



User Guide

TL-WR843N

300Mbps Wireless AP/Client Router



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 © 2015 TP-LINK TECHNOLOGIES CO., LTD. All rights reserved.

<http://www.tp-link.com>

FCC STATEMENT



This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

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

- 1) This device may not cause harmful interference.
- 2) This device must accept any interference received, including interference that may cause undesired operation.

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

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

FCC RF Radiation Exposure Statement

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

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

CE Mark Warning

CE 1588

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.

Canadian Compliance Statement

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

- (1) This device may not cause interference, and
- (2) This device must accept any interference, including interference that may cause undesired operation of the device.

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

- (1) cet appareil ne doit pas provoquer d'interférences et
- (2) cet appareil doit accepter toute interférence, y compris celles susceptibles de provoquer un fonctionnement non souhaité de l'appareil.

This device has been designed to operate with the antennas listed below, and having a maximum gain of 4 dBi. Antennas not included in this list or having a gain greater than 4 dBi are strictly prohibited for use with this device. The required antenna impedance is 50 ohms.

Industry Canada Statement

Complies with the Canadian ICES-003 Class B specifications.

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

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

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

brouilleur du Canada.

Korea Warning Statements

당해 무선설비는 운용중 전파혼신 가능성이 있음.

NCC Notice & BSMI Notice

注意！

依據 低功率電波輻射性電機管理辦法

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

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

減少電磁波影響，請妥適使用。

安全諮詢及注意事項

- 請使用原裝電源供應器或只能按照本產品注明的電源類型使用本產品。
- 清潔本產品之前請先拔掉電源線。請勿使用液體、噴霧清潔劑或濕布進行清潔。
- 注意防潮，請勿將水或其他液體潑灑到本產品上。
- 插槽與開口供通風使用，以確保本產品的操作可靠並防止過熱，請勿堵塞或覆蓋開口。
- 請勿將本產品置放於靠近熱源的地方。除非有正常的通風，否則不可放在密閉位置中。
- 請不要私自打開機殼，不要嘗試自行維修本產品，請由授權的專業人士進行此項工作。



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



Safety Information

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

This product can be used in the following countries:

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

DECLARATION OF CONFORMITY

For the following equipment:

Product Description: **300Mbps Wireless AP/Client Router**

Model No.: **TL-WR843N**

Trademark: **TP-LINK**

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

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

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

EN 300 328 V1.8.1:2012-06

EN 301 489-1 V1.9.2:2011 & EN 301 489-17 V2.2.1:2012

EN 55022:2010+AC:2011

EN 55024:2010

EN 61000-3-2:2014

EN 61000-3-3:2013

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

EN 50385:2002

The product carries the CE Mark:

CE 1588

Person is responsible for marking this declaration:



Yang Hongliang

Product Manager of International Business

Date of issue: 2015

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. Introduction.....	2
1.1 Overview of the Router	2
1.2 Conventions	3
1.3 Main Features	3
1.4 Panel Layout	4
1.4.1 The Front Panel	4
1.4.2 The Rear Panel.....	5
Chapter 2. Connecting the Router	6
2.1 System Requirements	6
2.2 Installation Environment Requirements.....	6
2.3 Connecting the Router.....	6
Chapter 3. Quick Installation Guide.....	9
3.1 TCP/IP Configuration	9
3.2 Quick Installation Guide.....	11
3.2.1 Configuration for Router Mode	13
3.2.2 Configuration for Client Router Mode	17
Chapter 4. Configuring the Router	23
4.1 Login	23
4.2 Status.....	23
4.3 Quick Setup	24
4.4 WPS.....	24
4.5 Working Mode.....	27
4.6 Network.....	27
4.6.1 WAN	28
4.6.2 MAC Clone.....	37
4.6.3 LAN	38
4.7 Wireless	39
4.7.1 Wireless Settings	39
4.7.2 Wireless Security	45
4.7.3 Wireless MAC Filtering	48
4.7.4 Wireless Advanced	50

4.7.5	Wireless Statistics.....	52
4.8	DHCP.....	54
4.8.1	DHCP Settings.....	54
4.8.2	DHCP Client List.....	55
4.8.3	Address Reservation	55
4.9	Forwarding.....	57
4.9.1	Virtual Servers	57
4.9.2	Port Triggering	59
4.9.3	DMZ	60
4.9.4	UPnP.....	61
4.10	Security	62
4.10.1	Basic Security	62
4.10.2	Advanced Security.....	63
4.10.3	Local Management	65
4.10.4	Remote Management	66
4.11	Parental Control.....	67
4.12	Access Control.....	69
4.12.1	Rule.....	69
4.12.2	Host.....	75
4.12.3	Target	76
4.12.4	Schedule	79
4.13	Advanced Routing	80
4.13.1	Static Routing.....	81
4.13.2	System Routing Table.....	82
4.14	Bandwidth Control	82
4.14.1	Control Settings	83
4.14.2	Rules List	83
4.15	IP & MAC Binding	84
4.15.1	Binding Settings.....	84
4.15.2	ARP List	86
4.16	Dynamic DNS	87
4.16.1	Comexe.cn DDNS.....	87
4.16.2	Dyndns.org DDNS	88
4.16.3	No-ip.com DDNS	89
4.17	System Tools.....	99

4.17.1 Time Settings	99
4.17.2 Diagnostic	101
4.17.3 Firmware Upgrade	102
4.17.4 Factory Defaults.....	103
4.17.5 Backup & Restore	104
4.17.6 Reboot.....	104
4.17.7 Password	105
4.17.8 System Log	105
4.17.9 Statistics.....	107
Appendix A: FAQ	110
Appendix B: Configuring the PC.....	115
Appendix C: Specifications	119
Appendix D: Glossary	120

Package Contents

The following items should be found in your package:

- TL-WR843N 300Mbps Wireless AP/Client Router
- Power Adapter for TL-WR843N 300Mbps Wireless AP/Client Router
- Passive PoE Injector
- Ethernet cable
- Quick Installation Guide
- Resource CD for TL-WR843N 300Mbps Wireless AP/Client Router, including:
 - This 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. Introduction

1.1 Overview of the Router

The TL-WR843N 300Mbps Wireless AP/Client Router integrates 4-port Switch, Firewall, NAT-Router and Wireless AP. Powered by 2x2 MIMO technology, the 300Mbps Wireless AP/Client 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.

Incredible Speed

The TL-WR843N 300Mbps Wireless AP/Client 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 much faster than 802.11g. It is also compatible with all IEEE 802.11g and IEEE 802.11b products.

Multiple Working Modes

The TL-WR843N 300Mbps Wireless AP/Client Router supports two working modes. The WISP Client Router mode allows the TL-WR843N to connect to the WISP and create a local area network via wireless connection. The Standard Wireless Router mode enables the TL-WR843N to work as a router for network sharing with high speed.

Multiple Security Protections

With multiple protection measures, including SSID broadcast control and wireless LAN 64/128/152-bit WEP encryption, WiFi protected Access (WPA2- PSK, WPA- PSK), as well as advanced Firewall protections, the TL-WR843N 300Mbps Wireless AP/Client Router provides complete data privacy.

Flexible Access Control

The TL-WR843N 300Mbps Wireless AP/Client 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 Conventions

The Router or TL-WR843N mentioned in this guide stands for TL-WR843N 300Mbps Wireless AP/Client Router without any explanation.

1.3 Main Features

- Complies with IEEE 802.11n to provide a wireless data rate of up to 300Mbps.
- One 10/100M Auto-Negotiation RJ45 INTERNET port, supporting passive POE at AP Client Router mode.
- Four 10/100M Auto-Negotiation RJ45 LAN ports, supporting Auto MDI/MDIX.
- Provides WPA/WPA2, WPA-PSK/WPA2-PSK authentication, TKIP/AES encryption security.
- Shares data and Internet access for users, supporting Dynamic IP/Static IP/PPPoE Internet access.
- Supports Client Router mode for WISP Connection.
- Supports Virtual Server, Special Application and DMZ host.
- Supports UPnP, Dynamic DNS, Static Routing.
- Provides Automatic-connection and Scheduled Connection on certain time to the Internet
- Built-in NAT and DHCP server supporting static IP address distributing.
- Supports Parental Control and Access Control.
- Connects Internet on demand and disconnects from the Internet when idle for PPPoE.
- Provides 64/128/152-bit WEP encryption security and wireless LAN ACL (Access Control List).
- Supports Flow Statistics.
- Supports firmware upgrade and Web management.

1.4 Panel Layout

1.4.1 The Front Panel

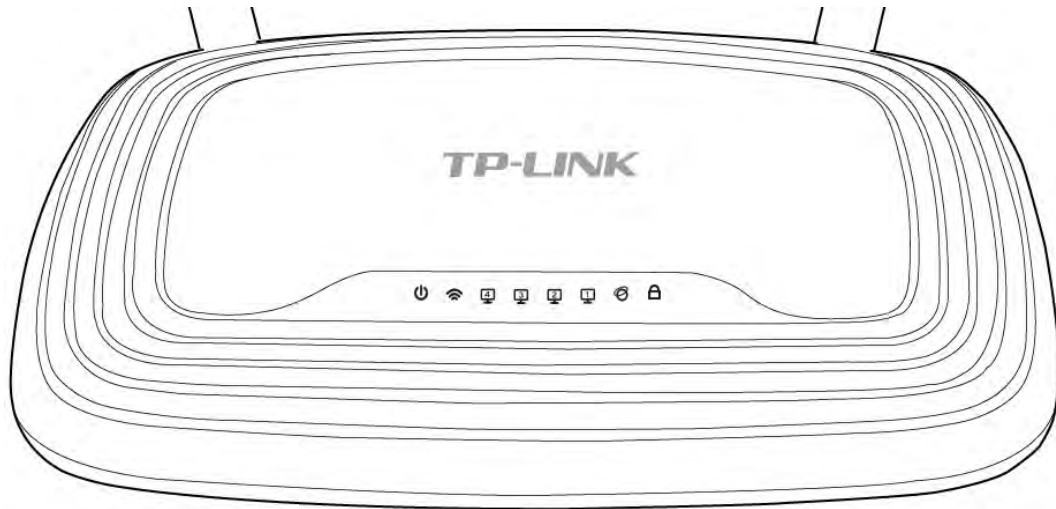


Figure 1-1 Front Panel sketch

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

Name	Status	Indication
⏻ (Power)	Off	Power is off.
	On	Power is on.
📶 (WLAN)	Off	The Wireless function is disabled.
	Flashing	The Wireless function is enabled.
🌐 (LAN 1-4) 🌐 (WAN)	Off	There is no device linked to the corresponding port.
	On	There is a device linked to the corresponding port but there is no activity.
	Flashing	There is an active device linked to the corresponding port.
🌐 (WAN)	Green	Connected to Internet.
	Orange	Off-line.
🔒 (WPS)	Slow Flash	A wireless device is connecting to the network by WPS function. This process will last in the first 2 minutes.
	On	A wireless device has been successfully added to the network by WPS function.
	Quick Flash	A wireless device failed to be added to the network by WPS function.

Table 1-1 The LEDs Description

Note:

After a device is successfully added to the network by WPS function, the WPS LED will keep on for about 5 minutes and then turn off.

1.4.2 The Rear Panel

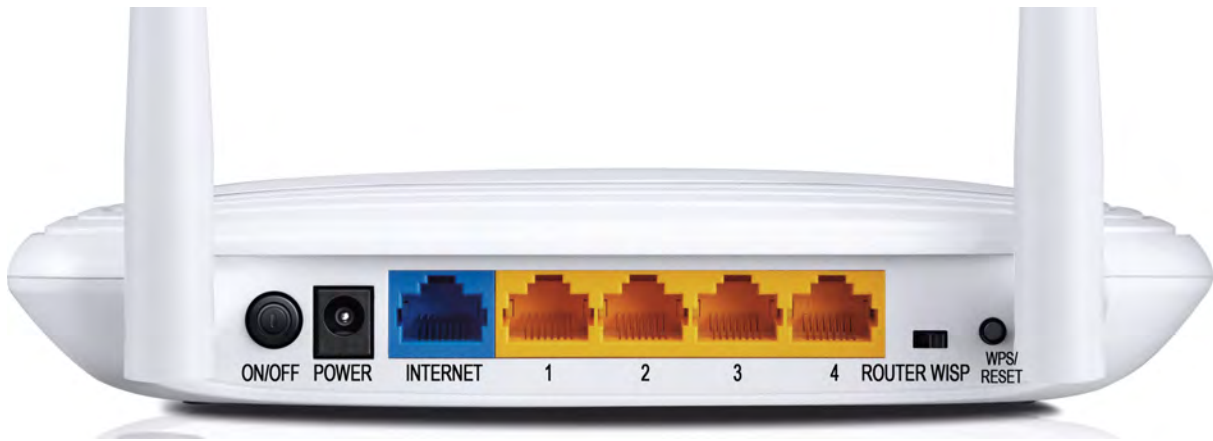


Figure 1-2 Rear Panel sketch

The following parts are located on the rear panel (View from left to right).

- **ON/OFF:** The switch for the power.
- **POWER:** The Power socket is where you will connect the power adapter. Please use the power adapter provided with this TL-WR843N 300Mbps Wireless AP/Client Router.
- **INTERNET:** This INTERNET port is where you will connect the DSL/cable Modem, or Ethernet.
- **4,3,2,1 (LAN):** These ports (4,3,2,1) connect the Router to the local PC(s).
- **ROUTER WISP:** This switch is used to select working mode.
- **WPS/RESET:** This button is used for both WPS and Reset function. To use the WPS function, press it for less than five seconds; to use the RESET function, press it for more than five seconds.

- **Used as RESET button:**

There are two ways to reset to the Router's factory defaults:

- 1) Use the **Factory Defaults** function on **System Tools** → **Factory Defaults** page in the Router's Web-based Utility.
- 2) Use the **WPS/RESET** button: With the Router powered on, press and hold the **WPS/RESET** button (more than 5 seconds) until the SYS LED becomes quick-flash from slow-flash. Then release the button and wait the Router to reboot to its factory default settings.

- **Used as WPS button:**

If you have client devices, such as wireless adapters, that support Wi-Fi Protected Setup, then you can press this button to quickly establish a connection between the Router and client devices and automatically configure wireless security for your wireless network.

- **Wireless antenna:** To receive and transmit the wireless data.

Chapter 2. Connecting the Router

2.1 System Requirements

- Broadband Internet Access Service (DSL/Cable/Ethernet)
- One DSL/Cable Modem that has an RJ45 connector (which is not necessary if the Router is connected directly to the 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 °C ~ 40 °C (32 °F ~ 104 °F)
- Operating Humidity: 10%~90%RH, Non-condensing

2.3 Connecting the Router

To connect the Router, please follow the steps below:

- 1) Locate an optimum location for the Router. The best place is usually at the center of your wireless network. The place must accord with the [Installation Environment Requirements](#).
- 2) Adjust the direction of the antenna. Normally, upright is a good direction.

After finishing the steps above, please choose the working mode you need and carry out the corresponding steps. There are two working mode supported by this router: **WISP Client Router** and **Standard Wireless Router**.

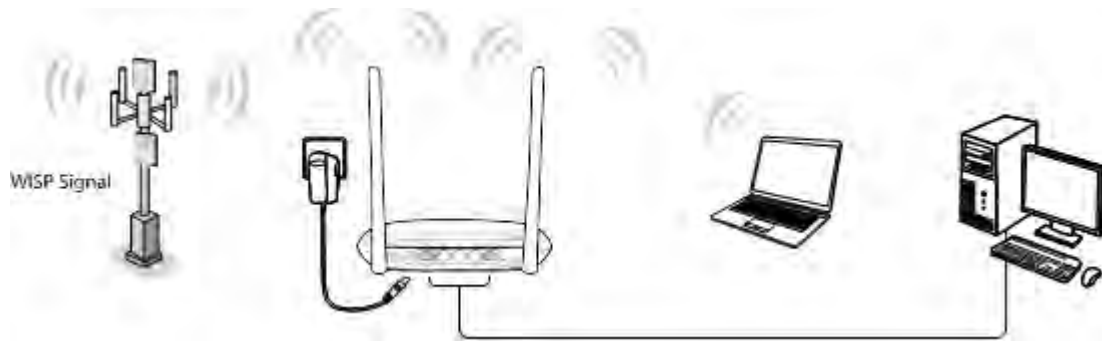
a) WISP Client Router Mode

Figure 2-1 Hardware Installation of the TL-WR843N in WISP Client Router mode

1. Connect the notebook/PC to the LAN port of TL-WR843N router with an Ethernet cable.
2. Plug one end of the provided power adapter into the POWER jack of the router, and the other end to a standard electrical wall socket.
3. Press the ON/OFF button of the router.

b) Standard Wireless Router Mode

Figure 2-2 Hardware Installation of the TL-WR843N in Router mode

1. Connect the PC(s)/Switch/Hub in your LAN to the LAN Ports on the Router.
2. Connect the DSL/Cable Modem to the INTERNET port on the Router.
3. Plug one end of the provided power adapter into the POWER jack of the router, and the other end to a standard electrical wall socket.
4. Press the ON/OFF button of the router.

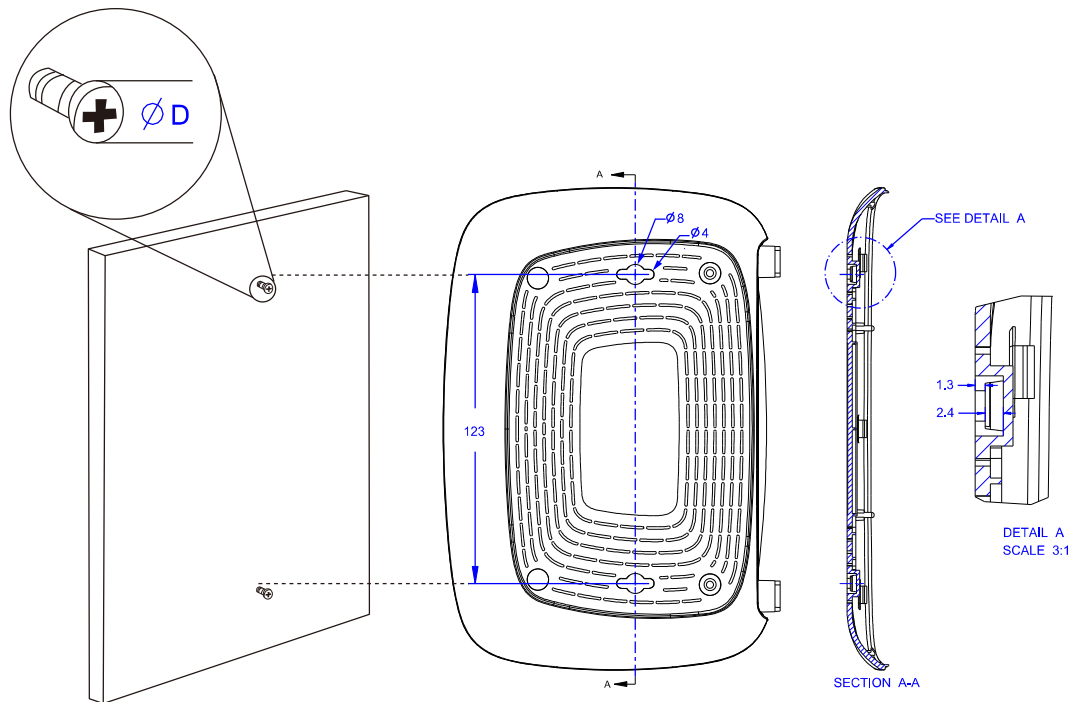


Figure 2-3 Wall-mount Install

Note: The diameter of the screw, $4\text{mm} < D < 8\text{mm}$, and the distance of two screws is 123mm. The screw that project from the wall need around 4mm based, and the length of the screw need to be at least 20mm to withstand the weight of the product.

Chapter 3. Quick Installation Guide

This chapter will show you how to configure the basic functions of your TL-WR843N 300Mbps Wireless AP/Client Router using **Quick Setup Wizard** within minutes.

3.1 TCP/IP Configuration

The default domain name of the TL-WR843N 300Mbps Wireless AP/Client Router is <http://tplinkwifi.net>, the default IP address is 192.168.0.1, and the default Subnet Mask is 255.255.255.0. These values can be changed as you desire. In this guide, we use all the default values for description.

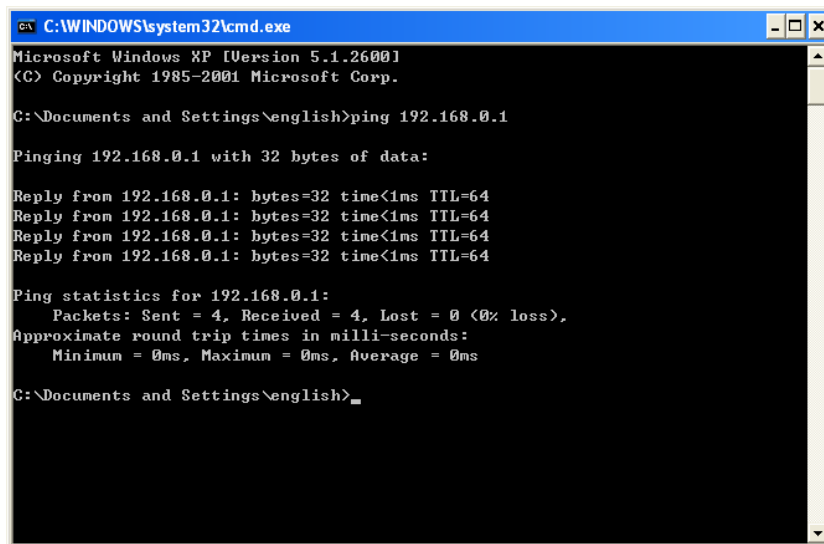
Connect the local PC to the LAN ports of the Router. And then you can configure the IP address for your PC in the following two ways.

- Configure the IP address manually
 - 1) Set up the TCP/IP Protocol for your PC. If you need instructions as to how to do this, please refer to [Appendix B: "Configuring the PC"](#).
 - 2) Configure the network parameters. The IP address is 192.168.0.xxx ("xxx" is any number from 2 to 254), Subnet Mask is 255.255.255.0, and Gateway is 192.168.0.1 (The Router's default IP address)
- Obtain an IP address automatically
 - 1) Set up the TCP/IP Protocol in "**Obtain an IP address automatically**" mode on your PC. If you need instructions as to how to do this, please refer to [Appendix B: "Configuring the PC"](#).
 - 2) Then the built-in DHCP server will assign IP address for the PC.

Now, you can run the Ping command in the **command prompt** to verify the network connection between your PC and the Router. The following example is in Windows XP.

Open a command prompt, and type *ping 192.168.0.1*, and then press **Enter**.

- If the result displayed is similar to the Figure 3-1, it means the connection between your PC and the Router has been established well.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\english>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

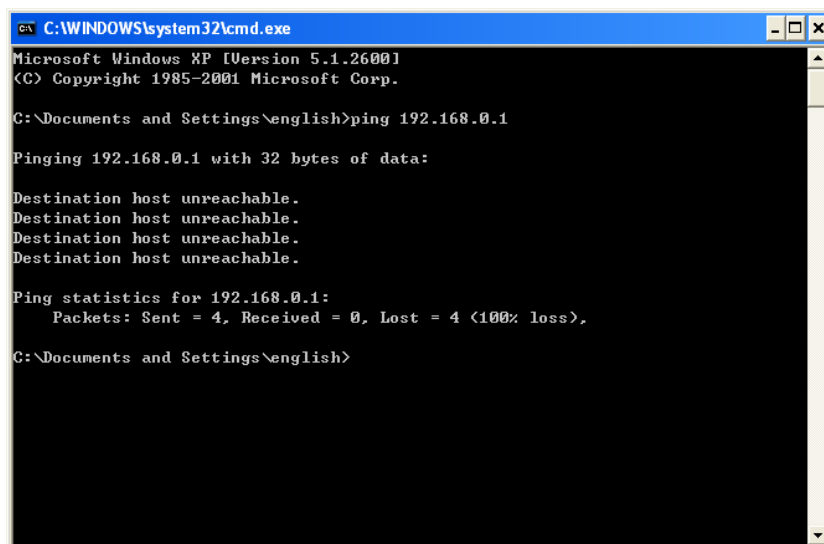
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\english>
```

Figure 3-1 Success result of Ping command

- If the result displayed is similar to the Figure 3-2, it means the connection between your PC and the Router is failed.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\english>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\english>
```

Figure 3-2 Failure result of Ping command

Please check the connection following these steps:

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

Note:

The 1/2/3/4 LEDs of LAN ports which you link to on the Router and LEDs on your PC's adapter should be lit.

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

Note:

If the Router's IP address is 192.168.0.1, your PC's IP address must be within the range of 192.168.0.2 ~ 192.168.0.254.

3. Is the default LAN IP of the Router correct?

 Note:

If the LAN IP of the modem connected with your router is 192.168.0.x, the default LAN IP of the Router will automatically switch from 192.168.0.1 to 192.168.1.1 to avoid IP conflict. Therefore, in order to verify the network connection between your PC and the Router, you can open a command prompt, and type *ping 192.168.1.1*, and then press **Enter**.

3.2 Quick Installation Guide

With a Web-based utility, it is easy to configure and manage the TL-WR843N 300Mbps Wireless AP/Client 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 in the default address <http://tplinkwifi.net> in the address field of the browser.



Figure 3-3 Log in the Router

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



Figure 3-4 Login Windows

 Note:

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 a successful login, you can click the **Quick Setup** menu to quickly configure your Router.

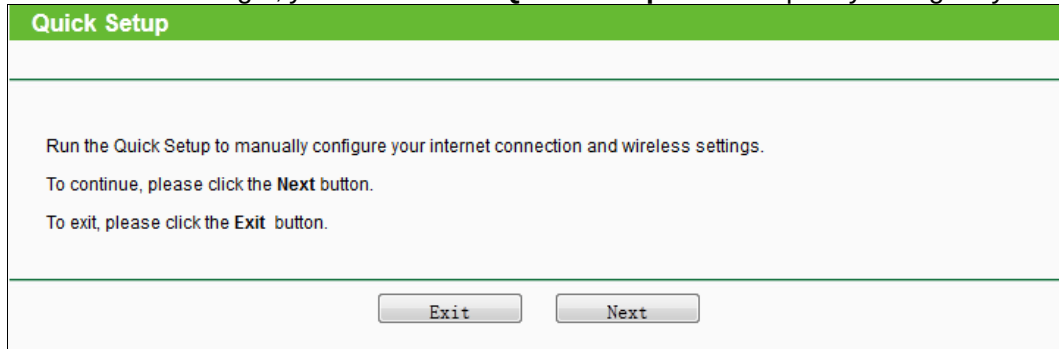


Figure 3-5 Quick Setup

3. Click **Next**, and then **Working Mode** page will appear. Tick **Control the system mode by software**, as shown in Figure 3-6.

