I want to:

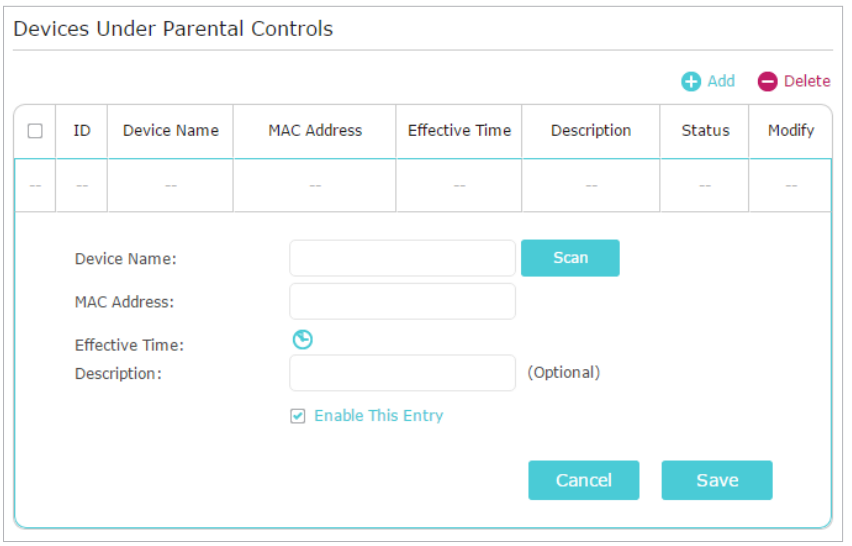
Control the times of day my children or other home network users are allowed to access the Internet and even types of websites they can visit.

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) at the weekend and not other times.

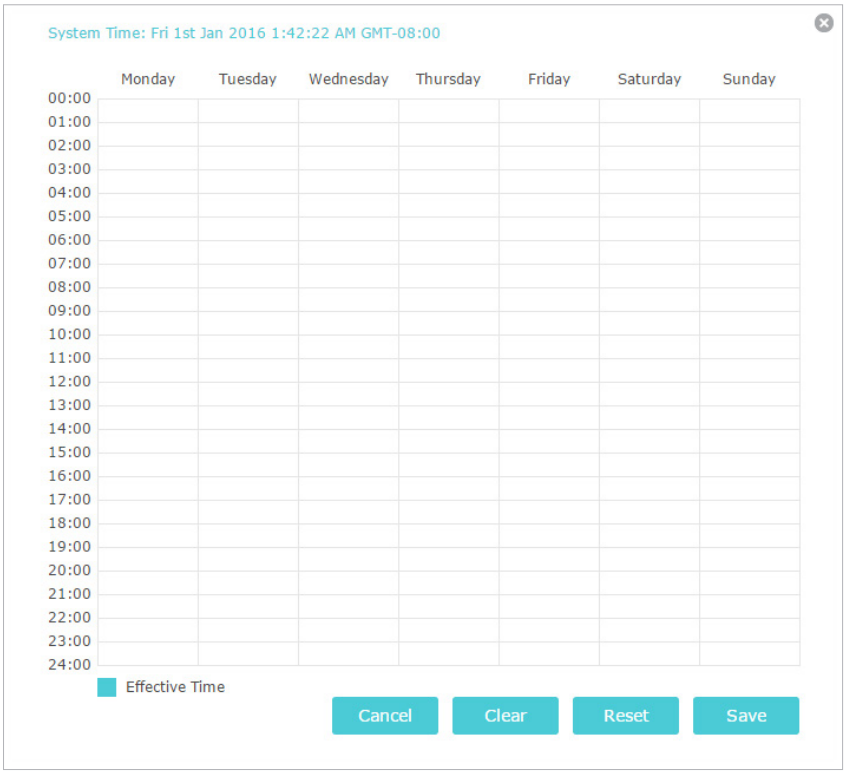
How can I do that?

1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > Parental Controls and enable Parental Controls.

3. Click Add. And then Click Scan, and select the access device. Or, input the Device Name and MAC Address manually.

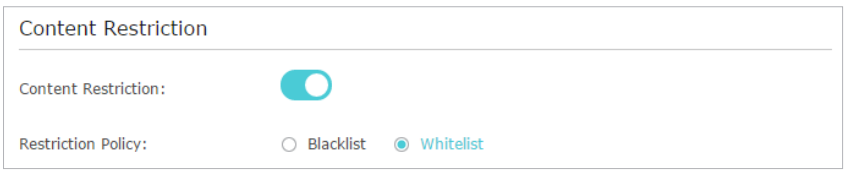


4. Click the icon to set the Effective Time. Drag the cursor over the appropriate cell(s) and click Save.



5. Enter a Description for the entry, Tick the Enable This Entry checkbox, and then click Save.

6. Enable Content Restriction, and select Whitelist as the restriction policy.



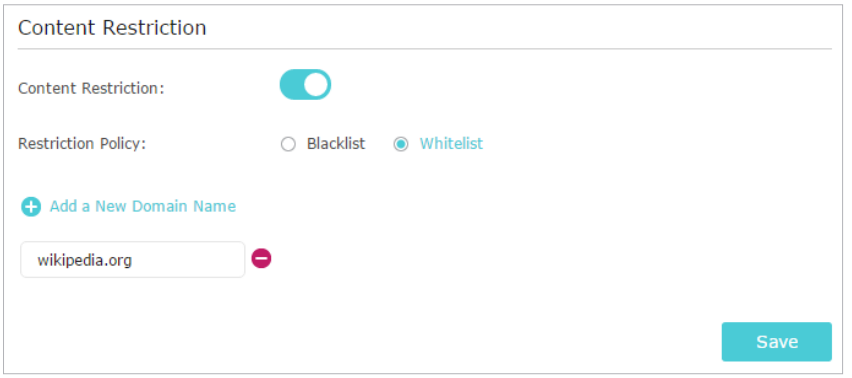
Tips:

- With Blacklist selected, the controlled devices cannot access any websites containing the specified keywords during the Internet Access Time period.
- With Whitelist selected, the controlled devices can only access websites containing the specified keywords during the Internet Access Time period.

7. Click Add a New Domain Name . Enter a website and click Save.

   You can add up to 32 keywords for either Blacklist or Whitelist. Below are some sample entries to allow access.

   - For Whitelist: Enter a web address (e.g. wikipedia.org) to allow access only to its related websites. If you wish to block all Internet browsing access, do not add any keyword to the Whitelist.
   - For Blacklist: Specify a web address (e.g. wikipedia.org), a web address keyword (e.g. wikipedia) or a domain suffix (eg. .edu or .org) to block access only to the websites containing that keyword or suffix.



Done! Now you can control your children's Internet access as needed.

Chapter 10

QoS

This chapter introduces how to create a QoS (Quality of Service) rule to specify prioritization of traffic and minimize the impact caused when the connection is under heavy load.

It contains the following sections:

- Prioritize Internet Traffic with QoS
- Update the Database

10. 1. Prioritize Internet Traffic with QoS

QoS (Quality of Service) is designed to ensure the efficient operation of the network when come across network overload or congestion.

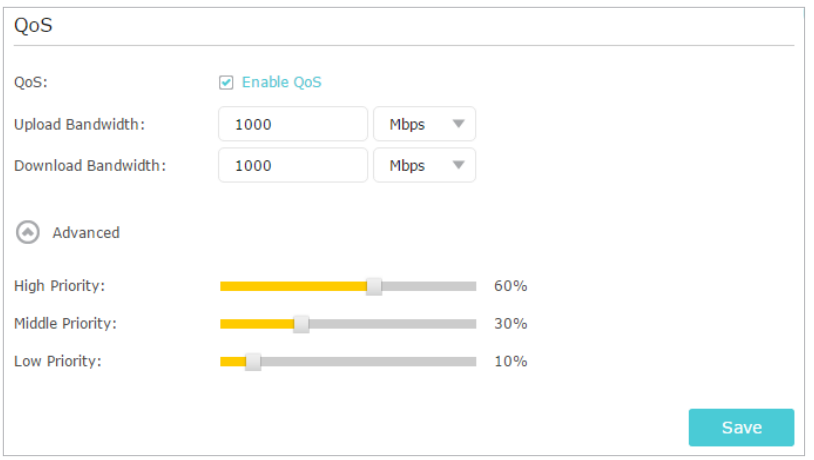
I want to:

Specify priority levels for some devices or applications.

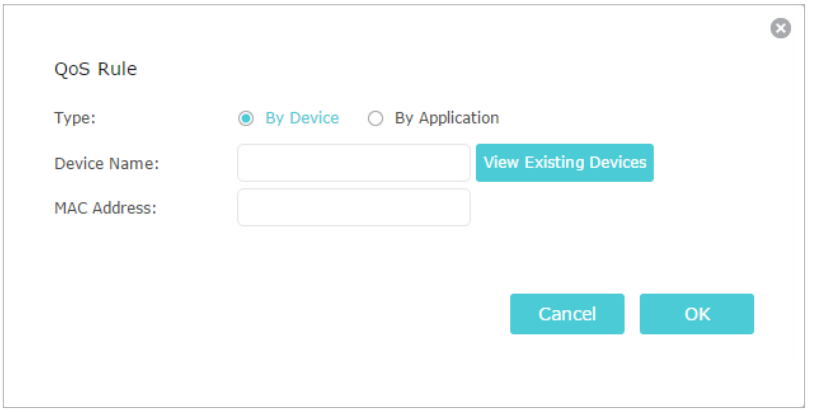
For example, I have several devices that are connected to my wireless network. I would like to set an intermediate speed on the Internet for my phone.

How can I do that?

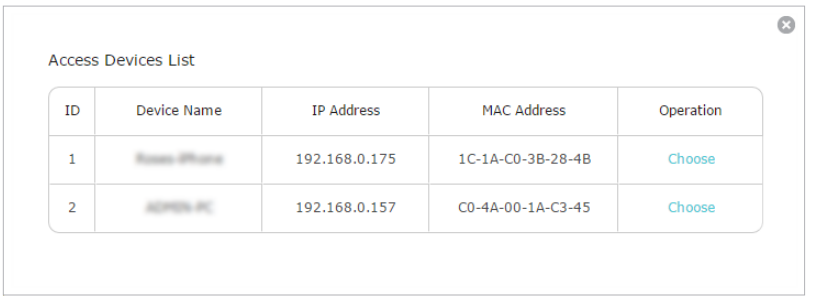
1. Enable QoS and set bandwidth allocation.
   1) Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
   2) Go to Advanced > QoS > Settings.
   3) Select Enable QoS.
   4) Input the maximum upload and download bandwidth provided by your Internet service provider. 1Mbps equals to 1000Kbps.
   5) Click Advanced and drag the scroll bar to set the bandwidth priority percentage.
   6) Click Save.



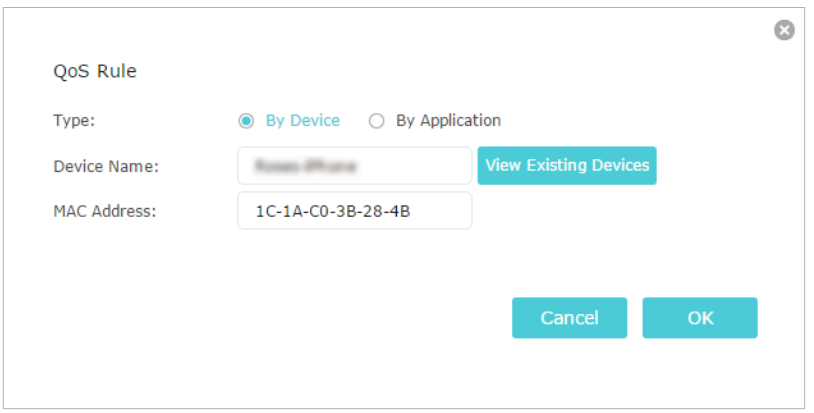
2. Add a middle priority QoS rule for the phone.
   1) Select By Device and then click View Existing Devices.



2) Choose the respective device from the list.



3) Click OK.



3. Refer to the steps above to apply other QoS rules if any.

Note:

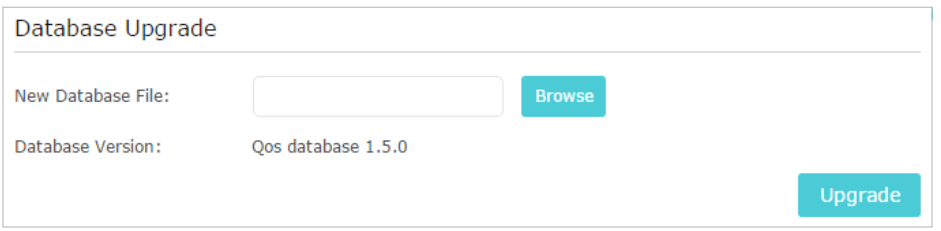
If you want to delete a QoS rule, click to remove the responding rule from the list.

Done! Now QoS is implemented to prioritize Internet traffic.

10. 2. Update the Database

This function can help to add or update the applications the router supports. If the applications you need are not listed in the Application list, you can try to download the new version and upgrade the datebase. New database versions are posted at www.tp-link.com and can be downloaded for free.

1. Download the latest QoS database from our website www.tp-link.com.
2. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
3. Go to Advanced > QoS > Database. Click Browse to select the database upgrade file, and then click Upgrade. Wait until the upgrade is completed and do not operate during the process.



Chapter 11

Network Security

This chapter guides you on how to protect your home network from cyber attacks and unauthorized users by implementing these three network security functions. You can protect your home network against DoS (Denial of Service) attacks from flooding your network with server requests using DoS Protection, block or allow specific client devices to access your network using Access Control, or you can prevent ARP spoofing and ARP attacks using IP & MAC Binding.

It contains the following sections:

- Protect the Network from Cyber Attacks
- Access Control
- IP & MAC Binding

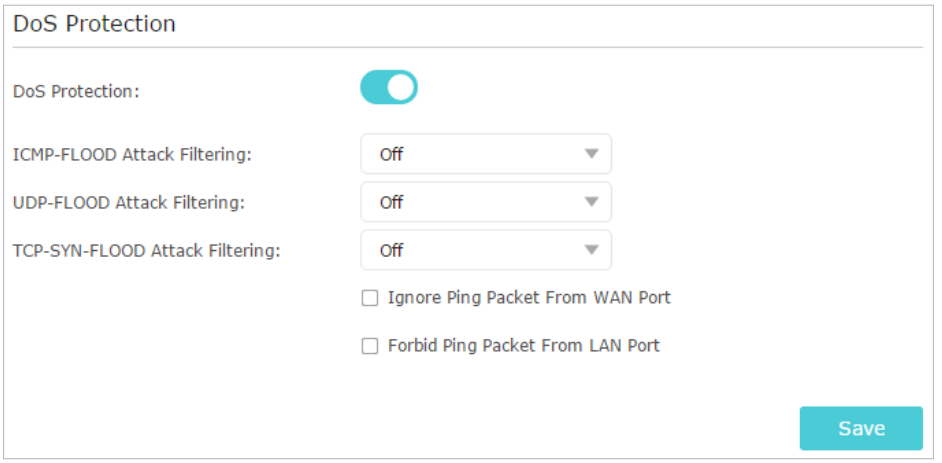
11. 1. Protect the Network from Cyber Attacks

The SPI (Stateful Packet Inspection) Firewall and DoS (Denial of Service) Protection protect the router from cyber attacks.

The SPI Firewall can prevent cyber attacks and validate the traffic that is passing through the router based on the protocol. This function is enabled by default, and it's recommended to keep the default settings.

DoS Protection can protect your home network against DoS attacks from flooding your network with server requests. Follow the steps below to configure DoS Protection.

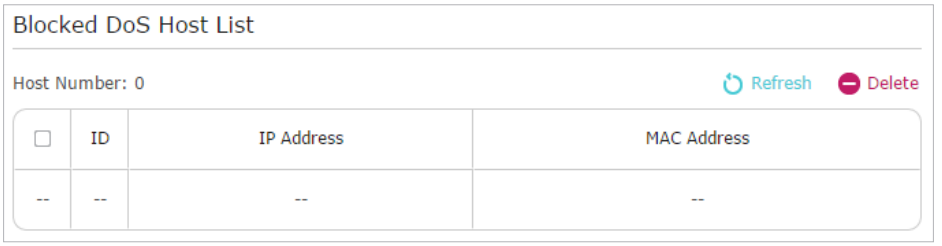
1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > Security > Firewall & Dos Protection.



3. Enable DoS Protection.
4. Set the level (Off, Low, Middle or High) of protection for ICMP-FLOOD Attack Filtering, UDP-FlOOD Attack Filtering and TCP-SYN-FLOOD Attack Filtering.
   - ICMP-FLOOD Attack Filtering - Enable to prevent the ICMP (Internet Control Message Protocol) flood attack.
   - UDP-FlOOD Attack Filtering - Enable to prevent the UDP (User Datagram Protocol) flood attack.
   - TCP-SYN-FLOOD Attack Filtering - Enable to prevent the TCP-SYN (Transmission Control Protocol-Synchronize) flood attack.

   Tips:

   The level of protection is based on the number of traffic packets. The protection will be triggered immediately when the number of packets exceeds the preset threshold value (the value can be set on Advanced > System Tools > System Parameters > DoS Protection Level Settings), and the vicious host will be displayed in the Blocked DoS Host List.



5. If you want to ignore the ping packets from the WAN port, select Ignore Ping Packet From WAN Port; if you want to ignore the ping packets form the LAN port, select Ignore Ping Packet From LAN Port.
6. Click Save.

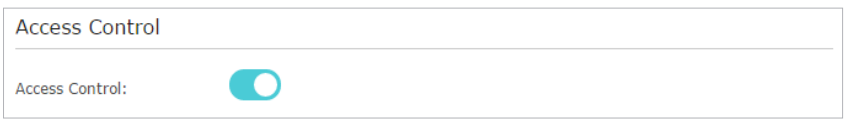
11. 2. Access Control

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 your TP-Link ID or the password you set for the router.
2. Go to Advanced > Security > Access Control.
3. Enable Access Control.

