User Guide

300Mbps Wireless N 4G LTE Router

TL-MR6400

COPYRIGHT & TRADEMARKS

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

http://www.tp-link.com

CE Mark Warning

CE

This is a class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

RF Exposure Information

This device meets the EU requirements (2014/53/EU Article 3.1a) on the limitation of exposure of the general public to electromagnetic fields by way of health protection.

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

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

EAC

Safety Information

● When product has power button, the power button is one of the way to shut off the product; when there is no power button, the only way to completely shut off power is to disconnect the product or the power adapter from the power source.

● Don't disassemble the product, or make repairs yourself. You run the risk of electric shock and voiding the limited warranty. If you need service, please contact us.

● Avoid water and wet locations.

● Adapter shall be installed near the equipment and shall be easily accessible.

● The plug considered as disconnect device of adapter.

● Use only power supplies which are provided by manufacturer and in the original packing of this product. If you have any questions, please don't hesitate to contact us.

Explanation of the symbols on the product label

Symbol	Explanation
===	DC voltage

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

CONTENTS

About This Guide

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

When using this guide, please notice that features of the router may vary slightly depending on the model and software version you have, and on your location, language, and internet service provider. All screenshots, images, parameters and descriptions documented in this guide are used for demonstration only.

Conventions

In this guide, the following conventions are used:

Convention	Description
Teal Underlined	Hyperlinks are in blue with an underline. You can click to redirect to a website or a specific section.
Teal	Contents to be emphasized and texts on the web page are in teal, including the menus, items, buttons, etc.
→	The menu structures to show the path to load the corresponding page. For example, Network → WAN Settings means the WAN settings configuration page is under the Network menu.
☞ Note	Ignoring this type of note might result in a malfunction or damage to the device.

More Info

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

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

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

A Technical Support Forum is provided for you to discuss our products at http://forum.tp-link.com.

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

Chapter 1. Introduction

1.1 Product Overview

TP-Link's Wireless N 4G LTE router shares the latest generation 4G LTE network with multiple Wi-Fi devices anywhere you want.

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

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

1.2 Product Appearance

1.2.1 LEDs

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

Name	Status	Indication
⏻ (Power)	On	The system has started up successfully.
	Flashing	The system is starting up or firmware is being upgraded. Do not disconnect or power off your modem router.
	Off	Power is off.
(Internet)	On	The router is connected to the internet.
	Off	There is no internet connection.
4G (4G)	On	The router is connected to the 4G network.
	Off	The router is disconnected from the 4G network.

	On	The wireless function is enabled.
(Wireless)	Off	The wireless function is disabled.
	On	At least one LAN port is connected to a powered-on device.
(LAN)	Off	No LAN port is connected to a powered-on device.
	On/Off	This light remains on for 5 minutes when a WPS connection is established, then turns off.
(WPS)	Flashing	WPS connection is in progress. This may take up to 2 minutes.
(Signal Strength)	On	Indicates the signal strength received from the mobile internet network. More lit bars indicate a better signal strength.
	Off	There is no mobile internet signal.

1.2.2   Ports and Buttons

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

Status	Indication
POWER	The power socket is where you will connect the power adapter. Please use the power adapter provided.
POWER ON/OFF	The switch for the power.
LAN (1, 2, 3)	These ports (1, 2, 3) connect the router to the local PC(s).
LAN4/WAN	This port can be LAN or WAN port depending on the working mode.
WPS/RESET	The switch for the WPS function or resetting the modem router. Refer to the note below for more information.
WiFi ON/OFF	This switch is used to enable/disable the router's wireless function.
SIM Card	Insert the SIM card into the slot.

☞ Note:

The WPS/RESET button is used for both WPS and RESET function.

(1) Used as RESET button

With the router powered on, press and hold the WPS/RESET button on the rear panel of the router until the Power LED starts flashing. Wait while the router will restore and reboot automatically.

(2) 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. For details, refer to 4.3 WPS.

☞ Note:

Chapter 2.   Connecting the router

2.1 System Requirements

➢   SIM card with internet access enabled

➢   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 Positioning the Router

➢   Place the router in a well-ventilated place far from any heater or heating vent

➢   Avoid direct irradiation of any strong light (such as sunlight)

➢   Keep at least 2 inches (5 cm) of clear space around the router

➢   Operating Temperature: 0℃~40℃ (32℉~104℉)

➢   Operating Humidity: 10%~90%RH, Non-condensing

2.3 Connecting the Router

The router supports two modes, 3G/4G router mode and Standard Wireless Router mode. You can deploy the mode appropriate to your actual network environment. To connect the router, please take the following steps for different modes.

a.   3G/4G Router Mode

In 3G/4G router mode, with a 3G/4G SIM card, this router can join a 3G/4G network as well as act as a wireless central hub to broadcast its SSID. Thus, the other wireless devices can connect to the router so as to join the same 3G/4G network.
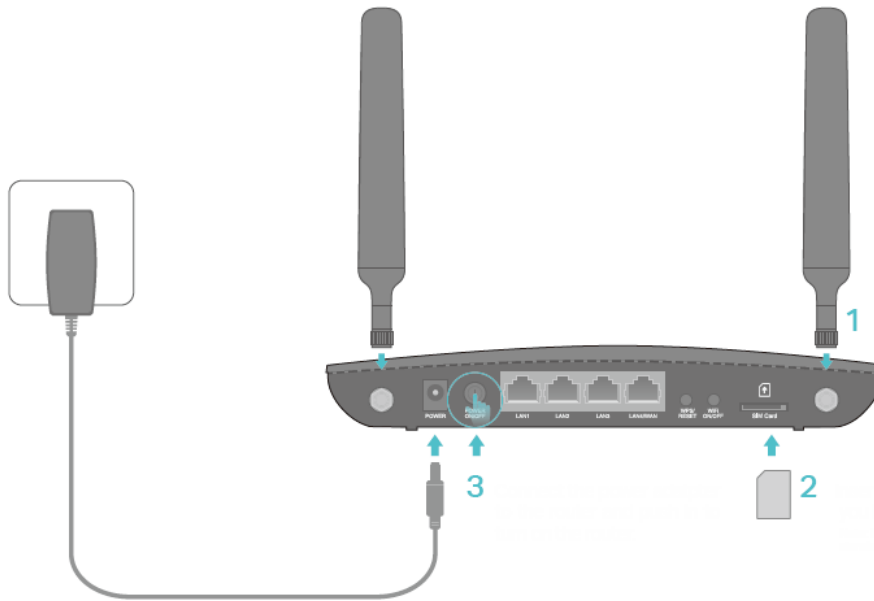
1. Install the 4G LTE antennas and position them upwards.

2. Insert the SIM card into the slot until you hear a click.

    ☞ Note:

    A micro or nano SIM card must be converted using the SIM card adapter provided.

3. Connect the power adapter to the router and push in to turn on the router.

4. Verify the hardware connection by checking the following LEDs' status. If the Internet LED

    ⌇ is on, your router is connected to the internet successfully.

    ☞ Note:

    For better internet connection, make sure 3 or 4 bars of the Signal Strength LED ▮▮▮▮ are lit. Otherwise, try relocating the router to a location that may receive a stronger mobile internet signal, such as near a window.

b. Standard Wireless Router Mode

Before installing the router, make sure your PC is connected to the internet through the broadband service successfully. If there is any problem, please contact your ISP. After that, please install the router according to the following steps. Don't forget to pull out the power plug and keep your hands dry.

1. Power off your modem (if the modem has a backup battery, remove it too.), and disconnect your existing router if you have one.

2. Connect the LAN4/WAN port on your router to the modem's LAN port with an Ethernet cable.

3. Power on the modem and wait for 2 minutes.

4. Make sure the WiFi ON/OFF switch is ON. Then plug the provided power adapter into the power jack and the other end to a standard electrical wall socket. Press the POWER ON/OFF button to power on the router. (Before you power on the router, please make sure your computer is NOT connected to any other wireless network.)

Chapter 3. Quick Installation Guide

This chapter will show you how to configure the basic functions of your 4G LTE router using Quick Setup within minutes.

3.1 3G/4G Router Mode

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

2. Connect your computer to the router (wired or wireless).

   Wired: Connect your computer to the router's LAN port via an Ethernet cable.

   Wireless: Connect wirelessly by using the SSID (network name) and Wireless Password printed on the product label at the bottom of the router.

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

4. After a moment, a login window will appear. Enter admin for the Username and Password, both in lower case letters. Then click Log in or press the Enter key.

☞ **Note:**

If the above screen does not pop-up, it means that your web browser has been set to a proxy. Go to Tools > Internet Options > Connections > LAN Settings, in the screen that appears, cancel the Using Proxy checkbox, and click OK to finish it.

5. Go to Quick Setup and click Next.
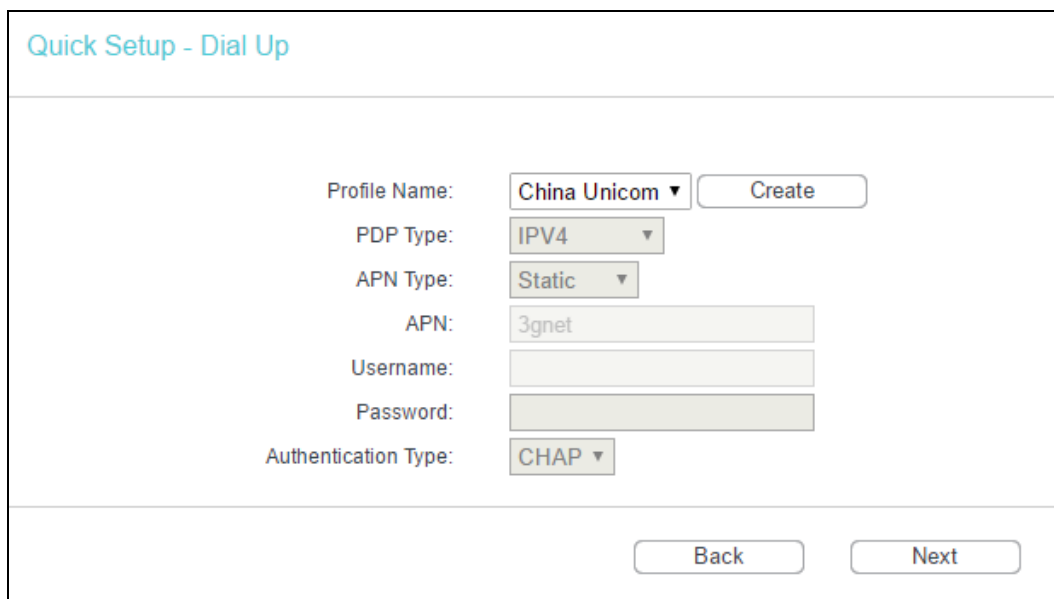
> **Quick Setup**
>
> Run the Quick Setup to manually configure your internet connection and wireless settings.
>
> To continue, please click the **Next** button.
>
> To exit, please click the **Exit** button.
>
> [Exit]   [Next]

6. Choose your Timezone, and then click Next.

7. The Dial Up page shows the ISP information of the SIM card inserted. Click Next to continue if you are sure the information is correct. If these settings are not correct, please click Create to create a new profile with the correct parameters, and then choose the new profile from the Profile Name List.

> **Quick Setup - Dial Up**
>
> Profile Name: [China Unicom ▾]   [Create]
> PDP Type: [IPV4 ▾]
> APN Type: [Static ▾]
> APN: [3gnet]
> Username: [   ]
> Password: [   ]
> Authentication Type: [CHAP ▾]
>
> [Back]   [Next]

8. Set your wireless parameters. It's recommended that you edit the following two items, and then click Next.

    1) Create a unique and easy-to-remember Wireless Network Name.

    2) Select WPA-PSK/WPA2-PSK under Wireless Security and enter a password in the field.

Quick Setup - Wireless

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

Wireless Radio: Enable   ▼

Wireless Network Name: TP-Link_60C4   (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**

Back   Next

9. Click Finish to make the settings effective.

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.
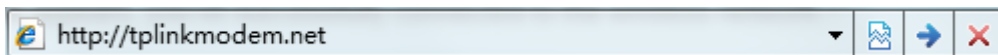
Back   Finish

3.2 Standard Wireless Router Mode

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.

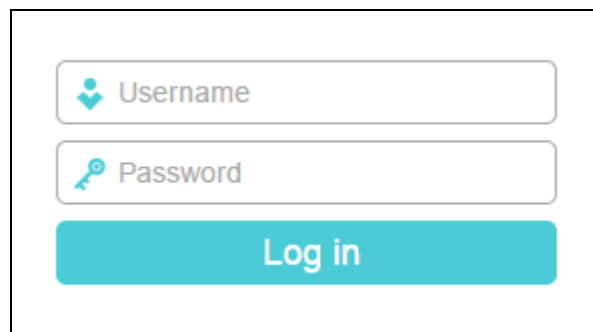2. Connect your computer to the router (wired or wireless).

   Wired: Connect your computer to the router's LAN port via an Ethernet cable.

   Wireless: Connect wirelessly by using the SSID (network name) and Wireless Password printed on the product label at the bottom of the router.

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

   http://tplinkmodem.net
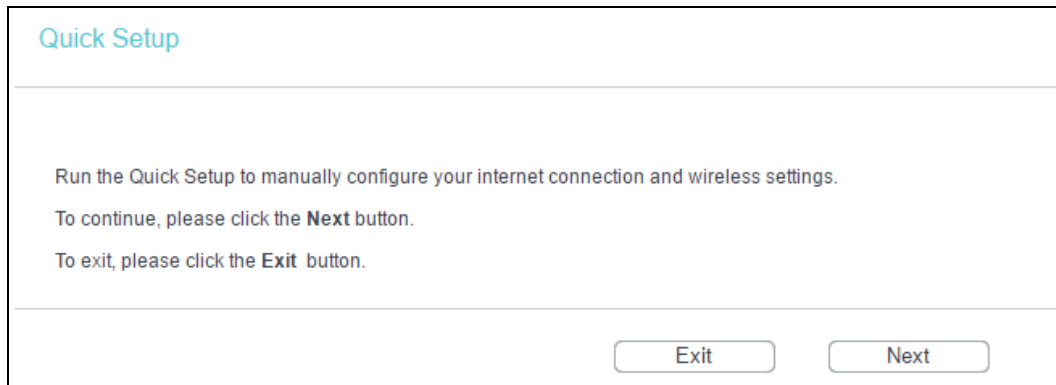
4. After a moment, a login window will appear. Enter admin for the User Name and Password, both in lower case letters. Then click Log in or press the Enter key.

☞ **Note:**

If the above screen does not pop-up, it means that your web browser has been set to a proxy. Go to Tools > Internet Options > Connections > LAN Settings, in the screen that appears, cancel the Using Proxy checkbox, and click OK to finish it.

5. Go to Working Mode page, choose Standard Wireless Router and click Save.

☞ Note:

The router will reboot automatically after you click Save.

6. Log in to the web management page again, go to Quick Setup and click Next to continue.

7. Choose your Timezone, and then click Next.

8. Then WAN Connection Type page will appear. Select your connection type or click Auto-Detect.

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

 Let the router automatically detect the internet connection type provided by your ISP.

○ Dynamic IP (Most Common Cases)

○ 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]

☞ Note:

1) L2TP and PPTP cannot be detected by the router. You must select it manually.
2) Before continuing, please make sure the cable of the WAN port is well connected to your device. If the WAN port is not connected, the cable is unplugged page will appear

Setup Wizard - WAN Connection Type

The cable is unplugged.

Before continuing, please make sure the cable of the WAN port is well connected to your device.

[Back]   [Retry]

9. If you select Auto-Detect, the router will automatically detect the connection type your ISP provides. The appropriate configuration page will be displayed when an active internet service is successfully detected by the router.

● If the connection type is Dynamic IP, the MAC Clone page appears. In most cases, there is no need to clone the MAC address. You can select "No, I am connected by another computer (do NOT clone MAC address)" and then click Next. If it is necessary in your case, please select "Yes, I am connected by the main router (clone MAC address)" and then click Next.

Quick Setup - MAC Clone

Please read help carefully on the right.

○ Yes, I am connected by the main computer (clone MAC address).

◉ No, I am connected by another computer (do NOT clone MAC address).

WAN MAC Address: 3C-46-D8-E0-60-C5   Restore Factory MAC

Your PC's MAC Address: d4-3d-7e-bf-61-5f   Clone MAC Address

Back   Next

● If the connection type is Static IP, the next screen will appear.

Quick Setup - Static IP

IP Address: 0.0.0.0
Subnet Mask: 0.0.0.0
Default Gateway: 0.0.0.0
Primary DNS: 0.0.0.0
Secondary DNS: 0.0.0.0   (Optional)

Back   Next

➢ 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 blank.

➢ Primary DNS - Enter the DNS Server IP address into the blank.

➢ Secondary DNS - If your ISP provides another DNS server, enter it into this field.

● If the connection type is PPPoE/Russian PPPoE, the next screen will appear. Configure the following parameters and then click Next.

