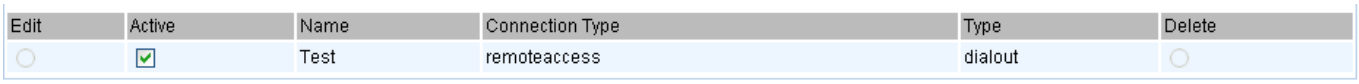
5.3.5 VPN – Virtual Private Networks

Virtual Private Networks is ways to establish secured communication tunnels to an organization's network via the Internet. Your router supports three main types of VPN (Virtual Private Network), **PPTP**, **IPSec** and **L2TP**

5.3.5.1 PPTP (Point-to-Point Tunneling Protocol)

There are two types of PPTP VPN supported; **Remote Access** and **LAN-to-LAN** (please refer below for more information.). Click Configuration/VPN/PPTP.



Name: A given name for the connection.

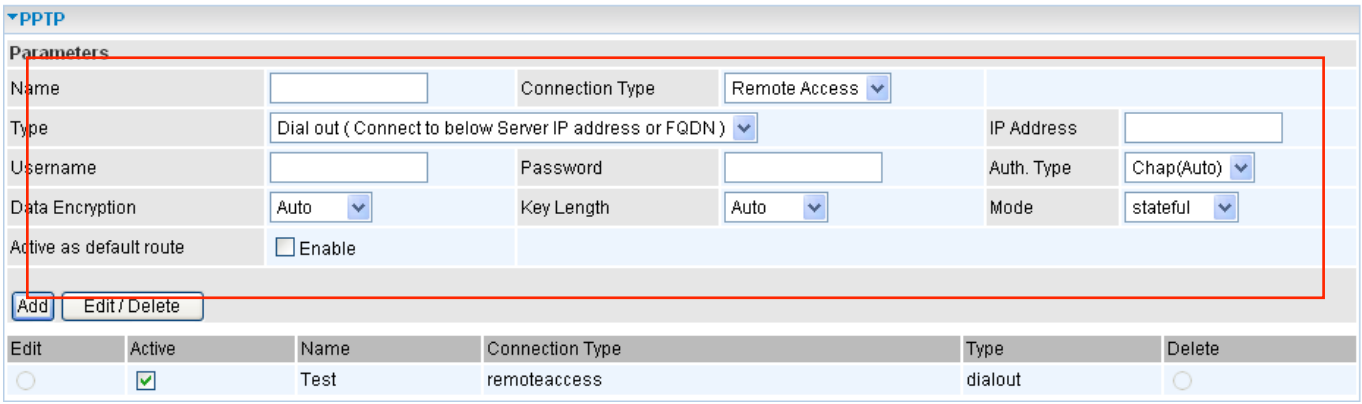
Active: This function activates or deactivates the PPTP connection. Check Active checkbox if you want the protocol of tunnel to be activated and vice versa.

Note: When the Active checkbox is checked, the function of Edit and Delete will not be available.

Connection Type: It informs your PPTP tunnel connection condition.

Type: This refers to your router operates as a client or a server, **Dialout** or **Dialin** respectively.

PPTP Connection - Remote Access



Name: A given name for the connection (e.g. "connection to office").

Connection Type: Remote Access or **LAN to LAN**

Type: Check **Dial Out** if you want your router to operate as a client (connecting to a remote VPN server, e.g. your office server), check **Dial In** operates as a VPN server.

- When configuring your router as a Client, enter the remote **Server IP Address (or Domain Name)** you wish to connect to.
- When configuring your router as a server, enter the **Private IP Address Assigned to Dial in User** address.

Username: If you are a Dial-Out user (client), enter the username provided by your Host. If you are a Dial-In user (server), enter your own username.

Password: If you are a Dial-Out user (client), enter the password provided by your Host. If you are a Dial-In user (server), enter your own password.

Authentication 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.

Data Encryption: Data sent over the VPN connection can be encrypted by an MPPE algorithm. Default is **Auto,** so that this setting is negotiated when establishing a connection, or else you can manually **Enable** or **Disable** 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.

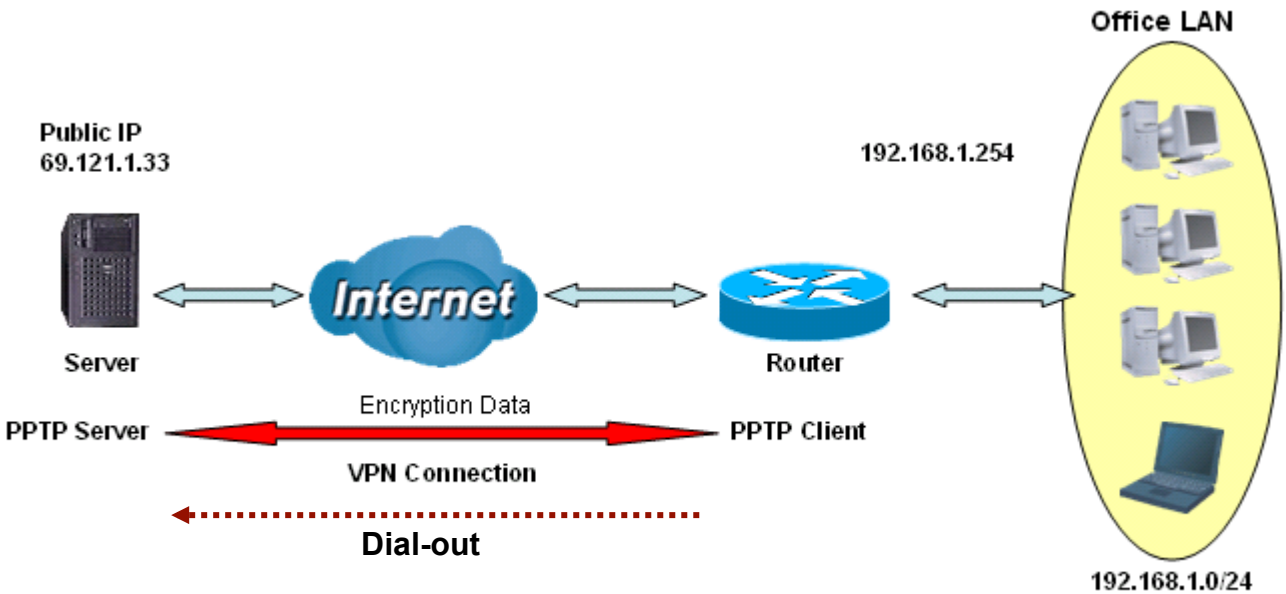
Mode: You may select **Stateful** or **Stateless** mode. The key will be changed every 256 packets when you select Stateful mode. If you select Stateless mode, the key will be changed in each packet.

Active as default route: Commonly used by the *Dial-out* connection which all packets will route through the VPN tunnel to the Internet; therefore, active the function may degrade the Internet performance.

Click **Edit/Delete** button to save your changes.

Example: Configuring a Remote Access PPTP VPN Dial-out Connection

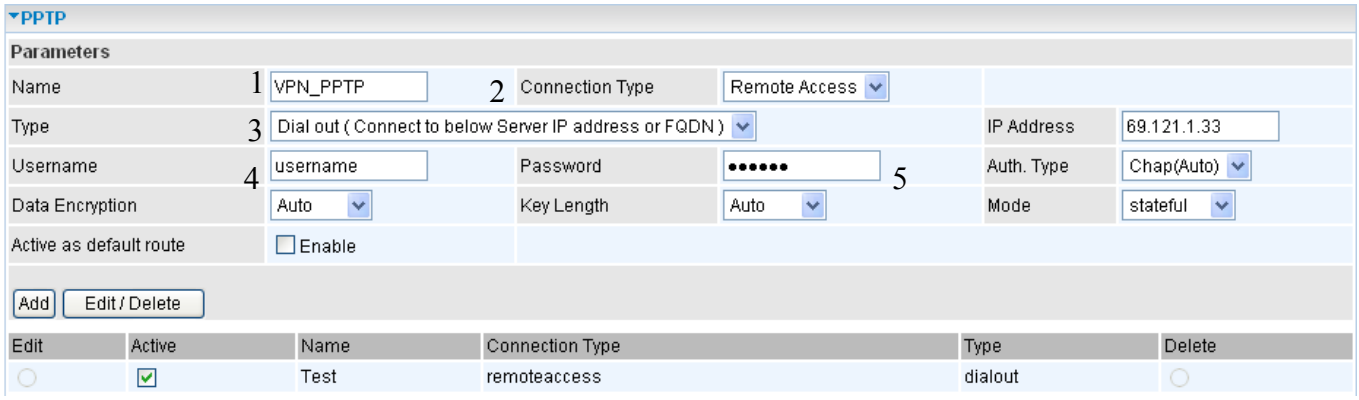
A company's office establishes a PPTP VPN connection with a file server located at a separate location. The router is installed in the office, connected to a couple of PCs and Servers.



PPTP VPN-Remote Access (Dial-out)

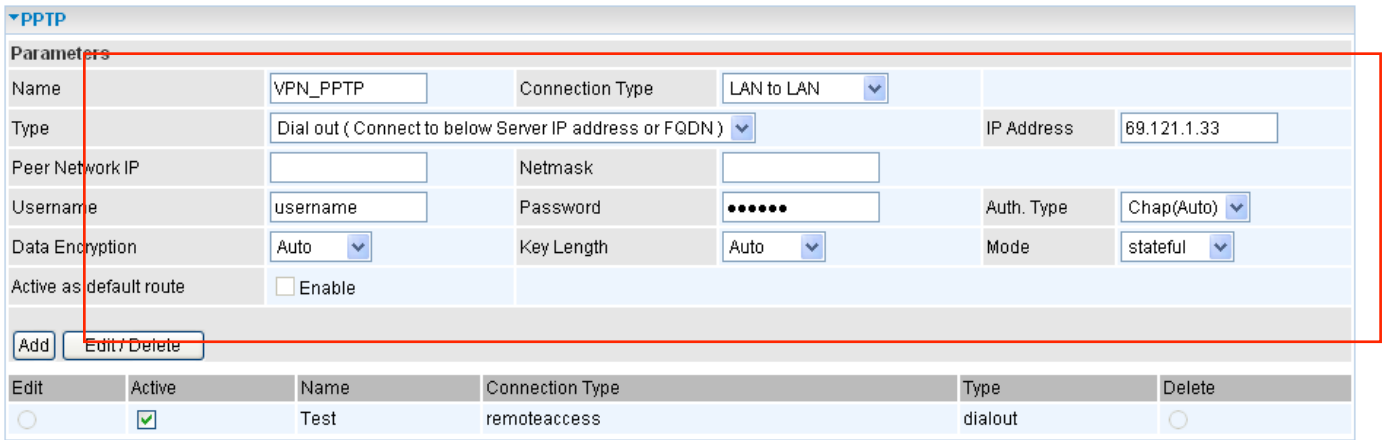
Configuring the PPTP VPN in the Office

Click **Configuration/VPN/PPTP**. Choose **Remote Access** from **Connect Type** drop-down menu. You can either input the IP address (69.121.1.33 in this case) or hostname to reach the server.



