

# **Configuration Guide**

### For VPN

TL-ER6120/TL-ER6020/TL-ER604W/TL-R600VPN

1910012268 REV1.0.0

January 2018

### CONTENTS

VPN	1
Overview	1
Supported Features	2
Configuration Guidelines	4
LAN-to-LAN VPN Configuration	6
Network Topology	6
IPsec LAN-to-LAN VPN Configuration	7
Configuring the IPsec Policy for the Responder	7
Configuring IPsec Policy for the Initiator	
(Optional) Implementing configuration for NAT Devices	
Verifying the Connectivity of the IPsec VPN Tunnel	
L2TP LAN-to-LAN VPN Configuration	
Configuring L2TP VPN Server	
Configuring L2TP VPN Client	
(Optional) Implementing Configuration for NAT Devices	
Verifying the Connectivity of the L2TP VPN Tunnel	
PPTP LAN-to-LAN VPN Configuration	
Configuring PPTP VPN Server	
Configuring PPTP VPN Client	
(Optional) Implementing Configuration for NAT Devices	
Verifying the Connectivity of the PPTP VPN Tunnel	
Client-to-LAN VPN Configuration	
Network Topology	
IPsec Client-to-LAN VPN Configuration	
Configuring IPsec VPN Server	
(Optional) Implementing Configuration for NAT Devices	
Configuring the IPsec VPN Client Software	
Verifying the Connectivity of the IPsec VPN Tunnel	
L2TP Client-to-LAN VPN Configuration	
Configuring L2TP VPN Server	
(Optional) Implementing Configuration for NAT Devices	
Configuring the L2TP VPN Client Software	
Verifying the Connectivity of the L2TP VPN Tunnel	
(Optional) Configuring Access to the Internet via Proxy Gateway.	
PPTP Client-to-LAN VPN Configuration	
Configuring PPTP VPN Server	

Optional) Implementing Configuration for NAT Devices	59
Configuring the PPTP VPN Client Software	60
Verifying the Connectivity of the PPTP VPN Tunnel	68
(Optional) Configuring Access to the Internet via Proxy Gateway	69

## 1 VPN

#### 1.1 Overview

VPN (Virtual Private Network) provides a means for secure communication between remote computers across a public WAN (Wide Area Network), such as the internet. Virtual indicates the VPN connection is based on the logical end-to-end connection instead of the physical end-to-end connection. Private indicates users can establish the VPN connection according to their requirements and only specific users are allowed to use the VPN connection.

The core of VPN is to realize tunnel communication, which fulfills the task of data encapsulation, data transmission and data decompression via the tunneling protocol. Common tunneling protocols are Layer 2 tunneling protocol and Layer 3 tunneling protocol.

Depending on your network topology, there are two basic application scenarios: LAN-to-LAN VPN and Client-to-LAN VPN.

LAN-to-LAN VPN

In this scenario, different private networks are connected together via the internet. For example, the private networks of the branch office and head office in a company are located at different places. LAN-to-LAN VPN can satisfy the demand that hosts in these private networks need to communicate with each other. The following figure shows the typical network topology in this scenario.



Figure 1-1 LAN-to-LAN VPN

Client-to-LAN VPN

In this scenario, the remote host is provided with secure access to the local hosts. For example, an employee on business can access the private network of his company

securely. Client-to-LAN VPN can satisfy this demand. The following figure shows the typical network topology in this scenario.



#### **1.2 Supported Features**

TP-Link SafeStream VPN Routers support Layer 2 tunneling protocol (PPTP, L2TP) and Layer 3 tunneling protocol (IPsec).



#### IPsec

IPsec (IP Security) can provide security services such as data confidentiality, data integrity and data origin authentication at the IP layer. IPsec uses IKEv1 (Internet Key Exchange version 1) to handle negotiation of protocols and algorithms based on the user-specified policy, and generate the encryption and authentication keys to be used by IPsec. IKEv1 negotiation includes two phases, that is IKEv1 Phase-1 and IKEv1 Phase-2. The basic concepts of IPsec are as follows:

Proposal

Proposal is the security suite configured manually to be applied in IPsec IKEv1 negotiation. Specifically speaking, it refers to hash algorithm, symmetric encryption algorithm, asymmetric encryption algorithm applied in IKEv1 Phase-1, and security protocol, hash algorithm, symmetric encryption algorithm applied in IKEv1 Phase-2.

Negotiation Mode

The negotiation mode configured for IKEv1 Phase-1 negotiation determines the role that the VPN router plays in the negotiation process. You can specify the negotiation mode as responder mode or initiator mode.

**Responder Mode**: In responder mode, the VPN router responds to the requests for IKEv1 negotiation and acts as the VPN server or the responder.

**Initiator Mode**: In initiator mode, the VPN router sends requests for IKEv1 negotiation and acts as the VPN client or the initiator.

Exchange Mode

The exchange mode determines the way VPN routers negotiate in IKEv1 Phase-1. You can specify the exchange mode as main mode or aggressive mode.

**Main Mode**: In main mode, the identification information for authentication is encrypted, thus enhancing security.

**Aggressive Mode**: In aggressive mode, less packets are exchanged, thus improving speed.

Authentication ID Type

The authentication ID type determines the type of authentication identifiers applied in IKEv1 Phase-1. It includes the local ID type and the remote ID type. The local ID indicates the authentication identifier sent to the other end, and the remote ID indicates that expected from the other end. You can specify the authentication ID type as IP address or name.

**IP Address**: The router uses the IP address for authentication.

Name: The router uses the FQDN (Fully Qualified Domain Name) for authentication.

Encapsulation Mode

The encapsulation mode determines how packets transfered in the VPN tunnel are encapsulated. You can select tunnel mode or transport mode as the encapsulation mode. For most users, it is recommended to use the tunnel mode.

PFS

PFS (Perfect Forward Secrecy) determines whether the key generated in IKEv1 Phase-2 is relevant with that in IKEv1 Phase-1. You can specify PFS as none, dh1, dh2, or dh5. None indicates that no PFS is configured, and the key generated in IKEv1 Phase-2 is relevant with that in IKEv1 Phase-1, whereas dh1, dh2, or dh5 means different key exchange groups, which make the key generated in IKEv1 Phase-2 irrelevant with that in IKEv1 Phase-1.

#### L2TP

L2TP (Layer 2 Tunneling Protocol) provides a way for a dial-up user to make a virtual PPP (Point-to-Point Protocol) connection to a VPN server. Because of the lack of confidentiality inherent in the L2TP protocol, it is often implemented along with IPsec. The basic concepts of L2TP are as follows:

IPsec Encryption

IPsec encryption determines whether the traffic of the tunnel is encrypted with IPsec. You can select encrypted or unencrypted as the IPsec encryption. If encrypted is selected,

a pre-shared key needs to be entered, and then the L2TP traffic will be encrypted with a default IPsec configuration. If unencrypted is selected, the VPN tunnel traffic will not be encrypted.

Authentication

L2TP uses an account name and password for authentication on the VPN server. Only legal clients can set up a tunnel with the server, thus enhancing network security.

#### PPTP

PPTP (Point-to-Point Tunneling Protocol) is a network protocol that enables the secure transfer of data from a remote client to a private enterprise server by creating a VPN across TCP/IP-based data networks. PPTP supports on-demand, multi-protocol, virtual private networking over public networks, such as the internet. The basic concepts of PPTP are as follows:

MPPE Encryption

MPPE (Microsoft Point-to-Point Encryption) scheme is a means of representing PPP packets in an encrypted form defined in RFC 3078. You can select encrypted or unencrypted as MPPE encryption. If encrypted is selected, the VPN tunnel traffic will be encrypted with RSA RC4 algorithm to ensure data confidentiality. If unencrypted is selected, the VPN tunnel traffic will not be encrypted.

Authenticaiton

PPTP uses an account name and password for authentication on the VPN server. Only legal clients can set up a tunnel with the server, thus enhancing network security.

#### **1.3 Configuration Guidelines**

VPN does not involve the creation of a new physical connection. Instead, it is an additional feature built on the basis of the current network connection. Hence, the first step when creating a VPN tunnel is to acquire basic information about the network, such as the network topology. The necessary information is as follows.

- The IP addresses of both ends of the VPN tunnel
- The network topology of both ends of the VPN tunnel

Generally, if both ends are private networks, establish a LAN-to-LAN VPN tunnel. If one end is a remote client and the other end is a private network, establish a Client-to-LAN VPN tunnel.

• Whether any NAT devices exist between the ends of the tunnel

NAT devices may affect the establishment of VPN tunnel, so specific configuration needs to be implemented in that case, and IP addresses of NAT devices are also necessary. Please contact your ISP for that information.

• Whether you wish the remote client access the internet via the VPN proxy gateway

To satisfy this demand, you can establish an L2TP/PPTP Client-to-LAN VPN tunnel with specific configuration.

## **2** LAN-to-LAN VPN Configuration

#### 2.1 Network Topology

LAN-to-LAN VPN is deployed when different private networks are connected together via the internet. For example, the branch office and head office of a company are located at different places, and need to communicate with each other privately over the internet. The following figure shows the typical network topology.



In actual network environments, NAT devices may exist in front of the VPN routers. The following figure shows the network topology in this scenario.



Figure 2-2 LAN-to-LAN VPN with NAT

LAN-to-LAN VPN can be established via three methods, including IPsec LAN-to-LAN VPN, PPTP LAN-to-LAN VPN, and L2TP LAN-to-LAN VPN. The topology shown in Figure 2-1 is used as an example, with TL-ER6120 used as the VPN router for demonstration purposes. Configuration instructions for the three methods are given below.

#### 2.2 IPsec LAN-to-LAN VPN Configuration

To configure the IPsec LAN-to-LAN VPN, follow these steps:

- 1) Configure the IPsec policy for the responder.
- 2) Configure the IPsec policy for the initiator.
- 3) (Optional) Implement configuration for NAT devices.
- 4) Verify the connectivity of the IPsec VPN tunnel.

#### 2.2.1 Configuring the IPsec Policy for the Responder

Select any one of the VPN routers as the responder. Here we select VPN Router B as the responder. Follow these steps to configure IPsec policy for the responder.

 Choose the menu VPN > IPSec > IPSec Policy and click Add to load the following page. Configure the basic parameters for the IPsec policy.

