TP-LINK®

TX-W6961N
User Guide
N300 Wireless GPON Router

REV1.0.0 1910011749

Contents

About This Guide

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

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

Conventions

In this guide, the following conventions are used:

Convention	Description
Blue Italic	Hyperlinks are in blue italic. You can click to redirect to a website or a specific section.
Blue	Contents to be emphasized and texts on the web page are in blue, including the menus, items, buttons, etc.
>	The menu structures to show the path to load the corresponding page. For example, Advanced > Wireless > MAC Filtering means the MAC Filtering function page is under the Wireless menu that is located in the Advanced tab.
Note:	Ignoring this type of note might result in a malfunction or damage to the device.
Tips:	Indicates important information that helps you make better use of your device.
symbols on the web page	• ✎ click to edit the corresponding entry. • 🗑 click to delete the corresponding entry. • 💡 click to enable or disable the corresponding entry. • ? click to view more information about items on the page.

More Info

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

The Quick Installation Guide (QIG) can be found where you find this guide or inside the package of the 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 the Contact Technical Support page at *http://www.tp-link.com/support*.

Chapter 1

Get to Know About Your GPON Router

This chapter introduces what the router can do and shows its main features and appearance.

This chapter contains the following sections:

- *Product Overview*
- *Product Appearance*

1. 1. Product Overview

TP-LINK’s GPON Router is a combined wired/wireless network connection device with integrated high speed GPON ONT, NAT router, 4-port switch, and wireless N access point, reducing hassle of configuration and saving space.

With extremely high downstream and upstream access speed, the router gives you unparalleled surfing experience.

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

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

1. 2. Product Appearance

1. 2. 1. Front Panel

The router’s front panel provides LEDs. You can check the router’s working status by following the LED Explanation table.

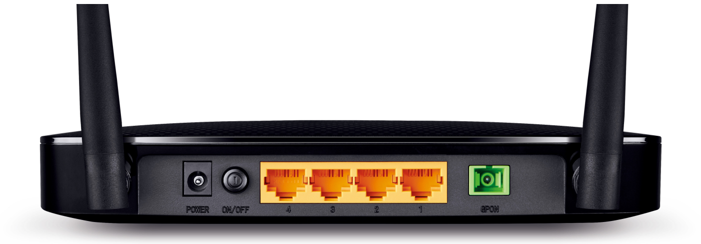
LED	Status	Indication
⏻ Power	On	Power is on.
	Off	Power is off.

LED	Status	Indication
GPON	On	The router is registered with the ISP.
	Flashing	The router is trying to register with the ISP.
	Off	The router is not yet registered with the ISP.
LOS	On	The router is unable to transmit optical signal.
	Flashing	No optical signal is received or the received signal is too weak.
	Off	The router is receiving optical signal properly.
LAN	On	A device is connected to the LAN port.
	Flashing	The LAN port is transmitting or receiving data.
	Off	No device is connected to the LAN port.
Wi-Fi	On	The wireless radio band is enabled.
	Flashing	The router is transmitting or receiving data via Wi-Fi.
	Off	The wireless radio band is disabled.
WPS	On/Off	The LED stays on for 30 seconds when a WPS connection is established, then turns off.
	Flashing	WPS connection is in progress. This may take up to 2 minutes.

Note:

If the GPON LED is off or the LOS LED is on or flashing, check your Internet connection first. Refer to *Connect Your GPON Router* for more information about how to make Internet connection correctly. If you have already made a right connection, contact your ISP to make sure your Internet service is available now.

1. 2. 2. Back Panel



The router's back panel provides connection ports, Power button and antennas. Refer to the following for detailed instructions.

Item	Description
GPON	For connecting the router to the Internet. Connect the port to the splitter via a fiber line. For details, please refer to *Connect Your GPON Router*.
LAN (1-4)	For connecting the router to your PC or other Ethernet network devices.
Power On/Off	The switch for the power. Press it to power on or off the router.

Item	Description
POWER	For connecting the router to power socket via the provided power adapter.
Antennas	Used for wireless operation and data transmission. Upright them for the best Wi-Fi performance.

1. 2. 3. Side Panel

The router's side panel provides buttons. Refer to the following for detailed instructions.

Button	Description
RESET	Press and hold for about 5 seconds until all LEDs turn off momentarily to reset the router to factory default settings.
WPS	The switch for the WPS function.
Wi-Fi	Press to turn the Wi-Fi on or off.

Chapter *2*

Connect the Hardware

This chapter contains the following sections:

- *Position Your GPON Router*
- *Connect Your GPON Router*

2. 1. Position Your GPON Router

With the 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 router. Many obstacles may limit the range of the wireless signal, for example, concrete structures and thick walls.

For your safety and best Wi-Fi performance, please:

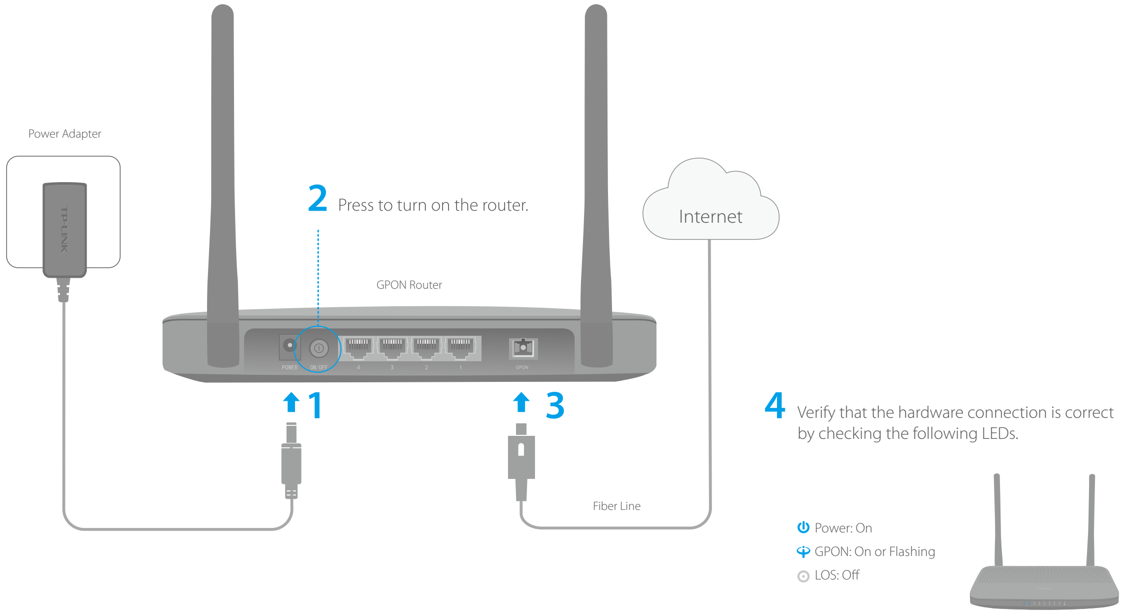
- Do Not locate the router in the place where it will be exposed to moisture or excessive heat.
- Keep away from the strong electromagnetic radiation and the device of electromagnetic sensitive.
- Place the router in a location where it can be connected to the various devices as well as to a power source.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

Tips: The router can be placed on a shelf or desktop and can be hung on the wall.

2. 2. Connect Your GPON Router

Follow the steps below to connect your router.

1. Connect the power adapter and the fiber line. The electrical outlet shall be installed near the device and shall be easily accessible.



2 Press to turn on the router.

4 Verify that the hardware connection is correct by checking the following LEDs.

Power: On
GPON: On or Flashing
LOS: Off

2. Connect your computer to the router.

Method 1: Wired

Connect your computer’s Ethernet port to a LAN port on the router via an Ethernet cable.

Method 2: Wireless

Connect wirelessly by using the default SSID (Wireless Network Name) and Wireless Password printed on the product label of the router.

Method 3: Use 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.)

Note:

The WPS function cannot be configured if the wireless function of the 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) Tab the WPS icon on the device’s screen.

2) Immediately press the WPS button on your 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 been successfully connected to the router.

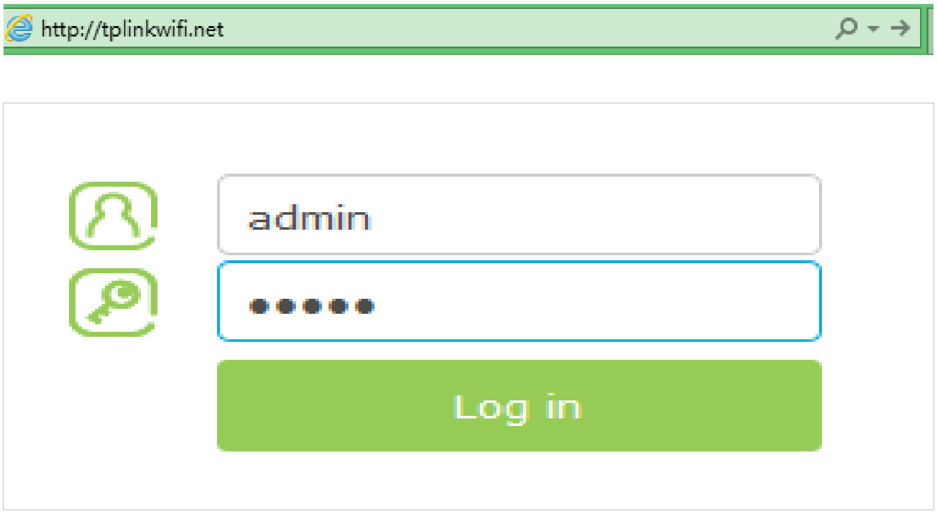
Chapter 3

Log into Your GPON Router

With a web management page, it is easy to configure and manage the router. The web management page can be used on any Windows, Macintosh or UNIX OS with a Web browser, such as Microsoft Internet Explorer, Mozilla Firefox or Apple Safari.

Follow the steps below to log into your router.

1. If the TCP/IP Protocol on your computer is set to the static (fixed) IP address, you need to change it to obtain an IP address automatically. Refer to *Appendix: Troubleshooting* to configure your computer.
2. Launch a web browser and go to *http://tplinkwifi.net* or *http://192.168.1.1*. Use admin for both username and password, and then click Log in.



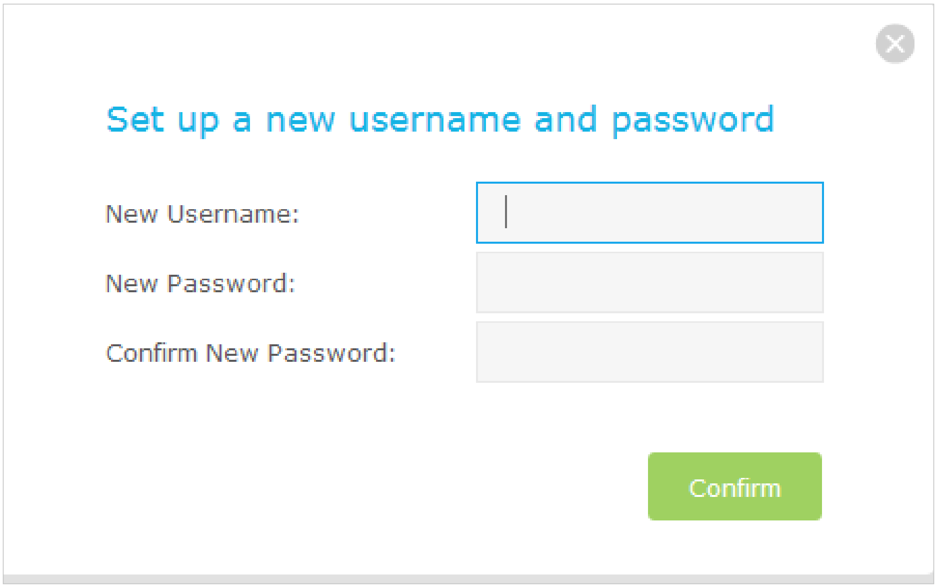
http://tplinkwifi.net

admin

●●●●●

Log in

3. Create a new username and password for subsequent logins and click Confirm.



Set up a new username and password

New Username:

New Password:

Confirm New Password:

Confirm

Chapter *4*

Set Up Internet Connections

This chapter introduces how to connect your router to the Internet. The router is equipped with a web-based Quick Setup wizard. It has many ISP information built in, automates many of the steps and verifies that those steps have been successfully completed. Furthermore, you can also set up an IPv6 connection if your ISP provides IPv6 service.

This chapter includes the following sections:

- *Use Quick Setup Wizard*
- *Manually Set Up an Internet Connection*
- *Test Internet Connectivity*
- *Set Up an IPv6 Connection*

4. 1. Use Quick Setup Wizard

To set up your router with several easy steps quickly:

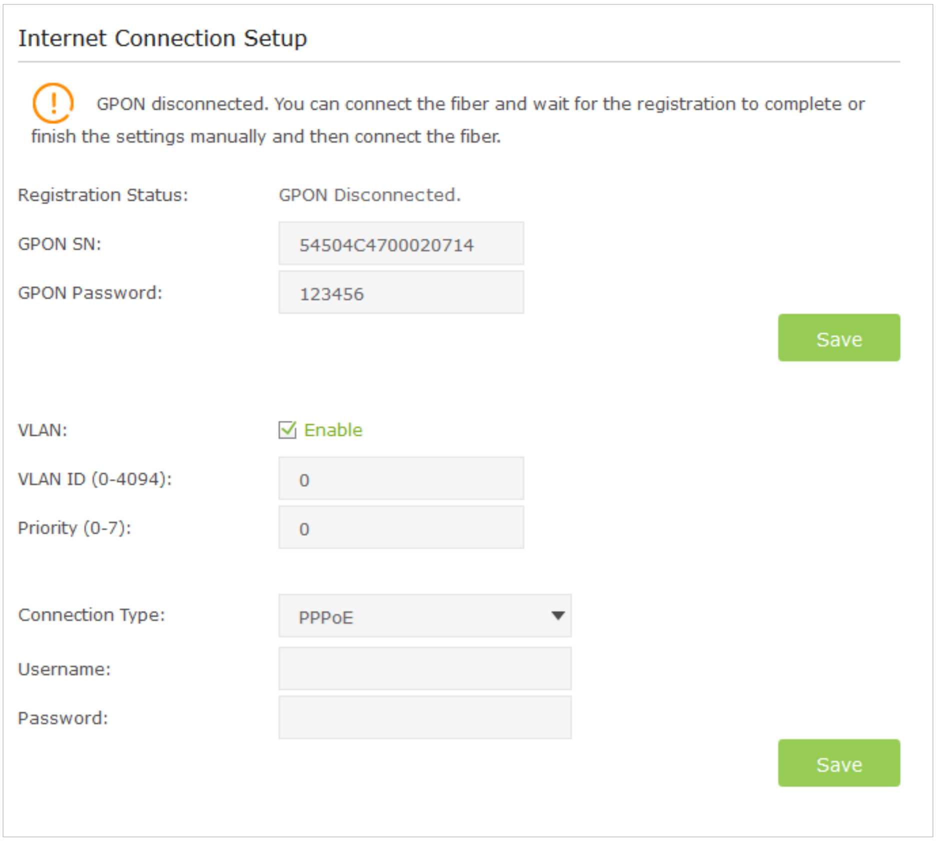
1. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
2. Select your Region and Time Zone, then click Next.
3. Follow the step-by-step instructions of the Quick Setup to complete the initial configuration.

Note:

During the quick setup process, you can change the preset wireless network name (SSID) and wireless password. After that, all your wireless devices must use the new SSID and password to connect to the router.

4. 2. Manually Set Up an Internet Connection

1. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
2. Go to Basic > Internet page. Enter the GPON SN and GPON password provided by your ISP. Click Save.



Internet Connection Setup

GPON disconnected. You can connect the fiber and wait for the registration to complete or finish the settings manually and then connect the fiber.

Registration Status: GPON Disconnected.

GPON SN: 54504C4700020714

GPON Password: 123456

VLAN: ☑ Enable

VLAN ID (0-4094): 0

Priority (0-7): 0

Connection Type: PPPoE

Username:

Password:

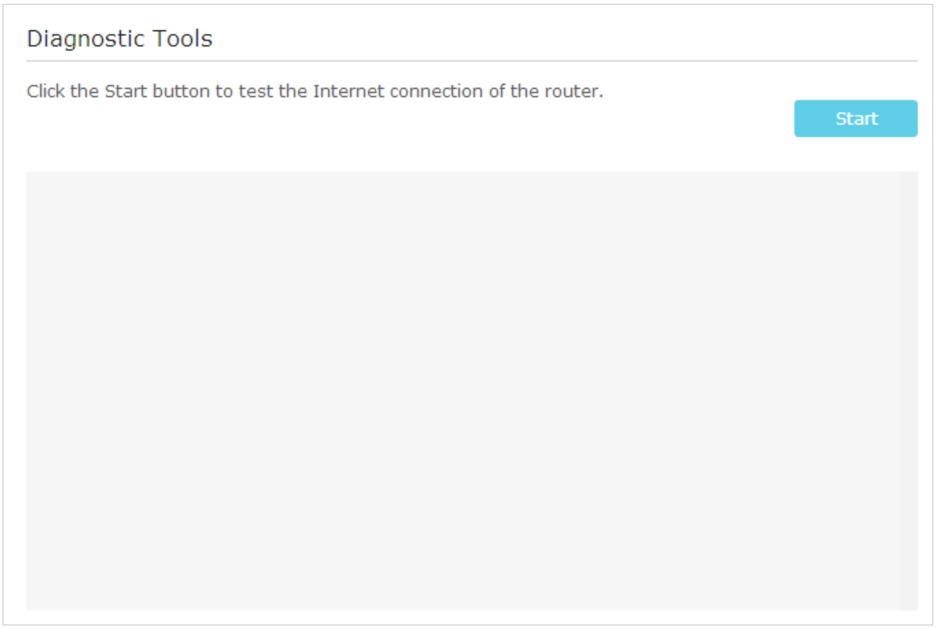
3. Wait until the Registration Status becomes Registered and enter the rest parameters provided by your ISP.
4. Click Save to make the settings effective, and you can refer to *Test Internet Connectivity* to test the Internet connection.

Tips: You can view and edit all Internet connections on Advanced > Network > Internet page.

4. 3. Test Internet Connectivity

After manually setting up the Internet connection, you need to test the Internet connectivity. The router provides a diagnostic tool to help you locate the malfunction.

1. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
2. Go to Advanced > System Tools > Diagnostics page.



Diagnostic Tools

Click the Start button to test the Internet connection of the router.

3. Click Start to test the Internet connectivity and you will see the test result in the gray box.

4. 4. Set Up an IPv6 Connection

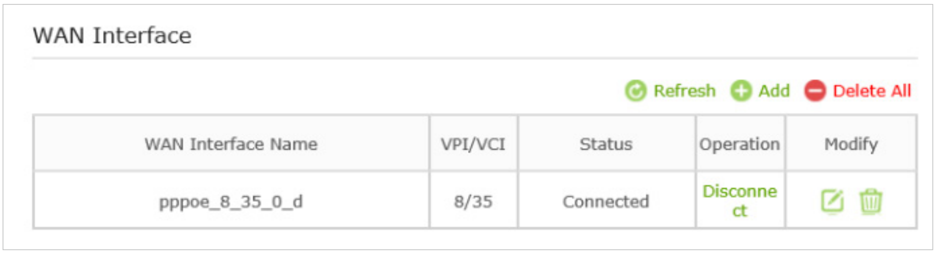
If your ISP has provided a GPON line that supports IPv6 connection as well as some detailed IPv6 parameters, you can manually set up an IPv6 connection.

Follow the steps below to set up an IPv6 connection:

1. Make sure you have set up an IPv4 connection by using Quick Setup wizard or manually before setting up an IPv6 connection.

2. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.

3. Go to Advanced > Network > Internet page.

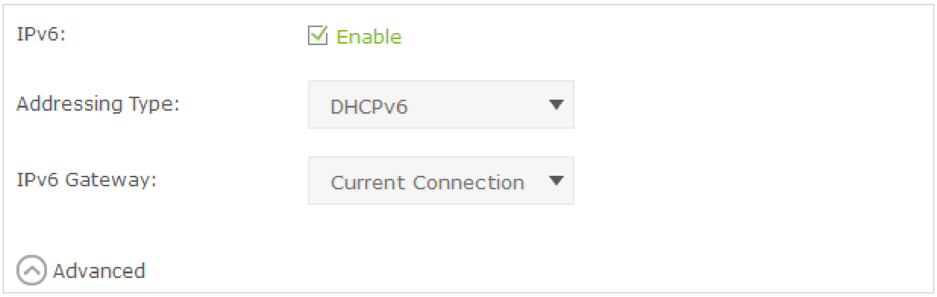


WAN Interface

WAN Interface Name	VPI/VCI	Status	Operation	Modify
pppoe_8_35_0_d	8/35	Connected	Disconnect	✎ 🗑

4. Select your WAN Interface Name (Status should be Connected) and click the ✎ (Edit) icon.

5. Scroll down the page, enable IPv6, and configure the IPv6 parameters.



IPv6: ☑ Enable

Addressing Type: DHCPv6

IPv6 Gateway: Current Connection

Addressing Type: Consult your ISP for the addressing type, DHCPv6 or SLAAC. SLAAC is the most commonly used addressing type.

IPv6 Gateway: Keep the default setting as Current Connection.

Note: If your ISP has provided the IPv6 address, click Advanced to reveal more settings. Check to use IPv6 specified by ISP and enter the parameters provided by your ISP.

