User Guide

300Mbps Wireless N USB VDSL/ADSL Modem

TD-W9970
COPYRIGHT & TRADEMARKS

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

No part of the specifications may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from TP-Link Technologies Co., Ltd. Copyright © 2016 TP-Link Technologies Co., Ltd. All rights reserved.

http://www.tp-link.com
FCC STATEMENT

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

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

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

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

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

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

FCC RF Radiation Exposure Statement

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

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

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

RF Exposure Information

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

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

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

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="DC voltage symbol" /></td>
<td>DC voltage</td>
</tr>
<tr>
<td><img src="image" alt="Indoor use only symbol" /></td>
<td>Indoor use only</td>
</tr>
</tbody>
</table>

### 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.
About This Guide.................................................................................................................. 1

Chapter 1. Introduction ....................................................................................................... 2
  1.1 Product Overview ........................................................................................................ 2
  1.2 Product Appearance...................................................................................................... 2
    1.2.1 LEDs .................................................................................................................... 2
    1.2.2 Ports and Buttons ................................................................................................ 4

Chapter 2. Connecting the Modem Router .................................................................... 5
  2.1 Positioning the Modem Router .................................................................................. 5
  2.2 Connecting the Modem Router .................................................................................. 6

Chapter 3. Quick Installation Guide................................................................................. 8

Chapter 4. Configuring the Modem Router ................................................................. 12
  4.1 Login ......................................................................................................................... 12
  4.2 Status........................................................................................................................ 12
  4.3 Operation Mode ......................................................................................................... 13
  4.4 Network....................................................................................................................... 14
    4.4.1 WAN Settings ...................................................................................................... 15
    4.4.2 3G/4G Settings .................................................................................................. 31
    4.4.3 Interface Grouping ............................................................................................. 33
    4.4.4 LAN Settings ....................................................................................................... 35
    4.4.5 IPv6 LAN Settings ............................................................................................... 36
    4.4.6 MAC Clone .......................................................................................................... 37
    4.4.7 ALG Settings ....................................................................................................... 38
    4.4.8 DSL Settings ....................................................................................................... 39
    4.4.9 IPSec VPN ........................................................................................................... 39
  4.5 IPTV ............................................................................................................................. 45
  4.6 DHCP Server ............................................................................................................. 47
    4.6.1 DHCP Settings .................................................................................................... 47
    4.6.2 Clients List ........................................................................................................... 48
    4.6.3 Address Reservation ......................................................................................... 48
    4.6.4 Conditional Pool ............................................................................................... 49
  4.7 Wireless ...................................................................................................................... 51
4.7.1 Basic Settings ............................................................................................................ 51
4.7.2 WPS Settings ............................................................................................................ 53
4.7.3 Wireless Security ....................................................................................................... 55
4.7.4 Wireless Schedule ..................................................................................................... 57
4.7.5 Wireless MAC Filtering ............................................................................................... 58
4.7.6 Wireless Advanced ..................................................................................................... 59
4.7.7 Wireless Status .......................................................................................................... 60
4.8 Guest Network ................................................................................................................. 61
4.8.1 Basic Settings ............................................................................................................ 61
4.8.2 Guest Network Status ............................................................................................... 62
4.9 USB Settings ................................................................................................................... 62
4.9.1 USB Mass Storage ..................................................................................................... 63
4.9.2 User Accounts .......................................................................................................... 63
4.9.3 Storage Sharing ......................................................................................................... 64
4.9.4 FTP Server ................................................................................................................ 67
4.9.5 Media Server ............................................................................................................. 68
4.9.6 Print Server ............................................................................................................... 69
4.10 Route Settings ................................................................................................................. 70
4.10.1 Default Gateway ....................................................................................................... 70
4.10.2 Static Route ............................................................................................................. 70
4.10.3 RIP Settings ............................................................................................................ 71
4.11 IPv6 Route Settings ......................................................................................................... 72
4.11.1 IPv6 Default Gateway ............................................................................................... 72
4.11.2 IPv6 Static Route ...................................................................................................... 72
4.12 Forwarding ....................................................................................................................... 73
4.12.1 Virtual Server .......................................................................................................... 73
4.12.2 Port Triggering ......................................................................................................... 75
4.12.3 DMZ ........................................................................................................................ 77
4.12.4 UPnP ....................................................................................................................... 77
4.13 Parental Control ............................................................................................................... 78
4.14 Firewall .......................................................................................................................... 79
4.14.1 Rule .......................................................................................................................... 80
4.14.2 LAN Host .................................................................................................................. 81
4.14.3 WAN Host ............................................................................................................... 82
4.14.4 Schedule .................................................................................................................... 83
4.15 IPv6 Firewall .................................................................................................................... 84
4.15.1 IPv6 Rule ................................................................. 84
4.15.2 IPv6 LAN Host .......................................................... 86
4.15.3 IPv6 WAN Host ......................................................... 86
4.15.4 IPv6 Schedule ............................................................ 87
4.16 IPv6 Tunnel ................................................................. 88
4.17 Bandwidth Control ...................................................... 90
4.18 IP & MAC Binding ...................................................... 92
  4.18.1 Binding Settings .................................................... 92
  4.18.2 ARP List .............................................................. 93
4.19 Dynamic DNS ............................................................. 94
4.20 Diagnostic ................................................................. 94
4.21 System Tools ............................................................. 95
  4.21.1 System Log .......................................................... 95
  4.21.2 Time Settings ....................................................... 96
  4.21.3 Manage Control .................................................. 97
  4.21.4 CWMP Settings .................................................. 98
  4.21.5 SNMP Settings .................................................. 99
  4.21.6 Backup & Restore ................................................ 100
  4.21.7 Factory Defaults ................................................ 100
  4.21.8 Firmware Upgrade .............................................. 101
  4.21.9 Reboot ............................................................... 102
  4.21.10 Statistics .......................................................... 102
4.22 Logout ...................................................................... 104

Appendix A: Configuring the PC ........................................ 105
Appendix B: Troubleshooting ............................................. 110
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:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Teal Underlined</td>
<td>Hyperlinks are in blue with an underline. You can click to redirect to a website or a specific section.</td>
</tr>
<tr>
<td>Teal</td>
<td>Contents to be emphasized and texts on the web page are in teal, including the menus, items, buttons, etc.</td>
</tr>
<tr>
<td>→</td>
<td>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.</td>
</tr>
<tr>
<td>🚨 Note</td>
<td>Ignoring this type of note might result in a malfunction or damage to the device.</td>
</tr>
</tbody>
</table>

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 Modem router is a combined wired/wireless network connection device with integrated wireless router and DSL modem, reducing hassle of configuration and saving space.

With DSL and WAN ports, the modem router is compatible with DSL connections and fiber/cable access.

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

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

1.2 Product Appearance

1.2.1 LEDs

The modem 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.
<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
<th>Indication</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Power)</td>
<td>On</td>
<td>System start-up complete.</td>
</tr>
<tr>
<td></td>
<td>Flash</td>
<td>System starting up or device updating.</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>The modem router is off. Please ensure that the power adapter is</td>
</tr>
<tr>
<td></td>
<td></td>
<td>connected correctly.</td>
</tr>
<tr>
<td>(DSL)</td>
<td>On</td>
<td>DSL line is synchronized and ready to use.</td>
</tr>
<tr>
<td></td>
<td>Flash</td>
<td>The DSL negotiation is in progress.</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>There is no connection to the DSL Port or DSL synchronization fails.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Please refer to Note 1 for troubleshooting.</td>
</tr>
<tr>
<td>(Internet)</td>
<td>On</td>
<td>The network is available with a successful Internet connection.</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>There is no successful Internet connection or the modem router</td>
</tr>
<tr>
<td></td>
<td></td>
<td>is operating in Bridge mode. Please refer to Note 2 for troubleshooting.</td>
</tr>
<tr>
<td>(Wireless)</td>
<td>On</td>
<td>The wireless function is working properly.</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>The wireless function is disabled.</td>
</tr>
<tr>
<td>(WPS)</td>
<td>On/Off</td>
<td>It turns on when a wireless device has been successfully</td>
</tr>
<tr>
<td></td>
<td></td>
<td>connected to the network via WPS. After about 5 minutes, the WPS LED will</td>
</tr>
<tr>
<td></td>
<td></td>
<td>turn off.</td>
</tr>
<tr>
<td></td>
<td>Flash</td>
<td>WPS handshaking is in process and will continue for about 2 minutes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Please press the WPS/RESET button on other wireless devices that you want</td>
</tr>
<tr>
<td></td>
<td></td>
<td>to add to the network while the LED is flashing.</td>
</tr>
<tr>
<td>(USB)</td>
<td>On</td>
<td>The USB device is identified and ready to use.</td>
</tr>
<tr>
<td></td>
<td>Flash</td>
<td>The USB device is being identified.</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>No USB device is plugged in to the USB port.</td>
</tr>
<tr>
<td>(LAN1-4)</td>
<td>On</td>
<td>There is a device connected to this LAN port.</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>There is no device connected to this LAN port.</td>
</tr>
</tbody>
</table>

**Note:**

1. If the DSL LED is off, please check your Internet connection first. Refer to 2.2 Connecting the Modem Router for more information about how to make Internet connection correctly. If you have already made a right connection, please contact your ISP to make sure if your Internet service is available now.
2. If the Internet LED is off, please check your DSL LED first. If your DSL LED is also off, please refer to Note 1. If your DSL LED is GREEN ON, please check your Internet configuration. You may need to check this part of information with your ISP and make sure everything have been input correctly.

3. You can also refer to 4.7.2 WPS Settings for more information.

### 1.2.2 Ports and Buttons

<table>
<thead>
<tr>
<th>Status</th>
<th>Indication</th>
</tr>
</thead>
<tbody>
<tr>
<td>VDSL</td>
<td>Through the port, you can connect the modem router with the telephone. Or you can connect them by an external separate splitter. For details, please refer to 2.2 Connecting the Modem Router.</td>
</tr>
<tr>
<td>LAN4/WAN, LAN3, LAN2, LAN1</td>
<td>Through these ports, you can connect the modem router to your PC or the other Ethernet network devices.</td>
</tr>
<tr>
<td>USB</td>
<td>The USB port connects to a USB storage device, a USB printer or a 3G/4G Modem.</td>
</tr>
<tr>
<td>WiFi</td>
<td>The switch for the WiFi function. Press the button to enable/disable the WiFi function.</td>
</tr>
<tr>
<td>WPS/RESET</td>
<td>The switch for the WPS function or resetting the modem router.</td>
</tr>
<tr>
<td>ON/OFF</td>
<td>The switch for the power.</td>
</tr>
<tr>
<td>POWER</td>
<td>The Power plug is where you will connect the power adapter.</td>
</tr>
<tr>
<td>Antennas</td>
<td>Used for wireless operation and data transmit.</td>
</tr>
</tbody>
</table>
Chapter 2. Connecting the Modem Router

2.1 Positioning the Modem Router

With the modem router, you can access your network from anywhere within the wireless network coverage. However, the wireless signal strength and coverage vary depending on the actual environment of your modem router. Many obstacles may limit the range of the wireless signal, for example, concrete structures or thick walls.

For your security and best Wi-Fi performance, please note the following:

- Do NOT locate the modem router in a place where it will be exposed to moisture or excessive heat.
- Keep away from the strong electromagnetic radiation and the device of electromagnetic sensitive.
- Place the modem router in a location where it can be connected to the various devices as well as to a power source.
- Make sure the cables and power cord are safely placed out of the way so they do not create a tripping hazard.

Generally, the modem router is placed on a horizontal surface, such as a shelf or desktop. The device also can be mounted on the wall as shown below.

