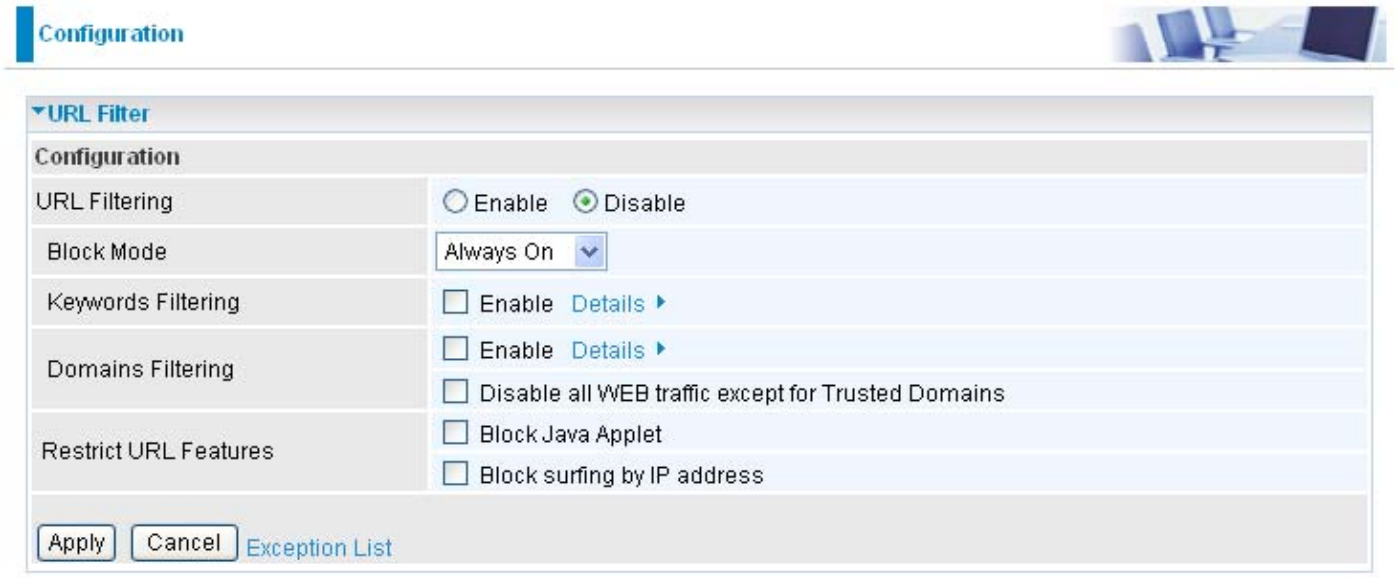
URL Filter

URL (Uniform Resource Locator – e.g. an address in the form of http://www.abcde.com or http://www.example.com) filter rules allow you to prevent users on your network from accessing particular websites by their URL. There are no pre-defined URL filter rules; you can add filter rules to meet your requirements.



Enable/Disable: To enable or disable URL Filter feature.

Block Mode: A list of the modes that you can choose to check the URL filter rules. The default is set to **Always On.**

- **Disabled:** No action will be performed by the Block Mode.
- **Always On:** Action is enabled. URL filter rules will be monitoring and checking at all hours of the day.
- **TimeSlot1 ~ TimeSlot16:** It is self-defined time period. You may specify the time period to check the URL filter rules, i.e. during working hours. For setup and detail, refer to **Time Schedule** section.

Keywords Filtering: Allows blocking by specific keywords within a particular URL rather than having to specify a complete URL (e.g. to block any image called “advertisement.gif”). When enabled, your specified keywords list will be checked to see if any keywords are present in URLs accessed to determine if the connection attempt should be blocked. Please note that the URL filter blocks web browser (HTTP) connection attempts using port 80 only.

For example, if the URL is **http://www.abc.com/abcde.html**, it will be dropped as the keyword “abcde” occurs in the URL.

Domains Filtering: This function checks the whole URL not the IP address, in URLs accessed against your list of domains to block or allow. If it is matched, the URL request will be sent (Trusted) or dropped (Forbidden). For this function to be activated, both check-boxes must be checked. Here is the checking procedure:

1. Check the domain in the URL to determine if it is in the trusted list. If yes, the connection attempt is sent to the remote web server.
2. If not, check if it is listed in the forbidden list. If yes, then the connection attempt will be dropped.
3. If the packet does not match either of the above two items, it is sent to the remote web server.
4. Please be note that the completed URL, “www” + domain name shall be specified. For example to block traffic to **www.google.com.au**, enter “**www.google**” or “**www.google.com**”

In the example below, the URL request for **www.abc.com** will be sent to the remote web server because it is listed in the trusted list, whilst the URL request for **www.google** or **www.google.com** will be dropped, because **www.google** is in the forbidden list.

Example:

Andy wishes to disable all WEB traffic except for ones listed in the trusted domain, which would prevent Bobby from accessing other web sites. Andy selects both functions in the Domain Filtering and thinks that it will stop Bobby. But Bobby knows this function, Domain Filtering, ONLY disables all WEB traffic except for Trusted Domain, BUT not its IP address. If this is the situation, Block surfing by IP address function can be handy and helpful to Andy. Now, Andy can prevent Bobby from accessing other sites.

Restrict URL Features: This function enhances the restriction to your URL rules.

- **Block Java Applet:** This function can block Web content that includes the Java Applet. It is to prevent someone who wants to damage your system via standard HTTP protocol.

- **Block surfing by IP address:** Preventing someone who uses the IP address as URL for skipping Domains Filtering function. Activates only and if Domain Filtering enabled.

IM / P2P Blocking

IM, short for Instant Message, is required to use client program software that allows users to communicate, in exchanging text message, with other IM users in real time over the Internet. A P2P application, known as Peer-to-peer, is group of computer users who share file to specific groups of people across the Internet. Both Instant Message and Peer-to-peer applications make communication faster and easier but your network can become increasingly insecure at the same time. Billion's IM and P2P blocking helps users to restrict LAN PCs to access to the commonly used IM, Yahoo and MSN, and P2P, BitTorrent and eDonkey, applications over the Internet.

Instant Message Blocking: The default is set to Disabled.

- **Disabled:** Instant Message blocking is not triggered. No action will be performed.
- **Always On:** Action is enabled.
- **TimeSlot1 ~ TimeSlot16:** This is the self-defined time period. You may specify the time period to trigger the blocking, i.e. during working hours. For setup and detail, refer to **Time Schedule** section.

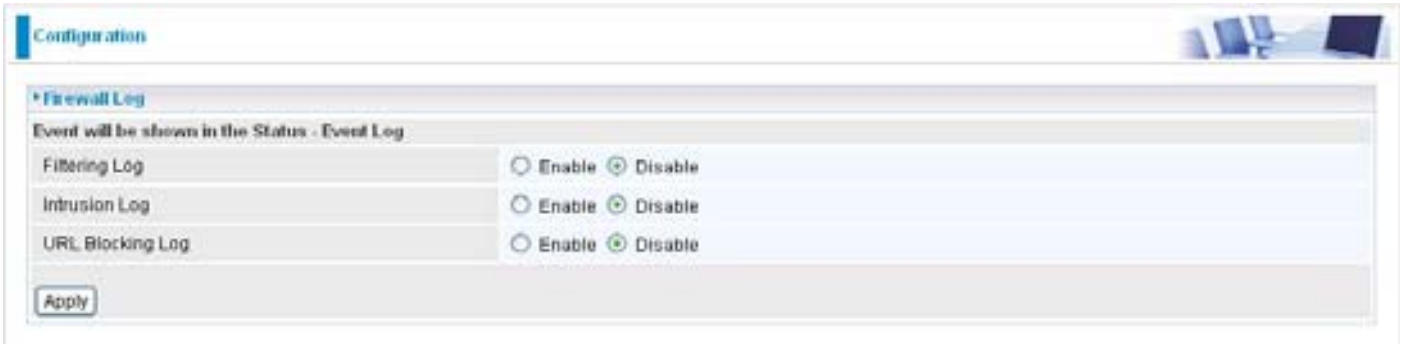
Yahoo/MSN Messenger: Check the box to block either or both Yahoo or/and MSN Messenger. To be sure you enabled the *Instant Message Blocking* first.

- **Peer to Peer Blocking:** The default is set to Disabled.
- **Disabled:** Instant Message blocking is not triggered. No action will be performed.
- **Always On:** Action is enabled.

TimeSlot1 ~ TimeSlot16: This is the self-defined time period. You may specify the time period to trigger the blocking, i.e. during working hours. For setup and detail, refer to Time Schedule section.

BitTorrent / eDonkey: Check the box to block either or both Bit Torrent or/and eDonkey. To be sure you enabled the Peer to Peer Blocking first.

Firewall Log



Firewall Log display log information of any unexpected action with your firewall settings.

Check the Enable box to activate the logs.

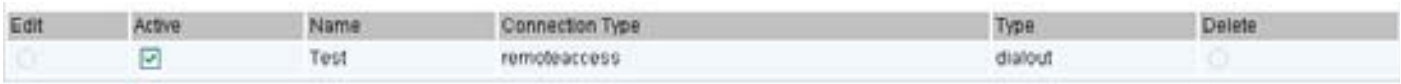
Log information can be seen in the Status – Event Log after enabling.

VPN - Virtual Private Networks *(Only available for BiPAC 7404V(G)OX)*

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**.

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 VPNserver, 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 the Dial in User.

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.

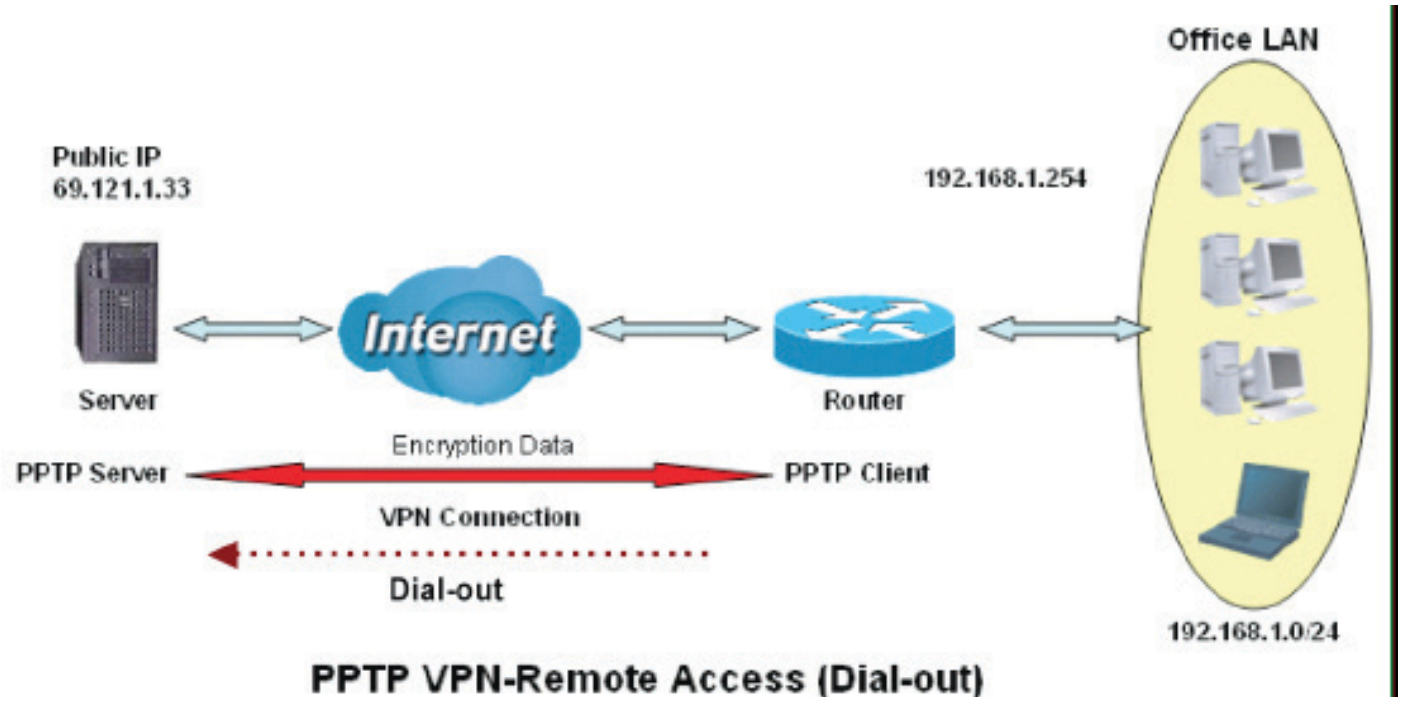
Active: This function activates or deactivates the PPTP connection. Check Active checkbox if you want the protocol of tunnel to be activated and vice versa.

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

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)

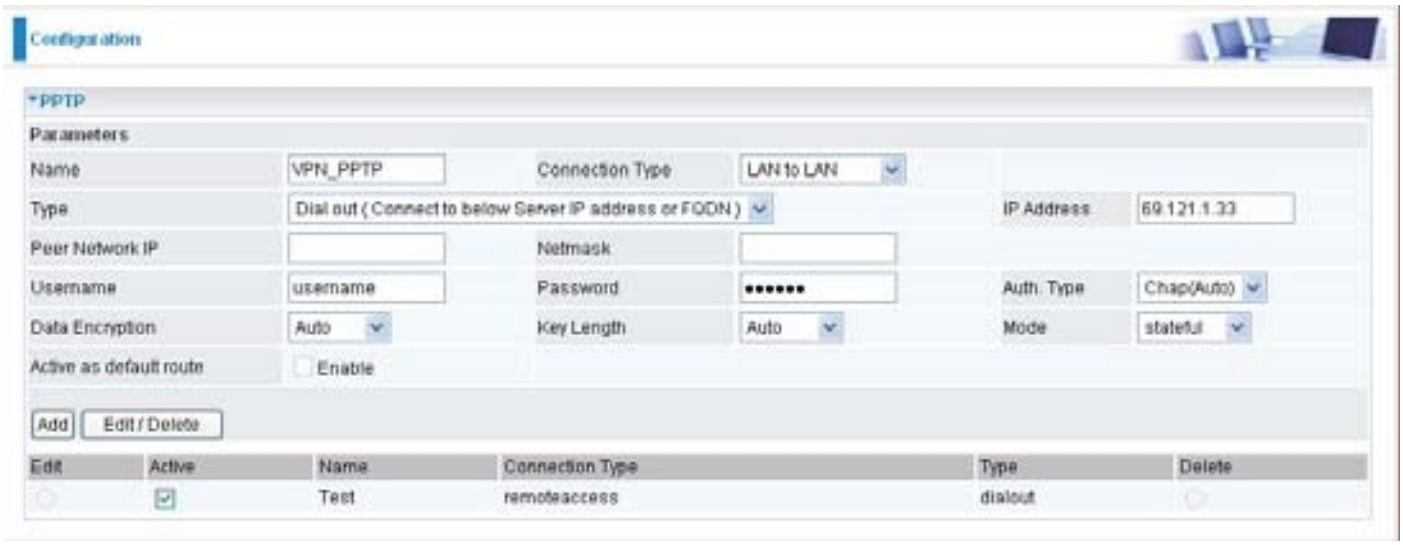
Configuring the PPTP VPN in the Office

Click Configuration/VPN/PPTP. Choose Remote Access from Connect Type drop-down menu. You can either input the IP address (69.1.121.33 in this case) or hostname to reach the server.

Function		Description
Name	VPN_PPTP	Given name of PPTP connection
Connection Type	Remote Access	Select Remote Access from the Connection Type drop-down menu
Type	Dial out	Select Dial out from the Type drop-down menu
IP Address (or Domain name)	69.121.1.33	An Dialed server IP
Username	Username	A given username & password
Password	123456	
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

Click Configuration/VPN/PPTP. Choose LAN to LAN from Connect Type drop-down menu.



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 VPNserver, 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 the Dial in User.

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 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.

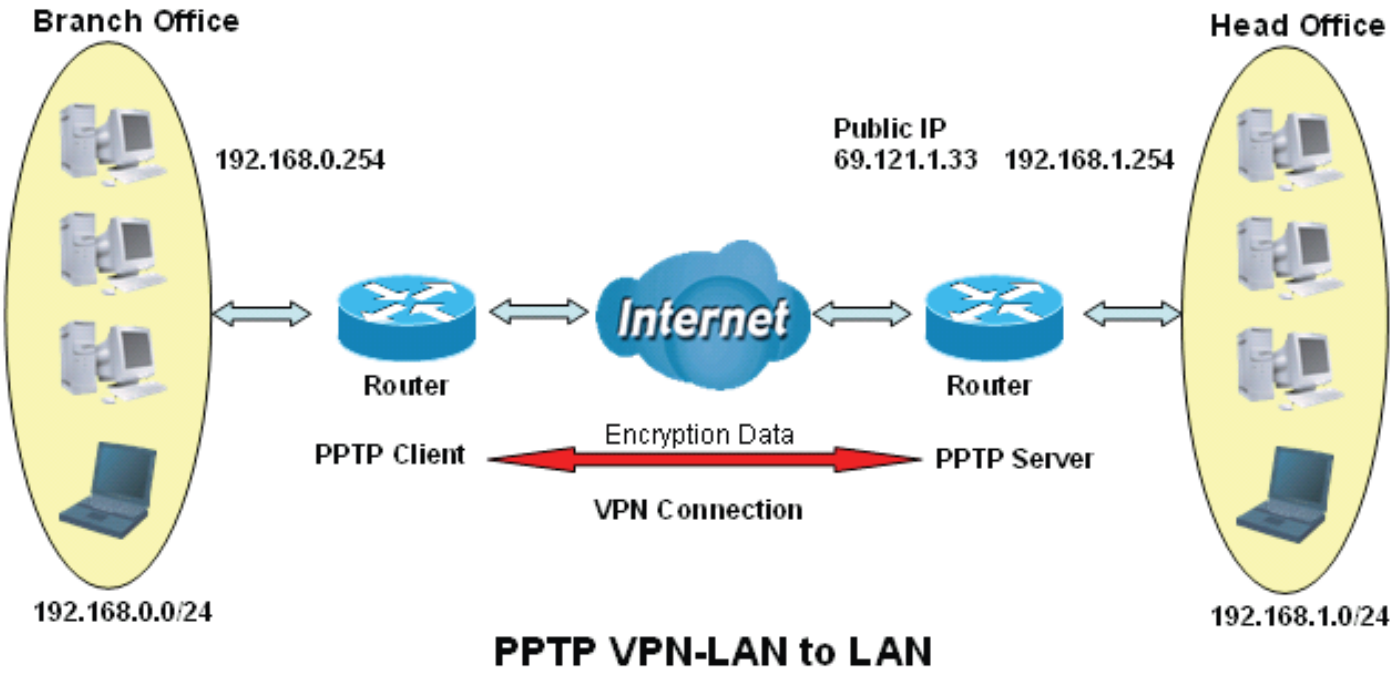
Active: This function activates or deactivates the PPTP connection. Check Active checkbox if you want the protocol of tunnel to be activated and vice versa.

