virtual Servers**" page, click **Add**， and enter “1720” for the service port, using 192.168.1.222 for Server IP Address, remember to click the **Save/Apply** button.



Note:

Your opposite side should call your WAN IP, which is displayed on the “Status” page.

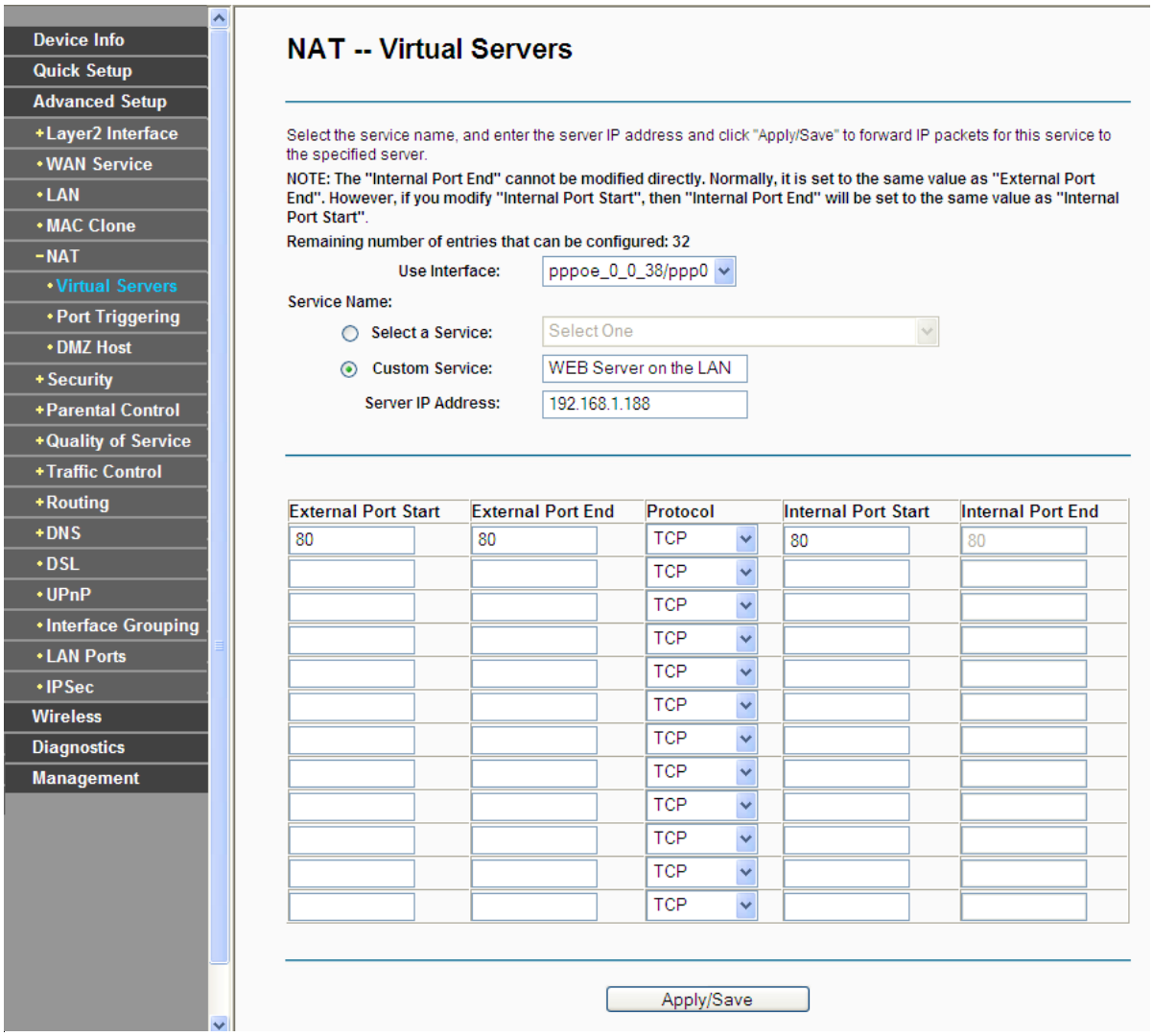
4) How to enable DMZ Host: Log in to the Router, click the “**Advanced Setup-NAT**” menu on the left of your browser, and click "**DMZ Host**" submenu. On the "DMZ" page, type your IP address into the “DMZ Host IP Address” field, using 192.168.1.222 as an example, remember to click the **Save/Apply** button.



4. I want to build a WEB Server on the LAN, what should I do?

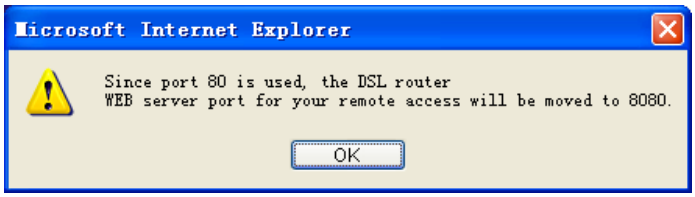
Log in to the Router, click the “**Advanced Setup-NAT**” menu on the left of your browser, and click

the "**Virtual Servers**" submenu. On the "**Virtual Servers**" page, click **Add New**, then on the "**Add or Modify a Virtual Server**" page, enter use "80" as service port, and your IP address next to the "**Server IP Address**", assuming 192.168.1.188 for an example, and remember to click the **Save/Apply** button.



☞ **Note:**

Because the WEB Server port 80 will interfere with the WEB management port 80 on the Router, you will be prompt to change the WEB management port number to avoid interference.