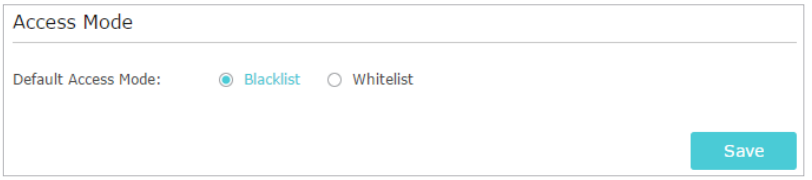


4. If you also want to control access of the devices connected to the guest network, toggle on Guest Devices Control.

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

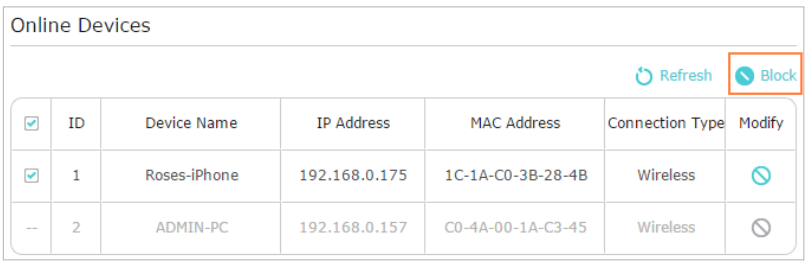
   To block specific device(s)

   1) Select Blacklist and click Save.



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

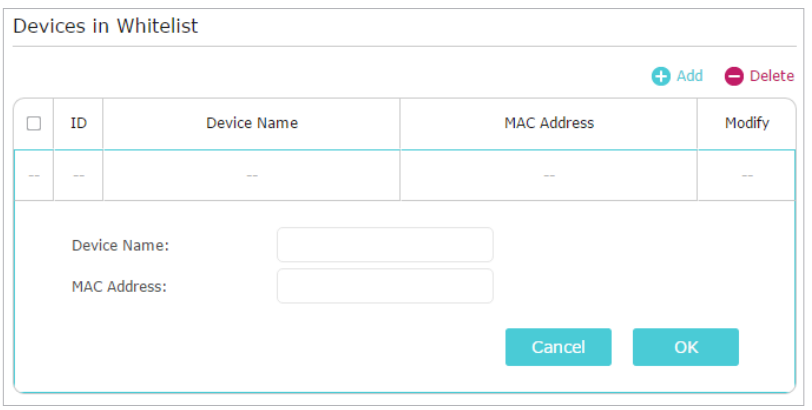
3) Click Block above the Online Devices table. The selected devices will be added to Devices in Blacklist automatically.



To allow specific device(s)

1) Select Whitelist and click Save.

2) Click Add in the Devices in Whitelist section. Enter the Device Name and MAC Address (You can copy and paste the information from the Online Devices list if the device is connected to your network).



3) 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.

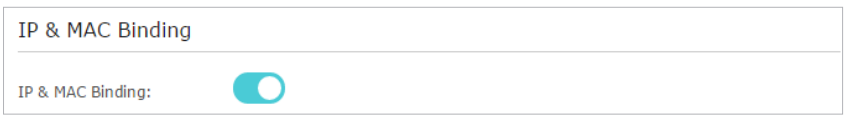
11. 3. IP & MAC Binding

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 an 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 your TP-Link ID or the password you set for the router.
2. Go to Advanced > Security > IP & MAC Binding.
3. Enable IP & MAC Binding.



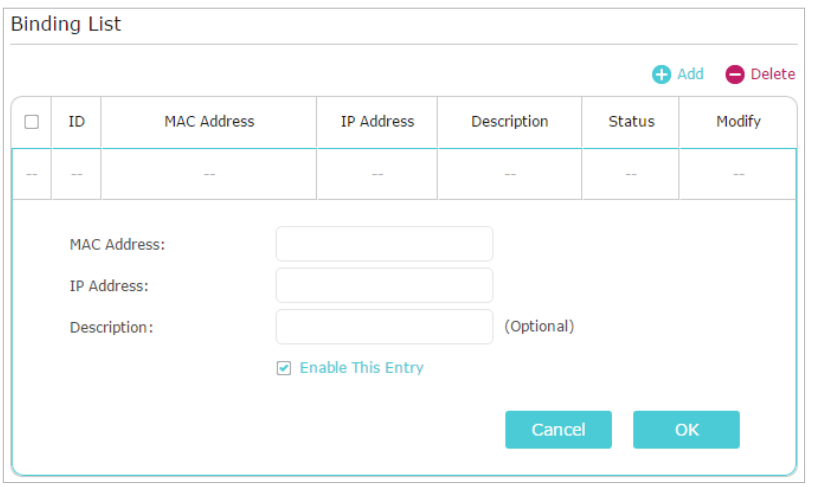
4. Bind your device(s) according to your need.

   To bind the connected device(s):

   Click to add the corresponding device to the Binding List.

   To bind the unconnected device

   1) Click Add in the Binding List section.



   2) Enter the MAC address and IP address that you want to bind. Enter a Description for this binding entry.

   3) Check the box for Enable This Entry and click OK.

Done! Now you don't need to worry about ARP spoofing and ARP attacks!

Chapter 12

NAT Forwarding

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

With the forwarding feature the router can penetrate the isolation of NAT and allows devices on the internet to initiatively communicate with devices on the local network, thus realizing some special functions.

The TP-Link router supports 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.

It contains the following sections:

- Share Local Resources on the Internet by Virtual Servers
- Open Ports Dynamically by Port Triggering
- Make Applications Free from Port Restriction by DMZ
- Make Xbox Online Games Run Smoothly by UPnP

12. 1. Share Local Resources on the Internet by Virtual Servers

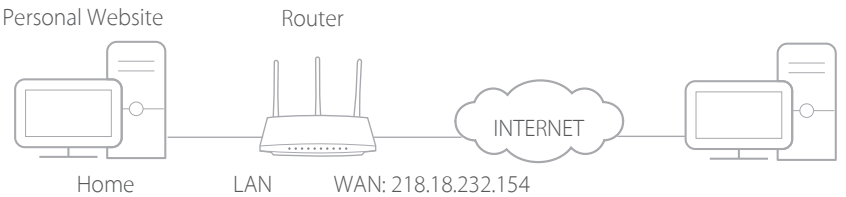
When you build up a server on the local network and want to share it on the internet, Virtual Servers can realize the service and provide it to internet users. At the same time Virtual Servers can keep the local network safe as other services are still invisible from the internet.

Virtual Servers can be used for setting up public services on your local network, such as HTTP, FTP, DNS, POP3/SMTP and Telnet. Different services use different service ports. 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:

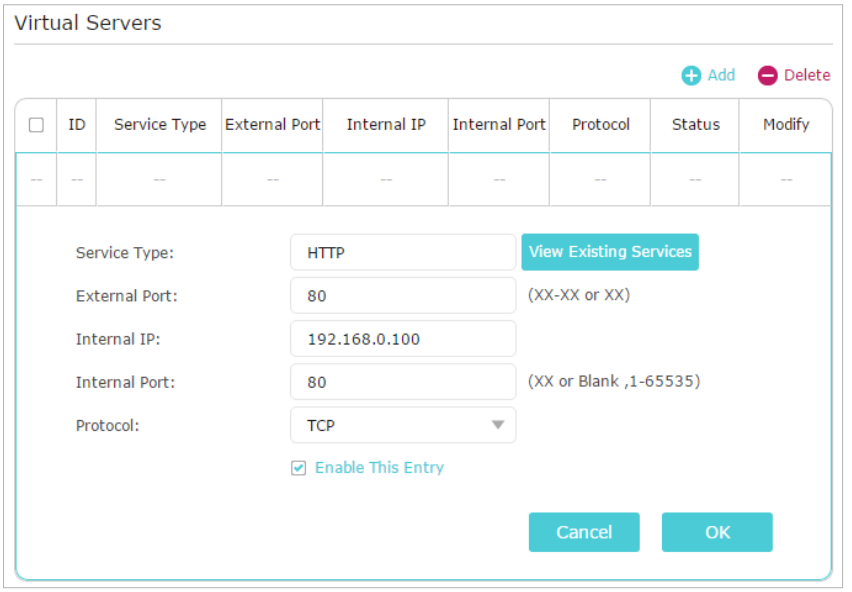
Share my personal website I've built in local network with my friends through the internet.

For example, the personal website has been built on my home PC (192.168.0.100). I hope that my friends on 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 192.168.0.100.
2. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
3. Go to Advanced > NAT Forwarding > Virtual Servers.
4. Click Add. Click View Existing Services and select HTTP. The External Port, Internal Port and Protocol will be automatically filled in. Enter the PC's IP address 192.168.0.100 in the Internal IP field.
5. Click OK.



Tips:

- 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.
- 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.
- You can add multiple virtual server rules if you want to provide several services in a router. Please note that the External Port should not be overlapped.

Done!

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

Tips:

- The WAN IP should be a public IP address. For the WAN IP is assigned dynamically by the ISP, it is recommended to apply and register a domain name for the WAN referring to Set Up a Dynamic DNS Service Account. Then users on the internet can use http:// domain name to visit the website.
- 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.

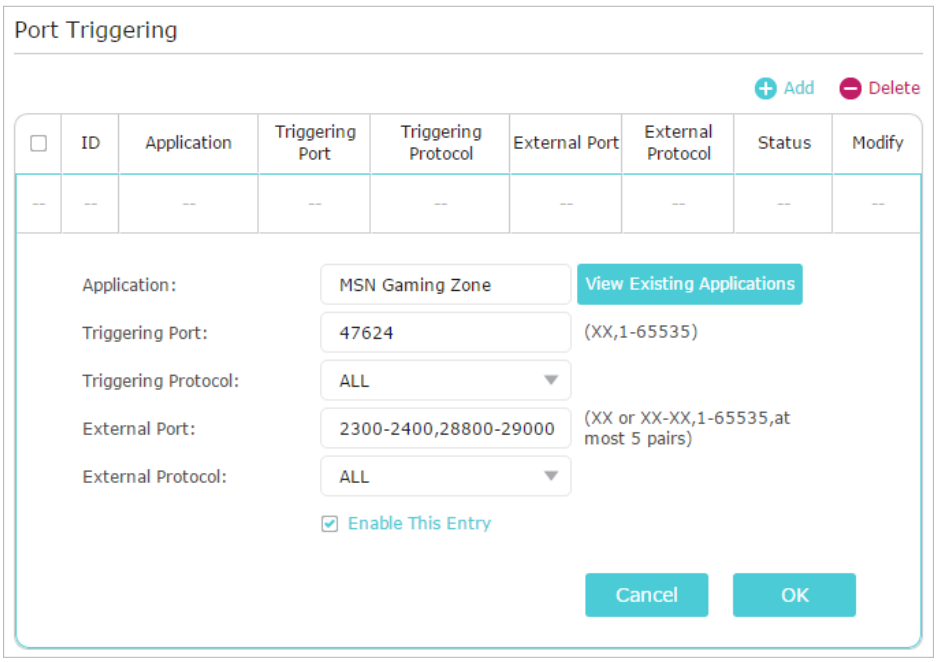
12. 2. Open Ports Dynamically by Port Triggering

Port Triggering can specify a triggering port and its corresponding external ports. When a host on 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, video players and common applications including 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 your TP-Link ID or the password you set for the router.
2. Go to Advanced > NAT Forwarding > Port Triggering and click Add.

3. Click View Existing Applications, and select the desired application. The Triggering Port, External Port and Protocol will be automatically filled in. The following picture takes application MSN Gaming Zone as an example.
4. Click OK.



Tips:

- You can add multiple port triggering rules according to your network need.
- The triggering ports can not be overlapped.
- 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.

12. 3. Make Applications Free from Port Restriction by DMZ

When a PC is set to be a DMZ (Demilitarized Zone) host on the local network, it is totally exposed to the internet, which 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, such as IP camera and database software, you can set the PC to be a DMZ host.

Note:
When DMZ is enabled, the DMZ host is totally exposed to the internet, which may bring some potential safety hazards. If DMZ is not in use, please disable it in time.

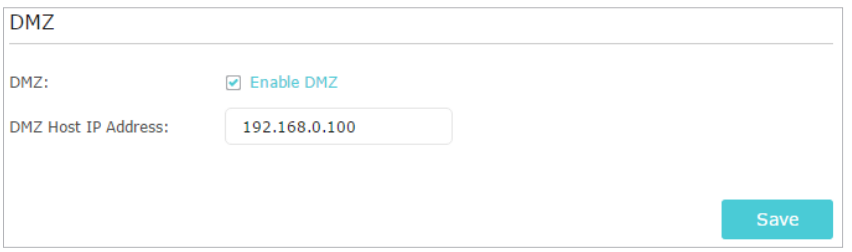
I want to:

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 login normally but cannot join a team with other players. To solve this problem, set your PC as a DMZ host with all ports open.

How can I do that?

1. Assign a static IP address to your PC, for example 192.168.0.100.
2. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
3. Go to Advanced > NAT Forwarding > DMZ and select Enable DMZ.
4. Enter the IP address 192.168.0.100 in the DMZ Host IP Address filed.



5. Click Save.

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.

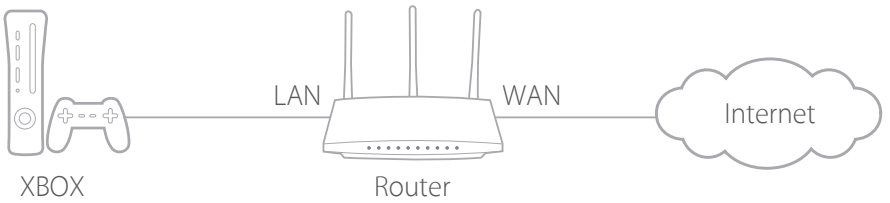
12. 4. Make Xbox Online Games Run Smoothly by UPnP

The UPnP (Universal Plug and Play) protocol allows 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 on the local network and the internet can freely communicate with each other thus 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:

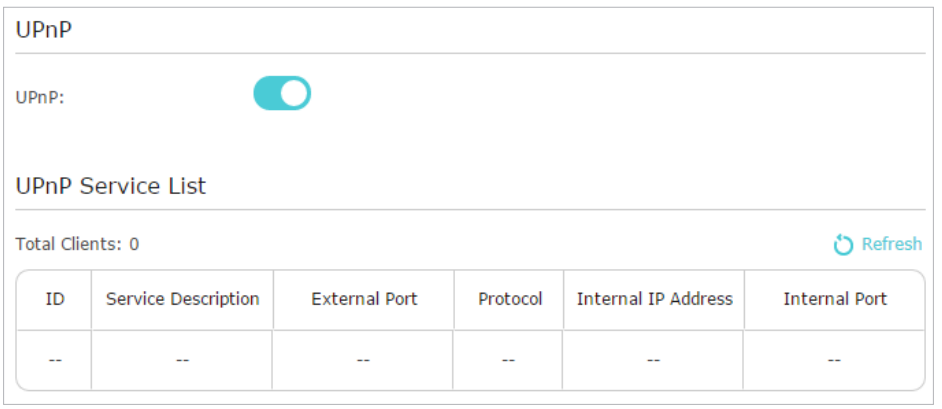
- UPnP is enabled by default in this router.
- Only the application supporting UPnP protocol can use this feature.
- UPnP feature needs the support of operating system (e.g. Windows Vista/ Windows 7/ Windows 8, etc. Some of operating system need to install the UPnP components).

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 allowing 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 your TP-Link ID or the password you set for the router.
2. Go to Advanced > NAT Forwarding > UPnP and toggle on or off according to your needs.



Chapter 13

VPN Server

The VPN (Virtual Private Networking) Server allows you to access your home network in a secured way through internet when you are out of home. The router offers two ways to setup VPN connection: OpenVPN and PPTP (Point to Point Tunneling Protocol) VPN.

OpenVPN is somewhat complex but with greater security and more stable. It is suitable for restricted environment, such as campus network and company intranet.

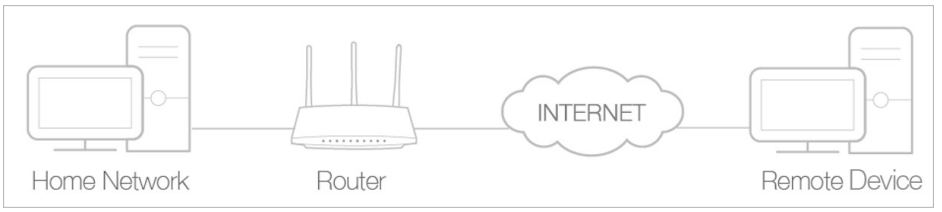
PPTP VPN is more easily used and its speed is faster, it's compatible with most operating systems and also supports mobile devices. Its security is poor and your packets may be cracked easily, and PPTP VPN connection may be prevented by some ISP.

It contains the following sections, please choose the appropriate VPN server connection type as needed.

- Use OpenVPN to Access Your Home Network
- Use PPTP VPN to Access Your Home Network

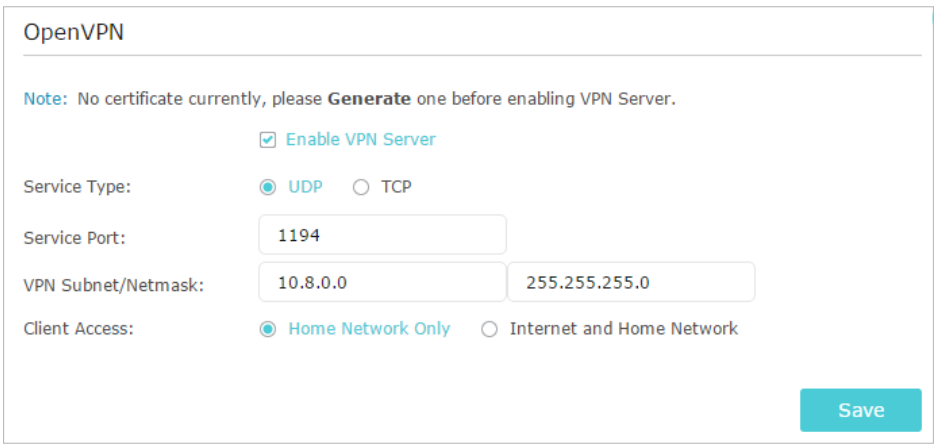
13. 1. Use OpenVPN to Access Your Home Network

In the OpenVPN connection, the home network can act as a server, and the remote device can access the server through the router which acts as an OpenVPN Server gateway. To use the VPN feature, you should enable OpenVPN Server on your router, and install and run VPN client software on the remote device. Please follow the steps below to set up an OpenVPN connection.



