

Ø Tips:

To view guest network information, go to Network Map and locate the Guest Network section. You can turn on or off the guest network function conveniently.

8.2. Customize Guest Network Options

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with your TP-Link ID or the password you set for the router.
- 2. Go to Advanced > Wireless > Guest Network. Locate the Guest Permissions section.
- 3. Customize guest network options according to your needs.

Guest Permissions	
Control the data that guests can access.	
c	Allow guests to see each other
C	Allow guests to access your local network

Allow guests to see each other

Tick this checkbox if you want to allow the wireless clients on your guest network to communicate with each other via methods such as network neighbors and Ping.

• Allow guests to access your local network

Tick this checkbox if you want to allow the wireless clients on your guest network to communicate with the devices connected to your router's LAN ports or main network via methods such as network neighbors and Ping.

4. Click SAVE. Now you can ensure network security and privacy!

Chapter 9

USB Settings

This chapter describes how to use the USB ports to share files and media from the USB storage devices over your home network locally, or remotely through the internet.

The router supports USB external flash drives and hard drives.

It contains the following sections:

- <u>Access the USB Storage Device</u>
- Media Sharing
- Time Machine

9.1. Access the USB Storage Device

Insert your USB storage device into the router's USB port and then access files stored there locally or remotely.

Ø Tips:

- If you use USB hubs, make sure no more than 4 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, exFat, NTFS or HFS+.
- Before you physically disconnect a USB device from the router, safely remove it to avoid data damage: Go to Advanced
 > USB > USB Storage Device and click Remove.

9. 1. 1. Access the USB Device Locally

Insert your USB storage device into the router's USB port and then refer to the following table to access files stored on your USB storage device.

	Method 1:	
	Go to Computer > Network, then click the Network Server Name (TP- SHARE by default) in the Computer section.	
	Note: Operations in different systems are similar. Here we take Windows 7 as an example.	
	File Edit View Tools Help	
	File Edit View Tools Help	
Windows	Organize Metwork and Sharing Center Add a printer	
computer	Favorites Computer (3)	
	Libraries TP-SHARE	
	Media Devices (1)	
	14 Computer	
	Network / Network Infrastructure (1)	
	Andrea (100	

Windows computer	 Method 2: Open the Windows Explorer (or go to Computer) and type the server address \\tplinkwifi.net or ftp://tplinkwifi.net in the address bar, then press Enter.
Мас	 Select Go > Connect to Server. Type the server address smb://tplinkwifi.net. Click Connect. Image: Connect to Server in the server is the server i
Tablet	Use a third-party app for network files management.

Ø Tips:

You can also access your USB storage device by using your Network/Media Server Name as the server address. Refer to <u>To Customize the Address of the USB Storage Device</u> to learn more.

9. 1. 2. Access the USB Device Remotely

You can access your USB disk outside the local area network. For example, you can:

- Share photos and other large files with your friends without logging in to (and paying for) a photo-sharing site or email system.
- Get a safe backup for the materials for a presentation.
- Remove the files on your camera's memory card from time to time during the journey.

Note:

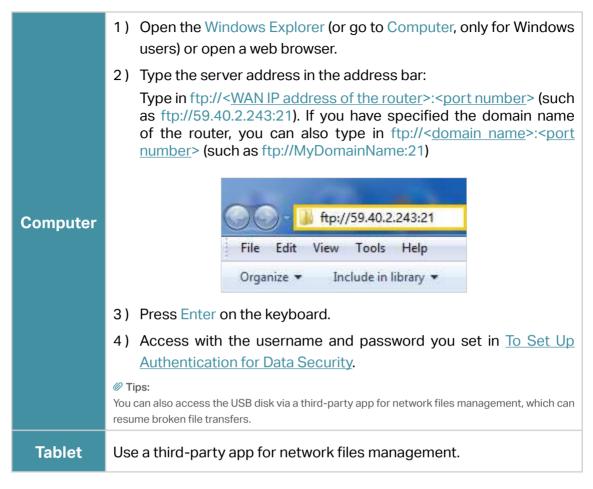
If your ISP assigns a private WAN IP address (such as 192.168.x.x or 10.x.x.x), you cannot use this feature because private addresses are not routed on the internet.

Follow the steps below to configure remote access settings.

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with your TP-Link ID or the password you set for the router.
- 2. Go to Advanced > USB > USB Storage Device.
- 3. Tick the Internet FTP checkbox, and then click SAVE.

Access Method			
Select the method access address.	for accessing your USB	storage device. The device can then be reac	hed via the
Network/I	ledia Server Name:	'P-Share	
Enable	Access Metho	d Address	Port
	Samba for Win	tows 0.TP-Share	
	Local FTP	ftp://192.168.0.1:21	21
	Internet FTP	ftp://0.0.0.0.21 Set DDNS	21

4. Refer to the following table to access your USB disk remotely.



Ø Tips:

Click Set Up a Dynamic DNS Service Account to learn how to set up a domain name for you router.

9. 1. 3. Customize the Access Settings

By default, all the network clients can access all folders on your USB disk. You can customize your sharing settings by setting a sharing account, sharing specific contents and setting a new sharing address on the router's web management page.

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

• To Customize the Address of the USB Storage Device

You can customize the server name and use the name to access your USB storage device.

