How to configure VPN function on TP-LINK Routers

1. VPN Overview

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

With the wide application of the Internet, more and more data are needed to be shared through the Internet. Connecting the local network to the Internet directly, though can allow the data exchange, will cause the private data to be exposed to all the users on the Internet. The VPN (Virtual Private Network) technology is developed and used to establish the private network through the public network, which can guarantee a secured data exchange.

VPN adopts the tunneling technology to establish a private connection between two endpoints. It is a connection secured by encrypting the data and using point-to-point authentication. As the packets are encapsulated and de-encapsulated in the Router, the tunneling topology implemented by encapsulating packets is transparent to users.

The tunneling protocols supported by TP-LINK Routers are as below:

Product Model	Tunneling Protocol
TL-ER6120	IPsec、PPTP、L2TP
TL-ER6020	IPsec、PPTP、L2TP
TL-ER604W	IPsec、PPTP、L2TP
TL-R600VPN	IPsec、PPTP

2. How to configure LAN-to-LAN IPsec VPN on TP-LINK Router

Suitable for: TL-ER6120, TL-ER6020, TL-ER604W, TL-R600VPN

To setup an IPsec VPN tunnel on TP-LINK routers you need to perform the following steps:

A. **Connecting the devices together**
B. **Verify the settings needed for IPsec VPN on router**
C. **Configuring IPsec VPN settings on TL-ER6120 (Router A)**
D. **Configuring IPsec VPN settings on TL-R600VPN (Router B)**
E. **Checking IPsec SA**

NOTE: We use TL-ER6120 and TL-R600VPN in this example, the way to configure IPsec VPN on TL-ER6020/TL-ER604W is the same as that on TL-ER6120.

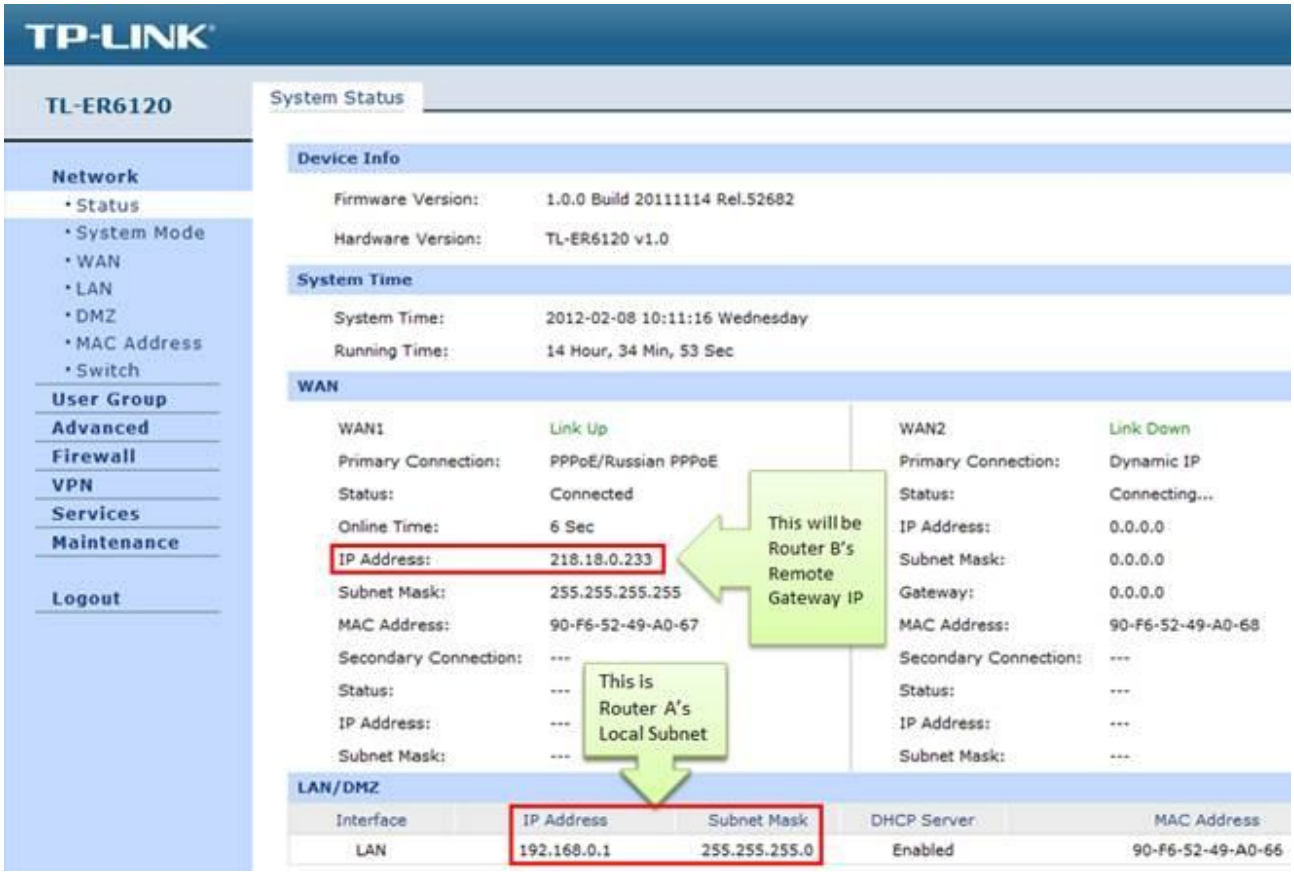
A. Connecting the devices together

Before setup a VPN tunnel, you need to ensure that the two routers are connected to the Internet. After ensuring that there is an active Internet connection on each router, you need to verify the VPN settings of the two routers, please follow the instruction below.

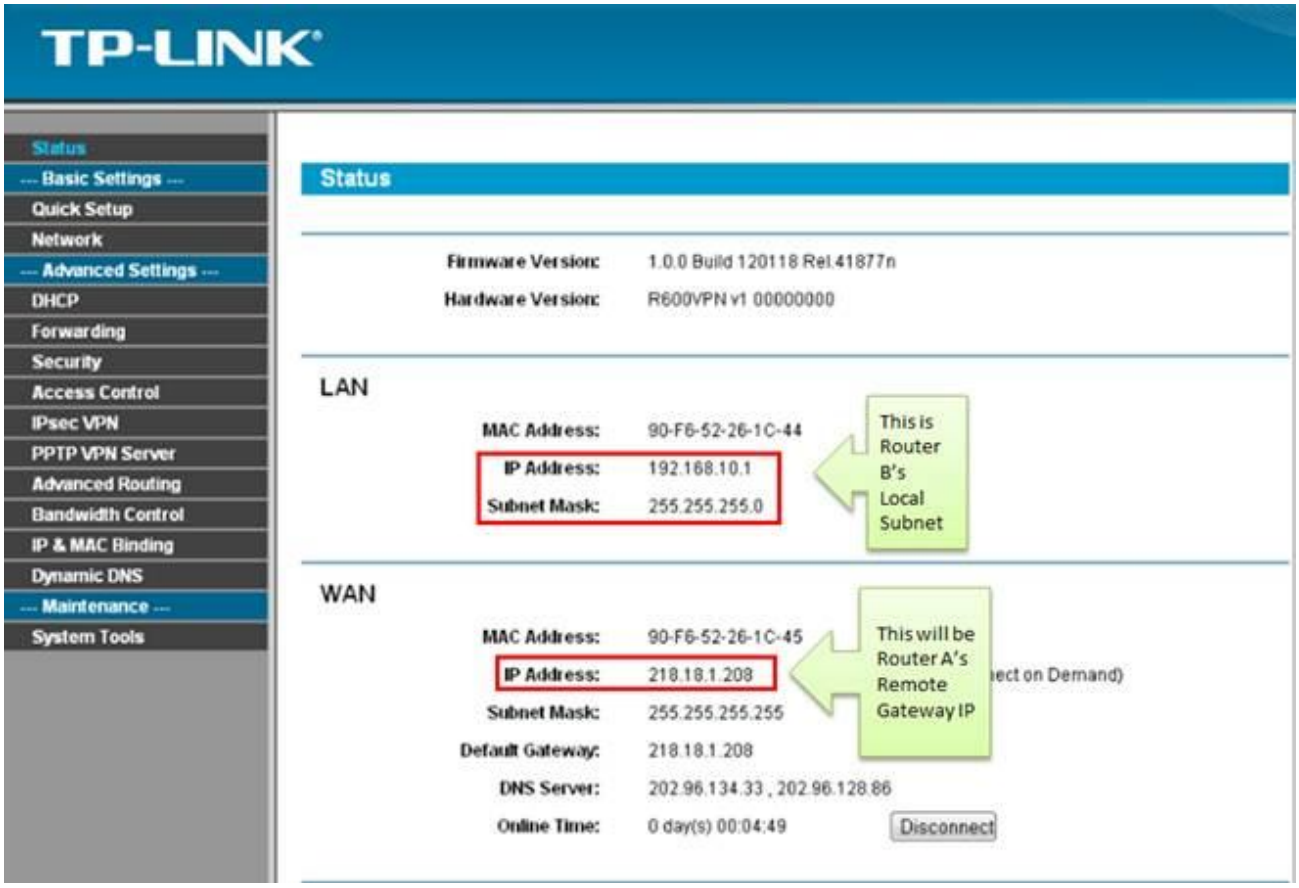
B. Verify the settings needed for IPsec VPN on router

To verify the settings needed on the two routers, please login the router's management webpage.

Router A's Status page:



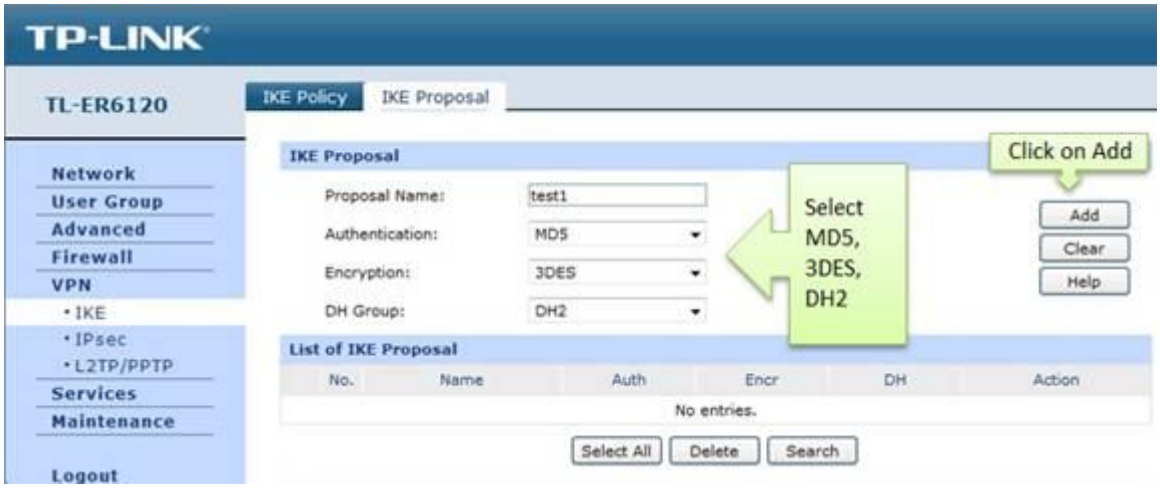
Router B's Status page:



C. Configuring IPsec VPN settings on TL-ER6120 (Router A)

Step 1 : On the management webpage, click on VPN then IKE Proposal.

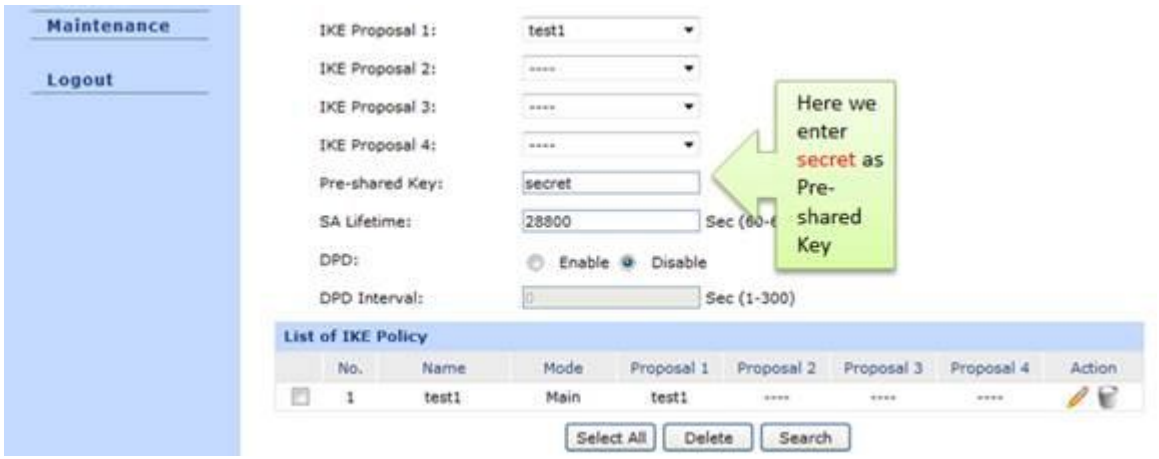
Under IKE Proposal, enter Proposal Name whatever you like, select Authentication, Encryption and DH Group, we use MD5,3DES, DH2 in this example.



Step 2 : Click on Add.

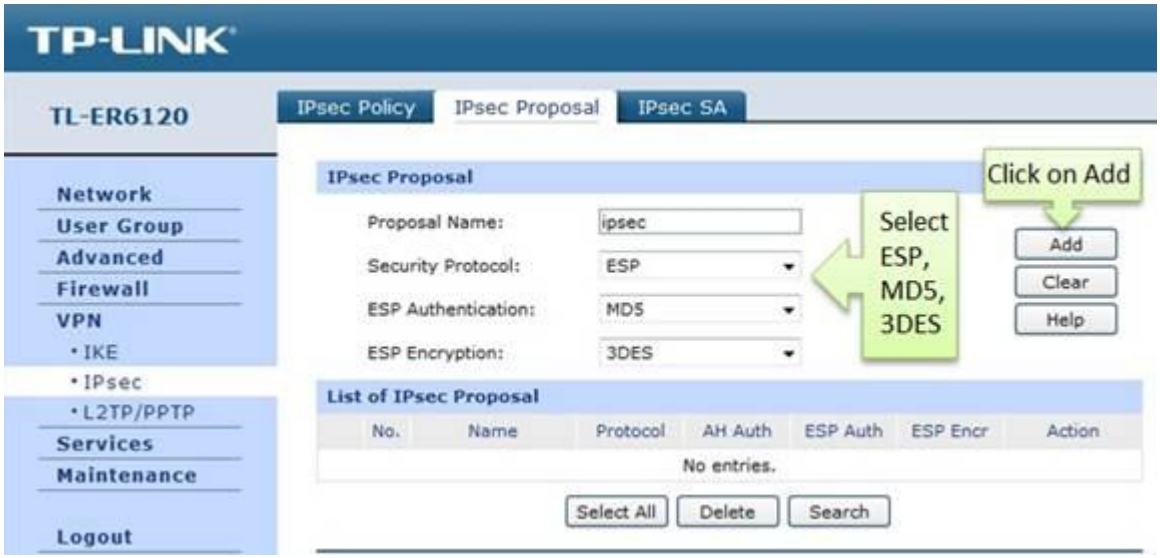
Step 3 : Click on IKE Policy, enter Policy Name whatever you like, select Exchange Mode, in this example we use Main, select IP Address as ID Type.

Step 4 : Under IKE Proposal 1, we use test1 in this example. Enter Pre-shared Key and SA Lifetime you want, DPD is disabled.



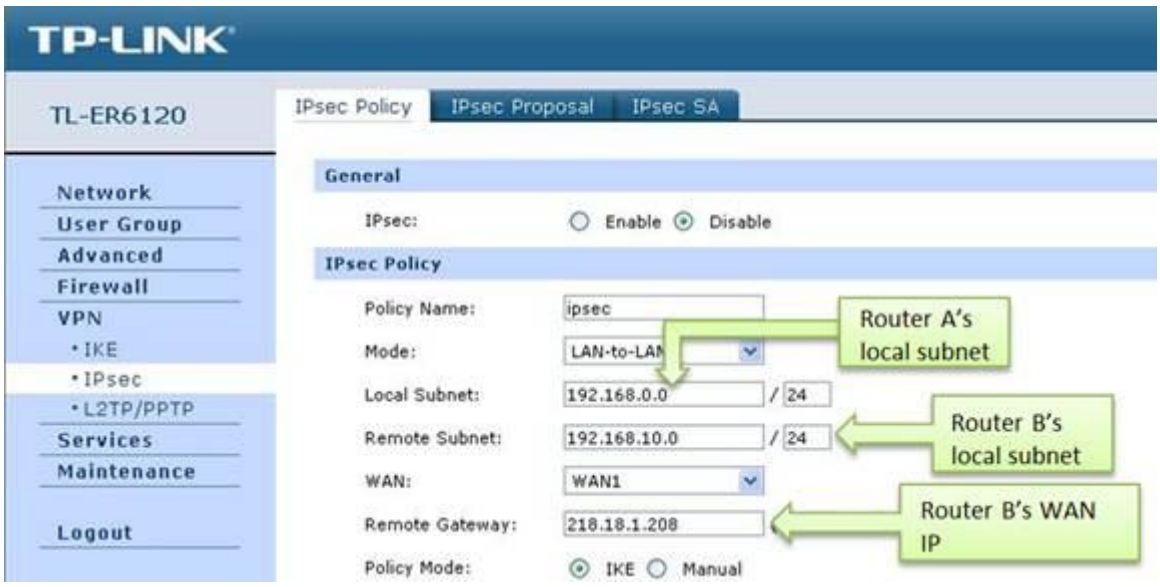
Step 5 : Click on Add.

Step 6 : Click on IPsec on the left menu, then IPsec Proposal. Select Security Protocol, ESP Authentication and ESP Encryption you want to enable on VPN tunnel. Here we use ESP, MD5 and 3DES for example.



Step 7 : Click on Add.

Step 8 : Click on IPsec Policy, enter Policy Name whatever you like, the Mode should be LAN-to-LAN. Enter Local Subnet and Remote Subnet.



Step 9 : Select WAN you use and type in Remote Gateway. In this example, the Remote Gateway is Router B's WAN IP address, 218.18.1.208.

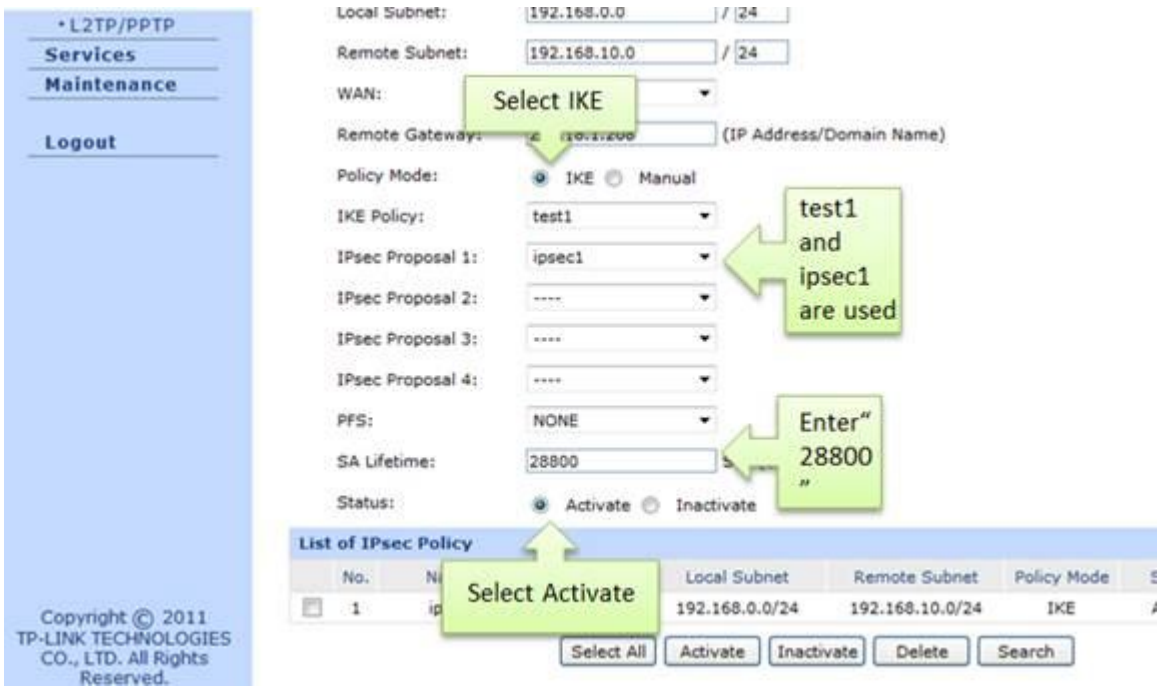
Step 10 : Look for Policy Mode and select IKE.

Step 11 : Under IKE Policy, we select test1 which is used.

Step 12 : Under IPsec Proposal, we use ipsec1 in this example.

Step 13 : Look for PFS, we set NONE here, under SA Lifetime, enter “28800” or the period you want.

Step 14 : Look for Status then select Activate



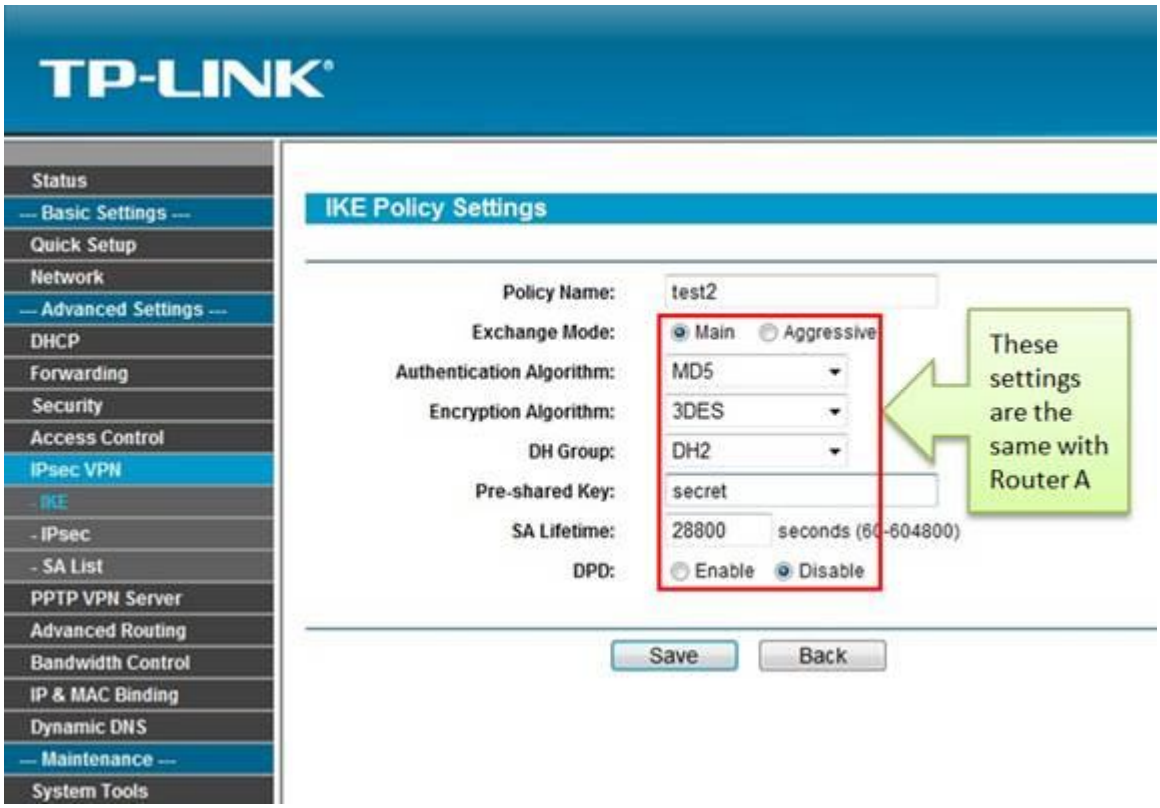
Step 15 : Click on Add.