Quick Setup - PPPoE

User Name:

Password:

Confirm Password:

Secondary Connection: ⦿ Disabled   ○ Dynamic IP   ○ Static IP   (For Dual Access/Russia PPPoE)

Back   Next

➢ User Name and Password - Enter the User Name and Password provided by your ISP. These fields are case sensitive. If you have difficulty with this process, please contact your ISP.

➢ Confirm Password - Re-enter the password provided by your ISP to ensure the Password you entered is correct.

Check the radio button of Dynamic/Static IP to activate the secondary connection if your ISP provides an extra Connection type such as Dynamic/Static IP to connect to a local area network.

● If the connection type is L2TP/Russian L2TP, the next screen will appear as shown below. Configure the following parameters and then click Next.

Quick Setup - L2TP

User Name:

Password:

Confirm Password:

⦿ Dynamic IP   ○ Static IP

Server IP Address/Name:

Back   Next

➢ User Name and Password - Enter the User Name and Password provided by your ISP. These fields are case sensitive. If you have difficulty with this process, please contact your ISP.

➢ Confirm Password - Re-enter the password provided by your ISP to ensure the password you entered is correct.

Select Dynamic IP if none of IP Address, Subnet Mask, Gateway and DNS server address are provided. Then you just need to enter server IP address or domain name provided by your ISP.

◉ Dynamic IP   ◯ Static IP

Server IP Address/Name: [_____]

Back   Next

Select Static IP if the above parameters have been provided by your ISP. Then please enter server IP address or domain name provided by your ISP, and also enter the corresponding parameters.

◯ 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]

Back   Next

● If the connection type is PPTP/Russian PPTP, the next screen will appear as shown below. Configure the following parameters and then click Next.

Quick Setup - PPTP

User Name: [_____]
Password: [_____]
Confirm Password: [_____]

◉ Dynamic IP   ◯ Static IP

Server IP Address/Name: [_____]

Back   Next

➤ User Name and Password - Enter the User Name and Password provided by your ISP. These fields are case sensitive. If you have difficulty with this process, please contact your ISP.

➤ Confirm Password - Re-enter the password provided by your ISP to ensure the Password you entered is correct.

Select Dynamic IP if none of IP Address/ Subnet Mask/ Gateway and DNS server address are provided. Then you just need to enter server IP address or domain name provided by your ISP.

Select Static IP if the above parameters have been provided by your ISP. Then please enter server IP address or domain name provided by your ISP, and also enter the corresponding parameters.

10. Click Next to continue, the Wireless page will appear as shown below.

Quick Setup - Wireless

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

Wireless Radio: Enable   ▼

Wireless Network Name: TP-Link_60C4   (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**

[Back]   [Next]

➢ Wireless Radio - Enable or disable the wireless function.

➢ Wireless Network Name - Enter a string 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 four 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-PSK/WPA2-PSK based on pre-shared passphrase.

● Wireless 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 Wirelss.

11. Click Finish to complete the Quick Setup.

Quick Setup - Finish

Congratulations! This device is now connecting you to the Internet. For detail settings, please click other menus if necessary.

Back   Finish

Chapter 4.   3G/4G Router Mode

This chapter will show each web page's key functions and the configuration way on 3G/4G Router Mode.

4.1 Login

After your successful login, you will see the main menus on the left of the web management page. On the right, there are the corresponding explanations and instructions.

Status
Quick Setup
WPS
Working Mode
Network
SMS
Wireless
Guest Network
DHCP
Forwarding
Security
Parental Control
Access Control
Advanced Routing
IP & MAC Binding
Dynamic DNS
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 device. All information is read-only.

Status

Firmware Version:	1.0.12 Build 170223 Rel.55038n	
Hardware Version:	MR6400 v2 00000000	
IMEI:	350000000001504	

3G/4G

ISP:	China Unicom
Signal Strength:	75%
Network Type:	LTE
Connection Status:	Connected
IP Address:	10.20.89.190
DNS Server:	210.21.196.6

Traffic Statistics

Total Used:	103.27 KB
Upstream Rate:	0 KB/s
Downstream Rate:	0 KB/s

LAN

MAC Address:	3C-46-D8-E0-60-C4
IP Address:	192.168.1.64
Subnet Mask:	255.255.255.0

Wireless

Wireless Radio:	Enable
Name (SSID):	TP-Link_60C4
Mode:	11bgn mixed
Channel Width:	Automatic
Channel:	Auto (Current channel 1)
MAC Address:	3C-46-D8-E0-60-C4
WDS Status:	Disable

System Up Time:	0 days 17:40:52	Refresh

4.3 WPS

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

a). Choose WPS, and you will see the next screen.

WPS (Wi-Fi Protected Setup)

SSID:	TP-Link_60C4	
WPS Status:	Enabled [Disable WPS]	
Current PIN:	04428121 [Restore PIN] [Gen New PIN]	
	☐ Disable PIN of this device	
Add a new device:	[Add Device]	

➢ WPS Status - Enable or disable the WPS function here.

➢ Current PIN - The current value of this device's PIN displayed here. The default value can be found in the label.

➢ Restore PIN - Restore the PIN of this device to its default.

➢ Gen New PIN - Click this button, and then you can get a new random value for this device'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 the 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 WPS button.

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

You can also keep the default WPS Status as Enabled and click Add Device, then Choose "Press the button of the new device in two minutes" and click Connect.

Add A New Device

○ Enter the new device's PIN.
  PIN: [＿＿＿＿＿＿＿]
◉ Press the button of the new device in two minutes.

[Back] [Connect]

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

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

Use this method if your client device does not have the WPS button, but has a Wi-Fi Protected Setup PIN number.

Step 1: Keep the default WPS Status as Enabled and click Add Device, then the following screen will appear.

Add A New Device

◉ Enter the new device's PIN.
  PIN: [＿＿＿＿＿＿＿]
○ Press the button of the new device in two minutes.

[Back] [Connect]

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

Step 3: "Connect successfully" will appear, 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.
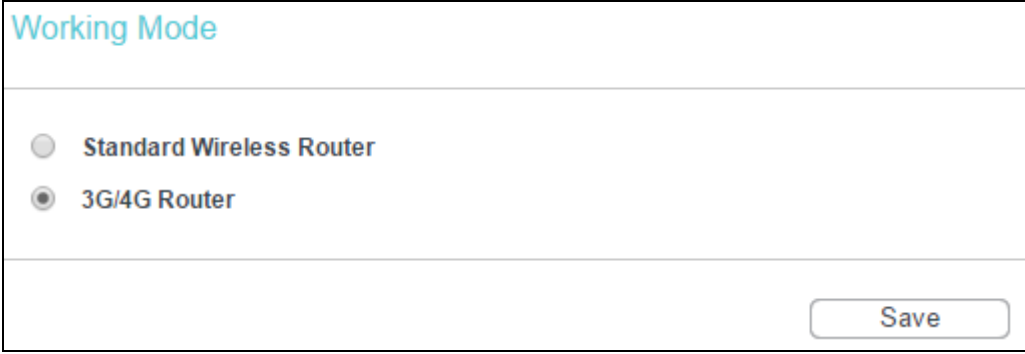
Step 3: When the WPS LED is on, the client device has successfully connected to the router.

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

☞ Note:

1) The WPS LED on the router will light 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.

4.4 Working Mode
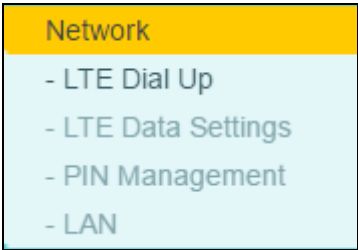
➢ Standard Wireless Router - In this mode, this device will only use LAN/WAN port to access internet. The inner hosts can access internet via 3 LAN ports or wireless.

➢ 3G/4G Router - In this mode, this device enables multiusers to share internet via 3G/4G modem. The LAN/WAN port acts the same as a LAN port while at 3G/4G Router mode.

Click Save to make the settings effective.

☞ Note:

The router will reboot automatically after you click Save.

4.5 Network

There are four submenus under the Network menu: LTE Dial Up, LTE Data Settings, PIN Management and LAN. Click any of them, and you will be able to configure the corresponding function.

4.5.1   LTE Dial Up

Go to Network → LTE Dial Up, you can configure dial-up settings on this page.

➢ Connection Status - Shows whether the internet is connected or disconnected at present.

➢ Mobile Data - It is enabled by default. You can disable it to prohibit internet access.

➢ Data Roaming - It is disabled by default. If disabled, data service is not allowed when roaming. If enabled, data service is allowed when roaming, but may incur significant roaming charges.

➢ Network Mode - The device supports three modes of network connection - 4G Preferred, 4G Only, 3G Only. If your SIM card supports WCDMA, select 3G only; if your SIM card supports LTE, select 4G Preferred or 4G only as you need.

➢ Profile Name - A list of profile for you to select. After selecting one profile from the list, you can further modify its parameters. Show the name of the profile you've selected here.

➢ PDP Type - Select the type of your PDP (Packet Data Protocol).

➢ APN Type - Select the type of your APN, either Dynamic or Static. If you select Dynamic, the device will have dynamic APN, which does not need to be specified. If you select Static, you can manually specify your APN.

➢ APN - Access Point Name, provided by your ISP. You need to set APN only after selecting the static APN type. You are recommended to keep the default value.

➢ Username/Password - Enter the username and password provided by your ISP. These fields are case-sensitive. You are recommended to keep the default value.

➢ Authentication Type - Some ISPs need a specific authentication type, please confirm it with your ISP or keep the default value.

• None - No any authentication is needed.

- PAP - Password Authentication Protocol. This protocol allows the device to establish authentication with the peer using two handshakes. Select this option if the ISP requires this authentication type.

- CHAP - Challenge Handshake Authentication Protocol. This protocol allows the device to establish authentication with the peer using three handshakes and checking the peer identity periodically. Select this option if the ISP requires this authentication type.

Click Delete to delete a profile.

Click Create to create a new profile.

Click Save to make the settings effective.

4.5.2   LTE Data Settings

Go to Network → LTE Data Settings, you can configure data settings on this page.

> Total/Monthly Used - Total/Monthly data used. You can click Correct and input the actual data amount to correct the data.

> Data Limit - You can enable or disable the function of data limit. If enabled, you can set the data quota and usage alert.

> Total/Monthly Allowance - Set the allowed amount of total/monthly data. When data usage exceeds the allowance, the device will disconnect internet and display a message on the screen asking whether to connect internet.

> Monthly Data Statistic - You can enable or disable the function of traffic data resetting.

> Start Date - Enable the function and schedule a date, the data will reset to zero on the date. If disabled, total data information is displayed. If enabled, monthly data information is displayed.

Click Save to make the settings effective.

4.5.3   PIN Management

Go to Network → PIN Management, you can configure PIN code on this page.

PIN Management

SIM Card Status:	PIN disabled
PIN Management:	Enable ▾
PIN:	Remaining Attempts: 3
Auto-unlock PIN upon Power-on:	☐

Apply
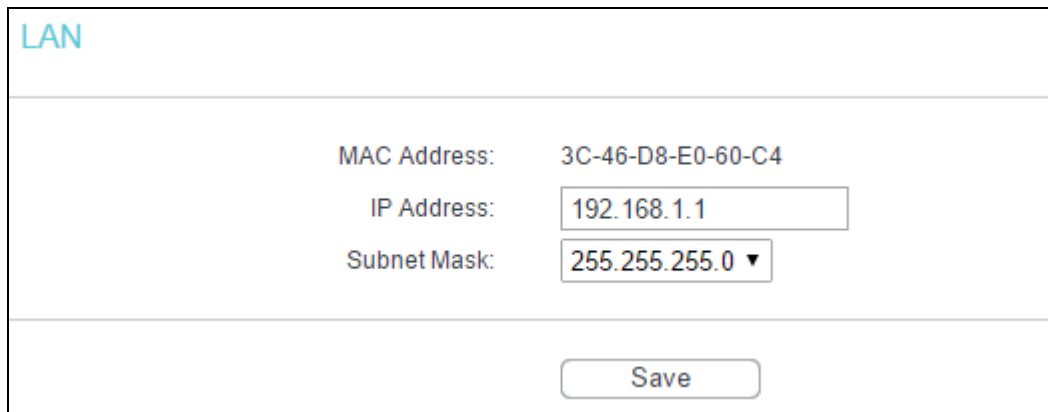
➢ SIM Card Status - Shows the status of your SIM card.

➢ PIN Management - You can select whether to enable this function or not. Once the PIN code function is enabled, every time you start the device with this SIM card inserted, you need to enter the PIN code. But you can go to enable the auto-unlock PIN function, which could save you this trouble.

➢ PIN - Personal Identification Number of the SIM card. It consists of 4-8 digits.

➢ PUK - PIN Unlocked Key. It consists of 8 digits.

➢ Remaining Attempts - Shows how many attempts are left for you to try entering the PIN or PUK code. You have 3 attempts at most for entering the PIN code and 10 attempts at most for entering the PUK code.

➢ Auto-unlock PIN upon Power-on - When the PIN code is required upon device restarting, it will be validated automatically once. If validation failed, you need to enter the PIN code on the Status page.

☞ Note:

1.   If the current status of PIN is disabled, you can select Enable and set a PIN code, and then click Apply to make your settings take effect.

2.   If the SIM current status is PIN enabled and verified, you can select Disable and enter the current PIN code, or select Modify and set a new PIN code, and then click Apply to make your settings take effect.

4.5.4 LAN

Go to Network → LAN, You can configure the IP parameters of LAN on this page.

➤ MAC Address - The physical address of the LAN ports, as seen from the LAN. The value cannot be changed.

➤ IP Address - Enter the IP address of your Router in dotted-decimal notation (factory default - 192.168.1.1).

➤ Subnet Mask - An address code that determines the size of the network. Usually it is 255.255.255.0.

☞ Note:

1. If you change the LAN IP address, you must use the new IP address to log in to the router.

2. If the new LAN IP address you set is not in the same subnet with the previous one, the IP Address pool in the DHCP server will be configured automatically, but the Virtual Server and DMZ Host will not take effect until they are re-configured.

Click Save to make the settings effective.

4.6 SMS
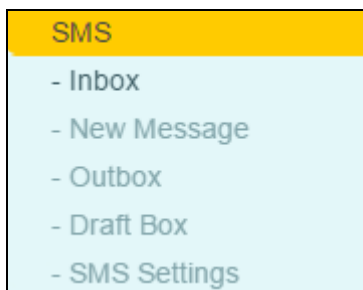
There are five submenus under the Wireless menu: Inbox, New Message, Outbox, Draft Box, SMS Settings. Click any of them, and you will be able to configure the corresponding function.

4.6.1 Inbox

➢ Status - Show the status of message, either read or new.

➢ Phone Number - Shows the phone number that sent this message.

➢ Content - Click to unfold and read the detailed content of the message.

➢ Received - Shows the time when the message was received.

Click Refresh to refresh the inbox, and get any new message.

Click Delete to delete the message(s) you select.

Click Previous to get messages of the previous page.

Click Next to get messages of the next page.

4.6.2 New Message

➢ Phone Number - Enter the receiver's phone number.

➢ Content - Text your message in this box. The message is limited to 160 letters or numbers, any exceeding characters will be sent in the next message.

Click Send to send the message.

Click Save to save the message to the draft box.

4.6.3 Outbox

<table>
<tr><td>Outbox</td><td></td><td></td></tr>
<tr><td>☐</td><td>**Phone Number**</td><td>**Content**</td><td>**Sent**</td></tr>
<tr><td></td><td colspan="3">Refresh   Delete</td></tr>
<tr><td></td><td colspan="3">Previous   Next</td></tr>
</table>

➢ Phone Number - Shows the phone number that this message was planned to be sent to.

➢ Content - Click to unfold and read the detailed content of the message.

➢ Sent - Shows the time when the message was sent.

Click Refresh to refresh the outbox.

Click Delete to delete the message(s) you select.

Click Previous to get messages of the previous page.

Click Next to get messages of the next page.

4.6.4 Draft Box

You can review the unsent saved messages on this page.
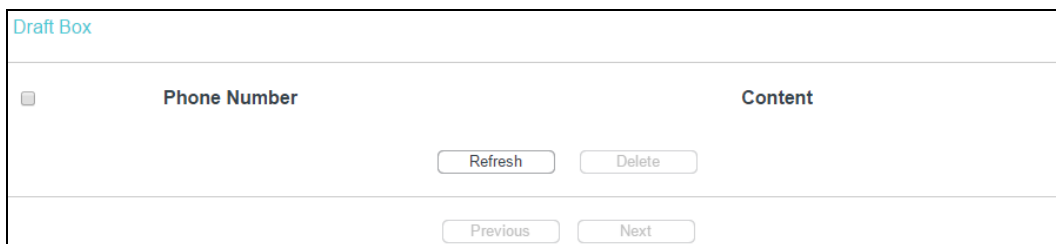
<table>
<tr><td>Draft Box</td><td></td></tr>
<tr><td>☐</td><td>**Phone Number**</td><td>**Content**</td></tr>
<tr><td></td><td colspan="2">Refresh   Delete</td></tr>
<tr><td></td><td colspan="2">Previous   Next</td></tr>
</table>

➢ Phone Number - Shows the phone number that this message was planned to be sent to.