Item	Function		Description
1	Name	VPN_PPTP	Given name of PPTP connection
2	Connection Type	Remote Access	Select Remote Access from Connection Type drop-down menu
3	Type	Dial out	Select Dial out from Type drop-down menu
	IP Address (or Domain name)	69.121.1.33	An Dialed server IP
4	Username	username	A given username & password
	Password	123456	
5	Auth.Type	Chap(Auto)	Keep as default value in most of the cases, PPTP server & client will determine the value automatically. Refer to manual for details if you want to change the setting.
	Data Encryption	Auto	
	Key Length	Auto	
	Mode	stateful	

PPTP Connection - LAN to LAN



Name: A given name of the connection.

Connection Type: Remote Access or **LAN to LAN.**

Type: Check **Dial Out** if you want your router to operate as a client (connecting to a remote VPN server, e.g. your office server), check **Dial In** operates as a VPN server.

- When configuring your router as a Client, enter the remote **Server IP Address (or Domain name)** you wish to connect to.

- When configuring your router as a server, enter the **Private IP Address Assigned to Dial in User** address.

Peer Network IP: Enter Peer network IP address.

Netmask: Enter the subnet mask of peer network based on the Peer Network IP setting.

Username: If you are a Dial-Out user (client), enter the username provided by your Host. If you are a Dial-In user (server), enter your own username.

Password: If you are a Dial-Out user (client), enter the password provided by your Host. If you are a Dial-In user (server), enter your own password.

Authentication 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 the client has not been replaced by an intruder.

Data Encryption: Data sent over the VPN connection can be encrypted by an MPPE algorithm. Default is **Auto,** so that this setting is negotiated when establishing a connection, or else you can manually **Enable** or **Disable** 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.

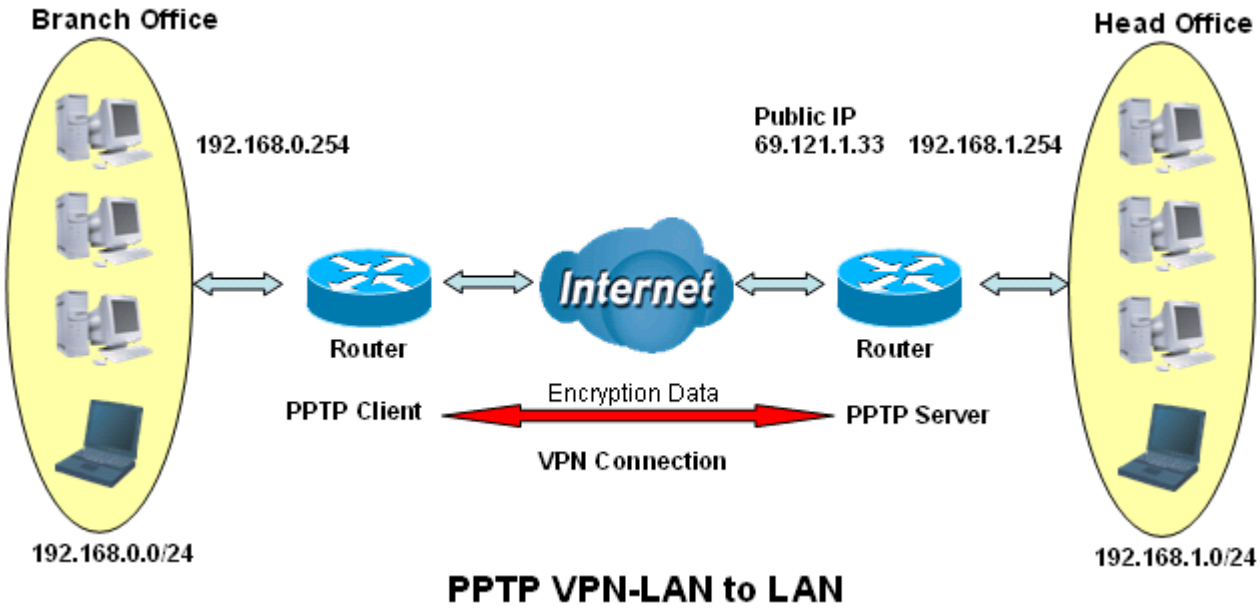
Mode: You may select **Stateful** or **Stateless** mode. The key will be changed every 256 packets when you select Stateful mode. If you select Stateless mode, the key will be changed in each packet.

Active as default route: As the connection type is LAN to LAN, this function will become to disable.

Click **Edit/Delete** button to save your changes.

Example: Configuring a PPTP LAN-to-LAN 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.



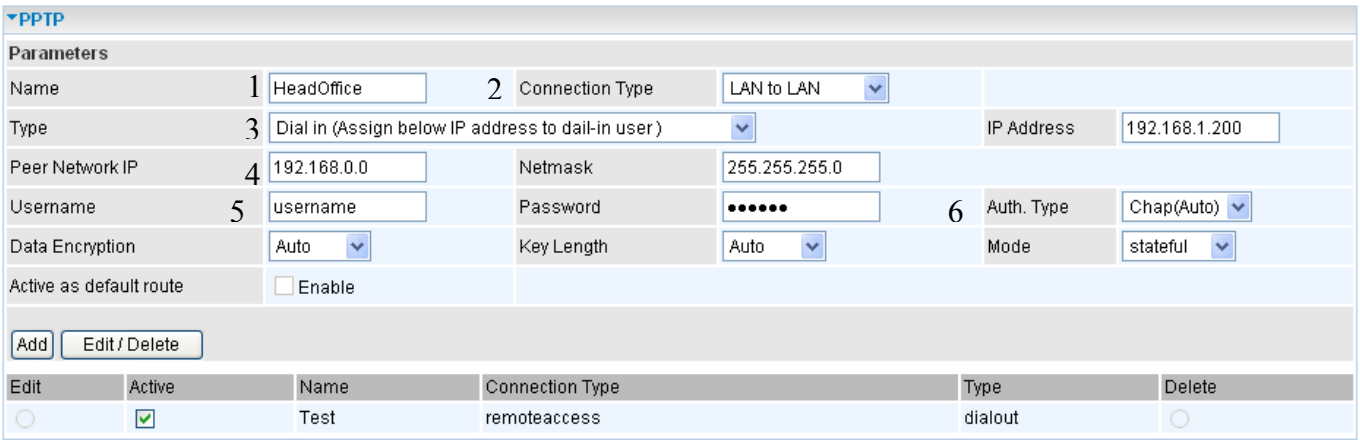
PPTP VPN-LAN to LAN

Attention

Both office LAN networks **MUST in different subnet** with LAN to LAN application.

Configuring PPTP VPN in the Head Office

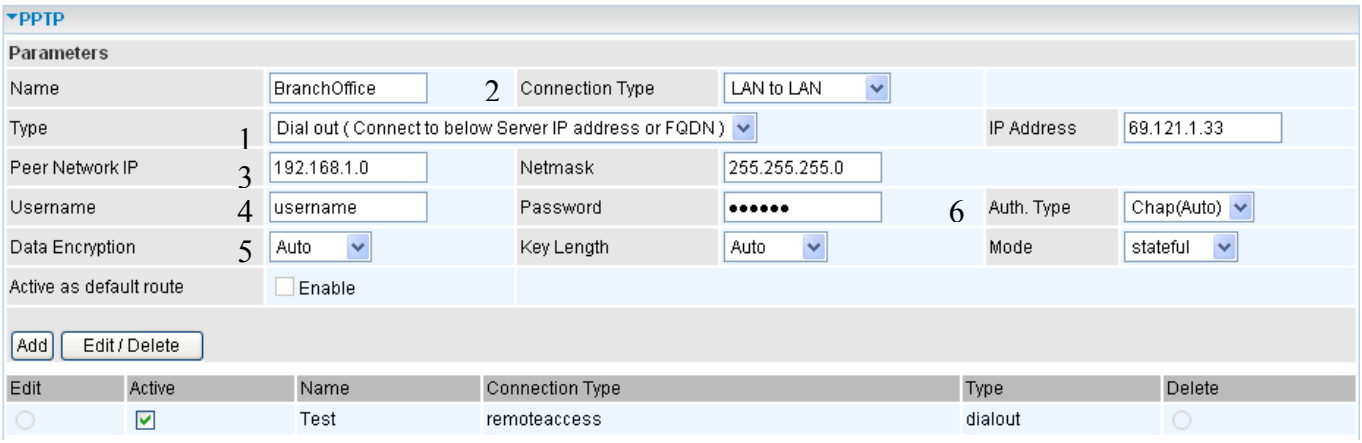
The IP address 192.168.1.201 will be assigned to the router located in the branch office. Please make sure this IP is not used in the head office LAN.



