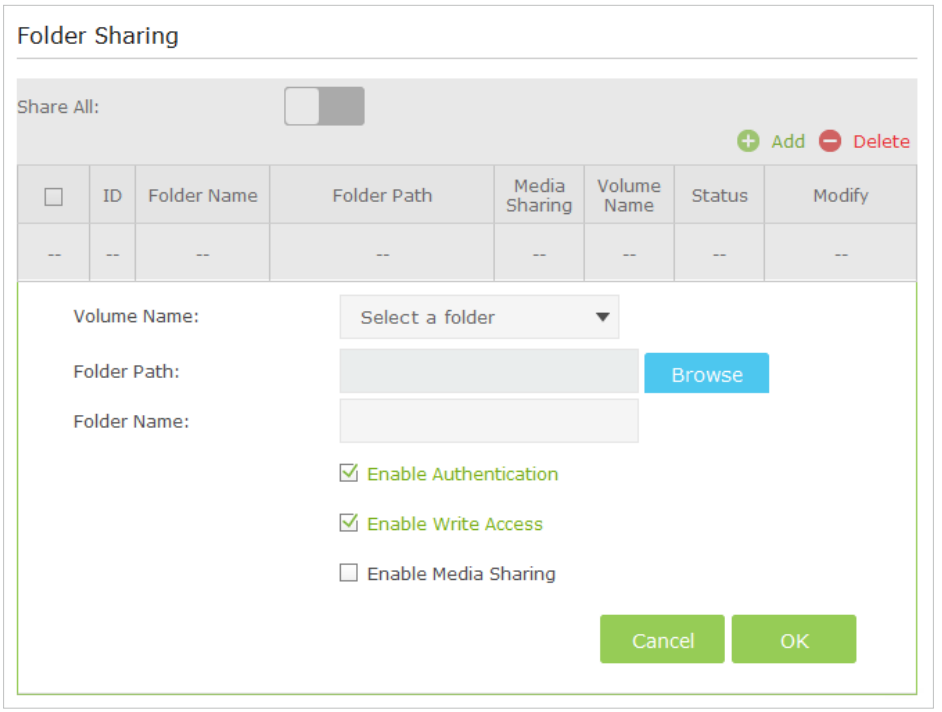


5. Click OK.

Tips:

The router can share 32 volumes at most. You can click on the page to detach the corresponding volume you do not need to share.

6. 3. Media Sharing

The feature of Media Sharing allows you to view photos, play music and watch movies stored on the USB disk directly from DLNA-supported devices, such as your computer, pad and PS2/3.

6. 3. 1. Access the USB disk

1. Connect Your USB Disk

Insert your USB storage device into the router's USB port directly or using a USB cable. Wait several seconds until the USB LED becomes solid on.

Tips:

- If you use USB hubs, make sure no more than four devices are connected to the router.
- If the USB storage device requires using bundled external power, make sure the external power has been connected.
- If you use a USB hard drive, make sure its file system is FAT32,NTFS.
- Before you physically disconnect a USB device from the router, safely remove it to avoid data damage: Go to *Advanced* > *USB Settings* > *Device Settings* and click Safety Remove.

2. Play the Media on Your USB Disk

Now the DLNA-supported devices (such as your computer and pad) connected to the router can detect and play the media files on the USB disks.

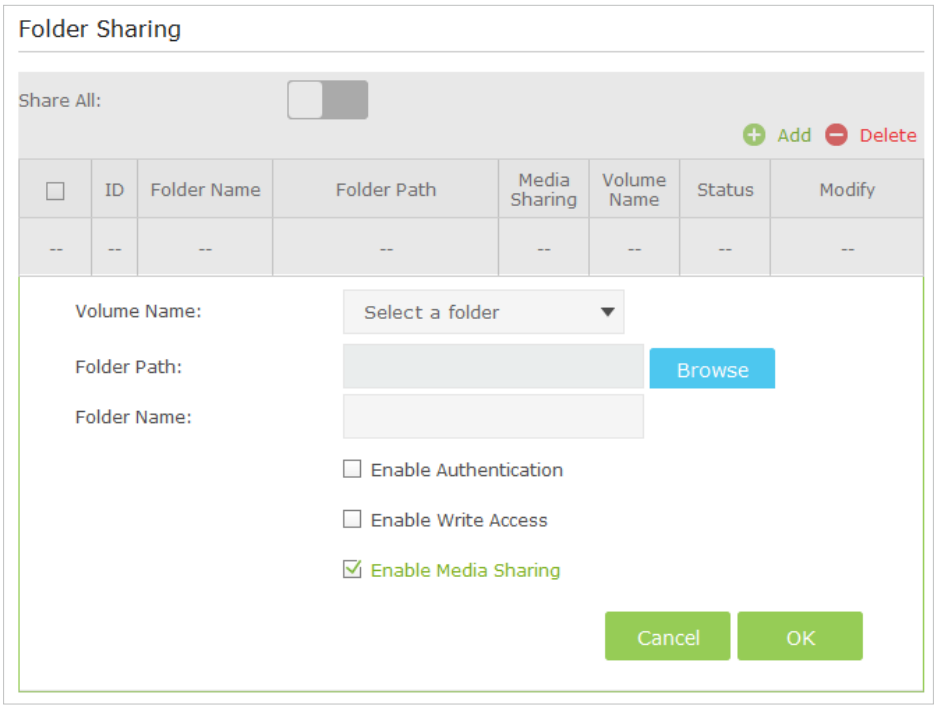
Windows computer	1. Open the Windows Media Player. 2. Click the media server name (such as Genie Media Severs) under the list of Other Libraries, then you can directly view photos, play music and watch movies that you share on the USB disks.
Pad	• Use a third-party DLNA-supported player.

6. 3. 2. Customize Your Settings

➢ To Only Share Specific Content

By default, Share All is enabled so all content on the USB disk is shared. If you want to only share specific folders, follow the steps below:

1. Visit *http://tplinkwifi.net*, then log in with the username and password you set for the router.
2. Go to *Advanced* > *USB Settings* > *Sharing Access*.
3. Focus on the section of Folder Sharing. Click the button to disable Share All, then click Add to add a new sharing folder.
4. Select the Volume Name and Folder Path, then enter a Folder Name as you like.
5. Select Enable Media Sharing and click OK.



Tips:

The router can share 32 volumes at most. You can click on the page to detach the corresponding volume you do not need to share.

6. 4. Printer Sharing

The feature of Printer Sharing helps you share a printer with different computers connected to the router.

Note:

Printers unlisted may be incompatible with the router. You can check Printer Compatibility List to verify whether your printer is supported by the router: *http://www.tp-link.com/common/compatible/print-server/*.

1. **Install the Driver of the Printer**

   Make sure you have installed the driver of the printer on each computer that needs printer service.

   If you do not have the driver, contact the printer manufacturer.

2. **Connect the Printer**

   Cable a printer to the USB port with the USB cable. Wait several seconds until the USB LED becomes solid on.

3. **Install the TP-LINK USB Printer Controller Utility**

   TP-LINK USB Printer Controller Utility helps you access the shared printer. Download and install the utility on each computer that needs printer service.

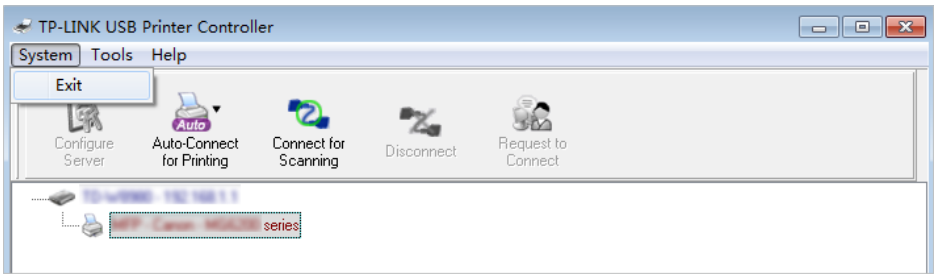
   You can get the utility from *http://www.tp-link.com/app/usb/*. PC Utility is for Windows computer and Mac Utility is for Mac computer.

4. Access the Printer

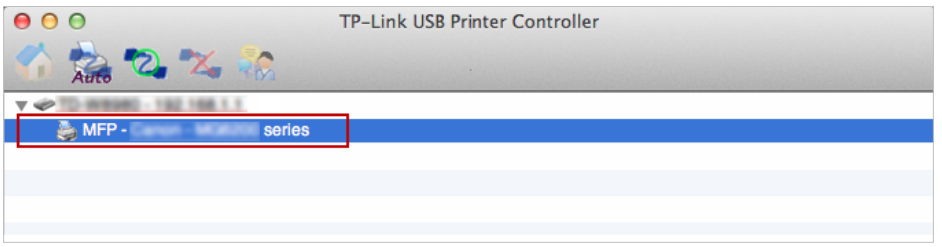
You should set the shared printer as Auto-Connect Printer on every computer that needs printer service.

1) Double-click the icon on your desktop to launch the USB Printer Controller.

2) Highlight the printer you share.