6. Click OK to make the settings effective. Now IPv6 service is available for your network.

Chapter 5

Bandwidth Control

The Bandwidth Control feature is used to fully utilize your limited bandwidth and optimize the load respectively. With this feature enabled, you can assign a specific minimum or maximum bandwidth for each computer, thus minimizing the impact caused by heavy load.

I want to:

Use an independent bandwidth and enjoy a good Internet experience without being affected by other users who are sharing the same router.

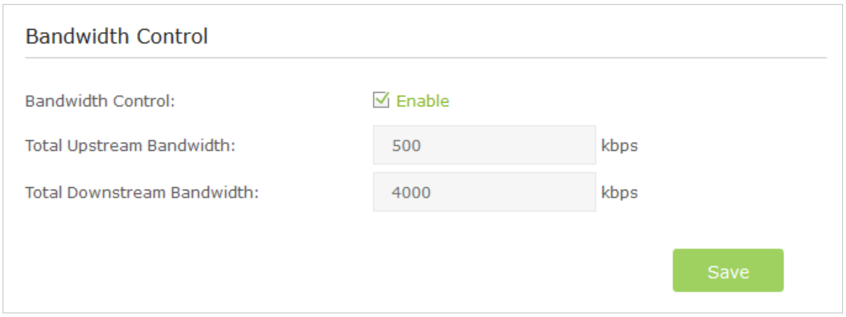
For example, my roommate and I share 512Kbps Upstream Bandwidth and 4Mbps Downstream Bandwidth via this router, she likes to watch live show and play online games, which may take up much bandwidth. I don't want to be affected, so we agree to equally distribute the bandwidth. Our IP addresses are 192.168.1.101 and 192.168.1.110.

Tips:

To use the bandwidth control feature, you'd better set static IP address on each computer to be controlled or configure address reservation on the router in order to manage easily. About how to configure address reservation, please refer to *Reserve LAN IP Addresses*.

How can I do that?

1. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
2. Go to Advanced > Bandwidth Control page.



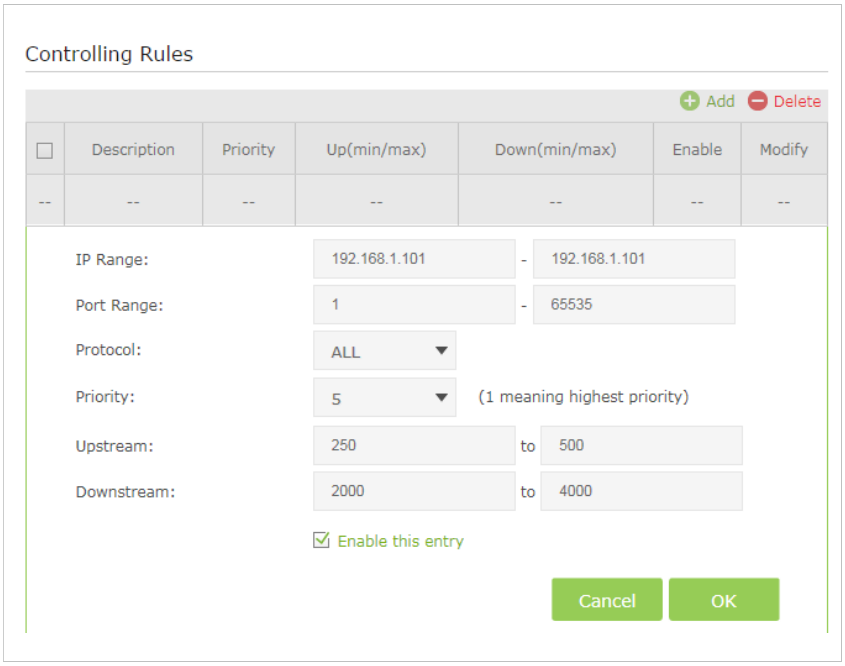
Bandwidth Control

Bandwidth Control: ☑ Enable

Total Upstream Bandwidth: 500 kbps

Total Downstream Bandwidth: 4000 kbps

3. Enable Bandwidth Control.
4. Enter the Total Upstream Bandwidth and the Total Downstream Bandwidth given by your ISP (1Mbps=1024kbps). Click Save to save the settings.
5. Click Add to add a controlling rule.



Controlling Rules

□	Description	Priority	Up(min/max)	Down(min/max)	Enable	Modify
--	--	--	--	--	--	--

IP Range: 192.168.1.101 - 192.168.1.101

Port Range: 1 - 65535

Protocol: ALL

Priority: 5 (1 meaning highest priority)

Upstream: 250 to 500

Downstream: 2000 to 4000

☑ Enable this entry

1) IP Range: Enter the IP address. The field can be single IP address or IP address range according to your demands. When you configure the single IP address, the computer with this IP address will get independent given bandwidth. When you configure the IP address range, all computers in the range will share the given bandwidth.

2) Port Range: Keep the default settings. The default port range of TCP protocol or UDP protocol is from 1 to 65535.

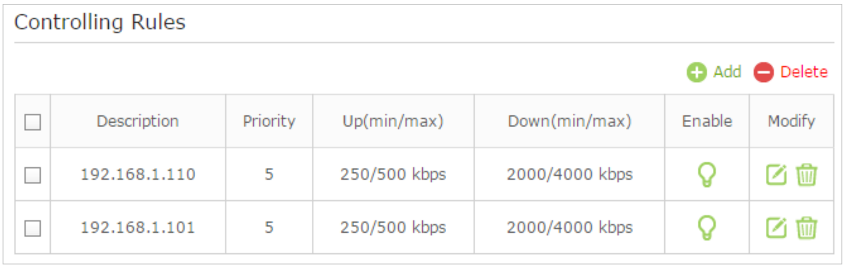
3) Protocol: Keep the default setting. Or you can choose the TCP protocol or UDP protocol or both of them.

4) Priority: Keep the default setting. You can change the value if you want to first guarantee the bandwidth for one computer. The smaller value has the higher priority.

5) Upstream/Downstream: Enter the bandwidth according to your division.

6) Enable this entry: Check to enable this entry and click OK to save the settings.

6. Repeat Step 5 to add a rule for the other computer. And then you will get the following table.



Controlling Rules

□	Description	Priority	Up(min/max)	Down(min/max)	Enable	Modify
□	192.168.1.110	5	250/500 kbps	2000/4000 kbps	💡	✎ 🗑
□	192.168.1.101	5	250/500 kbps	2000/4000 kbps	💡	✎ 🗑

Done!

Now you and your roommate have an independent bandwidth.

Chapter *6*

Network Security

This chapter guides you on how to protect your home network from unauthorized users by implementing these three network security functions. You can block or allow specific client devices to access your wireless network using MAC Filtering, or using Access Control for wired and wireless networks, or you can prevent ARP spoofing and ARP attacks by using IP & MAC Binding.

- *MAC Filtering*
- *Access Control*
- *IP & MAC Binding*

6. 1. MAC Filtering

This function exploits the uniqueness of the MAC (Medium Access Control) address, a unique 12-digit hexadecimal address (for example, D8:5D:4C:B4:46:EA) of every network device, to determine if the device can or cannot access your wireless network.

I want to:

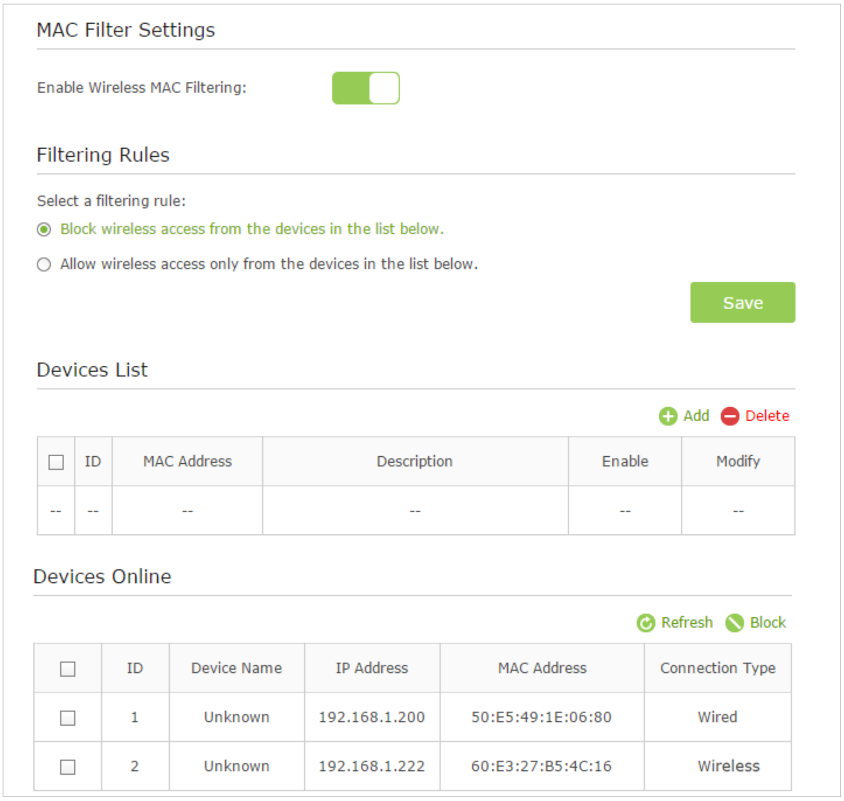
Prevent unauthorized users from accessing my wireless network by utilizing the network device's MAC address.

For example, I have a computer that is connected to my wireless network. Now, an unknown device (an intruder) is also using my wireless network, which affects my Internet speed. I would like to control my wireless network with the following capabilities:

- My computer is always allowed to access the wireless network.
- The unknown device is not allowed to access the wireless network.
- I don't have to keep changing my wireless password as often.

How can I do that?

1. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
2. Go to Advanced > Wireless > MAC Filtering and enable Wireless MAC Filtering.



MAC Filter Settings

Enable Wireless MAC Filtering: ON

Filtering Rules

Select a filtering rule:

● Block wireless access from the devices in the list below.

○ Allow wireless access only from the devices in the list below.

Devices List

□	ID	MAC Address	Description	Enable	Modify
--	--	--	--	--	--

Devices Online

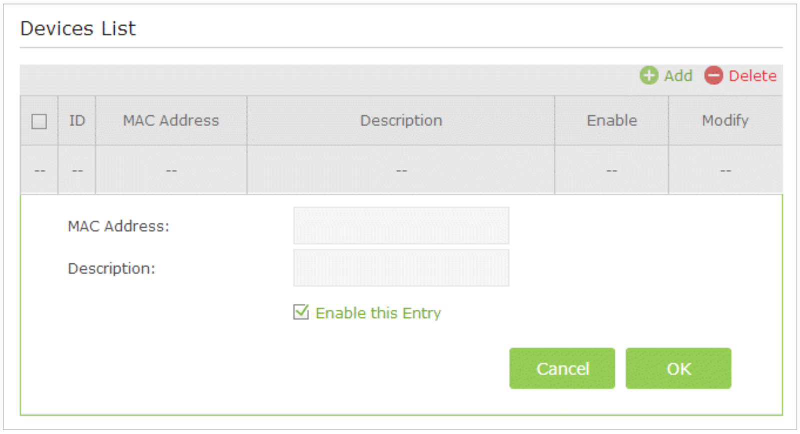
□	ID	Device Name	IP Address	MAC Address	Connection Type
□	1	Unknown	192.168.1.200	50:E5:49:1E:06:80	Wired
□	2	Unknown	192.168.1.222	60:E3:27:B5:4C:16	Wireless

3. Select the filtering rule to either block (recommended) or allow the device(s) in the list.

   To block/allow specific device(s)

   1) Select Block wireless access from the devices in the list below or Allow wireless access only from the devices in the list below and click Save.

   2) Click Add.



Devices List

□	ID	MAC Address	Description	Enable	Modify
--	--	--	--	--	--

MAC Address:

Description:

☑ Enable this Entry

   3) Enter the MAC Address manually. (You can copy and paste the information from Devices Online table if the device is connected to your network).

   4) Enter the Description of the device.

   5) Select the check box to enable this entry, and click OK.

Done! Now MAC Filtering is implemented to protect your wireless network.

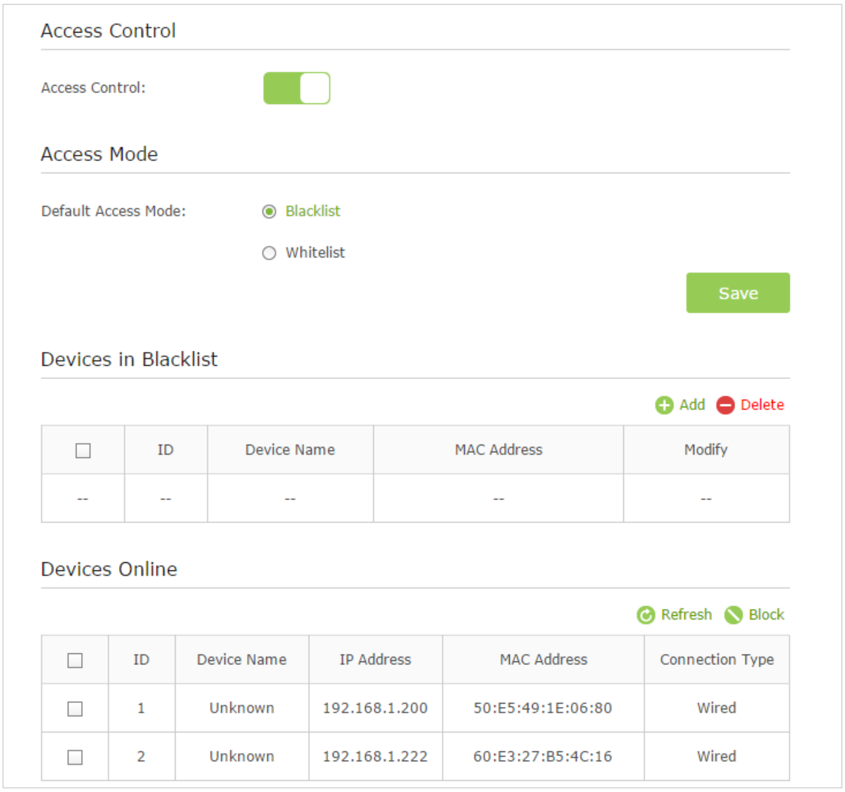
6. 2. Access Control

Access Control is used to block or allow specific client devices to access your network (via wired or wireless) based on a list of blocked devices (Blacklist) or a list of allowed devices (Whitelist).

I want to: Block or allow specific client devices to access my network (via wired or wireless).

How can I do that?

1. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
2. Go to Advanced > Security > Access Control and enable Access Control.



Access Control

Access Control: ●

Access Mode

Default Access Mode: ● Blacklist

○ Whitelist

Devices in Blacklist

□	ID	Device Name	MAC Address	Modify
--	--	--	--	--

Devices Online

□	ID	Device Name	IP Address	MAC Address	Connection Type
□	1	Unknown	192.168.1.200	50:E5:49:1E:06:80	Wired
□	2	Unknown	192.168.1.222	60:E3:27:B5:4C:16	Wired

3. Select the access mode to either block (recommended) or allow the device(s) in the list.

To block specific device(s)

1) Select Blacklist and click Save.

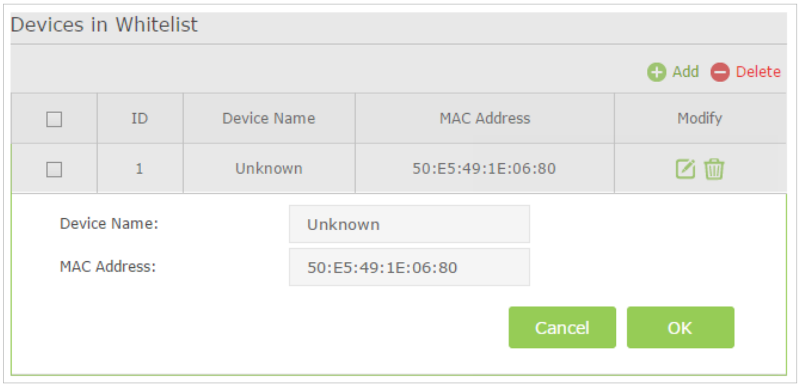
2) Select the device(s) to be blocked in the Devices Online table.

3) Click Block above the Devices Online table. The selected devices will be added to Devices in Blacklist automatically.

To allow specific device(s)

1) Select Whitelist and click Save.

2) Click Add.



Devices in Whitelist

□	ID	Device Name	MAC Address	Modify
□	1	Unknown	50:E5:49:1E:06:80	✎ 🗑

Device Name: Unknown

MAC Address: 50:E5:49:1E:06:80

3) Enter the Device Name and MAC Address (You can copy and paste the information from Devices Online table if the device is connected to your network).

4) Click OK.

Done! Now you can block or allow specific client devices to access your network (via wired or wireless) using the Blacklist or Whitelist.

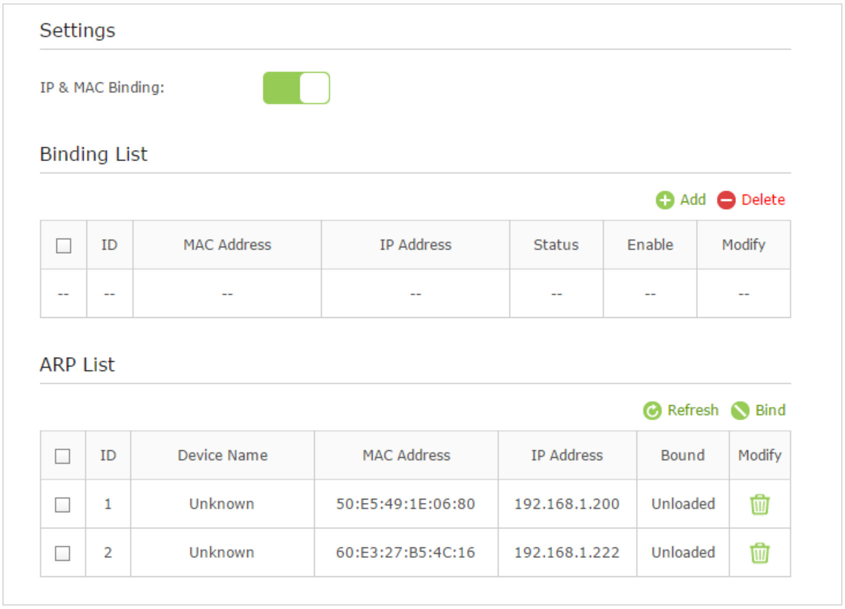
6. 3. IP & MAC Binding

IP & MAC Binding, namely, ARP (Address Resolution Protocol) Binding, is used to bind network device’s IP address to its MAC address. This will prevent ARP spoofing and other ARP attacks by denying network access to a device with matching IP address in the Binding list, but unrecognized MAC address.

I want to: Prevent ARP spoofing and ARP attacks.

How can I do that?

1. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
2. Go to Advanced > Security > IP & MAC Binding and enable IP & MAC Binding.



Settings

IP & MAC Binding: (on)

Binding List

□	ID	MAC Address	IP Address	Status	Enable	Modify
--	--	--	--	--	--	--

ARP List

□	ID	Device Name	MAC Address	IP Address	Bound	Modify
□	1	Unknown	50:E5:49:1E:06:80	192.168.1.200	Unloaded	🗑
□	2	Unknown	60:E3:27:B5:4C:16	192.168.1.222	Unloaded	🗑

3. Bind your device(s) according to your needs.

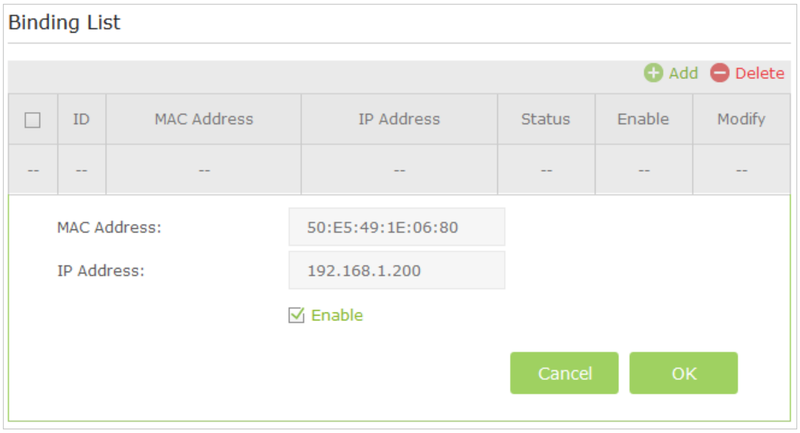
To bind the connected device(s)

1) Select the device(s) to be bound in the ARP List.

2) Click Bind to add to the Binding List.

To bind the unconnected device

1) Click Add.



Binding List

□	ID	MAC Address	IP Address	Status	Enable	Modify
--	--	--	--	--	--	--

MAC Address: 50:E5:49:1E:06:80

IP Address: 192.168.1.200

☑ Enable

2) Enter the MAC address and IP address that you want to bind.

3) Select the check box to enable the entry and click OK.

Done!

Now you don’t need to worry about ARP spoofing and ARP attacks.

Chapter 7

Parental Controls

This function allows you to block inappropriate, explicit and malicious websites, and control access to specified websites at specified time.