Note:

The diameter of the screw, 3.5mm<\( D < 7.8 \text{mm} \), and the distance of two screws is 107.5mm. The screw that project from the wall need around 4mm based, and the length of the screw need to be at least 20mm to withstand the weight of the product.
2.2 Connecting the Modem Router

Before installing the device, please make sure your broadband service provided by your ISP is available. If there is any problem, please contact your ISP. Before cable connection, cut off the power supply and keep your hands dry. You can follow the steps below to install it.

Step 1: Connect the DSL Line.

**Method one**: Directly connect the modem router to the phone jack with the DSL line.

**Method two**: Connect the modem router to the phone jack via a separate splitter. External splitter can divide the data and voice, and then you can access the Internet and make calls at the same time. The external splitter has three ports:

- **LINE**: Connect to the wall jack
- **PHONE**: Connect to the phone sets
- **MODEM**: Connect to the DSL port of the modem router

Plug one end of the twisted-pair DSL cable into the VDSL port on the rear panel of the modem router. Connect the other end to the MODEM port of the external splitter.

Step 2: Connect your computer to the modem router.

**Method One: Wired**

Connect the computer to a LAN port on your modem router with an Ethernet cable.
Method Two: Wireless

Click the network icon of your computer or go to Wi-Fi Setting of your smart device, then use the default SSID (Wireless Network Name) and Wireless Password printed on the product label of the modem router to join the network.

Method Three: Via the WPS button

Wireless devices that support WPS, including Android phones, tablets, most USB network cards, can be connected to your router through this method. (WPS is not supported by iOS devices.)

ős Note:
The WPS function cannot be configured if the wireless function of the modem router is disabled. Also, the WPS function will be disabled if your wireless encryption is WEP. Please make sure the wireless function is enabled and is configured with the appropriate encryption before configuring the WPS.

1) Tap the WPS icon on the device’s screen.
2) Immediately press the WPS button on your modem router.
3) The WPS LED flashes for about two minutes during the WPS process.
4) When the WPS LED is on, the client device has successfully connected to the modem router.

Step 3: Attach the power adapter. The electrical outlet shall be installed near the device and shall be easily accessible.
Chapter 3. Quick Installation Guide

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

1. If the TCP/IP Protocol on your computer is set to a static IP address, you need to change it to obtain an IP address automatically. Please refer to Appendix A: Configuring the PC for more detailed instruction.

2. To access the web management page, open a web browser and enter the default address http://tplinkmodem.net in the address field of the browser.

   ![Login window](Image)

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

   ![Quick Setup screen](Image)

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

3. After your successful login, you will see the Quick Setup screen. Click Next to start Quick Setup.
4. Select your Region and Time Zone from the drop-down list, then click Next.

```
<table>
<thead>
<tr>
<th>Quick Setup - Region and Time Zone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Please select your region and time zone.</td>
</tr>
<tr>
<td>Region</td>
</tr>
<tr>
<td>Time Zone</td>
</tr>
<tr>
<td>Back</td>
</tr>
</tbody>
</table>
```

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

```
<table>
<thead>
<tr>
<th>Quick Setup - Auto Detection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto-Detect Connection Type:</td>
</tr>
<tr>
<td>This Setup Wizard can detect the type of Internet connection you have. Do you want The Smart Setup Wizard to try and detect The connection type now?</td>
</tr>
<tr>
<td>Yes.</td>
</tr>
<tr>
<td>No. I want to configure The Internet Connection myself.</td>
</tr>
<tr>
<td>Back</td>
</tr>
</tbody>
</table>
```

6. Configure parameters for WAN connection. Here we take PPPoE as an example. Enter the User name and Password provided by your ISP. Then click Next.

```
<table>
<thead>
<tr>
<th>Quick Setup - PPPoE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto-detection has succeeded!</td>
</tr>
<tr>
<td>VLAN ID: 0</td>
</tr>
<tr>
<td>Connection Type: PPPoE</td>
</tr>
<tr>
<td>Please enter the Username and Password. If the Username/Password are unknown, please contact your ISP.</td>
</tr>
<tr>
<td>User name:</td>
</tr>
<tr>
<td>Password:</td>
</tr>
<tr>
<td>Confirm password:</td>
</tr>
<tr>
<td>Back</td>
</tr>
</tbody>
</table>
```

7. 3G/4G Router Mode can be set as a backup Internet access method. If you do not want to configure 3G/4G settings now, just click Next to continue.
8. The wireless function is enabled by default. You can rename your wireless network name and create your own password in this page. The default wireless name is TP-LINK_XXXX. Click Next to continue.
9. Confirm all parameters. Click **Back** to modify or click **Save** to make your configuration effective.

![Quick Setup - Confirm](image)

10. You will see the **Complete** screen, click **Finish** to complete these settings.
Chapter 4. Configuring the Modem Router

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

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.

<table>
<thead>
<tr>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quick Setup</td>
</tr>
<tr>
<td>Operation Mode</td>
</tr>
<tr>
<td>Network</td>
</tr>
<tr>
<td>IPTV</td>
</tr>
<tr>
<td>DHCP Server</td>
</tr>
<tr>
<td>Wireless</td>
</tr>
<tr>
<td>Guest Network</td>
</tr>
<tr>
<td>USB Settings</td>
</tr>
<tr>
<td>Route Settings</td>
</tr>
<tr>
<td>IPv6 Route Settings</td>
</tr>
<tr>
<td>Forwarding</td>
</tr>
<tr>
<td>Parent Control</td>
</tr>
<tr>
<td>Firewall</td>
</tr>
<tr>
<td>IPv6 Firewall</td>
</tr>
<tr>
<td>IPv6 Tunnel</td>
</tr>
<tr>
<td>Bandwidth Control</td>
</tr>
<tr>
<td>IP &amp; MAC Binding</td>
</tr>
<tr>
<td>Dynamic DNS</td>
</tr>
<tr>
<td>Diagnostic</td>
</tr>
<tr>
<td>System Tools</td>
</tr>
<tr>
<td>Logout</td>
</tr>
</tbody>
</table>

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

4.2 Status

Choose Status, you can see the basic status of the modem router. All information on this page is read-only.
4.3 Operation Mode

Choose Operation Mode, you will see the screen as shown below. Select your desired mode and then click Save.
Operation Mode

- **DSL Modem Router Mode**: In this mode, the device enables multi-users to share Internet via ADSL/VDSL using its VDSL port and share it wirelessly.
- **3G/4G Router Mode**: In this mode, the device allows multi-users to share a 3G/4G mobile broadband connection via wired or wireless connection.
- **Wireless Router Mode**: In this mode, the device enables multi-users to share Internet via Ethernet WAN (EWAN) using its interchangeable LAN/WAN port and share it wirelessly at 300Mbps wireless 802.11n speeds.

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

Note Dialog

### 4.4 Network

Choose **Network**, you will see the following submenus. Click any one of them, and you can configure the corresponding function.
4.4.1 WAN Settings

Go to Network → WAN Settings, and you will see the WAN Port Information.

☞ Note:
Some modem routers may not support VDSL mode, please refer to 4.4.1.1 ADSL WAN Settings.

4.4.1.1 ADSL WAN Settings

For ADSL mode, there are six different configurations for the connection types, which are Static IP, Dynamic IP, PPPoE, PPPoA, IPoA and Bridge. You can select the corresponding types according to your needs.

Click Add to add a new entry, you can configure the parameters for PTM and WAN Service in the next screen.

DSL Modulation Type:

➢ DSL Modulation Type: Select ADSL or VDSL according to your needs.
ATM Configuration:

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

1) **Static IP**

Select this option if your ISP provides static IP information to you. You should set static IP address, IP subnet mask, and gateway address in the screen below.

Click Advance, you can see the advanced selections of ATM Configuration.

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

**WAN Service Setup:**

- **Enable IPv4:** Check the box to enable IPv4.
- **IP Address:** Enter the IP address in dotted-decimal notation provided by your ISP.
- **Subnet Mask:** Enter the subnet mask in dotted-decimal notation provided by your ISP, usually is 255.255.255.0.
- **Gateway** (Optional): Enter the gateway IP address in dotted-decimal notation provided by your ISP.
- **DNS Server/ Secondary DNS Server**: Here you can set DNS Server (at least one) manually. The router will use this DNS Server for priority.
- **Default Gateway**: Select a WAN Interface from the drop-down list as the IPv4 default gateway.
- **Enable IPv6**: Check the box to enable IPv6.
- **IPv6 Address**: Enter the IPv6 address provided by your ISP.
- **Prefix Length**: Enter the prefix length of the IPv6 address. The default value is 64.
- **IPv6 Gateway**: Enter the gateway IPv6 address provided by your ISP.
- **IPv6 DNS Server / Secondary IPv6 DNS Server**: Here you can set IPv6 DNS Server (at least one) manually. The router will use this IPv6 DNS Server for priority.
- **IPv6 Default Gateway**: Select a WAN Interface from the drop-down list as the IPv6 default gateway.

Click **Advance**, you can see the advanced selections of WAN Service Setup.

- **MTU (Bytes)**: Maximum Transmission Unit Size. Check this box then you can change the MTU size. The default MTU value is 1500 Bytes. It is not recommended that you change the default value unless required by your ISP.
- **Enable NAT**: This technology translates the IP addresses of a local area network to a different IP address for the Internet. If this modem router is hosting your network's connection to the Internet, please select the check box. If another router exists in your network, you don't need to select the option.
- **Enable Fullcone NAT**: It is a type of NAT. If not enabled, the default NAT will act.
- **Enable SPI Firewall**: A SPI firewall enhances network's security. Select the option to use a firewall, or else without a firewall.
- **Enable IGMP Proxy**: IGMP (Internet Group Management Protocol) is used to manage multicasting on TCP/IP networks. Some ISPs use IGMP to perform remote configuration for client devices, such as the modem router. The default value is disabled, and if you are not sure, please contact your ISP or just leave it.

Click **Save** to make the settings effective.

2) **Dynamic IP**

Select this option, and the modem router can obtain IP network information dynamically from a DHCP server provided by your ISP.
Click **Advance**, advanced selections for WAN Service Setup can be shown.

- **MTU (Bytes):** Maximum Transmission Unit Size. Check this box then you can change the MTU size. The default MTU value is 1500 Bytes. It is not recommended that you change the default value unless required by your ISP.

- **Enable NAT:** This technology translates the IP addresses of a local area network to a different IP address for the Internet. If this modem router is hosting your network’s connection to the Internet, please select the check box. If another Router exists in your network, you don’t need to select the option.

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

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

- **Enable IGMP Proxy:** IGMP (Internet Group Management Protocol) is used to manage multicasting on TCP/IP networks. Some ISPs use IGMP to perform remote configuration for
client devices, such as the modem router. The default value is disabled, and if you are not sure, please contact your ISP or just leave it.

- **Get IP with Unicast**: This is disabled by default. The minority of DHCP Server of ISP will not support to enable this. When the Route is connected right but IP cannot get, you can select this box.

- **Set DNS Server manually**: Choose Set DNS Server manually, you can set DNS Server manually here. The modem router will use this DNS Server for priority.

- **Get IPv6 Address with Unicast**: This is disabled by default. The minority of DHCPv6 Server of ISP will not support to enable this. When the modem router is connected right but IPv6 address cannot get, you can select this box.

- **Set IPv6 DNS Server manually**: Choose this option, and you can set IPv6 DNS Server manually here. The modem router will use this IPv6 DNS Server for priority.

- **Host Name**: Displays model No. of your modem router.

Click **Save** to make the settings effective.

3) **PPPoE**

If your ISP provides a PPPoE connection and you need to use an ATM Interface, choose **PPPoE** in the drop-down list, and then the screen will be displayed as below.
- **PPP Username/Password/Confirm Password**: Enter the Username, Password and Confirm Password provided by your ISP. These fields are case-sensitive.
- **Connection Mode**: For PPPoE connection, you can select **Always on** or **Connect on demand** or **Connect manually**. Connect on demand is dependent on the traffic. If there is no traffic (or Idle) for a pre-specified period of time, the connection will tear down automatically. And once there is traffic send or receive, the connection will be automatically on.
- **Authentication Type**: Select the **Authentication Type** from the drop-down list, the default method is **AUTO_AUTH**, and you can leave it as a default setting.
- **Enable IPv4**: Check this box to enable IPv4.
- **Default Gateway**: Select a WAN connection from the drop-down list as the IPv4 default gateway.
- **Enable IPv6**: Check this box to enable IPv6.
- **Addressing Type**: Select the **Addressing Type** from the drop-down list.
- IPv6 Default Gateway: Select a WAN connection from the drop-down list as the IPv6 default gateway.