Item	Function		Description
1	Name	HeadOffice	Given a name of PPTP connection
2	Connection Type	LAN to LAN	Select LAN to LAN from Connection Type drop-down menu
3	Type	Dial in	Select Dial in from Type drop-down menu
	IP Address	192.168.1.200	IP address assigned to branch office network
4	Peer Network IP	192.168.0.0	Branch office network
	Netmask	255.255.255.0	
5	Username	username	Input username & password to authenticate branch office network
	Password	123456	
6	Auth.Type	Chap(Auto)	Keep as default value in most of the cases, PPTP server & client will determine the value automatically. Refer to manual for details if you want to change the setting.
	Data Encryption	Auto	
	Key Length	Auto	
	Mode	stateful	

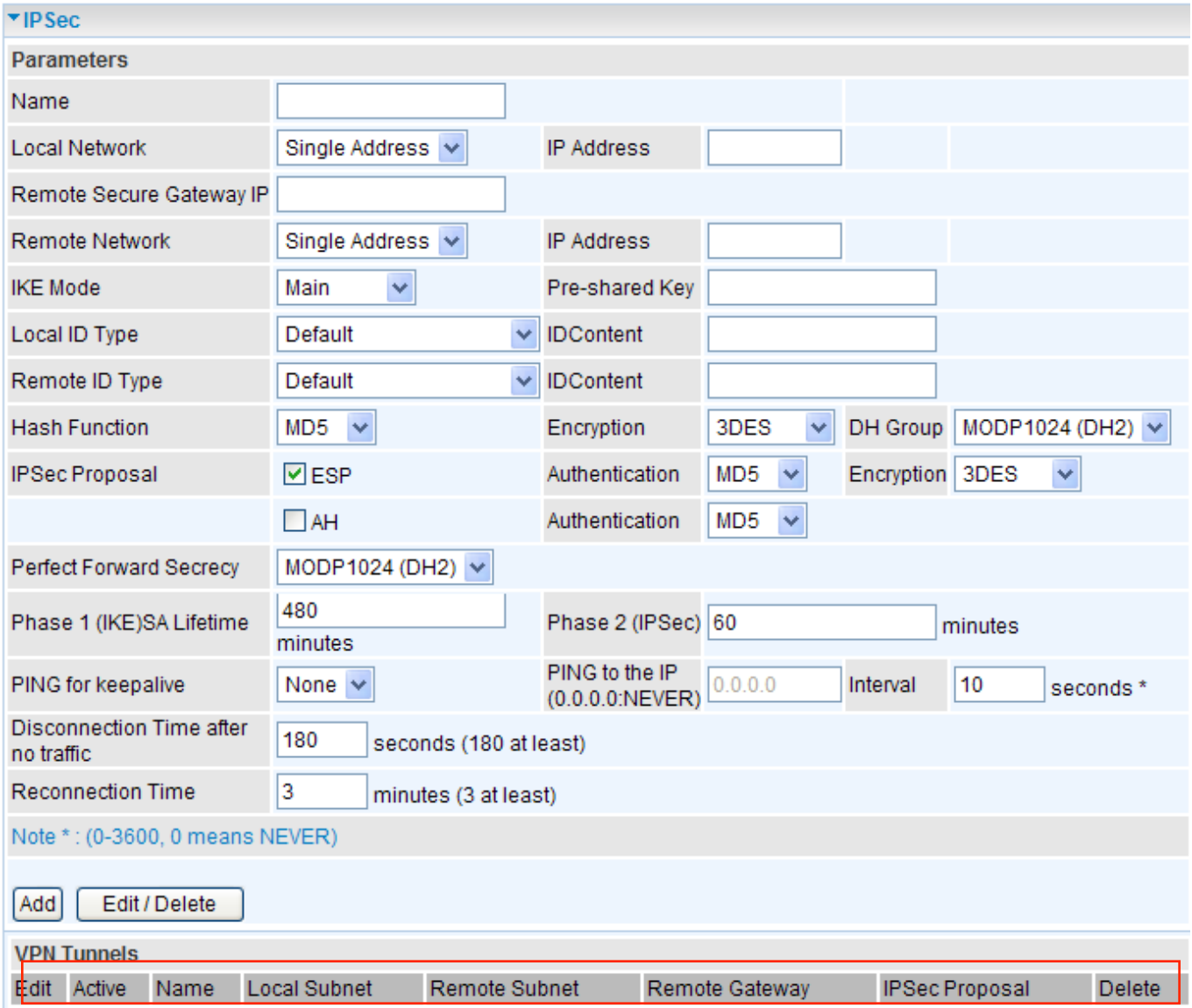
Configuring PPTP VPN in the Branch Office

The IP address 69.121.1.33 is the **Public IP** address of the router located in head office. If you registered the DDNS (please refer to the **DDNS** section of this manual), you can also use the domain name instead of the IP address to reach the router.



Item	Function		Description
1	Name	BranchOffice	Given a name of PPTP connection
2	Connection Type	LAN to LAN	Select LAN to LAN from Connection Type drop-down menu
3	Type	Dial out	Select Dial out from Type drop-down menu
	IP Address (or Domain name)	69.121.1.33	IP address of the head office router (in WAN side)
4	Peer Network IP	192.168.1.0	Head office network
	Netmask	255.255.255.0	
5	Username	username	Input username & password to authenticate head office network
	Password	123456	
6	Auth.Type	Chap(Auto)	Keep as default value in most of the cases, PPTP server & client will determine the value automatically. Refer to manual for details if you want to change the setting.
	Data Encryption	Auto	
	Key Length	Auto	
	Mode	stateful	

5.3.5.2 IPSec (IP Security Protocol)



Active: This function activates or deactivates the IPSec connection. Check Active checkbox if you want the protocol of tunnel to be activated and vice versa.

Note: When the Active checkbox is checked, the function of Edit and Delete will not be available.

Name: This is a given name of the connection.

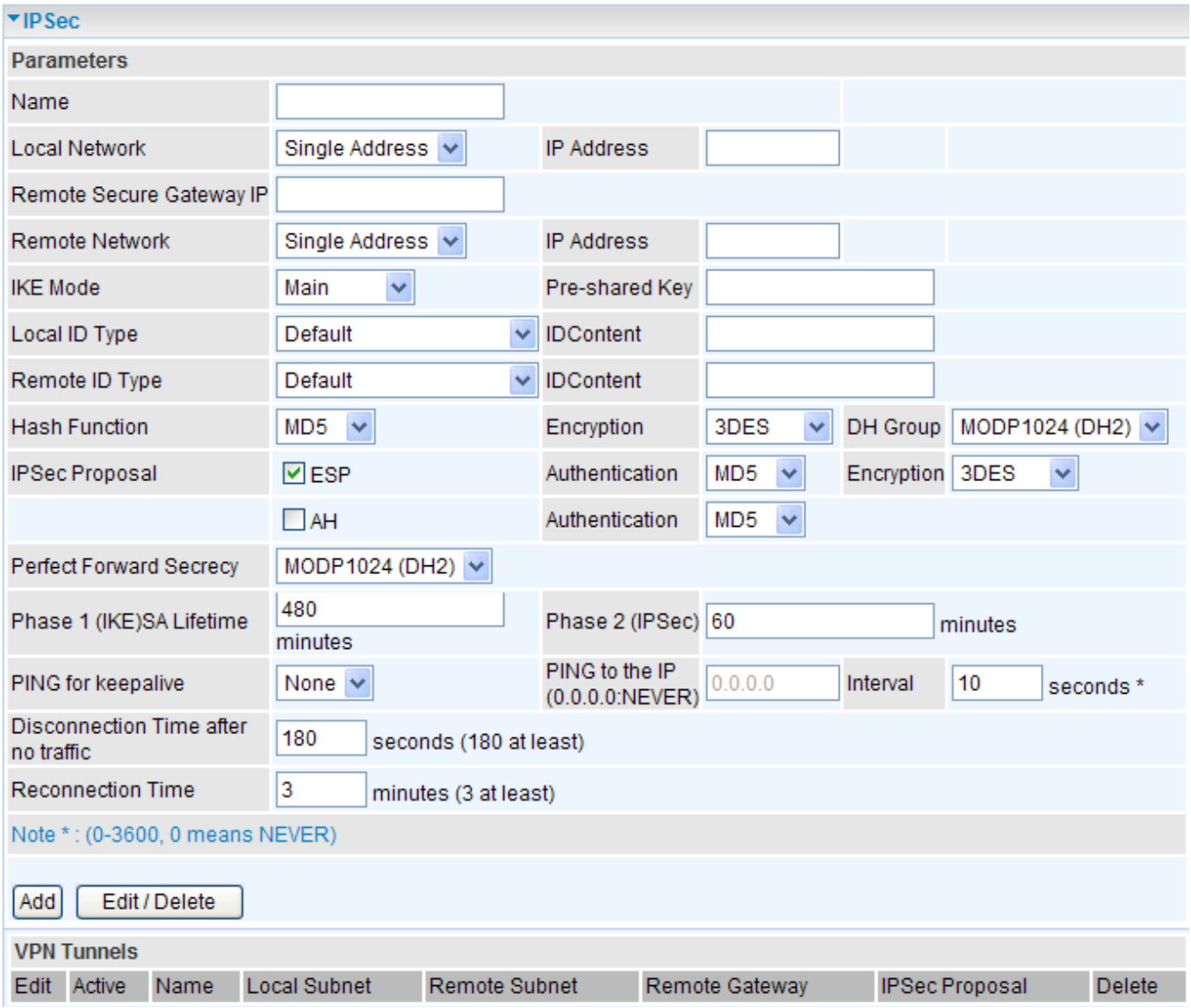
Local Subnet: Displays IP address and subnet of the local network.

Remote Subnet: Displays IP address and subnet of the remote network.

Remote Gateway: This is the IP address or Domain Name of the remote VPN device that is connected and established a VPN tunnel.

IPSec Proposal: This is selected IPSec security method.

IPSec VPN Connection



Name: A given name for the connection (e.g. “connection to office”).

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

- **Single Address:** The IP address of the local host.
- **Subnet:** The subnet of the local network. For example, IP: 192.168.1.0 with netmask 255.255.255.0 specifies one class C subnet starting from 192.168.1.1 (i.e. 192.168.1.1 through to 192.168.1.254).
- **IP Range:** The IP address range of the local network. For example, IP: 192.168.1.1, end IP: 192.168.1.10.

Remote Secure Gateway Address (or Domain Name): The IP address or hostname of the remote VPN device that is connected and establishes a VPN tunnel.

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

IKE (Internet key Exchange) Mode: Select IKE mode to Main mode or Aggressive mode. This IKE provides secured key generation and key management.

Local ID:

- **Content:** Input ID’s information, like domain name www.ipsectest.com.

Remote ID:

- **Identifier:** Input remote ID’s information, like domain name www.ipsectest.com.

Hash Function: It is a Message Digest algorithm which coverts any length of a message into a unique

set of bits. It is widely used MD5 (Message Digest) and SHA-1 (Secure Hash Algorithm) algorithms. SHA1 is more resistant to brute-force attacks than MD5, however it is slower.

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

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

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

DH (Diffie-Hellman) 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). There are three modes, MODP 768-bit, MODP 1024-bit and MODP 1536-bit. MODP stands for Modular Exponentiation Groups.

IPSec Proposal: Select the IPSec security method. There are two methods of checking the authentication information, AH (authentication header) and ESP (Encapsulating Security Payload). Use ESP for greater security so that data will be encrypted and authenticated. Using AH data will be authenticated but not encrypted.

Authentication: Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmit. There are three options, Message Digest 5 (**MD5**), Secure Hash Algorithm (**SHA1**) or **NONE**. SHA1 is more resistant to brute-force attacks than MD5, however it is slower.

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

Encryption: Select the encryption method from the pull-down menu. There are several options, **DES**, **3DES**, **AES (128, 192 and 256)** and **NULL**. NULL means it is a tunnel only with no encryption. 3DES and AES are more powerful but increase latency.