5. The wireless stations cannot connect to the Router.

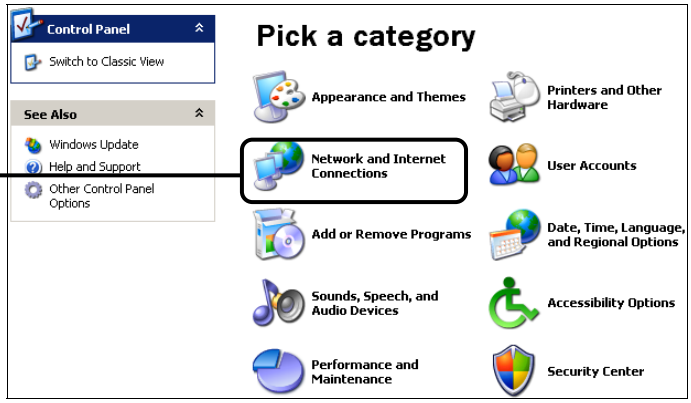
1) Make sure the "**Enable Wireless Router Radio**" is checked.
2) Make sure that the wireless stations' SSID accord with the Router's SSID.
3) Make sure the wireless stations have right KEY for encryption when the Router is encrypted.
4) If the wireless connection is ready, but you can't access the Router, check the IP Address of your wireless stations.

Appendix B: Configuring the PC

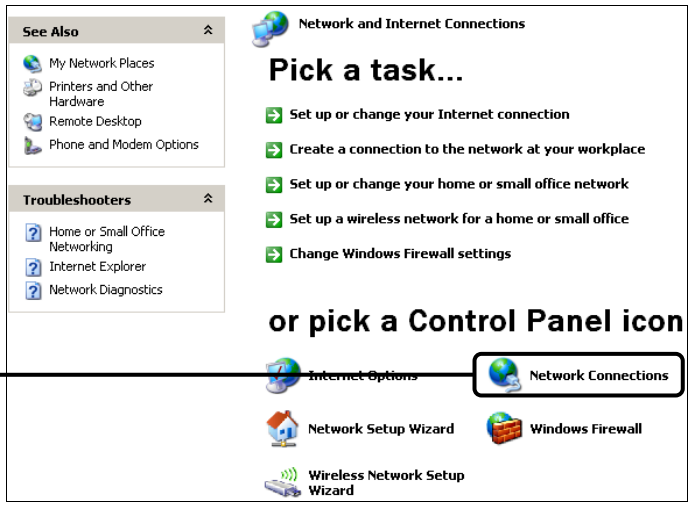
For Windows XP OS

Go to **Start** > **Control Panel**, you will then see the following page.