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

Click Edit/Delete button to save your changes.

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



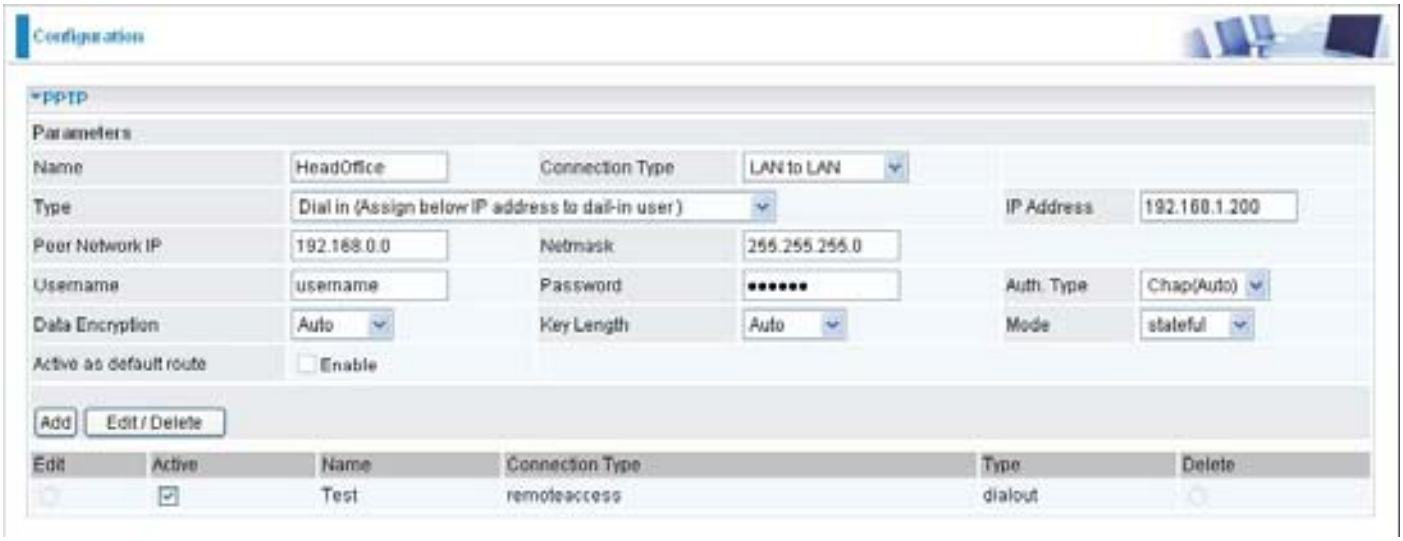
PPTP VPN-LAN to LAN

Attention

Both office LAN networks must be in different subnet with the LAN-LAN application.

Configuring the PPTP VPN in the Head Office

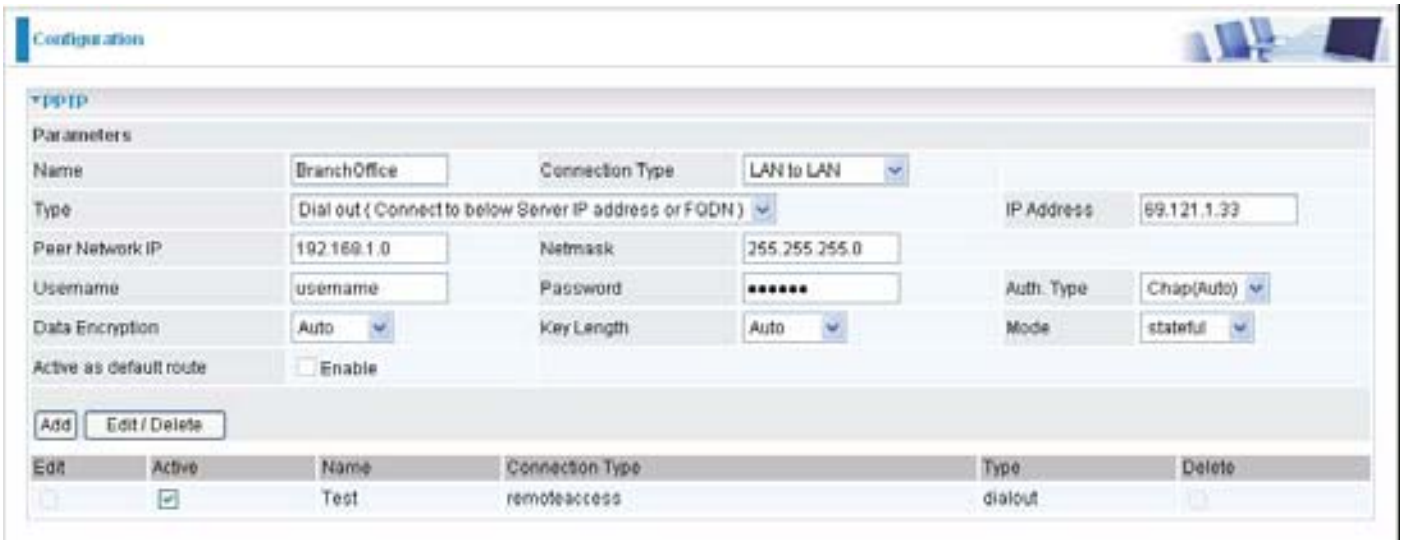
The IP address 192.168.1.201 will be assigned to the router located in the branch office. Please make sure this IP is not used in the head office LAN.



Function		Description
Name	HeadOffice	Given name of PPTP connection
Connection Type	LAN to LAN	Select LAN to LAN from the Connection Type drop-down menu
Type	Dial in	Select Dial in from the Type drop-down menu
IP Address	192.168.1.200	IP address assigned to branch office network.
Peer Network IP	192.168.0.0	Branch office network
Netmask	255.255.255.0	
Username	Username	A given username & password to authenticate branch office network.
Password	123456	
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	

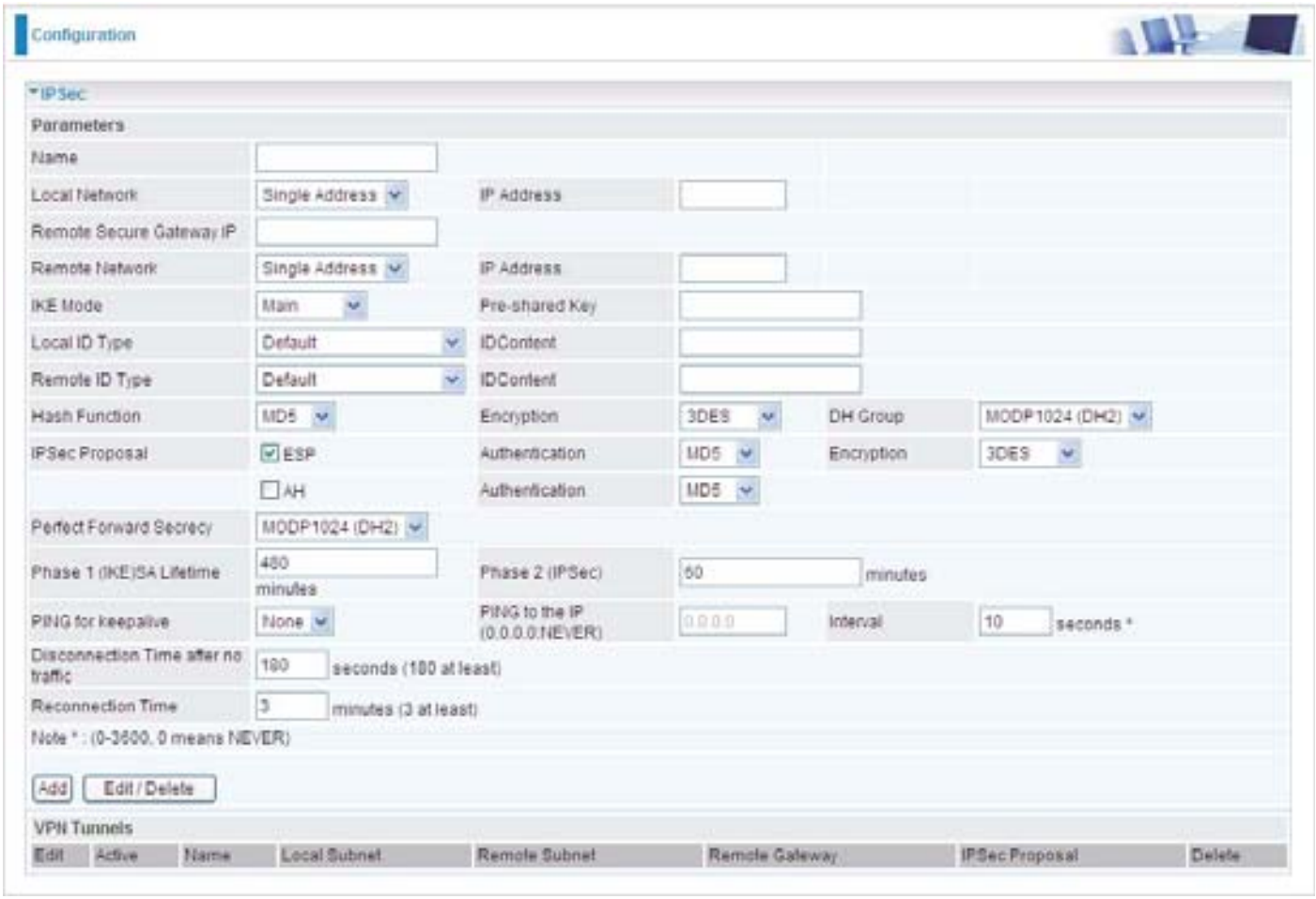
Configuring the PPTP VPN in the Head Office

The IP address 69.1.121.30 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.



Function		Description
Name	HeadOffice	Given name of PPTP connection
Connection Type	LAN to LAN	Select LAN to LAN from the Connection Type drop-down menu
Type	Dial out	Select Dial out from the Type drop-down menu
IP Address (or Domain Name)	69.121.1.33	IP address assigned to branch office network.
Peer Network IP	192.168.1.0	Head office network
Netmask	255.255.255.0	
Username	Username	A given username & password to authenticate branch office network.
Password	123456	
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	

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.

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).

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.

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 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.

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 afther 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. 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.

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 an IPSec LAN to LAN VPN Connection

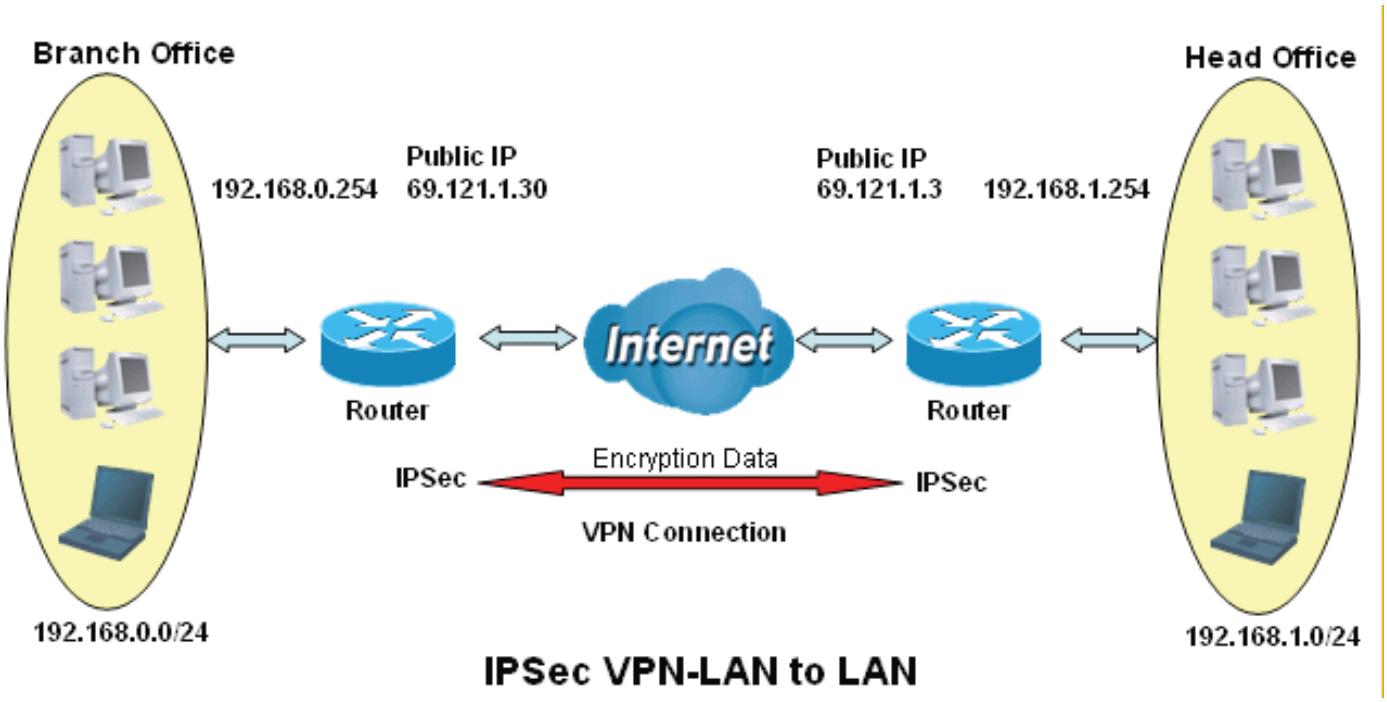


Table 3: Network Configuration and Security Plan

	Branch Office	Head Office
Local Network ID	192.168.0.0/24	192.168.1.0/24
Local Router IP	69.1.121.30	69.1.121.3
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

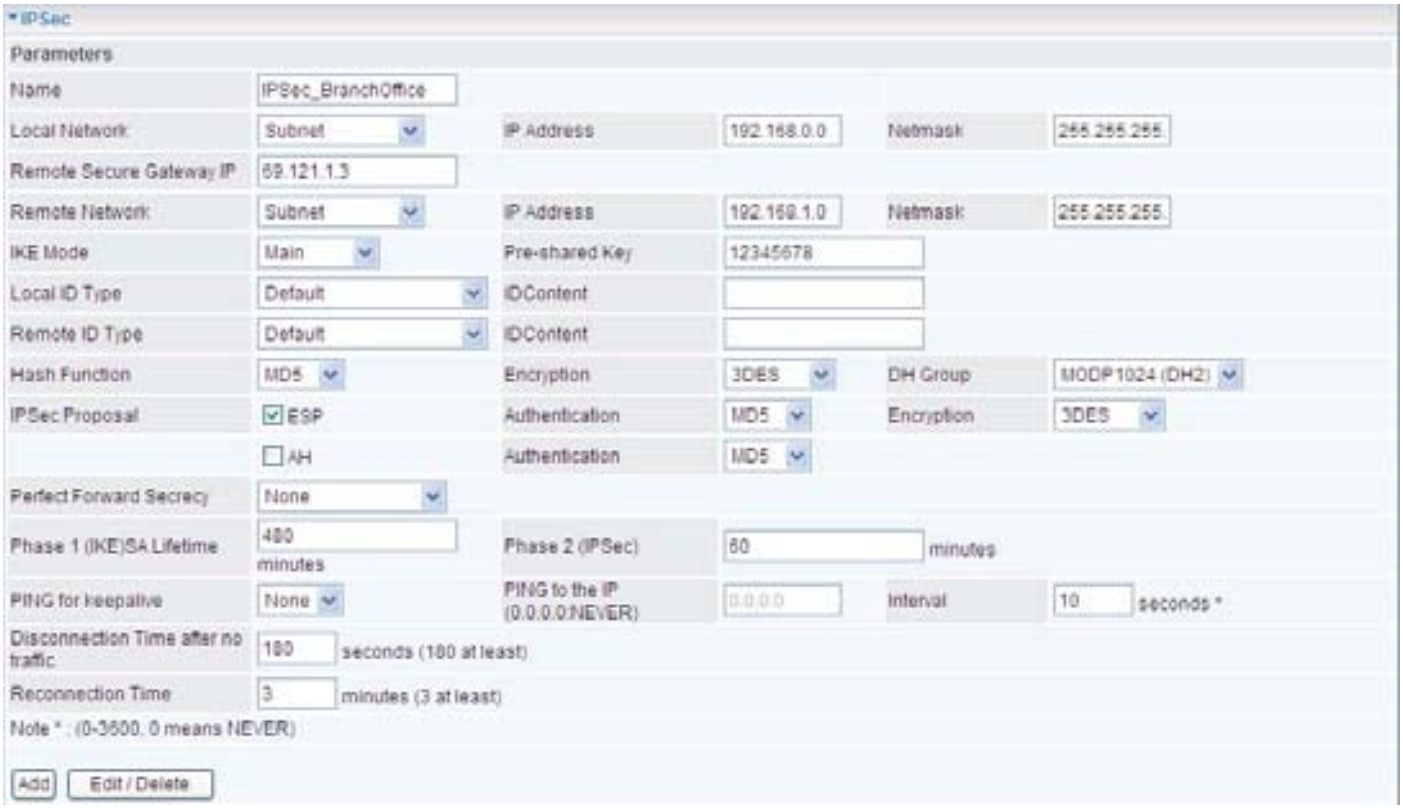
Both office LAN networks must be in different subnet with the LAN-LAN application.