1	PSec Po	olicy List									
										0	Add 😑 Delete
		ID	Policy Name	e Mode	Remo	te Gatev	vay	Local Subnet	Remote Subnet	Status	Operation
	Policy Name: VPN			(1-3	2 characters)						
	Remote Gateway: 10.10.10.20		10.10.10.20	20 (IP Address/Domain			Address/Domain Nam	ne)			
	WAN: WAN1 👻										
	Local Subnet: 192		192.168.0.0	/	24						
	Remote Subnet:         192.168.10.0         /         24           Pre-shared Key:         123456         0		(1-1	28 characters)							
		Status:		Enable							
		Advance	ced Settings								
		OK	Cancel								

Figure 2-3 Configuring the IPsec policy

Policy Name	Specify the name of IPsec Policy. Here we enter <b>VPN</b> .
Mode	Specify the mode as LAN-to-LAN.
Remote Gateway	Specify the remote gateway as <b>10.10.10.20</b> . This should be the IP address of the other end of the VPN tunnel.
WAN	Specify WAN as <b>WAN1</b> . This should be the WAN port which the VPN tunnel is established on.
Local Subnet	Specify the local subnet as <b>192.168.0.0/24</b> . This should be the subnet
	address of the local network.
Remote Subnet	Specify the remote subnet as <b>192.168.10.0/24</b> . This should be the subnet address of the remote network.
Remote Subnet Pre-shared key	address of the local network.         Specify the remote subnet as <b>192.168.10.0/24</b> . This should be the subnet address of the remote network.         Specify the pre-shared key as you like. Here we enter <b>123456</b> .

### 2) Click **Advanced Settings** to load the following page. In the **Phase-1 Settings** section, configure the IKE phase-1 parameters for the IPsec policy.

Figure 2-4 Configuring the IKE phase-1 parameters

Phase-1 Settings				
Proposal:	md5-des-dh1 🔹			
Proposal:	•			
Proposal:	•			
Proposal:	•			
Exchange Mode:	● Main Mode 🛛 Aggressive Mode			
Negotiation Mode:	🔾 Initiator Mode 🛛 💿 Responder Mo	de		
Local ID Type:	🔾 IP Address 💿 NAME			
Local ID:	123	(1-28 non-blank characters)		
Remote ID Type:	○ IP Address 💿 NAME			
Remote ID:	321	(1-28 non-blank characters)		
SA Lifetime:	28800	seconds (60-604800)		
DPD:	🗌 Enable			
DPD Interval:	10	seconds (1-300)		
Proposal	Select the proposal from	m the drop-down list. H	lere we select <b>md5-des-dh1</b> .	
Exchange Mode	Specify the exchange r exchange mode as <b>Mai</b>	mode according to you <b>n Mode</b> .	ur needs. Here we specify the	
Negotiation Mode	Specify the negotiation mode as <b>Responder Mode</b> .			
Local ID Type/ Remote ID Type	Specify the local ID type local ID type and remote	e and remote ID type a e ID type as <b>NAME</b> .	s you like. Here we specify the	

Local ID/ Remote ID	Specify the local ID and remote ID as you like. Here we specify the local ID as <b>123</b> and remote ID as <b>321</b> .
SA Lifetime	Specify the SA lifetime as your like. Here we keep the default setting.
DPD	Enable or disable DPD (Dead Peer Detection) according to your needs. Here we disable DPD.

3) In the **Phase-2 Settings** section, configure the IKE phase-2 parameters for the IPsec policy. Click **OK**.

Phase-2 Settings			
Enconculation Mode	Tunnel Made     O     Transport Made		
Encapsulation Mode:			
Proposal:	esp-md5-des 🔻		
Proposal:	<b>*</b>		
Proposal:	<b>*</b>		
Proposal:	<b>v</b>		
PFS:	none 🔻		
SA Lifetime:	28800 seconds (120-604800)		
OK Cancel			
Encapsulation Mod	de Specify the encapsulation mode as <b>Tunnel Mode.</b>		
Proposal	Select the proposal from the drop-down list. Here we select <b>esp-md5-des</b> .		
PFS	Select the PFS from the drop-down list according to your needs. Here we select <b>none</b> .		
SA Lifetime	Specify the SA lifetime according to your needs. Here we keep the default setting.		

Figure 2-5 Configuring the IKE phase-2 parameters

#### 2.2.2 Configuring IPsec Policy for the Initiator

Select the other VPN Router as the Initiator of IPsec negotiation. Here we select VPN Router A as the Initiator. Follow these steps to configure IPsec Policy for the initiator.

 Choose the menu VPN > IPSec > IPSec Policy and click Add to load the following page. Configure the basic parameters for the IPsec policy.

IPSec Po	olicy List										
										•	Add 😑 Delete
	ID	Policy Name	Mode	Ren	note (	Gatewa	ау	Local Subnet	Remote Subnet	Status	Operation
					-	-					
1	Policy Name: VPN			(	(1-32	characters)					
	Mode:		LAN-to-LAN			•					
1	Remote Ga	ateway:	10.10.10.10			(	(IP Address/Domain Name)				
	WAN:		WAN1	-		•					
1	Local Subr	net:	192.168.10.0		/	24					
1	Remote Su	ibnet:	192.168.0.0		/	24					
1	Pre-share	d Key:	123456				(1-12)	3 characters)			
	Status:		✓ Enable								
	Advan	ced Settings									
[	ОК	Cancel									

Figure 2-6 Configuring the IPsec policy

Policy Name	Specify the name of IPsec policy. Here we enter <b>VPN</b> .
Mode	Specify the mode as LAN-to-LAN.
Remote Gateway	Specify the remote gateway as <b>10.10.10.10</b> . This should be the IP address of the other end of the VPN tunnel.
WAN	Specify WAN as <b>WAN1</b> . This should be the WAN port which the VPN tunnel is established on.
Local Subnet	Specify the local subnet as <b>192.168.10.0/24</b> . This should be the subnet address of the local network.
Remote Subnet	Specify the remote subnet as <b>192.168.0.0/24</b> . This should be the subnet address of the remote network.
Pre-shared key	Specify a pre-shared key as <b>123456</b> . This should be kept the same as that of the responder configuration.
Status	Enable the IPsec policy list entry.

2) Click **Advanced Settings** to load the following page. In the **Phase-1 Settings** section, configure the IKE phase-1 parameters for the IPsec policy.

Phase-1 Settings						
Proposal:	md5-des-dh1 🔹					
Proposal:	🔻					
Proposal:	•					
Proposal:	•					
Exchange Mode:	Main Mode O Aggressive Mod	e				
Negotiation Mode:	● Initiator Mode 🛛 C Responder M	ode				
Local ID Type:	○ IP Address					
Local ID:	321	(1-28 non-blank characters)				
Remote ID Type:	○ IP Address					
Remote ID:	123	(1-28 non-blank characters)				
SA Lifetime:	28800	seconds (60-604800)				
DPD:	🗆 Enable					
DPD Interval:	10	seconds (1-300)				
Proposal	Select <b>md5-des-dh1</b> as of the responder configu	Select <b>md5-des-dh1</b> as the proposal. This should be kept the same as that of the responder configuration.				
Exchange Mode	Specify the exchange m that of the responder co	Specify the exchange mode as <b>Main Mode</b> . This should be kept the same as that of the responder configuration.				
Negotiation Mode	Specify the negotiation i	mode as <b>Initiator Mode.</b>				
Local ID Type/ Remote ID Type	Specify the local ID typ and remote ID type sh configuration.	Specify the local ID type and remote ID type as <b>NAME</b> . The local ID type and remote ID type should be kept the same as that of the responder configuration.				
Local ID/ Remote ID	Specify the Local ID as <b>321</b> and Remote ID as <b>123.</b> The local ID and remote ID should be reversed in comparison to the responder.					
SA Lifetime	Specify the SA lifetime as your like. Here we keep the default setting.					
DPD	Enable or disable DPD (Dead Peer Detection) according to your needs. Here we disable DPD.					

Figure 2-7 Configuring the IKE phase-1 parameters

3) In the **Phase-2 Settings** section, configure the IKE phase-2 parameters for the IPsec policy. Click **OK**.

Figure 2-8 Configuring the IKE phase-2 parameters

Phase-2 Settings			
Encapsulation Mode:	Tunnel Mode O Transport Mode		
Proposal:	esp-md5-des 🔻		
Proposal:	<b>*</b>		
Proposal:	<b>·</b>		
Proposal:	<b>*</b>		
PFS:	none 💌		
SA Lifetime:	28800 seconds (120-604800)		
OK Cancel			
Encapsulation Mod	de Specify the encapsulation mode as <b>Tunnel Mode.</b>		
Proposal	Select <b>esp-md5-des</b> as the proposal. This should be kept the same as that of the responder configuration.		
PFS	Select <b>none</b> as the PFS. This should be kept the same as that of the responder configuration.		
SA Lifetime	Specify the SA Lifetime according to your needs. Here we keep the default setting.		

#### 2.2.3 (Optional) Implementing configuration for NAT Devices

If there are NAT devices on the network, the suitable network topology is shown in Figure 2-2. In this scenario, please verify the configuration on both VPN routers, configure virtual servers on NAT Device B, and configure IPsec ALG on both NAT devices. The configuration steps are as follows:

For both VPN routers, choose the menu VPN > IPSec > IPSec Policy, select the IPsec policy list entry which is previously created, and click it to load the following page. Please make sure that in the Phase-1 Settings section, the local ID type and remote ID type are both specified as NAME, and in the Phase-2 Settings section, the proposal is not specified as ah-md5 or ah-sha1. Otherwise, the VPN tunnel may fail to be established.

Phase-1 Settings		
Proposal:	md5-des-dh1 🔹	
Proposal:	•	
Proposal:	•	
Proposal:	•	
Exchange Mode:	Main Mode O Aggressive Mode	2
Negotiation Mode:	Initiator Mode O Responder M	lode
Local ID Type:	○ IP Address	
Local ID:	321	(1-28 non-blank characters)
Remote ID Type:	O IP Address   NAME	
Remote ID:	123	(1-28 non-blank characters)
SA Lifetime:	28800	seconds (60-604800)
DPD:	Enable	
DPD Interval:	10	seconds (1-300)

Figure 2-9 Verifying the phase-1 configuration

Figure 2-10 Verifying the phase-2 configuration

Phase-2 Settings		
Encapsulation Mode:	• Tunnel Mode	) Transport Mode
Proposal:	esp-md5-des	•
Proposal:		•
Proposal:		•
Proposal:		•
PFS:	none	•
SA Lifetime:	28800	
OK Cancel		

 For NAT Device B, choose the menu Transmission > NAT > Virtual Servers and click Add to load the following page. Configure the parameters for the virtual server. Click OK.

Figure 2-11	Configuring virtual	server for IPsec
-------------	---------------------	------------------

	ID	Name Ir		Interface	External Port	Internal Port	Internal Server IP	Protocol	Status	Operation
-										
Name:		IPseo	:1							
	Int	erface:	WAN1 🔻							
	Ext	ernal Port:	500			(XX or XX-X	(,1-65535)			
	Int	ernal Port:	500			(XX or XX-X	(,1-65535)			
	Inte	ernal Server IP:	172.	16.10.2		•				
	Pro	tocol:	UDP		•					
Statuci		tus:	<ul> <li>Enal</li> </ul>	ble						

Name	Specify a name for the virtual server list entry. Here we enter <b>IPsec1</b> .
Interface	Specify WAN as <b>WAN1</b> . This should be the WAN port which the VPN tunnel is established on.
External Port/ Internal Port	Specify the external port and the internal port as <b>500</b> .
Internal Server IP	Specify the internal server IP as <b>172.16.10.2.</b> This should be the WAN IP address of the responder.
Protocol	Specify the protocol as <b>UDP</b> .
Status	Enable the virtual server list entry.