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

- Service Name/Server Name: Enter the Service Name and Server Name if it was provided by your ISP. You can leave them blank, if the ISP doesn’t provide them.

- MTU (Bytes): Maximum Transmission Unit Size. Check this box then you can change the MTU size. The default MTU value is 1500 Bytes. It is not recommended that you change the default value unless required by your ISP.

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

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

- Enable IGMP Proxy: IGMP (Internet Group Management Protocol) is used to manage multicasting on TCP/IP networks. Some ISPs use IGMP to perform remote configuration for client devices, such as the modem router. The default value is disabled, and if you are not sure, please contact your ISP or just leave it.

- Use IP address specified by ISP: Choose Use IP address specified by ISP, you can enter the IP address provided by your ISP.

- Echo request interval: The router will detect Access Concentrator online at every interval. The default value is 0. You can input the value between 0 and 120. The value 0 means no detect.

- Set DNS Server manually: Choose this option, and you can set DNS Server manually here. The modem router will use this DNS Server for priority.

- Use IPv6 address specified by ISP: Choose Use IPv6 address specified by ISP, you can enter the IPv6 address provided by your ISP.

- Set IPv6 DNS Server manually: Choose Set IPv6 DNS Server manually, you can set IPv6 DNS Server manually here. The modem router will use this IPv6 DNS Server for priority.

Click Save to make the settings effective.

4) PPPoA

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

The configuration is similar to PPPoE. Please refer to the section 3) PPPoE to configure this part.
5) IPoA

If your ISP provides an IPoA connection, select IPoA option for the Connection Type on the screen.
IP Address/Subnet Mask: Enter the IP Address and Subnet Mask provided by ISP. If you forget, you can ask your ISP.

Gateway: Enter the gateway IP address in dotted-decimal notation provided by your ISP.

DNS Server/Secondary DNS Server: Type in your preferred DNS server.

Default Gateway: Select a WAN Interface from the drop-down list as the IPv4 default gateway.

6) Bridge

If you select this type of connection, the modem router can be configured to act as a bridging device between your LAN and your ISP. Bridges are devices that enable two or more networks to communicate as if they are two segments of the same physical LAN.
After you finishing the Internet configuration, please click **Save** to make the settings take effect.

### 4.4.1.2 VDSL WAN Settings

For **VDSL** mode, there are four connection types, which are Static IP, Dynamic IP, PPPoE and Bridge. You can select the corresponding types according to your needs.

Click **Add** to add a new entry, you can configure the parameters for PTM and WAN Service in the next screen as shown below.
DSL Modulation Type:

- **DSL Modulation Type**: Select ADSL or VDSL according to your needs.

PTM Configuration:

- **Enable VLAN ID**: Check the box to enable the Virtual LAN ID.
- **VLAN ID (1~4049)**: This indicates the VLAN group, and the valid range is from 1 to 4049.

1) **Static IP**

Select this option if your ISP provides static IP information to you. You should set static IP address, IP subnet mask, and gateway address in the screen below.
WAN Service Setup:

- **Enable IPv4**: Check the box to enable IPv4.
- **IP Address**: Enter the IP address in dotted-decimal notation provided by your ISP.
- **Subnet Mask**: Enter the subnet mask in dotted-decimal notation provided by your ISP, usually it is 255.255.255.0.
- **Gateway (Optional)**: Enter the gateway IP address in dotted-decimal notation provided by your ISP.
- **DNS Server/Secondary DNS Server**: Here you can set DNS Server (at least one) manually. The router will use this DNS Server for priority.
- **Default Gateway**: Select a WAN Interface from the drop-down list as the IPv4 default gateway.
- **Enable IPv6**: Check the box to enable IPv6.
- **IPv6 Address**: Enter the IPv6 address provided by your ISP.
Prefix Length: Enter the prefix length of the IPv6 address. The default value is 64.
IPv6 Gateway: Enter the gateway IPv6 address provided by your ISP.
IPv6 DNS Server/Secondary IPv6 DNS Server: Here you can set IPv6 DNS Server (at least one) manually. The Route will use this IPv6 DNS Server for priority.
IPv6 Default Gateway: Select a WAN Interface from the drop-down list as the IPv6 default gateway.

Click Advance, you can see the advanced selections of WAN Service Setup.

MTU (Bytes): Maximum Transmission Unit Size. Check this box then you can change the MTU size. The default MTU value is 1500 Bytes. It is not recommended that you change the default value unless required by your ISP.
Enable NAT: This technology translates the IP addresses of a local area network to a different IP address for the Internet. If this modem router is hosting your network’s connection to the Internet, please select the check box. If another Router exists in your network, you don’t need to select the option.
Enable Fullcone NAT: It is a type of NAT, if not enabled, the default NAT will act.
Enable SPI Firewall: A SPI firewall enhances network’s security. Select the option to use a firewall, or else without a firewall.
Enable IGMP Proxy: IGMP (Internet Group Management Protocol) is used to manage multicasting on TCP/IP networks. Some ISPs use IGMP to perform remote configuration for client devices, such as the modem router. The default value is disabled, and if you are not sure, please contact your ISP or just leave it.

Click Save to make the settings effective.

2) Dynamic IP
Select this option, the modem router can obtain IP network information dynamically from a DHCP server provided by your ISP.
Click **Advance**, you can see the advanced selections for **WAN Service Setup**.

- **MTU (Bytes):** Maximum Transmission Unit Size. Check this box then you can change the MTU size. The default MTU value is 1500 Bytes. It is not recommended that you change the default value unless required by your ISP.

- **Enable NAT:** This technology translates the IP addresses of a local area network to a different IP address for the Internet. If this modem router is hosting your network’s connection to the Internet, please select the check box. If another router exists in your network, you don’t need to select the option.

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

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

- **Enable IGMP Proxy:** IGMP (Internet Group Management Protocol) is used to manage multicasting on TCP/IP networks. Some ISPs use IGMP to perform remote configuration for client devices, such as the modem router. The default value is disabled, and if you are not sure, please contact your ISP or just leave it.

- **Get IP with Unicast:** This is disabled by default. The minority of DHCP Server of ISP will not support to enable this. When the router is connected right but cannot get IP, you can select this box.
Set DNS Server manually: Choose Set DNS Server manually, you can set DNS Server manually here. The modem router will use this DNS Server for priority.

Get IPv6 Address with Unicast: This is disabled by default. The minority of DHCPv6 Server of ISP will not support to enable this. When the modem router is connected right but cannot get IPv6 address, you can select this box.

Set IPv6 DNS Server manually: Choose Set IPv6 DNS Server manually, you can set IPv6 DNS Server manually here. The modem router will use this IPv6 DNS Server for priority.

Host Name: Here displays model No. of your modem router.

Click Save to make the settings effective.

3) PPPoE

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

- PPP Username/Password/Confirm password: Enter the Username, Password and Confirm password provided by your ISP. These fields are case-sensitive.
- Connection Mode: For PPPoE connection, you can select Always on or Connect on demand or Connect manually. Connect on demand is dependent on the traffic. If there is no traffic for a pre-specified period of time, the connection will drop down automatically. And once there is traffic sent or received, the connection will be automatically on.
- Authentication Type: Select the Authentication Type from the drop-down list, the default method is AUTO_AUTH, and you can leave it as a default setting.
- Enable IPv4: Check this box to enable IPv4.
➢ **Enable IPv6**: Check this box to enable IPv6.

➢ **Default Gateway**: Select a WAN connection from the drop-down list as the IPv4 default gateway.

➢ **IPv6 Default Gateway**: Select a WAN connection from the drop-down list as the IPv6 default gateway.

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

➢ **Service Name/Server Name**: Enter the Service Name and Server Name if it was provided by your ISP. You can leave them blank, if the ISP doesn’t provide them.

➢ **MTU (Bytes)**: Maximum Transmission Unit Size. Check this box then you can change the MTU size. The default MTU value is 1500 Bytes. It is not recommended that you change the default value unless required by your ISP.

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

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

➢ **Enable IGMP Proxy**: IGMP (Internet Group Management Protocol) is used to manage multicasting on TCP/IP networks. Some ISPs use IGMP to perform remote configuration for client devices, such as the modem router. The default value is disabled, and if you are not sure, please contact your ISP or just leave it.

➢ **Use IP address specified by ISP**: Choose this option and you can enter the IP address provided by your ISP.

➢ **Set DNS Server manually**: Choose this option and you can set DNS Server manually here. The modem router will use this DNS server for priority.

➢ **Use IPv6 address specified by ISP**: Choose this option and you can enter the IPv6 address provided by your ISP.

➢ **Set IPv6 DNS Server manually**: Choose this option and you can set IPv6 DNS Server manually here. The modem router will use this IPv6 DNS Server for priority.

Click **Save** to make the settings effective.

4) **Bridge**

If you select this type of connection, the modem router can be configured to act as a bridging device between your LAN and your ISP. Bridges are devices that enable two or more networks to communicate as if they are two segments of the same physical LAN.
Note:

After you finish the Internet configuration, click Save to make the settings effective.

4.4.2 3G/4G Settings

If your modem router is in 3G/4G Router Mode, go to Network → 3G/4G Settings, you can configure parameters for 3G/4G function on the screen below. To use the 3G/4G function, you should first insert your USB modem on the USB port of the modem router. There is already much 3G/4G USB modem information embedded in the modem router. If your USB modem is supported by the modem router, then Successfully Identified will display in the USB 3G/4G Modem field. Select the correct Location and Mobile ISP manually, and the USB modem parameters will be set automatically.

Some 3G/4G USB modem may not be supported by the modem router. For more information, please refer to Compatibility List on our website: www.tp-link.com. If your 3G/4G USB modem is incompatible with our modem router, please contact our technical support by referring to the Technical Support card found in your package.
- **Location**: Please select the location where you’re enjoying the 3G/4G card.

- **Mobile ISP**: Please select the ISP (Internet Service Provider) you apply to for 3G/4G service. The modem router will show the default Dial Number and APN of that ISP.

- **Set the Dial Number, APN, Username and Password manually**: Check the box and fill the Dial Number and APN blanks below if your ISP is not listed in the Mobile ISP list or the default values are not the latest ones.

- **Dial Number**: Enter the Dial Number provided by your ISP.

- **APN**: Enter the APN (Access Point Name) provided by your ISP.

- **Username/Password**: Enter the username and password provided by your ISP. These fields are case-sensitive.

- **Always on**: Connect automatically after the modem router is disconnected. This option is enabled by default.

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

- **Connect manually**: You can click Connect/Disconnect to connect/disconnect connection immediately. This mode also supports the Max Idle Time function as Connect on demand mode. If you want your Internet connection to remain active at all times, enter 0 in the Max Idle Time field.

---

*Note:*

Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time because some applications visit the Internet continually in the background.
Authentication Type: Some ISPs need a specific authentication type, please confirm it with your ISP or keep the default settings.

Click Advance to configure advanced settings for 3G/4G Setup.

- **MTU size (in bytes):** The default MTU (Maximum Transmission Unit) size is 1480 bytes, which is usually fine. For some ISPs, you need modify the MTU. This should not be done unless you are sure it is necessary for your ISP.

- **Echo request interval:** The router will detect Access Concentrator online at every interval. The default value is 0. You can input the value between 0 and 120. The value 0 means no detect.

- **Use the following IP address:** If your ISP specifies an IP address for you, check the box, and fill the Static IP Address.