Step 16 : Select Enable then click on Save.

D. Configuring IPsec VPN settings on TL-R600VPN (Router B)

Step 1 : Go to IPsec VPN -> IKE, click on Add New

Step 2 : Enter Policy Name whatever you like, here we use test2. Exchange Mode, select Main.



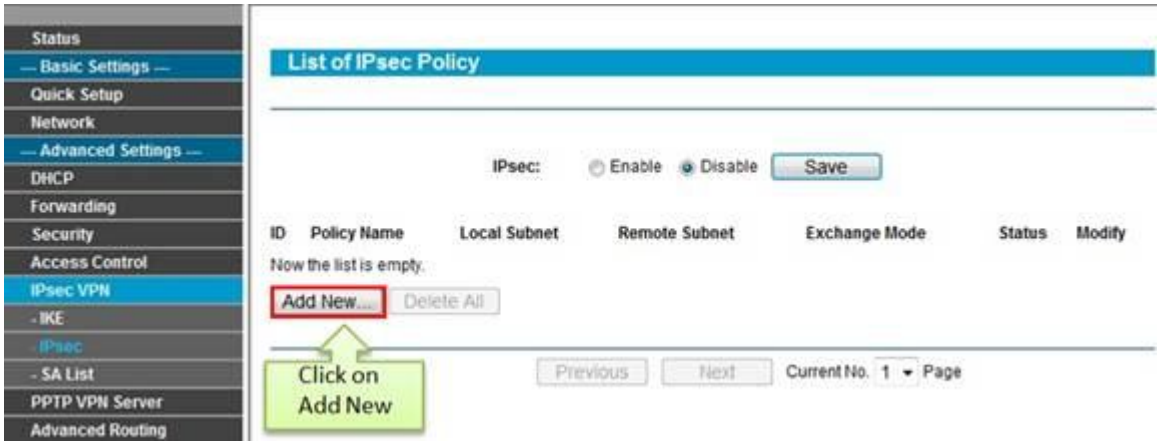
Step 3 : Authentication Algorithm and Encryption Algorithm are the same with Router A, we use MD5 and 3DES in this example.

Step 4 : DH Group, select DH2, the same with Router A.

Step 5 : Enter Pre-share Key and SA Lifetime, make sure that they are the same with Router A.

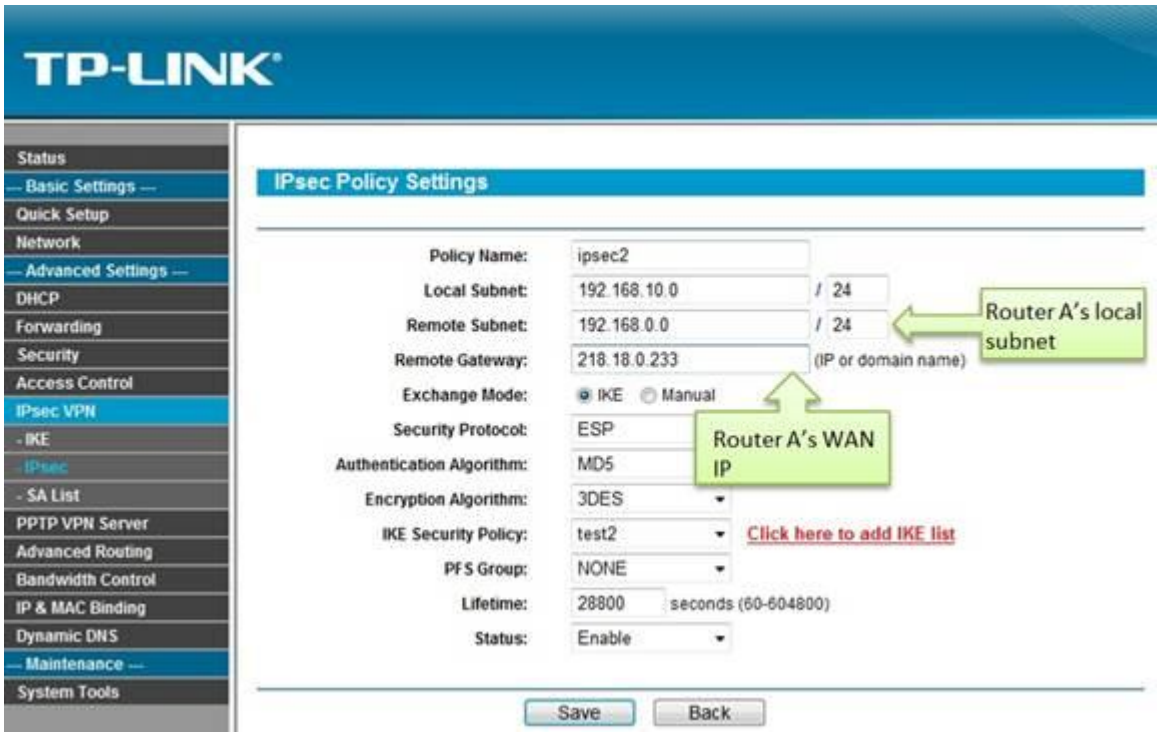
Step 6 : Click on Save.

Step 7 : Click on IPsec on left side, click on Add New.



Step 8 : Enter Policy Name, we use ipsec2 in this example.

Step 9 : Enter Local Subnet and Remote Subnet, and then enter Remote Gateway, it's Router A's WAN IP address, 218.18.0.233.



Step 10 : Look for Exchange mode, please select IKE, and Security Protocol, we use ESP here.

Step 11 : Authentication Algorithm and Encryption Algorithm are the same with Router A, we use MD5 and 3DES in this example.

Step 12 : IKE Security Policy, we use test2 in this example.

Step 13 : Look for PFS, we set NONE here, under Lifetime, enter “28800” or the period you want.

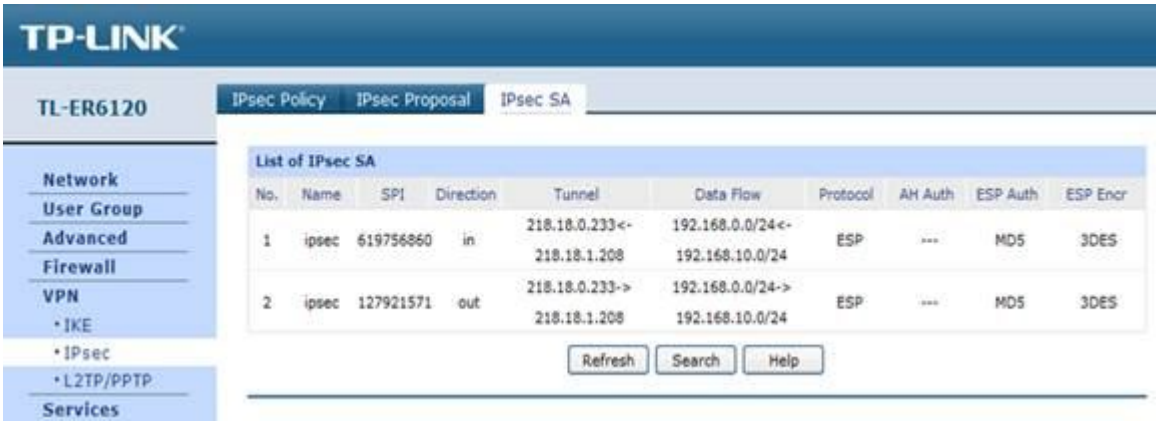
Step 14 : Look for Status then select Enable.

Step 15 : Click on Save.

Step 16 : Enable IPsec and then click on Save.

E. Checking IPsec SA

Router A:

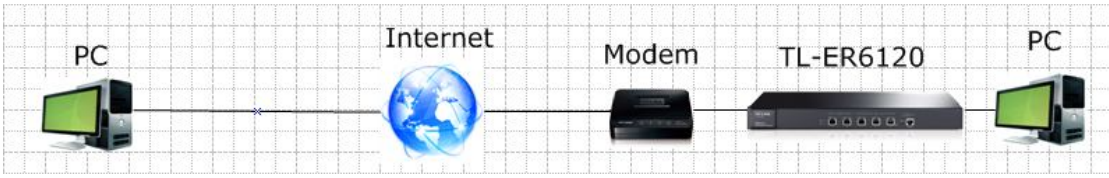


Router B:


TP-LINK
Status
--- Basic Settings ---
Quick Setup
Network
--- Advanced Settings ---
DHCP
Forwarding
Security
Access Control
IPsec VPN
- IKE
- IPsec
- SA List
List of Security Association
ID Name SPI Tunnel Initiator Tunnel Receiver Security Protocol AH Auth ESP Auth ESP Encr
1 ipsec2 619756860 218.18.1.208 218.18.0.233 ESP -- MD5 3DES
2 ipsec2 127921571 218.18.0.233 218.18.1.208 ESP -- MD5 3DES
Refresh

3. How to configure GreenBow IPsec VPN Client with a TP-LINK VPN Router

Suitable for: TL-ER6120, TL-ER6020, TL-ER604W



GreenBow IPsec VPN Client is an IPsec VPN client software developed by TheGreenBow company. It can be downloaded from download page for TL-ER6120 (http://www.tp-link.com/en/support/download/?model=TL-ER6120&version=V1) or official website of TheGreenBow (http://www.thegreenbow.com/vpn/vpn-client.html?utm_expid=333874-5.xSdTaggCQhu28X37j2BKrw.1&utm_referrer=http%3A%2F%2Fwww.thegreenbow.com%2Fservices.html).

To setup an IPsec VPN tunnel between the GreenBow IPsec VPN Client and the TP-LINK VPN Router you need to perform the following steps:

A. **Make sure PCs of two sides can access to Internet**
B. **Configuring the TP-LINK VPN Router**
C. **Configuring the GreenBow VPN Client**

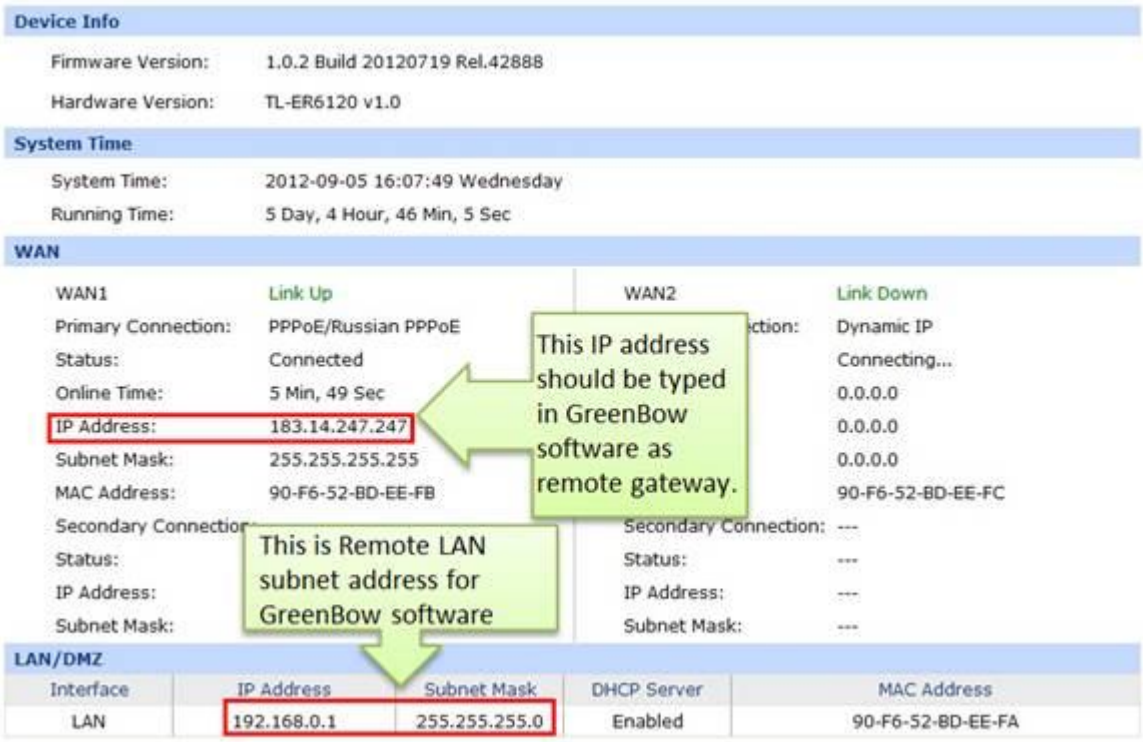
A. Make sure PCs of two sides can access to Internet

Before setup a VPN tunnel, you need to ensure that PCs of two sides are connected to the Internet. After ensuring that there is an active Internet connection on each side, you need to verify the VPN settings of the two sides, please follow the instruction below.

B. Configuring the TP-LINK VPN Router

Step 1:

Access the router's management webpage, verify the settings needed on the router.

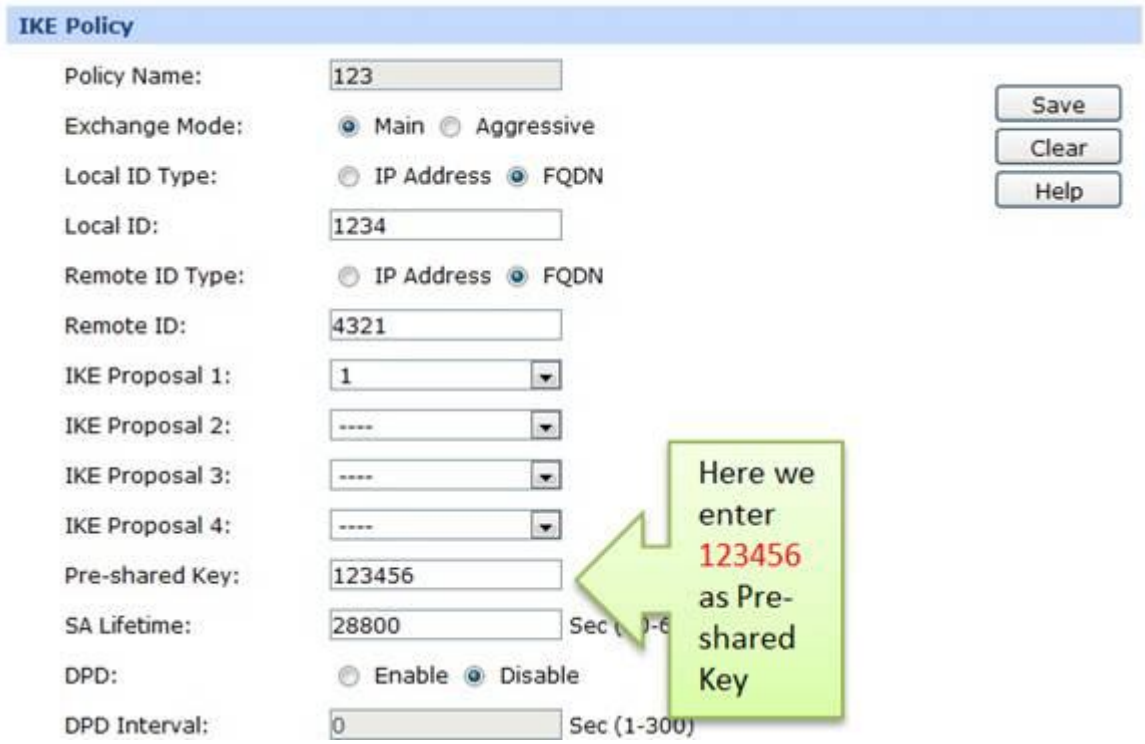


Step 2:

On the management webpage, click on VPN then IKE Proposal. Under IKE Proposal, enter Proposal Name whatever you like, select Authentication, Encryption and DH Group, we use MD5, 3DES, DH2 in this example.

Step 3:

Click on IKE Policy, enter Policy Name whatever you like, select Exchange Mode, in this example we use Main, select FQDN as ID Type and enter Local ID and Remote ID whatever you like, here we enter “1234” for Local ID and “4321” for Remote ID.



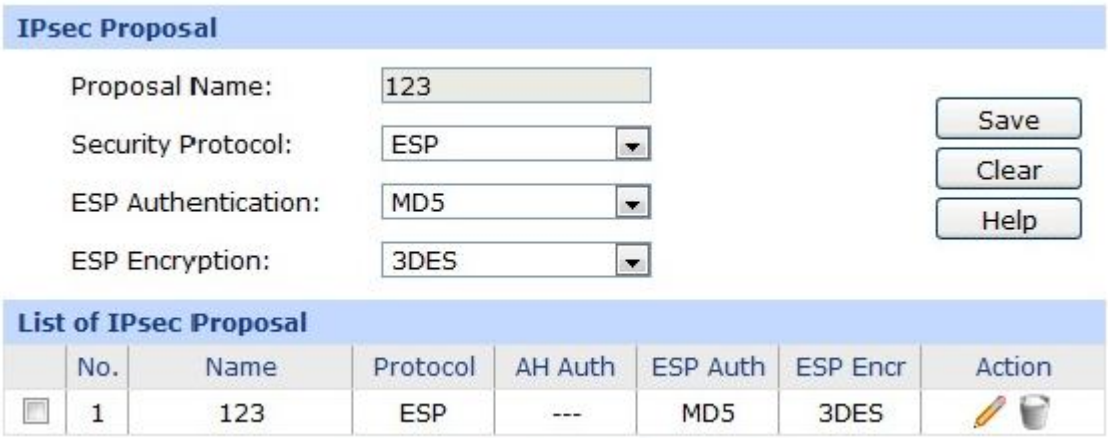
NOTE: No matter on Main mode or Aggressive mode, once the client PC is behind a NAT device, we have to select FQDN as ID Type and the NAT device must support VPN passthrough, otherwise the VPN tunnel can't be established.

Step 4:

Under IKE Proposal 1, we select 1 in this example. Enter Pre-shared Key and SA Lifetime you want, DPD is disabled.

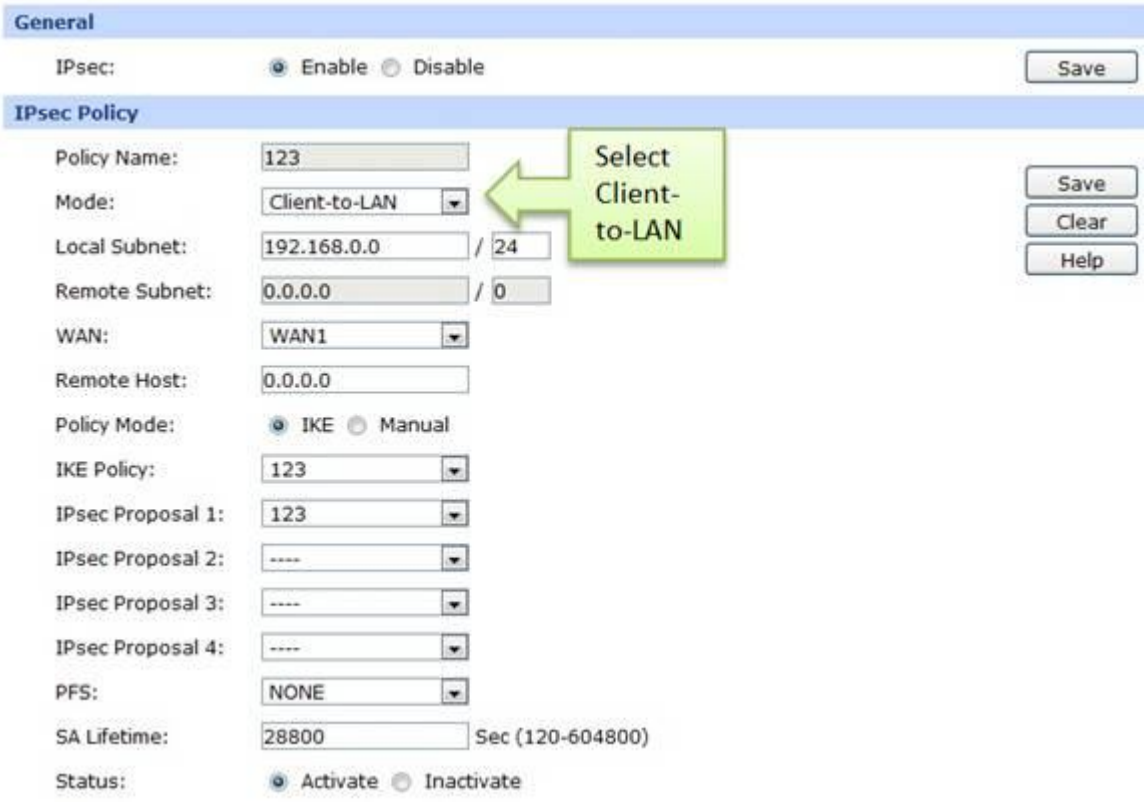
Step 5:

Click on IPsec on the left menu, then IPsec Proposal. Select Security Protocol, ESP Authentication and ESP Encryption you want to enable on VPN tunnel. Here we use ESP, MD5 and 3DES for example.



Step 6:

Click on IPsec Policy, enter Policy Name whatever you like, the Mode should be Client-to-LAN. Enter Local Subnet and select WAN port.



Step 7:

Look for Policy Mode and select IKE. Under IKE Policy, we select 123 which is used. Under IPsec Proposal, we use 123 in this example.

Step 8:

Look for PFS, we set NONE here, under SA Lifetime, enter “28800” or the period you want. Look for Status then select Activate.