Similarly, add another virtual server list entry, with the name IPsec2, and set the external and internal port as 4500.

Figure 2-12 Configuring virtual server for IPsec

	Serv	er List									
									🔁 Ac	id 😑 Dele	
	ID	Name		Interface	External Port	Internal Port	Internal Server IP	Protocol	Status	Operation	
Name:		IPsec	:2								
	Inte	erface:	WAN	1	•						
	Exte	ernal Port:	4500 4500			(XX or XX-XX ,1-65535)					
	Inte	ernal Port:				(XX or XX-XX	,1-65535)				
	Inte	ernal Server IP:	172.16.10.2								
Protocol:		UDP		•	r						
	Stat	tus:	🕑 Enat	ble							

3) For NAT Device A and NAT Device B, choose the menu **Transmission** > **NAT** > **ALG** to load the following page. Enable the IPsec ALG, and click **Save**.

Figure 2-13 Configuring IPsec ALG

ALG	
✓ FTP ALG	
✓ H.323 ALG	
♥ PPTP ALG	
✓ SIP ALG	
✓ IPSec ALG	
Save	

#### 2.2.4 Verifying the Connectivity of the IPsec VPN Tunnel

Choose the menu **VPN** > **IPSec** > **IPSec SA** to load the following page.

Figure 2-14	IPSec SA list
i iguic z i <del>-</del>	11 OCC OA 1131

IPSec SA List										
Entry Count: 2							🕖 Refresh			
	ID	Name	SPI	Directio n	Tunnel ID	Data Flow	Protocol	AH Authenticatio n	ESP Authenticatio n	ESP Encryption
	1	VPN	33402697 75	in	10.10.10.10<- -10.10.10.20	192.168.0.0/24 <- - 192.168.10.0/24	ESP		MD5	DES
	2	VPN	26819373 80	out	10.10.10.10 >10.10.10.20	192.168.0.0/24 > 192.168.10.0/24	ESP		MD5	DES

The IPsec SA list shows the information about the established IPsec VPN tunnel. Here, you can verify the connectivity of the IPsec VPN tunnel.

#### 2.3 L2TP LAN-to-LAN VPN Configuration

To complete the L2TP LAN-to-LAN VPN, follow these steps:

- 1) Configure L2TP VPN server.
- 2) Configure L2TP VPN client.
- 3) (Optional) Implement configuration for NAT devices.
- 4) Verify the connectivity of the L2TP VPN tunnel.

#### 2.3.1 Configuring L2TP VPN Server

Select any one of the VPN routers as the VPN server. Here we select VPN Router B as the VPN server. Follow these steps to configure the L2TP VPN server.

1) Choose the menu **Preferences** > **VPN IP Pool** > **VPN IP Pool** and click **Add** to load the following page. Configure the parameters for the VPN IP pool. Click **OK**.

Figure 2-15 Configuring VPN IP Pool list

VPN IP Po	ool List					
						🕂 Add 🛛 😑 Delete
	ID	IP Pool Name		Starting IP Address	Ending IP Address	Operation
IF S E	P Pool Nar tarting IP nding IP 4 OK	ne: Address: Address: Cancel	pool1 172.16.10.100 172.16.10.200			
IP Poo	ol Nam	е	Specify t	he IP pool name as you:	like. Here we enter <b>poo</b>	l1.

Starting IP Address/	Specify the starting IP address and ending IP address for the VPN IP
Ending IP Address	pool. The VPN server will assign an IP address to the remote client when
	the tunnel is established. You can specify any reasonable IP address
	that will not cause conflict. Here we specify the starting IP address as
	172.16.10.100 and the ending IP address as 172.16.10.200.

2) Choose the menu **VPN** > **Users** > **Users** and click **Add** to load the following page. Configure the parameters for the user account. Click **OK**.

						G	Add 🤤 D
ID	Account Name	Protocol	Local IP Address	IP Address Pool	Network Mode	Remote Subnet	Operat
Account	Name:	tplink					
Passwor	d:	•••••					
		Low	Middle High				
Protocol	:	L2TP	•				
Protocol: Local IP	: Address:	L2TP 172.31.1	<b>▼</b> 1.16				
Protocol: Local IP IP Addre	: Address: ess Pool:	L2TP 172.31.1 pool1	▼ 1.16 ▼				
Protocol: Local IP IP Addre DNS Add	: Address: Iss Pool: Iress:	L2TP 172.31.1 pool1 8.8.8.8	<ul><li>▼</li><li>1.16</li><li>▼</li></ul>				
Protocol: Local IP IP Addre DNS Add Network	: Address: Iss Pool: Iress: Mode:	L2TP 172.31.1 pool1 8.8.8.8 LAN-to-L	• 1.16 • AN •				

Figure 2-16 Configuring L2TP users

Account Name	Specify the account name as you like. Here we enter <b>tplink</b> .
Password	Specify the password as you like. Here we enter <b>123456</b> .
Protocol	Specify the protocol as L2TP.
Local IP Address	This is the virtual IP address which the remote client will set up a point-to-point connection with. You can specify any reasonable IP address that will not cause conflict. Here we specify the Local IP address as <b>172.31.1.16</b> .
IP Address Pool	Select <b>pool1</b> as the IP address pool from the drop-down list. This is the VPN IP pool we have just configured.
DNS Address	Specify the DNS address according to your network environment. This is the DNS address to be assigned to the remote client. Here we enter <b>8.8.8.8</b> .
Network Mode	Specify the network mode as LAN-to-LAN.
Remote Subnet	Specify the remote subnet as <b>192.168.10.0/24</b> . This should be the subnet address of the remote network.

3) Choose the menu **VPN** > **L2TP** > **L2TP Server** and click **Add** to load the following page. Configure the parameters for the L2TP server. Click **OK**.

Figure 2-17	Configuring L2TP server
inguio z in	oorniguning Ez moorvor

L2TP Server Settings							
					🕂 Add 🛛 😑 Delete		
	ID	WAN	IPSec Encryption	Status	Operation		
WAN: IPSec Encryption: Status: OK Cancel		WAN1  Unencrypted  Enable					
WAN		Specify WAN as <b>WAN1</b> . This should be the WAN port which the VPN tunnel is established on.					
IPsec Enc	Encryption Specify the IPsec encryption according to your needs. Here we specify the IPsec encryption as <b>Unencrypted</b> .						
Status		Enable the L2TP server.					

#### 2.3.2 Configuring L2TP VPN Client

Here we select the VPN Router A as the L2TP VPN client. For VPN Router A, choose the menu **VPN** > **L2TP** > **L2TP Client** and click **Add** to load the following page. Configure the parameters for the L2TP client. Click **OK**.

2ТР С	Client Se	ttings								
C	ID	Tunnel	Account Name	WAN	Server IP	IPSec	Remote Subnet	Working	• Ado Status	d Operatio
	Tunnel: Accoun Passwo WAN: Server IPSec E	: t Name: rd: IP: Encryption:	I2tp tplink •••••• WAN1 10.10.10.1 Unencrypt	ddle 10 ed	(1-12 char	acters)				
Remote Subnet: Upstream Bandwidth: Downstream Bandwidth:		192.168.0.0 / 24 1000000 1000000		24 Kbps(100- Kbps(100-	1000000) 1000000)					
	Workin Status:	g Mode:	<ul> <li>NAT ○</li> <li>✓ Enable</li> </ul>	Route		,				
[	Downst Workin Status: OK	tream Bandwidth g Mode: Cancel	: 1000000 ● NAT ○ ✓ Enable	Route	Kbps(100-	100000)				

Figure 2-18 Configuring L2TP client

Tunnel	Specify the tunnel name as you like. Here we enter <b>I2tp</b> .
Account Name	Specify the account name as <b>tplink.</b> This should be kept the same as that of the L2TP server configuration.
Password	Specify the password as <b>123456.</b> This should be kept the same as that of the L2TP server configuration.
WAN	Specify WAN as <b>WAN1</b> . This should be the WAN port which the VPN tunnel is established on.
Server IP	Specify the server IP as <b>10.10.10.10</b> .
Server IP IPSec Encryption	Specify the server IP as <b>10.10.10.10</b> . Specify IPSec encryption as <b>Unencrypted</b> . This should be kept the same as that of the L2TP server configuration.
Server IP IPSec Encryption Remote Subnet	Specify the server IP as 10.10.10.10.Specify IPSec encryption as Unencrypted. This should be kept the same as that of the L2TP server configuration.Specify the remote subnet as 192.168.0.0/24. This should be the subnet address of the remote network.

Working Mode	Specify the working mode as <b>NAT</b> or <b>Route</b> according to your needs. Here we specify the working mode as <b>NAT</b> .
	<b>NAT</b> : NAT mode allows the router to translate source IP address of L2TP packets to its WAN IP when forwarding L2TP packets.
	<b>Route</b> : Route mode allows the router to forward L2TP packets via routing protocol.
Status	Enable the L2TP client.

#### 2.3.3 (Optional) Implementing Configuration for NAT Devices

If there are NAT devices on the network, the suitable network topology is shown in Figure 2-2. In this scenario, please verify the configuration on both VPN routers, and configure virtual servers on NAT Device B. The configuration steps are as follows:

 For VPN Router A, choose the menu VPN > L2TP > L2TP Client, select the L2TP client list entry which is previously created, and click it to load the following page. Please make sure that the IPsec encryption is specified as Unencrypted. Otherwise, the VPN tunnel may fail to be established.

ID     Tunnel     Account Name       Tunnel:     I2tp       Account Name:     tplink       Password:     Iune       WAN:     WAN1	L2TP Client Settings								
ID     Tunnel     Account Name       Tunnel:     I2tp       Account Name:     tplink       Password:     Image:	🔂 Add 🛛 🤤 Delete								
Tunnel: I2tp Account Name: tplink Password: •••••• WAN: WAN1	e WAN	Server IP	IPSec Encryption	Remote Subnet	Working Mode	Status	Operation		
Tunnel:I2tpAccount Name:tplinkPassword:••••••LowWAN:									
Server IP: 10.10.10 IPSec Encryption: Unencry Remote Subnet: 192.168 Upstream Bandwidth: 1000000 Downstream Bandwidth: 1000000 Working Mode: NAT Status: Status: Enable	Middle Hig 0.10 0.00 / : 0.00 / :	(1-12 chai ) 4 Kbps(100- Kbps(100-	racters) -1000000) -1000000)						

Figure 2-19 Verifying the L2TP client configuration

2) For VPN Router B, choose the menu VPN > L2TP > L2TP Server, select the L2TP server list entry which is previously created, and click it to load the following page. Please make sure that the IPsec encryption is specified as Unencrypted. Otherwise, the VPN tunnel may fail to be established.