- **Use the following DNS Servers:** If your ISP specifies a DNS server IP address for you, check the box, and fill the Primary DNS and Secondary DNS blanks below. The Secondary DNS is optional. Otherwise, the DNS servers will be assigned dynamically from ISP.

- **Primary DNS:** Enter the DNS IP address in dotted-decimal notation provided by your ISP.

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

Click Save to make the settings effective.

Once the connection is successful, click Status and you will see the 3G/4G status.

<table>
<thead>
<tr>
<th>Name</th>
<th>Connection Type</th>
<th>VPI/VCI or VCI</th>
<th>IP/Netmask</th>
<th>Gateway</th>
<th>DNS</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>ppp_USB_3G</td>
<td>PPP3G</td>
<td>N/A</td>
<td>10.160.112.89/8</td>
<td>10.64.64.65</td>
<td>120.80.80.80 221.0.88.88</td>
<td>Connected</td>
</tr>
</tbody>
</table>

Note:

After connecting a 4G modem to the modem router, please access the web management page by visiting [http://tplinkmodem.net](http://tplinkmodem.net).

### 4.4.3 Interface Grouping

Go to Network → Interface Grouping, you can view all the current groups on this page.
Enable the Virtual LAN Ports feature: Virtual LAN (VLAN) is a group of devices on one or more LANs that are configured so that they can communicate as if they were attached to the same LAN. Because VLANs are based on logical instead of physical connections, it is very flexible for user/host management, bandwidth allocation and resource optimization. If you want to active Interface Grouping function, please check the box to enable the Virtual LAN Ports feature.

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

To support this feature, you need to click Add to create mapping groups with appropriate LAN and WAN interfaces. Click Remove to remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

Click Add to add a new interface group in the next screen. For example, you want LAN1 and LAN3 to be a group called Group 1 over br_ptm_1_0 WAN interface, you can refer to the following figure.

Click Save to make the entry effective immediately.
4.4.4 LAN Settings

Go to Network → LAN Settings, and you will see the LAN screen. Please configure the parameters for LAN ports according to the descriptions below.

- **IP Address**: You can configure the modem router’s IP address and subnet mask for LAN Interface.
  - **IP Address**: Enter the modem router’s local IP address, then you can access to the web management page via the IP address. The default value is 192.168.1.1.
  - **Subnet Mask**: Enter the modem router’s subnet mask. The default value is 255.255.255.0.
- **Enable IGMP Snooping**: If you select the option, please choose the IGMP mode: Standard Mode or Blocking Mode.
- **Enable Second IP**: You can configure the modem router’s second IP Address and Subnet Mask for LAN Interface through which you can also access to the Web-based management page as the default IP Address and Subnet Mask.
- **DHCP Server**: These settings allow you to configure the modem router’s Dynamic Host Configuration Protocol (DHCP) server function. The DHCP server is enabled by default for the modem router’s Ethernet LAN interface. DHCP service will supply IP settings to computers which are configured to automatically obtain IP settings that are connected to the modem router through the Ethernet port. When the modem router is set for DHCP, it becomes the default gateway for DHCP client connected to it. Keep in mind that if you change the IP address of the modem router, you must change the range of IP addresses in the pool used for DHCP on the LAN.
  - **Start IP Address**: Enter a value for the DHCP server to start with when issuing IP addresses. Because the default IP address for the modem router is 192.168.1.1, the default Start IP Address is 192.168.1.100, and the Start IP Address must be 192.168.1.100 or greater, but smaller than 192.168.1.254.
- **End IP Address**: Enter a value for the DHCP server to end with when issuing IP addresses. The End IP Address must be smaller than 192.168.1.254. The default End IP Address is 192.168.1.254.

- **Leased Time**: The leased time is the amount of time in which a network user will be allowed connection to the modem router with their current dynamic IP address. Enter the amount of time in hours, then the user will be leased this dynamic IP address. After the dynamic IP address has expired, the user will be automatically assigned a new dynamic IP address. The default is 1440 minutes.

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

### 4.4.5 IPv6 LAN Settings

Go to **Network → IPv6 LAN Settings**, you can configure LAN IPv6 interface for your modem router.

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

1) If RADVD is selected, it doesn’t need to be configured.
2) If DHCPv6 Server is selected, please complete the following parameters.

- **Start IPv6 Address**: Enter a value for the DHCPv6 server to start with when issuing IPv6 addresses.
• **End IPv6 Address:** Enter a value for the DHCPv6 server to end with when issuing IPv6 addresses.

• **Leased Time:** The leased time is the amount of time in which a network user will be allowed connection to the modem router with their current dynamic IPv6 address. Enter the amount of time, in hours, then the user will be leased this dynamic IPv6 address. After the dynamic IPv6 address has expired, the user will be automatically assigned a new dynamic IPv6 address. The default is 86400 seconds.

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

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

   ![Site Prefix Configuration Type: Delegated or Static](image)

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

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

   ![Site Prefix Configuration Type: Delegated or Static](image)

• **Site Prefix:** Enter a value for the site prefix.

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

Click **Save** to make the settings effective.

### 4.4.6 MAC Clone

Go to **Network → MAC Clone**, you can configure the MAC address of the WAN interface as shown below.

The WAN Interface List displays the WAN interfaces you have configured on section **4.4.1 WAN Settings** and its default MAC address. You can select the corresponding WAN interface from the drop-down list and click **Clone MAC To** to clone your current PC MAC, and then click **Save**.

![MAC Clone](image)

**Note:**

1. MAC clone may cause reconnection.
2. If MAC Clone has been performed, any bridge connections sharing the same VPI/VCI configurations with other connections may not work.
Note:

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

4.4.7 ALG Settings

Go to Network → ALG Settings, and then you can configure the basic security in the screen as shown below.

<table>
<thead>
<tr>
<th>ALG Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Private Network (VPN):</td>
</tr>
<tr>
<td>PPTP Pass-through: ○ Enable ○ Disable</td>
</tr>
<tr>
<td>L2TP Pass-through: ○ Enable ○ Disable</td>
</tr>
<tr>
<td>IPSec Pass-through: ○ Enable ○ Disable</td>
</tr>
<tr>
<td>Application Layer Gateway (ALG):</td>
</tr>
<tr>
<td>FTP ALG: ○ Enable ○ Disable</td>
</tr>
<tr>
<td>TFTP ALG: ○ Enable ○ Disable</td>
</tr>
<tr>
<td>H323 ALG: ○ Enable ○ Disable</td>
</tr>
<tr>
<td>SIP ALG: ○ Enable ○ Disable</td>
</tr>
</tbody>
</table>

- **Virtual Private Network (VPN):** VPN Passthrough must be enabled if you want to allow VPN tunnels using VPN protocols to pass through the modem 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 modem 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 modem 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 modem router, click Enable.

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

Click **Save** to make the settings effective.

### 4.4.8 DSL Settings

Go to **Network → DSL Settings**, you can select the DSL Modulation Type and Annex Type in the next screen. The DSL feature can be selected when you meet the physical connection problem. Please check the proper settings with your Internet service provider.

![DSL Settings](image)

- **DSL Modulation Type**: Select the DSL operation modulation type which your DSL connection uses.
- **Annex Type**: Select the DSL operation annex type which your DSL connection uses.

Click **Save** to make the settings effective.

### 4.4.9 IPSec VPN

Go to **Network → IPSec VPN**, you can Add/Remove or Enable/Disable the IPSec tunnel connections on the screen as shown.

![IPSec Tunnel Mode Connections](image)

This section will guide you to configure a VPN tunnel between two modem routers. The topology is as follows.
**Note:**

You could also use other VPN Routers to set VPN tunnels with the modem router. It supports up to 10 VPN tunnels simultaneously.
Click **Add New Connection** and then you will enter the screen shown below.

### IPSec Settings

<table>
<thead>
<tr>
<th>IPSec Connection Name:</th>
<th>Enter a name for your VPN.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote IPSec Gateway Address (URL):</td>
<td>Enter the destination gateway IP address in the box which is the public WAN IP or domain name of the remote VPN server endpoint. (For example: Input 219.134.112.247 in Device1, Input 219.134.112.246 in Device2)</td>
</tr>
<tr>
<td>Tunnel access from local IP addresses:</td>
<td>Choose <strong>Subnet</strong> if you want the whole LAN to join the VPN network, or else choose <strong>Single Address</strong> if you want a single IP to join the VPN network.</td>
</tr>
<tr>
<td>IP Address for VPN:</td>
<td>Enter the IP address of your LAN. (For example: Input 192.168.1.1 in Device1, Input 192.168.2.1 in Device2)</td>
</tr>
<tr>
<td>IP Subnetmask:</td>
<td>Enter the Subnet mask of your LAN. (For example: Input 255.255.255.0 in both Device1 and Device2)</td>
</tr>
<tr>
<td>Tunnel access from remote IP addresses:</td>
<td>Choose Subnet if you want the Remote Whole LAN to join the VPN network, or else choose Single Address if you want single IP to join the VPN network.</td>
</tr>
<tr>
<td>IP Address for VPN:</td>
<td>Enter the IP address of the Remote LAN. (For example: Input 192.168.2.1 in Device1, Input 192.168.1.1 in Device2)</td>
</tr>
<tr>
<td>IP Subnetmask:</td>
<td>Enter the subnetmask of the remote LAN. (For example: Input 255.255.255.0 in both Device1 and Device2)</td>
</tr>
<tr>
<td>Key Exchange Method:</td>
<td>Select <strong>Auto (IKE)</strong> or <strong>Manual</strong>.</td>
</tr>
</tbody>
</table>

If you select Auto as **Key Exchange Method**, the screen will display as follows:
Authentication Method: Select Pre-Shared Key (recommended).

Pre-Shared Key: Enter the Pre-shared Key for IKE authentication, and ensure both the two peers use the same key. The key should consist of visible characters without blank space.

Perfect Forward Secrecy: PFS is an additional security protocol.

We recommend you leave the Advanced Settings as default value.

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

Note:
The VPN Servers Endpoint from both ends must use the same pre-shared keys and Perfect Forward Secrecy settings.
Click **Show Advanced Settings** and then you can configure the Advanced Settings.

![Configuration Settings](image)

### Settings for Phase 1:

- **Mode**: You can select **Main** or **Aggressive**. Select **Main** to configure the standard negotiation parameters for IKE phase 1. Select **Aggressive** to configure IKE phase 1 of the VPN Tunnel to carry out negotiation in a shorter amount of time. (Not Recommended - Less Secure)

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

- **My Identifier Type** - Select the local ID type for IKE negotiation. **Local Wan IP**: use an IP address as the ID in IKE negotiation. **FQDN**: use a name as the ID.

- **My Identifier** - This field does not need to enter if **Local WAN IP** is selected in **My Identifier Type** field. And the WAN IP will be used automatically as Identifier. If Name type is selected, enter a name for the local device as the ID in IKE negotiation.

- **Remote Identifier Type** - The remote gateway IP will be entered automatically if IP Address type is selected. If Name type is selected, enter the name of the remote peer as the ID in IKE negotiation.
Remote Identifier - This field does not need to enter if Remote WAN IP is selected in Remote Identifier Type field. And the remote gateway IP will be used automatically as Identifier. If Name type is selected, enter the name of the remote peer as the ID in IKE negotiation.

Encryption Algorithm - Specify the encryption algorithm for IKE negotiation. Options include: DES, 3DES, AES-128, AES-192, AES-256.

Integrity Algorithm - Select the authentication algorithm for IKE negotiation. Options include: MD5 and SHA1.

Select Diffie-Hellman Group for Key Exchange - Select the DH (Diffie-Hellman) group to be used in key negotiation phase 1. The DH Group sets the strength of the algorithm in bits.

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

Settings for Phase 2:

Encryption Algorithm - Specify the encryption algorithm for IKE negotiation. Options include: DES, 3DES, AES-128, AES-192, AES-256.