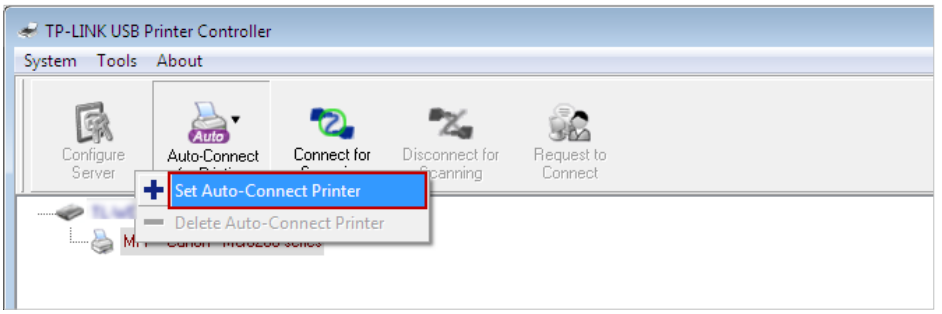


Windows

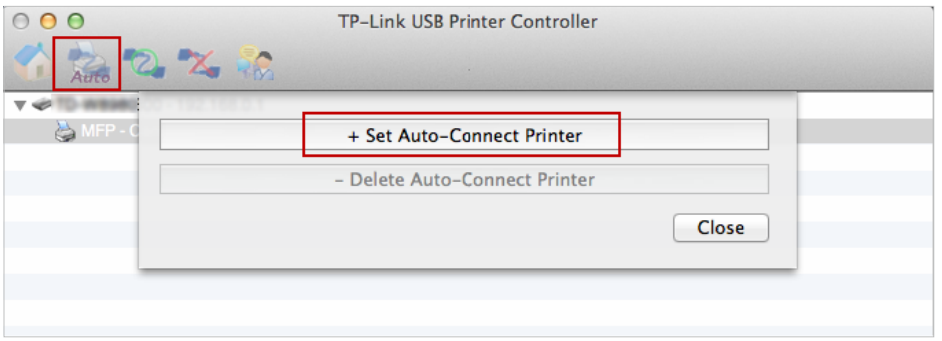


Mac

3) Click the Auto-Connect for printing tab to pull down a list, then select Set Auto-Connect Printer.

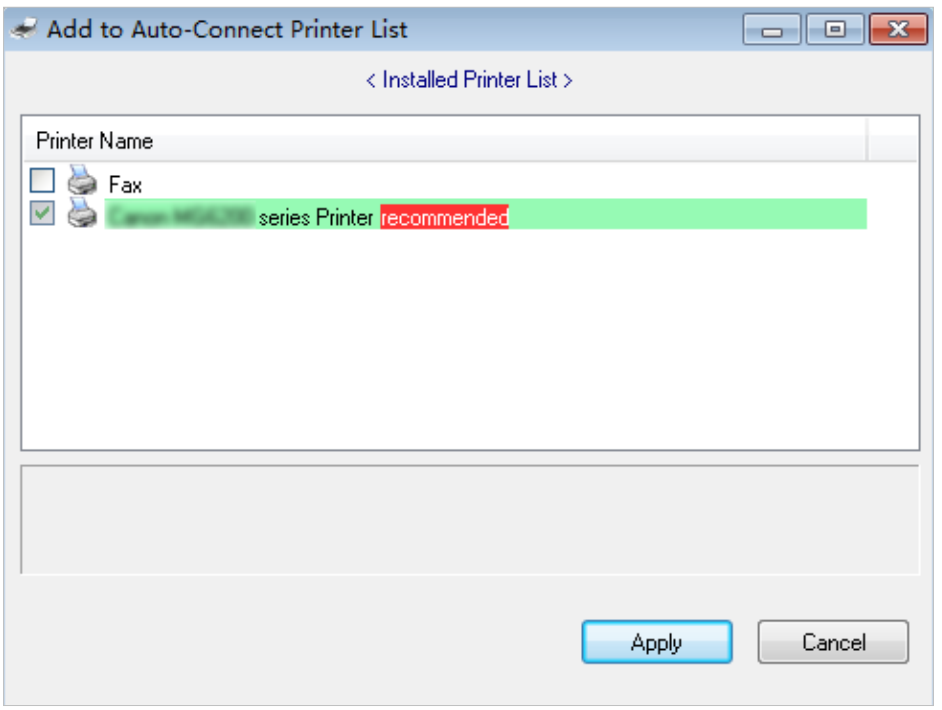


Windows

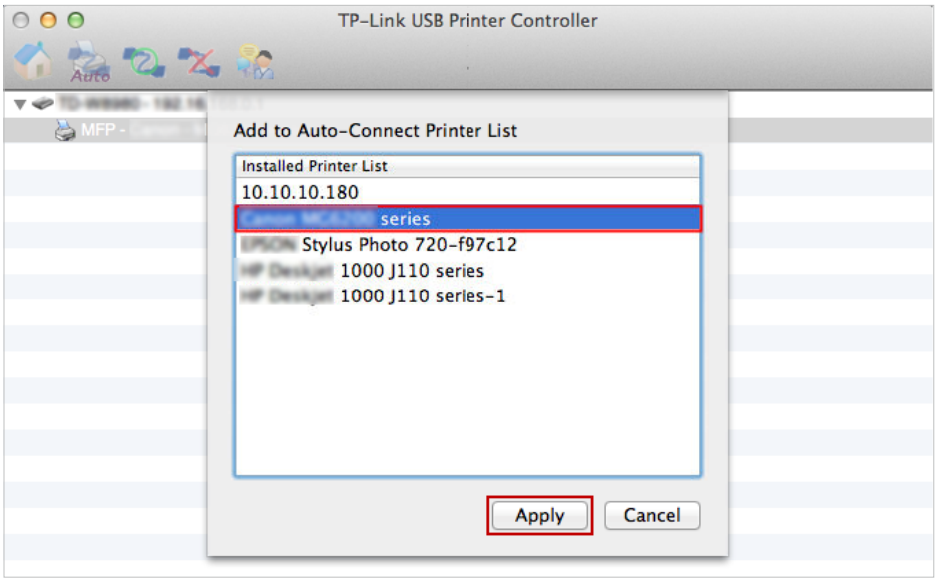


Mac

4) Select the printer you share, then click Apply.

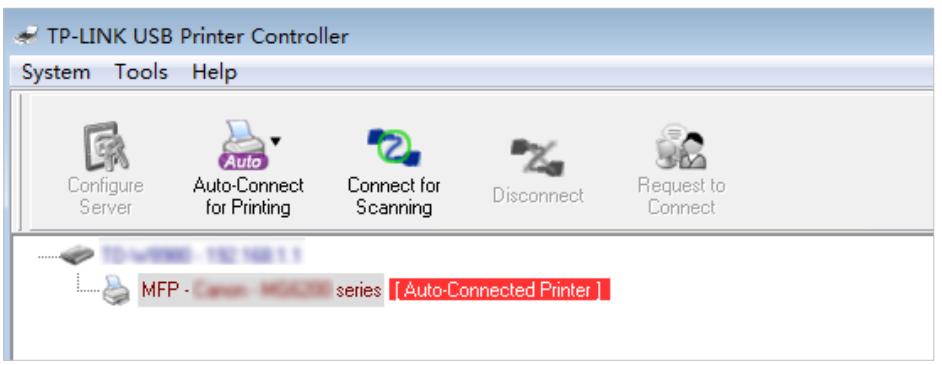


Windows

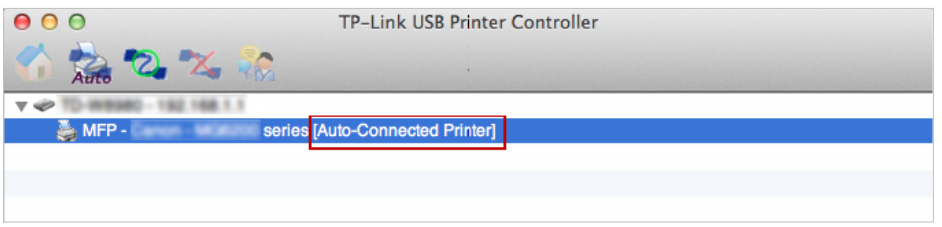


Mac

5) You will see the printer marked as Auto-Connect Printer. Now you can print with this printer.



Windows



Mac

Tips:

The Print Server also allows different clients to share the scan feature of MFPs (Multi-Function Printers). To scan with TP-LINK USB Printer Controller, right-click the printer and select Network Scanner. Then, a scanning window will pop up. Finish the scanning process by following the on-screen instructions.

Chapter 7

Parental Controls

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

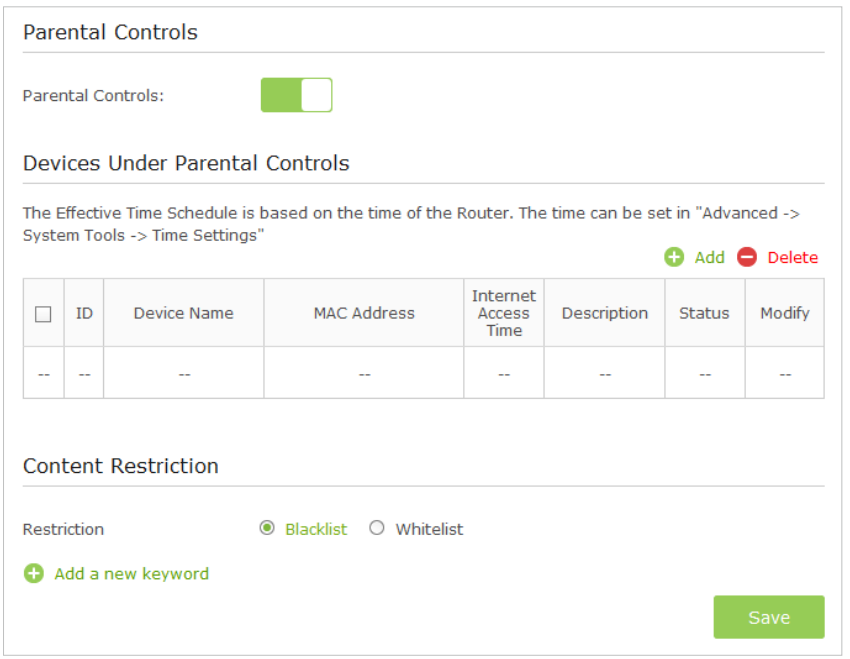
I want to:

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

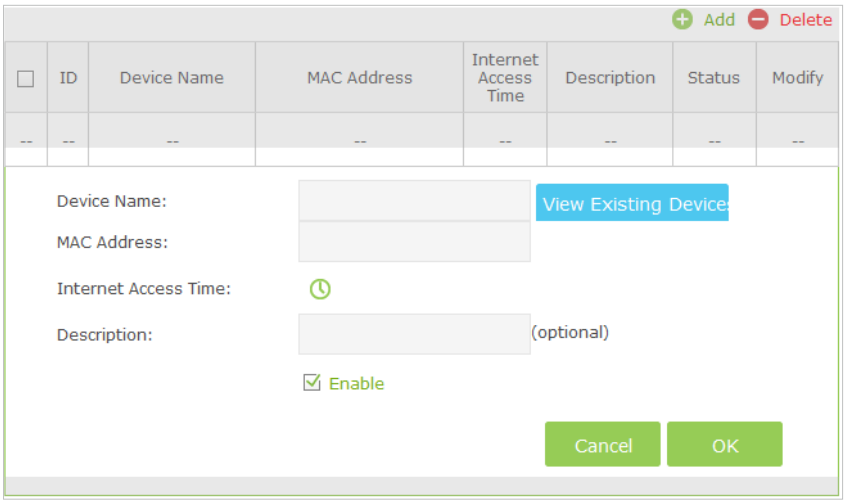
For example, I want to allow my children's devices (e.g. a computer or a tablet) to access only *www.tp-link.com* and *Wikipedia.org* from 18:00 (6PM) to 22:00 (10PM) at the weekend and not other times.

How can I do that?

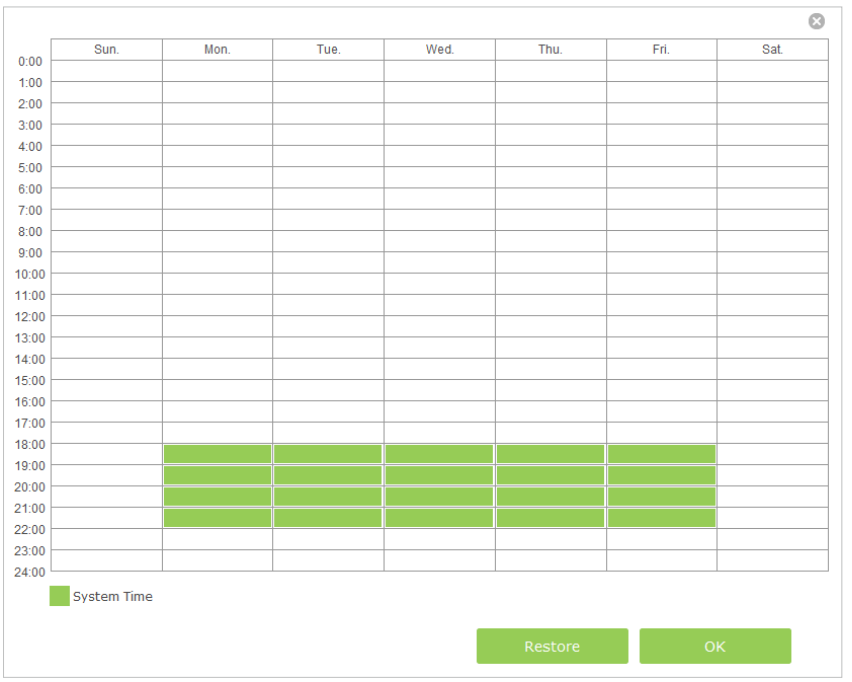
1. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
2. Go to *Basic* or *Advanced* > *Parental Controls* and enable Parental Controls.



3. Click Add.
4. Click View Existing Devices, and select the access device. Or, enter the Device Name and MAC Address manually.



5. Click the icon to set the Internet Access Time. Drag the cursor over the appropriate cell(s) and click OK.

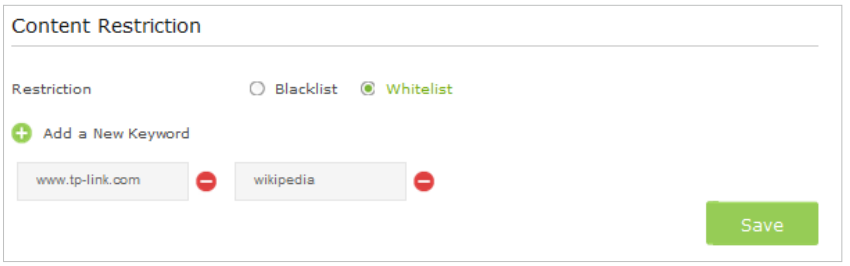


6. Enter a Description for the entry. Keep the Enable This Entry checkbox available. Click OK.

7. Select the restriction policy.

   1) In Blacklist mode, the controlled devices cannot access any websites containing the specified keywords during the Internet Access Time period.

   2) In Whitelist mode, the controlled devices can only access websites containing the specified keywords during the Internet Access Time period.



8. Click Add a new keyword to Block. You can add up to 32 keywords for either Blacklist or Whitelist. Below are some sample entries to allow access.
   1) Enter a web address (e.g. wikipedia.org) or a web address keyword (e.g. wikipedia) to only allow or block access to the websites containing that keyword.
   2) Specify the domain suffix (eg. .edu or .org) to allow access only to the websites with that suffix.
   3) If you wish to block all Internet browsing access, do not add any keyword to the Whitelist.
9. Enter a keyword or a website and click Save.

Done!

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

Chapter *8*

Bandwidth Control

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

I want to:

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

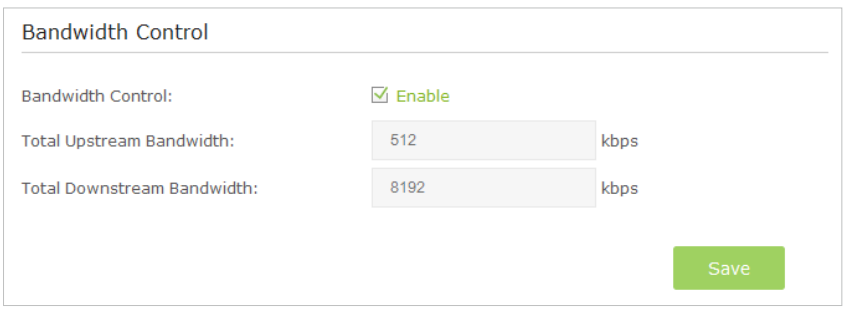
For example, my roommate and I share 512Kbps Upstream Bandwidth and 8Mbps Downstream Bandwidth via this router, she likes to watch live show and play online games, which may take up much bandwidth. I don't want to be affected, so we agree to equally distribute the bandwidth. Our IP addresses are 192.168.0.101 and 192.168.0.110.

Tips:

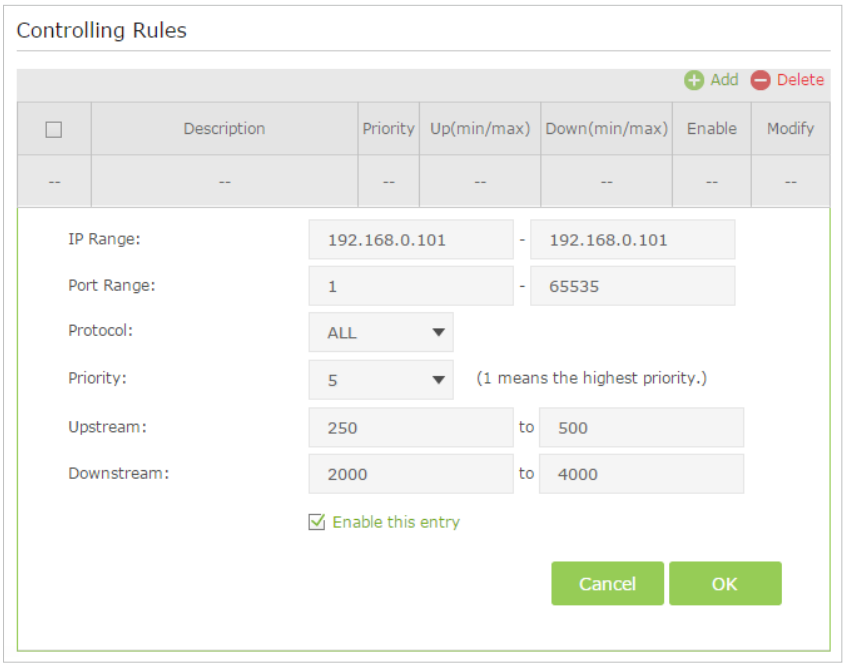
To use the bandwidth control feature, you'd better set static IP Address on each computer to be controlled or configure Address reservation on the router in order to manage easily. About how to configure address reservation, please refer to *To reserve an IP address for a specified client device*.

How can I do that?

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



3. Enable Bandwidth Control.
4. Enter the Total Upstream Bandwidth and the Total Downstream Bandwidth given by your ISP. (1Mbps=1024Kbps). Click Save to save the settings.
5. Click Add to add controlling rules for each computer respectively.



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

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

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

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

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

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

6. Follow the steps above to add a rule for the other computer. And then you will get the following table.

Controlling Rules

Add Delete

	Description	Priority	Up(min/max)	Down(min/max)	Enable	Modify
	192.168.0.110	5	250/500 kbps	2000/4000 kbps		
	192.168.0.101	5	250/500 kbps	2000/4000 kbps		

Done! Now you and your roommate have an independent bandwidth.

Chapter *9*

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 function.