13. 1. 1. Step1. Set up OpenVPN Server on Your Router

1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > VPN Server > OpenVPN, and select Enable VPN Server.



Note:

- Before you enable VPN Server, we recommend you configure Dynamic DNS Service (recommended) or assign a static IP address for router's WAN port and synchronize your System Time with internet.
- The first time you configure the OpenVPN Server, you may need to Generate a certificate before you enable the VPN Server.

3. Select the Servive Type (communication protocol) for OpenVPN Server: UDP, TCP.
4. Enter a VPN Service Port to which a VPN device connects, and the port number should be between 1024 and 65535.
5. In the VPN Subnet/Netmask fields, enter the range of IP addresses that can be leased to the device by the OpenVPN server.

6. Select your Client Access type. Select Home Network Only if you only want the remote device to access your home network; select Internet and Home Network if you also want the remote device to access internet through the VPN Server.
7. Click Save.
8. Click Generate to get a new certificate.

Note:
If you have already generated one, please skip this step, or click Generate to update the certificate.

9. Click Export to save the OpenVPN configuration file which will be used by the remote device to access your router.

13. 1. 2. Step 2. Configure OpenVPN Connection on Your Remote Device

1. Visit http://openvpn.net/index.php/download/community-downloads.html to download the OpenVPN software, and install it on your device where you want to run the OpenVPN client utility.

Note:
You need to install the OpenVPN client utility on each device that you plan to apply the VPN funxtion to access your router. Mobile devices should download a third-party app from Google Play or Apple App Store.

2. After the installation, copy the file exported from your router to the OpenVPN client utility's "config" folder (for example, C:\Program Files\OpenVPN\config on Windows). The path depends on where the OpenVPN client utility is installed.
3. Run the OpenVPN client utility and connect it to OpenVPN Server.

13. 2. Use PPTP VPN to Access Your Home Network

PPTP VPN Server is used to create a VPN connection for remote device. To use the VPN feature, you should enable PPTP VPN Server on your router, and configure the PPTP connection on the remote device. Please follow the steps below to set up a PPTP VPN connection.

13. 2. 1. Step 1. Set up PPTP VPN Server on Your Router

1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > VPN Server > PPTP VPN, and select Enable VPN Server.

Note:

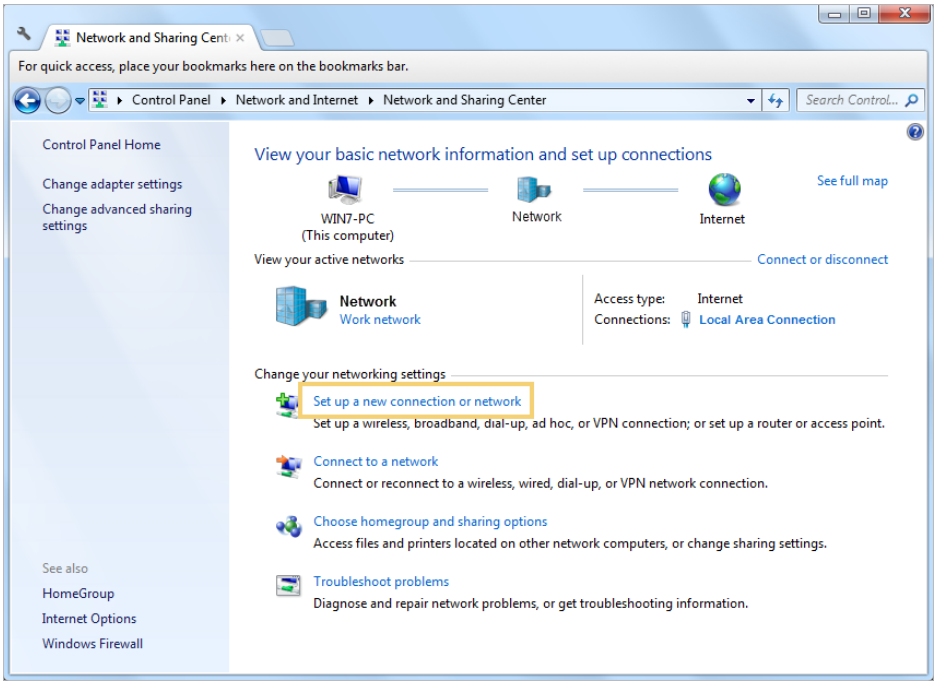
Before you enable VPN Server, we recommend you configure Dynamic DNS Service (recommended) or assign a static IP address for router's WAN port and synchronize your System Time with internet.

3. In the Client IP Address filed, enter the range of IP addresses (up to 10) that can be leased to the devices by the PPTP VPN server.
4. Enter the Username and Password to authenticate clients to the PPTP VPN server.
5. Click Save.

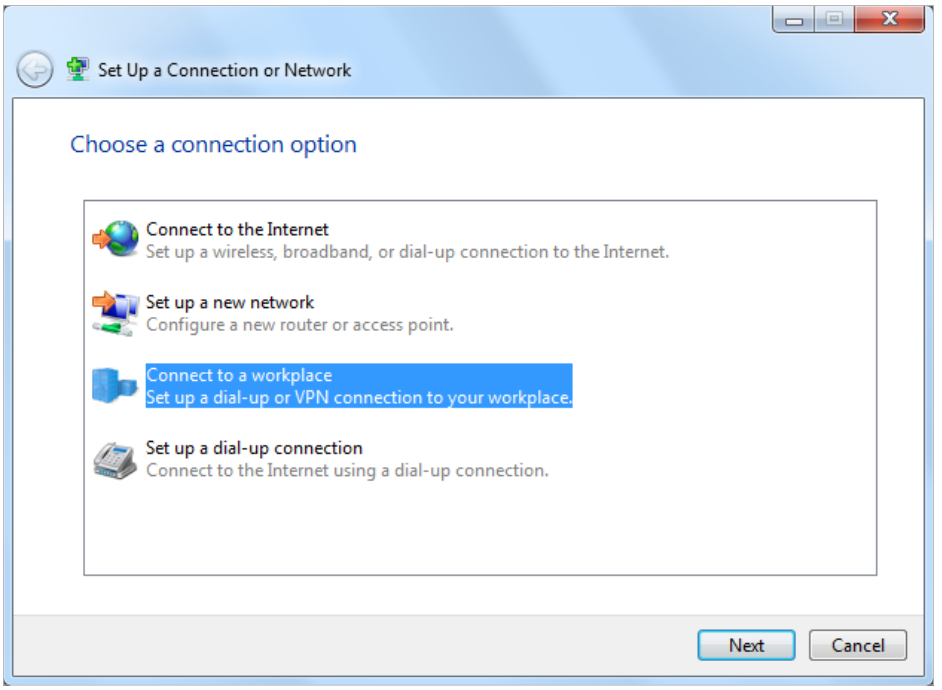
13. 2. 2. Step 2. Configure PPTP VPN Connection on Your Remote Device

The remote device can use the Windows built-in PPTP software or a third-party PPTP software to connect to PPTP Server. Here we use the Windows built-in PPTP software as an example.

1. Go to Start > Control Panel > Network and Internet > Network and Sharing Center.
2. Select Set up a new connection or network.

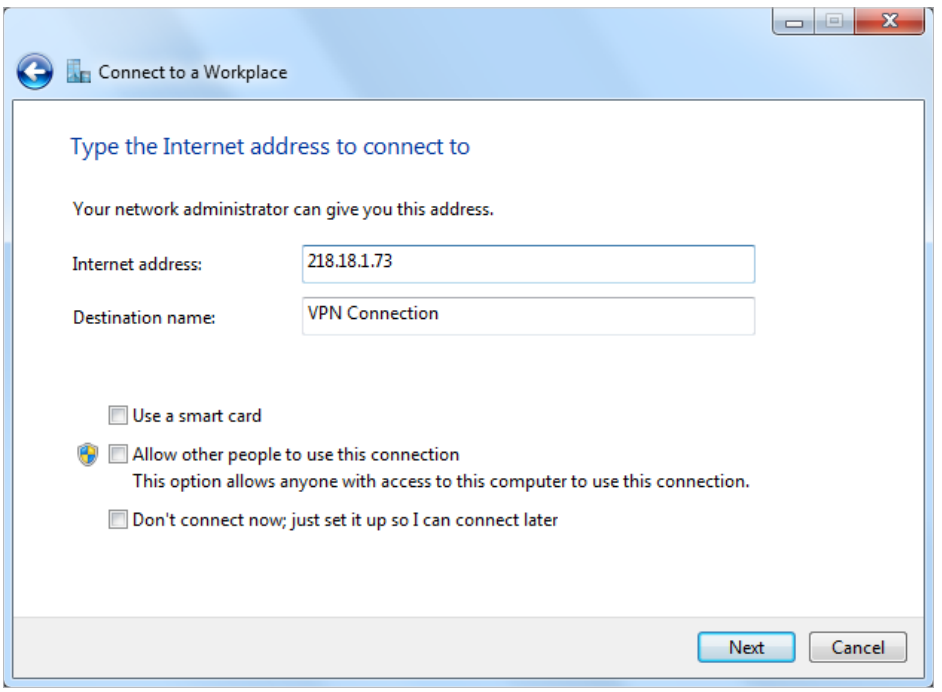


3. Select Connect to a workplace and click Next.

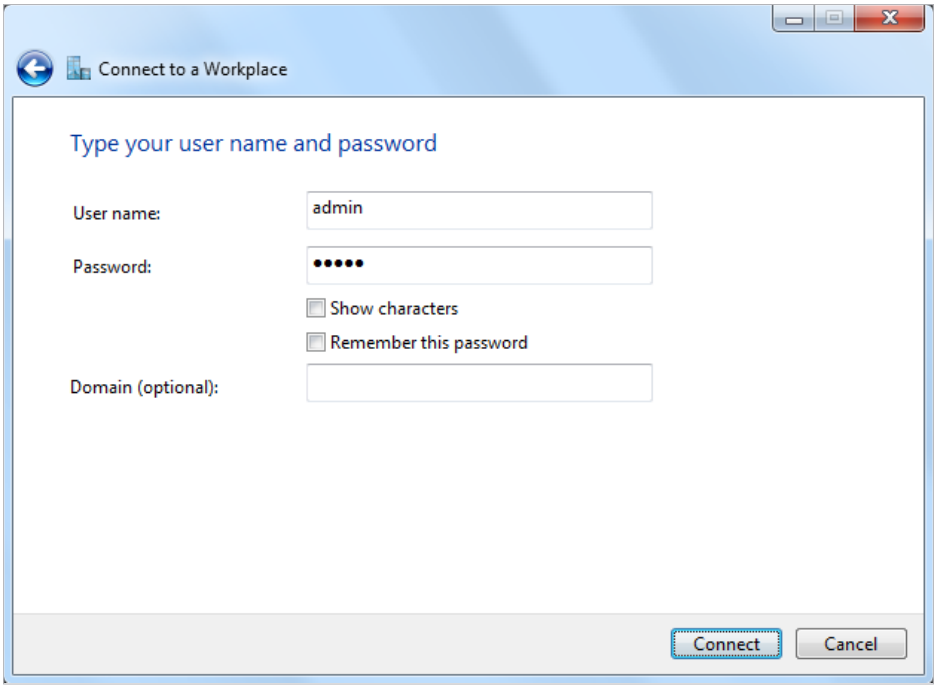


4. Select Use my Internet connection (VPN).

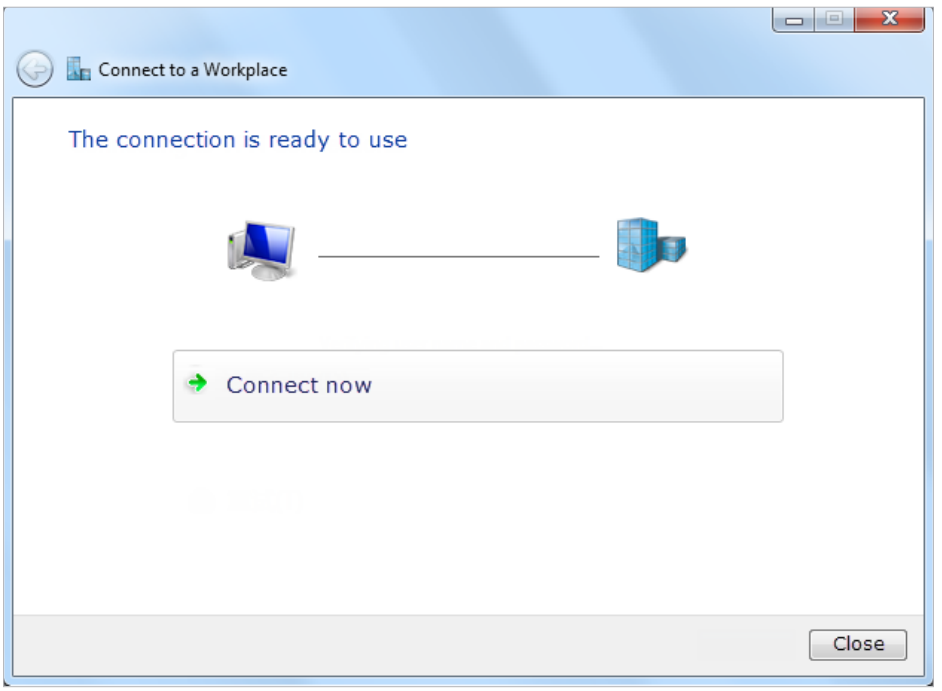
5. Enter the internet IP address of the router (for example: 218.18.1.73) in the Internet address field. Click Next.



6. Enter the User name and Password you have set for the PPTP VPN server on your router, and click Connect.



7. The PPTP VPN connection is created and ready to use.



Chapter 14

Customize Your Network Settings

This chapter guides you on how to configure advanced network features.

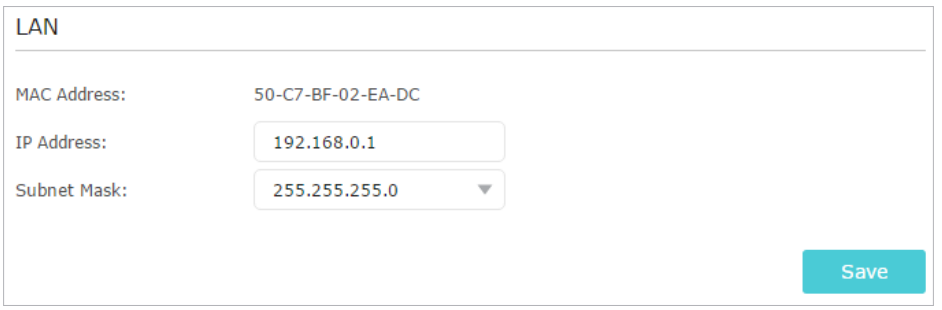
It contains the following sections:

- Change the LAN Settings
- Set Up Link Aggregation
- Configure to Support IPTV Service
- Specify DHCP Server Settings
- Set Up a Dynamic DNS Service Account
- Create Static Routes
- Specify Wireless Settings
- Use WPS for Wireless Connection
- Schedule Your Wireless Function

14. 1. Change the LAN Settings

The router is preset with a default LAN IP 192.168.0.1, 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 on your local network or your network requires a specific IP subnet, you can change it.

1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > Network > LAN.
3. Type in a new IP Address appropriate to your needs. And leave the Subnet Mask as the default settings.



4. Click Save.

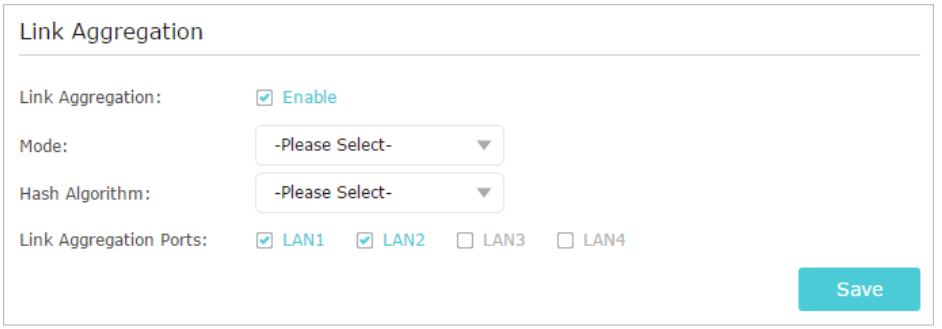
Note:

If you have set the Virtual Server, DMZ or DHCP address reservation, and the new LAN IP address is not in the same subnet with the old one, then you should reconfigure these features.

14. 2. Set Up Link Aggregation

The Link Aggregation feature combines two ports together to make a single highbandwidth data path, thus sustaining a higher-speed and more stable wired network.

1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > Network > LAN.



3. Enable Link Aggregation.
4. Select aggregation Mode and Hash Algorithm.
5. Specify two ports for link aggregation.
6. Click Save.

14. 3. Configure to Support IPTV Service

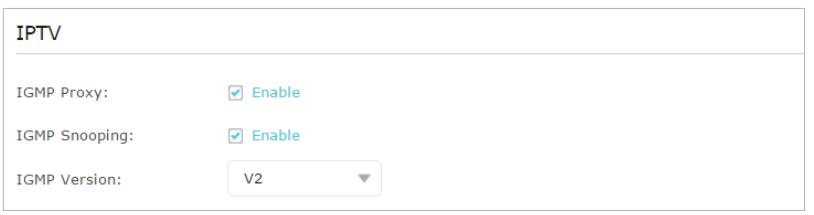
I want to:

Configure IPTV setup to enable Internet/IPTV/Phone service provided by my internet service provider (ISP).

How can I do that?

1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > Network > IPTV.
3. **If your ISP provides the networking service based on IGMP technology**, e.g., British Telecom(BT) and Talk Talk in UK:

   1) Check the box for IGMP Proxy and select the IGMP Version, either V2 or V3, as required by your ISP.



   2) Click Save.

