

VPN (BiPAC 8920AX only)

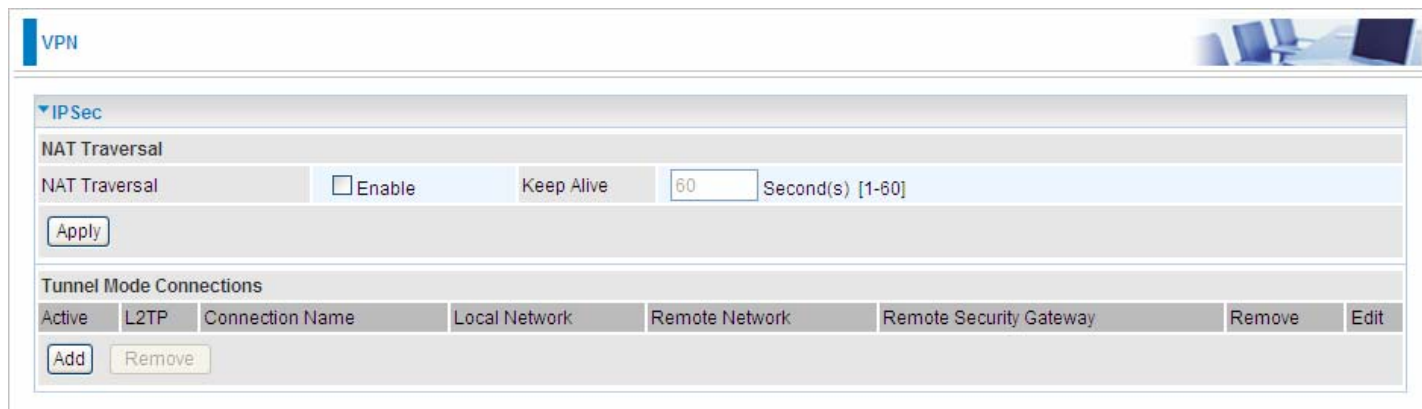
A **virtual private network (VPN)** is a private network that interconnects remote (and often geographically separate) networks through primarily public communication infrastructures such as the Internet. VPNs provide security through tunneling protocols and security procedures such as encryption. For example, a VPN could be used to securely connect the branch offices of an organization to a head office network through the public Internet.

IPSec

Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPsec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session.

IPsec is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite. It can be used in protecting data flows between a pair of security gateways (*network-to-network*), or between a security gateway and a host (*network-to-host*).

Note: A maximum of 16 sessions for IPsec.



The screenshot shows a web-based configuration interface for VPN settings. At the top, there is a 'VPN' tab. Below it, the 'IPSec' section is expanded. Under 'NAT Traversal', there is a checkbox for 'Enable' which is currently unchecked. To its right is a 'Keep Alive' section with a text input field containing '60' and a label 'Second(s) [1-60]'. Below these fields is an 'Apply' button. Further down, the 'Tunnel Mode Connections' section contains a table with columns: 'Active', 'L2TP', 'Connection Name', 'Local Network', 'Remote Network', 'Remote Security Gateway', 'Remove', and 'Edit'. Below the table are 'Add' and 'Remove' buttons.

Active	L2TP	Connection Name	Local Network	Remote Network	Remote Security Gateway	Remove	Edit
--------	------	-----------------	---------------	----------------	-------------------------	--------	------

NAT Traversal

NAT Traversal: This directive enables use of the NAT-Traversal IPsec extension (NAT-T). NAT-T allows one or both peers to reside behind a NAT gateway (i.e., doing address- or port-translation).

Keep Alive: Type the interval time(sec) for sending packets to keep the NAT Traversal alive.

Click **Apply** to save and apply your settings.

Click **Add** to create IPSec connections.

The screenshot shows the 'VPN' configuration window with the 'IPSec' tab selected. The 'IPSec Settings' section includes a checkbox for 'L2TP over IPsec' (unchecked). Below this are fields for 'Connection Name', 'WAN Interface' (set to 'Default'), 'IP Version' (set to 'IPv4'), 'Local Network' (set to 'Single Address'), 'IP Address', 'Netmask', 'Remote Security Gateway', 'Anonymous' checkbox (unchecked), 'Remote Network' (set to 'Single Address'), 'IP Address', 'Netmask', 'Key Exchange Method' (set to 'IKE'), 'IPsec Protocol' (set to 'ESP'), 'Pre-Shared Key', 'Local ID Type' (set to 'Default'), 'ID Content', 'Remote ID Type' (set to 'Default'), and 'ID Content'. The 'Phase 1' section includes 'Mode' (set to 'Main'), 'Encryption Algorithm' (set to '3DES'), 'Integrity Algorithm' (set to 'MD5'), 'DH Group' (set to 'MODP1024(DH2)'), 'SA Lifetime' (set to '480 Minute(s) [60-1440]'), 'Phase 2' (set to 'Main'), 'Encryption Algorithm' (set to '3DES'), 'Integrity Algorithm' (set to 'MD5'), 'DH Group' (set to 'None'), 'IPsec Lifetime' (set to '60 Minute(s) [60-1440]'), 'Keep Alive' (set to 'None'), and 'MTU' (set to '0 (0 : Default)'). An 'Apply' button is located at the bottom left of the settings area.

IPSec Settings

L2TP over IPSec: Select Enable if user wants to use L2TP over IPSec. See [L2TP over IPSec](#)

Connection Name: A given name for the connection, but it should contain no spaces (e.g. "connection-to-office").

WAN Interface: Select the set used interface for the IPSec connection, when you select adsl pppoe_0_0_35/ppp0.1 interface, the IPSec tunnel would transmit data via this interface to connect to the remote peer.

IP Version: Select the IP version base on your network framework.

Local Network: Set the IP address or subnet of the local network.

- ① **Single Address:** The IP address of the local host, for establishing an IPSec connection between a security gateway and a host (*network-to-host*).
- ① **Subnet:** The subnet of the local network, for establishing an IPSec tunnel between a pair of security gateways (*network-to-network*)

IP Address: The local network address.

Netmask: The local network netmask.

Remote Secure Gateway: The IP address of the remote VPN device that is connected and establishes a VPN tunnel.

Anonymous: Enable any IP to connect in.

Remote Network: Set the IP address or subnet of the remote network.

- ① **Single Address:** The IP address of the local host, for establishing an IPSec connection between a security gateway and a host (*network-to-host*). If the remote peer is a host, select Single Address.
- ① **Subnet:** The subnet of the local network, for establishing an IPSec tunnel between a pair of security gateways (*network-to-network*), If the remote peer is a network, select Subnet.

Key Exchange Method: Displays key exchange method.

Pre-Shared Key: This is for the Internet Key Exchange (IKE) protocol, a string from 1 to 32 characters. Both sides should use the same key. IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require a key. Before any IPSec traffic can be passed, each router must be able to verify the identity of its peer. This can be done by manually entering the pre-shared key into both sides (router or hosts).

Local ID Type and Remote ID Type: When the mode of phase 1 is aggressive, Local and Remote peers can be identified by other IDs.

ID content: Enter ID content the name you want to identify when the Local and Remote Type are Domain Name; Enter ID content IP address you want to identify when the Local and Remote Type are IP addresses (IPv4 and IPv6 supported).

Phase 1

Mode: Select IKE mode from the drop-down menu: **Main** or **Aggressive**. This IKE provides secured key generation and key management.

Encryption Algorithm: Select the encryption algorithm from the drop-down menu. There are several options: 3DES and AES (128, 192 and 256). 3DES and AES are more powerful but increase latency.

- ① **DES:** Stands for Triple Data Encryption Standard, it uses 56 bits as an encryption method.
- ① **3DES:** Stands for Triple Data Encryption Standard, it uses 168 (56*3) bits as an encryption method.
- ① **AES:** Stands for Advanced Encryption Standards, you can use 128, 192 or 256 bits as encryption method.

Integrity Algorithm: Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmit. There are 2 options: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA1). SHA1 is more resistant to brute-force attacks than MD5. However, it is slower.

- ① **MD5:** A one-way hashing algorithm that produces a 128-bit hash.
- ① **SHA1:** A one-way hashing algorithm that produces a 160-bit hash.

DH Group: It is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). MODP stands for Modular Exponentiation Groups.

SA Lifetime: Specify the number of minutes that a Security Association (SA) will stay active before new encryption and authentication key will be exchanged. Enter a value to issue an initial connection request for a new VPN tunnel. Default is 480 minutes (28800 seconds). A short SA time increases security by forcing the two parties to update the keys. However, every time when the VPN tunnel re-negotiates, access through the tunnel will be temporarily disconnected.

Phase 2

Encryption Algorithm: Select the encryption algorithm from the drop-down menu. There are several options: 3DES and AES (128, 192 and 256). 3DES and AES are more powerful but increase latency.

Integrity Algorithm: Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmit. There are 2 options: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA1). SHA1 is more resistant to brute-force attacks than MD5. However, it is slower.

DH Group: It is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). MODP stands for Modular Exponentiation Groups.

IPSec Lifetime: Specify the number of minutes that IPSec will stay active before new encryption and authentication key will be exchanged. Enter a value to negotiate and establish secure authentication. Default is 60 minutes (3600 seconds). A short time increases security by forcing the two parties to update the keys. However, every time when the VPN tunnel re- negotiates, access through the tunnel will be temporarily disconnected.

Ping for Keep Alive: Select the operation methods:

- ① **None:** The default setting is “None”. To this mode, it will not detect the remote IPSec peer has been lost or not. It only follows the policy of Disconnection time after no traffic, which the remote IPSec will be disconnected after the time you set in this function.
- ① **DPD:** Dead peer detection (DPD) is a keeping alive mechanism that enables the router to be detected lively when the connection between the router and a remote IPSec peer has lost. Please be noted, it must be enabled on the both sites.

Detection Interval	180	Second(s) [180-86400]	Idle Timeout	5	Consecutive times [5-99]
--------------------	-----	-----------------------	--------------	---	--------------------------

Detection Interval: The period cycle for dead peer detection. The interval can be 180~86400 seconds.

Idle Timeout: Auto-disconnect the IPSec connection after trying several consecutive times.

- ① **Ping:** This mode will detect whether the remote IPSec peer has lost or not by pinging specify IP address.

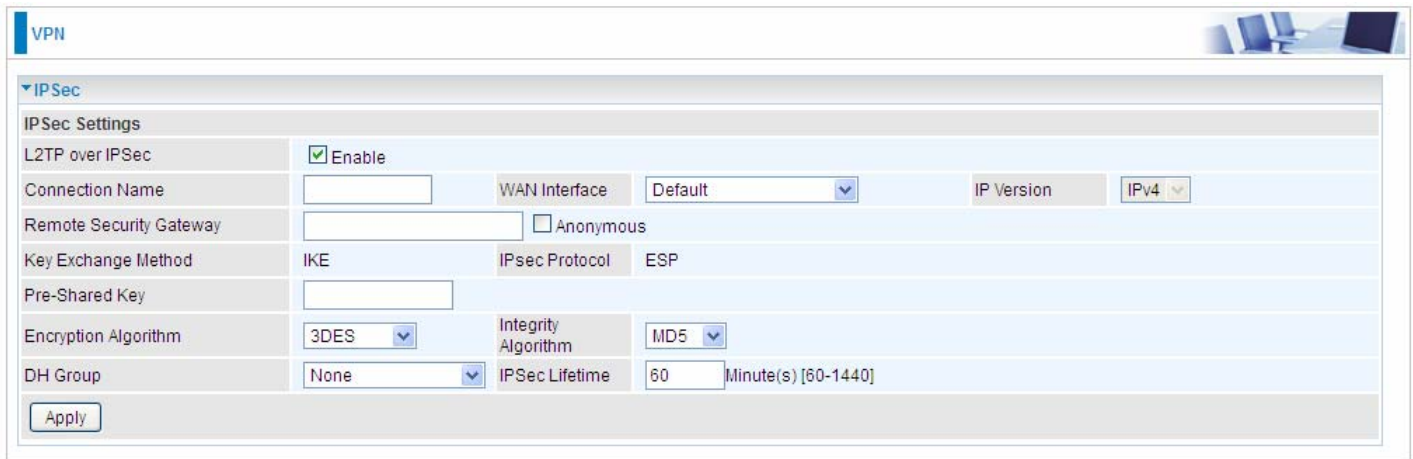
Ping IP (0.0.0.0 : NEVER)	0.0.0.0	Interval	10	Second(s) [0-3600, 0 : NEVER]
---------------------------	---------	----------	----	-------------------------------

Ping IP: Type the IP for ping operation. It is able to IP Ping the remote PC with the specified IP address and alert when the connection fails. Once alter message is received, Router will drop this tunnel connection. Reestablish of this connection is required. Default setting is 0.0.0.0 which disables the function.

Interval: This sets the time interval between Pings to the IP function to monitor the connection status. Default interval setting is 10 seconds. Time interval can be set from 0 to 3600 second, 0 second disables the function.

MTU: Maximum Transmission Unit, maximum value is 1500.

IPSec for L2TP



The screenshot shows a web-based configuration interface for a VPN. At the top, there is a 'VPN' tab. Below it, the 'IPSec' section is expanded. The 'IPSec Settings' tab is active. The configuration fields are as follows:

Field	Value
L2TP over IPSec	☒ Enable
Connection Name	[Empty text box]
WAN Interface	Default
IP Version	IPv4
Remote Security Gateway	[Empty text box] ☐ Anonymous
Key Exchange Method	IKE
IPsec Protocol	ESP
Pre-Shared Key	[Empty text box]
Encryption Algorithm	3DES
Integrity Algorithm	MD5
DH Group	None
IPsec Lifetime	60 Minute(s) [60-1440]

An 'Apply' button is located at the bottom left of the configuration area.

Connection Name: A given name for the connection, but it should contain no spaces (e.g. “connection-to-office”).

WAN Interface: Select the set interface for the IPSec tunnel.

Remote Security Gateway: Input the IP of remote security gateway.

Key Exchange Method: Displays key exchange method.

Pre-Shared Key: This is for the Internet Key Exchange (IKE) protocol, a string from 1 to 32 characters. Both sides should use the same key. IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require a key. Before any IPSec traffic can be passed, each router must be able to verify the identity of its peer. This can be done by manually entering the pre-shared key into both sides (router or hosts).

Encryption Algorithm: Select the encryption algorithm from the drop-down menu. There are several options: 3DES and AES (128, 192 and 256). 3DES and AES are more powerful but increase latency.

- ① **DES:** Stands for Triple Data Encryption Standard, it uses 56 bits as an encryption method.
- ① **3DES:** Stands for Triple Data Encryption Standard, it uses 168 (56*3) bits as an encryption method.
- ① **AES:** Stands for Advanced Encryption Standards, you can use 128, 192 or 256 bits as encryption method.

Integrity Algorithm: Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmit. There are 2 options: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA1). SHA1 is more resistant to brute-force attacks than MD5. However, it is slower.

- ① **MD5:** A one-way hashing algorithm that produces a 128-bit hash.
- ① **SHA1:** A one-way hashing algorithm that produces a 160-bit hash.

DH Group: It is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). MODP stands for Modular Exponentiation Groups.

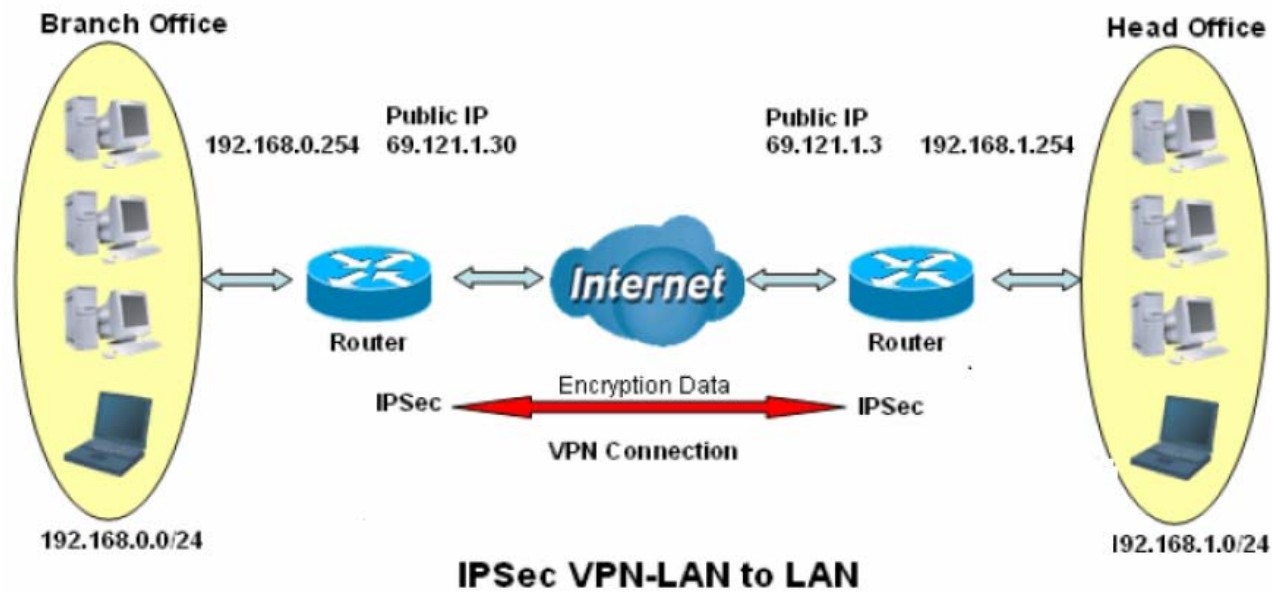
IPSec Lifetime: Specify the number of minutes that IPSec will stay active before new encryption and authentication key will be exchanged. Enter a value to negotiate and establish secure authentication. Default is 60 minutes (3600 seconds). A short time increases security by forcing the two parties to update the keys. However, every time when the VPN tunnel re- negotiates, access through the tunnel will be temporarily disconnected.

Examples:

1. LAN-to-LAN connection

Two BiPAC 7800VDOXs want to setup a secure IPSec VPN tunnel

Note: The IPSec Settings shall be consistent between the two routers.



Head Office Side:

Setup details:

Item	Function		Description
1	Connection Name	H-to-B	Give a name for IPSec connection
2	Local Network		
	Subnet		Select Subnet
	IP Address	192.168.1.0	Head Office network
	Netmask	255.255.255.0	
3	Secure Gateway Address(Hostanme)	69.121.1.30	IP address of the Branch office router (on WAN side)
4	Remote Network		
	Subnet		Select Subnet
	IP Address	192.168.0.0	Branch office network
	Netmask	255.255.255.0	
5	Proposal		
	Method	ESP	Security Plan
	Authentication	MD5	
	Encryption	3DES	
	Prefer Forward Security	MODP 1024(group2)	
	Pre-shared Key	123456	



▼ IPsec

IPsec Settings

L2TP over IPsec	☐ Enable				
Connection Name	H-to-B	WAN Interface	Default	IP Version	IPv4
Local Network	Subnet	IP Address	192.168.1.0	Netmask	255.255.255.0
Remote Security Gateway	69.121.1.30	☐ Anonymous			
Remote Network	Subnet	IP Address	192.168.0.0	Netmask	255.255.255.0
Key Exchange Method	IKE	IPsec Protocol	ESP		
Pre-Shared Key	123456				
Local ID Type	Default	ID Content			
Remote ID Type	Default	ID Content			

Phase 1

Mode	Main
Encryption Algorithm	3DES
Integrity Algorithm	MD5
DH Group	MODP1024(DH2)
SA Lifetime	480 Minute(s) [60-1440]

Phase 2

Encryption Algorithm	3DES
Integrity Algorithm	MD5
DH Group	None
IPsec Lifetime	60 Minute(s) [60-1440]
Keep Alive	DPD
Detection Interval	180 Second(s) [180-86400]
Idle Timeout	5 Consecutive times [5-99]
MTU	1500 (0 : Default)

Branch Office Side:

Setup details: the same operation as done in Head Office side

Item	Function		Description
1	Connection Name	B-to-H	Give a name for IPSec connection
2	Local Network		Branch Office network
	Subnet		
	IP Address	192.168.0.0	
	Netmask	255.255.255.0	
3	Remote Secure Gateway Address(Hostname)	69.121.1.3	IP address of the Head office router (on WAN side)
4	Remote Network		Head office network
	Subnet		
	IP Address	192.168.1.0	
	Netmask	255.255.255.0	
5	Proposal		Security Plan
	Method	ESP	
	Authentication	MD5	
	Encryption	3DES	
	Prefer Forward Security	MODP 1024(group2)	
	Pre-shared Key	123456	

VPN

IPSec

IPSec Settings

L2TP over IPSec

☐ Enable

Connection Name

B-to-H

WAN Interface

Default

IP Version

IPv4

Local Network

Subnet

IP Address

192.168.0.0

Netmask

255.255.255.0

Remote Security Gateway

69.121.1.3

Anonymous

☐ Anonymous

Remote Network

Subnet

IP Address

192.168.1.0

Netmask

255.255.255.0

Key Exchange Method

IKE

IPsec Protocol

ESP

Pre-Shared Key

123456

Local ID Type

Default

ID Content

Remote ID Type

Default

ID Content

Phase 1

Mode

Main

Encryption Algorithm

3DES

Integrity Algorithm

MD5

DH Group

MODP1024(DH2)

SA Lifetime

480

Minute(s) [60-1440]

Phase 2

Encryption Algorithm

3DES

Integrity Algorithm

MD5

DH Group

None

IPSec Lifetime

60

Minute(s) [60-1440]

Keep Alive

DPD

Detection Interval

180

Second(s) [180-86400]

Idle Timeout

5

Consecutive times [5-99]

MTU

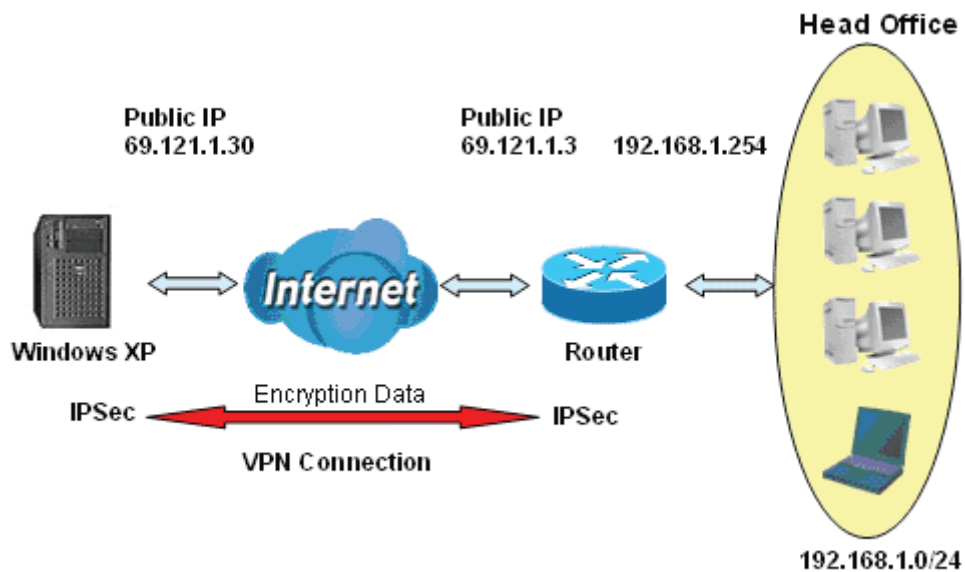
1500

(0 : Default)

Apply

1. Host to LAN

Router servers as VPN server, and host should install the IPSec client to connect to head office through IPSec VPN.



IPSec VPN-Host to LAN

Item	Function		Description
1	Connection Name	Headoffice-to-Host	Give a name for IPSec connection
2	Local Network		Head Office network
	Subnet		
	IP Address	192.168.1.0	
	Netmask	255.255.255.0	
3	Remote Secure Gateway (Hostanme)	69.121.1.30	IP address of the Branch office router (on WAN side)
4	Remote Network		Host
	Single Address	69.121.1.30	
5	Proposal		Security Plan
	Method	ESP	
	Authentication	MD5	
	Encryption	3DES	
	Prefer Forward Security	MODP 1024(group2)	
	Pre-shared Key	123456	



▼ IPsec

IPsec Settings

L2TP over IPsec	☐ Enable				
Connection Name	Headoffice-to-H	WAN Interface	Default	IP Version	IPv4
Local Network	Subnet	IP Address	192.168.1.0	Netmask	255.255.255.0
Remote Security Gateway	69.121.1.30	☐ Anonymous			
Remote Network	Single Address	IP Address	69.121.1.30	Netmask	255.255.255.0
Key Exchange Method	IKE	IPsec Protocol	ESP		
Pre-Shared Key	123456				
Local ID Type	Default	ID Content			
Remote ID Type	Default	ID Content			

Phase 1

Mode	Main
Encryption Algorithm	3DES
Integrity Algorithm	MD5
DH Group	MODP1024(DH2)
SA Lifetime	480 Minute(s) [60-1440]

Phase 2

Encryption Algorithm	3DES
Integrity Algorithm	MD5
DH Group	None
IPsec Lifetime	60 Minute(s) [60-1440]
Keep Alive	DPD
Detection Interval	180 Second(s) [180-86400]
Idle Timeout	5 Consecutive times [5-99]
MTU	1500 (0 : Default)

VPN Account

PPTP and L2TP server share the same account database set in VPN Account page.