This chapter contains the following sections:

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

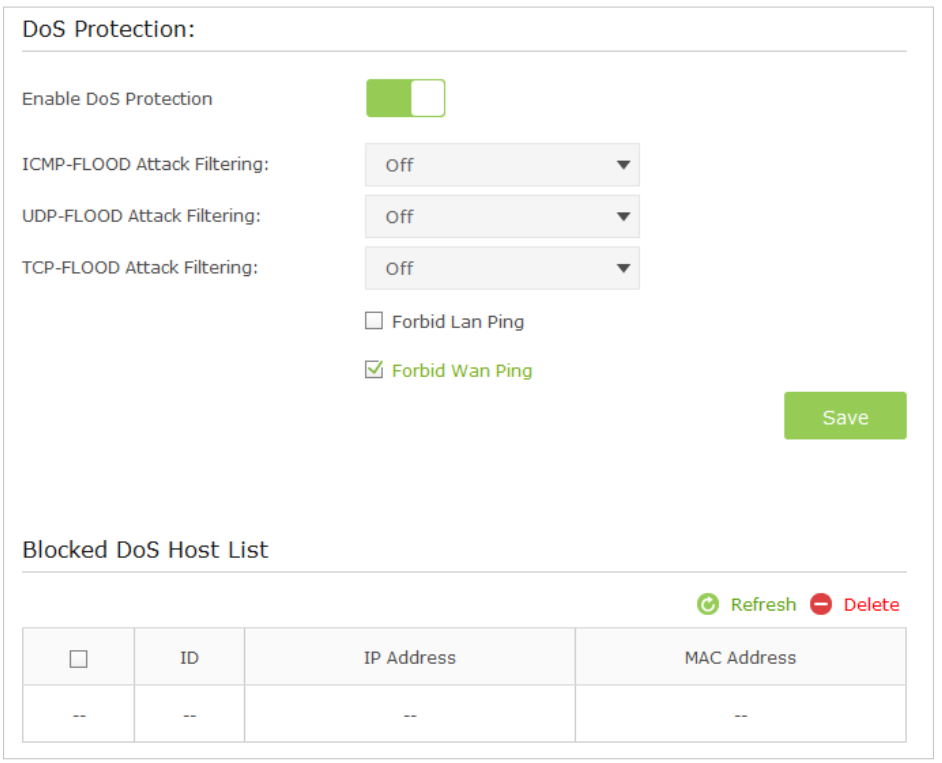
9. 1. Protect the Network from Cyber Attacks

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 setting.

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 the username and password you set for the router.
2. Go to *Advanced > Security > Settings.*



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 Internet Control Message Protocol (ICMP) flood attack.
   - UDP-FlOOD Attack Filtering - Enable to prevent the User Datagram Protocol (UDP) flood attack.

- TCP-SYN-FLOOD Attack Filtering - Enable to prevent the Transmission Control Protocol-Synchronize (TCP-SYN) flood attack.

Tips:

The level of protection is based on the traffic packets number. 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. Select Ignore Ping Packet From WAN Port if you want to ignore the ping packets from WAN port.
6. Select Forbid Ping Packet From LAN Port if you want to ignore the ping packets from LAN port.
7. Click Save to make the settings effective.

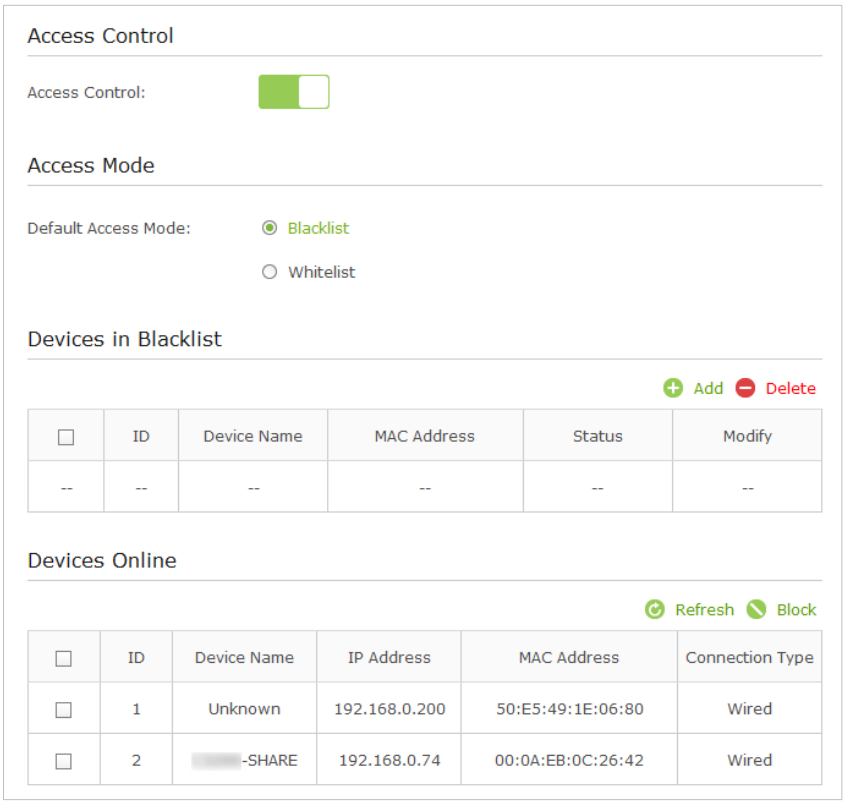
9. 2. Access Control

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

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

How can I do that?

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



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

   To block specific device(s)

   1) Select Blacklist.

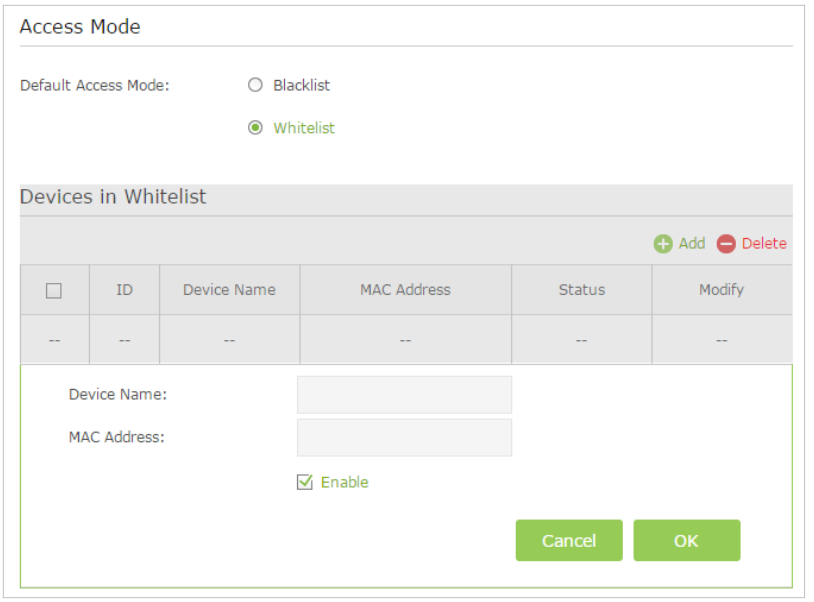
   2) Select the device(s) to be blocked in the Devices Online table.

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

   To allow specific device(s)

   1) Select Whitelist and click Save.

   2) Click Add.



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

4) Click OK.

Done!

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

9. 3. IP & MAC Binding

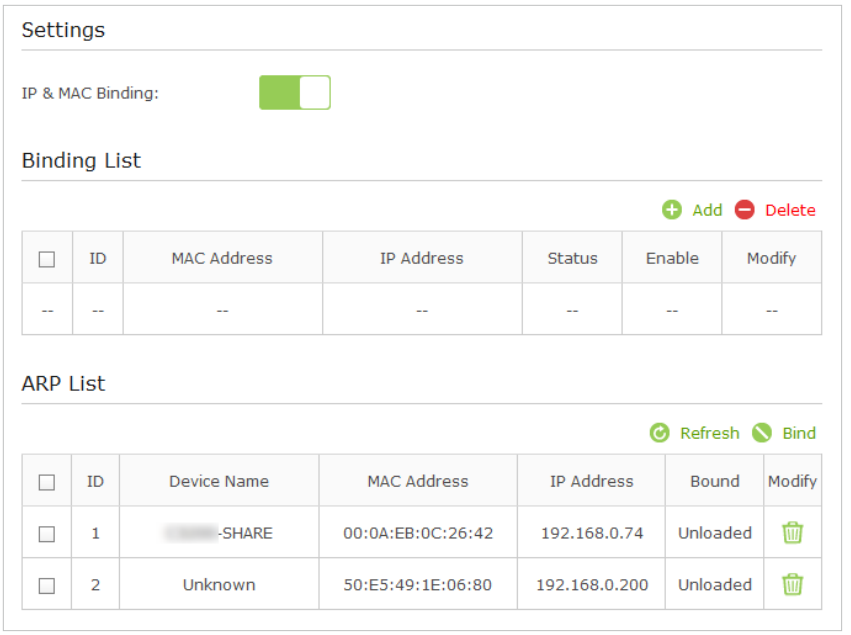
IP & MAC Binding, namely, ARP (Address Resolution Protocol) Binding, is used to bind network device's IP address to its MAC address. This will prevent ARP Spoofing and other ARP attacks by denying network access to an device with matching IP address in the Binding list, but unrecognized MAC address.

I want to:

Prevent ARP spoofing and ARP attacks.

How can I do that?

1. Visit *http://tplinkwifi.net*, and log in with the username and 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.

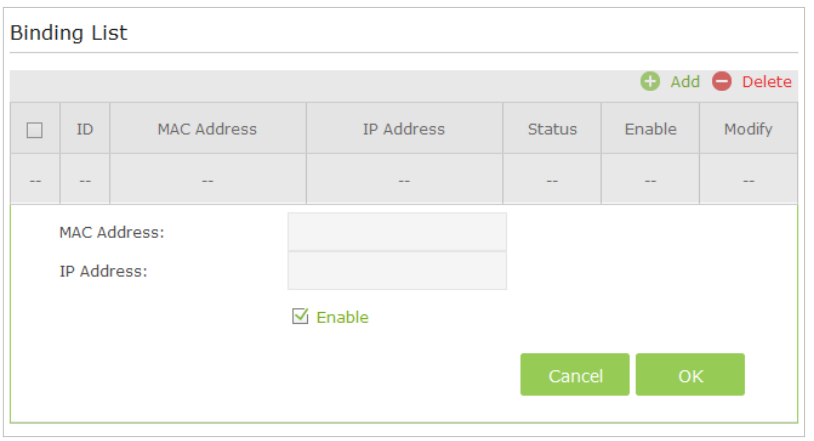
To bind the connected device(s)

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

2) Click Bind to add to the Binding List.