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

Perfect Forward Secrecy: Choose whether to enable PFS using Diffie-Hellman public-key cryptography to change encryption keys during the second phase of VPN negotiation. This function will provide better security, but extends the VPN negotiation time. Diffie-Hellman 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). There are three modes, MODP 768-bit, MODP 1024-bit and MODP 1536-bit. MODP stands for Modular Exponentiation Groups.

Pre-shared Key: This is for the Internet Key Exchange (IKE) protocol, a string from 4 to 128 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).

SA Lifetime: Specify the number of minutes that a Security Association (SA) will stay active before new encryption and authentication key will be exchanged. There are two kinds of SAs, IKE and IPSec. IKE negotiates and establishes SA on behalf of IPSec, an IKE SA is used by IKE.

⊙ **Phase 1 (IKE):** To issue an initial connection request for a new VPN tunnel. The range can be from 5 to 15,000 minutes, and the default is 480 minutes.

⊙ **Phase 2 (IPSec):** To negotiate and establish secure authentication. The range can be from 5 to 15,000 minutes, and the default is 60 minutes.

A short SA time increases security by forcing the two parties to update the keys. However, every time the VPN tunnel re-negotiates, access through the tunnel will be temporarily disconnected.

PING for Keep Alive:

⊙**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.

⊙**PING:** This mode will detect the remote IPSec peer has lost or not by pinging specify IP address.

⊙**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.

PING to the IP: 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. Re-establish 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.

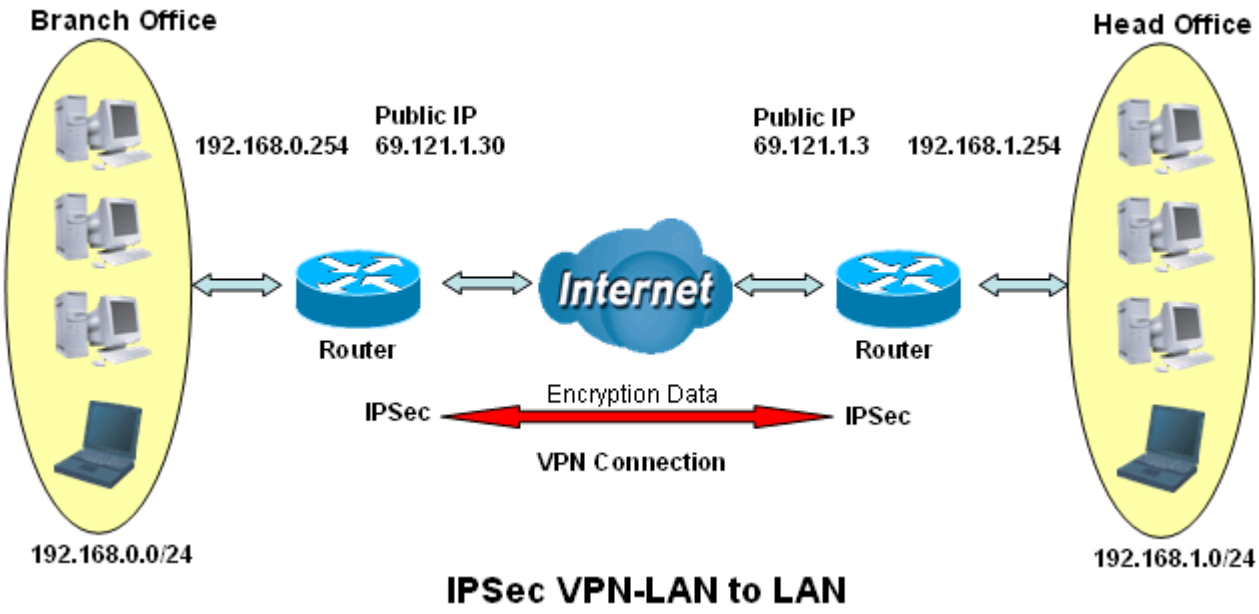
Ping to the IP	Interval (sec)	*Ping to the IP* Action
0.0.0.0	0	No
0.0.0.0	2000	No
xxx.xxx.xxx.xxx (A valid IP Address)	0	No
xxx.xxx.xxx.xxx(A valid IP Address)	2000	Yes, activate it in every 2000 second.

Disconnection Time after no traffic: It is the NO Response time clock. When no traffic stage time is beyond the Disconnection time set, Router will automatically halt the tunnel connection and re-establish it base on the **Reconnection Time** set. **180 seconds** is minimum time interval for this function.

Reconnection Time: It is the reconnecting time interval after NO TRAFFIC is initiated. **3 minutes** is minimum time interval for this function.

Click **Edit/Delete** to save your changes.

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



IPSec VPN-LAN to LAN

Table 3: Network Configuration and Security Plan

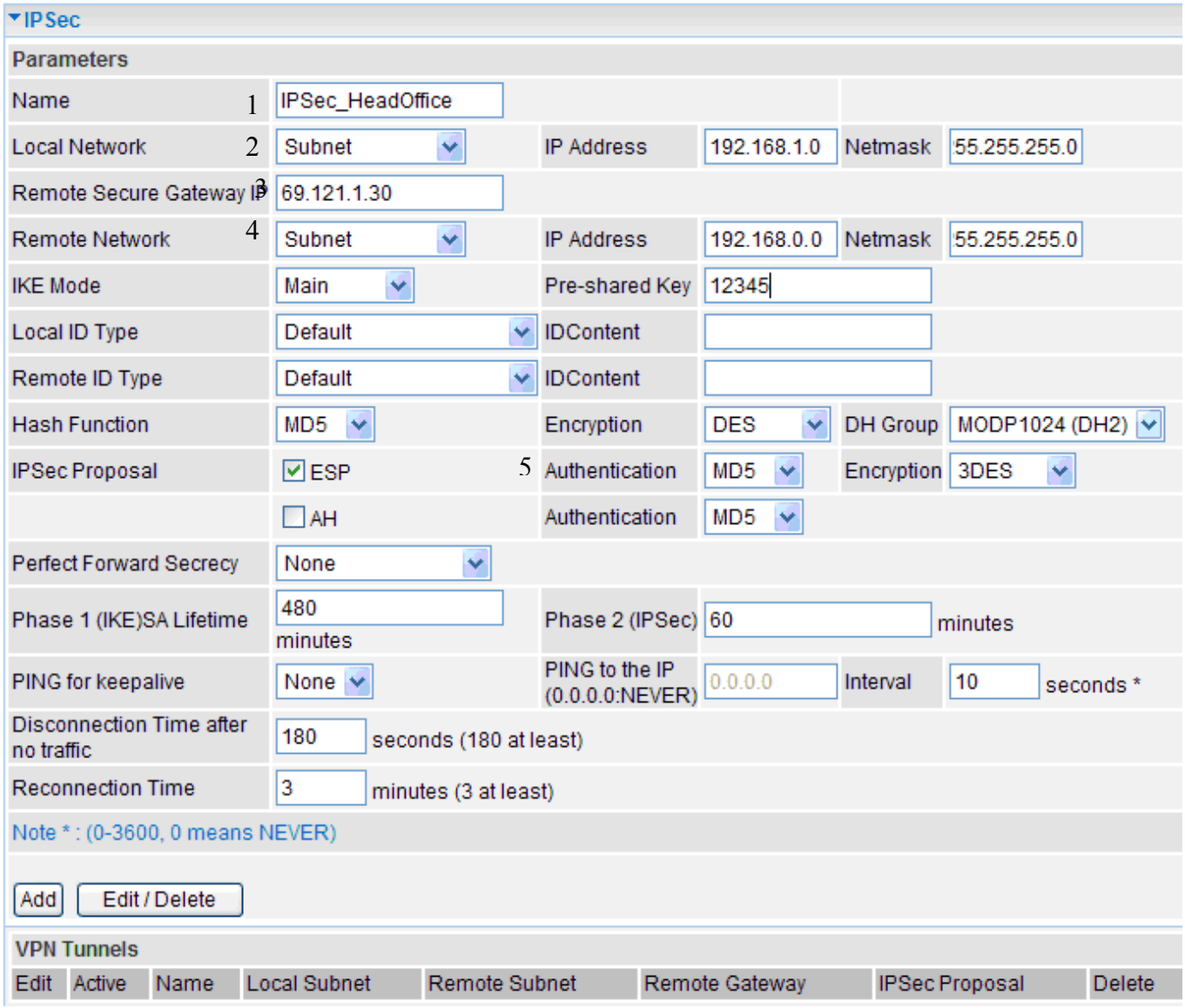
	Branch Office	Head Office
Local Network ID	192.168.0.0/24	192.168.1.0/24
Local Router IP	69.121.1.30	69.121.1.3
Remote Network ID	192.168.1.0/24	192.168.0.0/24
Remote Router IP	69.1.121.3	69.1.121.30
IKE Pre-shared Key	12345678	12345678
VPN Connection Type	Tunnel mode	Tunnel mode
Security Algorithm	ESP:MD5 with AES	ESP:MD5 with AES

Attention

Both office LAN networks **MUST in different subnet** with LAN to LAN application.