Figure 2-20	Verifying the L2TP server configuration	
-------------	---	--

L	2TP Server Se	ettings				
						🔂 Add 🛛 😑 Delete
		ID	WAN	IPSec Encryption	Status	Operation
	14/A NI.					
	WAN: IPSec Encryption:		WANI			
			Unencrypted 🔹			
	Status:		Enable			
	OK	Cancel				

 For NAT Device B, choose the menu Transmission > NAT > Virtual Servers and click Add to load the following page. Configure the parameters for the virtual server. Click OK.

Figure 2-21 Configuring virtual server for L2TP

Virtua	I Serv	ver List								
									<b>O</b> A	dd 😑 Delete
	ID	Name		Interface	External Port	Internal Port	Internal Server IP	Protocol	Status	Operation
Name: Interface: External Port: Internal Port: Internal Server IP: Protocol: Status: OK Cancel			L2TP WAN 1701 1701 172.1 UDP @ Enat	1 6.10.2 ole	•	(XX or XX-X (XX or XX-X	X ,1-65535) X ,1-65535)			
Nar	ne		Spec	ify the r	ame for	the virtu	al server list entry. H	ere we e	nter <b>L2TP</b>	
Inte	erfa	ce	Spec is est	ify WAN ablishe	l as <b>WA</b> d on.	N1. This	should be the WAN	port whi	ch the VP	N tunnel
Ext Inte	erna erna	al Port/ I Port	Specify the external port and internal port as <b>1701</b> .							
Inte	erna	l Server IP	Specify the internal server IP as <b>172.16.10.2.</b> This should be the WAN IF address of the VPN server.					WAN IP		

Protocol	Specify the protocol as <b>UDP</b> .
Status	Enable the virtual server list entry.

#### 2.3.4 Verifying the Connectivity of the L2TP VPN Tunnel

Choose the menu VPN > L2TP > Tunnel List to load the following page.

Figure 2-22 L2TP tunnel list

Tunnel List							
							🙆 Refresh
ID	Account Name	Mode	Tunnel	Local IP	Remote IP	Remote Local IP	DNS
1	tplink	Server	l2tp	172.31.1.16	10.10.10.20	172.16.10.100	

The tunnel list shows the information about the established VPN tunnel. Here, you can verify the connectivity of the L2TP VPN tunnel.

#### 2.4 **PPTP LAN-to-LAN VPN Configuration**

To configure the PPTP LAN-to-LAN VPN, follow these steps:

- 1) Configure PPTP VPN server.
- 2) Configure PPTP VPN client.
- 3) (Optional) Implement configuration for NAT devices.
- 4) Verify the connectivity of the PPTP VPN tunnel.

#### 2.4.1 Configuring PPTP VPN Server

1) Choose the menu Preferences > VPN IP Pool > VPN IP Pool and click Add to load the following page. Configure the parameters for the VPN IP pool. Click OK.

Figure 2-23	Configuring VPN IP pool list	

VPN IP Pool List				
				🕂 Add 🛛 🖨 Delete
	P Pool Name	Starting IP Address	Ending IP Address	Operation
IP Pool Name: Starting IP Address: Ending IP Address:	pool1 172.16.10.100 172.16.10.200			

IP Pool Name	Specify the IP pool name as you like. Here we enter <b>pool1.</b>
Starting IP Address/ Ending IP Address	Specify the starting IP address and ending IP address for the VPN IP pool. The VPN server will assign an IP address to the remote client when the tunnel is established. You can specify any reasonable IP address that will not cause conflict. Here we specify the starting IP address as <b>172.16.10.100</b> and the ending IP address as <b>172.16.10.200</b> .

2) Choose the menu **VPN** > **Users** > **Users** and click **Add** to load the following page. Configure the parameters for the PPTP user account. Click **OK**.

User Account List								
							O	Add 😑 Delete
	ID	Account Name	Protocol	Local IP Address	IP Address Pool	Network Mode	Remote Subnet	Operation
				ar 10				
	Account Passwor	Name: rd:	tplink •••••	Middle High				
	Protocol	:	PPTP	•				
	Local IP	Address:	172.31.1	.16				
	IP Addre	ss Pool:	pool1	-				
DNS Address:			8.8.8.8					
Network Mode: LAN-to-LAN 🔻			AN 🔻					
	Remote	Subnet:	192.168	.10.0 / 24				
[	ОК	Cancel						

Figure 2-24 Configuring PPTP users

Account Name	Specify the account name as you like. Here we enter <b>tplink</b> .
Password	Specify the password as you like. Here we enter <b>123456</b> .
Protocol	Specify the protocol as <b>PPTP.</b>
Local IP Address	This is the virtual IP address the remote client will set up a point-to-point connection with. You can specify any reasonable IP Address that will not cause conflict. Here we specify the local IP address as <b>172.31.1.16</b> .
IP Address Pool	Select <b>pool1</b> as the IP address pool from the drop-down list. This is the VPN IP pool we have just configured.
DNS Address	Specify the DNS address according to your network environment. This is the DNS address to be assigned to the remote client. Here we enter <b>8.8.8.8</b> .
Network Mode	Specify the network mode as LAN-to-LAN.
Remote Subnet	Specify the remote subnet as <b>192.168.10.0/24</b> . This should be the subnet address of the remote network.

3) Choose the menu **VPN** > **PPTP** > **PPTP Server** and click **Add** to load the following page. Configure the parameters for the PPTP server. Click **OK**.

Server List							
					🕂 Add 🛛 😑 Delete		
	ID	WAN	MPPE Encryption	Status	Operation		
WAN: MPPE Status	Encryption: s: Cancel	WAN1  Unencrypted  Enable					
WAN	WAN Specify WAN as <b>WAN1</b> . This should be the WAN port which the VPN tuni is established on.						
MPPE End	cryption	Specify the MPPE encryption according to your needs. Here we specify the MPPE encryption as <b>Unencrypted</b> .					
Status		Enable the PPTP server.					

#### 2.4.2 Configuring PPTP VPN Client

Here we select the VPN Router A as PPTP VPN client. For VPN Router A, choose the menu **VPN >PPTP > PPTP Client** and click **Add** to load the following page. Configure the parameters for PPTP client. Click **OK**.

(	Client	List									
		ID	Tunnel	Account Name	Server IP	WAN	MPPE Encryption	Remote Subnet	Working Mode	🔂 Ad Status	d Operation
		Tunnel: Accoun Passwo WAN: Server	: t Name: ord: IP:	PPTP tplink •••••• Low N WAN1 10.10.10.1	tiddle High	(1-12 char	acters)				
	MPPE Encryption: Remote Subnet: Upstream Bandwidth: Downstream Bandwidth:			Unencrypt 192.168.0 1000000 : 1000000	ed 🗸	Kbps (100 Kbps (100	-1000000) -1000000)				
	Working Mode: <ul> <li>NAT O Route</li> <li>Status:</li> <li>Enable</li> </ul> OK Cancel										

Figure 2-26 Configuring PPTP client

Tunnel	Specify the tunnel name as you like. Here we enter <b>PPTP</b> .
Account Name	Specify the account name as <b>tplink.</b> This should be kept the same as that of the PPTP server configuration.
Password	Specify the password as <b>123456.</b> This should be kept the same as that of the PPTP server configuration.
WAN	Specify WAN as <b>WAN1</b> . This should be the WAN port which the VPN tunnel is established on.
Server IP	Specify the server IP as <b>10.10.10.10</b> .
Server IP MPPE Encryption	Specify the server IP as <b>10.10.10.10</b> . Specify MPPE encryption as <b>Unencrypted</b> . This should be kept the same as that of the PPTP server configuration.
Server IP MPPE Encryption Remote Subnet	Specify the server IP as 10.10.10.10.Specify MPPE encryption as Unencrypted. This should be kept the same as that of the PPTP server configuration.Specify the remote subnet as 192.168.0.0/24. This should be the subnet address of the remote network.

Working Mode	Specify the working mode as NAT or Route according to your needs. Here we specify the working mode as <b>NAT</b> .
	<b>NAT</b> : NAT mode allows the router to translate source IP address of PPTP packets to its WAN IP when forwarding PPTP packets.
	<b>Route</b> : Route mode allows the router to forward PPTP packets via routing protocol.
Status	Enable the PPTP client.

#### 2.4.3 (Optional) Implementing Configuration for NAT Devices

If there are NAT devices on the network, the suitable network topology is shown in Figure 2-2. In this scenario, please configure virtual servers on NAT Device B, and configure PPTP ALG on both NAT devices. The configuration steps are as follows:

1) For NAT Device B, choose the menu **Transmission** > **NAT** > **Virtual Servers** and click **Add** to load the following page. Configure the parameters for virtual server. Click **OK**.

Virtua	l Serv	ver List								
									⊕ A¢	dd 😑 Delet
	ID	Name		Interface	External Port	Internal Port	Internal Server IP	Protocol	Status	Operation
	Name:					]				
	Interface:		WAN1 -							
	External Port:		1723			(XX or XX-X	( ,1-65535)			
	Internal Port: 172		1723			(XX or XX-X	(,1-65535)			
	Internal Server IP: 172.		16.10.2							
	Pro	tocol:	TCP		•					
	Sta	tus:	🕑 Enat	ole						
		OK Cancel								
Name Specify the name for the virtual se				ual server list entry. H	lere we e	enter <b>PPT</b>	P.			
Inte	rfac	e.	Specify WAN as <b>WAN1</b> . This should be the WAN port which the VPN tu is established on.				N tunnel			
Exte Inte	erna rnal	Il Port/ I Port	Specify the External Port and Internal Port as <b>1723</b> .							
Inte	rnal	Server IP	Specify the Internal Server IP as <b>172.16.10.2.</b> This should be the WAN IP address of the VPN server.							
D			Specify the protocol as <b>TCP</b> .							

Figure 2-27 Configuring virtual server for PPTP

Enable the virtual server list entry.

2) For NAT Device A and NAT Device B, choose the menu **Transmission** > **NAT** > **ALG** to load the following page. Enable the PPTP ALG, and click **Save**.

Figure 2-28	Configuring PPTP ALG
ALG	
E li bec Alo	
Save	

#### 2.4.4 Verifying the Connectivity of the PPTP VPN Tunnel

Choose the menu **VPN > PPTP > Tunnel List** to load the following page.

Figure 2-29 PPTP tunnel list

Tunnel List									
							🙆 Refresh		
ID	Account Name	Mode	Tunnel	Local IP	Remote IP	Remote Local IP	DNS		
1	tplink	Server	РРТР	172.31.1.16	10.10.10.20	172.16.10.100			

The tunnel list shows the information about the established VPN tunnel. Here, you can verify the connectivity of the PPTP VPN Tunnel.

## **3** Client-to-LAN VPN Configuration

#### 3.1 Network Topology

Client-to-LAN VPN is deployed when a remote host is provided with secure access to the local hosts. For example, an employee on business needs to access the private network of his company securely via the internet. The following figure shows the typical network topology.