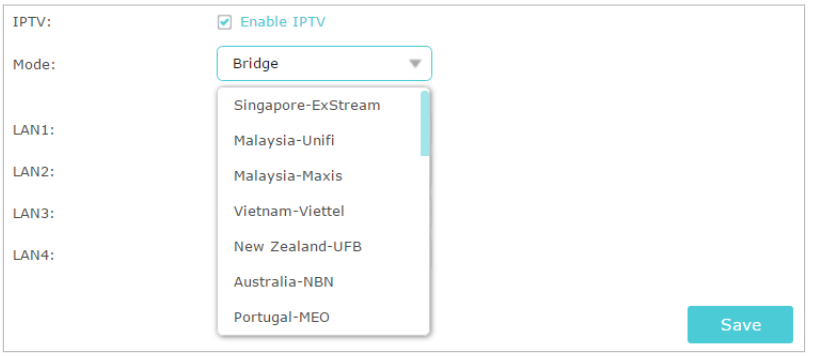
   3) After configuring IGMP proxy, IPTV can work behind your router now. You can connect your set-top box to any of the router's Ethernet port.

   If IGMP is not the technology your ISP applies to provide IPTV service:

   1) Tick Enable IPTV.

2) Select the appropriate Mode according to your ISP.

- Select Bridge if your ISP is not listed and no other parameters are required.
- Select Custom if your ISP is not listed but provides necessary parameters.



3) After you have selected a mode, the necessary parameters, including the LAN port for IPTV connection, are predetermined. If not, select the LAN type to determine which port is used to support IPTV service.

4) Click Save.

5) Connect the set-top box to the corresponding LAN port which is predetermined or you have specified in Step 3.

Done!

Your IPTV setup is done now! You may need to configure your set-top box before enjoying your TV.

Tips:

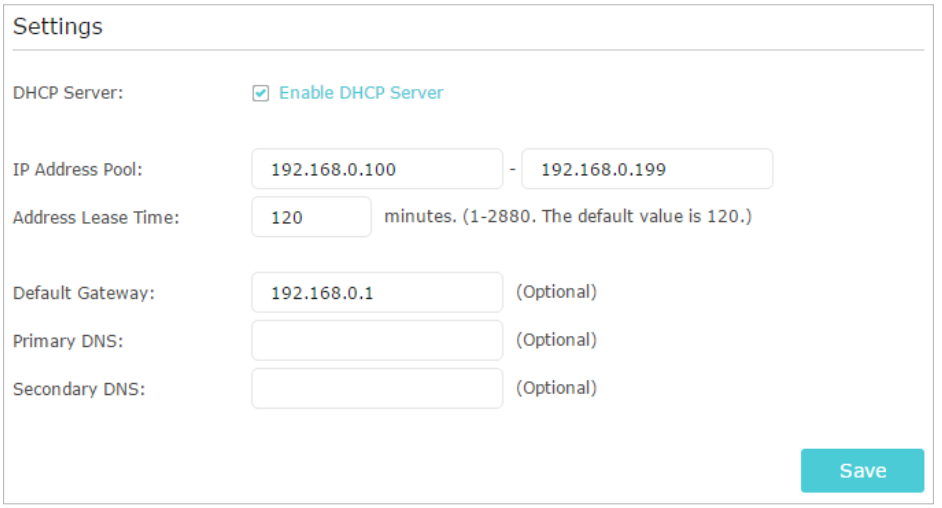
Qos and IPTV cannot be enabled at the same time.

14. 4. Specify DHCP Server Settings

By default, the DHCP (Dynamic Host Configuration Protocol) Server is enabled and the router acts as a DHCP server; it dynamically assigns TCP/IP parameters to client devices from the IP Address Pool. You can change the settings of the DHCP Server if necessary, and you can reserve LAN IP addresses for specified client devices.

1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > Network > DHCP Server.

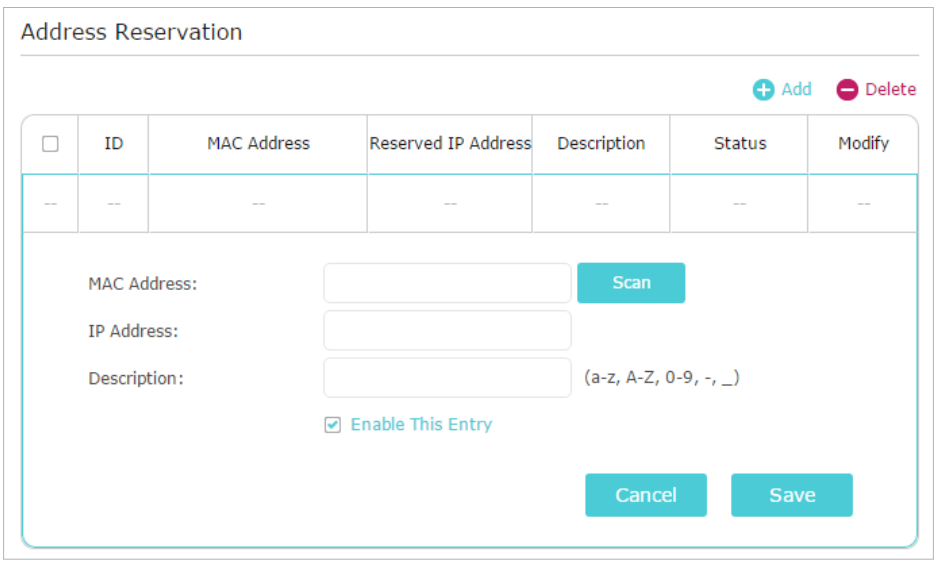
➢ **To specify the IP address that the router assigns:**



1. Check the box for Enable DHCP Server.
2. Enter the starting and ending IP addresses in the IP Address Pool.
3. Enter other parameters if the ISP offers. The Default Gateway is automatically filled in and is the same as the LAN IP address of the router.
4. Click Save.

➢ **To reserve an IP address for a specified client device:**

1. Click Add in the Address Reservation section.



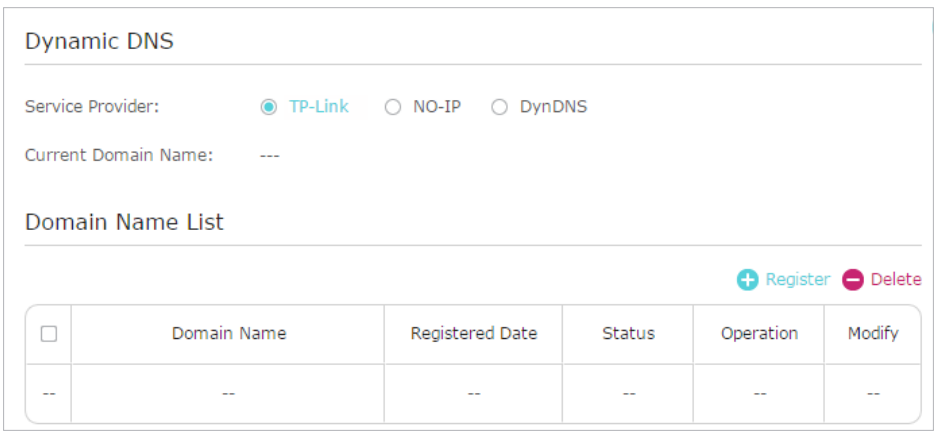
2. Click Scan or enter the MAC address of the client device.
3. Enter the IP address to reserve for the client device.
4. Enter the Description for this entry.
5. Tick the Enable This Entry checkbox and click OK.

14. 5. Set Up a Dynamic DNS Service Account

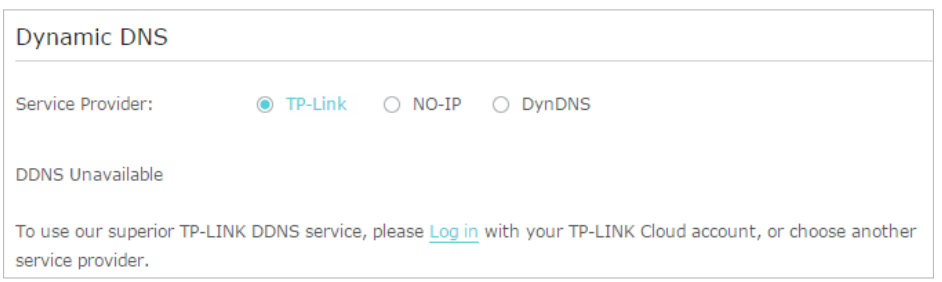
Most ISPs assign a dynamic IP address to the router and you can use this IP address to access your router remotely. However, the IP address can change from time to time and you don't know when it changes. In this case, you might apply the DDNS (Dynamic Domain Name Server) feature on the router to allow you and your friends to access your router and local servers (FTP, HTTP, etc.) using a domain name without 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.

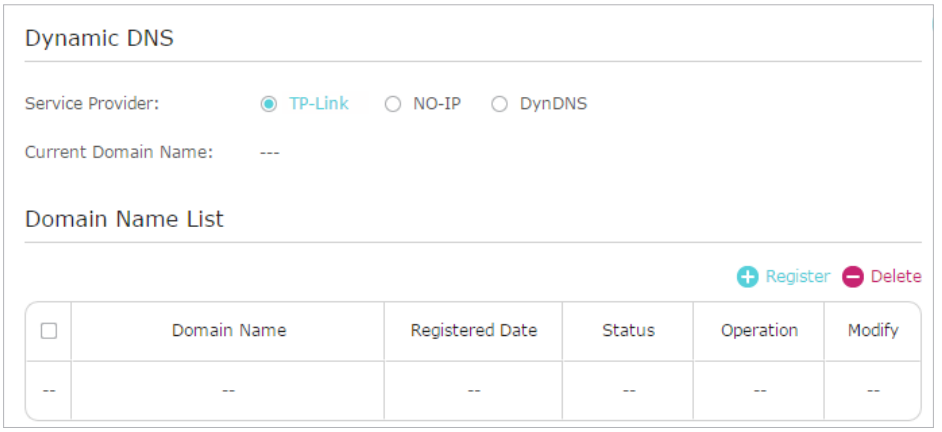
1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > Network > Dynamic DNS.
3. Select the DDNS Service Provider (TP-Link, NO-IP or DynDNS). It is recommended to select TP-Link so that you can enjoy TP-Link's superior DDNS service. Otherwise, please select NO-IP or DynDNS. If you don't have a DDNS account, you have to register first by clicking Go to register.



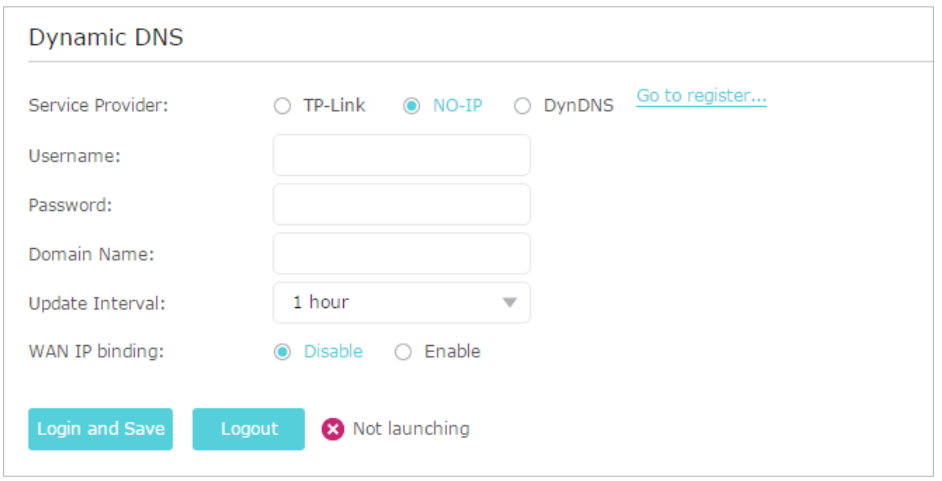
Note:
To enjoy TP-Link's DDNS service, you have to log in with a TP-Link ID. If you have not logged in with one, click Log in.



4. Click Register in the Domain Name List if you have chosen TP-Link, and enter the Domain Name as needed.



If you have chosen NO-IP or DynDNS, enter the username, password and domain name of your account.



5. Click Login and Save.

Tips:
If you want to use a new DDNS account, please click logout first, and then log in with a new account.

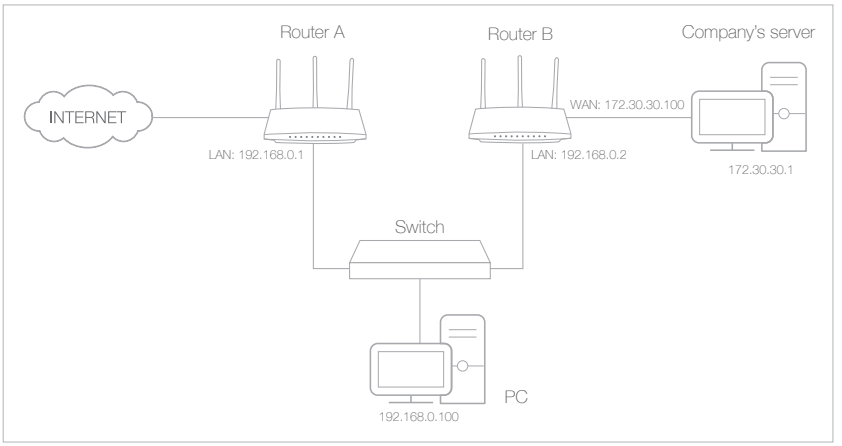
14. 6. Create Static Routes

Static routing is a form of routing that is configured manually by a network administrator or a user by adding entries into a routing table. The manually-configured routing information guides the router in forwarding data packets to the specific destination.

I want to: Visit multiple networks and servers at the same time.

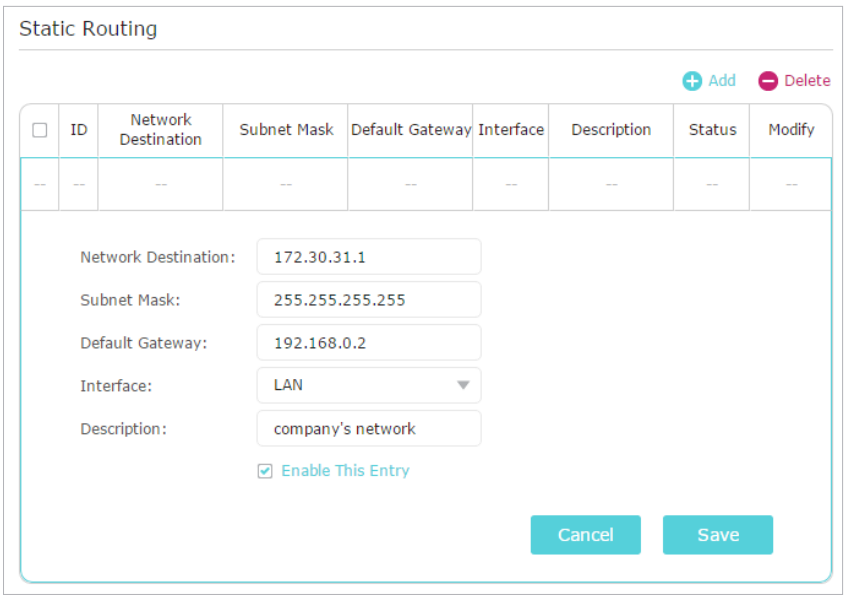
For example, in a small office, my PC can surf the internet through Router A, but I also want to visit my company's network. Now I have a switch and Router B. I connect the devices as shown in the following figure so that the physical connection between my PC and my company's server is established. To 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. Change the routers' LAN IP addresses to two different IP addresses on the same subnet. Disable Router B's DHCP function.
2. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for Router A.
3. Go to Network > Static Routing.
4. Click Add and finish the settings according to the following explanations:



Network Destination: 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 Router A. In the example, the IP address of the company network is the destination IP

address, so here enter 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 enter 255.255.255.255.

Default 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 data. In the example, the data packets will be sent to the LAN port of Router B and then to the Server, so the default gateway should be 192.168.0.2.

Interface: Determined by the port (WAN/LAN) that sends out data packets. In the example, the data are sent to the gateway through the LAN port of Router A, so LAN should be selected.

Description: Enter a description for this static routing entry.

5. Click Save.
6. Check the System Routing Table below. If you can find the entry you've set, the static routing is set successfully.

System Routing Table

Active Routes Number: 1 Refresh

ID	Network Destination	Subnet Mask	Gateway	Interface
1	192.168.0.0	255.255.255.0	0.0.0.0	lan

Done!

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

14. 7. Specify 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 label of the router. You can customize the wireless settings according to your needs.

Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.

➢ **To enable or disable the wireless function:**

1. Go to Basic > Wireless.

2. The wireless radio is enabled by default. If you want to disable the wireless function of the router, just uncheck the box for Enable Wireless Radio. In this case, all the wireless settings will be invalid.

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

1. Go to Basic > Wireless.
2. Create a new SSID in Network Name (SSID) and customize the password for the network in Password. The value is case-sensitive.

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

➢ **To hide SSID:**

1. Go to Basic > Wireless.
2. Select Hide SSID, and your SSID won't display when you scan for local wireless networks on your wireless device and you need to manually join the network.

➢ **To change the security option:**

1. Go to Advanced > Wireless > Wireless Settings.
2. Select the wireless network 2.4GHz or 5GHz.
3. Select an option from the Security drop-down list. We recommend you don't change the default settings unless necessary. If you select other options, configure the related parameters according to the help page.

In addition

- Mode - Select a transmission mode according to your wireless client devices. It is recommended to just leave it as default.
- Channel Width - Select a channel width (bandwidth) for the wireless network.
- Channel - Select an operating channel for the wireless network. It is recommended to leave the channel to Auto, if you are not experiencing the intermittent wireless connection issue.
- Transmit Power - Select either High, Middle or Low to specify the data transmit power. The default and recommended setting is High.

14. 8. 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.

14. 8. 1. Method 1: Use the WPS Button

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

1. Press the WPS button of 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.

14. 8. 2. Method 2: Use the WPS Button on the Web Management Page

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

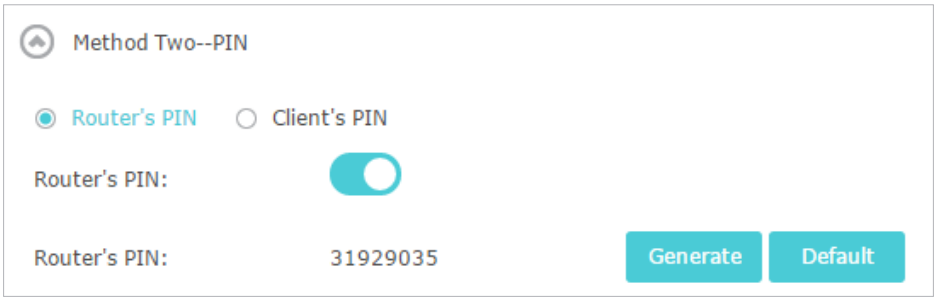
1. Visit http://tplinkmodem.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > Wireless > WPS.