Click **Network and Internet Connections**

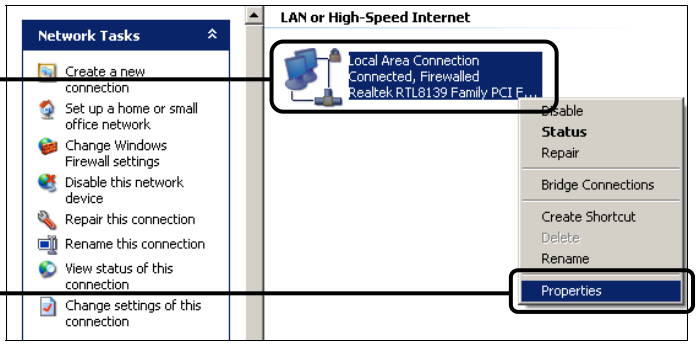


Click **Network Connections**

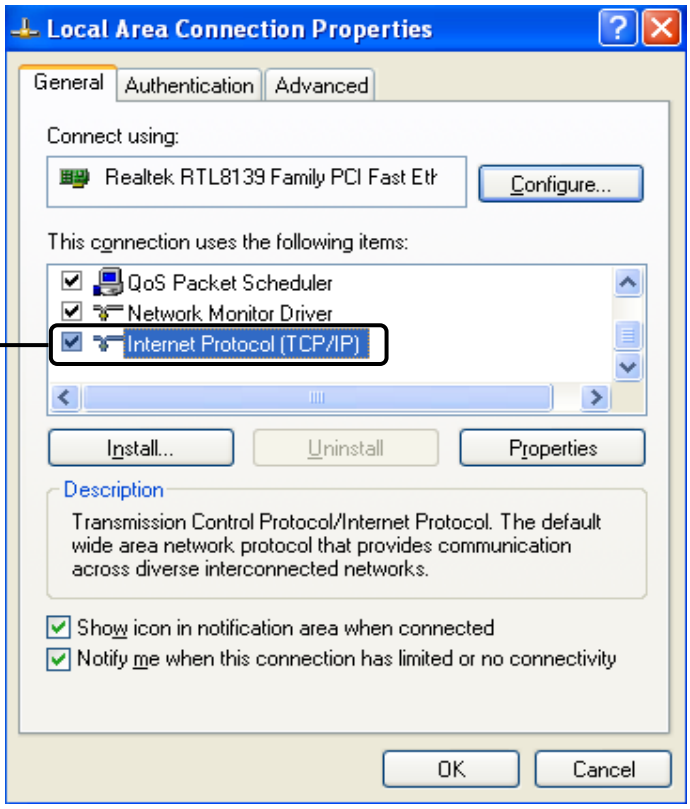


Right-click **Local Area Connection**

Click **Properties**



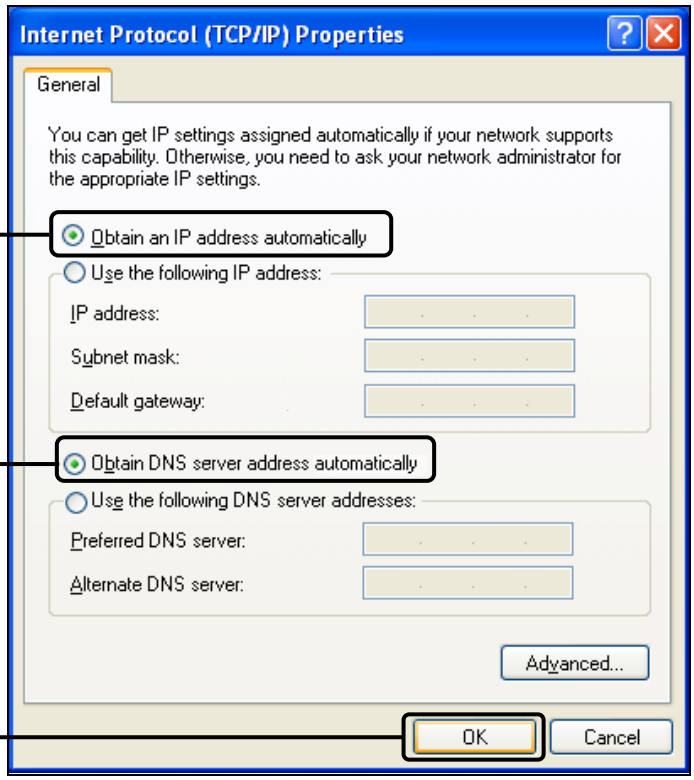
Double-click **Internet Protocol (TCP/IP)**

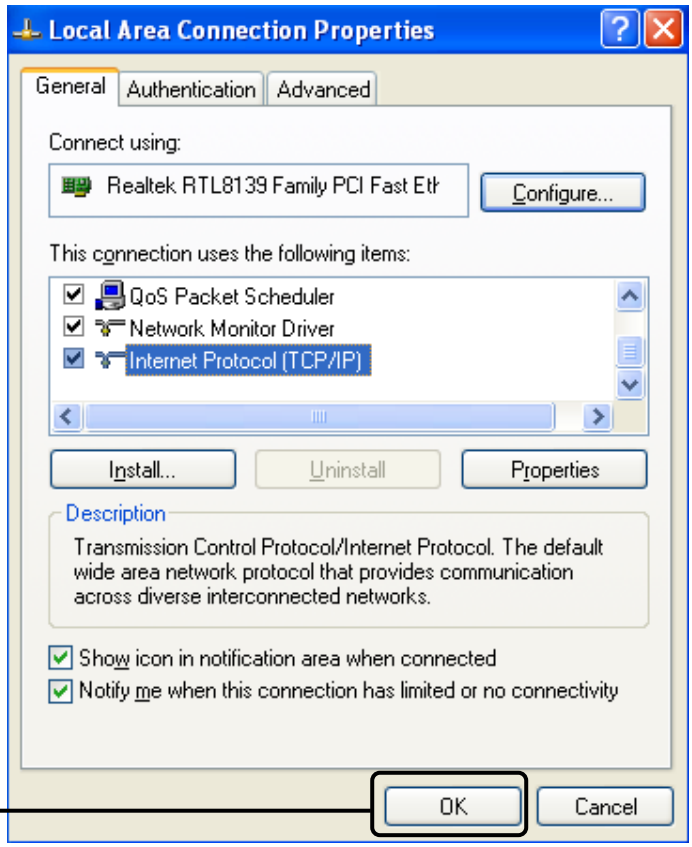


Select **Obtain an IP address automatically**

Select **Obtain DNS server address automatically**

Click **OK**



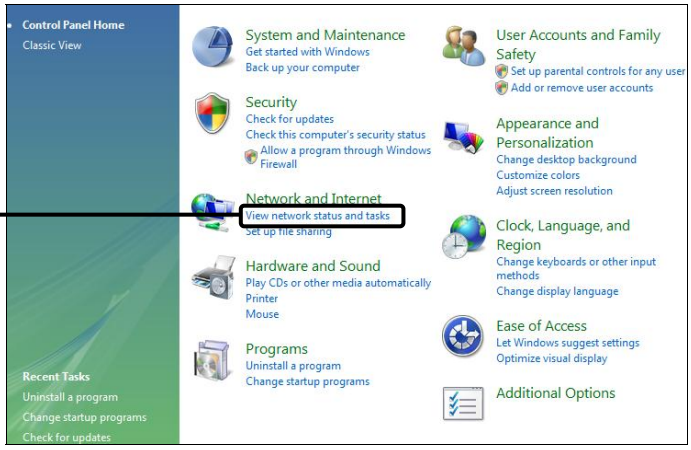

Local Area Connection Properties
General
Authentication
Advanced
Connect using:
Realtek RTL8139 Family PCI Fast Eth
Configure...
This connection uses the following items:
QoS Packet Scheduler
Network Monitor Driver
Internet Protocol (TCP/IP)
Install...
Uninstall
Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
Show icon in notification area when connected
Notify me when this connection has limited or no connectivity
OK
Cancel

Click **OK**

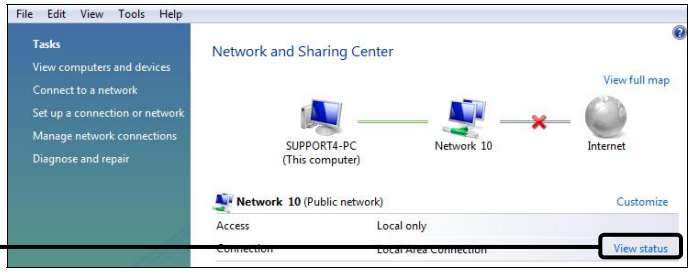
For Windows Vista OS

Go to **Start** > **Settings** >**Control Panel**, and then you will see the following page.