In actual network environments, NAT devices may exist in front of the VPN router. The following figure shows the network topology in this scenario.

Figure 3-2 Client-to-LAN VPN with NAT



Client-to-LAN VPN can be established via three methods, including IPsec Client-to-LAN VPN, PPTP Client-to-LAN VPN, and L2TP Client-to-LAN VPN. To establish an IPsec

Client-to-LAN VPN, it is recommended to use a 3rd-party IPsec VPN client software, such as TheGreenBow VPN client software, whereas to establish a PPTP or L2TP Client-to-LAN VPN, you can use the built-in client software of the operating system. The topology shown in Figure 3-1 is used as an example, with TL-ER6120 used as the VPN router for demonstration purposes. Configuration instructions for the three methods are given below.

#### 3.2 IPsec Client-to-LAN VPN Configuration

To complete the IPsec Client-to-LAN VPN, follow these steps:

- 1) Configure IPsec VPN server.
- 2) (Optional) Implement configuration for NAT devices.
- 3) Configure the IPsec VPN client software.
- 4) Verify the connectivity of the IPsec VPN tunnel.

#### 3.2.1 Configuring IPsec VPN Server.

 Choose the menu VPN > IPSec >IPSec Policy and click Add to load the following page on the VPN router. Configure the basic parameters for the IPsec policy.

Figure 3-3 Configuring the IPsec policy

IPSec Policy Li	st							
							•	dd 😑 Delete
_ ID	Policy Name	Mode	Remote Gate	way	Local Subnet	Remote Subnet	Status	Operation
Policy M Mode: Remote WAN: Local S Pre-sha Status: © Adv	lame: Host: ubnet: red Key: ranced Settings	VPN2 Client-to-LAN 10.10.10.20 WAN1 192.168.0.0 123456 ✓ Enable	/ 24	(1-3 (IP 4	2 characters) Address/Domain N 28 characters)	lame)		

Policy Name	Specify the name of IPsec policy. Here we enter <b>VPN2</b> .
Mode	Specify the mode as <b>Client-to-LAN</b> .
Remote Host	Specify the remote host as <b>10.10.10.20</b> . This should be the IP address of the other end of the VPN tunnel.
WAN	Specify WAN as <b>WAN1</b> . This should be the WAN port which the VPN tunnel is established on.
Local Subnet	Specify the local subnet as <b>192.168.0.0/24</b> . This should be the subnet address of the local network.
Pre-shared key	Specify the pre-shared key as you like. Here we enter <b>123456</b> .
Status	Enable the IPsec policy list entry.

2) Click **Advanced Settings** to load the following page. In the **Phase-1 Settings** section, configure the IKE phase-1 parameters for the IPsec policy.

Phase-1 Settings						
Branasalı	md5 2dec db2					
Proposal.	mu5-sdes-dnz					
Proposal:	•					
Proposal:	•					
Proposal:	•					
Exchange Mode:	○ Main Mode  ● Aggressive Mo	de				
Negotiation Mode:	○ Initiator Mode 🛛 ● Responder	Mode				
Local ID Type:	○ IP Address					
Local ID:	123	(1-28 non-blank characters)				
Remote ID Type:	○ IP Address					
Remote ID:	321	(1-28 non-blank characters)				
SA Lifetime:	28800	seconds (60-604800)				
DPD:	🗆 Enable					
DPD Interval:	10	seconds (1-300)				

Figure 3-4 Configuring the IKE phase-1 parameters

Proposal	Select the proposal from the drop-down list. Here we select <b>md5-3des-dh2</b> .
Exchange Mode	Specify the exchange mode according to your needs. Here we Specify the exchange mode as <b>Aggressive Mode</b> .
Negotiation Mode	Specify the negotiation mode as <b>Responder Mode.</b>
Local ID Type/ Remote ID Type	Specify the local ID type and remote ID type as you like. Here we specify the local ID type and remote ID type as <b>NAME</b> .

Local ID/ Remote ID	Specify the local ID and remote ID as you like. Here we specify the local ID as <b>123</b> and remote ID as <b>321</b> .
SA Lifetime	Specify the SA lifetime as your like. Here we keep the default setting.
DPD	Enable or disable DPD (Dead Peer Detection) according to your needs. Here we disable DPD.

3) In the **Phase-2 Settings** section, configure the IKE phase-2 parameters for the IPsec policy. Click **OK**.

Phase-2 Settings								
Encapsulation Mode:   Tunnel Mode  Transport Mode								
Proposal:	esp-md5-3des	•						
Proposal:		•						
Proposal:		•						
Proposal:		•						
PFS:	none	•						
SA Lifetime:	28800		seconds (120-604800)					
OK Cancel								
Encapsulation Mode Specify the encapsulation mode as <b>Tunnel Mode</b> .								
Proposal	Select the <b>esp-md5-3</b> 6	e propo d <b>es</b> .	sal from the drop	o-down list. Here we select				

Figure 3-5 Configuring the IKE phase-2 parameters

PFS

SA Lifetime

Specify the SA lifetime as your like. Here we keep the default setting.

select none.

Select the PFS from the drop-down list according to your needs. Here we

#### 3.2.2 (Optional) Implementing Configuration for NAT Devices

If there are NAT devices on the network, the suitable network topology is shown in Figure 3-2. In this scenario, please verify the configuration on the VPN router, configure virtual servers on the NAT device, and configure IPsec ALG on both the remote gateway and the NAT device. The configuration steps are as follows:

For the VPN router, choose the menu VPN > IPSec > IPSec Policy, select the IPsec policy list entry which is previously created, and click it to load the following page. Please make sure that in the Phase-1 Settings section, the local ID type and remote ID type are both specified as NAME, and in the Phase-2 Settings section, the proposal is not specified as ah-md5 or ah-sha1. Otherwise, the VPN tunnel may fail to be established.

Phase-1 Settings		
Proposal:	md5-3des-dh2 🔹	
Proposal:	•	
Proposal:	•	
Proposal:	•	
Exchange Mode:	○ Main Mode ● Aggressive Mo	de
Negotiation Mode:	○ Initiator Mode 🔹 Responder	Mode
Local ID Type:	○ IP Address	
Local ID:	123	(1-28 non-blank characters)
Remote ID Type:	○ IP Address	
Remote ID:	321	(1-28 non-blank characters)
SA Lifetime:	28800	seconds (60-604800)
DPD:	Enable	
DPD Interval:	10	seconds (1-300)

Figure 3-6 Verifying the phase-1 configuration

Figure 3-7 Verifying the phase-2 configuration

Phase-2 Settings			
Encapsulation Mode:	◉ Tunnel Mode 🛛 1	ransport Mode	
Proposal:	esp-md5-3des	-	
Proposal:		•	
Proposal:		•	
Proposal:		•	
PFS:	none	•	
SA Lifetime:	28800	seconds (1	20-604800)
OK Cancel			

 For the NAT device, choose the menu Transmission > NAT > Virtual Servers and click Add to load the following page. Configure the parameters for the virtual server. Click OK.

Virtua	al Serv	ver List								
										d 🗖 Doloto
D ID Name				Interface	External Port	Internal Port	Internal Server IP	Protocol	Status	Operation
Name:			IPsec1							
	Int	erface:	WAN1 🔻							
	Ext	ernal Port:	500			(XX or XX-XX ,1-65535)				
Internal Port:			500			(XX or XX-X	X ,1-65535)			
	Internal Server IP:			172.16.10.2						
	Pro	tocol:	UDP	DP 🔻						
	Sta	tus:	🕑 Enal	ble						
		OK Cancel								
Nar	ne		Speci	fy the n	ame for	the virtua	al server list entry. Her	e we ent	er <b>IPsec1</b> .	
Inte	erfac	e	Specify WAN as <b>WAN1</b> . This should be the WAN port which the VPN tunnel is established on.							
External Port/ Internal Port			Specify the external port and internal port as <b>500</b> .							
Internal Server IP			Specify the internal server IP as <b>172.16.10.2.</b> This should be the WAN IP address of the VPN server.							
Protocol Specify the protocol a			as UDP.							
Status Enable the virtual serv			ver list er	ntry.						

Figure 3-8 Configuring virtual server for IPsec
Similarly, add another virtual server list entry with the name IPsec2, and set the external and internal port as 4500.

Figure 3-9 Configuring virtual server for IPsec

١	Virtual Server List										
										🔂 Ado	d 😑 Delete
	ID     Name			Interface	External Port	Internal Port	Internal Server IP	Protocol	Status	Operation	
	Name:		IPse	:2							
	Interface:		WAN1 🔻								
		Ext	ernal Port:	4500 4500		(XX or XX-XX ,1-65535)					
		Int	ernal Port:			(XX or XX-XX ,1-65535)					
		Int	ernal Server IP:	172.16.10.2							
	Protocol: Status:		UDP		•						
			✓ Enable								
		OK Cancel									

3) For the remote gateway and the NAT device, choose the menu **Transmission** > **NAT** > **ALG** to load the following page. Enable IPsec ALG, and click **Save**.

Figure 3-10 Configur	ring IPsec ALG
----------------------	----------------

ALG	
✓ FTP ALG	
✓ H.323 ALG	
✓ PPTP ALG	
✓ SIP ALG	
✓ IPSec ALG	
Save	

### 3.2.3 Configuring the IPsec VPN Client Software

There are many 3rd-party IPsec VPN client softwares. With any one of them launched on the remote host, you can set up an IPsec Client-to-LAN VPN tunnel with the VPN router successfully. Here we take TheGreenBow VPN client software for example. Follow these steps to configure TheGreenBow VPN client software.

- Go to the website http://www.tp-link.com/en/download/TL-ER6120\_V1.html to download TheGreenBow VPN client software. Then install and launch the client software.
- 2) Click the client icon in the toolbar on the bottom of your desktop to load the following page.



Figure 3-11 Configuring TheGreenBow IPSec VPN client

 Right click VPN Configuration, click New Phase 1 and then choose the menu Gateway > Authentication to load the following page. Configure the parameters for the IPsec policy.

uthentica	tion Advanced Certifi	cate							
Addr	esses								
Interface 192.168.10.2									
Remote Gateway 10.10.10.10									
Auth	entication ———								
	Preshared Key	•••••							
	Confirm	•••••							
	Certificate								
IKE									
	Encryption	3DES 👻							
Authentication MD5									
Key Group DH2 (1024) 🔻									
	Key Group	DH2 (1024) -							

Figure 3-12 Configuring TheGreenBow IPSec VPN client

Interface	Select <b>192.168.10.2</b> as the Interface from the drop-down list. This should be the IP address of the remote host.
Remote Gateway	Specify the remote gateway as <b>10.10.10.10</b> . This should be the IP address of the other end of the VPN tunnel.
Preshared Key	Specify the preshared key as <b>123456</b> . This should be the same as the VPN server configuration. Then confirm the preshared key by inputting it again in <b>Confirm</b> .
Encryption/ Authentication/ Key Group	Specify encryption as <b>3DES</b> , authentication as <b>MD5</b> , Key Group as <b>DH2 (1024)</b> . This should be kept the same as the VPN server configuration.