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

14. 8. 3. 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://tplinkmodem.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > Wireless > WPS. Click Method Two--PIN.



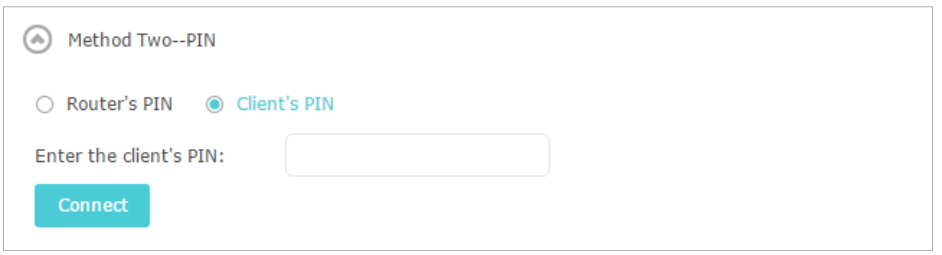
3. Take a note of the router's PIN. You can also click Generate to get a new PIN.
4. On the client device, enter the router's PIN. (The default PIN is also printed on the label of the router.)
5. The WPS LED flashes for about two minutes during the WPS process.
6. When the WPS LED is on, the client device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

Note:

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

14. 8. 4. Method 4: Enter the Client Device's PIN on the Router

1. Visit http://tplinkmodem.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > Wireless > WPS. Click Method Two--PIN.



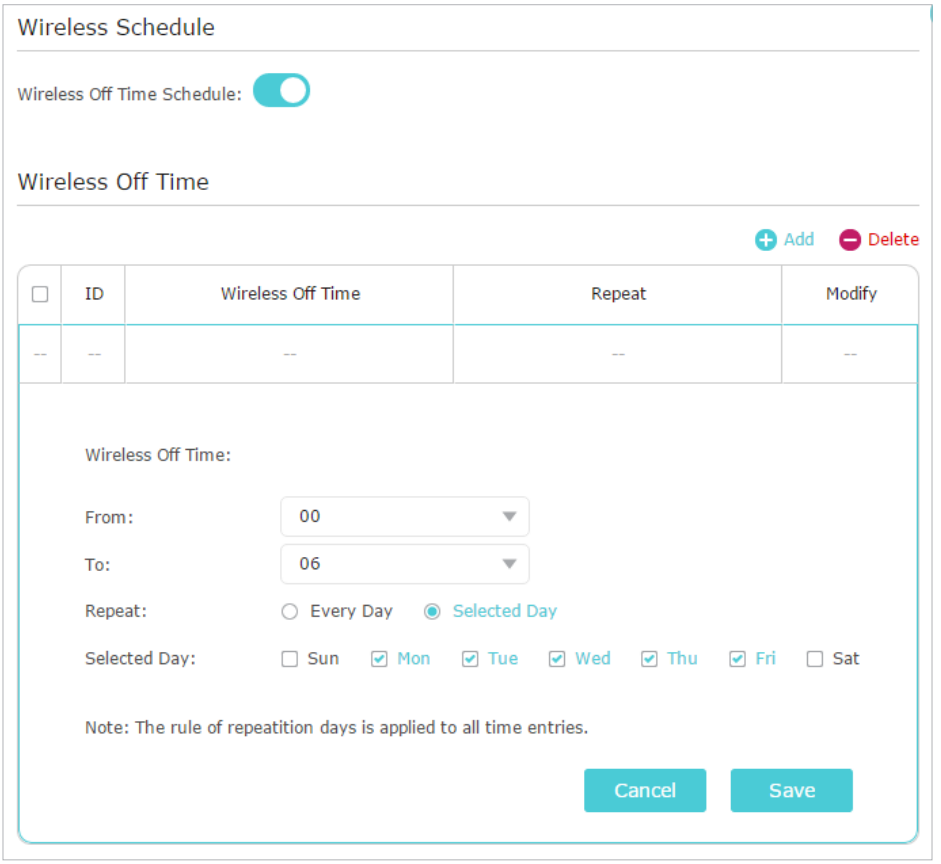
3. Select Client's PIN.
4. Enter the client device's PIN in the field. Then click the Connect button.
5. Connect successfully will appear on the above screen, which means the client device has successfully connected to the router.

14. 9. Schedule Your Wireless Function

The wireless network(s) can be automatically off at a specific time when you do not need the wireless connection.

1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > Wireless > Wireless Schedule.

3. Toggle on the button to enable the Wireless Schedule feature.



4. Click Add to set the Wireless Off Time, and click Save.

5. Repeat Step 3 and 4 to set another entry if needed.

Note:

- Make sure that the time of the router is correct before applying this function. For details, refer to Set Up System Time.
- The wireless LEDs (2.4GHz and 5GHz) will be off if the wireless schedule takes effect.
- The wireless network(s) will be automatically turned on after the time period you have set.

Chapter 15

Manage the Router

This chapter will show you the configuration for managing and maintaining your router.

It contains the following sections:

- Set Up System Time
- Control LEDs
- Test the Network Connectivity
- Set Up Port Mirroring
- Upgrade the Firmware
- Backup and Restore Configuration Settings
- Set the Router to Reboot Regularly
- Change the Administrator Account
- Default Password Recovery
- Local Management
- Remote Management
- System Log
- Monitor the Internet Traffic Statistics

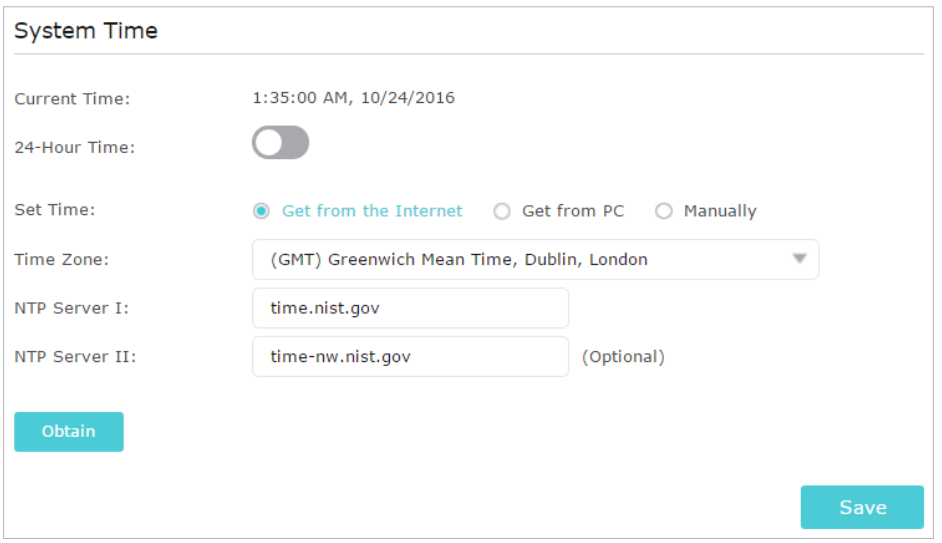
15. 1. Set Up System Time

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. You can choose the way to obtain the system time as needed.

1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > System Tools > Time Settings.
3. If you want the time to be displayed in 24-hour format, toggle on the 24-Hour Time button.

➢ **To get time from the Internet:**

1. In the Set Time field, select Get from the Internet.

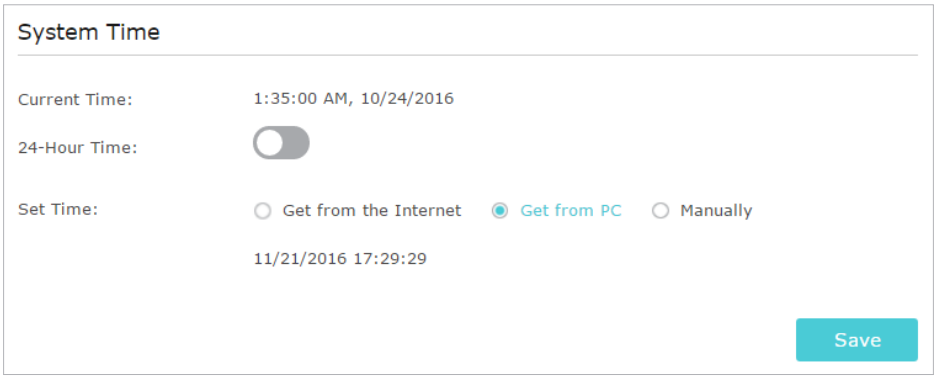


2. Select your local Time Zone from the drop-down list.
3. In the NTP Server I fileld, enter the IP address or domain name of your desired NTP Server.
4. (Optional) In the NTP Server II fileld, enter the IP address or domain name of the second NTP Server.
5. Click Obtain to get the current internet time and click Save.

➢ **To get time from PC**

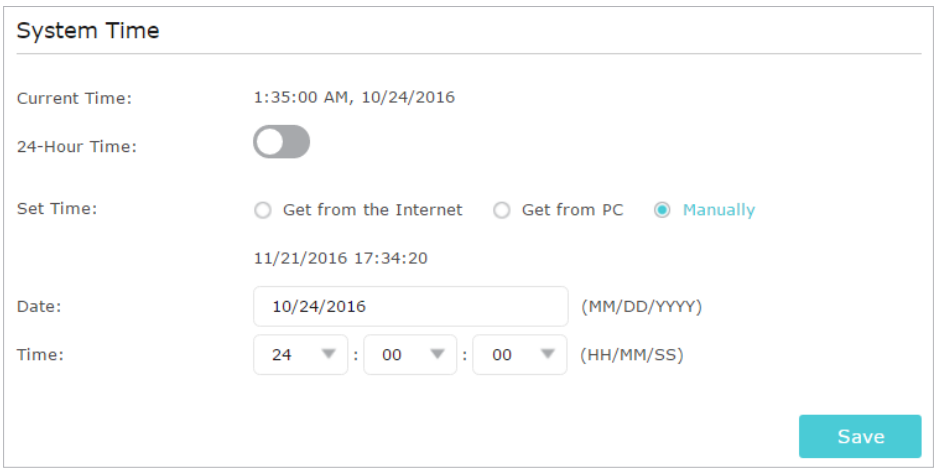
1. In the Set Time field, select Get from PC.
2. The current system time and date of your PC will display below. Click Save.

Tips:
Make sure the time on your PC is correct if you want to get the PC's system time.



➢ **To manually set the time:**

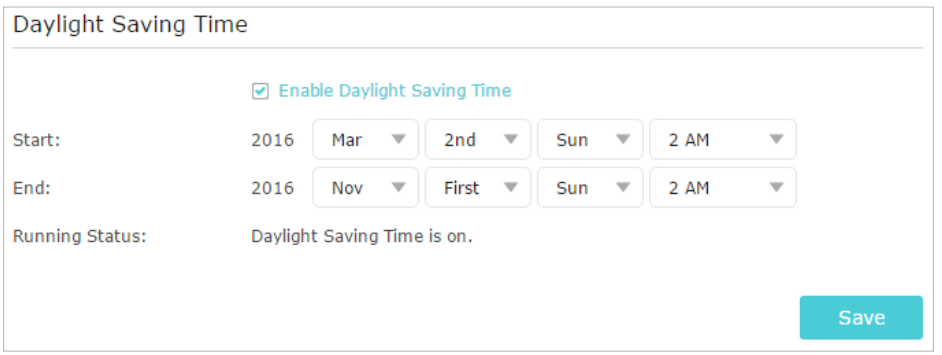
1. In the Set Time field, select Manually.



2. Set the current Date (In MM/DD/YYYY format).
3. Set the current Time (In HH/MM/SS format).
4. Click Save.

➢ **To set up Daylight Saving Time:**

1. Select Enable Daylight Saving Time.

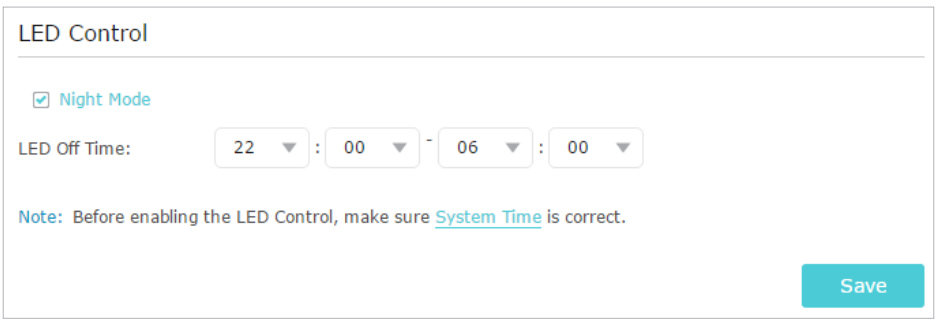


2. Select the correct Start date and time when daylight saving time starts at your local time zone.
3. Select the correct End date and time when daylight saving time ends at your local time zone.
4. Click Save.

15. 2. Control LEDs

The router's LEDs indicate router's activities and status. You can turn on or turn off the LEDs either from the web management page or by pressing the LED button.

1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > System Tools > LED Control.
3. Tick the Night Mode checkbox.
4. Specify a time period in the LED Off Time as needed, and the LEDs will be off during this period.

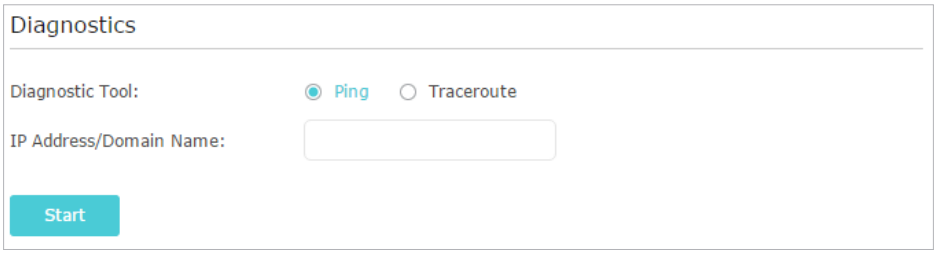


5. Click Save.

15. 3. Test the Network Connectivity

Diagnostics is used to test the connectivity between the router and the host or other network devices.

1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > System Tools > Diagnostics.



3. Enter the information with the help of page tips:

1) Choose Ping or Traceroute as the diagnostic tool to test the connectivity;

- Ping is used to test the connectivity between the router and the tested host, and measure the round-trip time.
- Traceroute is used to display the route (path) your router has passed to reach the tested host, and measure transit delays of packets across an Internet Protocol network.

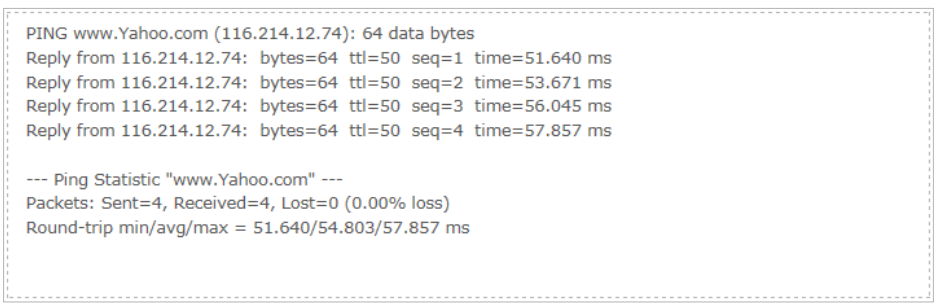
2) Enter the IP Address or Domain Name of the tested host.

4. Click Start to begin the diagnostics.

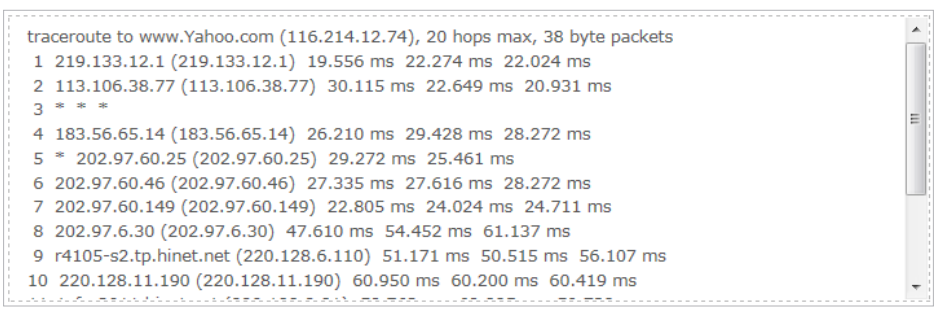
Tips:

Click Advanced, you can modify the ping count, ping packet size or the Traceroute Max TTL. It's recommended to keep the default value.

The figure below indicates the proper connection between the router and the Yahoo server (www.Yahoo.com) tested through Ping.



The figure below indicates the proper connection between the router and the Yahoo server (www.Yahoo.com) tested through Traceroute.

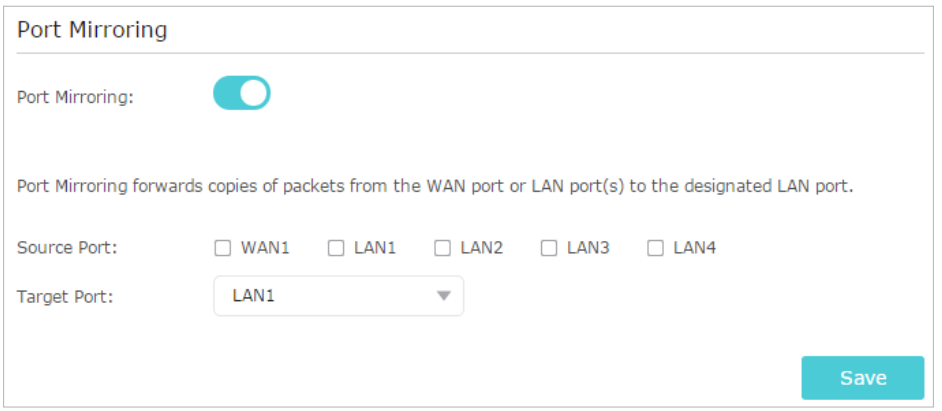


15. 4. Set Up Port Mirroring

Port Mirroring refers to the process of forwarding copies of packets from a mirrored port to a mirroring port. Usually, the mirroring port is connected to a data diagnose device, which is used to analyze the mirrored packets for monitoring and troubleshooting the network.