1. In the Access Method session, make sure Samba for Windows is ticked, and enter a Network/Media Server Name as you like, such as MyShare, then click SAVE.

ess address	an and any first state and an	device. The device can then be reach	
Network/M	ledia Server Name MyShare		
Enable	Access Method	Address	Port
8	Samba for Windows	WTP-Share	-
8	Local FTP	ftp://192.168.0.1.21	25
0	internet FTP	Tp://0.0.0.0.21	21

2. Now you can access the USB storage device by visiting \\MyShare (for Windows) or smb://MyShare (for Mac).

• To Only Share Specific Content

Focus on the File Sharing section. Specify sharing folders that you want to share and click SAVE.

Sharing	g Contents:	
	Share Selected Folders	Ø
	G:/Document	

• To Set Up Authentication for Data Security

You can set up authentication for your USB storage device so that network clients will be required to enter username and password when accessing the USB storage device.

1. In the File Sharing section, enable Secure Sharing.

ecure Sharing				
unionize the access	entropy to ensure data	recards.		
Usemame	Password		Permissions	Modity
admin		ø	Read&Wite	2
wat		çő.	Read	E)

2. Click is to modify the access account. The username and password are both admin for default administrator account, and both visit for default visitor account. Accessing as an administrator can read and modify the shared folders while visitors can only read the shared folders.

Note:

- 1. For Windows users, do not set the sharing username the same as the Windows username. Otherwise, Windows credential mechanism may cause the following problems:
 - If the sharing password is also the same as the Windows password, authentication will not work since the Windows will automatically use its account information for USB access.
 - If the sharing password is different from the Windows password, the Windows will be unable to remember your credentials and you will always be required to enter the sharing password for USB access.
- 2. Due to Windows credential mechanism, you might be unable to access the USB disk after changing Authentication settings. Please log out from the Windows and try to access again. Or you can change the address of the USB disk by referring to <u>To Customize the Address of the USB Storage Device</u>.

9.2. Media Sharing

The feature of Media Sharing allows you to view photos, play music and watch movies stored on the USB storage device directly from DLNA-supported devices, such as your computer, tablet and PS2/3/4.

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with your TP-Link ID or the password you set for the router.
- 2. Go to Advanced > USB > USB Storage Device.
- 3. Enable Media Sharing.

Media Sharing
View photos, play music and watch movies stored on the USB storage device via the access address.
Media Sharing: 🔍

- 4. When your USB storage device is inserted into the router, your DLNA-supported devices (such as your computer and pad) connected to the router can detect and play the media files on the USB storage devices.
- 5. Refer to the following table for detailed instructions.



9.3. Time Machine

Time Machine backs up all files on your Mac computer to a USB storage device connected to your router.

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

Time Machine		
Back up all files on your Mac to a USB s	torage device connected to y	our router.
Time Machine:	Enable	
Backup Location:		
	Please select a location	for Time Machine backups
	SELECT	
Storage Limit for Backups:	0.0	GB
	(Enter "0" for no limit.)	

- 3. Tick the checkbox to enable Time Machine.
- 4. Click Select to select a location for Time Machine backups.
- 5. Set the Size Limit for Backups.

Note: 0 means no limit for the space.

6. Click SAVE.

Chapter 10

HomeShield

Customize your home network with enhanced security using a kit of features built in TP-Link HomeShield. Whether protecting your sensitive data or limiting the access of kids and guests, TP-Link HomeShield provides you the tools you need to fully manage your network.

It contains the following sections:

- Network Check
- Parental Controls
- <u>QoS</u>
- More Features

*For an easier way to check your home network protection system, you can download the Tether app to enjoy full Homeshield Pro feature.

10.1. Network Check

Scan your whole network to help analyze and optimize your network.

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with your TP-Link ID or the password you set for the router.
- 2. Go to Advanced > HomeShield > Network Check.
- 3. Click SCAN.
- 4. Optimize your network according to the tips.

Network Check		
Check your network for better n	etwork performance and security.	
	The following items can be optimited in the following items can be optimited in the optimited items in the optited items in the optimited items in the optited i	ized. 1 risk To be optimized
Network Sercurity 🕜		
DMZ		0
Port Triggering		0
Port Forwarding		0
Guest Network		0
Wi-Fi Password	rong. It is recommended to use a comi I.	Change Password bination of English letters,numbers,
Firmware Version		•
Network Performance		
Wi-Fi Interference	h.	Optimize

10.2. Parental Controls

Parental Controls allows you to set up unique restrictions on internet access for each member of your family. You can block inappropriate content, set daily limits for the total time spent online and restrict internet access to certain times of the day.

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with your TP-Link ID or the password you set for the router.
- 2. Go to Advanced > HomeShield > Parental Controls.
- 3. Click 🔂 📶 to create a profile for a family member.
- 4. Add basic profile information.

Create Profile		×
(Gardeline)	Content Filter	Time Controls
Basic Info		
Profile Name	Age 🕥	
	Prefer Not to Say 🧠	
Devices		
+ Add Devrane]	
	- 0	ANCEL NET

- 1) Enter a Name for the profile to make it easier to identify. Set the age to get the corresponding filter level.
- 2) Under Devices, click
- 3) Select the devices that belong to this family member. Access restrictions will be applied to these devices. Click Add when finished.

Note: Only devices that have previously been connected to your router's network are listed here. If you are unable to find the device you want to add, connect it to your network and then try again.