VPN

VPN Account

VPN Account applied to PPTP Server and L2TP Server.

Parameters

Name		Tunnel	☒ Enable ☐ Disable
Username		Password	
Connection Type	☒ Remote Access ☐ LAN to LAN		
Peer Network IP		Peer Netmask	

Name: A user-defined name for the connection.

Tunnel: Select **Enable** to activate the account. PPTP(L2TP) server is waiting for the client to connect to this account.

Username: Please input the username for this account.

Password: Please input the password for this account.

Connection Type: Select Remote Access for single user, Select LAN to LAN for remote gateway.

Peer Network IP: Please input the subnet IP for remote network.

Peer Netmask: Please input the Netmask for remote network.

Exceptional Rule Group

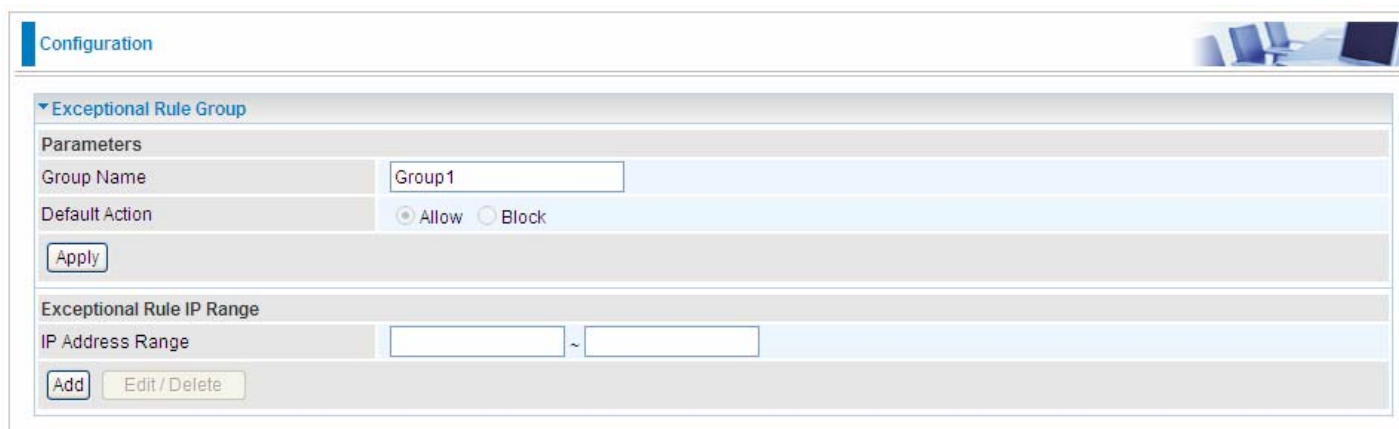
Exceptional Rule is dedicated to giving or blocking PPTP/L2TP server access to some specific IP or IPs(range). Users are allowed to set 8 different exceptional rule groups at most. In each group, user can add specific IP or IP range.



The screenshot shows the 'Configuration' page with a tab for 'Exceptional Rule Group'. Below the tab is a table with the following columns: Group Index, Group Name, Default Action, Exceptional Rule IP Range, and Edit. There are 8 rows, each representing a group from Group1 to Group8. All Default Actions are set to 'Allow'. Each row has an 'Edit' button in the last column.

Group Index	Group Name	Default Action	Exceptional Rule IP Range	Edit
1	Group1	Allow		Edit
2	Group2	Allow		Edit
3	Group3	Allow		Edit
4	Group4	Allow		Edit
5	Group5	Allow		Edit
6	Group6	Allow		Edit
7	Group7	Allow		Edit
8	Group8	Allow		Edit

Press **Edit** to set the exceptional IP (IP Range).



The screenshot shows the 'Configuration' page with a tab for 'Exceptional Rule Group'. Below the tab is a form for editing a group. The form has two main sections: 'Parameters' and 'Exceptional Rule IP Range'. In the 'Parameters' section, there is a 'Group Name' field with 'Group1' entered, a 'Default Action' section with radio buttons for 'Allow' (selected) and 'Block', and an 'Apply' button. In the 'Exceptional Rule IP Range' section, there is an 'IP Address Range' field with two input boxes separated by a tilde (~), and 'Add' and 'Edit / Delete' buttons.

Default Action: Please first set the range to make “**Default Action**” setting available. Set “Allow” to ban the listed IP or IPs to access the PPTP and L2TP server.

Check “Block” to grant access to the listed IP or IPs to the PPTP and L2TP server.

Apply: Press **Apply** button to apply the change.

Exceptional Rule Range

IP Address Range: Specify the IP address range; IPv4 address range can be supported.

Click **Add** to add the IP Range.

For instance, if user wants to block IP range of 172.16.1.102-172.16.1.106 from accessing your PPTP and L2TP server, you can add this IP range and valid it.

Configuration

Exceptional Rule Group

Parameters

Group Name

Group1

Default Action

☒ Allow

☐ Block

Apply

Exceptional Rule IP Range

IP Address Range

~

Add

Edit / Delete

Edit	Action	IP Address Range	Delete
☐	Block	172.16.1.102 ~ 172.16.1.106	☐
☐	Block	172.16.1.108 ~ 172.16.1.108	☐

182

PPTP

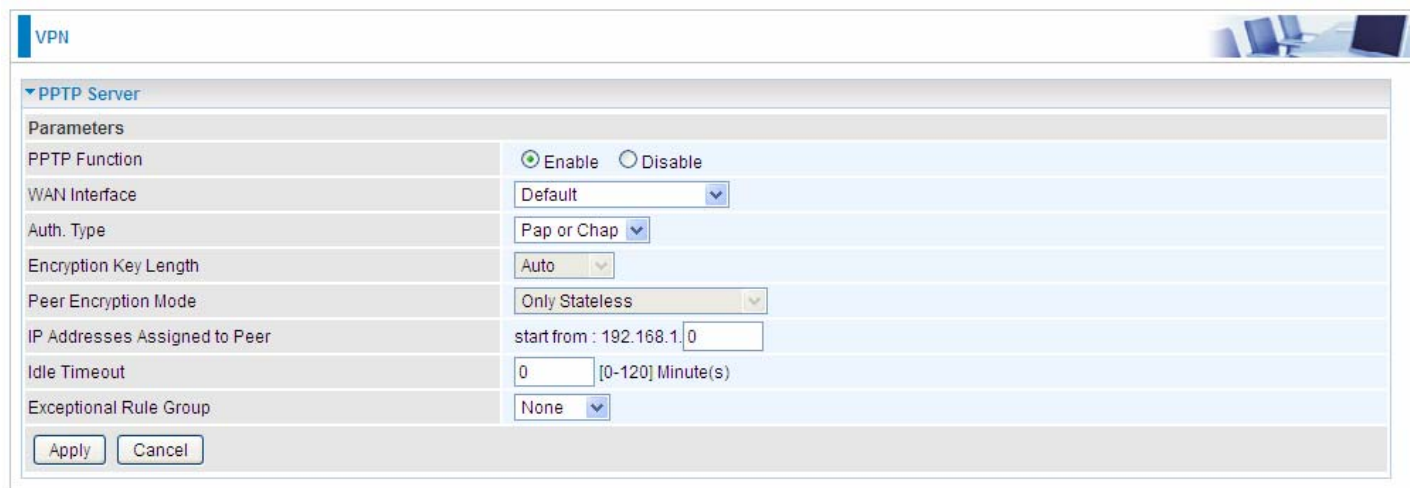
The **Point-to-Point Tunneling Protocol** (PPTP) is a Layer2 tunneling protocol for implementing virtual private networks through IP network. PPTP uses an enhanced GRE (Generic Routing Encapsulation) mechanism to provide a flow- and congestion-controlled encapsulated datagram service for carrying PPP packets.

In the Microsoft implementation, the tunneled PPP traffic can be authenticated with PAP, CHAP, Microsoft CHAP V1/V2 or EAP-TLS. The PPP payload is encrypted using Microsoft Point-to-Point Encryption (MPPE) when using MSCHAPv1/v2 or EAP-TLS.

Note: 4 sessions for Client and 4 sessions for Server respectively.

PPTP Server

In PPTP session, users can set the basic parameters(authentication, encryption, peer address, etc) for PPTP Server, and accounts in the next page of PPTP Account. They both constitutes the PPTP Server setting.



The screenshot shows the 'PPTP Server' configuration window. It has a 'Parameters' section with the following fields:

- PPTP Function:** Radio buttons for 'Enable' (selected) and 'Disable'.
- WAN Interface:** A dropdown menu with 'Default' selected.
- Auth. Type:** A dropdown menu with 'Pap or Chap' selected.
- Encryption Key Length:** A dropdown menu with 'Auto' selected.
- Peer Encryption Mode:** A dropdown menu with 'Only Stateless' selected.
- IP Addresses Assigned to Peer:** A text field with 'start from : 192.168.1.0'.
- Idle Timeout:** A text field with '0' and a range '[0-120] Minute(s)'.
- Exceptional Rule Group:** A dropdown menu with 'None' selected.

At the bottom of the configuration area are 'Apply' and 'Cancel' buttons.

PPTP Function: Select **Enable** to activate PPTP Server. **Disable** to deactivate PPTP Server function.

WAN Interface: Select the exact WAN interface configured for the tunnel. Select **Default** to use the now-working WAN interface for the tunnel.

Auth. Type: The authentication type, Pap or Chap, PaP, Chap and MS-CHAPv2. When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that an intruder has not replaced the client. When passed the authentication with MS-CHAPv2, the MPPE encryption is supported.

Encryption Key Length: The data can be encrypted by MPPE algorithm with 40 bits or 128 bits. Default is Auto, it is negotiated when establishing a connection. 128 bit keys provide stronger encryption than 40 bit keys.

Peer Encryption Mode: You may select "Only Stateless" or "Allow Stateless and Stateful" mode. The key will be changed every packet when you select Stateless mode.

IP Addresses Assigned to Peer: 192.168.1.x: please input the IP assigned range from 1~ 254.

Idle Timeout: Specify the time for remote peer to be disconnected without any activities, from 0~120

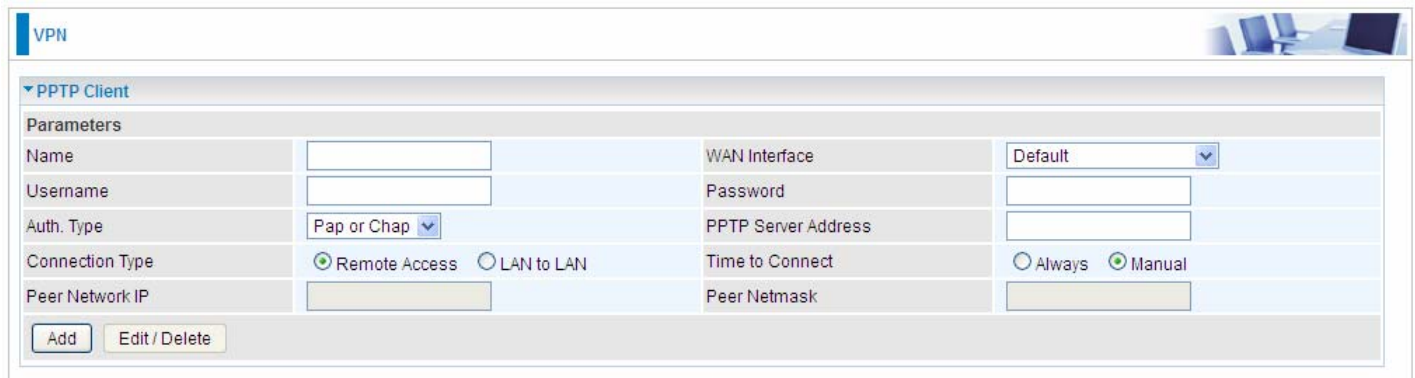
minutes.

Exceptional Rule Group: Select to grant or block access to a group of IPs to the PPTP server. See [Exceptional Rule Group](#). If there is not any restriction, select none.

Click **Apply** to submit your PPTP Server basic settings.

PPTP Client

PPTP client can help you dial-in the PPTP server to establish PPTP tunnel over Internet.



Name: user-defined name for identification.

WAN Interface: Select the exact WAN interface configured for the tunnel. Select Default to use the now-working WAN interface for the tunnel.

Username: Enter the username provided by your VPN Server.

Password: Enter the password provided by your VPN Server.

Auth. Type: Default is Auto if you want the router to determine the authentication type to use, or else manually specify CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol) if you know which type the server is using (when acting as a client), or else the authentication type you want clients connecting to you to use (when acting as a server). When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that an intruder has not replaced the client.

PPTP Server Address: Enter the IP address of the PPTP server.

Connection Type: Select Remote Access for single user, Select LAN to LAN for remote gateway.

Time to Connect: Select Always to keep the connection always on, or Manual to connect manually any time.

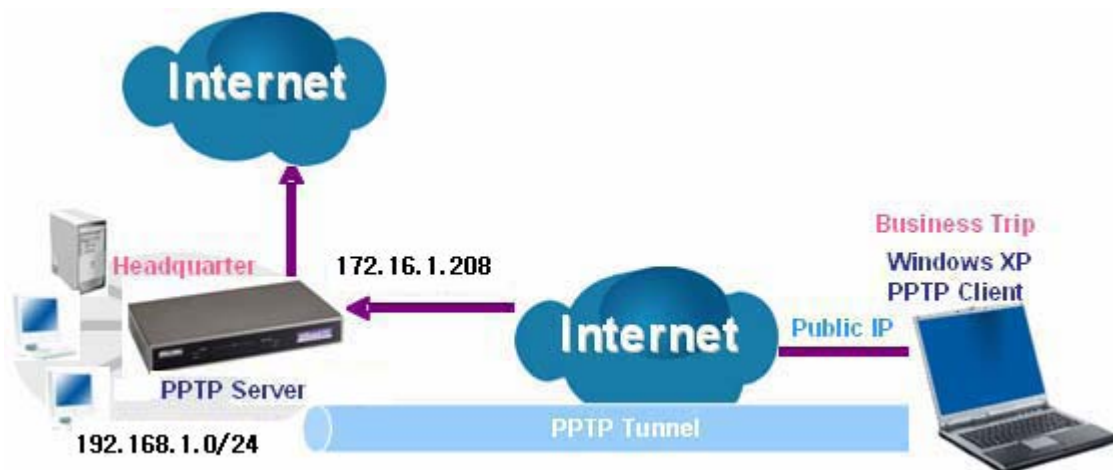
Peer Network IP: Please input the subnet IP for Server peer.

Peer Netmask: Please input the Netmask for server peer.

Click **Add** button to save your changes.

Example: PPTP Remote Access with Windows7

(Note: inside test with 172.16.1.208, just an example for illustration)



Server Side:

1. Configuration > VPN > PPTP and Enable the PPTP function, Click **Apply**.

VPN

▼ PPTP Server

Parameters

PPTP Function	☒ Enable ☐ Disable
WAN Interface	Default
Auth. Type	MS-CHAPv2
Encryption Key Length	Auto
Peer Encryption Mode	Only Stateless
IP Addresses Assigned to Peer	start from : 192.168.1.00
Idle Timeout	10 [0-120] Minute(s)
Exceptional Rule Group	None

Apply Cancel

2. Create a PPTP Account “test”.

VPN

▼ VPN Account

VPN Account applied to PPTP Server and L2TP Server.

Parameters

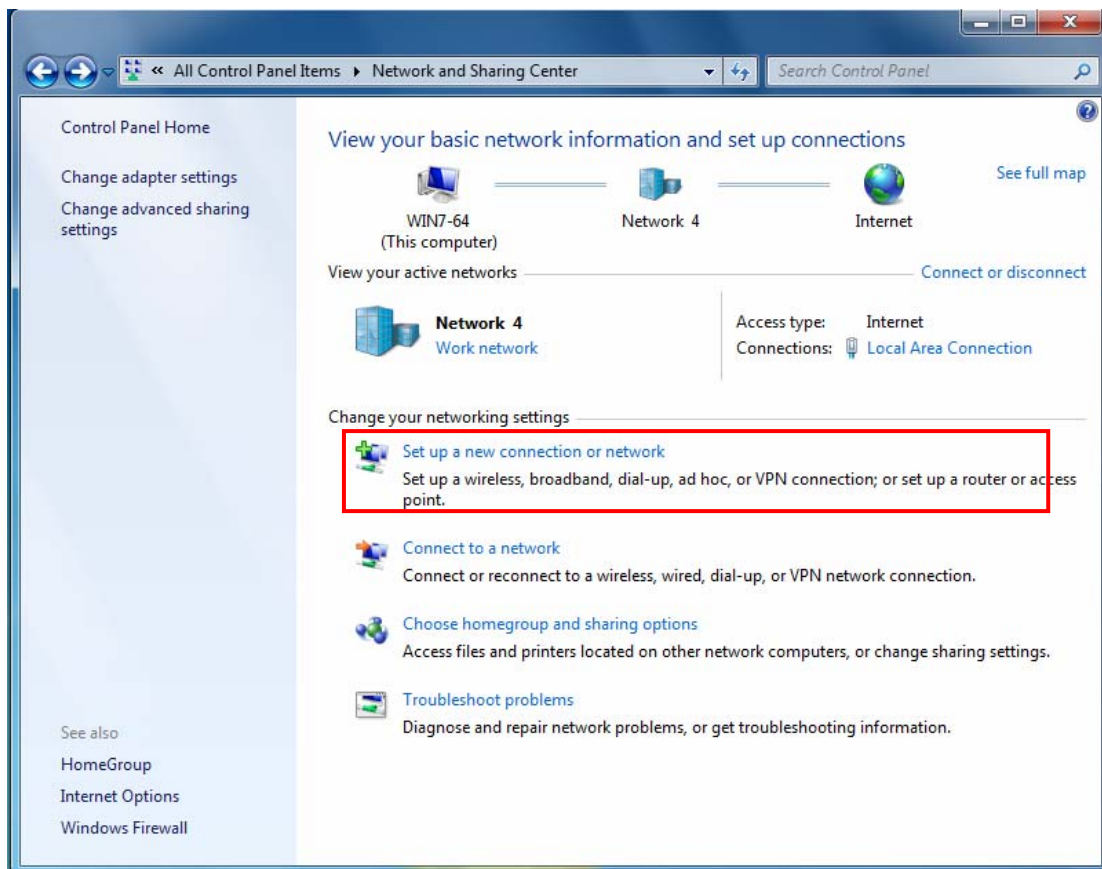
Name		Tunnel	☒ Enable ☐ Disable
Username		Password	
Connection Type	☒ Remote Access ☐ LAN to LAN		
Peer Network IP		Peer Netmask	

Add Edit / Delete

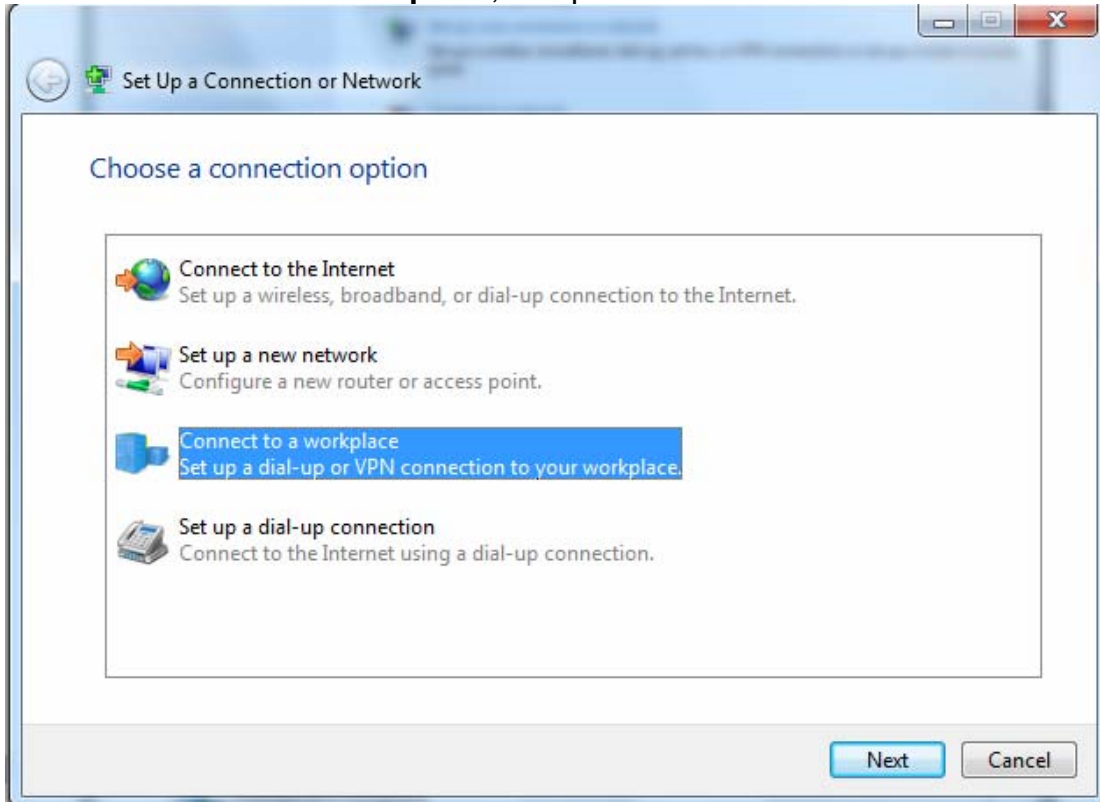
Edit	Name	Tunnel	Connection Type	Peer Network IP	Peer Netmask	Delete
☐	test	Enable	Remote Access			☐

Client Side:

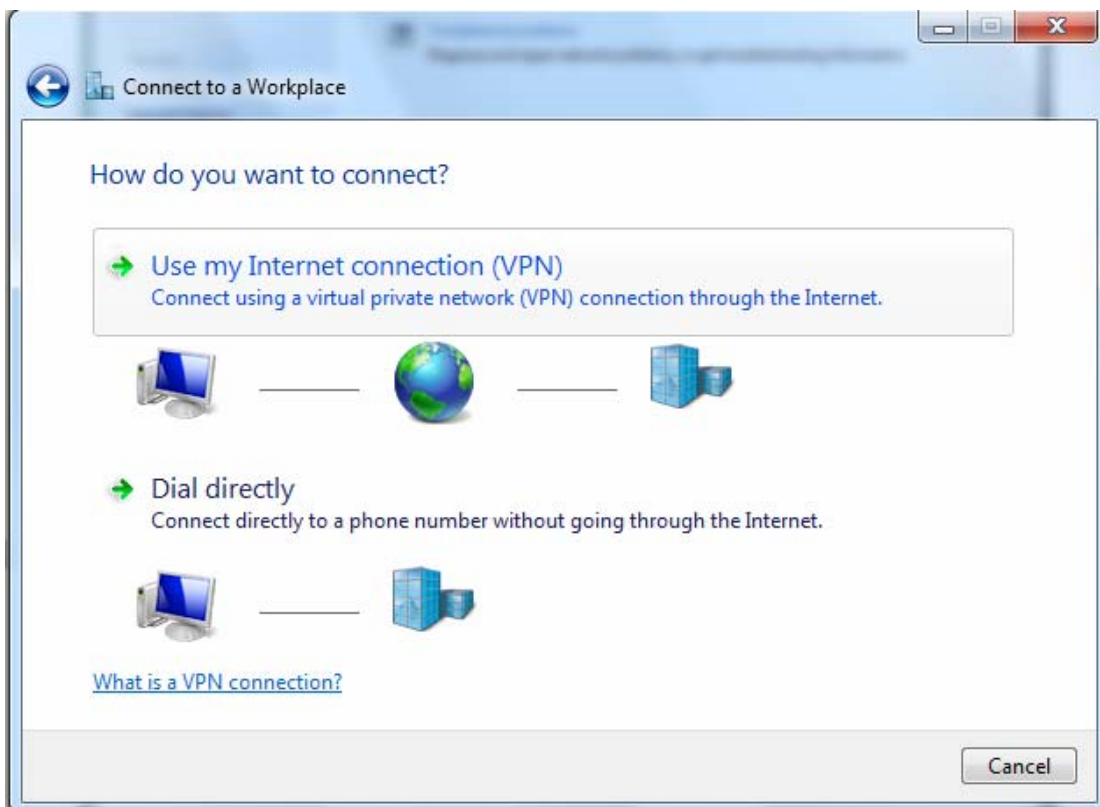
1. In Windows7 click **Start > Control Panel> Network and Sharing Center**, Click **Set up a new connection network**.