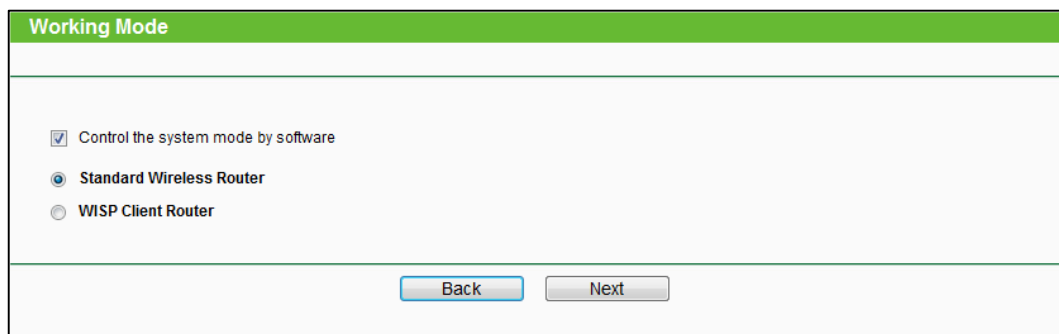
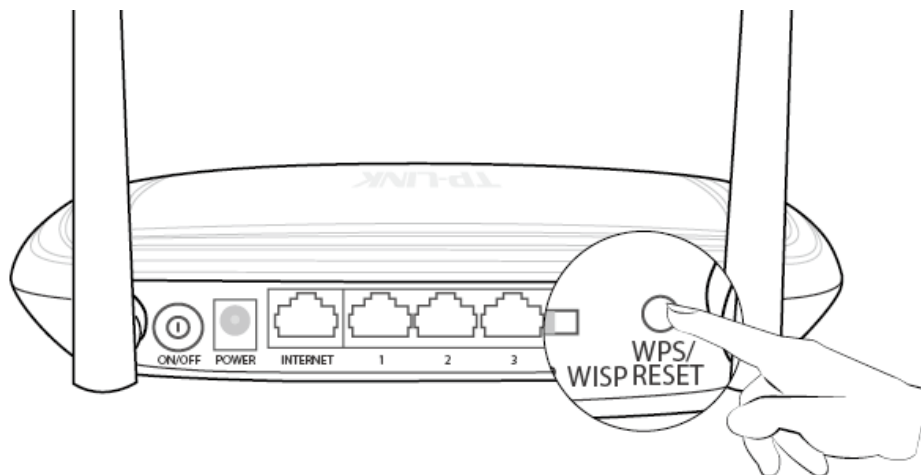


Figure 3-6 Working Mode

 Note:

- 1) The Router supports two working modes for multi-user to access the Internet: Standard Wireless Router and WISP Client Router, you can either select working mode by software as shown above or select it by turn the **work mode switch** at the back panel of your router, as shown below.



- 2) If you are unsure about which one to select, please refer to **Working Mode Help** page on the right. You can configure your device quickly by the following steps in different modes.

3.2.1 Configuration for Router Mode

When you choose **Standard Wireless Router** on **Working Mode** page as shown in Figure 3-6 , take the following steps:

1. Click **Next**, and then **WAN Connection Type** page will appear as shown in Figure 3-7.

Quick Setup - WAN Connection Type

The Quick Setup is preparing to set up your internet connection, please choose one type below according to your ISP. The detailed description will be displayed after you choose the corresponding type.

☐ Auto-Detect

☒ **Dynamic IP (Most Common Cases)**
For Cable/DSL/Broadband connection which makes your computer immediately online without any setting or signing-in.

☐ Static IP

☐ PPPoE/Russian PPPoE

☐ L2TP/Russian L2TP

☐ PPTP/Russian PPTP

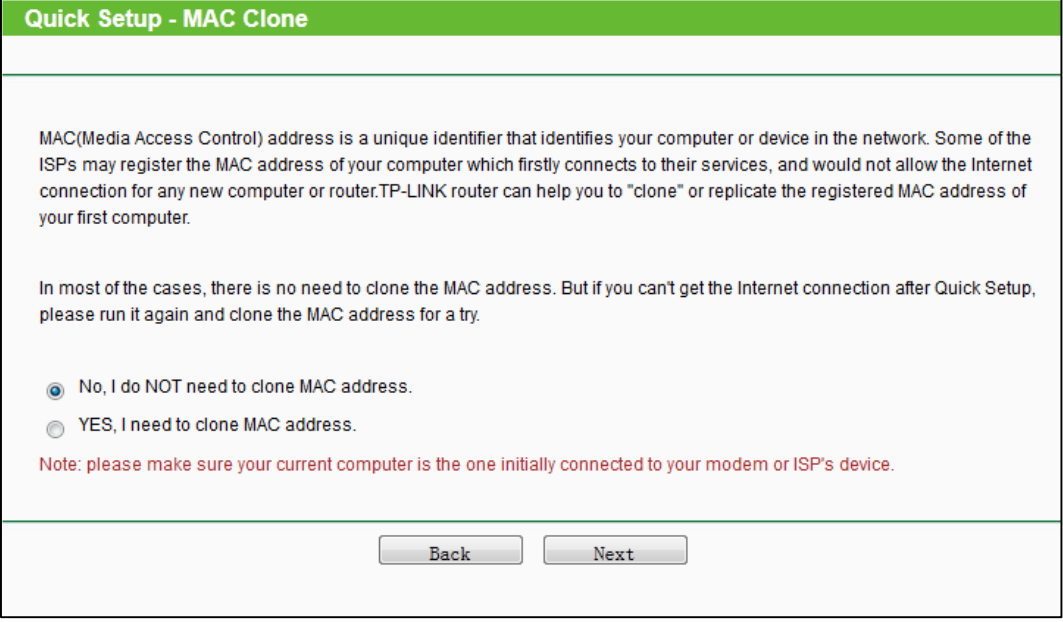
Note: For users in some areas (such as Russia, Ukraine etc.), please contact your ISP to choose connection type manually.

Back Next

Figure 3-7 WAN Connection Type

The Router provides **Auto-Detect** function and supports five popular ways **Dynamic IP**, **Static IP**, **PPPOE/Russian L2TP**, **L2TP/Russian L2TP** and **PPTP/Russian PPTP** to connect to the Internet. It's recommended that you make use of the **Auto-Detect** function. If you are sure of what kind of connection type your ISP provides, you can select the very type and click **Next** to continue configuring.

2. If you select **Auto-Detect**, the Router will automatically detect the connection type your ISP provides. Make sure the cable is securely plugged into the WAN port before detection. The appropriate configuration page will be displayed when an active Internet service is successfully detected by the Router.
 - 1) If the connection type detected is **Dynamic IP**, the next screen will appear as shown in Figure 3-8. **MAC Clone** is necessary for most users using Cable Modem. It's highly recommended to do this on the **MAIN COMPUTER** that was originally connected to your Cable Modem.



Quick Setup - MAC Clone

MAC(Media Access Control) address is a unique identifier that identifies your computer or device in the network. Some of the ISPs may register the MAC address of your computer which firstly connects to their services, and would not allow the Internet connection for any new computer or router. TP-LINK router can help you to "clone" or replicate the registered MAC address of your first computer.

In most of the cases, there is no need to clone the MAC address. But if you can't get the Internet connection after Quick Setup, please run it again and clone the MAC address for a try.

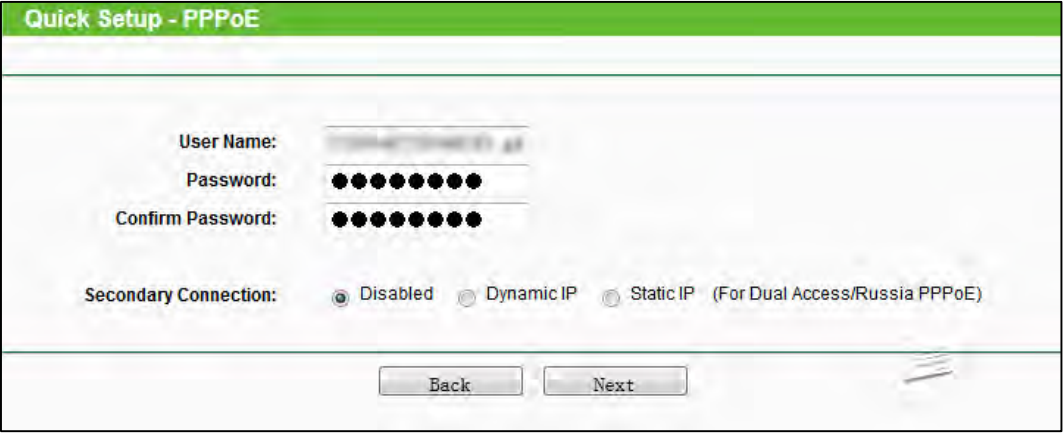
☒ No, I do NOT need to clone MAC address.
☐ YES, I need to clone MAC address.

Note: please make sure your current computer is the one initially connected to your modem or ISP's device.

Back Next

Figure 3-8 MAC Clone

- 2) If the connection type detected is **PPPoE/Russian PPPoE**, the next screen will appear as shown in Figure 3-9.



Quick Setup - PPPoE

User Name:

Password:

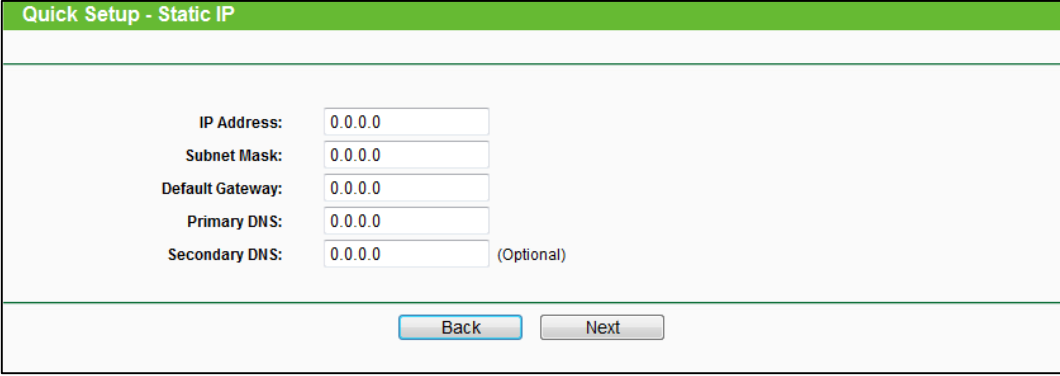
Confirm Password:

Secondary Connection: ☒ Disabled ☐ Dynamic IP ☐ Static IP (For Dual Access/Russian PPPoE)

Back Next

Figure 3-9 Quick Setup - PPPoE

- 3) If the connection type detected is **Static IP**, the next screen will appear as shown in Figure 3-10.



Quick Setup - Static IP

IP Address:

Subnet Mask:

Default Gateway:

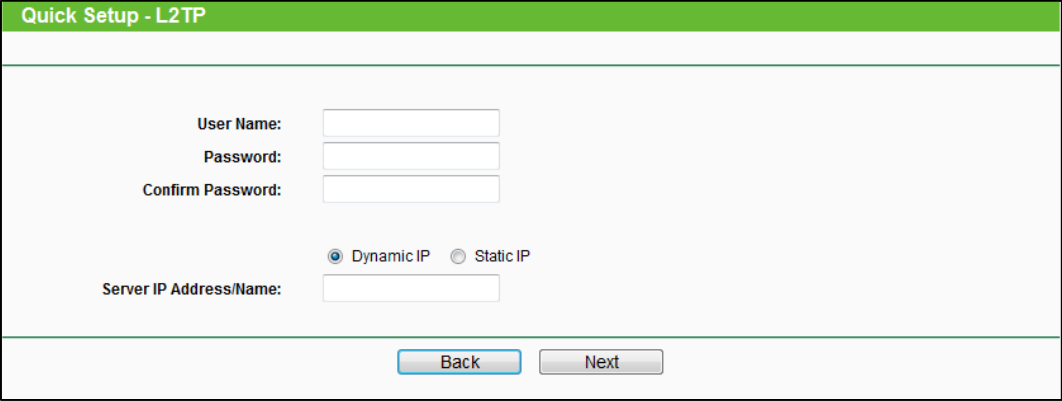
Primary DNS:

Secondary DNS: (Optional)

Back Next

Figure 3-10 Quick Setup - Static IP

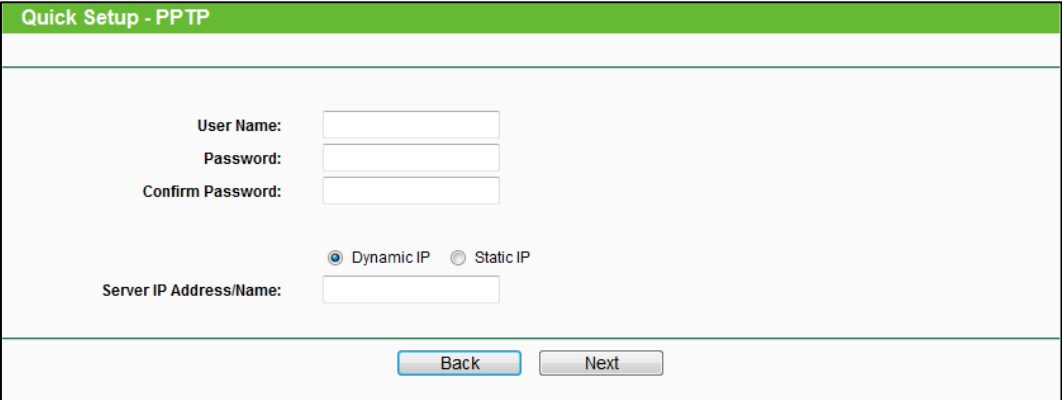
- 4) If the connection type detected is **L2TP/Russian L2TP**, the next screen will appear as shown in Figure 3-11.



The screenshot shows the 'Quick Setup - L2TP' configuration page. It features a green header bar with the title. Below the header, there are three input fields for 'User Name:', 'Password:', and 'Confirm Password:'. Underneath these, there are two radio buttons: 'Dynamic IP' (which is selected) and 'Static IP'. Below the radio buttons is a single input field for 'Server IP Address/Name:'. At the bottom of the form, there are two buttons: 'Back' and 'Next'.

Figure 3-11 Quick Setup – L2TP

- 5) If the connection type detected is **PPTP/Russian PPTP**, the next screen will appear as shown in Figure 3-12.



The screenshot shows the 'Quick Setup - PPTP' configuration page. It features a green header bar with the title. Below the header, there are three input fields for 'User Name:', 'Password:', and 'Confirm Password:'. Underneath these, there are two radio buttons: 'Dynamic IP' (which is selected) and 'Static IP'. Below the radio buttons is a single input field for 'Server IP Address/Name:'. At the bottom of the form, there are two buttons: 'Back' and 'Next'.

Figure 3-12 Quick Setup – PPTP

3. Click **Next** to continue, the Wireless settings page will appear as shown in Figure 3-13.

Quick Setup - Wireless

The Internet settings have been completed, now please configure the wireless settings.

Wireless Radio: (Also called the SSID)

Wireless Network Name: (Also called the SSID)

Wireless Security:

☐ Disable Security

☒ WPA-PSK/WPA2-PSK

Wireless Password: (You can enter ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 64.)

☐ No Change (use the current security settings.)

☐ More Advanced Wireless Settings

Figure 3-13 Quick Setup – Wireless

- **Wireless Radio** - The wireless radio can only be enabled and disabled.
- **Wireless Network Name** - Enter a value of up to 32 characters. The same name of SSID (Service Set Identification) must be assigned to all wireless devices in your network. Considering your wireless network security, the default SSID is set to be TP-LINK_XXXX (XXXX indicates the last unique six numbers of each Router's MAC address). This value is case-sensitive. For example, *TEST* is NOT the same as *test*.
- **Disable Security** - The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the Router without encryption. It is recommended strongly that you choose one of following options to enable security.
- **WPA-PSK/WPA2-PSK** - Select WPA based on pre-shared passphrase.
 - **PSK Password** - You can enter **ASCII** or **Hexadecimal** characters.

For **ASCII**, the key can be made up of any numbers 0 to 9 and any letters A to Z, the length should be between 8 and 63 characters.

For **Hexadecimal**, the key can be made up of any numbers 0 to 9 and letters A to F, the length should be between 8 and 64 characters.

Please also note the key is case sensitive, this means that upper and lower case keys will affect the outcome. It would also be a good idea to write down the key and all related wireless security settings.
- **No Change** - If you chose this option, wireless security configuration will not change!

These settings are only for basic wireless parameters. For advanced settings, please refer to [4.7 Wireless](#).

- Click the **Next** button. You will see the page as shown in Figure 3-14. Please click the **Reboot/Finish** button to make your configuration take effect and finish the **Quick Setup**.

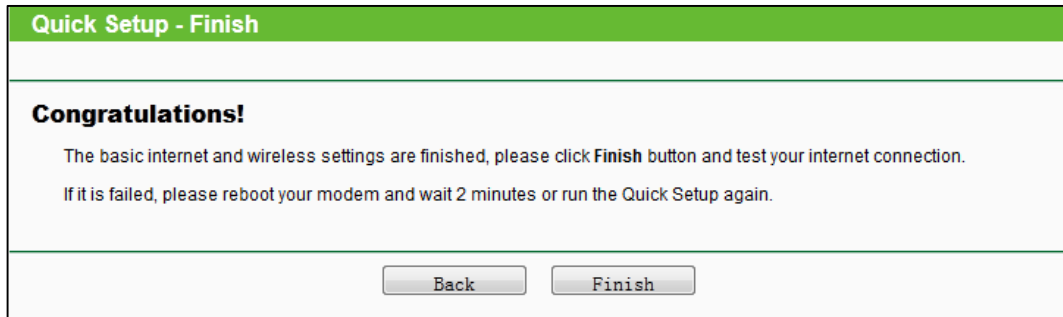


Figure 3-14 Quick Setup – Finish

3.2.2 Configuration for WISP Client Router Mode

When you choose **WISP Client Router** on **Working Mode** page in Figure 3-6 , take the following steps:

- Click **Next**, and then WAN Connection Type page will appear as shown in Figure 3-15.

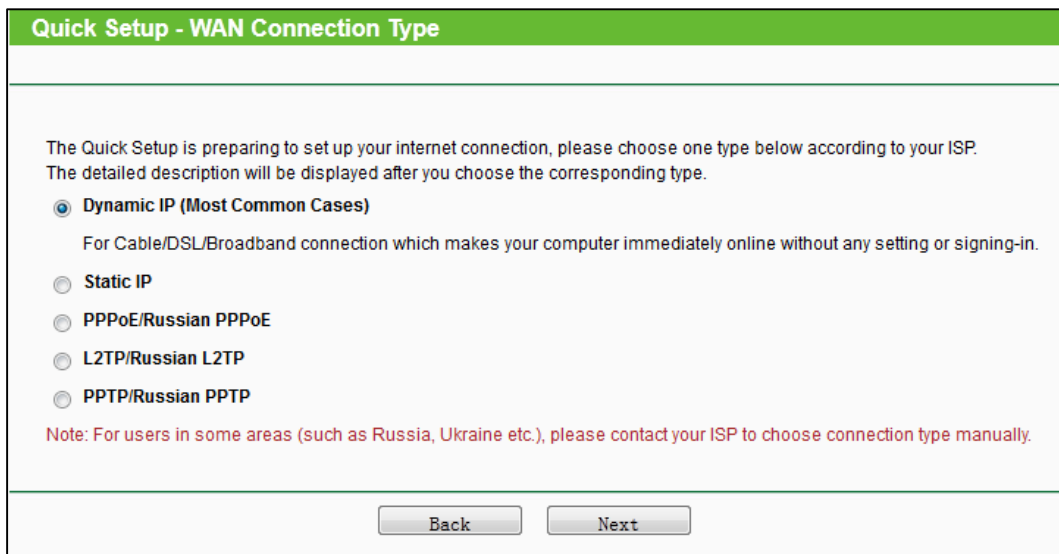


Figure 3-15 Quick Setup – WAN Connection Type

The router in WISP Client Router mode supports three popular ways to connect to the Internet. Please select the one compatible with your ISP.

- a) If you choose "**Dynamic IP**", the router will automatically receive the IP parameters from your ISP without needing to enter any parameters.
- b) If you choose "**PPPoE/Russian PPPoE**", you will see this page shown in Figure 3-16.

Figure 3-16 PPPoE

- **User Name and Password** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
 - **Confirm Password** - Enter again the Password provided by your ISP to ensure the password you entered is correct.
- c) If you Choose "**Static IP**", the Static IP settings page will appear as shown in Figure 3-17.

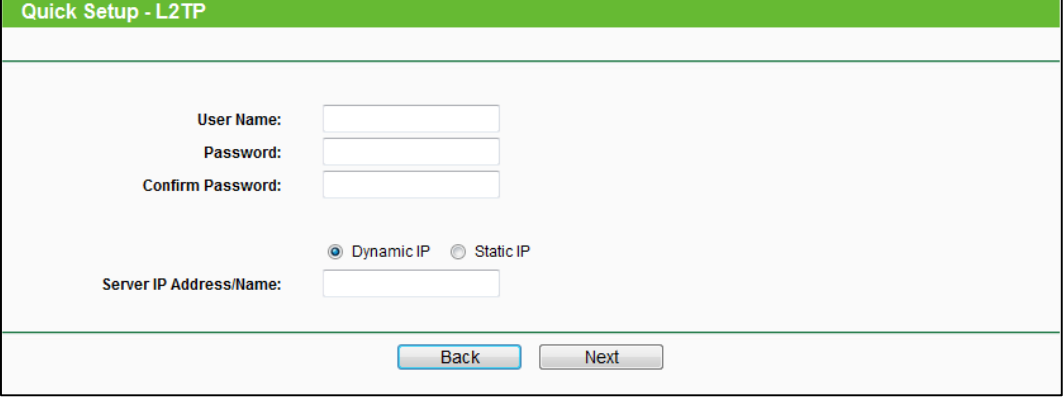
Figure 3-17 Static IP

 Note:

The IP parameters should have been provided by your ISP.

- **IP Address** - This is the WAN IP address as seen by external users on the Internet (including your ISP). Enter the IP address into the field.
- **Subnet Mask** - The Subnet Mask is used for the WAN IP address, it is usually 255.255.255.0.

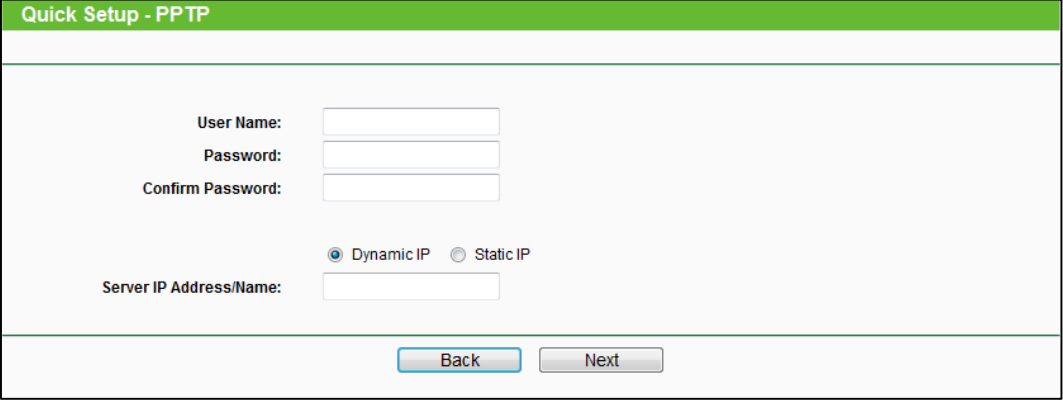
- **Default Gateway** - Enter the gateway IP address into the box if required.
 - **Primary DNS** - Enter the DNS Server IP address into the boxes if required.
 - **Secondary DNS** - If your ISP provides another DNS server, enter it into this field.
- d) If the connection type detected is **L2TP/Russian L2TP**, the next screen will appear as shown in Figure 3-18.



The screenshot shows the 'Quick Setup - L2TP' configuration page. It features a green header bar with the title. Below the header, there are three input fields for 'User Name:', 'Password:', and 'Confirm Password:'. Underneath these, there are two radio buttons: 'Dynamic IP' (which is selected) and 'Static IP'. Below the radio buttons is a single input field for 'Server IP Address/Name:'. At the bottom of the form, there are two buttons: 'Back' and 'Next'.

Figure 3-18 Quick Setup – L2TP

- e) If the connection type detected is **PPTP/Russian PPTP**, the next screen will appear as shown in Figure 3-19.



The screenshot shows the 'Quick Setup - PPTP' configuration page. It features a green header bar with the title. Below the header, there are three input fields for 'User Name:', 'Password:', and 'Confirm Password:'. Underneath these, there are two radio buttons: 'Dynamic IP' (which is selected) and 'Static IP'. Below the radio buttons is a single input field for 'Server IP Address/Name:'. At the bottom of the form, there are two buttons: 'Back' and 'Next'.

Figure 3-19 Quick Setup – PPTP

2. Click **Next**, and the Wireless settings page will appear as shown in Figure 3-20.

Quick Setup - Wireless

Client Setting

SSID:

BSSID: Example:00-1D-0F-11-22-33

Key type:

WEP Index:

Auth type:

Password:

AP Setting

Local SSID:

Wireless Security Mode:

Wireless Password:

You can enter ASCII or Hexadecimal characters. For Hexadecimal, the length should be between 8 and 64 characters; for ASCII, the length should be between 8 and 63 characters. For good security it should be of ample length and should not be a commonly known phrase.

Figure 3-20 Quick Setup – Wireless

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

Click **Survey** button on the Wireless page as shown in Figure 3-20, and then AP List page will appear as shown in Figure 3-21. Find the SSID of the Access Point you want to access, and click **Connect** in the corresponding row. For example, the first item is selected. The target network's SSID will be automatically filled into the corresponding box which is shown as the Figure 3-22.

AP List						
AP Count: 49						
ID	BSSID	SSID	Signal	Channel	Security	Choose
1	00-0A-EB-0C-26-42	TP-LINK_2642	84dB	11	WPA-PSK/WPA2-PSK	Connect
2	00-0A-EB-13-09-19	TP-LINK_0919	74dB	1	WPA2-PSK	Connect
3	80-F6-2E-0A-A3-62	and-Business	69dB	6	None	Connect
Back Next						

Figure 3-21 AP List

Quick Setup - Wireless	
Client Setting SSID: TP-LINK_2642 BSSID: 00-0A-EB-0C-26-42 Example:00-1D-0F-11-22-33 Survey Key type is selected. Key type: WPA-PSK/WPA2-PSK WEP Index: 1 Auth type: open Password:	
AP Setting Local SSID: TP-LINK_7B00 Wireless Security Mode: Most Secure(WPA/WPA2-PSK) Wireless Password: 12345670 You can enter ASCII or Hexadecimal characters. For Hexadecimal, the length should be between 8 and 64 characters; for ASCII, the length should be between 8 and 63 characters. For good security it should be of ample length and should not be a commonly known phrase.	
Back Next	

Figure 3-22 Quick Setup – Wireless

 Note:

If you know the SSID of the desired AP, you can also input it into the field "SSID" manually.

- **Local SSID-** Enter a value of up to 32 characters. The same Name (SSID) must be assigned to all wireless devices in your network.
 - **Wireless Security Mode** – Select one of the three options: No Security, Secure(WEP), Most Secure(WPA/WPA2-PSK). WPA/WPA2-PSK is recommended.
 - **Wireless Password-** Enter a unique and easy-to-remember password for your own wireless network.
3. After you have completed the above, click **Next**, the Finish page will appear as below. Please click the **Reboot/Finish** button to make your configuration take effect and finish the **Quick Setup**.

Quick Setup - Finish

Congratulations!

The basic internet and wireless settings are finished, please click **Finish** button and test your internet connection.

If it is failed, please reboot your modem and wait 2 minutes or run the Quick Setup again.

The change of working mode config will not take effect until this device reboot.