Integrity Algorithm - Select the authentication algorithm for IKE negotiation. Options include: MD5 and SHA1.

Diffie-Hellman Group for Key Exchange - Select the DH (Diffie-Hellman) group to be used in key negotiation phase 1. The DH Group sets the strength of the algorithm in bits.

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

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

If you select Manual as Key Exchange Method, the screen will display as follows:

- Encryption Algorithm - Specify the encryption algorithm. Options include: DES, 3DES, AES (aes-cbc).
- Encryption Key - Place the mouse in this field about 2s, the requirements of the Encryption Key will be displayed automatically. Enter the Encryption Key, and ensure both the two peers use the same key.
**Authentication Algorithm** - Select the authentication algorithm. Options include: MD5 and SHA1.

**Authentication Key** - Place the mouse in this field about 2s, the requirements of the Authentication Key will be displayed automatically. Then enter the authentication Key.

**SPI** - Specify the SPI (Security Parameter Index) manually. The SPI here must match the SPI value at the other end of the tunnel, and vice versa.

### 4.5 IPTV

Choose **IPTV**, and you will see the screen as shown as blow.

![IPTV Settings](image)

- **Enable IPTV**: Check the box to enable IPTV function.
- **Enable a wireless connection for IPTV**: If enabled, the set-top box can connect wirelessly to the modem router. To use this function, follow the steps below:
  1. Select **Enable IPTV**.
  2. Select **Enable a wireless connection for IPTV**.
  3. Enable SSID2 or SSID3 for IPTV connection and click **Save**. You may rename the SSID.
4. Select your desired wireless network for IPTV connection.

**Note:** When the WLAN port is set for an IPTV connection, the wireless functionality is only available for that IPTV connection.

- **TP-LINK_50F2_01**
- **TP-LINK_50F2_02**

➢ **DSL Modulation Type:** The modem router supports two modulation types: ADSL and VDSL, you can select the corresponding types according to your needs.

If you choose **ADSL**, you will see the screen as shown in the following figure:

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

If you choose **VDSL**, you will see the screen as shown in the following figure:

- **VLAN:** Check the box to enable the Virtual LAN ID.
- **VLAN ID (1~4049):** This indicates the VLAN group, and the valid range is from 1 to 4049.

Click **Save** to make the settings effective.
4.6 DHCP Server

Choose DHCP Server, you can see the next submenus. Click any of them, and you will be able to configure the corresponding function.

4.6.1 DHCP Settings

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

- **Start IP Address**: Enter a value for the DHCP server to start with when issuing IP addresses. The default Start IP Address is 192.168.1.100.
- **End IP Address**: Enter a value for the DHCP server to end with when issuing IP addresses. The default End IP Address is 192.168.1.199.
- **Lease Time**: The Leased Time is the amount of time in which a network user will be allowed connection to the modem router with their current dynamic IP address. Enter the amount of time, in hours, then the user will be "leased" this dynamic IP address. After the dynamic IP address has expired, the user will be automatically assigned a new dynamic IP address. The default is 1440 minutes.
- **Default Gateway**: (Optional.) It is suggested to input the IP address of the LAN port of the modem router. The default value is 192.168.1.1.
- **Default Domain**: (Optional.) Input the domain name of your network.
- **Primary DNS**: (Optional.) Input the DNS IP address provided by your ISP or consult your ISP.
- **Secondary DNS**: (Optional.) Input the IP address of another DNS server if your ISP provides two DNS servers.
- **DHCP Relay**: Select DHCP Relay, then you will see the next screen, and the modem router will work as a DHCP Relay. A DHCP relay is a computer that forwards DHCP data between
computers that request IP addresses and the DHCP server that assigns the addresses. Each of the device's interfaces can be configured as a DHCP relay. If it is enabled, the DHCP requests from local PCs will forward to the DHCP server runs on WAN side. To have this function working properly, please run on router mode only, disable the DHCP server on the LAN port, and make sure the routing table has the correct routing entry.

**Note:**

1) To use the DHCP server function of the modem router, you must configure all computers on the LAN as Obtain an IP Address automatically.

2) You have to disable NAT of the WAN connections, or the DHCP Relay may not take effect.

3) If you select Disabled, the DHCP function will not take effect.

Click **Save** to make the settings effective.

### 4.6.2 Clients List

Go to **DHCP Server → Clients List**, you can view the information about the clients attached to the modem router in the screen as shown below.

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

To update this page and to show the current wireless devices, click **Refresh**.

### 4.6.3 Address Reservation

Go to **DHCP Server → Address Reservation**, you can view and add a reserved address for clients via the next screen. 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 an IP address.
➢ **IP Address**: The IP address reserved for the PC by the modem router.
➢ **Status**: The status of this entry either **Enabled** or **Disabled**.

**To Reserve an IP address:**

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

**To modify or delete an existing entry:**

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

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

Click **Delete Selected** to selected entries.

**4.6.4 Conditional Pool**

Go to **DHCP Server → Conditional Pool**, you can see the next screen. This page displays vendor class settings and allows you to set parameters for vendor class by clicking corresponding buttons.
To add a vendor class:
1. Click Add New.
2. Enter parameters for the vendor class.
   Click Save.

To modify or delete an existing entry:
1. Click Edit in the entry you want to modify. If you want to delete the entry, click the Delete.
2. Modify the information.
3. Click Save.
   Click Enable Selected / Disable Selected to make selected entries enabled/disabled.

Click Delete Selected to select entries.
4.7 Wireless

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

4.7.1 Basic Settings

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

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

- **Mode**: Select the desired mode.
  - **11b only**: Select if all of your wireless clients are 802.11b.
  - **11g only**: Select if all of your wireless clients are 802.11g.
  - **11n only**: Select only if all of your wireless clients are 802.11n.
  - **11bg mixed**: Select if you are using both 802.11b and 802.11g wireless clients.
  - **11bgn mixed**: Select if you are using a mix of 802.11b, 11g, and 11n wireless clients.
Select the desired wireless mode. When 802.11g mode is selected, only 802.11g wireless stations can be connected to the modem router. When 802.11n mode is selected, only 802.11n wireless stations can connect to the modem router. It is strongly recommended that you set the Mode to 802.11b&g&n, and all of 802.11b, 802.11g, and 802.11n wireless stations can connect to the modem router.

- **Channel:** Select the channel you want to use from the drop-down List of Channel. This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.

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

**Note:**

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

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

- **Enable WDS:** Check this box to enable WDS. With this function, the modem router can bridge two or more Wlans. If this checkbox is selected, you will have to set the following parameters as shown in the figure below. Make sure the following settings are correct.

- **SSID (to be bridged):** The SSID of the AP your modem router is going to connect to as a client. You can also use the search function to select the SSID to join.

- **BSSID (to be bridged):** The BSSID of the AP your modem router is going to connect to as a client. You can also use the search function to select the BSSID to join.

- **Scan:** Click to search the AP which runs in the current channel.

- **Key type:** This option should be chosen according to the AP’s security configuration. It is recommended that the security type is the same as your AP’s security type.

- **WEP Index:** This option should be chosen if the key type is WEP(ASCII) or WEP(HEX). It indicates the index of the WEP key.

- **Authentication Type:** This option should be chosen if the key type is WEP(ASCII) or WEP(HEX). It indicates the authorization type of the Root AP.
**Password**: If the AP your modem router is going to connect needs password, you need to fill the password in this blank. Click **Save** to make the settings effective.

### 4.7.2 WPS Settings

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

a). Choose **WPS Settings**, and you will see the next screen shown below.

![WPS Settings](image)

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

b). To add a new device:

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

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

I. **Use PBC (Push Button Configuration) method**

Use this method if your client device has a WPS button.

**Step 1**: Press the WPS/RESET button and hold on 1 second on the back panel of the modem router, as shown in the following figure.
You can also keep the default WPS Status as Enabled and click Add device. Then choose Press the button of the new device in two minutes and click Connect.

Step 2: Press and hold the WPS button of the client device directly.
Step 3: The WPS LED flashes for two minutes during the WPS process.
Step 4: When the WPS LED is on, the client device has successfully connected to the modem router.

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

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

Use this method if your client device has a WPS PIN number.

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

Step 2: Enter the PIN number from the client device in the field on the above WPS screen. Then click Connect button.
Step 3: Connect successfully will appear on the screen, which means the client device has successfully connected to the modem router.

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

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

Step 1: On the client device, enter the PIN number listed on the modem router’s WPS screen. (It is also labeled on the bottom of the modem router.)
Step 2: The WPS LED flashes for two minutes during the WPS process.
Step 3: When the WPS LED is on, the client device has successfully connected to the modem router.
Step 4: Refer back to your client device or its documentation for further instructions.

Note:

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

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

4.7.3 Wireless Security

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

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

- **Disable Wireless Security**: If you do not want to use wireless security, check this radio button. But it’s strongly recommended to choose one of the following modes to enable security.

- **WPA/WPA2-Personal**: It’s the WPA/WPA2 authentication type based on pre-shared passphrase. The modem router is configured by this security type by default.
  
  - **Authentication Type**: You can choose the type for the WPA/WPA2-Personal security on the drop-down list. The default setting is **Auto**, which can select **WPA-PSK** or **WPA2-PSK** authentication type automatically based on the wireless station's capability and request.
  
  - **Encryption**: You can select **Auto**, **TKIP** or **AES** as Encryption.
- **Wireless Password**: You can enter ASCII characters between 8 and 63 characters or 8 to 64 Hexadecimal characters. The default password is the same with the default PIN code, which is labeled on the bottom of the router or can be found in Figure 4-43.

- **Group Key Update Period**: Specify the group key update interval in seconds. The value should be 30 or above. Enter 0 to disable the update.

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

  ![WPA/WPA2 - Enterprise](image)

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

- **Encryption**: You can select Auto, TKIP or AES as Encryption.

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

- **RADIUS Server Port**: Enter the port that radius service used.

- **RADIUS Server Password**: Enter the password for the Radius Server.

- **Group Key Update Period**: Specify the group key update interval in seconds. The value should be 30 or above. Enter 0 to disable the update.

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

  ![WEP](image)

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

- **WEP Key Format**: Hexadecimal and ASCII formats are provided here. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length. ASCII format stands for any combination of keyboard characters in the specified length.

- **WEP Key**: Select which of the four keys will be used and enter the matching WEP key that you create. Make sure these values are identical on all wireless stations in your network.

- **Key Type**: You can select the WEP key length (64-bit, or 128-bit.) for encryption. "Disabled" means this WEP key entry is invalid.
64-bit: You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not promoted) or 5 ASCII characters.

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

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

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

4.7.4 Wireless Schedule

Go to Wireless → Wireless Schedule, you can configure the Task Schedule as shown below.

Note:
Click the schedule table or use the Add button to choose the period you need the wireless off. Before configure the wireless schedule, please set system time first which refer to 4.21.2 Time Settings, then you can enable or disable Wireless Schedule.

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

Click Clear Schedule to clear your settings in the table.

Click Save to complete the settings.
4.7.5 Wireless MAC Filtering

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

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

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

To Add a Wireless MAC Address filtering entry, click the Add New button. The following page will appear:

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

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

To edit or delete an existing entry:

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

Click Enable/ Disabled Selected to make selected entries enabled or disabled.
Click **Delete Selected** to delete selected entries.

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

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

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

![Filtering Rules Table](image)

**4.7.6 Wireless Advanced**

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

![Wireless LAN Advanced Settings](image)

*Note: Fragmentation is not allowed with HT mode.*
Transmit Power: Here you can specify the transmit power of modem router. You can select High, Middle or Low which you would like. High is the default setting and is recommended.

Beacon Interval: Enter a value between 25-1000 milliseconds for Beacon Interval here. The beacons are the packets sent by the modem router to synchronize a wireless network. Beacon Interval value determines the time interval of the beacons. The default value is 100.