2. Click **Connect to a workplace**, and press **Next**.



3. Select **Use my Internet connection (VPN)** and press **Next**.



4. Input **Internet address** and **Destination name** for this connection and press **Next**.

Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: [Example: Contoso.com or 157.54.0.1 or 3ffe:1234::1111]

Destination name: VPN Connection

☐ Use a smart card

☐ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

☐ Don't connect now; just set it up so I can connect later

Next Cancel

Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: 172.16.1.208

Destination name: test

☐ Use a smart card

☒ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

☒ Don't connect now; just set it up so I can connect later

Next Cancel

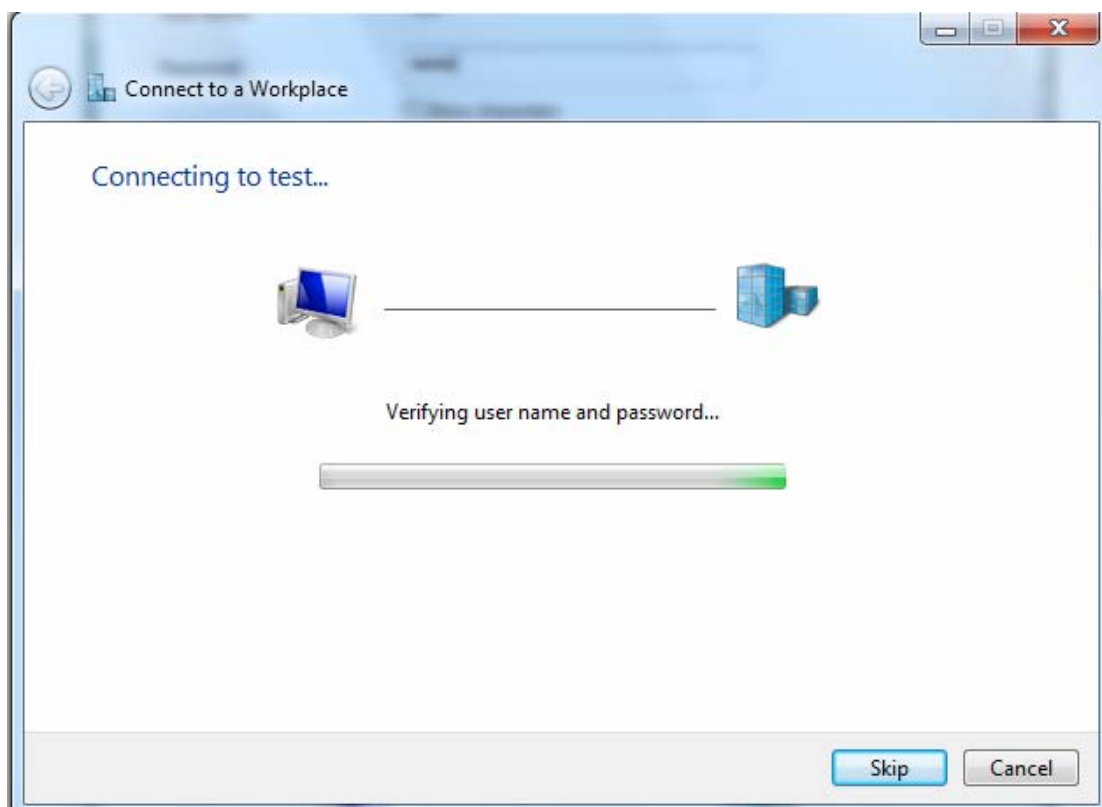
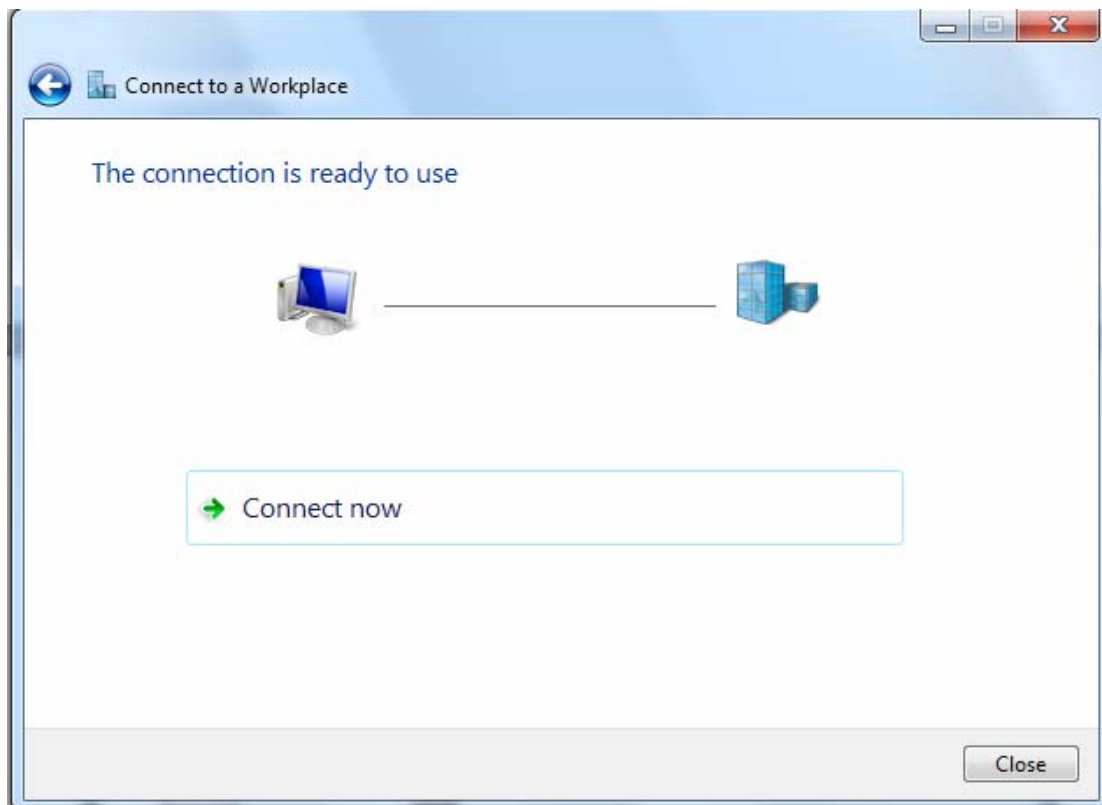
5. Input the account (**user name** and **password**) and press **Create**.

The image displays two sequential screenshots of a Windows-style dialog box titled "Connect to a Workplace".

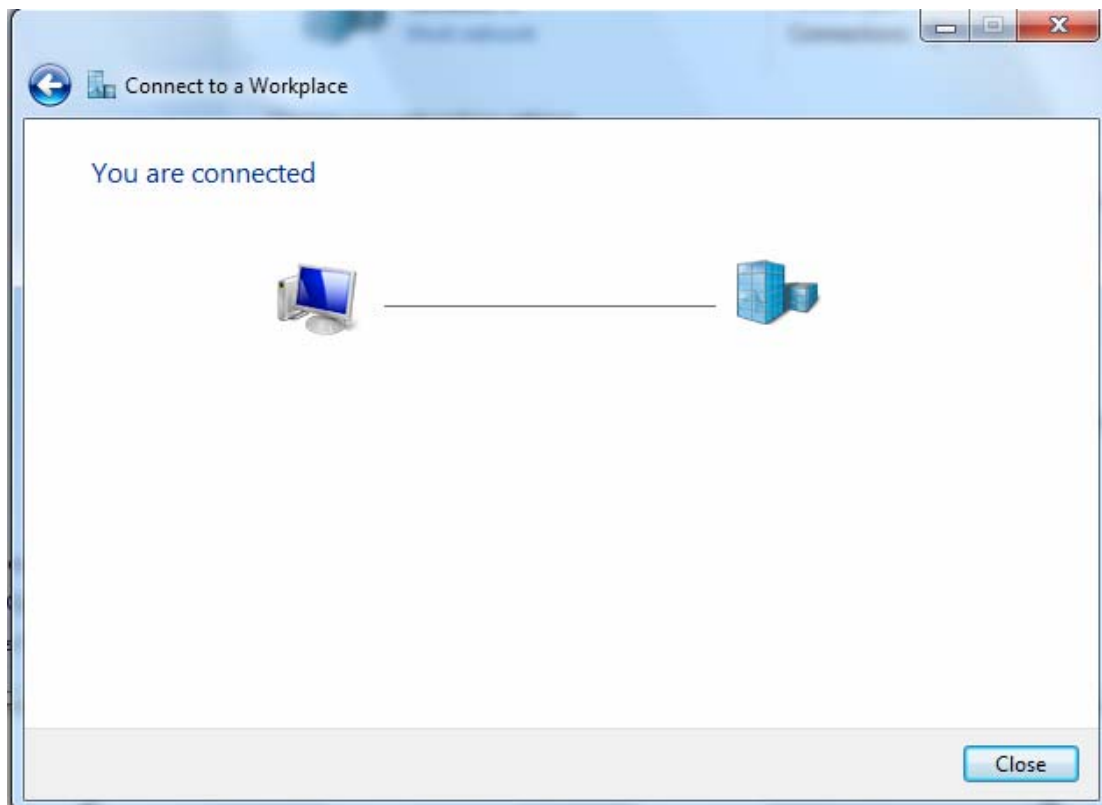
Top Screenshot: The dialog box contains the instruction "Type your user name and password". It features four input fields: "User name:", "Password:", "Domain (optional):", and a checkbox area with "Show characters" and "Remember this password". The "User name" and "Password" fields are currently empty.

Bottom Screenshot: This screenshot shows the same dialog box after some input. The "User name" field now contains the text "test". The "Password" field contains four masked characters (dots). The "Domain (optional)" field remains empty. The "Show characters" and "Remember this password" checkboxes are still unchecked.

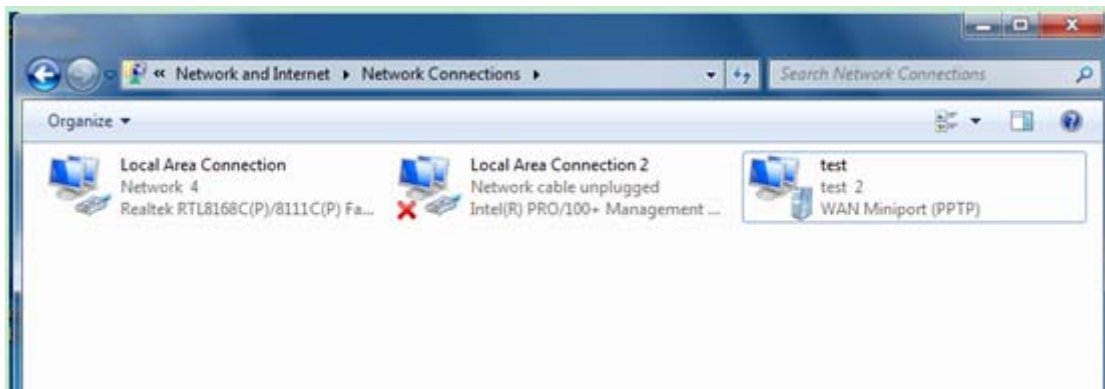
6. Connect to the server.

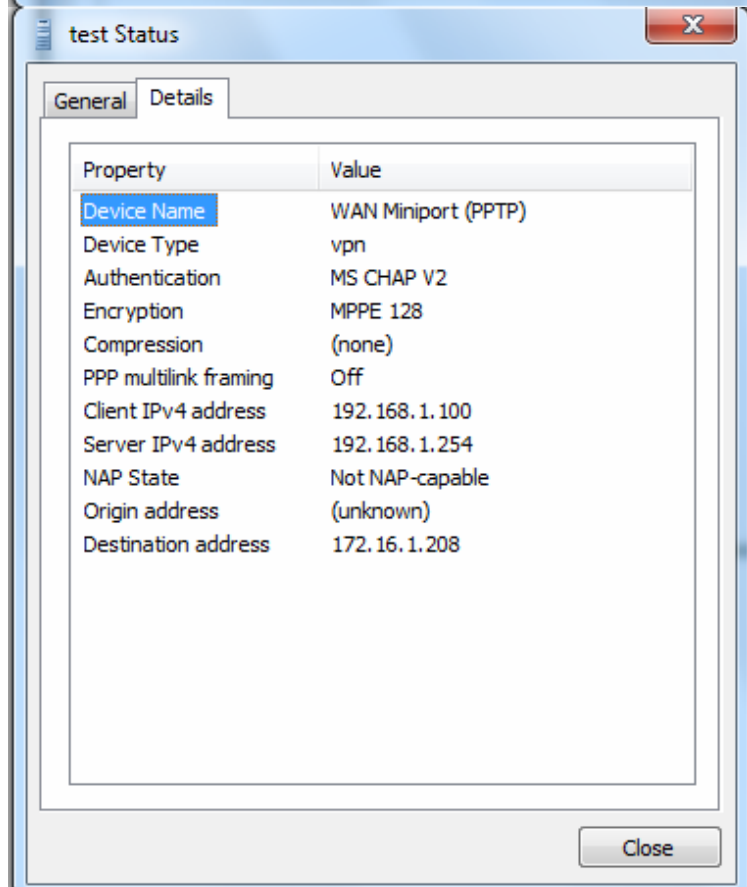
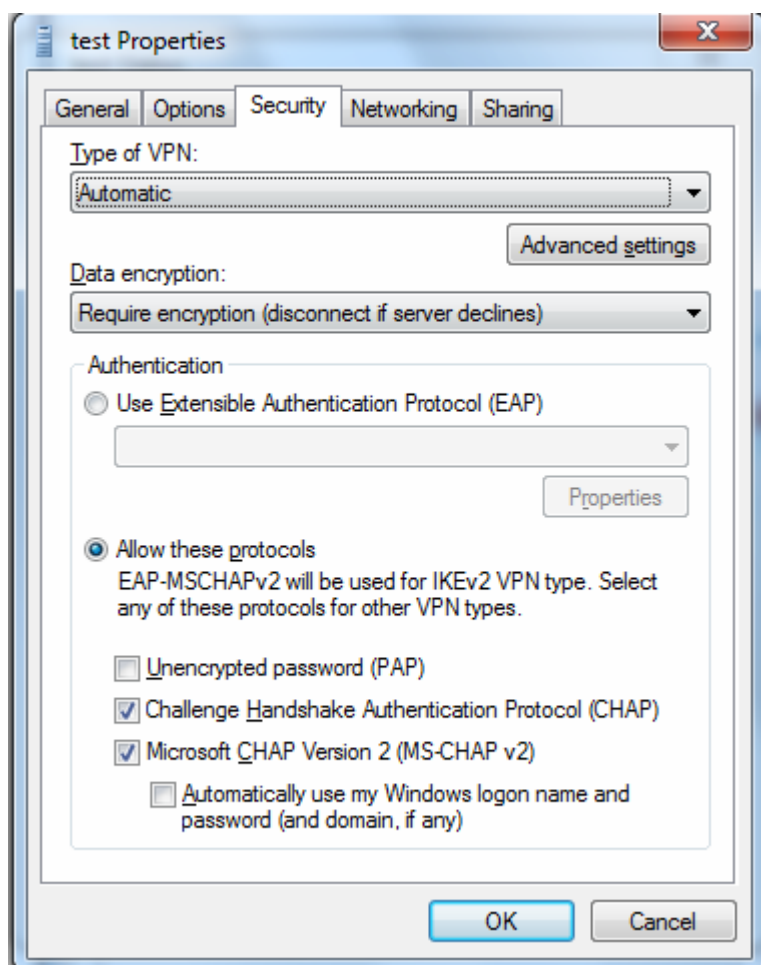


7. Successfully connected.



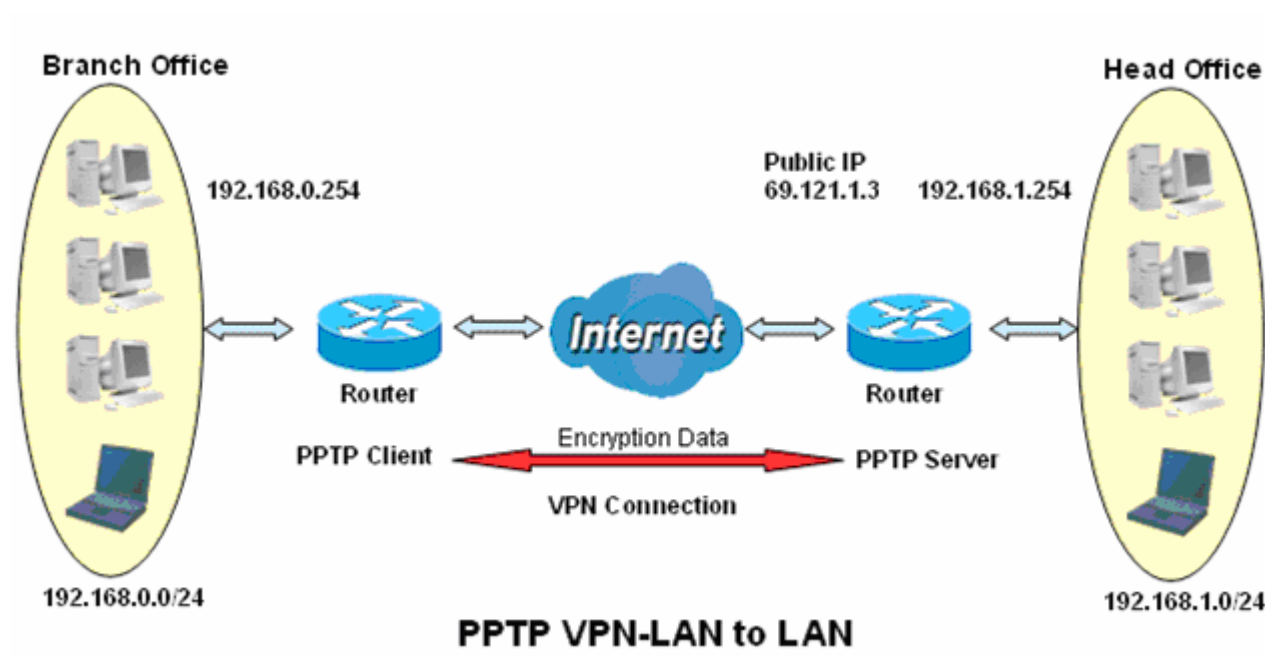
PS: You can also go to **Network Connections** shown below to check the detail of the connection. Right click "test" icon, and select "Properties" to change the security parameters (if the connection fails, users can go here to change the settings)





Example: Configuring a LAN-to-LAN PPTP VPN Connection

The branch office establishes a PPTP VPN tunnel with head office to connect two private networks over the Internet. The routers are installed in the head office and branch offices accordingly.



Server side: Head Office

VPN

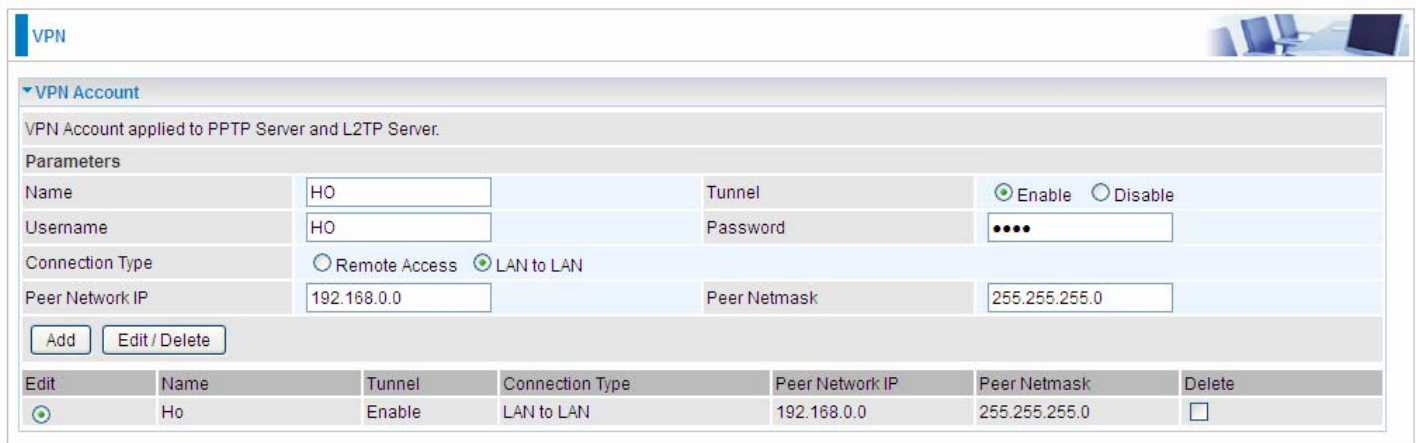
▼ PPTP Server

Parameters	
PPTP Function	☒ Enable ☐ Disable
WAN Interface	Default
Auth. Type	MS-CHAPv2
Encryption Key Length	Auto
Peer Encryption Mode	Only Stateless
IP Addresses Assigned to Peer	start from : 192.168.1.00
Idle Timeout	10 [0-120] Minute(s)
Exceptional Rule Group	None

Apply Cancel

The above is the common setting for PPTP Server, set as you like for authentication and encryption. The settings in Client side should be in accordance with settings in Server side.

Then the PPTP Account.



VPN

▼ **VPN Account**

VPN Account applied to PPTP Server and L2TP Server.

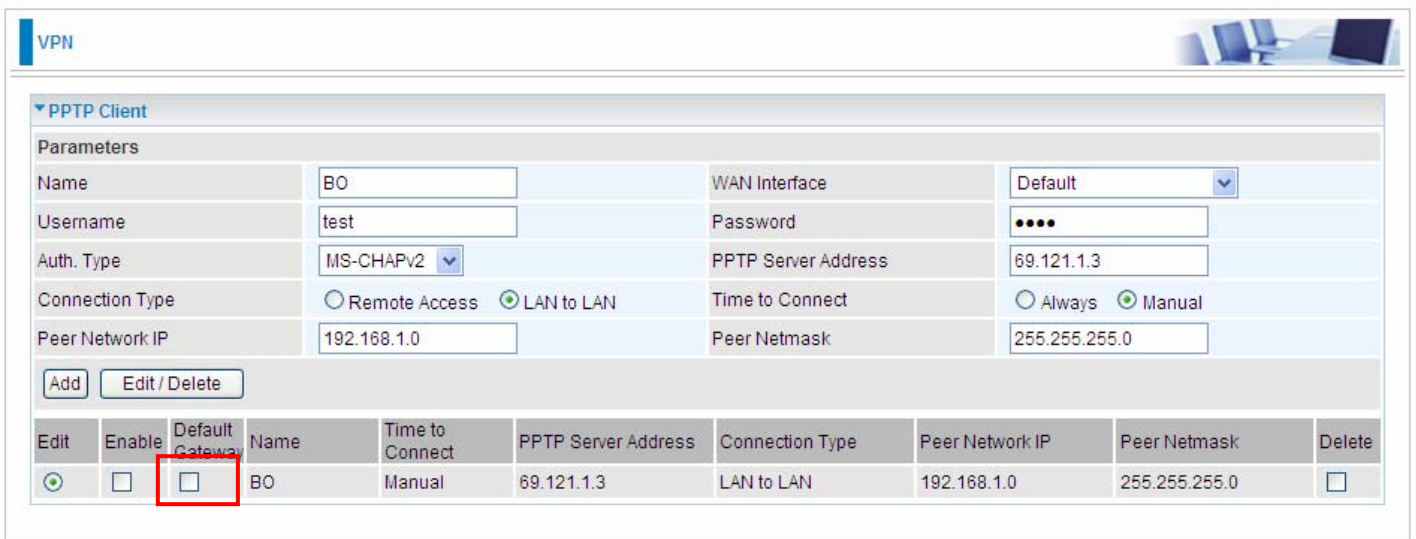
Parameters

Name	HO	Tunnel	☒ Enable ☐ Disable
Username	HO	Password	••••
Connection Type	☐ Remote Access ☒ LAN to LAN		
Peer Network IP	192.168.0.0	Peer Netmask	255.255.255.0

Edit	Name	Tunnel	Connection Type	Peer Network IP	Peer Netmask	Delete
☒	Ho	Enable	LAN to LAN	192.168.0.0	255.255.255.0	☐

Client Side: Branch Office

The client user can set up a tunnel connecting to the PPTP server, and can also set the tunnel as the default route for all outgoing traffic.



VPN

▼ **PPTP Client**

Parameters

Name	BO	WAN Interface	Default
Username	test	Password	••••
Auth. Type	MS-CHAPv2	PPTP Server Address	69.121.1.3
Connection Type	☐ Remote Access ☒ LAN to LAN		
Peer Network IP	192.168.1.0	Peer Netmask	255.255.255.0

Edit	Enable	Default Gateway	Name	Time to Connect	PPTP Server Address	Connection Type	Peer Network IP	Peer Netmask	Delete
☒	☐	☐	BO	Manual	69.121.1.3	LAN to LAN	192.168.1.0	255.255.255.0	☐

Note: users can see the “Default Gateway” item in the bar, and user can check to select the tunnel as the default gateway (default route) for traffic. If selected, all outgoing traffic will be forwarded to this tunnel and routed to the next hop.