➢ **To forward copies of packets to the designated port:**

1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > System Tools > Diagnostics, and focue on the Port Mirroring section.
3. Enable Port Mirroring.



4. Select the desired port(s) as Source Port(s).
5. Select a desired port as Target Port.
6. Click Save.

Note:
A port cannot be set as the Source Port and the Target Port simultaneously.

15. 5. Upgrade the Firmware

TP-Link aims at providing better network experience for users.

We will inform you throught the web management page if there's any update firmware available for your router. Also, the latest firmware will be released at the TP-Link official website www.tp-link.com, and you can download it from the Support page for free.

Note:
- Make sure you remove all attached USB devices from the router before the firmware upgrade to prevent data loss.
- Backup your router configuration before firmware upgrade.
- Do NOT turn off the router during the firmware upgrade.

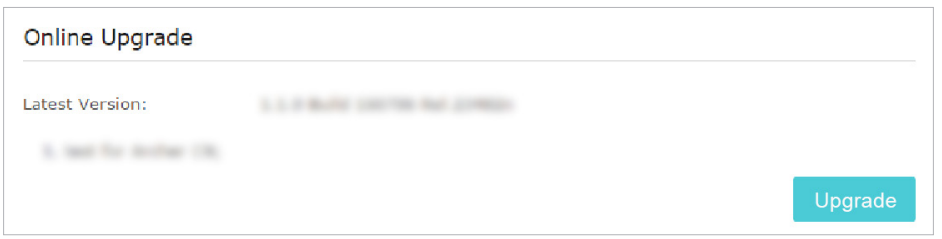
15. 5. 1. Online Upgrade

1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. When the latest firmware is available for your router, the update icon

will display in the top-right corner of the page. Click the icon to go to the Firmware Upgrade page.

   Alternatively, you can go to Advanced > System Tools > Firmware Upgrade, and click Check for upgrade to see whether the latest firmware is released.

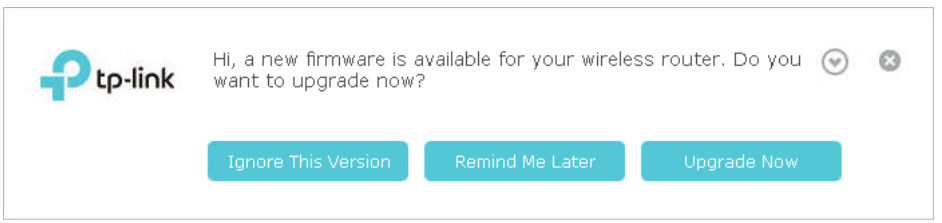
3. Focus on the Online Upgrade section, and click Upgrade.



4. Wait a few minutes for the upgrade and reboot to complete.

Tips:

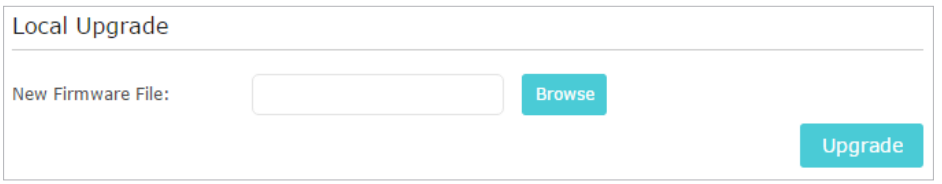
If there's a new and important firmware update for your router, you will see the notification (similar as shown below) on your computer as long as a web browser is opened. Click Upgrade now, and log into the web management page with the username and password you set for the router. You will see the Firmware Upgrade page.



15. 5. 2. Local Upgrade

1. Download the latest firmware file for the router from www.tp-link.com.
2. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
3. Go to Advanced > System Tools > Firmware Upgrade.

4. Focus on the Device Information section. Make sure the downloaded firmware file is matched with the Hardware Version.
5. Focus on the Local Upgrade section. Click Browse to locate the downloaded new firmware file, and click Upgrade.



6. Wait a few minutes for the upgrade and reboot to complete.

15. 5. 3. Restore Interrupted Upgrade after Power Failure

If your router cannot start up after an upgrade interruption due to power failure, follow the steps below to restore the interrupted upgrade. Otherwise, your router cannot work again.

1. Make sure you have the latest firmware file in your computer. If not, try another way to connect your computer to the Internet and download the latest firmware file from www.tp-link.com.
2. Connect your computer to the router with an Ethernet cable.
3. Visit 192.168.0.1 and you will see the following upgrade page.

4. Click Browse and select the downloaded firmware file.
5. Click Upgrade and wait for a few minutes until the router completes the upgrading and restarts.

15. 6. Backup and Restore Configuration Settings

The configuration settings are stored as a configuration file in the router. You can backup 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 necessary you can erase the current settings and reset the router to the default factory settings.

1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.

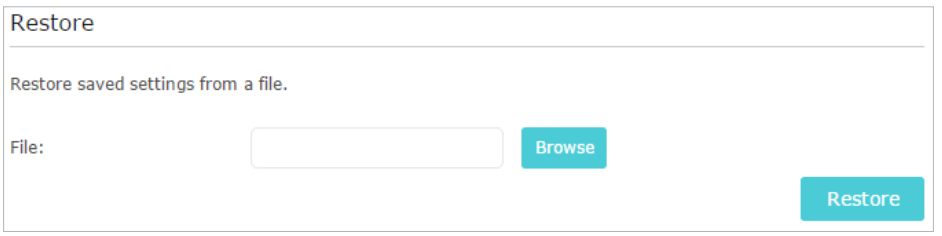
2. Go to Advanced > System Tools > Backup & Restore.

➢ **To backup configuration settings:**

Click Backup to save a copy of the current settings to your local computer. A '.bin' file of the current settings will be stored to your computer.

➢ **To restore configuration settings:**

1. Click Browse to locate the backup configuration file stored on your computer, and click Restore.

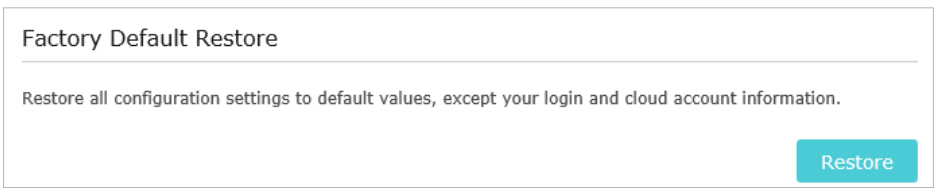


2. Wait a few minutes for the restoring and rebooting.

Note: During the restoring process, do not turn off or reset the router.

➢ **To reset the router except your login password and bound TP-Link ID:**

1. Click Restore under the Factory Default Restore session.



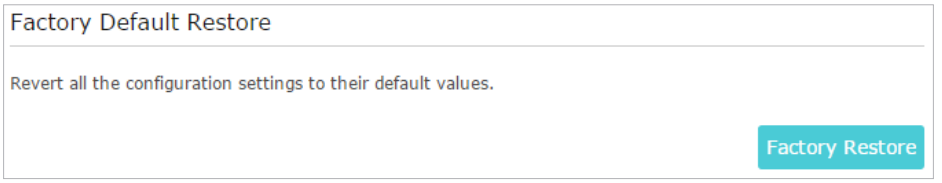
2. Wait a few minutes for the resetting and rebooting.

Note:

- During the resetting process, do not turn off the router.
- After reset, you can still use the current login password or the TP-Link ID to log in to the web management page.

➢ **To reset the router to factory default settings:**

1. Click Factory Restore to reset the router.



2. Wait a few minutes for the resetting and rebooting.

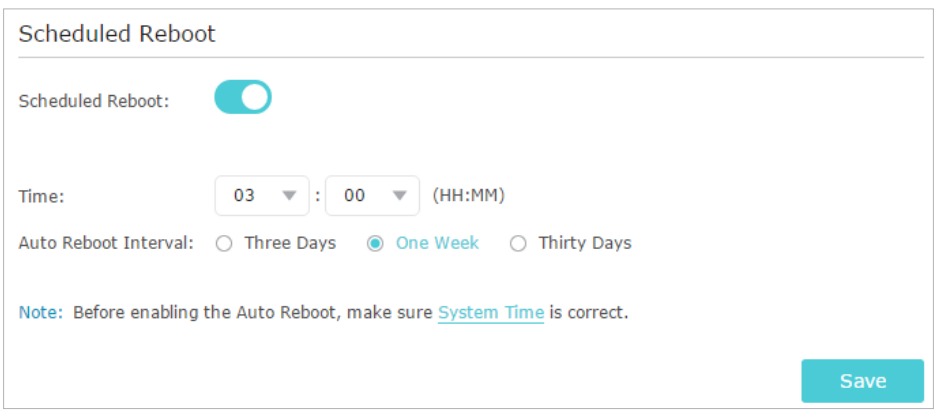
Note:

- During the resetting process, do not turn off or reset the router.
- We strongly recommend you backup the current configuration settings before resetting the router.

15. 7. Set the Router to Reboot Regularly

The Scheduled Reboot feature cleans the cache to enhance the running performance of the router.

1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > System Tools > Scheduled Reboot.
3. Toggle on Scheduled Reboot.
4. Specify the Time when the router reboots and Auto Reboot Interval to decide how often it reboots.



5. Click Save.

15. 8. Change the Administrator Account

The account management feature allows you to change your login password of the web management page.

Note:

If you are using a TP-Link ID to log in to the web management page, the account management feature will be disabled. To manage the TP-Link ID, go to Basic > TP-Link Cloud.

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

2. Go to Advanced > System Tools > Administration and focus on the Account Management section.

3. Enter the old password, then a new password twice (both case-sensitive). Click Save.
4. Use the new password for future logins.

15. 9. Default Password Recovery

This feature allows you to recover the login password you set for you router in case you forget it.

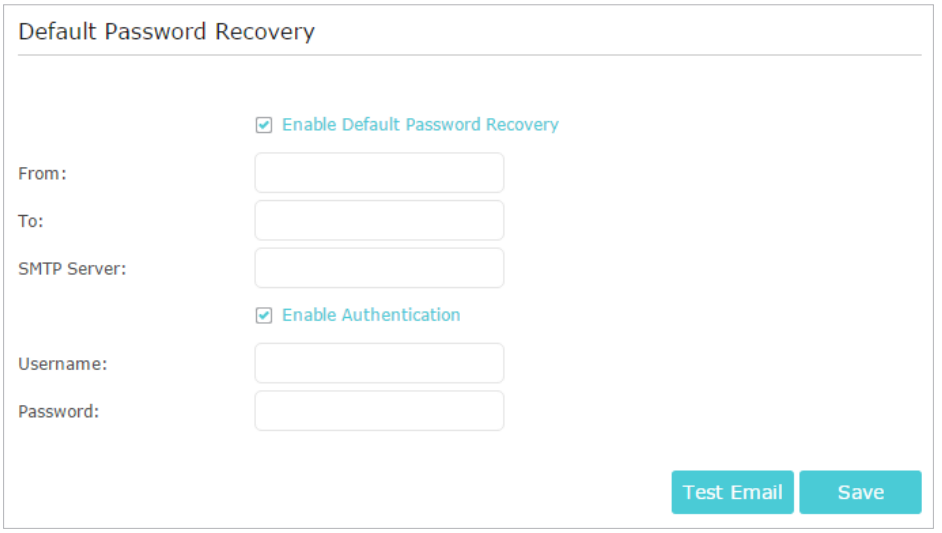
Note:

If you are using a TP-Link ID to log in to the web management page, the Password Recovery feature will be disabled. To manage the TP-Link ID, go to Basic > TP-Link Cloud.

1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Advanced > System Tools > Administration and focus on the Default Password Recovery section.
3. Check the box for Enable Default Password Recovery.
4. Specify a mailbox (From) for sending the recovery letter and enter its SMTP Server address. Specify a mailbox (To) for receiving the recovery letter. If the mailbox (From) to send the recovery letter requires encryption, select Enable Authentication and enter its username and password.

   Tips:

   - SMTP server is available for users in most webmail systems. For example, the SMTP server address of Gmail is smtp.gmail.com. You can refer to their Help page to learn the SMTP server address.
   - Generally, Enable Authentication should be selected if the login of the mailbox requires username and password.



5. Click Save.

You can click Test Email to test whether the configuration is successful.

To recover the login password, please visit http://tplinkwifi.net, click Forgot Password? on the login page and follow the instructions to set a new password.

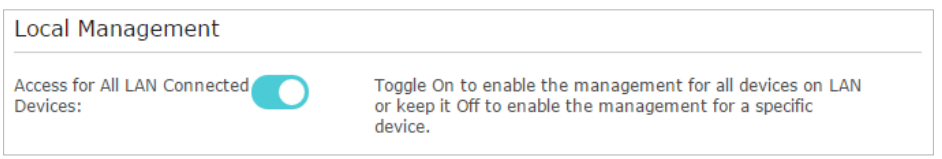
15. 10. Local Management

This feature allows you to limit the number of client devices on your LAN from accessing the router by using the MAC address-based authentication.

1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > System Tools > Administration and complete the settings In Local Management section as needed.

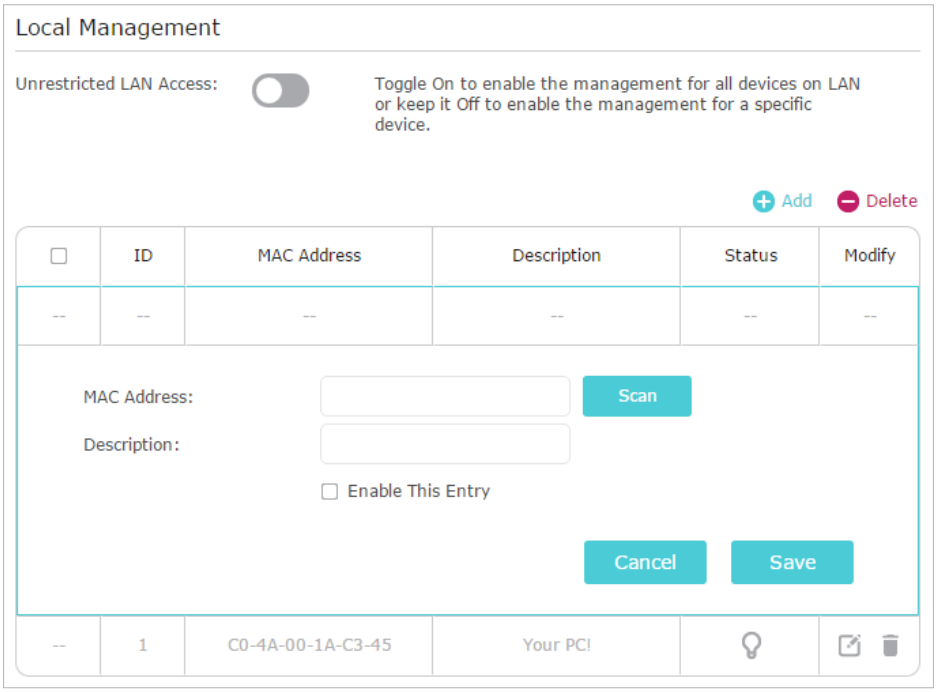
➢ **Allow all LAN connected devices to manage the router:**

Toggle on Access for All LAN Connected Devices.



➢ **Allow specific devices to manage the router:**

1. Toggle off Access for All LAN Connected Devices.
2. Click Add.

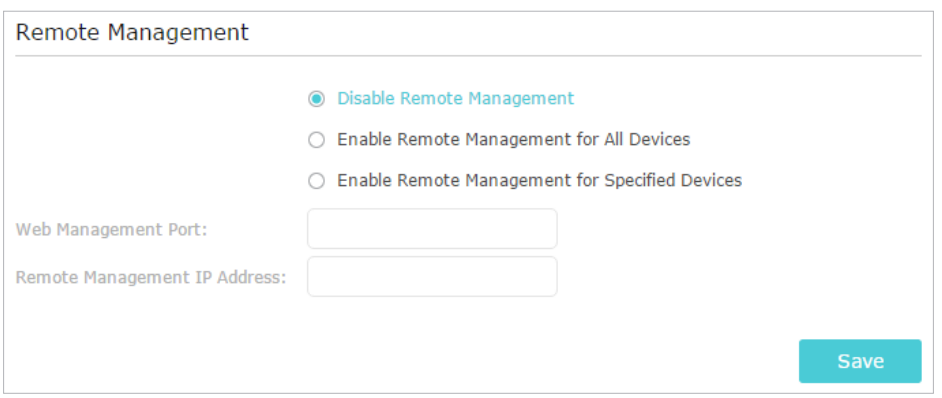


3. Click Scan and select the device to manage the router from the Existing Devices list, or enter the MAC address of the device manually.
4. Specify a Description for this entry.
5. Tick the Enable This Entry checkbox.
6. Click Save.

15. 11. Remote Management

This feature allows you to control remote devices' authority to manage the router.

1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > System Tools > Administration and complete the settings in Remote Management section as needed.



➢ **Forbid all devices to manage the router remotely:**

Select Disable Remote Management and click Save.

➢ **Allow all devices to manage the router remotely:**

1. Select Enable Remote Management for All Devices.
2. Enter Web Management Port (1024-65535 or 80).
3. Click Save.

Devices on the Internet can log in to http://Router's WAN IP address:port number (such as http://113.116.60.229:1024) to manage the router.

Tips:

- You can find the WAN IP address of the router on Basic > Network Maps > Internet.
- 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.

➢ **Allow specific devices to manage the router remotely:**

1. Select Enable Remote Management for Specified Devices.
2. Enter Web Management Port (1024-65535 or 80).
3. In Remote Management IP address, enter the IP address of the remote device to manage the router.
4. Click Save.

Devices using this WAN IP can manage the router by logging in to http://Router's WAN IP:port number (such as http://113.116.60.229:1024).