Functions of **Pre-shared keys, VPN Connection Type and Security Algorithm** must be identically setup on both sides.

Configuring IPSec VPN in the Head Office

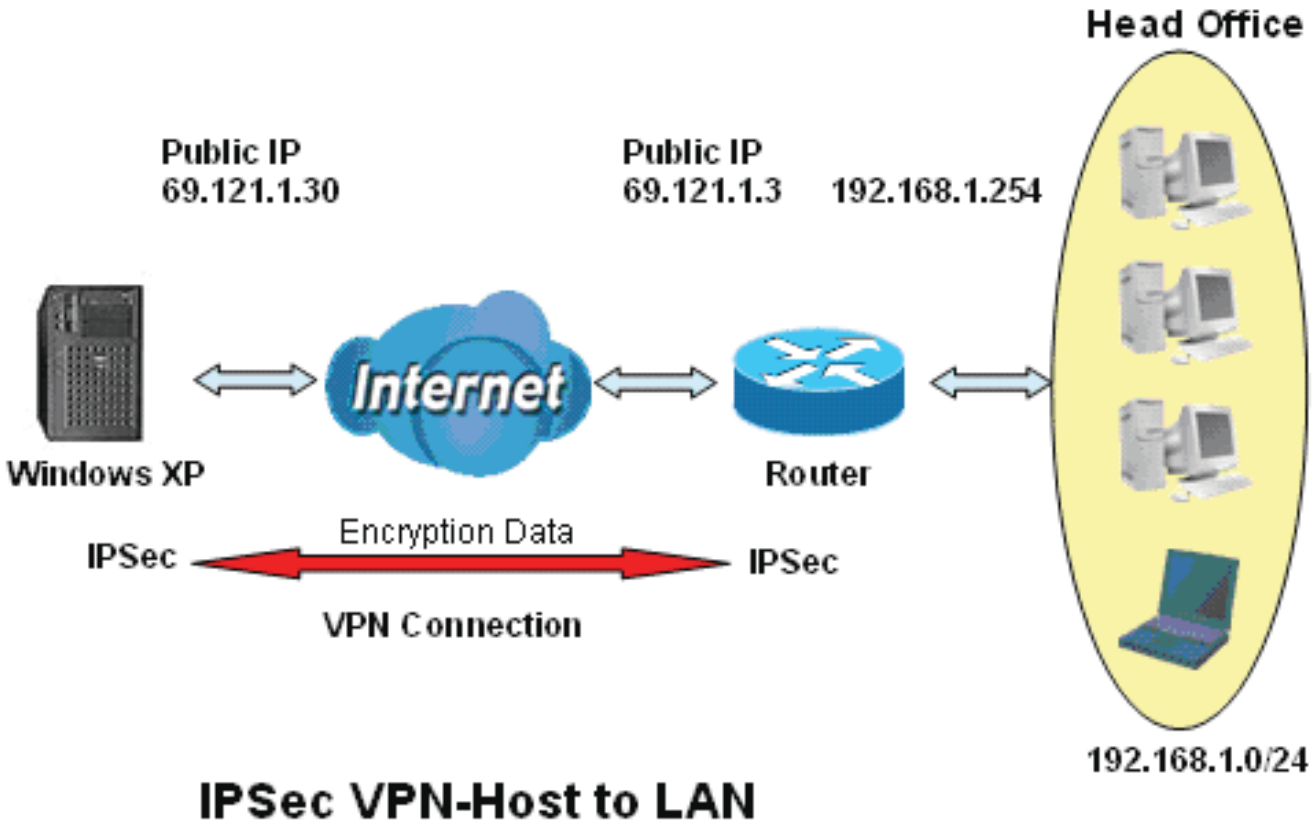
Function		Description
Name	IPSec_HeadOffice	Give a name of IPSec Connection
Local Network	Subnet	Select Subnet from Local Network drop-down menu.
IP Address	192.168.1.0	Head office network
Netmask	255.255.255.0	
Remote Secure Gateway IP (or Hostname)	69.121.1.30	IP address of the head office router (in WAN side)
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	
Pre-shared Key	12345678	Security plan
Authentication	MD5	
Encryption	3DES	
Prefer Forward Security	None	

Configuring IPSec VPN in the Branch Office



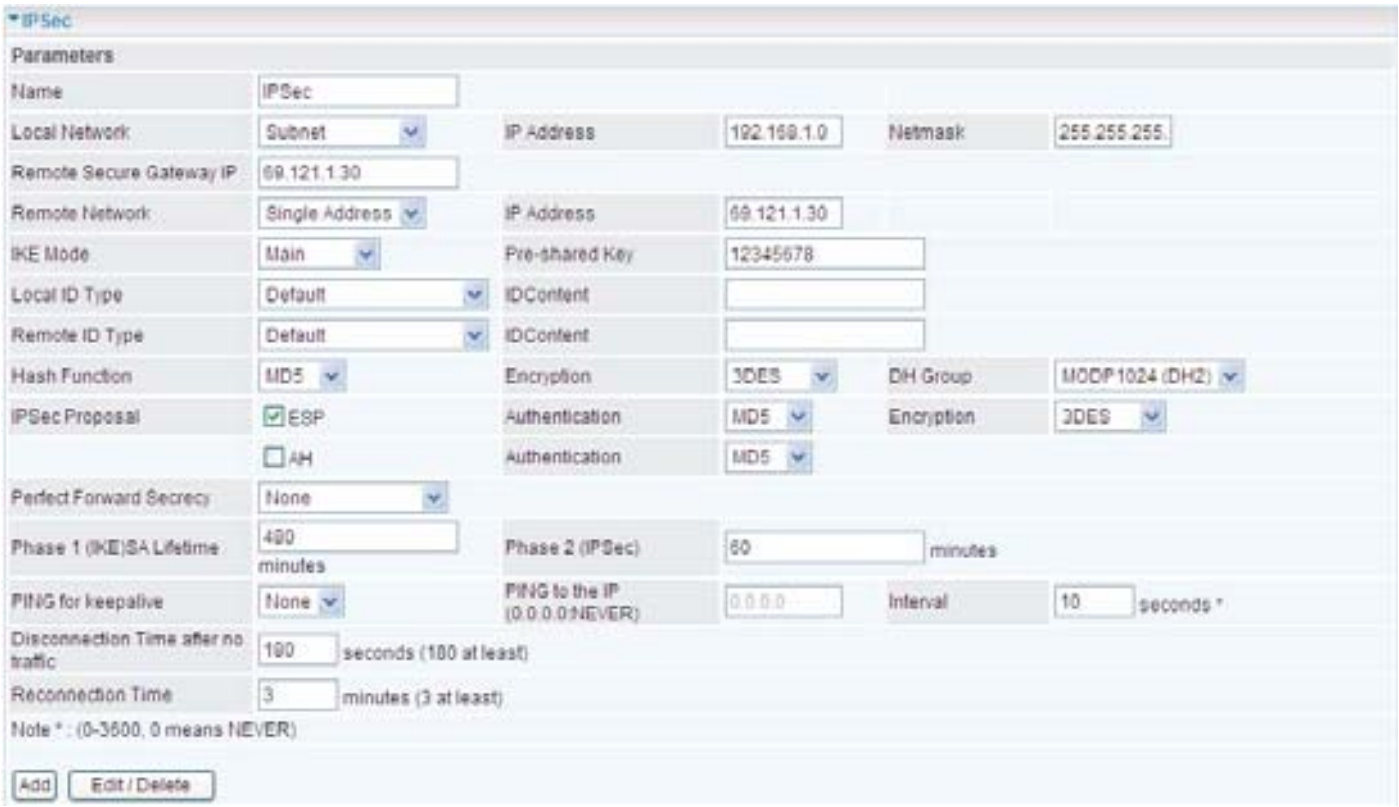
Function		Description
Name	IPSec_BranchOffice	Give a name of IPSec Connection
Local Network	Subnet	Select Subnet from Local Network drop-down menu.
IP Address	192.168.0.0	Branch office network
Netmask	255.255.255.0	
Remote Secure Gateway IP (or Hostname)	69.121.1.3	IP address of the head office router (in WAN side)
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	
Pre-shared Key	12345678	Security plan
Authentication	MD5	
Encryption	3DES	
Prefer Forward Security	None	

Example: Configuring an IPSec Host to LAN VPN Connection



IPSec VPN-Host to LAN

Configuring IPSec VPN in the Office



Function		Description
Name	IPSec	Give a name of IPSec Connection
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	
Remote Secure Gateway IP (or Hostname)	69.121.1.30	IP address of the head office router (in WAN side)
Remote Network	Single Address	Select Single Address from Remote Network drop-down menu
IP Address	69.121.1.30	Remote worker's IP address
Pre-shared Key	12345678	Security plan
Authentication	MD5	
Encryption	3DES	
Prefer Forward Security	None	

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 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.

Name: This is a given name of the connection.

Connection Type: Displays the condition of your L2TP tunneling connection.

Type: This refers to your router whether it operates as a client or a server, Dial-out or Dial-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”).

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 Hostname) you wish to connect to.

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

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.

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.

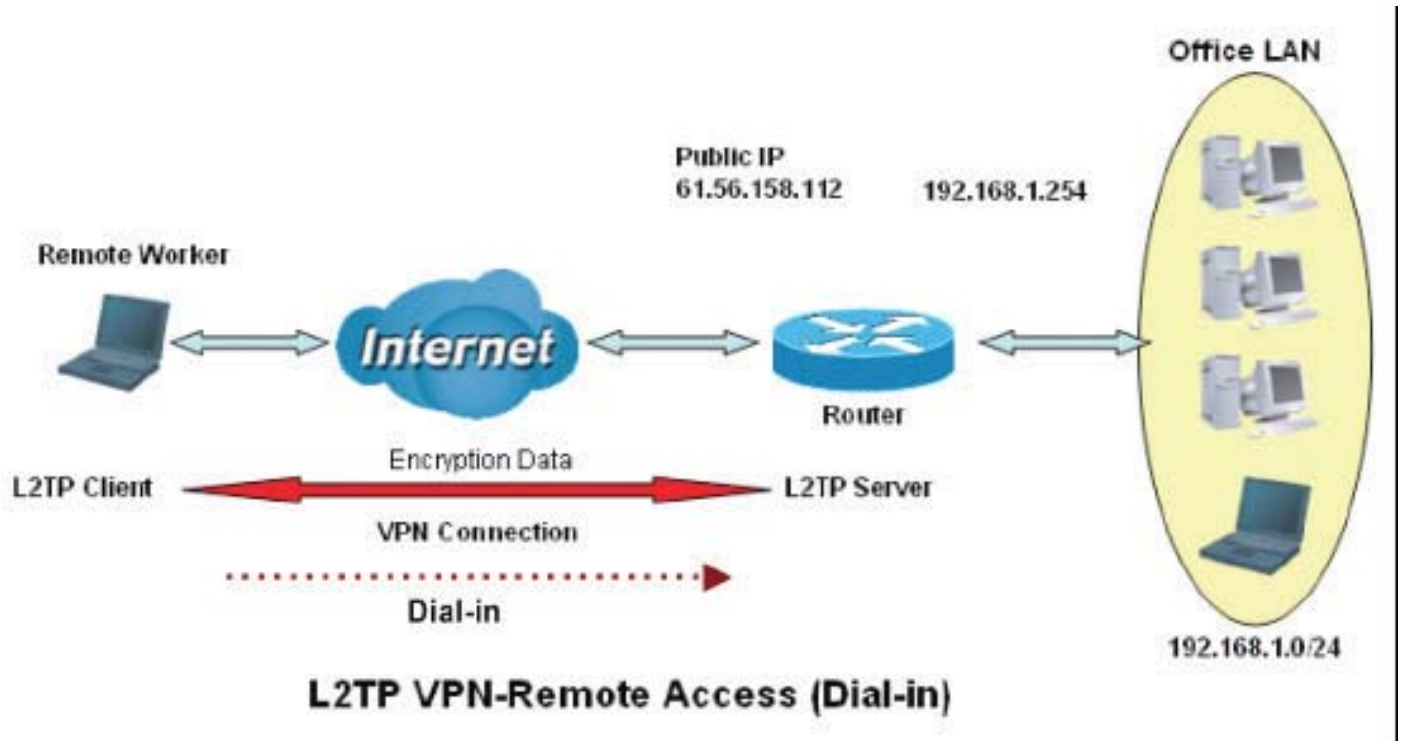
Perfect Forward Secrecy: Choose whether to enable PFS using Diffie-Hellman public-key cryptography to change encryption keys during the second phase of VPN negotiation. This function will provide better security, but extends the VPN negotiation time. Diffie-Hellman is a public-key cryptography protocol 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)

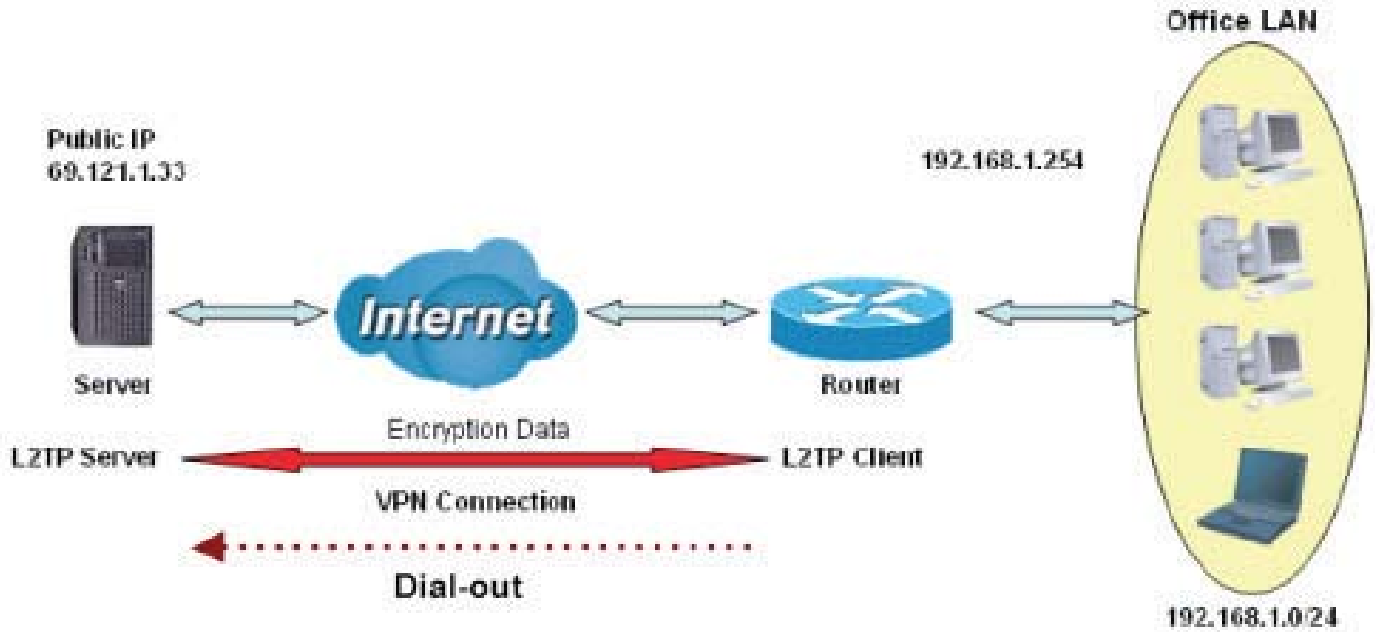
Configuring L2TP VPN in the Office

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.

Function		Description
Name	VPN_L2TP	Give a name of L2TP Connection
Connection Type	Remote Access	Select Remote Access from the Connection Type drop-down menu
Type	Dial in	Select Dial in from the Type drop down menu
IP Address	192.168.1.200	An IP assigned to the remote client
Username	username	Enter the username and password to authenticate a remote client
Password	123456	
Auth. Type	Chap (Auto)	Keep this as the default value for most cases
IPSec	Enable	Enable this to enhance your L2TP VPN security
Authentication	MD5	Both sides 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 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.

Function		Description
Name	VPN_L2TP	Give a name of L2TP Connection
Connection Type	Remote Access	Select Remote Access from the Connection Type drop-down menu
Type	Dial out	Select Dial out from the Type drop down menu
IP Address (or Hostname)	69.121.1.33	A Dialed Server IP
Username	username	An assigned username and password
Password	123456	
Auth. Type	Chap (Auto)	Keep this as the default value for most cases
IPSec	Enable	Enable this to enhance your L2TP VPN security
Authentication	MD5	Both sides 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 for 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 to have it operate as a VPN server.

When configuring your router to establish a connection to a remote LAN, enter the remote Server IP Address (or Hostname) you wish to connect to.

When configuring your router as a server to accept incoming connections, enter the Private IP Address assigned to the Dial in User.

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: 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.