RTS Threshold: Here you can specify the RTS (Request to Send) Threshold. If the packet is larger than the specified RTS Threshold size, the modem router will send RTS frames to a particular receiving station and negotiate the sending of a data frame. The default value is 2346.

Fragmentation Threshold: This value is the maximum size determining whether packets will be fragmented. Setting the Fragmentation Threshold too low may result in poor network performance because of excessive packets. 2346 is the default setting and is recommended.

DTIM Interval: This value determines the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the modem router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. You can specify the value between 1-255 Beacon Intervals. The default value is 1, which indicates the DTIM Interval is the same as Beacon Interval.

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

Enabled Client isolation: This function can isolate wireless stations on your network from each other. Wireless devices will be able to communicate with the modem router but not with each other. To use this function, check this box. Client isolation is disabled by default.

Enable WMM: WMM function can guarantee the packets with high-priority messages being transmitted preferentially. It is strongly recommended.

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.

4.7.7 Wireless Status

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

<table>
<thead>
<tr>
<th>Wireless Stations Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>This page displays the basic information of all stations connected to the wireless network.</td>
</tr>
<tr>
<td>Wireless Stations Currently Connected: 0</td>
</tr>
</tbody>
</table>

- **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
To update this page and to show the current connected wireless stations, click Refresh.

4.8 Guest Network

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

4.8.1 Basic Settings

Go to Guest Network → Basic Settings, and you will see the screen as shown below. This feature allows you to create a separate network for your guests without allowing them to access your main network and the computers connected to it.

- **Guest Network**: You can choose your guest network. When you enable this function, you could set wireless parameters for guest network.
- **SSID**: The guest network name. When setting up a guest network, it is strongly recommended to use a name that easily distinguishes it from your primary network. The default SSID is set to be TP-LINK_Guest.
- **Security**: The default value is disabled, but it’s strongly recommended to enable WPA/WPA2-Personal. WPA/WPA2-Personal is the WPA/WPA2 authentication type based on pre-shared passphrase.
- **Authentication Type**: Select the Authentication Type from the drop-down list, the default method is Auto, and you can leave it as a default setting.
- **Encryption**: You can select either Auto, or TKIP or AES.
- **Wireless Password**: You can enter ASCII characters between 8 and 63 characters or 8 to 64 Hexadecimal characters.
- **Group Key Update Period**: Specify the group key update interval in seconds. The value
should be 30 or above. Enter 0 to disable the update.

- **Allow Guests to access my Local Network**: The guests have access to your Local Network, but cannot login the modem router's Web-Management page.
- **Allow Guests to access my USB Storage Sharing**: The guests can access the specified files on the USB storage device via the function of USB Storage Sharing, but the function of FTP Server, Media Server and Print Server are not available in Guest Network. For more details please refer to 4.9.3 Storage Sharing.
- **Guest Network Isolation**: This function can isolate wireless clients on your guest network from each other. Client isolation is disabled by default.
- **Guest Network Bandwidth Control**: With this function, you can configure the Upstream Bandwidth and Downstream Bandwidth for guest network.

Click **Save** to make the settings effective.

### 4.8.2 Guest Network Status

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

<table>
<thead>
<tr>
<th>Guest Network Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Currently Connected Guest Network Clients: 0</td>
</tr>
</tbody>
</table>

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

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

### 4.9 USB Settings

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

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

<table>
<thead>
<tr>
<th>Disk1: Kingston (DataTraveler G2) 1.00</th>
<th>Connected: Disconnect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume: sda1</td>
<td>File System: NTFS</td>
</tr>
</tbody>
</table>

- **Volume**: The volume name of the USB drive the users have access to.
- **File System**: The system of the USB drive.
- **Capacity**: The storage capacity of the USB driver.
- **Status**: Indicates the shared or non-shared status of the volume. **Active** means volume can be shared, while **Standby** means volume cannot be shared. If **Deactivate** in Action field is clicked, **Inactive** will be displayed in the Status field, which means volume cannot be shared.
- **Action**: When the volume is shared, you can click the **Deactivate** to stop sharing the volume; when volume is non-shared, you can click **Activate** to share the volume.

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

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

4.9.2 User Accounts

You can specify the username and password for Storage Sharing and FTP Server users on this page. Storage Sharing users can access the folders by entering the following URL into the address field of your browser or Windows Explorer, such as \192.168.1.1. FTP Server users can log into the FTP Server via FTP Client.
There are five users here, which provide means to control the access to the USB mass storage by Storage Sharing or FTP. The Super User has the right to read and write to Storage Sharing and FTP Server.

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

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

**4.9.3 Storage Sharing**

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

Storage Sharing enables you to share files saved on a USB storage device with other computers on the local network.

Server Status: Indicates the Storage Sharing’s current status.

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

For Windows OS:
Open the "Run" window within the Start menu and enter \( \text{IP Address} \) or \( \text{(IP Address)} \) (Share Name)
e.g. 192.168.1.1 or 192.168.1.1\text{\_share}.

For Mac OS:
Open the "Connect to Server" window within the Go menu and enter smb://\( \text{(IP Address)} \) or smb://\( \text{(IP Address)} \) (Share Name),
e.g. smb://192.168.1.1 or smb://192.168.1.1\text{\_share}.

Folder Table: (Any modifications to this table will not take effect until you Apply these changes)

- **Share Name**: This folder's display name.
- **Directory**: The real full path of the specified folder.
- **User Access**: The authorization of the user is displayed.
  - Users mean Super Users who have the full-access permission to all activated volumes and share folders. Grey users mean the users who have no right to use this function. Others are common users.
- **Status**: The status of the entry is enabled or disabled.
- **Edit**: Click Edit in the table, and then you can modify the entry.
To add a new folder, follow the instructions below.

1. Click **Add New Folder**.

2. Click **Browse**, and then select the **Select Volume** from the drop-down list.

3. Enter display name of the share folder in **Share Name** filed.

4. Click **Apply** to apply the settings.

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

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

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

**Note:**

1. The max share folders number is 10. If you want to share a new folder when the number has reached 10, you can delete an existing share folder and then add a new one.

2. If you want to change the Storage Sharing settings, you can click **Apply** to make the changes take effect.
4.9.4 FTP Server

Go to USB Settings → FTP Server, you can create an FTP server that can be accessed from the Internet or your local network.

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

To add a new folder, follow the instructions below.

1. Click Add New Folder.
2. Click **Browse**, and then select the **Select Volume** from the drop-down list.

3. Enter display name of the share folder in **Share Name** field.

4. Click **Apply** to apply the settings.

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

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

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

**Note:**

1. The max share folders number is 10. If you want to share a new folder when the number has reached 10, you can delete an existing share folder and then add a new one.

2. If you want to change the FTP settings, you can click **Apply** to make the changes take effect.

### 4.9.5 Media Server

Go to **USB Settings → Media Server**, you can create media server that allows you to share stored content with other computers and devices on your home network and on the Internet.
To add a new share folder for your media server, please follow the instructions below:

a) Click Add New Folder, and you will see the screen as shown below.

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

c) Click Apply to apply the configuration.

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

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

4.9.6 Print Server

Go to USB Settings → Print Server, you can configure print server on this page as shown below.

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

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

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

4.10.1 Default Gateway

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

![Default Gateway Settings](image)

Click Add Interface, you can add WAN Interfaces. Click Save to make the settings effective.

4.10.2 Static Route

Go to Route Settings → Static Route. You can see the Static Route screen, this screen allows you to configure the static routes. A static route is a pre-determined path that network information must travel to reach a specific host or network.

![Static Route](image)

To add static routing entries:

1. Click Add New, and you will see the screen as shown below.
2. Enter the following data:

- **Destination IP Address**: The Destination IP Address 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**: Here you should type the gateway address correctly, and the option for Interface will adopt the default gateway address for the Static Route.

- **Interface**: Select the interface name in the text box, or else, the default interface will be adopted for the Static Route.

- **Status**: Select Enabled or Disabled from the drop-down list.

3. Click Save to make the settings effective.

To modify or delete an existing entry:

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

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

Click Delete Selected to delete selected entries.

### 4.10.3 RIP Settings

Go to Route Settings → RIP Settings, you can see the RIP (Routing Information Protocol) screen which allows you to configure the RIP.
Note:
RIP cannot be configured on the WAN Interface which has NAT enabled (such as PPPoE).

4.11 IPv6 Route Settings

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

4.11.1 IPv6 Default Gateway

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

Click Add Interface, you can add WAN Interfaces.
Click Save to make the settings effective.

4.11.2 IPv6 Static Route

Go to IPv6 Route Settings → IPv6 Static Route. You can see the IPv6 Static Route screen. This screen allows you to configure the IPv6 static routes. An IPv6 static route is a pre-determined path that network information must travel to reach a specific host or network.

To add a new entry, follow the instructions below.
1. Click Add New, and you will see the screen as shown below.
2. Enter the following data:

- **Destination IPv6 Address**: The IPv6 address of the network or host that you want to assign to a static route.
- **Prefix Length**: The prefix length of the destination IPv6 address.
- **Gateway**: Type in the correct IPv6 Gateway address for the IPv6 Static Route.
- **Interface**: Select the Interface from the drop-down list.
- **Status**: Select Enabled or Disabled from the drop-down list.

3. Click **Save** to make the settings effective.

**To modify or delete an existing entry:**

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

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

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

### 4.12 Forwarding

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

#### 4.12.1 Virtual Server

Go to **Forwarding → Virtual Server**, and then you can view and add virtual servers in the next screen. 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 the Start port and YYY is the End port).
- **IP Address**: The IP address of the PC running the service application.
- **Internal Port**: The Internal Service Port number of the PC running the service application. You can leave it blank if the **Internal Port** is the same as the **Service Port**, or enter a specific port number when the **Service Port** is a single one.
- **Protocol**: The protocol used for this application, either TCP, UDP, or All (all protocols supported by the modem router).
- **Status**: The status of this entry, **Enabled** means the virtual server entry is enabled.
- **WAN**: The WAN service interface providing the service application.
- **Edit**: To modify or delete an existing entry.

**To set up a virtual server entry:**

1. Click **Add New**.
2. Select the service you want to use from the **Common Service Port** list. If the **Common Service Port** menu does not list the service that you want to use, enter the number of the service port or service port range in the **Service Port** field.
3. Enter the IP address of the computer running the service application in the **IP Address** field.
4. Select the protocol used for this application in the **Protocol** drop-down list, either TCP, UDP, or All.
5. Select **Enabled** option in the **Status** drop-down list.
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 or delete an existing entry:
1. Find the desired entry in the table.
2. Click Edit as desired on the Edit column.
Click Enable/ Disabled Selected to make selected entries enabled/ disabled.
Click Delete Selected to delete selected entries.

Note:
If you set the service port of the virtual server as 80, you must set the Web management port on System Tools → Manage Control page to be any other value except 80 such as 8080. Otherwise there will be a conflict to disable the virtual server.

4.12.2 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 modem router.

To add a new rule, follow the steps below.
1. Click Add New, the next screen will pop-up as shown below.
2. Select a common application from the Common Service Port drop-down list, then the Trigger Port field and the Open Ports field will be automatically filled. If the Common Service Port does not have the application you need, enter the Trigger Port and the Open Ports manually.
3. Select the protocol used for Trigger Port from the Trigger Protocol drop-down list, either TCP, UDP, or All.
4. Select the protocol used for Incoming Ports from the Open Protocol drop-down list, either TCP or UDP, or All.

5. Select Enable in Status field.

6. Click Save to save the new rule.

---

**Port Trigger**

Various applications require multiple connections, for example online games, video conferencing, VoIP, etc. Due to the internal firewall, these applications will not run effectively with a pure NAT router. In these cases, Port Triggering may provide a solution in improving the performance of these particular applications. Note: Port Triggering is only supported when there is an available interface.