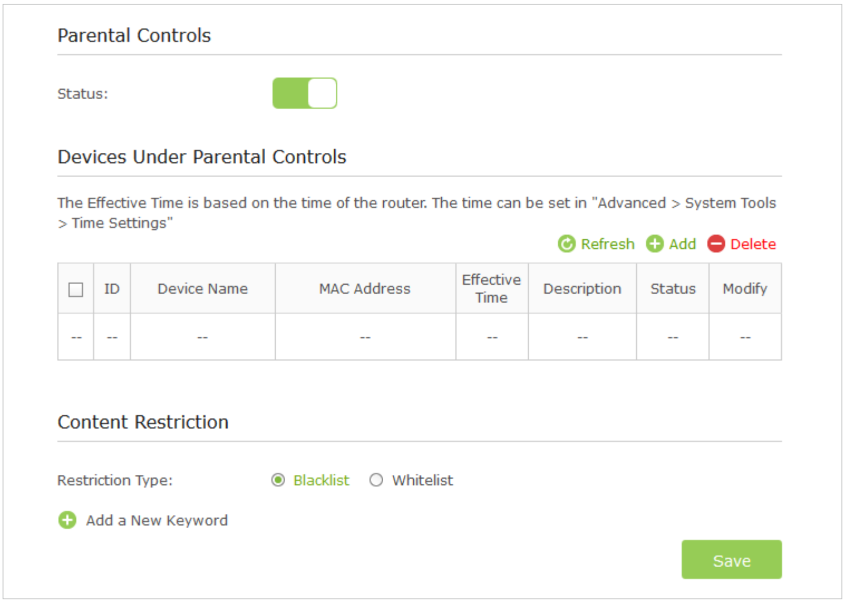
I want to:

Control what types of websites my children or other home network users can visit and even the time of day they are allowed to access the Internet.

For example, I want to allow my children's devices (e.g. a computer or a tablet) to access only www.tp-link.com and Wikipedia.org from 18:00 (6PM) to 22:00 (10PM) on weekdays and not other time.

How can I do that?

1. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
2. Go to Basic or Advanced > Parental Controls and enable Parental Controls.



Parental Controls

Status: (on)

Devices Under Parental Controls

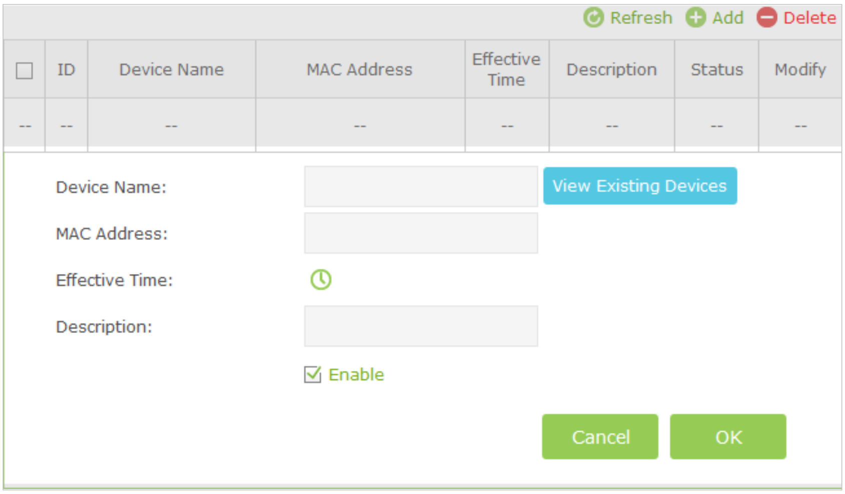
The Effective Time is based on the time of the router. The time can be set in "Advanced > System Tools > Time Settings"

□	ID	Device Name	MAC Address	Effective Time	Description	Status	Modify
--	--	--	--	--	--	--	--

Content Restriction

Restriction Type: ● Blacklist ○ Whitelist

3. Click Add.



□	ID	Device Name	MAC Address	Effective Time	Description	Status	Modify
--	--	--	--	--	--	--	--

Device Name:

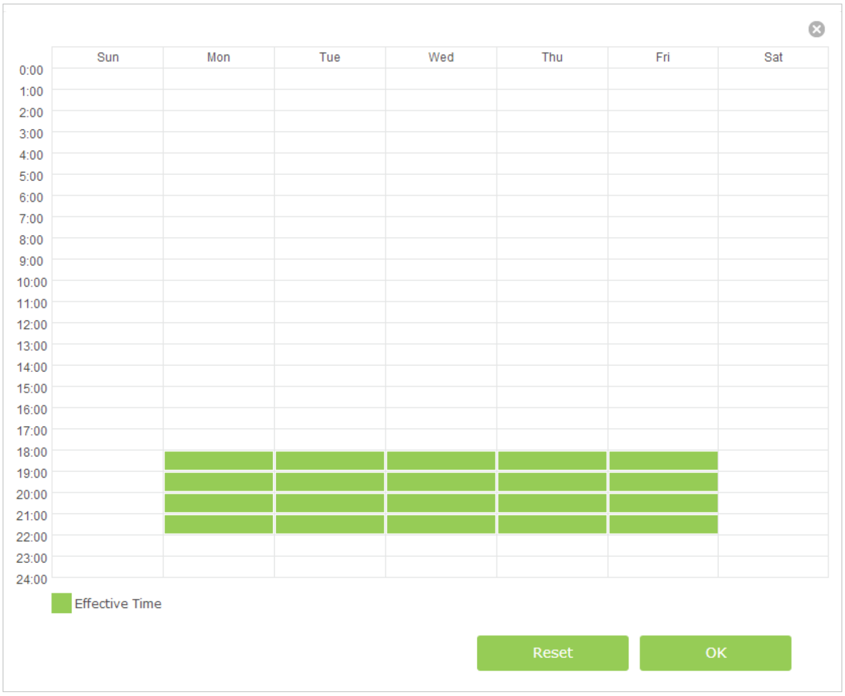
MAC Address:

Effective Time:

Description:

☑ Enable

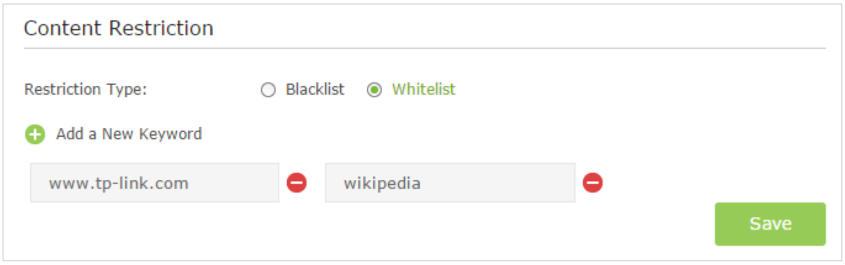
4. Click View Existing Devices, and select the device to be controlled. Or, enter the Device Name and MAC Address manually.
5. Click the 🕓 icon to set the Effective Time. Drag the cursor over the appropriate cell(s) and click OK.



	Sun	Mon	Tue	Wed	Thu	Fri	Sat
0:00							
1:00							
2:00							
3:00							
4:00							
5:00							
6:00							
7:00							
8:00							
9:00							
10:00							
11:00							
12:00							
13:00							
14:00							
15:00							
16:00							
17:00							
18:00		🟩	🟩	🟩	🟩	🟩	
19:00		🟩	🟩	🟩	🟩	🟩	
20:00		🟩	🟩	🟩	🟩	🟩	
21:00		🟩	🟩	🟩	🟩	🟩	
22:00							
23:00							
24:00							

🟩 Effective Time

6. Enter a Description for the entry.
7. Select the check box to enable this entry and click OK.
8. Select the restriction mode.
   1) In Blacklist mode, the controlled devices cannot access any websites containing the specified keywords during the Effective Time period.
   2) In Whitelist mode, the controlled devices can only access websites containing the specified keywords during the Effective Time period.



Content Restriction

Restriction Type: ○ Blacklist ● Whitelist

Add a New Keyword

www.tp-link.com

wikipedia

9. Click Add a New Keyword. You can add up to 200 keywords for both Blacklist and Whitelist. Below are some sample entries to allow access.

   1) Enter a web address (e.g. www.tp-link.com) or a web address keyword (e.g. wikipedia) to only allow or block access to the websites containing that keyword.

   2) Specify the domain suffix (eg. .edu or .org) to allow access only to the websites with that suffix.

   3) If you wish to block all Internet browsing access, do not add any keyword to the Whitelist.

10. Enter the keywords or websites you want to add and click Save.

Done!

Now you can control your children's Internet access according to your needs.

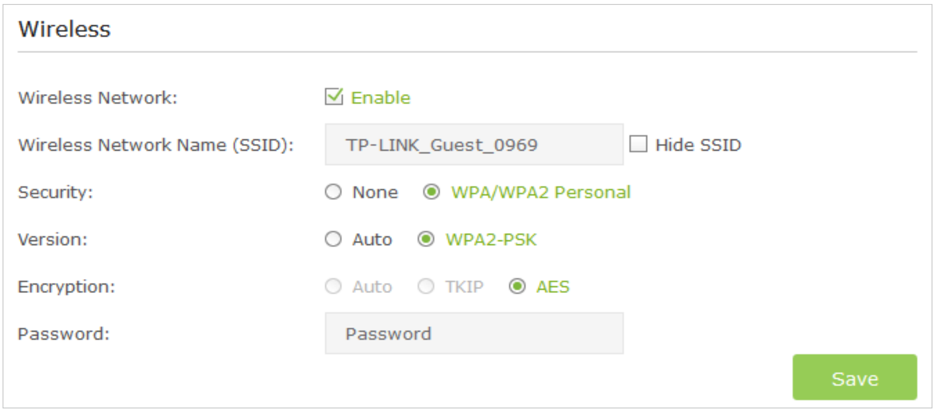
Chapter *8*

Guest Network

This function allows you to provide Wi-Fi access for guests without disclosing your main network. When you have guests in your house, apartment, or workplace, you can create a guest network for them. In addition, you can assign network authorities and bandwidth for guests to ensure network security, privacy, and fluency.

8. 1. Create a Network for Guests

1. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
2. Go to Advanced > Guest Network. Locate the Wireless section.
3. Create a guest network according to your needs.



Wireless

Wireless Network:	☑ Enable
Wireless Network Name (SSID):	TP-LINK_Guest_0969 □ Hide SSID
Security:	○ None ● WPA/WPA2 Personal
Version:	○ Auto ● WPA2-PSK
Encryption:	○ Auto ○ TKIP ● AES
Password:	Password

1) Enable wireless guest network.

2) Set an easy-to-identify SSID. Don't select Hide SSID unless you want your guests and other people to manually input this SSID for Wi-Fi access.

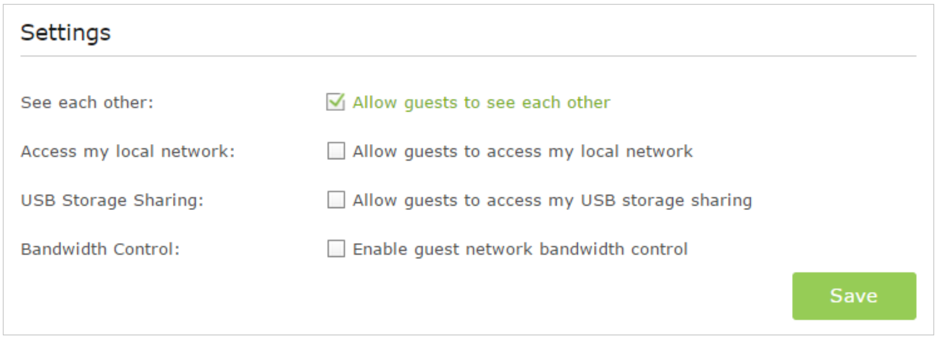
3) Set Security to WPA/WPA2 Personal, keep the default Version and Encryption values, and set an easy-to-remember password.

4. Click Save. Now your guests can access your guest network using the SSID and password you set!

Tips:
To view guest network information, go to Advanced > Status and find the Guest Network section.

8. 2. Customize Guest Network Options

1. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
2. Go to Advanced > Guest Network. Locate the Settings section.



Settings

See each other: ☑ Allow guests to see each other

Access my local network: □ Allow guests to access my local network

USB Storage Sharing: □ Allow guests to access my USB storage sharing

Bandwidth Control: □ Enable guest network bandwidth control

3. Assign network authorities and bandwidth according to your needs.

Note:

Some routers may not offer some of these guest network options.

- Allow guests to see each other

  Select this check box to allow the clients in your guest network to access each other.

- Allow guests to access my local network

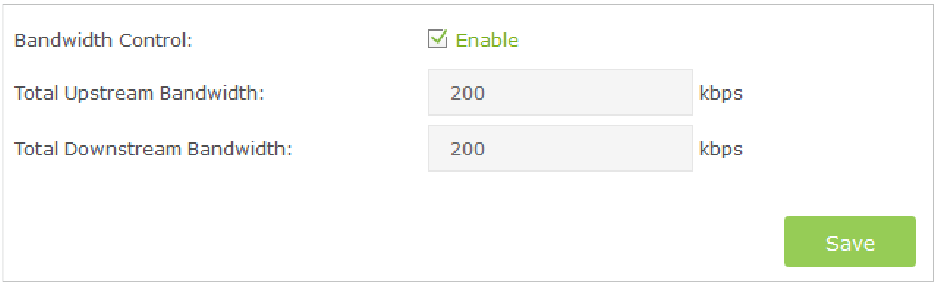
  Select this check box to allow the clients in your guest network to access your local network, not just Internet access.

- Allow guests to access my USB storage sharing

  Select this check box to allow the clients in your guest network to access your router's USB storage sharing.

- Enable guest network bandwidth control

  Select this check box to assign the upstream and downstream bandwidth of the guest network. This option is available only when Bandwidth Control is enabled on the Advanced > Bandwidth Control page.



Bandwidth Control: ☑ Enable

Total Upstream Bandwidth: 200 kbps

Total Downstream Bandwidth: 200 kbps

4. Click Save. Now users in your guest network can enjoy only the network authorities and bandwidth you assigned!

Tips:

To view guest network information, go to Advanced > Status and find the Guest Network section.

Chapter 9

NAT Forwarding

The router's NAT (Network Address Translation) feature makes the devices in the LAN use the same public IP address to communicate in the Internet, which protects the local network by hiding IP addresses of the devices. However, it also brings about the problem that external host cannot initiatively communicate with the specified device in the local network.

With forwarding feature the router can penetrate the isolation of NAT and allows the external hosts in the Internet to initiatively communicate with the devices in the local network, thus to realize some special functions.

TP-LINK router includes four forwarding rules. If two or more rules are set, the priority of implementation from high to low is Virtual Servers, Port Triggering, UPnP and DMZ.

This chapter contains the following sections:

9. 1. Share Local Resources in the Internet by Virtual Server

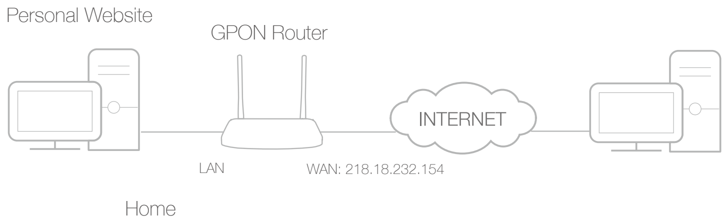
When you build up a server in the local network and want to share it on the Internet, Virtual Server can realize the service and provide it to the Internet users. At the same time virtual server can keep the local network safe as other services are still invisible from the Internet.

Virtual server can be used for setting up public services in your local network, such as HTTP, FTP, DNS, POP3/SMTP and Telnet. Different service uses different service port. Port 80 is used in HTTP service, port 21 in FTP service, port 25 in SMTP service and port 110 in POP3 service. Please verify the service port number before the configuration.

I want to:

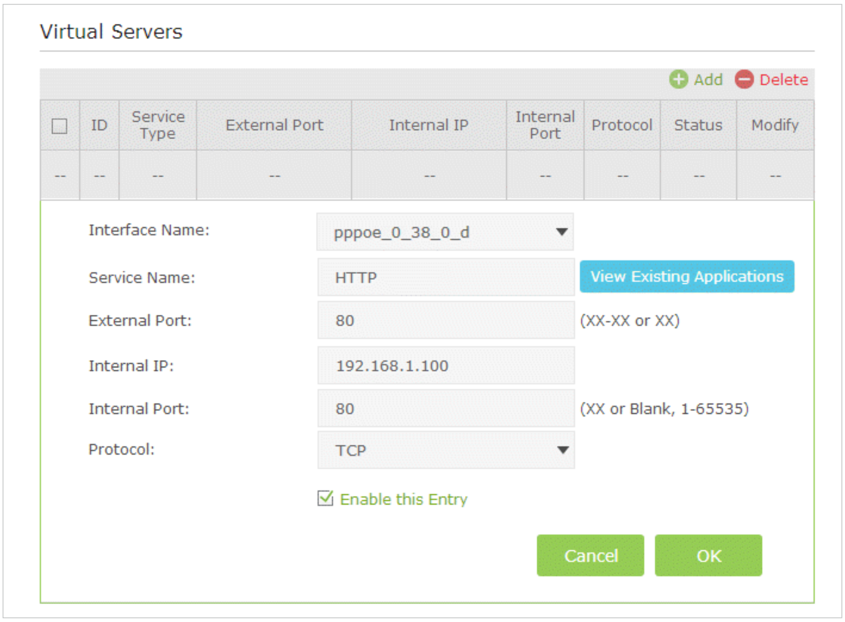
Share my personal website I've built in local network with my friends through the Internet.

For example, the personal website has been built in my home PC (192.168.1.100). I hope that my friends in the Internet can visit my website in some way. The PC is connected to the router with the WAN IP address 218.18.232.154.



How can I do that?

1. Assign a static IP address to your PC, for example 192.168.1.100.
2. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
3. Go to Advanced > NAT Forwarding > Virtual Servers, click Add.



Virtual Servers

□	ID	Service Type	External Port	Internal IP	Internal Port	Protocol	Status	Modify
--	--	--	--	--	--	--	--	--

Interface Name:	pppoe_0_38_0_d	
Service Name:	HTTP	
External Port:	80	(XX-XX or XX)
Internal IP:	192.168.1.100	
Internal Port:	80	(XX or Blank, 1-65535)
Protocol:	TCP	

☑ Enable this Entry

4. Click View Existing Services, and choose HTTP. The external port, internal port and protocol will be automatically filled with contents. Enter the PC's IP address 192.168.1.100 in the Internal IP field.

5. Click OK to save the settings.

Tips:

1. It is recommended to keep the default settings of Internal Port and Protocol if you are not clear about which port and protocol to use.
2. If the service you want to use is not in the Service Type, you can enter the corresponding parameters manually. You should verify the port number that the service needs.
3. You can add multiple virtual server rules if you want to provide several services in a router. Please note that the External Port cannot be overlapped.

Done!

Users in the Internet can enter http:// *WAN IP* (in this example: http:// 218.18.232.154) to visit your personal website.

Tips:

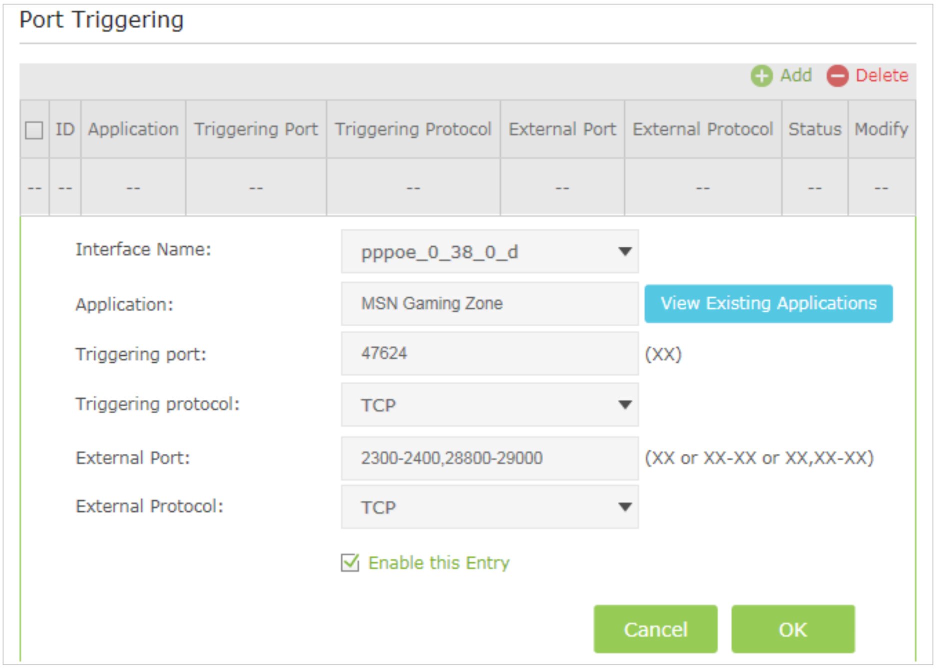
1. WAN IP should be a public IP address. For the WAN IP is assigned dynamically by ISP, it is recommended to apply and register a domain name for the WAN by DDNS, go to *Set Up a Dynamic DNS Service Account* for more information. Then you can use http:// *domain name* to visit the website.
2. If you have changed the default External Port, you should use http:// *WAN IP*: *External Port* or http:// *domain name*: *External Port* to visit the website.

9. 2. Open Ports Dynamically by Port Triggering

Port triggering can specify a triggering port and its corresponding external ports. When a host in the local network initiates a connection to the triggering port, all the external ports will be opened for subsequent connections. The router can record the IP address of the host. When the data from the Internet return to the external ports, the router can forward them to the corresponding host. Port triggering is mainly applied to online games, VoIPs and video players. Common applications include MSN Gaming Zone, Dialpad and Quick Time 4 players, etc.