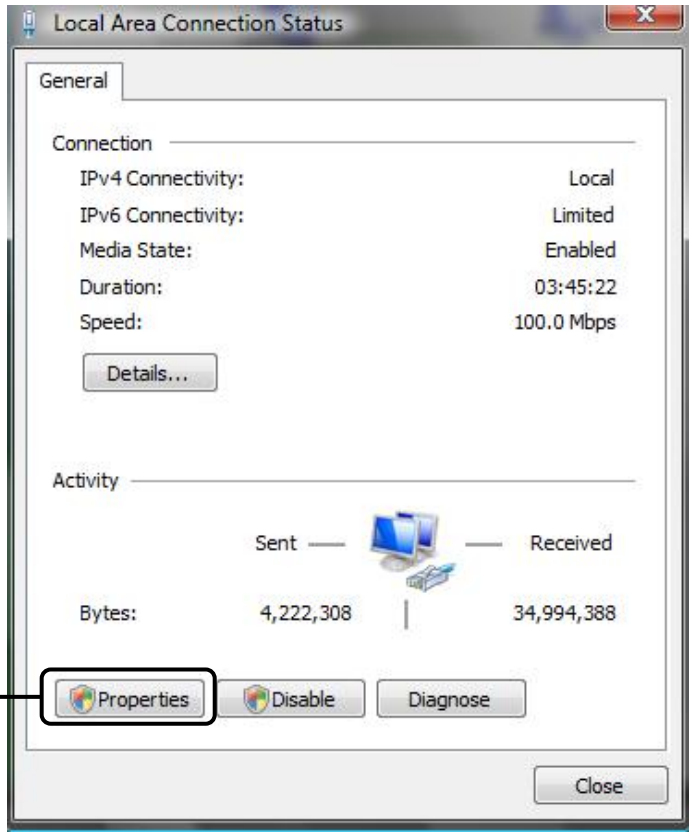
Click **View network status and tasks**



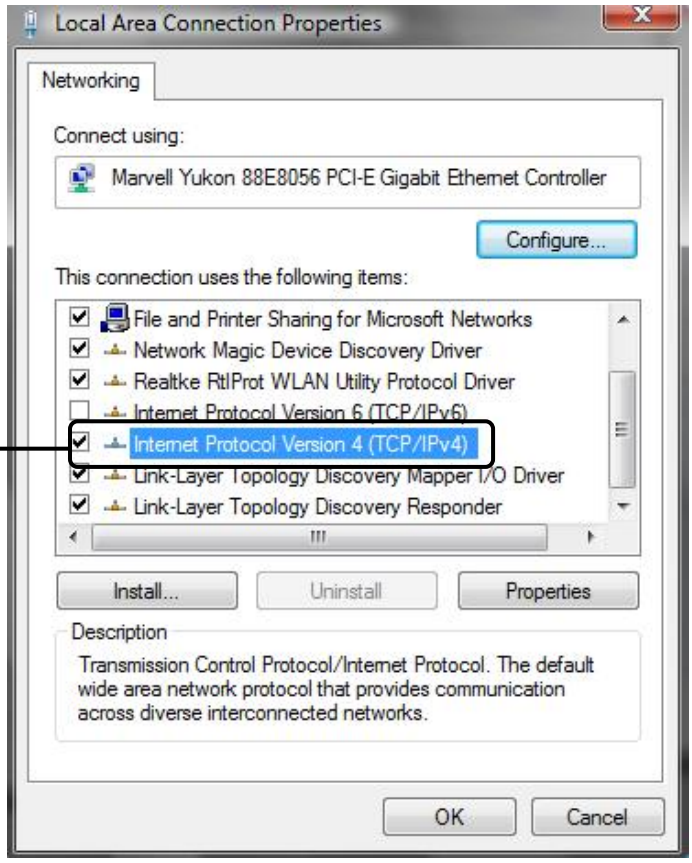
Click **View status**



Click **Properties**



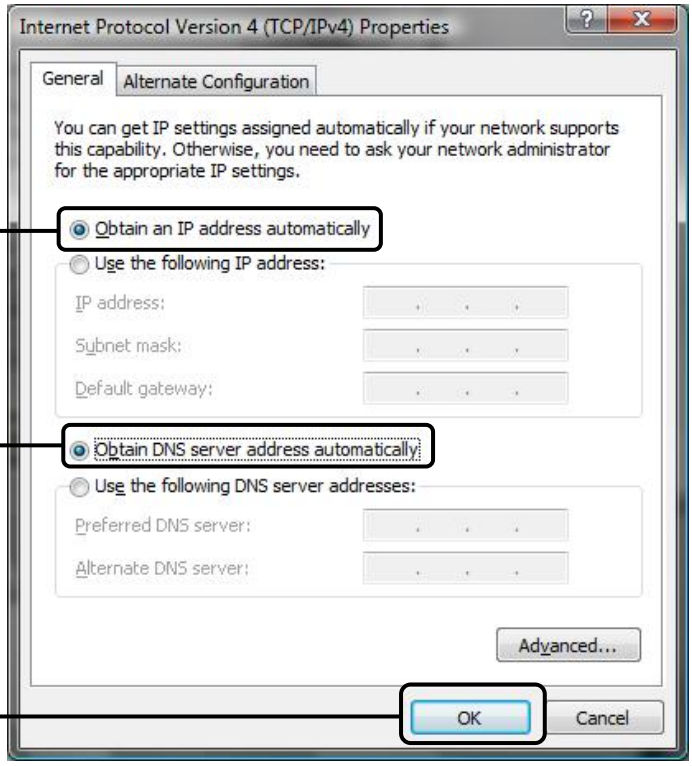
Double-click **Internet Protocol Version 4 (TCP/IPv4)**