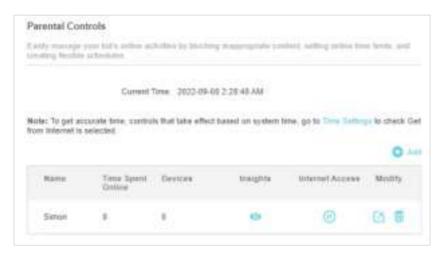
- 4) Click NEXT
- 5. Block content for this profile.

Create Profile			>
Basic lefts	Cunterel Filler	Time Control	
Content Filter			
Select categories to plack the	conveponding current.		
Select Categories 🧿			
Adult Content	Sex Education	Gambling	
Online Communication	Social Networking	Pey to Surf	
Media	Doeminad	Games	
Blocked Websites			
	iting a UEL, or block all websi	les containing a specific keywo	
Enter a beyond or URL	244		
		BACK NE	at

- 1) Select the content categories to block in the Content Filter list.
- 2) You can also block a specific website. Enter a keyword (for example, "Facebook") or a URL (for example, "www.facebook.com"), then click Add.
- 3) Click NEXT.
- 6. Set time restrictions on internet access.

Create Profile		×
Basic Info	Content Filter	Time Controls
Time Controls Set internet access time for th	e profile.	
Bedtime		
When enabled, internet is una	vailable during this period.	
Bedtime:	D	
From:	v:00 v	PM v
To:	✓ : 00 ✓	AM 🗸 (next day)
	entrols? Go to Homeshield > More I Tether to enjoy full Homeshield Pr	
		SACK SAVE

- 4) Enable Bed Time and use the up/down arrows or enter times in the fields. Devices under this profile will be unable to access the internet during this time period.
- 5) Click SAVE.
- 6) After adding a profile, you can click the Insight icon to check the detailed visited history, and click (11) the pause the network for this profile anytime.



Note: You can go to Advanced > HomeShield > More Features for a detailed introduction and download Tether to enjoy full Homeshield Pro feature.

10.3. QoS

QoS (Quality of Service) allows you to prioritize connection of specific devices for a set duration. Devices set as high priority will be allocated more bandwidth and so continue to run smoothly even when there is heavy traffic on the network.

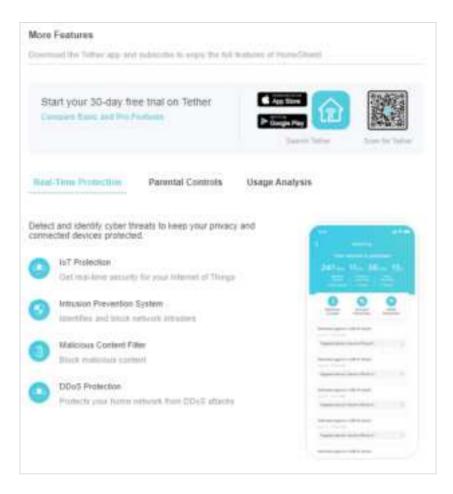
- 1. Visit <u>http://tplinkwifi.net</u>, and log in with your TP-Link ID or the password you set for the router.
- 2. Go to Advanced > HomeShield > QoS.
- 3. Enable QoS to set the total bandwidth. Then click SAVE.
- 4. Enable High Priority for the desired device and set its effective time.

solution is affect of specific do	teres to from store a	fetto cineat	206	
200	Enable			
Download Bandwidth	1000	Magai	4	
Uptned Bandwidth:	1000	Maps	0	
information	Real-line Nate	traffic there	ingh.	Timing
UNKNOWN	1 0 Kb/b			
(III) PG-04485. (III.79234	4 0 100	040		Alertyt
	GoS Downtuad Bandwidth Upload Bandwidth Sritty	GoS Enable Downtrad Bandwidth 1000 Uptrad Bandwidth 1000	Op5. Enable Downtoad Bandwidth 1000 Mitps Uptual Bandwidth 1000 Mitps	OoS Enable Downtoad Bandwieth: 1000 Mitgs - Optical Bandwieth: 1000 Mitgs - Strity

10.4. More Features

Download the Tether app and subscribe to enjoy the full features of HomeShield.

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with your TP-Link ID or the password you set for the router.
- 2. Go to Advanced > HomeShield > More Features.
- 3. Follow the web instructions to get full features of HomeShield.



Chapter 1

EasyMesh with Seamless Roaming

This product is compatible with EasyMesh. This chapter introduces the EasyMesh feature.

It contains the following sections:

- Add a Router as a Satellite Device
- Add a Range Extender as a Satellite Device
- Manage Devices in the EasyMesh Network

EasyMesh routers and extenders work together to form one unified Wi-Fi network. Walk through your home and stay connected with the fastest possible speeds thanks to EasyMesh's seamless coverage.

Note: Routers and range extenders must be compatible with EasyMesh or OneMesh™. Firmware upgrades may be required.