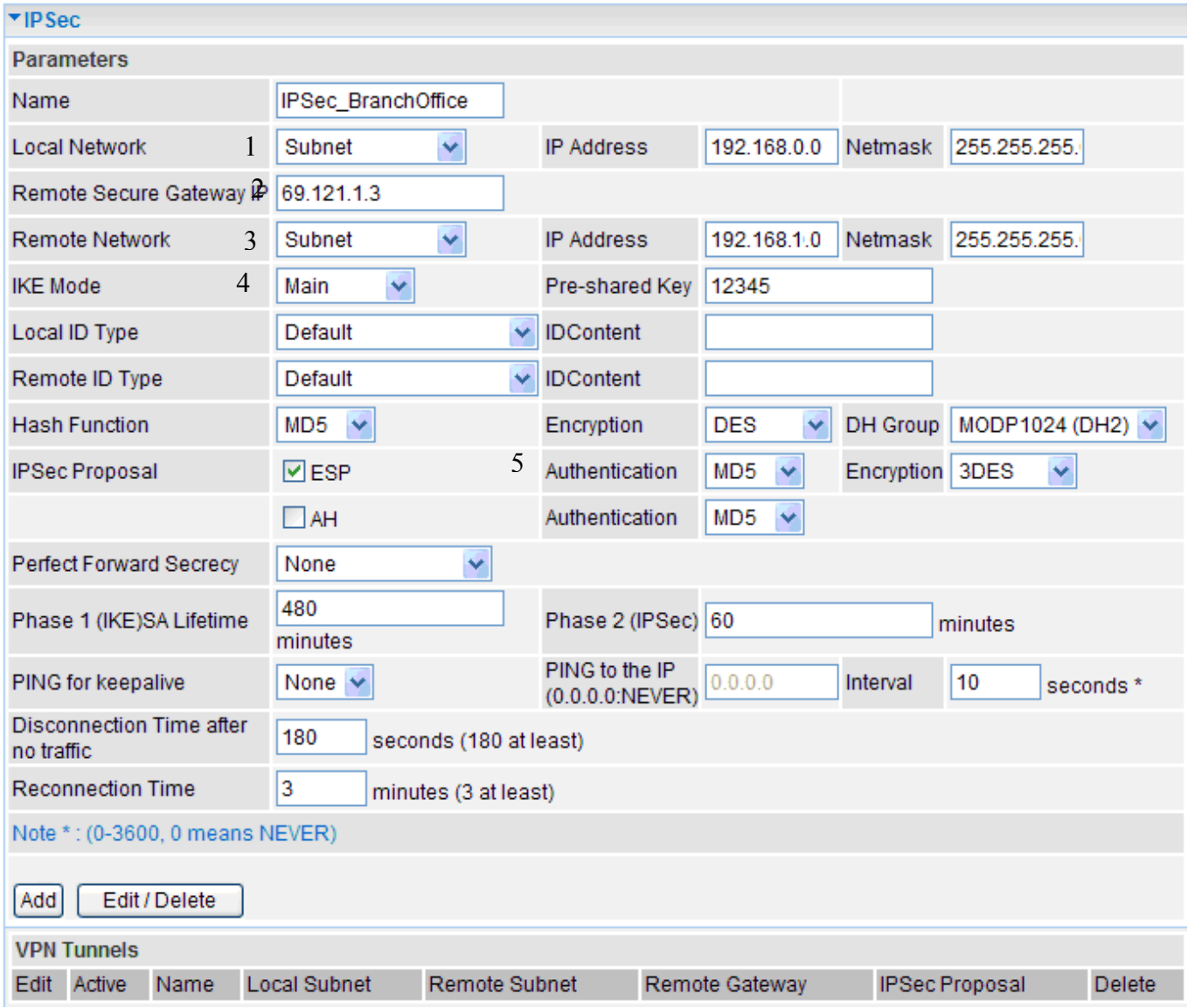
Functions of **Pre-shared Key, VPN Connection Type and Security Algorithm MUST BE** identically set up on both sides.

Configuring IPSec VPN in the Head Office



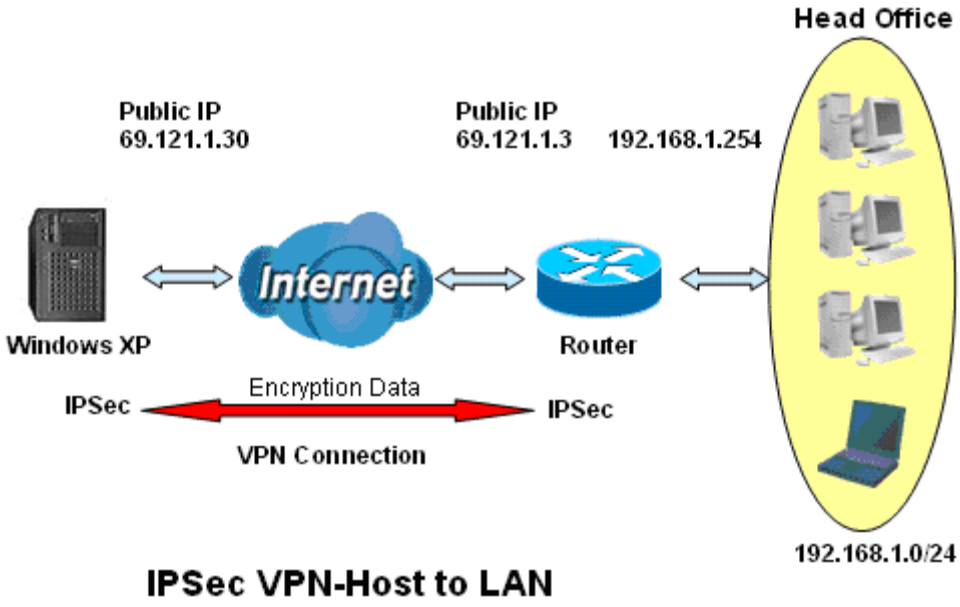
Item	Function		Description
1	Name	IPSec_HeadOffice	Given a name of IPSec connection
2	Local Network	Subnet	Select Subnet from Local Network drop-down menu.
	IP Address	192.168.1.0	Head office network
	Netmask	255.255.255.0	
3	Remote Secure Gateway IP (or Hostname)	69.121.1.30	IP address of the branch office router (in WAN side)
4	Remote Network	Subnet	Select Subnet from Remote Network drop-down menu
	IP Address	192.168.0.0	Branch office network
	Netmask	255.255.255.0	
5	Authentication	MD5	Security plan
	Encryption	3DES	
	Prefer Forward Security	None	
	Pre-shared Key	12345	

Configuring IPSec VPN in the Branch Office



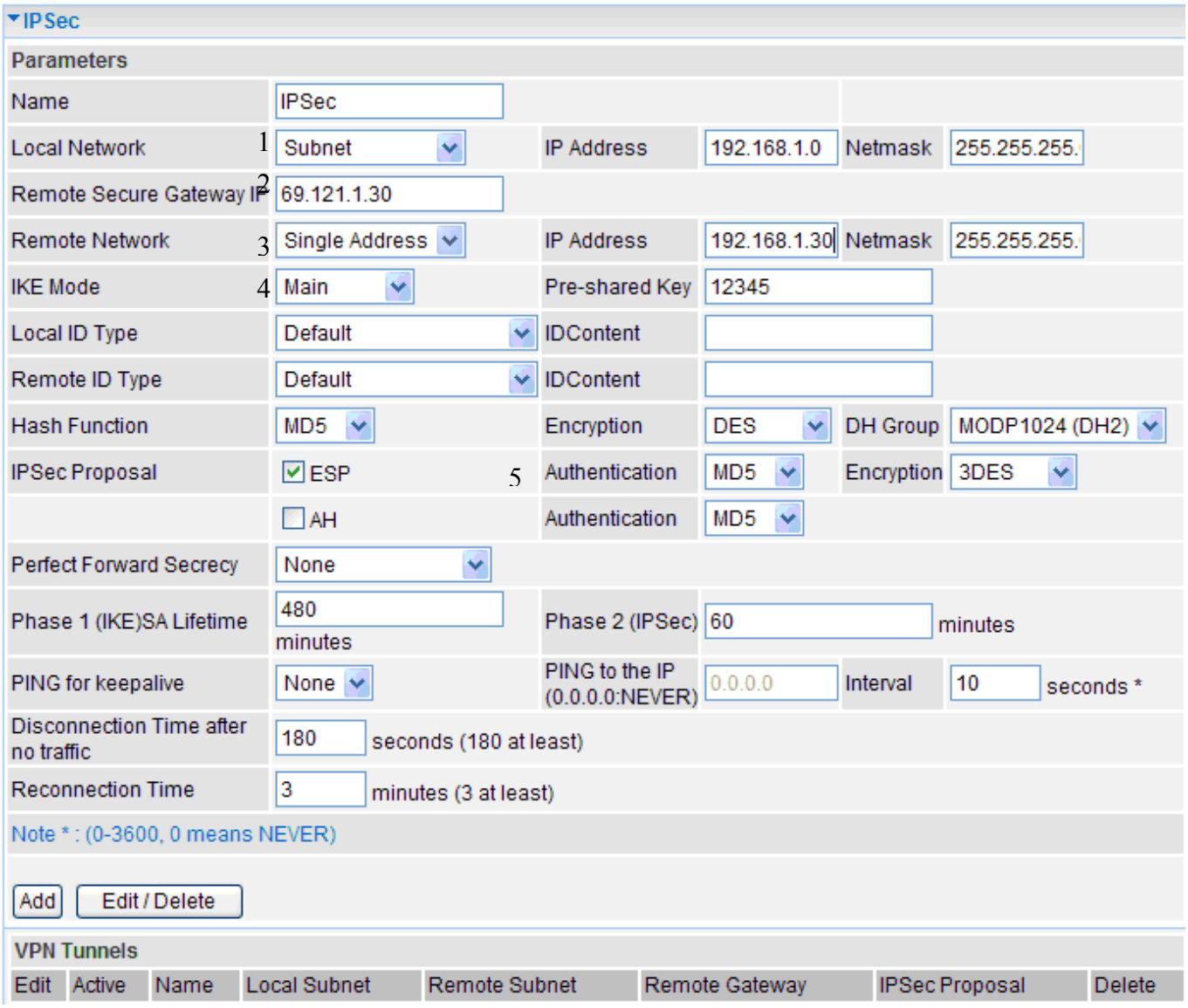
Item	Function		Description
1	Name	IPSec_Branch Office	Given a name of IPSec connection
2	Local Network	Subnet	Select Subnet from Local Network drop-down menu.
	IP Address	192.168.0.0	Branch office network
	Netmask	255.255.255.0	
3	Remote Secure Gateway IP (or Hostname)	69.121.1.3	IP address of the head office router (in WAN side)
4	Remote Network	Subnet	Select Subnet from Remote Network drop-down menu
	IP Address	192.168.1.0	Head office network
	Netmask	255.255.255.0	
5	Authentication	MD5	Security plan
	Encryption	3DES	
	Prefer Forward Security	None	
	Pre-shared Key	12345	