4) Choose the menu **Gateway > Advanced** to load the following page. Configure the parameters for the IPsec policy.

Advanced features				
Mode Config	Redun. GW			
Aggressive Mode	NAT-T Automatic			
X-Auth				
X-Auth Popup	Login			
🚺 🗌 Hybrid Mode	Password			
Local and Remote ID —				
Type of ID:	Value for the ID:			
Local ID DNS	▼ 321			
Remote ID DNS	▼ 123			
-				
Aggressive Mode	Check <b>aggressive mode</b> . This should be kept the same as the VPN server configuration.			
NAT-T	Select Automatic as NAT-T from the drop-down list.			
Local ID/ Remote ID	Specify type of local ID and remote ID as <b>DNS</b> . Specify the local ID as <b>321</b> and the remote ID as <b>123</b> . This should be reversed in comparison to the VPN server configuration.			

Figure 3-13 Configuring TheGreenBow IPSec VPN client

5) Right click **Gateway** and click **New Phase 2**. Choose the menu **Tunnel > IPSec** to load the following page. Configure the parameters for the IPsec policy.

IPSec Advanced Scripts Remote	Sharing							
Addresses								
VPN Client address	192 . 168 . 10 . 2							
Address type	Subnet address 👻							
Remote LAN address	192 . 168 . 0 . 0							
Subnet mask	255 . 255 . 255 . 0							
ESP								
Encryption	3DES 🔻							
Authentication	MD5 -							
Mode	Tunnel 🔻							
PFS								
PFS Group								

Figure 3-14 Configuring TheGreenBow IPSec VPN client

VPN Client Address	Specify the VPN client address as <b>192.168.10.2</b> . This should be the IP address of the remote host.
Address Type	Select <b>subnet address</b> as the address type from the drop-down list.
Remote LAN Address/ Subnet Mask	Specify the remote LAN address as <b>192.168.0.0</b> and subnet mask as <b>255.255.255.0</b> . This should be the IP address and subnet mask of the local hosts.
Encryption/ Authentication/ Mode	Specify encryption as <b>3DES</b> , authentication as <b>MD5</b> , mode as <b>Tunnel</b> . This should be kept the same as the VPN server configuration.
PFS	Uncheck the PFS. This should be kept the same as the VPN server configuration.

6) Click **Save.** Right click **Tunnel** and then click **Open tunnel** on the following page to establish the IPsec VPN tunnel.

TheGreenBow IPSec VPN Client				×
Configuration Tools ?				
THEGREENBOL				
			IPSec VPN Cli	ont
			IT SEC VI IN OIL	ent
Save Apply	Tunnel: IPS			
VPN Configuration	IPSec Advanced	Scripts Remote S	Sharing	
Global Parameters				
Gateway	Addresses			
Open tun	nel Ctrl+O	VPN Client address	192 . 168 . 10 . 2	
Export		Address type	Subnet address	
Сору	Ctrl+C	emote LAN address	192 . 168 . 0 . 0	
Rename	F2	Subnet mask	255 . 255 . 255 . 0	
Delete	Del			
	ESP			
		Encryption	3DES 🔻	
		Authentication	MD5 🔹	
		Mode	Tunnel 🔻	
	PES			
	PFS	Group	<b>.</b>	
VPN Client ready	1			

Figure 3-15 Configuring TheGreenBow IPSec VPN client

### 3.2.4 Verifying the Connectivity of the IPsec VPN Tunnel

Choose the menu **VPN > IPsec > IPsec SA** to load the following page.

Figure 3-16 IPSec SA list

IPSec SA List											
Entry Count: 2									🕜 Refresh		
		ID	Name	SPI	Direction	Tunnel ID	Data Flow	Protocol	AH Authentication	ESP Authentication	ESP Encryption
		1	VPN2	348545766 3	in	10.10.10.10<10.1 0.10.20	192.168.0.0/24 < 192.168.1 0.2/32	ESP		MD5	3DES
		2	VPN2	116448897 2	out	10.10.10.10 >10.10.10.20	192.168.0.0/24> 192.168.1 0.2/32	ESP		MD5	3DES

The IPsec SA list shows the information about the established IPsec VPN tunnel. Here, you can verify the connectivity of the IPsec VPN tunnel.

# 3.3 L2TP Client-to-LAN VPN Configuration

To configure the L2TP Client-to-LAN VPN, follow these steps:

- 1) Configure L2TP VPN server.
- 2) (Optional) Implement configuration for NAT devices.

- 3) Configure the L2TP VPN client software.
- 4) Verify the connectivity of the L2TP VPN tunnel.
- 5) (Optional) Configure access to the internet via proxy gateway.

### 3.3.1 Configuring L2TP VPN Server

 Choose the menu Preferences > VPN IP Pool > VPN IP Pool and click Add to load the following page on the VPN router. Configure the parameters for the VPN IP pool. Click OK.

Fiaure 3-17	Configuring VPN IP	pool list
rigalo o Tr	ooringaning vi ivii	p0011100

VPN IP Pool List									
						🕂 Add 🛛 😑 Delete			
	ID	I	P Pool Name	Starting IP Address	Ending IP Address	Operation			
IF St Er	IP Pool Name: Starting IP Address: Ending IP Address: OK Cancel		pool1 172.16.10.100 172.16.10.200						
IP Pool Name Specify the IP pool name as you like. Here we enter <b>pool1.</b>									
Starting IP Address/ Ending IP AddressSpecify the starting IP address a The VPN server will assign IP address established. You can specify any conflict. Here we specify the star ending IP address as 172.16.10.2					and ending IP address for Iress to the remote host reasonable IP address rting IP address as <b>172.</b> 200.	or the VPN IP pool. when the tunnel is that will not cause <b>16.10.100</b> and the			

2) Choose the menu **VPN > Users > Users** and click **Add** to load the following page. Configure the parameters for the L2TP user account. Click **OK**.

							O	Add 😑 De
	ID	Account Name	Protocol	Local IP Address	IP Address Pool	Network Mode	Remote Subnet	Operatio
	Account	Name:	tplink					
1	Passwor	Password:						
	Drotocol		Low	Middle High				
I	Protocol	:	Low L2TP	Middle High				
I	Protocol Local IP	: Address:	Low L2TP 172.31.1	Middle High • 1.16				
1 1 1	Protocol Local IP IP Addre	: Address: :ss Pool:	Low L2TP 172.31.1 pool1	Middle High				
	Protocol: Local IP IP Addre DNS Add	: Address: :ss Pool: Iress:	Low L2TP 172.31.1 pool1 8.8.8.8	Middle High I.16				
	Protocol: Local IP IP Addre DNS Add Network	: Address: :ss Pool: iress: :Mode:	Low L2TP 172.31.1 pool1 8.8.8.8 Client-to	Middle High .1.16				

Figure 3-18 Configuring L2TP users

Account Name	Specify the account name as you like. Here we enter <b>tplink</b> .
Password	Specify the password as you like. Here we enter <b>123456</b> .
Protocol	Specify the Protocol as L2TP.
Local IP Address	This is the virtual IP address which the remote host will set up a point-to-point connection with. You can specify any reasonable IP address that will not cause conflict. Here we specify the Local IP Address as <b>172.31.1.16</b> .
IP Address Pool	Select <b>pool1</b> as the IP address pool from the drop-down list. This is the VPN IP pool we have just configured.
DNS Address	Specify the DNS address according to your network environment. This is the DNS address to be assigned to the remote host. Here we enter <b>8.8.8.8</b> .
Network Mode	Specify the network mode as <b>Client-to-LAN</b> .
Max Connections	Specify the max connections according to your needs. Here we specify max connections as 5.

 Choose the menu VPN > L2TP > L2TP Server and click Add to load the following page. Configure the parameters for the L2TP server. Click OK.

L2TP Server Settings						
					🕂 Add 🛛 😑 Delete	
	ID	WAN	IPSec Encryption	Status	Operation	
WAN: IPSec Encryption: Status: OK Cancel		WAN1  Unencrypted  Enable				
WAN		Specify WAN as <b>WAN</b> established on.	1. This should be th	ne WAN port which	the VPN tunnel is	
IPsec Encryption Specify the IPsec IPsec encryption a		Specify the IPsec end IPsec encryption as <b>U</b>	cryption according nencrypted.	to your needs. Her	re we specify the	
Status Enable the L2TP server.						

# 3.3.2 (Optional) Implementing Configuration for NAT Devices

If there are NAT devices on the network, the suitable network topology is shown in **Figure 3-2**. In this scenario, please verify the configuration on the VPN router, and configure virtual servers on the NAT device. The configuration steps are as follows:

For the VPN router, choose the menu VPN > L2TP > L2TP Server, select the L2TP server list entry which is previously created, and click it to load the following page. Please make sure that the IPsec encryption is specified as Unencrypted. Otherwise, the VPN tunnel may fail to be established.

L	L2TP Server Settings							
						🕂 Add 🛛 😑 Delete		
		ID	WAN	IPSec Encryption	Status	Operation		
	WAN: IPSec	Encryption:	WAN1  VINencrypted  VINencrypted					
	Status	:	Enable					
	OK	Cancel						

Figure 3-20 Verifying the L2TP server configuration

 For the NAT device, choose the menu Transmission > NAT > Virtual Servers and click Add to load the following page . Configure the parameters for the virtual server. Click OK.

Virtual Server List										
	🔂 Add 🛛 🖨 Delete									
	D ID Name			Interface	External Port	Internal Port	Internal Server IP	Protocol	Status	Operation
Name: Interface: External Port: Internal Port: Internal Server IP: Protocol: Status: OK Cancel			L2TP WAN 1701 1701 172.1 UDP ♥ Enal	1 6.10.2 Dle	•	(XX or XX-X (XX or XX-X	X ,1-65535) X ,1-65535)			
Nar	ne		Spec	ify the n	ame for	the virtua	al server list entry. He	re we en	ter <b>L2TP</b> .	
Inte	erfac	ce	Specify WAN as <b>WAN1</b> . This should be the WAN port which the VPN tunnel is established on.							
Ext Inte	External Port/ Specify the external port Specify the external port			port and i	nternal port as <b>1701</b> .					
Inte	Internal Server IP Specification Specificati		Specify the internal server IP as <b>172.16.10.2.</b> This should be the WAN IP address of the VPN server.							
Protocol Specify the protocol a			as <b>UDP</b> .							
Status Enable the virtual serv			ver list er	ntry.						

Figure 3-21 Configuring virtual server for L2TP

# 3.3.3 Configuring the L2TP VPN Client Software

Here we use the built-in VPN client software in Windows7 Operating System on the remote host. To configure the VPN client software, follow these steps.

 In Windows Control Panel, choose the menu Network and Internet > Network and Sharing Center. Click Set up a new connection or network to load the following page.