1.1. Add a Router as a Satellite Device

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

EasyMesh	
Connect EasyMesh and OneMesh devices to centralized management.	create a mesh network for seamless WI-FI coverage and
EasyMesh: 🚺	
Tip: Enable Smart Connect to work with Easy!	Mesh for better seamless roaming.
What's EasyMesh?	
EasyMesh Network	
Set up and manage your EasyMesh network.	
Current Mode: Main Router	🖨 Change Mode
In this mode, you can add EasyMesh and One	Mesh devices to boost WI-FI coverage.
ADO S	BATELLITE DEVICES

3. Click ADD SATELLITE DEVICES, select TP-Link Router, then click NEXT.

Add Satellite Devices	3
With type of samilie devices its you want to add?	
TP-Last Reader Jackailes 77-Last Calcolect and Continent Seconds	
TP-Law Extender products TP-CHA Excellents and Orienteen diversioned	
Citiens protocol Careptonal Insurance of allow being to	
0	NEXT NEXT

4. Follow the page instructions to prepare your satellite router, then click DONE.

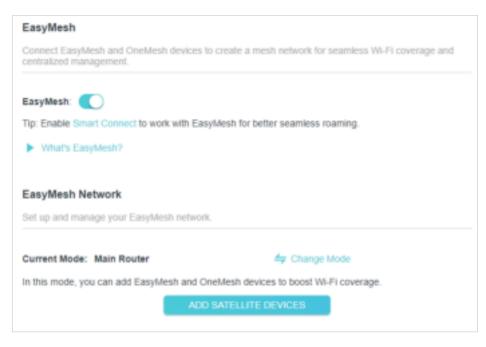


5. Click ADD. When prompted "This device has been added successfully", click OK, then click FINISH.

nii Salatina Ro	uters		×
		to the mesty petieds	N.
	Cameline Funder Header F.		
			Seatting
Name	MAC Address	Reptat	Ade
Aither CBS	34-65-79-67-62-99	4	1000
		NACK.	FREN.
	marity TP-Lon i nge tim maha ha ngi tensora7	nge Der mehne ha Catellin Finaler mader) Nat Genützen?	martin TP-Link Salelitte routies, and add them to the mesh networking the model (the model in Cambin Finales model) Tot broken? (Name MAAC Address Rights Archer Call 3448-PH-61-62-98 af

1.2. Add a Range Extender as a Satellite Device

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



- 3. Plug in the extender next to the main router.
- 4. With in 2 minutes, press the WPS button on main router and on the extender. Wait until the WPS process is complete.
- 5. Done! You can check the mesh device on the router's web page too.

EasyMesh					
Connect EasyMesh and OneMes centralized management.	h devices to create	a mesh netw	ork for sear	nless Wi-Fi cov	erage and
EasyMesh: 🚺					
Tip: Enable Smart Connect to wo	rk with EasyMesh f	for better sean	nless roami	ng.	
What's EasyMesh?					
EasyMesh Network					
Set up and manage your EasyMe	sh network.				
Current Mode: Main Router		4 CI	hange Mode	1	
In this mode, you can add EasyM	lesh and OneMesh	devices to bo	ost WI-Fi co	werage.	
Note: TP-Link satellite routers wit	I follow the main ro	uter's LED Co	ontrol Setting	gs.	
Satellite Devices: 1					
Device Info	IP Address	Location	Clients	Connectio n	Modify
Art_E5 00-AA-EB-07-20-66	192.168.0.22	Not set	0	aff	0
	ADD SATEL	LITE DEVICE	s		

1.3. Add a Range Extender as a Satellite Device

In an EasyMesh network, you can manage all mesh devices and connected clients on your main router's web page.

• To view mesh devices and connected clients in the network:

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with your TP-Link ID or the password you set for the router.
- 2. Go to Network Map.
- 3. Click 💆 to view all mesh devices, and click 💆 to view all connected clients.
- To manage an EasyMesh device in the network:
- 1. Visit <u>http://tplinkwifi.net</u>, and log in with your TP-Link ID or the password you set for the router.
- 2. Go to Advanced > EasyMesh.



3. Click the Modify button to view detailed information and change its settings.

and a later		1000		
here		-	Device Name	Pagentikkt arent
Scenario	-Panel Arest	935	Provident	102 198.5.11 35-46 07.43 Cit-26
(* Address	12.94172			
MAC Address	CT 10. 5 10 7 20 M			
Spectropy	-41			
List Speed	2 Mays (2 alter) 2 (lays (4094) mind net			

- Change device information.
- Click Manage to redirect to the web management page of this device.
- Click Remove to delete this device from the EasyMesh network.

Chapter 12

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 from cyber attacks, block or allow specific client devices to access your network using Access Control, you can prevent ARP spoofing and ARP attacks using IP & MAC Binding, protect your network security by isolating your IoT devices.

It contains the following sections:

- Protect the Network from Cyber Attacks
- <u>Access Control</u>
- IP & MAC Binding
- <u>ALG</u>
- IoT Security

*For a more comprehensive home network protection system, refer to the <u>HomeShield</u> chapter.

12.1. Protect the Network from Cyber Attacks

The SPI (Stateful Packet Inspection) Firewall protects the router from cyber attacks and validate the traffic that is passing through the router based on the protocol. This function is enabled by default.

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with your TP-Link ID or the password you set for the router.
- 2. Go to Advanced > Security > Firewall. It's recommended to keep the default settings.



12.2. 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:

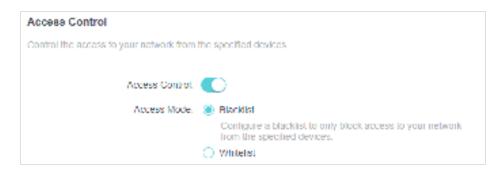
Block or allow specific client devices to access my network (via wired or wireless).

How can I do that?

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with your TP-Link ID or the password you set for the router.
- 2. Go to Advanced > Security > Access Control.
- 3. Toggle on to 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) Click 🕂 Add and select devices you want to be blocked and Click ADD.
- 3) The Operation Succeeded message will appear on the screen, which means the selected devices have been successfully added to the blacklist.