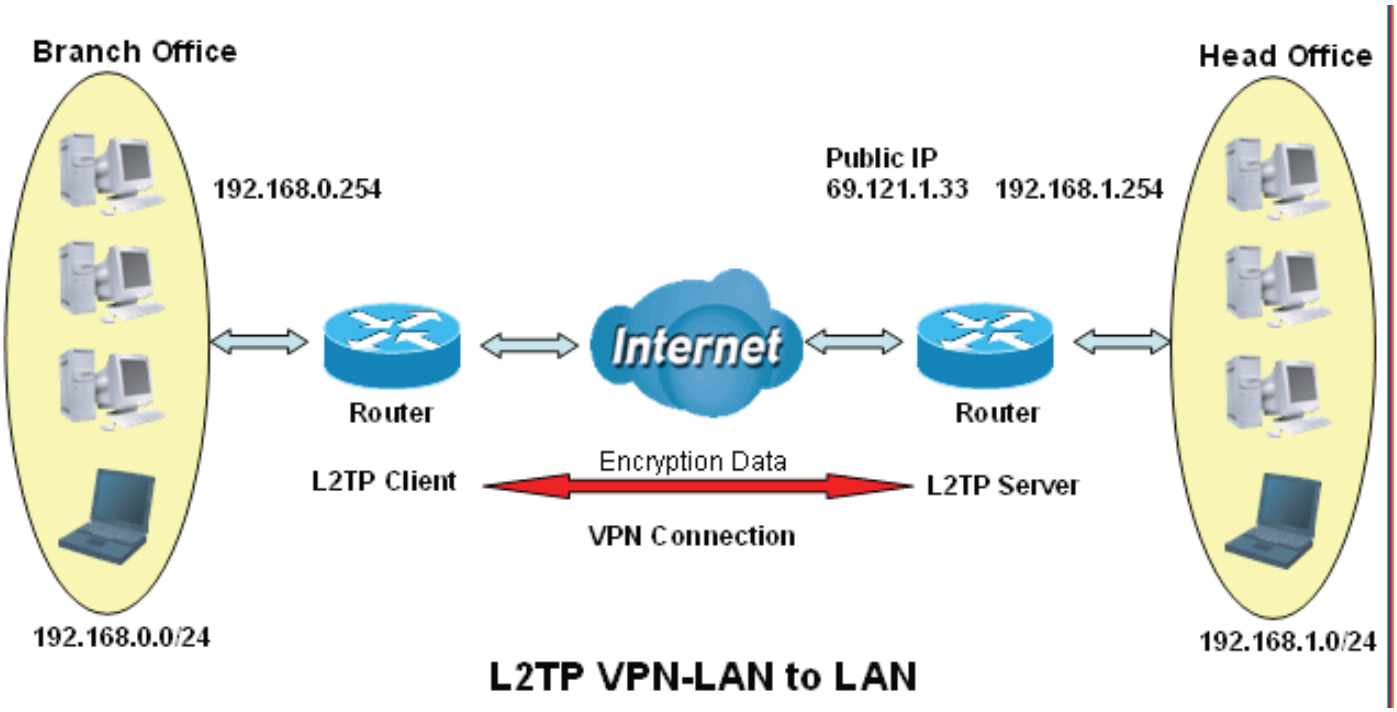
Perfect Forward Secrecy: Choose whether to enable PFS using Diffie-Hellman public-key cryptography to change encryption keys during the second phase of VPN negotiation. This function will provide better security, but extends the VPN negotiation time. Diffie-Hellman is a public-key cryptography protocol 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 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

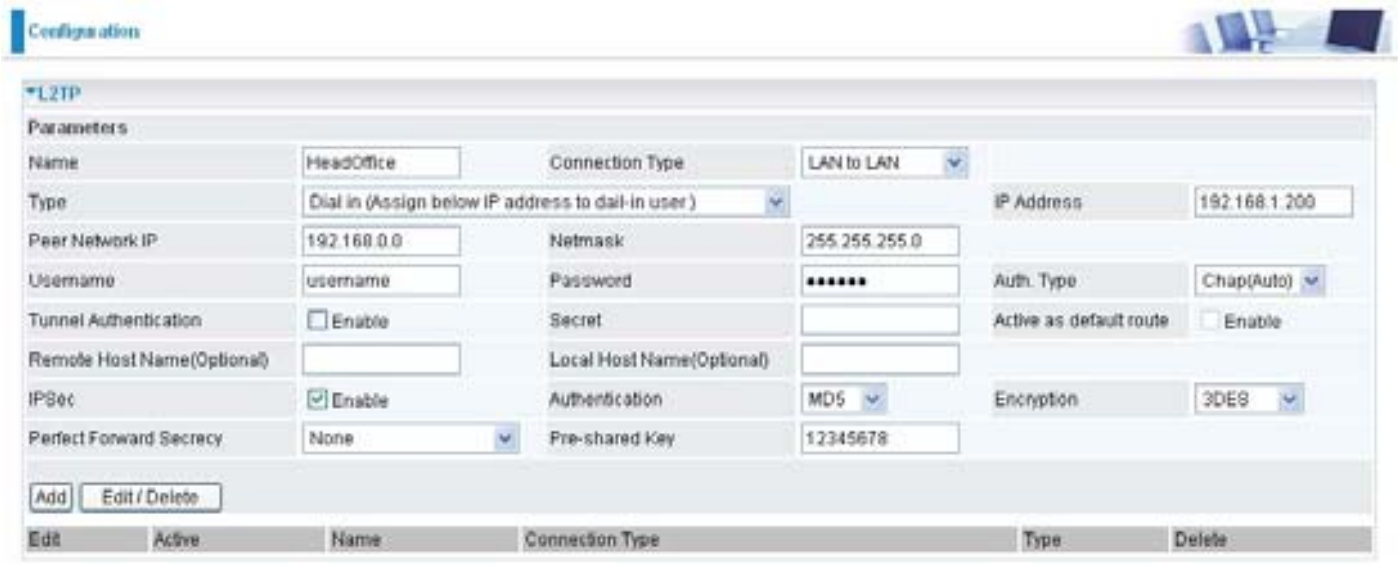
Attention

Both office LAN networks must be in different subnet with the LAN-LAN application.

Functions of **Pre-shared keys, VPN Connection Type and Security Algorithm** must be identically setup 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.



Function		Description
Name	HeadOffice	Give a name of L2TP Connection
Connection Type	LAN to LAN	Select LAN to LAN from the Connection Type drop-down menu
Type	Dial in	Select Dial in from the Type drop down menu
IP Address	192.168.1.200	IP address assigned to branch office network
Peer Network IP	192.168.0.0	Branch office network
Username	username	An assigned username and password to authenticate branch office network
Password	123456	
Auth. Type	Chap (Auto)	Keep this as the default value for most cases
IPSec	Enable	Enable this to enhance your L2TP VPN security
Authentication	MD5	Both sides 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 69.1.121.30 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.

Function		Description
Name	BranchOffice	Give a name of L2TP Connection
Connection Type	LAN to LAN	Select LAN to LAN from the Connection Type drop-down menu
Type	Dial out	Select Dial out from the Type drop down menu
IP Address (or Hostname)	69.121.1.33	IP address assigned to branch office network
Peer Network IP	192.168.1.0	Head office network
Netmask	255.255.255.0	
Username	username	An assigned username and password to authenticate branch office network
Password	123456	
Auth. Type	Chap (Auto)	Keep this as the default value for most cases
IPSec	Enable	Enable this to enhance your L2TP VPN security
Authentication	MD5	Both sides should use the same value
Encryption	3DES	
Perfect Forward Secrecy	None	
Pre-Shared Key	12345678	

VoIP - Voice over Internet Protocol

VoIP enables telephone calls through existing Internet connection instead of going through the PSTN (Public Switched Telephone Network). It is not only cost-effective, especially for a long distance telephone charges, but also toll-quality voice calls over the Internet.

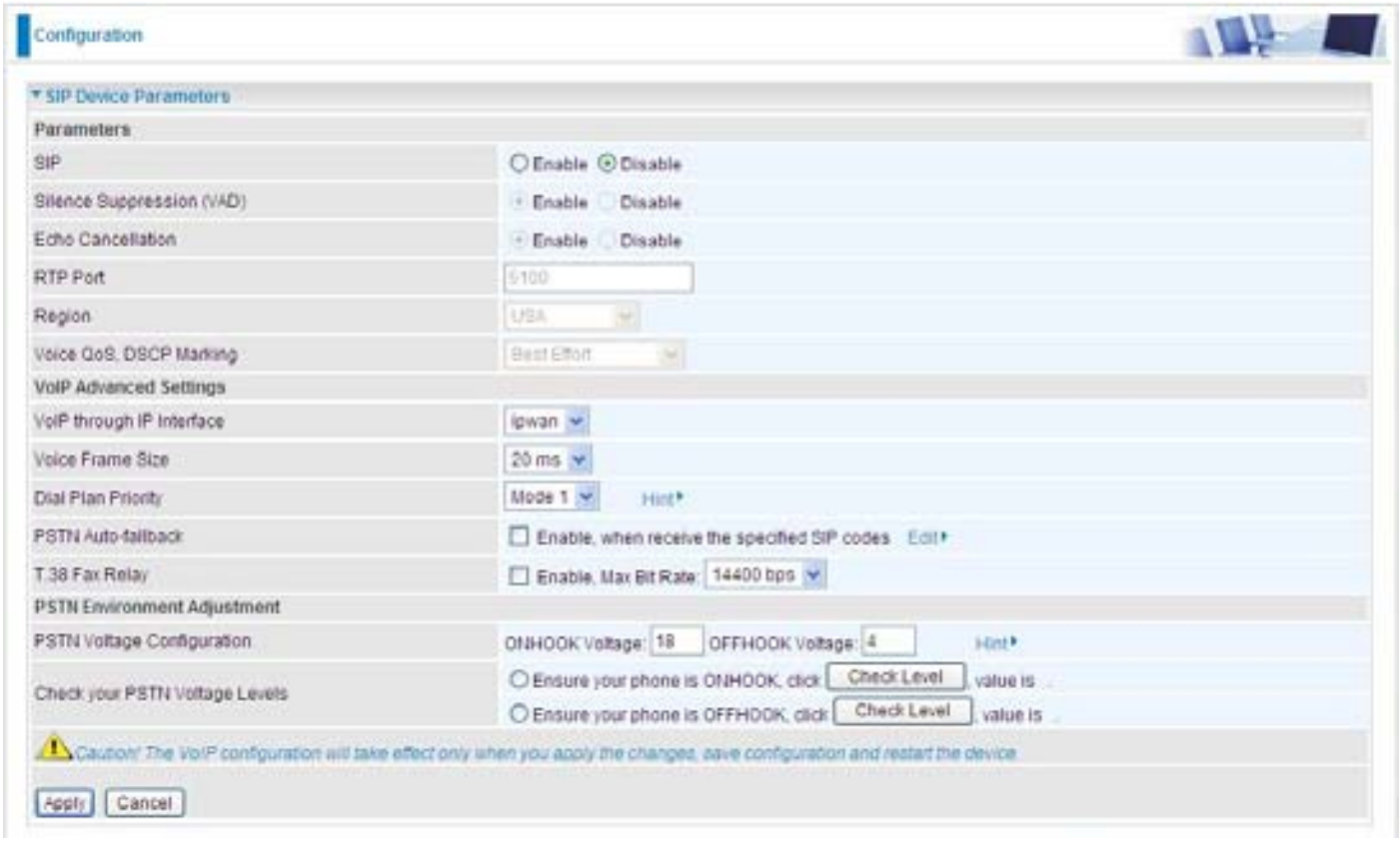
Attention

After completing VoIP configuration, remember to apply the changes. SAVE CONFIG and restart to activate your VoIP.

Here are the items within the VoIP section: **SIP Device Parameters, SIP Accounts, Phone Port, PSTN Dial Plan, VoIP Dial Plan, Call Features, Speed Dial** and **Ring &Tone.**

SIP Device Parameters

This section provides easy setup for your VoIP service. Phone port 1 and 2 can be registered to different SIP Service Provider.



SIP Device Parameters

SIP: To use VoIP SIP as VoIP call signaling protocol. Default is set to Disable.

Silence Suppression (VAD): Voice Activation Detection (VAD) prevents transmitting the nature silence to consume the bandwidth. It is also known as Silence Suppression which is a software application that ensures the bandwidth is reserved only when voice activity is activated. Default is set to Enable.

Echo Cancellation: G.168 echo canceller is an ITU-T standard. It is used for isolating the echo while you are on the phone. This helps you not to hear much of your own voice reflecting on the phone while you talk. Default is set to Enable.

RTP Port: Provide the based value from the media (RTP) ports that are assigned for various endpoints and the different call sessions that may exist within an end-point. (Range from 5100 to 65535, default value is 5100)

Region: This selection is a drop-down box, which allows user to select the country for which the VoIP device must work. When a country is selected, the country parameters are automatically loaded.

Voice QoS, DSCP Marking: Differentiated Services Code Point (DSCP), it is the first 6 bits in the ToS byte. DSCP Marking allows users to assign specific application traffic to be executed in priority by the next Router based on the DSCP value. See Table 4. The DSCP Mapping Table:

Note: To be sure the router(s) in the backbones network have the capability in executing and checking the DSCP through-out the QoS network.

Advanced – Parameters

VoIP through IP Interface: IP Interface decides where to send/receive the voip traffic; it includes: ipwan and iplan. Easy way to select the interface is to check the location of the SIP server. If it locates some where in the Internet then select **ipwan.** If the VoIP SIP server is on the local Network then select **iplan.**

Voice Frame Size: Frame size is available from 10ms to 60ms. Frame size meaning how many milliseconds the Voice packets will be queued and sent out. It is ideal to have the same frame size in both of Caller and Receiver.

Dial Plan Priority: Define the priority between VoIP and PSTN dial plan.

PSTN Auto-fallback: Whenever VoIP SIP responses error and error code matching with the codes in the **Edit** section, the VoiP calls will automatically fallback to PSTN. In the other word, the call will be called via the PSTN when VoIP SIP returns an error code.

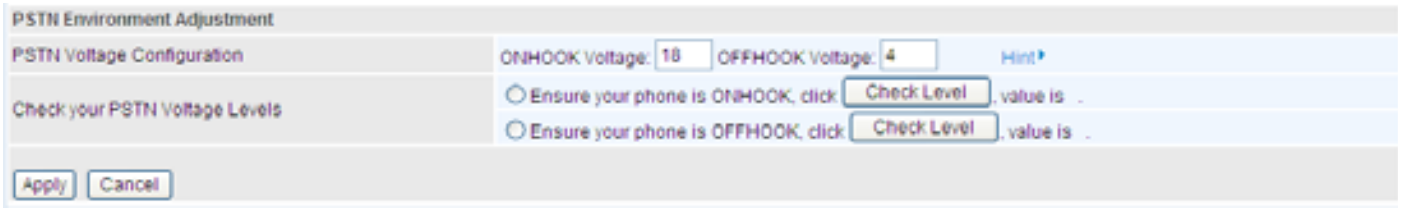
Click the Edit to add or remove the responses code. To be sure the code is separated by a comma (,).

For more information about SIP responses codes, please check Here to link to **http://voip-info.org/wiki/view/sip+response+codes** where you can get to know the meaning of each error code.

T.38 Fax Relay: It allows the transfer of facsimile documents in real-time between two standard Group 3 facsimile terminals over the Internet or other networks using IP protocols. It will only function when both sites are support this feature and enabled.

Advanced – PSTN Environment Adjustment

PSTN Environment Adjustment options will help you to adjust the onhook and offhook voltage detection values for your environment. You should use these if the default values are incorrect and result in PSTN calls not being detected properly, e.g. calls being terminated within 5 seconds of being answered. The actual levels are determined by your environment including the number and type of telephones used.



Note: ONHOOK means hung up.

To take your phone OFFHOOK, lift the receiver then press Hook/Flash until you hear your normal PSTN dialtone, not your VoIP dialtone. Wait several seconds and then press Check Level.

You should check the OFFHOOK value for each telephone you have connected to this device. Set the OFFHOOK voltage to the lowest setting registered for all your telephones, e.g. if your telephones return values of 4, 5 and 7 then you should set your OFFHOOK voltage to 4.

Note: The detected values will not automatically be set by the Check Level function; you must enter the lowest level detected after testing all your telephones.

SIP Accounts

This section reflects and contains basic settings for the VoIP module from selected provider in the Wizard section. Fail to provide correct information will halt making calls out to the Internet.

Profile Name: User-defined name is for identifying the Profile.

Registrar Address (or Hostname): Indicate the VoIP SIP registrar IP address.

Registrar Port: Specify the port of the VoIP SIP registrar on which it will listen for register requests from VoIP device.

Expire: Expire time for the registration message sending.

User Domain/Realm: Set different domain name for the VoIP SIP proxy server.

Outbound Proxy Address: Indicate the VoIP SIP outbound proxy server IP address. This parameter is very useful when VoIP device is behind a NAT.

Outbound Proxy Port: Specify the port of the VoIP SIP outbound proxy on which it will listen for messages.

Phone Number: This parameter holds the registration ID of the user within the VoIP SIP registrar.

Username: Same as Phone Number.

Password: This parameter holds the password used for authentication within VoIP SIP registrar.

Display Name: This parameter will be appeared on the Caller ID.

Direct in Dial: Select the ringing port when getting an incoming VoIP call.

Phone Port

This section displays status and allows you to edit the account information of your Phones. Click Edit to update your phone information.

Port: It allows you to change the phone port setting for specify FXS port.

***69 (Return Call):** Dial *69 to return the last missed call. It is only available for VoIP call(s).

***20 (Do not Disturb ON):** Dial *20 to set the No Disturb on. Your phone will not ring if someone calls.

***80 (Do not Disturb OFF):** Dial *80 to set the No Disturb off. Your will be able to hear ring tone when someone calls.

***90x (Blind Call Transfer):** Dial *90 + phone-number to translate a call to a third party. This feature is enabled by default.

x# Speed Dial (x:2..9): Refer to Phone Port section in the Web GUI. Set up your Speed Dial phone book first before accessing the Speed Dial feature. It is enabled by default.