L2TP

The **Layer 2 Tunneling Protocol (L2TP)** is a Layer2 tunneling protocol for implementing virtual private networks.

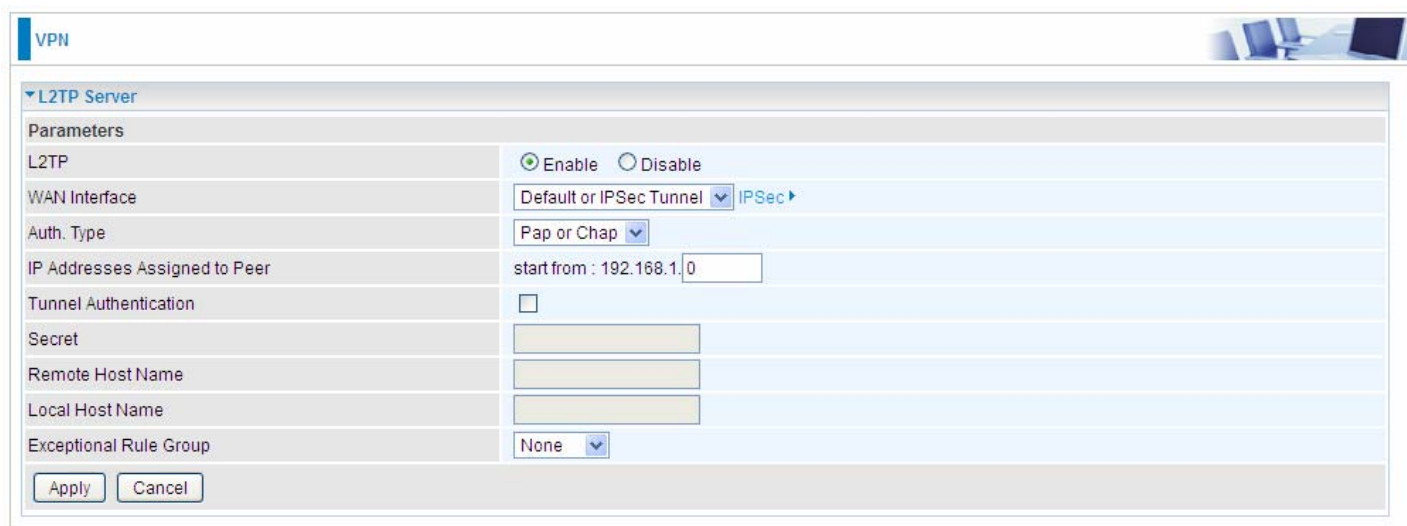
L2TP does not provide confidentiality or strong authentication by itself. IPsec is often used to secure L2TP packets by providing confidentiality, authentication and integrity. The combination of these two protocols is generally known as L2TP/IPsec.

In L2TP section, both pure L2TP and L2TP/IPSec are supported. Users can choose your preferable option for your own needs.

Note: 4 sessions for Client and only one for Server respectively.

L2TP Server

In L2TP session, users can set the basic parameters(authentication, encryption, peer address, etc) for L2TP Server, and accounts in the page of VPN Account. They both constitutes the complete L2TP Server settings.



L2TP: Select **Enable** to activate L2TP Server. **Disable** to deactivate L2TP Server.

WAN Interface: Select the exact WAN interface configured as source for the tunnel. Select different interfaces, you will decide whether to use L2TP over IPsec or the pure L2TP.

- ① **L2TP over IPsec,** Select “Default or IPsec Tunnel” only when there is IPsec for L2TP rule in place.
- ① **Pure L2TP,** Select Default (there is no IPsec for L2TP in place) or other interface to activate the pure L2TP.

Auth. Type: The authentication type, Pap or Chap, PaP, Chap. When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that an intruder has not replaced the client.

IP Addresses Assigned to Peer: 192.168.1.x: please input the IP assigned range from 1~ 254.

Tunnel Authentication: Select whether to enable L2TP tunnel authentication. Enable it if needed

and set the same in the client side.

Secret: Enter the secretly pre-shared password for tunnel authentication.

Remote Host Name: Enter the remote host name (of peer) featuring the destination of the L2TP tunnel.

Local Host Name: Enter the local host name featuring the source of the L2TP tunnel.

Exceptional Rule Group: Select to grant or block access to a group of IPs to the L2TP server. See [Exceptional Rule Group](#). If there is not any restriction, select none.

Click **Apply** to submit your L2TP Server basic settings.

L2TP Client

L2TP client can help you dial-in the L2TP server to establish L2TP tunnel over Internet.

Parameters			
Name		L2TP over IPsec	☐ Enable
WAN Interface	Default		
Username		Password	
Auth. Type	Pap or Chap	L2TP Server Address	
Connection Type	☒ Remote Access ☐ LAN to LAN		
Peer Network IP		Peer Netmask	
Tunnel Authentication	☐	Secret	
Remote Host Name		Local Host Name	

Name: user-defined name for identification.

L2TP over IPsec: If your L2TP server has used L2TP over IPsec feature, please enable this item. under this circumstance, client and server communicate using L2TP over IPsec.

① Enable

Parameters			
Name		L2TP over IPsec	☒ Enable
IPSec Tunnel	test2	IPSec	
Username		Password	
Auth. Type	Pap or Chap	L2TP Server Address	
Connection Type	☒ Remote Access ☐ LAN to LAN		
Peer Network IP		Peer Netmask	
Tunnel Authentication	☐	Secret	
Remote Host Name		Local Host Name	

IPsec Tunnel: Select the appropriate IPsec for L2TP rule configured for the L2TP Client.

Username: Enter the username provided by your L2TP Server.

Password: Enter the password provided by your L2TP Server.

Auth. Type: Default is Pap or CHap if you want the router to determine the authentication type to use, or else manually specify CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol) if you know which type the server is using. When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that an intruder has not replaced the client.

L2TP Server Address: Enter the IP address of the L2TP server.

Connection Type: Select Remote Access for single user, Select LAN to LAN for remote gateway.

Peer Network IP: Please input the subnet IP for Server.

Peer Netmask: Please input the Netmask for Server.

Tunnel Authentication: Select whether to enable L2TP tunnel authentication, if the server side enables this feature, please follow.

Secret: Enter the set secret password in the server side.

Remote Host Name: Enter the remote host name featuring the destination of the L2TP tunnel.

Local Host Name: Enter the local host name featuring the source of the L2TP tunnel.

Click **Add** button to save your changes.

❶ Disable



The screenshot shows the 'VPN' configuration page with a sub-tab for 'L2TP Client'. Under the 'Parameters' section, there is a table of configuration fields:

Name		L2TP over IPSec	☐ Enable
WAN Interface	Default		
Username		Password	
Auth. Type	Pap or Chap	L2TP Server Address	
Connection Type	☒ Remote Access ☐ LAN to LAN		
Peer Network IP		Peer Netmask	
Tunnel Authentication	☐	Secret	
Remote Host Name		Local Host Name	

At the bottom of the form are two buttons: 'Add' and 'Edit / Delete'.

WAN Interface: Select the exact WAN interface configured for the tunnel. Select Default to use the now-working WAN interface for the tunnel. Under this circumstance, client and server communicate through pure L2TP server.

Username: Enter the username provided by your L2TP Server.

Password: Enter the password provided by your L2TP Server.

Auth. Type: Default is Pap or CHap if you want the router to determine the authentication type to use, or else manually specify CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol) if you know which type the server is using. When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that an intruder has not replaced the client.

L2TP Server Address: Enter the IP address of the L2TP server.

Connection Type: Select Remote Access for single user, Select LAN to LAN for remote gateway.

Peer Network IP: Please input the subnet IP for Server.

Peer Netmask: Please input the Netmask for server.

Tunnel Authentication: Select whether to enable L2TP tunnel authentication, if the server side enables this feature, please follow.

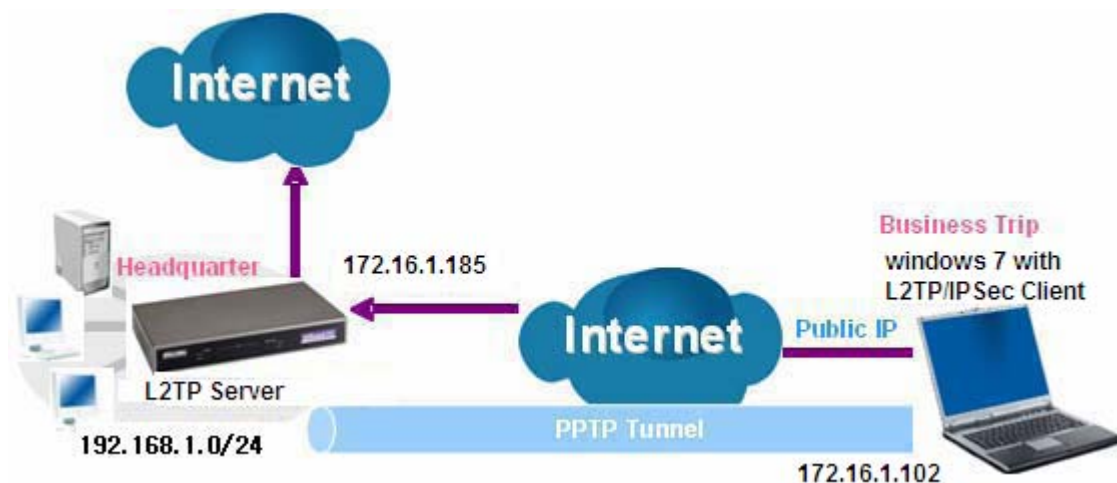
Secret: Enter the set secret password in the server side.

Remote Host Name: Enter the remote host name featuring the destination of the L2TP tunnel.

Local Host Name: Enter the local host name featuring the source of the L2TP tunnel.

Click **Add** button to save your changes.

Example: L2TP over IPSec Remote Access with Windows7
(Note: inside test with 172.16.1.185, just an example for illustration)



Server Side:

- 1. Configuration > VPN > L2TP** and Enable the L2TP function, Click **Apply**.

VPN

L2TP Server

Parameters

L2TP ☒ Enable ☐ Disable

WAN Interface

Auth. Type

IP Addresses Assigned to Peer start from : 192.168.1.10

Tunnel Authentication ☐

Secret

Remote Host Name

Local Host Name

Exceptional Rule Group

The IPSec for L2TP rule

VPN

IPSec

IPSec Settings

L2TP over IPSec ☒ Enable

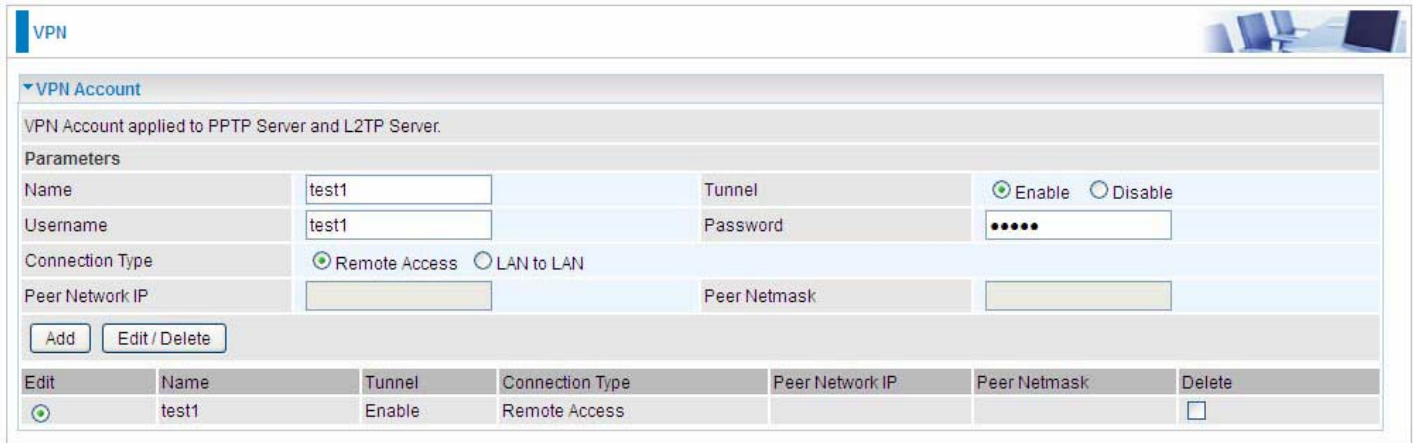
Connection Name WAN Interface IP Version

Remote Security Gateway ☒ Anonymous

Key Exchange Method IPsec Protocol

Pre-Shared Key

2. Create a L2TP Account “test1”.



VPN

VPN Account

VPN Account applied to PPTP Server and L2TP Server.

Parameters

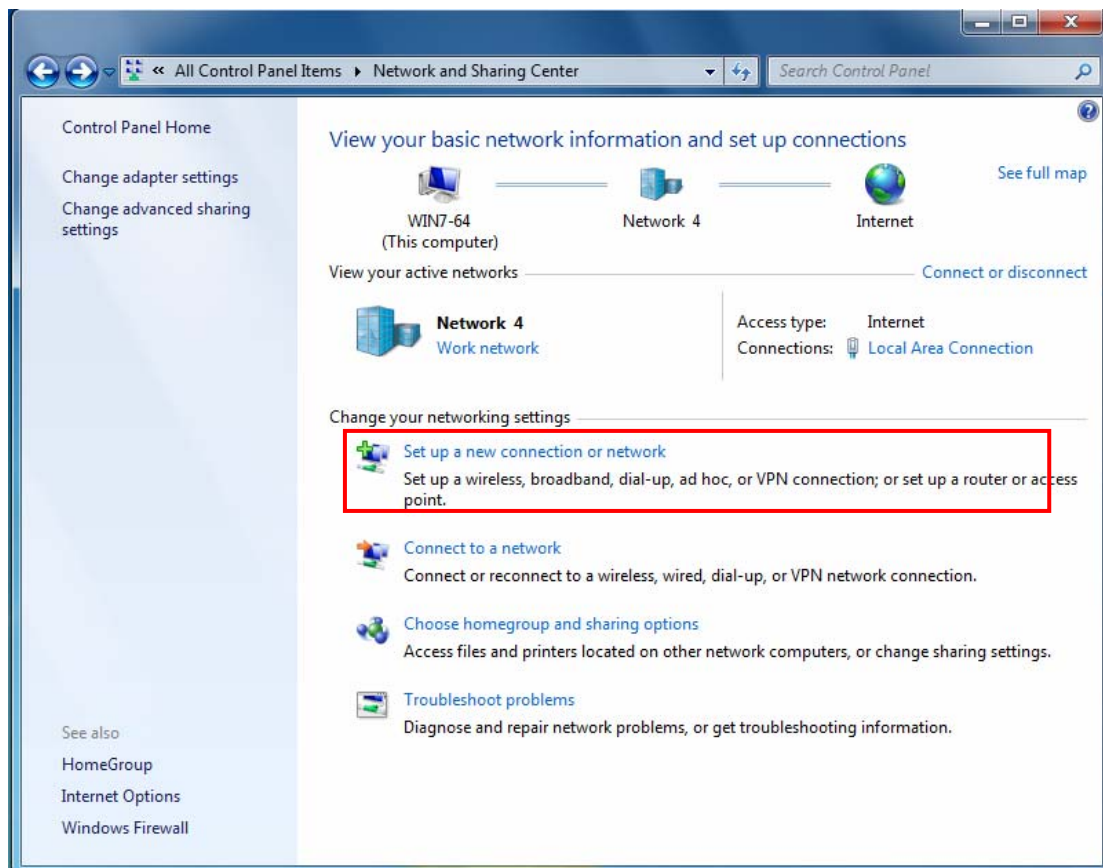
Name	test1	Tunnel	☒ Enable ☐ Disable
Username	test1	Password	
Connection Type	☒ Remote Access ☐ LAN to LAN		
Peer Network IP		Peer Netmask	

Add Edit / Delete

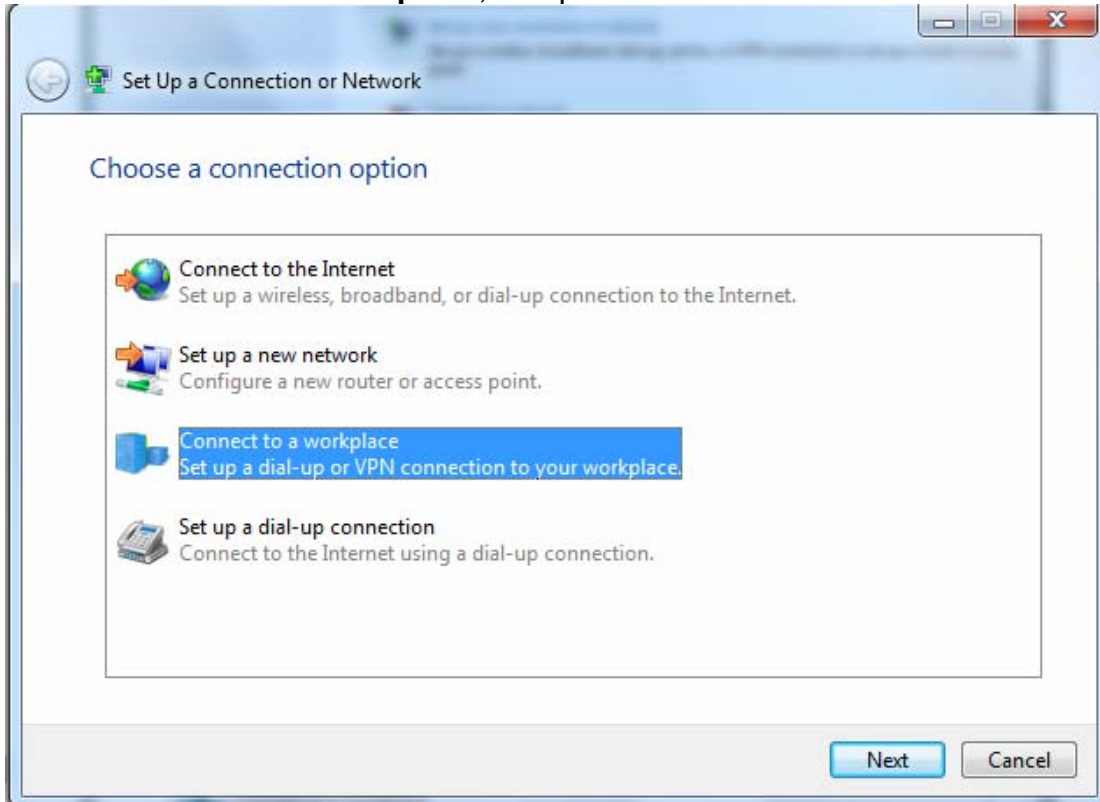
Edit	Name	Tunnel	Connection Type	Peer Network IP	Peer Netmask	Delete
☒	test1	Enable	Remote Access			☐

Client Side:

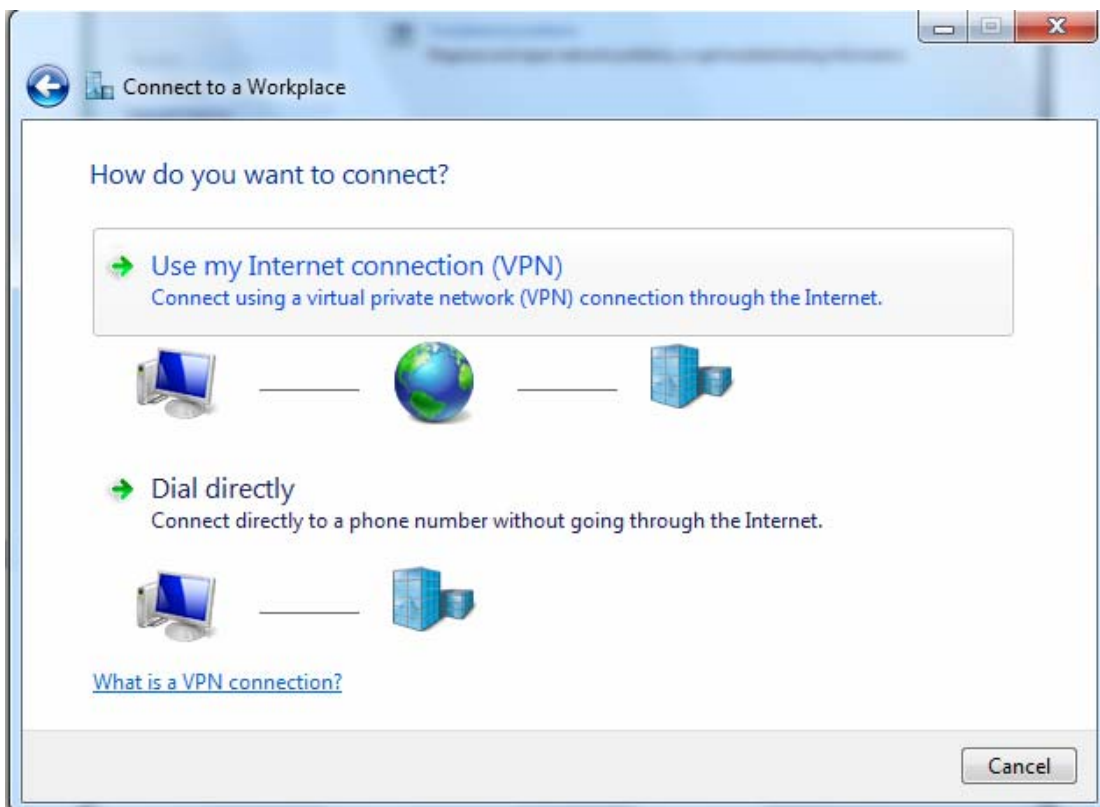
1. In Windows7 click **Start > Control Panel> Network and Sharing Center**, Click **Set up a new connection network**.



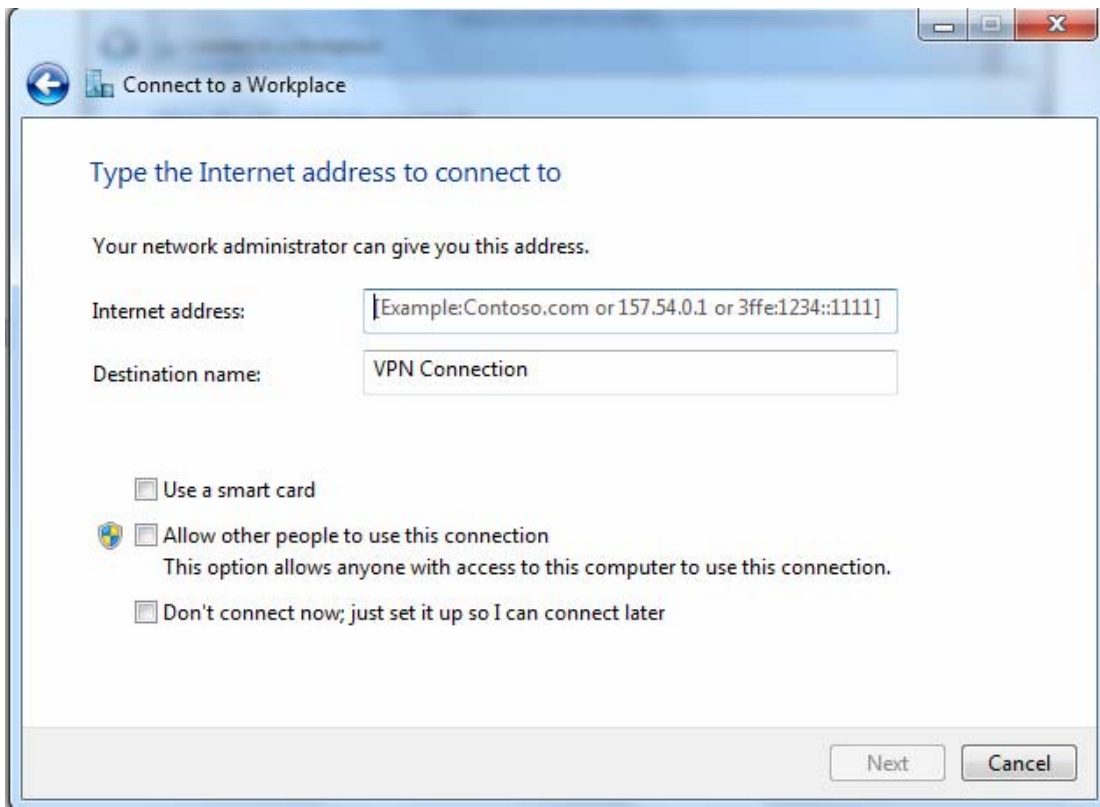
2. Click **Connect to a workplace**, and press **Next**.