To allow specific device(s):

1) Select Whitelist and click SAVE.

Access Control	
Control the access to your network from	the specified devices.
Access Control:	
Access Mode:	O Blacklist
	Whitelist Configure a whitelist to only allow access to your network
	from the specified devices.

2) Your own device is in the whitelist by default and cannot be deleted. Click 😏 🚧 to add other devices to the whitelist.

Device Type	Device Name	MAC Address	Modify
	UNKNOWN	00-19-66-35-E1-B0	1

- Add connected devices
- 1) Click Select From Device List.
- 2) Select the devices you want to be allowed and click ADD.

Add Devices	×
Select From Device List Add Manually	
Yan Maring Control Andrews	ana ana ana ana ana ana
	CARCES. ADD

- 3) The Operation Succeeded message will appear on the screen, which means the selected devices have been successfully added to the whitelist.
- Add unconnected devices
- 1) Click Add Manually.
- 2) Enter the Device Name and MAC Address of the device you want to be allowed and click ADD.

Add Devices					×	8
Select From		Jat				
MAC Address	12	a:	2	2		
					CANICEL ADD	Į.

3) The Operation Succeeded message will appear on the screen, which means the device has been successfully added to the whitelist.

Done!

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

12.3. IP & MAC Binding

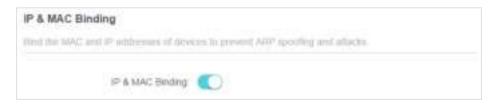
IP & MAC Binding, namely, ARP (Address Resolution Protocol) Binding, is used to bind network device's IP address to its MAC address. This will prevent ARP Spoofing and other ARP attacks by denying network access to an device with matching IP address in the Binding list, but unrecognized MAC address.

I want to:

Prevent ARP spoofing and ARP attacks.

How can I do that?

- 1. Visit <u>http://tplinkwifi.net</u>, 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):

1) Click 😌 🚧 in the Binding List section.

Binding List			
Add or delete binding end	1914		
			O Act
Device Name	MAC Address	IP Address	Modify
No Entries			

2) Click VIEW CONNECTED DEVICES and select the device you want to bind. The MAC Address and IP Address fields will be automatically filled in.

Add Binding Entry		×
MAC Address	3 2 3 2 3)	
1	VEW CONNECTED DEVICES	
IP Address		
	CANKIEL	540 D

3) Click SAVE.

To bind the unconnected device:

1) Click 😌 🚧 in the Binding List section.

linding List			
aa or acente binding era	1916		
			0 40
Device Name	MAC Address	IP Address	Modify
No Entries			

- 2) Enter the MAC Address and IP Address that you want to bind.
- 3) Click SAVE.

Done!

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

12.4. ALG

ALG allows customized NAT traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols such as FTP, TFTP, H323 etc. It is recommended to keep the default settings.

You may need to disable SIP ALG when you are using voice and video applications to create and accept a call through the router, since some voice and video communication applications do not work well with SIP ALG.

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

ALG	
Check the ALC (Application Layer Gates	way) settings. It is recommended to keep them as default
PPTP Passthrough.	
L2TP Passthrough.	
IPSec Passthrough.	
LIPALG.	
IT TPALG.	
RISPALG.	
1323 ALG.	
SIPALG.	

12.5. IoT Security

Some devices, such as IoT devices, are vulnerable to security threats. To keep your important devices and data safe, you can isolate these devices to protect your network from being infected.

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with your TP-Link ID or the password you set for the router.
- 2. Go to Advanced > Security > IoT Security. Enable Device Isolation.

Device Isolation			
solate devices (such as le	oT devices) to protect your net	twork from security threats	
Dev	nce isolation. 🌔 🔗		
Note: We recommend dis	abling AP Isolation which may	isolate all devices from each o	alher.
solated Devices, 0			•
services, o			🔂 Add
Device Type	Device Name	MAC Address	Modify
~	Device Name	MAC Address	Modify

Chapter 13

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 Port Forwarding, Port Triggering, UPNP and DMZ.

It contains the following sections:

- Share Local Resources on the Internet by Port Forwarding
- Open Ports Dynamically by Port Triggering
- <u>Make Applications Free from Port Restriction by DMZ</u>
- Make Xbox Online Games Run Smoothly by UPnP

13.1. Share Local Resources on the Internet by Port Forwarding

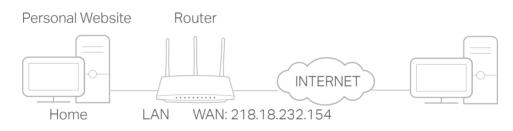
When you build up a server on the local network and want to share it on the internet, Port Forwarding can realize the service and provide it to internet users. At the same time Port Forwarding can keep the local network safe as other services are still invisible from the internet.

Port Forwarding 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 <u>http://tplinkwifi.net</u>, and log in with your TP-Link ID or the password you set for the router.
- 3. Go to Advanced > NAT Forwarding > Port Forwarding.
- 4. Click 😏 👫.