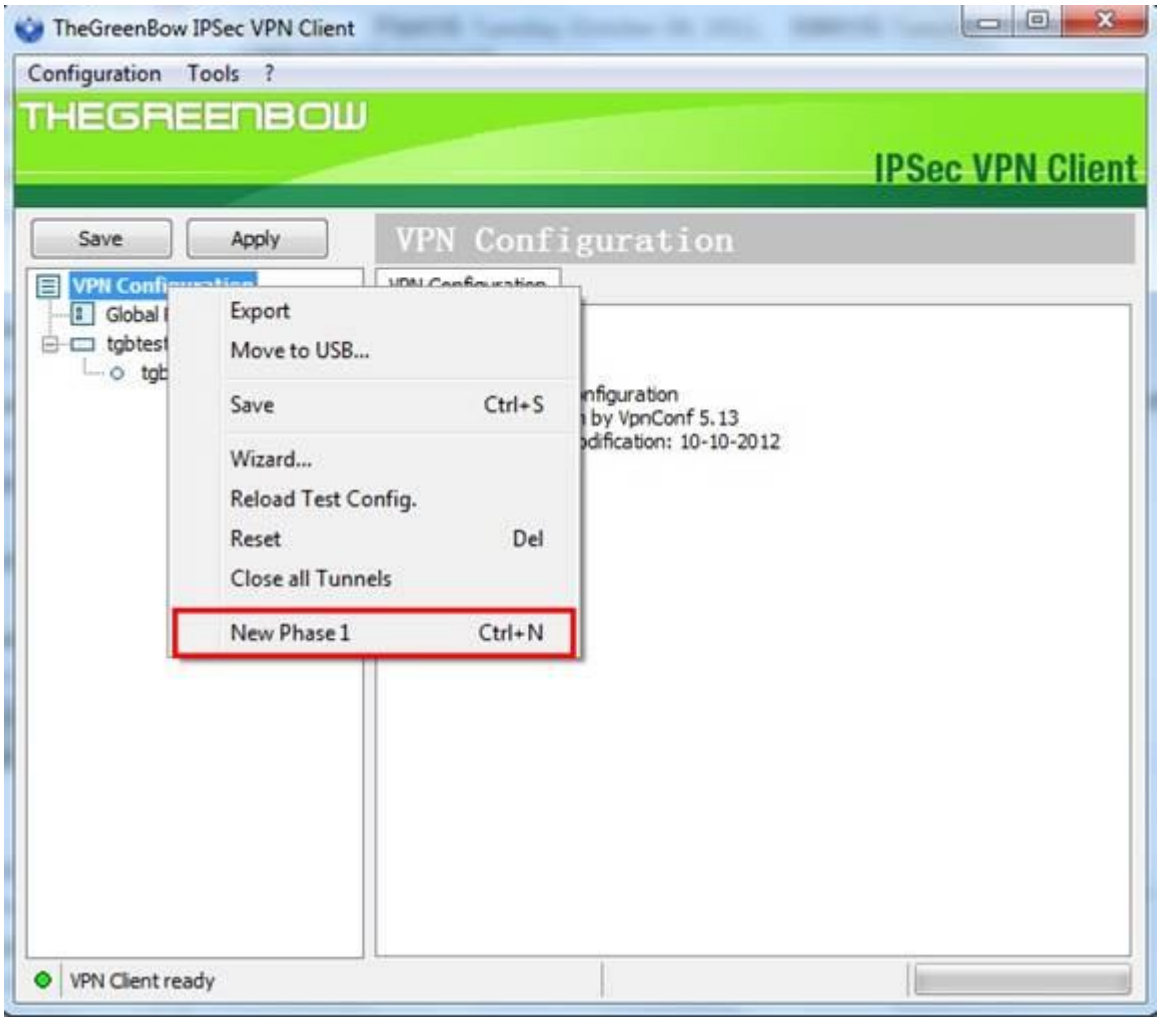
Step 9:

Enable IPsec and then click on Save.

C. Configuring the GreenBow VPN Client

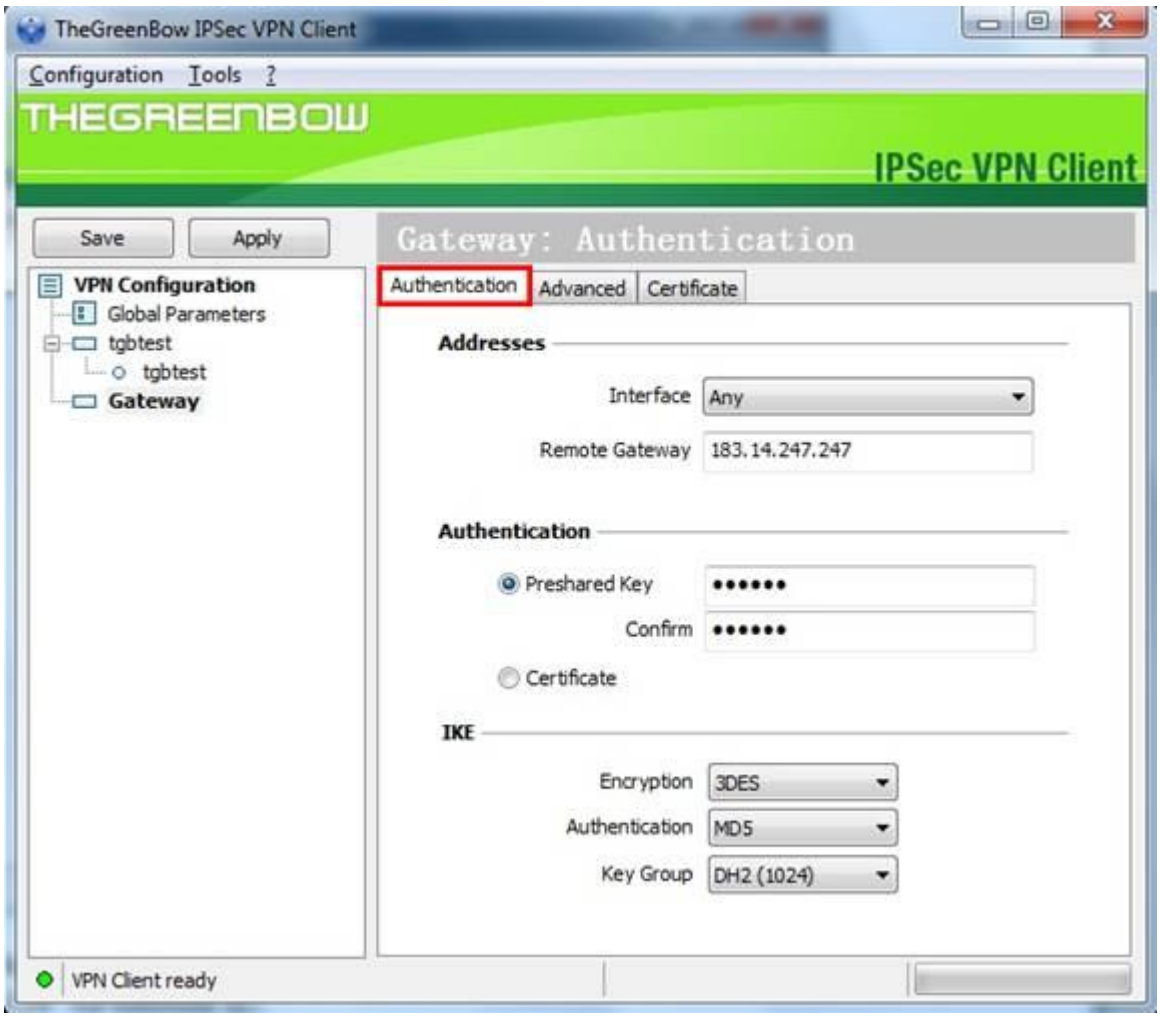
Step 1:

Right click on VPN Configuration and click on New Phrase 1.



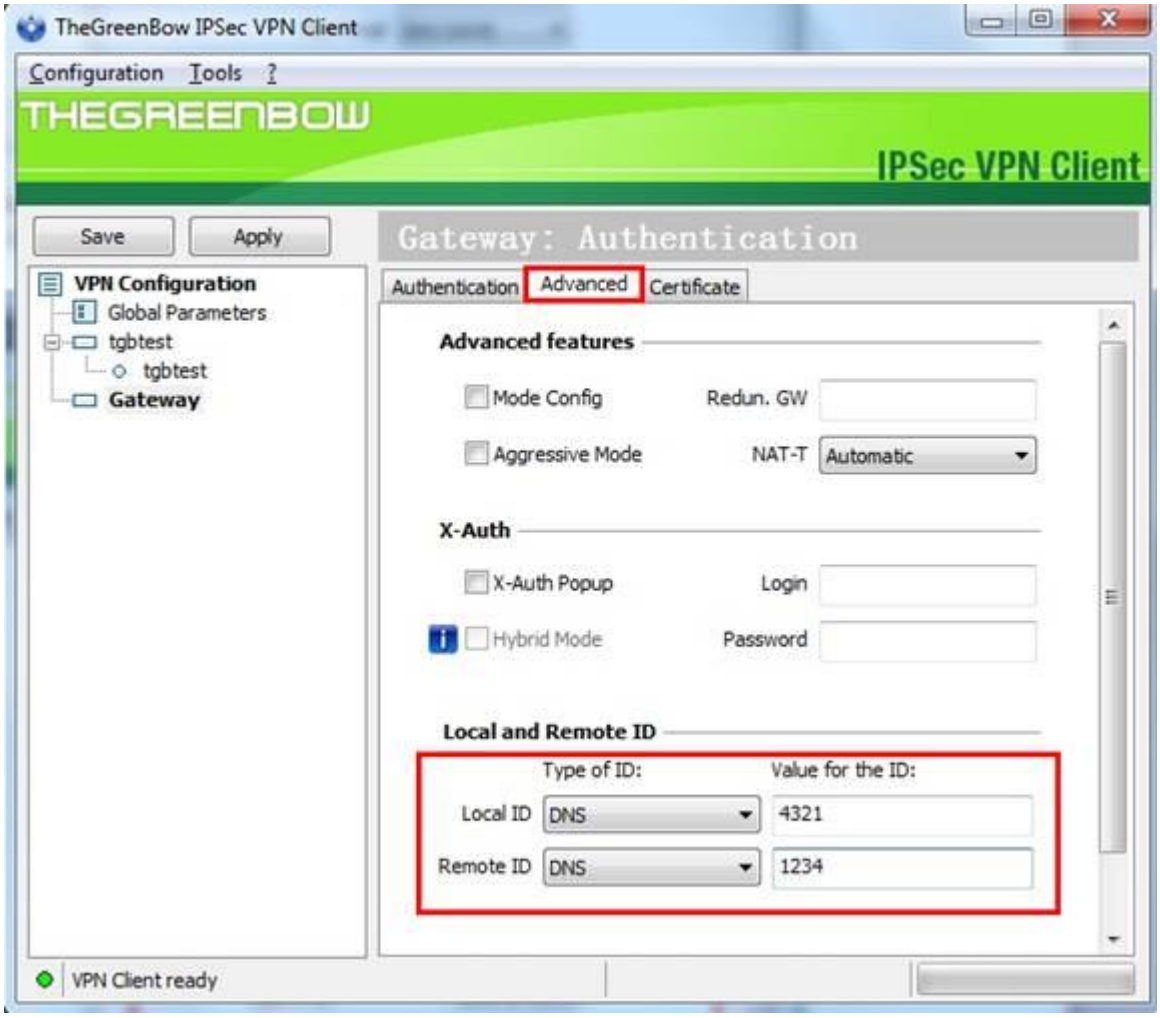
Step 2:

Under Remote Gateway, enter the router's WAN IP address, the Pre-shared Key should be the same with router's, it is "123456".on IKE section, the Encryption, Authentication and Key Group are the same with router's, we use 3DES, MD5and DH2 here.



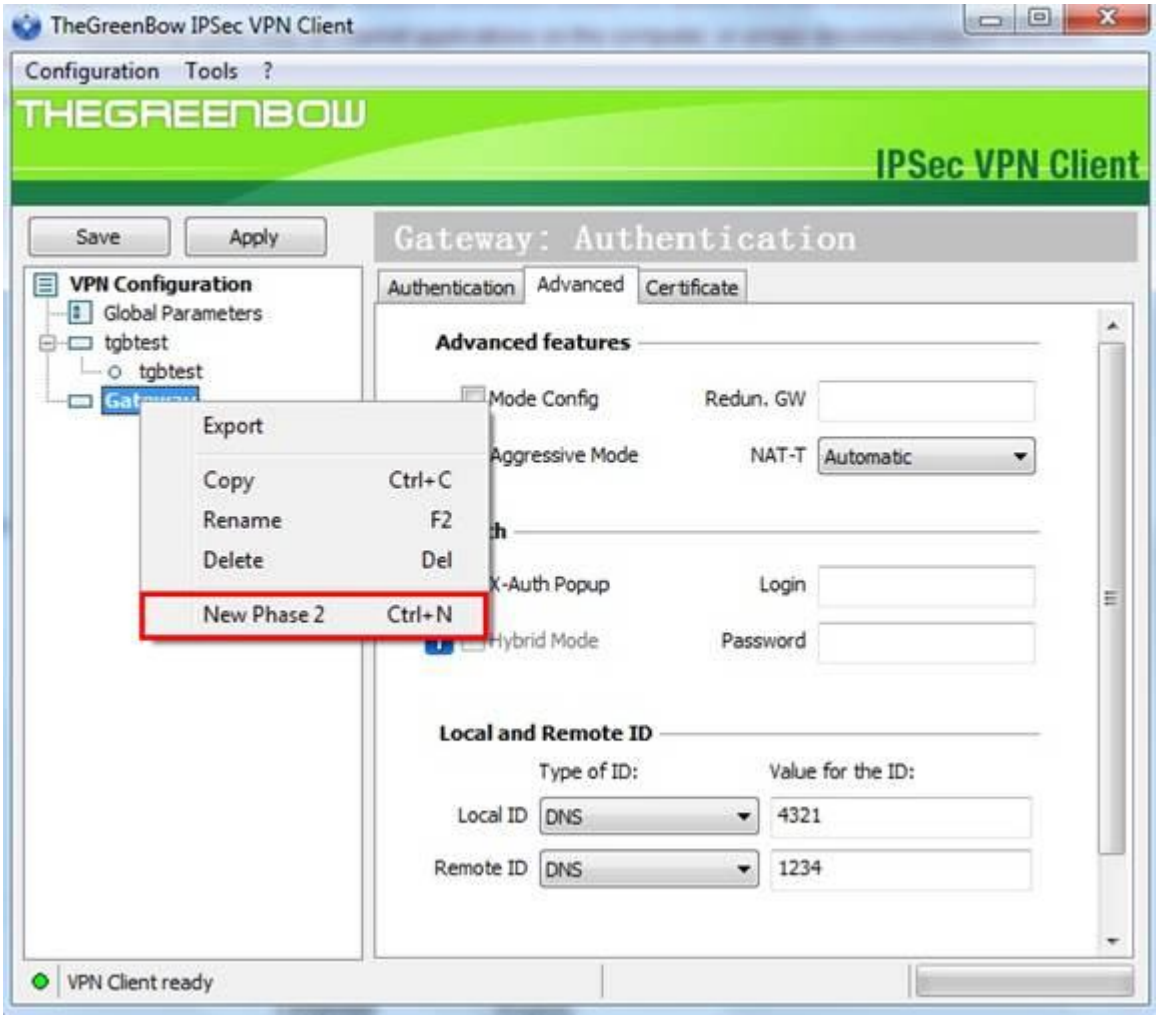
Step 3:

Go to Advanced tab, select DNS as Type of ID, and then enter "4321" for Local ID and "1234" for Remote ID.



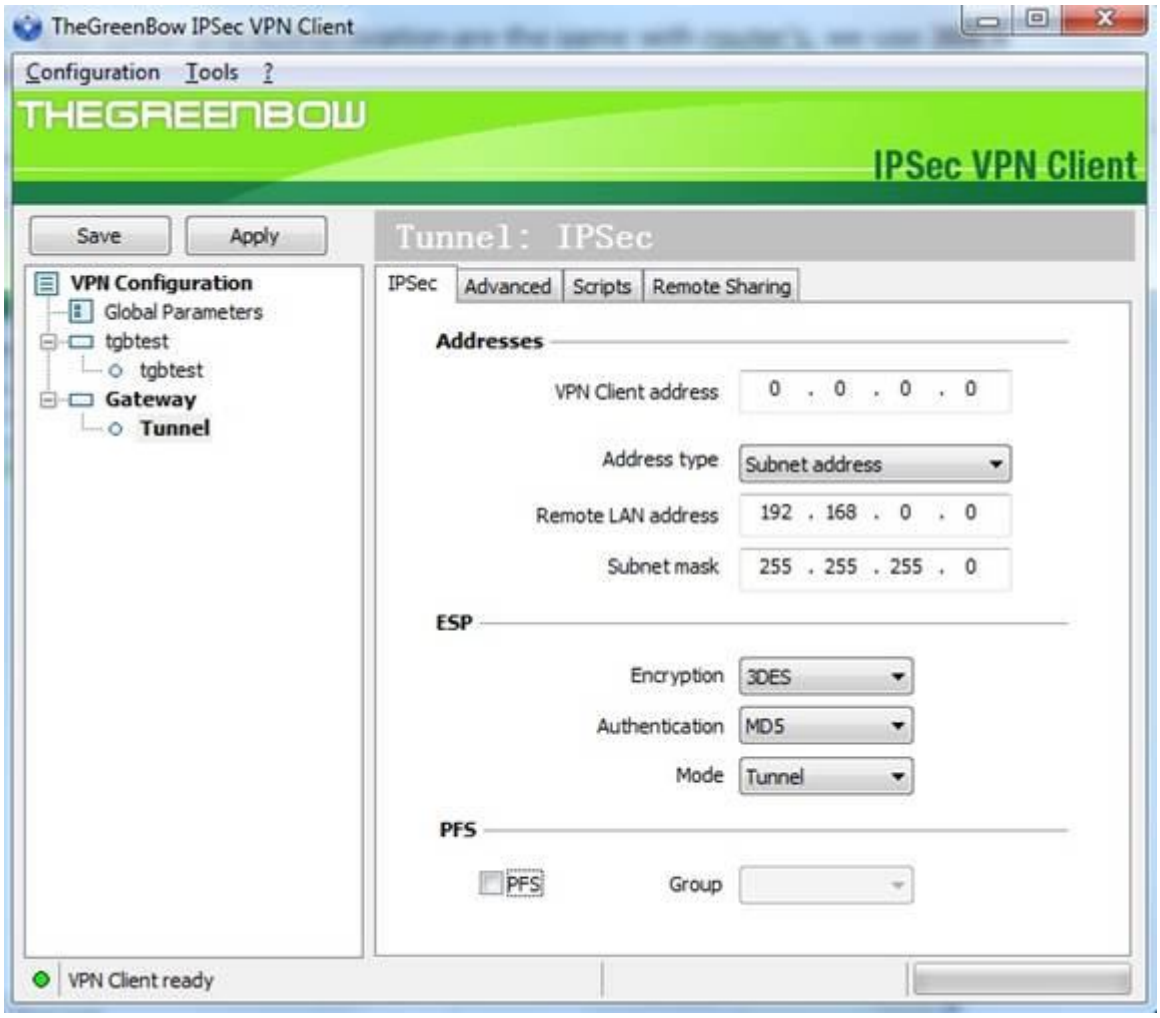
Step 4:

Right click on Phase 1, add a new phrase 2.



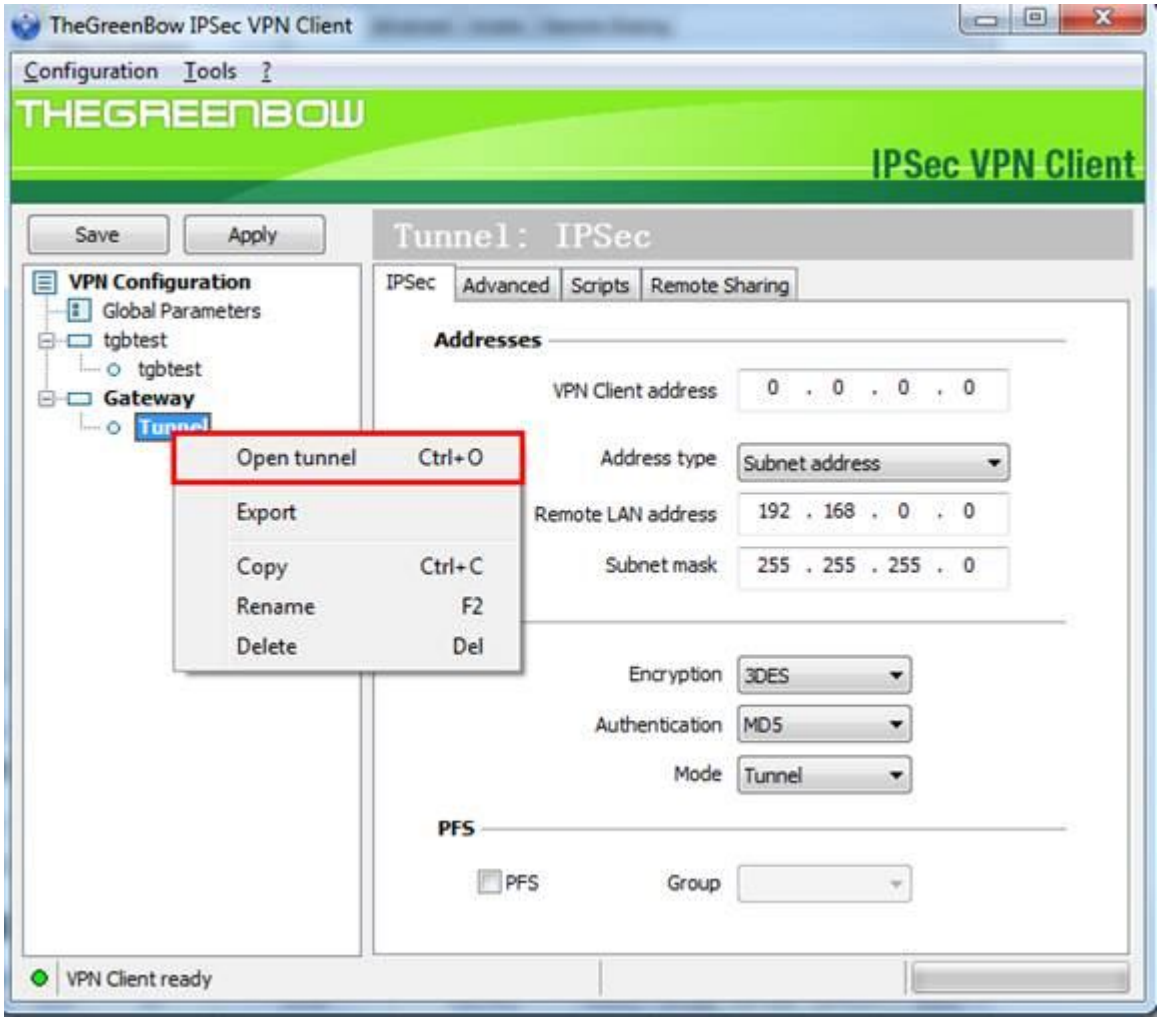
Step 5:

Enter remote LAN address and Subnet mask, in the example, the IP address is 192.168.0.0, Subnet mask is 255.255.255.0. Encryption and Authentication are the same with routers; we use 3DES and MD5 here. The Mode should be Tunnel.