➢ Content - Click to unfold and read the detailed content of the message, or for further edition and delivery.
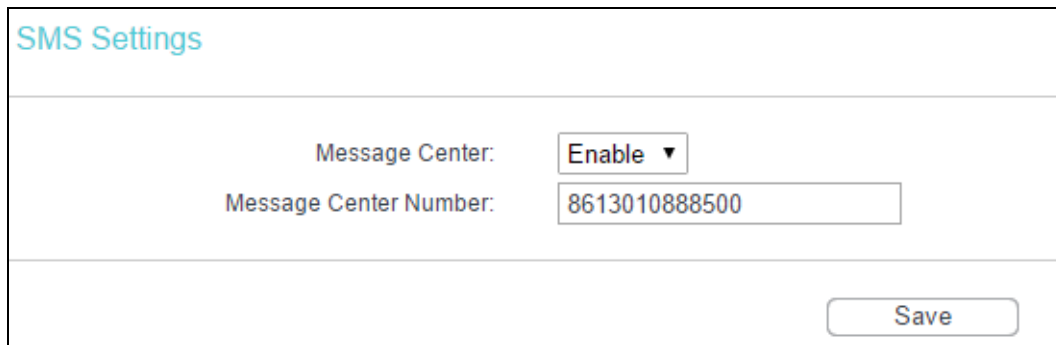
Click Refresh to refresh the drafts.

Click Delete to delete the message(s) you select.

Click Previous to get messages of the previous page.

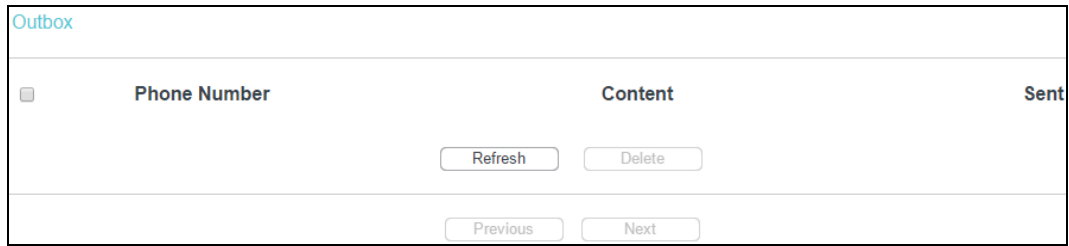Click Next to get messages of the next page.

4.6.5   SMS Settings

SMS Settings

	Message Center:	Enable ▾
	Message Center Number:	8613010888500

Save

➢ Message Center - Disabled by default. Do not enable it unless you want to manually set the message center number.

➢ Message Center Number - When the message center is enabled, you can enter the message center number of the local ISP. If you enter a wrong number, the message function would be affected.

Click Save to make the settings effective.

4.7 Wireless

Wireless
- Wireless Settings
- Wireless Security
- Wireless MAC Filtering
- Wireless Advanced
- Wireless Statistics

There are five submenus under the Wireless menu: 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

Go to Wireless → Wireless Settings, and then you can configure the basic settings for the wireless network on this page.

➢ Wireless Network Name - Enter a value of up to 32 characters. The same Name (SSID) must be assigned to all wireless devices in your network.

➢ Mode - Select transmission mode according to your wireless devices.

➢ Channel Width - The bandwidth of the wireless channel.

➢ Channel - This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point. If you select auto, then AP will choose the best channel automatically.

➢ 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. 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 search the AP which runs in the current channel.

➢ WDS Mode - This field determines which WDS Mode will be used. It is not necessary to change the WDS Mode unless you notice network communication problems with root AP. If you select Auto, then Router will choose the appropriate WDS Mode automatically.

➢ 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.

4.7.2 Wireless Security

Go to Wireless → Wireless Security, and then you can configure the security settings of your wireless network.

> ➢ **Disable Security** - If you do not want to use wireless security, select this check box, but it's strongly recommended to choose one of the following modes to enable security.

> ➢ **WPA/WPA2 – 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 WPA2) automatically based on the wireless station's capability and request.

> • **Encryption** - you can select either Automatic, or TKIP or AES as Encryption.

> ☞ **Note:**

> If you check the WPA/WPA2–Personal (Recommended) radio button and choose TKIP encryption, you will find a notice in red as shown below.

- **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.

- **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.

Click Save to make the settings effective.

➢ **WPA /WPA2 - Enterprise** - It's based on Radius Server.

- **Version** - you can choose the version of the WPA security on the pull-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.
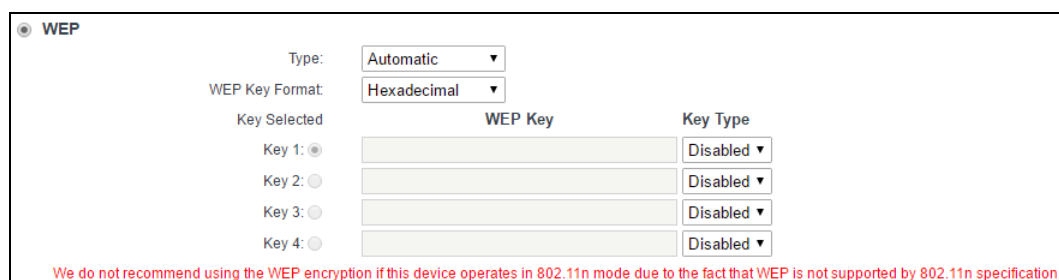
☞ Note:

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

- **Radius Server IP** - Enter the IP address of the Radius Server.

- **Radius Port** - Enter the port that radius service used.

- **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.
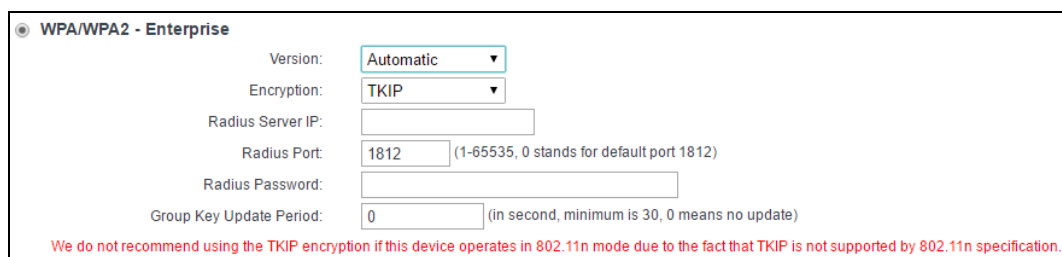
➢ **WEP** - It is based on the IEEE 802.11 standard. If you select this check box, you will find a notice in red as show below.

- Type - you can choose the type for the WEP security on the pull-down list. The default setting is Automatic, which can select Open System or Shared Key authentication type automatically based on the wireless station's capability and request.

- WEP Key Format - Hexadecimal and ASCII formats are provided. 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 (64bit, or 128bit, or 152bit.) for encryption. "Disabled" means this WEP key entry is invalid.

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

128bit - You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, null key is not permitted) or 13 ASCII characters.
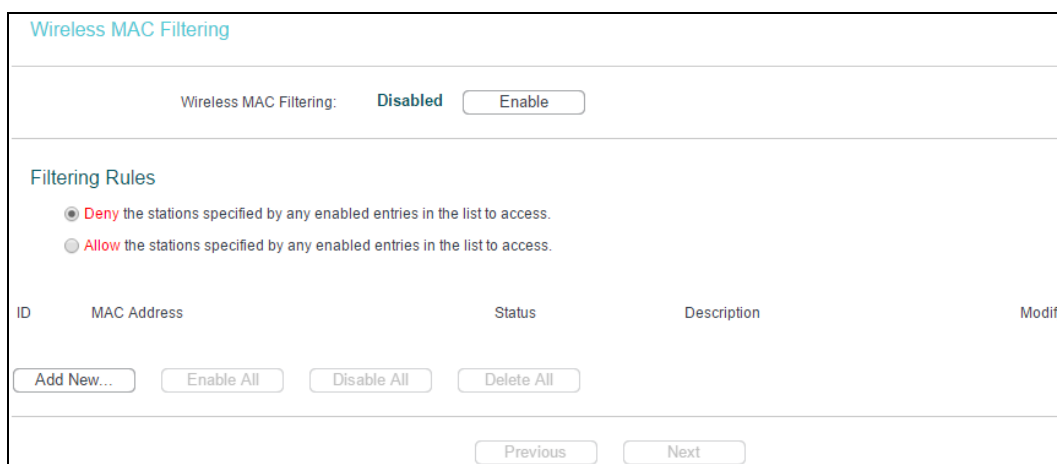
152bit - You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, null key is not permitted) or 16 ASCII characters.

☞ 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.

4.7.3 Wireless MAC Filtering

Go to Wireless → MAC Filtering, and then you can control the wireless access by configuring the Wireless MAC Address Filtering function.

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

➢ MAC Address - The wireless station's MAC address that you want to filter.

➢ Status - The status of this entry is either Enabled or Disabled.

➤ Description - A simple description of the wireless station.

To Add a Wireless MAC Address filtering entry, click Add New…. The Add or Modify Wireless MAC Address Filtering entry page will appear:

Add or Modify Wireless MAC Address Filtering entry	
MAC Address:	[ ]
Description:	[ ]
Status:	Enabled ▾
	Save Back

To add 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-00-07-8A.

2. Enter a simple description of the wireless station in the Description field. For example: Wireless station A.

3. Status - Select Enabled or Disabled for this entry on the Status drop-down list.

4. Click Save.

To modify an existing entry:

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

Click Delete in the entry you want to delete to delete an existing entry.

Click Enable All to make all entries enabled.

Click Disable All to make all entries disabled.

Click Delete All to delete all entries.

Click Next to go to the next page.

Click Previous to return to the previous page.

For example: If you desire that the wireless station A with MAC address 00-0A-EB-00-07-8A and the wireless station B with MAC address 00-0A-EB-00-23-11 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 Enable to enable this function.

2. Select the radio button: Allow the stations not 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 Add New... and enter the MAC address 00-0A-EB-00-07-8A /00-0A-EB-00-23-11 in the MAC Address field, then enter wireless station A/B in the Description field, while select Enabled in the Status drop-down list. Finally, click Save.

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

4.7.4 Wireless Advanced

Go to Wireless → Wireless Advanced, and then you can configure the advanced settings of your wireless network.

- ➢ Transmit Power - Here you can specify the transmit power of this device. You can select High, Middle or Low which you would like. High is the default setting and is recommended.

- ➢ Beacon Interval - The beacons are the packets sent by this device to synchronize a wireless network. Beacon Interval value determines the time interval of the beacons. You can specify a value between 40-1000 milliseconds. 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, this device 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 since excessive packets. 2346 is the default setting and is recommended. (This value for the mode of 11N series can not be changed)

- ➢ DTIM Interval - This value determines the interval of the Delivery Traffic Indication Message (DTIM). 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 enabled.

- ➢ Enable Short GI - This function is recommended for it will increase the data capacity by reducing the guard interval time.

- ➢ Enable AP Isolation - Isolate all connected wireless stations so that wireless stations cannot access each other through WLAN. This function will be disabled if WDS/Bridge is enabled.

☞ 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

Go to Wireless → Wireless Statistics, and then you can see the MAC Address, Current Status, Received Packets and Sent Packets for each connected wireless station.

➢ 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 is enabled, deny the station to access.

Allow: if the Wireless MAC Filtering function is enabled, 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 Refresh.

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

☞ Note:

This page will be refreshed automatically every 5 seconds.

4.8 Guest Network
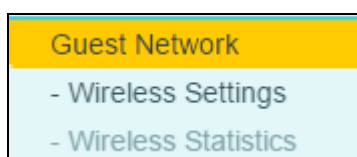
There are two submenus under the Guest Network menu: Wireless Settings and Wireless Statistics. Click any of them, and you will be able to configure the corresponding function.

4.8.1 Wireless Settings

Go to Guest Network → Wireless Settings, you can configure the basic settings for the Guest network on this page.

Guest Network Wireless Settings

Access

Allow Guest To Access My Local Network: ☐

Wireless

Guest Network: ☐

Network Name: TP-Link_GUEST_60C4 (Also called the SSID)

Wireless Security: Disable Security ▼

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.

➢ **Guest Network** - 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 the time the wireless stations could accessing the router.

4.8.2 Wireless Statistics

Go to Guest Network → Wireless Statistics, and then you can see the MAC Address, Current Status, Received Packets and Sent Packets for each connected wireless station.

Guest network Wireless Statistics

Current Connected Wireless Stations numbers: 0 Refresh

Previous Next

➢ **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 Refresh.

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

☞ Note:

This page will be refreshed automatically every 5 seconds.

4.9　DHCP

There are three submenus under the DHCP menu: 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

Go to DHCP → DHCP Settings, and then you can configure the DHCP Server on the page. 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.

➢ **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. 192.168.1.100 is the default start address.

➢ **End IP Address** - Specify an IP address for the DHCP Server to end with when assigning IP addresses. 192.168.1.199 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) Suggest to input the IP address of the LAN port of the router, default value is 192.168.1.1.

➢ **Default Domain** - (Optional) Input the domain name of your network.

➢ **Primary DNS** - (Optional) Input the DNS IP address provided by your ISP. 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" mode. This function will take effect until this device reboots. Click Save to make the settings effective.

4.9.2 DHCP Client List

Go to DHCP → DHCP Client List, and then you can view the information about the clients attached to the router in the next screen.

ID	Client Name	MAC Address	Assigned IP	Lease Time
1	TP-Link	CC-08-8D-19-0A-35	192.168.1.105	01:59:56

Refresh

➢ **ID** - The index of the DHCP Client.

➢ **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.
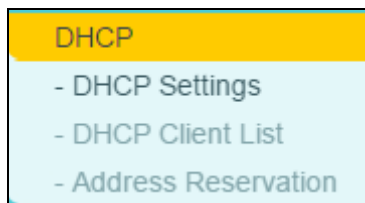
➢ Lease Time - The time of the DHCP client leased.

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

4.9.3 Address Reservation

Go to DHCP → Address Reservation, and then you can view and add a reserved address for clients. 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.

➢ MAC Address - The MAC address of the PC for which you want to reserve IP address.
➢ Reserved IP Address - The IP address of the router reserved.
➢ Status - The status of this entry is either Enabled or Disabled.

To Reserve IP addresses:

1. Click Add New ….

2. Enter the MAC Address (The format for the MAC Address is XX-XX-XX-XX-XX-XX) and the IP address in dotted-decimal notation of the computer you wish to add.

3. Click Save.

To modify an existing entry:

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

3. Click Save.

Click Delete in the entry you want to delete to delete an existing entry.

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

Click Delete All to delete all entries.

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

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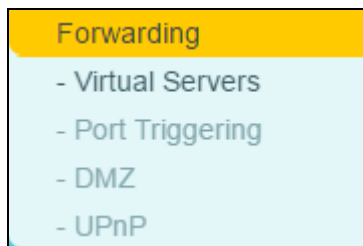
There are four submenus under the Forwarding menu: Virtual Servers, Port Triggering, DMZ and UPnP. Click any of them, and you will be able to configure the corresponding function.

4.10.1 Virtual Servers

Go to Forwarding → Virtual Servers, you can view and add virtual servers. Virtual servers can be used for setting up public services on your LAN. A virtual server is defined as a service port, and all requests from internet to this service port will be redirected to the computer specified by the server IP. Any PC that was used for a virtual server must have a static or reserved IP address because its IP address may change when using the DHCP function.
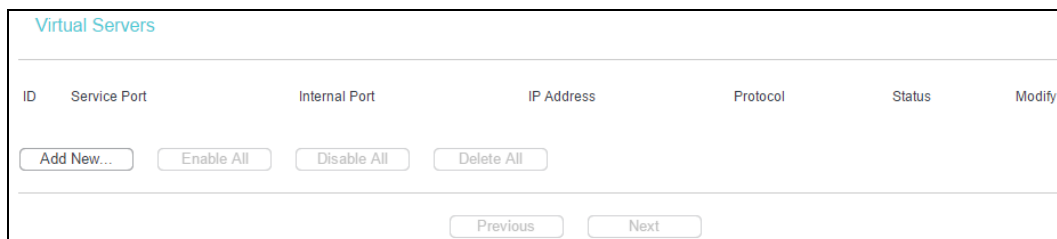
➢   Service Port - The numbers of External Service Ports. You can enter a service port or a range of service ports (the format is XXX - YYY, XXX is Start port, YYY is End port).

➢   Internal Port - The Internal Service Port number of the PC running the service application. You can enter a specific port number, or leave it blank if the Internal Port is the same as the Service Port.

➢   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, "Enabled" means the virtual server entry is enabled. The status of this entry is either Enabled or Disabled.

To setup a virtual server entry:

1. Click Add New….

Add or Modify a Virtual Server Entry

Service Port:	[ ] (XX-XX or XX)
Internal Port:	[ ] (XX, Enter a specific port number or leave it blank)
IP Address:	[ ]
Protocol:	All ▼
Status:	Enabled ▼
Common Service Port:	--Select One-- ▼

Save   Back

2. Select the service 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 number of the service port 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 or UDP, or All.