Tips:

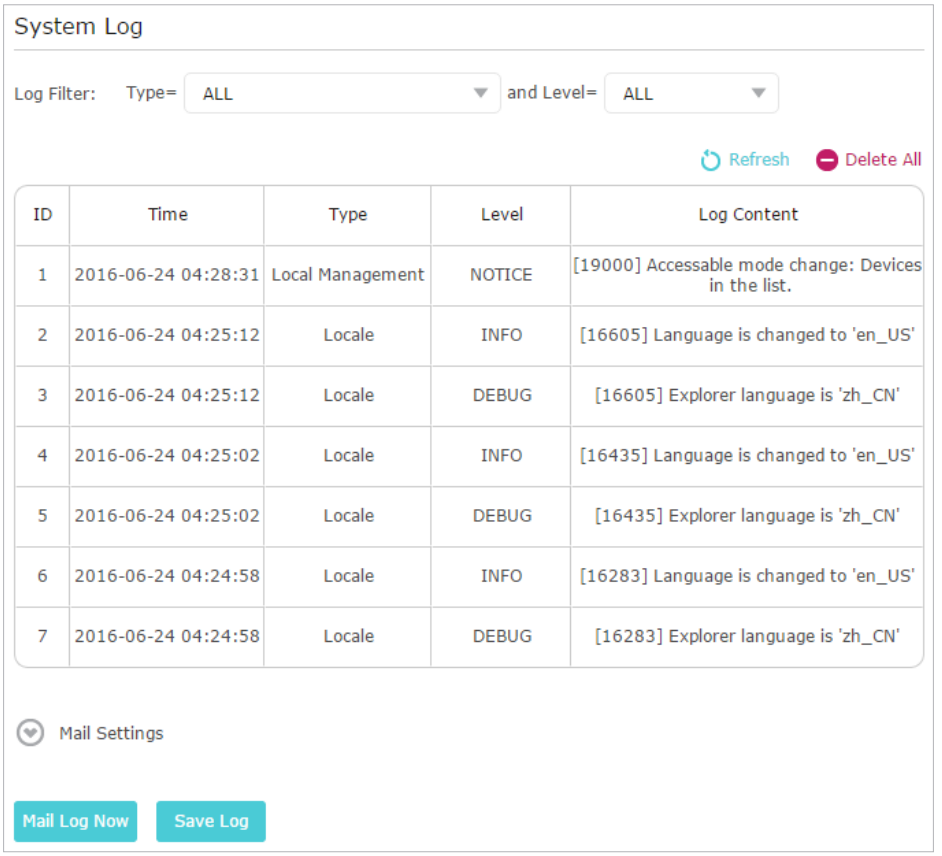
The router's WAN IP is usually a dynamic IP. Please refer to Set Up a Dynamic DNS Service Account if you want to log in to the router through a domain name.

15. 12. System Log

When the router does not work normally, you can save the system log and send it to the technical support for troubleshooting.

➢ **To save the system log in local:**

1. Visit http://tplinkwifi.net, and log in your TP-Link ID or the password you set for the router.
2. Go to Advanced > System Tools > System Log.
3. Choose the type and level of the system logs as needed.
4. Click Save Log to save the system logs to local.

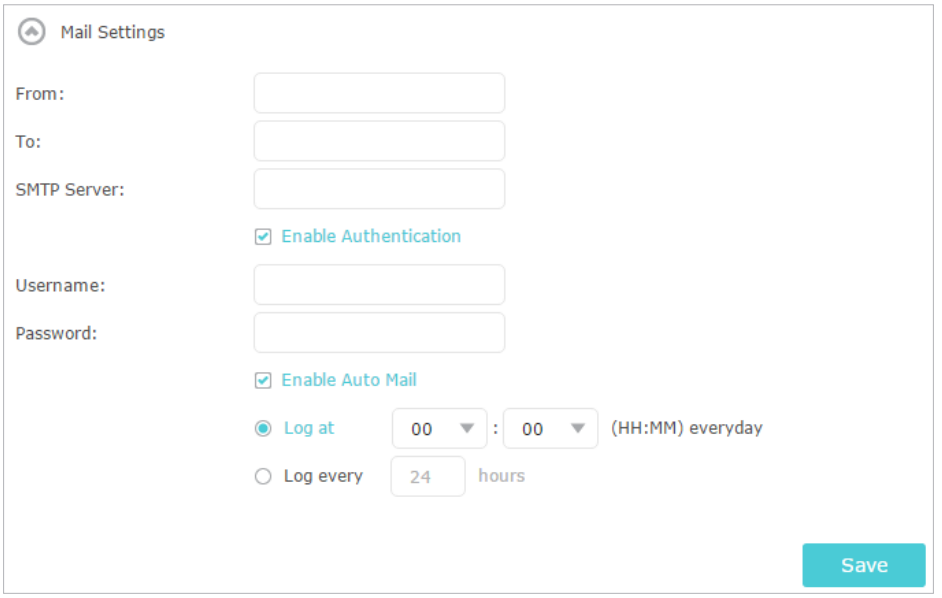


ID	Time	Type	Level	Log Content
1	2016-06-24 04:28:31	Local Management	NOTICE	[19000] Accessable mode change: Devices in the list.
2	2016-06-24 04:25:12	Locale	INFO	[16605] Language is changed to 'en_US'
3	2016-06-24 04:25:12	Locale	DEBUG	[16605] Explorer language is 'zh_CN'
4	2016-06-24 04:25:02	Locale	INFO	[16435] Language is changed to 'en_US'
5	2016-06-24 04:25:02	Locale	DEBUG	[16435] Explorer language is 'zh_CN'
6	2016-06-24 04:24:58	Locale	INFO	[16283] Language is changed to 'en_US'
7	2016-06-24 04:24:58	Locale	DEBUG	[16283] Explorer language is 'zh_CN'

➢ **To send the system log to a mailbox at a fixed time:**

For example, I want to check my router's working status at a fixed time every day, however, it's too troublesome to log in to the web management page every time I want to go checking. It would be great if the system logs could be sent to my mailbox at 8 a.m. every day.

1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > System Tools > System Log.
3. Click Mail Settings.
4. Enter the information required:



1) From: Enter the email address used for sending the system log.

2) To: Enter the recipient's email address, which can be the same as or different from the sender's email address.

3) SMTP Server: Enter the SMTP server address.

Tips: SMTP server is available for users in most webmail systems. For example, the SMTP server address of Hotmail is smtp-mail.outlook.com. You can refer to their Help page to learn the SMTP server address.

4) Select Enable Authentication.

Tips: Generally, Enable Authentication should be selected if the login of the mailbox requires username and password.

5) Username: Enter the email address used for sending the system log.

6) Password: Enter the password to login the sender's email address.

7) Select Enable Auto Mail.

Tips: The router will send the system log to the designated email address if this option is enabled.

8) Set a fixed time. The recipient will receive the system log sent at this time every day.

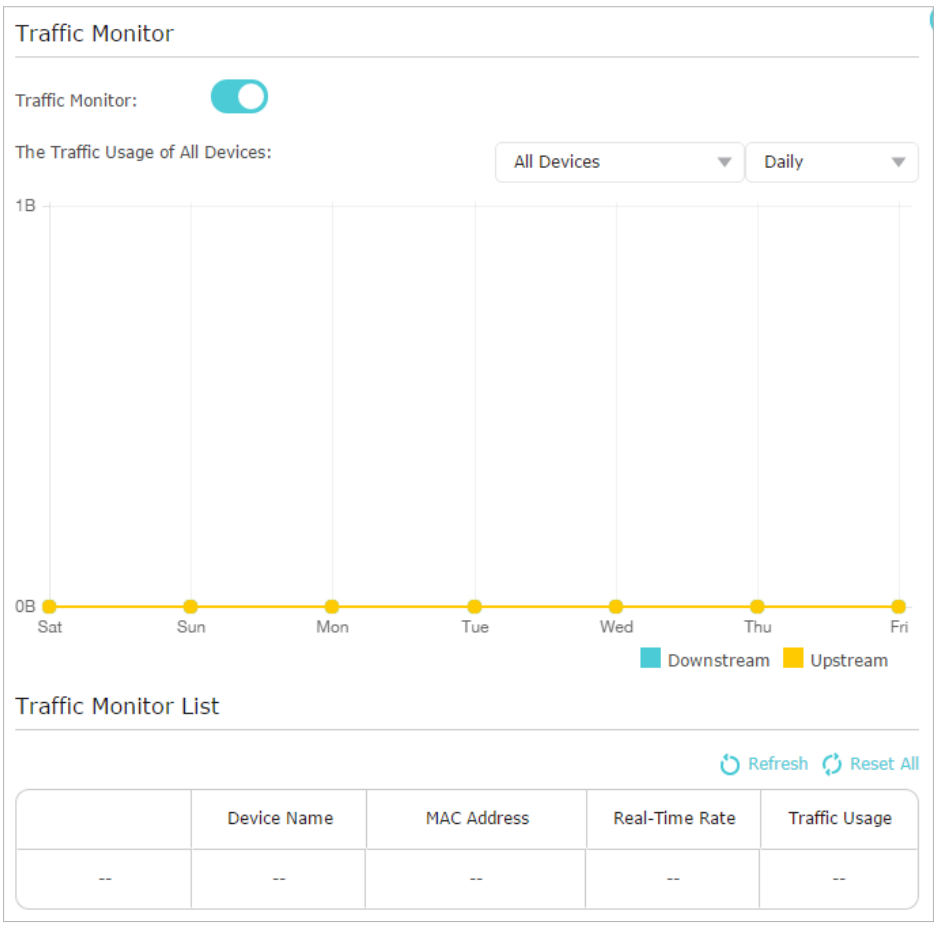
5. Click Save.

15. 13. Monitor the Internet Traffic Statistics

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

1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > System Tools > Traffic Monitor.

3. Toggle on Traffic Monitor, and then you can monitor the traffic statistics.



- Traffic Monitor: This section displays the traffic usage of a device in the past 10 minutes or that of all devices in the past 10 minutes/24 hours/7 days.
- Traffic Monitor List: The list is grouped by the connection type of devices: wired or wireless.

FAQ

Q1. What should I do if I forget my wireless password?

The default wireless password is printed on the label of the router. If the password has been altered:

1. Connect your computer to the router using an Ethernet cable.
2. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
3. Go to Basic > Wireless to retrieve or reset your wireless password.

Q2. What should I do if I forget my web management password?

- If you are using a TP-Link ID to log in, or you have enabled the Password Recovery feature of the router, click Forgot password on the login page and then follow the instructions to reset it.
- Alternatively, press and hold the Reset button of the router until the Power LED binks to reset it, and then visit http://tplinkwifi.net to create a new login password.

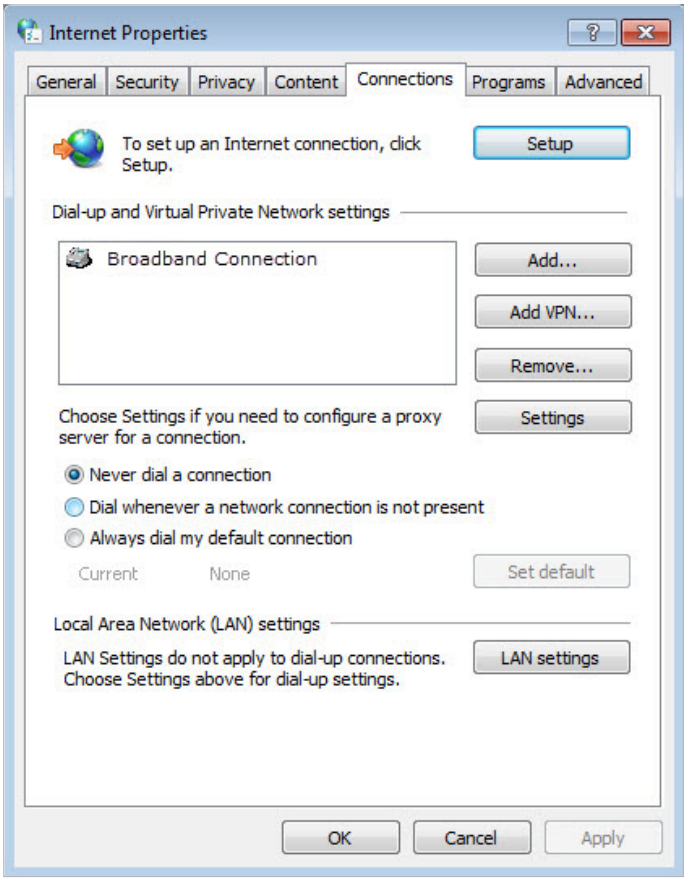
Note:

- Please refer to Password Recovery to learn how to configure Password Recovery.
- You'll need to reconfigure the router to surf the internet once the router is reset, and please mark down your new password for future use.

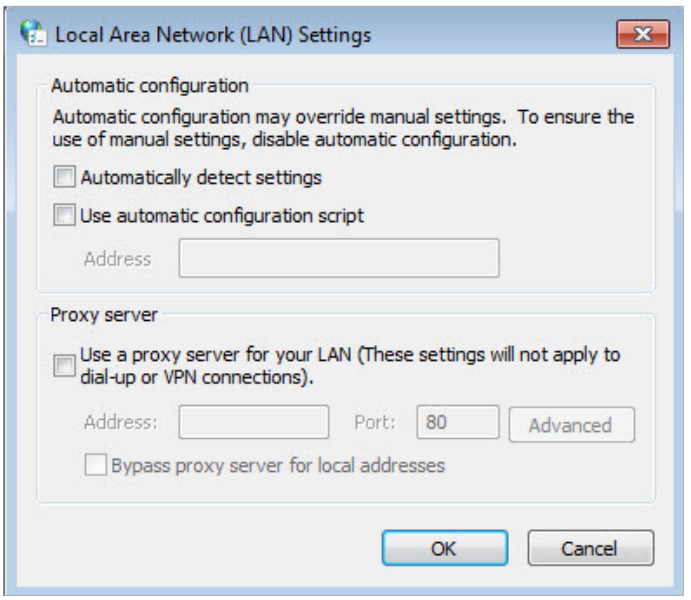
Q3. What should I do if I cannot log in to the router's web management page?

This can happen for a variety of reasons. Please try the methods below to log in again.

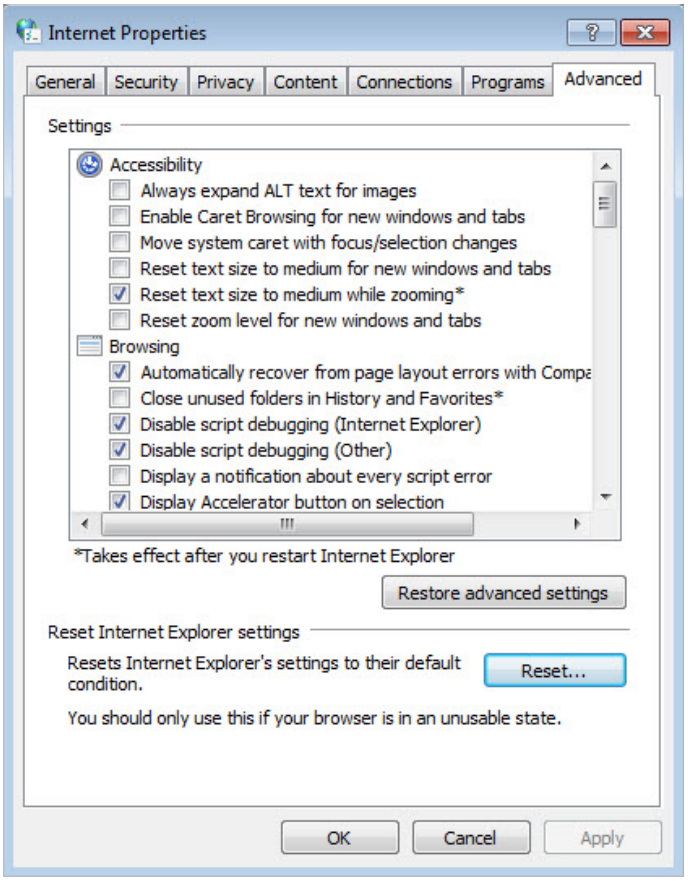
- Make sure your computer is connected to the router correctly and the corresponding LED indicator(s) light up.
- Make sure the IP address of your computer is configured as Obtain an IP address automatically and Obtain DNS server address automatically.
- Make sure http://tplinkwifi.net or http://192.168.0.1 is correctly entered.
- Check your computer's settings:
  1) Go to Start > Control Panel > Network and Internet, and click View network status and tasks.
  2) Click Internet Options on the bottom left.
  3) Click Connections and select Never dial a connection.



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



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



- Use another web browser or computer to log in again.
- Reset the router to factory default settings and try again. If login still fails, please contact the technical support.

Note: You'll need to reconfigure the router to surf the internet once the router is reset.

Q4. How do I use the WDS Bridging function to extend my wireless network?

For example, my house covers a large area. The wireless 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 root router.

Note:

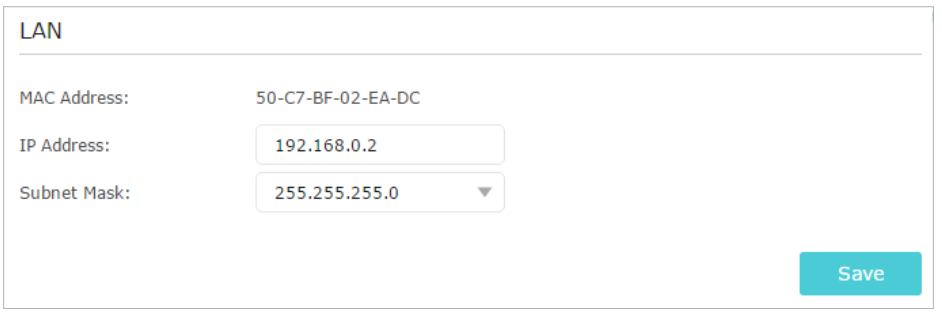
- WDS bridging only requires configuration on the extended router.
- WDS bridging function can be enabled either in 2.4GHz frequency or 5GHz frequency for a dual-band router. We use the WDS bridging function in 2.4GHz frequency as example.

1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. Configure the IP address of the router:
   1) Go to Advanced > Network > LAN, configure the IP address of the extended router to be in the same subnet with the root router; (For example, the IP address

of the root router is 192.168.0.1, the IP address of the extended router can be 192.168.0.2~192.168.0.254. We take 192.168.0.2 as example.)

2) Click Save.

Note: Log in to the web management page again if the IP address of the router is altered.