Back

Reboot

Figure 3-23 Finish

Chapter 4. Configuring the Router

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

4.1 Login

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

Status
Quick Setup
WPS
Working Mode
Network
Wireless
Guest Network
DHCP
Forwarding
Security
Parental Control
Access Control
Advanced Routing
Bandwidth Control
IP & MAC Binding
Dynamic DNS
IPv6 Support
System Tools
Logout

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

4.2 Status

The Status page provides the current status information about the Router. All information is read-only.

Status		
Firmware Version:	3.16.9 Build 150525 Rel.62249n	
Hardware Version:	WR843N v2 00000000	
LAN		
MAC Address:	00-0A-EB-13-7B-00	
IP Address:	192.168.0. 1	
Subnet Mask:	255.255.255.0	
Wireless		
Wireless Radio:	Enable	
Name (SSID):	TP-LINK_7B00	
Channel:	Auto (Current channel 1)	
Mode:	11bgn mixed	
Channel Width:	Automatic	
MAC Address:	00-0A-EB-13-7B-00	
Client Status:	Init...	
WAN		
MAC Address:	00-0A-EB-13-7B-01	
IP Address:	0.0.0.0	Dynamic IP
Subnet Mask:	0.0.0.0	
Default Gateway:	0.0.0.0	WAN port is unplugged!
DNS Server:	0.0.0.0 , 0.0.0.0	
Traffic Statistics		
	Received	Sent
Bytes:	0	0
Packets:	0	0
System Up Time:	3 days 00:37:46	Refresh

Figure 4-1 Router Status

4.3 Quick Setup

Please refer to [3.2 Quick Installation Guide](#).

4.4 WPS

This section will guide you to add a new wireless device to an existing network quickly by WPS (Wi-Fi Protected Setup) function.

- Choose menu "WPS", and you will see the next screen (shown in Figure 4-2).

WPS (Wi-Fi Protected Setup)

WPS Status: **Enabled** [Disable WPS](#)

Current PIN: **12345670** [Restore PIN](#) [Gen New PIN](#)

☐ Disable PIN of this device

Add a new device: [Add Device](#)

Figure 4-2 WPS

- **WPS Status** - Enable or disable the WPS function here.
- **Current PIN** - The current value of the Router's PIN is displayed here. The default PIN of the Router can be found in the label attached on the router.
- **Restore PIN** - Restore the PIN of the Router to its default.
- **Gen New PIN** - Click this button, and then you can get a new random value for the Router's PIN. You can ensure the network security by generating a new PIN.
- **Disable PIN of this device** - You can disable the Router's PIN manually here. If the router receives multiple failed attempts to authenticate an external registrar, this function will be disabled automatically.
- **Add Device** - You can add a new device to the existing network manually by clicking this button.

b). To add a new device:

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

 Note:

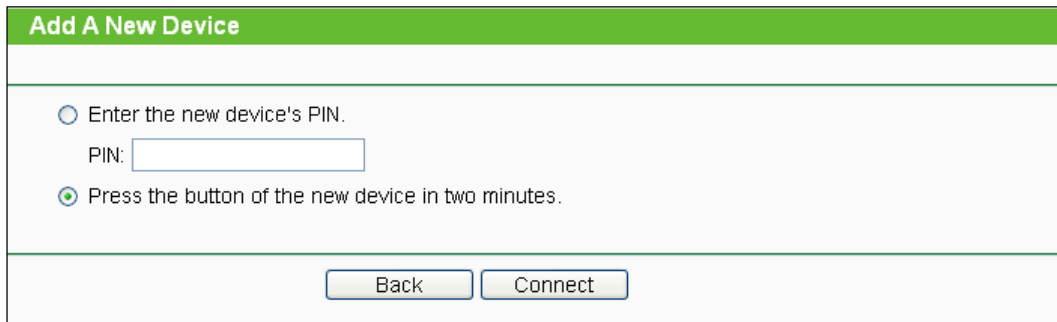
To build a successful connection by WPS, you should also do the corresponding configuration of the new device for WPS function meanwhile.

I. Use the Wi-Fi Protected Setup Button

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

Step 1: Press the WPS/RESET button on the back panel of the Router for one second.

You can also keep the default WPS Status as **Enabled** and click the **Add Device** button in Figure 4-2, then Choose “**Press the button of the new device in two minutes**” and click **Connect**. (Shown in the following figure)



The screenshot shows a web interface titled "Add A New Device" in a green header bar. Below the header, there are two radio button options. The first option, "Enter the new device's PIN.", is selected with a blue dot. It includes a text input field labeled "PIN:". The second option, "Press the button of the new device in two minutes.", is unselected. At the bottom of the form, there are two buttons: "Back" and "Connect".

Figure 4-3 Add A New Device

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

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

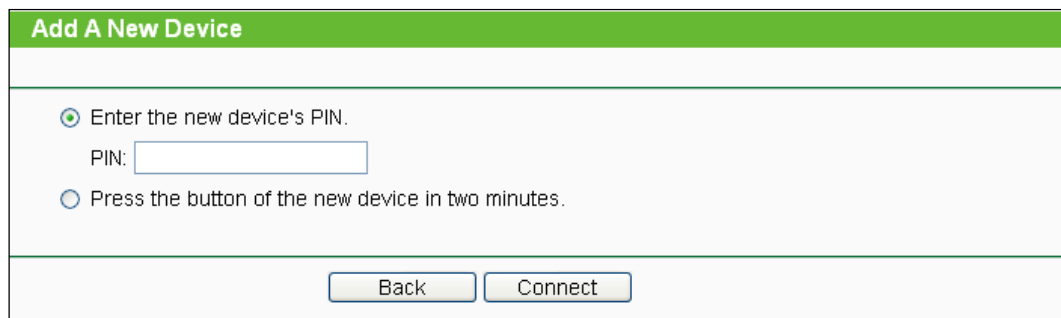
Step 4: When the WPS LED is on, the client device has successfully connected to the Router.

Step 5: Refer back to your client device or its documentation for further instructions.

II. Enter the client device's PIN on the Router

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

Step 1: Keep the default WPS Status as **Enabled** and click the **Add Device** button in Figure 4-2, then the following screen will appear.



This screenshot is similar to Figure 4-3, but the second radio button option, "Press the button of the new device in two minutes.", is now selected with a blue dot. The "Enter the new device's PIN." option is unselected. The "PIN:" input field and the "Back" and "Connect" buttons remain the same.

Figure 4-4 Add A New Device

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

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

III. Enter the Router's PIN on your client device

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

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

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

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

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

 Note:

- 1) The WPS LED on the Router will light green for five minutes if the device has been successfully added to the network.
- 2) The WPS function cannot be configured if the Wireless Function of the Router is disabled. Please make sure the Wireless Function is enabled before configuring the WPS.

4.5 Working Mode

The Router supports two working modes: **Standard Wireless Router** and **WISP Client Router**. Please select one you want. Click **Save** to save your choice, which is shown as Figure 4-5.

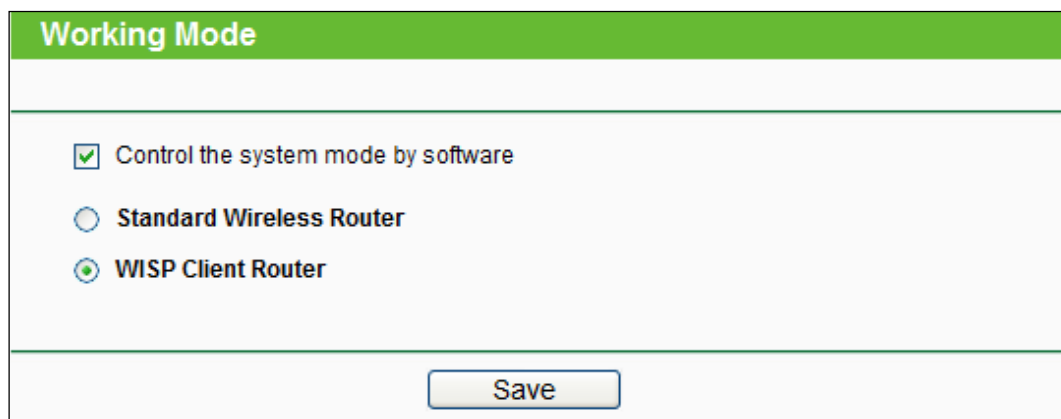


Figure 4-5 Working Mode

- **Control the system mode by software** – Tick this item, you will see the two options of working mode. You can also select it by turn the work mode switch at the back panel of your Router.
- **Standard Wireless Router** - In this mode, the device enables multi-users to share Internet via ADSL/Cable Modem. The wireless port share the same IP to ISP through Ethernet WAN port. The Wireless port acts the same as a LAN port while at Router mode.
- **WISP Client Router** - In this mode, the device enables multi-users to share Internet from WISP. The LAN port devices share the same IP from WISP through Wireless port. While connecting to WISP, the Wireless port works as a WAN port at Client Router mode. The Ethernet port acts as a LAN port.

4.6 Network

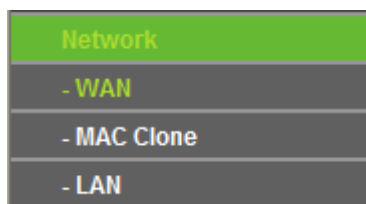


Figure 4-6 the Network menu

There are three submenus under the Network menu (shown in Figure 4-6): **WAN**, **MAC Clone** and **LAN**. Click any of them, and you will be able to configure the corresponding function.

4.6.1 WAN

Choose menu “**Network** → **WAN**”, you can configure the IP parameters of the WAN on the screen below.

1. If your ISP provides the DHCP service, please choose **Dynamic IP** type, and the Router will automatically get IP parameters from your ISP. You can see the page as follows (Figure 4-7):

The screenshot shows the WAN configuration interface with a green header bar labeled 'WAN'. The 'WAN Connection Type' is set to 'Dynamic IP' with a 'Detect' button next to it. Below this, the IP Address, Subnet Mask, and Default Gateway are all set to '0.0.0.0'. There are 'Renew' and 'Release' buttons, and a red error message 'WAN port is unplugged!'. The 'MTU Size (in bytes)' is set to '1500' with a note '(The default is 1500, do not change unless necessary.)'. There is a checkbox for 'Use These DNS Servers' which is unchecked. Below it, 'Primary DNS' and 'Secondary DNS' are both set to '0.0.0.0' with a note '(Optional)'. The 'Host Name' field is empty. At the bottom, there is a checkbox for 'Get IP with Unicast DHCP (It is usually not required.)' which is unchecked, and a 'Save' button.

Figure 4-7 WAN – Dynamic IP

This page displays the WAN IP parameters assigned dynamically by your ISP, including IP address, Subnet Mask, Default Gateway, etc. Click the **Renew** button to renew the IP parameters from your ISP. Click the **Release** button to release the IP parameters.

- **MTU Size** - The normal **MTU** (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. It is not recommended that you change the default **MTU Size** unless required by your ISP.
- **Use These DNS Servers** - If your ISP gives you one or two DNS addresses, select **Use These DNS Servers** and enter the primary and secondary addresses into the correct fields. Otherwise, the DNS servers will be assigned dynamically from your ISP.

Note:

If you find error when you go to a website after entering the DNS addresses, it is likely that your DNS servers are set up improperly. You should contact your ISP to get DNS server

addresses.

- **Host Name** - This option specifies the Host Name of the Router.
- **Get IP with Unicast DHCP** - A few ISPs' DHCP servers do not support the broadcast applications. If you cannot get the IP Address normally, you can choose this option. (It is rarely required.)

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

2. If your ISP provides a static or fixed IP Address, Subnet Mask, Gateway and DNS setting, select **Static IP**. The Static IP settings page will appear, shown in Figure 4-8.

WAN

WAN Connection Type: Static IP Detect

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Default Gateway: 0.0.0.0 (Optional)

MTU Size (in bytes): 1500 (The default is 1500, do not change unless necessary.)

Primary DNS: 0.0.0.0 (Optional)

Secondary DNS: 0.0.0.0 (Optional)

Save

Figure 4-8 WAN - Static IP

- **IP Address** - Enter the IP address in dotted-decimal notation provided by your ISP.
- **Subnet Mask** - Enter the subnet Mask in dotted-decimal notation provided by your ISP, usually is 255.255.255.0.
- **Default Gateway** - (Optional) Enter the gateway IP address in dotted-decimal notation provided by your ISP.
- **MTU Size** - The normal **MTU** (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. It is not recommended that you change the default **MTU Size** unless required by your ISP.
- **Primary/Secondary DNS** - (Optional) Enter one or two DNS addresses in dotted-decimal notation provided by your ISP.

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

3. If your ISP provides a PPPoE connection, select **PPPoE/Russia PPPoE** option. Then should enter the following parameters (Figure 4-9):

The image shows a web-based configuration interface for a WAN connection. The title bar is green and labeled 'WAN'. Below it, the 'WAN Connection Type' is set to 'PPPoE/Russia PPPoE' with a 'Detect' button. The 'PPPoE Connection' section includes 'User Name' (username), 'Password' (masked with dots), and 'Confirm Password' (masked with dots). The 'Secondary Connection' section has three radio buttons: 'Disabled' (selected), 'Dynamic IP', and 'Static IP' (with a note '(For Dual Access/Russia PPPoE)'). The 'Wan Connection Mode' section has four radio buttons: 'Connect on Demand' (selected), 'Connect Automatically', 'Time-based Connecting' (with a 'Period of Time' field showing 'from 0 : 0 (HH:MM) to 23 : 59 (HH:MM)'), and 'Connect Manually'. Below these are two 'Max Idle Time' fields, both set to '15 minutes (0 means remain active at all times.)'. At the bottom are 'Connect', 'Disconnect', and 'Save' buttons. A status indicator shows 'Disconnected!'.

Figure 4-9 WAN - PPPoE

- **User Name/Password** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Secondary Connection** - It's available only for PPPoE Connection. If your ISP provides an extra Connection type such as Dynamic/Static IP to connect to a local area network, then you can check the radio button of Dynamic/Static IP to activate this secondary connection.
 - **Disabled** - The Secondary Connection is disabled by default, so there is PPPoE connection only. This is recommended.
 - **Dynamic IP** - You can check this radio button to use Dynamic IP as the secondary connection to connect to the local area network provided by ISP.
 - **Static IP** - You can check this radio button to use Static IP as the secondary connection to connect to the local area network provided by ISP.
- **Connect on Demand** - In this mode, the Internet connection can be terminated automatically after a specified inactivity period (**Max Idle Time**) and be re-established when you attempt to access the Internet again. If you want your Internet connection keeps active all the time, please enter "0" in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet access disconnects.

- **Connect Automatically** - The connection can be re-established automatically when it was down.
- **Time-based Connecting** - The connection will only be established in the period from the start time to the end time (both are in HH:MM format).

 Note:

Only when you have configured the system time on “**System Tools** → **Time settings**” page, will the **Time-based Connecting** function take effect.

- **Connect Manually** - You can click the **Connect/Disconnect** button to connect/disconnect immediately. This mode also supports the **Max Idle Time** function as **Connect on Demand** mode. The Internet connection can be disconnected automatically after a specified inactivity period and re-established when you attempt to access the Internet again.

Click the **Connect** button to connect immediately. Click the **Disconnect** button to disconnect immediately.

Caution: Sometimes the connection cannot be terminated although you specify a time to Max Idle Time because some applications are visiting the Internet continually in the background.

If you want to do some advanced configurations, please click the **Advanced** button, and the page shown in Figure 4-10 will then appear:

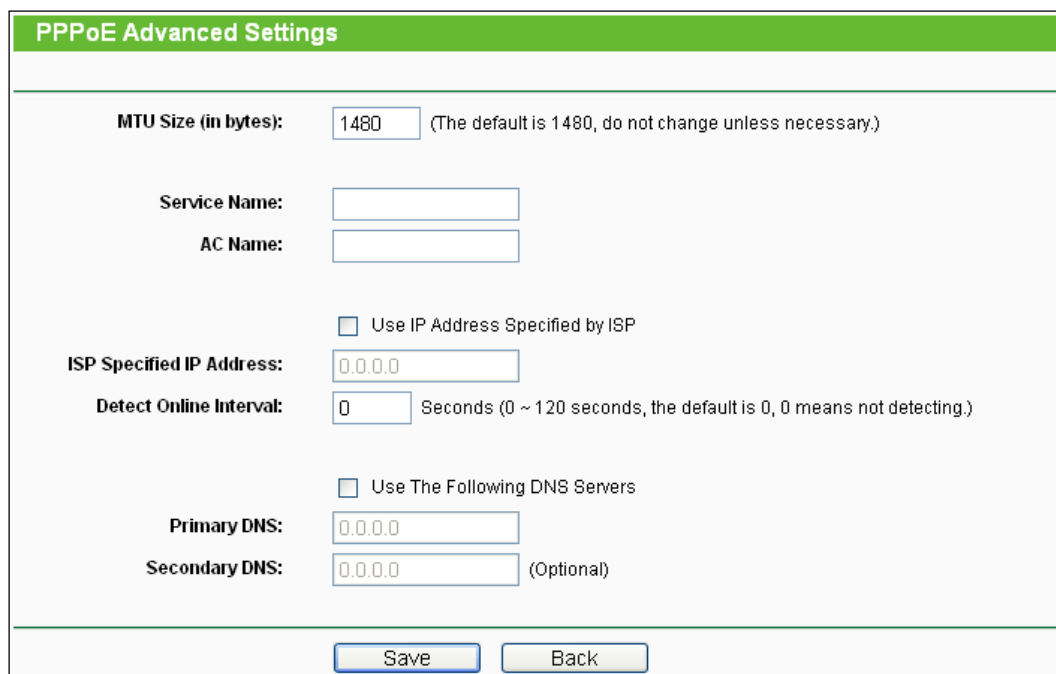


Figure 4-10 PPPoE Advanced Settings

- **MTU Size** - The default MTU size is “1480” bytes, which is usually fine. It is not recommended that you change the default **MTU Size** unless required by your ISP.
- **Service Name/AC Name** - The service name and AC (Access Concentrator) name should not

be configured unless you are sure it is necessary for your ISP. In most cases, leaving these fields blank will work.

- **ISP Specified IP Address** - If your ISP does not automatically assign IP addresses to the Router during login, please click **“Use IP address specified by ISP”** check box and enter the IP address provided by your ISP in dotted-decimal notation.
- **Detect Online Interval** - The Router will detect Access Concentrator online at every interval. The default value is “0”. You can input the value between “0” and “120”. The value “0” means no detect.
- **Primary DNS/Secondary DNS** - If your ISP does not automatically assign DNS addresses to the Router during login, please click **“Use the following DNS servers”** check box and enter the IP address in dotted-decimal notation of your ISP’s primary DNS server. If a secondary DNS server address is available, enter it as well.

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

4. If your ISP provides BigPond Cable (or Heart Beat Signal) connection, please select **BigPond Cable**. And you should enter the following parameters (Figure 4-11):

The image shows a web-based configuration interface for a WAN connection. The title bar is green and labeled 'WAN'. The main content area is white with a light blue border. It contains several configuration fields and buttons.

- WAN Connection Type:** A dropdown menu with 'BigPond Cable' selected.
- User Name:** A text input field containing 'username'.
- Password:** A text input field with masked characters (dots).
- Auth Server:** A text input field containing 'sm-server'.
- Auth Domain:** An empty text input field.
- MTU Size (in bytes):** A text input field containing '1500'. To its right, a note says '(The default is 1500, do not change unless necessary.)'
- Connection Mode:** Three radio buttons are present:
 - Connect on Demand:** Selected (indicated by a filled circle).
 - Connect Automatically:** Unselected (indicated by an empty circle).
 - Connect Manually:** Unselected (indicated by an empty circle).
- Max Idle Time:** Two text input fields, both containing '15'. To their right, a note says '(0 means remain active at all times.)'.
- Status Buttons:** Three buttons are located at the bottom of the configuration area: 'Connect' (highlighted in blue), 'Disconnected' (disabled), and 'Disconnected!' (disabled).
- Save Button:** A button labeled 'Save' is located at the bottom center of the form.

Figure 4-11

- **User Name/Password** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.

- **Auth Server** - Enter the authenticating server IP address or host name.
- **Auth Domain** - Type in the domain suffix server name based on your location.
e.g.
NSW / ACT - **nsw.bigpond.net.au**
VIC / TAS / WA / SA / NT - **vic.bigpond.net.au**
QLD - **qld.bigpond.net.au**
- **MTU Size** - The normal **MTU** (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. It is not recommended that you change the default **MTU Size** unless required by your ISP.
- **Connect on Demand** - In this mode, the Internet connection can be terminated automatically after a specified inactivity period (**Max Idle Time**) and be re-established when you attempt to access the Internet again. If you want your Internet connection keeps active all the time, please enter "0" in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet access disconnects.
- **Connect Automatically** - The connection can be re-established automatically when it was down.
- **Connect Manually** - You can click the **Connect/Disconnect** button to connect/disconnect immediately. This mode also supports the **Max Idle Time** function as **Connect on Demand** mode. The Internet connection can be disconnected automatically after a specified inactivity period and re-established when you attempt to access the Internet again.

Click the **Connect** button to connect immediately. Click the **Disconnect** button to disconnect immediately.

Caution: Sometimes the connection cannot be terminated although you specify a time to Max Idle Time because some applications are visiting the Internet continually in the background.

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

5. If your ISP provides L2TP connection, please select **L2TP/Russia L2TP** option. And you should enter the following parameters (Figure 4-12):

WAN

WAN Connection Type: L2TP/Russia L2TP

User Name: username

Password: ••••••••

Connect Disconnect **Disconnected!**

☒ Dynamic IP ☐ Static IP

Server IP Address/Name:

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Gateway: 0.0.0.0

DNS: 0.0.0.0, 0.0.0.0

Internet IP Address: 0.0.0.0

Internet DNS: 0.0.0.0, 0.0.0.0

MTU Size (in bytes): 1460 (The default is 1460, do not change unless necessary.)

Max Idle Time: 15 minutes (0 means remain active at all times.)

Connection Mode: ☒ Connect on Demand ☐ Connect Automatically ☐ Connect Manually

Save

Figure 4-12

- **User Name/Password** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Dynamic IP/ Static IP** - Choose either as you are given by your ISP. Click the **Connect** button to connect immediately. Click the **Disconnect** button to disconnect immediately.
- **Server IP Address/Name** - Enter the Server IP Address/Name provided by your ISP. It can be IP address or Domain Name.
- **Connect on Demand** - You can configure the Router to disconnect from your Internet connection after a specified period of inactivity (**Max Idle Time**). If your Internet connection has been terminated due to inactivity, **Connect on Demand** enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, check the radio button. If you want your Internet connection to remain active at all times, enter 0 in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.
- **Connect Automatically** - Connect automatically after the Router is disconnected. To use this

option, check the radio button.

- **Connect Manually** - You can configure the Router to make it connect or disconnect manually. After a specified period of inactivity (**Max Idle Time**), the Router will disconnect from your Internet connection, and you will not be able to re-establish your connection automatically as soon as you attempt to access the Internet again. To use this option, check the radio button. If you want your Internet connection to remain active at all times, enter "0" in the **Max Idle Time** field. Otherwise, enter the number of minutes that you wish to have the Internet connecting last unless a new link is requested.

Caution: Sometimes the connection cannot be disconnected although you specify a time to **Max Idle Time**, because some applications are visiting the Internet continually in the background.

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

6. If your ISP provides PPTP connection, please select **PPTP/Russia PPTP** option. And you should enter the following parameters (Figure 4-13):

WAN

WAN Connection Type: PPTP/Russia PPTP

User Name: username

Password: ••••••••

Connect Disconnect Disconnected!

☒ Dynamic IP ☐ Static IP

Server IP Address/Name:

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Gateway: 0.0.0.0

DNS: 0.0.0.0, 0.0.0.0

Internet IP Address: 0.0.0.0

Internet DNS: 0.0.0.0, 0.0.0.0

MTU Size (in bytes): 1420 (The default is 1420, do not change unless necessary.)

Max Idle Time: 15 minutes (0 means remain active at all times.)

Connection Mode: ☒ Connect on Demand ☐ Connect Automatically ☐ Connect Manually

Save

Figure 4-13 PPTP Settings

- **User Name/Password** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Dynamic IP/ Static IP** - Choose either as you are given by your ISP and enter the ISP's IP address or the domain name.

If you choose static IP and enter the domain name, you should also enter the DNS assigned by your ISP. And click the **Save** button.

Click the **Connect** button to connect immediately. Click the **Disconnect** button to disconnect immediately.

- **Connect on Demand** - You can configure the Router to disconnect from your Internet connection after a specified period of inactivity (**Max Idle Time**). If your Internet connection has been terminated due to inactivity, **Connect on Demand** enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, check the radio button. If you want your Internet connection to remain active at all times, enter "0" in the **Max Idle Time** field. Otherwise, enter

the number of minutes you want to have elapsed before your Internet connection terminates.

- **Connect Automatically** - Connect automatically after the Router is disconnected. To use this option, check the radio button.
- **Connect Manually** - You can configure the Router to make it connect or disconnect manually. After a specified period of inactivity (**Max Idle Time**), the Router will disconnect from your Internet connection, and you will not be able to re-establish your connection automatically as soon as you attempt to access the Internet again. To use this option, click the radio button. If you want your Internet connection to remain active at all times, enter "0" in the **Max Idle Time** field. Otherwise, enter the number in minutes that you wish to have the Internet connecting last unless a new link is requested.

Caution: Sometimes the connection cannot be disconnected although you specify a time to **Max Idle Time** because some applications are visiting the Internet continually in the background.

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

 Note:

If you don't know how to choose the appropriate connection type, click the **Detect** button to allow the Router to automatically search your Internet connection for servers and protocols. The connection type will be reported when an active Internet service is successfully detected by the Router. This report is for your reference only. To make sure the connection type your ISP provides, please refer to the ISP. The various types of Internet connections that the Router can detect are as follows:

- **PPPoE** - Connections which use PPPoE that requires a user name and password.
- **Dynamic IP** - Connections which use dynamic IP address assignment.
- **Static IP** - Connections which use static IP address assignment.

The Router can not detect PPTP/L2TP/BigPond connections with your ISP. If your ISP uses one of these protocols, then you must configure your connection manually.

4.6.2 MAC Clone

Choose menu "**Network** → **MAC Clone**", you can configure the MAC address of the WAN on the screen below, Figure 4-14:

MAC Clone	
WAN MAC Address:	00-0A-EB-13-09-1A
Your PC's MAC Address:	40-61-86-CF-20-7A
	Restore Factory MAC
	Clone MAC Address
Save	

Figure 4-14 MAC Address Clone

Some ISPs require that you register the MAC Address of your adapter. Changes are rarely needed here.

- **WAN MAC Address** - This field displays the current MAC address of the WAN port. If your ISP requires you to register the MAC address, please enter the correct MAC address into this field in XX-XX-XX-XX-XX-XX format (X is any hexadecimal digit).
- **Your PC's MAC Address** - This field displays the MAC address of the PC that is managing the Router. If the MAC address is required, you can click the **Clone MAC Address To** button and this MAC address will fill in the **WAN MAC Address** field.

Click **Restore Factory MAC** to restore the MAC address of WAN port to the factory default value.