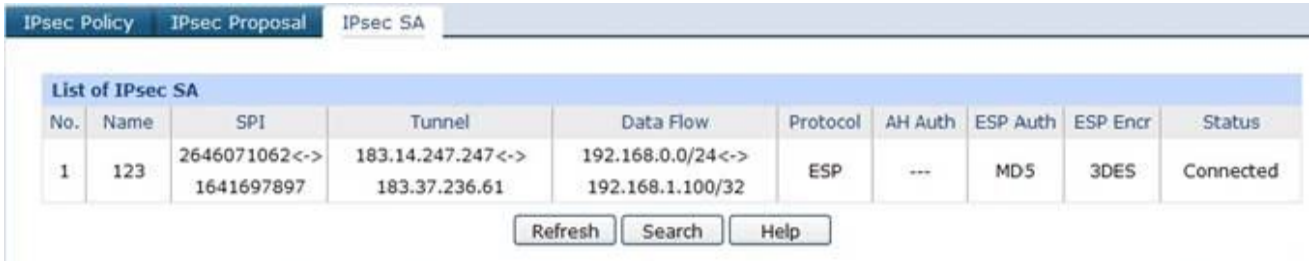
Step 6:

Click Save and Apply and then right click on Phrase 2(Tunnel), click on Open Tunnel.



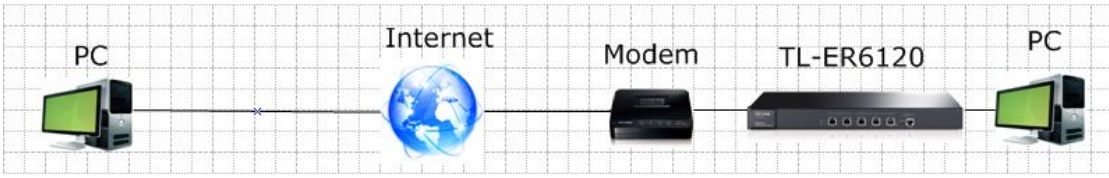
Step 7:

If the client connect to the VPN Server successfully, you can see IPsec SA on the list.



4. How to configure Shrew Soft VPN IPsec Client with TP-LINK Router

Suitable for: TL-ER6120, TL-ER6020, TL-ER604W



Shrew Soft VPN IPsec Client is an VPN Client software developed by Shrew Soft Inc. It can be downloaded from official website of Shrew Soft(https://www.shrew.net/download/vpn).

To set up an IPsec VPN tunnel, you need to perform the following steps:

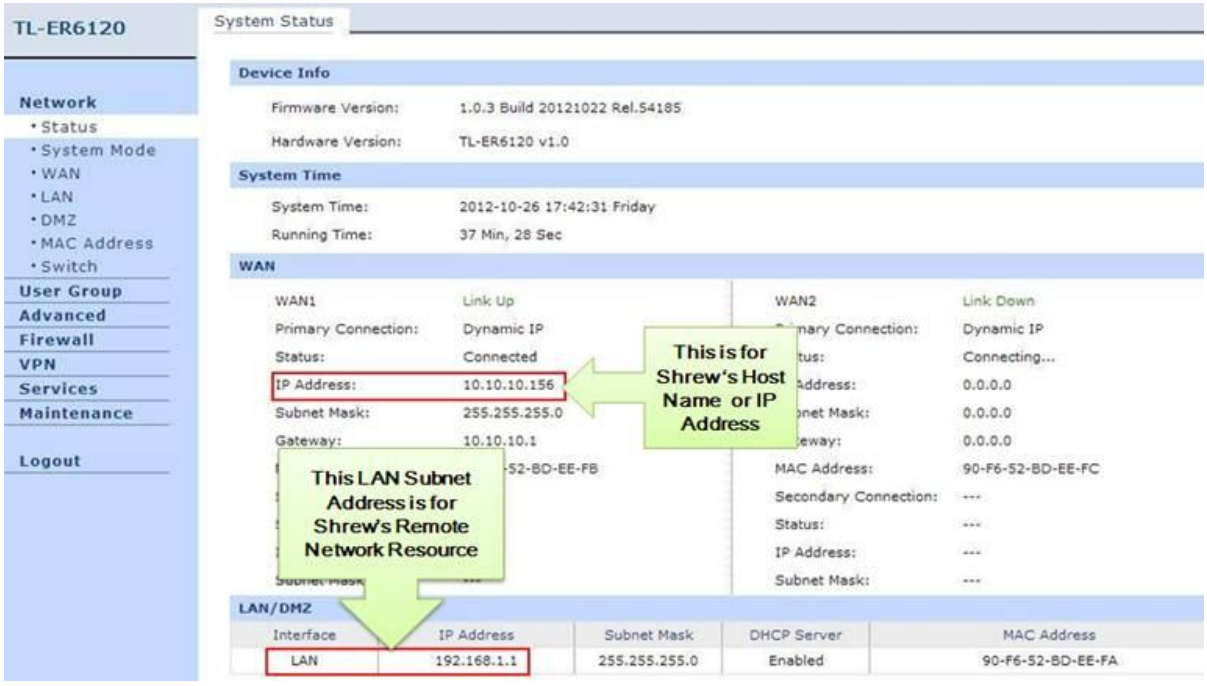
A. **Make sure PCs of two sides can access to Internet**
B. **Configuring IPsec VPN settings on TL-ER6120**
C. **Configuring the Shrew VPN Client**

A. Make sure PCs of two sides can access to Internet

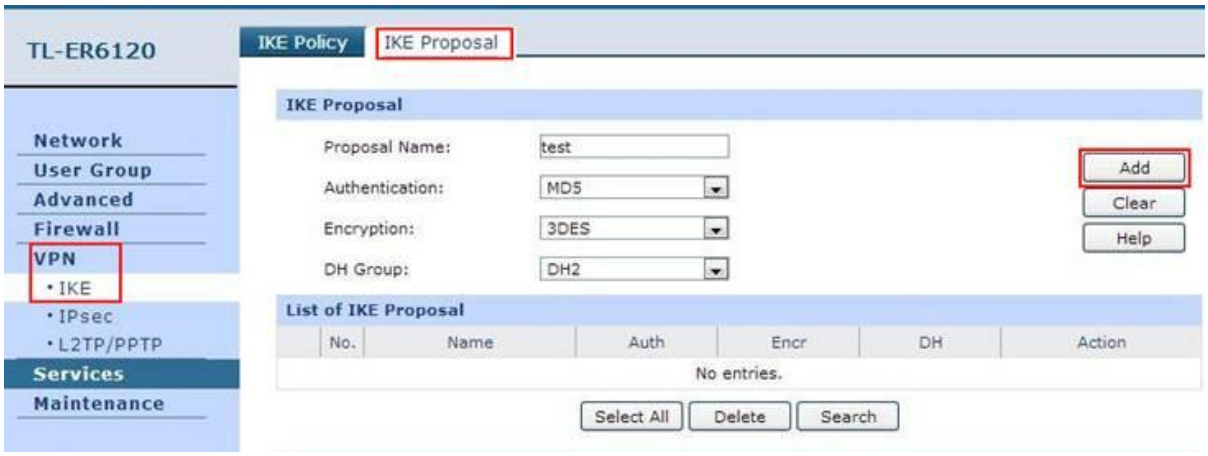
Before setup a VPN tunnel, you need to ensure that PCs of two sides are connected to the Internet. After ensuring that there is an active Internet connection on each side, you need to verify the VPN settings of the two sides, please follow the instruction below.

B. Configuring IPsec VPN settings on TL-ER6120

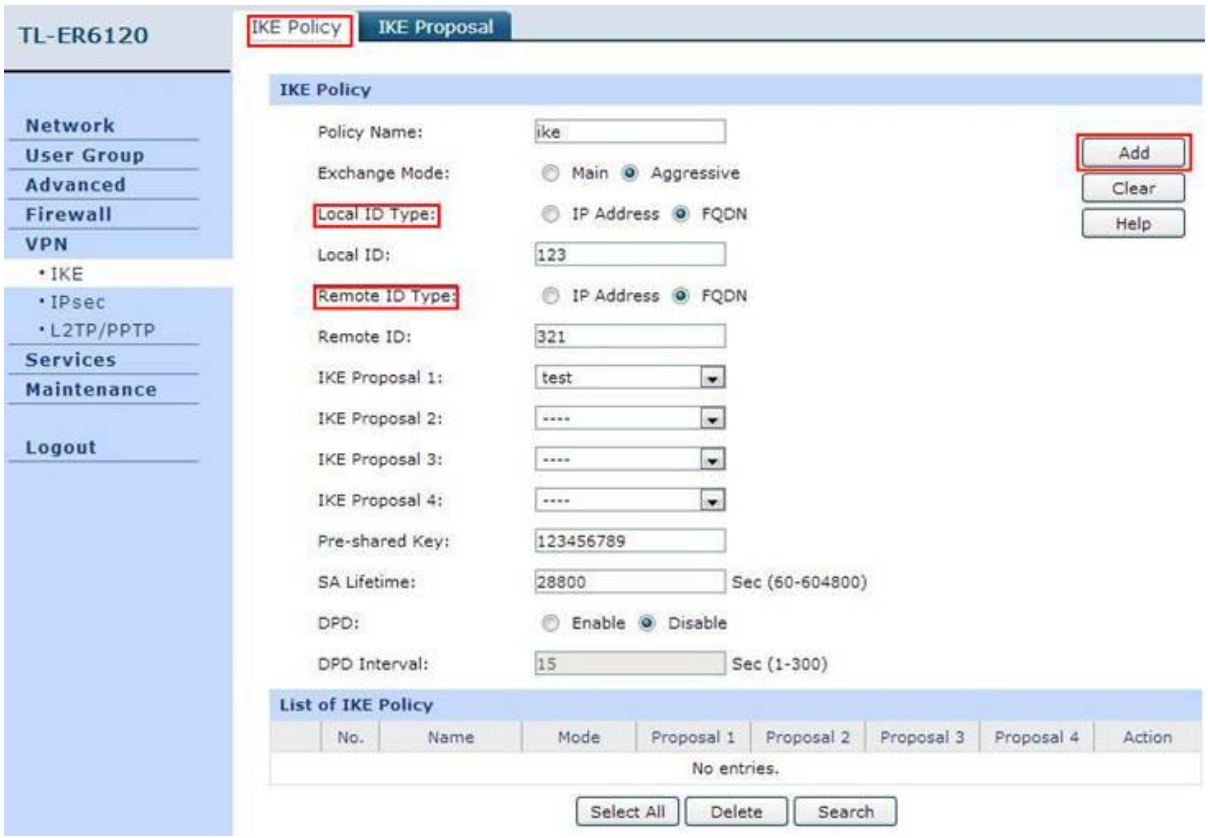
Step 1: Access the router's management webpage; verify the settings needed on the router.



Step 2: On the management webpage, click on VPN then IKE Proposal. Under IKE Proposal, enter Proposal Name whatever you like, select Authentication, Encryption and DH Group, we use MD5, 3EDS, DH2 in this example. Click on Add.



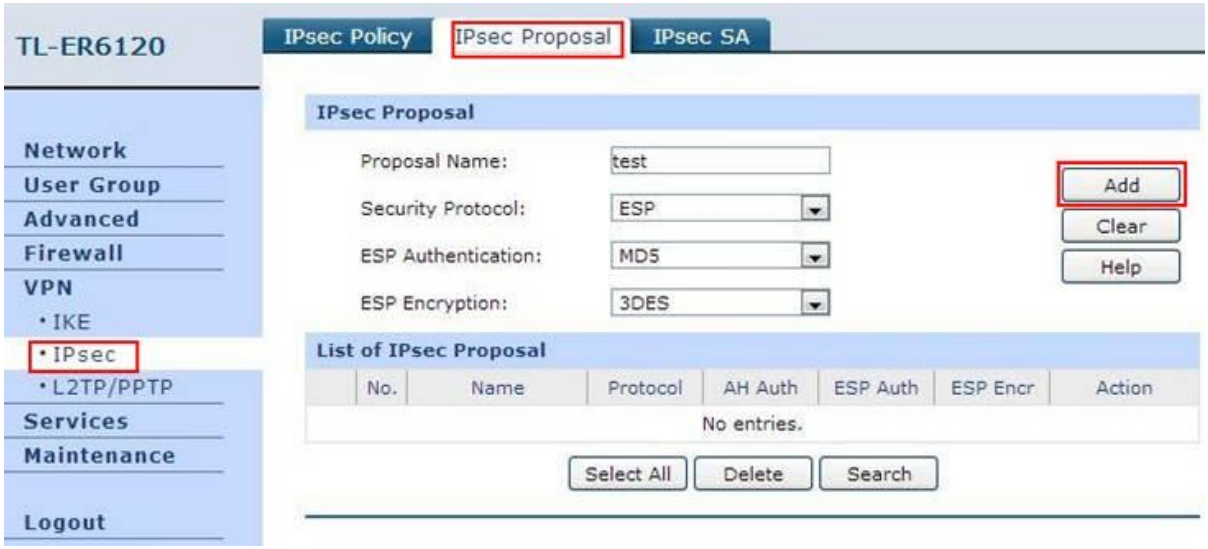
Step 3: Click on IKE Policy, enter Policy Name whatever you like, we select Aggressive for Exchange Mode, select FQDN as ID Type and enter Local ID whatever you like, here we enter “123” for Local ID and “321” for Remote ID.



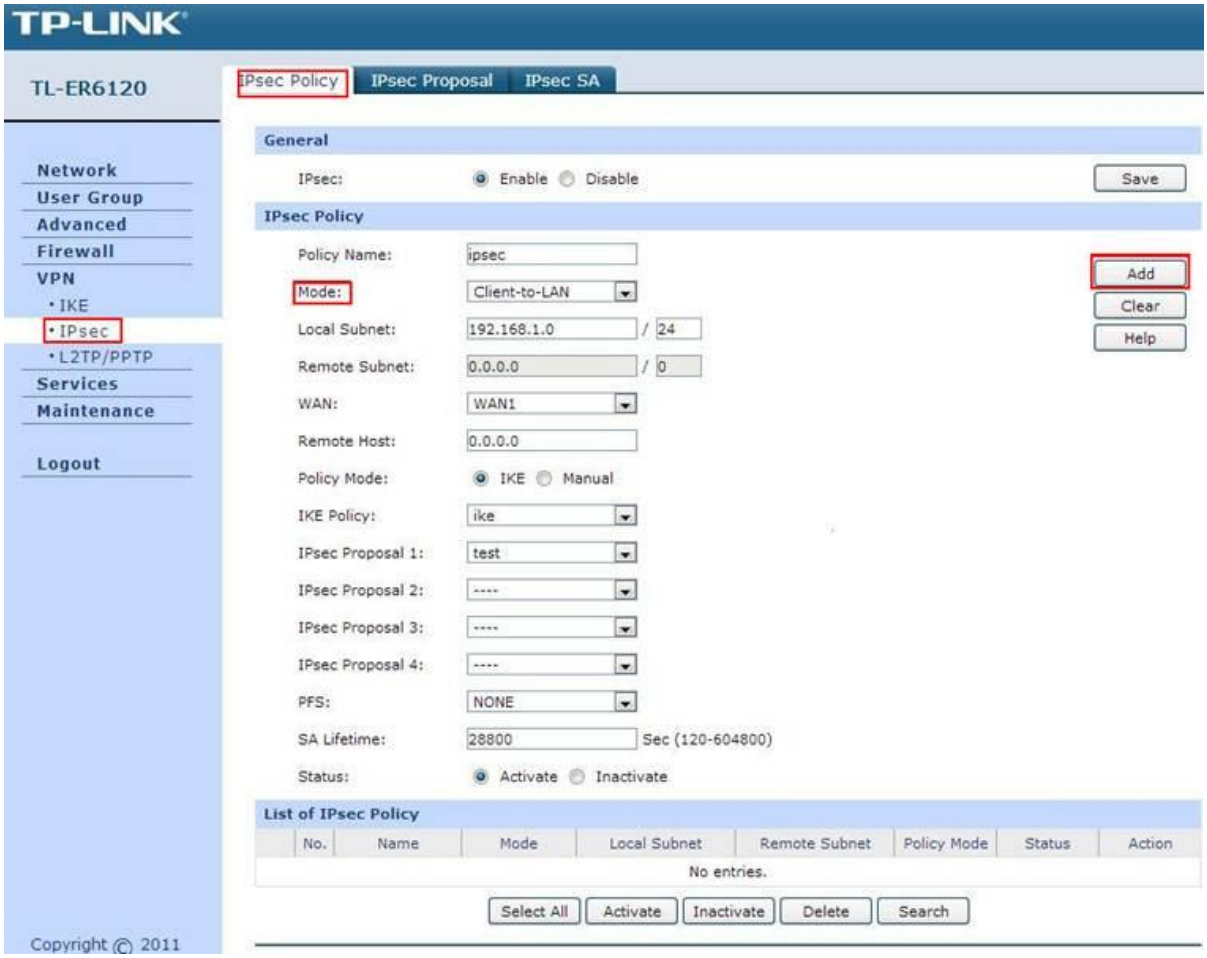
NOTE: No matter on Main mode or Aggressive mode, once the client PC is behind a NAT device, we have to select FQDN as ID Type and the NAT device must support VPN passthrough, otherwise the VPN tunnel can't be established.

Step 4: Under IKE Proposal 1, we select test in this example. Enter Pre-shared Key and SA Lifetime you want, DPD is disabled. Click on Add.

Step 5: Click on IPsec on the left menu, then IPsec Proposal. Select Security Protocol, ESP Authentication and ESP Encryption you want to enable on VPN tunnel. Here we use ESP, MD5 and 3DES for example. Click on Add.



Step 6: Click on IPsec Policy, enter Policy Name whatever you like, the Mode should be Client-to-LAN. Enter Local Subnet and select WAN port.



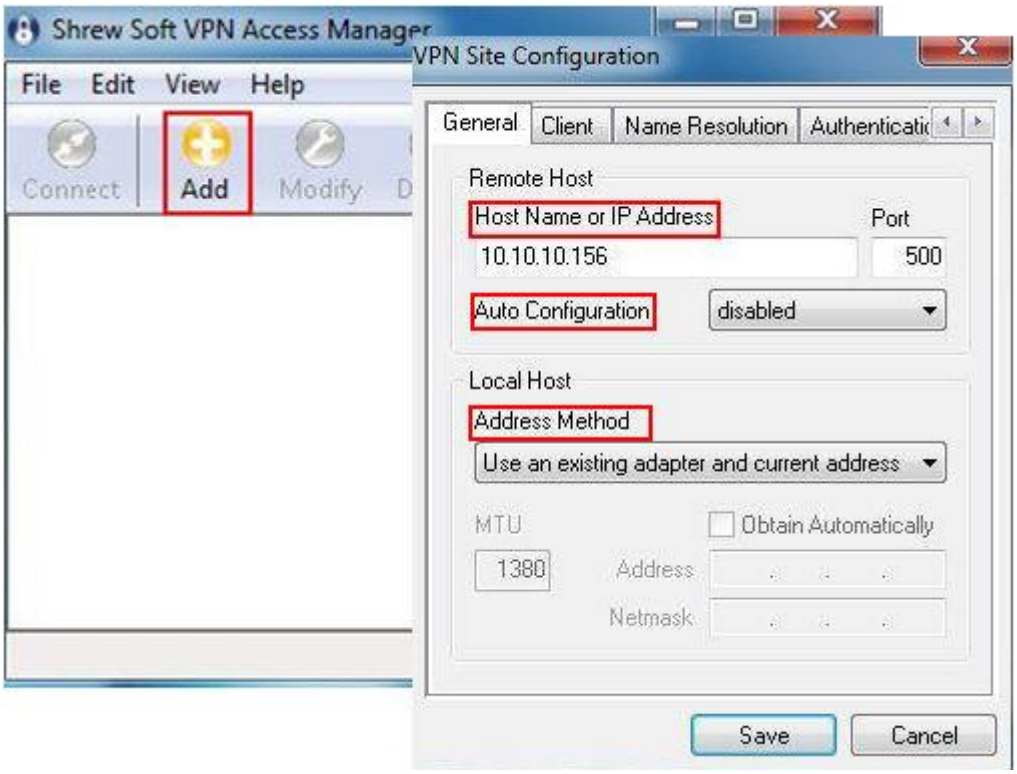
Step 7: Look for Policy Mode and select IKE. Under IKE Policy, we select ike which is used. Under IPsec Proposal, we use test in this example.

Step 8: Look for PFS, we set NONE here, under SA Lifetime, enter “28800” or the period you want. Look for Status then select Activate.

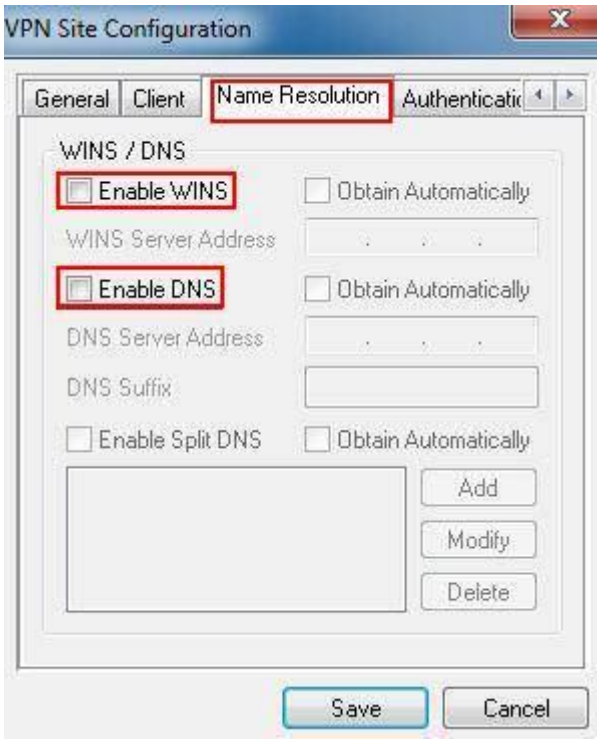
Step 9: Enable IPsec and then click on Add.