To bind the unconnected device

1) Click Add.



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

3) Select the checkbox to enable the entry and click OK.

Done!

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

Chapter *10*

NAT Forwarding

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

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

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

This chapter contains the following sections:

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

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

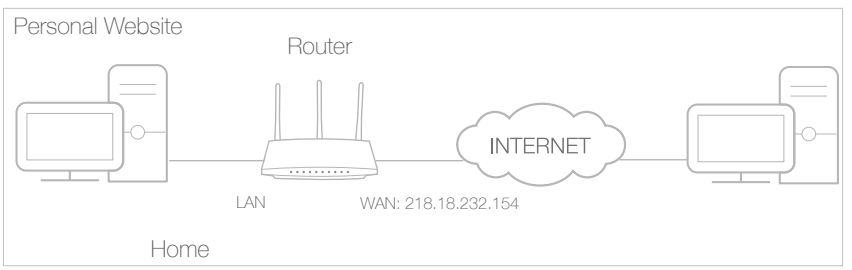
When you build up a server in the local network and want to share it on the Internet, Virtual Server can realize the service and provide it to the Internet users. At the same time virtual server can keep the local network safe as other services are still invisible from the Internet.

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

I want to:

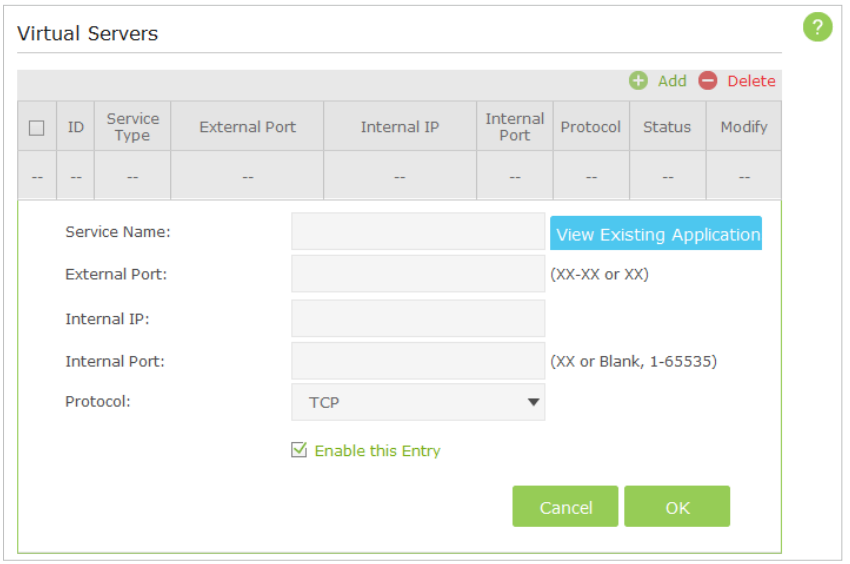
Share my personal website I've built in local network with my friends through the Internet.

For example, the personal website has been built in my home PC (192.168.0.100). I hope that my friends in the Internet can visit my website in some way. The PC is connected to the router with the WAN IP address 218.18.232.154.



How can I do that?

1. Assign a static IP address to your PC, for example 192.168.0.100.
2. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
3. Go to *Advanced* > *NAT Forwarding* > *Virtual Servers*, click Add.
4. Click View Existing Services, and select HTTP. The external port, internal port and protocol will be automatically filled with contents. Enter the PC's IP address 192.168.0.100 in the Internal IP field.
5. Click OK to save the settings.



Tips:

1. It is recommended to keep the default settings of Internal Port and Protocol if you are not clear about which port and protocol to use.
2. If the service you want to use is not in the Service Type, you can enter the corresponding parameters manually. You should verify the port number that the service need.
3. 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 in the Internet can enter http:// WAN IP (in this example: http:// 218.18.232.154) to visit your personal website.

Tips:

1. WAN IP should be a public IP address. For the WAN IP is assigned dynamically by ISP, it is recommended to apply and register a domain name for the WAN refer to *12. 4. Set Up a Dynamic DNS Service Account*. Then you can use http:// domain name to visit the website.
2. If you have changed the default External Port, you should use http:// WAN IP: External Port or http:// domain name: External Port to visit the website.

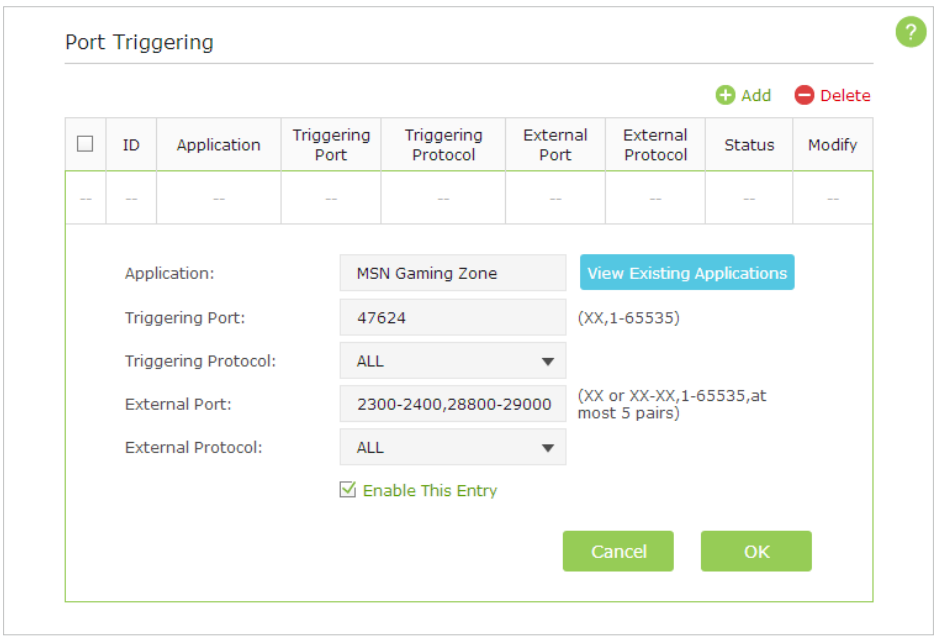
10. 2. Open Ports Dynamically by Port Triggering

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

Follow the steps below to configure the port triggering rules:

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

2. Go to *Advanced* > *NAT Forwarding* > *Port Triggering* and click Add.
3. Click View Existing Applications, and select the desired application. The external port, internal port and protocol will be automatically filled with contents. The following picture takes application MSN Gaming Zone as an example.
4. Click OK to save the settings.



Tips:

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

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

When a PC is set to be a DMZ (Demilitarized Zone) host in the local network, it is totally exposed to the Internet, 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:

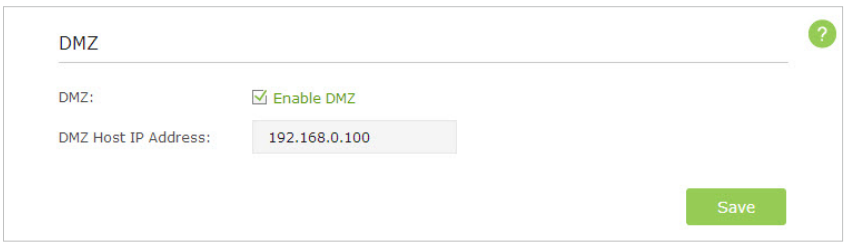
DMZ is more applicable in the situation that users are not clear about which ports to open. When it is enabled, the DMZ host is totally exposed to the Internet, which may bring some potential safety hazard. If DMZ is not in use, please disable it in time.

I want to: Make the home PC join the Internet online game without port restriction.

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

How can I do that?

1. Assign a static IP address to your PC, for example 192.168.0.100.
2. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
3. Go to *Advanced* > *NAT Forwarding* > *DMZ* and select the checkbox to enable DMZ.



4. Enter the IP address 192.168.0.100 in the DMZ Host IP Address filed.
5. Click Save to save the settings.

Done!

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

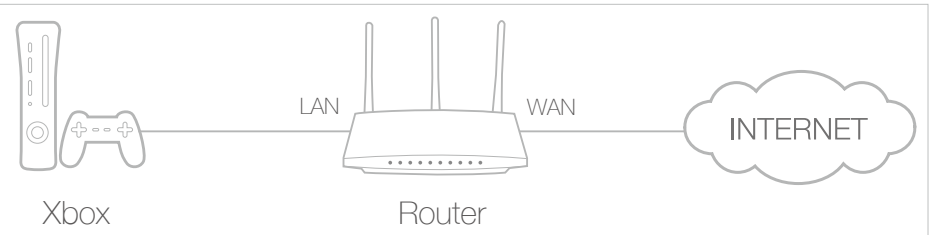
10. 4. Make Xbox Online Games Run Smoothly by UPnP

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

Tips:

1. UPnP is enabled by default in this router.
2. Only the application supporting UPnP protocol can use this feature.
3. 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 the username and password you set for the router;
2. Go to *Advanced* > *NAT Forwarding* > *UPnP* and toggle on or off according to your needs.

Chapter *11*

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.