Select **Obtain an IP address automatically**

Select **Obtain DNS server address automatically**

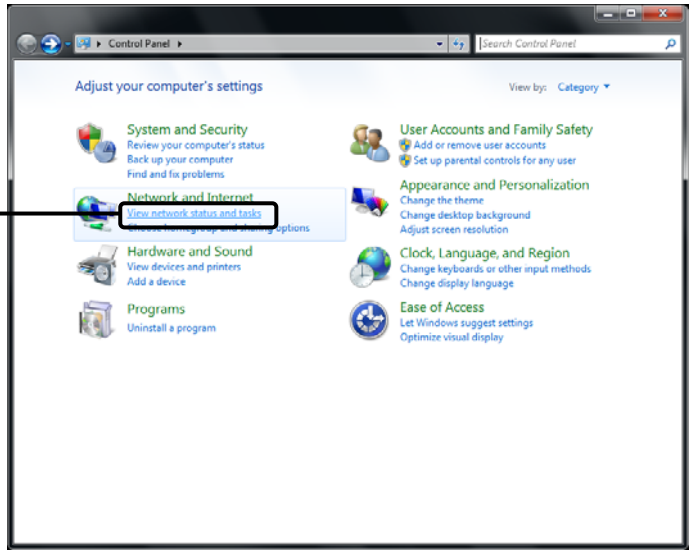
Click **OK**



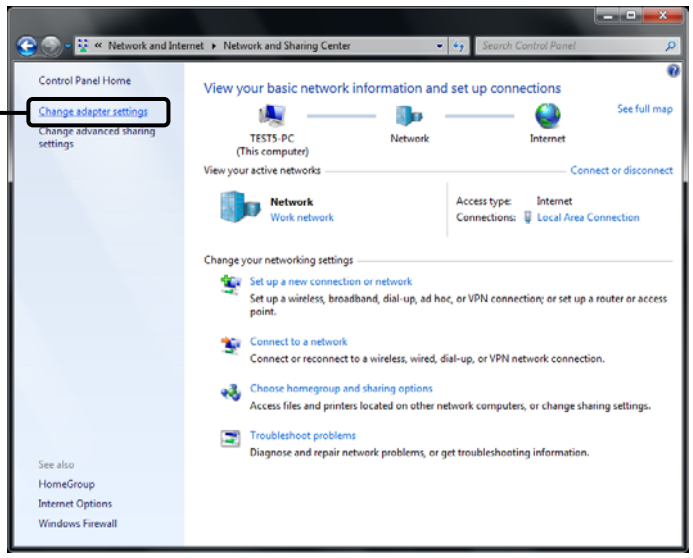
For Windows 7 OS

Go to **Start** > **Settings** > **Control Panel**, and then you will see the following page.