5. Select Enabled to enable the virtual server.

6. Click Save.

☞ Note:

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

To modify an existing entry:

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

Click Delete in the entry you want to delete to delete an existing entry.
Click Enable/Disable All to make all entries enabled/ disabled.
Click Delete All to delete all entries.
Click Next to go to the next page and click Previous 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

Go to Forwarding → Port Triggering, you can view and add port triggering in the next screen. Some applications require multiple connections, like internet games, video conferencing, internet telephoning and so on. Port Triggering is used for some of these applications that cannot work with a pure 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

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 Port** - The port or port range used by the remote system when it responds to the outgoing request. A response using one of these ports will be forwarded to the PC that triggered this rule. You can input at most 5 groups of ports (or port section). 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 is 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.

Add or Modify a Port Triggering Entry

Trigger Port:

Trigger Protocol: All ▼

Incoming Ports:

Incoming Protocol: All ▼

Status: Enabled ▼

Common Applications: --Select One-- ▼

Save   Back

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 Save to save the new rule.

To modify an existing entry:

1. Click the Modify in the entry you want to modify.

2. Modify the information.

3. Click Save.

Click Delete in the entry you want to delete to delete an existing entry.

Click Enable All to make all entries enabled

Click Disable All to make all entries disabled.

Click Delete All to delete all entries.

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

☞ Note:

1) When the trigger connection is released, the according opening ports will be closed.

2) Each rule can only be used by one host on the LAN at a time. The trigger connection of other hosts on the LAN will be refused.

3) Incoming Port Ranges cannot overlap each other.

4.10.3 DMZ

Go to Forwarding → DMZ, you can view and configure DMZ host in the screen. The DMZ host feature allows one local host to be exposed to the internet for a special-purpose service such as internet gaming or video conferencing. The router forwards packets of all services to the DMZ host. Any PC that is set to be DMZ host must have its DHCP client function disabled and should have a new static IP address assigned to it because its IP Address may change when using the DHCP function.

```
DMZ

    Current DMZ Status:       ○ Enable ● Disable
    DMZ Host IP Address:      [ 0.0.0.0                    ]

                                              [ Save ]
```

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

1. Click the Enable radio button

2. Enter the local host IP Address in the DMZ Host IP Address field

3. Click Save.

4.10.4 UPnP

Go to Forwarding → UPnP, you can view the information about UPnP (Universal Plug and Play) in the screen. 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.

```
UPnP

Current UPnP Status:     Enabled                    [ Disable ]

    Current UPnP Settings List
      ID    App Description      External Port      Protocol      Internal Port      IP Address      Status

                                               [ Refresh ]
```

➢ Current UPnP Status - UPnP can be enabled or disabled by clicking the Enable or Disable button. This feature is enabled by default.

➢ Current UPnP Settings List - This table displays the current UPnP information.

- App Description - The description provided by the application in the UPnP request

- External Port - External port, which the router opened for the application.

- Protocol - Shows which type of protocol is opened.

- Internal Port - Internal port, which the router opened for local host.

- IP Address - The UPnP device that is currently accessing the router.

- Status - The port's status displayed here. "Enabled" means that port is still active. Otherwise, the port is inactive.

Click Enable to enable UPnP.

Click Disable to disable UPnP.

Click Refresh to update the Current UPnP Settings List.

4.11 Security
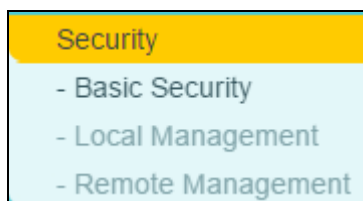
There are three submenus under the Security menu: Basic Security, Local Management and Remote Management. Click any of them, and you will be able to configure the corresponding function.

4.11.1 Basic Security

Go to Security → Basic Security, you can configure the 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 - 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, click Enable.

• L2TP Passthrough - Layer Two Tunneling Protocol (L2TP) is the method used to enable Point-to-Point sessions via the internet on the Layer Two level. To allow L2TP tunnels to pass through the router, click Enable.

• 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, click Enable.

➢ 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, click Enable.

• TFTP ALG - To allow TFTP clients and servers to transfer data across NAT, click Enable.

• H323 ALG - To allow Microsoft NetMeeting clients to communicate across NAT, click Enable.

• RTSP ALG - To allow some media player clients to communicate with some streaming media servers across NAT, click Enable.

• SIP ALG - To allow some multimedia clients to communicate across NAT, click Enable.

Click Save to make the settings effective.

4.11.2 Local Management

Go to Security → Local Management, you can configure the management rule. The management feature allows you to deny LAN computers from accessing the router.

Local Management

Management Rules

⦿ All the PCs on the LAN are allowed to access the Router's Web-Based Utility

◯ Only the PCs listed can browse the built-in web pages to perform Administrator tasks

MAC 1:

MAC 2:

MAC 3:

MAC 4:

Your PC's MAC Address: 50-E5-49-1E-06-80   Add

Save

By default, the radio button All the PCs on the LAN are allowed to access the Router's Web-Based Utility is selected. 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, click 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 the MAC address listed can use the password to browse the built-in web pages to perform Administrator tasks and all the others will be blocked.

After click Add, your PC's MAC Address will be placed in the Control List above.

Click Save to make the settings effective.

☞ Note:

If your PC is blocked and you want to access the router again, press and hold down the WPS/RESET button on the rear panel of the router until the Power LED starts flashing to reset the router's factory defaults in the router's web management page.

4.11.3 Remote Management

Go to Security → Remote Management, you can configure the Remote Management function. 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

➢ 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 65535 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.

To access the router, you should enter your router's WAN IP address into your browser's address (in IE) or location (in Netscape) box, followed by a colon and the custom port number you set in the Web Management Port box. For example, if your Router's WAN address is 202.96.12.8 and you use port number 8080, enter http://202.96.12.8:8080 in your browser. You will be asked for the router's password. After successfully entering the password, you will be able to access the router's web management page.

☞ Note:

1) Some ports are commonly used for other services (Such as 21, 25, 110, 119, 139, 145 and 445). For security reasons, these ports will be restricted.

2) Be sure to change the router's default password to a secure password.

3) If the web management port conflicts with the one used for a Virtual Server entry, the entry will be automatically disabled after the setting is saved.

4.12 Parental Control

Choose menu Parental Control, and you can configure the parental control. The Parental Control function can be used to control the internet activities of the child, limit the child to access certain websites and restrict the time of surfing. On this page, you can create the rule.

➢ 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 Copy To Above 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 Add New… and the next screen will pop-up.

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

Save   Back

2. Enter the MAC address of the PC (e.g. 00-11-22-33-44-AA) you'd like to control in the MAC Address of Children's 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 Website Name field. Any domain name with keywords in it (www.tp-link.com, www.tp-link.com.cn) 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 Save.

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

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

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

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

For example: If you desire that the child 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. Choose Parental Control menu 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, then click Save.

2. Go to Access Control → Schedule 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, then click Save.

3. Choose Parental Control menu to go back to the Add or Modify Parental Control Entry page:

   1) Click Add New....

   2) Enter 00-11-22-33-44-AA in the MAC Address of Children's PC field.

   3) Enter "Allow TP-Link" in the Website Description field.

   4) Enter "www.tp-link.com" in the Allowed Website Name field.

   5) Select "Schedule_1" you create just now from the Effective Time drop-down list.

   6) 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.

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
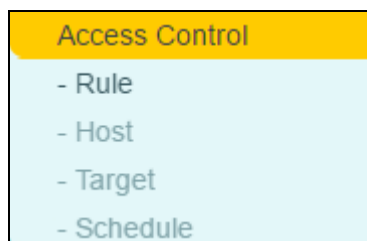
4.13 Access Control

There are four submenus under the Access Control menu: Rule, Host, Target and Schedule. Click any of them, and you will be able to configure the corresponding function.

4.13.1 Rule

Go to Access Control → Rule, and then you can view and set Access Control rules.

> ➢ 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.

> ➢ Enable - Here displays the status of the rule, enabled or not. Check this option to enable a specific entry.

> ➢ Modify - Here you can edit or delete an existing rule.

> ➢ Move - You can change the entry's order as desired. Enter in the first box the ID number of the entry you want to move and in the second box another ID number, and then click the Move button to change the entries' order.

Click Setup Wizard to create a new rule entry.

Click Add New... to add a new rule entry.

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

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

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

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

There are two methods to add a new rule.

Method One:

1. Click Setup Wizard and the next screen will appear.

Quick Setup - Create a Host Entry

Mode: IP Address ▼

Host Description:

LAN IP Address: ___ - ___

Back   Next

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

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

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. 192.168.1.23).

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.

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

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

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

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. 192.168.1.23).

➢ 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.cn) will be blocked or allowed.

3. Click Next when finishing creating the access target entry, and the next screen will appear.

Quick Setup - Create an Advanced Schedule Entry

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)

Back   Next

➢ 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.

Quick Setup - Create an Internet Access Control Entry

Rule Name:	
Host:	Host_1 ▼
Target:	Target_1 ▼
Schedule:	Schedule_1 ▼
Status:	Enabled ▼

Back   Finish

➢ Rule Name - 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 filed, 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, Enable or Disable. Select Enable so that the rule will take effect. Select Disable so that the rule won't take effect.

5. Click Finish to complete adding a new rule.

Method Two:

1. Click Add New… and the next screen will pop up as.

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-sown 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 Save.

Add Internet Access Control Entry

Rule Name:	[ ]
Host:	Host_1 ▼ Click Here To Add New Host List.
Target:	Any Target ▼ Click Here To Add New Target List.
Schedule:	Anytime ▼ Click Here To Add New Schedule.
Status:	Enabled ▼

[Save]   [Back]

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", then click Save.

2. We recommend that you click Setup Wizard 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, then click Save.

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, then click Save.

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, then click Save.

6. Click the submenu Rule of Access Control in the left, Click Add New... button to add a new rule as follows:

    1) In Rule Name field, create a name for the rule. Note that this name should be unique, for example Rule_1.

    2) In Host field, select Host_1.

    3) In Target field, select Target_1.

    4) In Schedule field, select Schedule_1.

    5) In Status field, select Enable.

    6) 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	Status	Modify
1	Rule_1	Host_1	Target_1	Schedule_1	☑	Edit Delete

4.13.2 Host

Go to Access Control → Host, you can view and set a Host list. The host list is necessary for the Access Control Rule.

Host Settings			
ID	Host Description	Information	Modify
1	Host_1	IP: 192.168.1.23	Edit Delete

Add New...   Delete All

Previous   Next   Current No. 1 ▼ Page

➢ **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 Add New….

2. In the Mode field, select IP Address or MAC Address.

- If you select IP Address, you will see the screen shown as below.

Add or Modify a Host Entry

Mode: IP Address ▼
Host Description:
LAN IP Address: -

Save   Back

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, you will see the screen shown as below.

Add or Modify a Host Entry

Mode: MAC Address ▼
Host Description:
MAC Address:

Save   Back

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 Save to complete the settings.

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

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

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... 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

Go to Access Control → Target, you can view and set a Target list. The target list is necessary for the Access Control Rule.

ID	Target Description	Information	Modify

Target Settings

Add New...   Delete All

Previous   Next   Current No. 1 ▼ Page

➢ **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 Add New….

2. In Mode field, select IP Address or Domain Name.

● If you select IP Address, you will see the screen shown as below.

Add or Modify an Access Target Entry

Mode:	IP Address ▼	
Target Description:		
IP Address:		-
Target Port:		-
Protocol:	All ▼	
Common Service Port:	--Please Select-- ▼	

Save   Back

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, you will see the screen shown as below.

Add or Modify an Access Target Entry

Mode:	Domain Name ▼
Target Description:	
Domain Name:	

Save   Back

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.cn) will be blocked or allowed. You can enter 4 domain names.

3. Click Save.

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

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

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… 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

Go to Access Control → Schedule, you can view and set a Schedule list. 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

➤ 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... and the next screen will pop-up.

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)

Save   Back

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 Delete All to delete all the entries in the table.

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

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... 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
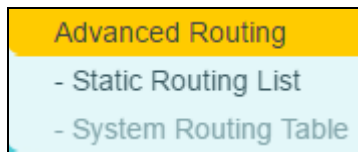
There are two submenus under the Advanced Routing menu: Static Routing List and System Routing Table. Click any of them, and you will be able to configure the corresponding function.

4.14.1 Static Routing List

Go to Advanced Routing → Static Routing List, you can configure the static route in the next screen. A static route is a pre-determined path that network information must travel to reach a specific host or network.
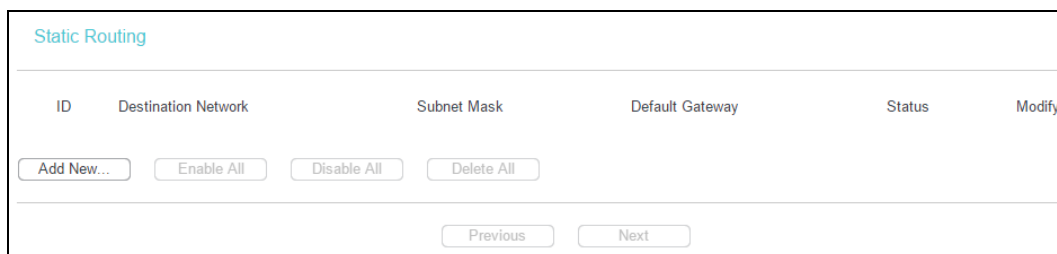
To add static routing entries:

1. Click Add New…, you will see the following screen.

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.

➢ Gateway - This is the IP Address of the gateway device that allows for contact between the router and the network or host.

3. Select Enabled or Disabled for this entry on the Status pull-down list.

4. Click Save to make the entry effective.

Click Delete to delete the entry.

Click Enable All to enable all the entries.

Click Disable All to disable all the entries.

Click Delete All to delete all the entries.

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

4.14.2 System Routing Table

Go to Advanced Routing → System Routing Table, you can configure the system routing table in the next screen. System routing table views all of the valid route entries in use.

ID	Destination Network	Subnet Mask	Gateway	Interface
	System Routing Table			
1	192.168.1.0	255.255.255.0	0.0.0.0	LAN & WLAN
2	10.20.89.0	255.255.255.0	0.0.0.0	WAN
3	239.0.0.0	255.0.0.0	0.0.0.0	LAN & WLAN
4	0.0.0.0	0.0.0.0	10.20.89.190	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).

4.15 IP & MAC Binding

IP & MAC Binding
- Binding Settings
- ARP List

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

4.15.1 Binding Settings

This page displays the Binding Settings table, you can operate it in accord with your desire.

➢ 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 Add New or Modify, and then you will go to the next page. This page is used for adding or modifying an IP & MAC Binding entry.

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

1. Click Add New....

2. Enter the MAC Address and IP Address.

3. Select the Bind checkbox.

4. Click Save.

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

1. Find the desired entry in the table.

2. Click Modify or Delete as desired on the Modify column.

To find an existing entry, follow the steps below.

1. Click Find.

2. Enter the MAC Address or IP Address.

3. Click Find in the page as shown below.

Find IP & MAC Binding Entry

MAC Address:

IP Address:

| ID | MAC Address | IP Address | Bind | Link |

Now the current list is empty.

Find   Back

Click Enable All to make all entries enabled.

Click Disable All to make all entries disabled.

Click Delete All to delete all entries.

4.15.2 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.

ARP List

ID	MAC Address	IP Address	Status	Configure
1	D0-25-98-6F-B9-06	192.168.1.103	Unbound	Load Delete
2	50-E5-49-1E-06-80	192.168.1.200	Unbound	Load Delete

Bind All   Load All   Refresh

➢ 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 - These buttons are for loading or deleting an item.

- Load - Load the item to the IP & MAC Binding list.

- Delete - Delete the item from the list.

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 cannot 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 have no interference with the IP & MAC Binding list.

4.16 Dynamic DNS

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

The router offers a Dynamic Domain Name System (DDNS) feature. DDNS lets you assign a fixed host and domain name to a dynamic internet IP address. It is useful when you are hosting your own website, FTP server, or other server behind the router. Before using this feature, you need to sign up with DDNS service providers such as dyn.com, www.noip.com. The Dynamic DNS client service provider will give you a password or key.

4.16.1 dyn.com DDNS

If the dynamic DNS Service Provider you select is dyn.com, the page will appear.