P	ort Forward	ling					
Sţ	ecify ports to	make specific d	evices or service	es on your loo	al network acce	ssible over the	e internet.
							🕒 Add
	Service Name	Device IP Address	External Port	Internal Port	Protocol	Status	Modify
	No Entries						

- 5. Click VIEW COMMON SERVICES and select HTTP. The External Port, Internal Port and Protocol will be automatically filled in.
- 6. Click VIEW CONNECTED DEVICES and select your home PC. The Device IP Address will be automatically filled in. Or enter the PC's IP address 192.168.0.100 manually in the Device IP Address field.
- 7. Click SAVE.

Add a Port Forwarding Entry		×
Service Name:	НТТР	
	VIEW COMMON SERVICES	
Device IP Address:	192.168.0.100	
	VIEW CONNECTED DEVICES	
External Port:	80	
Internal Port:	80	
Protocot:	TCP V	
	Enable This Entry	
	CANCEL	SAVE

- Ø 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 common services list, you can enter the corresponding parameters
 manually. You should verify the port number that the service needs.
- You can add multiple port forwarding 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.

Ø 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 <u>Set Up a Dynamic DNS Service Account</u>. 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.

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

	s (from the inter			mically open spe red it.	cific external p	ports and
						0
Service Name	Triggering Port	Triggering Protocol	External Port	External Protocol	Status	Modify

2. Go to Advanced > NAT Forwarding > Port Triggering and click 😌 🚧.

3. Click VIEW COMMON SERVICES, and select the desired application. The Triggering Port, Triggering Protocol and External Port will be automatically filled in. The following picture takes application MSN Gaming Zone as an example.

Add a Port Triggering Entry			×
Service Name:	MSN Gaming Zone		
	VIEW COMMON S	SERVICES	
Triggering Port:	47624		
Triggering Protocol:	Al	~	
External Port:	2300-2400,28800-29	000	
	(XX or XX-XX, 1-6553)	5,at most 5 pairs)	
External Protocol:	All	~	
	Enable This Entry		
		CANCEL	SAVE

4. Click SAVE.

Ø 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.

13.3. 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 log in 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 <u>http://tplinkwifi.net</u>, and log in with your TP-Link ID or the password you set for the router.
- 3. Go to Advanced > NAT Forwarding > DMZ and tick to enable DMZ.
- 4. Click VIEW CONNECTED DEVICES and select your PC. The Device IP Address will be automatically filled in. Or enter the PC's IP address 192.168.0.100 manually in the DMZ Host IP Address field.

DMZ	
Expose a specific device in your local ne real-time communications.	twork to the internet for applications such as online gaming and
DMZ	C Enable
DMZ Host IP Address:	192.168.0.100
	VIEW CONNECTED DEVICES

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.

13.4. 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 <u>http://tplinkwifi.net</u>, 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.

JPnP
mattie UPhill (Universal Plug and Play) to allow devices on your socal network to dynamically open ports or applications with an multiplayer galling and real-lane communications.
UPnP:

Chapter 14

VPN Server&Client

The router offers several ways to set up VPN connections:

VPN Server allows remote devices to access your home network in a secured way through the internet. The router supports three types of VPN Server:

OpenVPN is somewhat complex but with higher security and more stability, suitable for restricted environments such as campus network and company intranet.

PPTP VPN is easy to use with the built-in VPN software of computers and mobile devices, but it is vulnerable and may be blocked by some ISPs.

L2TP/IPSec VPN is more secure but slower than PPTP VPN, and may have trouble getting around firewalls.

VPN Client allows devices in your home network to access remote VPN servers, without the need to install VPN software on each device.

This chapter contains the following sections:

- Use OpenVPN to Access Your Home Network
- Use PPTP VPN to Access Your Home Network
- Use L2TP/IPSec VPN to Access Your Home Network
- Use VPN Client to Access a Remote VPN Server

14.1. Use OpenVPN to Access Your Home Network

OpenVPN Server is used to create an OpenVPN connection for remote devices to access your home network.

To use the VPN feature, you need to enable OpenVPN Server on your router, and install and run VPN client software on remote devices. Please follow the steps below to set up an OpenVPN connection.



Step1. Set up OpenVPN Server on Your Router

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

OpenVPN	
Set up an OpenVPN for secure, remote	access to your network.
Note: No certificate has been created. O	Senerate one below before enabling OpenVPN.
OpenVPN:	C Enable
Service Type:	UDP
	O TCP
Service Port:	1194
VPN Subnet:	10.8.0.0
Netmask:	255.255.255.0
Client Access:	Home Network Only

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 Service 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.

Certificate		
Generate the certricale		
	GENERATE	

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.

Configuration File		
Export the configuration file.		
	EXPORT	

Step 2. Configure OpenVPN Connection on Your Remote Device

1. Visit <u>http://openvpn.net/index.php/download/community-downloads.html</u> 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 function 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.

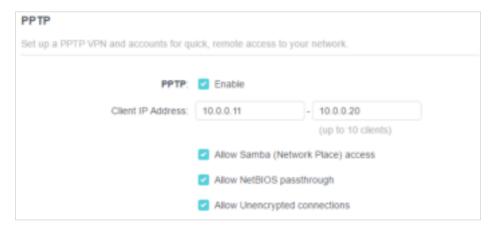
14.2. Use PPTP VPN to Access Your Home Network

PPTP VPN Server is used to create a PPTP VPN connection for remote devices to access your home network.

To use the VPN feature, you need to set up PPTP VPN Server on your router, and configure the PPTP connection on remote devices. Please follow the steps below to set up a PPTP VPN connection.