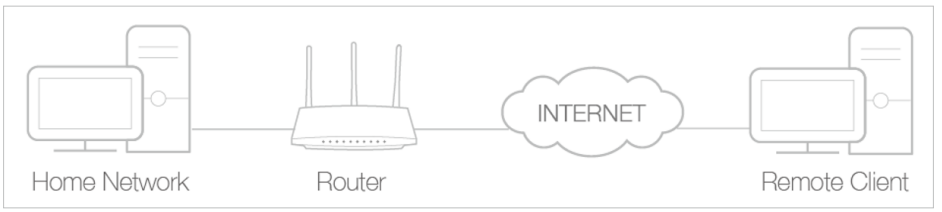
Please choose the appropriate VPN server connection type according to your needs.

This chapter contains the following sections:

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

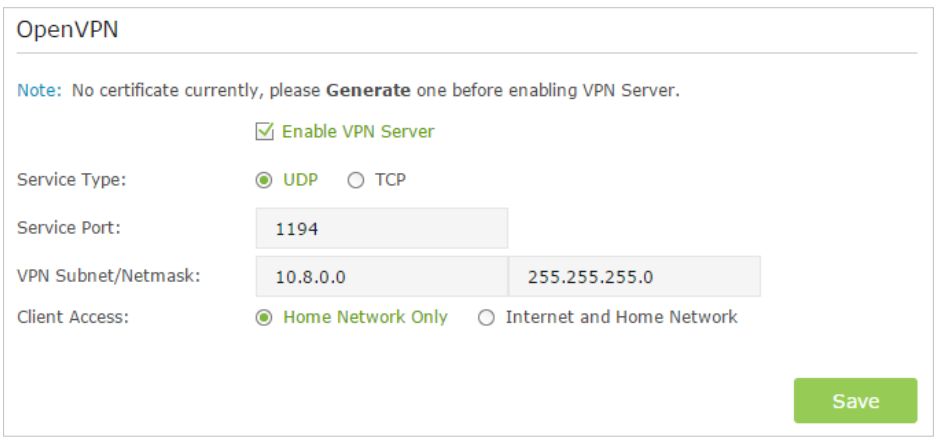
11. 1. Use OpenVPN to Access Your Home Network

In the OpenVPN connection, the home network can act as a server, and the remote client 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 client. Please follow the steps below to set up an OpenVPN connection.



Step1. Set up OpenVPN Server on Your Router

1. Visit *http://tplinkwifi.net*, and log in with the username and password you've set for the router.
2. Go to Advanced > VPN Server > OpenVPN. And then Select Enable VPN Server.



Note:

1. 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.
2. 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 client connects, and the port number should be between 1024 and 65535.

Note:

If you have configured NAT Settings, please make sure the Service Port number is not the same as the external port of NAT Settings.

5. In VPN Subnet/Netmask field, enter the range of IP addresses that can be leased to the client by the OpenVPN server.

6. Select your Client Access type., select Home Network Only if you only want the remote client to access your home network, select Internet and Home Network if the remote client also want to access Internet through VPN Server.
7. Click Save.
8. Click Generate to generate 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. Remote client will use this configuration file to access your router.

Step 2. Configure OpenVPN Connection on Your Remote Client

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

Note:
You need to install the OpenVPN client utility on each client that you plan to use for VPN connections to your router. Mobile devices should download third-party app from Google Play or APP Store.

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

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

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

Step 1. Set up PPTP VPN Server on Your Router

1. Visit *http://tplinkwifi.net*, and log in with the username and password you've set for the router.
2. Go to Advanced > VPN Server > PPTP VPN. And then select Enable VPN Server.

Note:

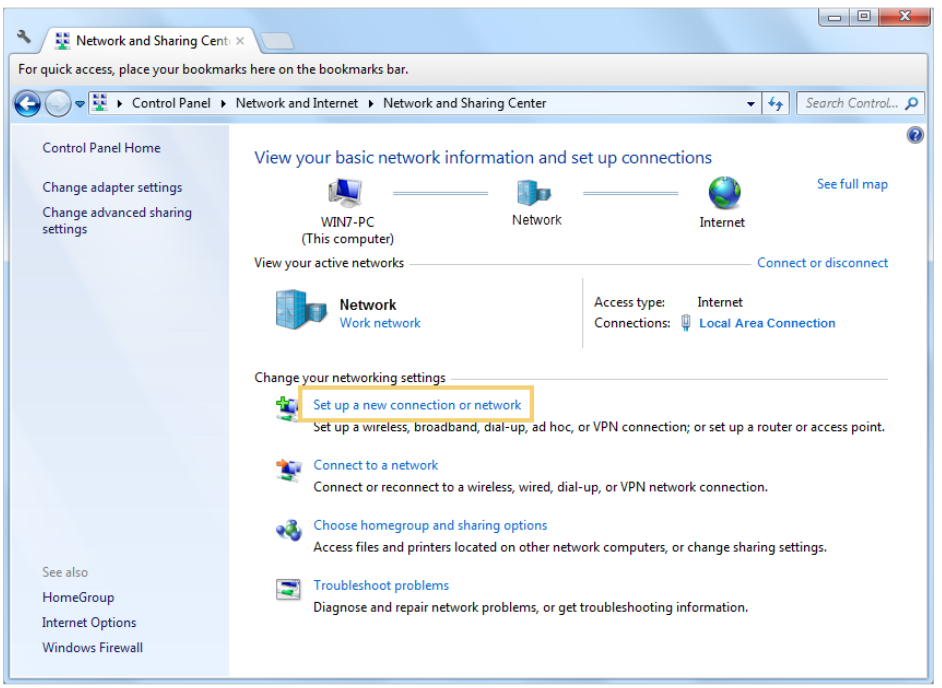
Before you enable VPN Server, we recommend you configure Dynamic DNS Service (recommended) or assign a static IP address for router's WAN port and synchronize your System Time with Internet. If you have configured NAT Settings, please make sure your external port of NAT settings is not 1723.

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

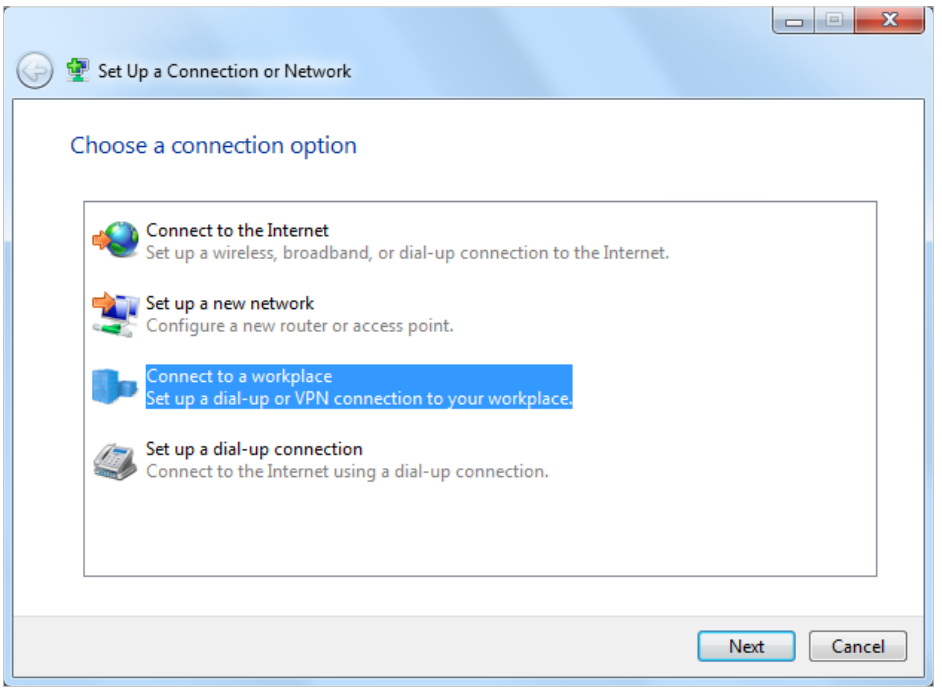
Step 2. Configure PPTP VPN Connection on Your Remote Client

Remote client can use Windows built-in PPTP software or third-party PPTP software to connect to PPTP Server. Here we use 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.