To set up for DDNS, follow these instructions:

1. Enter the User Name for your DDNS account.

2.   Enter the Password for your DDNS account.

3.   Enter the Domain Name you received from dynamic DNS service provider here.

4.   Click Login to log in to the DDNS service.

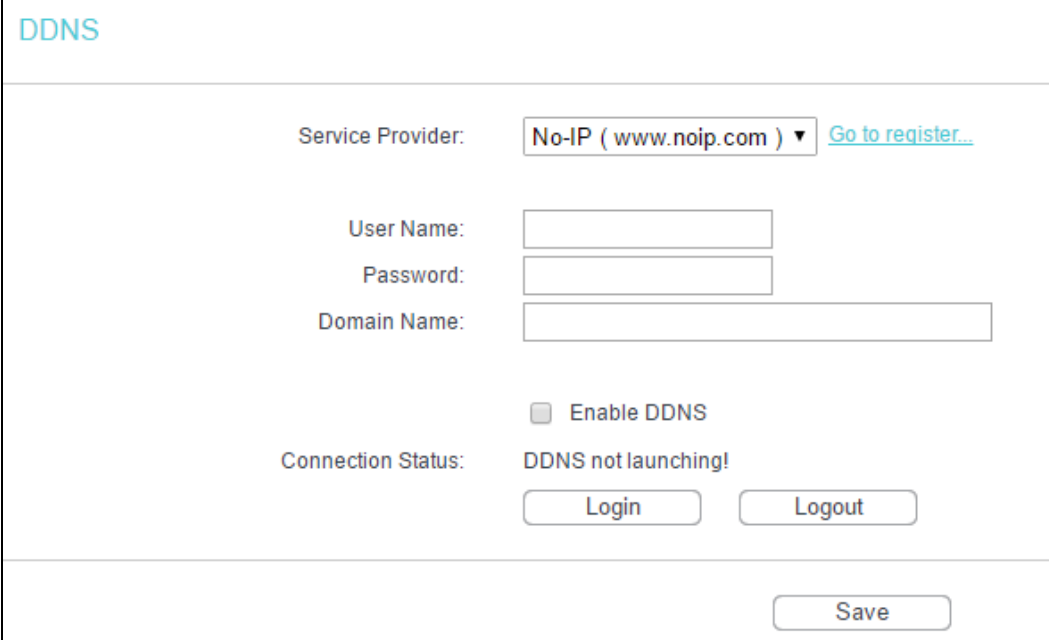Connection Status - The status of the DDNS service connection is displayed here.

Click Logout to logout of the DDNS service.

☞ Note:

If you want to log in again with another account after a successful login, please click Logout, then input your new username and password and click Login.

4.16.2   www.noip.com DDNS

If the dynamic DNS Service Provider you select is www.noip.com, the page will appear.

To set up for DDNS, follow these instructions:

1.   Enter the User Name for your DDNS account.

2.   Enter the Password for your DDNS account.

3.   Enter the Domain Name you received from dynamic DNS service provider.

4.   Click Login 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.

☞ Note:

If you want to log in again with another account after a successful login, please click Logout, then input your new username and password and click Login.

4.17 System Tools
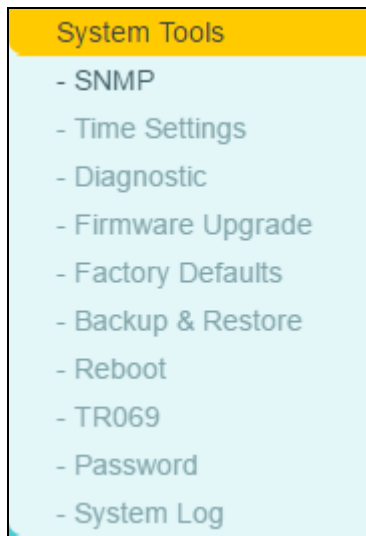
Choose System Tools, and you can see the submenus under the main menu: SNMP, Time Settings, Diagnostic, Firmware Upgrade, Factory Defaults, Backup & Restore, Reboot, TR069, Password and System Log. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.17.1 SNMP

Simple Network Management Protocol (SNMP) is a popular network monitoring and management protocol.

➢ SNMP Agent - Choose Enable to open this function if you want to have remote control through SNMPv1/v2 agent with MIB-II. Choose Disable to close this function.

➢ SysContact - The textual identification of the contact person for this managed node.

➢ SysName - An administratively-assigned name for this managed node.

➢ SysLocation - The physical location of this node.

☞ Note:

Specifying one of these values via the Device's web management page makes the corresponding object read-only. If there isn't such a config setting, then the write request will succeed (assuming suitable access control settings), but the new value would be forgotten the next time the agent was restarted.

➢ Get Community - Enter the community name that allows Read-Only access to this device's SNMP information. The community name can be considered a group password. The default setting is public.

➢ Get Source - Get source defines the IP address or subnet for management systems that can read information from this 'get' community device.

➢ Set Community - Enter the community name that allows Read/Write access to this device's SNMP information. The community name can be considered a group password. The default setting is private.

➢ Set Source - Set source defines the IP address or subnet for management systems that can control this 'set' community device.

☞ Note:

A restricted source can be a specific IP address (e.g. 10.10.10.1), or a subnet - represented as IP/BITS (e.g. 10.10.10.0/24). If an IP Address of 0.0.0.0 is specified, the agent will accept all requests under the corresponding community name.

Click Save to make the settings effective.

4.17.2 Time Settings

Go to System Tools → Time Settings, and then you can configure the time on the following screen.

Time Settings

Time zone:	(GMT) Greenwich Mean Time ▼
Date:	3 14 2017 (MM/DD/YY)
Time:	2 59 53 (HH/MM/SS)
NTP Server 1:	0.0.0.0 (Optional)
NTP Server 2:	0.0.0.0 (Optional)

Get GMT

☐ Enable DaylightSaving

Start: 2017 Mar ▼ 3rd ▼ Sun ▼ 2am ▼
End: 2017 Nov ▼ 2nd ▼ Sun ▼ 3am ▼
Daylight Saving Status:

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.

Save

➢ Time Zone - Select your local time zone from this pull 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.
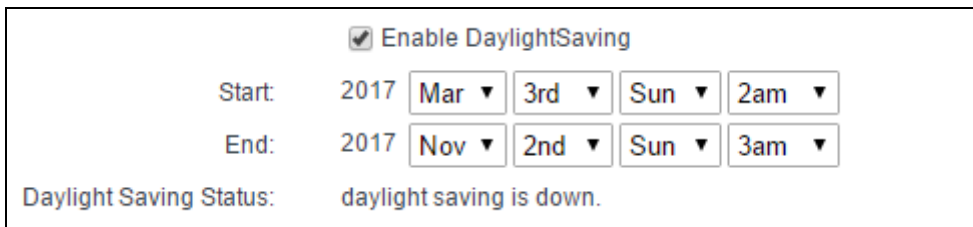3. Enter the Time in Hour/Minute/Second format.
4. Click Save.

To set time automatically:
1. Select your local time zone.
2. Enter the address or domain of the NTP Server 1 or NTP Server 2.

3. Click the Get GMT button to get system time from internet if you have connected to the internet.

To set up 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 Save to make the settings effective.

☑ Enable DaylightSaving
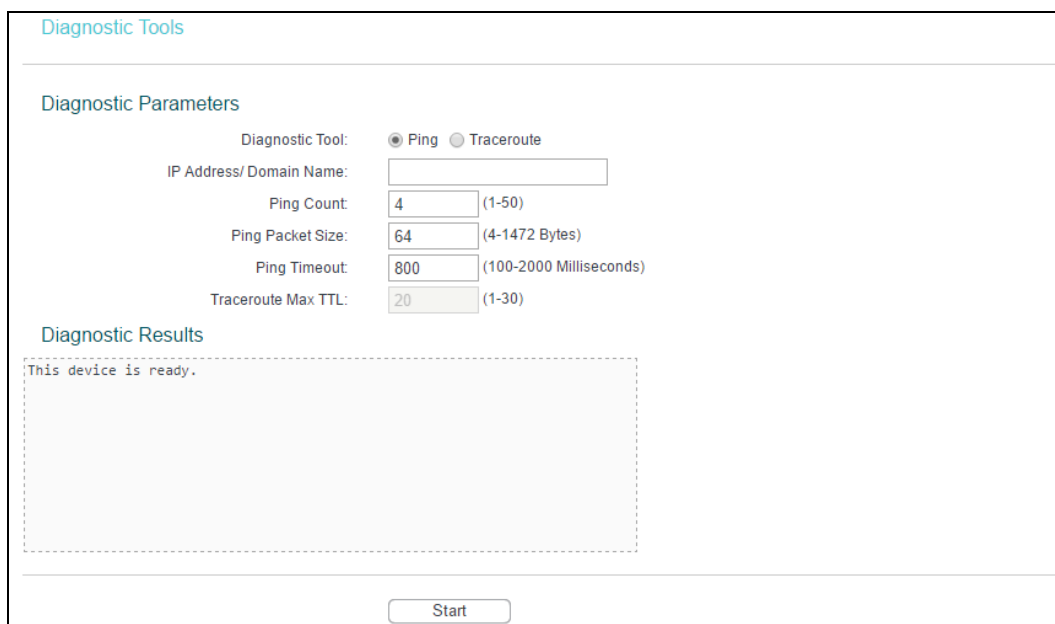
Start:	2017	Mar ▼	3rd ▼	Sun ▼	2am ▼
End:	2017	Nov ▼	2nd ▼	Sun ▼	3am ▼
Daylight Saving Status:	daylight saving is down.				

☞ Note:

1) This setting will be used for some time-based functions such as firewall. You must specify your time zone once you log in 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) In daylight saving configuration, start time shall be earlier than end time.

4.17.3 Diagnostic

Go to System Tools → Diagnostic, you can transact Ping or Traceroute function to check connectivity of your network in the following screen.

Diagnostic Tools

Diagnostic Parameters

Diagnostic Tool:	◉ Ping ○ Traceroute
IP Address/ Domain Name:	
Ping Count:	4 (1-50)
Ping Packet Size:	64 (4-1472 Bytes)
Ping Timeout:	800 (100-2000 Milliseconds)
Traceroute Max TTL:	20 (1-30)

Diagnostic Results

This device is ready.

Start

➢ 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 - Enter the IP Address or Domain Name of the PC whose connection you wish to diagnose.

➢ Pings Count - Specifies the number of Echo Request messages sent. The default is 4.

➢ Ping Packet Size - Specifies the number of data bytes to be sent. The default is 64.

➢ Ping Timeout - Time to wait for a response, in milliseconds. The default is 800.

➢ Traceroute Max TTL - Set the maximum number of hops (max TTL to be reached) in the path to search for the target (destination). The default is 20.

Click Start to start the diagnostic procedure.

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.

```
Diagnostic Results

Pinging 202.108.22.5 with 64 bytes of data:

Reply from 202.108.22.5:  bytes=64  time=164   TTL=51  seq=1
Reply from 202.108.22.5:  bytes=64  time=164   TTL=51  seq=2
Reply from 202.108.22.5:  bytes=64  time=164   TTL=51  seq=3
Reply from 202.108.22.5:  bytes=64  time=165   TTL=51  seq=4

Ping statistics for 202.108.22.5
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
Approximate round trip times in milliseconds:
  Minimum = 164, Maximum = 165, Average = 164
```

☞ Note:

Only one user can use this tool at one time. Options "Ping Count", "Ping Packet Size" and "Ping Timeout" are used for Ping function. Option "Traceroute Max TTL" are used for Tracert function.

4.17.4 Firmware Upgrade

Go to System Tools → Firmware Upgrade, you can update the latest version of firmware for the router on the following screen.

➢ **Firmware Version** - Displays the current firmware version.

➢ **Hardware Version** - Displays the current hardware version. The hardware version of the upgrade file must accord with the 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 official website (http://www.tp-link.com).

2. Click Choose File, then enter or select the path name where you save the downloaded file on the computer into the File Name blank.

3. Click Upgrade.

4. The router will reboot while the upgrading has been finished.

☞ Note:

The firmware version must correspond to the hardware. The upgrade process takes a few moments and this device restarts automatically when the upgrade is complete. It is important to keep power applied during the entire process. Loss of power during the upgrade could damage this device.

4.17.5 Factory Defaults

Go to System Tools → Factory Defaults, and you can restore the configurations of the router to factory defaults on the following screen.

Click Restore to reset all configuration settings to their default values.
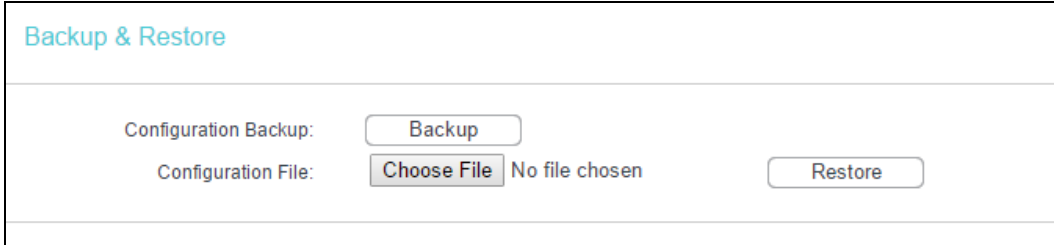
- The default Username: admin

- The default Password: admin

- The default IP Address: 192.168.1.1

- The default Subnet Mask: 255.255.255.0

☞ Note:

All changed settings will be lost when defaults are restored.

4.17.6 Backup & Restore

Go to 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.

Backup & Restore

Configuration Backup: Backup

Configuration File: Choose File No file chosen   Restore
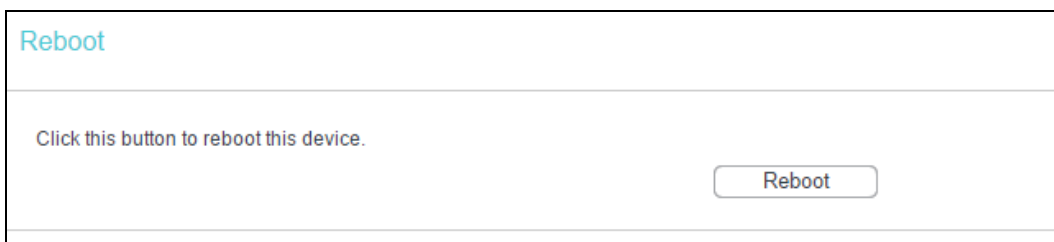
➢ Click Backup to save all configuration settings to your local computer as a file.

➢ To restore this device's configuration, follow these instructions:

1) Click Choose File to find the configuration file which you want to restore.

2) Click Restore to update the configuration with the file whose path is the one you have input or selected in the blank.

☞ Note:

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

4.17.7 Reboot

Go to System Tools → Reboot, you can click Reboot to reboot the router.

Reboot

Click this button to reboot this device.

Reboot

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 Web Management Port.
- Upgrade the firmware of this device (system will reboot automatically).
- Restore this device's settings to the factory defaults (system will reboot automatically).
- Update the configuration with the file (system will reboot automatically).

4.17.8 TR069

TR-069 is a protocol for communication between a CPE and Auto-Configuration Server (ACS) that encompasses secure auto-configuration as well as other CPE management functions within a common framework.

```
TR069 Settings

              TR069:         ◉ Disable  ○ Enable

     WAN IP Address:         0.0.0.0

           ACS Login:
            ACS URL:         http://acs.tp-link.com.cn:80
          User Name:         [                    ]
           Password:         [                    ]

             Inform:         ○ Disable  ◉ Enable
     Inform Interval:        [30                  ]  (1-3600)

           CPE Login:
  Connection Request User:   [admin               ]
  Connection Request Password: [•••••             ]
     Connection Port:        [8099                ]

                             [    Save    ]
```

➢ TR069 - Enable or Disable the TR069 function. If you disable this function, your router (CPE) will not automatically configured by Auto-Configuration Server (ACS).

➢ ACS URL - This field specifies the URL for your router (CPE) to connect to the ACS.

➢ User Name - This field used to authenticate your router (CPE) when making a connection to the ACS. This username is used only for HTTP-based authentication of your router (CPE).

➢ Password - The Password used to authenticate your router (CPE) when making a connection to the ACS. This password is used only for HTTP-based authentication of your router (CPE).

➢ Inform - Whether or not your router (CPE) must periodically send CPE info to Server using the Inform method call.

➢ Inform Interval - The duration in seconds of the interval for which your router (CPE) MUST attempt to connect with the ACS and call the Inform method if PeriodicInform-Enable is true.

➢ Connection Request User/Password - Enter the username/password for the ACS server to log in to the router.

➢ Connection Port - Connection request server port, for an ACS to make a connection request notification to your router (CPE).

4.17.9 Password

Go to System Tools → Password, you can change the factory default user name and password of the router in the next screen.

```
                        Password


    Username and password can contain between 1 - 15 characters and may not incluede spaces.

                    Old User Name:   [_____]
                    Old Password:    [_____]


                    New User Name:   [_____]
                    New Password:    [_____]
                Confirm New Password: [_____]


                            [   Save   ]    [  Clear All  ]
```

It is strongly recommended that you change the factory default user name and password of this device. All users who try to access this device's web management page will be prompted for this device's user name and password.

☞ Note:

The new username and password must not exceed 15 characters in length and must not include any spaces. Enter the new Password twice to confirm it.

Click Save when finished.

Click Clear All to clear all.