Redial: Press ## to redial the latest number you dialed. This feature is enabled by default.

***74<x><number>#:** Use your phone key pad to insert a phone number to the Speed Dial phone book. Or you can update your Speed Dial phone number manually. Refer to the Phone Port section in the Web GUI for details.

***67 Anonymous Call:** Hide the own phone number for each call and it will not be displayed on the remote site. It is only applied to the next call when you enter this control character. The detailed operation procedure is “Off Hook -> *67 -> On Hook -> Off Hook -> Dial”. This feature is disabled by default.

Phone Number + #: This is the fast dial which you can dial out a phone number immediately

without waiting.

Note: Refer to Special Dial Code section in this Manual for more details.

Codec Preference

Codec is known as Coder-Decoder used for data signal conversion. Set the priority of voice compression; Priority 1 owns the top priority.

G.729: It is used to encoder and decoder voice information into a single packet which reduces the bandwidth consumption.

G.711μ-LAW: It is a basic non-compressed encoder and decoder technique. μ-LAW uses pulse code modulation (PCM) encoder and decoder to convert 14-bit linear sample.

G.711A-LAW: It is a basic non-compressed encoder and decoder technique. A-LAW uses pulse code modulation (PCM) encoder and decoder to convert 13-bit linear sample.

G.726-32: It is used to encoder and decoder voice information into a single packet which reduces the bandwidth consumption. Currently only supports bit rate with 32Kbps.

DTMF Method: The Inband, RFC 2833 and SIP INFO (RFC 2976) are supported.

Volume Control

Volume control helps you to adjust the voice quality of telephone to the best comfortable listening level.

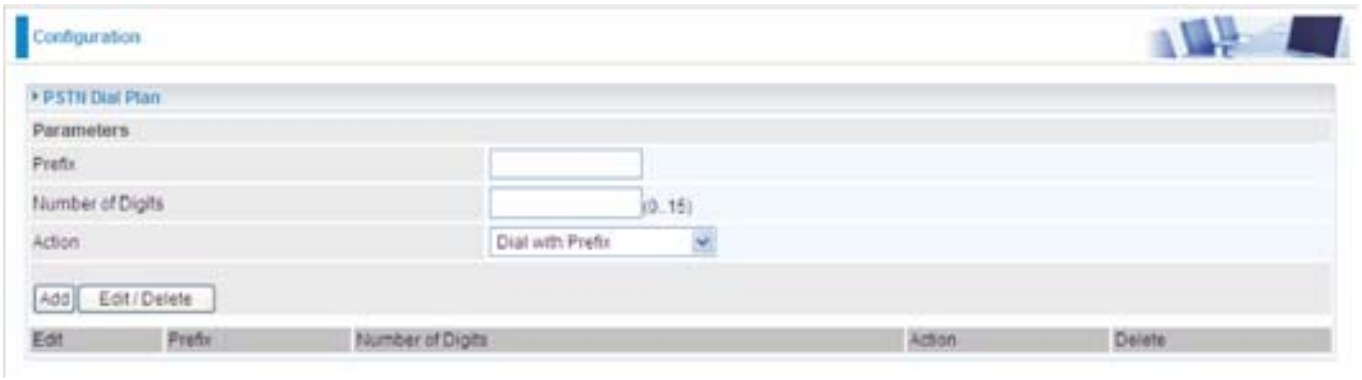
Press “-“, the minus sign, to reduce either microphone or/both speaker’s level of your telephone.

Press “+“, the plus sign, to increase either microphone or/both speaker’s level of your telephone.

PSTN Dial Plan (Router with LINE port only)

This section enables you to configure “VoIP with PSTN switching” on your system. You can define a range of dial plans to make regular call from VoIP switching to PSTN line. Prefix numbers is essential key to make a distinguishing between VoIP and Regular phone call. If actual numbers dialed matches with prefix number defined in this dial plan, the dialed number will be routed to the PSTN to make a regular call. Otherwise, the number will be routed to the VoIP networks.

Reminder! In order to utilize this feature, you must have registered and connected to your SIP Server first.



Prefix: Specify number(s) for switching to a PSTN call.

Number of Digits: Specify the total number of digits wish to dial out. Maximum digit number is 15.

Action: Specify a dialing method you wish to make PSTN call(s).

- **Dial with Prefix:** The dialed number ***with*** prefix will be sent call through the PSTN.

Note: The actual dialed number of valid digits length requires matching in the Number of Digits filed.

- **Dial without Prefix:** The dialed number will be sent call through the PSTN ***without*** prefix.

Note: The actual dialed number of valid digits length requires matching in the Number of Digits filed.

- **Dial at Timeout:** The dialed number will be sent call through the PSTN ***with*** the prefix when timeout starts. This timeout activates when no more digits are dialed in a specific duration.

Note: The actual dialed number of valid digits length MUST NOT exceed in the Number of Digits filed.

- **Dial at Timeout no Prefix:** The dialed number will be sent call through the PSTN ***without*** prefix when timeout starts. This timeout activates when no more digits are dialed in a specific duration.

Note: The actual dialed number of valid digits length MUST NOT exceed in the Number of Digits filed.

Attention

Phone port 1 & 2 will automatically reply to PSTN line when:

- Power is down
- Internet service fail. i.e. lost of WAN IP address
- SIP option is disabled. See VoIP General Settings section.
- Calls match with rule(s) defined in the PSTN Digit Plan.
- SIP service is not accessible. This exclude when:
  - User manually disable Registration
  - User insert a wrong authentication username or password
  - User dials a wrong SIP number, only and if the PSTN
  - auto-fallback function is not enabled. See VoIP General Settings / Advance for more information.

PSTN Dial Plan Examples:

1. Dial with Prefix

If you dial 01223 707070, number 01223707070 will be dialed out via FXO to make a regular phone call.

2. Dial without Prefix

If you dial 9102, the number 102 will only be dialed out via FXO port to make a regular phone call.

3. Dial at Timeout

If you only dial 01223 7070 and no more numbers, after the timeout activates, 012237070 will be dialed to make a regular call via FXO port.

Even though 7070 (only 4 digits) does not match with number of digits 6 defined in the filed, 7070 is still a valid phone number since it has not exceeded 6 digits.

4. Dial at Timeout no Prefix

If you only dial 97070 and no more numbers, after the timeout activates, 7070 will be dialed without prefix to make a regular call via FXO port.

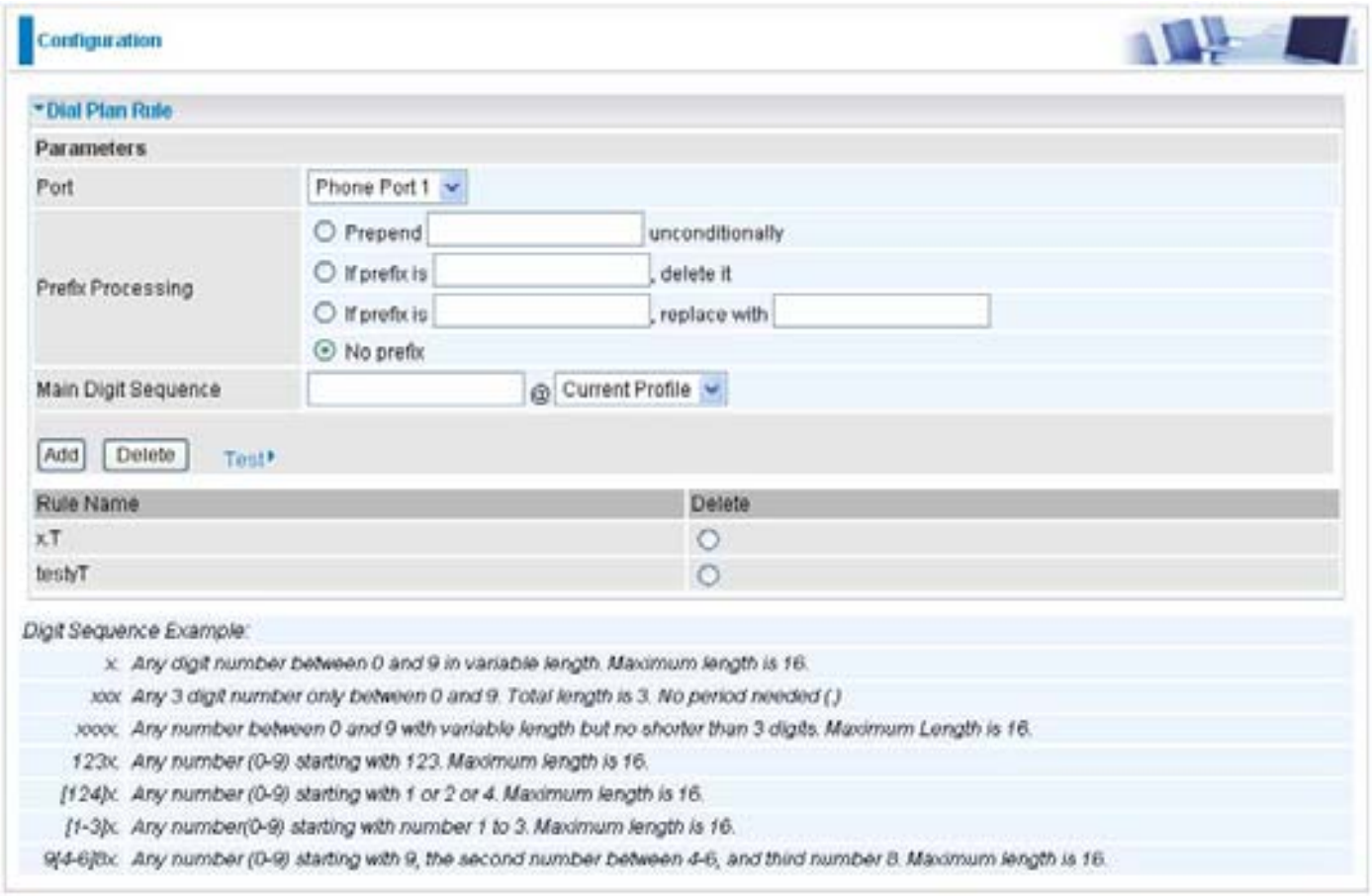
Even though 7070 (only 4 digits) does not match with number of digits 6 defined in the filed, 7070 is still a valid phone number since it has not exceed 6 digits.

VoIP Dial Plan

This section helps you to make a telephony number dialed as making a regular call via VoIP. You no longer need to memorize a long dial string of number for making a VoIP call. Go to Configuration > VoIP > VoIP Dial Plan.

Dial Plan Rules

Click the Add button to create and define a VoIP dial-plan rule(s).



Prefix Processing:

Prepend xxx unconditionally: xxx number is appended unconditionally to the front of the dialing number when making a call. Prefix can also be included with any number and/or character such as **+**, *****, **#**.

Note: For special service with +, *, #, you may need to check with your VoIP or Local Telephone Service Provider for information.

If Prefix is xxx, delete it: Prefix xxx is removed from the dialing numbers before making a call.

If Prefix is xxx, replace with: Prefix xxx is appended to the front of the dialing numbers when making a call.

No prefix: No prefix is appended to the front of the dialing numbers. It is set as in default settings.

Main Digit Sequence: The call(s) can be called out via SIP or PSTN or ENUM.

x: Any numeric number between 0 and 9.

. (period): Repeat numeric number(s) between 0 and 9.

*** (asterisk sign):** It is normal character '*' on phone key pad. Please check if special service(s) is provided by your VoIP Service Provider or your Local Telephone Service Provider.

 # (pound sign): It is normal character '#' on phone key pad. Please check if it is provided by your VoIP Service Provider or Local Telephone Service Provider for special service(s).

<@ Current Profile>: Referring to the VoIP account registered on the *VoIP Wizard* for Port 1 / 2.

<@ PSTN>: Meaning making call(s) via the PSTN line.

<@ENUM>: Meaning making a VoIP SIP direct call via E.164 number ("ENUM") to an ENUM callee.

Electronic Number (ENUM) uses the DNS (Domain Network System) based technology to map between a traditional phone number (PSTN) to an Internet addresses/ SIP URL. The ENUM number must be registered via a public ENUM site or your VoIP Service Provider.

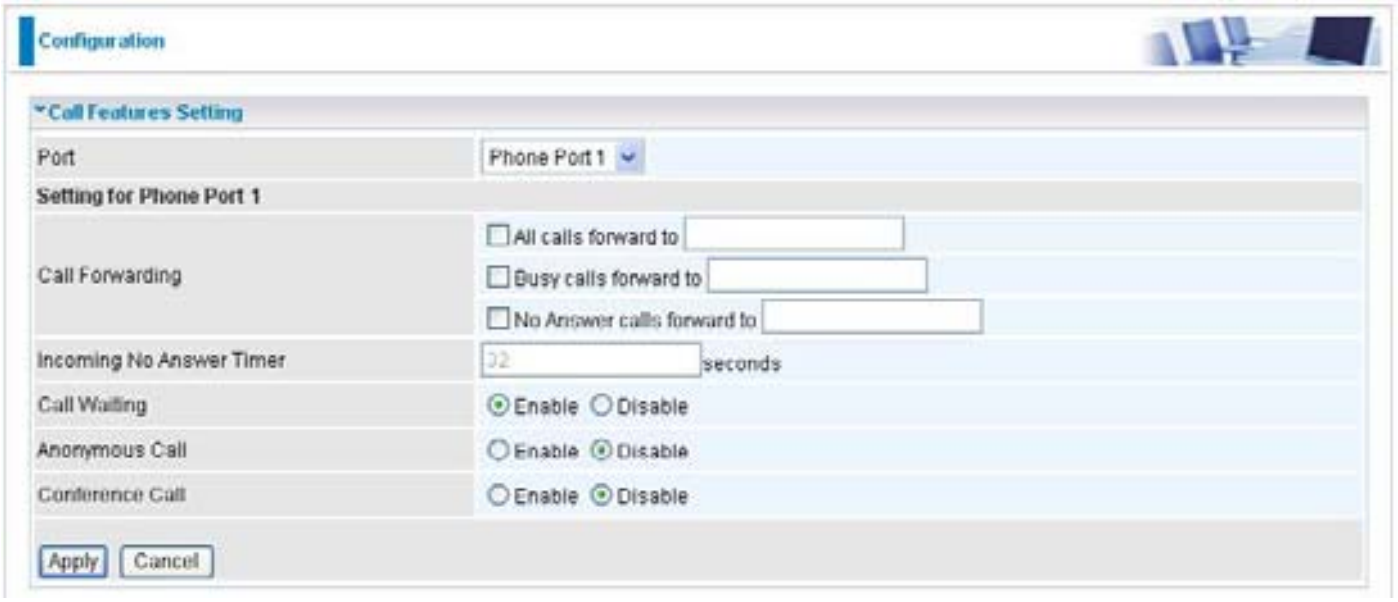
<@ SIPgateway>: It is used for the Intelligent Call Routing feature where you need to set up your SIP account on the VoIP User-defined Profiles link on the VoIP Wizard page. Go to the VoIP Wizard in this manual for more information.

Dial-Plan Examples:	Description
x.	Any digit number between 0 and 9 in variable length. Maximum length is 16.
xxx	Any 3 digit number only between 0 and 9. Total length is 3. ***Note: No period is needed (.)***
xxxx.	Any number between 0 and 9 with variable length but no shorter than 3 digits. Maximum length is 16.
123x.	Any number (0-9) starting with 123. Maximum length is 16.
[x…x]x. For example: [124]x.	Any number (0-9) starting with 1 or 2 or 4. Maximum length is 16.
[x-x]x. For example: [1-3]x.	Any number (0-9) starting with number 1 to 3. Maximum length is 16.
x[x-x]x. For example: 9[4-6]8x.	Any number (0-9) starting with 9, the second number between 4-6, and third number 8. Maximum length is 16.
Special Dial Plan Examples:	**Description**
*xx*x.	Starting with '* sign' + any two digit numbers + any number (0-9) in variable length. Maximum length is 16.
*xx	Starting with '* sign' + any 2 digit numbers between 0 and 9. Total length including the * is 3. ***Note: No period is needed (.)***

**xx*x.	Starting with ‘** sign’ + any two digit numbers between 0 + any number (0-9) in variable length. Maximum length is 16.
#xx.	Starting with ‘# sign’ + any digit number (0-9) in variable length but no shorter than 1 digits. Maximum length is 16.
##xx*x.	Starting with ‘## sign’ + any two digit numbers + ‘* sign’ + any number (0-9) in variable length. Maximum length is 16.

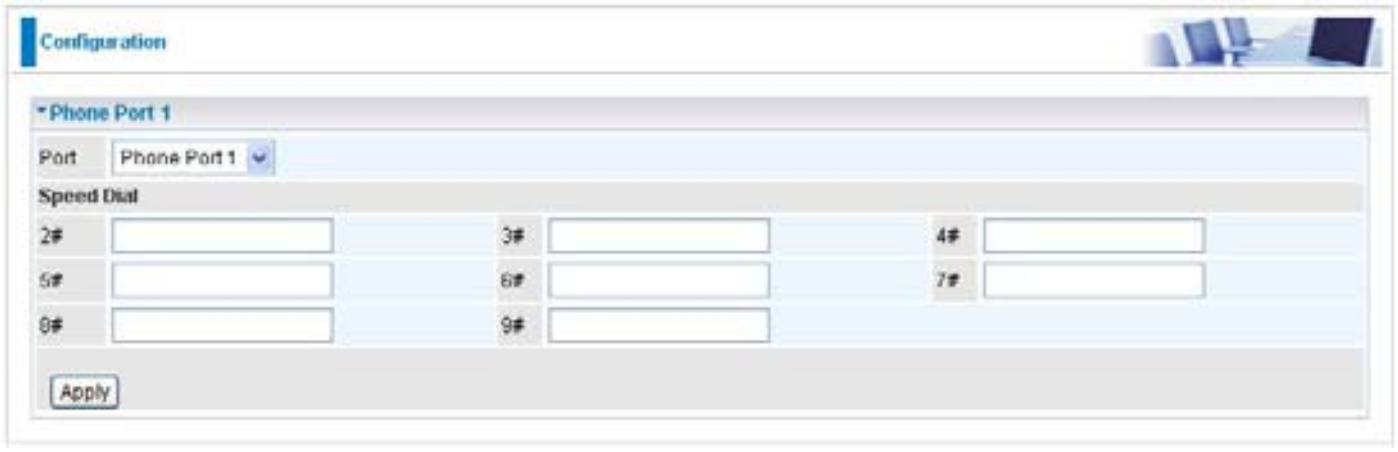
Call Feature

VoIP has all the basic features of a traditional phone. Besides the provided basic features, VoIP also comes with several enhanced features that allows you to further customize their settings to suit your personal needs such as call forwarding setting, call waiting time length, conference call feature, anonymous call feature and incoming no answer timer.