3. Select **Use my Internet connection (VPN)** and press **Next**.



4. Input **Internet address** and **Destination name** for this connection and press **Next**.



Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: [Example:Contoso.com or 157.54.0.1 or 3ffe:1234::1111]

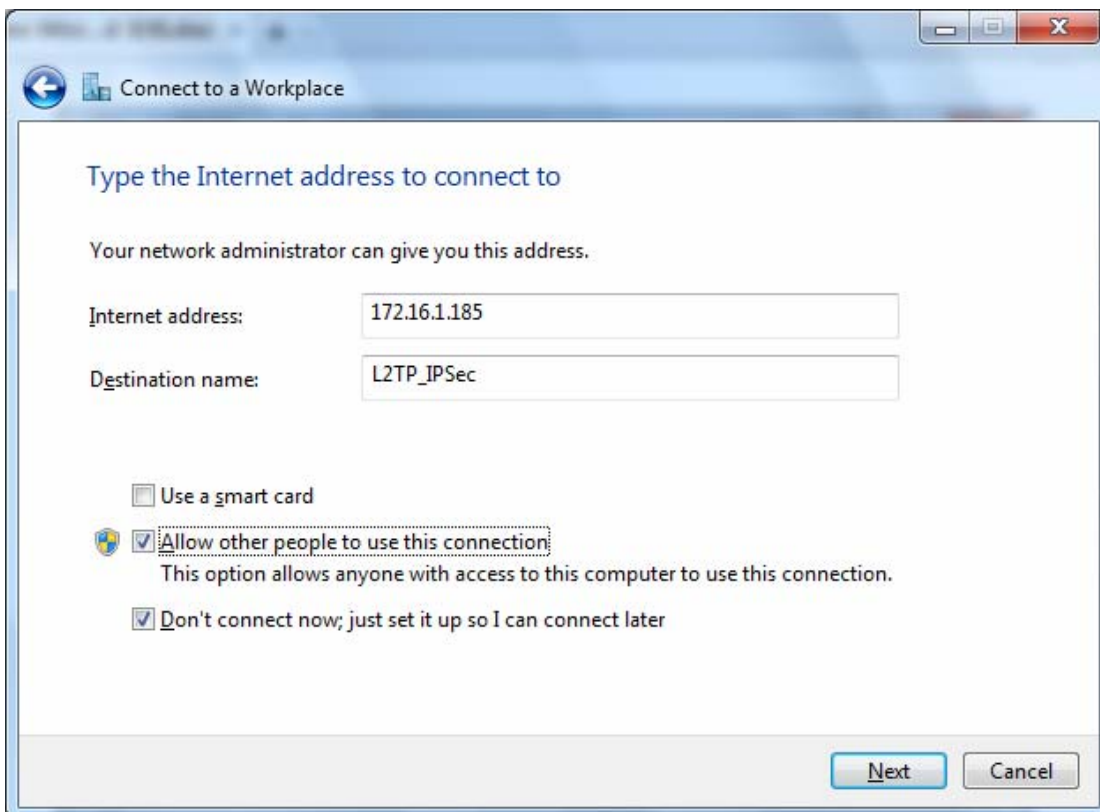
Destination name: VPN Connection

☐ Use a smart card

☐ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

☐ Don't connect now; just set it up so I can connect later

Next Cancel



Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: 172.16.1.185

Destination name: L2TP_IPSec

☐ Use a smart card

☒ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

☒ Don't connect now; just set it up so I can connect later

Next Cancel

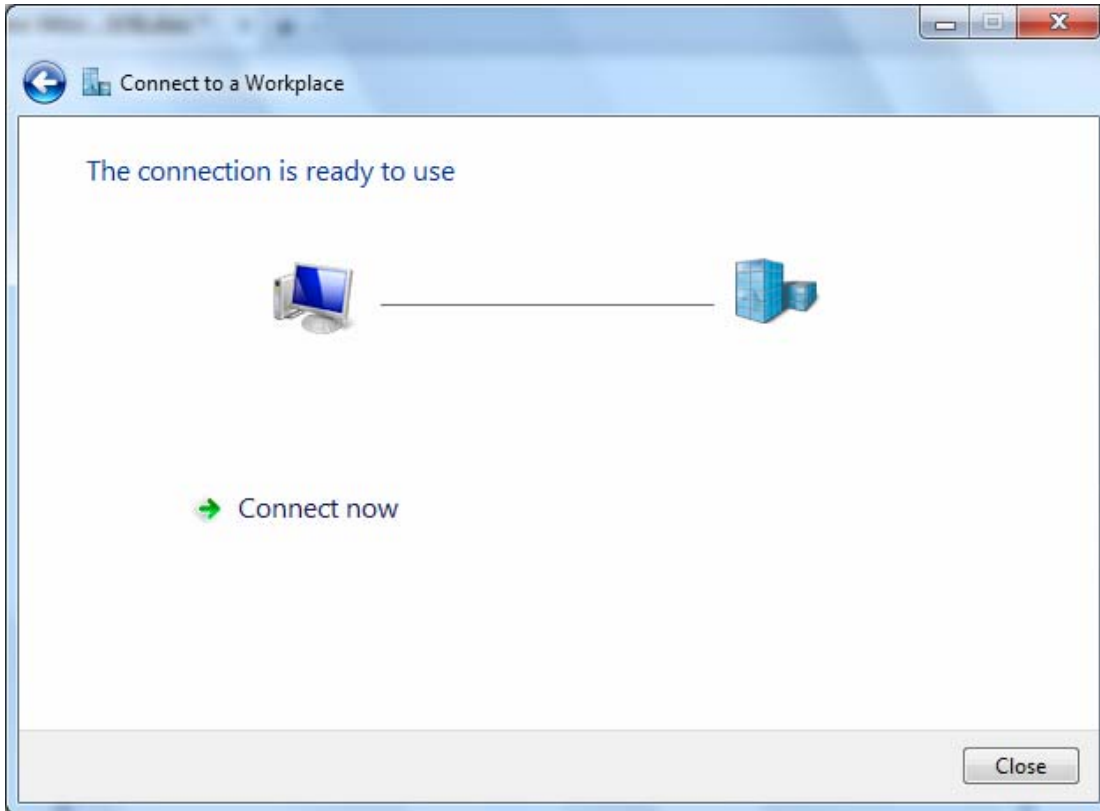
5. Input the account (**user name** and **password**) and press **Create**.

The image displays two sequential screenshots of a software dialog box titled "Connect to a Workplace".

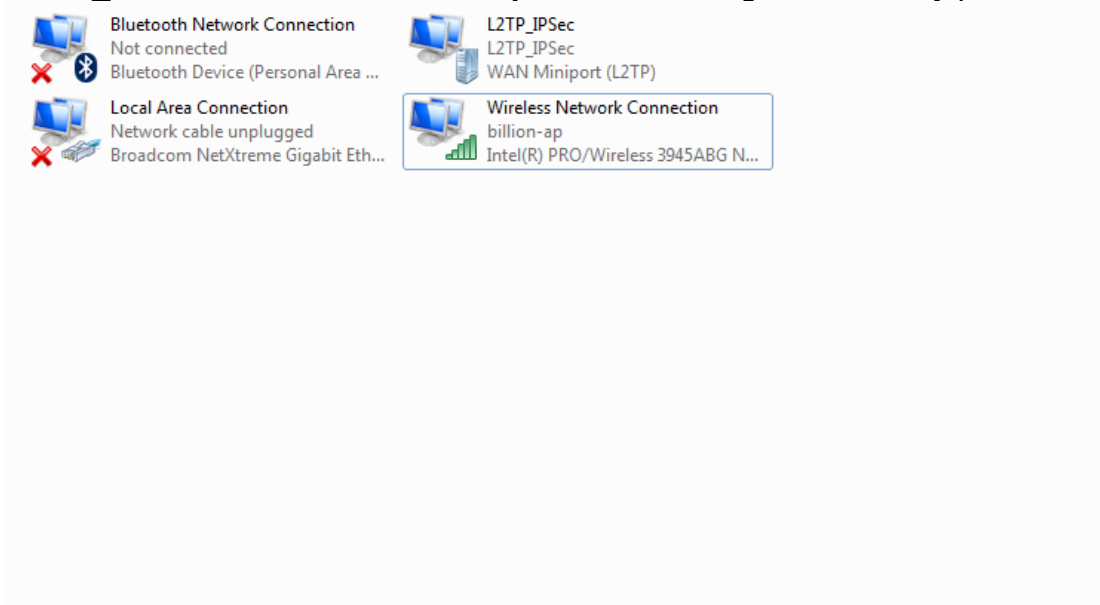
Top Screenshot: The dialog box is open, showing the title bar with standard window controls. The main area is titled "Type your user name and password". It contains three input fields: "User name:", "Password:", and "Domain (optional):". The "User name" field has a cursor. Below the "Password" field are two checkboxes: "Show characters" and "Remember this password". At the bottom right are "Create" and "Cancel" buttons.

Bottom Screenshot: The same dialog box is shown, but the "User name" field now contains the text "test1". The "Password" field contains five dots, indicating masked input. The other elements remain the same.

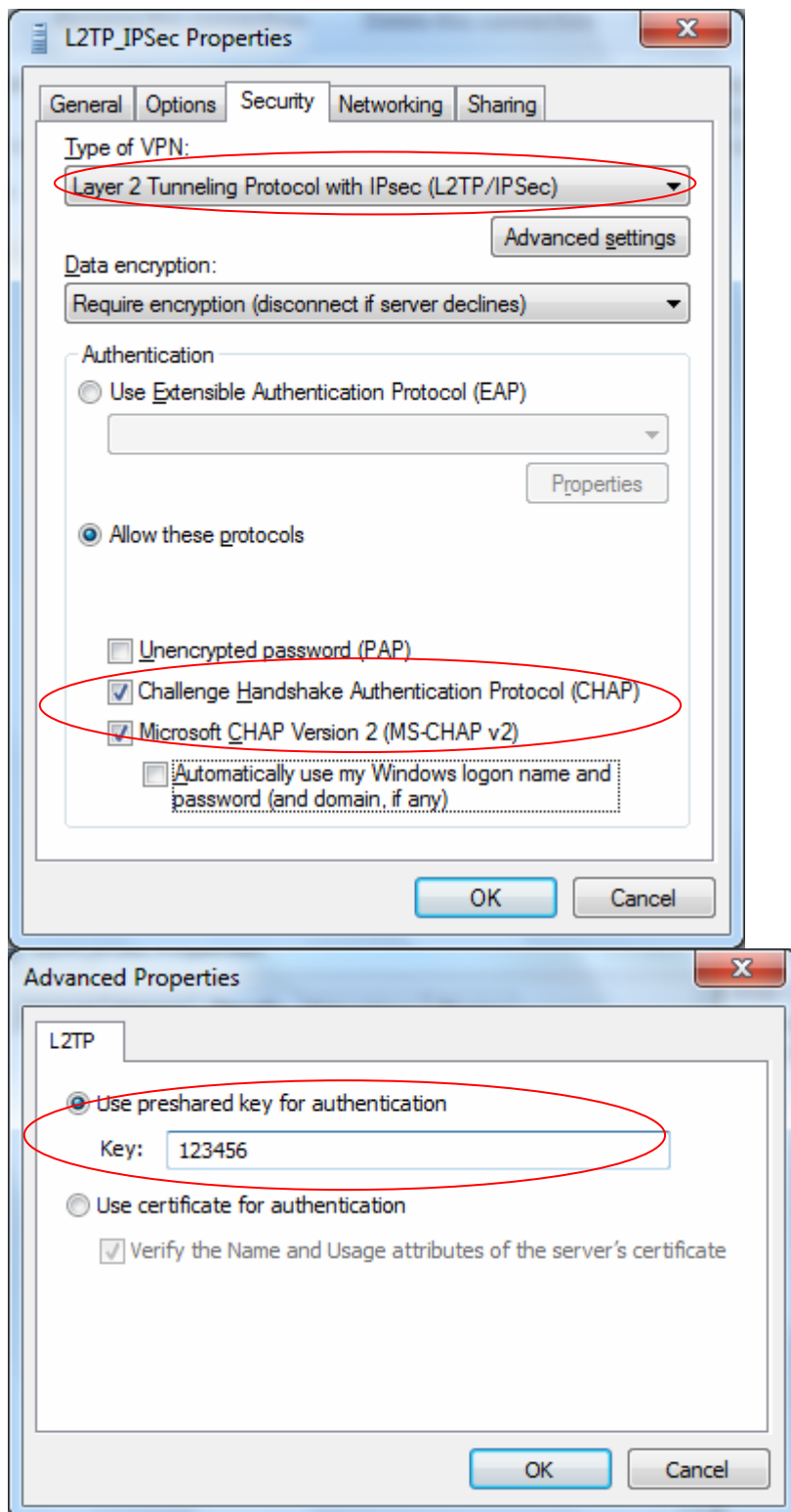
6. Connection created. Press **Close**.



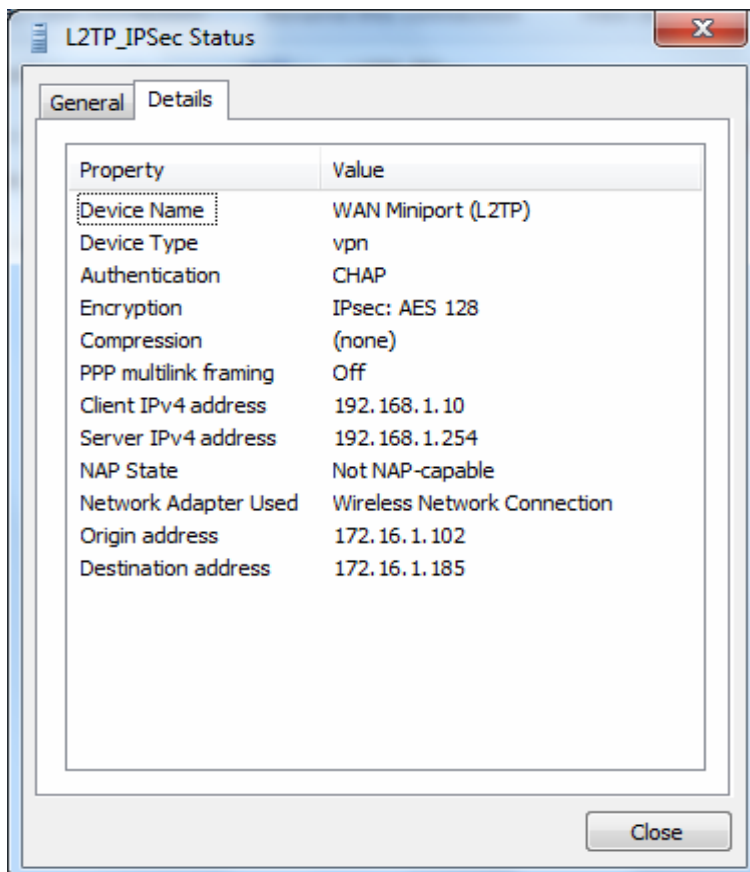
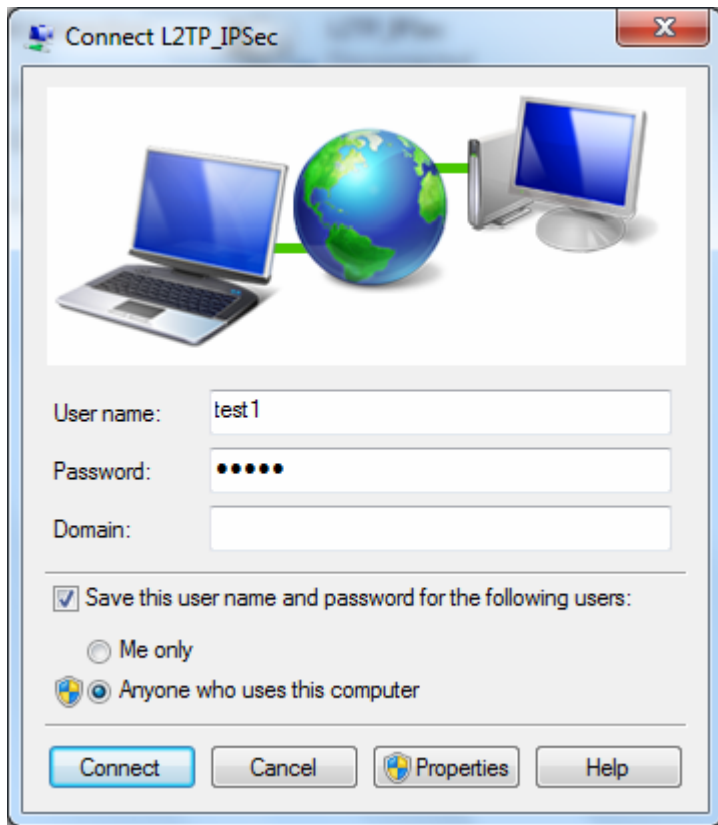
7. Go to **Network Connections** shown below to check the detail of the connection. Right click "L2TP_IPSec" icon, and select "**Properties**" to change the security parameters.



8. Change the type of VPN to “**Layer 2 Tunneling Protocol with IPsec (L2TP/IPSec)**” and Click Advanced Settings to set the pre-shared (set in IPsec) key for authentication.



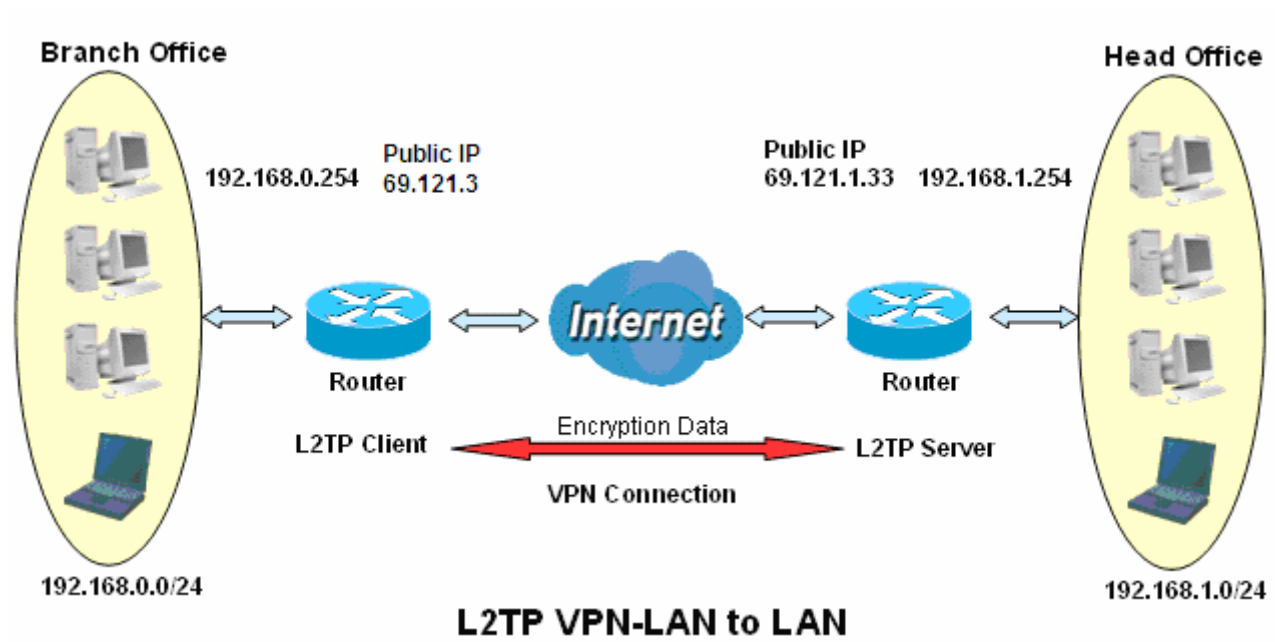
9. Go to **Network connections**, enter username and password to connect L2TP_IPSec and check the connection status.



Example: Configuring L2TP LAN-to-LAN VPN Connection

The branch office establishes a L2TP VPN tunnel with head office to connect two private networks over the Internet. The routers are installed in the head office and branch office accordingly.

Note: Both office LAN networks must be in different subnets with the LAN-LAN application.



Server side: Head Office

VPN

L2TP Server

Parameters

L2TP	☒ Enable ☐ Disable
WAN Interface	Default or IPsec Tunnel IPSec
Auth. Type	Chap
IP Addresses Assigned to Peer	start from : 192.168.1.10
Tunnel Authentication	☐
Secret	
Remote Host Name	
Local Host Name	
Exceptional Rule Group	None

Apply **Cancel**

VPN

IPSec

IPSec Settings

L2TP over IPsec	☒ Enable				
Connection Name	test2	WAN Interface	Default	IP Version	IPv4
Remote Security Gateway	69.121.1.3	☐ Anonymous			
Key Exchange Method	IKE	IPsec Protocol	ESP		
Pre-Shared Key	123456				
Encryption Algorithm	3DES	Integrity Algorithm	MD5		
DH Group	MODP1024(DH2)	IPsec Lifetime	60	Minute(s) [60-1440]	

Apply

Tunnel Mode Connections							
Active	L2TP	Connection Name	Local Network	Remote Network	Remote Security Gateway	Remove	Edit
☒	✓	test1			Anonymous	☐	Edit
☐	✓	test2			69.121.1.3	☐	Edit

The above is the commonly setting for L2TP Server, set as you like for authentication and encryption. The settings in Client side should be in accordance with settings in Server side.

Then account the L2TP Account.

VPN

VPN Account

VPN Account applied to PPTP Server and L2TP Server.

Parameters

Name
HO

Tunnel
☒ Enable ☐ Disable

Username
test2

Password

Connection Type
☐ Remote Access ☒ LAN to LAN

Peer Network IP
192.168.0.0

Peer Netmask
255.255.255.0

Add Edit / Delete

Edit	Name	Tunnel	Connection Type	Peer Network IP	Peer Netmask	Delete
☒	HO	Enable	LAN to LAN	192.168.0.0	255.255.255.0	☐

Client Side: Branch Office

The client user can set up a tunnel connecting to the PPTP server, and can also set the tunnel as the default route for all outgoing traffic.

VPN

L2TP Client

Parameters

Name

BO

L2TP over IPSec

☒ Enable

IPSec Tunnel

test2

IPSec

Username

test2

Password

.....

Auth. Type

Chap

L2TP Server Address

69.121.1.33

Connection Type

☐ Remote Access

☒ LAN to LAN

Peer Network IP

192.168.1.0

Peer Netmask

255.255.255.0

Tunnel Authentication

☐

Secret

Remote Host Name

Local Host Name

Add

Edit / Delete

Edit

Enable

Default Gateway

Name

L2TP Server Address

Connection Type

Peer Network IP

Peer Netmask

Delete

☒

☐

☐

BO

69.121.1.33

LAN to LAN

192.168.1.0

255.255.255.0

☐

Note: users can see the “Default Gateway” item in the bar, and user can check to select the tunnel as the default gateway (default route) for traffic. If selected, all outgoing traffic will be forwarded to this tunnel and routed to the next hop.

GRE

Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a wide variety of network layer protocol packets inside virtual point-to-point links over an Internet Protocol (IP) network. And the common use can be GRE over IPsec.

Note: up to 8 tunnels can be added, but only 4 can be activated.



The screenshot shows a web-based configuration interface for GRE tunnels. At the top, there is a 'VPN' tab and a small graphic of a laptop. Below this, a 'GRE' section is expanded, showing a 'Parameters' table. The table has two columns for configuration fields. The first column contains: 'Name' (text input), 'Local Tunnel Virtual IP' (text input), 'Remote Tunnel Virtual IP' (text input), 'Remote Network' (dropdown menu with 'Single Address' selected), 'Enable Keepalive' (checkbox), and 'Add' (button). The second column contains: 'WAN Interface' (dropdown menu with 'Default' selected), 'Local Netmask' (text input), 'Remote Gateway IP' (text input), 'IP Address' (text input), 'Netmask' (text input), 'Keepalive Retry Times' (text input with '10'), 'Keepalive Interval' (text input with '3'), and 'Edit / Delete' (button). The 'Keepalive Interval' field is followed by the text 'Second(s)'.

Name: User-defined identification.

WAN Interface: Select the exact WAN interface configured for the tunnel as the source tunnel IP. Select Default to use the now-working WAN interface for the tunnel.

Local Tunnel Virtual IP: Please input the virtual IP for the local tunnel.

Local Netmask: Input the netmask for the local tunnel.

Remote Tunnel Virtual IP: Please input the virtual destination IP for tunnel.

Remote Gateway IP: Set the destination IP for the tunnel.

Remote Network: Select the peer topology, Single address (client) or Subnet.

IP Address: Set the IP address if the peer is a client. If the peer is a subnet, please enter the IP and netmask.

Enable Keepalive: Normally, the tunnel interface is always up. Enable keepalive to determine when the tunnel interface is to be closed. The local router sends keepalive packets to the peer router, if keepalive response is not received from peer router within the allowed time ('retry time' multiply 'interval', based on default settings, the time interval can be 30 seconds), the local router will shut up its tunnel interface.

Keepalive Retry Times: Set the keepalive retry times, default is 10.

Keepalive Interval: Set the keepalive Interval, unit in seconds. Default is 3 seconds.