Step 1. Set up PPTP VPN Server on Your Router

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



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 field, enter the range of IP addresses (up to 10) that can be leased to the devices by the PPTP VPN server.
- 4. Set the PPTP connection permission according to your needs.
 - Select Allow Samba (Network Place) access to allow your VPN device to access your local Samba server.
 - Select Allow NetBIOS passthrough to allow your VPN device to access your Samba server using NetBIOS name.
 - Select Allow Unencrypted connections to allow unencrypted connections to your VPN server.

5. Click SAVE.

6. Configure the PPTP VPN connection account for the remote device. You can create up to 16 accounts.

Account List		
Similgure accounts (up to 55)	that can be used by remote clemb to correct	t to the VPN serves.
		O And
Usemame	Password	Modify
admin	admin	C 0

- 1) Click Add.
- 2) Enter the Username and Password to authenticate devices to the PPTP VPN Server.

Add Account			×
	Username: Password:		
		CANCEL	ADD

3) Click ADD.

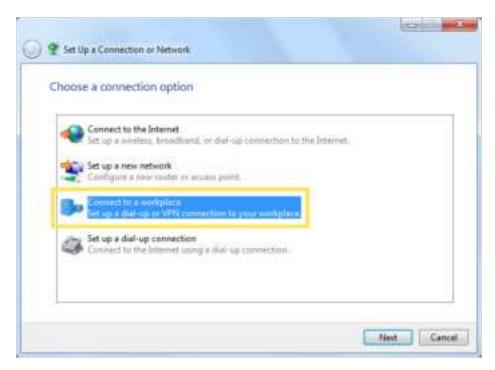
Step 2. Configure PPTP VPN Connection on Your Remote Device

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.

S Hetwork and During Ce	The second	
Tor quick young, place your books	ranks here on the busikmanity but	
Construction	Network and Determined. In Retrock and Sharing Contex	• [• =] [• = • 0 - = •
Control Panel Hanes	View your basic network information and	set up connections
Charge adapter offinge Outrip advanced sharing officies	ysäär-PC (This sempater) View ysud active retheraits	San had may
	Charge page (set-setting)	Accessifyer: Drivert Connections Q Local Anna Committee
	Set up a new interestant or reduced left up a version, biological, dair og, of her, Set up a version, biological, dair og, of her,	or VMI convertings or off-up a reader of access parent.
	Connect or reconnect to a scredul, whell do Connect or reconnection of the scredule of the scr	
Security Hereal-Stage Internet Options Hindowy Fremal	Traditionity of problems Diagnosis and input network problems, or ga	t houbleducting information.

3. Select Connect to a workplace and click Next.



4. Select Use my Internet connection (VPN).

How do you wa	ant to connect?				
	ternet connection g a virtual private oev		mection throug	the Internet	
-	63		-		
100					
 Dial direct Connect direct 	ty ctly to a pixone numbe	er without goin	g through the li	itemet.	
1		1			
What is a VPN cone	1374				

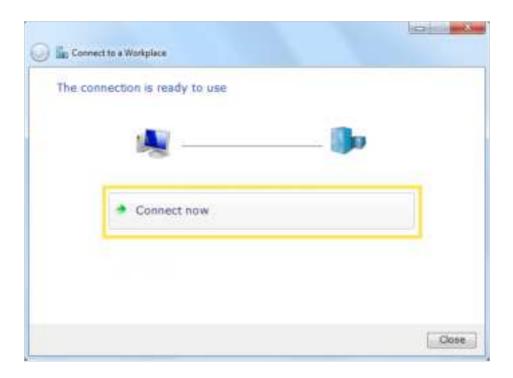
5. Enter the internet IP address of the router (for example: 218.18.1.73) in the Internet address field. Click Next.

Type the Internet a	address to connect to
Your network administr	ator can give you this address.
Internet address	218181.73
Destination names	VPN Connection
🗇 Use a smart care	
	ple to use this connection ws anyone with access to this computer to use this connection.
🔲 Don't connect n	rovc just set it up to I can connect later

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

User name:	Table .	
Paspwordt		
	Show characters	
Domain (optionali:	Remember this password	

7. Click Connect Now when the VPN connection is ready to use.



Use L2TP/IPSec VPN to Access Your Home 14.3. **Network**

L2TP/IPSec VPN Server is used to create a L2TP/IPSec VPN connection for remote devices to access your home network.

To use the VPN feature, you need to set up L2TP/IPSec VPN Server on your router, and configure the L2TP/IPSec connection on remote devices. Please follow the steps below to set up the L2TP/IPSec VPN connection.



Remote Devices

Step 1. Set up L2TP/IPSec 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 > L2TP/IPSec, and enable L2TP/IPSec.

Note:

- Firmware update may be required to support L2TP/IPSec VPN Server.
- · 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.

2TP/IPSec		
fer up a Litt Himfler, VPN and accounts	for quick, remate a	access to your network.
L2TP#PSec	Enable	
Client IP Address	10.9.0.11	- 10 3.0 20
		(Opino 101 cilients)
IPSec Encryption	Encrypted	¥.
IPSec Pre-Shared Key		

- 3. In the Client IP Address field, enter the range of IP addresses (up to 10) that can be leased to the devices by the L2TP/IPSec VPN server.
- 4. Keep IPSec Encryption as Encrypted and create an IPSec Pre-Shared Key.
- 5. Click SAVE.
- 6. Configure the L2TP/IPSec VPN connection account for the remote device. You can create up to 16 accounts.

count List		
infigure accounts (up to 18)	that can be used by remote clemb to connec	t to the VPN serves.
		O Ad
Usemane	Password	Modify
admin	admin	C 🗇

- 4) Click Add.
- 5) Enter the Username and Password to authenticate devices to the L2TP/IPSec VPN Server.