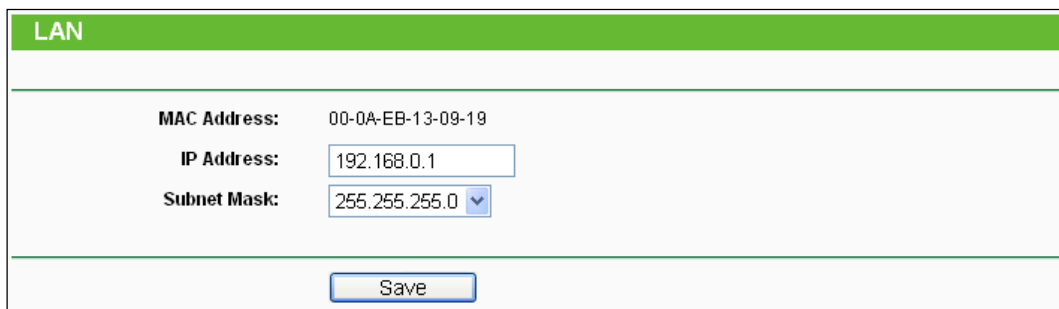
Click the **Save** button to save your settings.

 Note:

Only the PC on your LAN can use the MAC Address Clone function.

4.6.3 LAN

Choose menu “**Network** → **LAN**”, you can configure the IP parameters of the LAN on the screen as below.



LAN	
MAC Address:	00-0A-EB-13-09-19
IP Address:	192.168.0.1
Subnet Mask:	255.255.255.0
Save	

Figure 4-15 LAN

- **MAC Address** - The physical address of the Router, as seen from the LAN. The value can't be changed.
- **IP Address** - Enter the IP address of your Router or reset it in dotted-decimal notation (factory default: 192.168.0.1).
- **Subnet Mask** - An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask.

 Note:

- 1) If you change the IP Address of LAN, you must use the new IP Address to log in the Router.
- 2) If the new LAN IP Address you set is not in the same subnet, the IP Address pool of the DHCP server will change accordingly at the same time, while the Virtual Server and DMZ Host will

not take effect until they are re-configured.

4.7 Wireless

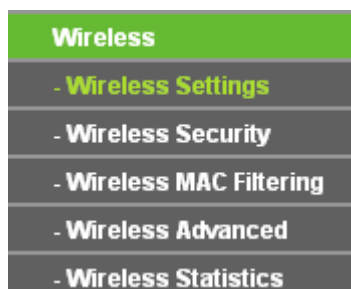


Figure 4-16 Wireless menu

There are five submenus under the Wireless menu (shown in Figure 4-16): **Wireless Settings**, **Wireless Security**, **Wireless MAC Filtering**, **Wireless Advanced** and **Wireless Statistics**. Click any of them, and you will be able to configure the corresponding function.

4.7.1 Wireless Settings

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

4.7.1.1. Wireless Settings on Router Mode

If you select **Standard Wireless Router** mode in Figure 4-5, the Wireless Settings page will display as Figure 4-17.

Figure 4-17 Wireless Settings

- **Wireless Network Name (also called the SSID)** - Enter a value of up to 32 characters. The same name of SSID (Service Set Identification) must be assigned to all wireless devices in your network. Considering your wireless network security, the default SSID is set to be TP-LINK_XXXXXXX (XXXXXX indicates the last unique six numbers of each Router's MAC address). This value is case-sensitive. For example, *TEST* is NOT the same as *test*.
- **Mode** - Select the desired mode. The default setting is 11bgn mixed.
 - 11bg mixed** - Select if you are using both 802.11b and 802.11g wireless clients.
 - 11bgn mixed** - Select if you are using a mix of 802.11b, 11g, and 11n wireless clients.

It is strongly recommended that you set the Mode to **802.11b&g&n**, and all of 802.11b, 802.11g, and 802.11n wireless stations can connect to the Router.
- **Channel width** - Select the channel width from the pull-down list. The default setting is Auto, which can automatically adjust the channel width for your clients.

 Note:

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

- **Channel** - This field determines which operating frequency will be used. The default channel is set to 6. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- **Enable Wireless Router Radio** - The wireless radio of the Router can be enabled or disabled to allow wireless stations access. If enabled, the wireless stations will be able to access the Router. Otherwise, wireless stations will not be able to access the Router.
- **Enable SSID Broadcast** - If you select the Enable SSID Broadcast checkbox, the wireless router will broadcast its name (SSID) on the air.
- **Enable WDS Bridging** - You can select this to enable WDS Bridging, with this function, the Router can bridge two or more WLANs. NOTE: If this checkbox is selected, you had better make sure the following settings are correct.

- **SSID (to be bridged)** - The SSID of the AP your Router is going to connect to as a client. You can also use the survey function to select the SSID to join.
- **BSSID (to be bridged)** - The BSSID of the AP your Router is going to connect to as a client. You can also use the survey function to select the BSSID to join.
- **Survey** - Click this button, you can survey the AP which runs nearby.
- **WDS Mode** – WDS1 3-address corresponds to frame format, WDS2 corresponds to 4-address frame format.
- **Key type** - This option should be chosen according to the AP's security configuration. It is recommended that the security type is the same as your AP's security type.
- **WEP Index** - This option should be chosen if the key type is WEP (ASCII) or WEP (HEX). It indicates the index of the WEP key.
- **Auth Type** - This option should be chosen if the key type is WEP (ASCII) or WEP (HEX). It indicates the authorization type of the Root AP.
- **Password** - If the AP your Router is going to connect needs password, you need to fill the password in this blank.

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

 Note:

- 1) The operating distance or range of your wireless connection varies significantly based on the physical placement of the Router. For best results, place your Router.
 - Near the center of the area in which your wireless stations will operate.
 - In an elevated location such as a high shelf.
 - Away from the potential sources of interference, such as PCs, microwaves, and cordless phones.
 - With the Antenna in the upright position.
 - Away from large metal surfaces.
- 2) Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the Router.

4.7.1.2. Wireless Settings on WISP Client Router Mode

If you select **WISP Client Router** mode in Figure 4-5, the Wireless Settings page will display as Figure 4-18.

Figure 4-18 Wireless Settings

- **SSID** - The SSID of the AP your Router is going to connect to as a client. You can also use the search function to select the SSID to join.
- **BSSID** - The BSSID of the AP your Router is going to connect to as a client. You can also use the search function to select the BSSID to join.
- **Survey** - Click this button, you can search the AP which runs nearby.
- **Key type** - This option should be chosen according to the AP's security configuration. It is recommended that the security type is the same as your AP's security type.
- **WEP Index** - This option should be chosen if the key type is WEP (ASCII) or WEP (HEX). It indicates the index of the WEP key.
- **Auth type** - This option should be chosen if the key type is WEP (ASCII) or WEP (HEX). It indicates the authorization type of the Root AP.
- **Password** - If the AP your Router is going to connect needs password, you need to fill the password in this blank.
- **Local SSID** - Enter a value of up to 32 characters. The same Name (SSID) must be assigned to all wireless devices in your network.
- **Enable Wireless Router Radio** - The wireless radio of the Router can be enabled or disabled to allow wireless stations access. If enabled, the wireless stations will be able to access the

Router. Otherwise, wireless stations will not be able to access the Router and you cannot access to the WISP.

- **Enable SSID Broadcast** - If you select the **Enable SSID Broadcast** checkbox, the wireless router will broadcast its name (SSID) on the air.
- **Disable Local Wireless Access** - If you select the **Disable Local Wireless Access** checkbox, the wireless router will disable local wireless access; other stations will not be able to access the Router by wireless.

Click **Survey** button on the Wireless page shown as Figure 4-18, and then AP List page will appear, as shown in Figure 4-19. Find the SSID of the Access Point you want to access, and click **Connect** in the corresponding row. For example, the desired item is selected. The target network's SSID will be automatically filled into the corresponding box which is shown as the Figure 4-20.

AP List						
AP Count: 49						
ID	BSSID	SSID	Signal	Channel	Security	Choose
1	00-0A-EB-0C-26-42	TP-LINK_2642	84dB	11	WPA-PSK/WPA2-PSK	Connect
2	00-0A-EB-13-09-19	TP-LINK_0919	74dB	1	WPA2-PSK	Connect
3	80-F6-2E-0A-A3-62	and-Business	69dB	6	None	Connect

Figure 4-19 AP List

Quick Setup - Wireless	
Client Setting	
SSID:	TP-LINK_2642
BSSID:	00-0A-EB-0C-26-42 Example:00-1D-0F-11-22-33
	Survey
	Key type is selected.
Key type:	WPA-PSK/WPA2-PSK
WEP Index:	1
Auth type:	open
Password:	
AP Setting	
Local SSID:	TP-LINK_7B00
Wireless Security Mode:	Most Secure(WPA/WPA2-PSK)
Wireless Password:	12345670
You can enter ASCII or Hexadecimal characters. For Hexadecimal, the length should be between 8 and 64 characters; for ASCII, the length should be between 8 and 63 characters. For good security it should be of ample length and should not be a commonly known phrase.	
Back Next	

Figure 4-20

 Note:

If you know the SSID of the desired AP, you can also input it into the field "Wireless Name of WISP Station" manually.

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

 Note:

- 1) The operating distance or range of your wireless connection varies significantly based on the physical placement of the Router. For best results, place your Router.
 - Near the center of the area in which your wireless stations will operate.
 - In an elevated location such as a high shelf.
 - Away from the potential sources of interference, such as PCs, microwaves, and cordless phones.
 - With the Antenna in the upright position.
 - Away from large metal surfaces.
- 2) Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the Router.

4.7.2 Wireless Security

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

There are five wireless security modes supported by the Router: WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), WPA2 (Wi-Fi Protected Access 2), WPA-PSK (Pre-Shared Key), WPA2-PSK (Pre-Shared Key).

Wireless Security

☐ Disable Security

☒ WPA/WPA2 - Personal(Recommended)

Version: Automatic(Recommended) ▼

Encryption: Automatic(Recommended) ▼

Wireless Password: 12345670
(You can enter ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 64.)

Group Key Update Period: 0 Seconds (Keep it default if you are not sure, minimum is 30, 0 means no update)

☐ WPA/WPA2 - Enterprise

Version: Automatic ▼

Encryption: Automatic ▼

Radius Server IP:

Radius Port: 1812 (1-65535, 0 stands for default port 1812)

Radius Password:

Group Key Update Period: 0 (In second, minimum is 30, 0 means no update)

☐ WEP

Type: Automatic ▼

WEP Key Format: Hexadecimal ▼

Key Selected	WEP Key	Key Type
Key 1: ☐		Disabled ▼
Key 2: ☐		Disabled ▼
Key 3: ☐		Disabled ▼
Key 4: ☐		Disabled ▼

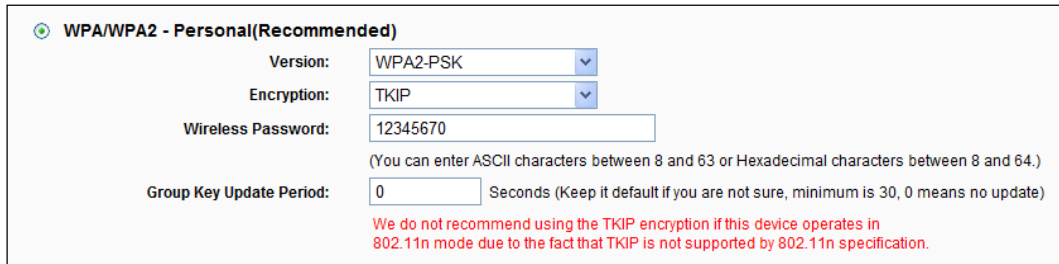
Save

Figure 4-21 Wireless Security

- **Disable Security** - If you do not want to use wireless security, check this radio button. But it's strongly recommended to choose one of the following modes to enable security.
- **WPA-PSK/WPA2-PSK – Personal (Recommended)** - It's the WPA/WPA2 authentication type based on pre-shared passphrase.
 - **Version** - you can choose the version of the WPA-PSK security on the drop-down list. The default setting is **Automatic**, which can select **WPA-PSK** (Pre-shared key of WPA) or **WPA2-PSK** (Pre-shared key of WPA) automatically based on the wireless station's capability and request.
 - **Encryption** - When **WPA-PSK** or **WPA** is set as the Authentication Type, you can select either **Automatic**, or **TKIP** or **AES** as Encryption.

Note:

If you check the **WPA-PSK/WPA2-PSK – Personal (Recommended)** radio button and choose TKIP encryption, you will find a notice in red as shown in Figure 4-22.



WPA/WPA2 - Personal(Recommended)

Version:

Encryption:

Wireless Password:

(You can enter ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 64.)

Group Key Update Period: Seconds (Keep it default if you are not sure, minimum is 30, 0 means no update)

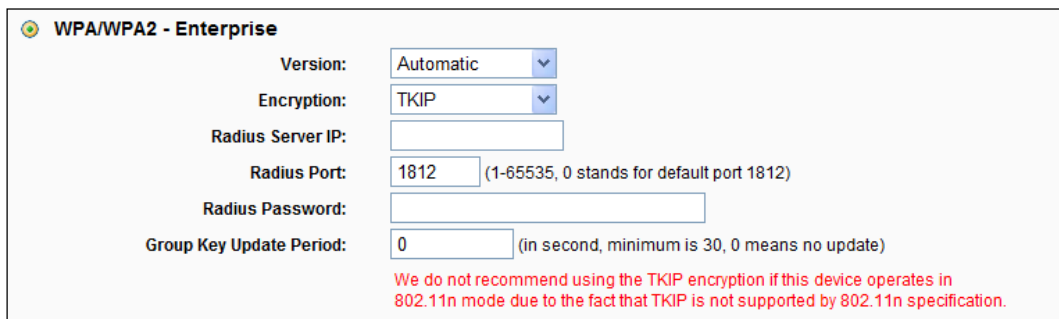
We do not recommend using the TKIP encryption if this device operates in 802.11n mode due to the fact that TKIP is not supported by 802.11n specification.

Figure 4-22

- **PSK Password** - You can enter ASCII characters between 8 and 63 characters or 8 to 64 Hexadecimal characters.
 - **Group Key Update Period** - Specify the group key update interval in seconds. The value should be 30 or above. Enter 0 to disable the update.
- **WPA /WPA2 – Enterprise** - It's based on Radius Server.
- **Version** - you can choose the version of the WPA security on the drop-down list. The default setting is **Automatic**, which can select **WPA** (Wi-Fi Protected Access) or **WPA2** (WPA version 2) automatically based on the wireless station's capability and request.
 - **Encryption** - You can select either **Automatic**, or **TKIP** or **AES**.

 Note:

If you check the **WPA /WPA2 – Enterprise** radio button and choose TKIP encryption, you will find a notice in red as shown in Figure 4-23.



WPA/WPA2 - Enterprise

Version:

Encryption:

Radius Server IP:

Radius Port: (1-65535, 0 stands for default port 1812)

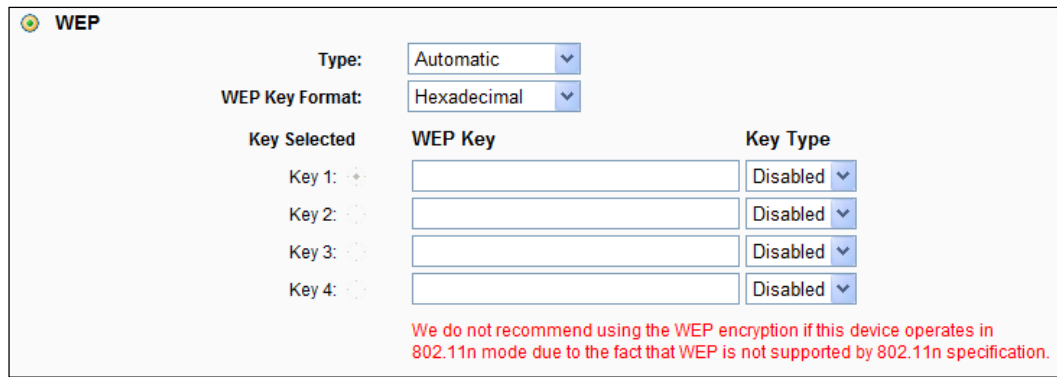
Radius Password:

Group Key Update Period: (in second, minimum is 30, 0 means no update)

We do not recommend using the TKIP encryption if this device operates in 802.11n mode due to the fact that TKIP is not supported by 802.11n specification.

Figure 4-23

- **Radius Server IP** - Enter the IP address of the Radius server.
 - **Radius Port** - Enter the port number of the Radius server.
 - **Radius Password** - Enter the password for the Radius server.
 - **Group Key Update Period** - Specify the group key update interval in seconds. The value should be 30 or above. Enter 0 to disable the update.
- **WEP** - It is based on the IEEE 802.11 standard. If you check this radio button, you will find a notice in red as show in Figure 4-24.



WEP

Type: Automatic ▼

WEP Key Format: Hexadecimal ▼

Key Selected	WEP Key	Key Type
Key 1: ☒		Disabled ▼
Key 2: ☐		Disabled ▼
Key 3: ☐		Disabled ▼
Key 4: ☐		Disabled ▼

We do not recommend using the WEP encryption if this device operates in 802.11n mode due to the fact that WEP is not supported by 802.11n specification.

Figure 4-24

- **Type** - you can choose the type for the WEP security on the drop-down list. The default setting is **Automatic**, which can select **Shared Key** or **Open System** authentication type automatically based on the wireless station's capability and request.
- **WEP Key Format** - **Hexadecimal** and **ASCII** formats are provided here. **Hexadecimal** format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length. **ASCII** format stands for any combination of keyboard characters in the specified length.
- **WEP Key** - Select which of the four keys will be used and enter the matching WEP key that you create. Make sure these values are identical on all wireless stations in your network.
- **Key Type** - You can select the WEP key length (64-bit, or 128-bit, or 152-bit.) for encryption. "Disabled" means this WEP key entry is invalid.
 - 64-bit** - You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not promoted) or 5 ASCII characters.
 - 128-bit** - You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not promoted) or 13 ASCII characters.
 - 152-bit** - You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not promoted) or 16 ASCII characters.

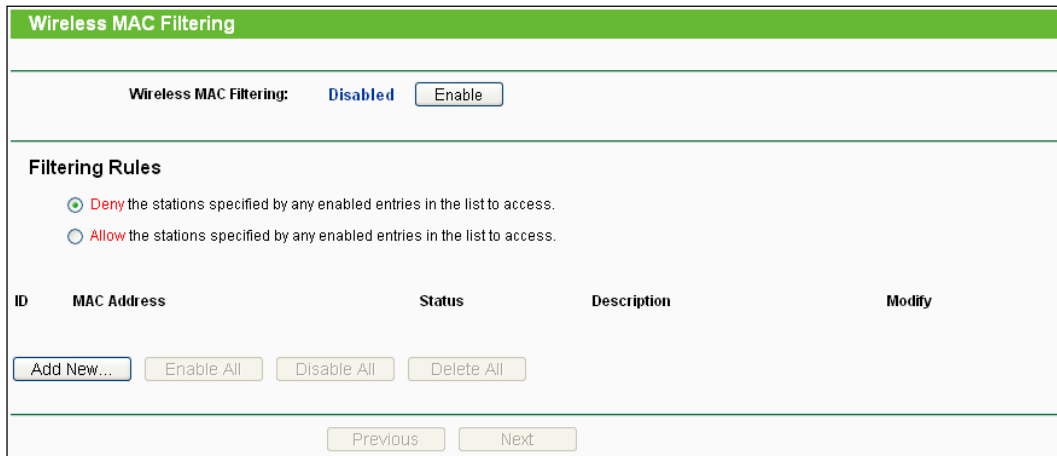
 Note:

If you do not set the key, the wireless security function is still disabled even if you have selected Shared Key as Authentication Type.

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

4.7.3 Wireless MAC Filtering

Choose menu "**Wireless** → **MAC Filtering**", you can control the wireless access by configuring the **Wireless MAC Filtering** function, shown in Figure 4-25.



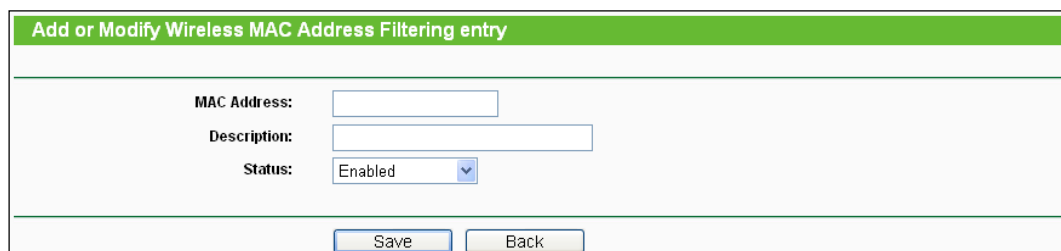
The screenshot shows the 'Wireless MAC Filtering' configuration page. At the top, there's a green header bar with the title. Below it, the status 'Wireless MAC Filtering: Disabled' is shown with an 'Enable' button. Under 'Filtering Rules', there are two radio buttons: 'Deny' (selected) and 'Allow'. Below this is a table with columns: ID, MAC Address, Status, Description, and Modify. At the bottom of the table area, there are buttons: 'Add New...', 'Enable All', 'Disable All', and 'Delete All'. At the very bottom, there are 'Previous' and 'Next' navigation buttons.

Figure 4-25 Wireless MAC Filtering

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

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

To Add a Wireless MAC Address filtering entry, click the **Add New...** button. The "**Add or Modify Wireless MAC Address Filtering entry**" page will appear, shown in Figure 4-26:



The screenshot shows the 'Add or Modify Wireless MAC Address Filtering entry' page. It has a green header bar with the title. Below it, there are three input fields: 'MAC Address:', 'Description:', and 'Status:'. The 'Status' field is a dropdown menu currently set to 'Enabled'. At the bottom, there are 'Save' and 'Back' buttons.

Figure 4-26 Add or Modify Wireless MAC Address Filtering entry

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

1. Enter the appropriate MAC Address into the **MAC Address** field. The format of the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). For example: 00-0A-EB-B0-00-0B.
2. Give a simple description for the wireless station in the **Description** field. For example: Wireless station A.
3. Select **Enabled** or **Disabled** for this entry on the **Status** drop-down list.
4. Click the **Save** button to save this entry.

To modify or delete an existing entry:

1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.

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

Click the **Enable All** button to make all entries enabled

Click the **Disable All** button to make all entries disabled.

Click the **Delete All** button to delete all entries.

Click the **Next** button to go to the next page.

Click the **Previous** button to return to the previous page.

For example: If you desire that the wireless station A with MAC address 00-0A-EB-B0-00-0B and the wireless station B with MAC address 00-0A-EB-00-07-5F are able to access the Router, but all the other wireless stations cannot access the Router, you can configure the **Wireless MAC Address Filtering** list by following these steps:

1. Click the **Enable** button to enable this function.
2. Select the radio button “Allow the stations specified by any enabled entries in the list to access” for **Filtering Rules**.
3. Delete all or disable all entries if there are any entries already.
4. Click the **Add New...** button.
 - 1) Enter the MAC address 00-0A-EB-B0-00-0B/00-0A-EB-00-07-5F in the **MAC Address** field.
 - 2) Enter wireless station A/B in the **Description** field.
 - 3) Select **Enabled** in the **Status** drop-down list.
 - 4) Click the **Save** button.
 - 5) Click the **Back** button.

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

Filtering Rules				
☐ Deny the stations specified by any enabled entries in the list to access.				
☒ Allow the stations specified by any enabled entries in the list to access.				
ID	MAC Address	Status	Description	Modify
1	00-0A-EB-B0-00-0B	Enabled	wireless station A	Modify Delete
2	00-0A-EB-00-07-5F	Enabled	wireless station B	Modify Delete

4.7.4 Wireless Advanced

Choose menu “**Wireless → Wireless Advanced**”, you can configure the advanced settings of your wireless network.

Wireless Advanced

Transmit Power: High

Beacon Interval: 100 (40-1000)

RTS Threshold: 2346 (256-2346)

Fragmentation Threshold: 2346 (256-2346)

DTIM Interval: 1 (1-255)

☒ Enable WMM

☒ Enable Short GI

☐ Enable AP Isolation

Save

Figure 4-27 Wireless Advanced

- **Transmit Power** - Here you can specify the transmit power of Router. You can select High, Middle or Low which you would like. High is the default setting and is recommended.
- **Beacon Interval** - Enter a value between 40-1000 milliseconds for Beacon Interval here. The beacons are the packets sent by the Router to synchronize a wireless network. Beacon Interval value determines the time interval of the beacons. The default value is 100.
- **RTS Threshold** - Here you can specify the RTS (Request to Send) Threshold. If the packet is larger than the specified RTS Threshold size, the Router will send RTS frames to a particular receiving station and negotiate the sending of a data frame. The default value is 2346.
- **Fragmentation Threshold** - This value is the maximum size determining whether packets will be fragmented. Setting the Fragmentation Threshold too low may result in poor network performance because of excessive packets. 2346 is the default setting and is recommended.
- **DTIM Interval** - This value determines the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. You can specify the value between 1-255 Beacon Intervals. The default value is 1, which indicates the DTIM Interval is the same as Beacon Interval.
- **Enable WMM** - WMM function can guarantee the packets with high-priority messages being transmitted preferentially. It is strongly recommended.
- **Enable Short GI** - This function is recommended for it will increase the data capacity by reducing the guard interval time.
- **Enabled AP Isolation** - This function can isolate wireless stations on your network from each other. Wireless devices will be able to communicate with the Router but not with each other. To use this function, check this box. AP Isolation is disabled by default.

Note:

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

4.7.5 Wireless Statistics

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

Wireless Statistics					
Current Connected Wireless Stations numbers: 1 Refresh					
ID	MAC Address	Current Status	Received Packets	Sent Packets	Configure
1	A8-26-D9-EE-3F-84	WPA2-PSK	638	557	Deny
Previous Next					

Figure 4-28 Wireless Statistics

- **MAC Address** - The connected wireless station's MAC address.
- **Current Status** - The connected wireless station's running status, one of **STA-AUTH/ STA-ASSOC/ STA-JOINED/ WPA/ WPA-PSK/ WPA2/ WPA2-PSK/ AP-UP/ AP-DOWN/ Disconnected**.
- **Received Packets** - Packets received by the station.
- **Sent Packets** - Packets sent by the station.
- **Configure** - The button is used for loading the item to the Wireless MAC Filtering list.
 - **Deny** - if the Wireless MAC Filtering function enable, deny the station to access.
 - **Allow** - if the Wireless MAC Filtering function enable, allow the station to access.

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

If the numbers of connected wireless stations go beyond one page, click the **Next** button to go to the next page and click the **Previous** button to return the previous page.

Note:

This page will be refreshed automatically every 5 seconds.

4.8 Guest Network

Guest Network
- Wireless Settings

There are two submenus under the Guest Network menu : **Wireless Settings**. Click either of them, and you will be able to configure the corresponding functions.

4.8.1 Wireless Settings

Choose menu “**Guest Network** → **Wireless Settings**”, you can configure the Guest Network Wireless Settings on the page as shown in Figure 4-44.

Guest Network Wireless Settings

Access And Bandwidth Control

Allow Guest To Access My Local Network: ☐

Enable Guest Network Bandwidth Control: ☐

Egress Bandwidth For Guest Network: 256 Kbps (Range:1~100000)

Ingress Bandwidth For Guest Network: 1024 Kbps (Range:1~100000)

Wireless

Guest Network: ☐

Network Name: TP-LINK_GUEST_7B00 (Also called the SSID)

Wireless Security: WPA/WPA2-Personal

Version: WPA2-PSK

Encryption: AES

PSK Password: 12345670
(You can enter ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 64.)