Advanced Setup

There are sub-items within the System section: [Routing](#), [DNS](#), [Static ARP](#), [UPnP](#), [Certificate](#), [Multicast](#), [Management](#), and [Diagnostics](#).

▸ Status
▸ Quick Start
▸ Configuration
▼ Advanced Setup
▸ Routing
▸ DNS
▸ Static ARP
▸ UPnP
▸ Certificate
▸ Multicast
▸ Management
▸ Diagnostics

Routing

Default Gateway

Advanced Setup

▼Default Gateway

Default Gateway Interface List

Only one default gateway interface will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected.

Selected Default Gateway Interfaces		Available Routed WAN Interfaces
ppp0.1	-> <-	eth4.1 USB3G0

Preferred WAN Interface As The System Default IPv6 Gateway

Selected WAN Interface

pppoe_0_8_35/ppp0.1

ApplyCancel

WAN port: Select the port this gateway applies to.

To set **Default Gateway** and **Available Routed WAN Interface**. This interfaces are the ones you have set in WAN section, here select the one you want to be the default gateway by moving the interface via

->

 or

<-

 . And select a Default IPv6 Gateway from the drop-down menu.

Note: Only one default gateway interface will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected.

Static Route

With static route feature, you can control the routing of all the traffic across your network. With each routing rule created, you can specifically assign the destination where the traffic will be routed.

Advanced Setup

Static Route

Parameters

IP Version	Dst IP / Prefix Length	Gateway	Interface	Metric	Remove
AddRemove					

Above is the static route listing table, click **Add** to create static routing.

Advanced Setup

Static Route

Parameters

IP Version

IPv4

Destination IP Address / Prefix Length

Interface

Gateway IP Address

Metric

[greater than or equal to zero]

Apply

Cancel

IP Version: Select the IP version, IPv4 or IPv6.

Destination IP Address / Prefix Length: Enter the destination IP address and the prefix length. For IPv4, the prefix length means the number of ‘1’ in the submask, it is another mode of presenting submask. One IPv4 address,192.168.1.0/24, submask is 255.255.255.0. While in IPv6, IPv6 address composes of two parts, thus, the prefix and the interface ID, the prefix is like the net ID in IPv4, and the interface ID is like the host ID in IPv4. The prefix length is to identify the net ID in the address. One IPv6 address, 3FFE:FFFF:0:CD30:0:0:0:0 / 64, the prefix is 3FFE:FFFF:0:CD3.

Interface: Select an interface this route associated.

Gateway IP Address: Enter the gateway IP address.

Metric: Metric is a policy for router to commit router, to determine the optimal route. Enter one number greater than or equal to 0.

Click **Apply** to apply this route and it will be listed in the route listing table.

In listing table you can remove the one you don't want by checking the checking box and press **Remove** button.

Advanced Setup

Static Route

Parameters

IP Version	Dst IP/Prefix Length	Gateway	Interface	Metric	Remove
4	192.168.1.0/24		ppp0	1	☒

Add

Remove

Policy Routing

Here users can set a route for the host (source IP) in a LAN interface to access outside through a specified Default Gateway or a WAN interface.

The following is the policy Routing listing table.

Advanced Setup

▼ Policy Routing

Parameters

Policy Name	Source IP	LAN Port	WAN	Default Gateway	Remove
Add Remove					

Click **Add** to create a policy route.

Advanced Setup

▼ Policy Routing

Parameters

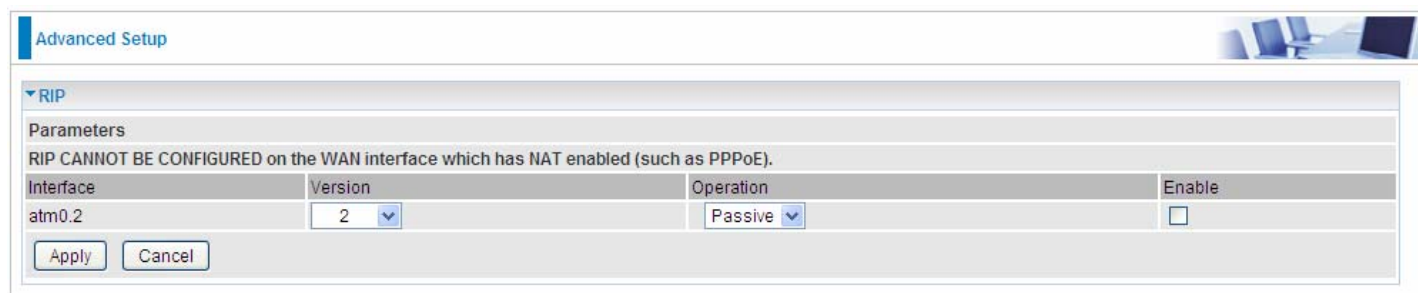
Policy Name	
Physical LAN Port	▼
Source IP	
Interface	pppoe_0_0_35/ppp0.1 ▼
Default Gateway	
Apply Cancel	

- Policy Name:** User-defined name.
- Physical LAN Port:** Select the LAN port.
- Source IP:** Enter the Host Source IP.
- Interface:** Select the WAN interface which you want the Source IP to access outside through.
- Default Gateway:** Enter the default gateway which you want the Source IP to access outside through.

Click **Apply** to apply your settings. And the item will be listed in the policy Routing listing table. Here if you want to remove the route, check the remove checkbox and press **Remove** to delete it.

RIP

RIP, Router Information Protocol, is a simple Interior Gateway Protocol (IGP). RIP has two versions, RIP-1 and RIP-2.



The screenshot shows the 'Advanced Setup' window for configuring RIP. It includes a warning message and a table for interface configuration.

Advanced Setup

▼ RIP

Parameters

RIP CANNOT BE CONFIGURED on the WAN interface which has NAT enabled (such as PPPoE).

Interface	Version	Operation	Enable
atm0.2	2	Passive	☐

Apply Cancel

Interface: the interface the rule applies to.

Version: select the RIP version, there are two versions, RIP-1 and RIP-2.

Operation: RIP has two operation mode.

- ① **Passive:** only receive the routing information broadcasted by other routers and modifies its routing table according to the received information.
- ① **Active:** working in this mode, the router sends and receives RIP routing information and modifies routing table according to the received information.

Enable: check the checkbox to enable RIP rule for the interface.

Note: RIP can't be configured on the WAN interface which has NAT enabled (such as PPPoE).

Click **Apply** to apply your settings.

DNS

DNS, Domain Name System, is a distributed database of TCP/IP application. DNS provides translation of Domain name to IP.

DNS

▼ DNS

Parameters

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses OR IP addresses provided by Parental Control Provider for the system.
In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.
DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected.
Priority order can be changed by removing all and adding them back in again.

☒ Select DNS Server Interface from available WAN interfaces

Selected DNS Server Interfaces

ppp0.1
USB3G0

Available WAN Interfaces

->
<-

☐ Use the following Static DNS IP address

Primary DNS server

Secondary DNS server

☐ Use the IP Addresses provided by Parental Control Provider

Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface.

☒ Obtain IPv6 DNS info from a WAN interface

WAN Interface selected

pppoe_0_8_35/ppp0.1 ▼

☐ Use the following Static IPv6 DNS address

Primary IPv6 DNS server

Secondary IPv6 DNS server

Apply

Cancel

➤ IPv4

Three ways to set an IPv4 DNS server

- ① **Select DNS server from available WAN interfaces:** Select a desirable WAN interface as the IPv4 DNS server.
- ① **User the following Static DNS IP address:** To specify DNS server manually by entering your primary and secondary DNS server addresses.
- ① **Use the IP address provided by Parental Control Provider:** If user registers and gets an DNS account in the parental control provider website, expecting to enjoy a more reliable and safer internet surfing environment, please select this option (need to configure at [Parental Control Provider](#)).

➤ IPv6:

IPv6 DNS Server's operation is similar to IPv4 DNS server. There are two modes to get DNS server address: Auto and Static mode.

Obtain IPv6 DNS info from a WAN interface

WAN Interface selected: Select one configured IPv6 WAN connection from the drop-down menu to be as an IPv6 DNS.

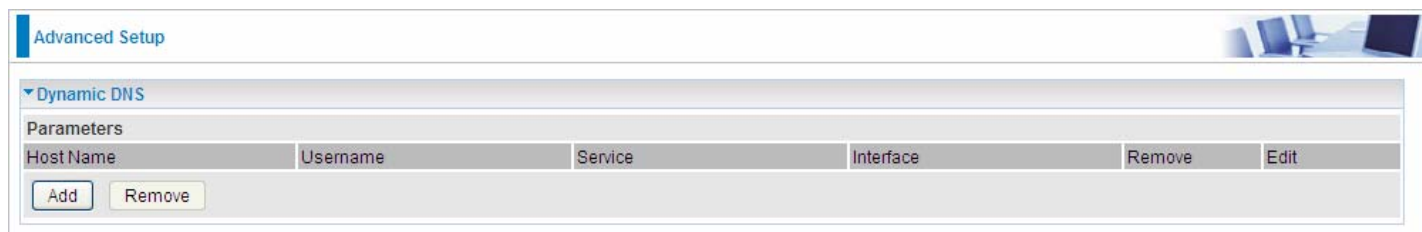
Use the following Static IPv6 DNS address

Primary IPv6 DNS Server / Secondary IPv6 DNS Server: Type the specific primary and secondary IPv6 DNS Server address.

Dynamic DNS

The Dynamic DNS function allows you to alias a dynamic IP address to a static hostname, allowing users whose ISP does not assign them a static IP address to use a domain name. This is especially useful for hosting servers via your ADSL connection, so that anyone wishing to connect to you may use your domain name, rather than having to use your dynamic IP address, which changes from time to time. This dynamic IP address is the WAN IP address of the router, which is assigned to you by your ISP.

Here users can register different WAN interfaces with different DNS(es).



Advanced Setup

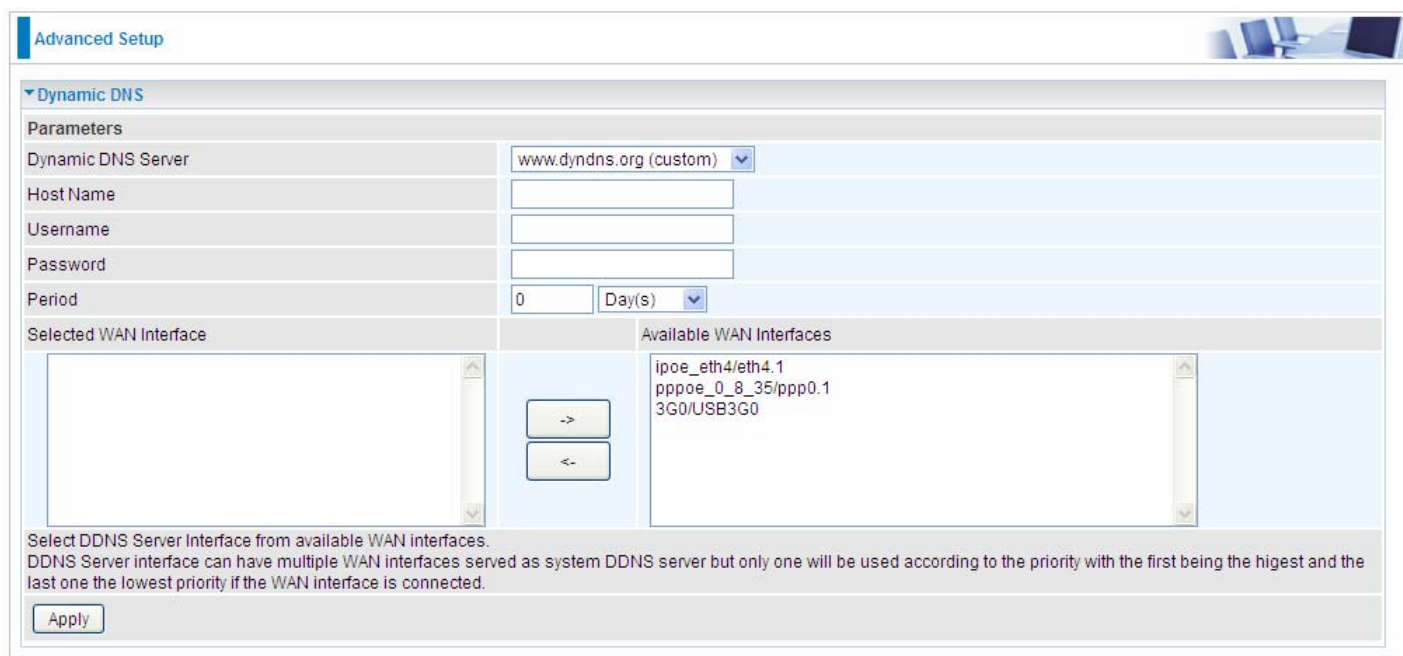
Dynamic DNS

Parameters

Host Name	Username	Service	Interface	Remove	Edit
-----------	----------	---------	-----------	--------	------

Add Remove

Click **Add** to register a WAN interface with the exact DNS.



Advanced Setup

Dynamic DNS

Parameters

Dynamic DNS Server:

Host Name:

Username:

Password:

Period: Day(s)

Selected WAN Interface:

Available WAN Interfaces:

- ipoe_eth4/eth4.1
- pppoe_0_8_35/ppp0.1
- 3G0/USB3G0

Select DDNS Server Interface from available WAN interfaces.
DDNS Server interface can have multiple WAN interfaces served as system DDNS server but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected.

Apply

You will first need to register and establish an account with the Dynamic DNS provider using their website, for example <http://www.dyndns.org/>

Dynamic DNS Server: Select the DDNS service you have established an account with.

Host Name, Username and Password: Enter your registered domain name and your username and password for this service.

Period: Set the time period between updates, for the Router to exchange information with the DDNS server. In addition to updating periodically as per your settings, the router will perform an update when your dynamic IP address changes.

Selected WAN Interface: Select the Interface that is bound to the registered Domain name.

User can register different DDNS to different interfaces.

Examples: **Note** first users have to go to the Dynamic DNS registration service provider to register an account.

User **test** register two Dynamic Domain Names in DDNS provider <http://www.dyndns.org/> .

- 1. pppoe_0_8_35 with DDNS: www.hometest.com using username/password test/test

Advanced Setup

Dynamic DNS

Parameters

Dynamic DNS Server

www.dyndns.org (custom)

Host Name

www.hometest.com

Username

test

Password

....

Period

25

Day(s)

Selected WAN Interface

pppoe_0_8_35/ppp0.1

Available WAN Interfaces

ipoe_eth4/eth4.1
3G0/USB3G0

->

<-

Select DDNS Server Interface from available WAN interfaces.
DDNS Server interface can have multiple WAN interfaces served as system DDNS server but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected.

Apply

Advanced Setup

Dynamic DNS

Parameters

Host Name	Username	Service	Interface	Remove	Edit
www.hometest.com	test	dyndns-custom	ppp0.1	☐	Edit

Add

Remove

2. ipoe_eth4 with DDNS: www.hometest1.com using username/password test/test.

Advanced Setup

Dynamic DNS

Parameters

Dynamic DNS Server

www.dyndns.org (custom)

Host Name

www.hometest1.com

Username

test

Password

....

Period

25

Day(s)

Selected WAN Interface

ipoe_eth4/eth4.1

Available WAN Interfaces

pppoe_0_8_35/ppp0.1
3G0/USB3G0

Select DDNS Server Interface from available WAN interfaces.
DDNS Server interface can have multiple WAN interfaces served as system DDNS server but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected.

Apply

Advanced Setup

Dynamic DNS

Parameters

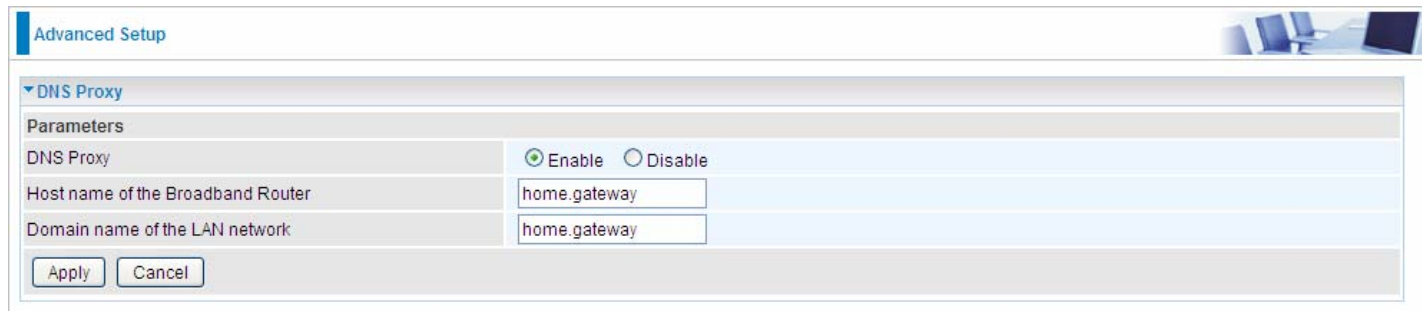
Host Name	Username	Service	Interface	Remove	Edit
www.hometest.com	test	dyndns-custom	ppp0.1	☐	Edit
www.hometest1.com	test	dyndns-custom	eth4.1	☐	Edit

Add

Remove

DNS Proxy

DNS proxy is used to forward request and response message between DNS Client and DNS Server. Hosts in LAN can use router serving as a DNS proxy to connect to the DNS Server in public to correctly resolve Domain name to access the internet.



Parameters	
DNS Proxy	☒ Enable ☐ Disable
Host name of the Broadband Router	home.gateway
Domain name of the LAN network	home.gateway

DNS Proxy: Select whether to enable or disable DNS Proxy function, default is enabled.

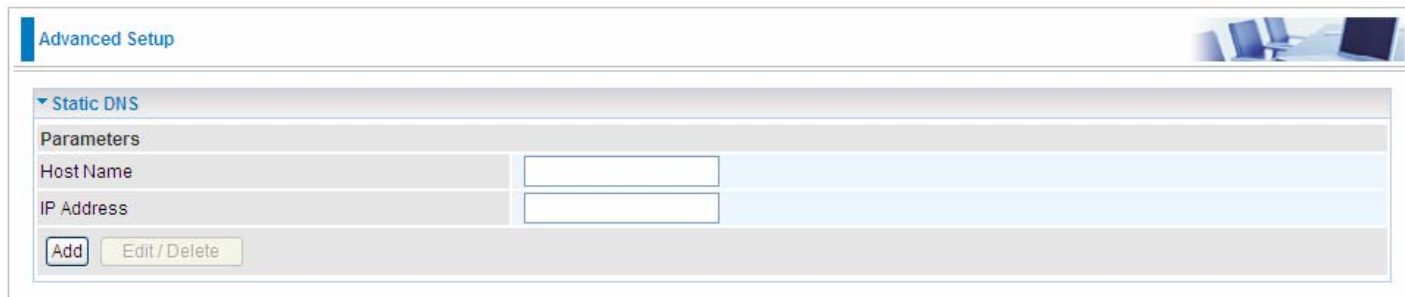
Host name of the Broadband Router: Enter the host name of the router. Default is home.gateway.

Domain name of the LAN network: Enter the domain name of the LAN network. home.gateway.

Static DNS

Static DNS is a concept relative to Dynamic DNS; in static DNS system, the IP mapped is static without change.

You can map the specific IP to a user-friendly domain name. In LAN, you can map a PC to a domain name for convenient access. Or you can set some well-known Internet IP mapping item so your router will response quickly for your DNS query instead of querying from the ISP's DNS server.



The screenshot shows a web interface for a router's 'Advanced Setup' page. The 'Static DNS' section is expanded, showing a table with two columns: 'Host Name' and 'IP Address'. There are two empty input fields for these columns. Below the table are two buttons: 'Add' and 'Edit/Delete'.

Static DNS	
Parameters	
Host Name	
IP Address	
Add Edit/Delete	

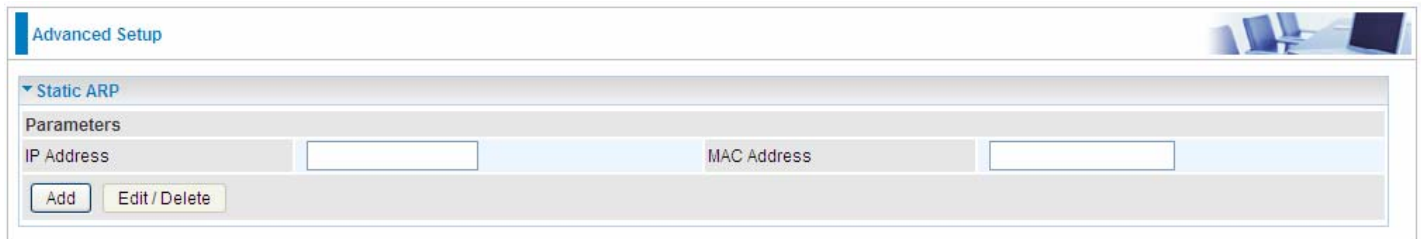
Host Name: Type the domain name (host name) for the specific IP .

IP Address: Type the IP address bound to the set host name above.

Click **Add** to save your settings.

Static ARP

ARP (Address Resolution Protocol) is a TCP/IP protocol that allows the resolution of network layer addresses into the link layer addresses. And “Static ARP” here allows user to map manually the layer-3 MAC (Media Access Control) address to the layer-2 IP address of the device.

The screenshot shows a web-based configuration interface. At the top, there is a blue header bar with the text "Advanced Setup" on the left and a small graphic of a desk with a laptop on the right. Below the header, there is a section titled "Static ARP" with a dropdown arrow. Under this section, there is a "Parameters" label. Below the label, there are two input fields: "IP Address" on the left and "MAC Address" on the right. Below these fields, there are two buttons: "Add" and "Edit / Delete".

Static ARP	
Parameters	
IP Address	MAC Address
Add	Edit / Delete

IP Address: Enter the IP of the device that the corresponding MAC address will be mapped to.

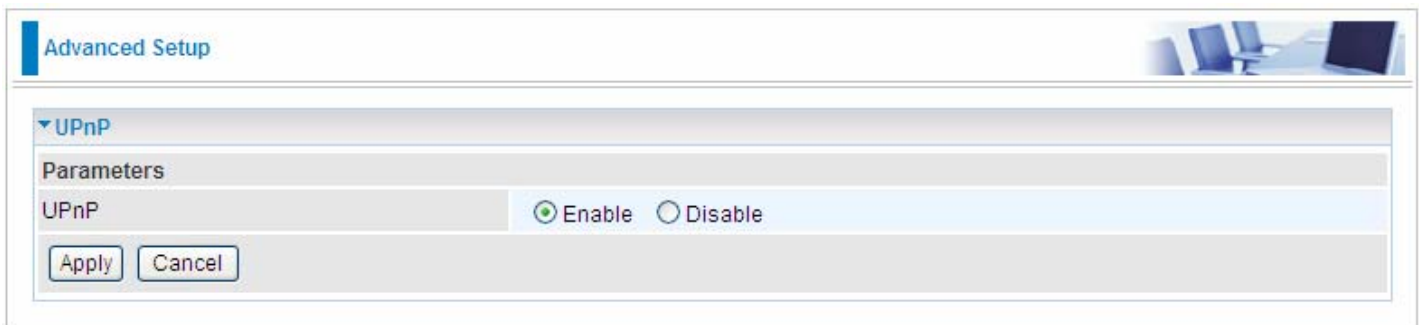
MAC Address: Enter the MAC address that corresponds to the IP address of the device.

Click **Add** to confirm the settings.

UPnP

UPnP offers peer-to-peer network connectivity for PCs and other network devices, along with control and data transfer between devices. UPnP offers many advantages for users running NAT routers through UPnP NAT Traversal, and on supported systems makes tasks such as port forwarding much easier by letting the application control the required settings, removing the need for the user to control advanced configuration of their device.

Both the user's Operating System and the relevant application must support UPnP in addition to the router. Windows XP and Windows Me natively support UPnP (when the component is installed), and Windows 98 users may install the Internet Connection Sharing client from Windows XP in order to support UPnP. Windows 2000 does not support UPnP.