C. Configuring the Shrew VPN Client

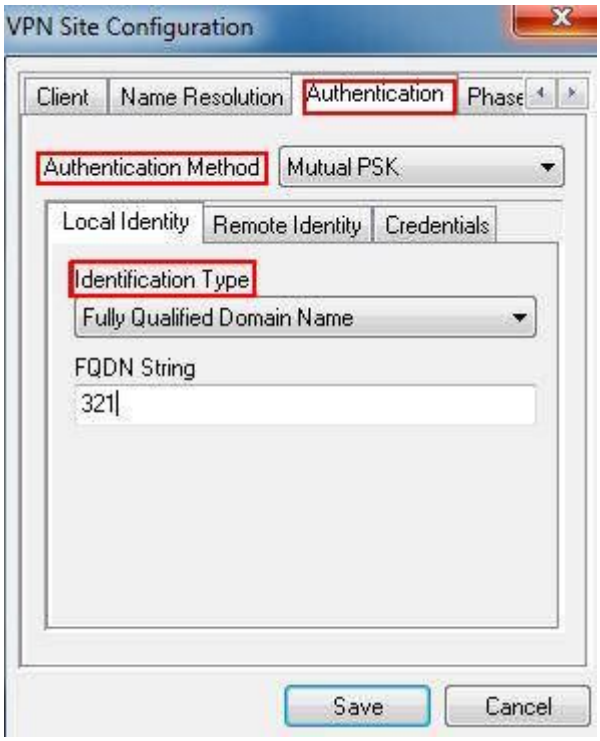
Step 1: Click on Add. Under Host Name or IP Address, enter the TL-ER6120’s WAN IP address, select disable for Auto Configuration. Under Address Method, we select Using an existing adapter and current address.



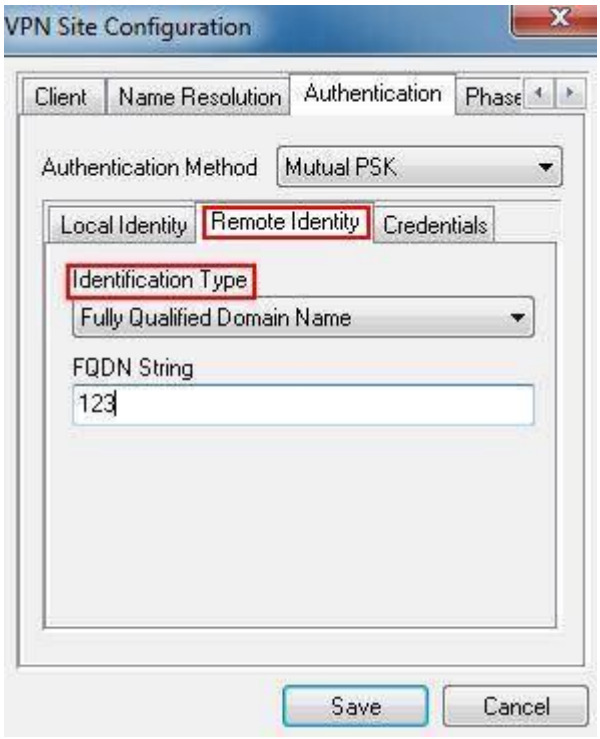
Step 2: Click on Name Resolution on the top menu, don’t tick the Enable WINS and Enable DNS.



Step 3: Click on Authentication on the top menu, select Mutual PSK as Authentication. Under Identification Type, select Fully Qualified Domain Name and enter “321” for FQDN String.

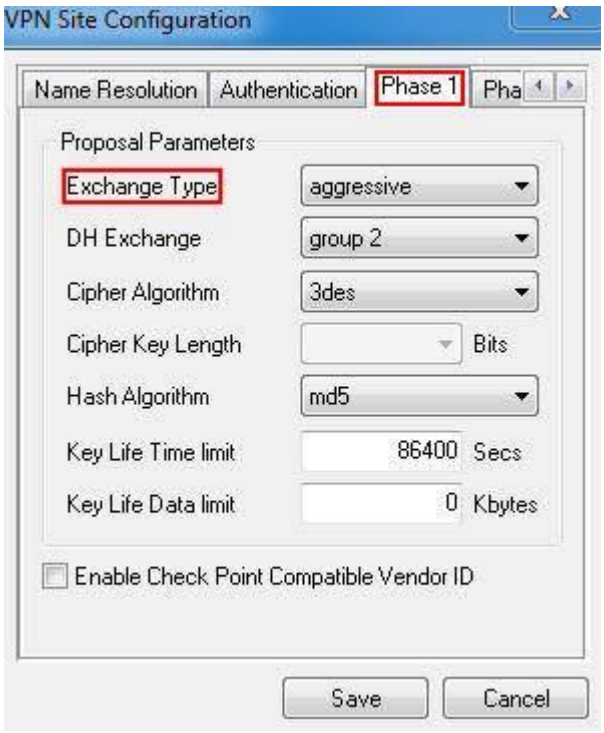


Step 4: Click on Remote Identity, select Fully Qualified Domain Name as Identification Type and enter “123” for FQDN String.

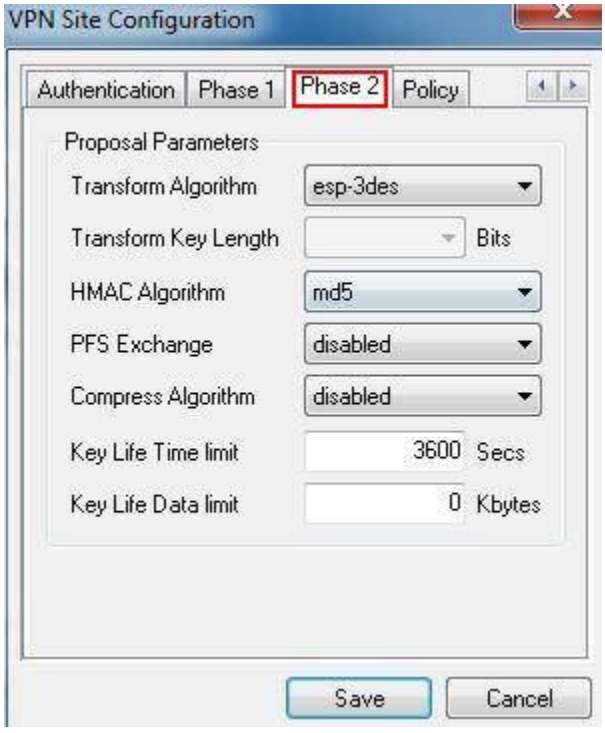


Step 5: Click on Credentials, the Pre Shared Key, should be the same as the Pre-shared Key on the TL-ER6120, it's "123456789".

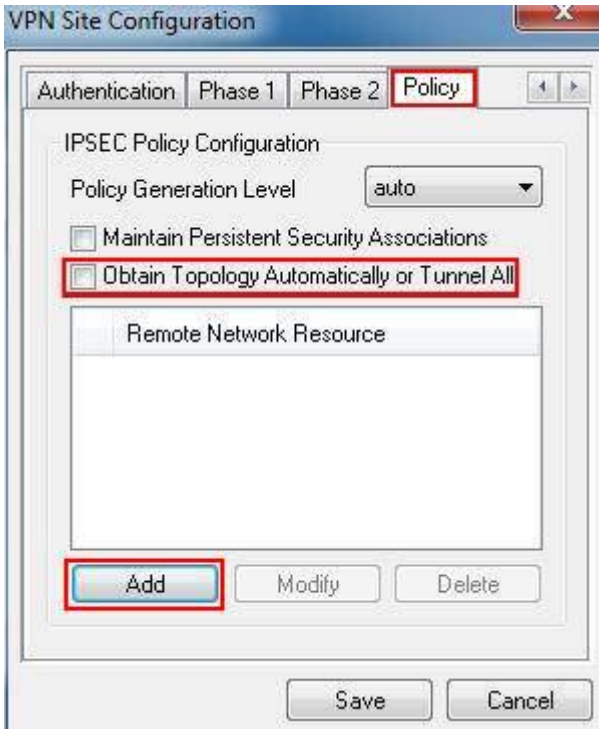
Step 6: Click on Phase 1, under the Proposal Parameters, the Exchange Type, DH Exchange, Cipher Algorithm, and Hash Algorithm are the same with TL-ER6120's, we use aggressive, group 2, 3des, md5 here.



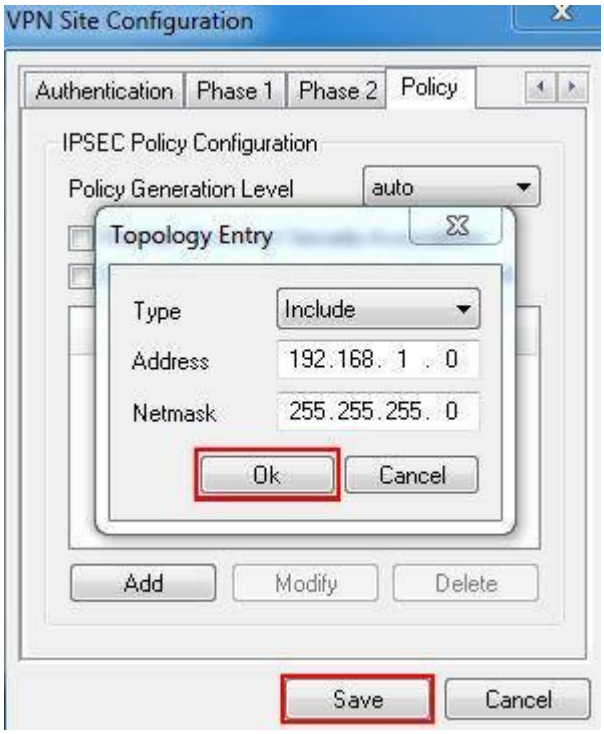
Step 7: Click on Phase 2, under the Proposal Parameters, the Transform Algorithm, HMAC Algorithm are the same with TL-ER6120's we use esp-3des, md5 here. PFS Exchange and Compress Algorithm are disabled.



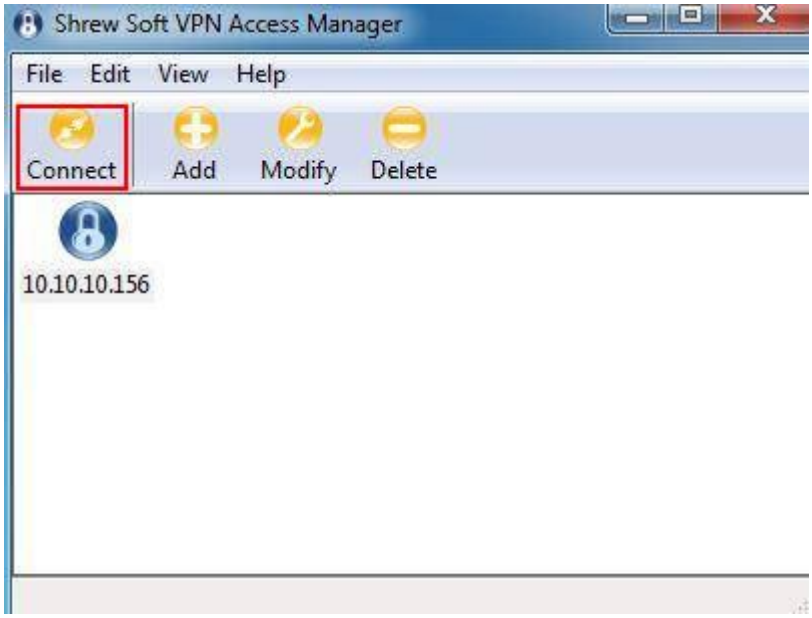
Step 8: Click on Policy, don't tick Obtain Topology Automatically or Tunnel All. Then click on Add.



Step 9: Select Include as Type, enter the TL-ER6120's LAN Subnet Address and Subnet Mask, it's 192.168.1.0, 255.255.255.0. Then click on OK and Save.

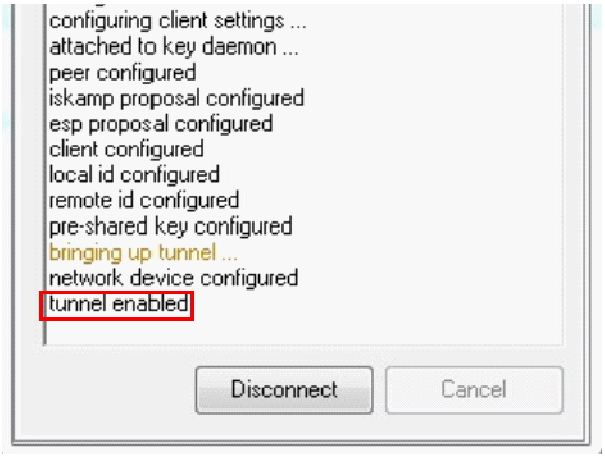


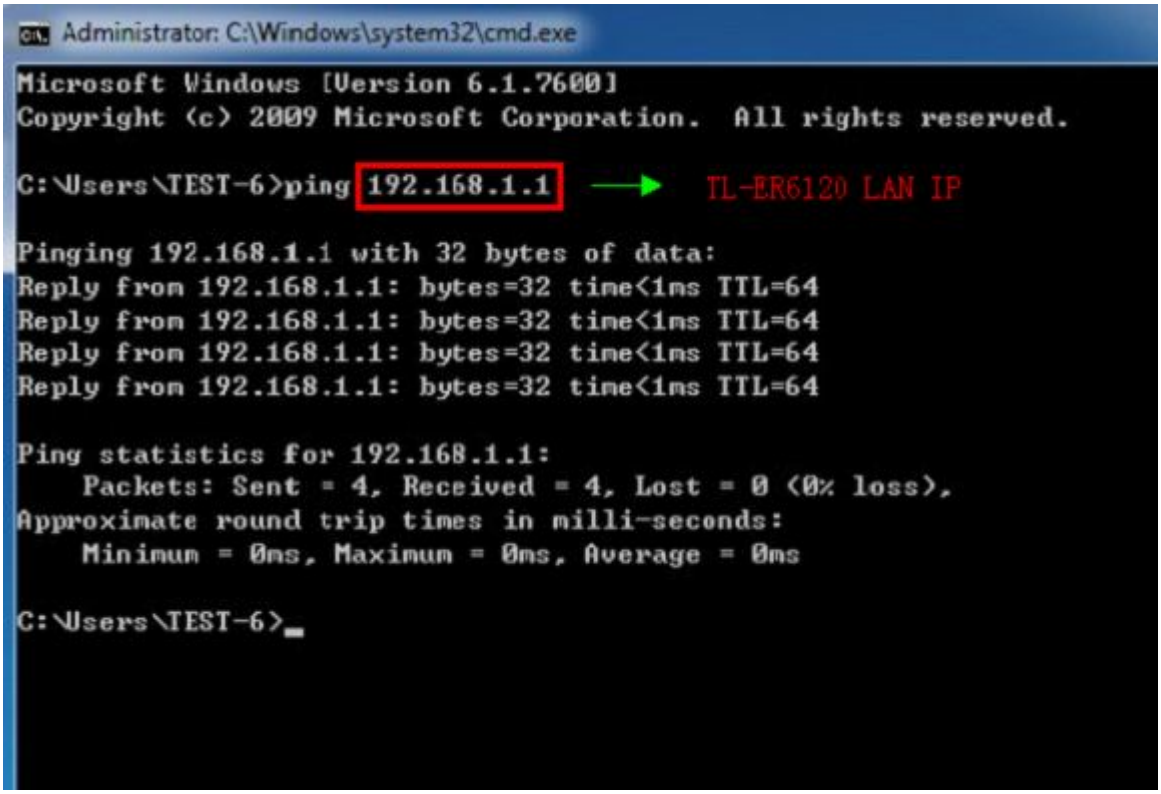
Step 10: Click on Connect.



Step 11: Click on Connect.

Step 12: After Shrew Soft VPN show tunnel enabled as the followings, you need ping TL-ER6120 LAN IP.





Step 13: If client connect to the VPN Server successfully, you can see IPsec SA on the list.

5. How to configure LAN-to-LAN L2TP/PPTP VPN on TP-LINK Router

Suitable for: TL-ER6120, TL-ER6020, TL-ER604W

LAN-to-LAN L2TP/PPTP VPN connection is established between two VPN routers. To configure LAN-to-LAN L2TP/PPTP VPN on TL-LINK Routers, please follow the instructions below:

A. Connecting the devices together
B. Verify the settings needed for L2TP/PPTP VPN on Router
C. Configuring a L2TP/PPTP Server on TP-LINK router(Router A)
D. Configuring a L2TP/PPTP Client on TP-LINK router(Router B)

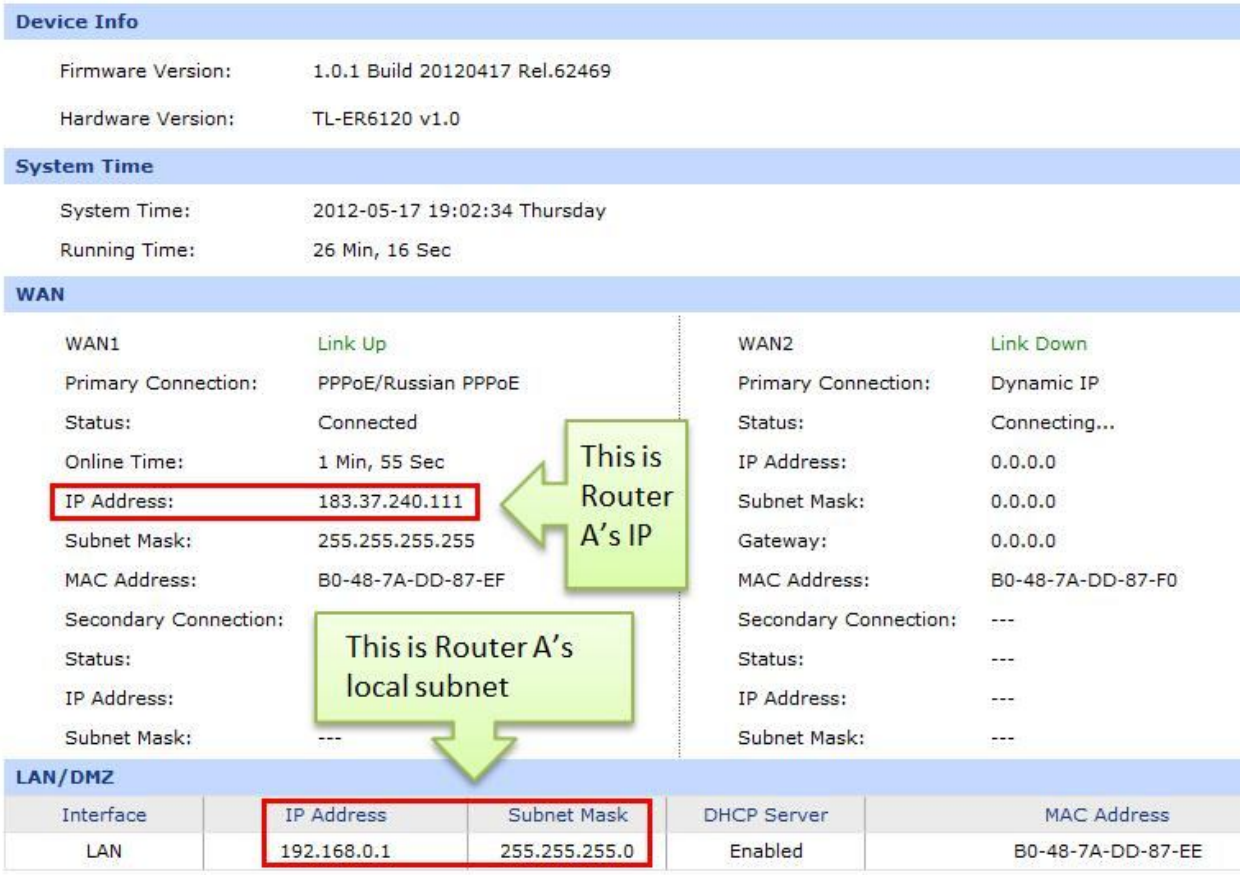
NOTE: We give the guide to configure LAN-to-LAN PPTP VPN in this example, the way to configure LAN-to-LAN L2TP VPN is similar. If the TP-LINK Router configured as PPTP Server is behind a NAT device, Virtual Server or DMZ should be configured on the NAT device, otherwise the VPN tunnel can't be established.

A. Connecting the devices together

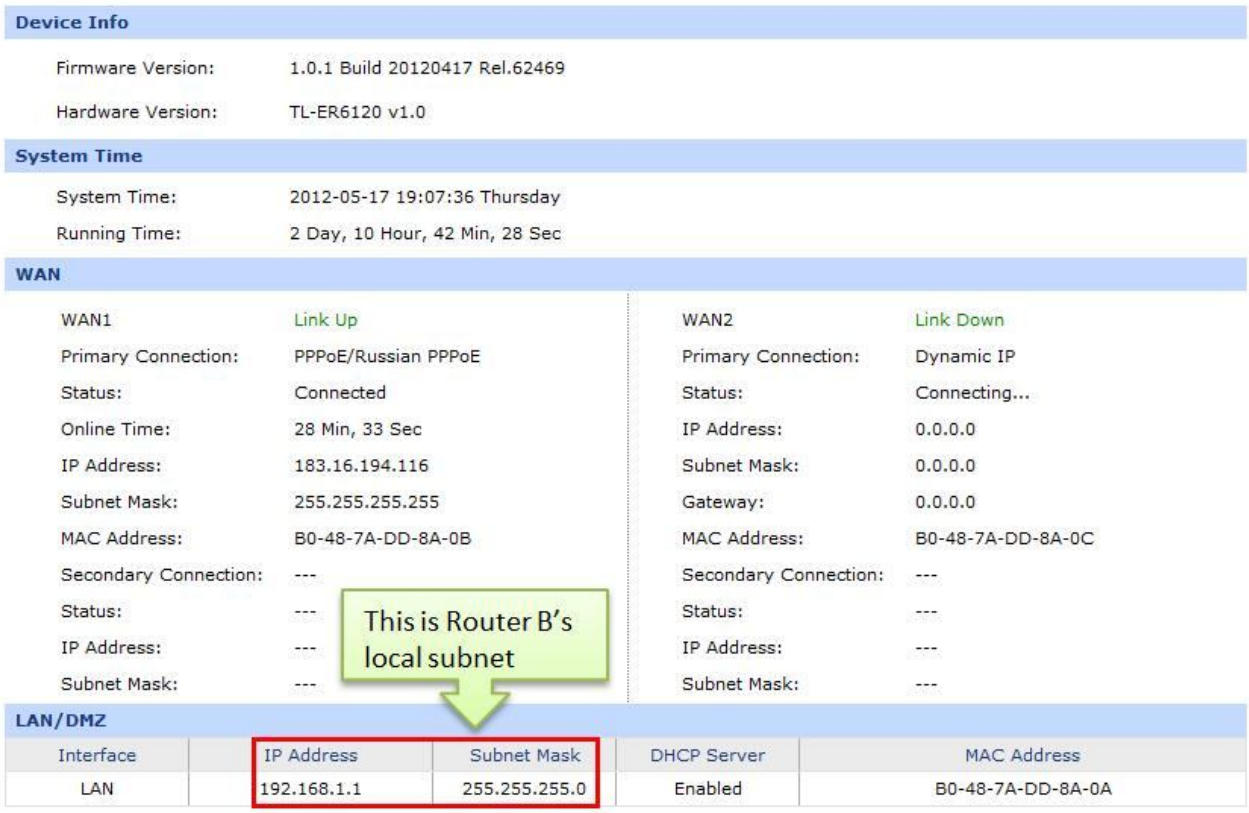
Before setup a VPN tunnel, you need to ensure that the two routers are connected to the Internet. After ensuring that there is an active Internet connection on each router, you need to verify the VPN settings of the two routers, please follow the instruction below.