Follow the steps below to configure the port triggering rules:

1. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
2. Go to Advanced > NAT Forwarding > Port Triggering and click Add.



Port Triggering

□	ID	Application	Triggering Port	Triggering Protocol	External Port	External Protocol	Status	Modify
--	--	--	--	--	--	--	--	--

Interface Name: pppoe_0_38_0_d

Application: MSN Gaming Zone

Triggering port: 47624 (XX)

Triggering protocol: TCP

External Port: 2300-2400,28800-29000 (XX or XX-XX or XX,XX-XX)

External Protocol: TCP

☑ Enable this Entry

3. Click View Existing Applications, and select the desired application. The triggering port and protocol, the external port and protocol will be automatically filled with contents. Here we take application MSN Gaming Zone as an example.
4. Click OK to save the settings.

Tips:

1. You can add multiple port triggering rules according to your network need.
2. If the application you need is not listed in the Existing Applications list, please enter the parameters manually. You should verify the external ports the application uses first and enter them into External Port field according to the format the page displays.

9. 3. Free Applications from Port Restriction by DMZ

When a PC is set to be a DMZ (Demilitarized Zone) host in the local network, it is totally exposed to the Internet. This can realize the unlimited bidirectional communication between internal hosts and external hosts. The DMZ host becomes a virtual server with all ports opened. When you are not clear about which ports to open in some special applications, like IP camera and database software, you can set the PC to be a DMZ host.

Note:

DMZ is more applicable in the situation that users are not clear about which ports to open. When it is enabled, the DMZ host is totally exposed to the Internet, which may bring some potential safety hazard. If DMZ is not in use, please disable it in time.

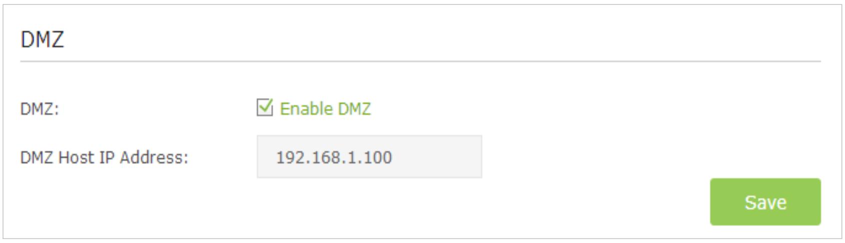
I want to:

Make the home PC join the Internet online game without port restriction.

For example, due to some port restriction, when playing the online games, you can log in normally but cannot join a team with other players. To solve this problem, set your PC as a DMZ with all ports opened.

How can I do that?

1. Assign a static IP address to your PC, for example 192.168.1.100.
2. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
3. Go to Advanced > NAT Forwarding > DMZ and select the check box to enable DMZ.



DMZ

DMZ: ☑ Enable DMZ

DMZ Host IP Address: 192.168.1.100

4. Enter the IP address 192.168.1.100 in the DMZ Host IP Address field.
5. Click Save to save the settings.

Done!

The configuration is completed. You've set your PC to a DMZ host and now you can make a team to game with other players.

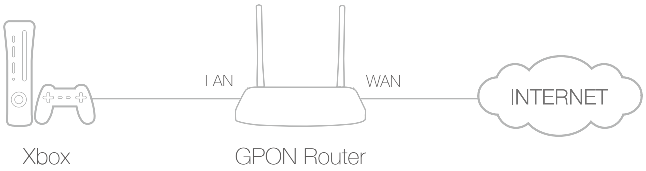
9. 4. Make Xbox Online Games Run Smoothly by UPnP

UPnP (Universal Plug and Play) protocol allows the applications or host devices to automatically find the front-end NAT device and send request to it to open the corresponding ports. With UPnP enabled, the applications or host devices in both sides of NAT device can freely communicate with each other realizing the seamless connection of the network. You may need to enable the UPnP if you want to use applications for multiplayer gaming, peer-to-peer connections, real-time communication (such as VoIP or telephone conference) or remote assistance, etc.

Tips:

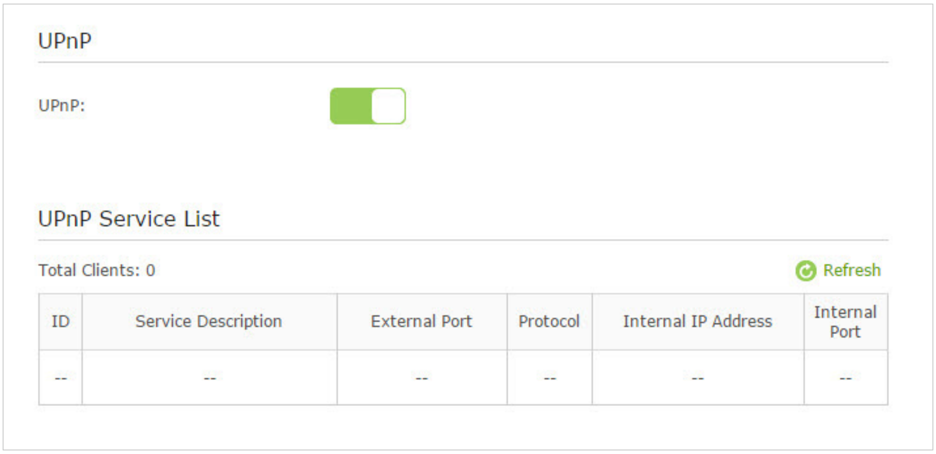
1. UPnP is enabled by default in this router.
2. Only the application supporting UPnP protocol can use this feature.
3. The UPnP feature needs the support of operating system (e.g. Windows Vista/ Windows 7/ Windows 8, etc. Some of operating system need to install the UPnP components).

For example, when you connect your Xbox to the router which has connected to the Internet to play online games, UPnP will send request to the router to open the corresponding ports, which allows the following data penetrating the NAT to transmit. Therefore, you can play Xbox online games without a hitch.



If necessary, you can follow the steps to change the status of UPnP.

1. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router;
2. Go to Advanced > NAT Forwarding > UPnP and toggle on or off according to your needs.



UPnP

UPnP: ●

UPnP Service List

Total Clients: 0

Refresh

ID	Service Description	External Port	Protocol	Internal IP Address	Internal Port
--	--	--	--	--	--

Chapter *10*

Specify Your Network Settings

This chapter introduces how to change the default settings or adjust the basic configuration of the router using the web management page.

This chapter contains the following sections:

- *LAN Settings*
- *IPv6 LAN Settings*
- *Wireless Settings*
- *Set Up a Dynamic DNS Service Account*
- *Create Static Routes*
- *Set up a VPN Connection*
- *Interface Binding*

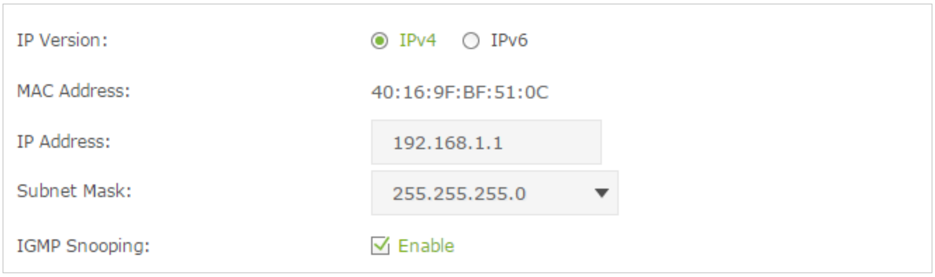
10. 1. LAN Settings

10. 1. 1. Change the LAN IP Address

The router is preset with a default LAN IP 192.168.1.1, which you can use to log in to its web management page. The LAN IP address together with the Subnet Mask also defines the subnet that the connected devices are on. If the IP address conflicts with another device in your local network or your network requires a specific IP subnet, you can change it.

Follow the steps below to change your IP address.

1. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
2. Go to Advanced > Network > LAN Settings page and select IPv4.



IP Version: ● IPv4 ○ IPv6

MAC Address: 40:16:9F:BF:51:0C

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

IGMP Snooping: ☑ Enable

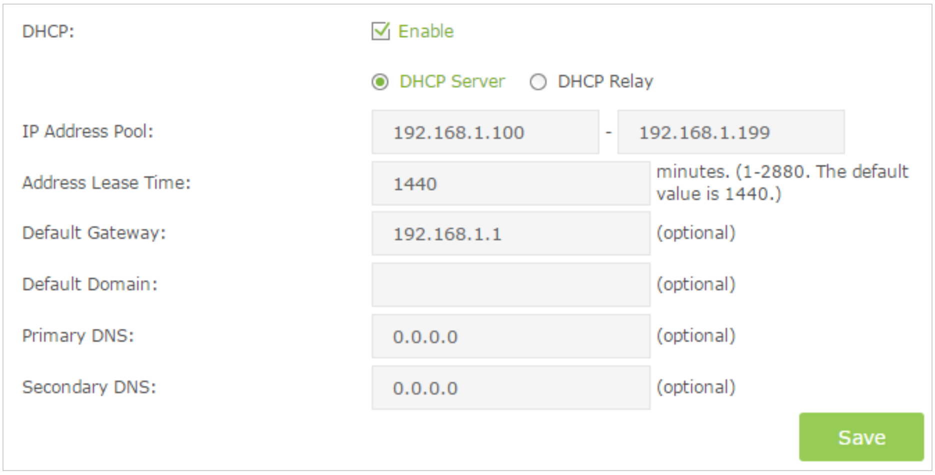
3. Type in a new IP Address appropriate to your needs.
4. Select the Subnet Mask from the drop-down list. The subnet mask together with the IP address identifies the local IP subnet.
5. Keep IGMP Snooping as enabled by default. IGMP snooping is the process of listening to IGMP (Internet Group Management Protocol) network traffic. The function prevents hosts on a local network from receiving traffic for a multicast group they have not explicitly joined.
6. You can configure the router's Second IP and Subnet Mask for LAN interface through which you can also access the web management page.
7. Leave the rest of the default settings as they are.
8. Click Save to make the settings effective.

10. 1. 2. Use the GPON Router as a DHCP Server

You can configure the router to act as a DHCP server to assign IP addresses to its clients. To use the DHCP server function of the router, you must configure all computers on the LAN to obtain an IP Address automatically.

Follow the steps below to configure DHCP server.

1. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
2. Go to Advanced > Network > LAN Settings page and select IPv4.



DHCP: ☑ Enable

● DHCP Server ○ DHCP Relay

IP Address Pool: 192.168.1.100 - 192.168.1.199

Address Lease Time: 1440 minutes. (1-2880. The default value is 1440.)

Default Gateway: 192.168.1.1 (optional)

Default Domain: (optional)

Primary DNS: 0.0.0.0 (optional)

Secondary DNS: 0.0.0.0 (optional)

3. Select DHCP to enable the DHCP function and select DHCP Server.
4. Specify the IP Address Pool, the start address and end address must be on the same subnet with LAN IP. The router will assign addresses within this specified range to its clients. It is from 192.168.1.100 to 192.168.1.199 by default.
5. Enter a value for the Address Lease Time. The Address Lease Time is the amount of time in which a DHCP client can lease its current dynamic IP address assigned by the router. After the dynamic IP address expires, the user will be automatically assigned a new dynamic IP address. The default is 1440 minutes.
6. Keep the rest of the settings as default and click Save.

Note:

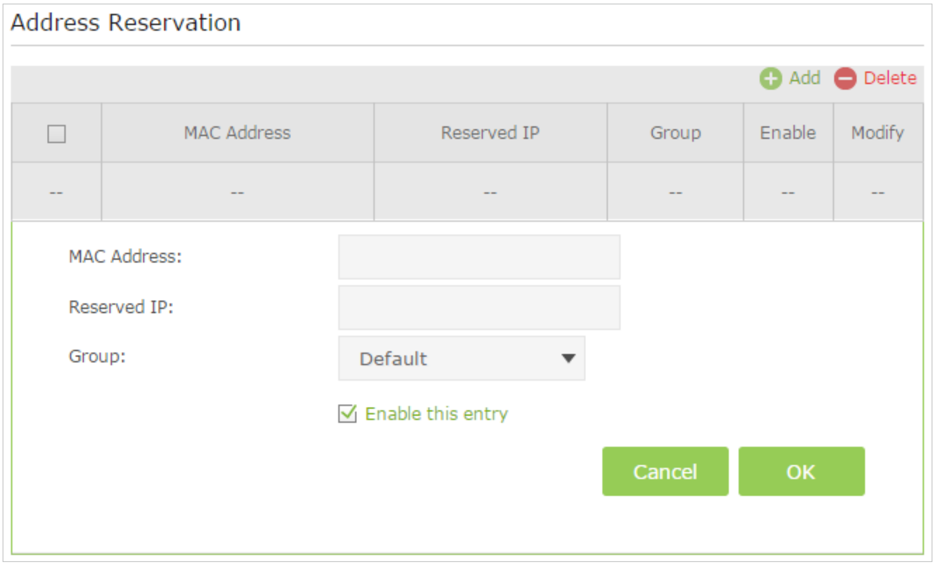
1. The router can be configured to work as a DHCP Relay. A DHCP relay is a computer that forwards DHCP data between computers that request IP addresses and the DHCP server that assigns the addresses. Each of the device's interfaces can be configured as a DHCP relay. If it is enabled, the DHCP requests from local PCs will be forwarded to the DHCP server that runs on WAN side.
2. You can also appoint IP addresses within a specified range to devices of the same type by using the Condition Pool feature. For example, you can assign IP addresses within the range (192.168.1.50 to192.168.1.80) to Camera devices, thus facilitating the network management. Enable the DHCP feature and configure the parameters according to your actual situation on Advanced > Network > LAN Settings page.

10. 1. 3. Reserve LAN IP Addresses

You can view and add a reserved address for a client. When you specify an IP address for a device on the LAN, that device will always receive the same IP address each time when it accesses the DHCP server. If there are some devices in the LAN that require permanent IP addresses, please configure Address Reservation on the router for the purpose.

Follow the steps below to reserve an IP address for your device.

1. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
2. Go to Advanced > Network > LAN Settings page and select IPv4.
3. Scroll down to locate the Address Reservation table and click Add to add an address reservation entry for your device.



Address Reservation

□	MAC Address	Reserved IP	Group	Enable	Modify
--	--	--	--	--	--

MAC Address:

Reserved IP:

Group: Default

☑ Enable this entry

4. Enter the MAC address of the device for which you want to reserve IP address.
5. Specify the IP address which will be reserved by the router.
6. Check to Enable this entry and click OK to make the settings effective.

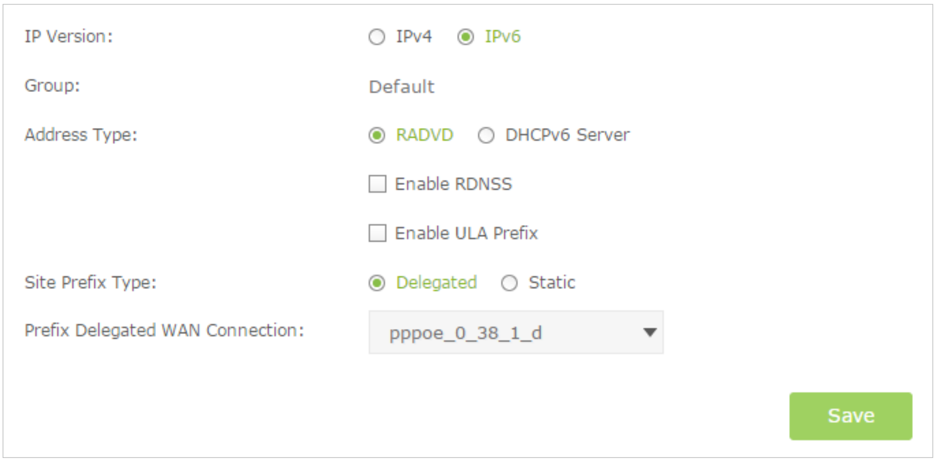
10. 2. IPv6 LAN Settings

Based on the IPv6 protocol, the router provides two ways to assign IPv6 LAN addresses:

- Configure the RADVD (Router Advertisement Daemon) address type
- Configure the DHCPv6 Server address type

10. 2. 1. Configure the RADVD Address Type

1. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
2. Go to Advanced > Network > LAN Settings.
3. Select IPv6 to configure IPv6 LAN parameters.



IP Version:	○ IPv4 ● IPv6
Group:	Default
Address Type:	● RADVD ○ DHCPv6 Server □ Enable RDNSS □ Enable ULA Prefix
Site Prefix Type:	● Delegated ○ Static
Prefix Delegated WAN Connection:	pppoe_0_38_1_d ▼

1) Select the RADVD address type to make the router assign IPv6 address prefixes to hosts.

Note:
Do not select the Enable RDNSS and Enable ULA Prefix check boxes unless required by your ISP. Otherwise you may not be able to access the IPv6 network. For more information about RDNSS and ULA Prefix, contact our technical support.

2) Keep Site Prefix Type as the default value Delegated. If your ISP has provided a specific IPv6 site prefix, select Static and enter the prefix.

3) Keep Prefix Delegated WAN Connection as the default value.

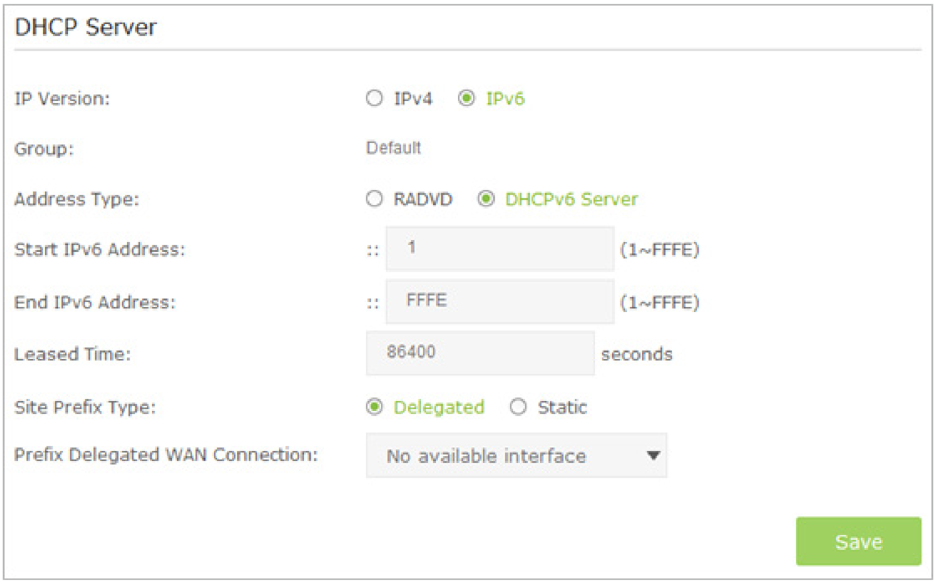
4. Click Save to make the settings effective.

10. 2. 2. Configure the DHCPv6 Server Address Type

1. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.

2. Go to Advanced > Network > LAN Settings.

3. Select IPv6 to configure IPv6 LAN parameters.



DHCP Server

IP Version:	○ IPv4 ● IPv6
Group:	Default
Address Type:	○ RADVD ● DHCPv6 Server
Start IPv6 Address:	:: 1 (1~FFFE)
End IPv6 Address:	:: FFFE (1~FFFE)
Leased Time:	86400 seconds
Site Prefix Type:	● Delegated ○ Static
Prefix Delegated WAN Connection:	No available interface ▼

1) Select the DHCPv6 Server address type to make the router assign IPv6 addresses to hosts.

2) Specify the Start/End IPv6 Address for the IPv6 suffixes. The router will generate IPv6 addresses within the specified range.

3) Keep Leased Time as the default value.

4) Keep Site Prefix Type as the default value Delegated. If your ISP has provided a specific IPv6 site prefix, select Static and enter the prefix.

5) Keep Prefix Delegated WAN Connection as the default value.

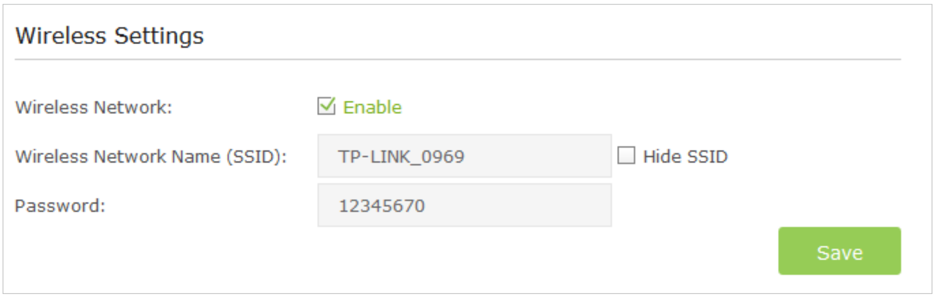
4. Click Save to make the settings effective.

10. 3. Wireless Settings

10. 3. 1. Specify Basic Wireless Settings

The router's wireless network name (SSID) and password, and security option are preset in the factory. The preset SSID and password can be found on the product label. You can customize the wireless settings according to your needs.

Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router. Go to Basic > Wireless page.



Wireless Settings

Wireless Network: ☑ Enable

Wireless Network Name (SSID): TP-LINK_0969 □ Hide SSID

Password: 12345670

➢ To enable or disable the wireless function:

Enable the Wireless Network. If you don't want to use the wireless function, just deselect the box. If you disable the wireless function, all the wireless settings won't be effective.