Group Key Update Period: 0 Seconds (Keep it default if you are not sure, minimum is 30, 0 means no update)

Access Time: Schedule can not be connected.

☒ Everyday ☐ Select Days

☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat ☐ Sun

☒ All day-24 Hours

Start Time: (HHMM)

End Time: (HHMM)

Save

- **Allow Guest To Access My Local Network** - If enabled, guests can communicate with hosts.
- **Enable Guest Network Bandwidth Control** - If enabled, the Guest Network Bandwidth Control rules will take effect.
- **Egress Bandwidth For Guest Network** - The upload speed through the WAN port for Guest Network.
- **Ingress Bandwidth For Guest Network** - The download speed through the WAN port for Guest Network.
- **Guest Network (2.4G/5G)** - Enabled or disable the Guest Network function here.
- **Network Name** - Enter a value of up to 32 characters. The same Name (SSID) must be assigned to all wireless devices in your Guest Network.
- **Wireless Security** - You can configure the security of Guest Network here.
- **Access Time** - During this time the wireless stations could accessing the AP.

Note:

The range of bandwidth for Guest Network is calculated according to the setting of Bandwidth Control on the page “Bandwidth Control->Control Settings”.

4.9 DHCP

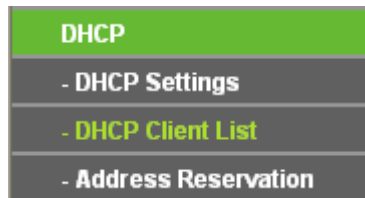


Figure 4-29 The DHCP menu

There are three submenus under the DHCP menu (shown in Figure 4-29): **DHCP Settings**, **DHCP Client List** and **Address Reservation**. Click any of them, and you will be able to configure the corresponding function.

4.9.1 DHCP Settings

Choose menu “**DHCP → DHCP Settings**”, you can configure the DHCP Server on the page as shown in Figure 4-30. The Router is set up by default as a DHCP (Dynamic Host Configuration Protocol) server, which provides the TCP/IP configuration for all the PC(s) that are connected to the Router on the LAN.

 A screenshot of a web form titled "DHCP Settings". The form has a green header bar. Below the header, there are several configuration options:

- DHCP Server:** Two radio buttons, "Disable" and "Enable". The "Enable" button is selected.
- Start IP Address:** A text input field containing "192.168.0.100".
- End IP Address:** A text input field containing "192.168.0.199".
- Address Lease Time:** A text input field containing "120", followed by the text "minutes (1~2880 minutes, the default value is 120)".
- Default Gateway:** A text input field containing "192.168.0.1", followed by the text "(Optional)".
- Default Domain:** A text input field, followed by the text "(Optional)".
- Primary DNS:** A text input field containing "0.0.0.0", followed by the text "(Optional)".
- Secondary DNS:** A text input field containing "0.0.0.0", followed by the text "(Optional)".

 At the bottom of the form is a "Save" button.

Figure 4-30 DHCP Settings

- **DHCP Server - Enable or Disable** the DHCP server. If you disable the Server, you must have another DHCP server within your network or else you must configure the computer manually.
- **Start IP Address** - Specify an IP address for the DHCP Server to start with when assigning IP addresses. 192.168.0.100 is the default start address.
- **End IP Address** - Specify an IP address for the DHCP Server to end with when assigning IP addresses. 192.168.0.199 is the default end address.
- **Address Lease Time** - The **Address Lease Time** is the amount of time a network user will be allowed connection to the Router with their current dynamic IP Address. Enter the amount

of time in minutes and the user will be "leased" this dynamic IP Address. After the time is up, the user will be automatically assigned a new dynamic IP address. The range of the time is 1 ~ 2880 minutes. The default value is 120 minutes.

- **Default Gateway** - (Optional.) It is suggested to input the IP address of the LAN port of the Router. The default value is 192.168.0.1.
- **Default Domain** - (Optional.) Input the domain name of your network.
- **Primary DNS** - (Optional.) Input the DNS IP address provided by your ISP or consult your ISP.
- **Secondary DNS** - (Optional.) Input the IP address of another DNS server if your ISP provides two DNS servers.

 Note:

To use the DHCP server function of the Router, you must configure all computers on the LAN as "Obtain an IP Address automatically".

4.9.2 DHCP Client List

Choose menu "**DHCP** → **DHCP Client List**", you can view the information about the clients attached to the Router in the screen as shown in Figure 4-31.

DHCP Client List				
ID	Client Name	MAC Address	Assigned IP	Lease Time
1	viola	40-61-86-CF-20-7A	192.168.0.100	01:29:35
Refresh				

Figure 4-31 DHCP Clients List

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

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

4.9.3 Address Reservation

Choose menu "**DHCP** → **Address Reservation**", you can view and add a reserved address for clients via the next screen (shown in Figure 4-32). When you specify a reserved IP address for a PC on the LAN, that PC will always receive the same IP address each time when it accesses the DHCP server. Reserved IP addresses should be assigned to the servers that require permanent IP

settings.

Address Reservation				
ID	MAC Address	Reserved IP Address	Status	Modify
Add New... Enable All Disable All Delete All				
Previous Next				

Figure 4-32 Address Reservation

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

To Reserve an IP address:

1. Click the **Add New...** button. Then Figure 4-33 will pop up.
2. Enter the MAC address (in XX-XX-XX-XX-XX-XX format.) and IP address (in dotted-decimal notation) of the computer for which you want to reserve an IP address.
3. Click the **Save** button.

Add or Modify an Address Reservation Entry

MAC Address:

Reserved IP Address:

Status: Enabled ▼

Figure 4-33 Add or Modify an Address Reservation Entry

To modify or delete an existing entry:

1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click the **Save** button.

Click the **Enable/Disable All** button to make all entries enabled/disabled

Click the **Delete All** button to delete all entries.

Click the **Next** button to go to the next page and Click the **Previous** button to return the previous page.

4.10 Forwarding

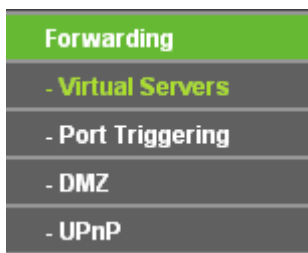


Figure 4-34 The Forwarding menu

There are four submenus under the Forwarding menu (shown in Figure 4-34): **Virtual Servers**, **Port Triggering**, **DMZ** and **UPnP**. Click any of them, and you will be able to configure the corresponding function.

4.10.1 Virtual Servers

Choose menu "**Forwarding** → **Virtual Servers**", you can view and add virtual servers in the screen as shown in Figure 4-35. 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 be changed when using the DHCP function.

Virtual Servers						
ID	Service Port	Internal Port	IP Address	Protocol	Status	Modify
1	11130	11120	192.168.0.198	ALL	Enabled	Modify Delete
Add New... Enable All Disable All Delete All						
Previous Next						

Figure 4-35 Virtual Servers

- **Service Port** - The numbers of External Ports. You can type a service port or a range of service ports (in XXX – YYY format, XXX is the start port number, YYY is the end port number).
- **Internal Port** - The Internal Service Port number of the PC running the service application. You can leave it blank if the **Internal Port** is the same as the **Service Port**, or enter a specific port number when **Service Port** is a single one.
- **IP Address** - The IP Address of the PC providing the service application.
- **Protocol** - The protocol used for this application, either **TCP**, **UDP**, or **All** (all protocols supported by the Router).
- **Status** - The status of this entry, either **Enabled** or **Disabled**.

To set up a virtual server entry:

1. Click the **Add New...** button, the next screen will pop-up as shown in Figure 4-36.
2. Select the service port you want to use from the **Common Service Port** list. If the **Common Service Port** list does not have the service that you want to use, type the service port number or service port range in the **Service Port** box.
3. Type the IP Address of the computer in the **IP Address** box.
4. Select the protocol used for this application, either **TCP**, **UDP**, or **All**.
5. Select the **Enable** to enable the virtual server.
6. Click the **Save** button.

Figure 4-36 Add or Modify a Virtual Server Entry

Note:

If your computer or server has more than one type of available service, please select another service, and enter the same IP Address for that computer or server.

To modify or delete an existing entry:

1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click the **Save** button.

Click the **Enable/Disable All** button to make all entries enabled/disabled.

Click the **Delete All** button to delete all entries.

Click the **Next** button to go to the next page and click the **Previous** button to return the previous page.

Note:

If you set the service port of the virtual server as 80, you must set the Web management port on “**Security** → **Remote Management**” page to be any other value except 80 such as 8080. Otherwise there will be a conflict to disable the virtual server.

4.10.2 Port Triggering

Choose menu “**Forwarding** → **Port Triggering**”, you can view and add port triggering in the screen as shown in Figure 4-37. Some applications require multiple connections, like Internet games, video conferencing, Internet calling and so on. These applications cannot work with a pure NAT Router. Port Triggering is used for some of these applications that can work with an NAT Router.

Port Triggering						
ID	Trigger Port	Trigger Protocol	Incoming Ports	Incoming Protocol	Status	Modify
Add New... Enable All Disable All Delete All						
Previous Next						

Figure 4-37 Port Triggering

Once the Router is configured, the operation is as follows:

1. A local host makes an outgoing connection using a destination port number defined in the Trigger Port field.
 2. The Router records this connection, opens the incoming port or ports associated with this entry in the Port Triggering table, and associates them with the local host.
 3. When necessary, the external host will be able to connect to the local host using one of the ports defined in the **Incoming Ports** field.
- **Trigger Port** - The port for outgoing traffic. An outgoing connection using this port will trigger this rule.
 - **Trigger Protocol** - The protocol used for Trigger Ports, either **TCP**, **UDP**, or **All** (all protocols supported by the Router).
 - **Incoming Ports** - The port or port range used by the remote system when it responds to the outgoing request. A response using one of these ports will be forwarded to the PC that triggered this rule. You can input at most 5 groups of ports (or port sections). Every group of ports must be set apart with ",". For example, 2000-2038, 2050-2051, 2085, 3010-3030.
 - **Incoming Protocol** - The protocol used for Incoming Ports Range, either **TCP** or **UDP**, or **ALL** (all protocols supported by the Router).
 - **Status** - The status of this entry, either **Enabled** or **Disabled**.

To add a new rule, follow the steps below.

1. Click the **Add New...** button, the next screen will pop-up as shown in Figure 4-38.
2. Select a common application from the **Common Applications** drop-down list, then the **Trigger Port** field and the **Incoming Ports** field will be automatically filled. If the **Common Applications** do not have the application you need, enter the **Trigger Port** and the **Incoming Ports** manually.

3. Select the protocol used for Trigger Port from the **Trigger Protocol** drop-down list, either **TCP**, **UDP**, or **All**.
4. Select the protocol used for Incoming Ports from the **Incoming Protocol** drop-down list, either **TCP** or **UDP**, or **All**.
5. Select **Enable** in **Status** field.
6. Click the **Save** button to save the new rule.

Figure 4-38 Add or Modify a Port Triggering Entry

To modify or delete an existing entry:

1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click the **Save** button.

Click the **Enable All** button to make all entries enabled

Click the **Disable All** button to make all entries disabled.

Click the **Delete All** button to delete all entries

Note:

- 1) When the trigger connection is released, the corresponding opening ports will be closed.
- 2) Each rule is allowed to be used only by one host on LAN synchronously. The trigger connection of other hosts on LAN will be refused.
- 3) Incoming Ports cannot overlap each other.

4.10.3 DMZ

Choose menu "**Forwarding** → **DMZ**", you can view and configure DMZ host in the screen as shown in Figure 4-39. The DMZ host feature allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing. 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 be changed when using the DHCP function.

Figure 4-39 DMZ

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

1. Check the **Enable** radio button.
2. Enter the IP Address of a local host in the **DMZ Host IP Address** field.
3. Click the **Save** button.

Note:

After you set the DMZ host, the firewall related to the host will not work.

4.10.4 UPnP

Choose menu “**Forwarding** → **UPnP**”, you can view the information about **UPnP** (Universal Plug and Play) in the screen as shown in Figure 4-40. The UPnP feature allows the devices, such as Internet computers, to access the local host resources or devices as needed. UPnP devices can be automatically discovered by the UPnP service application on the LAN.

ID	App Description	External Port	Protocol	Internal Port	IP Address	Status
1	BitComet(192.168.0.100:23959)	23959	TCP	23959	192.168.0.100	Enabled
2	BitComet(192.168.0.100:23959)	23959	UDP	23959	192.168.0.100	Enabled

Figure 4-40 UPnP

- **Current UPnP Status** - UPnP can be enabled or disabled by clicking the **Enable** or **Disable** button.
- **Current UPnP Settings List** - This table displays the current UPnP information.
 - **App Description** - The description provided by the application in the UPnP request.

- **External Port** - The external port the Router opens for the application.
- **Protocol** - The type of protocol the Router opens for the application.
- **Internal Port** - The Internal port the Router opens for local host.
- **IP Address** - The IP address of the UPnP device that is currently accessing the Router.
- **Status** - The status of the port is displayed here. "Enabled" means that the port is still active. Otherwise, the port is inactive.

Click **Refresh** to update the Current UPnP Settings List.

4.11 Security



Figure 4-41 The Security menu

There are four submenus under the Security menu as shown in Figure 4-41: **Basic Security**, **Advanced Security**, **Local Management** and **Remote Management**. Click any of them, and you will be able to configure the corresponding function.

4.11.1 Basic Security

Choose menu "**Security** → **Basic Security**", you can configure the basic security in the screen as shown in Figure 4-42.

Basic Security	
Firewall	
SPI Firewall:	☒ Enable ☐ Disable
VPN	
PPTP Passthrough:	☒ Enable ☐ Disable
L2TP Passthrough:	☒ Enable ☐ Disable
IPSec Passthrough:	☒ Enable ☐ Disable
ALG	
FTP ALG:	☒ Enable ☐ Disable
TFTP ALG:	☒ Enable ☐ Disable
H323 ALG:	☒ Enable ☐ Disable
RTSP ALG:	☒ Enable ☐ Disable
Save	

Figure 4-42 Basic Security

- **Firewall** - A firewall protects your network from the outside world. Here you can enable or disable the Router's firewall.
 - **SPI Firewall** - SPI (Stateful Packet Inspection, also known as dynamic packet filtering) helps to prevent cyber attacks by tracking more state per session. It validates that the traffic passing through the session conforms to the protocol. SPI Firewall is enabled by factory default. If you want all the computers on the LAN exposed to the outside world, you can disable it.
- **VPN** - VPN Passthrough must be enabled if you want to allow VPN tunnels using IPSec, PPTP, or L2TP protocols to pass through the Router's firewall.
 - **PPTP Passthrough** - Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. To allow PPTP tunnels to pass through the Router, keep the default, **Enabled**.
 - **L2TP Passthrough** - Layer 2 Tunneling Protocol (L2TP) is the method used to enable Point-to-Point sessions via the Internet on the Layer 2 level. To allow L2TP tunnels to pass through the Router, keep the default, **Enabled**.
 - **IPSec Passthrough** - Internet Protocol Security (IPSec) is a suite of protocols for ensuring private, secure communications over Internet Protocol (IP) networks, through the use of cryptographic security services. To allow IPSec tunnels to pass through the Router, keep the default, **Enabled**.
- **ALG** - It is recommended to enable Application Layer Gateway (ALG) because ALG allows customized Network Address Translation (NAT) traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols such as FTP, TFTP, H323 etc.
 - **FTP ALG** - To allow FTP clients and servers to transfer data across NAT, keep the default **Enable**.
 - **TFTP ALG** - To allow TFTP clients and servers to transfer data across NAT, keep the default **Enable**.
 - **H323 ALG** - To allow Microsoft NetMeeting clients to communicate across NAT, keep the default **Enable**.
 - **RTSP ALG** - To allow some media player clients to communicate with some streaming media servers across NAT, click **Enable**.

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

4.11.2 Advanced Security

Choose menu "**Security** → **Advanced Security**", you can protect the Router from being attacked by TCP-SYN Flood, UDP Flood and ICMP-Flood in the screen as shown in Figure 4-43.

Figure 4-43 Advanced Security

- **Packets Statistics Interval (5~60)** - The default value is 10. Select a value between 5 and 60 seconds from the drop-down list. The Packets Statistics Interval value indicates the time section of the packets statistics. The result of the statistics is used for analysis by SYN Flood, UDP Flood and ICMP-Flood.
- **DoS Protection** - Denial of Service protection. Check the Enable or Disable button to enable or disable the DoS protection function. Only when it is enabled, will the flood filters be enabled.

 Note:

Dos Protection will take effect only when the **Traffic Statistics** in “**System Tool** → **Traffic Statistics**” is enabled.

- **Enable ICMP-FLOOD Attack Filtering** - Enable or Disable the ICMP-FLOOD Attack Filtering.
- **ICMP-FLOOD Packets Threshold (5~3600)** - The default value is 50. Enter a value between 5 ~ 3600. When the current ICMP-FLOOD Packets number is beyond the set value, the Router will startup the blocking function immediately.
- **Enable UDP-FLOOD Filtering** - Enable or Disable the UDP-FLOOD Filtering.
- **UDP-FLOOD Packets Threshold (5~3600)** - The default value is 500. Enter a value between 5 ~ 3600. When the current UPD-FLOOD Packets number is beyond the set value, the Router will startup the blocking function immediately.
- **Enable TCP-SYN-FLOOD Attack Filtering** - Enable or Disable the TCP-SYN-FLOOD Attack Filtering.

- **TCP-SYN-FLOOD Packets Threshold (5~3600)** - The default value is 50. Enter a value between 5 ~ 3600. When the current TCP-SYN-FLOOD Packets numbers is beyond the set value, the Router will startup the blocking function immediately.
- **Ignore Ping Packet From WAN Port to Router** - Enable or Disable Ignore Ping Packet From WAN Port to Router. The default setting is disabled. If enabled, the ping packet from the Internet cannot access the Router.
- **Forbid Ping Packet From LAN Port to Router** - Enable or Disable Forbid Ping Packet From LAN Port to Router. The default setting is disabled. If enabled, the ping packet from LAN cannot access the Router. This function can be used to defend against some viruses.

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

Click the **Blocked DoS Host List** button to display the DoS host table by blocking.

4.11.3 Local Management

Choose menu “**Security → Local Management**”, you can configure the management rule in the screen as shown in Figure 4-44. The management feature allows you to deny computers in LAN from accessing the Router.

Figure 4-44 Local Management

By default, the radio button “**All the PCs on the LAN are allowed to access the Router's Web-Based Utility**” is checked. If you want to allow PCs with specific MAC Addresses to access the Setup page of the Router's Web-Based Utility locally from inside the network, check the radio button “**Only the PCs listed can browse the built-in web pages to perform Administrator tasks**”, and then enter each MAC Address in a separate field. The format for the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). Only the PCs with MAC address listed can use the password to browse the built-in web pages to perform Administrator tasks while all the others will be blocked.

After click the **Add** button, your PC's MAC Address will be placed in the list above.

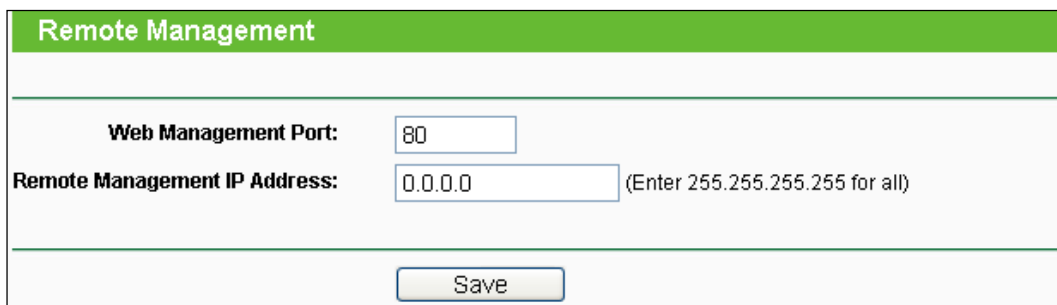
Click the **Save** button to save your settings.

 Note:

If your PC is blocked but you want to access the Router again, press and hold the **WPS/RESET** button on the back panel for about 8 seconds to reset the Router's factory defaults.

4.11.4 Remote Management

Choose menu "**Security** → **Remote Management**", you can configure the Remote Management function in the screen as shown in Figure 4-45. This feature allows you to manage your Router from a remote location via the Internet.



Remote Management	
Web Management Port:	80
Remote Management IP Address:	0.0.0.0 (Enter 255.255.255.255 for all)
Save	

Figure 4-45 Remote Management

- **Web Management Port** - Web browser access normally uses the standard HTTP service port 80. This Router's default remote management web port number is 80. For greater security, you can change the remote management web port to a custom port by entering that number in the box provided. Choose a number between 1 and 65534 but do not use the number of any common service port.
- **Remote Management IP Address** - This is the current address you will use when accessing your Router from the Internet. This function is disabled when the IP address is set to the default value of 0.0.0.0. To enable this function change 0.0.0.0 to a valid IP address. If set to 255.255.255.255, then all the hosts can access the Router from internet.

 Note:

- 1) To access the Router, you should type your Router's WAN IP address into your browser's address (in IE) or Location (in Navigator) box, followed by a colon and the custom port number. For example, if your Router's WAN address is 202.96.12.8, and the port number used is 8080, please enter <http://202.96.12.8:8080> in your browser. Later, you may be asked for the Router's password. After successfully entering the username and password, you will be able to access the Router's web-based utility.
- 2) Be sure to change the Router's default password to a very secure password.

4.12 Parental Control

Choose menu “**Parental Control**”, and you can configure the parental control in the screen as shown in Figure 4-46. The Parental Control function can be used to control the internet activities of the children, limit the children to access certain websites and restrict the time of surfing.

Figure 4-46 Parental Control Settings

- **Parental Control** - Check **Enable** if you want this function to take effect, otherwise check **Disable**.
- **MAC Address of Parental PC** - In this field, enter the MAC address of the controlling PC, or you can make use of the **Copy To Above** button below.
- **MAC Address of Your PC** - This field displays the MAC address of the PC that is managing this Router. If the MAC Address of your adapter is registered, you can click the Copy To Above button to fill this address to the MAC Address of Parental PC field above.
- **Website Description** - Description of the allowed website for the PC controlled.
- **Schedule** - The time period allowed for the PC controlled to access the Internet. For detailed information, please go to “**Access Control** → **Schedule**”.
- **Modify** - Here you can edit or delete an existing entry.

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

1. Click the **Add New...** button and the next screen will pop-up as shown in Figure 4-47.
2. Enter the MAC address of the PC (e.g. 00-11-22-33-44-AA) you'd like to control in the MAC Addresses of Children PC field. Or you can choose the MAC address from the All Address in Current LAN drop-down list.
3. Give a description (e.g. Allow TP-LINK) for the website allowed to be accessed in the Website Description field.

4. Enter the allowed domain name of the website, either the full name or the keywords (e.g. tp-link) in the Allowed Domain Name field. Any domain name with keywords in it (www.tp-link.com, www.tp-link.com/en/support) will be allowed.
5. Select from the Effective Time drop-down list the schedule (e.g. Schedule_1) you want the entry to take effect. If there are not suitable schedules for you, click the **Schedule** in red below to go to the Advance Schedule Settings page and create the schedule you need.
6. In the Status field, you can select **Enabled** or **Disabled** to enable or disable your entry.
7. Click the **Save** button.

Click the **Enable All** button to enable all the rules in the list.

Click the **Disable All** button to disable all the rules in the list.

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

Click the **Next** button to go to the next page, or click the **Previous** button return to the previous page.

Add or Modify Parental Control Entry

The Schedule is based on the time of the Router. The time can be set in "System Tools -> [Time settings](#)".

MAC Address of Children's PC:	
All MAC Address In Current LAN:	--Please Select-- ▼
Website Description:	
Allowed Website Name:	
Effective Time:	Anytime ▼ The time schedule can be set in "Access Control -> Schedule"
Status:	Enabled ▼

Figure 4-47 Add or Modify Parental Control Entry

For example: If you desire that the children's PC with MAC address 00-11-22-33-44-AA can access www.tp-link.com on Saturday only while the parent PC with MAC address 00-11-22-33-44-BB is without any restriction, you should follow the settings below.

1. Click **"Parental Control"** menu on the left to enter the Parental Control Settings page. Check **Enable** and enter the MAC address 00-11-22-33-44-BB in the MAC Address of Parental PC field.
2. Click **"Access Control → Schedule"** on the left to enter the Schedule Settings page. Click **Add New...** button to create a new schedule with Schedule Description is Schedule_1, Day is Sat and Time is all day-24 hours.
3. Click **"Parental Control"** menu on the left to go back to the Add or Modify Parental Control Entry page:
 - Click **Add New...** button.
 - Enter 00-11-22-33-44-AA in the **MAC Address of Children's PC** field.
 - Enter "Allow TP-LINK" in the **Website Description** field.
 - Enter "www.tp-link.com" in the **Allowed Website Name** field.
 - Select "Schedule_1" you create just now from the **Effective Time** drop-down list.
 - In **Status** field, select **Enable**.
4. Click **Save** to complete the settings.

Then you will go back to the Parental Control Settings page and see the following list, as shown in Figure 4-48.

ID	MAC address	Website Description	Schedule	Status	Modify
1	00-11-22-33-44-AA	Allow TP-LINK	Schedule_1	☒	Edit Delete
Add New... Enable All Disable All Delete All					

Figure 4-48 Parental Control Settings

4.13 Access Control

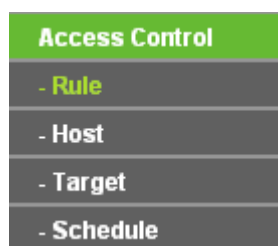


Figure 4-49 Access Control

There are four submenus under the Access Control menu as shown in Figure 4-49: **Rule**, **Host**, **Target** and **Schedule**. Click any of them, and you will be able to configure the corresponding function.

4.13.1 Rule

Choose menu **"Access Control → Rule"**, you can view and set Access Control rules in the screen

as shown in Figure 4-50.

Figure 4-50 Access Control Rule Management

- **Enable Internet Access Control** - Select the check box to enable the Internet Access Control function, so the Default Filter Policy can take effect.
- **Rule Name** - Here displays the name of the rule and this name is unique.
- **Host** - Here displays the host selected in the corresponding rule.
- **Target** - Here displays the target selected in the corresponding rule.
- **Schedule** - Here displays the schedule selected in the corresponding rule.
- **Status** - This field displays the status of the rule. **Enabled** means the rule will take effect, **Disabled** means the rule will not take effect.
- **Modify** - Here you can edit or delete an existing rule.

There are two methods to add a new rule.

Method One:

1. Click **Setup Wizard** button and the next screen will appear as shown in Figure 4-51.

Quick Setup - Create a Host Entry

Mode: IP Address ▼

Host Description:

LAN IP Address: -

Back Next

Figure 4-51 Quick Setup – Create a Host Entry

- **Mode** - Here are two options, **IP Address** and **MAC Address**. You can select either of them from the drop-down list.

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

If the **IP Address** is selected, you can see the following item:

- **LAN IP Address** - Enter the IP address or address range of the host in dotted-decimal format (e.g. 192.168.0.23).

If the **MAC Address** is selected, you can see the following item:

- **MAC Address** - Enter the MAC address of the host in XX-XX-XX-XX-XX-XX format (e.g. 00-11-22-33-44-AA).