B. Verify the settings needed for PPTP VPN on Router

Router A's Status Page:



Router B's Status Page:

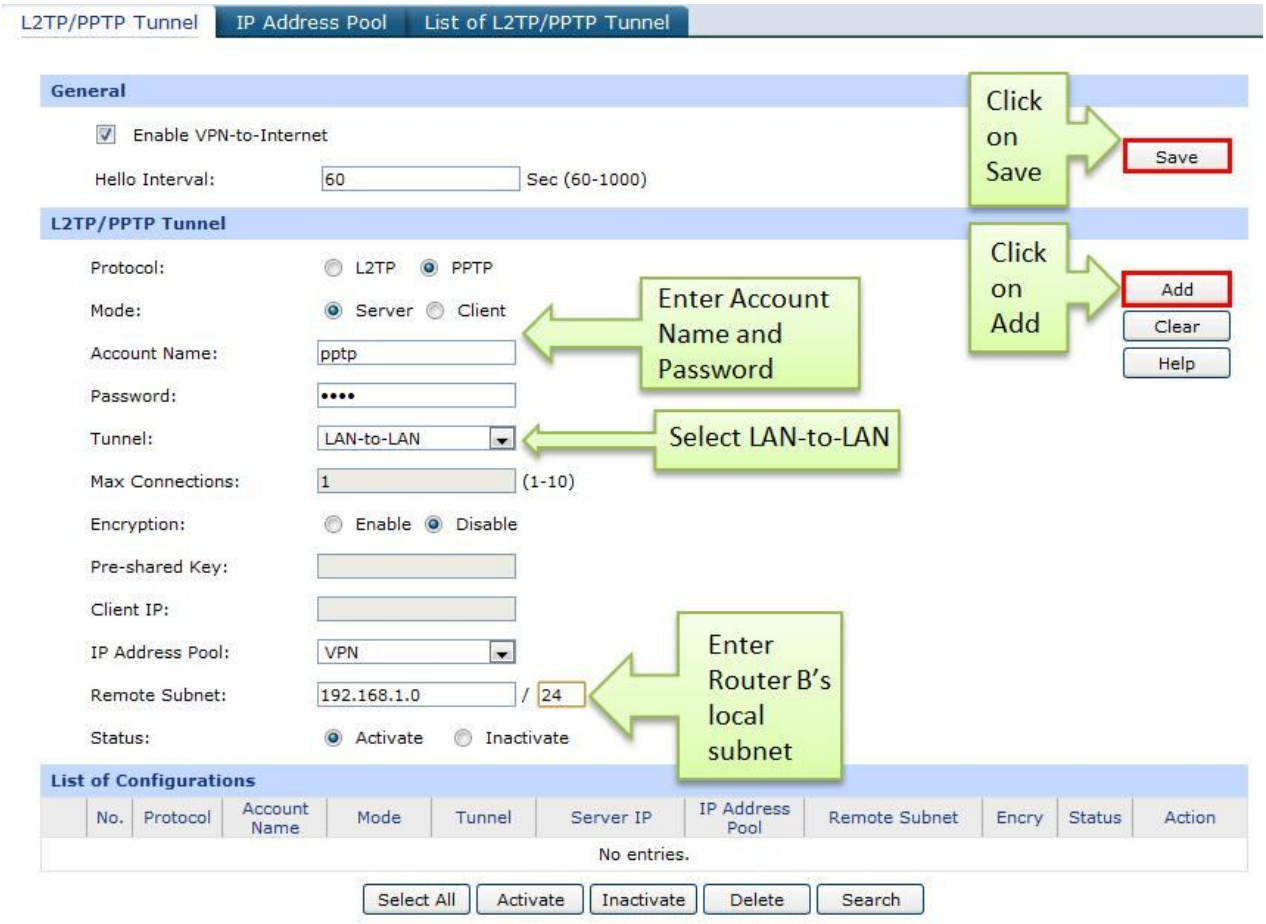


C. Configuring a PPTP Server on TP-LINK router

Step 1 : Access Router A's management page, click on VPN->L2TP/PPTP->IP Address Pool, enter Pool Name and IP Address Range, and then click on Add.

NOTE: IP Address pool must be different range from LAN IP address range.

Step 2 : Go to L2TP/PPTP Tunnel, look for protocol, select PPTP; the Mode should be Server.



Step 3 : Enter Account Name and Password whatever you like, here we use "pptp" as account name, password is "pptp".

Step 4 : Under Tunnel, select LAN-to-LAN.

Step 5 : Under IP Address Pool, select “VPN” we have added before.

Step 6 : Under Remote Subnet, enter Router B’s local subnet, we enter “192.168.1.0/24” in this example.

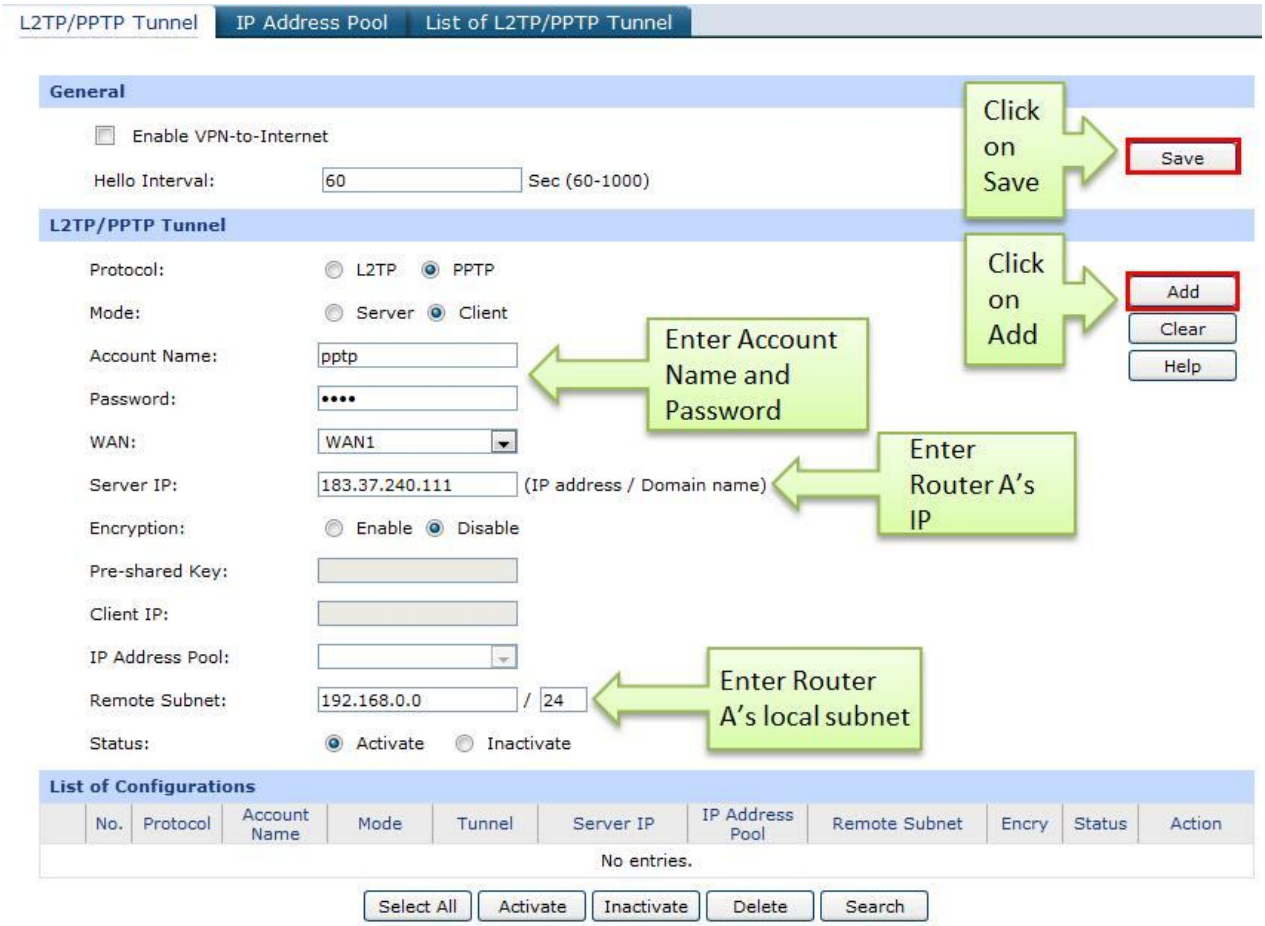
Step 7 : Look for Status, select Active.

Step 8 : Click on Add and then click on Save.

D. Configuring a PPTP client on TP-LINK Router

Step 1 : Access Router B’s management page, go to L2TP/PPTP Tunnel, look for protocol, select PPTP; the Mode should beClient.

Step 2 : Enter “pptp” as Account Name and “pptp” as Password.



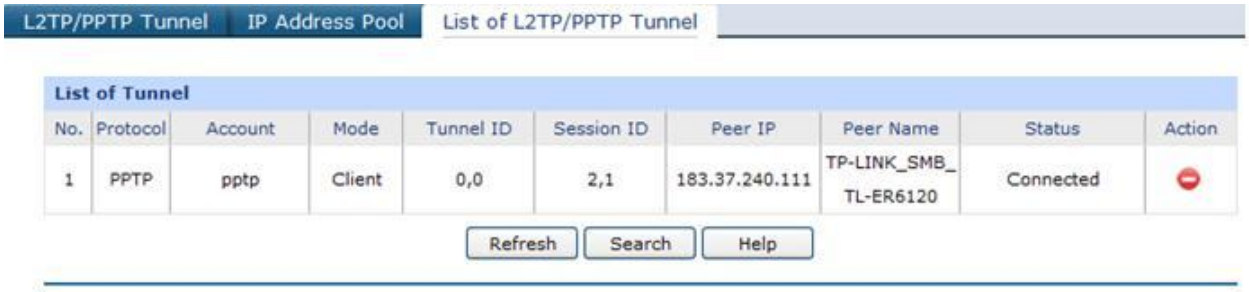
Step 3 : Under Server IP, enter Router A’s IP address, which is 183.37.240.111.

Step 4 : Under Remote Subnet, enter Router B’s local subnet, we enter “192.168.1.0/24” in this example.

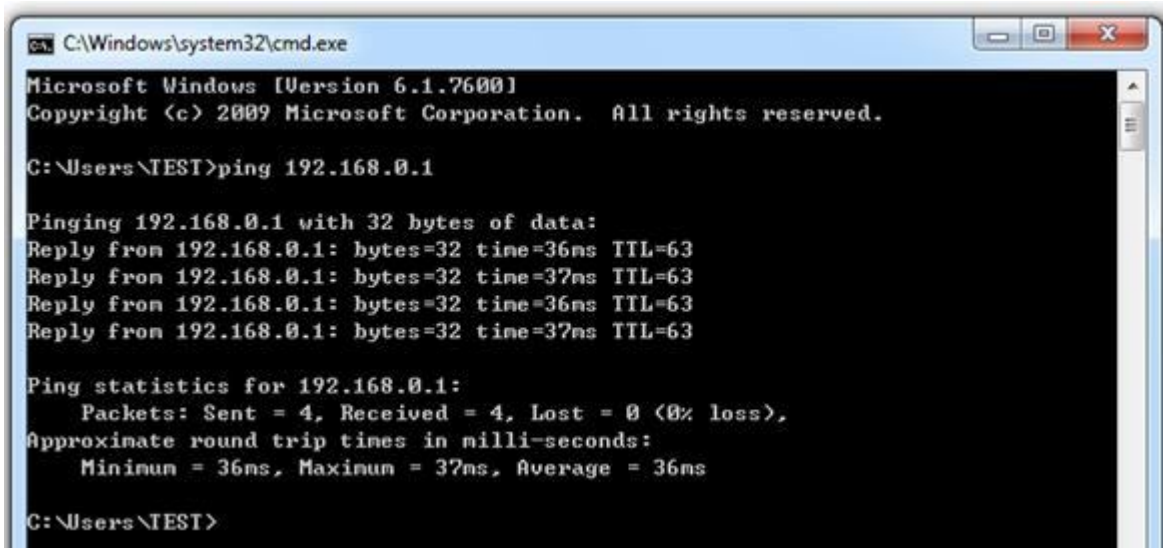
Step 5 : Look for Status, select Active.

Step 6 : Click on Add and then click on Save.

Step 7: If the PPTP tunnel is established successfully, you can check it on List of Tunnel.

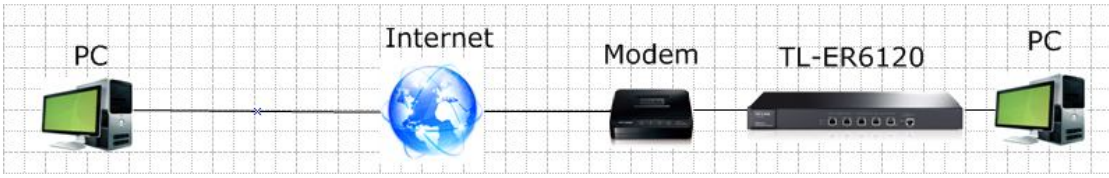


Also, PC within the local subnet of Router B, can ping Router A's LAN IP (192.168.0.1).



6. How to configure a PPTP Server on TP-LINK Router

Suitable for: TL-ER6120, TL-ER6020, TL-ER604W



PPTP (Point to Point Tunneling Protocol) Server is used to create a VPN connection for remote clients. To configure PPTP Server on TP-LINK router, please follow the instructions below:

A. **Make sure PCs of two sides can access to Internet**
B. **Configuring a PPTP Server on TP-LINK router**
C. **Configuring PPTP client on remote PC (Windows 7)**

NOTE: If the TP-LINK Router is behind a NAT device, Virtual Server or DMZ should be configured on the NAT device, otherwise the VPN tunnel can't be established.

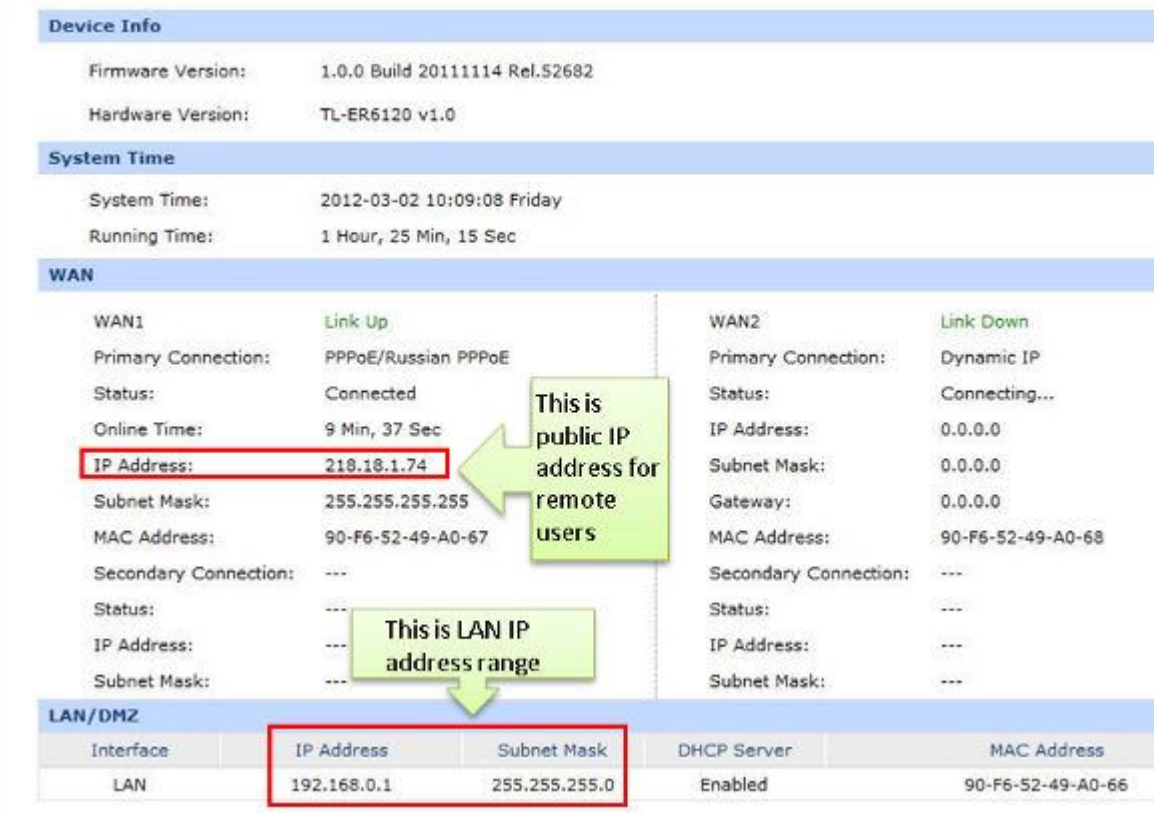
A. Make sure PCs of two sides can access to Internet

Before setup a VPN tunnel, you need to ensure that PCs of two sides are connected to the Internet. After ensuring that there is an active Internet connection on each side, you need to verify the VPN settings of the two sides, please follow the instruction below.

B. Configuring a PPTP Server on TP-LINK router

Step 1:

Access the router's management webpage, verify the settings needed on the router.



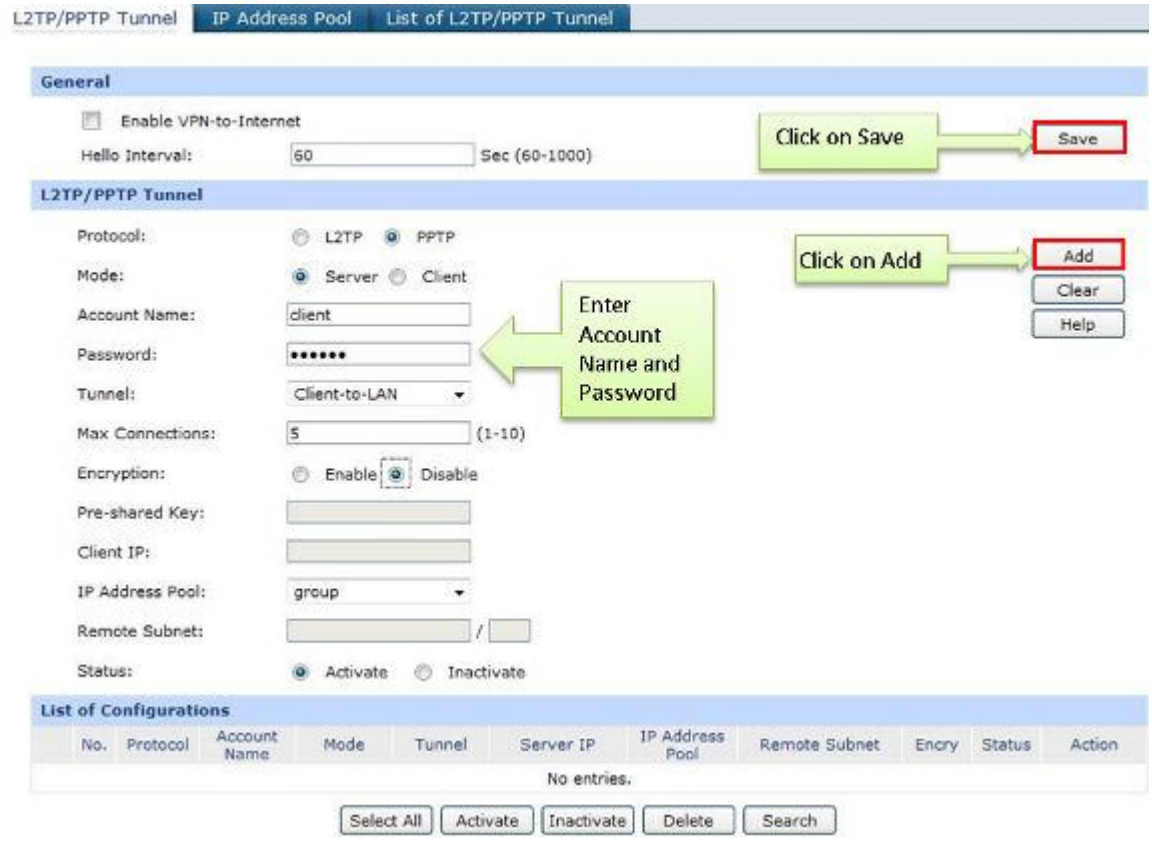
Step 2:

Click on VPN->L2TP/PPTP->IP Address Pool, enter Pool Name and IP Address Range, and then click on Add.

NOTE: IP Address pool must be different range from LAN IP address range.

Step 3:

Look for protocol, select PPTP; the Mode should be Server.



Step 4:

Enter Account Name and Password whatever you like, here we use “client” as account name, password is “123456”.

Step 5:

Under Tunnel, select Client-to-LAN.

Step 6:

The tunnel supports up to 10 connections, we enter 5 in this example.

Step 7:

Under IP Address Pool, select “group” we have added before.

Step 8:

Look for Status, select Active.

Step 9:

Click on Add and then click on Save.

C. Configuring PPTP client on remote PC (Windows 7)

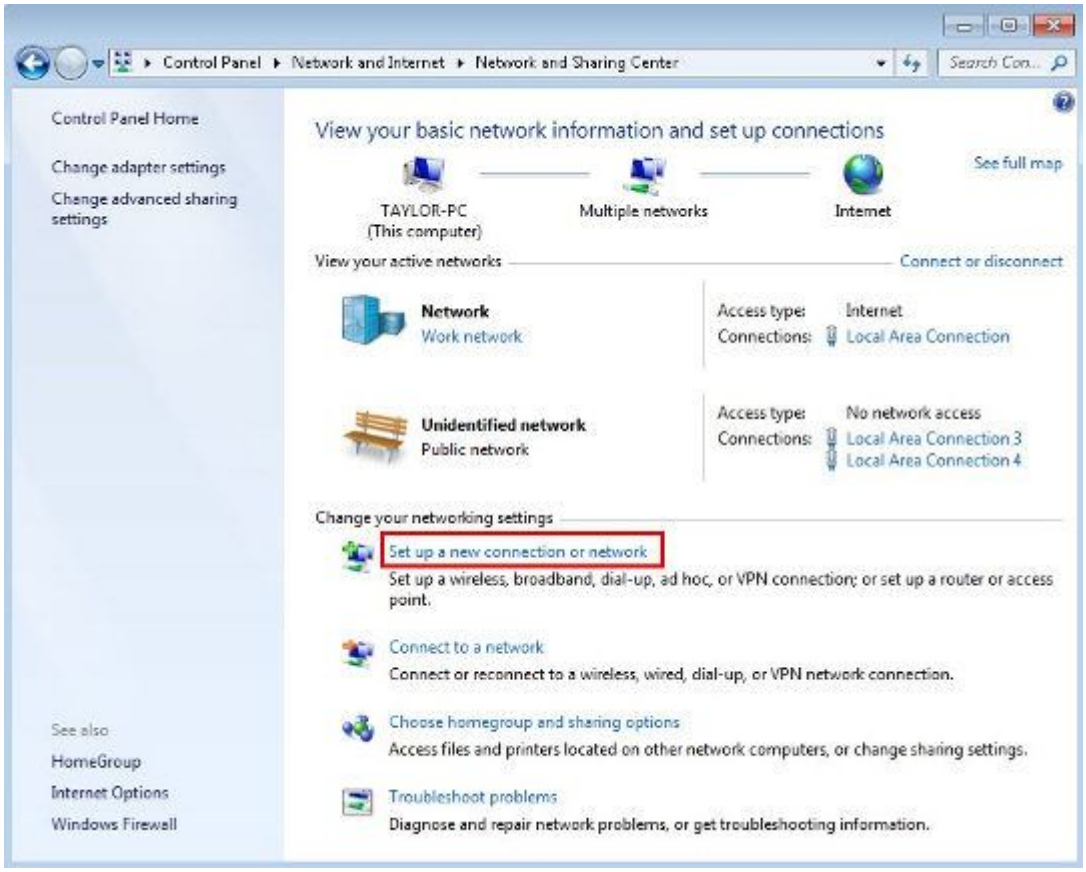
NOTE: For remote PC to connect to PPTP server, it can use Windows built-in PPTP software or Third-party PPTP software.