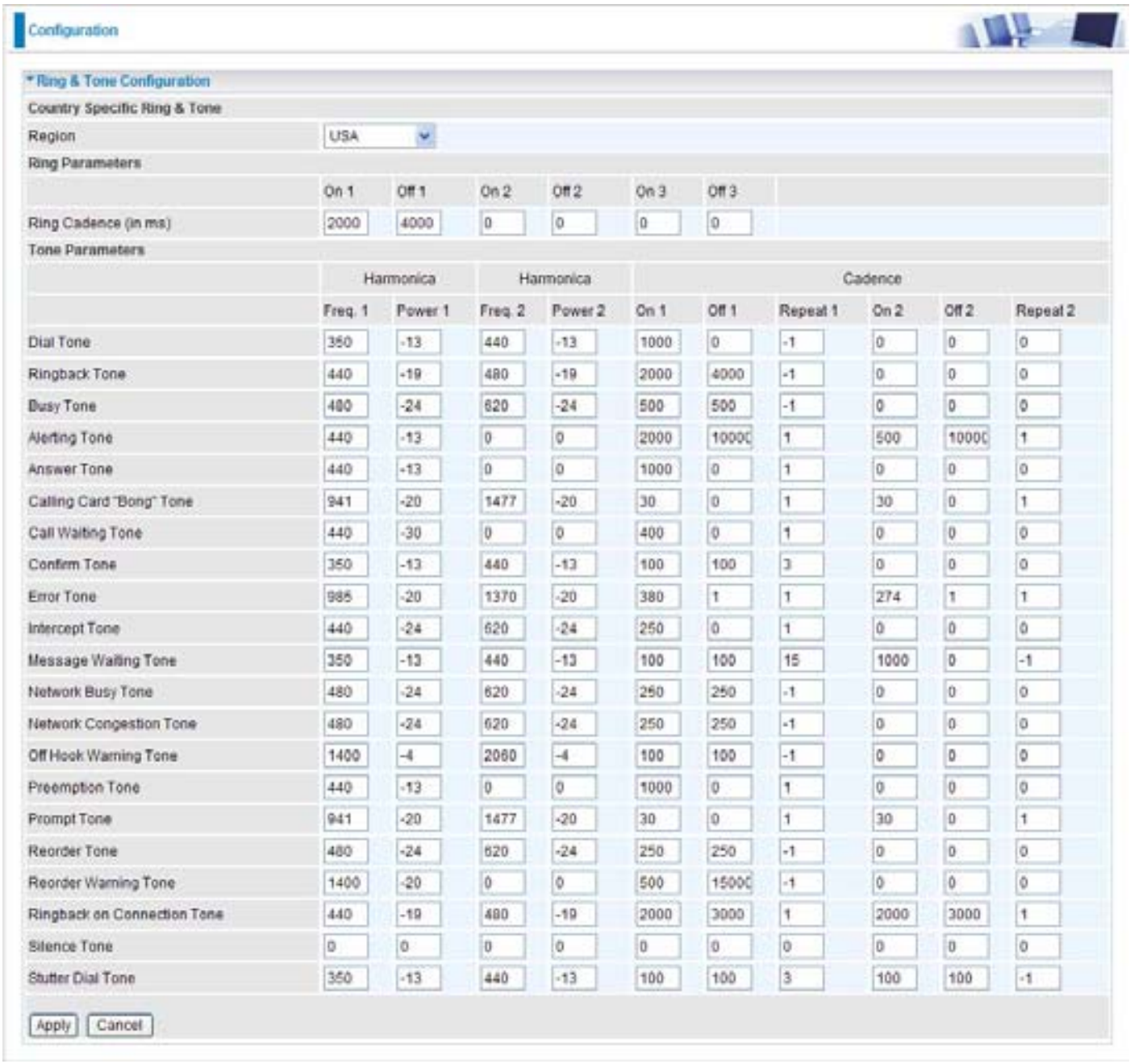
Speed Dial

Speed Dial comes in handy to store frequently used telephone numbers which you can press number from 0 to 9 and the pound sign (#) on the phone keypad to activate the function. For example, speed dial to phone number lists on 9, just press keypad 9 then #. Your router will automatically call out to number listed on entry 9.



Ring & Tone

This section allows advanced user to change the existing or newly defined parameters for the various ring tones (dial tone, busy tone, answer tone and etc.)



Configuration

Ring & Tone Configuration

Country Specific Ring & Tone

Region: USA

Ring Parameters

	On 1	Off 1	On 2	Off 2	On 3	Off 3
Ring Cadence (in ms)	2000	4000	0	0	0	0

Tone Parameters

	Harmonica		Harmonica		Cadence					
	Freq. 1	Power 1	Freq. 2	Power 2	On 1	Off 1	Repeat 1	On 2	Off 2	Repeat 2
Dial Tone	350	-13	440	-13	1000	0	-1	0	0	0
Ringback Tone	440	-19	480	-19	2000	4000	-1	0	0	0
Busy Tone	480	-24	620	-24	500	500	-1	0	0	0
Alerting Tone	440	-13	0	0	2000	10000	1	500	10000	1
Answer Tone	440	-13	0	0	1000	0	1	0	0	0
Calling Card "Bong" Tone	941	-20	1477	-20	30	0	1	30	0	1
Call Waiting Tone	440	-30	0	0	400	0	1	0	0	0
Confirm Tone	350	-13	440	-13	100	100	3	0	0	0
Error Tone	985	-20	1370	-20	380	1	1	274	1	1
Intercept Tone	440	-24	620	-24	250	0	1	0	0	0
Message Waiting Tone	350	-13	440	-13	100	100	15	1000	0	-1
Network Busy Tone	480	-24	620	-24	250	250	-1	0	0	0
Network Congestion Tone	480	-24	620	-24	250	250	-1	0	0	0
Off Hook Warning Tone	1400	-4	2060	-4	100	100	-1	0	0	0
Preemption Tone	440	-13	0	0	1000	0	1	0	0	0
Prompt Tone	941	-20	1477	-20	30	0	1	30	0	1
Reorder Tone	480	-24	620	-24	250	250	-1	0	0	0
Reorder Warning Tone	1400	-20	0	0	500	15000	-1	0	0	0
Ringback on Connection Tone	440	-19	480	-19	2000	3000	1	2000	3000	1
Silence Tone	0	0	0	0	0	0	0	0	0	0
Stutter Dial Tone	350	-13	440	-13	100	100	3	100	100	-1

Apply Cancel

Country Specific Ring & Tone

Region: Select a country ring-tone, from the drop-down list, where you are located. This VoIP router provides default parameter of ring tones according to different countries. The ring-tone parameters are automatically displayed after entering a specific country. If your country is not in the list, you may manually create ring-tone parameters.

Ring Parameters

Ring Cadence (in ms): Ring cadence is defined by three fields, Frequency: On Time1, Off Time1, On Time2, Off Time2 and On Time3, Off Time3. Frequency is specified in Hertz. Time is given in milliseconds.

Tone Parameters

You may need to check with your local telephone service provider for such information. Also, it is recommended that this option be configured by advanced user unless you are instructed to do so.

Click **Apply** to apply the settings.

QoS - Quality of Service

QoS function helps you to control your network traffic for each application from LAN (Ethernet and/or Wireless) to WAN (Internet). It facilitates you to control the different quality and speed of through put for each application when the system is running with full loading of upstream.

Here are the items within the QoS section: **Prioritization, Outbound IP Throttling & Inbound IP Throttling (bandwidth management).**

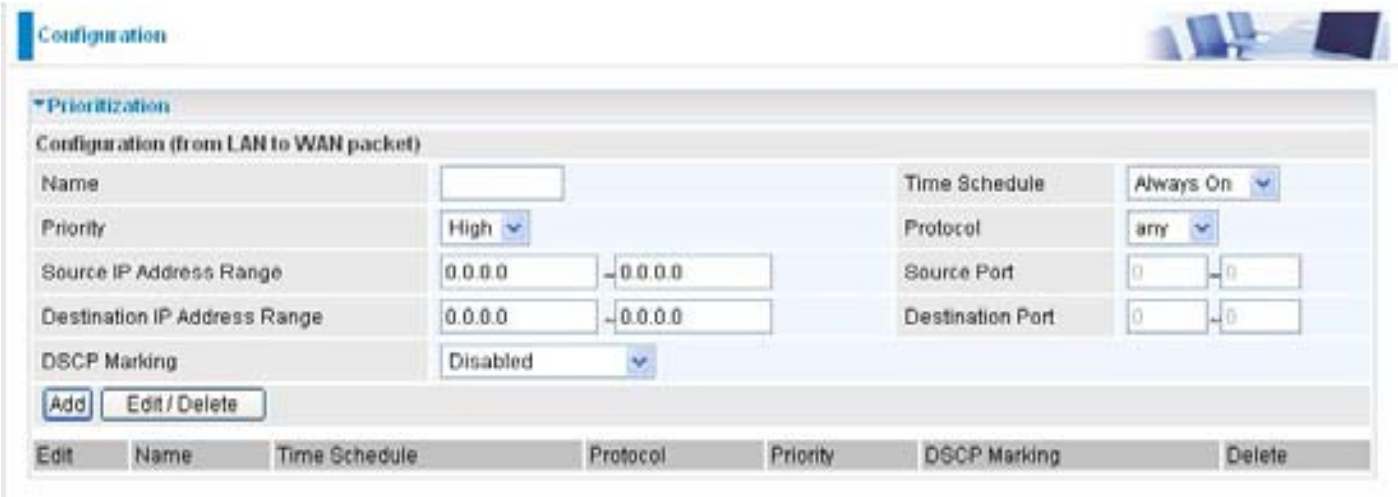
Prioritization

There are three priority settings to be provided in the Router:

- **High**
- **Normal** (The default is normal priority for all of traffic without setting)
- **Low**

And the balances of utilization for each priority are High (60%), Normal (30%) and Low (10%).

To delete the application, you can choose Delete option and then click Edit/Delete.



Name: User-define description to identify this new policy/application.

Time Schedule: Scheduling your prioritization policy.

Priority: The priority given to each policy/application. Its default setting is set to High; you may adjust this setting to fit your policy/application.

Protocol: The name of supported protocol.

Source IP Address Range: The source IP address or range of packets to be monitored.

Source Port: The source port of packets to be monitored.

Destination IP address Range: The destination IP address or range of packets to be monitored.

Destination Port: The destination port of packets to be monitored.

DSCP Marking: Differentiated Services Code Point (DSCP), it is the first 6 bits in the ToS byte. DSCP Marking allows users to assign specific application traffic to be executed in priority by the next Router based on the DSCP value. See Table 4 for **DSCP Mapping Table**.

Note: To be sure the router(s) in the backbones network have the capability in executing and checking the DSCP through-out the QoS network.

Table 4: DSCP Mapping Table

DSCP Mapping Table	
(Wireless) ADSL Router	Standard DSCP
Disabled	None
Best Effort	Best Effort (000000)
Premium	Express Forwarding (101110)
Gold service (L)	Class 1, Gold (001010)
Gold service (M)	Class 1, Silver (001100)
Gold service (H)	Class 1, Bronze (001110)
Silver service (L)	Class 2, Gold (010010)
Silver service (M)	Class 2, Silver (010100)
Silver service (H)	Class 2, Bronze (010110)
Bronze service (L)	Class 3, Gold (011010)
Bronze service (M)	Class 3, Silver (011100)
Bronze service (H)	Class 3, Bronze (011110)

Outbound IP Throttling (LAN to WAN)

IP Throttling allows you to limit the speed of IP traffic. The value entered will limit the speed of the application that you set to the specified value's multiple of 32kbps.

Name: User-define description to identify this new policy/name.

Time Schedule: Scheduling your prioritization policy. Refer to **Time Schedule** for more

information.

Protocol: The name of supported protocol.

Rate Limit: To limit the speed of outbound traffic

Source IP Address Range: The source IP address or range of packets to be monitored.

Source Port(s): The source port of packets to be monitored.

Destination IP Address Range: The destination IP address or range of packets to be monitored.

Destination Port(s): The destination port of packets to be monitored.

Inbound IP Throttling (WAN to LAN)

IP Throttling allows you to limit the speed of IP traffic. The value entered will limit the speed of the application that you set to the specified value's multiple of 32kbps.

Name: User-define description to identify this new policy/application.

Time Schedule: Scheduling your prioritization policy. Refer to **Time Schedule** for more information.

Protocol: The name of supported protocol.

Rate Limit: To limit the speed of for inbound traffic.

Source IP Address Range: The source IP address or range of packets to be monitored.

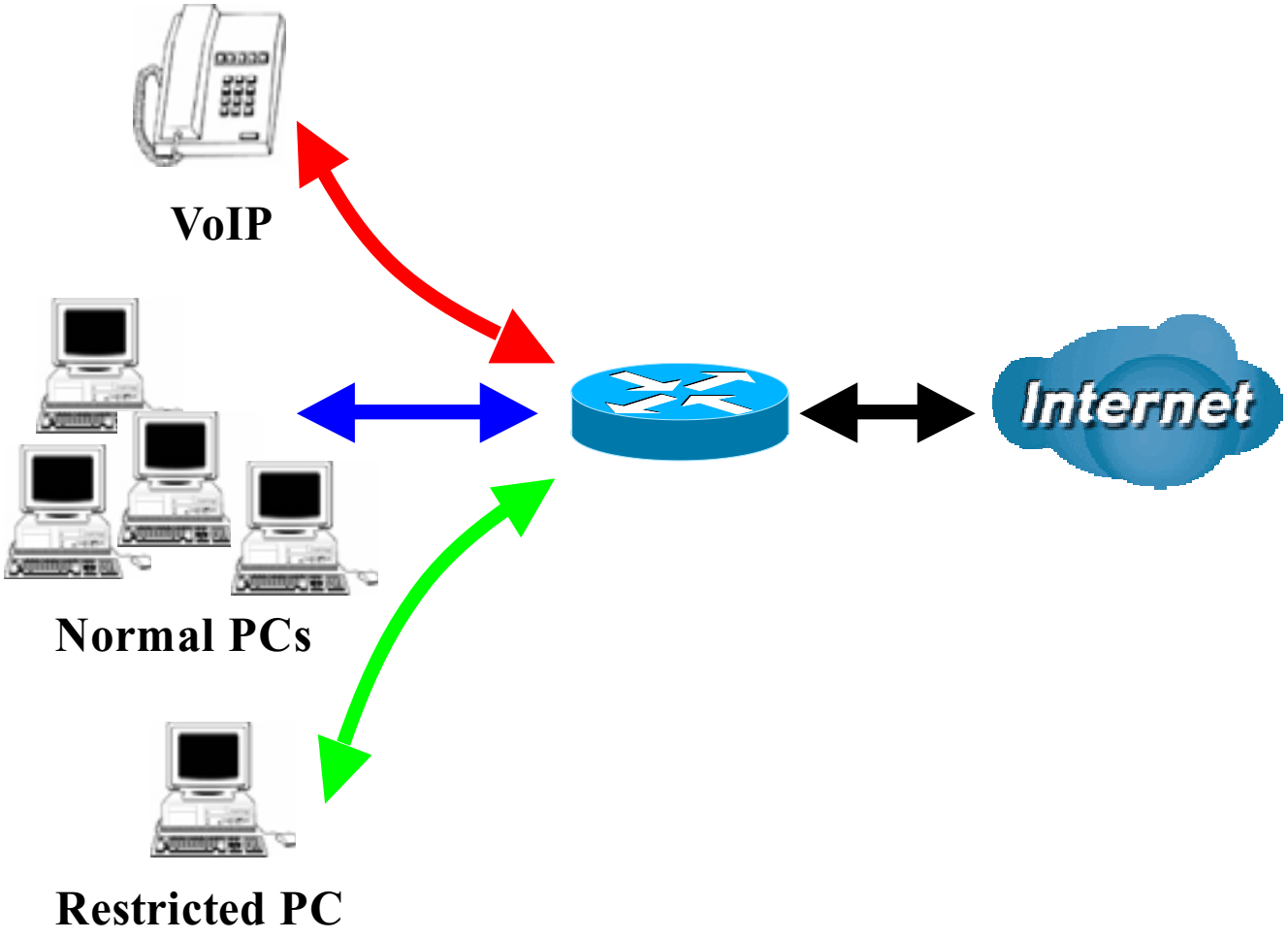
Source Port(s): The source port of packets to be monitored.

Destination IP Address Range: The destination IP address or range of packets to be monitored.

Destination Port(s): The destination port of packets to be monitored.