2. Click **Next** when finishing creating the host entry, and the next screen will appear as shown in Figure 4-52.

Quick Setup - Create an Access Target Entry

Mode: IP Address ▼

Target Description:

IP Address: -

Target Port: -

Protocol: All ▼

Common Service Port: --Please Select-- ▼

Back Next

Figure 4-52 Quick Setup – Create an Access Target Entry

- **Mode** - Here are two options, **IP Address** and **Domain Name**. You can choose either of them from the drop-down list.

- **Target Description** - In this field, create a description for the target. Note that this description should be unique (e.g. Target_1).

If the **IP Address** is selected, you will see the following items:

- **IP Address** - Enter the IP address (or address range) of the target (targets) in dotted-decimal format (e.g. 192.168.0.23).
- **Target Port** - Specify the port or port range for the target. For some common service ports, you can make use of the Common Service Port item below.
- **Protocol** - Here are four options, All, TCP, UDP, and ICMP. Select one of them from the drop-down list for the target.
- **Common Service Port** - Here lists some common service ports. Select one from the drop-down list, and the corresponding port number will be filled in the Target Port field automatically. For example, if you select "FTP", "21" will be filled in the Target Port automatically.

If the **Domain Name** is selected, you will see the following items:

Domain Name - Here you can enter 4 domain names, either the full name or the keywords (for example, tp-link). Any domain name with keywords in it (www.tp-link.com, www.tp-link.com/en/support) will be blocked or allowed.

3. Click **Next** when finishing creating the access target entry, and the next screen will appear as shown in Figure 4-53.

Figure 4-53 Quick Setup – Create an Advanced Schedule Entry

- **Schedule Description** - In this field, create a description for the schedule. Note that this description should be unique (e.g. Schedule_1).
- **Day** - Choose Select Days and select the certain day (days), or choose Everyday.
- **Time** - Select "24 hours", or specify the Start Time and Stop Time yourself.

- **Start Time** - Enter the start time in HHMM format (HHMM are 4 numbers). For example 0800 is 8:00.
 - **Stop Time** - Enter the stop time in HHMM format (HHMM are 4 numbers). For example 2000 is 20:00.
4. Click **Next** when finishing creating the advanced schedule entry, and the next screen will appear as shown in Figure 4-54.

Figure 4-54 Quick Setup – Create an Internet Access Control Entry

- **Rule** - In this field, create a name for the rule. Note that this name should be unique (e.g. Rule_1).
 - **Host** - In this field, select a host from the drop-down list for the rule. The default value is the **Host Description** you set just now.
 - **Target** - In this field, select a target from the drop-down list for the rule. The default value is the **Target Description** you set just now.
 - **Schedule** - In this field, select a schedule from the drop-down list for the rule. The default value is the **Schedule Description** you set just now.
 - **Status** - In this field, there are two options, **Enabled** or **Disabled**. Select **Enabled** so that the rule will take effect. Select **Disabled** so that the rule won't take effect.
5. Click **Finish** to complete adding a new rule.

Method Two:

1. Click the **Add New...** button and the next screen will pop up as shown in Figure 4-55.
2. Give a name (e.g. Rule_1) for the rule in the **Rule Name** field.
3. Select a host from the **Host** drop-down list or choose "**Click Here To Add New Host List**".
4. Select a target from the **Target** drop-down list or choose "**Click Here To Add New Target List**".
5. Select a schedule from the **Schedule** drop-down list or choose "**Click Here To Add New Schedule**".

6. In the **Status** field, select **Enabled** or **Disabled** to enable or disable your entry.
7. Click the **Save** button.

Add Internet Access Control Entry

Rule Name:

Host: [Click Here To Add New Host List](#)

Target: [Click Here To Add New Target List](#)

Schedule: [Click Here To Add New Schedule](#)

Status:

Figure 4-55 Add Internet Access Control Entry

For example: If you desire to allow the host with MAC address 00-11-22-33-44-AA to access www.tp-link.com only from 18:00 to 20:00 on Saturday and Sunday, and forbid other hosts in the LAN to access the Internet, you should follow the settings below:

1. Click the submenu **Rule of Access Control** in the left to return to the Rule List page. Select Enable Internet Access Control and choose "Allow the packets specified by any enabled access control policy to pass through the Router".
2. We recommend that you click **Setup Wizard** button to finish all the following settings.
3. Click the submenu **Host of Access Control** in the left to enter the Host List page. Add a new entry with the Host Description is Host_1 and MAC Address is 00-11-22-33-44-AA.
4. Click the submenu **Target of Access Control** in the left to enter the Target List page. Add a new entry with the Target Description is Target_1 and Domain Name is www.tp-link.com.
5. Click the submenu **Schedule of Access Control** in the left to enter the Schedule List page. Add a new entry with the Schedule Description is Schedule_1, Day is Sat and Sun, Start Time is 1800 and Stop Time is 2000.
6. Click the submenu **Rule of Access Control** in the left, Click **Add New...** button to add a new rule as follows:
 - In Rule Name field, create a name for the rule. Note that this name should be unique, for example Rule_1.
 - In Host field, select Host_1.
 - In Target field, select Target_1.
 - In Schedule field, select Schedule_1.
 - In Status field, select Enable.
 - Click Save to complete the settings.

Then you will go back to the Access Control Rule Management page and see the following list.

ID	Rule Name	Host	Target	Schedule	Enable	Modify
1	Rule_1	Host_1	Target_1	Schedule_1	☒	Edit Delete

4.13.2 Host

Choose menu “**Access Control** → **Host**”, you can view and set a Host list in the screen as shown in Figure 4-56. The host list is necessary for the Access Control Rule.

Host Settings			
ID	Host Description	Information	Modify
1	Host_1	IP: 192.168.0.1 - 192.168.0.23	Edit Delete
Add New... Delete All			
Previous Next Current No. 1 Page			

Figure 4-56 Host Settings

- **Host Description** - Here displays the description of the host and this description is unique.
- **Information** - Here displays the information about the host. It can be IP or MAC.
- **Modify** - To modify or delete an existing entry.

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

1. Click the **Add New...** button.
2. In the **Mode** field, select IP Address or MAC Address.
 - If you select IP Address, the screen shown is Figure 4-57.
 - 1) In **Host Description** field, create a unique description for the host (e.g. Host_1).
 - 2) In **LAN IP Address** field, enter the IP address.
 - If you select MAC Address, the screen shown is Figure 4-58.
 - 1) In **Host Description** field, create a unique description for the host (e.g. Host_1).
 - 2) In **MAC Address** field, enter the MAC address.
3. Click the **Save** button to complete the settings.

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

Click the **Next** button to go to the next page, or click the **Previous** button return to the previous page.

Add or Modify a Host Entry

Mode: IP Address

Host Description: Host_1

LAN IP Address: 192.168.0.1 - 192.168.0.23

Save **Back**

Figure 4-57 Add or Modify a Host Entry

Add or Modify a Host Entry

Mode: MAC Address

Host Description: Host_1

MAC Address: 00-11-22-33-44-AA

Save **Back**

Figure 4-58 Add or Modify a Host Entry

For example: If you desire to restrict the internet activities of host with MAC address 00-11-22-33-44-AA, you should first follow the settings below:

1. Click **Add New...** button in Figure 4-56 to enter the Add or Modify a Host Entry page.
2. In **Mode** field, select MAC Address from the drop-down list.
3. In **Host Description** field, create a **unique** description for the host (e.g. Host_1).
4. In **MAC Address** field, enter 00-11-22-33-44-AA.
5. Click **Save** to complete the settings.

Then you will go back to the Host Settings page and see the following list.

ID	Host Description	Information	Modify
1	Host_1	MAC: 00-11-22-33-44-AA	Edit Delete

4.13.3 Target

Choose menu “**Access Control** → **Target**”, you can view and set a Target list in the screen as shown in Figure 4-59. The target list is necessary for the Access Control Rule.

ID	Target Description	Information	Modify
1	Target_1	192.168.0.2 - 192.168.0.23/21/TCP	Edit Delete

Current No. 1 Page

Figure 4-59 Target Settings

- **Target Description** - Here displays the description about the target and this description is unique.
- **Information** - The target can be IP address, port, or domain name.
- **Modify** - To modify or delete an existing entry.

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

1. Click the **Add New...** button.
2. In **Mode** field, select IP Address or Domain Name.
 - If you select **IP Address**, the screen shown is Figure 4-60.
 - 1) In **Target Description** field, create a unique description for the target (e.g. Target_1).
 - 2) In **IP Address** field, enter the IP address of the target.
 - 3) Select a common service from **Common Service Port** drop-down list, so that the **Target Port** will be automatically filled. If the **Common Service Port** drop-down list doesn't have the service you want, specify the **Target Port** manually.
 - 4) In **Protocol** field, select TCP, UDP, ICMP or ALL.
 - If you select **Domain Name**, the screen shown is Figure 4-61.
 - 1) In **Target Description** field, create a unique description for the target (e.g. Target_1).
 - 2) In **Domain Name** field, enter the domain name, either the full name or the keywords (for example tp-link) in the blank. Any domain name with keywords in it (www.tp-link.com, www.tp-link.com/en/support) will be blocked or allowed. You can enter 4 domain names.
3. Click the **Save** button.

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

Click the **Next** button to go to the next page, or click the **Previous** button return to the previous page.

Add or Modify an Access Target Entry

Mode: IP Address ▼

Target Description:

IP Address: -

Target Port: -

Protocol: ALL ▼

Common Service Port: --please select-- ▼

Figure 4-60 Add or Modify an Access Target Entry

Add or Modify an Access Target Entry

Mode: Domain Name ▼

Target Description:

Domain Name:

Figure 4-61 Add or Modify an Access Target Entry

For example: If you desire to restrict the internet activities of host with MAC address 00-11-22-33-44-AA in the LAN to access **www.tp-link.com** only, you should first follow the settings below:

1. Click **Add New...** button in Figure 4-59 to enter the Add or Modify an Access Target Entry page.
2. In **Mode** field, select Domain Name from the drop-down list.
3. In **Target Description** field, create a unique description for the target (e.g. Target_1).
4. In **Domain Name** field, enter www.tp-link.com.
5. Click **Save** to complete the settings.

Then you will go back to the Target Settings page and see the following list,

ID	Target Description	Information	Modify
1	Target_1	www.tp-link.com	Edit Delete

4.13.4 Schedule

Choose menu “**Access Control** → **Schedule**”, you can view and set a Schedule list in the next screen as shown in Figure 4-62. The Schedule list is necessary for the Access Control Rule.

Schedule Settings				
ID	Schedule Description	Day	Time	Modify
Add New... Delete All				
Previous Next Current No. 1 Page				

Figure 4-62 Schedule Settings

- **Schedule Description** - Here displays the description of the schedule and this description is unique.
- **Day** - Here displays the day(s) in a week.
- **Time** - Here displays the time period in a day.
- **Modify** - Here you can edit or delete an existing schedule.

To add a new schedule, follow the steps below.

1. Click **Add New...** button shown in Figure 4-62 and the next screen will pop-up as shown in Figure 4-63.
2. In **Schedule Description** field, create a unique description for the schedule (e.g. Schedule_1).
3. In **Day** field, select the day or days you need.
4. In **Time** field, you can select all day-24 hours or you may enter the Start Time and Stop Time in the corresponding field.
5. Click **Save** to complete the settings.

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

Click the **Next** button to go to the next page, or click the **Previous** button return to the previous page.

Advance Schedule Settings

Note: The Schedule is based on the time of the Router.

Schedule Description:

Day: ☒ Everyday ☐ Select Days

☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat ☒ Sun

Time: all day-24 hours: ☒

Start Time: (HHMM)

Stop Time: (HHMM)

Figure 4-63 Advanced Schedule Settings

For example: If you desire to restrict the internet activities of host with MAC address 00-11-22-33-44-AA to access www.tp-link.com only from **18:00 to 20:00** on **Saturday** and **Sunday**, you should first follow the settings below:

1. Click **Add New...** button shown in Figure 4-62 to enter the Advanced Schedule Settings page.
2. In **Schedule Description** field, create a unique description for the schedule (e.g. Schedule_1).
3. In **Day** field, check the Select Days radio button and then select Sat and Sun.
4. In **Time** field, enter 1800 in Start Time field and 2000 in Stop Time field.
5. Click **Save** to complete the settings.

Then you will go back to the Schedule Settings page and see the following list.

ID	Schedule Description	Day	Time	Modify
1	Schedule_1	Sat Sun	18:00 - 20:00	Edit Delete

4.14 Advanced Routing

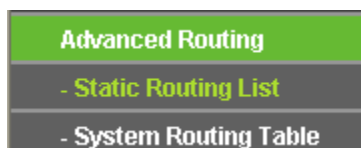


Figure 4-64 Advanced Routing Menu

There are two submenus under the Network menu (shown in Figure 4-64): **Static Routing List** and **System Routing Table**. Click any of them, and you will be able to configure the corresponding function.

4.14.1 Static Routing

Choose menu “**Advanced Routing** → **Static Routing**”, and you can configure the static route in the next screen, shown in Figure 4-65. A static route is a pre-determined path that network information must travel to reach a specific host or network.

ID	Destination Network	Subnet Mask	Default Gateway	Status	Modify
Add New... Enable All Disable All Delete All					
Previous Next					

Figure 4-65 Static Routing

To add static routing entries, follow the steps below.

1. Click **Add New...** shown in Figure 4-65, you will see the following screen Figure 4-66.

Add or Modify a Static Route Entry

Destination Network:

Subnet Mask:

Default Gateway:

Status: ▼

Figure 4-66 Add or Modify a Static Route Entry

2. Enter the following data.
 - **Destination Network** - The **Destination Network** is the address of the network or host that you want to assign to a static route.
 - **Subnet Mask** - The **Subnet Mask** determines which portion of an IP Address is the network portion, and which portion is the host portion.
 - **Default Gateway** - This is the IP Address of the default gateway device that allows for the contact between the Router and the network or host.
3. Select **Enabled** or **Disabled** for this entry on the **Status** drop-down list.
4. Click the **Save** button to make the entry take effect.

Click the **Delete** button to delete the entry.

Click the **Enable All** button to enable all the entries.

Click the **Disable All** button to disable all the entries.

Click the **Delete All** button to delete all the entries.

Click the **Previous** button to view the information in the previous screen, click the **Next** button to view the information in the next screen.

4.14.2 System Routing Table

Choose menu “**Advanced Routing** → **System Routing Table**”, and you can view all of the valid route entries in use. The Destination IP address, Subnet Mask, Gateway, and Interface will be displayed for each entry.

System Routing Table				
ID	Destination Network	Subnet Mask	Gateway	Interface
1	192.168.1.0	255.255.255.0	0.0.0.0	WAN
2	192.168.0.0	255.255.255.0	0.0.0.0	LAN & WLAN
3	0.0.0.0	0.0.0.0	192.168.1.1	WAN

Refresh

- **Destination Network** - The Destination Network is the address of the network or host to which the static route is assigned.
- **Subnet Mask** - The Subnet Mask determines which portion of an IP address is the network portion, and which portion is the host portion.
- **Gateway** - This is the IP address of the gateway device that allows for contact between the Router and the network or host.
- **Interface** - This interface tells you whether the Destination IP Address is on the **LAN & WLAN** (internal wired and wireless networks), the **WAN(Internet)**.

Click the **Refresh** button to refresh the data displayed.

4.15 Bandwidth Control

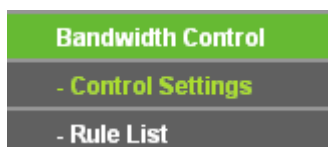


Figure 4-67

There are two submenus under the Bandwidth Control menu as shown in Figure 4-67. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.15.1 Control Settings

Choose menu “**Bandwidth Control** → **Control Settings**”, you can configure the Egress Bandwidth and Ingress Bandwidth in the next screen. Their values you configure should be less than 100000Kbps. For optimal control of the bandwidth, please select the right Line Type and ask your ISP for the total bandwidth of the egress and ingress.

Figure 4-68 Bandwidth Control Settings

- **Enable Bandwidth Control** - Check this box so that the Bandwidth Control settings can take effect.
- **Line Type** - Select the right type for you network connection. If you don't know how to choose, please ask your ISP for the information.
- **Egress Bandwidth** - The upload speed through the WAN port.
- **Ingress Bandwidth** - The download speed through the WAN port.

4.15.2 Rules List

Choose menu “**Bandwidth Control** → **Rules List**”, you can view and configure the Bandwidth Control rules in the screen below.

Figure 4-69 Bandwidth Control Rules List

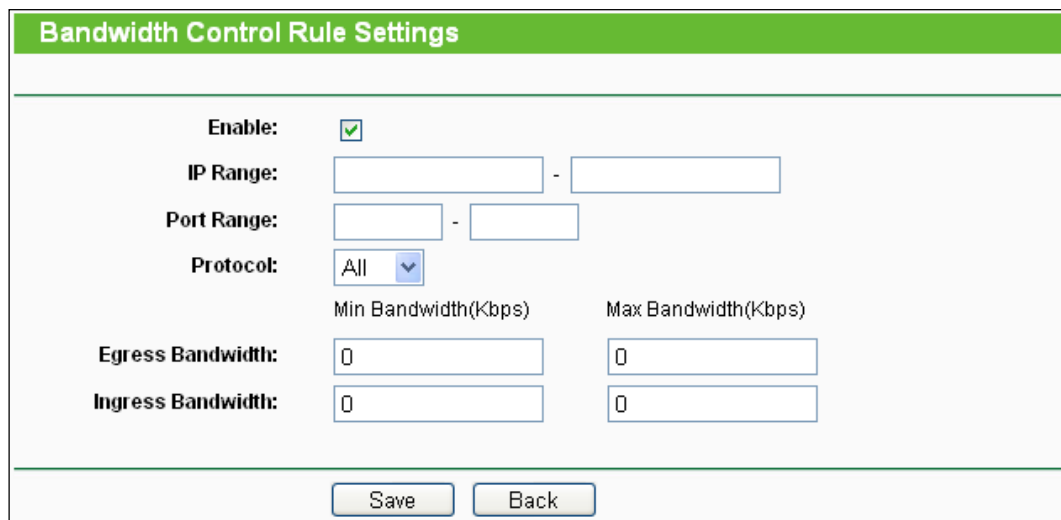
- **Description** - This is the information about the rules such as address range.
- **Egress bandwidth** - This field displays the max and mix upload bandwidth through the WAN port, the default is 0.

- **Ingress bandwidth** - This field displays the max and mix download bandwidth through the WAN port, the default is 0.
- **Enable** - This displays the status of the rule.
- **Modify** - Click **Modify** to edit the rule. Click **Delete** to delete the rule.

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

Step 1: Click **Add New...** shown in Figure 4-69, you will see a new screen shown in Figure 4-70.

Step 2: Enter the information like the screen shown below.



The image shows a web form titled "Bandwidth Control Rule Settings". It contains the following fields and controls:

- Enable:** A checkbox that is checked.
- IP Range:** Two text input boxes separated by a hyphen.
- Port Range:** Two text input boxes separated by a hyphen.
- Protocol:** A dropdown menu currently set to "All".
- Min Bandwidth(Kbps):** A label above two columns of text input boxes.
- Max Bandwidth(Kbps):** A label above two columns of text input boxes.
- Egress Bandwidth:** Two text input boxes, each containing the number "0".
- Ingress Bandwidth:** Two text input boxes, each containing the number "0".
- Buttons:** "Save" and "Back" buttons at the bottom.

Figure 4-70 Bandwidth Control Rule Settings

Step 3: Click the **Save** button.

4.16 IP & MAC Binding

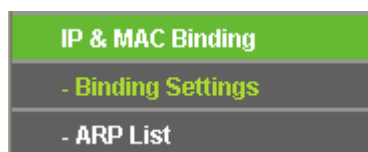


Figure 4-71 the IP & MAC Binding menu

There are two submenus under the **IP & MAC Binding** menu (shown in Figure 4-71): **Binding Settings** and **ARP List**. Click any of them, and you will be able to scan or configure the corresponding function. The detailed explanations for each submenu are provided below.

4.16.1 Binding Settings

This page displays the **IP & MAC Binding** table; you can operate it in accord with your desire as shown in Figure 4-72.

Figure 4-72 Binding Settings

- **MAC Address** - The MAC address of the controlled computer in the LAN.
- **IP Address** - The assigned IP address of the controlled computer in the LAN.
- **Bind** - Check this option to enable ARP binding for a specific device.
- **Modify** - To modify or delete an existing entry.

When you want to add or modify an IP & MAC Binding entry, you can click the **Add New...** button or **Modify** button, and then you will go to the next page. This page is used for adding or modifying an IP & MAC Binding entry, shown in Figure 4-73.

Figure 4-73 IP & MAC Binding Settings

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

1. Click the **Add New...** button as shown in Figure 4-72.
2. Enter the MAC Address and IP Address.
3. Select the Bind checkbox.
4. Click the **Save** button to save it.

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

1. Find the desired entry in the table.

- Click **Modify** or **Delete** as desired on the **Modify** column.

To find an existing entry, follow the steps below.

- Click the **Find** button as shown in Figure 4-72.
- Enter the MAC Address or IP Address.
- Click the **Find** button in the page as shown in Figure 4-74.

Find IP & MAC Binding Entry				
MAC Address:	00-14-5E-91-19-E3			
IP Address:				
ID	MAC Address	IP Address	Bind Link	
2	00-14-5E-91-19-E3	192.168.1.56	☒	To page
Find Back				

Figure 4-74 Find IP & MAC Binding Entry

Click the **Enable All** button to make all entries enabled.

Click the **Delete All** button to delete all entries.

4.16.2 ARP List

To manage the computer, you could observe the computers in the LAN by checking the relationship of MAC address and IP address on the ARP list, and you could configure the items on the ARP list also. This page displays the ARP List; it shows all the existing IP & MAC Binding entries as shown in Figure 4-75.

ARP List				
ID	MAC Address	IP Address	Status	Configure
1	40-61-86-FC-74-93	192.168.0.100	Unbound	Load Delete
Bind All Load All Refresh				

Figure 4-75 ARP List

- **MAC Address** - The MAC address of the controlled computer in the LAN.
- **IP Address** - The assigned IP address of the controlled computer in the LAN.
- **Status** - Indicates whether or not the MAC and IP addresses are bound.
- **Configure** - Load or delete an item.
 - **Load** - Load the item to the IP & MAC Binding list.

- **Delete** - Delete the item.

Click the **Bind All** button to bind all the current items, available after enable.

Click the **Load All** button to load all items to the IP & MAC Binding list.

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

 Note:

An item could not be loaded to the IP & MAC Binding list if the IP address of the item has been loaded before. Error warning will prompt as well. Likewise, "Load All" only loads the items without interference to the IP & MAC Binding list.

4.17 Dynamic DNS

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

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

4.17.1 Comexe.cn DDNS

If the dynamic DNS **Service Provider** you select is www.comexe.cn, the page will appear as shown in Figure 4-76.

DDNS

Service Provider: Comexe (www.comexe.cn) [Go to register...](#)

Domain Name:

Domain Name:

Domain Name:

Domain Name:

Domain Name:

User Name:

Password:

☐ Enable DDNS

Connection Status: DDNS not launching!

Figure 4-76 Comexe.cn DDNS Settings

To set up for DDNS, follow these instructions:

1. Type the **Domain Name** received from your dynamic DNS service provider.
2. Type the **User Name** for your DDNS account.
3. Type the **Password** for your DDNS account.
4. Click the **Login** button to log in to the DDNS service.

Connection Status -The status of the DDNS service connection is displayed here.

Click **Logout** to log out of the DDNS service.

4.17.2 Dyndns.org DDNS

If the dynamic DNS **Service Provider** you select is www.dyndns.org, the page will appear as shown in Figure 4-77.

DDNS

Service Provider: Dyndns (www.dyndns.org) [Go to register...](#)

User Name: username

Password: ••••••••

Domain Name:

☐ Enable DDNS

Connection Status: DDNS not launching!

Login Logout

Save

Figure 4-77 Dyndns.org DDNS Settings

To set up for DDNS, follow these instructions:

1. Type the **User Name** for your DDNS account.
2. Type the **Password** for your DDNS account.
3. Type the **Domain Name** you received from dynamic DNS service provider here.
4. Click the **Login** button to log in to the DDNS service.

Connection Status -The status of the DDNS service connection is displayed here.

Click **Logout** to logout of the DDNS service.

4.17.3 No-ip.com DDNS

If the dynamic DNS **Service Provider** you select is www.no-ip.com, the page will appear as shown in Figure 4-78.

DDNS

Service Provider: No-IP (www.no-ip.com) [Go to register...](#)

User Name: username

Password: ••••••••

Domain Name:

☐ Enable DDNS

Connection Status: DDNS not launching!

Login Logout

Save

Figure 4-78 No-ip.com DDNS Settings

To set up for DDNS, follow these instructions:

1. Type the **User Name** for your DDNS account.
2. Type the **Password** for your DDNS account.
3. Type the **Domain Name** you received from dynamic DNS service provider.
4. Click the **Login** button to log in the DDNS service.

Connection Status - The status of the DDNS service connection is displayed here.

Click **Logout** to log out the DDNS service.

4.18 IPv6 Support

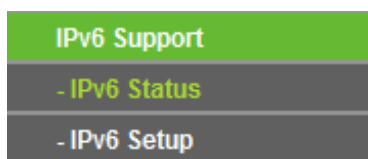


Figure 4-79 IPv6 Support

There are two submenus under the IPv6 Support menu: **IPv6 Status** and **IPv6 Setup**. Click either of them, and you will be able to scan or configure the corresponding function. The detailed explanations for each submenu are provided below.

4.18.1 IPv6 Status

IPv6 Status	
WAN	
Connection Type:	PPPoE v6
IPv6 Address:	2000::7757:264c:fe14:a397/64
IPv6 Default Gateway:	fe80::c8a4:7ec7:5a6a:750b
Primary IPv6 DNS:	2a04:2c00:1:c000::2
Secondary IPv6 DNS:	
LAN	
IPv6 Address Assign Type:	RADVD
IPv6 Address:	2a04:2c01:0:801e:20a:ebff:fe13:919/64
Link-local Address:	fe80::20a:ebff:fe13:919/64

The **IPv6 Status** page displays the router's current IPv6 status and configuration. All information is read-only.

➤ WAN

- **Connection Type** - The IPv6 connection way for WAN
- **IPv6 Address** - The WAN IPv6 address

- **IPv6 Default Gateway** - The router's default gateway
- **Primary IPv6 DNS** - The primary IPv6 DNS address
- **Secondary IPv6 DNS** - The secondary IPv6 DNS address

➤ **LAN**

- **IPv6 Address Assign Type** - There are two types of assignation for IPv6 address: RADVD(Router Advertisement Daemon) and DHCPv6 (Dynamic Host Configuration Protocol for IPv6) Server.
- **IPv6 Address** - The LAN global IPv6 address of the Router.
- **Link-local Address** - The LAN Link-local Address of the Router.

4.18.2 IPv6 Setup

WAN Setup

Enable IPv6: ☒

WAN Connection Type: DHCPv6

IPv6 Address: 2000::ddc7:25a2:6a14:b2b1

Default Gateway: fe80::6e62:6dff:fe5:aac4

Renew Release Connected

☒ Get IPv6 DNS Server Automatically

Primary IPv6 DNS: 2a04:2c00:1:c000::2

Secondary IPv6 DNS:

☐ Use the following IPv6 DNS Servers

LAN Setup

Address Autoconfiguration Type: ☒ RADVD ☐ DHCPv6 Server

Site Prefix Configuration Type: ☒ Delegated ☐ Static

Lan IPv6 Address: 2a04:2c01:0:801e:20a:ebff:fe13:919/64

Save

- **Enable IPv6** - Tick the checkbox to enable the IPv6 function. It's enabled by default.
- **WAN Connection Type** - Choose the correct WAN connection type based on your ISP network topology.
- **SLAAC** - Connections which use Radvd IPv6 address assignment.
 - **DHCPv6** - Connections which use dynamic IPv6 address assignment.
 - **Static IPv6** - Connections which use static IPv6 address assignment.
 - **PPPoE v6** - Connections which use PPPoE v6 that requires a user name and password.
 - **Tunnel 6to4** - Connections which use 6to4 address assignment.