) 🕎 Set l	Jp a Connection or Network	
Choos	e a connection option	
<b>*</b>	Connect to the Internet Set up a wireless, broadband, or dial-up connection to the li Set up a new network Configure a new router or access point.	nternet.
	Connect to a workplace Set up a dial-up or VPN connection to your workplace.	
	Set up a dial-up connection Connect to the Internet using a dial-up connection.	
		Next Car

Figure 3-22 Configuring the L2TP VPN client

2) Click **Connect to a workplace** and click **Next** to load the following page.

Figure 3-23 Configuring the L2TP VPN client



3) Click **Use my Internet connection (VPN)** to load the following page.

Figure 3-24 Configuring the L2TP VPN client

🚱 🌆 Connect to a Workplace	
Do you want to set up an Internet connection before continuing?	
An Internet connection is necessary for using a VPN connection.	
Set up an Internet connection	
I'll set up an Internet connection later	
	Cancel

4) Click I'll set up an Internet connection later to load the following page. Specify the internet address as 10.10.10.10. Check Don't connect now, just set it up so I can connect later.

Figure 3-25	Configuring the L2TP VPN client

🕒 🌆 Connect to a Workplace								
Type the Internet address to connect to								
Your network administrator	can give you this address.							
Internet address:	10.10.10.10	]						
Destination name:	VPN Connection	-						
Use a smart card								
🛞 🔲 Allow other people t This option allows a	o use this connection nyone with access to this computer to use this connection.							
Don't connect now;	just set it up so I can connect later							
	Nex	t Cancel						

 Click Next to load the following page. Specify the User name as tplink and Password as 123456. This should be the same as the VPN server configuration. Click Create.

Figure 3-26	Configuring	the L2TP	VPN client
0			

Connect to a Workplace		
Type your user name	and password	
User name:	tplink	
Password:	123456	
	Show characters	
	Remember this password	
Domain (optional):		
		Create Cancel

6) In Windows Control Panel, choose the menu Network and Internet > Network and Sharing Center. Click Change adapter settings. Right click VPN Connection and click Properties to load the following page. Specify the host name or IP address of destination as 10.10.10.10.

VPN Connection Properties
General Options Security Networking Sharing
157.54.0.1 or 3ffe:1234::1111):
- First connect
Windows can first connect to a public network, such as the Internet, before trying to establish this virtual connection.
Dial another connection first:
See our online <u>privacy statement</u> for data collection and use information.
OK Cancel

Figure 3-27 Configuring the L2TP VPN client

7) Choose the menu **Options** to load the following page. Specify Redial attempts as **0**.

Figure 3-28 Configuring the L2TP VPN client

VPN Connection Properties	×								
General Options Security Networking	Sharing								
Dialing options Display progress while connecting Prompt for name and password, cert Include Windows logon domain	ificate, etc.								
Redialing options									
Redial attempts:	0								
Time between redial attempts:	1 minute 👻								
Idle time before hanging up:	never 🔻								
Idl <u>e</u> threshold:	· · · · · · · · · · · · · · · · · · ·								
Redial if line is dropped	Redial if line is dropped								
PPP Settings									
	OK Cancel								

 Choose the menu Security to load the following page. Select Layer 2 Tunneling Protocol with IPsec (L2TP/IPSec) as the type of VPN from the drop-down list. Select Optional encryption (connect even if no encryption) as data encryption from the drop down list. Click OK.

VPN Connection Properties
General Options Security Networking Sharing
Type of VPN:
Layer 2 Tunneling Protocol with IPsec (L2TP/IPSec)
Data encryption:
Optional encryption (connect even if no encryption)
Authentication
C Use Extensible Authentication Protocol (EAP)
· · · · · · · · · · · · · · · · · · ·
Properties
Allow these protocols
Unencrypted password (PAP)
Challenge <u>Handshake Authentication Protocol</u> (CHAP)
Microsoft CHAP Version 2 (MS-CHAP v2)
Automatically use my Windows logon name and password (and domain. if any)
OK Cancel

Figure 3-29 Configuring the L2TP VPN client

9) Right click VPN Connection and click Connect to load the following page. Specify the User name as tplink, and the Password as 123456. This should be the same as the VPN server configuration. Click Connect to establish the VPN tunnel.



Figure 3-30 Configuring the L2TP VPN client

# 3.3.4 Verifying the Connectivity of the L2TP VPN Tunnel

Choose the menu **VPN > L2TP > Tunnel List** to load the following page.

Figure 3-31 L2TP tunnel list

Tunn	el List						
							🖉 Refresh
ID	Account Name	Mode	Tunnel	Local IP	Remote IP	Remote Local IP	DNS
1	tplink	Server		172.31.1.16	10.10.10.20	172.16.10.100	

The tunnel list shows the information about the established VPN tunnel. Here, you can verify the connectivity of the L2TP VPN tunnel.

# 3.3.5 (Optional) Configuring Access to the Internet via Proxy Gateway.

In this scenario, the remote host accesses the internet via the VPN router, and the VPN router acts as a proxy gateway. To meet this demand, please configure Multi-Nets NAT on the VPN router, and configure **Use default gateway on remote network** on the remote host.

1) For the VPN Router, choose the menu **Tansmission > NAT > Multi-Nets NAT** and click **Add** to load the following page. Configure the parameters for Multi-Nets NAT. Click **OK**.

Multi-Ne	ts NAT List							
							0	Add 😑 Delete
	ID	Name	è	Interface	Source IP Range	Status	Description	Operation
	Name: Interface: Source IP F Status: Description OK	tange: : Cancel	VPN WAN1 172.1 V Enab	L • 6.10.0 / 24 le	Optional)			
Name	е		Speci	fy the name for th	ne Multi-Nets NAT list e	ntry. Here w	ve enter <b>VPN</b>	I.
Inter	face		Speci tunne	fy the interface a I is established o	as <b>WAN1</b> . This should n.	be the WAN	I port which	the VPN
Sour	ce IP Ra	nge	Specit pool c	fy the source IP r onfigured for the	range as <b>172.16.10.0/2</b> • VPN router.	<b>4</b> . This shou	uld include th	ne VPN IP

Figure 3-32 Configuring Multi-Nets NAT

Status	Enable the Multi-Nets NAT list entry.

2) For the remote host, choose the menu Network and Internet > Network and Sharing Center in Windows Control Panel. Click Change adapter settings. Right click VPN Connection and click Properties. Choose the menu Networking to load the following page.

VPN Connection Properties	×
General Options Security Networking Sharing	
This connection uses the following items:	
Install Uninstall Properties	
Description Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.	
OK Can	cel

Figure 3-33 Configuring the L2TP VPN client connection properties

3) Double click Internet Protocol Version 4 (TCP/IPv4) to load the following page. Select Obtain an IP address automatically and select Obtain DNS server address automatically.

Internet Protocol Version 4 (TCP/IPv4)	Properties
General	
You can get IP settings assigned autor supports this capability. Otherwise, you administrator for the appropriate IP setti	natically if your network need to ask your network ings.
Obtain an IP address automatical	y
Use the following IP address:	
IP address:	
Obtain DNS server address auton Obtain DNS server address auton	natically dresses:
Preferred DNS server:	
Alternate DNS server:	
	Advanced
	OK Cancel

Figure 3-34 Configuring the L2TP VPN client connection properties

# 4) Click Advanced to load the following page. Please check Use default gateway on remote network. Click OK.

Figure 3-35 Configuring the L2TP VPN client connection properties

Advanced TCP/IP Settings	3
IP Settings DNS WINS	
This checkbox only applies when you are connected to a local network and a dial-up network simultaneously. When checked, data that cannot be sent on the local network is forwarded to the dial-up network.	
Vise default gateway on remote network	
Disable class based route addition	
Interface metric:	
OK Cancel	

# 3.4 PPTP Client-to-LAN VPN Configuration

To complete the PPTP Client-to-LAN VPN, follow these steps:

- 1) Configure PPTP VPN server.
- 2) (Optional) Implement configuration for NAT devices.
- 3) Configure the PPTP VPN client software.
- 4) Verify the connectivity of the PPTP VPN tunnel.
- 5) (Optional) Configure access to the internet via proxy gateway.

### 3.4.1 Configuring PPTP VPN Server

 For the VPN router, choose the menu Preferences > VPN IP Pool > VPN IP Pool and click Add to load the following page. Configure the parameters for the VPN IP pool. Click OK.

VPN IP P	ool List					
						🕂 Add 🛛 😑 Delete
	ID	1	P Pool Name	Starting IP Address	Ending IP Address	Operation
I S E	P Pool Nar Starting IP Ending IP / OK	me: Address: Address: Cancel	pool1 172.16.10.100 172.16.10.200			
IP Poo	ol Nam	е	Specify t	he IP pool name as you	like. Here we enter <b>pool</b> 1	1.
Starti Endin	ng IP A g IP Ac	ddress/ Idress	Specify t The VPN establish	he starting IP address a server will assign IP address and the server will assign IP address and the server will assign IP address and the server will be a	and ending IP address fo dress to the remote host y reasonable IP address	or the VPN IP pool. when the tunnel is that will not cause

Figure 3-36 Configuring VPN IP pool list

2) Choose the menu **VPN > Users > Users** and click **Add** to load the following page. Configure the parameters for the PPTP user account. Click **OK**.

ending IP address as 172.16.10.200.

conflict. Here we specify the starting IP address as 172.16.10.100 and the

Figure 3-37	Configuring PPTP users
0	0 0

ser Account Lis	st						
						•	Add 😑 Dele
D ID	Account Name	Protocol	Local IP Address	IP Address Pool	Network Mode	Remote Subnet	Operation
Account Passwor Protocol Local IP IP Addre DNS Add Network Max Con	Name: rd: : Address: ess Pool: tress: : Mode: anections: Cancel	tplink 	Middle High .16 .16 .16 .16 .16 .16 .16 .16	0)			

Account Name

Specify the account name as you like. Here we enter **tplink**.

Password	Specify the password as you like. Here we enter <b>123456</b> .
Protocol	Specify the protocol as <b>PPTP.</b>
Local IP Address	This is the virtual IP address which the remote host will set up a point-to-point connection with. You can specify any reasonable IP address that will not cause conflict. Here we specify the local IP address as <b>172.31.1.16</b> .
IP Address Pool	Select <b>pool1</b> as the IP address pool from the drop-down list. This is the VPN IP pool we have just configured.
DNS Address	Specify the DNS address according to your network environment. This is the DNS address to be assigned to the remote host. Here we enter <b>8.8.8.8</b> .
Network Mode	Specify the network mode as <b>Client-to-LAN</b> .
Max Connections	Specify the max connections according to your needs. Here we specify max connections as 5.

3) Choose the menu **VPN > PPTP > PPTP Server** and click **Add** to load the following page. Configure the parameters for the PPTP server. Click **OK**.