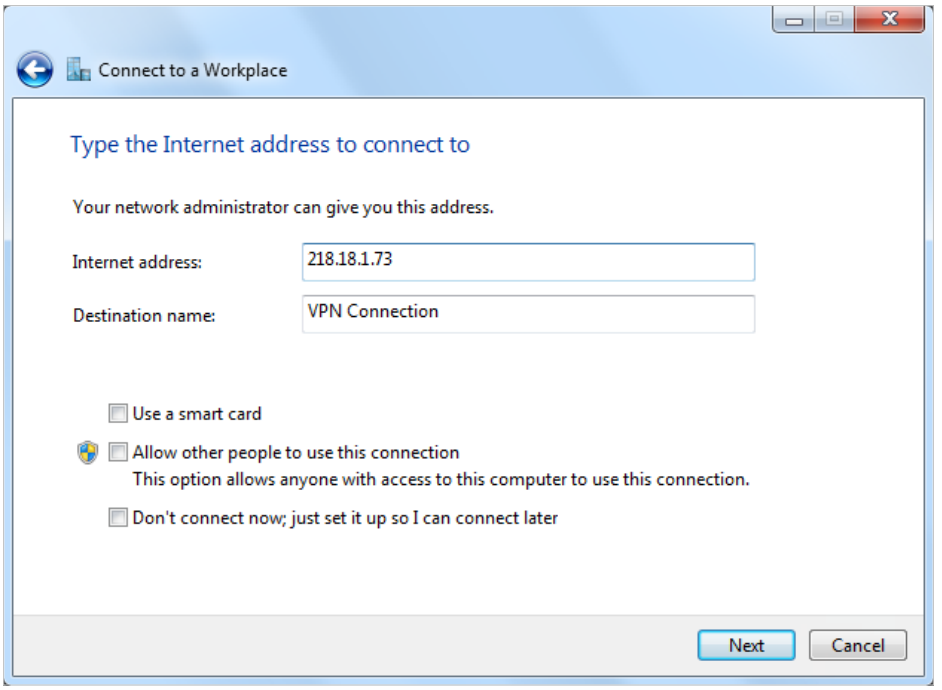


3. Select Connect to a workplace and click Next.

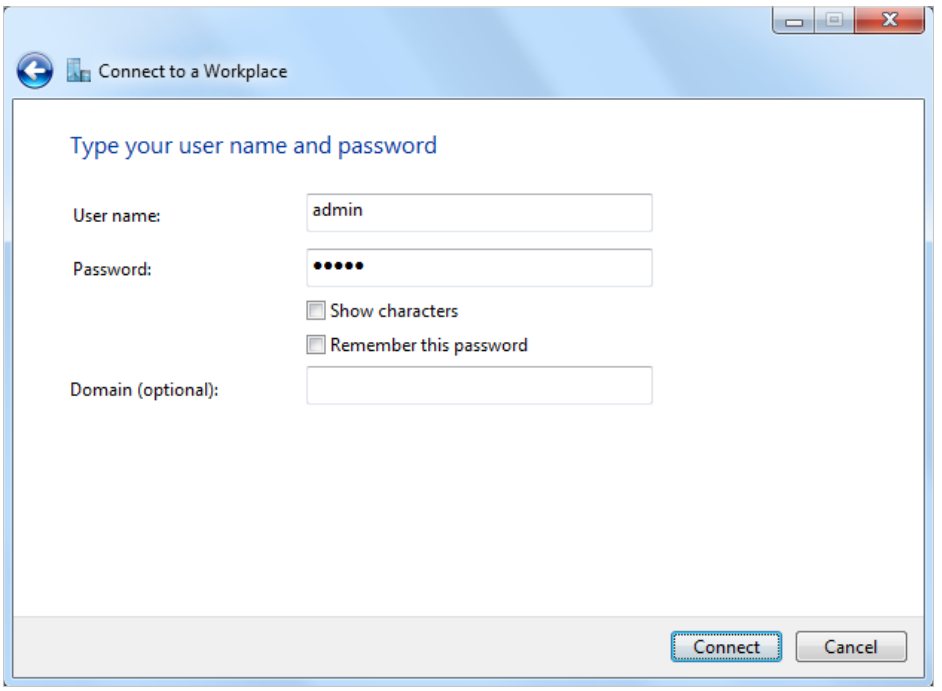


4. Select Use my Internet connection (VPN).

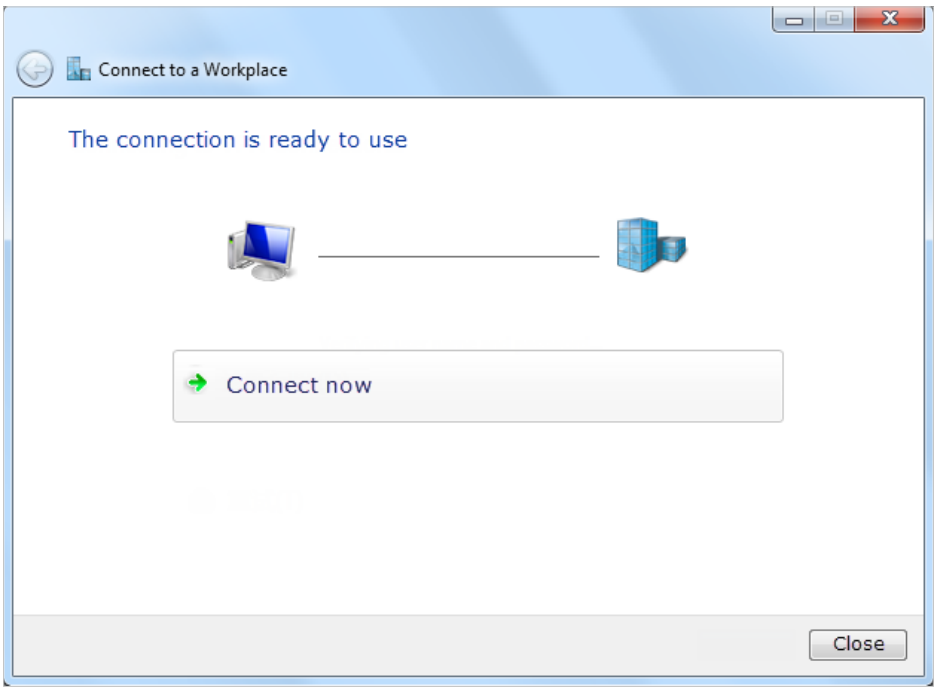
5. Enter the WAN IP address of the router (for example: 218.18.1.73) in the Internet address field. Click Next.



6. Enter the User name and Password, it's the username and password you have set on your router, and click Connect.



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



Chapter *12*

Customize Your Network Settings

This chapter guides you on how to configure advanced networking features that are available for this router.

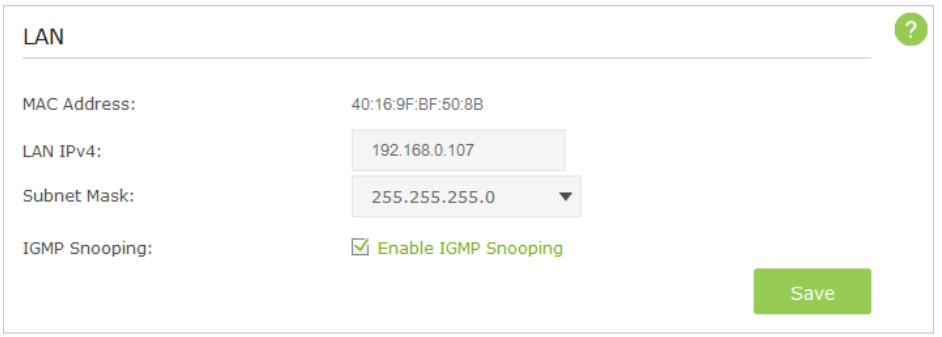
This chapter contains the following sections:

- *Change the LAN Settings*
- *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*
- *Set up a VPN Connection*

12. 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-based 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 the username and password you set for the router.
2. Go to *Advanced* > *Network* > *LAN* page.
3. Type in a new IP address appropriate to your needs.



4. Leave the Subnet Mask as the default settings.
5. Keep IGMP Snooping as enabled by default. IGMP Snooping is the process of listening to IGMP (Internet Group Management Protocol) network traffic. The function prevents hosts on a local network from receiving traffic for a multicast group they have not explicitly joined.
6. 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 them.

12. 2. Configure to Support IPTV Service

IPTV is the abbreviation of Internet Protocol Television. The service can only be delivered through the Internet, and our router provides a specific LAN port for IPTV.

By automatically seperating IPTV from Internet surfing, we guarantee you a high quality of vedio streaming and a high speed of Internet surfing.

I want to: Configure the router to enable Internet Protocol Television (IPTV) Services.

For example, I already bought IPTV service, but this service can only be delivered through the Internet. Therefore, I need to configure my router first.

How can I do that?

1. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
2. Go to *Advanced* > *Network* > *IPTV* to open the configuration page.
3. Configure IPTV settings:

1) Select the Enable IPTV check box.

2) Select the appropriate Mode according to your ISP. Select Bridge if your ISP is not listed and no other parameters are required, and then skip to substep 4. Select Custom if your ISP is not listed but provides necessary parameters.

3) After you have selected a mode, the necessary parameters are predetermined. You can perform other configuration, e.g. enter the IPTV Multicast VLAN ID and select the IPTV Multicast VLAN Priority in Russia mode according to your ISP.

4) select the IGMP Proxy version, either V2 or V3, according to the information provided by your ISP.

5) For Russia, Singapore-ExStream, Malaysia-Unifi and Malaysia-Maxis mode, connect device to the predetermined LAN port. For Bridge and Custom mode, select a LAN port as the IPTV port and connect the set-top box to the corresponding port.

6) Click Save.

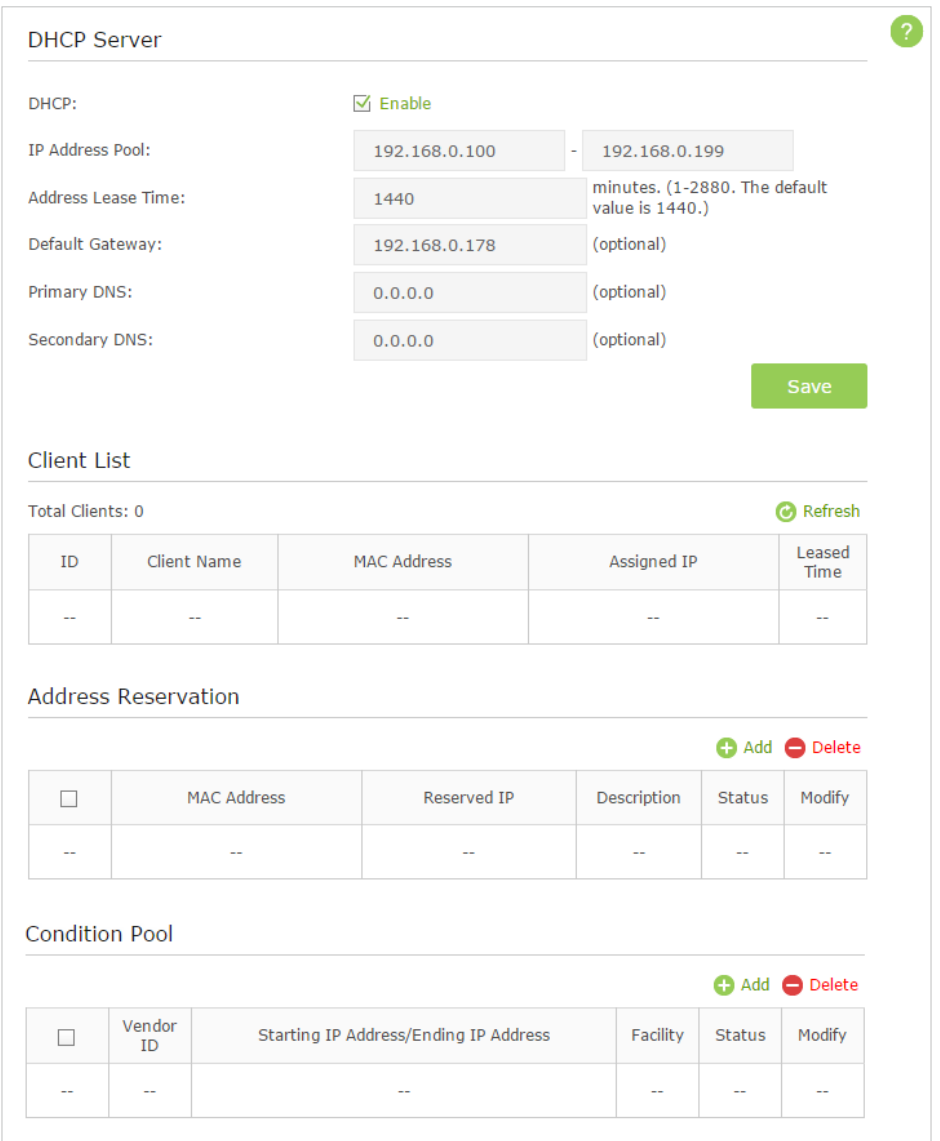
Done!