Example: Configuring a IPSec Host-to-LAN VPN Connection



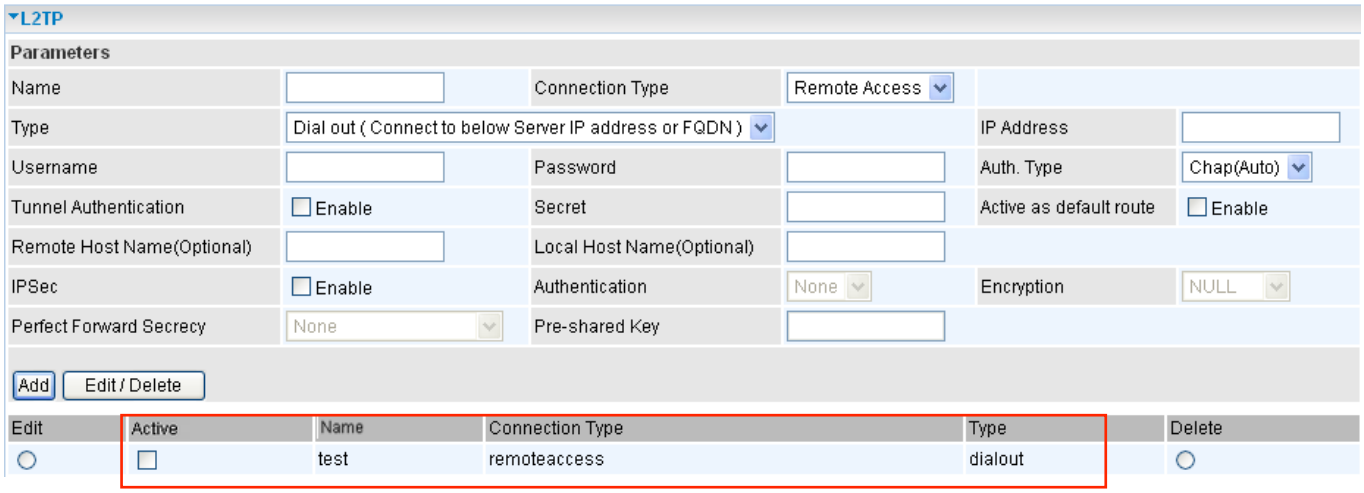
IPSec VPN-Host to LAN

Configuring IPSec VPN in the Office



Item	Function		Description
1	Name	IPSec	Given a name of IPSec connection
2	Local Network	Subnet	Select Subnet from Network drop-down menu
	IP Address	192.168.1.0	Head office network
	Netmask	255.255.255.0	
3	Remote Secure Gateway IP (or Hostname)	69.121.1.30	Remote worker's IP address
4	Remote Network	Single Address	Select Single Address from Remote Network drop-down menu
	IP Address	69.121.1.30	Remote worker's IP address
5	Authentication	MD5	Security plan
	Encryption	3DES	
	Prefer Forward Security	None	
	Pre-shared Key	12345	

5.3.5.3 L2TP (Layer Two Tunneling Protocol)



Two types of L2TP VPN are supported **Remote Access** and **LAN-to-LAN** (please refer below for more information.). Fill in the blank with information you need and click **Add** to create a new VPN connection account.

Active: This function activates or deactivates the L2TP connection. Check Active checkbox if you want the protocol of tunnel to be activated and vice versa.

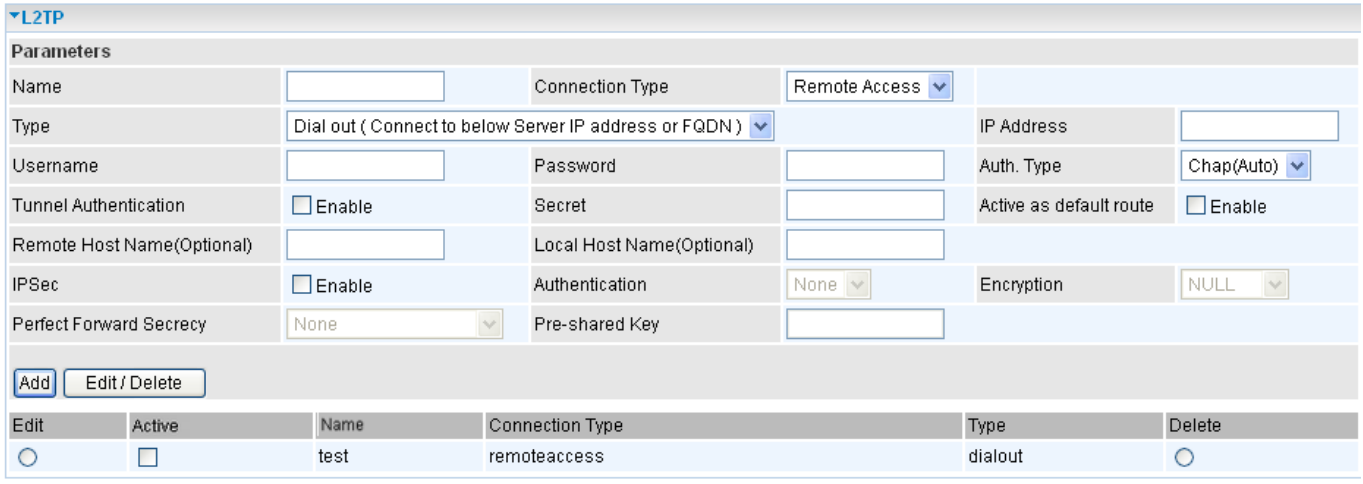
Note: When the Active checkbox is checked, the function of Edit and Delete will not be available.

Name: This is a given name of the connection.

Connection Type: It informs your L2TP tunnel connection condition.

Type: This refers to your router operates as a client or a server, **Dialout** or **Dialin** in respectively.

L2TP Connection - Remote Access



Connection Type: Remote Access or **LAN to LAN.**

Name: A given name for the connection (e.g. "connection to office").

Active: This function activates or deactivates the L2TP connection. Check Active checkbox if you want the protocol of tunnel to be activated and vice versa.

Note: When the Active checkbox is checked, the function of Edit and Delete will not be available.

Type: Check **Dial Out** if you want your router to operate as a client (connecting to a remote VPN server, e.g. your office server), check **Dial In** operates as a VPN server.

- When configuring your router as a Client, enter the remote **Server IP Address (or Hostname)** you wish to connection to.
- When configuring your router as a server, enter the **Private IP Address Assigned to Dial in User** address.

Username: If you are a Dial-Out user (client), enter the username provided by your Host. If you are a Dial-In user (server), enter your own username.

Password: If you are a Dial-Out user (client), enter the password provided by your Host. If you are a Dial-In user (server), enter your own password.

Authentication 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 the client has not been replaced by an intruder.

Tunnel Authentication: This enables router to authenticate both the L2TP remote and L2TP host. This is only valid when L2TP remote supports this feature.

Secret: The secure password length should be 16 characters which may include numbers and characters.

Active as default route: Commonly used by the *Dial-out* connection which all packets will route through the VPN tunnel to the Internet; therefore, active the function may degrade the Internet performance.

Remote Host Name (Optional): Enter hostname of remote VPN device. It is a tunnel identifier from the Remote VPN device matches with the Remote hostname provided. If remote hostname matches, tunnel will be connected; otherwise, it will be dropped.

Cautious: This is only when the router performs as a VPN server. This option should be used by advanced users only.

Local Host Name (Optional): Enter hostname of Local VPN device that is connected / establishes a VPN tunnel. As default, Router's default Hostname is **home.gateway.**

IPSec: Enable for enhancing your L2TP VPN security.

Authentication: Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmit. There are three options, Message Digest 5 (**MD5**), Secure Hash Algorithm (**SHA1**) or **NONE**. SHA1 is more resistant to brute-force attacks than MD5, however it is slower.

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

Encryption: Select the encryption method from the pull-down menu. There are four options, **DES**, **3DES**, **AES** and **NULL**. NULL means it is a tunnel only with no encryption. 3DES and AES are more powerful but increase latency.

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

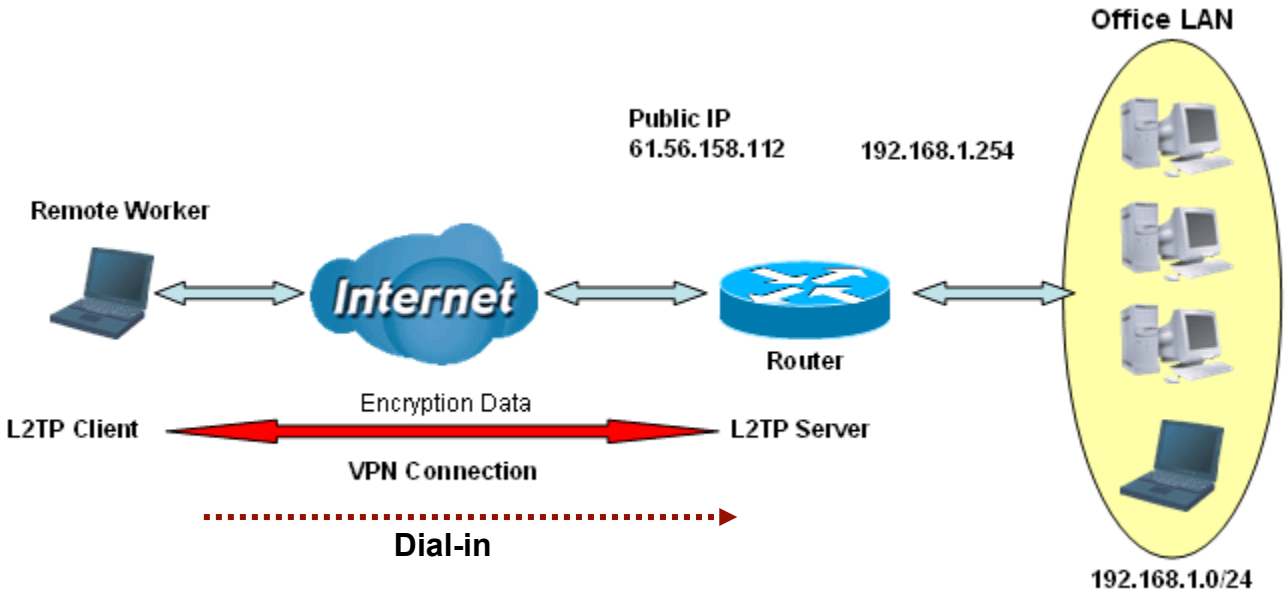
Perfect Forward Secrecy: Choose whether to enable PFS using Diffie-Hellman public-key cryptography to change encryption keys during the second phase of VPN negotiation. This function will provide better security, but extends the VPN negotiation time. Diffie-Hellman is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). There are three modes, MODP 768-bit, MODP 1024-bit and MODP 1536-bit. MODP stands for Modular Exponentiation Groups.

Pre-shared Key: This is for the Internet Key Exchange (IKE) protocol, a string from 4 to 128 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).

Click **Edit/Delete** to save your changes..