4.17.10 System Log

Go to 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                 │
    ├─────┼──────────────┼───────┼──────┼─────────────────────────────────────────┤
    │  1  │5th day 19:57:31│OTHER │INFO  │User clear system log.                    │
    └─────┴──────────────┴───────┴──────┴─────────────────────────────────────────┘


    Time = 2017-03-14 3:12:29 417451s

    H-Ver = MR6400 v2 00000000 : S-Ver = 1.0.12 Build 170223 Rel.55039n

    L = 192.168.1.64 : M = 255.255.255.0

    W1 = DHCP : W = 192.168.0.100 : M = 255.255.255.0 : G = 0.0.0.0


    [  Refresh  ]   [  Save Log  ]   [  Mail Log  ]   [  Clear Log  ]


                    [ Previous ]   [   Next   ]   Current No. [1 ▼]  Page
```

➢   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.

➢   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. The result will be shown in the later log soon.

➢   Clear Log - All the logs will be deleted from this device permanently, not just from the page.

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

Chapter 5. Standard Wireless Router Mode

This chapter will show each web page's key functions and the configuration way on Standard Wireless Router Mode.

5.1 Login

After your successful login, you will see the main menus on the left of the web management page. 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.

5.2 Status

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

Status

Firmware Version:	1.0.12 Build 170223 Rel.55026n
Hardware Version:	MR6400 v2 00000000
IMEI:	350000000002150n

LAN

MAC Address:	3C-46-D8-E0-60-C4
IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0

Wireless

Wireless Radio:	Enable
Name (SSID):	TP-Link_60C4
Mode:	11bgn mixed
Channel Width:	Automatic
Channel:	Auto (Current channel 6)
MAC Address:	3C-46-D8-E0-60-C4
WDS Status:	Disable

WAN

MAC Address:	3C-46-D8-E0-60-C5	
IP Address:	192.168.0.169	Dynamic IP
Subnet Mask:	255.255.255.0	
Default Gateway:	192.168.0.1	Release
DNS Server:	192.168.0.1 , 0.0.0.0	

System Up Time:	0 days 00:15:33	Refresh

5.3 WPS

The configuration is similar to WPS in 3G/4G Router mode. Please refer to 4.3 WPS.

5.4 Working Mode

The configuration is similar to Working Mode in 3G/4G Router mode. Please refer to 4.4 Working Mode.

5.5 Network

There are four submenus under the Network menu: WAN, MAC Clone, LAN and VLAN. Click any of them, and you will be able to configure the corresponding function.

5.5.1 WAN

Go to Network → WAN, and 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:

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

➢ 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.)

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 as shown below.

➢ IP Address - Enter the IP address in dotted-decimal notation provided by your ISP.

➢ Subnet Mask - Enter the subnet Mask provided by your ISP in dotted-decimal notation. Usually, the Sub Mask is 255.255.255.0.

➢ Default Gateway - (Optional) Enter the gateway IP address provided by your ISP in dotted-decimal notation.

➤ **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.

3. If your ISP provides a PPPoE connection, select PPPoE/Russia PPPoE option. And you should enter the following parameters:

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

➤ **Confirm Password -** Re-enter the Password provided by your ISP to ensure the Password you entered is correct.

➤ **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 to keep 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 page, will the Time-based Connecting function can take effect.

➢ Connect Manually - You can click Connect/Disconnect to connect/disconnect immediately. This mode also supports the Max Idle Time function as Connect on Demand mode. 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 terminated although you specify a time to Max Idle Time, since some applications are visiting the internet continually in the background.

If you want to do some advanced configurations, please click Advanced, and the page shown below will appear:

> ➢ 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, which 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 "15". You can input the value between "0"and "120". The value "0" means no detect.

> ➢ Primary 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.

> ➢ Secondary DNS - If your ISP provides another DNS server, enter it into this field.

  Click the Save button to make the settings effective.

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

- ➢ 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. 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.

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 make the settings effective.

5. If your ISP provides L2TP connection, please select L2TP/Russia L2TP. And you should enter the following parameters:

WAN

WAN Connection Type: L2TP/Russia L2TP ▼

User Name: [   ]
Password: [   ]
Confirm 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

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

➢ Confirm Password - Re-enter the Password provided by your ISP to ensure the Password you entered is correct.

➢ Dynamic IP/ Static IP - Select Static IP if IP address, subnet mask, gateway and DNS server address have been provided by your ISP. Otherwise, please select Dynamic IP.

➢ Server IP Address/Name - Enter server IP address or domain name provided by your ISP.

➢ IP address - Enter the IP address used for dial-up. (Only can be configured when Static IP is selected).

➢ Subnet Mask - Enter the subnet mask provided by your ISP. (Only can be configured when Static IP is selected)

➢ Gateway - Enter gateway provided by your ISP. (Only can be configured when Static IP is selected)

➤ DNS - Enter DNS server provided by your ISP. (Only can be configured when Static IP is selected)

➤ Internet IP Address - The internet IP address assigned by L2TP server.

➤ Internet DNS - The internet DNS server address assigned by L2TP server.

➤ Connect on Demand - You can configure the router to disconnect your internet connection after a specified period of the internet connectivity (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, 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 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, click 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, since some applications is visiting the internet continually in the background.

6. If your ISP provides PPTP connection, please select PPTP/Russia PPTP. And you should enter the following parameters:

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

> ➢ Confirm Password - Re-enter the Password provided by your ISP to ensure the Password you entered is correct.

> ➢ Dynamic IP/Static IP - Select Static IP if IP address, subnet mask, gateway and DNS server address have been provided by your ISP. Otherwise, please select Dynamic IP.

> ➢ Server IP Address/Name - Enter server IP address or domain name provided by your ISP.

> ➢ IP address - Enter the IP address used for dial-up. (Only can be configured when Static IP is selected).

> ➢ Subnet Mask - Enter the subnet mask provided by your ISP. (Only can be configured when Static IP is selected)

➢ Gateway - Enter gateway provided by your ISP. (Only can be configured when Static IP is selected)

➢ DNS - Enter DNS server provided by your ISP. (Only can be configured when Static IP is selected)

➢ Internet IP Address - The internet IP address assigned by PPTP server.

➢ Internet DNS - The internet DNS server address assigned by PPTP server.

➢ 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, 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 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, click 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, since some applications are visiting the internet continually in the background.

☞ Note:

If you don't know how to choose the appropriate connection type, click Detect 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 cannot detect PPTP/L2TP/BigPond connections with your ISP. If your ISP uses one of these protocols, then you must configure your connection manually.

5.5.2 MAC Clone

Go to Network → MAC Clone, and then you can configure the MAC address of the WAN:

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 Clone MAC Address 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 Save to make the settings effective.

☞ **Note:**
Only the PC on your LAN can use the MAC Address Clone function.

5.5.3 LAN

Go to Network → LAN, and then you can configure the IP parameters of the LAN on the screen as below.

➢ **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: 192.168.1.1).

➢ **Subnet Mask** - An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask.

➢ **IGMP Proxy** - If you want to watch TV through IGMP, please Enable it.

☞ **Note:**

1) If you change the IP Address of LAN, you must use the new IP Address to log in to 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.

Click Save to make the settings effective.

5.5.4 VLAN

Go to Network → VLAN, You can configure the VLAN parameters for different application on this page.

➢ **VLAN Enable** - Configure the function according to your ISP, otherwise the internet could

not be accessed. If "NO" is selected, the other options would be invalid.

➢ Internet VLAN ID - Tick the TAG checkbox if your ISP need internet VLAN. Enter the VLAN ID for internet access, which is provided by your ISP. Only the correct VLAN ID can make internet access successfully. If your ISP doesn't need internet VLAN, you should untick the TAG checkbox and then the internet VLAN ID option would become invalid.

➢ Internet VLAN Pri - Select the priority of internet VLAN. Keep it as default unless necessary. When you untick the TAG checkbox beside internet VLAN ID, the internet VLAN Pri option would become invalid.

➢ IPTV VLAN ID - Enter the VLAN ID for IPTV access, which is provided by your ISP. Only the correct VLAN ID can make IPTV access successfully.

➢ IPTV VLAN Pri - Select the priority of IPTV VLAN. Keep it as default unless necessary.

➢ IP-Phone VLAN ID - Enter the VLAN ID for IP-phone, which is provided by your ISP. Only the correct VLAN ID can make IP-phone service successfully.

➢ IP-Phone VLAN Pri - Select the priority of IP-phone. Keep it as default unless necessary.

➢ LAN1 Mode - LAN1 is worked on internet mode, which means you can use LAN1 to access internet and manage the router.

➢ LAN1~3 Mode - LAN1 is fixed as internet. LAN2~3 can be worked on internet mode, IPTV mode or IP-Phone mode. When it worked on internet mode, you can use it to access internet and manage the router; and when it worked on IPTV mode, you can connect the STB to the LAN port and get the IPTV service. When it worked on IP-Phone mode, you can get the VoIP service. Please check with your ISP for the service detail.

Click Save to make the settings effective.

5.6 Wireless

The configuration is similar to Wireless in 3G/4G Router mode. Please refer to 4.7 Wireless.

5.7 Guest Network

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

5.7.1 Wireless Settings

Go to Guest Network → Wireless Settings, you can configure the basic settings for the Guest network on this page.

➢ **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** - 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 the time the wireless stations could accessing the router.

5.7.2 Wireless Statistics

Go to Guest Network → Wireless Statistics, and then you can see the MAC Address, Current Status, Received Packets and Sent Packets for each connected wireless station.

```
Guest network Wireless Statistics
─────────────────────────────────────────────────────────────────
Current Connected Wireless Stations numbers:    0      Refresh

                                       Previous          Next
```

➢ 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 Refresh.

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

☞ Note:

This page will be refreshed automatically every 5 seconds.

5.8 DHCP

The configuration is similar to DHCP in 3G/4G Router mode. Please refer to 4.9 DHCP.

5.9 Forwarding

The configuration is similar to Fowarding in 3G/4G Router mode. Please refer to 4.10 Forwarding.

5.10 Security
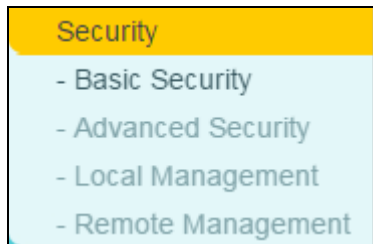
There are four submenus under the Security menu: Basic Security, Advanced Security, Local Management and Remote Management. Click any of them, and you will be able to configure the corresponding function.

5.10.1 Basic Security

Go to Security → Basic Security, and then you can configure the basic security in the screen as shown below.

➢ 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 VPN protocols to pass through the router.

- **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, click Enable.
- **L2TP Passthrough** - Layer Two Tunneling Protocol (L2TP) is the method used to enable Point-to-Point sessions via the internet on the Layer Two level. To allow L2TP tunnels to pass through the router, click Enable.
- **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, click Enable.

➢ **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, click Enable.
- **TFTP ALG** - To allow TFTP clients and servers to transfer data across NAT, click Enable.
- **H323 ALG** - To allow Microsoft NetMeeting clients to communicate across NAT, click Enable.
- **RTSP ALG** - To allow some media player clients to communicate with some streaming media servers across NAT, click Enable.
- **SIP ALG** - To allow some multimedia clients to communicate across NAT, click Enable.

Click Save to make the settings effective.

5.10.2 Advanced Security

Go to Security → Advanced Security, and then you can protect the router from being attacked by TCP-SYN Flood, UDP Flood and ICMP-Flood in the screen as shown below.

Advanced Security

Packets Statistics Interval (5 ~ 60): [10 ▼] Seconds

DoS Protection: ⊙ Disable ○ Enable

☐ Enable ICMP-FLOOD Attack Filtering

ICMP-FLOOD Packets Threshold (5 ~ 3600): [50] Packets/Secs

☐ Enable UDP-FLOOD Filtering

UDP-FLOOD Packets Threshold (5 ~ 3600): [500] Packets/Secs

☐ Enable TCP-SYN-FLOOD Attack Filtering

TCP-SYN-FLOOD Packets Threshold (5 ~ 3600): [50] Packets/Secs

☐ Ignore Ping Packet from WAN Port to Router
☐ Forbid Ping Packet from LAN Port to Router

[Save] [Blocked DoS Host List]

➢ 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 Current Statistics Status in System Tools → 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 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. (Defends against some viruses).

Click Save to make the settings effective.

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

5.10.3 Local Management

Go to Security → Local Management, and then you can configure the management rule in the screen as shown below. The management feature allows you to deny computers in LAN from accessing the router.

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 Add, your PC's MAC Address will be placed in the list above.
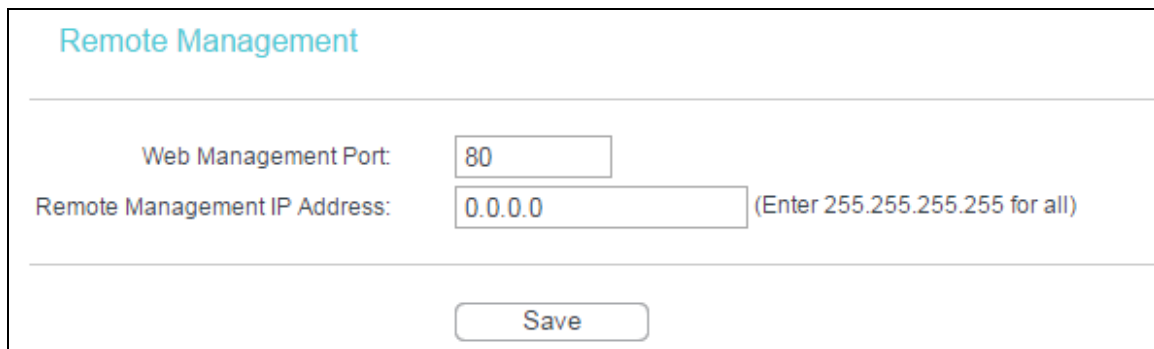
Click Save to make the settings effective.

☞ Note:

If your PC is blocked but you want to access the router again, press and hold down the WPS/RESET button on the rear panel of the router until the Power LED starts flashing to reset the router's factory defaults in the router's web management page.

5.10.4 Remote Management

Go to Security → Remote Management, and then you can configure the Remote Management function in the screen as shown below. 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

➤ 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 management page.

2)   Be sure to change the router's default password to a very secure password.

5.11 Parental Control

The configuration is similar to Parental Control in 3G/4G Router mode. Please refer to 4.12 Parental Control.

5.12 Access Control

The configuration is similar to Access Control in 3G/4G Router mode. Please refer to 4.13 Access Control.

5.13 Advanced Routing

The configuration is similar to Advanced Routing in 3G/4G Router mode. Please refer to 4.14 Advanced Routing.

5.14 Bandwidth Control
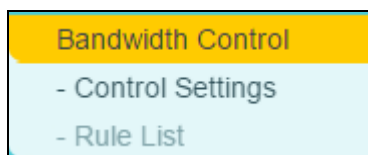
There are two submenus under the Bandwidth Control menu: Control Settings and Rule List. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

5.14.1 Control Settings

Go to Bandwidth Control → Control Settings, and then you can configure the Egress Bandwidth and Ingress Bandwidth in the next screen. 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.

➢   Enable Bandwidth Control - Select 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.

5.14.2 Rule List

Go to Bandwidth Control → Rule List, and then you can view and configure the Bandwidth Control rules in the screen below.

➢ **Description** - The information of description include address range, the port range and protocol of transport layer.

➢ **Egress Bandwidth** - The max upload speed which through the WAN port, default number is 0.

➢ **Ingress Bandwidth** - The max download speed which through the WAN port, default number is 0.

➢ **Enable** - Rule status, show whether the rule takes effect.

➢ **Modify** - Click Modify to edit the rule. Click Delete to delete the rule.

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

1. Click Add New…, you will see a new screen as shown below.

2. Enter the information like the screen shown below.

3. Click Save.

5.15 IP & MAC Binding

The configuration is similar to IP & MAC Binding Setting in 3G/4G Router mode. Please refer to 4.15 IP & MAC Binding.

5.16 Dynamic DNS

The configuration is similar to Dynamic DNS in 3G/4G Router mode. Please refer to 4.16 Dynamic DNS.

5.17 IPv6 Support
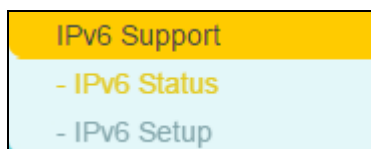
Choose menu IPv6 Support, and you can see the submenus under the main menu: IPv6 Status, IPv6 Setup. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

5.17.1 IPv6 Status

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

IPv6 Status

WAN

Connection Type:	Disabled
IPv6 Address:	
IPv6 Default Gateway:	
Primary IPv6 DNS:	
Secondary IPv6 DNS:	

LAN

IPv6 Address Assign Type:	RADVD
IPv6 Address:	
Link-local Address:	/0

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 - The way how the router assign IPv6 address for PC in LAN, 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.

5.17.2 IPv6 Setup

Go to IPv6 Support → IPv6 Setup, and then you can set up IPv6 service on the following screen.

WAN Setup

Enable IPv6:	☑
WAN Connection Type:	PPPoEv6 ▼
PPPoE Session:	○ Share with PPPoEv4 ● Create a new Session
Username:	
Password:	
Confirm Password:	
IPv6 Address:	
IPv6 Address Prefix:	
Default Gateway:	
MTU:	1492 Bytes,1492 as default, do not change unless necessary.
●	Get IPv6 DNS Server Automatically
Primary IPv6 DNS:	
Secondary IPv6 DNS:	
○	Use the following IPv6 DNS Servers
Connection Mode:	● Alway On ○ Connect Manual
	Connect Disconnect **Disconnected!**

LAN Setup

Address Autoconfiguration Type:	● RADVD ○ DHCPv6 Server
Site Prefix Configuration Type:	● Delegated ○ Static
Lan IPV6 Address:	/0

Save

To set up IPv6 service, please follow the steps below.

1. Please make sure that Enable IPv6 has been checked.

2. To Configure WAN Connection Type, if you are not sure what the connection type is, please contact your IPv6 provider. Here takes PPPoEv6 as an example. After the PPPoEv6 is selected, please input the Username and Password provided by the IPv6 Provider.

3. For LAN Setup, keep the default settings as shown above. The Address Autoconfiguration Type chooses RADVD; the Site Prefix Configuration Type chooses Delegated.

4. Click Save.
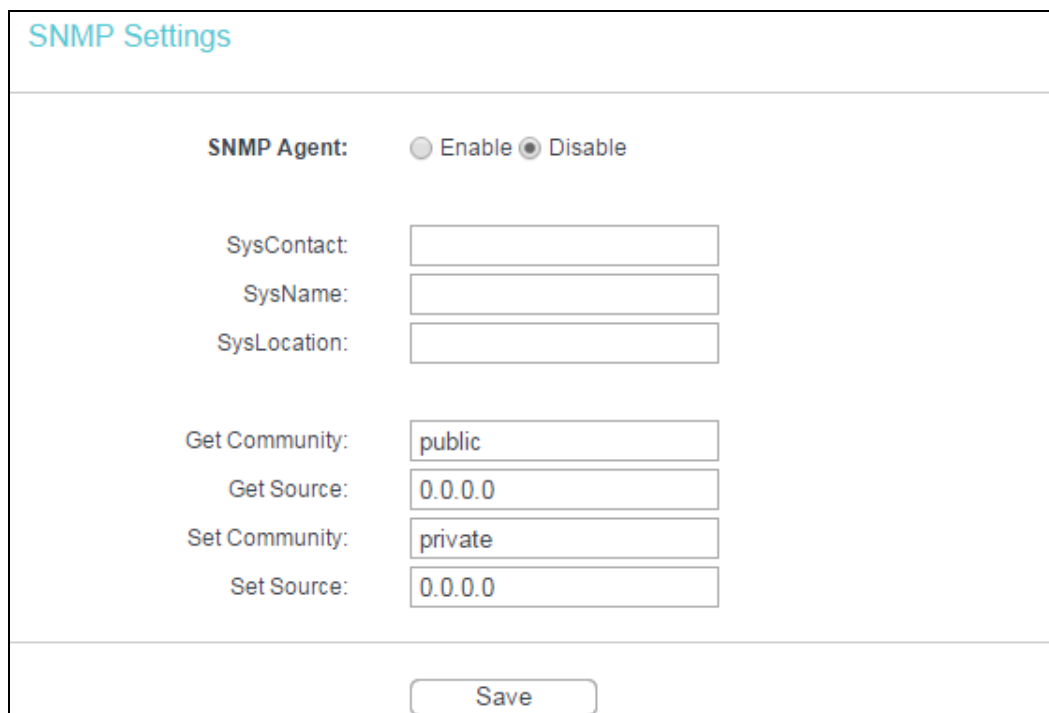
5.18 System Tools
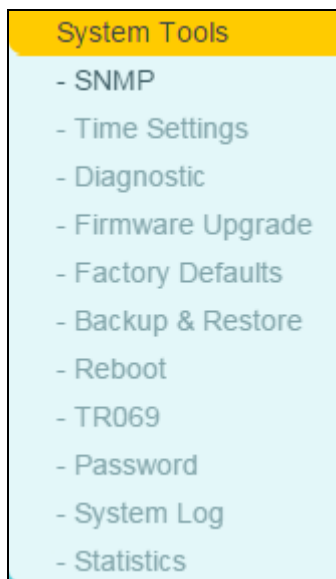
Choose menu System Tools, and you can see the submenus under the main menu: SNMP, Time Settings, Diagnostic, Firmware Upgrade, Factory Defaults, Backup & Restore, Reboot, TR069, Password, System Log and Statistics. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

5.18.1 SNMP

Simple Network Management Protocol (SNMP) is a popular network monitoring and management protocol.

➢ SNMP Agent - Choose Enable to open this function if you want to have remote control through SNMPv1/v2 agent with MIB-II. Choose Disable to close this function.

➢ SysContact - The textual identification of the contact person for this managed node.

➢ SysName - An administratively-assigned name for this managed node.

➢ SysLocation - The physical location of this node.

☞ Note:

Specifying one of these values via the Device's web management page makes the corresponding object read-only. If there isn't such a config setting, then the write request will succeed (assuming suitable access control settings), but the new value would be forgotten the next time the agent was restarted.

➢ Get Community - Enter the community name that allows Read-Only access to this device's SNMP information. The community name can be considered a group password. The default setting is public.

➢ Get Source - Get source defines the IP address or subnet for management systems that can read information from this 'get' community device.

➢ Set Community - Enter the community name that allows Read/Write access to this device's SNMP information. The community name can be considered a group password. The default setting is private.

➢ Set Source - Set source defines the IP address or subnet for management systems that can control this 'set' community device.

☞ Note:

A restricted source can be a specific IP address (e.g. 10.10.10.1), or a subnet - represented as IP/BITS (e.g. 10.10.10.0/24). If an IP Address of 0.0.0.0 is specified, the agent will accept all requests under the corresponding community name.

Click Save to make the settings effective.

5.18.2 Time Settings

Go to System Tools → Time Setting, and then you can configure the time on the following screen.

> ➢ Time Zone - Select your local time zone from this pull 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 1 or NTP Server 2.
3. Click the Get GMT button to get system time from internet if you have connected to the internet.

To set up 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 Save to make the settings effective.

☞ Note:

1) This setting will be used for some time-based functions such as firewall. You must specify your time zone once you log in 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) In daylight saving configuration, start time shall be earlier than end time.

5.18.3 Diagnostic

Go to System Tools → Diagnostic, you can transact Ping or Traceroute function to check connectivity of your network in the following screen.

> ➢ 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 - Enter the IP Address or Domain Name of the PC whose connection you wish to diagnose.

> ➢ Pings Count - Specifies the number of Echo Request messages sent. The default is 4.

> ➢ Ping Packet Size - Specifies the number of data bytes to be sent. The default is 64.

> ➢ Ping Timeout - Time to wait for a response, in milliseconds. The default is 800.

> ➢ Traceroute Max TTL - Set the maximum number of hops (max TTL to be reached) in the path to search for the target (destination). The default is 20.

Click Start to start the diagnostic procedure.

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.