Different types of WAN connection require you to do different settings. Below are the detailed explanations for the respective type.

1) SLAAC

The screenshot shows the 'WAN Setup' configuration page. At the top, there is a green header bar with the text 'WAN Setup'. Below this, the 'Enable IPv6' checkbox is checked. The 'WAN Connection Type' is set to 'SLAAC' in a dropdown menu. The 'IPv6 Address' field displays '2020:0000:0000:0000:020a:ebff:fe13:091a', the 'IPv6 Address Prefix' is '2020::/64', and the 'Default Gateway' is 'fe80::6e62:6dff:fe5:aac4'. There are 'Connect' and 'Disconnect' buttons, with 'Connected' text next to them. Below these fields, there are two radio button options for DNS: 'Get IPv6 DNS Server Automatically' (selected) and 'Use the following IPv6 DNS Servers'. The 'Primary IPv6 DNS' field shows '2a04:2c00:1:c000::2' and the 'Secondary IPv6 DNS' field is empty. A green header bar at the bottom of the WAN section is labeled 'LAN Setup'. Under 'LAN Setup', the 'Address Autoconfiguration Type' has 'RADVD' selected and 'DHCPv6 Server' unselected. The 'Site Prefix Configuration Type' has 'Delegated' selected and 'Static' unselected. The 'Lan IPv6 Address' field shows '2a04:2c01:0:801e:20a:ebff:fe13:919/64'. At the very bottom of the page is a 'Save' button.

- **Enable IPv6** - Enable or disable the IPv6 feature.
- **IPv6 Address** - The IPv6 address assigned by your ISP dynamically.
- **IPv6 Address Prefix** - Display the IPv6 Prefix Length in dotted-decimal notation provided by your ISP.
- **Default Gateway** - Display the default gateway in colon-hexadecimal notation provided by your ISP.
- Click the **Connect** button to connect immediately.
- Click the **Disconnect** button to disconnect immediately.

If your ISP gives you one or two DNS IPv6 addresses, select **Use the following IPv6 DNS Servers** and enter the **Primary IPv6 DNS** and **Secondary IPv6 DNS** into the correct fields. Otherwise, the DNS servers will be assigned from ISP dynamically.

- **Primary IPv6 DNS** - Enter the DNS IPv6 address in colon-hexadecimal notation provided by your ISP.
- **Secondary IPv6 DNS** - Enter another DNS IPv6 address in colon-hexadecimal notation provided by your ISP.

 Note:

If you get Address not found error when you access a Web site, it is likely that your DNS servers are set up improperly. You should contact your ISP to get DNS server addresses.

- **Address Autoconfiguration Type** – RADVD (Router Advertisement Daemon) and DHCPv6 (Dynamic Host Configuration Protocol for IPv6) Server.

DHCPv6 Server

- **Release Time** - the length of time a network user will be allowed to keep connecting to the router with the current DHCPv6 Address. Enter the amount of time (in seconds) that the DHCPv6 address will be leased. The time range is 1~691200 seconds. The default value is 86400 seconds.
- **Site Prefix Configuration Type** - The type of IPv6 address prefix.
 - **Delegated** - Get the IPv6 address prefix from the ISP automatically, and the device will delegate it to the LAN.
 - **Static** - Configure the Site Prefix and Site Prefix Length manually. Please contact your ISP to get more information before you configure them.

LAN IPv6 Address - Display the LAN IPv6 address created by the device.

2) DHCPv6

WAN Setup	
Enable IPv6:	☒
WAN Connection Type:	DHCPv6
IPv6 Address:	2000::ddc7:25a2:6a14:b2b1
Default Gateway:	fe80::6e62:6dff:fe5:aac4
	Renew Release Connected
	☒ Get IPv6 DNS Server Automatically
Primary IPv6 DNS:	2a04:2c00:1:c000::2
Secondary IPv6 DNS:	
	☐ Use the following IPv6 DNS Servers
LAN Setup	
Address Autoconfiguration Type:	☒ RADVD ☐ DHCPv6 Server
Site Prefix Configuration Type:	☒ Delegated ☐ Static
Lan IPv6 Address:	2a04:2c01:0:801e:20a:ebff:fe13:919/64
Save	

- **Enable IPv6** - Enable or disable the IPv6 feature.

- **IPv6 Address** - The IPv6 address assigned by your ISP dynamically.
- **Default Gateway** - Display the default gateway in colon-hexadecimal notation provided by your ISP.

Click the **Renew** button to renew the IPv6 parameters from your ISP.

Click the **Release** button to release the IPv6 parameters from your ISP.

If your ISP gives you one or two DNS IPv6 addresses, select **Use the following IPv6 DNS Servers** and enter the **Primary IPv6 DNS** and **Secondary IPv6 DNS** into the correct fields. Otherwise, the DNS servers will be assigned from ISP dynamically.

- **Primary IPv6 DNS** - Enter the DNS IPv6 address in colon-hexadecimal notation provided by your ISP.
- **Secondary IPv6 DNS** - Enter another DNS IPv6 address in colon-hexadecimal notation provided by your ISP.

 Note:

If you get Address not found error when you access a Web site, it is likely that your DNS servers are set up improperly. You should contact your ISP to get DNS server addresses.

- **Address Autoconfiguration Type** – RADVD (Router Advertisement Daemon) and DHCPv6 (Dynamic Host Configuration Protocol for IPv6) Server.

DHCPv6 Server

- **Release Time** - the length of time a network user will be allowed to keep connecting to the router with the current DHCPv6 Address. Enter the amount of time (in seconds) that the DHCPv6 address will be leased. The time range is 1~691200 seconds. The default value is 86400 seconds.
- **Site Prefix Configuration Type** - The type of IPv6 address prefix.
 - **Delegated** - Get the IPv6 address prefix from the ISP automatically, and the device will delegate it to the LAN.
 - **Static** - Configure the Site Prefix and Site Prefix Length manually. Please contact your ISP to get more information before you configure them.
 - **LAN IPv6 Address** - Display the LAN IPv6 address created by the device.

3) Static IPv6

WAN Setup	
Enable IPv6:	☒
WAN Connection Type:	Static IPv6 ▼
IPv6 Address:	2803:1a00:0:4::2
Default Gateway:	2803:1a00:0:4::1 (Optional)
MTU Size (in bytes):	1500 (The default is 1500, do not change unless necessary.)
Primary DNS:	2001:4860:4860::8888
Secondary DNS:	(Optional)
LAN Setup	
Address Autoconfiguration Type:	☒ RADVD ☐ DHCPv6 Server
Site Prefix:	2803:1a00:0:16::
Site Prefix Length:	64 (The default is 64, do not change unless necessary)
Lan IPv6 Address:	2803:1a00:0:16:20a:ebff:fe13:919/64
Save	

- **Enable IPv6** - Enable or disable the IPv6 feature.
- **IPv6 Address** - Enter the IPv6 address in dotted-decimal notation provided by your ISP.
- **Default Gateway** - Enter the default gateway in dotted-decimal notation provided by your ISP.
- **MTU Size** - The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs, you may need to modify the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.
- **Primary DNS** - Enter the DNS IPv6 address in dotted-decimal notation provided by your ISP.
- **Secondary DNS** - Enter another DNS IPv6 address in dotted-decimal notation provided by your ISP.
- **Address Autoconfiguration Type** - RADVD(Router Advertisement Daemon) and DHCPv6(Dynamic Host Configuration Protocol for IPv6) Server.

DHCPv6 Server

- **Release Time** - the length of time a network user will be allowed to keep connecting to the router with the current DHCPv6 Address. Enter the amount of time (in seconds) that the DHCPv6 address will be leased. The time range is 1~691200 seconds. The default value is 86400 seconds.
- **LAN IPv6 Address** - Display the LAN IPv6 address created by the device.

4) PPPoEv6

WAN Setup	
Enable IPv6:	☒
WAN Connection Type:	PPPoEv6
PPPoE Session:	☐ Share with PPPoEv4 ☒ Create a new Session
Username:	pppoe
Password:	
Confirm Password:	
IPv6 Address:	2000::7757:264c:fe14:a397
IPv6 Address Prefix:	2a04:2c01:0:801e::/64
Default Gateway:	fe80::c8a4:7ec7:5a6a:750b
MTU:	1492 Bytes, 1492 as default, do not change unless necessary.
	☒ Get IPv6 DNS Server Automatically
Primary IPv6 DNS:	2a04:2c00:1:c000::2
Secondary IPv6 DNS:	
	☐ Use the following IPv6 DNS Servers
Connection Mode:	☒ Always On ☐ Connect Manual
	Connect Disconnect Connected
LAN Setup	
Address Autoconfiguration Type:	☒ RADVD ☐ DHCPv6 Server
Site Prefix Configuration Type:	☒ Delegated ☐ Static
Lan IPv6 Address:	2a04:2c01:0:801e:20a:ebff:fe13:919/64
Save	

- **Enable IPv6** - Enable or disable the IPv6 feature.
- **PPPoE Session** - The PPP session type for IPv6 connection. There are two types:
 - **Share with PPPoEv4** - The PPPoEv6 and PPPoEv4 use the same PPP session.
 - **Create a new Session** - The PPPoEv6 and PPPoEv4 use different PPP sessions. It is default to select this option.
- **User Name/Password** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.

If your ISP gives you one or two DNS IPv6 addresses, select **Use the following IPv6 DNS Servers** and enter the **Primary IPv6 DNS** and **Secondary IPv6 DNS** into the correct fields. Otherwise, the DNS servers will be assigned from ISP dynamically.

- **Primary IPv6 DNS** - Enter the DNS IPv6 address in colon-hexadecimal notation provided by your ISP.
- **Secondary IPv6 DNS** - Enter another DNS IPv6 address in colon-hexadecimal notation provided by your ISP.

 Note:

If you get Address not found error when you access a Web site, it is likely that your DNS servers are set up improperly. You should contact your ISP to get DNS server addresses.

➤ **Connection Mode** - The way to connect the ISP.

- **Always On** - Connect automatically.
- **Connect Manual** - Connect by the user manually.

Click the **Connect** button to connect immediately.

Click the **Disconnect** button to disconnect immediately.

➤ **Address Autoconfiguration Type** – RADVD (Router Advertisement Daemon) and DHCPv6 (Dynamic Host Configuration Protocol for IPv6) Server.

DHCPv6 Server

- **Release Time** - the length of time a network user will be allowed to keep connecting to the router with the current DHCPv6 Address. Enter the amount of time (in seconds) that the DHCPv6 address will be leased. The time range is 1~691200 seconds. The default value is 86400 seconds.

➤ **Site Prefix Configuration Type** - The type of IPv6 address prefix.

- **Delegated** - Get the IPv6 address prefix from the ISP automatically, and the device will delegate it to the LAN.
- **Static** - Configure the Site Prefix and Site Prefix Length manually. Please contact your ISP to get more information before you configure them.

LAN IPv6 Address - Display the LAN IPv6 address created by the device.

5) Tunnel 6to4

WAN Setup	
Enable IPv6:	☒
WAN Connection Type:	Tunnel 6to4
Address:	192.168.3.11
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.3.3
Tunnel Address:	2002:c0a8:30b::c0a8:30b/48
MTU Size (in bytes):	1480 (The default is 1480, do not change unless necessary.)
	☐ Use the following IPv6 DNS Servers
Primary IPv6 DNS:	2001:4860:4860::8888
Secondary IPv6 DNS:	(Optional)
LAN Setup	
Address Autoconfiguration Type:	☒ RADVD ☐ DHCPv6 Server
Site Prefix Configuration Type:	☒ Delegated ☐ Static
Lan IPv6 Address:	2002:c0a8:30b:1:20a:ebff:fe13:919/64
Save	

➤ **Enable IPv6** - Enable or disable the IPv6 feature.

- **Address** - The IPv4 address assigned by your ISP dynamically.
- **Subnet Mask** - The IPv4 address assigned by your ISP dynamically.
- **Default Gateway** - The IPv4 default gateway assigned by your ISP dynamically.
- **Tunnel Address** - The 6to4 tunnel address created by the device to access to the IPv6 network.
- **MTU Size** - The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1480 Bytes. For some ISPs, you may need to modify the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.

If your ISP gives you one or two DNS IPv6 addresses, select **Use the following IPv6 DNS Servers** and enter the **Primary IPv6 DNS** and **Secondary IPv6 DNS** into the correct fields. Otherwise, the DNS servers will be assigned from ISP dynamically.

- **Primary IPv6 DNS** - Enter the DNS IPv6 address in dotted-decimal notation provided by your ISP.
- **Secondary IPv6 DNS** - Enter another DNS IPv6 address in dotted-decimal notation provided by your ISP.
- **Address Autoconfiguration Type** – RADVD (Router Advertisement Daemon) and DHCPv6 (Dynamic Host Configuration Protocol for IPv6) Server.

DHCPv6 Server

- **Release Time** - the length of time a network user will be allowed to keep connecting to the router with the current DHCPv6 Address. Enter the amount of time (in seconds) that the DHCPv6 address will be leased. The time range is 1~691200 seconds. The default value is 86400 seconds.
- **Site Prefix Configuration Type** - The type of IPv6 address prefix.
 - **Delegated** - Get the IPv6 address prefix from the ISP automatically, and the device will delegate it to the LAN.
 - **Static** - Configure the Site Prefix and Site Prefix Length manually. Please contact your ISP to get more information before you configure them.

LAN IPv6 Address - Display the LAN IPv6 address created by the device.

4.19 System Tools



Figure 4-80 The System Tools menu

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

4.19.1 Time Settings

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

The "Time Settings" configuration page has a green header. It contains several fields: "Time zone:" with a dropdown menu showing "(GMT+08:00) Beijing, Hong Kong, Perth, Singapore"; "Date:" with three input boxes for month (1), day (1), and year (2012), followed by "(MM/DD/YY)"; "Time:" with three input boxes for hour (2), minute (23), and second (13), followed by "(HH/MM/SS)"; "NTP Server 1:" and "NTP Server 2:" each with an input box containing "0.0.0.0" and the text "(Optional)"; a "Get GMT" button; a checkbox for "Enable Daylight Saving" which is unchecked; "Start:" and "End:" each with four dropdown menus for month, day, day of the week, and time; and "Daylight Saving Status:" with the text "daylight saving is down." Below these fields is a note: "Note: Click the 'GET GMT' to update the time from the internet with the pre-defined servers or entering the customized server (IP Address or Domain Name) in the above frames." At the bottom is a "Save" button.

Figure 4-81 Time settings

- **Time zone** - Select your local time zone from this drop-down list.
- **Date** - Enter your local date in MM/DD/YY into the right blanks.
- **Time** - Enter your local time in HH/MM/SS into the right blanks.
- **NTP Server 1 / NTP Server 2** - Enter the address or domain of the **NTP Server 1** or **NTP Server 2**, and then the Router will get the time from the NTP Server preferentially. In addition, the Router built-in some common NTP Servers, so it can get time automatically once it connects the Internet.
- **Enable Daylight Saving** - Check the box to enable the Daylight Saving function.
- **Start** - The time to start the Daylight Saving. Select the month in the first field, the week in the second field, the day in the third field and the time in the last field.
- **End** - The time to end the Daylight Saving. Select the month in the first field, the week in the second field, the day in the third field and the time in the last field.
- **Daylight Saving Status** - Displays the status whether the Daylight Saving is in use.

To set time manually:

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

To set time automatically:

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

To set Daylight Saving:

1. Check the box to enable Daylight Saving.
2. Select the start time from the drop-down lists in the **Start** field.
3. Select the end time from the drop-down lists in the **End** field.
4. Click the **Save** button to save the settings.

		☒ Enable Daylight Saving			
Start:	Mar	3rd	Sun	2am	
End:	Nov	2nd	Sun	3am	
Daylight Saving Status:	daylight saving is down.				
Note: Click the "GET GMT" to update the time from the internet with the pre-defined servers or entering the customized server (IP Address or Domain Name) in the above frames.					

 Note:

- 1) This setting will be used for some time-based functions such as firewall. You must specify your time zone once you login to the router successfully, otherwise, these functions will not take effect.
- 2) The time will be lost if the router is turned off.
- 3) The Router will automatically obtain GMT from the Internet if it is configured accordingly.
- 4) The Daylight Saving will take effect one minute after the configurations are completed.

4.19.2 Diagnostic

Choose menu “**System Tools** → **Diagnostic**”, you can transact Ping or Traceroute function to check connectivity of your network in the following screen.

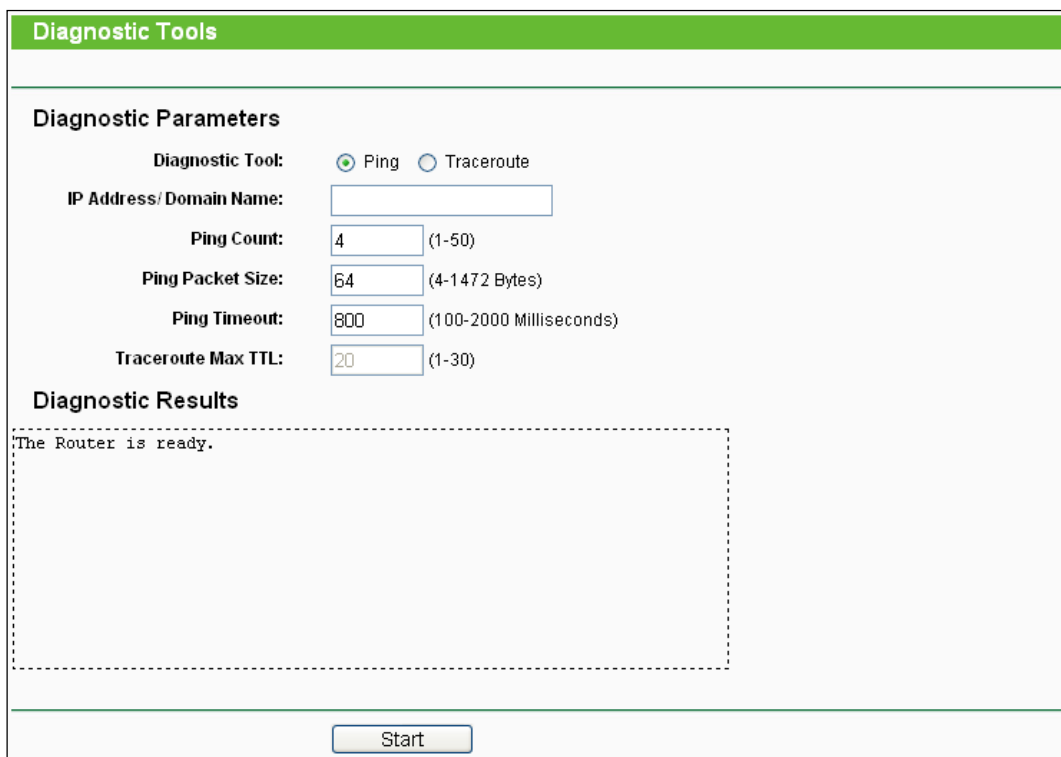


Figure 4-82 Diagnostic Tools

- **Diagnostic Tool** - Check the radio button to select one diagnostic tool.
 - **Ping** - This diagnostic tool troubleshoots connectivity, reachability, and name resolution to a given host or gateway.
 - **Traceroute** - This diagnostic tool tests the performance of a connection.

 Note:

You can use ping/traceroute to test both numeric IP address or domain name. If pinging/tracerouting the IP address is successful, but pinging/tracerouting the domain name is not, you might have a name resolution problem. In this case, ensure that the domain name you are specifying can be resolved by using Domain Name System (DNS) queries.

- **IP Address/Domain Name** - Type the destination IP address (such as 192.168.0.1) or Domain name (such as http://www.tp-link.com).
- **Pings Count** - The number of Ping packets for a Ping connection.
- **Ping Packet Size** - The size of Ping packet.
- **Ping Timeout** - Set the waiting time for the reply of each Ping packet. If there is no reply in the specified time, the connection is overtime.
- **Traceroute Max TTL** - The max number of hops for a Traceroute connection.

Click **Start** to check the connectivity of the Internet.

The **Diagnostic Results** page displays the result of diagnosis.

If the result is similar to the following screen, the connectivity of the Internet is fine.

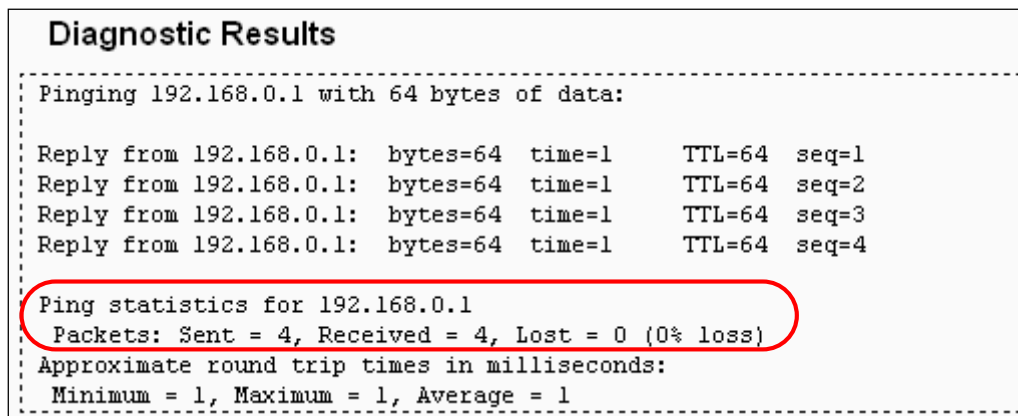


Figure 4-83 Diagnostic Results

Note:

Only one user can use this tool at one time. Options "Number of Pings", "Ping Size" and "Ping Timeout" are used for **Ping** function. Option "Tracert Hops" are used for **Tracert** function.

4.19.3 Firmware Upgrade

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

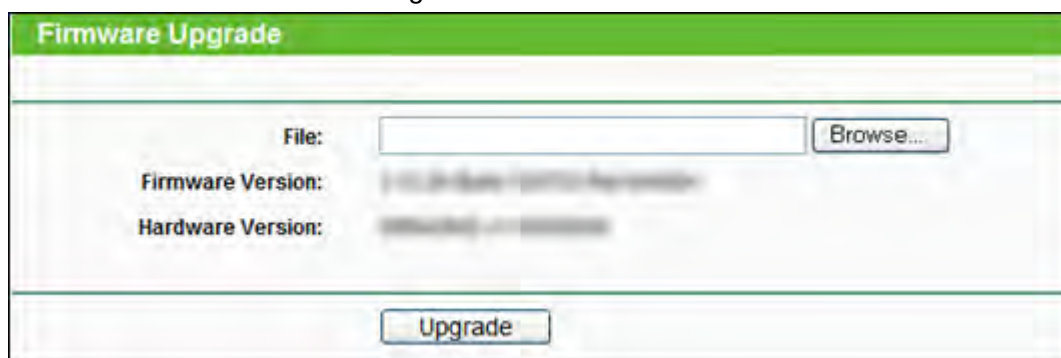


Figure 4-84 Firmware Upgrade

- **Firmware Version** - This displays the current firmware version.

- **Hardware Version** - This displays the current hardware version. The hardware version of the upgrade file must accord with the Router's current hardware version.

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

1. Download a more recent firmware upgrade file from the TP-LINK website (<http://www.tp-link.com>).
2. Type the path and file name of the update file into the **File** field. Or click the **Browse** button to locate the update file.
3. Click the **Upgrade** button.

 Note:

- 1) New firmware versions are posted at <http://www.tp-link.com> and can be downloaded for free. There is no need to upgrade the firmware unless the new firmware has a new feature you want to use. However, when experiencing problems caused by the Router rather than the configuration, you can try to upgrade the firmware.
- 2) When you upgrade the Router's firmware, you may lose its current configurations, so before upgrading the firmware please write down some of your customized settings to avoid losing important settings.
- 3) Do not turn off the Router or press the Reset button while the firmware is being upgraded, otherwise, the Router may be damaged.
- 4) The Router will reboot after the upgrading has been finished.

4.19.4 Factory Defaults

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

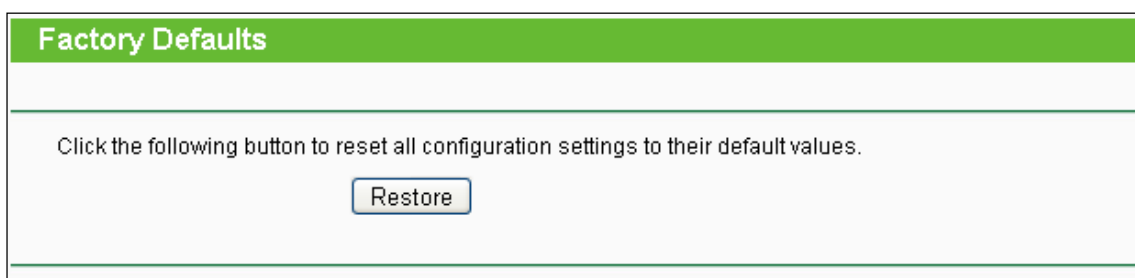


Figure 4-85 Restore Factory Default

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

- The default **User Name**: admin
- The default **Password**: admin
- The default **IP Address**: 192.168.0.1
- The default **Subnet Mask**: 255.255.255.0

Note:

Any settings you have saved will be lost when the default settings are restored.

4.19.5 Backup & Restore

Choose menu “**System Tools** → **Backup & Restore**”, you can save the current configuration of the Router as a backup file and restore the configuration via a backup file as shown in Figure 4-92.

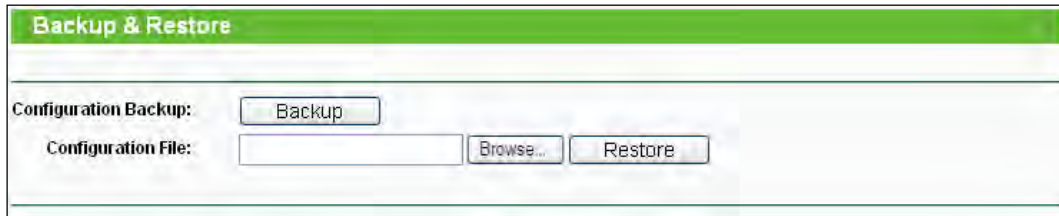


Figure 4-86 Backup & Restore Configuration

- Click the **Backup** button to save all configuration settings as a backup file in your local computer.
- To upgrade the Router's configuration, follow these instructions.
 - Click the **Browse...** button to locate the update file for the Router, or enter the exact path to the Setting file in the text box.
 - Click the **Restore** button.

Note:

The current configuration will be covered by the uploading configuration file. The upgrade process lasts for 20 seconds and the Router will restart automatically. Keep the Router on during the upgrading process to prevent any damage.

4.19.6 Reboot

Choose menu “**System Tools** → **Reboot**”, you can click the **Reboot** button to reboot the Router via the next screen.