Click **View network status and tasks**

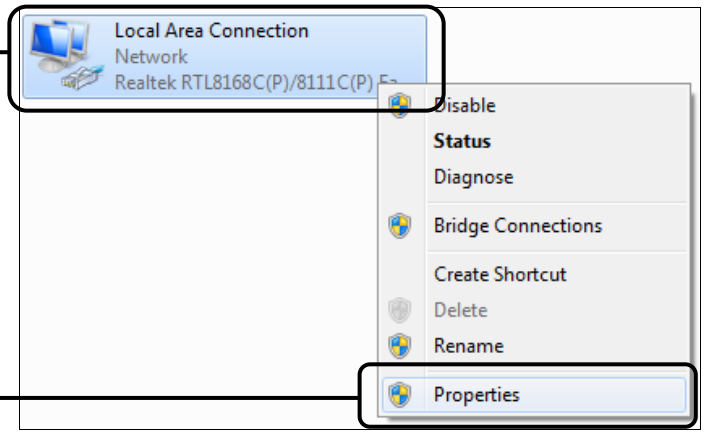


Click **Change adapter settings**

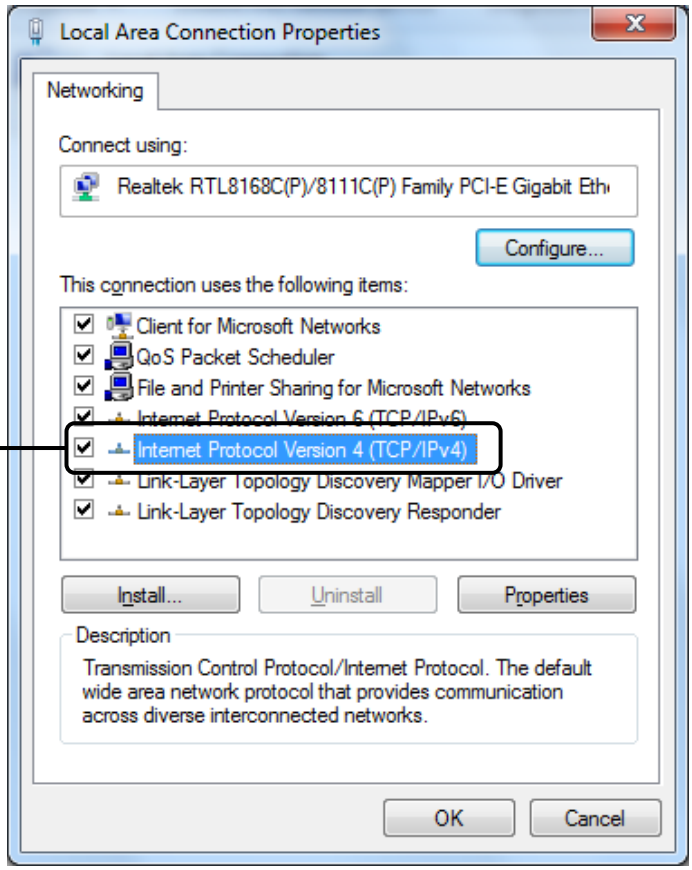


Right-click **Local Area Connection**

Click **Properties**



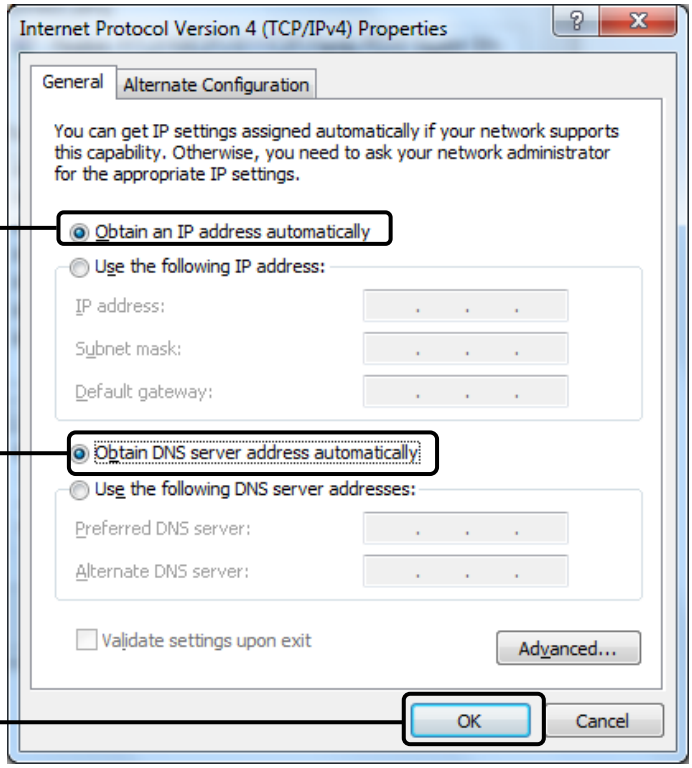
Double-click **Internet Protocol Version 4 (TCP/IPv4)**



Select **Obtain an IP address automatically**

Select **Obtain DNS server address automatically**

Click **OK**



Appendix C: Specifications

General	
Standards	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
Protocols	TCP/IP, IPoA , PPPoA , PPPoE, SNTP, HTTP, DHCP, ICMP, NAT
Ports	LAN Ports: Four 10/100M Auto-Negotiation RJ45 ports（Auto MDI/MDIX)
	Line Port: One RJ11 port
Cabling Type	10BASE-T: UTP category 3, 4, 5 cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m)
	100BASE-TX: UTP category 5, 5e cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m)
LED	1,2,3,4(LAN), WLAN, ADSL
	Power, Internet, WPS
Safety & Emissions	FCC, CE

Wireless	
Frequency Band	2.4~2.4835GHz
Radio Data Rate	11n: up to 300Mbps（Automatic） 11g: 54/48/36/24/18/12/9/6Mbps（Automatic） 11b: 11/5.5/2/1Mbps（Automatic）
Frequency Expansion	DSSS(Direct Sequence Spread Spectrum)
Modulation	DBPSK, DQPSK, CCK, OFDM, 16-QAM, 64-QAM
Security	WEP/WPA/WPA2/WPA2-PSK/WPA-PSK
Sensitivity @PER	270M: -62dBm@10% PER 130M: -64dBm@10% PER 54M: -68dBm@10% PER 11M: -85dBm@8% PER 6M: -88dBm@10% PER 1M: -90dBm@8% PER

Environmental and Physical	
Temperature	Operating: 0℃~40℃ (32℉~104℉)
	Storage: -40℃~70℃(-40℉~158℉)
Humidity	Operating: 10% ~ 90% RH, Non-condensing
	Storage: 5% ~ 90% RH, Non-condensing

Appendix D: Glossary

- **802.11n -** 802.11n builds upon previous 802.11 standards by adding MIMO (multiple-input multiple-output). MIMO uses multiple transmitter and receiver antennas to allow for increased data throughput via spatial multiplexing and increased range by exploiting the spatial diversity, perhaps through coding schemes like Alamouti coding. The Enhanced Wireless Consortium (EWC) [3] was formed to help accelerate the IEEE 802.11n development process and promote a technology specification for interoperability of next-generation wireless local area networking (WLAN) products.
- **802.11b -** The 802.11b standard specifies a wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.4GHz, and WEP encryption for security. 802.11b networks are also referred to as Wi-Fi networks.
- **802.11g -** specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology, using OFDM modulation and operating in the unlicensed radio spectrum at 2.4GHz, and backward compatibility with IEEE 802.11b devices, and WEP encryption for security.
- **2x to 3x eXtended Range™ WLAN Transmission Technology -** The WLAN device with 2x to 3x eXtended Range™ WLAN transmission technology make its sensitivity up to 105 dB, which gives users the ability to have robust, longer-range wireless connections. With this range-enhancing technology, a 2x to 3x eXtended Range™ based client and access point can maintain a connection at as much as three times the transmission distance of traditional 802.11b and 802.11g products, for a coverage area that is up to nine times greater. A traditional 802.11b and 802.11g product transmission distance is about 300m, a 2x to 3x eXtended Range™ based client and access point can maintain a connection transmission distance may be up to 830m.
- **Access Point -** A device that allows wireless-equipped computers and other devices to communicate with a wired network. Also used to expand the range of a wireless network.
- **Ad-hoc Network -** An ad-hoc network is a group of computers, each with a wireless adapter, connected as an independent IEEE 802.11 wireless LAN. Ad-hoc wireless computers operate on a peer-to-peer basis, communicating directly with each other without the use of an access point. Ad-hoc mode is also referred to as an Independent Basic Service Set (IBSS) or as peer-to-peer mode, and is useful at a departmental scale or SOHO operation.
- **AES** (**A**dvanced **E**ncryption **S**tandard) **-** A security method that uses symmetric 128-bit block data encryption.
- **ACS** (**A**uto-**C**onfiguration **S**erver) **-** Through **ACS** (Auto-Configuration Server) you can perform auto-configuration, provision, collection, and diagnostics to the device.
- **ATM** (**A**synchronous **T**ransfer **M**ode) **-** ATM is a cell based transfer mode that requires variable length user information to be segmented and reassembled to/from short, fixed length cells. It uses two different methods for carrying connectionless network interconnect traffic, routed and bridged Protocol Data Units (PDUs), over an ATM network.
- **Bridging -** A device that connects different networks.
- **Browser -** An application program that provides a way to look at and interact with all the information on the World Wide Web.