UPnP:

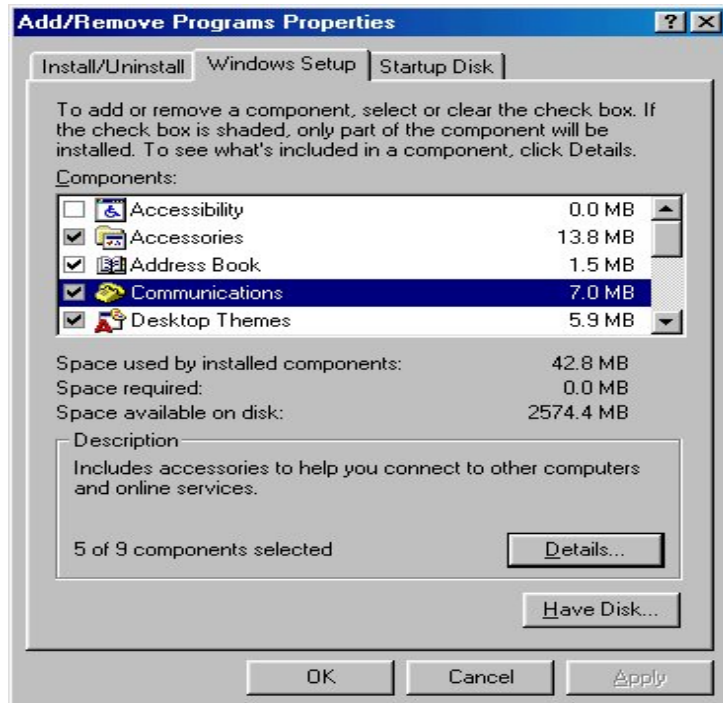
- ① **Enable:** Check to enable the router's UPnP functionality.
- ① **Disable:** Check to disable the router's UPnP functionality.

Installing UPnP in Windows Example

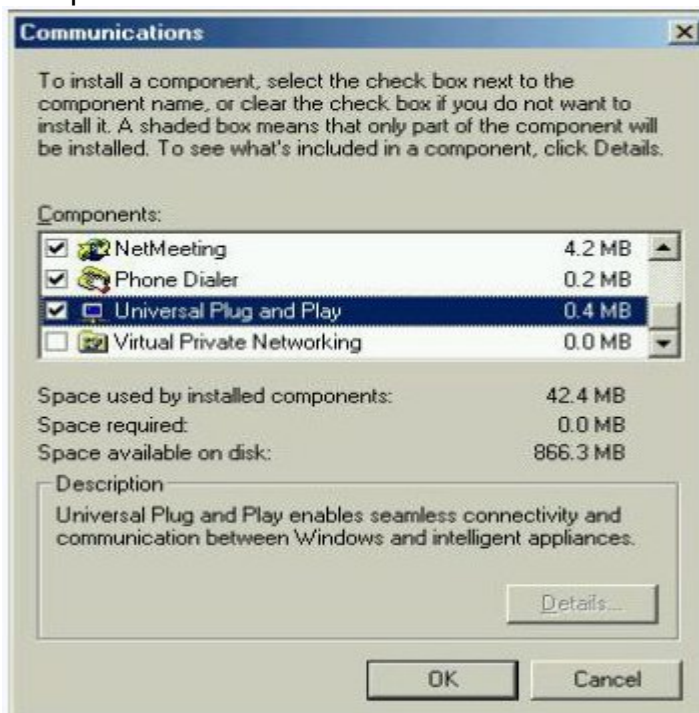
Follow the steps below to install the UPnP in Windows Me.

Step 1: Click Start and Control Panel. Double-click Add/Remove Programs.

Step 2: Click on the Windows Setup tab and select Communication in the Components selection box. Click Details.



Step 3: In the Communications window, select the Universal Plug and Play check box in the Components selection box.



Step 4: Click OK to go back to the Add/Remove Programs Properties window. Click Next.

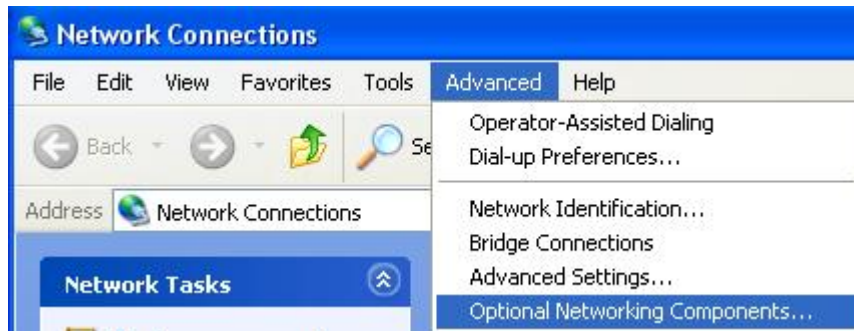
Step 5: Restart the computer when prompted.

Follow the steps below to install the UPnP in Windows XP.

Step 1: Click Start and Control Panel.

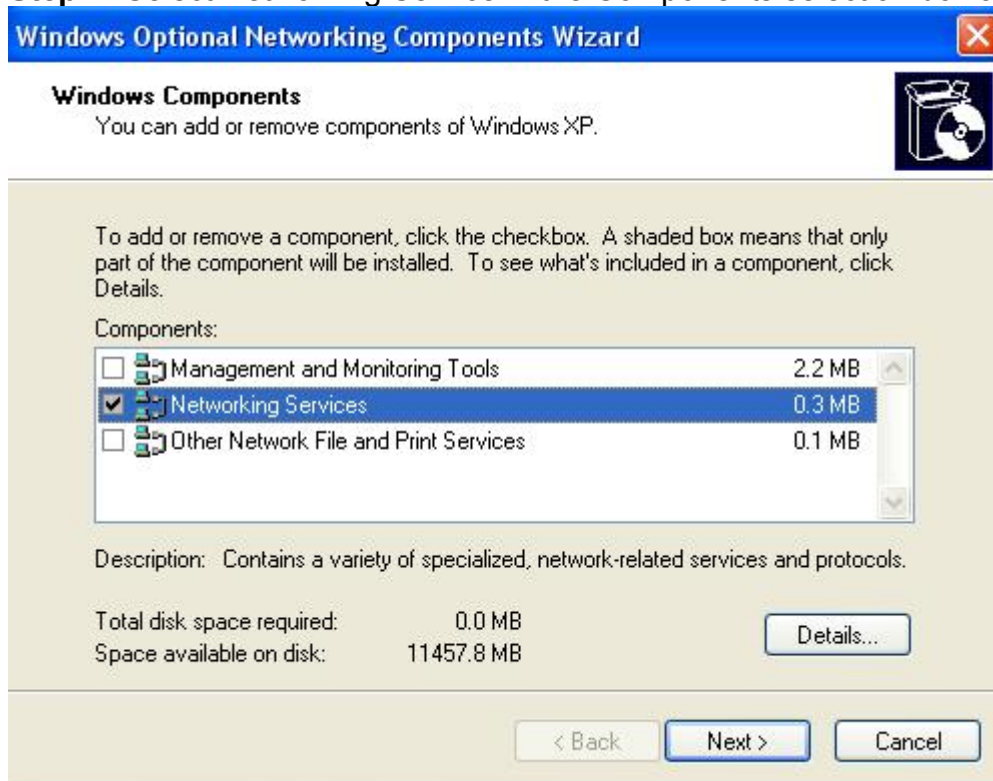
Step 2: Double-click Network Connections.

Step 3: In the Network Connections window, click Advanced in the main menu and select Optional Networking Components



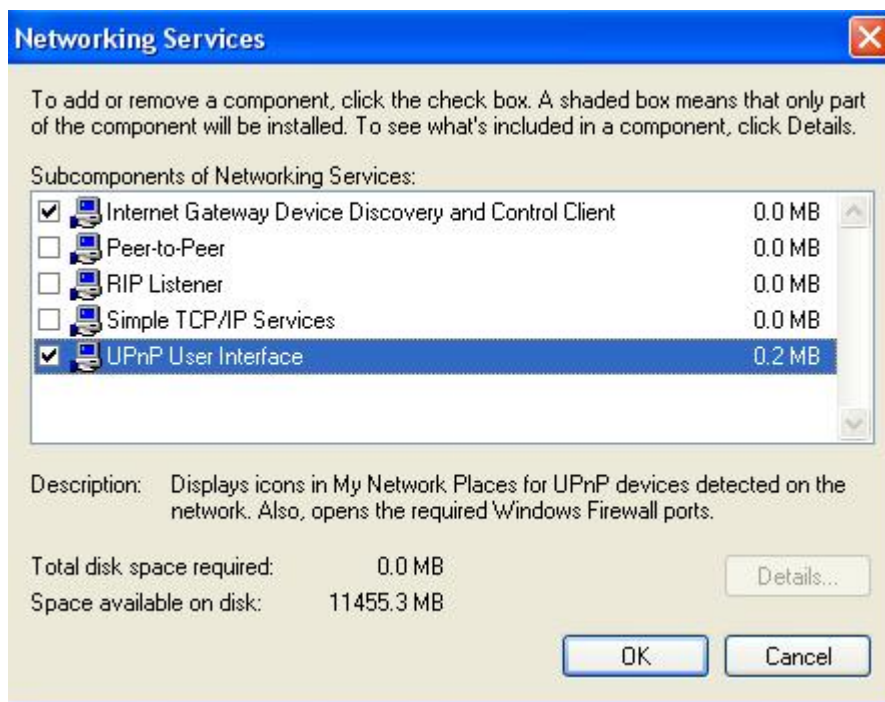
The Windows Optional Networking Components Wizard window displays.

Step 4: Select Networking Service in the Components selection box and click Details.



Step 5: In the Networking Services window, select the Universal Plug and Play check box.

Step 6: Click **OK** to go back to the Windows Optional Networking Component Wizard window and click **Next**.



Auto-discover Your UPnP-enabled Network Device

Step 1: Click start and Control Panel. Double-click Network Connections. An icon displays under Internet Gateway.

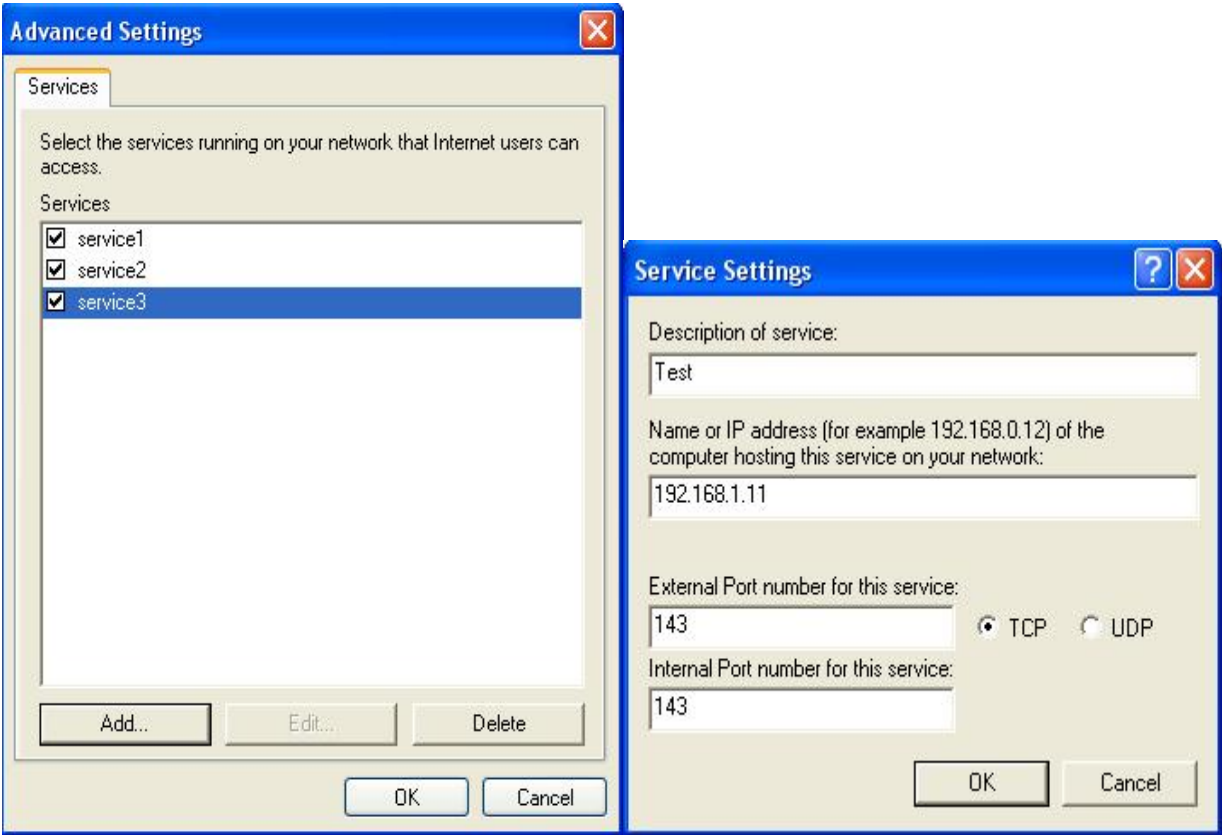
Step 2: Right-click the icon and select Properties.



Step 3: In the Internet Connection Properties window, click Settings to see the port mappings that were automatically created.

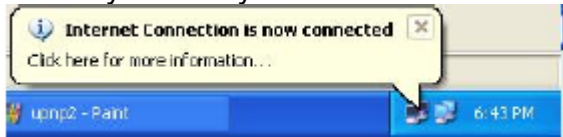


Step 4: You may edit or delete the port mappings or click Add to manually add port mappings.

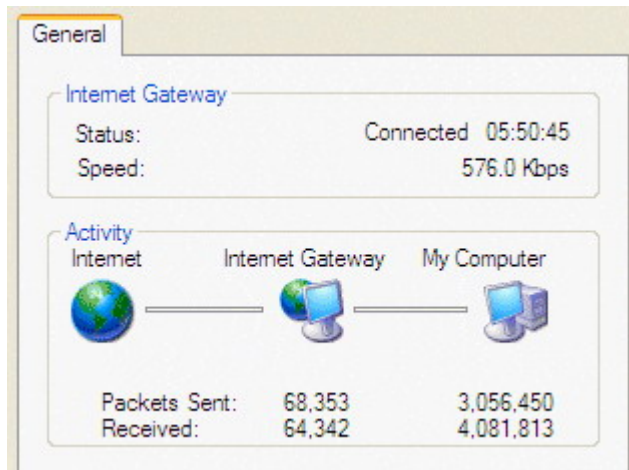


Step 5: Select Show icon in notification area when connected option and click OK. An icon displays

in the system tray



Step 6: Double-click on the icon to display your current Internet connection status.



Certificate

This feature is used for TR069 ACS Server authentication of the device using certificate, if necessary. If the imported certificate does not match the authorized certificate of the ACS Server, the device will have no access to the server.

Trusted CA

Advanced Setup

Trusted CA

Trusted CA (Certificate Authority) Certificates

Maximum certificates can be stored: 4

Name	Subject	Type	Action
Import Certificate			

Certificate Name: The certificate identification name.

Subject: The certificate subject.

Type: The certificate type information. "ca", indicates that the certificate is a CA-signed certificate. "self", indicates that the certificate is a certificate owner signed one.

"x.509", indicates the certificate is the one created and signed according to the definition of Public-Key System suggested by x.509.

Action:

-  View: view the certificate.
-  Remove: remove the certificate.

Click **Import Certificate** button to import your certificate.

Advanced Setup

Trusted CA -- Import CA certificate

Parameters

Name

Certificate

-----BEGIN CERTIFICATE-----
<insert certificate here>
-----END CERTIFICATE-----

Apply

Enter the certificate name and insert the certificate.

Advanced Setup

Trusted CA -- Import CA certificate

Parameters

Name

acscert

Certificate

-----BEGIN CERTIFICATE-----
MIICjDCCAfWgAwIBAgIEOUSLuTANBgkqhkiG9w0BAQUFADAmMQswCQYDVQQGEwJD
TjEXMBUGA1UEChMQQ0ZDQSBQb2xpY3kgQ0EwHhcNMDAwNjEyMDc0OTUyWhc
NMjAw
NjEyMDQzNzA2WjApMQswCQYDVQQGEwJDTjEaMBGGA1UEChMRQ0ZDQSBPcGV
yYXRp
b24gQ0EwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBANesUKqN1sWtSpN
ZuTJD
rSwXGjaexPnBis5zNJc70SPQYgVhn3Qv9+vIuU2jYFzF8qiDYPQBv7hFjI/
Uu9be
pUJBenxvYRgTIImUfJ0PEy+SsRUpcDAPxTWNp4Efv8QEnM0JGEHAOtLHDY73
/se+H
jB7Wh9HhzCTF5QqZRL3o2ILXAgMBAAGjgcMwgcAwSAYDVROfBEEwPzA9oDu
gOaQ3
MDUxCzAJBgNVBAYTAkNOMRcwFQYDVQQKEw5DRkNBIFBvbGljeSBBDQITENMA
GA1UE
AxMEQ1JUMMTALBgNVHQ8EBAMCAQYwHwYDVROjBBgwFoAUL5Jufe7tBb/wveS
FaAqX
k1NC0tAwHQYDVRO0BBYEFMMnxjZoyCd1JIevkadLJjMC5RrpMAwGA1UdEwQ

Apply

Click Apply to confirm your settings.

Advanced Setup

Trusted CA

Trusted CA (Certificate Authority) Certificates

Maximum certificates can be stored: 4

Name	Subject	Type	Action
acscert	C=CN/O=CFCA Operation CA	ca	View Remove

Import Certificate

Multicast

Multicast is one of the three network transmission modes, Unicast, Multicast, Broadcast. It is a transmission mode that supports point-to-multipoint connections between the sender and the recipient. IGMP protocol is used to establish and maintain the relationship between IP host and the host directly connected multicast router.

IGMP stands for **Internet Group Management Protocol**, it is a communications protocols used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and the adjacent multicast routers to establish multicast group members. There are three versions for IGMP, that is IGMPv1, IGMPv2 and IGMPv3.

MLD, short for **Multicast Listener Discovery** protocol, is a component if the Internet Protocol version 6(IPv6) suite. MLD is used by IPv6 to discover multicast listeners on a directly attached link, much as IGMP used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol. MLDv1 is similar to IGMPv2 and MLDv2 is similar to IGMPv3.

Advanced Setup

▼ Multicast

Multicast Precedence

Disable

lower value, higher priority

IGMP

Default Version

3

[1-3]

Query Interval

125

Query Response Interval

10

Last Member Query Interval

10

Robustness Value

2

Maximum Multicast Groups

25

Maximum Multicast Data Sources (for IGMPv3)

10

[1-24]

Maximum Multicast Group Members

25

Fast Leave

☒ Enable

MLD

Default Version

2

[1-2]

Query Interval

125

Query Response Interval

10

Last Member Query Interval

10

Robustness Value

2

Maximum Multicast Groups

10

Maximum Multicast Data Sources (for MLDv2)

10

[1-24]

Maximum Multicast Group Members

10

Fast Leave

☒ Enable

Apply

Cancel

IGMP

Multicast Precedence: It is for multicast QoS. With lower multicast precedence, IGMP packets will be put into higher-priority queue. Default is set to disable.

Default Version: Enter the supported IGMP version, 1-3, default is IGMP v3.

Query Interval: Enter the periodic query interval time (sec) the multicast router sending the query message to hosts to understand the group membership information.

Query Response Interval: Enter the response interval time (sec).

Last Member Query Interval: Enter the interval time (sec) the multicast router query the specified group after it has received leave message.

235

Robustness Value: Enter the router robustness parameter, 2-7, the greater the robustness value, the more robust the Querier is.

Maximum Multicast Groups: Enter the Maximum Multicast Groups.

Maximum Multicast Data Sources(for IGMP v3): Enter the Maximum Multicast Data Sources,1-24.

Maximum Multicast Group Members: Enter the Maximum Multicast Group Members.

Fast leave: Check to determine whether to support fast leave. If this value is enabled, IGMP proxy removes the membership of a group member immediately without sending an IGMP membership query on downstream. This is very helpful if user wants fast channel (group change) changing in cases like IPTV environment.

MLD

Default Version: Enter the supported MLD version, 1-2, default is MLDv2.

Query Interval: Enter the periodic query interval time (sec) the multicast router sending the query message to hosts to understand the group membership information.

Query Response Interval: Enter the response interval time (sec).

Last Member Query Interval: Enter the interval time (sec) the multicast router query the specified group after it has received leave message.

Robustness Value: Enter the router robustness parameter, default is 2, the greater the robustness value, the more robust the Querier is.

Maximum Multicast Groups: Enter the Maximum Multicast Groups.

Maximum Multicast Data Sources(for MLDv2): Enter the Maximum Multicast Data Sources,1-24.

Maximum Multicast Group Members: Enter the Maximum Multicast Group Members.

Fast leave: Check to determine whether to support fast leave. If this value is enabled, MLD proxy removes the membership of a group member immediately without sending an MLD membership query on downstream. This is very helpful if user wants fast channel (group change) changing in cases like IPTV environment.

.

Management

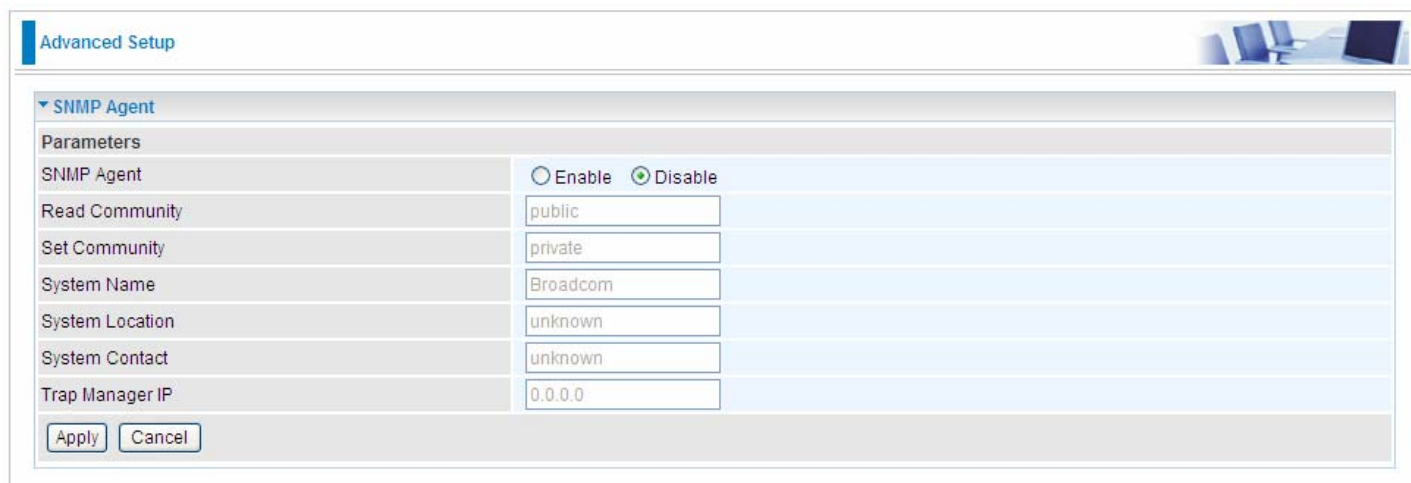
SNMP Agent

SNMP, Simple Network Management Protocol, is the most popular one in network. It consists of SNMP Manager, SNMP Agent and MIB. Every network device supporting SNMP will have a SNMP Agent which is a management software running in the device.

SNMP Manager, the management software running on the server, it uses SNMP protocol to send GetRequest, GetNextRequest, SetRequest message to Agent to view and change the information of the device.

SNMP Agents, the management software running in the device, accepts the message from the manager, Reads or Writes the management variable in MIB accordingly and then generates Response message to send it to the manager. Also, agent will send Trap message to the manager when agent finds some exceptions.

Trap message, is the message automatically sent by the managed device without request to the manager about the emergency events.



The screenshot shows a web-based configuration interface titled "Advanced Setup". Under the "SNMP Agent" section, there are several configuration fields. The "SNMP Agent" checkbox is currently unchecked, with "Enable" and "Disable" radio buttons. The "Read Community" field is set to "public", "Set Community" is set to "private", "System Name" is set to "Broadcom", "System Location" is set to "unknown", "System Contact" is set to "unknown", and "Trap Manager IP" is set to "0.0.0.0". There are "Apply" and "Cancel" buttons at the bottom of the configuration area.

Parameters	
SNMP Agent	☐ Enable ☒ Disable
Read Community	public
Set Community	private
System Name	Broadcom
System Location	unknown
System Contact	unknown
Trap Manager IP	0.0.0.0

Apply Cancel

SNMP Agent: enable or disable SNMP Agent.

Read Community: Type the Get Community, which is the authentication for the incoming Get-and GetNext requests from the management station.

Set Community: Type the Set Community, which is the authentication for incoming Set requests from the management station.

System Name: here it refers to your router.

System Location: user-defined location.