Your IPTV setup is done now! You may need other configurations on your set-top box before enjoying your TV.

12. 3. 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 DHCP Server if necessary, and you can reserve LAN IP address for specified client device.

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



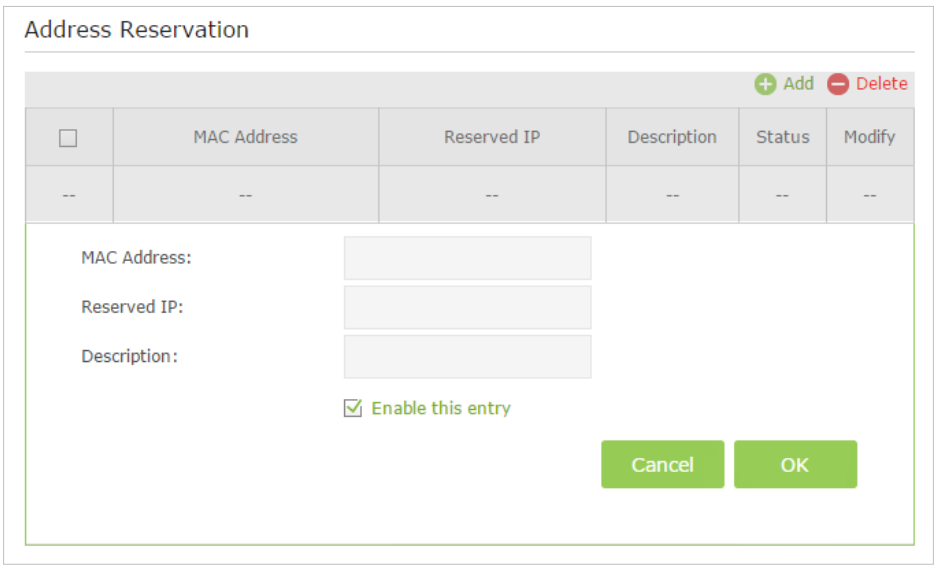
➢ **To specify the IP address that the router assigns**

1. Make sure that the Enable DHCP Server checkbox is selected.
2. Enter the starting and ending IP address in the IP Address Pool.

3. Enter other parameters if the ISP offers, the Default Gateway is automatically filled, which is the same as the LAN IP address of the router.
4. Click Save to make the settings effective.

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

1. Click the Add button.



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

Note:
You can also appoint IP addresses within a specified range to devices of the same type by using Condition Pool feature. For example, you can assign IP addresses within the range (192.168.0.50 to192.168.0.80) to Camera devices, thus facilitating the network management.

12. 4. Set Up a Dynamic DNS Service Account

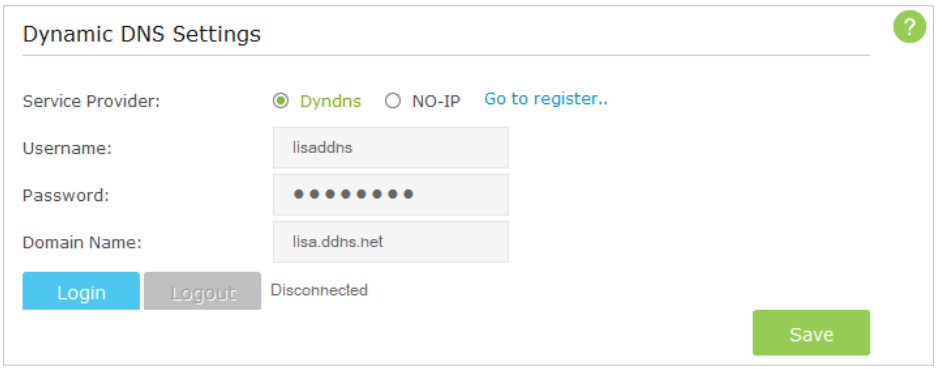
Most ISPs (Internet service provieders) assign a dynamic IP address to the router and you can use this IP address to access your router remotely. However, the IP address can change any time and you don't know when it changes. In this case, you might need the DDNS (Dynamic Domain Name Server) feature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

Note: DDNS does not work if the ISP assigns a private Internet IP address (such as 192.168.0.x) to the router.

To set up DDNS, please follow the instructions below:

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

2. Go to *Advanced* > *Network* > *Dynamic DNS*.
3. Select the DDNS Service Provider (Dyndns or NO-IP). If you don't have a DDNS account, select a service provider and click Go to register.



4. Enter the username, password and domain name of the account.
5. Click Login and click Save.

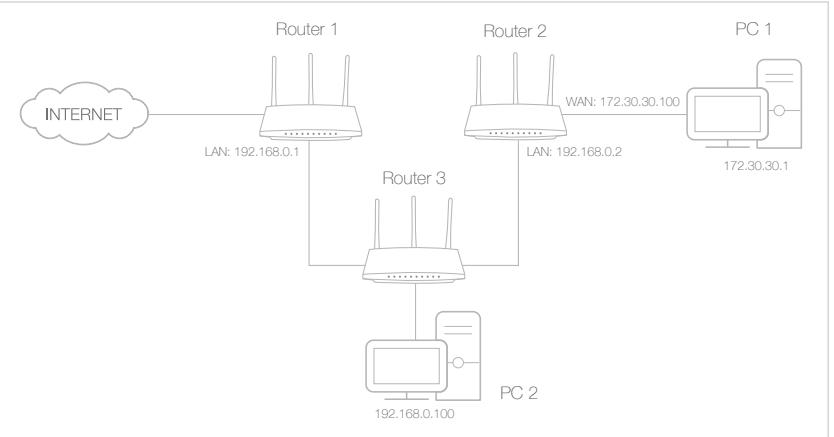
Tips: If you want to use a new DDNS account, please Logout first, then log in with the new account.

12. 5. 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.

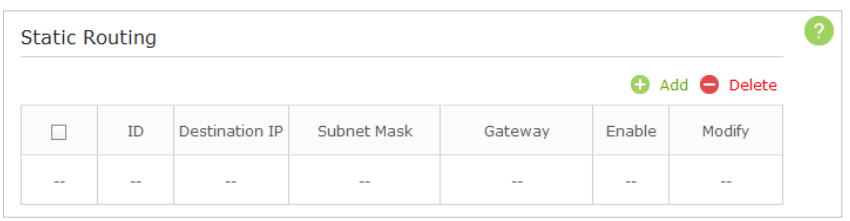
I want to: Visit multiple networks and multiple servers at the same time.

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

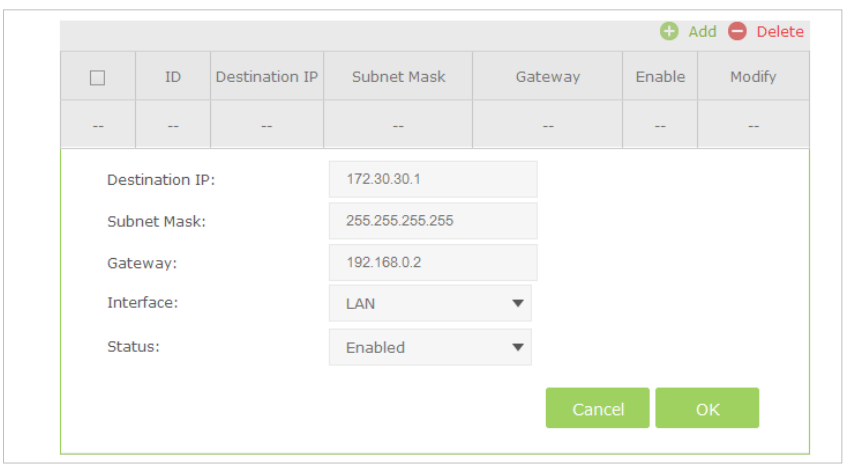


How can I do that?

1. Change the router's LAN IP addresses to two different IP addresses on the same subnet. Disable Router 2's DHCP function.
2. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
3. Go to *Network* > *Advanced Routing*.
4. Click Add to add a new static routing entry.



5. Finish the settings according to the following explanations:



Destination IP: The destination IP address that you want to assign to a static route. This IP address cannot be on the same subnet with the WAN IP or LAN IP of the router. In the example,