![Port Trigger Interface](image)

- **Interface:** Display the default gateway you have set.
- **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 modem router).
- **Open Port:** The port or port range used by the remote system when it responds to the outgoing request. A response using one of these ports will be forwarded to the PC which triggered this rule. You can input at most 5 groups of ports (or port sections). Every group of ports must be separated with "\," for example, 2000-2038, 2046, 2050-2051, 2085, 3010-3030.
- **Open Protocol:** The protocol used for Incoming Port, either TCP, UDP, or ALL (all protocols supported by the modem router).
- **Status:** The status of this entry, Enabled means the Port Triggering entry is enabled.
- **Common Service Port:** Some popular applications already listed in the drop-down list of Open Protocol.

**To modify or delete an existing entry:**

1. Find the desired entry in the table.
2. Click Edit as desired on the Edit column.
   - Click Enable/Disabled Selected to make selected entries enabled/disabled.
   - Click Delete Selected to delete selected entries.

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

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

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

4.12.3 DMZ

Go to Forwarding → DMZ, and then 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 videoconferencing. The modem router forwards packets of all services to the DMZ host. Any PC whose port is being forwarded must have its DHCP client function disabled and should have a new static IP Address assigned to it because its IP Address may be changed when using the DHCP function.

To assign a computer or server to be a DMZ server:
1. Click Enable.
2. Enter the IP address of a local PC that is set to be DMZ host in the DMZ Host IP Address field.
3. Click Save.

4.12.4 UPnP

Go to Forwarding → UPnP, and then you can view the information about UPnP in the screen. The Universal Plug and Play (UPnP) feature allows the devices, such as Internet computers, to access the local host resources or devices as needed. UPnP devices can be automatically discovered by the UPnP service application on the LAN.
Current UPnP Status: UPnP can be enabled or disabled by clicking **Enable** or **Disable**. This feature is enabled by default.

Current UPnP Settings List: This table displays the current UPnP information.

- **App Description**: The description about the application which initiates the UPnP request.
- **External Port**: The port which the modem router opens for the application.
- **Protocol**: The type of protocol which is opened.
- **Internal Port**: The port which the modem router opened for local host.
- **IP Address**: The IP address of the local host which initiates the UPnP request.
- **Status**: Either Enabled or Disabled. **Enabled** means that the port is still active; otherwise, the port is inactive.

Click **Enable** to enable UPnP.

Click **Disable** to disable UPnP.

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

### 4.13 Parental Control

Choose **Parental Control**, and you can configure the parental control in the screen as shown below. 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.
- **Enable Parental Control**: Check the box if you want this function to take effect. This function is disabled by default.

- **MAC Address of Parental PC**: In this field, enter the MAC address of the controlling PC, or you can make use of the Copy To… below.

- **MAC Address of Current PC**: This field displays the MAC address of the PC that is managing this modem router. If the MAC Address of your adapter is registered, you can click Copy To Above to fill this address to the MAC Address of Parental PC field above.

- **Add URL**: Here you can input the net addresses which the child is allowed to access. Click Save to make the settings effective.

### 4.14 Firewall

**Firewall**

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

4.14.1 Rule

Go to Firewall → Rule, and then you can view and set Access Control rules in the screen as shown below.

- **Enable Firewall**: Select the check box to enable the Firewall function, so the Default Filtering Rules can take effect.
- **Description**: Here displays the description of the rule and this name is unique.
- **LAN Host**: Here displays the host selected in the corresponding rule.
- **WAN Host**: Here displays the WAN host selected in the corresponding rule.
- **Schedule**: Here displays the schedule selected in the corresponding rule.
- **Status**: Here displays the status of the rule, enabled or not.
- **Edit**: Here you can edit or delete an existing rule.
- **Add New**: Click to add a new rule entry.
- **Enable Selected**: Click to enable the selected rules in the list.
- **Disable Selected**: Click to disable the selected rules in the list.
- **Delete Selected**: Click to delete the selected entries in the table.

**The methods to add a new rule:**
1. Click **Add New** and the next screen will pop up as shown below.
2. Give a name (e.g. Rule_1) for the rule in the **Description** field.
3. Select a host from the **LAN Host** drop-down list or choose **Add LAN Host**.
4. Select a target from the **WAN Host** drop-down list or choose **Add WAN Host**.
5. Select a schedule from the **Schedule** drop-down list or choose **Add Schedule**.
6. In the **Action** field, select **Deny** or **Allow** to deny or allow your entry.
7. In the **Status** field, select **Enabled** or **Disabled** to enable or disable your entry.

8. In the **Direction** field, select **IN** or **OUT** from the drop-down list for the direction.

9. In the **Protocol** field, here are four options, All, TCP, UDP, and ICMP. Select one of them from the drop-down list for the target.

10. Click **Save**.

4.14.2 LAN Host

Go to **Firewall → LAN Host**, and then you can view and set a Host list in the screen as shown below.

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

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

1. Click **Add New**.

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

4.14.3 WAN Host

Go to Firewall → WAN Host, and then you can view and set a Host list in the screen as shown below.

<table>
<thead>
<tr>
<th>Description</th>
<th>Details</th>
<th>Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host_1</td>
<td>202.143.71.2</td>
<td>Edit</td>
</tr>
</tbody>
</table>

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

**To add a new entry, please follow the steps below.**
1. Click Add New.
2. In Mode field, select IP Address, MAC Address or URL Address.

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

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

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

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

If you select **URL Address**, you will see the screen shown as below.

![WAN Host](image)

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

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

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

### 4.14.4 Schedule

Go to **Firewall → Schedule**, and then you can view and set a Schedule list in the next screen as shown below.

![Task Schedule](image)

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

**To add a new schedule, follow the steps below:**

1. Click **Add New**.

2. In **Description** field, create a unique description for the schedule (e.g. Schedule_1).

3. In **Apply To** field, select the day or days you need.

4. In **time** field, you can select all day-24 hours or you may enter the **Start Time** and **Stop Time** in the corresponding field.

5. Click **Save** to complete the settings.

Click **Clear Schedule** to clear your settings in the table.
Click **Delete Selected** to delete the selected entries in the table.

### 4.15 IPv6 Firewall

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

#### 4.15.1 IPv6 Rule

Go to **IPv6 Firewall → IPv6 Rule**, and then you can view and set Access Control rules in the screen as shown below.
Enable IPv6 Firewall: Select the check box to enable the IPv6 Firewall function, so the Default Filtering Rules can take effect.

Description: Here displays the description of the IPv6 rule and this name is unique.

IPv6 LAN Host: Here displays the LAN host selected in the corresponding rule.

IPv6 WAN Host: Here displays the WAN host selected in the corresponding rule.

Schedule: Here displays the schedule selected in the corresponding rule.

Status: Here displays the status of the rule either enabled or disabled.

Edit: Here you can edit or delete an existing rule.

To add a new IPv6 rule:

1. Click Add New, and you will see the screen as shown below.

2. Give a name (e.g. Rule_1) for the rule in the Description field.

3. Select a host from the IPv6 LAN Host drop-down list or choose Add IPv6 LAN Host.

4. Select a target from the IPv6 WAN Host drop-down list or choose Add IPv6 WAN Host.

5. Select a schedule from the IPv6 Schedule drop-down list or choose Add IPv6 Schedule.

6. In the Action field, select Deny or Allow to deny or allow your entry.

7. In the Status field, select Enabled or Disabled to enable or disable your entry.

8. In the Direction field, select IN or OUT from the drop-down list for the direction.
9. In the Protocol field, here are four options, All, TCP, UDP, and ICMPv6. Select one of them from the drop-down list for the target.

10. Click Save to make the settings effective.

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

Click Delete Selected to delete selected entries.

4.15.2 IPv6 LAN Host

Go to IPv6 Firewall → IPv6 LAN Host, and then you can view and set a Host list in the screen as shown below.

- Description: Here displays the description of the host and this description is unique.
- IPv6 Address Info: Here displays the information about the host.
- Edit: To modify an existing entry.

To add a new entry, follow the steps below.

1. Click Add New, and you will see the screen as shown below.

2. Create a unique name for the host (e.g. Host_1) in the Description field.

3. Enter an IPv6 address in the IPv6 Address field.

4. Enter the prefix length of the IPv6 address in the Prefix Length field.

5. Click Save to make the settings effective.

Click Delete Selected to delete selected entries.

4.15.3 IPv6 WAN Host

Go to IPv6 Firewall → IPv6 WAN Host, and then you can view and set a Host list in the screen as shown below.
Description: Here displays the description about the WAN and this description is unique.

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

Edit: To modify an existing entry.

To add a new entry, follow the steps below:
1. Click Add New, and you will see the screen as shown below.

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

Click Delete Selected to delete selected entries.

4.15.4 IPv6 Schedule

Go to IPv6 Firewall → IPv6 Schedule, and then you can view and set a Schedule list in the next screen as shown below.

Description: Here displays the description of the schedule and this description is unique.

Edit: Here you can modify an existing schedule.

To add a new schedule, follow the steps below:
1. Click Add New and you will see the screen as shown below.
2. Create a unique description for the schedule (e.g. Schedule_1) in Description field.
3. Select the day or days you need in Apply To field.
4. In time field, you can select all day-24 hours or you may enter the Start Time and Stop Time in the corresponding field.
5. Click Save.

Click Clear Schedule to clear your settings in the table.

Click Delete Selected to delete selected entries.

### 4.16 IPv6 Tunnel

IPv6 tunnel is a kind of transition mechanism to enable IPv6-only hosts to reach IPv4 services and to allow isolated IPv6 hosts and networks to reach each other over IPv4-only infrastructure before IPv6 completely supplants IPv4. It is a temporary solution for networks that do not support native dual-stack, where both IPv6 and IPv4 run independently.

Choose IPv6 Tunnel, and you will see the screen as shown below.
- **Enable**: Check the box to enable IPv6 Tunnel function. It is disabled by default.

- **Mechanism**: Select a type for IPv6 tunnel from the drop-down list. DS-Lite, 6RD and 6to4 are supported.

1) **DS-Lite**

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

![IPv6 Tunnel DS-Lite](image1)

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

- **Configuration Type**: Select a configuration type for this tunnel. Auto means to obtain the Remote IPv6 Address automatically while Manual means you set it manually.

- **Remote IPv6 Address**: Enter the IPv6 address of the remote node.

   **Note:**

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

2) **6RD**

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

![IPv6 Tunnel 6RD](image2)
- **WAN Connection**: Select a WAN connection from the drop-down list. Only the connected WAN connections can be shown in the drop-down list.

- **Configuration Type**: Select a configuration type for this tunnel. Auto means to obtain the following parameters automatically while Manual means you set them manually. If Auto is selected, only Dynamic IP connection can be selected from the drop-down list.

- **IPv4 Mask Length**: The length of the selected WAN connection’s IPv4 mask.

- **6RD Prefix**: The prefix of the 6RD tunnel.

- **6RD Prefix Length**: The length of the 6RD prefix.

- **Border Relay IPv4 Address**: The IPv4 address of the border relay router of 6RD tunnel.

**Note:**

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

3) **6to4**

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

![IPv6 Tunnel](image)

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

**Note:**

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

### 4.17 Bandwidth Control

Choose Bandwidth Control, and then you can configure the Upstream Bandwidth and Downstream Bandwidth in the next screen. The values you configure should be less than 1000000Kbps. For optimal control of the bandwidth, please select the right Line Type and ask your ISP for the total bandwidth of the egress and ingress.
- **Enable Bandwidth Control:** Check this box so that the bandwidth control settings can take effect.

- **Line Type:** Select the right type for your network connection. If you don’t know how to choose, please ask your ISP for the information.

- **Total Upstream Bandwidth:** The upload speed through the WAN port.

- **Total Downstream Bandwidth:** The download speed through the WAN port.

- **Description:** This is the information about the rules such as address range.