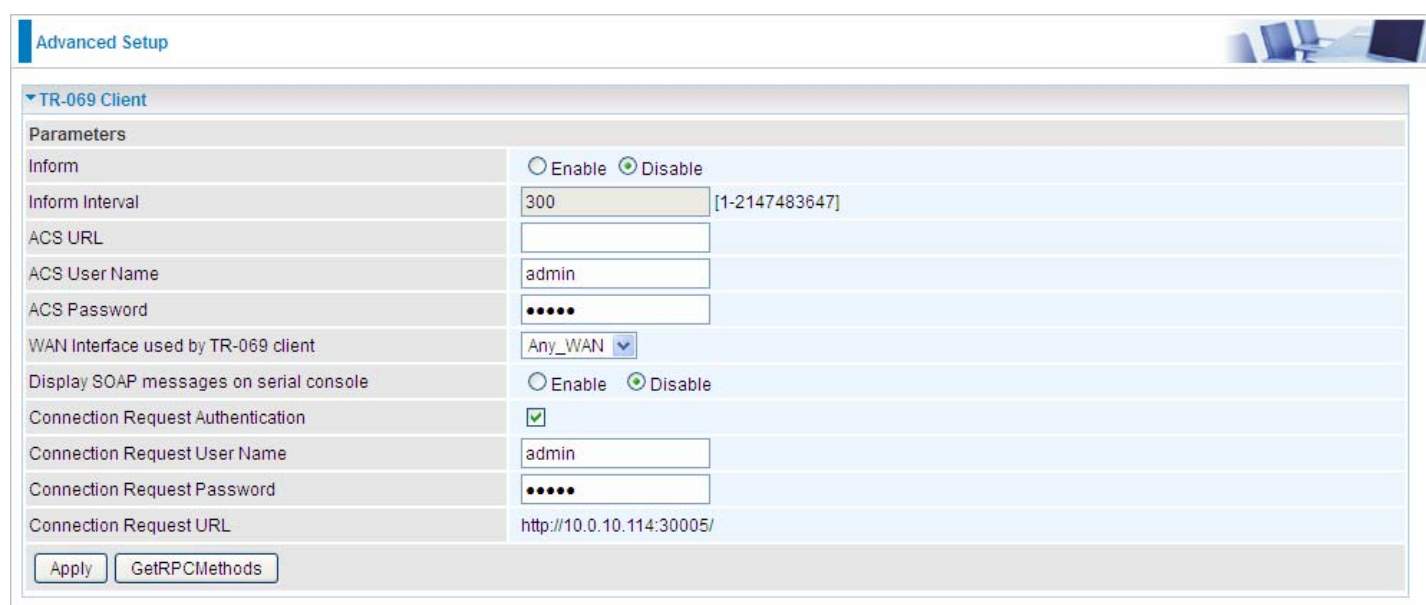
System Contact: user-defined contact message.

Trap manager IP: enter the IP address of the server receiving the trap sent by SNMP agent.

TR- 069 Client

TR-069 (short for Technical Report 069) is a DSL Forum (which was later renamed as Broadband Forum) technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices.

As a bidirectional SOAP/HTTP based protocol it can provides the communication between customer premises equipment (CPE) and Auto Configuration Server (ACS). It includes both a safe configuration and the control of other CPE management functions within an integrated framework. In the course of the booming broadband market, the number of different internet access possibilities grew as well (e.g. modems, routers, gateways, set-top box, VoIP-phones).At the same time the configuration of this equipment became more complicated –too complicated for end-users. For this reason, TR-069 was developed. It provides the possibility of auto configuration of the access types. Using TR-069 the terminals can get in contact with the Auto Configuration Servers (ACS) and establish the configuration automatically and let ACS configure CPE automatically.



The screenshot shows a web-based configuration interface titled "Advanced Setup". Under the "TR-069 Client" section, there is a "Parameters" table. The "Inform" parameter has radio buttons for "Enable" and "Disable", with "Disable" selected. The "Inform Interval" is set to 300, with a range of [1-2147483647] shown. The "ACS URL" is empty. The "ACS User Name" is "admin". The "ACS Password" is masked with dots. The "WAN Interface used by TR-069 client" is set to "Any_WAN" via a dropdown. The "Display SOAP messages on serial console" has radio buttons for "Enable" and "Disable", with "Disable" selected. The "Connection Request Authentication" is checked. The "Connection Request User Name" is "admin". The "Connection Request Password" is masked with dots. The "Connection Request URL" is "http://10.0.10.114:30005/". At the bottom are "Apply" and "GetRPCMethods" buttons.

Parameters	
Inform	☐ Enable ☒ Disable
Inform Interval	300 [1-2147483647]
ACS URL	
ACS User Name	admin
ACS Password	
WAN Interface used by TR-069 client	Any_WAN
Display SOAP messages on serial console	☐ Enable ☒ Disable
Connection Request Authentication	☒
Connection Request User Name	admin
Connection Request Password	
Connection Request URL	http://10.0.10.114:30005/

Apply GetRPCMethods

Inform: select enable to let CPE be authorized to send Inform message to automatically connect to ACS.

Inform Interval: Specify the inform interval time (sec) which CPE used to periodically send inform message to automatically connect to ACS. When the inform interval time arrives, the CPE will send inform message to automatically connect to ACS.

ACS URL: Enter the ACS server login name.

ACS User Name: Specify the ACS User Name for ACS authentication to the connection from CPE.

ACS password: Enter the ACS server login password.

WAN interface used by TR-069: select the interface used by TR-069.

Display SOAP message on serial console: select whether to display SOAP message on serial console.

Connection Request Authentication: Check to enable connection request authentication feature.

Connection Request User Name: Enter the username for ACS server to make connection request.

Connection Request User Password: Enter the password for ACS server to make connection request.

Connection Request URL: Automatically match the URL for ACS server to make connection request.

GetRPCMethods: Supported by both CPE and ACS, display the supported RFC listing methods.

Click **Apply** to apply your settings.

HTTP Port

The device equips user to change the embedded web server accessing port. Default is 80.

Advanced Setup

HTTP Port

Parameters

HTTP Port

80

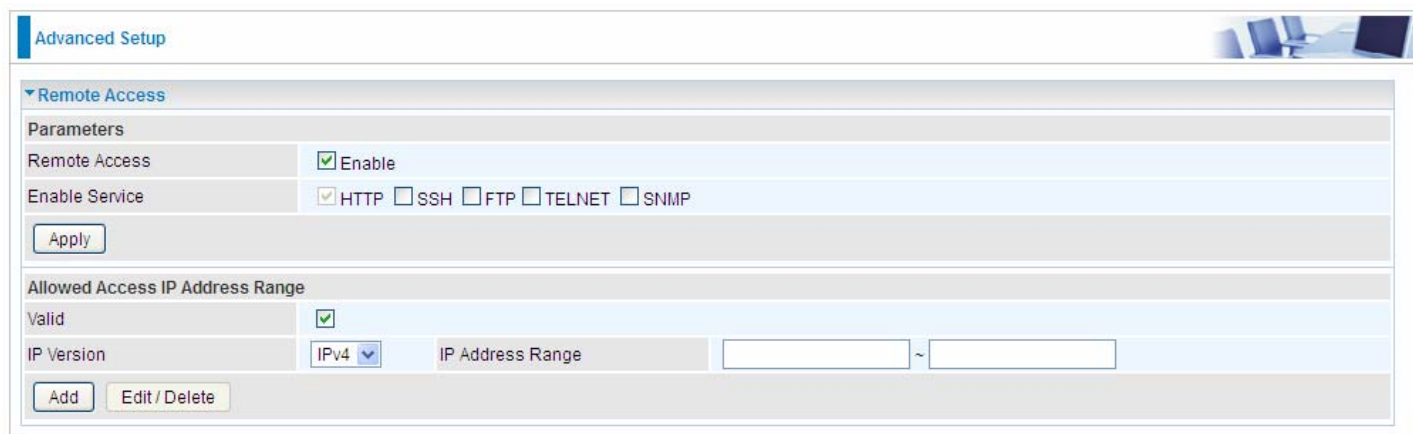
(Default: 80)

Apply

Cancel

Remote Access

It is to allow remote access to the router to view or configure.



The screenshot shows the 'Advanced Setup' page for 'Remote Access'. It includes a 'Parameters' section with 'Remote Access' set to 'Enable' and 'Enable Service' with checkboxes for HTTP (checked), SSH, FTP, TELNET, and SNMP. Below this is an 'Apply' button. The 'Allowed Access IP Address Range' section has a 'Valid' checkbox checked, an 'IP Version' dropdown set to 'IPv4', and an 'IP Address Range' field with a tilde separator. At the bottom are 'Add' and 'Edit / Delete' buttons.

Remote Access: Select “Enable” to allow management access from remote side (mostly from internet). If disabled, no remote access is allowed for any IPs even if you set allowed access IP address. So, please note that enabling remote access is an essential step before granting remote access to IPs.

Enable Service: Select to determine which service(s) is (are) allowed for remote access when remote access is enabled. By default (on condition that remote access is enabled), the web service (HTTP) is allowed for remote access.

Click **Apply** button to submit your settings.

"**Allowed Access IP Address Range**" was used to restrict which IP address could login to access system web GUI.

Valid: Enable/Disable Allowed Access IP Address Range

IP Address Range: Specify the IP address Range, IPv4 and IPv6 address range can be supported, users can set IPv4 and IPv6 address range individually.

Click **Add** to add an IP Range to allow remote access.

Note: 1. If user wants to grant remote access to IPs, first enable **Remote Access**.

2. Remote Access enabled:

- 1) Enable **Valid** for the specific IP(s) in the IP range to allow the specific IP(s) to remote access the router.
- 2) Disable **Valid** for all specific IP(s) in the IP range to allow any IP(s) to remote access the router.
- 3) No listing of IP range is to allow any IP(s) to remote access the router.

Power Management

Power management is a feature of some electrical appliances, especially computers that turn off the power or switch to a low-power state when inactive.
Five main parameters are listed for users to check to manage the performance of the router.

Advanced Setup

Power Management

Parameters

MIPS CPU Clock divider when Idle	☒ Enable	Status	Enabled
Wait instruction when Idle	☒ Enable	Status	Enabled
DRAM Self Refresh	☒ Enable	Status	Enabled
Energy Efficient Ethernet	☒ Enable	Status	Enabled
Ethernet Auto Power Down and Sleep	☒ Enable	Status	Enabled

Number of ethernet interfaces in:
Powered up: 3
Powered down: 3

Apply

Refresh

Time Schedule

The Time Schedule supports up to **32** timeslots which helps you to manage your Internet connection. In each time profile, you may schedule specific day(s) i.e. Monday through Sunday to restrict or allowing the usage of the Internet by users or applications.

This Time Schedule correlates closely with router’s time, since router does not have a real time clock on board; it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server from the Internet. Refer to [Internet Time](#) for details. You router time should synchronize with NTP server.

Management

Time Schedule

Parameters

Name

Day in a week

☐ Sun

☐ Mon

☐ Tue

☐ Wed

☐ Thu

☐ Fri

☐ Sat

Start Time

00 : 00

End Time

00 : 00

Add

Edit / Delete

For example, user can add a timeslot named “timeslot1” features a period of 9:00-19:00 on every weekday.

Management

Time Schedule

Parameters

Name

Day in a week

☐ Sun

☐ Mon

☐ Tue

☐ Wed

☐ Thu

☐ Fri

☐ Sat

Start Time

00 : 00

End Time

00 : 00

Add

Edit / Delete

Edit	Name	Day in a week	Start Time	End Time	Delete
☐	timeslot1	sMTWTFs	09:00	19:00	☐

Auto Reboot

Auto reboot offers flexible rebooting service (reboot with the current configuration) of router for users in line with scheduled timetable settings.

Advanced Setup

Auto Reboot

Parameters

Schedule

1. ☐ Enable ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat Time 00 : 00

2. ☐ Enable ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat Time 00 : 00

Apply

Enable to set the time schedule for rebooting.

For example, the router is scheduled to reboot at 22:00 every single weekday, and to reboot at 9:00 on Saturday and Sunday. You can set as follows:

Advanced Setup

Auto Reboot

Parameters

Schedule

1. ☒ Enable ☐ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☐ Sat Time 22 : 00

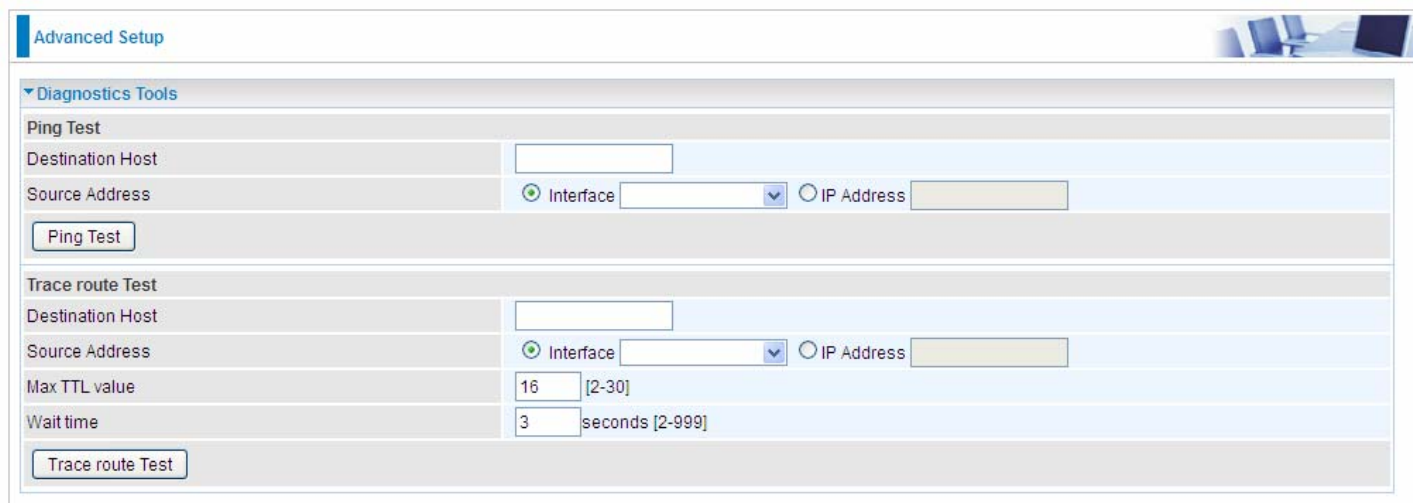
2. ☒ Enable ☒ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☒ Sat Time 09 : 00

Apply

Diagnostics

Diagnostics Tools

BiPAC 8920AX(L) offers diagnostics tools including “Ping” and “Trace route test” tools to check for problems associated with network connections.



The screenshot shows the 'Advanced Setup' interface with a 'Diagnostics Tools' section. It contains two test configurations:

- Ping Test:** Includes a 'Destination Host' text field, a 'Source Address' section with a selected 'Interface' (indicated by a green dot) and an 'IP Address' option (indicated by a radio button), and a 'Ping Test' button.
- Trace route Test:** Includes a 'Destination Host' text field, a 'Source Address' section with a selected 'Interface' and an 'IP Address' option, a 'Max TTL value' field set to '16' with a range '[2-30]', a 'Wait time' field set to '3' with a range 'seconds [2-999]', and a 'Trace route Test' button.

Ping Test: to verify the connectivity between source and destination.

Destination Host: Enter the destination host (IP, domain name) to be checked for connectivity.

Source Address: Select or set the source address to test the connectivity from the source to the destination.

Ping Test: Press this button to proceed ping test.

Trace route Test: to trace the route to see how many hops (also see the exact hops) the packet of data has to take to get to the destination.

Destination Host: Set the destination host (IP, domain name) to be traced.

Source Address: Select or set the source address to trace the route from the source to the destination.

Max TTL value: Set the max Time to live (TTL) value.

Wait time: Set waiting time for each response in seconds.

Example: Ping www.google.com

Advanced Setup

Diagnostics Tools

Ping Test

Destination Host:

Source Address: ☒ Interface ☐ IP Address

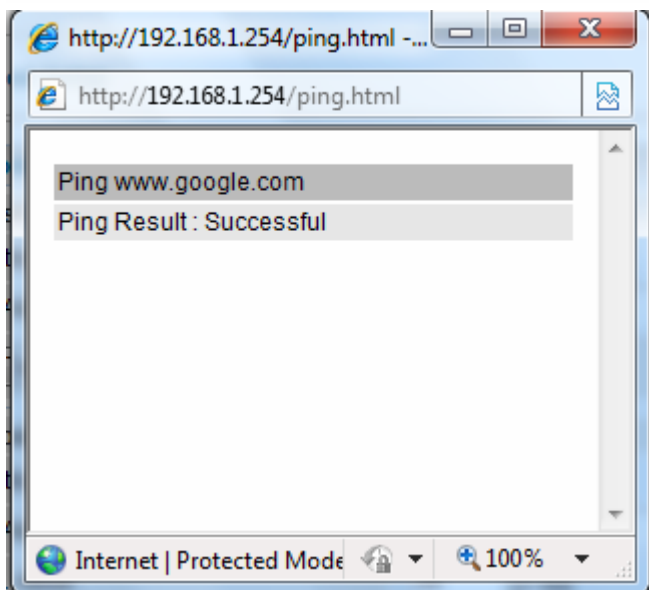
Trace route Test

Destination Host:

Source Address: ☒ Interface ☐ IP Address

Max TTL value: [2-30]

Wait time: seconds [2-999]



Example: "trace" www.google.com

Advanced Setup

▼Diagnostics Tools

Ping Test

Destination Host

Source Address ☒ Interface ☐ IP Address

Trace route Test

Destination Host

Source Address ☒ Interface ☐ IP Address

Max TTL value [2-30]

Wait time seconds [2-999]

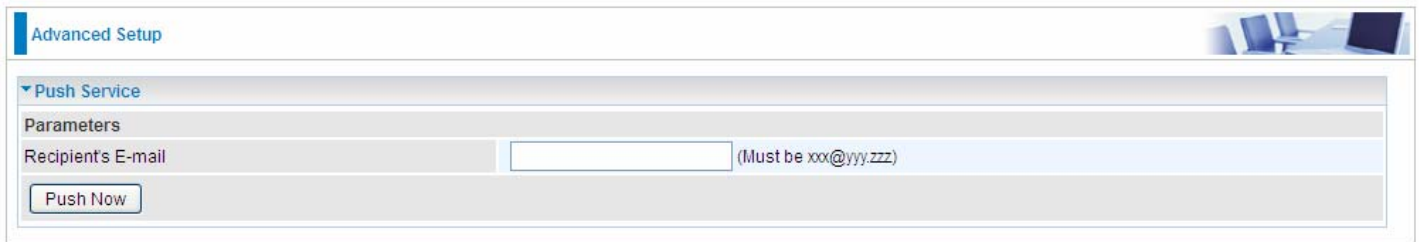
http://192.168.1.254/tracert.html - Windows Intern...

http://192.168.1.254/tracert.html

No.	Route Address	Time
1	112.86.208.1	22.229 ms
2	221.6.9.93	20.352 ms
3	221.6.2.169	24.345 ms
4	219.158.24.41	52.837 ms
5	219.158.23.18	54.696 ms
6	219.158.19.190	54.904 ms
7	219.158.3.238	57.824 ms
8	72.14.215.130	58.851 ms
9	209.85.248.60	57.644 ms
10	209.85.250.122	81.242 ms
11	209.85.250.103	81.351 ms
12	*	**
13	173.194.72.147	79.753 ms

Push Service

With push service, the system can send email messages with consumption data and system information.



The screenshot shows a web interface titled 'Advanced Setup' in the top left corner. Below the title bar, there is a section labeled 'Push Service' with a dropdown arrow. Under this section, there is a 'Parameters' label. Below the label, there is a text input field for 'Recipient's E-mail'. To the right of the input field, there is a hint text: '(Must be xxx@yyy.zzz)'. Below the input field, there is a button labeled 'Push Now'.

Recipient's E-mail: Enter the destination mail address. The email is used to receive **system log** , **system configuration**, **security log** sent by the device when the **Push Now** button is pressed (information sent only when pressing the button), but the mail address is not remembered.

Note: Please first set correct the SMTP server parameters in [Mail Alert](#).

Diagnostics

Check the connections, including Ethernet connection, Internet Connection and wireless connection. Click **Help** link that can lead you to the interpretation of the results and the possible, simply troubleshooting.

Advanced Setup

Test the connection to your local network --- pppoe_0_8_35

Test LAN Connection (P1)	FAIL	Help
Test LAN Connection (P3)	PASS	Help
Test LAN Connection (P4)	FAIL	Help
Test LAN Connection (P2)	FAIL	Help
Test your Wireless Connection	PASSPASS	Help

Test the connection to your DSL service provider

Test xDSL Synchronization	PASS	Help
Test ATM OAM F5 segment ping	PASS	Help
Test ATM OAM F5 end-to-end ping	PASS	Help

Test the connection to your Internet service provider

Test PPP server connection	PASS	Help
Test authentication with ISP	PASS	Help
Test the assigned IP address	PASS	Help
Ping default gateway	PASS	Help
Ping primary Domain Name Server	PASS	Help

Next Connection

Test

Test With OAM F4

Fault Management

IEEE 802.1ag Connectivity Fault Management (CFM) is a standard defined by IEEE. It defines protocols and practices for OAM (Operations, Administration, and Maintenance) for paths through 802.1 bridges and local area networks (LANs). Fault Management is to uniquely test the PTM connection; Push service

Advanced Setup

802.1ag Connectivity Fault Management

Parameters

This diagnostic is only used for xDSL PTM mode.

Maintenance Domain (MD) Level: 2

Destination MAC Address:

802.1Q VLAN ID: 0 [0-4095]

xDSL Traffic Type: Inactive

Test the connection to another Maintenance End Point (MEP)

Loopback Message (LBM)

Find Maintenance End Points (MEPs)

Linktrace Message (LTM)

Set MD Level Send Loopback Send Linktrace

Maintenance Domain (MD) Level: Maintenance Domains (MDs) are management spaces on a network, typically owned and operated by a single entity. MDs are configured with Names and Levels, where the eight levels range from 0 to 7. A hierarchal relationship exists between domains based on levels. The larger the domain, the higher the level value.

Maintenance End Point: Points at the edge of the domain, define the boundary for the domain. A MEP sends and receives CFM frames through the relay function, drops all CFM frames of its level or lower that come from the wire side.

Link Trace: Link Trace messages otherwise known as Mac Trace Route are Multicast frames that a MEP transmits to track the path (hop-by-hop) to a destination MEP which is similar in concept to User Datagram Protocol (UDP) Trace Route. Each receiving MEP sends a Trace route Reply directly to the Originating MEP, and regenerates the Trace Route Message.

Loop-back: Loop-back messages otherwise known as Mac ping are Unicast frames that a MEP transmits, they are similar in concept to an Internet Control Message Protocol (ICMP) Echo (Ping) messages, sending Loop-back to successive MIPs can determine the location of a fault. Sending a high volume of Loop-back Messages can test bandwidth, reliability, or jitter of a service, which is similar to flood ping. A MEP can send a Loop-back to any MEP or MIP in the service. Unlike CCMs, Loop back messages are administratively initiated and stopped.

Restart

This section lets you restart your router if necessary. Click  **Restart** in the low right corner of each configuration page.

Configuration

Restart

After restarting. Please wait for several seconds to let the system come up.

Restart device with

☐ Factory Default Settings

☒ Current Settings

Restart

If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select Factory Default Settings to reset to factory default settings. Or you just want to restart after the current setting, the select the Current Settings, and Click Restart.

progress

progress...

Do not switch off device during flash update or rebooting.

total :

8%

Chapter 5: Troubleshooting

If your router is not functioning properly, please refer to the suggested solutions provided in this chapter. If your problems persist or the suggested solutions do not meet your needs, please kindly contact your service provider or Billion for support.

Problems with the router

Problem	Suggested Action
None of the LEDs is on when you turn on the router	Check the connection between the router and the adapter. If the problem persists, most likely it is due to the malfunction of your hardware. Please contact your service provider or Billion for technical support.
You have forgotten your login username or password	Try the default username "admin" and password "admin". If this fails, you can restore your router to its factory settings by pressing the reset button on the device rear side.

Problems with WAN interface

Problem	Suggested Action
Frequent loss of ADSL line sync (disconnections)	Ensure that all other devices connected to the same telephone line as your router (e.g. telephones, fax machines, analogue modems) have a line filter connected between them and the wall socket (unless you are using a Central Splitter or Central Filter installed by a qualified and licensed electrician), and ensure that all line filters are correctly installed and the right way around. Missing line filters or line filters installed the wrong way around can cause problems with your ADSL connection, including causing frequent disconnections. If you have a back-to-base alarm system you should contact your security provider for a technician to make any necessary changes.

Problem with LAN interface

Problem	Suggested Action
Cannot PING any PC on LAN	Check the Ethernet LEDs on the front panel. The LED should be on for the port that has a PC connected. If it does not lit, check to see if the cable between your router and the PC is properly connected. Make sure you have first uninstalled your firewall program before troubleshooting.
	Verify that the IP address and the subnet mask are consistent for both the router and the workstations.

Appendix: Product Support & Contact

If you come across any problems please contact the dealer from where you purchased your product.

Contact Billion

Worldwide:

<http://www.billion.com>

MAC OS is a registered Trademark of Apple Computer, Inc.

Windows 98, Windows NT, Windows 2000, Windows Me, Windows XP, Windows Vista, Windows 7 and Windows 8 are registered Trademarks of Microsoft Corporation.

Federal Communication Commission Interference Statement

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

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

FCC Caution:

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

(1) This device may not cause harmful interference

(2) This device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. . This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

Co-location statement

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Radiation Exposure Statement

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