Example: Configuring a L2TP VPN - Remote Access Dial-in Connection

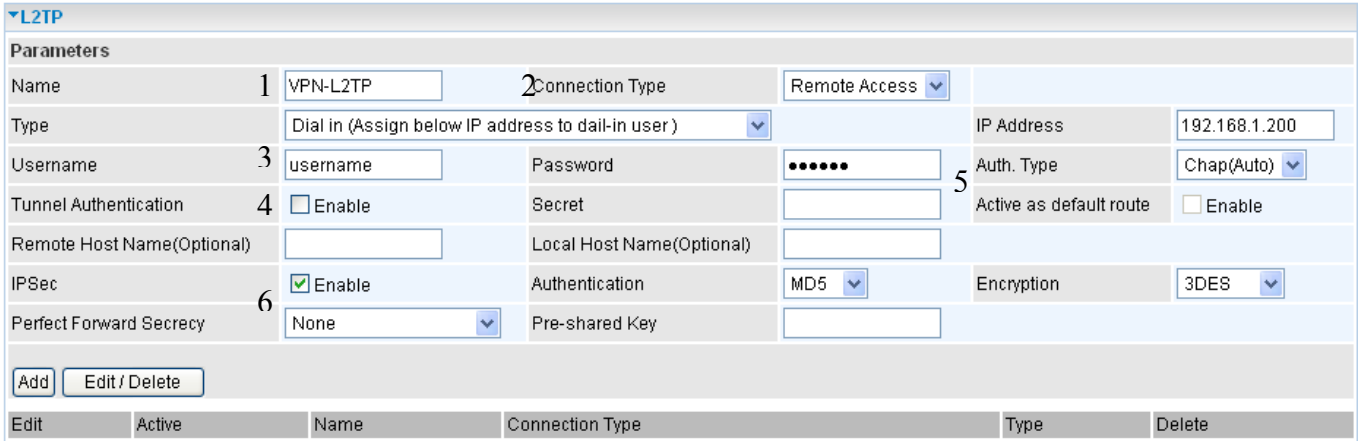
A remote worker establishes a L2TP VPN connection with the head office using Microsoft's VPN Adapter (included with Windows XP/2000/ME, etc.). The router is installed in the head office, connected to a couple of PCs and Servers.



L2TP VPN-Remote Access (Dial-in)

Configuring L2TP VPN in the Office

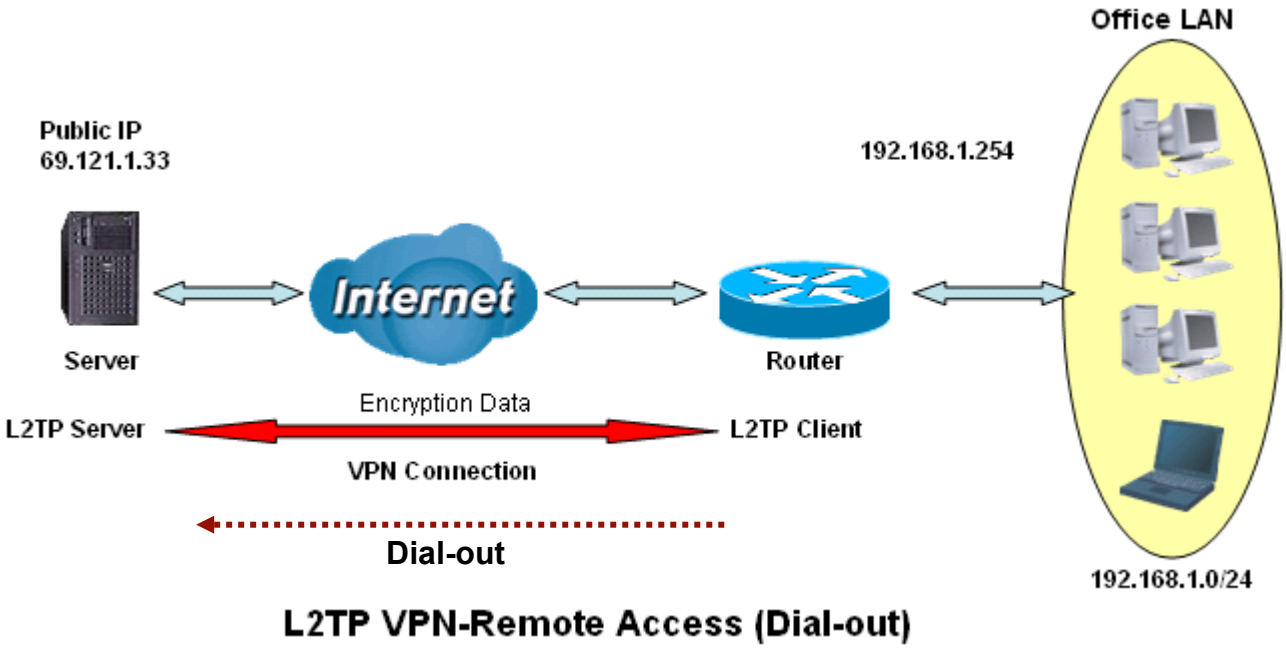
The input IP address 192.168.1.200 will be assigned to the remote worker. Please make sure this IP is not used in the Office LAN.



Item	Function		Description
1	Name	VPN_L2TP	Given a name of L2TP connection
2	Connection Type	Remote Access	Select Remote Access from Connection Type drop-down menu
3	Type	Dial in	Select Dial in from Type drop-down menu
	IP Address	192.168.1.200	An assigned IP address for the remote worker
4	Username	username	Input username & password to authenticate remote worker
	Password	123456	
5	Auth.Type	Chap(Auto)	Keep as default value in most of the cases.
6	IPSec	Enable	Enable for enhancing your L2TP VPN security.
	Authentication	MD5	Both sites should use the same value.
	Encryption	3DES	
	Perfect Forward Secrecy	None	
	Pre-shared Key	12345678	

Example: Configuring a Remote Access L2TP VPN Dial-out Connection

A company's office establishes a L2TP VPN connection with a file server located at a separate location. The router is installed in the office, connected to a couple of PCs and Servers.



L2TP VPN-Remote Access (Dial-out)

Configuring the L2TP VPN in the Office

L2TP

Parameters

Name 1	VPN-L2TP	2 Connection Type	Remote Access		
Type 3	Dial out (Connect to below Server IP address or FQDN)			IP Address	69.121.1.33
Username 4	username	Password	•••••• 5	Auth. Type	Chap(Auto)
Tunnel Authentication	Enable	Secret		Active as default route	Enable
Remote Host Name(Optional)		Local Host Name(Optional)			
IPSec 6	Enable	Authentication	MD5	Encryption	3DES
Perfect Forward Secrecy	None	Pre-shared Key	12345678		

Add | Edit / Delete

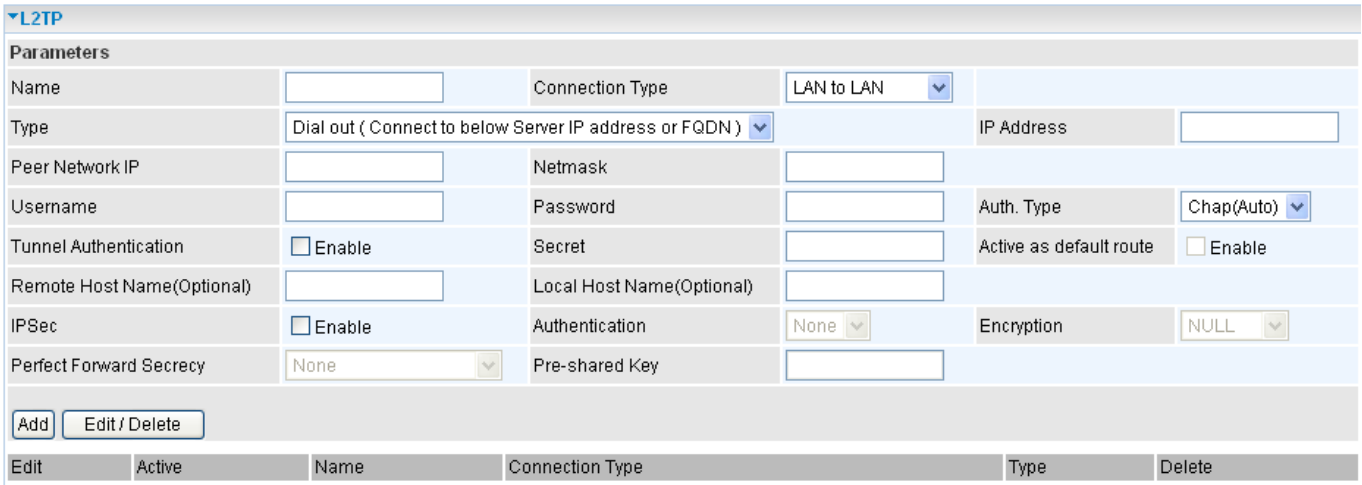
Edit	Active	Name	Connection Type	Type	Delete

Item	Function		Description
1	Name	VPN_L2TP	Given name of L2TP connection
2	Connection Type	Remote Access	Select Remote Access from Connection Type drop-down menu
3	Type	Dial out	Select Dial out from Type drop-down menu
	IP Address (or Hostname)	69.121.1.33	An Dialed server IP
4	Username	username	A given username & password
	Password	123456	
5	Auth.Type	Chap(Auto)	Keep as default value in most of the cases.
6	IPSec	Enable	Enable for enhancing your L2TP VPN security.
	Authentication	MD5	Both sites should use the same value.
	Encryption	3DES	
	Perfect Forward Secrecy	None	
	Pre-shared Key	12345678	

Example: Configuring your Router to Dial-in to the Server

Currently, Microsoft Windows operation system does not support L2TP incoming service. Additional software may be required to set up your L2TP incoming service.

L2TP Connection - LAN to LAN



L2TP VPN Connection

Name: A given name of the connection.

Connection Type: Remote Access or **LAN to LAN.**

Active: This function activates or deactivates the L2TP connection. Check Active checkbox if you want the protocol of tunnel to be activated and vice versa.

Note: When the Active checkbox is checked, the function of Edit and Delete will not be available.

Type: Check **Dial Out** if you want your router to operate as a client (connecting to a remote VPN server, e.g. your office server), check **Dial In** operates as a VPN server.

- When configuring your router establish the connection to a remote LAN, enter the remote **Server IP Address (or Hostname)** you wish to connection to.
- When configuring your router as a server to accept incoming connections, enter the **Private IP Address Assigned to Dial in User** address.

Peer Network IP: Enter Peer network IP address.

Netmask: Enter the subnet mask of peer network based on the Peer Network IP setting.

Username: If you are a Dial-Out user (client), enter the username provided by your Host. If you are a Dial-In user (server), enter your own username.

Password: If you are a Dial-Out user (client), enter the password provided by your Host. If you are a Dial-In user (server), enter your own password.

Authentication 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 the client has not been replaced by an intruder.

Tunnel Authentication: This enables router to authenticate both the L2TP remote and L2TP host. This is only valid when L2TP remote supports this feature.