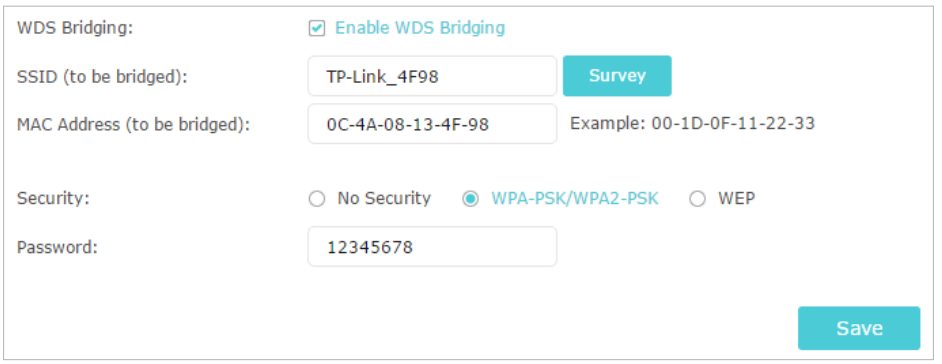
3. Survey the SSID to be bridged:

1) Go to Advanced > System Tools > System Parameters and focus on the 2.4GHz Wireless section, click Enable WDS Bridging.

2) Click Survey, locate the root router's SSID and click Choose (Here we take TP-Link_4F98 as example).

3) If the root router has wireless password, you should enter the wireless password of the root router.

4) Click Save.



4. Disable DHCP:

1) Go to Network > DHCP Server.

2) Deselect Enable DHCP Server and click Save.

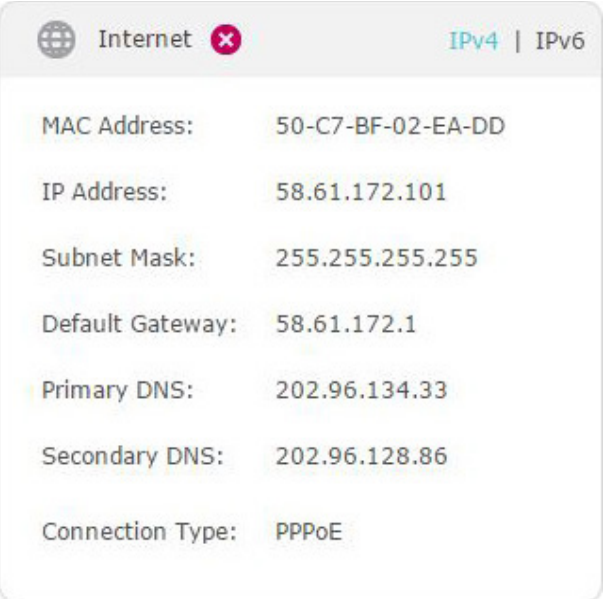
Now you can go to Advanced > Status > Wireless to check the WDS status. When the WDS status is Run, it means WDS bridging is successfully built.

Q5. What should I do if I cannot access the internet even though the

configuration is finished?

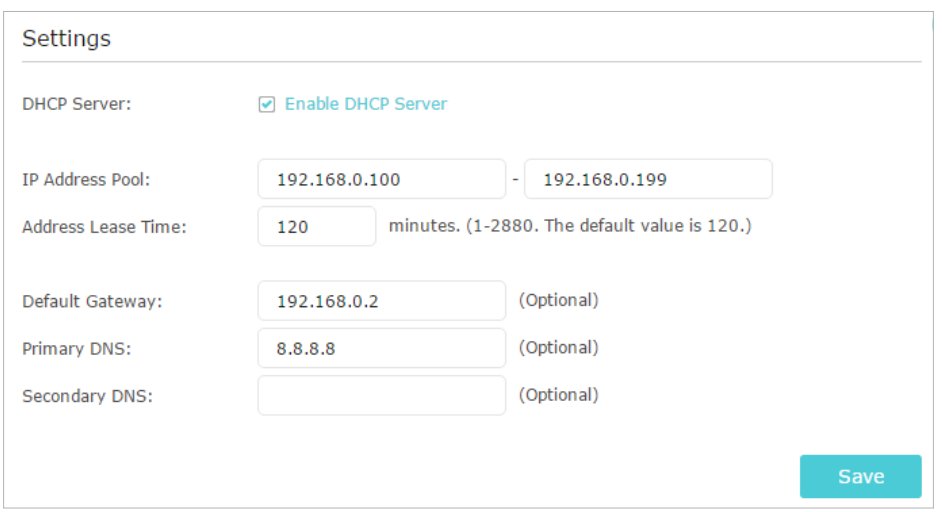
1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > Status to check internet status:

As the follow picture shows, if IP Address is a valid one, please try the methods below and try again:



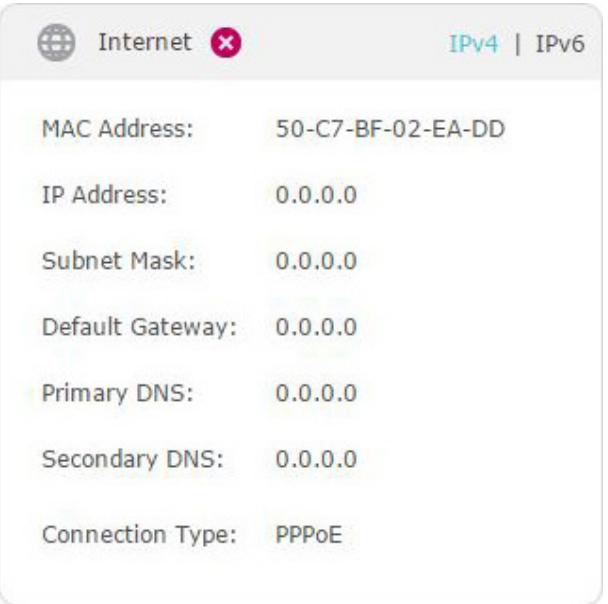
- Your computer might not recognize any DNS server addresses. Please manually configure the DNS server.
  1) Go to Advanced > Network > DHCP Server.
  2) Enter 8.8.8.8 as Primary DNS, click Save.

  Tips: 8.8.8.8 is a safe and public DNS server operated by Google.

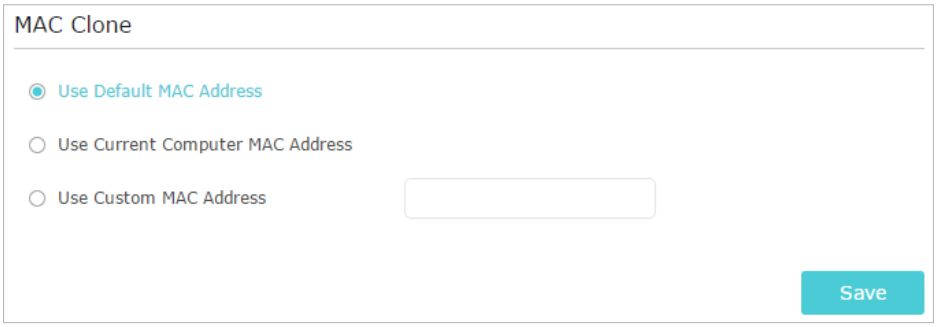


- Restart the modem and the router.
  1) Power off your modem and router, and leave them off for 1 minute.
  2) Power on your modem first, and wait about 2 minutes until it gets a solid cable or Internet light.
  3) Power on the router.
  4) Wait another 1 or 2 minutes and check the internet access.
- Reset the router to factory default settings and reconfigure the router.
- Upgrade the firmware of the router.
- Check the TCP/IP settings on the particular device if all other devices can get internet from the router.

As the picture below shows, if the IP Address is 0.0.0.0, please try the methods below and try again:



- Make sure the physical connection between the router and the modem is proper.
- Clone the MAC address of your computer.
  1) Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
  2) Go to Advanced > Network > Internet and focus on the MAC Clone section.
  3) Choose an option as needed (enter the MAC address if Use Custom MAC Address is selected), and click Save.



Tips:

- Some ISP will register the MAC address of your computer when you access the internet for the first time through their Cable modem, if you add a router into your network to share your internet connection, the ISP will not accept it as the MAC address is changed, so we need to clone your computer's MAC address to the router.
- The MAC addresses of a computer in wired connection and wireless connection are different.

- Modify the LAN IP address of the router.

Note:

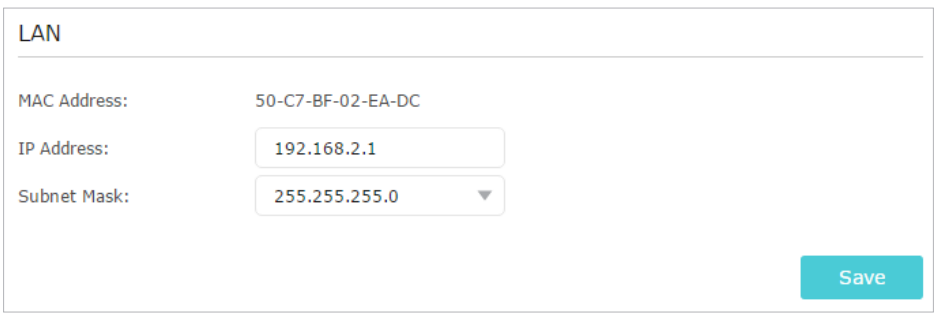
Most TP-Link routers use 192.168.0.1/192.168.1.1 as their default LAN IP address, which may conflict with the IP range of your existing ADSL modem/router. If so, the router is not able to communicate with your modem and you can't access the internet. To resolve this problem, we need to change the LAN IP address of the router to avoid such conflict, for example, 192.168.2.1.

1) Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.

2) Go to Advanced > Network > LAN.

3) Modify the LAN IP address as the follow picture shows. Here we take 192.168.2.1 as an example.

4) Click Save.



- Restart the modem and the router.

1) Power off your modem and router, and leave them off for 1 minute.

2) Power on your modem first, and wait about 2 minutes until it get a solid cable or Internet light.

3) Power on the router.

4) Wait another 1 or 2 minutes and check the internet access.

- Double check the internet connection type.

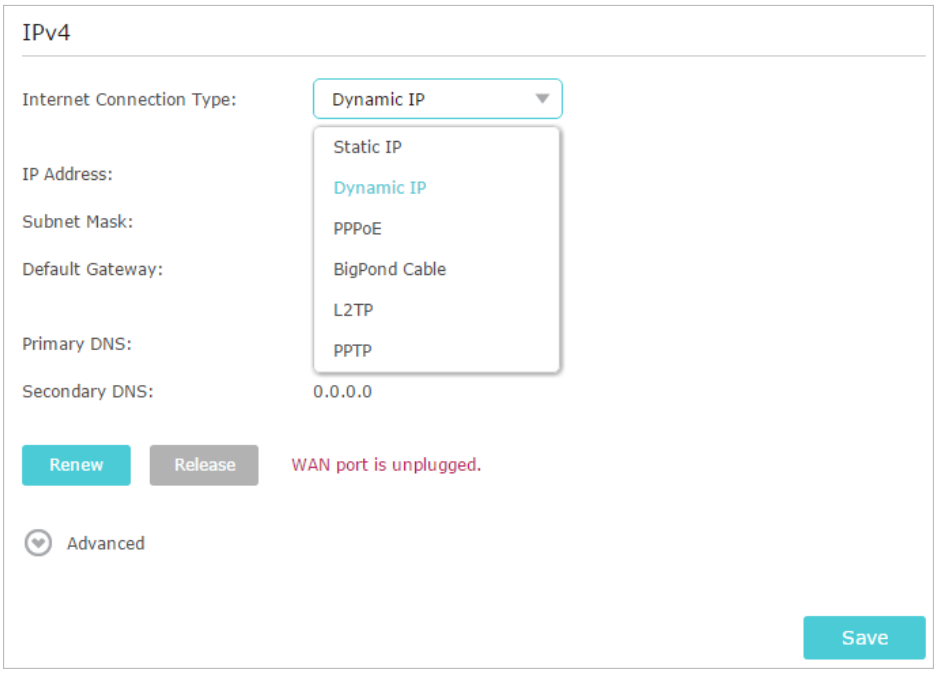
1) Confirm your internet connection type, which can be learned from the ISP.

2) Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.

3) Go to Advanced > Network > Internet.

4) Select your Internet Connection Type and fill in other parameters.

5) Click Save.



6) Restart the modem and the router again.

- Please upgrade the firmware of the router.

If you've tried every method above but still cannot access the internet, please contact the technical support.

Q6. What should I do if I cannot find my wireless network or I cannot connect the wireless network?

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

- Make sure the wireless function of your device 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.
- Make sure the wireless adapter driver is installed successfully and the wireless adapter is enabled.
  - **On Windows 7**

1) If you see the message No connections are available, it is usually because the wireless function is disabled or blocked somehow.

2) Click Troubleshoot and windows might be able to fix the problem by itself.

- **On Windows XP**

1) If you see the message Windows cannot configure this wireless connection, this is usually because windows configuration utility is disabled or you are running another wireless configuration tool to connect the wireless.

2) Exit the wireless configuration tool (the TP-Link Utility, for example).

3) Select and right click on My Computer on desktop, select Manage to open Computer Management window.

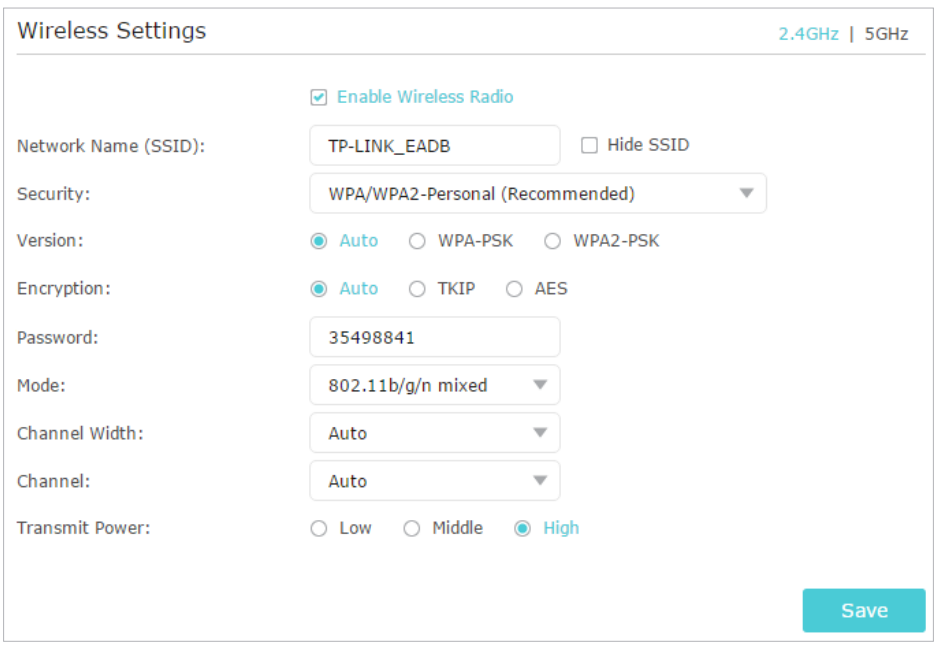
4) Expand Services and Applications > Services, find and locate Wireless Zero Configuration in the Services list on the right side.

5) Right click Wireless Zero Configuration, and then select Properties.

6) Change Startup type to Automatic, click on Start button and make sure the Service status is Started. And then click OK.

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

- Check the WLAN LED indicator on your wireless router/modem.
- Make sure your computer/device is still in the range of your router/modem. Move it closer if it is currently too far away.
- Go to Advanced > Wireless > Wireless Settings, and check the wireless settings. Double check your Wireless Network Name and SSID is not hided.



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

- **Authenticating problem/password mismatch:**

1) Sometimes you will be asked 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 label of your router.

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

3) If it continues to show note of Network Security Key Mismatch, it is suggested to confirm the wireless password of your wireless router.

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

- **Windows unable to connect to XXXX / Can not join this network / Taking longer than usual to connect to this network:**
  - Check the wireless signal strength of your network. If it is weak (1~3 bars), please move the router closer and try again.
  - Change the wireless Channel of the router to 1, 6 or 11 to reduce interference from other networks.
  - Re-install or update the driver for your wireless adapter of the computer.

COPYRIGHT & TRADEMARKS

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

No part of the specifications may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from TP-Link Technologies Co., Ltd. Copyright © 2017 TP-Link Technologies Co., Ltd. All rights reserved.

FCC STATEMENT

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

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

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

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

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

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

FCC RF Radiation Exposure Statement

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

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

The device is restricted in indoor environment only.

CE Mark Warning

CE 1588 ⓘ

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

RF Exposure Information

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

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

Restricted to indoor use.

Canadian Compliance Statement

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

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

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

This radio transmitter (IC: 8853A-C2300V1) has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain indicated. Antenna types not included in this list below, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Le présent émetteur radio (IC: 8853A-C2300V1) a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal. Les types d'antenne non inclus dans cette liste ci-dessous et dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

Antenna	Three dual band detachable antennas, 3dBi for 5GHz and 2dBi for 2.4GHz.

Caution:

1. The device for operation in the band 5150–5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;
2. For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the band 5745-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits specified for point-to-point and non-point-topoint operation as appropriate; and

The high-power radars are allocated as primary users (i.e. priority users) of the bands 5745-5850 MHz and that these radars could cause interference and/or damage to LELAN devices.

Avertissement:

1. Le dispositif fonctionnant dans la bande 5150-5250 MHz est réservé uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;
2. Le gain maximal d'antenne permis pour les dispositifs avec antenne(s) amovible(s) utilisant la bande 5745-5850 MHz doit se conformer à la limitation P.I.R.E spécifiée pour l'exploitation point à point et non point à point, selon le cas.

En outre, les utilisateurs devraient aussi être avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5745-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

Radiation Exposure Statement:

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

Déclaration d'exposition aux radiations:

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

Industry Canada Statement

CAN ICES-3 (B)/NMB-3(B)

Korea Warning Statements:

당해 무선설비는 운용중 전파혼신 가능성이 있음.

NCC Notice & BSMI Notice:

注意！

依據 低功率電波輻射性電機管理辦法

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

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

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.

For EU/EFTA, this product can be used in the following countries:

AT	BE	BG	CH	CY	CZ	DE	DK
EE	ES	FI	FR	GB	GR	HR	HU

IE	IS	IT	LI	LT	LU	LV	MT
NL	NO	PL	PT	RO	SE	SI	SK

Explanations of the symbols on the product label

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