Step 1:

Click on Start->Control Panel->Network and Internet->Network and Sharing Center.

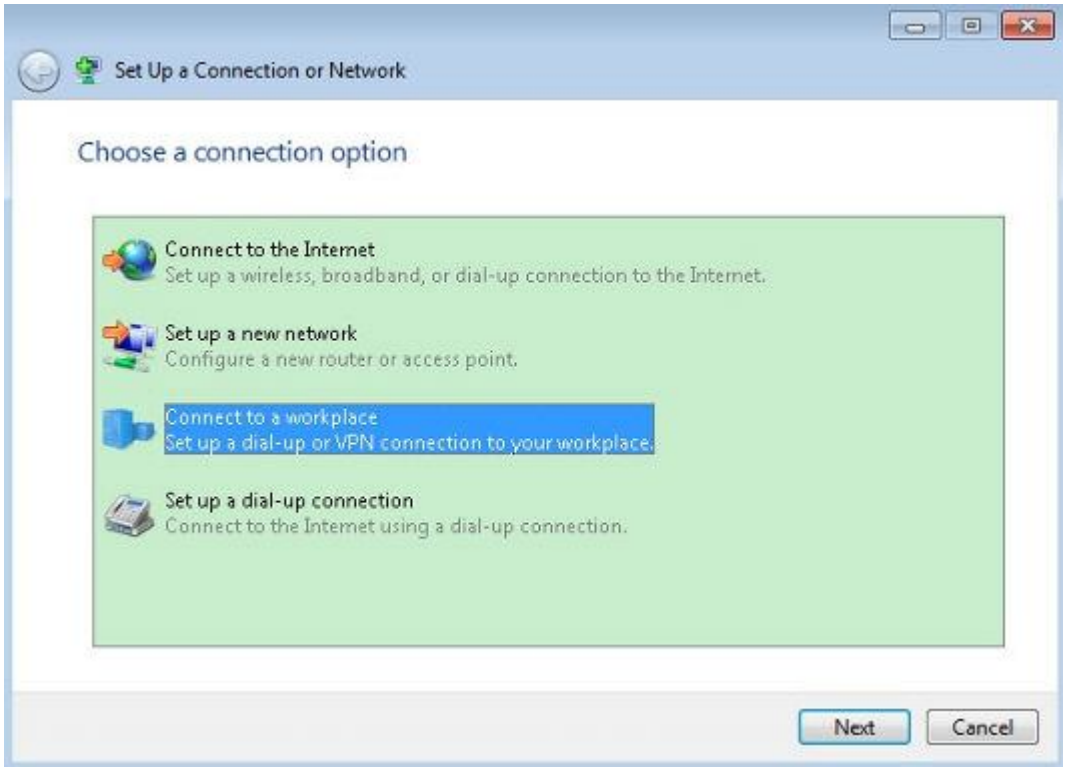
Step 2:

Click on Set up a new connection or network.



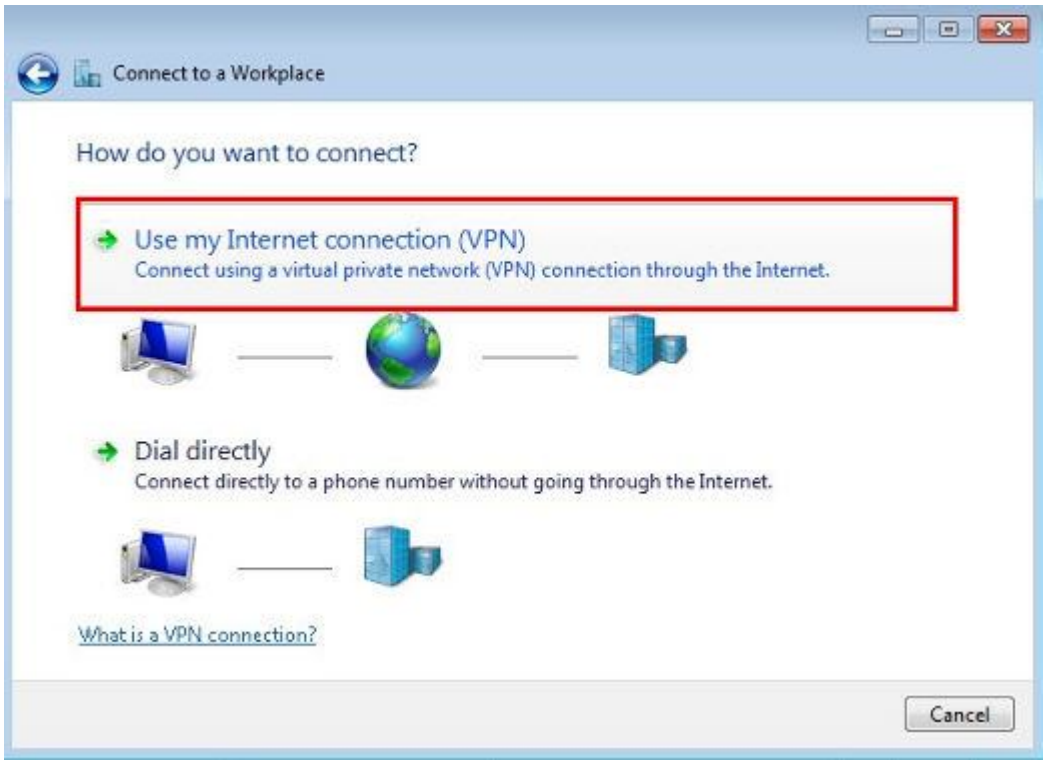
Step 3:

Choose Connect to a workplace, and then click on Next.



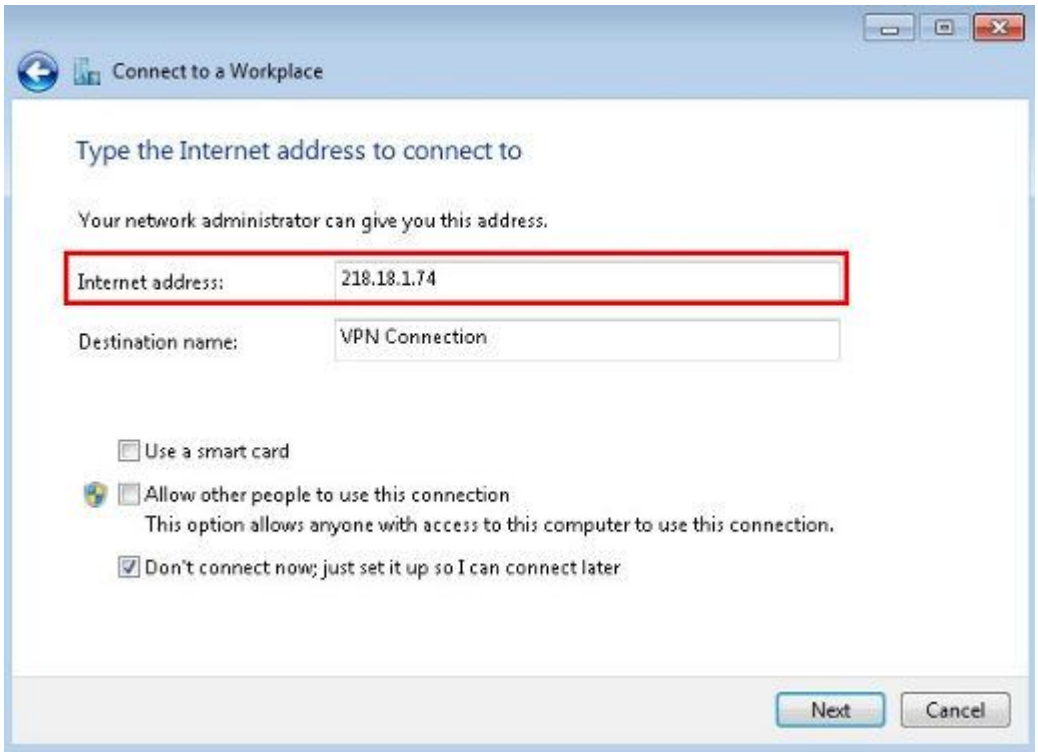
Step 4:

Select Use my Internet connection (VPN)



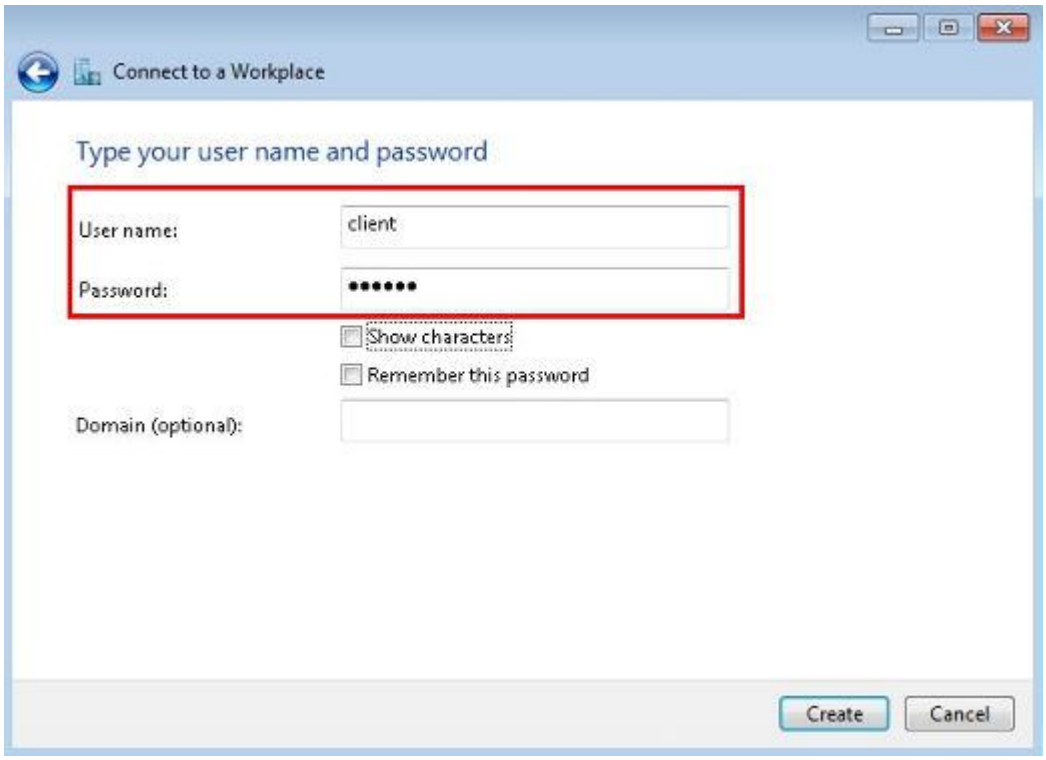
Step 5:

Under Internet address field, enter router's WAN IP address, and then click on Next.



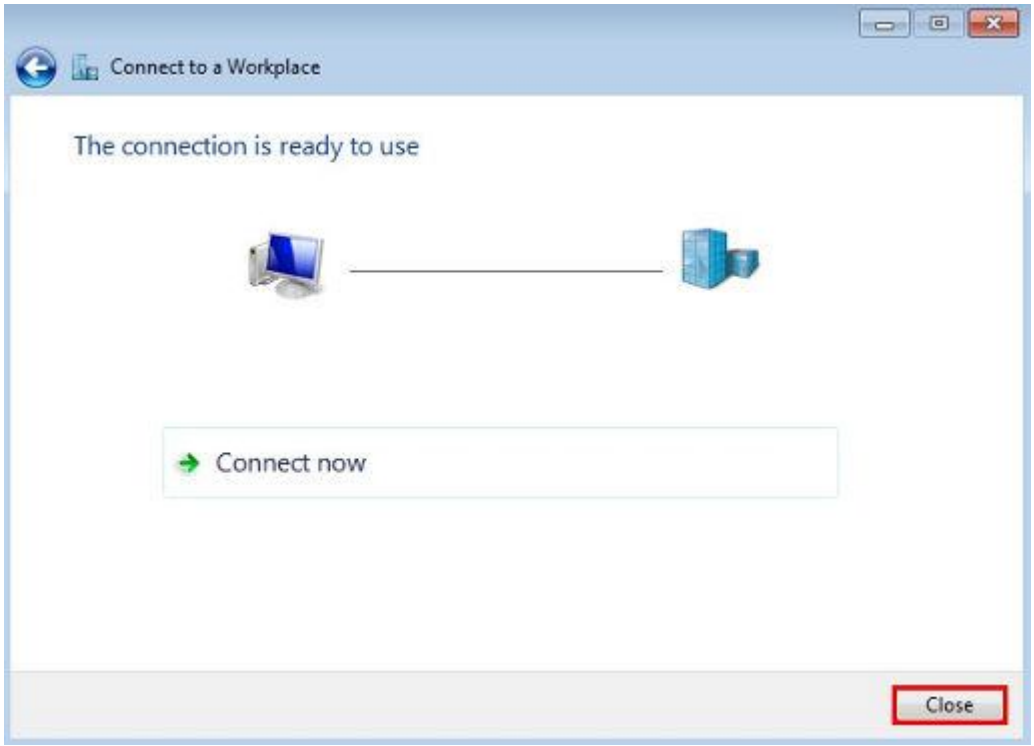
Step 6:

Enter User name and Password, and then click on Create.



Step 7:

The VPN connection is created and ready to use, click on Close.

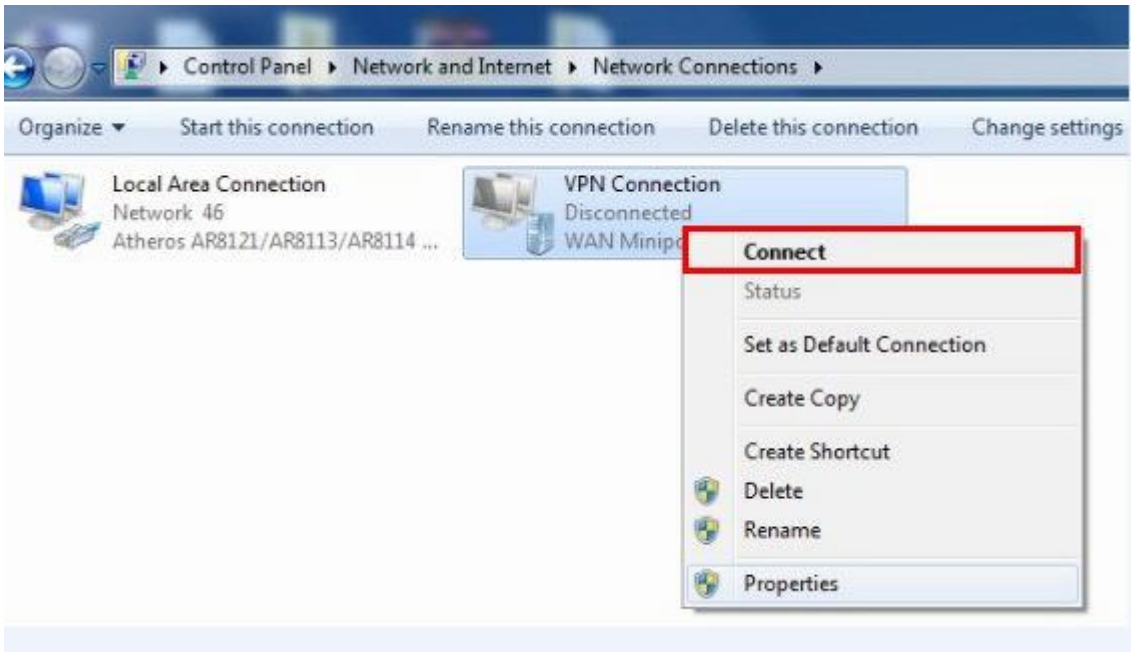


Step 8:

Go to Network and Sharing Center and click on Change adapter settings on the left menu.

Step 9:

Right Click on VPN Connection and select Connect.



Step 10:

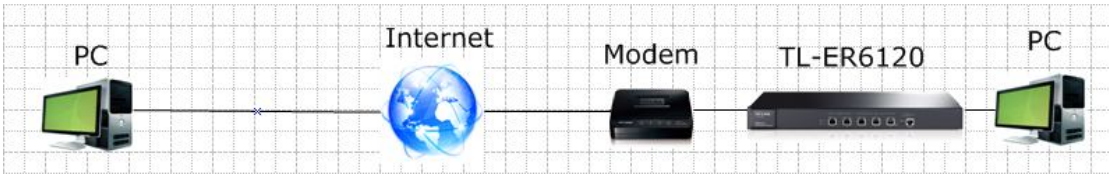
Enter User name and Password and then click on Connect.

Step 11:

If the PPTP tunnel is established successfully, you can check it on List of Tunnel.

7. How to configure a L2TP Server on TP-LINK Router

Suitable for: TL-ER6120, TL-ER6020, TL-ER604W



L2TP (Layer 2 Tunneling Protocol) Server is used to create a VPN connection for remote clients. To configure L2TP Server on TP-LINK router, please follow the instructions below:

A. Make sure PCs of two sides can access to Internet
B. Configuring a L2TP Server on TP-LINK router
C. Configuring L2TP client on remote PC (Windows 7)

NOTE: If the TP-LINK Router is behind a NAT device, Virtual Server or DMZ should be configured on the NAT device, otherwise the VPN tunnel can't be established.

A. Make sure PCs of two sides can access to Internet

Before setup a VPN tunnel, you need to ensure that PCs of two sides are connected to the Internet. After ensuring that there is an active Internet connection on each side, you need to verify the VPN settings of the two sides, please follow the instruction below.

B. Configuring a L2TP Server on TP-LINK router

Step 1:

Access the router's management web page; verify the settings needed on the router.

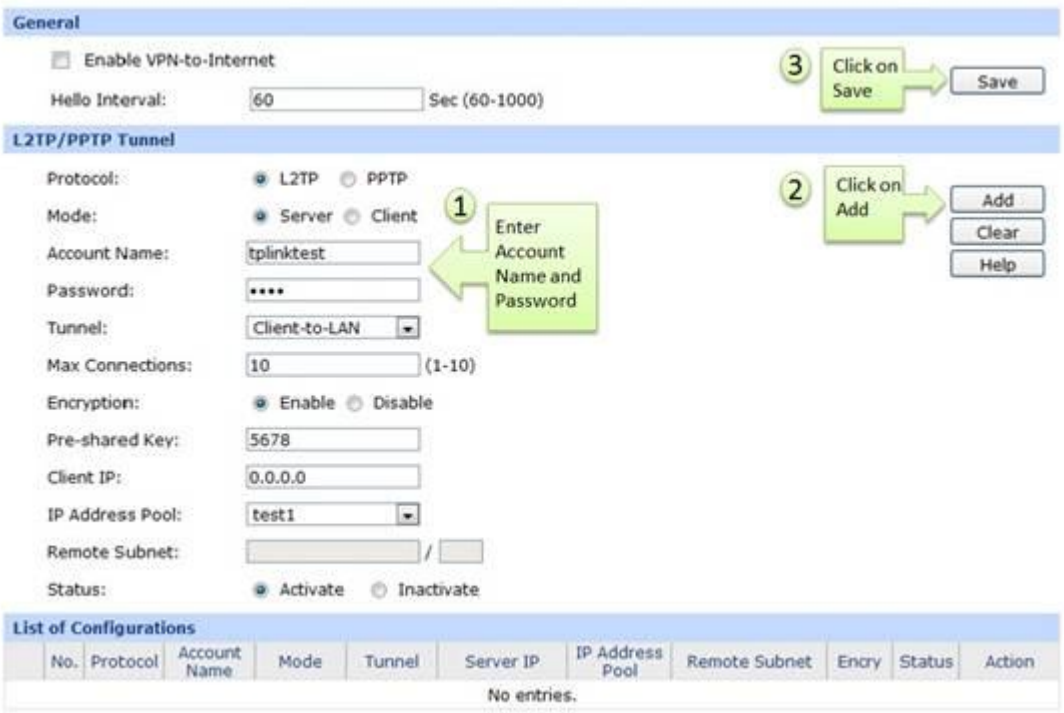
Step 2:

Click on VPN->L2TP/PPTP->IP Address Pool, enter Pool Name and IP Address Range, and then click on Add.

NOTE: IP Address pool must be different range from LAN IP address range.

Step 3:

Look for protocol, select L2TP; the Mode should be Server.



Step 4:

Enter Account Name and Password whatever you like, here we use “tplinktest” as account name, password is “1234”.

Step 5:

Under Tunnel, select Client-to-LAN.

Step 6:

The tunnel supports up to 10 connections, we enter 10 in this example.

Step 7:

Under Encryption, select Enable, and then enter “5678” as Pre-shared Key.

Step 8:

Under IP Address Pool, select “test1” we have added before.

Step 9:

Look for Status, select Active.

Step 10:

Click on Add.

Step 11:

As we enabled Encryption, we need to go to VPN->IPsec, enable IPsec and then click on Save.