➢ To change the wireless network name (SSID) and wireless password:

Enter a new SSID using up to 32 characters. The value is case-sensitive.

Note:

If you use a wireless device to change the wireless settings, you will be disconnected after the new settings are effective. Please write down the new SSID and password for future use.

➢ To hide SSID:

Select Hide SSID, and your SSID will not broadcast. Your SSID won't display on your wireless device when you scan for local wireless network list on your wireless device and you need to manually join the network.

➢ To change the mode or channel:

Go to Advanced > Wireless >Wireless Settings page.

Mode: Select the desired mode.

- 802.11n only: Select only if all of your wireless clients are 802.11n devices.
- 802.11gn mixed: Select if you are using both 802.11g and 802.11n wireless clients.
- 802.11bgn mixed: Select if you are using a mix of 802.11b, 11g, and 11n wireless clients.

  Note: When 802.11n only mode is selected, only 802.11n wireless stations can connect to the router. It is strongly recommended that you select 802.11bgn mixed, and all of 802.11b, 802.11g, and 802.11n wireless stations can connect to the router.

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

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.

➢ To change the security option:

1. Go to Advanced > Wireless >Wireless Settings page.
2. Select an option from the Security drop-down list. The router provides four options, None, WPA/WPA2 Personal (Recommended), WPA/WPA2 Enterprise, WEP. WPA2 uses the newest standard and the security level is the highest. We don't recommend that you change the default settings unless necessary.

10. 3. 2. Use WPS for Wireless Connection

You can use WPS (Wi-Fi Protected Setup) feature to add a new wireless device to your existing network quickly.

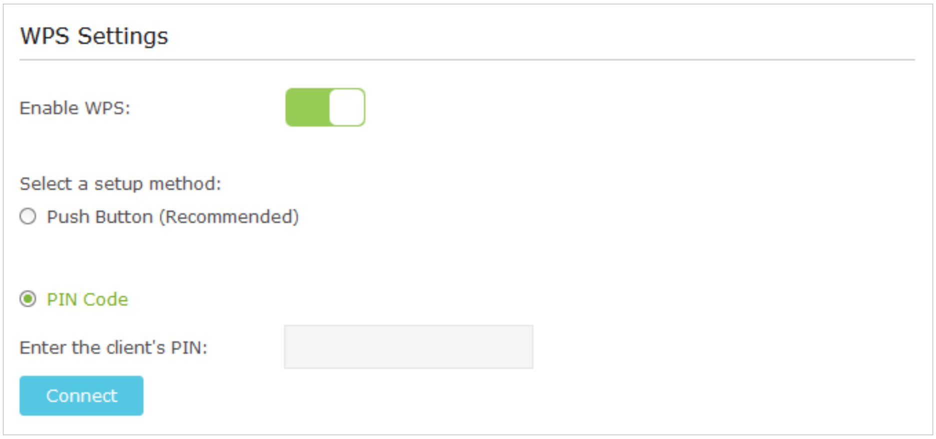
Method 1 Use the WPS Button

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

1. Press the WPS button on the router for 1 second.
2. Press the WPS button of the client device directly.
3. The WPS LED flashes for about 2 minutes during the WPS process.
4. When the WPS LED is on, the client device has successfully connected to the router.

Method 2 Enter the client device's PIN on the router

1. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
2. Go to Advanced > Wireless > WPS page.



WPS Settings

Enable WPS:

Select a setup method:

○ Push Button (Recommended)

● PIN Code

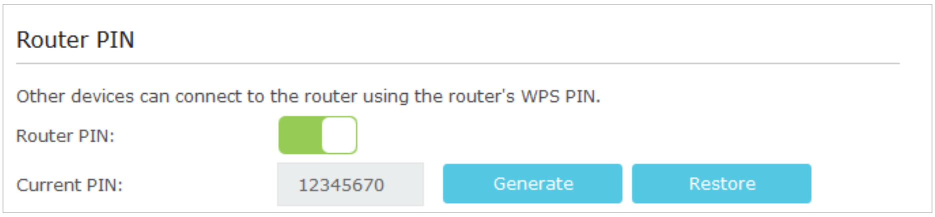
Enter the client's PIN:

3. Keep the default WPS status as Enabled and select the PIN Code radio button.
4. Enter the client device's PIN in the field on the above WPS screen. Then click the Connect button.
5. Connect successfully will appear on the above screen, which means the client device has successfully connected to the router.

Method 3 Enter the router's PIN on your client device

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

1. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
2. Go to Advanced > Wireless > WPS page.



Router PIN

Other devices can connect to the router using the router's WPS PIN.

Router PIN: ●

Current PIN: 12345670

3. Keep the Router's PIN status as enabled. Take a note of the Current PIN of the router. You can also click the Generate button to get a new PIN.
4. On the client device, enter the router's PIN. (The default PIN is also printed on the label of the router.)
5. The WPS LED flashes for about two minutes during the WPS process.
6. When the WPS LED is on, the client device has successfully connected to the router.

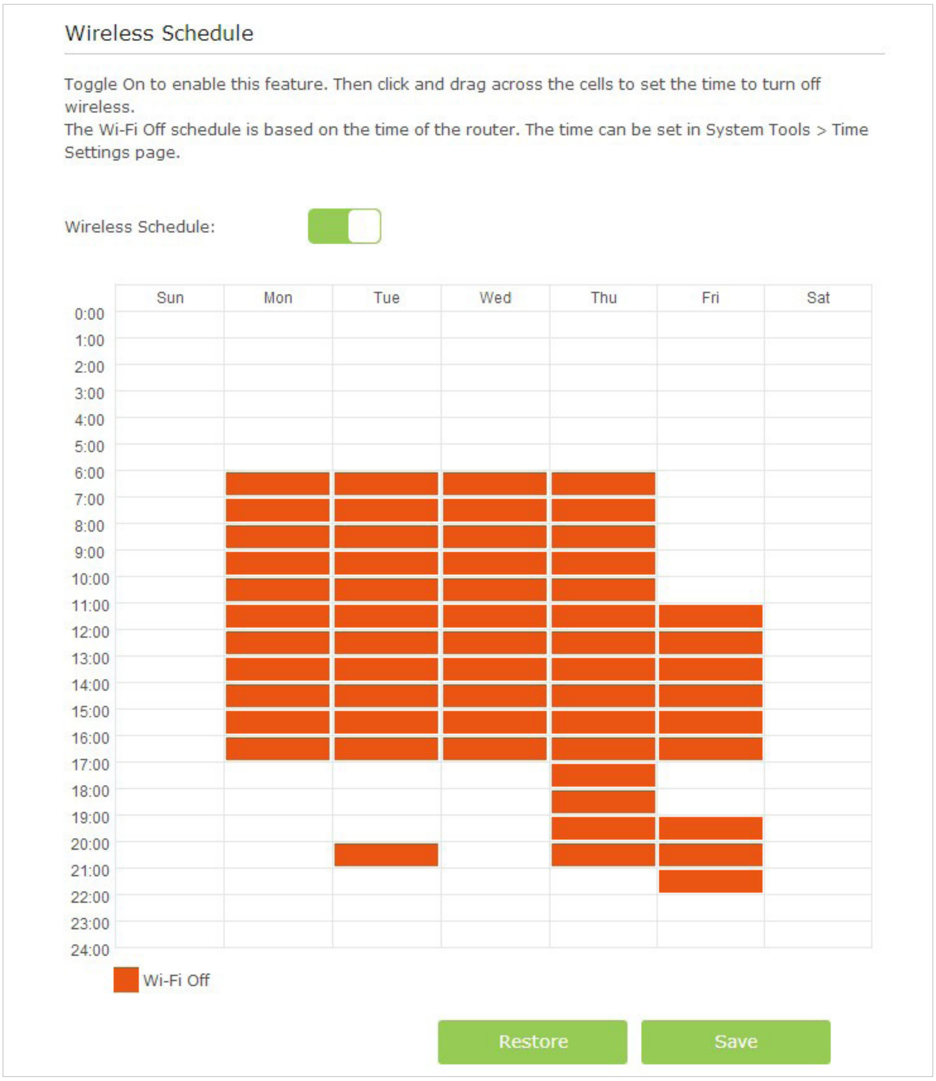
Note:

1. The WPS LED on the router will light on for 30 seconds if the device has been successfully added to the network.
2. The WPS function cannot be configured if the wireless function of the router is disabled. Please make sure the wireless function is enabled before configuring the WPS.

10. 3. 3. Schedule Your Wireless Function

You can automatically turn off your wireless network at the time when you do not need the wireless connection.

1. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
2. Go to Advanced > Wireless > Wireless Schedule page.
3. Toggle on the button to enable the Wireless Schedule feature.



Wireless Schedule

Toggle On to enable this feature. Then click and drag across the cells to set the time to turn off wireless.
The Wi-Fi Off schedule is based on the time of the router. The time can be set in System Tools > Time Settings page.

Wireless Schedule: ●

	Sun	Mon	Tue	Wed	Thu	Fri	Sat
0:00							
1:00							
2:00							
3:00							
4:00							
5:00							
6:00		🟥	🟥	🟥	🟥		
7:00		🟥	🟥	🟥	🟥		
8:00		🟥	🟥	🟥	🟥		
9:00		🟥	🟥	🟥	🟥		
10:00		🟥	🟥	🟥	🟥		
11:00		🟥	🟥	🟥	🟥	🟥	
12:00		🟥	🟥	🟥	🟥	🟥	
13:00		🟥	🟥	🟥	🟥	🟥	
14:00		🟥	🟥	🟥	🟥	🟥	
15:00		🟥	🟥	🟥	🟥	🟥	
16:00		🟥	🟥	🟥	🟥	🟥	
17:00					🟥		
18:00					🟥		
19:00					🟥	🟥	
20:00			🟥		🟥	🟥	
21:00						🟥	
22:00							
23:00							
24:00							

🟥 Wi-Fi Off

4. Set the time. Drag the cursor to cover the time area and click Save to make the settings effective. The selected time will be in red.

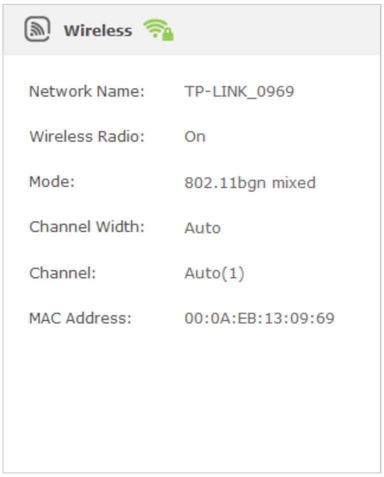
Note:

1. Please make sure that the time of the router is correct before using this function. For more details, refer to *Set System Time*.
2. The wireless LED will turn off if the wireless network is disabled.
3. The wireless network will be automatically turned on after the time period you set.

10. 3. 4. View Wireless Information

➢ **To view the detailed wireless network settings:**

1. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
2. Go to Advanced > Status page. You can see the Wireless box.



Network Name: TP-LINK_0969

Wireless Radio: On

Mode: 802.11bgn mixed

Channel Width: Auto

Channel: Auto(1)

MAC Address: 00:0A:EB:13:09:69

Tips: You can also see the wireless details by clicking the router icon on Basic> Network Map.

➢ **To view the detailed information of the connected wireless clients:**

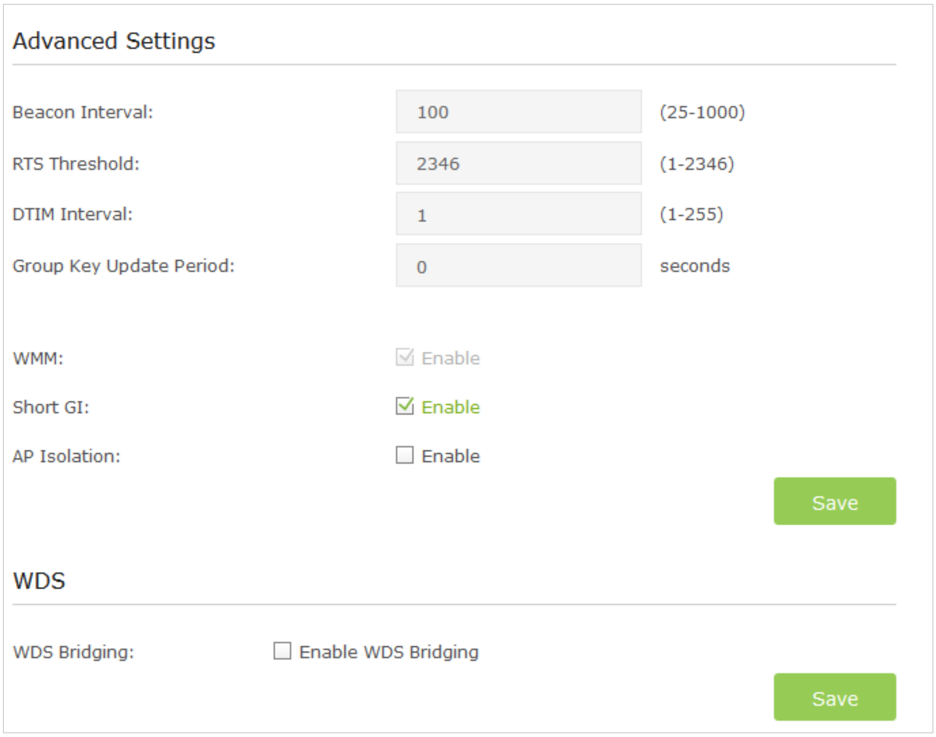
1. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
2. Go to Advanced > Wireless > Statistics page.
3. You can view the detailed information of the wireless clients, including its connection type and security option as well as the packets transmitted.

Tips: You can also see the wireless details by clicking the wireless clients icon on Basic> Network Map.

10. 3. 5. Advanced Wireless Settings

Advanced wireless settings are for those who have a network concept. If you are not familiar with the settings on this page, it's strongly recommended that you keep the provided default values; otherwise it may result in lower wireless network performance.

1. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
2. Go to Advanced > Wireless > Advanced Settings page.



Advanced Settings

Beacon Interval:	100	(25-1000)
RTS Threshold:	2346	(1-2346)
DTIM Interval:	1	(1-255)
Group Key Update Period:	0	seconds
WMM:	☑ Enable	
Short GI:	☑ Enable	
AP Isolation:	□ Enable	

WDS

WDS Bridging: □ Enable WDS Bridging

- Beacon Interval: Enter a value between 25 and 1000 in milliseconds to determine the duration between which beacon packets are broadcast by the router to synchronize the wireless network. The default is 100 milliseconds.
- RTS Threshold: Enter a value between 1 and 2346 to determine the packet size of data transmission through the router. By default, the RTS (Request to Send) Threshold size is 2346. If the packet size is greater than the preset threshold, the router sends Request to Send frames to a particular receiving station and negotiates the sending of a data frame, or else the packet will be sent immediately.
- DTIM Interval: Enter a value between 1 and 255 to determine the interval of the Delivery Traffic Indication Message (DTIM). 1 indicates the DTIM Interval is the same as Beacon Interval.
- Group Key Update Period: Enter the number of seconds to control the time interval for the encryption key automatic renewal. The default is 0, indicating no key renewal.
- WMM: This feature guarantees the packets with high-priority messages being transmitted preferentially. WMM is enabled compulsively under 802.11n or 802.11ac mode. It is strongly recommended to enable WMM.
- Short GI: This feature is enabled by default and recommended to increase the data capacity by reducing the Guard Interval (GI) time.
- AP Isolation: Select this check box to enable the AP Isolation feature that allows you to confine and restrict all wireless devices on your network from interacting with each other, but still able to access the Internet. AP isolation is disabled by default.

- WDS Bridging: Select this check box to enable the WDS (Wireless Distribution System) Bridging feature to allow the router to bridge with another access point (AP) in a wireless local area network (WLAN). Refer to *Appendix: Troubleshooting* for detailed instructions.

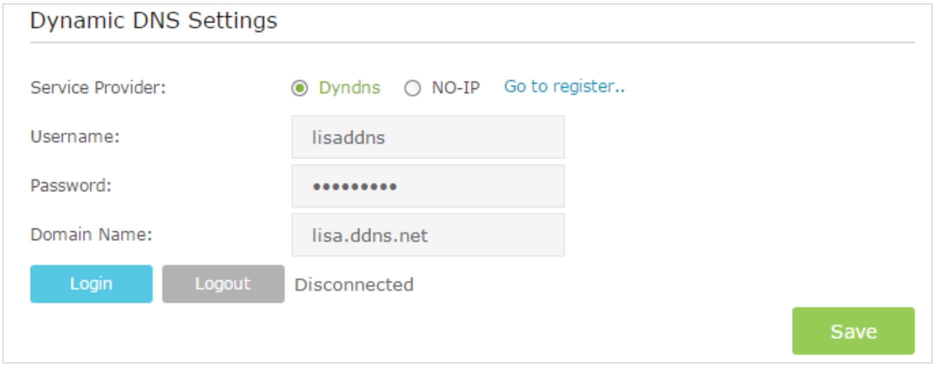
10. 4. Set Up a Dynamic DNS Service Account

Most ISPs (Internet service providers) assign a dynamic IP address to the router and you can use this IP address to access your router remotely. However, the IP address can change any time and you don't know when it changes. In this case, you might need the DDNS (Dynamic Domain Name Server) feature on the router to allow you and your friends to access your router and local servers (FTP, HTTP, etc.) using domain name, in no need of checking and remembering the IP address.

Note: DDNS does not work if the ISP assigns a private WAN IP address (such as 192.168.1.x) to the router.

To set up DDNS, please follow the instructions below:

1. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
2. Go to Advanced > Network> Dynamic DNS.
3. Select the DDNS service provider (Dyndns or NO-IP). If you don't have a DDNS account, select a service provider and click Go to register.



Dynamic DNS Settings

Service Provider: ● Dyndns ○ NO-IP Go to register..

Username: lisaddns

Password: ●●●●●●●●●

Domain Name: lisa.ddns.net

Disconnected

4. Enter the username, password and domain name of the account (such as lisa.ddns.net).
5. Click Login and Save.

Tips: If you want to use a new DDNS account, please log out first, then log in with the new account.

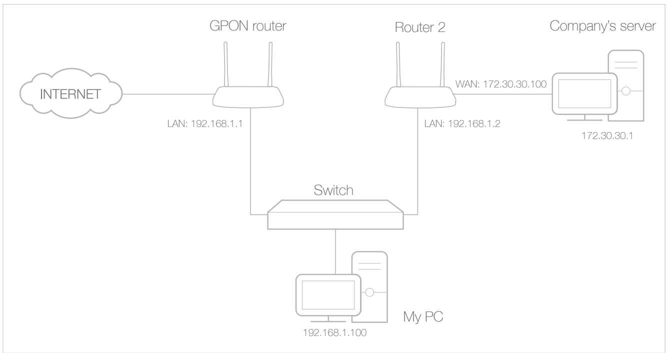
10. 5. Create Static Routes

A static route is a pre-determined path that network information must travel to reach a specific host or network. Data from one point to another will always follow the same path regardless of other considerations. Normal Internet usage does not require this setting to be configured.

I want to:

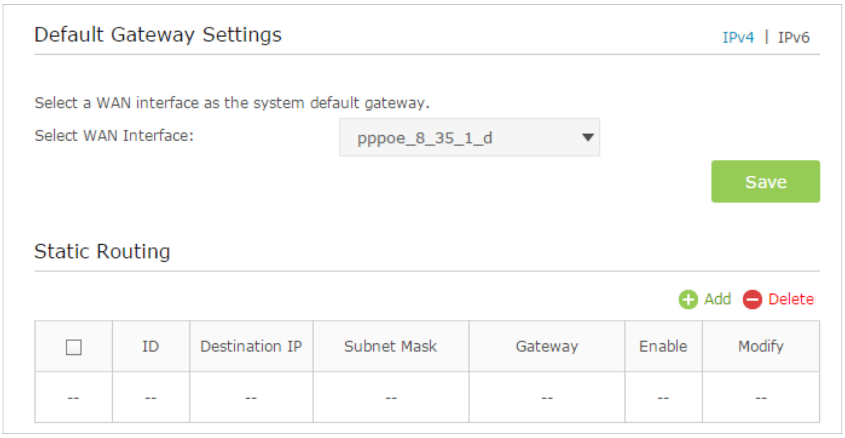
Visit multiple networks and multiple servers at the same time.

For example, in a small office, my PC can surf the Internet, but I also want to visit my company's server. Now I have a switch and another router. I connect the devices as shown in the following figure so that the physical connection between my PC and my company's server is achieved. To surf the Internet and visit my company's network at the same time, I need to configure the static routing.



How can I do that?

1. Make sure the routers use different LAN IP addresses on the same subnet. Disable Router 2's DHCP function.
2. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
3. Go to Advanced > Network > Advanced Routing. Select your current WAN Interface and click Save.