- **Priority:** Priority of Bandwidth Control rules. 1 stands for the highest priority while 8 stands for the lowest priority. The total Upstream/Downstream Bandwidth is first allocated to guarantee all the Min Rate of Bandwidth Control rules. If there is any bandwidth left, it is first allocated to the rule with the highest priority, then to the rule with the second highest priority, and so on.

- **Upstream bandwidth:** This field displays the max and min upload bandwidth through the WAN port, the default is 0.

- **Downstream bandwidth:** This field displays the max and min download bandwidth through the WAN port, the default is 0.

- **Status:** The status of this rule either Enabled or Disabled.

- **Edit:** Click **Edit** to modify the rule.

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

1. Click **Add New**.
2. Enter the information in the screen.
3. Click **Save**.

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

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

### 4.18 IP & MAC Binding

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

#### 4.18.1 Binding Settings

This page displays the **IP & MAC Binding Setting** 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.
- **Bounding Status**: Check this option to enable ARP binding for a specific device.
- **Edit**: 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 Edit, 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 Edit as desired on the Edit column.
   
   Click Enable/Disable Selected to make selected entries enabled or disabled.
   
   Click Delete Selected to delete selected entries.

4.18.2 ARP List

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

- **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.
- **Load/Delete Selected**: Load or delete the selected item to the IP & MAC Binding list.

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

Click Delete Selected to delete selected items.
Click Refresh to refresh all items.

4.19 Dynamic DNS

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

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

![DDNS Settings](image)

- **Service Provider**: This field displays the service provider of DDNS.
- **Domain Name**: Enter the Domain name you received from dynamic DNS service provider.
- **User name & Password**: Type the username and password for your DDNS account.
- **Enable DDNS**: Activate the DDNS function or not.
- **Login/Loginout**: Login to or logout of the DDNS service.

4.20 Diagnostic

Choose Diagnostic, you can view the test results for the connectivity of the physical layer and protocol layer for both LAN and WAN sides in the screen. Select the desired type and click Start.
4.21 System Tools

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

4.21.1 System Log

Go to System Tools → System Log, and then you can view the logs of the modem router.
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.

Clear Log: All the logs will be deleted from the modem router permanently, not just from the page.

Save Log: Click to save all the logs in a txt file.

Log Settings: Click to set the logs in the screen.

Save Locally: If Save Locally is selected, events will be recorded in the local memory.

Minimum Level: Select the Minimum level in the drop-down list, for the Minimum Level, all logged events above or equal to the selected level will be displayed.

Save Remotely: If Save Remotely is selected, events will be sent to the specified IP address and UDP port of the remote system log server.

Click Save to make the settings effective.

4.21.2 Time Settings

Go to System Tools → Time Settings, 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 modem router will get the time from the NTP Server preferentially. In addition, the modem router built-in some common NTP Servers, so it can get time automatically once it connects the Internet.

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

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

### 4.21.3 Manage Control

Go to System Tools → Manage Control, you can see the screen below.
Manage Control

Current User Status
- User Type: Admin
- User Name: admin
- Host IP Address: 192.168.1.200
- Host MAC Address: 00:E5:49:1E:06:80

Account Management
- The username and password must not exceed 15 characters in length.
  - Old Password:
  - New User Name:
  - New Password:
  - Confirm Password:

Service Configuration
- HTTP Service
  - Local Management: Port: 80
  - Remote Management: Enable Port: 80
- ICMP(ping): Remote Local

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

4.21.4 CWMP Settings

Go to System Tools → CWMP Settings, you can configure the CWMP function in the screen.

The modem router offers CWMP feature. The function supports TR-069 protocol which collects information, diagnoses the devices and configures the devices automatically via ACS (Auto-Configuration Server).
4.21.5 SNMP Settings

Go to System Tools → SNMP Settings, you can see the SNMP-Configuration screen as shown below.

SNMP (Simple Network Management Protocol) has been widely applied in the computer networks currently, which is used for ensuring the transmission of the management information between any two nodes. In this way, network administrators can easily search and modify the information on any node on the network. Meanwhile, they can locate faults promptly and implement the fault diagnosis, capacity planning and report generating.
An **SNMP Agent** is an application running on the modem router that performs the operational role of receiving and processing SNMP messages, sending responses to the SNMP manager, and sending traps when an event occurs. So a router contains SNMP agent software can be monitored and/or controlled by SNMP Manager using SNMP messages.

### 4.21.6 Backup & Restore

Go to **System Tools → Backup & Restore**, and then you can save the current configuration of the modem router as a backup file and restore the configuration via a backup file as shown below.

- **Backup**: Click Backup to save all configuration settings as a backup file in your local computer.
- **Browse**: To upgrade the modem router's configuration, follow these instructions.
  - Click **Browse** to find the configuration file which you want to restore.
  - 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 the device unmanaged. The restoring process lasts for 20 seconds and the modem router will restart automatically then. Keep the power of the modem router on during the process, in case of any damage.

### 4.21.7 Factory Defaults

Go to **System Tools → Factory Defaults**, and then and you can restore the configurations of the modem 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 Subnet Mask: 255.255.255.0

Note:
All changed settings will be lost when defaults are restored.

4.21.8 Firmware Upgrade

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

Firmware Upgrade

New features will be available once the firmware upgrade is successful.

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

Note:
1. Please select the correct firmware build corresponding to the hardware version of the device.
2. It is important to keep the device powered on during the upgrade process to avoid any damage to the device.
3. After the upgrade process is complete, the device will reboot automatically.

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

To upgrade the modem router’s firmware, follow these instructions below:
1) Download a most recent firmware upgrade file from our website (www.tp-link.com).
2) Enter or select the path name where you save the downloaded file on the computer.
3) Click Upgrade.
4) The modem router will reboot after the upgrading has been finished.

Note:
1) New firmware versions are posted at http://www.tp-link.com and can be downloaded for free. There is no need to upgrade the firmware unless the new firmware has a new feature you want to
use. However, when experiencing problems caused by the modem router rather than the configuration, you can try to upgrade the firmware.

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

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

4) The firmware version must correspond to the hardware.

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

4.21.9 Reboot

Go to System Tools → Reboot, and then you can click Reboot to reboot the modem router via the next screen.

<table>
<thead>
<tr>
<th>System Reboot</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Click Reboot to restart the device without applying any changes to your current settings.</strong></td>
</tr>
<tr>
<td><img src="image" alt="Reboot button" /></td>
</tr>
</tbody>
</table>

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

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

4.21.10 Statistics

Go to System Tools → Statistics, and then you can view the statistics of the modem router, including total traffic and current traffic of the last Packets Statistic Interval.
➢ **Traffic Statistics**: Enable or Disable. The default value is disabled. To enable it, click **Enable**. If it is disabled, the function of DoS protection in Security settings will be disabled.

➢ **Statistics Interval (5-60)**: The default value is 10. Select a value between 5 and 60 seconds in the drop-down list. The Packets Statistic interval indicates the time section of the packets statistic.

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

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

Click **Refresh** to refresh immediately.

**Statistics Table:**

<table>
<thead>
<tr>
<th>IP/MAC Address</th>
<th>The IP and MAC address are displayed with related statistics.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Total</strong></td>
<td></td>
</tr>
<tr>
<td>Packs</td>
<td>The total number of packets received and transmitted by the modem router.</td>
</tr>
<tr>
<td>Bytes</td>
<td>The total number of bytes received and transmitted by the modem router.</td>
</tr>
<tr>
<td><strong>Current</strong></td>
<td></td>
</tr>
<tr>
<td>Packs</td>
<td>The total number of packets received and transmitted in the last Packets Statistic interval seconds.</td>
</tr>
<tr>
<td>Bytes</td>
<td>The total number of bytes received and transmitted in the last Packets Statistic interval seconds.</td>
</tr>
<tr>
<td>ICMP Tx</td>
<td>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”.</td>
</tr>
<tr>
<td>UDP Tx</td>
<td>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”.</td>
</tr>
<tr>
<td>SYN Tx</td>
<td>The number of TCP SYN packets transmitted to the WAN per second at the specified Packets Statistics interval. It is shown like “current transmitting rate / Max transmitting rate”.</td>
</tr>
<tr>
<td><strong>Operation</strong></td>
<td></td>
</tr>
<tr>
<td>Reset</td>
<td>Reset the value of the entry to zero.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete the existing entry in the table.</td>
</tr>
</tbody>
</table>
4.22 Logout

Choose **Logout**, and you will back to the login screen as shown below.

![Login Screen](image)

- **Username**
- **Password**

[Login Button]
Appendix A: Configuring the PC

We’ll introduce how to install and configure the TCP/IP correctly on your computer. First make sure your Ethernet Adapter is working, refer to the adapter’s manual if necessary.

The default IP address of the modem router is 192.168.1.1. And the default Subnet Mask is 255.255.255.0. These values can be changed as you desire. Here we use all the default values for description and take Windows XP as example.

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

   ![LAN or High-Speed Internet](image)

   4) In the prompt page that showed below, double click on the **Internet Protocol (TCP/IP)**.
5) The following TCP/IP Properties window will display and the IP Address tab is open on this window by default.

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

➢ Setting IP address automatically

Select Obtain an IP address automatically, and choose Obtain DNS server 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 modem router’s LAN IP address is 192.168.1.1, specify the **IP address** as 192.168.1.x (x is from 2 to 254), and the **Subnet mask** as 255.255.255.0.

3) Type the modem router’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.** In the **Preferred DNS Server** field you can enter the same value as the **Default gateway** or type the local DNS server IP address.
Now: Click OK to keep your settings.

2. **Verify the network connection**

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

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

```
Ping 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

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

- If the result displayed is similar to the screen shown below, it means that your PC has not connected to the router.
You can check it by following the steps below:

1) **Is the connection between your PC and the router correct?**
   
   The LEDs of LAN port which you link to the device and the LEDs on your PC’s adapter should be lit.

2) **Is the TCP/IP configuration for your PC correct?**
   
   If the router’s IP address is 192.168.1.1, your PC’s IP address must be within the range of 192.168.1.2 ~ 192.168.1.254.
Appendix B: Troubleshooting

T1. What can I do if I don’t know or forget my password?

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

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

T2. How do I restore my modem router's configuration to its factory default settings?

Method one: With the modem router powered on, press and hold down the WPS/RESET button for about 8 seconds until all LEDs turn off momentarily, then release the button.

Method two: Restore the default setting from System Tools → Factory Defaults of the modem router’s web management page.

 caut Note:

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

T3. What can I do if I cannot access the web management page?

- Make sure the modem router connects to the computer correctly and the corresponding LED indicator(s) light up.
- Make sure the IP address of your computer is configured to obtain an IP address automatically and obtain DNS server address automatically.
- Make sure the default access is correctly entered in the address field.
- Check your computer’s settings:
  1) Go to Start → Control Panel → Network and Internet, and click View network status and tasks;
  2) Click Internet Options on the bottom left;
  3) Click Connections, and select Never dial a connection;
4) Click LAN settings, deselect the following three options and click OK;

5) Go to Advanced → Restore advanced settings, and click OK to make the settings effective.
Change a web browser or computer and log in again.
Reset the modem router to factory default settings.

Note:
You’ll need to reconfigure the modem router to surf the Internet once the modem router is reset.
Open a web browser and log in again. If login fails, please contact the technical support.

T4. What can I do if I cannot access the Internet?

1) Check to see if all the connectors are connected well, including the telephone line, Ethernet cables and power adapter.

2) Check to see if you can log in to the web management page of the modem router. If you can, try the following steps. If you cannot, please set your computer referring to T3 then try to see if you can access the Internet. If the problem persists, please go to the next step.

3) Consult your ISP and make sure all the VPI/VCI, Connection Type, account username and password are correct. If there are any mistakes, please correct the settings and try again.

4) If you still cannot access the Internet, please restore your modem router to its factory default settings and reconfigure your modem router by following the instructions in Chapter 3 Quick Installation Guide.

5) Please feel free to contact our Technical Support if the problem still exists.

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