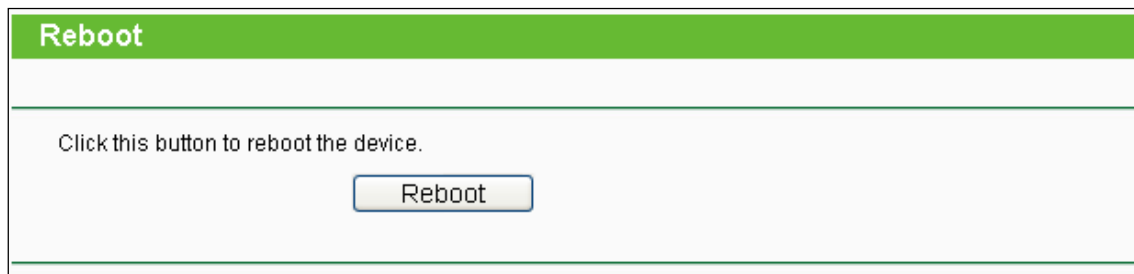


Figure 4-87 Reboot the Router

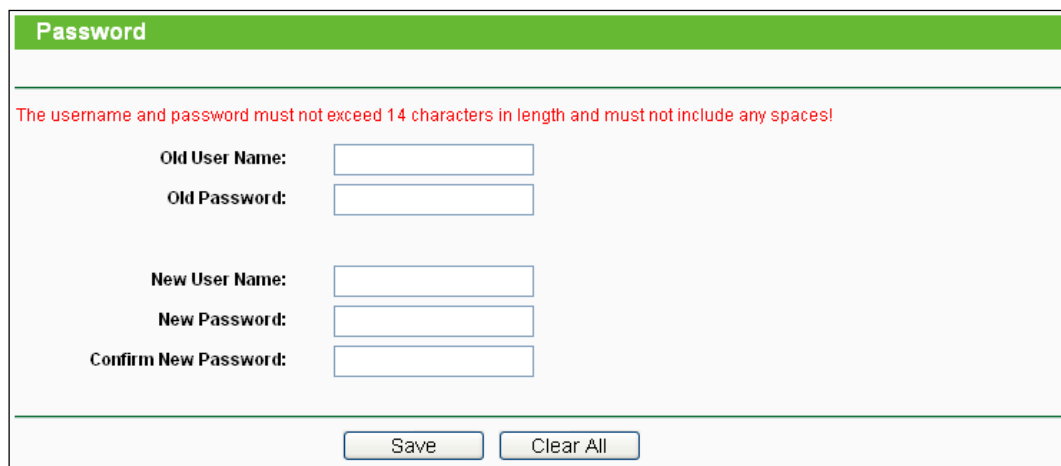
Some settings of the Router will take effect only after rebooting, which include

- Change the LAN IP Address (system will reboot automatically).

- Change the DHCP Settings.
- Change the Working Modes.
- Change the Web Management Port.
- Upgrade the firmware of the Router (system will reboot automatically).
- Restore the Router's settings to factory defaults (system will reboot automatically).
- Update the configuration with the file (system will reboot automatically).

4.19.7 Password

Choose menu “**System Tools** → **Password**”, you can change the factory default user name and password of the Router in the next screen as shown in Figure 4-94.



The screenshot shows the 'Password' configuration page. At the top, there is a green header bar with the word 'Password' in white. Below the header, a red warning message states: 'The username and password must not exceed 14 characters in length and must not include any spaces!'. The form contains six input fields arranged in three pairs. The first pair is labeled 'Old User Name:' and 'Old Password:'. The second pair is labeled 'New User Name:' and 'New Password:'. The third pair is labeled 'Confirm New Password:'. At the bottom of the form, there are two buttons: 'Save' and 'Clear All'.

Figure 4-88 Password

It is strongly recommended that you should change the factory default user name and password of the Router, because all users who try to access the Router's Web-based utility or Quick Setup will be prompted for the Router's default user name and password.

Note:

The new user name and password must not exceed 14 characters in length and not include any spaces. Enter the new Password twice to confirm.

Click the **Save** button when finished.

Click the **Clear All** button to clear all.

4.19.8 System Log

Choose menu “**System Tools** → **System Log**”, you can view the logs of the Router.

System Log

Auto Mail Feature: **Disabled** Mail Settings

Log Type: **ALL** Log Level: **ALL**

Index	Time	Type	Level	Log Content
6	Jul 24 14:31:26	SECURITY	INFO	FTP ALG enabled
5	Jul 24 14:31:26	SECURITY	INFO	IPSEC Passthrough enabled
4	Jul 24 14:31:26	SECURITY	INFO	L2TP Passthrough enabled
3	Jul 24 14:31:26	SECURITY	INFO	PPTP Passthrough enabled
2	Jul 24 14:31:26	DHCP	NOTICE	DHCP server started
1	Jul 24 14:31:21	OTHER	INFO	System started

Time =
H-Ver = : S-Ver =
L = 192.168.0.1 : M = 255.255.255.0
W1 = DHCP : W = 192.168.1.104 : M = 255.255.255.0 : G = 192.168.1.1

Refresh Save Log Mail Log Clear Log

Previous Next Current No. **2** Page

Figure 4-89 System Log

- **Auto Mail Feature** - Indicates whether auto mail feature is enabled or not.
- **Mail Settings** - Set the receiving and sending mailbox address, server address, validation information as well as the timetable for Auto Mail Feature, as shown in Figure 4-96.

Mail Account Settings

From:

To:

SMTP Server:

☒ Authentication

User Name:

Password:

Confirm The Password:

☐ Enable Auto Mail Feature

☒ Everyday, mail the log at : (HH:MM)

☐ Mail the log every hours

Save Back

Figure 4-90 Mail Account Settings

- **From** - Your mail box address. The Router would connect it to send logs.
- **To** - Recipient's address. The destination mailbox where the logs would be received.
- **SMTP Server** - Your smtp server. It corresponds with the mailbox filled in the From field. You can log on the relevant website for Help if you are not clear with the address.
- **Authentication** - Most SMTP Server requires Authentication. It is required by most mailboxes that need User Name and Password to log in.

 Note:

Only when you select **Authentication**, do you have to enter the User Name and Password in the following fields.

- **User Name** - Your mail account name filled in the From field. The part behind @ is included.
- **Password** - Your mail account password.
- **Confirm The Password** - Enter the password again to confirm.
- **Enable Auto Mail Feature** - Select it to mail logs automatically. You could mail the current logs either at a specified time everyday or by intervals, but only one could be the current effective rule. Enter the desired time or intervals in the corresponding field as shown in Figure 4-96

Click **Save** to keep your settings.

Click **Back** to return to the previous page.

- **Log Type** - By selecting the log type, only logs of this type will be shown.
- **Log Level** - By selecting the log level, only logs of this level will be shown.
- **Refresh** - Refresh the page to show the latest log list.
- **Save Log** - Click to save all the logs in a txt file.
- **Mail Log** - Click to send an email of current logs manually according to the address and validation information set in Mail Settings.
- **Clear Log** - All the logs will be deleted from the Router permanently, not just from the page.

Click the **Next** button to go to the next page, or click the **Previous** button return to the previous page.

4.19.9 Statistics

Choose menu "**System Tools** → **Statistics**", you can view the statistics of the Router, including total traffic and the value of the last Packets Statistic Interval in seconds.

Figure 4-91 Statistics

- **Current Statistics Status** - Enable or Disable. The default value is disabled. To enable, click the **Enable** button. If disabled, the function of DoS protection in Security settings will disabled.
- **Packets Statistics Interval (5-60)** - The default value is 10. Select a value between 5 and 60 seconds in the drop-down list. The Packets Statistic interval indicates the time section of the packets statistic.
- **Sorted Rules** – Choose how displayed statistics are sorted.

Select the **Auto-refresh** checkbox to refresh automatically.

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

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

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

Statistics Table:

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

	TCP SYN Tx	The number of TCP SYN packets transmitted to the WAN per second at the specified Packets Statistics interval. It is shown like "current transmitting rate / Max transmitting rate".
Modify	Reset	Reset the value of the entry to zero.
	Delete	Delete the existing entry in the table.

Click **Previous** to return to the previous page and **Next** to the next page.

4.20 Logout

Click the **Logout** tab at the bottom of the main menu, and then the web-page will be logged out and return to the login window.

Appendix A: FAQ

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

- 1) First, configure the ADSL Modem in bridge mode.
- 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, click the **"Network"** menu on the left of your browser, and click **"WAN"** submenu. On the **WAN** page, select "PPPoE" for WAN Connection Type. Type user name in the "User Name" field and password in the "Password" field, finish by clicking **Connect**.

The screenshot shows the 'WAN Connection Type' configuration page. At the top, 'WAN Connection Type' is set to 'PPPoE/Russia PPPoE' with a 'Detect' button next to it. Below this, the 'PPPoE Connection' section contains two fields: 'User Name' with the value 'username' and 'Password' with a masked password represented by ten dots.

Figure A-1 PPPoE Connection Type

- 4) If your ADSL lease is in "pay-according-time" mode, select "Connect on Demand" or "Connect Manually" for Internet connection mode. Type an appropriate number for "Max Idle Time" to avoid wasting paid time. Otherwise, you can select "Auto-connecting" for Internet connection mode.

The screenshot shows the 'Wan Connection Mode' configuration page. Under 'Wan Connection Mode', 'Connect on Demand' is selected with a radio button. Below it, 'Max Idle Time' is set to '15' minutes, with a note '(0 means remain active at all times.)'. Other options like 'Connect Automatically', 'Time-based Connecting', and 'Connect Manually' are unselected. The 'Time-based Connecting' section shows a period of time from 00:00 to 23:59. At the bottom, there are 'Connect', 'Disconnect', and 'Disconnected!' buttons.

Figure A-2 PPPoE Connection Mode

Note:

- 1) Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications is visiting the Internet continually in the background.
- 2) 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?

- 1) Log in to the Router, click the **"Network"** menu on the left of your browser, and click **"WAN"** submenu. On the **WAN** page, select "Dynamic IP" for "WAN Connection Type", finish by clicking **Save**.
- 2) Some ISPs require that you register the MAC Address of your adapter, which is connected

to your cable/DSL Modem during installation. If your ISP requires MAC register, log in to the Router and click the **"Network"** menu link on the left of your browser, and then click **"MAC Clone"** submenu link. On the **"MAC Clone"** page, if your PC's MAC address is proper MAC address, click the **Clone MAC Address** button and your PC's MAC address will fill in the "WAN MAC Address" field. Or else, type the MAC Address into the "WAN MAC Address" field. The format for the MAC Address is XX-XX-XX-XX-XX-XX. Then click the **Save** button. It will take effect after rebooting.

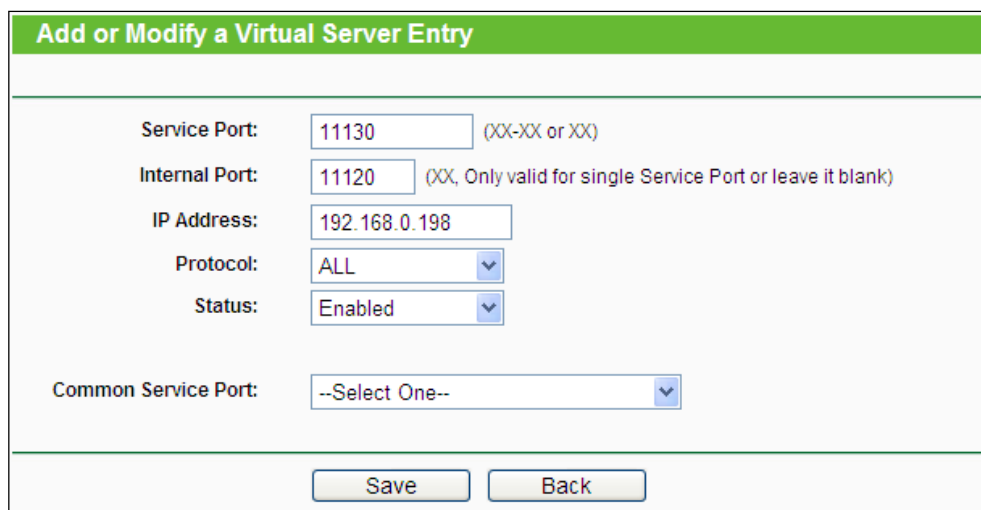
Figure A-3 MAC Clone

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 and make sure the H323 ALG is enabled.
- 3) How to configure Virtual Server: Log in to the Router, click the **"Forwarding"** menu on the left of your browser, and click **"Virtual Servers"** submenu. On the **"Virtual Servers"** page, click **Add New....** Then on the **"Add or Modify a Virtual Server Entry"** page, enter "11130" for the "Service Port" blank, and your IP address for the "IP Address" blank, taking 192.168.0.198 for an example, remember to **Enable** and **Save**.

ID	Service Port	Internal Port	IP Address	Protocol	Status	Modify
1	11130	11120	192.168.0.198	ALL	Enabled	Modify Delete

Figure A-4 Virtual Servers



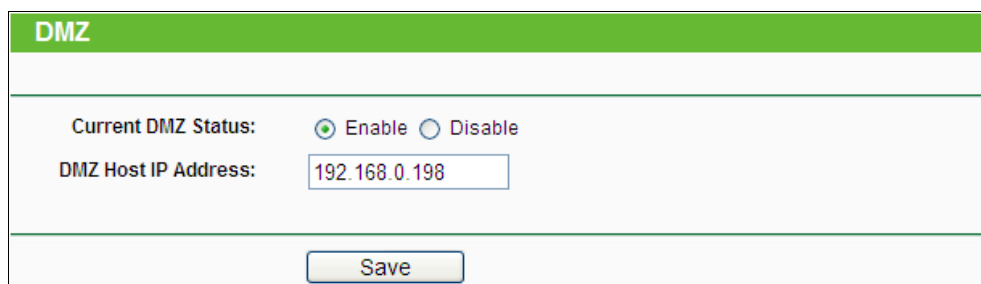
Add or Modify a Virtual Server Entry	
Service Port:	11130 (XX-XX or XX)
Internal Port:	11120 (XX, Only valid for single Service Port or leave it blank)
IP Address:	192.168.0.198
Protocol:	ALL
Status:	Enabled
Common Service Port:	--Select One--
Save Back	

Figure A-5 Add or Modify a Virtual server Entry

 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 “**Forwarding**” menu on the left of your browser, and click “**DMZ**” submenu. On the “DMZ” page, click **Enable** radio button and type your IP address into the “DMZ Host IP Address” field, using 192.168.0.198 as an example, remember to click the **Save** button.



DMZ	
Current DMZ Status:	☒ Enable ☐ Disable
DMZ Host IP Address:	192.168.0.198
Save	

Figure A-6 DMZ

- 5) How to enable H323 ALG: Log in to the Router, click the “**Security**” menu on the left of your browser, and click “**Basic Security**” submenu. On the “**Basic Security**” page, check the **Enable** radio button next to **H323 ALG**. Remember to click the **Save** button.

Basic Security	
Firewall	
SPI Firewall:	☒ Enable ☐ Disable
VPN	
PPTP Passthrough:	☒ Enable ☐ Disable
L2TP Passthrough:	☒ Enable ☐ Disable
IPSec Passthrough:	☒ Enable ☐ Disable
ALG	
FTP ALG:	☒ Enable ☐ Disable
TFTP ALG:	☒ Enable ☐ Disable
H323 ALG:	☒ Enable ☐ Disable
RTSP ALG:	☒ Enable ☐ Disable
Save	

Figure A-7 Basic Security

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

- 1) Because the WEB Server port 80 will interfere with the WEB management port 80 on the Router, you must change the WEB management port number to avoid interference.
- 2) To change the WEB management port number: Log in to the Router, click the "**Security**" menu on the left of your browser, and click "**Remote Management**" submenu. On the "**Remote Management**" page, type a port number except 80, such as 88, into the "Web Management Port" field. Click **Save** and reboot the Router.

Remote Management	
Web Management Port:	88
Remote Management IP Address:	0.0.0.0 (Enter 255.255.255.255 for all)
Save	

Figure A-8 Remote Management

Note:

If the above configuration takes effect, configure to the Router by typing 192.168.0.1:88 (the Router's LAN IP address: Web Management Port) in the address field of the Web browser.

- 3) Log in to the Router, click the "**Forwarding**" 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 "80" into the blank next to the

“**Service Port**”, and your IP address next to the “**IP Address**”, assuming 192.168.0.188 for an example, remember to **Enable** and **Save**.

Virtual Servers						
ID	Service Port	Internal Port	IP Address	Protocol	Status	Modify
1	80	21	192.168.0.188	ALL	Enabled	Modify Delete
Add New... Enable All Disable All Delete All						
Previous Next						

Figure A-9 Virtual Servers

Add or Modify a Virtual Server Entry	
Service Port:	80 (XX-XX or XX)
Internal Port:	21 (XX, Only valid for single Service Port or leave it blank)
IP Address:	192.168.0.188
Protocol:	ALL
Status:	Enabled
Common Service Port:	--Select One--
Save Back	

Figure A-10 Add or Modify a Virtual server Entry

5. The wireless stations cannot connect to the Router.

- 1) Make sure the "**Enable Wireless Router Radio**" is checked and the **Disable Local Wireless Access** is unchecked.
- 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

In this section, we'll introduce how to install and configure the TCP/IP correctly in Windows XP. First make sure your Ethernet Adapter is working, refer to the adapter's manual if necessary.

1. Configure TCP/IP component

- 1) On the Windows taskbar, click the **Start** button, and then click **Control Panel**.
- 2) Click the **Network and Internet Connections** icon, and then click on the **Network Connections** tab in the appearing window.
- 3) Right click the icon that showed below, select Properties on the prompt page.



Figure B-1

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

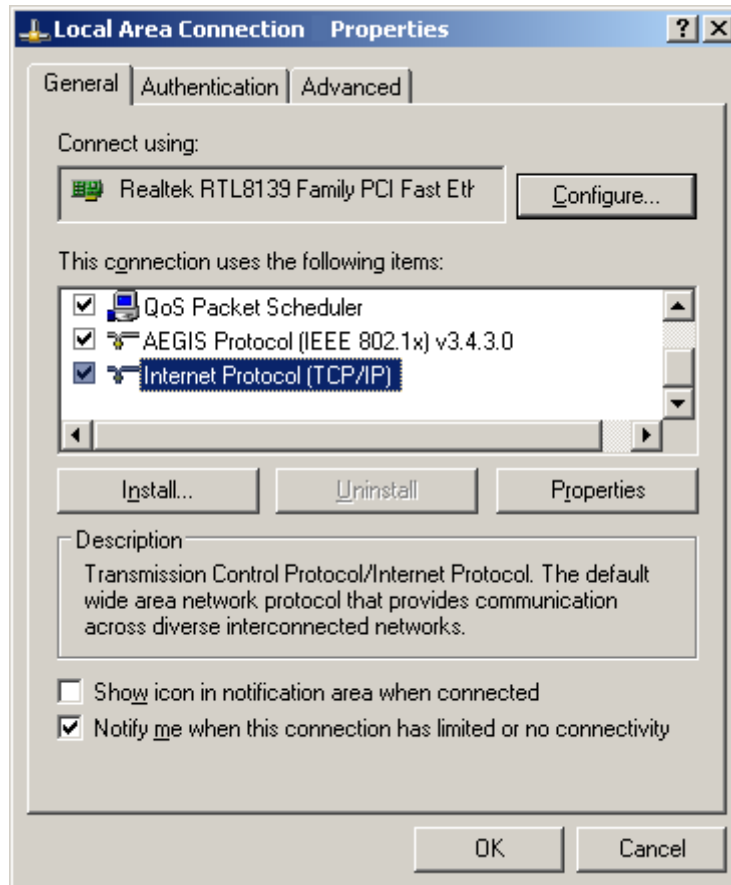


Figure B-2

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

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

➤ **Setting IP address automatically**

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

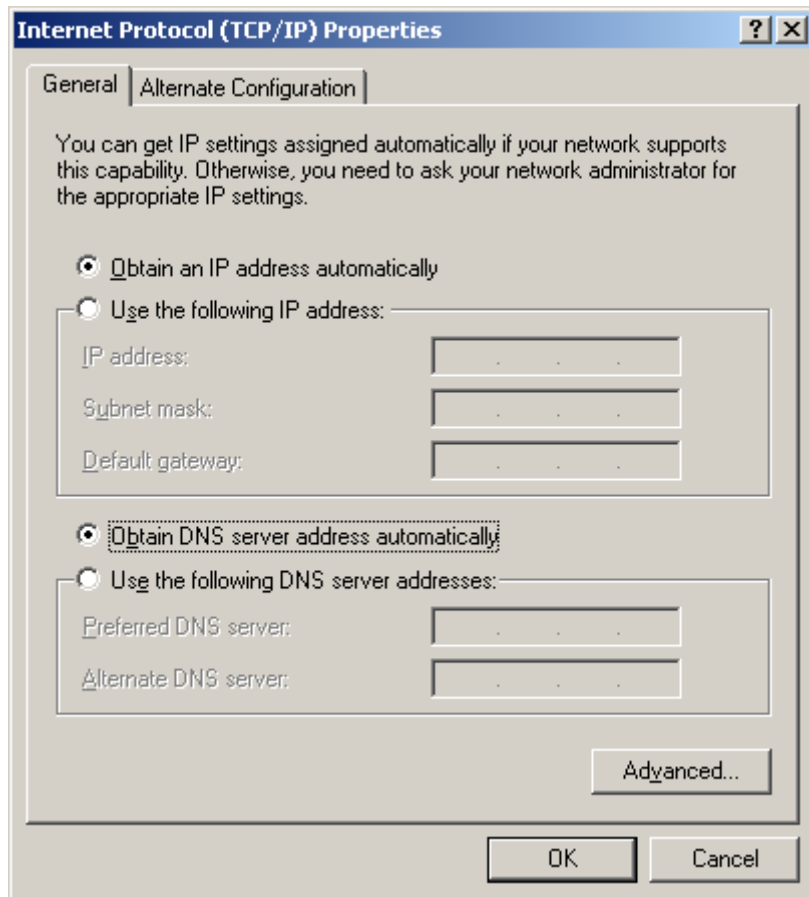


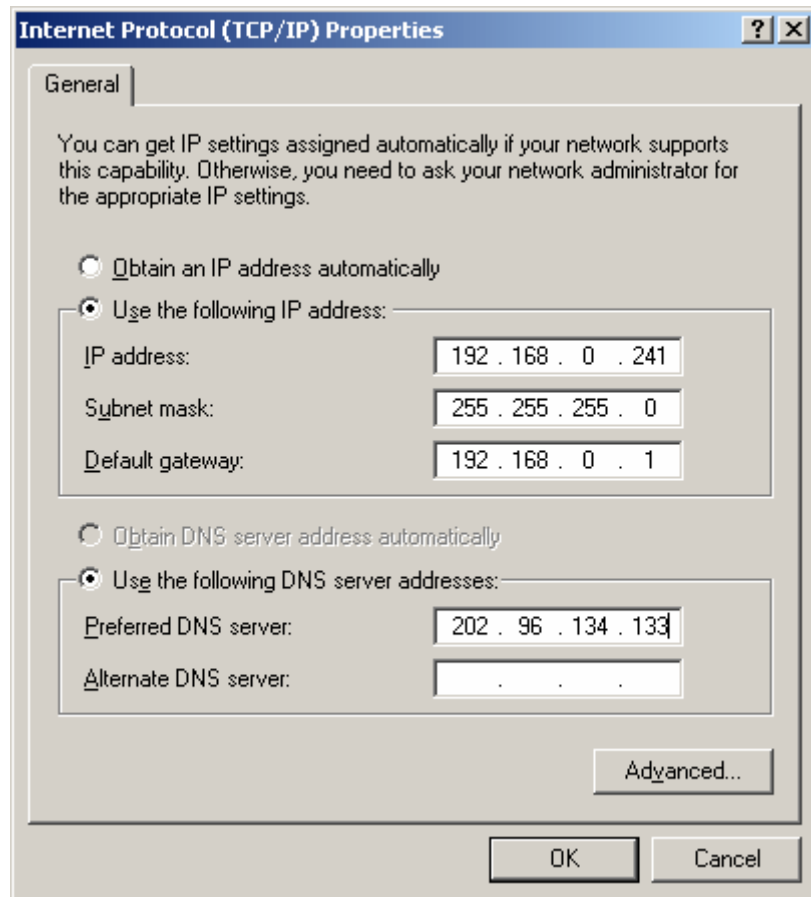
Figure B-3

 Note:

For Windows 98 OS or before, the PC and Router may need to be restarted.

➤ **Setting IP address manually**

- 1 Select **Use the following IP address** radio button. And the following items available
- 2 If the Router's LAN IP address is 192.168.0.1, specify the **IP address** as 192.168.0.x (x is from 2 to 254), and the **Subnet mask** as 255.255.255.0.
- 3 Type the Router's LAN IP address (the default IP is 192.168.0.1) into the **Default gateway** field.
- 4 Select **Use the following DNS server addresses**. In the **Preferred DNS Server** field you can enter the same value as the **Default gateway** or type the local DNS server IP address.



Now click **OK** to keep your settings.

Appendix C: Specifications

General	
Standards	IEEE 802.3, IEEE 802.3u, IEEE 802.11b, IEEE 802.11g and IEEE 802.11n
Protocols	TCP/IP, PPPoE, DHCP, ICMP, NAT, SNTP
Ports	One 10/100M Auto-Negotiation WAN RJ45 port, Four 10/100M Auto-Negotiation LAN RJ45 ports supporting Auto MDI/MDIX
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)
LEDs	⏻ (Power) , 📶 (WLAN), 🌐 (INTERNET), 🖥️ (LAN 1-4), 🔒 (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: -68dBm@10% PER; 130M: -68dBm@10% PER 108M: -68dBm@10% PER; 54M: -68dBm@10% PER 11M: -85dBm@8% PER; 6M: -88dBm@10% PER 1M: -90dBm@8% PER
Environmental and Physical	
Temperature	Operating : 0°C~40°C (32°F~104°F)
	Storage: -40°C~70°C(-40°F~158°F)
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.
- **DDNS (Dynamic Domain Name System)** - The capability of assigning a fixed host and domain name to a dynamic Internet IP Address.
- **DHCP (Dynamic Host Configuration Protocol)** - A protocol that automatically configure the TCP/IP parameters for the all the PC(s) that are connected to a DHCP server.
- **DMZ (Demilitarized Zone)** - A Demilitarized Zone allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing.
- **DNS (Domain Name System)** – An Internet Service that translates the names of websites into IP addresses.
- **Domain Name** - A descriptive name for an address or group of addresses on the Internet.
- **DSL (Digital Subscriber Line)** - A technology that allows data to be sent or received over existing traditional phone lines.
- **ISP (Internet Service Provider)** - A company that provides access to the Internet.
- **MTU (Maximum Transmission Unit)** - The size in bytes of the largest packet that can be transmitted.
- **NAT (Network Address Translation)** - NAT technology translates IP addresses of a local area network to a different IP address for the Internet.
- **PPPoE (Point to Point Protocol over Ethernet)** - PPPoE is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

- **SSID** - A **S**ervice **S**et **I**dentification 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.
- **WEP (Wired Equivalent Privacy)** - A data privacy mechanism based on a 64-bit or 128-bit or 152-bit shared key algorithm, as described in the IEEE 802.11 standard.
- **Wi-Fi** - A trade name for the 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 802.11b devices.
- **WLAN (Wireless Local Area Network)** - A group of computers and associated devices communicate with each other wirelessly, which network serving users are limited in a local area.