Default Gateway Settings

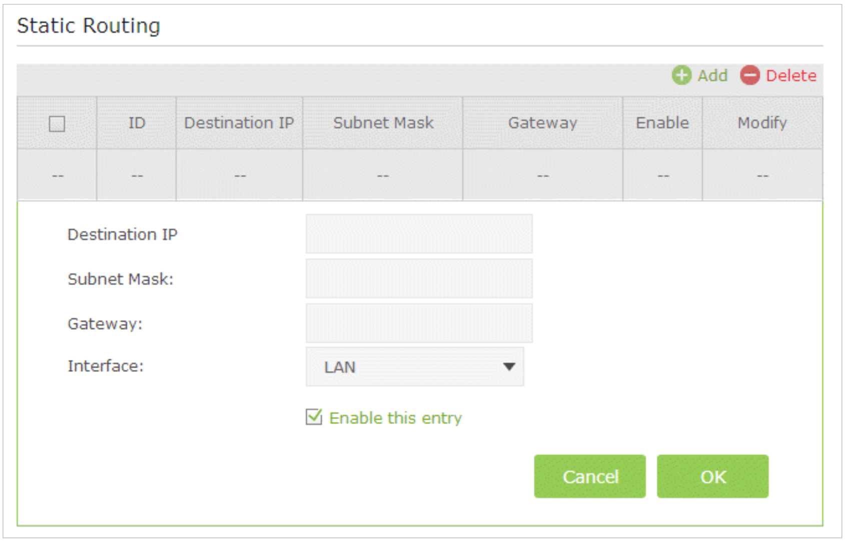
Select a WAN interface as the system default gateway.

Select WAN Interface: pppoe_8_35_1_d

Static Routing

□	ID	Destination IP	Subnet Mask	Gateway	Enable	Modify
--	--	--	--	--	--	--

4. Click Add to add a new static routing entry. Finish the settings according to the following explanations:



Static Routing

☐	ID	Destination IP	Subnet Mask	Gateway	Enable	Modify
--	--	--	--	--	--	--

Destination IP	
Subnet Mask:	
Gateway:	
Interface:	LAN

☑ Enable this entry

- Destination IP: The destination IP address that you want to assign to a static route. This IP address cannot be on the same subnet with the WAN IP or LAN IP of the router. In the example, the IP address of the company network is the destination IP address, so here enters 172.30.30.1.
- Subnet Mask: Determines the destination network with the destination IP address. If the destination is a single IP address, enter 255.255.255.255; otherwise, enter the subnet mask of the corresponding network IP. In the example, the destination network is a single IP, so here enters 255.255.255.255.
- Gateway: The IP address of the gateway device to which the data packets will be sent. This IP address must be on the same subnet with the router's IP which sends out the data. In the example, the data packets will be sent to the LAN port of Router 2 and then to the Server, so the default gateway should be 192.168.1.2.
- Interface: Determined by the port (WAN/LAN) that sends out the data packets. In the example, the data is sent to the gateway through the LAN port, so LAN should be selected.

5. Select the check box to enable this entry.

6. Click OK to save the settings.

Done!

Open a web browser on your PC. Enter the company server's IP address to visit the company network.

10. 6. Set up a VPN Connection

VPN (Virtual Private Network) is a private network established across the public network, generally via the Internet. However, the private network is a logical network without any physical network lines, so it is called Virtual Private Network.

With the wide application of the Internet, more and more data are needed to be shared through the Internet. Connecting the local network to the Internet directly, though can allow the data exchange, will cause the private data to be exposed to all the users on the Internet.

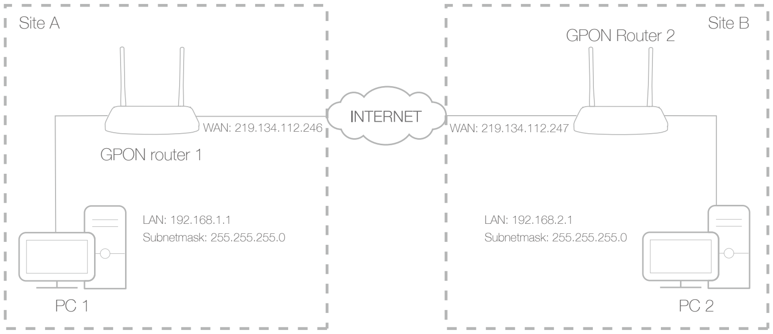
The VPN (Virtual Private Network) technology is developed and used to establish the private network through the public network, which can provides a secure communication to a remote computer or remote network, and guarantee a secured data exchange. IPSec is one of the major implementations of VPNs.

I want to:

Establish an IPSec VPN tunnel to connect two LANs via Internet so that the hosts in different remote LANs are able to communicate with each other as if they are in the same LAN.

For example, I am the network administrator of a regional office, I need to let my office staff visit the headquarter's servers and resources, and vice versa. I know that the router in my office and the device in headquarter both support IPSec VPN feature, so I decide to set up a VPN connection with the headquarter office.

The following diagram is a typical VPN topology. Here Site A refers to regional office's network (local network). And Site B refers to the headquarter's network (remote network) which I want to connect.

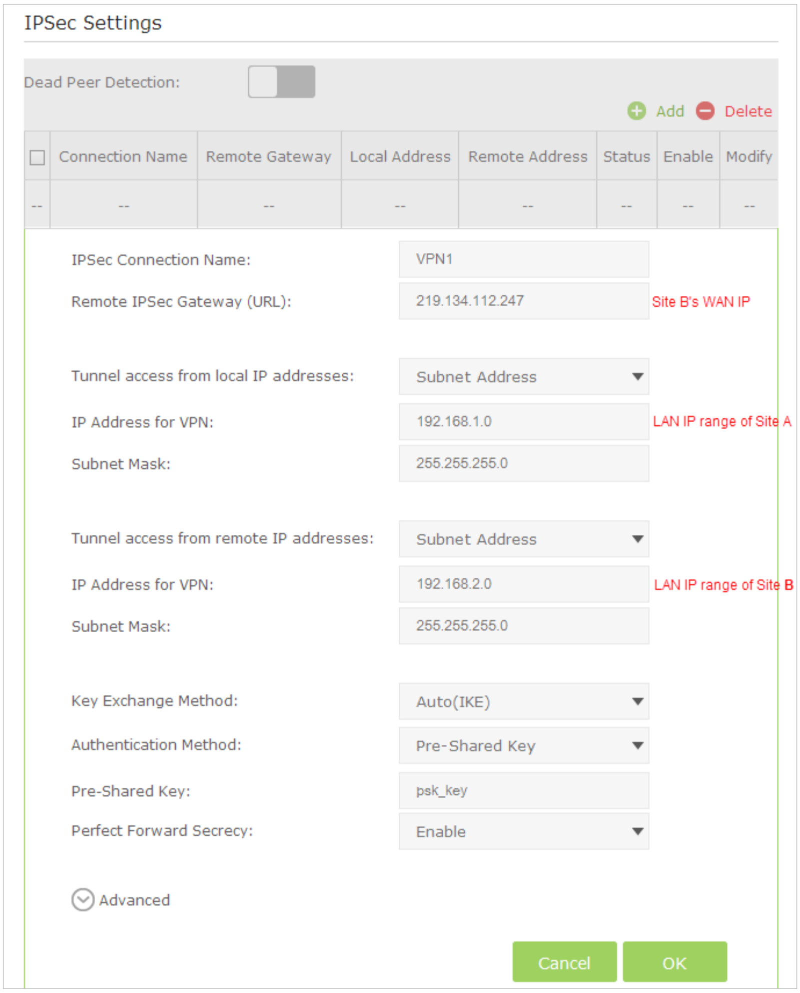


How can I do that?

1. Make sure of the topology you want to build and record site A (local network) and site B (remote network)'s LAN IP and WAN IP.
2. Configuration on site A (local network).

1) Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.

2) Go to Advanced > Network > IPSec VPN to open the configuration page. Click Add to set up a VPN tunnel.



IPSec Settings

Dead Peer Detection:

Add Delete

□	Connection Name	Remote Gateway	Local Address	Remote Address	Status	Enable	Modify
--	--	--	--	--	--	--	--

IPSec Connection Name: VPN1

Remote IPSec Gateway (URL): 219.134.112.247 Site B's WAN IP

Tunnel access from local IP addresses: Subnet Address

IP Address for VPN: 192.168.1.0 LAN IP range of Site A

Subnet Mask: 255.255.255.0

Tunnel access from remote IP addresses: Subnet Address

IP Address for VPN: 192.168.2.0 LAN IP range of Site B

Subnet Mask: 255.255.255.0

Key Exchange Method: Auto(IKE)

Authentication Method: Pre-Shared Key

Pre-Shared Key: psk_key

Perfect Forward Secrecy: Enable

3) In the IPSec Connection Name column, specify a name.

4) In the Remote IPSec Gateway (URL) column, Enter Site B's WAN IP address.

5) Configure Site A's LAN.

In the Tunnel access from local IP addresses column, here we take Subnet Address as an example. Then input the LAN IP range of Site A in the IP Address for VPN column, and input Subnet Mask of Site A.

6) Configure Site B's LAN.

In the Tunnel access from local IP addresses column, here we take Subnet Address as an example. Then input the LAN IP range of Site B in the IP Address for VPN column, and input Subnet Mask of Site B.

7) Select the Key Exchange Method for the policy. We select Auto(IKE) here.

8) Enter the Pre-Shared Key for IKE authentication. Then keep Perfect Forward Secrecy enabled.

Note:

Make sure Site A and Site B use the same key.

9) Leave the Advanced Settings as default value. Then click OK to save.

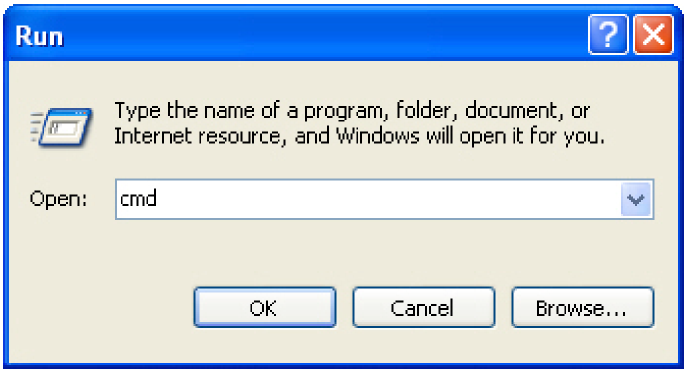
3. Configuration on Site B (remote network). Refer to step 2 configuration on Site A and make sure that Site A and Site B use the same pre-shared keys and Perfect Forward Secrecy settings.

4. The Status column will change to UP if the VPN connection has been set up successfully.

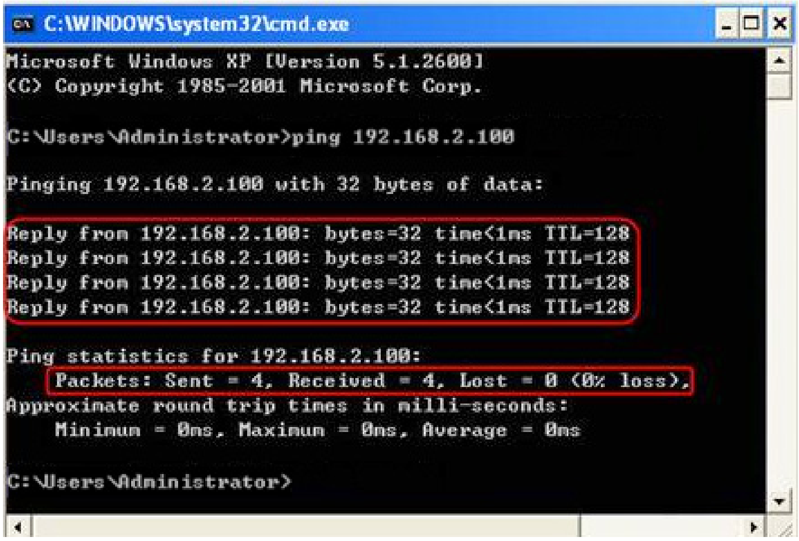
5. Check the VPN connection. You can ping site B' LAN IP from your computer in site A to verify that the IPSec VPN connection is set up correctly.

Tips: To check the VPN connection, you can do the following.

1. On the host in Site A, press [Windows Logo] + [R] to open Run dialog. Input "cmd" and hit OK.


Run
?
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
cmd
OK
Cancel
Browse...

2. In the CLI window, type in "ping 192.168.2.x" ("192.168.2.x" can be IP address of any host in Site B). Then press [Enter].



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

C:\Users\Administrator>ping 192.168.2.100

Pinging 192.168.2.100 with 32 bytes of data:

Reply from 192.168.2.100: bytes=32 time<1ms TTL=128
Reply from 192.168.2.100: bytes=32 time<1ms TTL=128
Reply from 192.168.2.100: bytes=32 time<1ms TTL=128
Reply from 192.168.2.100: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>
```

3. If Ping proceeds successfully (gets replies from host in Site B), the IPSec connection is working properly now.

Done! Now IPSec VPN is implemented to establish a connection.

Note:

1. The product supports a maximum of ten simultaneous connections.
2. If one of the site has been offline for a while, for example, if Site A has been disconnected, on Site B you need to click Disable and then click Enable after Site A back on line in order to re-establish the IPSec tunnel.

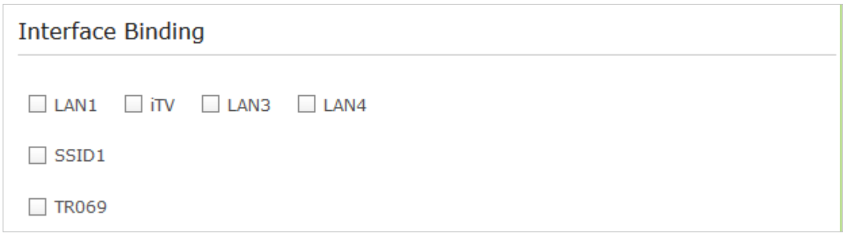
10. 7. Interface Binding

I want to: Bind some LAN ports to certain devices or functions so that these devices or functions can access the Internet without interference of other devices or functions.

For example, in my house, my IPTV is connected to LAN1. I want only my IPTV to access the Internet via LAN1 to ensure high quality while keep all other devices' access to the Internet.

How can I do that?

1. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
2. Go to Advanced > Network > Internet. Find your current connection and click the ☑ icon.
3. Scroll down to locate the Interface Binding section.



Interface Binding

□ LAN1 □ iTV □ LAN3 □ LAN4

□ SSID1

□ TR069

4. Check the boxes of LAN1 and iTPV.

Note: If your current connection is a bridge connection, you may need to Disable DHCP service for the bound LAN(s).

5. Click OK to save the settings.

Done!

Now your IPTV is bound to LAN1 and will not be interfered by other devices or functions!

Chapter 11

Administrate Your Network

This chapter introduces how to change the system settings and administrate your router's network.

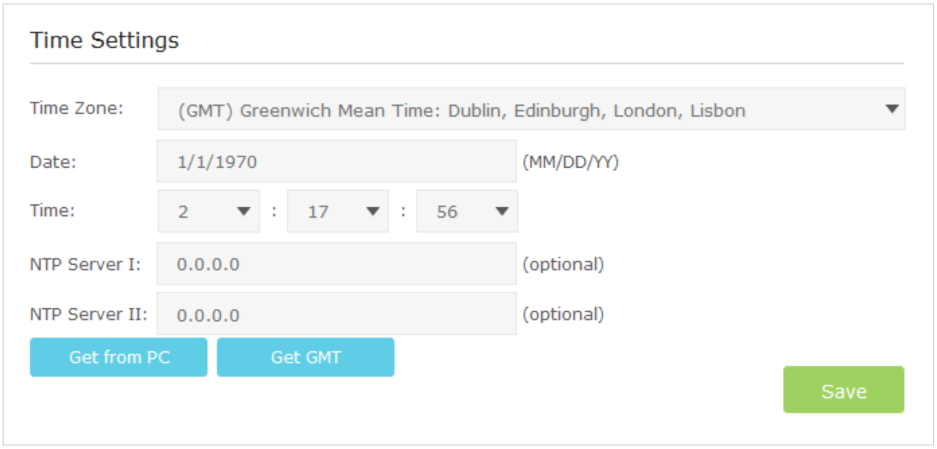
This chapter contains the following sections:

11. 1. Set System Time

System time is the time displayed while the router is running. The system time you configure here will be used for other time-based functions like Parental Controls and Wireless Schedule. You can manually set how to get the system time.

Follow the steps below to set your system time.

1. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
2. Go to Advanced > System Tools > Time Settings page.



Time Settings

Time Zone: (GMT) Greenwich Mean Time: Dublin, Edinburgh, London, Lisbon

Date: 1/1/1970 (MM/DD/YY)

Time: 2 : 17 : 56

NTP Server I: 0.0.0.0 (optional)

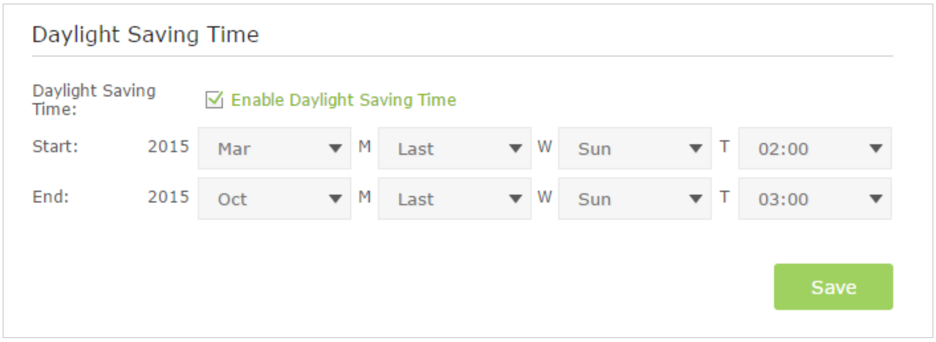
NTP Server II: 0.0.0.0 (optional)

3. Configure the system time using the following methods:

   Manually: Select your time zone and enter your local time.

   Get from PC: Click this button if you want to use the current managing PC's time.

   Get GMT: Click this button if you want to get time from the Internet. Make sure your router can access the Internet before you select this way to get system time.
4. Click Save.
5. After setting the system time, you can set Daylight Saving Time according to your needs. Tick the checkbox to enable Daylight Saving Time, set the start and end time and then click Save to make the settings effective.



Daylight Saving Time

Daylight Saving Time: ☑ Enable Daylight Saving Time

Start: 2015 Mar M Last W Sun T 02:00

End: 2015 Oct M Last W Sun T 03:00

11. 2. Update the Firmware

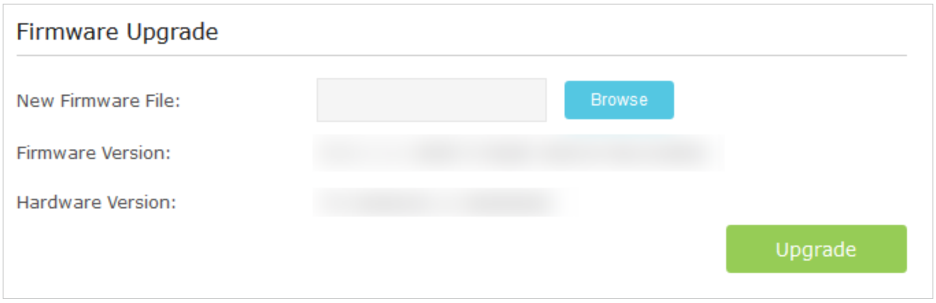
TP-LINK is dedicated to improving and richening the product features, giving you a better network experience. The latest firmware will be released at TP-LINK official website, you can download it from the Support page of our website *http://www.tp-link.com* for free.

Note:

1. Make sure that you have a stable connection between the router and your computer. It is NOT recommended to upgrade the firmware wirelessly.
2. Make sure you remove any USB storage device connected to the router before the firmware upgrade to prevent data loss.
3. Back up your router configuration before upgrading the firmware.
4. Do NOT turn off the router during the firmware upgrade.

Follow the steps below to update the firmware to the latest.

1. Download the latest firmware file for the router from our website *http://www.tp-link.com*.
2. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
3. Go to Advanced > System Tools > Firmware Upgrade.
4. Make sure the downloaded firmware file matches with the Hardware Version.
5. Click Browse to locate the downloaded new firmware file, and click Upgrade.



Firmware Upgrade

New Firmware File:

Firmware Version:

Hardware Version:

6. Wait a few moments for the upgrading and rebooting.

11. 3. Back Up and Restore Configuration Settings

The configuration settings are stored as a configuration file in the router. You can back up the configuration file to your computer for future use and restore the router to a previous settings from the backup file when needed. Moreover, if needed you can erase the current settings and reset the router to the default factory settings.

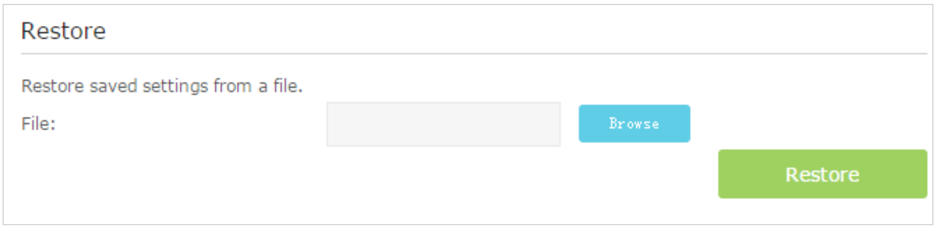
To back up configuration settings

1. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.

2. Click Advanced > System Tools > Backup & Restore page.
3. Click Backup to save a copy of the current settings to your local computer. A conf.bin file will be stored to your computer.

To restore configuration settings

1. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
2. Click Advanced > System Tools > Backup & Restore page.



Restore

Restore saved settings from a file.

File:

3. Click Browse to locate the previous backup configuration file, and click Restore.
4. Wait for the restoring and then the router will automatically reboot.

To reset the router to factory default settings

1. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
2. Click Advanced > System Tools > Backup & Restore page.
3. Click Factory Restore to reset the router.
4. Wait for the resetting and then the router will automatically reboot.

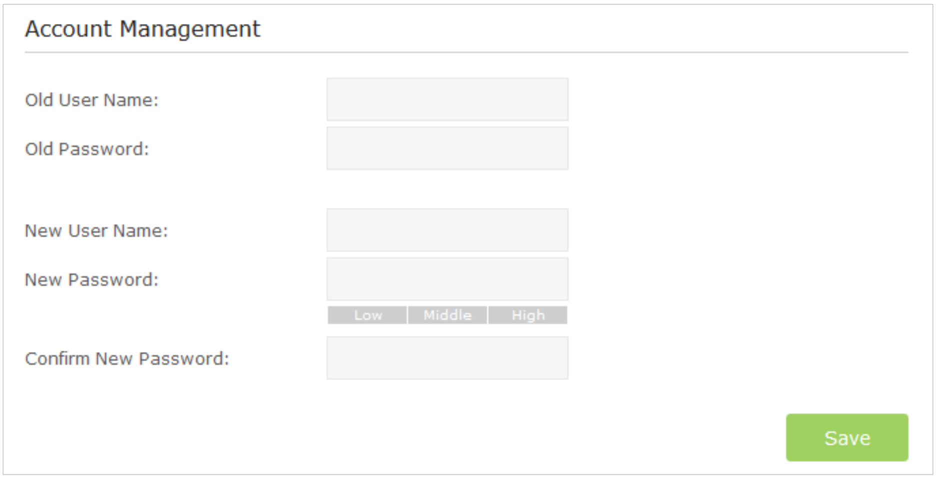
Note:

1. During the resetting process, do not turn off the router.
2. We strongly recommend you back up the current configuration settings before resetting the router.

11. 4. Change the Administrator Account

Admin account is used to log in to the router's web management page. You are required to set the admin account at first login. You can also change it on the web page.

1. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
2. Go to Advanced > System Tools> Administration page. Locate the Account Management section.



Account Management

Old User Name:

Old Password:

New User Name:

New Password:

Confirm New Password:

3. Enter the old user name and old password. Enter the new user name and new password.

4. Click Save to make the settings effective.

11. 5. Local Management

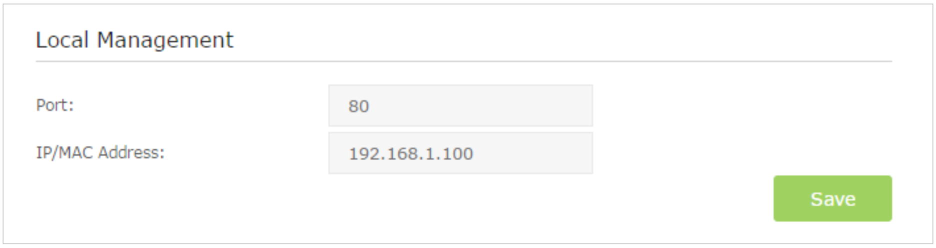
You can control the local devices' authority to manage the router via the Local Management feature. By default all local connected devices are allowed to manage the router. You can also allow only one device to manage the router.

Follow the steps below to specify the local management feature.

1. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.

2. Go to Advanced > System Tools> Administration page. Locate the Local Management section.

3. Keep the Port as the default setting. Enter the IP address or MAC address of the local device to manage the router.



Local Management

Port: 80

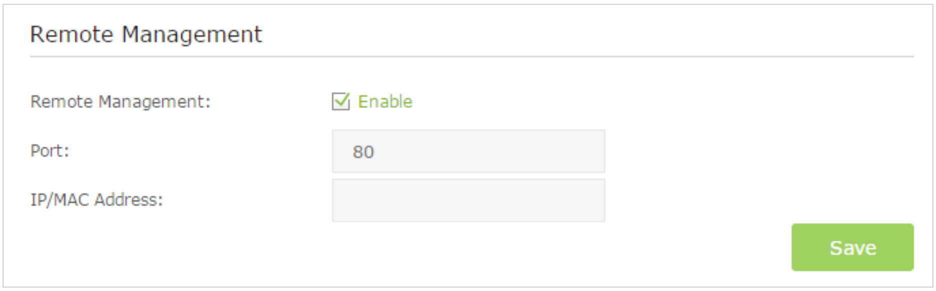
IP/MAC Address: 192.168.1.100

4. Click Save to make the settings effective. Now only the device (192.168.1.100) can manage the router. If you want that all local devices can manage the router, just leave the IP/MAC Address field blank.

11. 6. Remote Management

By default, the remote devices are not allowed to manage the router from the Internet. Follow the steps below to allow remote devices to manage the router.

1. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
2. Go to Advanced > System Tools> Administration page. Locate the Remote Management section.



Remote Management

Remote Management: ☑ Enable

Port: 80

IP/MAC Address:

3. Tick the check box to enable Remote Management. Keep the Port as the default setting. Leave the IP/MAC Address field blank. If you just want to allow a specific device to manage the router, you can enter the IP address of the remote device in the IP/MAC Address field.
4. Click Save to make the settings effective. Now, all devices on the Internet can log in to http://*modem router's WAN IP address* : *port number* (such as http://113.116.60.229:80) to manage the router.

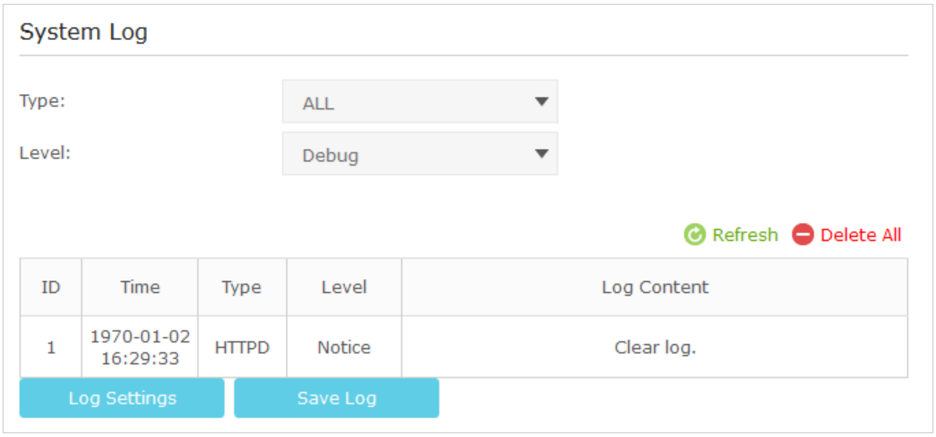
Tips:

1. You can find the WAN IP address of the router on Basic > Network Maps > Internet.
2. The router's WAN IP is usually a dynamic IP. Please refer to *Set Up a Dynamic DNS Service Account* if you want to log in to the router through a domain name.

11. 7. System Log

System Log can help you know what happened to your router, facilitating you to locate the malfunctions. For example when your router does not work properly, you will need to save the system log and send it to the technical support for troubleshooting.

1. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
2. Click Advanced > System Tools > System Log page.



System Log

Type: ALL

Level: Debug

ID	Time	Type	Level	Log Content
1	1970-01-02 16:29:33	HTTPD	Notice	Clear log.

To view the system logs:

You can view specific system logs by selecting the log Type and Level.

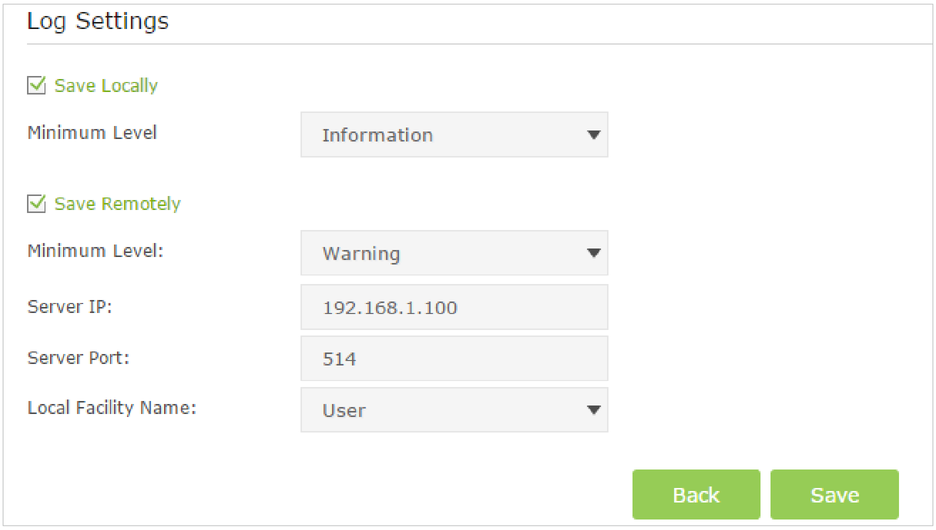
Click Refresh to refresh the log list.

To save the system logs:

You can choose to save the system logs to your local computer or a remote server.

Click Save Log to save the logs in a txt file to your computer.

Click Log Settings to set the storage path of logs.



Log Settings

☑ Save Locally

Minimum Level: Information

☑ Save Remotely

Minimum Level: Warning

Server IP: 192.168.1.100

Server Port: 514

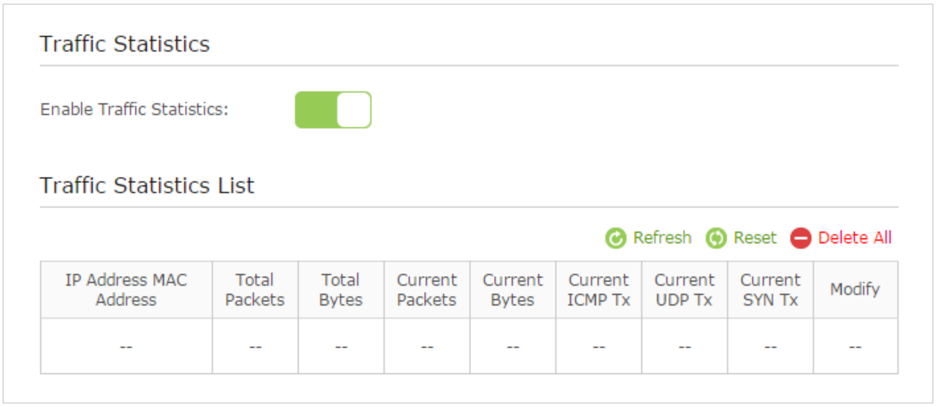
Local Facility Name: User

- Save Locally: Select this option to cache the system log to the router's local memory, select the minimum level of system log to be saved from the drop-down list. The logs will be shown in the table in descending order on the System Log page.
- Save Remotely: Select this option to send the system log to a remote server, select the minimum level of system log to be saved from the drop-down list and enter the information of the remote server. If the remote server has a log viewer client or a sniffer tool implemented, you can view and analyze the system log remotely in real-time.

11. 8. Monitor the Internet Traffic Statistics

The Traffic Statistics page displays the network traffic of the LAN-WAN and WLAN-WAN sent and received packets, allowing you to monitor the volume of Internet traffic statistics.

1. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
2. Go to Advanced > System Tools > Statistics.
3. Toggle on Enable Traffic Statistics, and then you can monitor the traffic statistics in Traffic Statistics List section. This function is disabled by default.



Traffic Statistics

Enable Traffic Statistics:

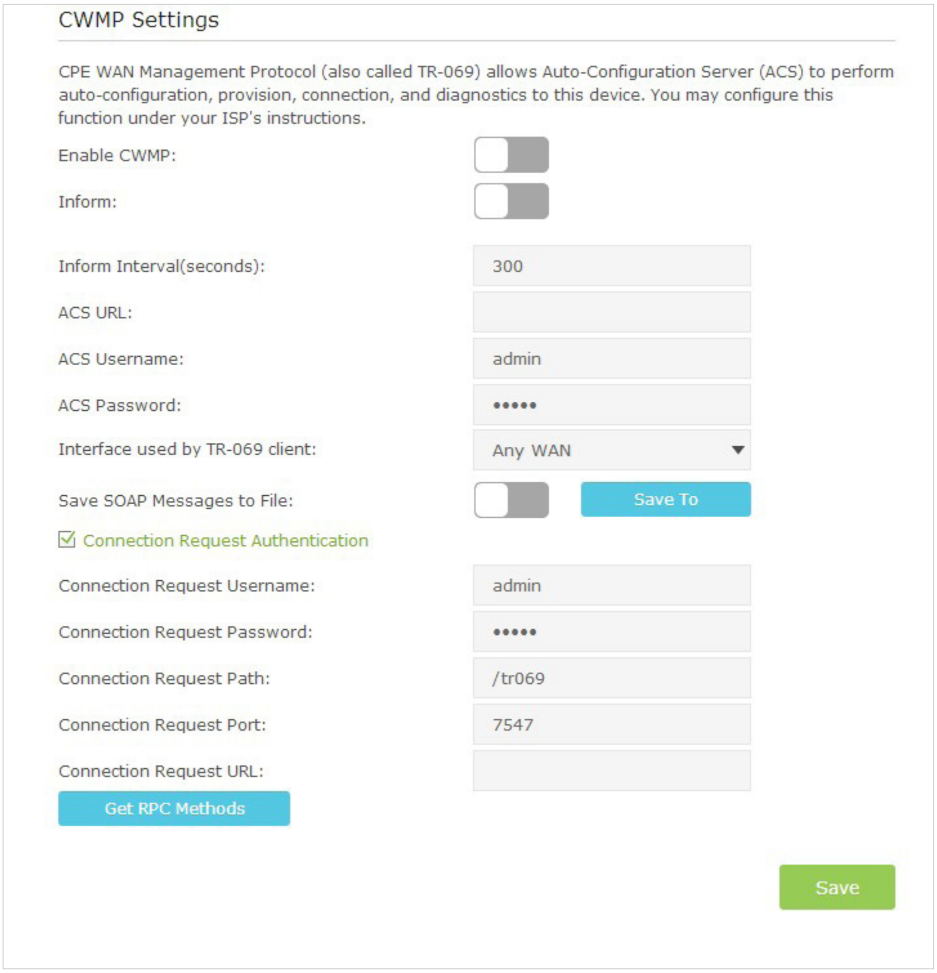
Traffic Statistics List

IP Address MAC Address	Total Packets	Total Bytes	Current Packets	Current Bytes	Current ICMP Tx	Current UDP Tx	Current SYN Tx	Modify
--	--	--	--	--	--	--	--	--

11. 9. CWMP Settings

The 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).

1. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
2. Go to Advanced > System Tools > CWMP Settings page.



CWMP Settings

CPE WAN Management Protocol (also called TR-069) allows Auto-Configuration Server (ACS) to perform auto-configuration, provision, connection, and diagnostics to this device. You may configure this function under your ISP's instructions.

Enable CWMP:	
Inform:	
Inform Interval(seconds):	300
ACS URL:	
ACS Username:	admin
ACS Password:	•••••
Interface used by TR-069 client:	Any WAN
Save SOAP Messages to File:	Save To

☑ Connection Request Authentication

Connection Request Username:	admin
Connection Request Password:	•••••
Connection Request Path:	/tr069
Connection Request Port:	7547
Connection Request URL:	

- Enable CWMP: Toggle On to enable the CWMP (CPE WAN Management Protocol) feature.
- Inform: Enable this feature to send an Inform message to the ACS (Auto Configuration Server) periodically.
- Inform Interval: Enter the time interval in seconds when the Inform message will be sent to the ACS.
- ACS URL: Enter the web address of the ACS which is provided by your ISP.
- ACS Username/Password: Enter the username/password to log in to the ACS server.
- Interface used by TR-069 client: Select which interface to be used by the TR-069 client.
- Save SOAP Messages to File: Toggle to enable or disable this feature. Click Save To to specify a path on your computer to save the SOAP messages.
- Connection Request Authentication: Select this checkbox to enable authentication for the connection request.
- Connection Request Username/Password: Enter the username/password for the ACS server to log in to the router.
- Connection Request Path: Enter the path for the ACS server to log in to the router.

- Connection Request Port: Enter the port that connects to the ACS server.
- Connection Request URL: Enter the URL that connects to the ACS server.
- Get RPC methods: Click to get the methods to support CWMP.

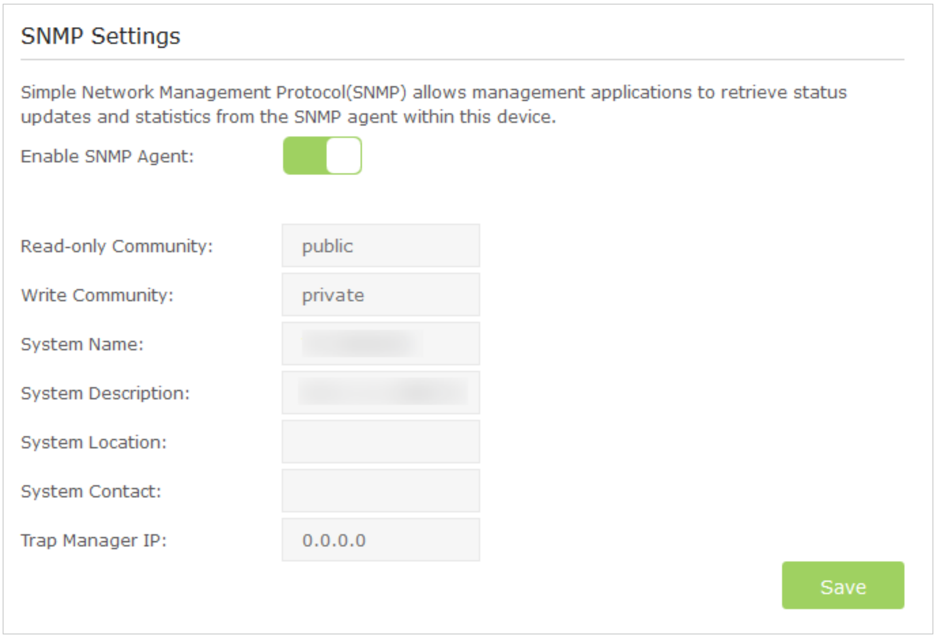
Click Save to make the settings effective.

11. 10. SNMP Settings

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 two nodes. In this way, network administrators can easily search and modify the information on any node on the network. Meanwhile, they can locate faults promptly and implement the fault diagnosis, capacity planning and report generating.