Server List						
					🔂 Add 🛛 🖨 Delete	
	ID	WAN MPPE Encryption Status Operation				
WAN: MPPE E Status OK	Encryption: : Cancel	WAN1  Unencrypted  Enable				
WAN	WAN Specify WAN as <b>WAN1</b> . This should be the WAN port which the VPN tunnel is established on.					
MPPE Enc	ryption	N Specify the MPPE encryption according to your needs. Here we specify the MPPE encryption as <b>Unencrypted</b> .				
Status	Enable the PPTP server.					

# 3.4.2 (Optional) Implementing Configuration for NAT Devices

If there are NAT devices on the network, the suitable network topology is shown in Figure 3-2. In this scenario, please configure virtual servers on the NAT device, and configure PPTP ALG on both the NAT device and the remote gateway. The configuration steps are as follows.

 For the NAT device, choose the menu Transmission > NAT > Virtual Servers and click Add to load the following page. Configure the parameters for the virtual server. Click OK.

Virtua	al Serv	ver List								
									• A	dd 😑 Delete
	ID	Name		Interface	External Port	Internal Port	Internal Server IP	Protocol	Status	Operation
	Nai	me:	PPTP	1		]				
	Int	erface:	WAN	1	•					
	Ext	ernal Port:	1723	}		(XX or XX-X	(,1-65535)			
	Int	ernal Port:	1723	}		(XX or XX-X	(,1-65535)			
	Int	ernal Server IP:	172.	16.10.2						
	Pro	tocol:	ТСР	· · · · · · · · · · · · · · · · · · ·						
	Sta	itus:	🕑 Ena	ble						
		OK Cancel								
Nan	ne		Spec	fy the n	ame for	the virtua	al server list entry. He	ere we ent	er <b>PPTP</b> .	
Inte	Iterface Specify WAN as <b>WAN1</b> . This should be the WAN port which the VPN tunnel is established on.				tunnel is					
Exte Inte	erna	l Port/ Port	Specify the external port and internal port as <b>1723</b> .							
Inte	rnal	Server IP	Specify the internal server IP as <b>172.16.10.2.</b> This should be the WAN IP address of the VPN server.							
Pro	toco	bl	Specify the protocol as <b>TCP</b> .							
Stat	tus		Enabl	e the vir	tual serv	ver list er	try.			

Figure 3-39 Configuring virtual server for PPTP

 For the remote gateway and the NAT device, choose the menu Transmission > NAT > ALG to load the following page. Enable PPTP ALG, and click Save.

Figure 3-40	Configuring PPTP ALG
ALG	
FTP ALG	
✔ H.323 ALG	
PPTP ALG	
SIP ALG	
✓ IPSec ALG	
Save	

### 3.4.3 Configuring the PPTP VPN Client Software

Here we use the built-in VPN client software in Windows7 Operating System on the remote host. To configure the VPN client software, follow these steps.

 In Windows Control Panel, choose the menu Network and Internet > Network and Sharing Center. Click Set up a new connection or network to load the following page.



🕞 🚽 Set Up a Connection or Network	
Choose a connection option	
Connect to the Internet Set up a wireless, broadband, or dial-up connection to the Inter	met.
Set up a new network Configure a new router or access point.	
Connect to a workplace Set up a dial-up or VPN connection to your workplace.	
Set up a dial-up connection Connect to the Internet using a dial-up connection.	
	Next Cancel

2) Click **Connect to a workplace** and click **Next** to load the following page.

Figure 3-42 Configuring the PPTP VPN client



3) Click **Use my Internet connection (VPN)** to load the following page.

Figure 3-43 Configuring the PPTP VPN client

🚱 🌆 Connect to a Workplace	
Do you want to set up an Internet connection before continuing?	
An Internet connection is necessary for using a VPN connection.	
Set up an Internet connection	
I'll set up an Internet connection later	
	Cancel
	cancer

4) Click **I'll set up an Internet connection later** to load the following page. Specify the internet address as **10.10.10.10**. Check **Don't connect now, just set it up so I can connect later**.

Fiaure 3-44	Configuring the	PPTP VPN client

🚱 🌆 Connect to a Workplace		
Type the Internet add	ress to connect to	
Your network administrator	can give you this address.	
Internet address:	10.10.10.10	
Destination name:	VPN Connection	•
🔲 Use a smart card		
🞯 🔲 Allow other people t This option allows an	o use this connection nyone with access to this computer to use this connection.	
Don't connect now;	just set it up so I can connect later	
	Nex	t Cancel

 Click Next to load the following page. Specify the user name as tplink and password as 123456. This should be the same as VPN server configuration. Then click Create.

Fiaure 3-45	Configuring	the PPTP	VPN client
J			

🚱 🌆 Connect to a Workplace		
Type your user name	and password	
User name:	tplink	
Password:	123456	
	Show characters	
Damaia (antianal):	Remember this password	
Domain (optional):		
		Create Cancel

6) In Windows Control Panel, choose the menu Network and Internet > Network and Sharing Center. Click Change adapter settings. Right click VPN Connection and click Properties to load the following page. Specify the host name or IP address of destination as 10.10.10.10.

VPN Connection Properties
General Options Security Networking Sharing
Host name or IP address of destination (such as microsoft.com or 157.54.0.1 or 3ffe:1234::1111):
10.10.10
First connect
Windows can first connect to a public network, such as the Internet, before trying to establish this virtual connection.
Dial another connection first:
See our online <u>privacy statement</u> for data collection and use information.
OK Cancel

Figure 3-46 Configuring the PPTP VPN client

7) Choose the menu **Options** to load the following page. Specify redial attempts as **0**.

Figure 3-47 Configuring the PPTP VPN client

VPN Connection Properties							
General Options Security Networking Sharing							
Dialing options         ✓ Display progress while connecting         ✓ Prompt for name and password, certificate, etc.         ✓ Include Windows logon domain							
Redialing options							
Redial attempts: 0							
Time between redial attempts:							
Idle time before hanging up:							
Idl <u>e</u> threshold:							
Redial if line is dropped							
PPP Settings							
OK Cancel							

8) Choose the menu Security to load the following page. Select Point to Point Tunnel Protocol (PPTP) as the type of VPN from the drop-down list. Select Optional encryption (connect even if no encryption) as data encryption from the drop down list. Click OK.

VPN Connection Properties							
General Options Security Networking Sharing							
Type of VPN:							
Point to Point Tunneling Protocol (PPTP)							
Advanced settings							
Optional encryption (connect even if no encryption)							
Authentication							
Use Extensible Authentication Protocol (EAP)							
· · · · · · · · · · · · · · · · · · ·							
Properties							
Allow these protocols							
I leasested assessed (PAP)							
Challenge Handebake Authentication Protocol (CHAP)							
Microsoft CHAP Version 2 (MS CHAP v2)							
password (and domain, if any)							
OK Cancel							

Figure 3-48 Configuring the PPTP VPN client

9) Right click VPN Connection and click Connect to load the following page. Specify the user name as tplink, and the password as 123456. This should be the same as the VPN server configuration. Click Connect to establish the VPN tunnel.

Seconnect VPN Connection							
User name:	tplink						
Password:	•••••						
Domain:							
Save this user name and password for the following users:							
Me only							
🔞 🔿 Anyone who uses this computer							
Connect	Cancel Properties Help						

Figure 3-49 Configuring the PPTP VPN client

# 3.4.4 Verifying the Connectivity of the PPTP VPN Tunnel

Choose the menu **VPN > PPTP > Tunnel List** to load the following page.

Figure 3-50 PPTP tunnel list

Tunnel List									
Refre									
ID	Account Name	Mode	Tunnel	Local IP	Remote IP	Remote Local IP	DNS		
1	tplink	Server		172.31.1.16	10.10.10.20	172.16.10.100			

The tunnel list shows the information about the established VPN Tunnel. Here, you can verify the connectivity of the PPTP VPN tunnel.

# 3.4.5 (Optional) Configuring Access to the Internet via Proxy Gateway.

In this scenario, the remote host access the internet via the VPN router, and the VPN router acts as a proxy gateway. To meet this demand, please configure Multi-Nets NAT on the VPN router, and configure **Use default gateway on remote network** on the remote host.

 For the VPN router, choose the menu Tansmission > NAT> Multi-Nets NAT and click Add to load the following page. Configure the parameters for the Multi-Nets NAT. Click OK.

Multi-Ne	ets NAT List							
							0	Add 😑 Delete
	ID	Name		Interface	Source IP Range	Status Description		Operation
Name: VPN Interface: WAN1 Source IP Range: 172.16.10.0 Status: Enable Description: OK Cancel			VPN WAN1 172.16 Y Enabl	.10.0 / 24 e	Optional)			
Name	Name Specify the name for the Multi-Nets NAT list entry. Here we enter <b>VPN</b> .							Ν.
Interf	Interface Specify the interface as <b>WAN1</b> . This should be the WAN port which the VF tunnel is established on.						h the VPN	
Sour	Source IP Range Specify source IP range as 172.16.10.0/24. This should include the VPN IP poo configured for the VPN router.						PN IP pool	
Statu	Status Enable the Multi-Nets NAT list entry.							

Figure 3-51 Configuring Multi-Nets NAT
2) For the remote host, choose the menu Network and Internet > Network and Sharing Center in Windows Control Panel. Click Change adapter settings. Right click VPN Connection and click Properties, Choose the menu Networking to load the following page.

VPN Connection Properties	×		
General Options Security Networking Sharing			
This connection uses the following items:	$\neg \parallel$		
Internet Protocol Version 4 (TCP/IPv4)  Image: A state of the			
Client for Microsoft Networks			
Install Uninstall Properties			
Description			
Transmission Control Protocol/Internet Protocol. The default			
across diverse interconnected networks.			
	i j		

Figure 3-52 Configuring the PPTP VPN client connection properties

3) Double click Internet Protocol Version 4 (TCP/IPv4) to load the following page. Select Obtain an IP address automatically and select Obtain DNS server address automatically.

Internet Protocol Version 4 (TCP/IPv4)	Properties ?		
General			
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.			
Obtain an IP address automatical	ly I		
Use the following IP address: —			
IP address:			
Obtain DNS server address autor	natically		
Use the following DNS server add	dresses:		
Preferred DNS server:			
Alternate DNS server:			
	Advanced		
	OK Cancel		

Figure 3-53 Configuring the PPTP VPN client connection properties

## 4) Click **Advanced** to load the following page. Please check **Use default gateway on remote network**. Click **OK**.

Figure 3-54 Configuring the PPTP VPN client connection properties

Advanced TCP/IP Settings
IP Settings DNS WINS
This checkbox only applies when you are connected to a local network and a dial-up network simultaneously. When checked, data that cannot be sent on the local network is forwarded to the dial-up network.
Use default gateway on remote network
Disable class based route addition
Interface metric:
OK Cancel

## **COPYRIGHT & TRADEMARKS**

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

No part of the specifications may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from TP-Link Technologies Co., Ltd. Copyright © 2018 TP-Link Technologies Co., Ltd. All rights reserved.

http://www.tp-link.com