Example: QoS for your Network

Connection Diagram



Information and Settings

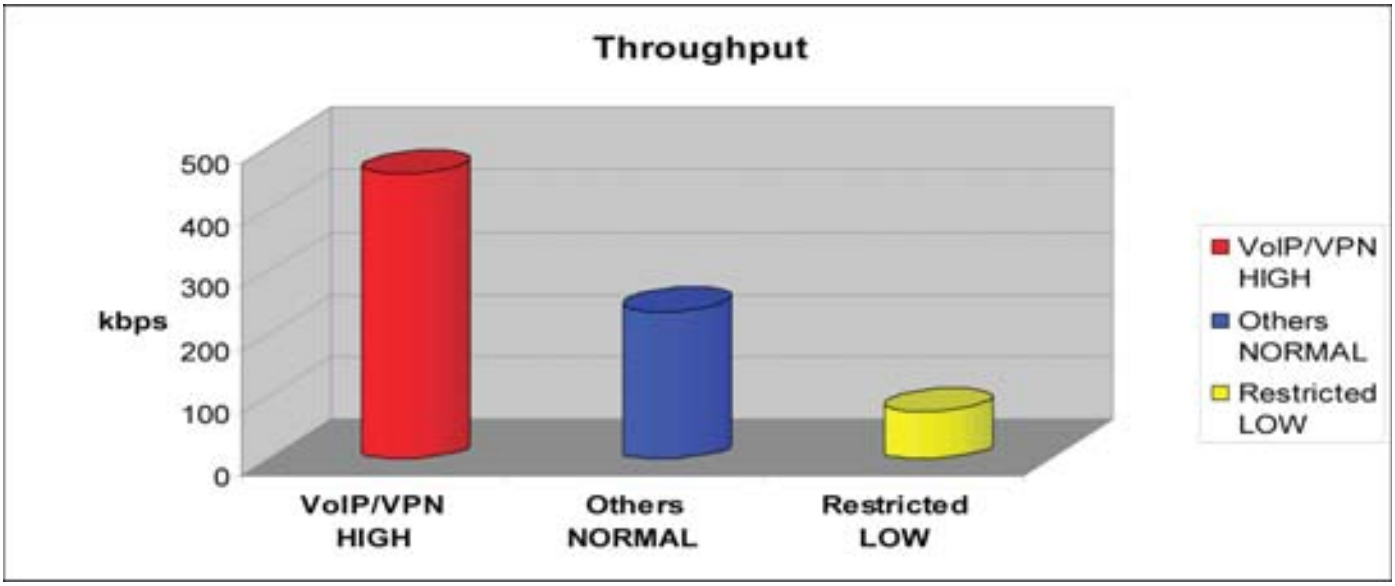
Upstream: 928 kbps

Downstream: 8 Mbps

VoIP User : 192.168.1.1

Normal Users : 192.168.1.2~192.168.1.5

Restricted User: 192.168.1.100



Mission-critical application

Mostly the VPN connection is mission-critical application for doing data exchange between head and branch office.

The mission-critical application must be sent out smoothly without any dropping. Set priority as high level for preventing any other applications to saturate the bandwidth.

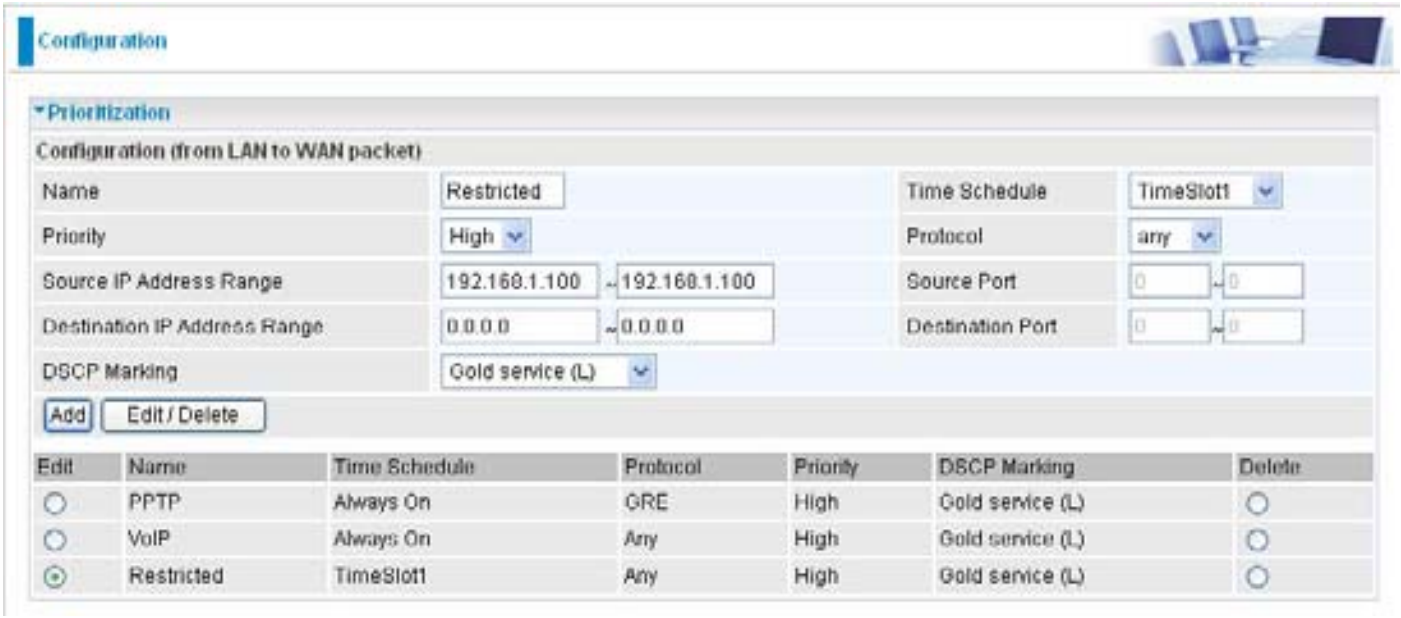
Voice application

Voice is latency-sensitive application. Most VoIP devices are use SIP protocol and the port number will be assigned by SIP module automatically. Better to use fixed IP address for catching VoIP packets as high priority.

Above settings will help to improve quality of your VoIP service when traffic is full loading.

Restricted Application

Some of companies will setup FTP server for customer downloading or home user sharing their files by using FTP.



With above settings that help to limit utilization of upstream of FTP. Time schedule also help you to only limit utilization at daytime.

Advanced setting by using IP throttling

With IP throttling you can specify more detail for allocating bandwidth; even the applications are located in the same level.

Upstream: 928kbps (29*32kbps)

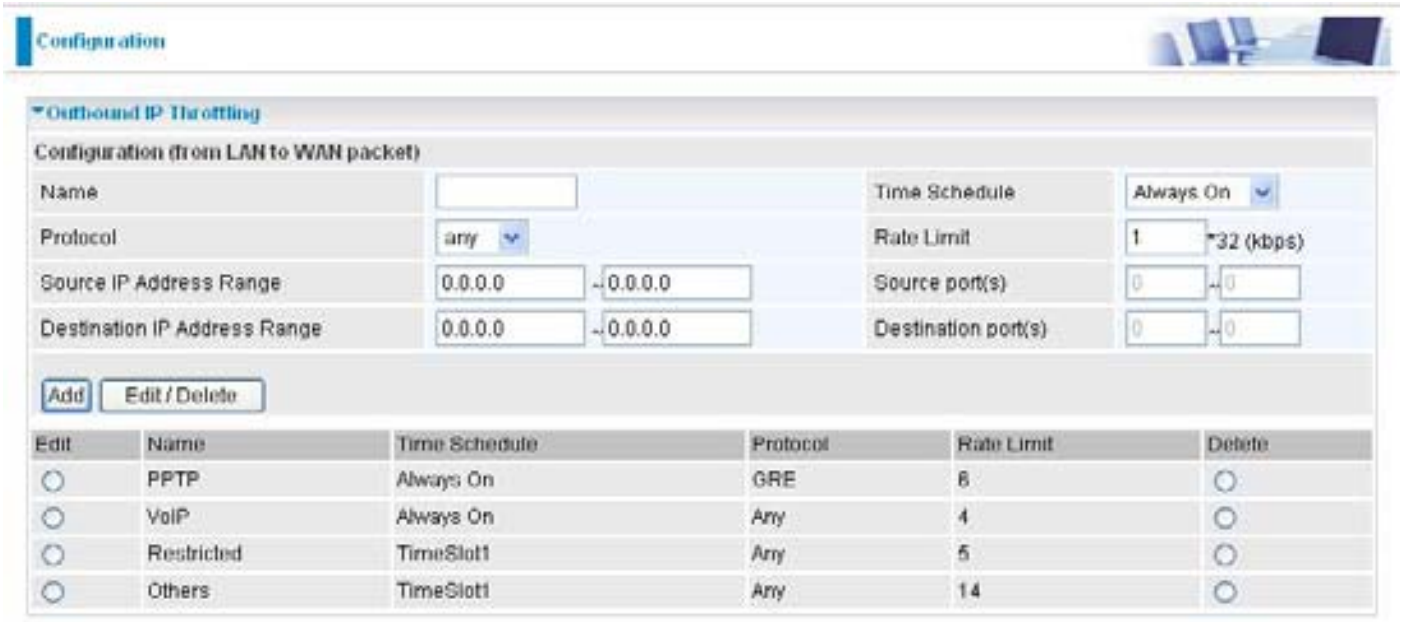
Mission-critical Application: 192kbps (6*32kbps)

Voice Application: 128kbps (4*32kbps)

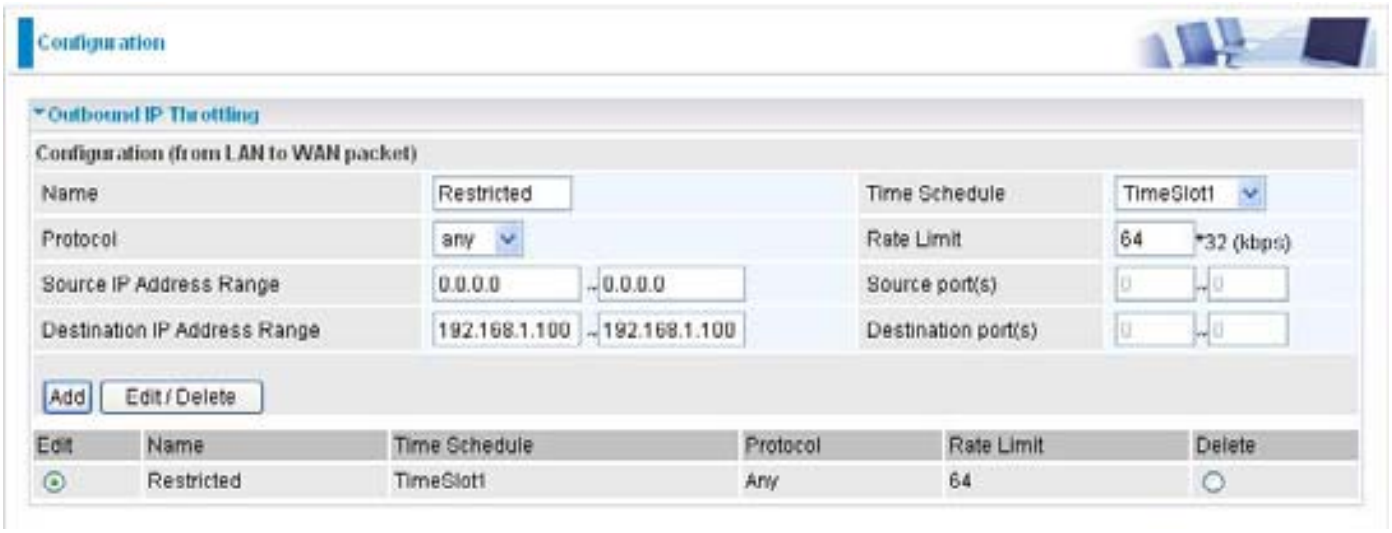
Restricted Application: 160kbps (5*32kbps)

Other Applications: 448kbps (14*32kbps)

6+4+14+5=29, 29*32kbps=928kbps



Sometime your customers or friends may upload their files to your FTP server and that will saturate your downstream bandwidth. The settings below help you to limit bandwidth for the restricted application.



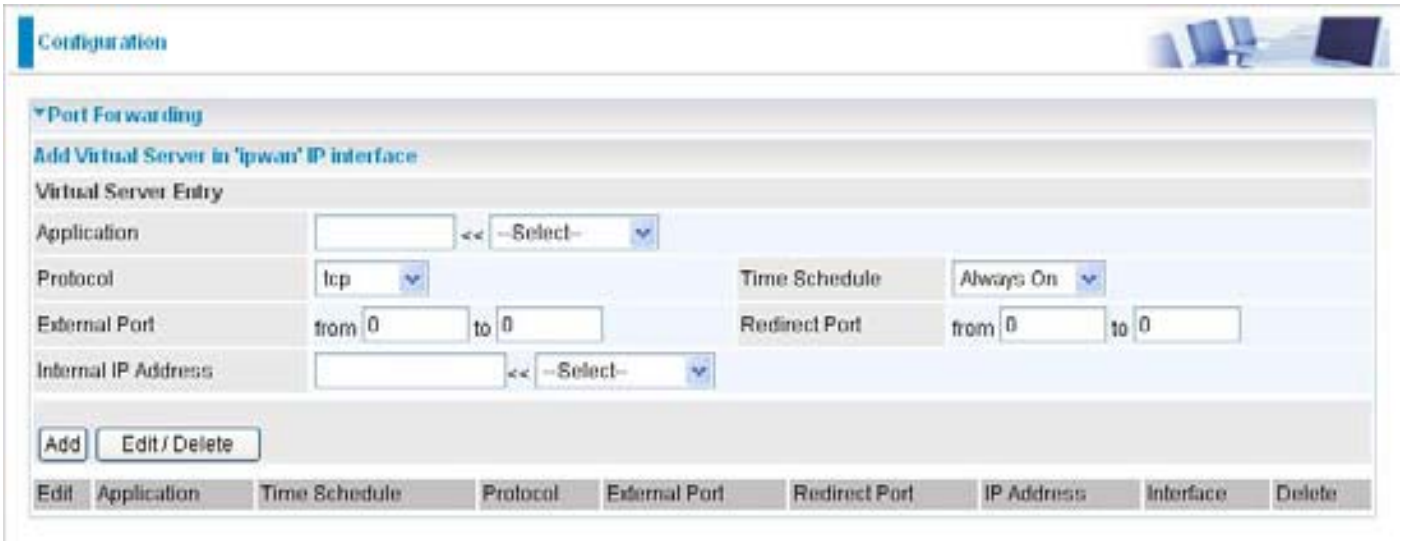
Virtual Server (known as Port Forwarding)

In TCP/IP and UDP networks a port is a 16-bit number used to identify which application program (usually a server) incoming connections should be delivered to. Some ports have numbers that are pre-assigned to them by the IANA (the Internet Assigned Numbers Authority), and these are referred to as “well-known ports”. Servers follow the well-known port assignments so clients can locate them.

If you wish to run a server on your network that can be accessed from the WAN (i.e. from other machines on the Internet that are outside your local network), or any application that can accept incoming connections (e.g. Peer-to-peer/P2P software such as instant messaging applications and P2P file-sharing applications) and are using NAT (Network Address Translation), then you will usually need to configure your router to forward these incoming connection attempts using specific ports to the PC on your network running the application. You will also need to use port forwarding if you want to host an online game server.

The reason for this is that when using NAT, your publicly accessible IP address will be used by and point to your router, which then needs to deliver all traffic to the private IP addresses used by your PCs. Please see the WAN configuration section of this manual for more information on NAT.

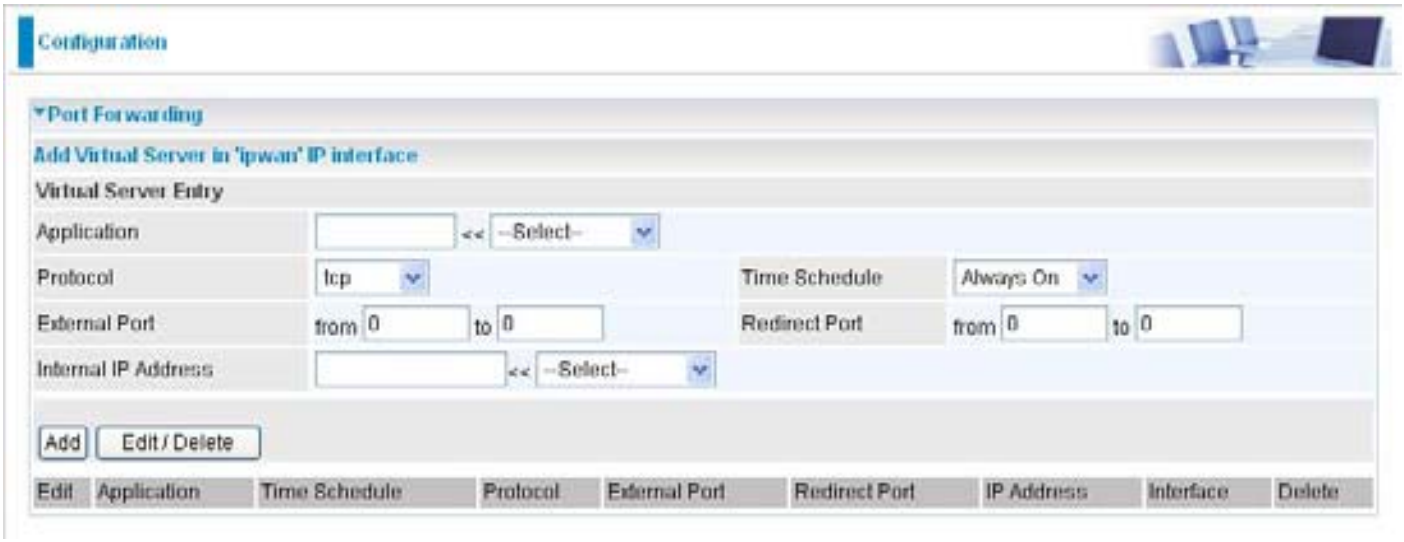
The device can be configured as a virtual server so that remote users accessing services such as Web or FTP services via the public (WAN) IP address can be automatically redirected to local servers in the LAN network. Depending on the requested service (TCP/UDP port number), the device redirects the external service request to the appropriate server within the LAN network



Add Virtual Server

Because NAT can act as a “natural” Internet firewall, your router protects your network from being accessed by outside users when using NAT, as all incoming connection attempts will point to your router unless you specifically create Virtual Server entries to forward those ports to a PC on your network.