- **DDNS** (**D**ynamic **D**omain **N**ame **S**ystem) **-** Allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (e.g., www.xyz.com) and a dynamic IP address.
- **Default Gateway -** A device that forwards Internet traffic from your local area network.
- **DHCP -** A networking protocol that allows administrators to assign temporary IP addresses to network computers by “leasing” an IP address to a user for a limited amount of time, instead of assigning permanent IP addresses.
- **DMZ** (**Dem**ilitarized **Z**one) **-** Removes the Router's firewall protection from one PC, allowing it to be “seen” from the Internet.
- **DNS** (**D**omain **N**ame **S**erver) **-** The IP address of your ISP's server, which translates the names of websites into IP addresses.
- **Domain -** A specific name for a network of computers.
- **DSL** (**D**igital **S**ubscriber **L**ine) **-** An always-on broadband connection over traditional phone lines.
- **Dynamic IP Address -** A temporary IP address assigned by a DHCP server.
- **EAP** (**E**xtensible **A**uthentication **P**rotocol) **-** A general authentication protocol used to control network access. Many specific authentication methods work within this framework.
- **Encryption -** Encoding data transmitted in a network.
- **Ethernet -** IEEE standard network protocol that specifies how data is placed on and retrieved from a common transmission medium.
- **Firewall -** A set of related programs located at a network gateway server that protects the resources of a network from users from other networks.
- **Gateway -** A device that interconnects networks with different, incompatible communications protocols.
- **IEEE 802.11b -** The IEEE 802.11b standard specifies a wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.4GHz, and WEP encryption for security. IEEE 802.11b networks are also referred to as Wi-Fi networks.
- **IEEE 802.11g -** Specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology, using OFDM modulation and operating in the unlicensed radio spectrum at 2.4GHz, and backward compatibility with IEEE 8021b devices, and WEP encryption for security.
- **Infrastructure Network -** An infrastructure network is a group of computers or other devices, each with a wireless adapter, connected as an IEEE 802.11 wireless LAN. In infrastructure mode, the wireless devices communicate with each other and to a wired network by first going through an access point. An infrastructure wireless network connected to a wired network is referred to as a Basic Service Set (BSS). A set of two or more BSS in a single network is referred to as an Extended Service Set (ESS). Infrastructure mode is useful at a corporation scale, or when it is necessary to connect the wired and wireless networks.
- **IP Address** - The address used to identify a computer or device on a network.
- **IPoA** (**IP** and **ARP** over **ATM**) **-** A protocol that provides extensions to the IP Group for handling IP over ATM flows.
- **ISP** (**I**nternet **S**ervice **P**rovider) **-** A company that provides access to the Internet.

- **LAN** - The computers and networking products that make up your local network.
- **MAC** (**M**edia **A**ccess **C**ontrol) **Address -** The unique address that a manufacturer assigns to each networking device.
- **NAT** (**N**etwork **A**ddress **T**ranslation) **-** NAT technology translates IP addresses of a local area network to a different IP address for the Internet.
- **MER** (**MAC E**ncapsulation **R**outing) **- MER** allows IP packet to be carried as bridged frames. There are many applications, such as IPoA, DSL networks and other frame-based network. Depending on your equipment, they can be either bridged or routed within the network.
- **Network -** A series of computers or devices connected for the purpose of data sharing, storage, and/or transmission between users.
- **Ping** (**P**acket **I**nternet **G**roper) **-** An Internet utility used to determine whether a particular IP address is online.
- **Port -** The connection point on a computer or networking device used for plugging in cables or adapters.
- **PPPoE** (**P**oint to **P**oint **P**rotocol **o**ver **E**thernet) **-** PPPoE stands for Point to Point protocol over Ethernet, this protocol is used as a type of broadband connection that provides authentication (username and password) in addition to data transport.
- **PPPoA** (**P**oint to **P**oint **P**rotocol over **ATM**) **-** PPPoA stands for Point to Point protocol over ATM, this protocol is also used as a type of broadband connection that provides authentication (username and password) in addition to data transport.
- **RADIUS** (**R**emote **A**uthentication **D**ial**-I**n **U**ser **S**ervice) **-** A protocol that uses an authentication server to control network access.
- **RJ45** (**R**egistered **J**ack**-45**) **-** An Ethernet connector that holds up to eight wires.
- **Router -** A networking device that connects multiple networks together.
- **RPC** (**R**emote **P**rocedure **C**alls) **-** RPC is a powerful technique for constructing distributed, client-server based applications. It is based on extending the notion of convention, or local procedure calling, so that the called procedure need not exist in the same address space as the calling procedure. The two processes may be on the same system, or they may be on different systems with a network connecting them. By using RPC, programmers of distributed applications avoid the details of the interface with the network. The transport independence of RPC isolates the application from the physical and logical elements of the data communications mechanism and allows the application to use a variety of transports.
- **Server -** Any computer whose function in a network is to provide user access to files, printing, communications, and other services.
- **SOHO** (**Small Office/Home Office**) **-** Market segment of professionals who work at home or in small offices.
- **SSID -** A Service Set Identification is a thirty-two character (maximum) alphanumeric key identifying a wireless local area network. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID. This is typically the configuration parameter for a wireless PC card. It corresponds to the ESSID in the wireless Access Point and to the wireless network name.
- **Static IP Address -** A fixed address assigned to a computer or device that is connected to a network.