C. Configuring L2TP client on remote PC (Windows 7)

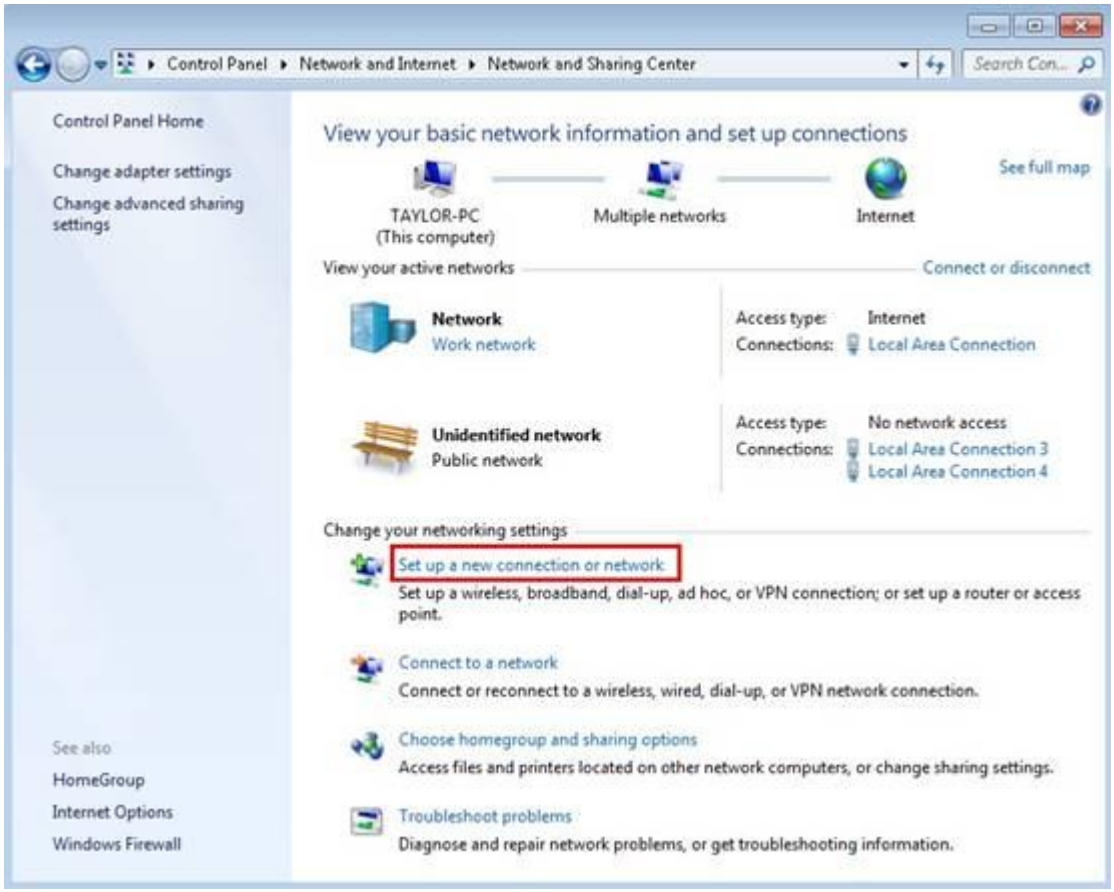
NOTE: For remote PC to connect to L2TP server, it can use Windows built-in L2TP software or Third-party L2TP software.

Step 1:

Click on Start->Control Panel->Network and Internet->Network and Sharing Center.

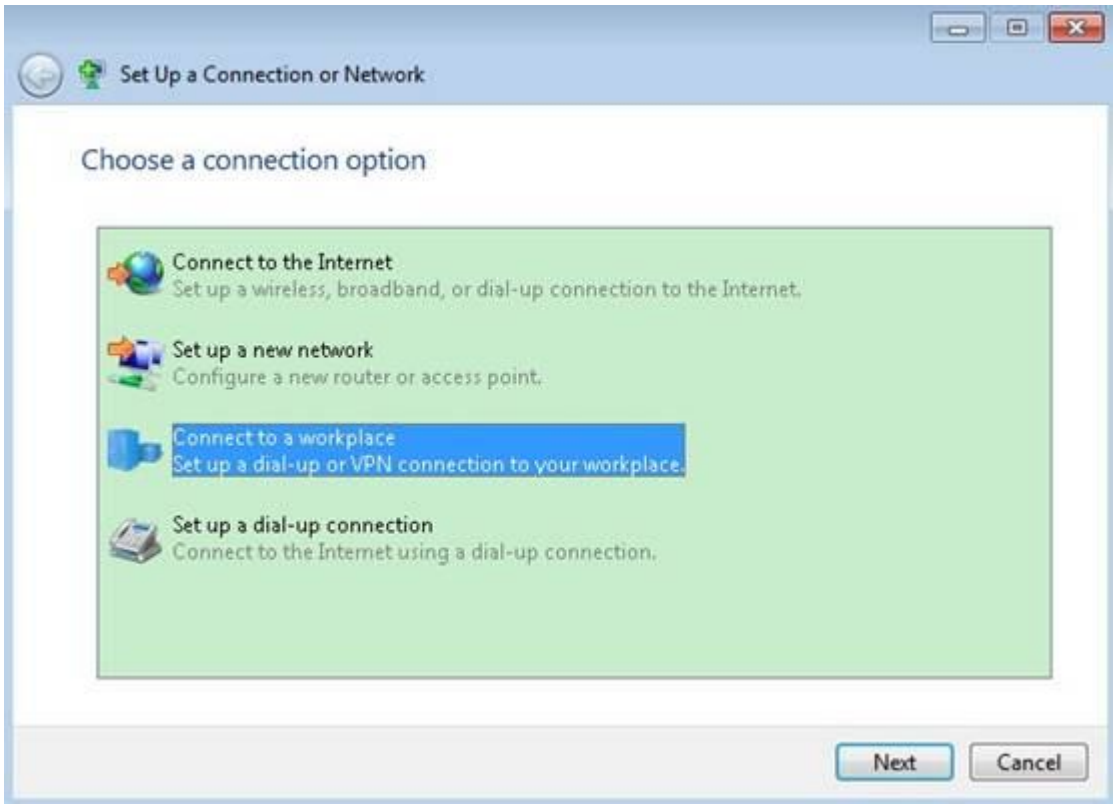
Step 2:

Click on Set up a new connection or network.



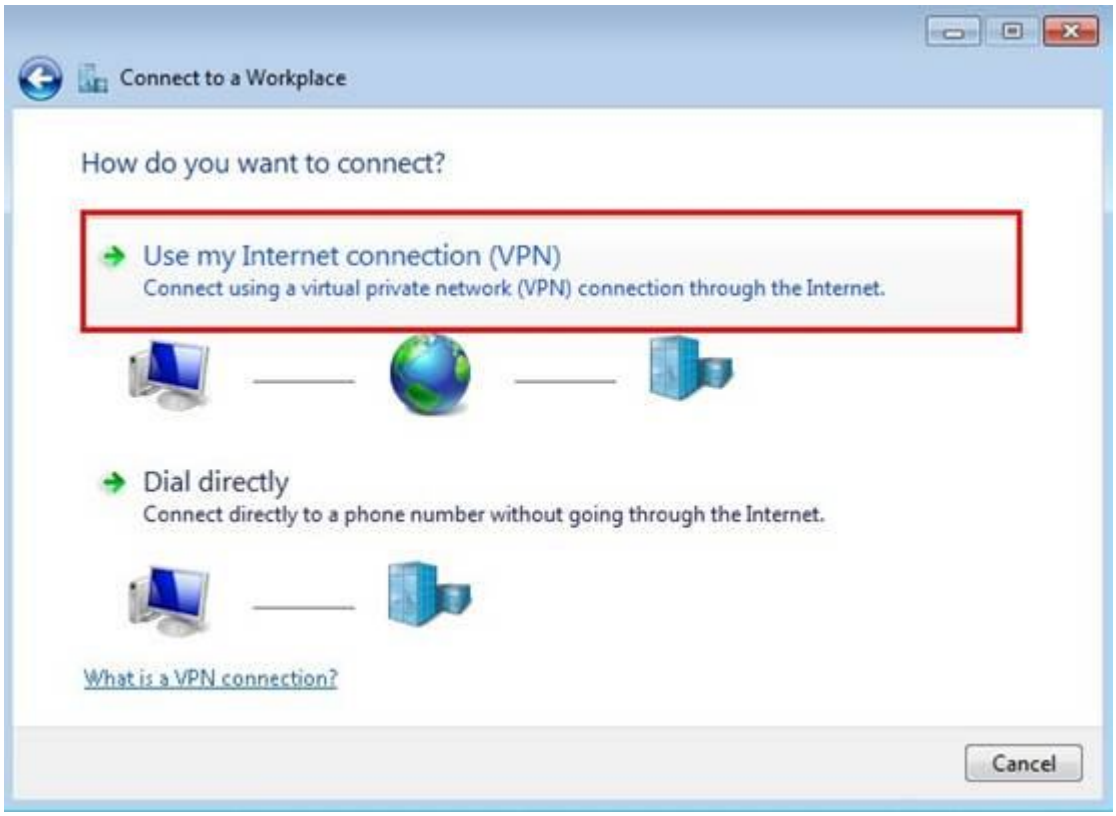
Step 3:

Choose Connect to a workplace, and then click on Next.



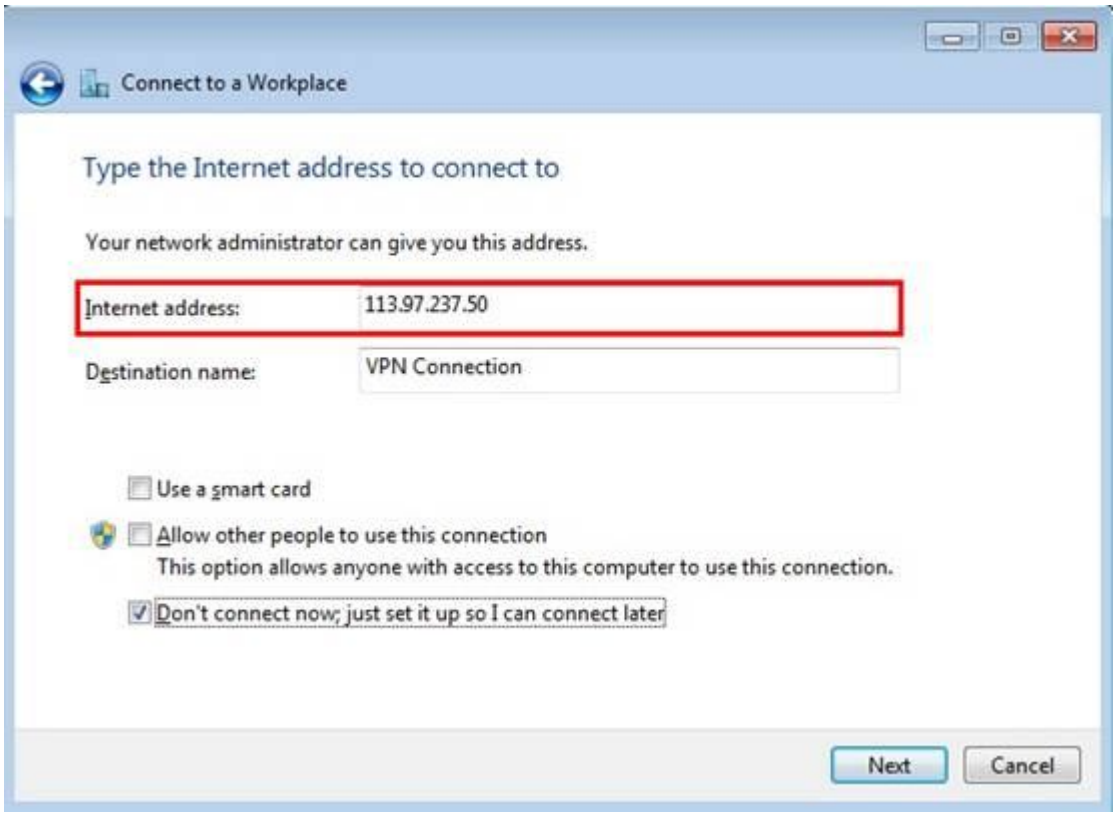
Step 4:

Select Use my Internet connection (VPN)



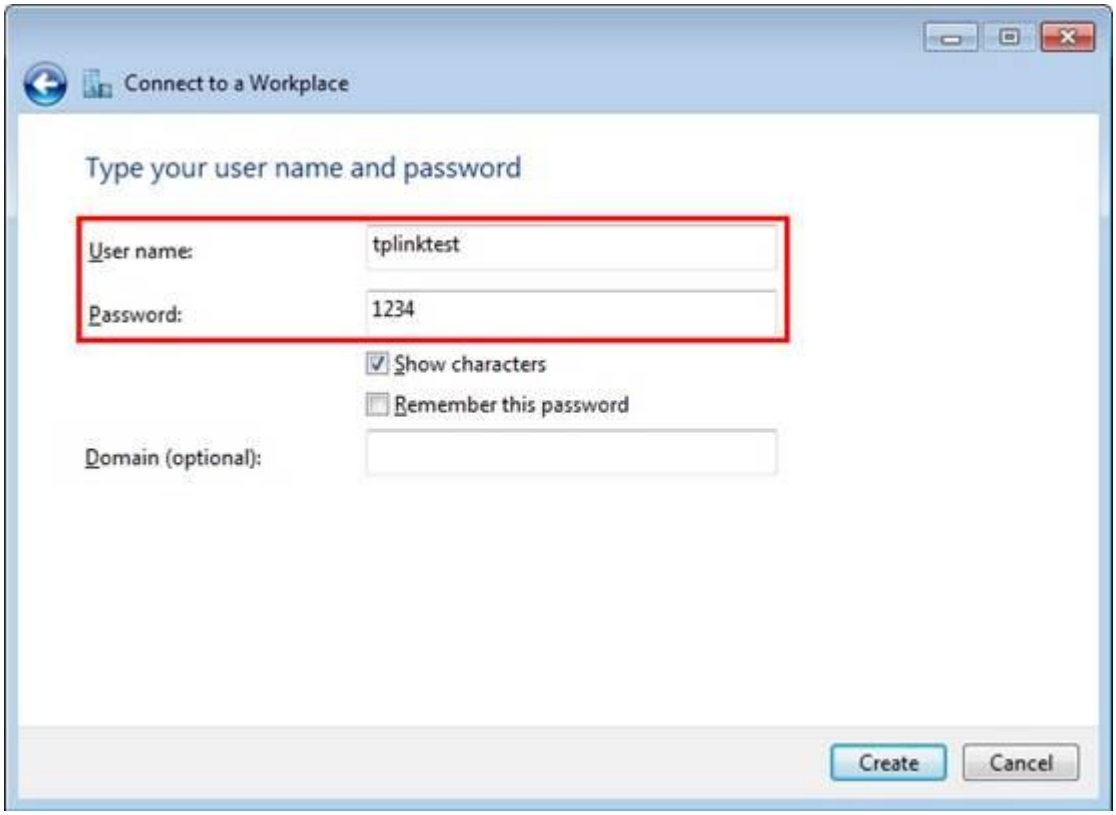
Step 5:

Under Internet address field, enter router's WAN IP address, and then click on Next.



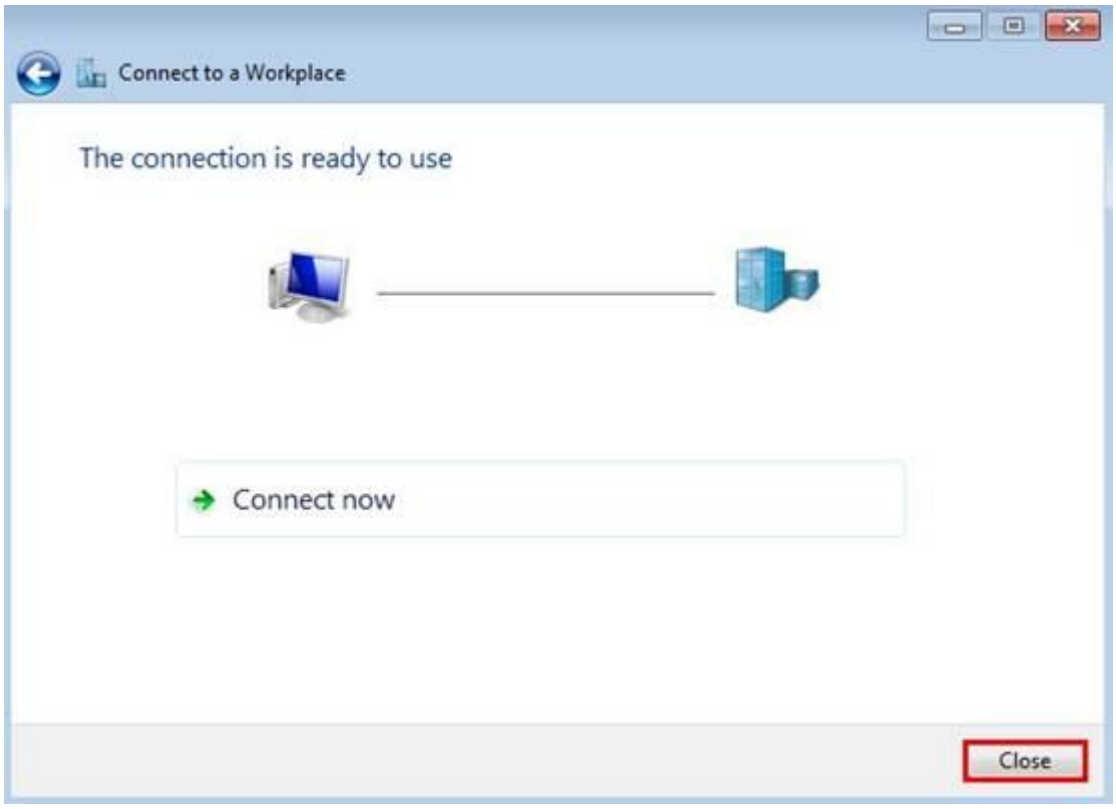
Step 6:

Enter User name and Password, and then click on Create.



Step 7:

The VPN connection is created and ready to use, click on Close.

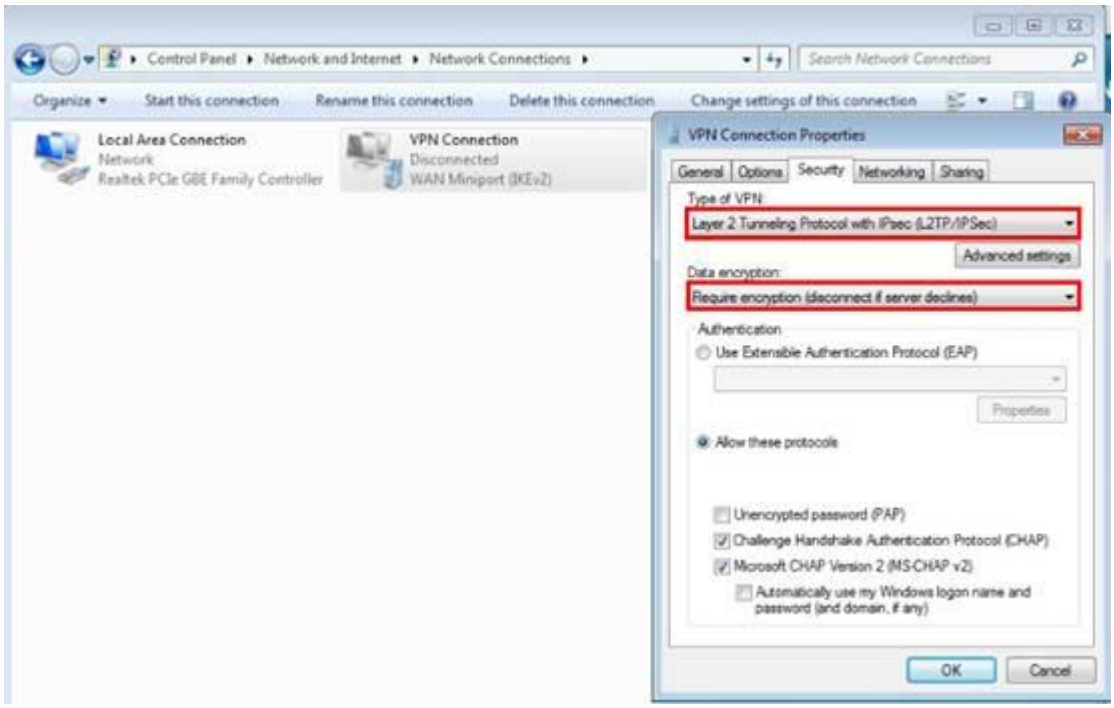


Step 8:

Go to Network and Sharing Center and click on Change adapter settings on the left menu.

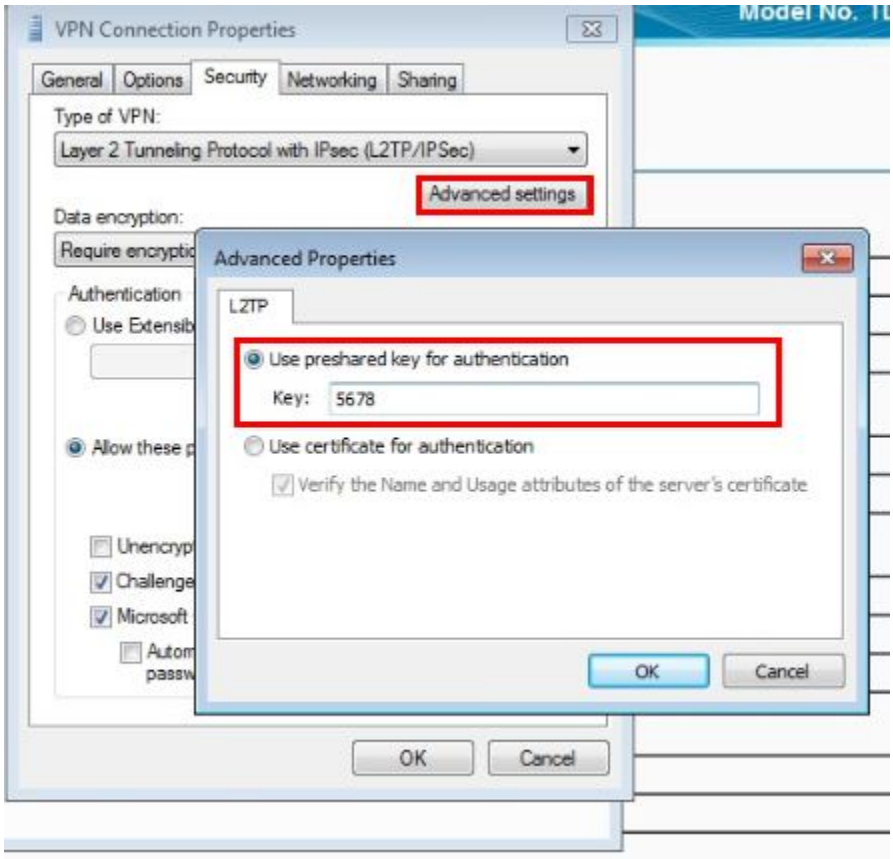
Step 9:

Right Click on VPN Connection and select Properties. On the Security tab, Select Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec), under Data encryption, select Require encryption (disconnect if server declines).



Step 10:

Click on Advanced settings, pick Use preshared key for authentication, and then enter the key, here is “5678”.



Step 11:

Double click on VPN Connection, enter User name and Password and then click on Connect.


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