```
Diagnostic Results

Pinging 202.108.22.5 with 64 bytes of data:

Reply from 202.108.22.5:  bytes=64  time=164   TTL=51   seq=1
Reply from 202.108.22.5:  bytes=64  time=164   TTL=51   seq=2
Reply from 202.108.22.5:  bytes=64  time=164   TTL=51   seq=3
Reply from 202.108.22.5:  bytes=64  time=165   TTL=51   seq=4

Ping statistics for 202.108.22.5
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
Approximate round trip times in milliseconds:
  Minimum = 164, Maximum = 165, Average = 164
```
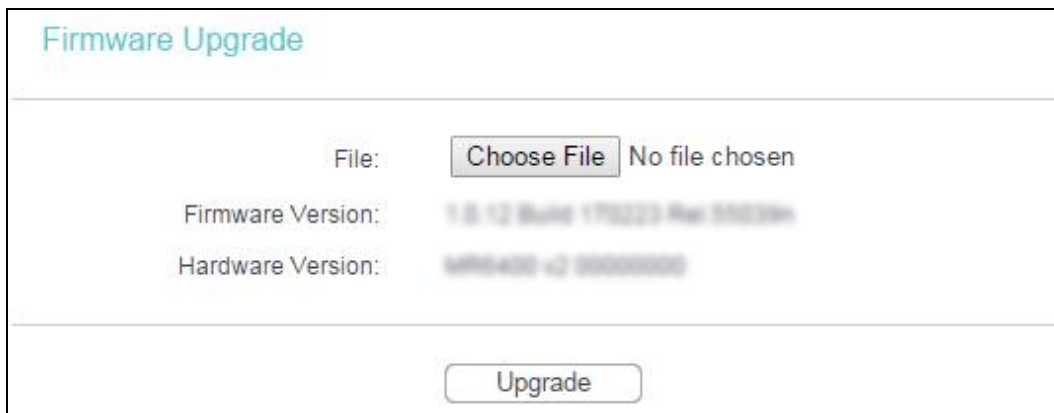
☞ Note:

Only one user can use this tool at one time. Options "Ping Count", "Ping Packet Size" and "Ping Timeout" are used for Ping function. Option "Traceroute Max TTL" are used for Tracert function.

5.18.4 Firmware Upgrade

Go to System Tools → Firmware Upgrade, you can update the latest version of firmware for the router on the following screen.

```
Firmware Upgrade

          File:       Choose File  No file chosen
Firmware Version:
Hardware Version:


                      Upgrade
```

➢ Firmware Version - Displays the current firmware version.

➢ Hardware Version - Displays the current hardware version. The hardware version of the upgrade file must accord with the 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 official website (http://www.tp-link.com).

2. Click Choose File, then enter or select the path name where you save the downloaded file on the computer into the File Name blank.

3. Click Upgrade.

4. The router will reboot while the upgrading has been finished.

☞ Note:

The firmware version must correspond to the hardware. The upgrade process takes a few moments and this device restarts automatically when the upgrade is complete. It is important to keep power applied during the entire process. Loss of power during the upgrade could damage this device.

5.18.5 Factory Defaults

Go to System Tools → Factory Defaults, and you can restore the configurations of the router to factory defaults on the following screen.
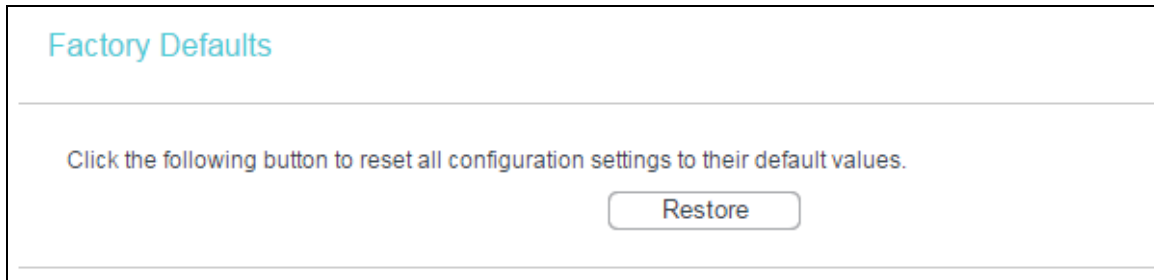
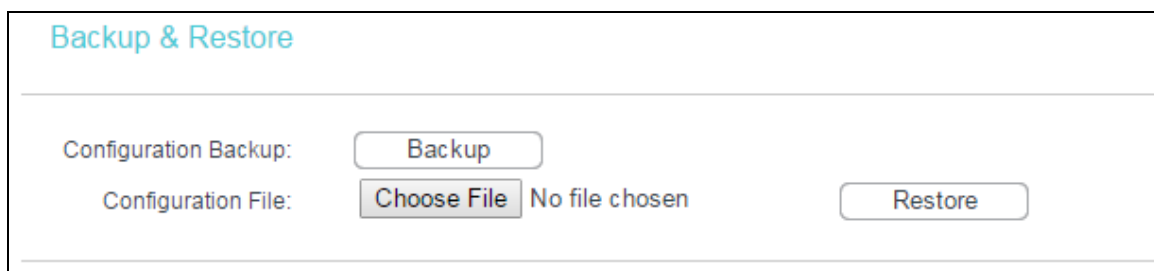Click Restore to reset all configuration settings to their default values.

- The default User Name: admin
- The default Password: admin
- The default IP Address: 192.168.1.1
- The default Subnet Mask: 255.255.255.0

☞ Note:

All changed settings will be lost when defaults are restored.

5.18.6 Backup & Restore

Go to 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.

➢ Click Backup to save all configuration settings to your local computer as a file.

➢ To restore this device's configuration, follow these instructions:

3) Click Choose File to find the configuration file which you want to restore.

4) Click Restore to update the configuration with the file whose path is the one you have input or selected in the blank.

☞ Note:

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

5.18.7 Reboot

Go to System Tools → Reboot, you can click Reboot to reboot the router.

Reboot

Click this button to reboot this device.

Reboot

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 Web Management Port.

- Upgrade the firmware of this device (system will reboot automatically).

- Restore this device's settings to the factory defaults (system will reboot automatically).

- Update the configuration with the file (system will reboot automatically).

5.18.8 TR069

TR-069 is a protocol for communication between a CPE and Auto-Configuration Server (ACS) that encompasses secure auto-configuration as well as other CPE management functions within a common framework.

TR069 Settings

TR069:	◉ Disable ○ Enable
WAN IP Address:	192.168.0.169
ACS Login:	
ACS URL:	http://acs.tp-link.com.cn:80
User Name:	
Password:	
Inform:	○ Disable ◉ Enable
Inform Interval:	30 (1-3600)
CPE Login:	
Connection Request User:	admin
Connection Request Password:	•••••
Connection Port:	8099

Save

➢ TR069 - Enable or Disable the TR069 function. If you disable this function, your router (CPE) will not automatically configured by Auto-Configuration Server (ACS).

➢ ACS URL - This field specifies the URL for your router (CPE) to connect to the ACS.

➢ User Name - This field used to authenticate your router (CPE) when making a connection to the ACS. This username is used only for HTTP-based authentication of your router (CPE).

➢ Password - The Password used to authenticate your router (CPE) when making a connection to the ACS. This password is used only for HTTP-based authentication of your router (CPE).

➢ Inform - Whether or not your router (CPE) must periodically send CPE info to Server using the Inform method call.

➢ Inform Interval - The duration in seconds of the interval for which your router (CPE) MUST attempt to connect with the ACS and call the Inform method if PeriodicInform-Enable is true.

➢ Connection Request User/Password - Enter the username/password for the ACS server to log in to the router.

System Log

Auto Mail Feature: Disabled   Mail Settings
Log Type: ALL   ▼   Log Level: ALL   ▼

Index	Time	Type	Level	Log Content
1	1st day 00:46:09	OTHER	INFO	User clear system log.

Time = 2017-01-01 0:46:17 2779s

H-Ver = MR6400 v2 00000000 : S-Ver = 1.0.12 Build 170223 Rel.55039n

L = 192.168.1.1 : M = 255.255.255.0

W1 = DHCP : W = 192.168.0.169 : M = 255.255.255.0 : G = 192.168.0.1

Refresh   Save Log   Mail Log   Clear Log

Previous   Next   Current No. 1 ▼ Page

➢ 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.

➢ 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. The result will be shown in the later log soon.

➢ Clear Log - All the logs will be deleted from this device permanently, not just from the page.

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

5.18.11 Statistics

Go to System Tools → Statistics, and then you can view the statistics of the router, including total traffic and current traffic of the last Packets Statistic Interval.

Statistics

Current Statistics Status:	**Disabled**				Enable			
Packets Statistics Interval(5~60):	10 ▼	Seconds						
	☐ Auto-refresh				Refresh			

| Sorted Rules: | Sorted by Current Bytes ▼ | | | Reset All | | Delete All | | |

	Total		Current					Modify
IP Address/ MAC Address	Packets	Bytes	Packets	Bytes	ICMP Tx	UDP Tx	SYN Tx	
The current list is empty.								

5 ▼ entries per page. Current No. 1 ▼ Page

Previous   Next

➢ Current Statistics Status - Enable or Disable. The default value is disabled. To enable it, click the Enable button. If it is disabled, the function of DoS protection in Security settings will be 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 Statistics interval indicates the time section of the packets statistic.

➢ Sorted Rules - Choose how the displayed statistics are sorted.

Select the Auto-refresh checkbox to refresh automatically.

Click Refresh 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".
	SYN Tx	The number of 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.

There would be 5 entries on each page. Click Previous to return to the previous page and Next to the next page.

Appendix A: FAQ

1. **What should I do if I cannot access the web management page?**

   A1. If the computer is set to a static IP address, change its settings to obtain an IP address automatically.

   A2. Make sure http://tplinkmodem.net or http://192.168.1.1 is correctly entered in the web browser.

   A3. Use another web browser and try again.

   A4. Reboot your router and try again.

   A5. Disable and enable the active network adapter in use.

2. **What can I do if I cannot access the internet?**

   A1. Verify that your SIM card is an LTE, WCDMA or GSM card.

   A2. Verify that your SIM card is in your internet service provider's service area.

   A3. Verify that your SIM card has sufficient credit.

   A4. Check the LAN connection:

   Open a web browser and enter http://tplinkmodem.net or http://192.168.1.1 in the address bar. If the login page does not appear, refer to FAQ > Q1 and then try again.

   A5. Check your ISP parameters:

   1) Open a web browser and log in to the web management page.

   2) Go to Network > LTE Dial Up to verify the parameters (including the APN, Username and Password) provided by your ISP are correctly entered. If the parameters are incorrect, click Create and enter the correct parameters, then select the new profile from the Profile Name list.

   A6. Check the PIN settings:

   1) Open a web browser and log in to the web management page.

   2) Go to Network > PIN Management to verify if PIN is required. If it is, enter the correct PIN provided by your ISP, and click Apply.

   A7. Check the Data Limit:

   1) Open a web browser and log in to the web management page.

2) Go to Network > LTE Data Settings to verify if the Total/Monthly Used exceeds the Total/Monthly Allowance. If it does, click Correct and set Total/Monthly Used to 0 (zero), or disable Data Limit.

A8. Check the Mobile Data:

1) Open a web browser and log in to the web management page.

2) Go to Network > LTE Dial Up to verify that Mobile Data is enabled. If not, enable it to access the internet.

A9. Check the Data Roaming:

1) Confirm with your ISP if you are in a roaming service area. If you are, open a web browser and log into the web management page.

2) Go to Network > LTE Dial Up to enable the Data Roaming.

3. **How do I restore the router to its factory default settings?**

A1. With the router powered on, press and hold the WPS/RESET button on the rear panel of the router until the Power LED starts flashing, then release the button. Wait while the router resets.
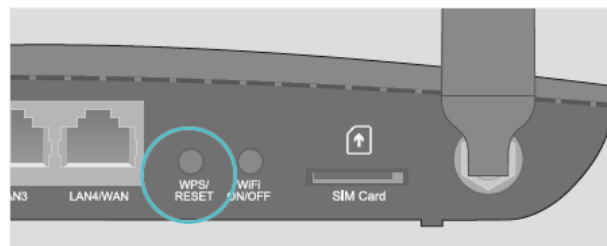
WPS/RESET Button - Press and hold until the Power LED starts flashing.

A2. Log in to the web management page of the router, and go to System Tools > Factory Defaults, click Restore and wait until the reset process is complete.

4. **What should I do if I forget my web management page password?**

A. Refer to FAQ > Q3 to reset the router and then use admin (all lower case) for both username and password to log in.

5. **What should I do if I forget my wireless network password?**

A1. The default Wireless Password is printed on the product label of the router.

A2. If the default Wireless Password has been changed, log in to the router's web management page and go to Wireless > Wireless Security to retrieve or reset your password.
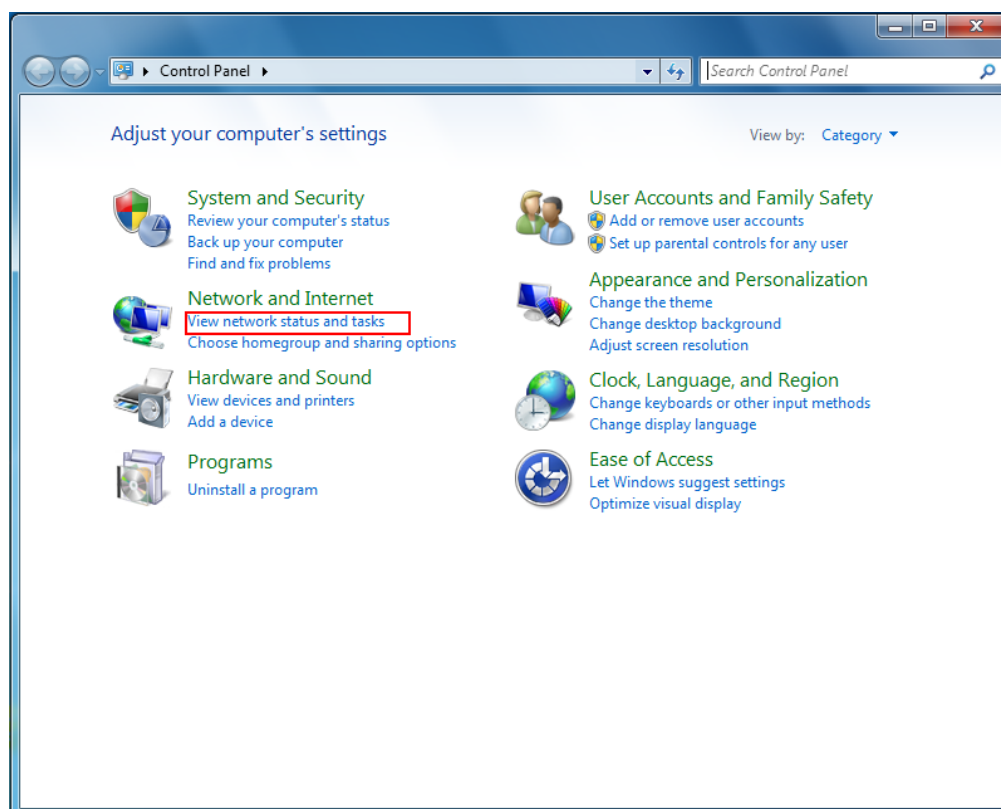
Appendix B: Configuring the PC

In this section, we'll introduce how to install and configure the TCP/IP correctly in Windows 7. First make sure your Ethernet Adapter is working, refer to the adapter's manual if needed.
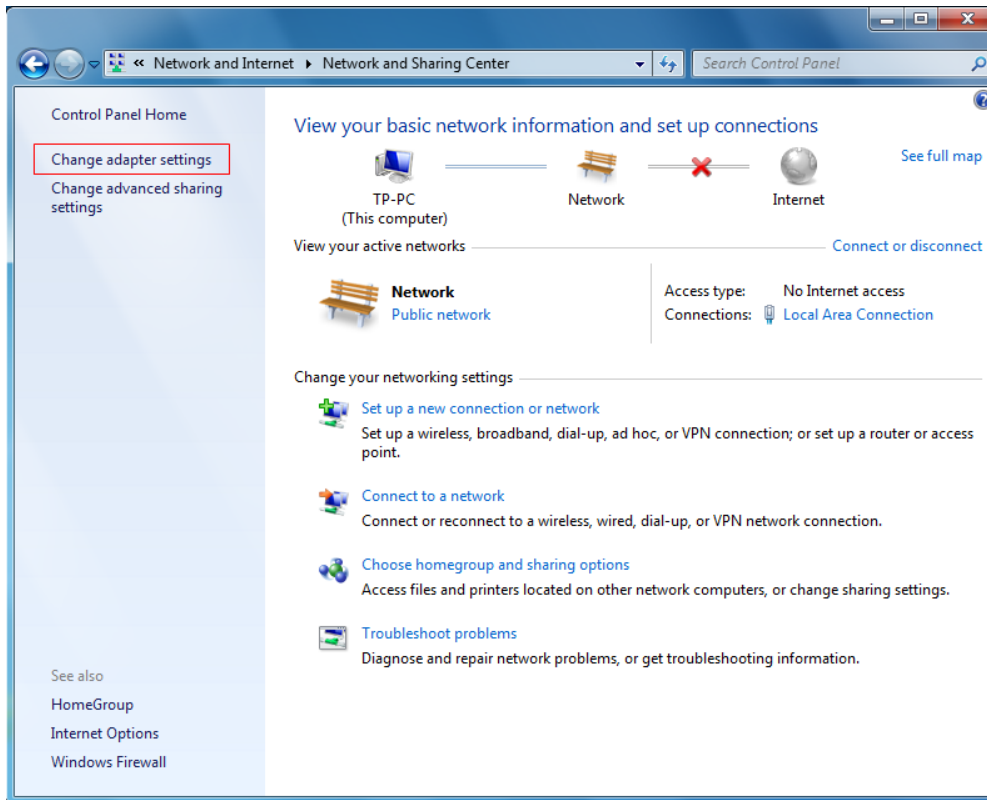
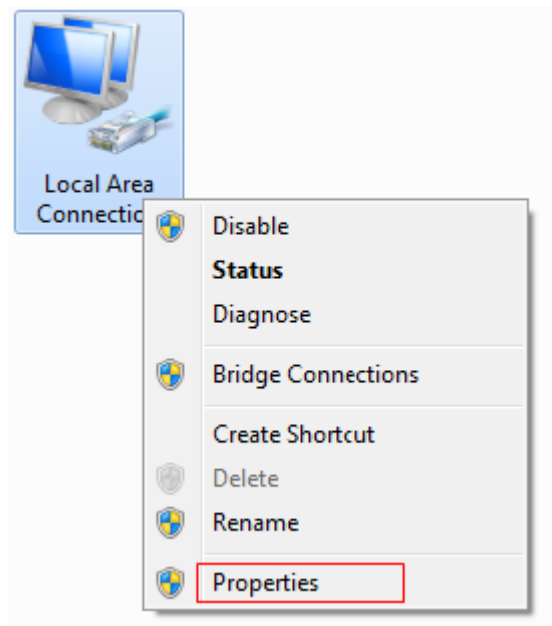1) On the Windows taskbar, click the Start button, and then click Control Panel.
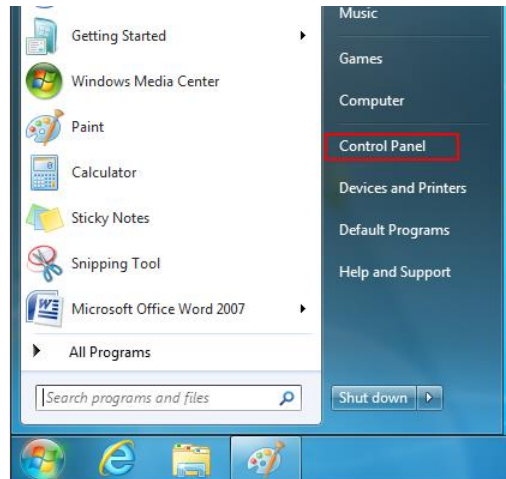
2) Click the View network status and tasks.

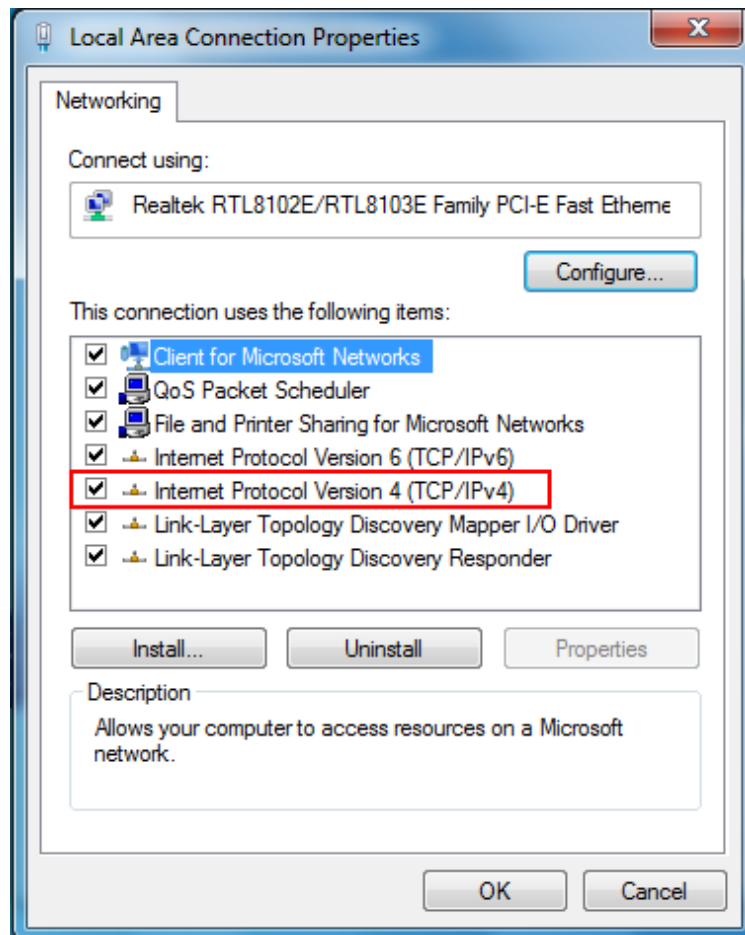3) Click the Change adapter settings.

4) Click the right button, and Select Properties.

5) In the prompt page that showed below, double click on the Internet Protocol Version 4 (TCP/IPv4).

6) The following Internet Protocol Version 4 (TCP/IPv4) Properties window will display and the IP Address tab is open on this window by default.

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 address automatically, as shown in the Figure below:
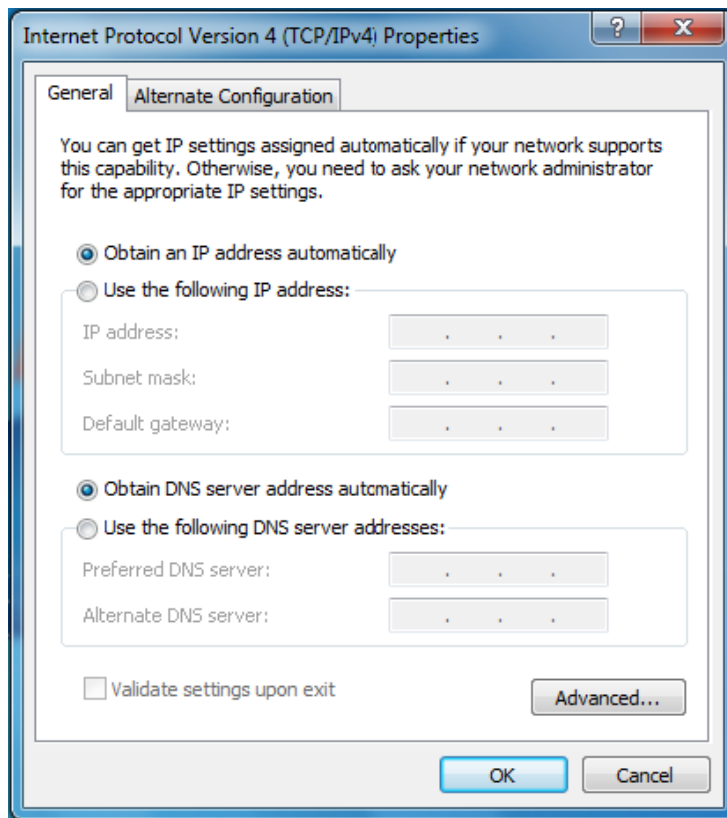
➢ Setting IP address manually

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

2 If the Device's LAN IP address is 192.168.1.1, type IP address is 192.168.1.x (x is from 2 to 254), and Subnet mask is 255.255.255.0.

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

4 Select Use the following DNS server addresses radio button. In the Preferred DNS Server field you can type the DNS server IP address, which has been provided by your ISP.
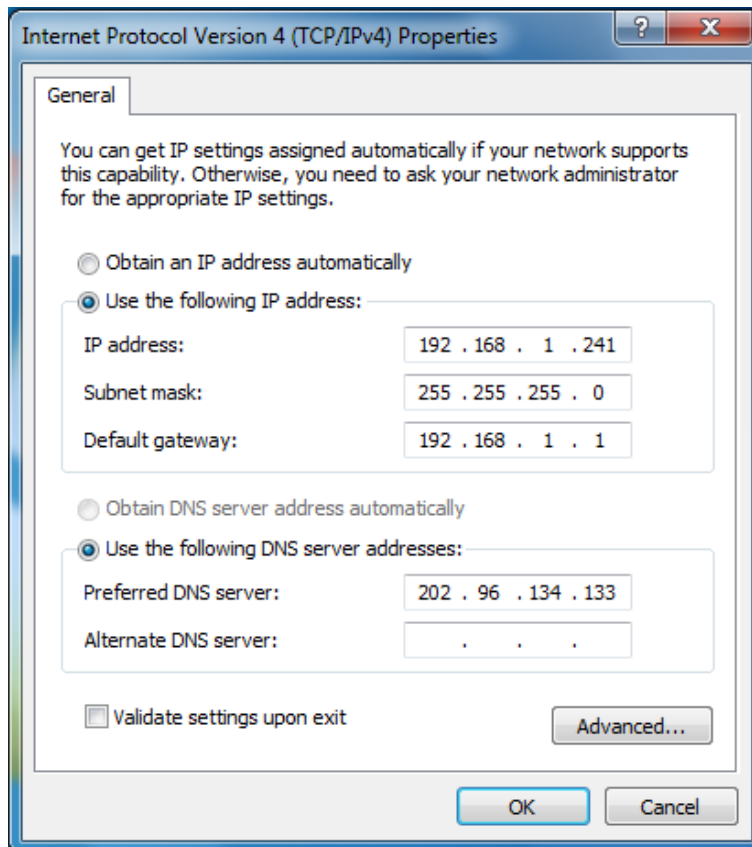
7) Now click OK to keep your settings.