- **Static Routing -** Forwarding data in a network via a fixed path.
- **Subnet Mask -** An address code that determines the size of the network.
- **TCP** (**T**ransmission **C**ontrol **P**rotocol) **-** A network protocol for transmitting data that requires acknowledgement from the recipient of data sent.
- **TCP/IP** (**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol) **-** A set of instructions PCs use to communicate over a network.
- **TKIP** (**T**emporal **K**ey **I**ntegrity **P**rotocol) **-** a wireless encryption protocol that provides dynamic encryption keys for each packet transmitted.
- **UDP** (**U**ser **D**atagram **P**rotocol) **-** A network protocol for transmitting data that does not require acknowledgement from the recipient of the data that is sent.
- **VCI** (**V**irtual **C**hannel **I**dentifier) - The identifier of the VC contained in the ATM cell header.
- **VPI** (**V**irtual **P**ath **I**dentifier) - The identifier of the VP contained in the ATM cell header.
- **Update -** To replace existing software or firmware with a newer version.
- **VLAN** (**V**irtual **L**ocal **A**ir **N**etwork) **-** Logical subgroups that constitute a Local Area Network (LAN). This is done in software rather than defining a hardware solution.
- **VLAN ID (0-4095) -** Indicates the ID number of the VLAN being configured. Up to 256 VLANs can be created.
- **WAN** (**W**ide **A**rea **N**etwork) **-** Networks that cover a large geographical area.
- **Web-based Utility** - The web page that allows you to manage the Router.
- **WEP** (**W**ired **E**quivalent **P**rivacy) **-** A data privacy mechanism based on a 64-bit or 128-bit or 152- bit shared key algorithm, as described in the IEEE 802.11g standard.
- **Wi-Fi -** A trade name for the IEEE 802.11b wireless networking standard, given by the Wireless Ethernet Compatibility Alliance (WECA, see http://www.wi-fi.net), an industry standards group promoting interoperability among IEEE 802.11b devices.
- **WLAN** (**W**ireless **L**ocal **A**rea **N**etwork) **-** A group of computers and associated devices communicate with each other wirelessly, which network serving users are limited in a local area.
- **WPA** (**Wi-Fi P**rotected **A**ccess) **-** A wireless security protocol use TKIP (Temporal Key Integrity Protocol) encryption, which can be used in conjunction with a RADIUS server.

Appendix E: Technical Support

Technical Support

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

Global
Tel: +86 755 26504400
E-mail: support@tp-link.com
Service time: 24hrs, 7 days a week

Singapore
Tel: +65 62840493
E-mail: support.sg@tp-link.com
Service time: 24hrs, 7 days a week

UK
Tel: +44 (0) 845 147 0017
E-mail: support.uk@tp-link.com
Service time: 24hrs, 7 days a week

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

Malaysia
Tel: 1300 88 875465 (1300 88TPLINK)
Email: support.my@tp-link.com
Service time: 24hrs, 7 days a week

Turkey
Tel: 444 19 25 (Turkish Service）
E-mail: support.tr@tp-link.com
Service time: 9:00 AM to 6:00 PM
7 days a week

Poland
Tel: +48 (0) 801 080 618 / +48 22 7217563 (if calls from mobile phone)
E-mail: support.pl@tp-link.com
Service time: Monday to Friday 9:00 AM to 5:00 PM. GMT+1 or GMT+2 (Daylight Saving Time)

Germany / Austria
Tel: +49 1805 875465 (German Service)
+49 1805 TPLINK
E-mail: support.de@tp-link.com
Fee: 0.14 EUR/min from the German fixed phone network and up to 0.42 EUR/min from mobile phone
Service time: Monday to Friday 9:00 AM to 6:00 PM. GMT+ 1 or GMT+ 2 (Daylight Saving Time in Germany)
*Except bank holidays in Hesse

Australia & New Zealand
Tel: AU 1300 87 5465
NZ 0800 87 5465
E-mail: support@tp-link.com.au
Service time: 24hrs, 7 days a week

Italy
Tel: +39 02 66987799
E-mail: support.it@tp-link.com
Service time: Monday to Friday
9:00 AM to 6:00 PM

Ukraine
Tel: +380 (44) 590-51-14
E-mail: support.ua@tp-link.com
Service time: Monday to Friday
14:00 PM to 22:00 PM

Brazil
Toll Free: 0800-770-4337 (Portuguese Service)
E-mail: suporte.br@tp-link.com
Service time: Monday to Saturday
08:00 AM to 08:00 PM

Indonesia
Tel: (+62) 021 6259 135
E-mail : support.id@tp-link.com
Service time : Monday to Friday
9:00 -12:00; 13:00 -18:00
*Except public holidays

Switzerland
Tel: +41 (0) 848 800998 (German Service)
E-mail: support.ch@tp-link.com
Fee: 4-8 Rp/min, depending on rate of different time
Service time: Monday to Friday 9:00 AM to 6:00 PM. GMT+ 1 or GMT+ 2
(Daylight Saving Time)

Russian Federation
Tel: 8 (495) 223-55-60
8 (800) 250-55-60 (toll-free call from any RF region)
E-mail: support.ru@tp-link.com
Service time: From 10:00 to 18:00
(Moscow time)
*Except weekends and holidays in Russian Federation