Secret: The secure password length should be 16 characters which may include numbers and characters.

Active as default route: As the connection type is LAN to LAN, this function will become to disable.

Remote Host Name (Optional): Enter hostname of remote VPN device. It is a tunnel identifier from the Remote VPN device matches with the Remote hostname provided. If remote hostname matches, tunnel will be connected; otherwise, it will be dropped.

Cautious: This is only when the router performs as a VPN server. This option should be used by advanced users only.

Local Host Name (Optional): Enter hostname of Local VPN device that is connected / establishes a VPN tunnel. As default, Router's default Hostname is **home.gateway.**

IPSec: Enable for enhancing your L2TP VPN security.

Authentication: Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmit. There are three options, Message Digest 5 (**MD5**), Secure Hash Algorithm (**SHA1**) or **NONE**. SHA-1 is more resistant to brute-force attacks than MD5, however it is slower.

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

Encryption: Select the encryption method from the pull-down menu. There are four options, **DES**, **3DES**, **AES** and **NULL**. NULL means it is a tunnel only with no encryption. 3DES and AES are more powerful but increase latency.

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

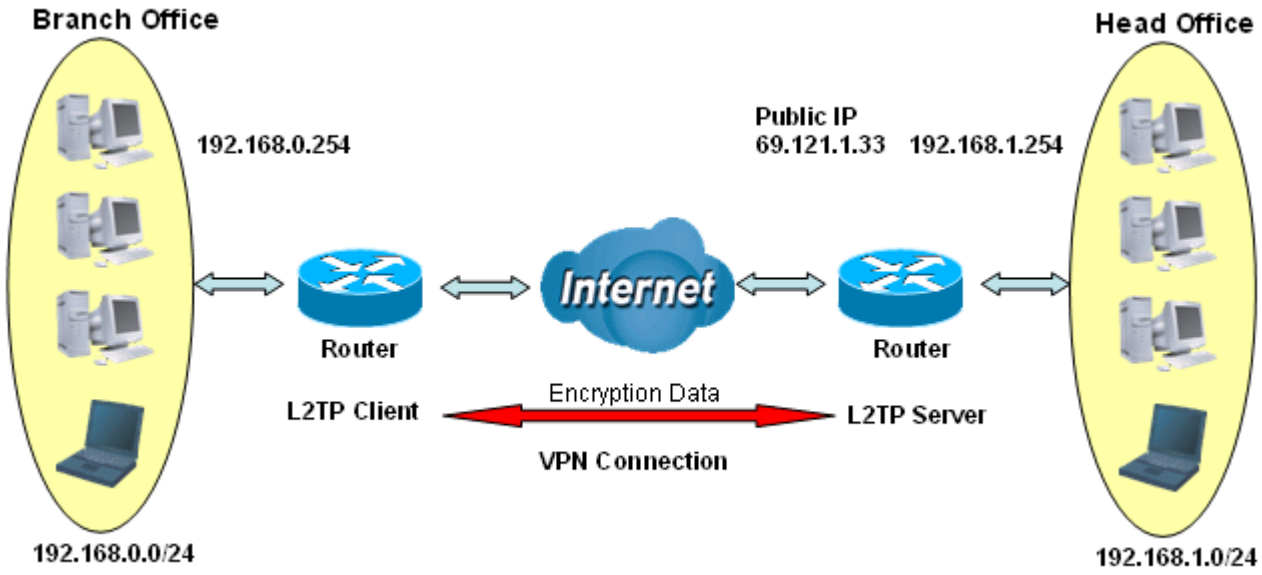
Perfect Forward Secrecy: Choose whether to enable PFS using Diffie-Hellman public-key cryptography to change encryption keys during the second phase of VPN negotiation. This function will provide better security, but extends the VPN negotiation time. Diffie-Hellman is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). There are three modes, MODP 768-bit, MODP 1024-bit and MODP 1536-bit. MODP stands for Modular Exponentiation Groups.

Pre-shared Key: This is for the Internet Key Exchange (IKE) protocol, a string from 4 to 128 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).

Click **Edit/Delete** to save your changes.

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.



L2TP VPN-LAN to LAN

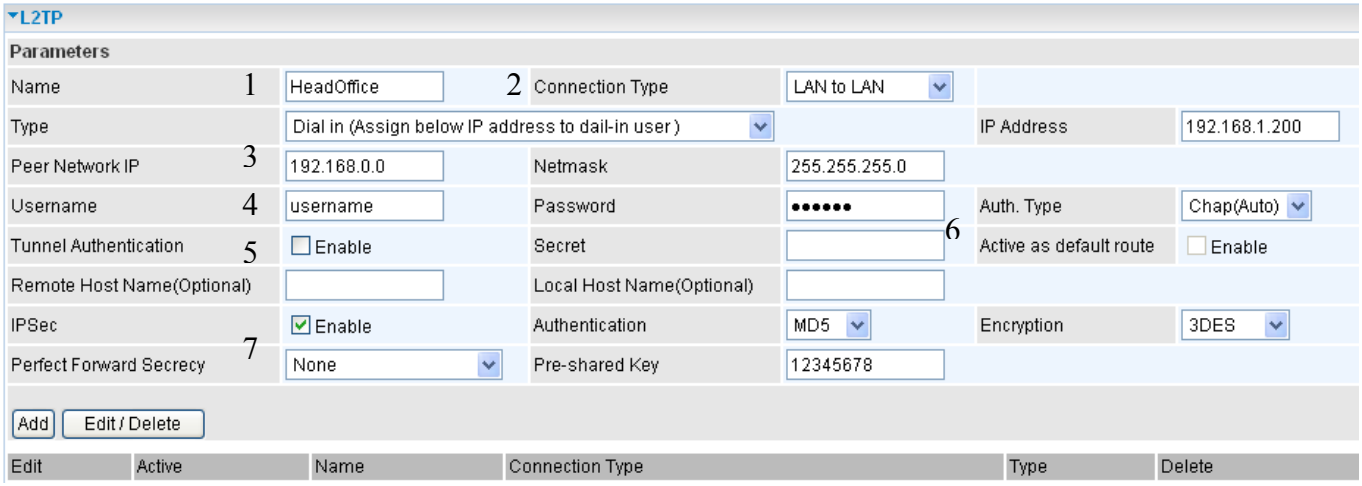
Attention

Both office LAN networks **MUST in different subnet** with LAN to LAN application.

Functions of **Pre-shared Key, VPN Connection Type and Security Algorithm MUST BE** identically set up on both sides.

Configuring L2TP VPN in the Head Office

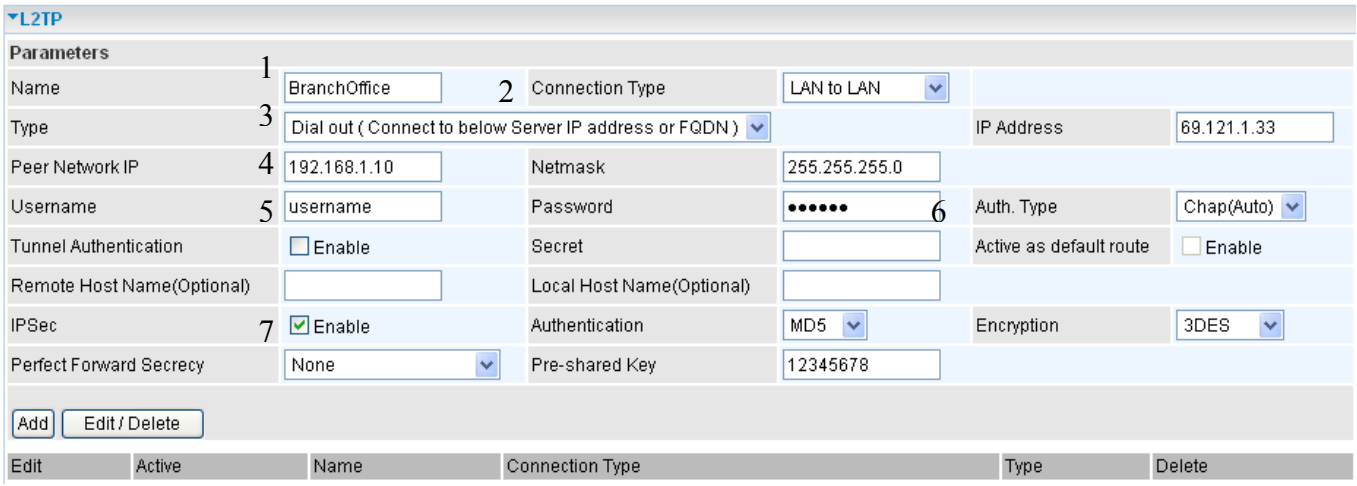
The IP address 192.168.1.200 will be assigned to the router located in the branch office. Please make sure this IP is not used in the head office LAN.



Item	Function		Description
1	Name	HeadOffice	Given a name of L2TP connection
2	Connection Type	LAN to LAN	Select LAN to LAN from Connection Type drop-down menu
3	Type	Dial in	Select Dial in from Type drop-down menu
	IP Address	192.168.1.200	IP address assigned to branch office network
4	Peer Network IP	192.168.0.0	Branch office network
	Netmask	255.255.255.0	
5	Username	username	Input username & password to authenticate branch office network
	Password	123456	
6	Auth.Type	Chap(Auto)	Keep as default value in most of the cases.
7	IPSec	Enable	Enable for enhancing your L2TP VPN security.
	Authentication	MD5	Both sites should use the same value.
	Encryption	3DES	
	Perfect Forward Secrecy	None	
	Pre-shared Key	12345678	

Configuring L2TP VPN in the Branch Office

The IP address 69.121.1.33 is the **Public IP** address of the router located in head office. If you registered the DDNS (please refer to the **DDNS** section of this manual), you can also use the domain name instead of the IP address to reach the router.



Item	Function		Description
1	Name	BranchOffice	Given a name of L2TP connection
2	Connection Type	LAN to LAN	Select LAN to LAN from drop-down menu
3	Type	Dial out	Select Dial out from drop-down menu
	IP Address (or Hostname)	69.121.1.33	IP address of the head office router (in WAN side)
4	Peer Network IP	192.168.1.0	Head office network
	Netmask	255.255.255.0	
5	Username	username	Input username & password to authenticate head office network
	Password	123456	
6	Auth.Type	Chap(Auto)	Keep as default value in most of the cases.
7	IPSec	Enable	Enable for enhancing your L2TP VPN security.
	Authentication	MD5	Both sites should use the same value.
	Encryption	3DES	
	Perfect Forward Secrecy	None	
	Pre-shared Key	12345678	