An SNMP Agent is an application running on the router that performs the operational role of receiving and processing SNMP messages, sending responses to the SNMP manager, and sending traps when an event occurs. So a router contains SNMP "agent" software can be monitored and/or controlled by SNMP Manager using SNMP messages.

1. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
2. Go to Advanced > System Tools > SNMP Settings page.



SNMP Settings

Simple Network Management Protocol(SNMP) allows management applications to retrieve status updates and statistics from the SNMP agent within this device.

Enable SNMP Agent:

Read-only Community:	public
Write Community:	private
System Name:	[redacted]
System Description:	[redacted]
System Location:	
System Contact:	
Trap Manager IP:	0.0.0.0

- Enable SNMP Agent: Toggle On to enable the built-in SNMP agent that allows the router to operate as the operational role in receiving and processing of SNMP messages, sending responses to the SNMP manager, and triggering SNMP traps when an event occurs.

- Read-only Community: Displays the default public community string that protects the router from unauthorized access.
- Write Community: Displays the default write community string that protects the router from unauthorized changes.
- System Name: Displays the administratively-assigned name for this managed device.
- System Description: Displays the textual description of the managed device. This value should include the full name and version identification of the system's hardware type, software operating-system, and networking software.
- System Location: Displays the physical location of this device (e.g., telephone closet, 3rd floor).
- System Contact: Displays the textual identification of the contact person for this managed device, together with information on how to contact this person.
- Trap Manager IP: Displays the IP address of the host to receive the traps.

You are suggested to keep the default settings. Click Save to make the settings effective.

Appendix: Troubleshooting

T1. How do I restore my router's configuration to its factory default settings?

There are two ways to reset the router:

- Method 1: Use the Reset button. For details, refer to the related button description.
- Method 2: Use the Backup & Restore page. For details, refer to the instructions in *To reset the router to factory default settings*.

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

T2. What can I do if I forgot my password?

Web management page password:

Restore the router to its factory default settings and then use admin for both username and password to log in.

Wireless network password:

1. The default Wireless Password/PIN is printed on the product label of the router.
2. If the default wireless password has been changed, log into the router's web management page and go to Basic > Wireless to retrieve or reset your password.

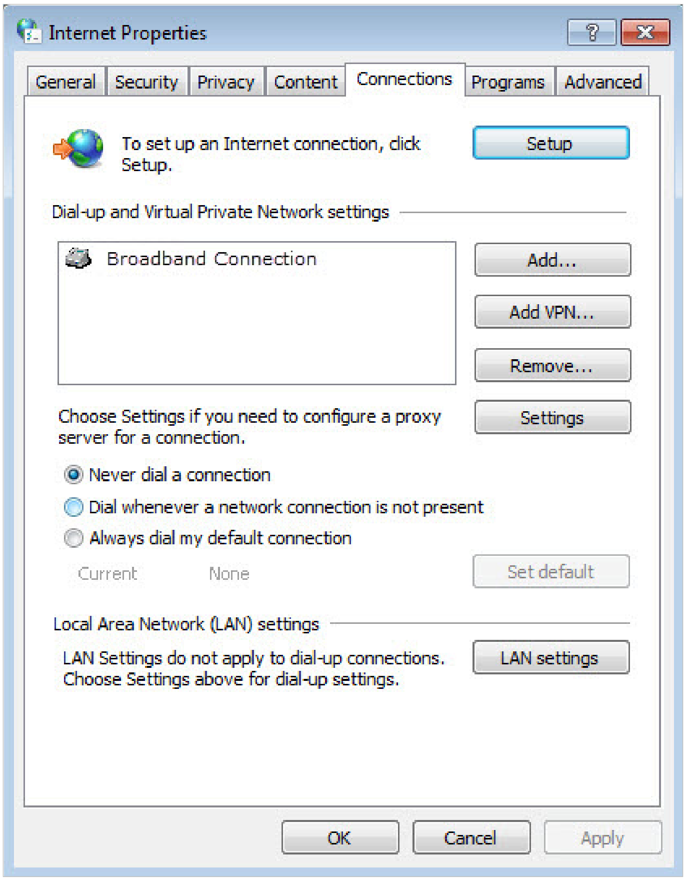
T3. What can I do if I cannot log in to the router's web management page?

- Make sure the 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 *http://192.168.1.1* or *http://tplinkwifi.net* is correctly input.
- 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, select Never dial a connection;



To set up an Internet connection, click Setup.

Broadband Connection

Choose Settings if you need to configure a proxy server for a connection.

● Never dial a connection

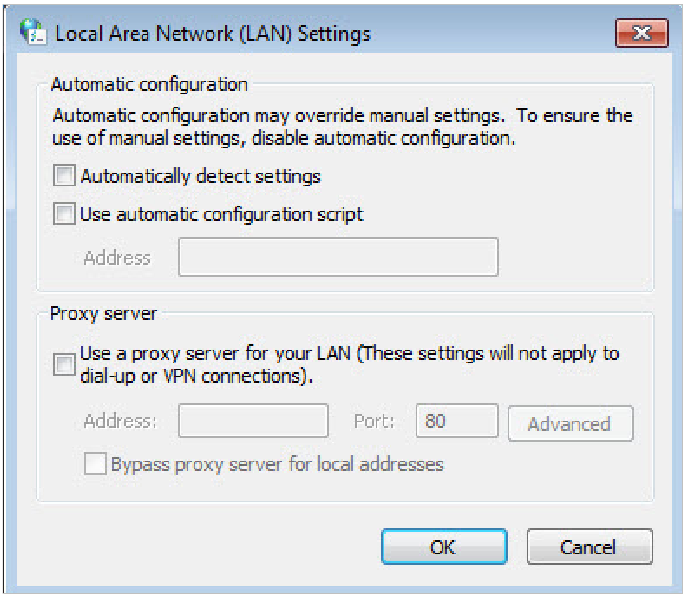
○ Dial whenever a network connection is not present

○ Always dial my default connection

Current None

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.

4) Click LAN settings, deselect the following three options and click OK;



Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

□ Automatically detect settings

□ Use automatic configuration script

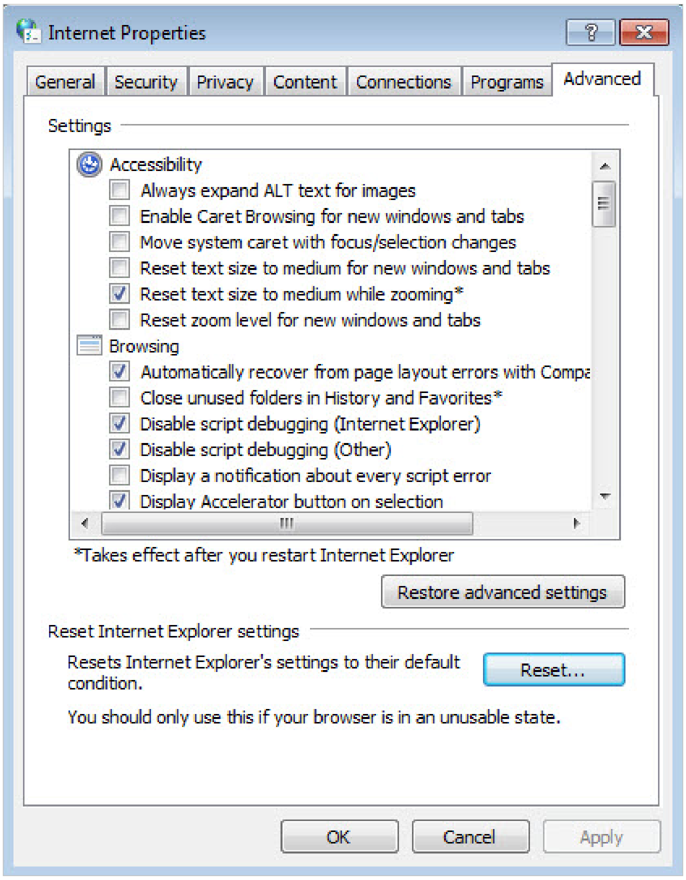
Address

□ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: Port: 80

□ Bypass proxy server for local addresses

5) Go to Advanced > Restore advanced settings, click OK to save the settings.



Settings

Accessibility

- □ Always expand ALT text for images
- □ Enable Caret Browsing for new windows and tabs
- □ Move system caret with focus/selection changes
- □ Reset text size to medium for new windows and tabs
- ☑ Reset text size to medium while zooming*
- □ Reset zoom level for new windows and tabs

Browsing

- ☑ Automatically recover from page layout errors with Compa
- □ Close unused folders in History and Favorites*
- ☑ Disable script debugging (Internet Explorer)
- ☑ Disable script debugging (Other)
- □ Display a notification about every script error
- ☑ Display Accelerator button on selection

*Takes effect after you restart Internet Explorer

Reset Internet Explorer settings

Resets Internet Explorer's settings to their default condition.

You should only use this if your browser is in an unusable state.

- Change a web browser or computer and log in again.
- Reset the router to factory default settings.

Note: You'll need to reconfigure the router to surf the Internet once the 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 fiber line, Ethernet cables and power adapter.
2. Check the GPON LED and make sure that it is lit and stable, indicating that the router is registered with the ISP. If not, make sure that the provided GPON SN and/or GPON Password are entered correctly in the Advanced > Network > GPON Settings page.
3. Check if you can log in to the web management page of the router. If you can, try the following steps. If you cannot, please set your computer by referring to T3 and then try to see if you can access the Internet. If the problem persists, please go to the next step.
4. Refer to T5 to clone the MAC address.

5. If you still cannot access the Internet, please restore your router to its factory default settings and reconfigure your router by following the instructions in *Use Quick Setup Wizard*.

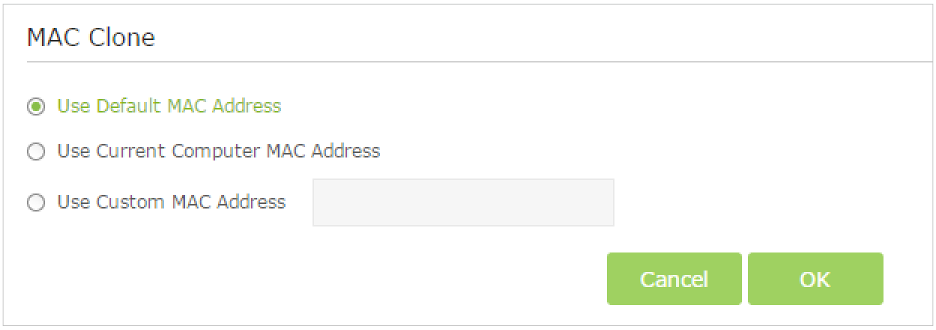
6. Please contact your ISP if the problem still exists.

T5. How to configure MAC Clone?

You can manually change the MAC address of the router. It is helpful when your Internet access account provided by your ISP is bound to one specific MAC address, in other words, your ISP just permits only one computer with the authenticated MAC address to access the Internet. In this case, you can use MAC Clone to allow more computers to access the Internet via the same account.

1. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.

2. Go to Advanced > Network > Internet page. Click the Add icon, and scroll down to get the MAC Clone section.



MAC Clone

● Use Default MAC Address

○ Use Current Computer MAC Address

○ Use Custom MAC Address

- If you are using the computer with the authenticated MAC address to access the router, please select Use Current Computer MAC Address.
- If you know the authenticated MAC address, please select Use Custom MAC Address and then enter the address.

3. Click OK to make the settings effective.

T6. How to use the WDS Bridging function to extend my wireless network?

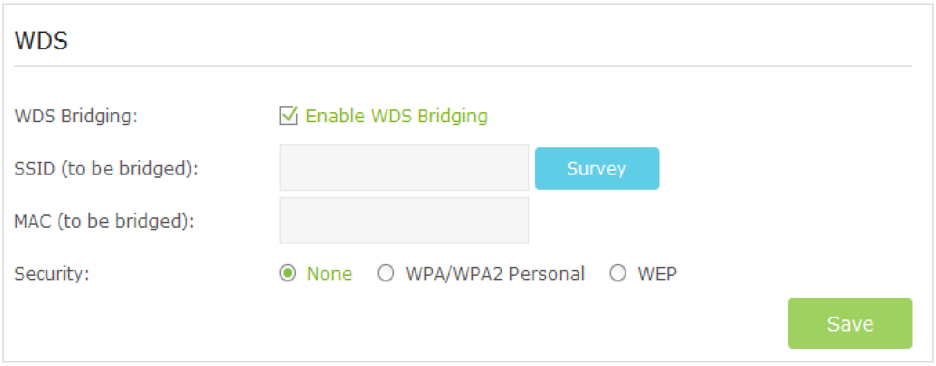
My house covers a large area. The wireless network coverage of the router I'm using (the root router) is limited. I want to use an extended router to extend the wireless network of the primary router. Follow the steps to configure the router.

1. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.

2. Configure the LAN IP address of the router in the same subnet as the root router. For example, if the IP address of the root router is 192.168.0.1, the IP address of the extended router should be from 192.168.0.2 to 192.168.0.254.).

3. Go to Advanced > Wireless > Advanced Settings page and locate the WDS section.

4. Select the check box to enable the WDS Bridging function.



WDS

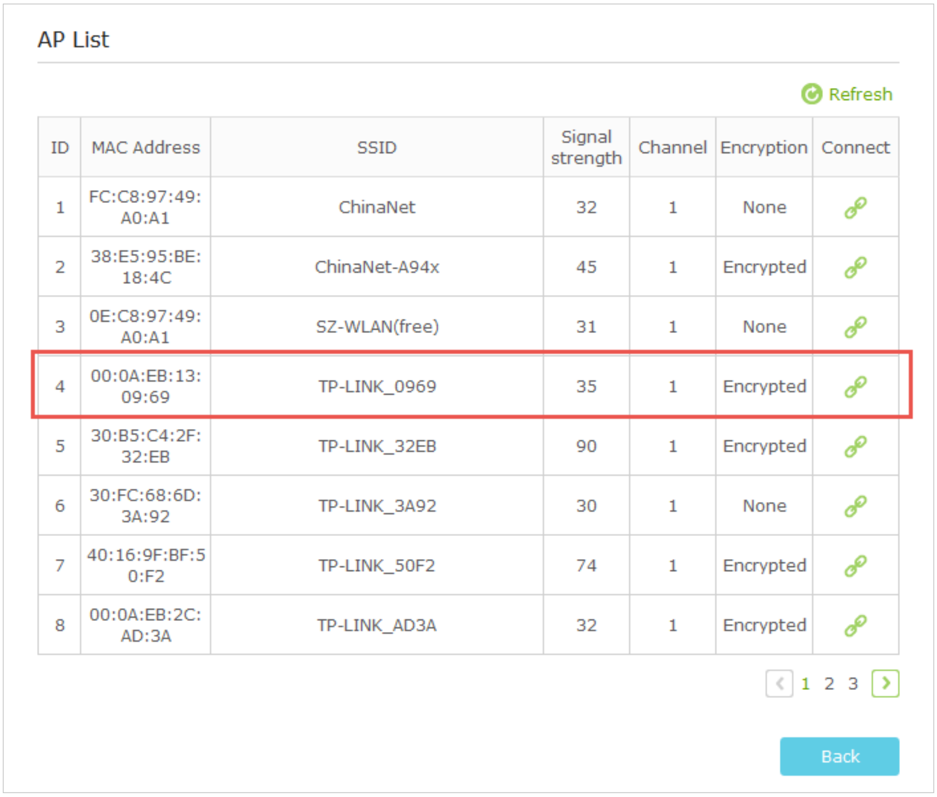
WDS Bridging: ☑ Enable WDS Bridging

SSID (to be bridged):

MAC (to be bridged):

Security: ● None ○ WPA/WPA2 Personal ○ WEP

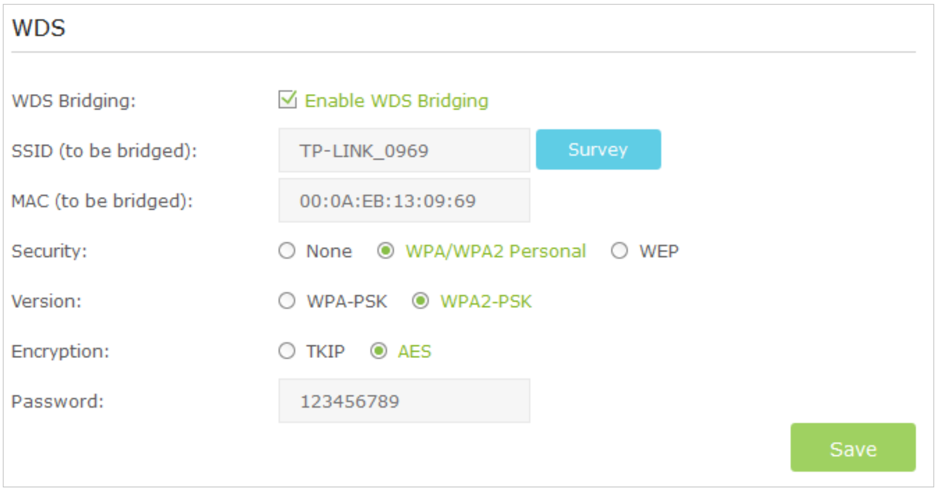
5. Click Survey to scan all the AP devices and choose the root AP to be bridged.



AP List

ID	MAC Address	SSID	Signal strength	Channel	Encryption	Connect
1	FC:C8:97:49:A0:A1	ChinaNet	32	1	None	🔗
2	38:E5:95:BE:18:4C	ChinaNet-A94x	45	1	Encrypted	🔗
3	0E:C8:97:49:A0:A1	SZ-WLAN(free)	31	1	None	🔗
4	00:0A:EB:13:09:69	TP-LINK_0969	35	1	Encrypted	🔗
5	30:B5:C4:2F:32:EB	TP-LINK_32EB	90	1	Encrypted	🔗
6	30:FC:68:6D:3A:92	TP-LINK_3A92	30	1	None	🔗
7	40:16:9F:BF:50:F2	TP-LINK_50F2	74	1	Encrypted	🔗
8	00:0A:EB:2C:AD:3A	TP-LINK_AD3A	32	1	Encrypted	🔗

6. Click the connect icon and then the SSID and MAC will be auto-populated. Configure the Security settings as the AP you choose to be bridged.



WDS

WDS Bridging: ☑ Enable WDS Bridging

SSID (to be bridged): TP-LINK_0969

MAC (to be bridged): 00:0A:EB:13:09:69

Security: ○ None ● WPA/WPA2 Personal ○ WEP

Version: ○ WPA-PSK ● WPA2-PSK

Encryption: ○ TKIP ● AES

Password: 123456789

7. Click Save to make the settings effective.
8. Go to Advanced > Network > LAN Settings page to disable DHCP.

Now, the root's wireless network is extended and you can use the router's SSID and password to enjoy the network.

Note: The extended router (GRPON router) can have different SSID and password from the root router, you can change your router's SSID and password on Basic > Wireless page.

T7. What can I do if I cannot find my wireless network or I cannot connect the wireless network?

➢ **If you fail to find any wireless network, follow the steps below:**

1. Make sure the wireless function is enabled if you're using a laptop with built-in wireless adapter. You can refer to the relevant document or contact the laptop manufacturer.
2. Make sure the wireless adapter driver is installed successfully and the wireless adapter is enabled. You can refer to the relevant document or contact the wireless adapter manufacturer.

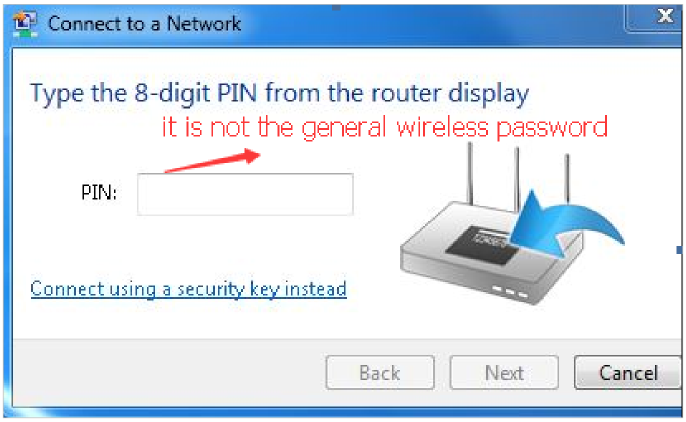
➢ **If you can find other wireless network except your own, follow the steps below:**

1. Check the Wi-Fi LED indicator on your wireless router/modem;
2. Make sure your computer/device is still in the range of your router/modem, move closer if it is currently too far away;
3. Go to Basic > Wireless page, and check the wireless router settings, double check your Wireless Name and the SSID is not hidden.
4. Connect to wireless network.

➢ **If you can find your wireless network but fail to connect, follow the steps below:**

1. Authenticating problem, password mismatch.

1) Sometimes it will ask you to type in a PIN number when you connect to the wireless network for the first time. This PIN number is different from the Wireless Password/Network Security Key, usually you can only find it on the back of your wireless router/modem;



Connect to a Network

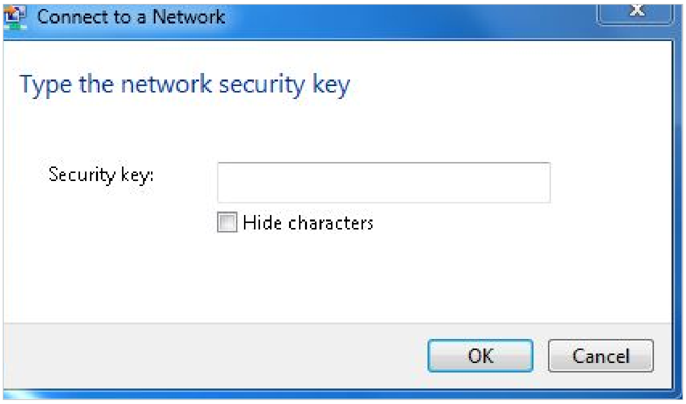
Type the 8-digit PIN from the router display

it is not the general wireless password

PIN:

Connect using a security key instead

2) If you cannot find the PIN or PIN failed, you may choose "Connecting using a security key instead", and then type in the Network Security Key/Wireless Password;



Connect to a Network

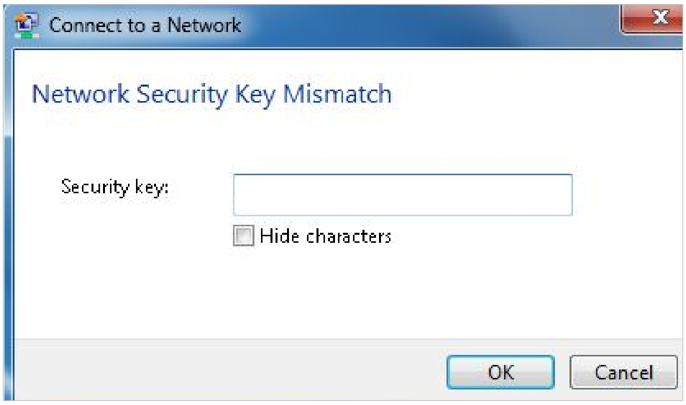
Type the network security key

Security key:

□ Hide characters

3) If it continues on saying network security key mismatch, it is suggested to confirm the wireless password on your wireless router/modem;

Note: Wireless password/Network Security Key is case sensitive.



Connect to a Network

Network Security Key Mismatch

Security key:

□ Hide characters

4) Connect to wireless network.

2. Windows was unable to connect to XXXX /Cannot join this network/Taking longer than usual to connect to this network.

1) Check the wireless signal strength of your network, if it is weak (1~3 bars), please move the router closer and try again;

2) Change the wireless Channel of the router to 1,6,or 11 to reduce interference from other networks;

3) Re-install or update the driver for your wireless adapter of the computer;

4) Connect to wireless network.

COPYRIGHT & TRADEMARKS

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.

Canadian Compliance Statement

This device complies with Industry Canada license-exempt RSSs. Operation is subject to the following two conditions:

1) This device may not cause interference, and

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

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

1) l'appareil ne doit pas produire de brouillage;

2）l’utilisateur de l’appareil doit accepter tout brouillage radioélectrique subi, meme si le brouillage est susceptible d’en compromettre le fonctionnement.

NCC Notice

注意！

依據 低功率電波輻射性電機管理辦法

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

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

BSMI Notice

安全諮詢及注意事項

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

Safety Information

- When product has power button, the power button is one of the way to shut off the product; when there is no power button, the only way to completely shut off power is to disconnect the product or the power adapter from the power source.
- Don’t disassemble the product, or make repairs yourself. You run the risk of electric shock and voiding the limited warranty. If you need service, please contact us.
- Avoid water and wet locations.
- Adapter shall be installed near the equipment and shall be easily accessible.
- The plug considered as disconnect device of adapter.
- Use only power supplies which are provided by manufacturer and in the original packing of this product. If you have any questions, please don’t hesitate to contact us.

Explanation of the symbols on the product label

Symbol	Explanation
⎓	DC voltage
	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.