×
ADD
A00

6) Click ADD.

Step 2. Configure L2TP/IPSec VPN Connection on Your Remote Device

The remote device can use the Windows or Mac OS built-in L2TP/IPSec software or a third-party L2TP/IPSec software to connect to L2TP/IPSec Server. Here we use the Windows built-in L2TP/IPSec 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.

hoose	e a connection option
•	Connect to the Internet Set up a wireless, fireoditamic or dial-up connection to the Internat.
Ľ	Set up a new network Carifigure a new router er access peint.
50	Connect III a workplace Set up a dial-up or VER connection to your workplace.
3	Set up a dial-up connection Connect to the Internet using a dial-up connection.
~	Conversion and automationship a search conversion

4. Select Use my Internet connection (VPN).

How do you wan	t to connect?			
	met connection (Vi a virtual private oetwork (igh the Internet.	
A -	- 🔘]_o		
 Dial directly Connect directly 	y to a phone number with	wut going through th	Internet.	
A	🌗			
What is a VPN connect	tion?			

5. Enter the internet IP address of the router (for example: 218.18.1.73) in the Internet address field, and select the checkbox Don't connect now; just set it up so I can connect later. Click Next.

Type the Internet a	ddress to connect to
Your network administr	ator can give you this address.
Internet address	218.38.1.73
Destination name	YPN Connection
🗇 Use a smart card	
	ple to use this connection as anyone with access to this computer to use this connection.
International section of the	over just set it up to I can connect later

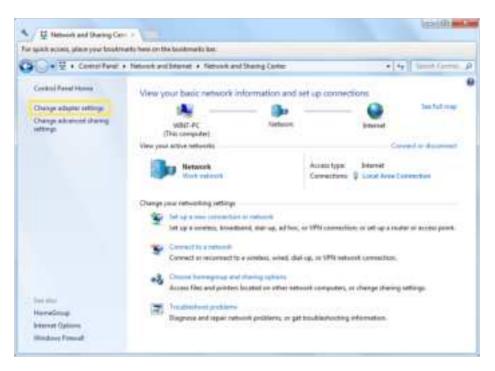
6. Enter the User name and Password you have set for the L2TP/IPSec VPN server on your router, and click Connect.

🔓 Connect to a Workpi	ice	
Type your user nar	ne and password	
User name:	MARK.	
Pasowordt	••••	
	Show characters	
100 AVT 600 (1990)	Remember this password	
Domain (optional):		
		Connect Cancel

7. Click Close when the VPN connection is ready to use

🕞 🌆 Coon	ect to a Workplace		
The co	nnection is ready to use		
	N	@ p	
	Connect now		
			Close

8. Go to Network and Sharing Center and click Change adapter settings.



9. Find the VPN connection you created, then double-click it.

 Starch Kenvart Cantechara
- F • 11
1

10. Enter the User name and Password you have set for the L2TP/IPSec VPN server on your router, and click Properties.

Se Cancerd SPM Convertion
Uier come de la come de
loga.
12 See the our range and passes of the file following same B Margo Grow and case the impact
Cored Carol Agents (16

11. Switch to the Security tab, select Layer 2 Tunneling Protocol with IPsec (L2TP/ IPSec) and click Advanced settings.

2 UPN Connection Properties	10.0
Gerand Collars Security Makazola	a Diana
Trave of VPM	
Saver & Turretting Planault with Plana	AJ10/02Sect ····
Date exception	Advanced settings
People incognized (discovered if party	e desilitati 🔹 🔹
Advertication C: Une Disordele Rubertication Pro- # Rev Press gratuce	
Culture region (parameter (PAP) Culture of Culture (Culture) Manual (ChiP Venture) MS Culture (ChiP Venture) MS Culture (Culture) (Culture) (Culture) Culture (Culture) (Culture	over bright memory and
1	OI Dece

12. Select Use preshared key for authentication and enter the IPSec Pre-Shared Key you have set for the L2TP/IPSec VPN server on your router. Then click OK.

Advanced Properties	
 ton protocol les fa autorita ton: 	-
C in police to extende Spot to have exting a	e de la companya de l La companya de la comp
	Oi Gent

Done! Click Connect to start VPN connection.

* Correct WHI Correction
(Jan vares 10) Descent
Began
Set Speec that care range and parameteris for the following same. A tagge Sector and the company Sector and the company
Coned Canal Agents (198

14. 4. Use VPN Client to Access a Remote VPN Server

VPN Client is used to create VPN connections for devices in your home network to access a remote VPN server.

To use the VPN feature, simply configure a VPN connection and choose your desired devices on your router, then these devices can access the remote VPN server. Please follow the steps below:



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

2. Go to Advanced > VPN Client.

Note: Firmware update may be required to support VPN Client.

3. Enable VPN Client, then save the settings.

VPN Client					
Set opporties for	alemba thus sell view. It	0.764	t function		
	VPN Client		ENABLE		

- 4. Add VPN servers, and enable the one you need.
 - 1) In the Server List section, click Add.
 - 2) Specify a description for the VPN, and choose the VPN type.