When your router needs to allow outside users to access internal servers, e.g. a web server, FTP server, Email server or game server, the router can act as a “virtual server”. You can set up a local server with a specific port number for the service to use, e.g. web/HTTP (port 80), FTP (port 21), Telnet (port 23), SMTP (port 25), or POP3 (port 110), When an incoming access request to the router for a specified port is received, it will be forwarded to the corresponding internal server.



Application: Users-define description to identify this entry or click the Application drop-down menu to select an existing predefined rules.

--Select-- **:** 20 predefined rules are available. Application, Protocol and External/Redirect Ports will be filled after the selection.

Protocol: It is the supported protocol for the virtual server. In addition to specifying the port number to be used, you will also need to specify the protocol used. The protocol used is determined by the particular application. Most applications will use TCP or UDP.

Time Schedule: User-defined time period to enable your virtual server. You may specify a time schedule or Always on for the usage of this Virtual Server Entry. For setup and detail, refer to **Time Schedule** section

External Port: The Port number on the Remote/WAN side used when accessing the virtual server.

Redirect Port: The Port number used by the Local server in the LAN network.

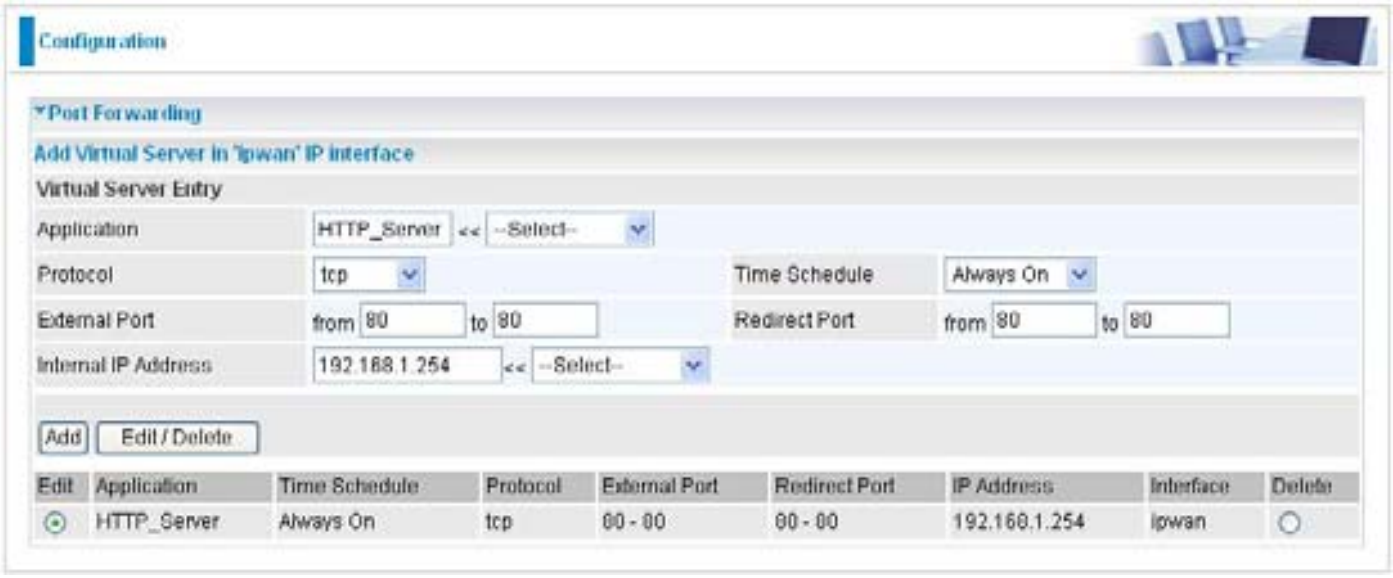
Internal IP Address: The private IP in the LAN network, which will be providing the virtual server application. --Select-- List all existing PCs connecting to the network. You may assign a PC with IP address and MAC from this list.

Example:

If you like to remote accessing your Router through the Web/HTTP at all time, you would need to

enable port number 80 (Web/HTTP) and map to Router's IP Address. Then all incoming HTTP requests from you (Remote side) will be forwarded to the Router with IP address of 192.168.1.254. Since port number 80 has already been predefined, next to the Application click Helper. A list of predefined rules window will pop and select HTTP_Sever.

Application: *HTTP_Sever*
Time Schedule: *Always On*
Protocol: *tcp*
External Port: *80-80*
Redirect Port: *80-80*
IP Address: *192.168.1.254*



Add: Click it to apply your settings.

Edit/Delete: Click it to edit or delete this virtual server application.

NOTE:

Using Port Forwarding does have implications, as outside users will be able to connect to the PCs on your network. For this reason, you are adviced to use specific Virtual Server entries just for the port your application requires instead of using DMZ. Doing so will result in all connections from WAN to attempt to access the public IP your DMZ specifies.

Attention

If you have disabled the NAT option in the WAN-ISP section, the Virtual Server will hence become invalid. If the DHCP option is enabled, you have to be very careful in assigning the IP addresses of the virtual servers in order to avoid conflicts. The easiest way of configuring Virtual Servers is to manually assign static IP address to each virtual server PC, with an address that does not fall into the range of IP addresses that are to be issued by the DHCP server. You can configure the virtual server IP address manually, but it must still be in the same subnet as the router.

Edit DMZ Host

The DMZ Host is a local computer exposed to the Internet. When setting a particular internal IP address as the DMZ Host, all incoming packets will be checked by the Firewall and NAT algorithms then passed to the DMZ host, when a packet received does not use a port number used by any other Virtual Server entries.

Cautious: This Local computer exposing to the Internet may face varies of security risks.

Go to Configuration > Virtual Server > Edit DMZ Host

Enabled: It activates your DMZ function.

Disabled: As set in default setting, it disables the DMZ function.

Internal IP Address: Give a static IP address to the DMZ Host when **Enabled** radio button is checked. Be aware that this IP will be exposed to the WAN/Internet.

List all existing PCs connecting to the network. You may assign a PC with IP address from this list.

Select the Apply button to apply your changes.

Edit One-to-One NAT (Network Address Translation)

One-to-One NAT maps a specific private/local IP address to a global/public IP address.

If you have multiple public/WAN IP addresses from you ISP, you are eligible for One-to-One NAT to utilize these IP addresses.

Go to Configuration > Virtual Server > Edit One-to-one NAT

NAT Type: Select desired NAT type. As set in default setting, it disables the One-to-One NAT function.

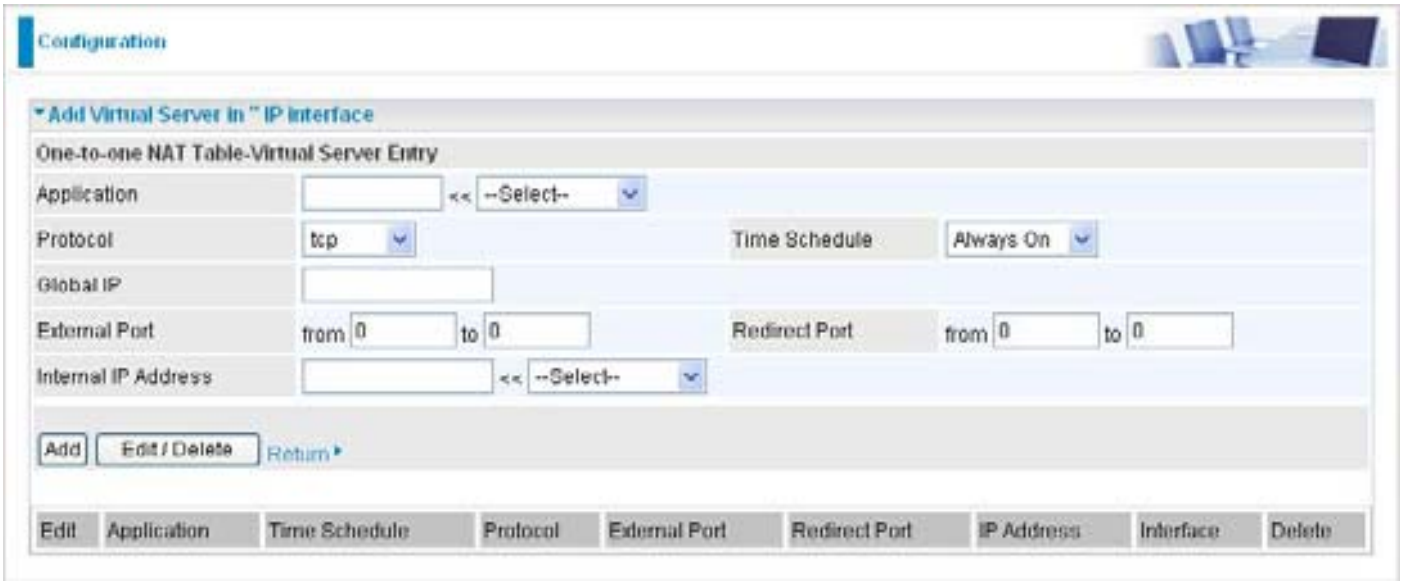
Global IP Address:

- **Subnet:** The subnet of the public/WAN IP address given by your ISP. If your ISP has provided this information, you may insert it here. Otherwise, use IP Range method.
- **IP Range:** The IP address range of your public/WAN IP addresses. For example, IP: 192.168.1.1, end IP: 192.168.1.10

Select the **Apply** button to apply your changes.

Check 

to create a new One-to-One NAT rule:



Application: Users-defined description to identify this entry or click --Select-- drop-down menu to select existing predefined rules.

--Select-- : 20 predefined rules are available. Application, Protocol and External/Redirect Ports will be filled after the selection.

Protocol: It is the supported protocol for the virtual server. In addition to specifying the port number to be used, you will also need to specify the protocol used. The protocol used is determined by the particular application. Most applications will use TCP or UDP;

Time Schedule: User-defined time period to enable your virtual server. You may specify a time schedule or Always on for the usage of this Virtual Server Entry. For setup and detail, refer to **Time Schedule** section

Global IP: Define a public/ WAN IP address for this Application to use. This Global IP address must be defined in the Global IP Address.

External Port: The Port number on the Remote/WAN side used when accessing the virtual server.

Redirect Port: The Port number used by the Local server in the LAN network.

Internal IP Address: The private IP in the LAN network, which will be providing the virtual server application. --Select-- List all existing PCs connecting to the network. You may assign a PC with IP address from this list.

Select the **Add** button to apply your changes.

Example: List of some well-known and registered port numbers.

The Internet Assigned Numbers Authority (IANA) is the central coordinator for the assignment of unique parameter values for Internet protocols. Port numbers range from 0 to 65535, but only ports numbers 0 to 1023 are reserved for privileged services and are designated as “well-known ports” (Please refer to Table 5). The registered ports are numbered from 1024 through 49151. The remaining ports, referred to as dynamic or private ports, are numbered from 49152 through 65535.

For further information, please see IANA’s website at **http://www.iana.org/assignments/port-numbers**

For help on determining which private port numbers are used by common applications on this list, please see the FAQs (Frequently Asked Questions) at **http://www.billion.com**

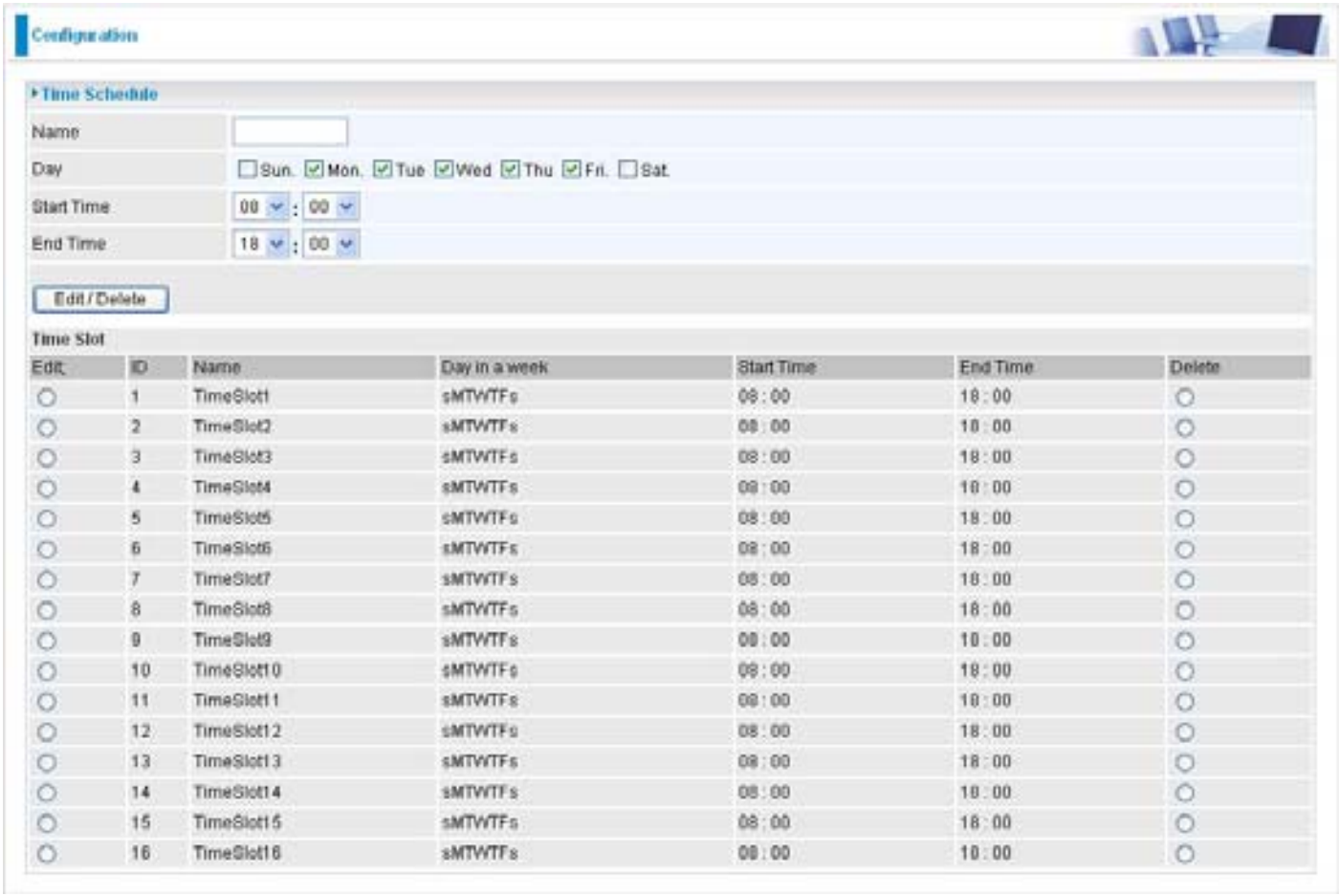
Table 5: Well-known and registered Ports

Port Number	Protocol	Description
20	TCP	FTP Data
21	TCP	FTP Control
22	TCP & UDP	SSH Remote Login Protocol
23	TCP	Telnet
25	TCP	SMTP (Simple Mail Transfer Protocol)
53	TCP & UDP	DNS (Domain Name Server)
69	UDP	TFTP (Trivial File Transfer Protocol)
80	TCP	World Wide Web HTTP
110	TCP	POP3 (Post Office Protocol Version 3)
119	TCP	NEWS (Network News Transfer Protocol)
123	UDP	NTP (Network Time Protocol) / SNTP (Simple Network Time Protocol)
161	TCP	SNMP
443	TCP & UDP	HTTPS
1503	TCP	T.120
1720	TCP	H.323
4000	TCP	ICQ
7070	UDP	RealAudio

Time Schedule

The Time Schedule supports up to 16 time slots 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 Time Zone for details. You router time should correspond with your local time. If the time is not set correctly, your Time Schedule will not function properly.



Configuration of Time Schedule

Edit a Time Slot

1. Choose any Time Slot (ID 1 to ID 16) to edit, click Edit radio button.

Note: Watch it carefully, the days you have selected will present in capital letter. Lower case letter shows the day(s) is not selected, and no rule will apply on this day(s).

2. A detailed setting of this Time Slot will be shown.

ID: This is the index of the time slot.

Name: A user-define description to identify this time portfolio.

Day in a week: The default is set from Monday through Friday. You may specify the days for the schedule to be applied.

Start Time: The default is set at 8:00 AM. You may specify the start time of the schedule.

End Time: The default is set at 18:00 (6:00PM). You may specify the end time of the schedule.

Choose Edit radio button and click Edit/Delete button to apply your changes.

Delete a Time Slot

Select the Delete radio button of the selected Time Slot under the Time Slot section, and click the Edit/Delete button to confirm the deletion of the selected Time profile, i.e. erase the Day and back to default setting of Start Time / End Time.

Advanced

Configuration options within the Advanced section are for users who wish to take advantage of the more advanced features of the router. Users who do not understand the features should not attempt to reconfigure their router, unless advised to do so by support staff.

Here are the items within the Advanced section: **Static Route, Dynamic DNS, Check Email, Device Management, IGMP** and **VLAN Bridge.**

Static Route

Go to Configuration > Advanced > Static Route.

Destination: This is the destination subnet IP address.

Netmask: Subnet mask of the destination IP addresses based on above destination subnet IP.

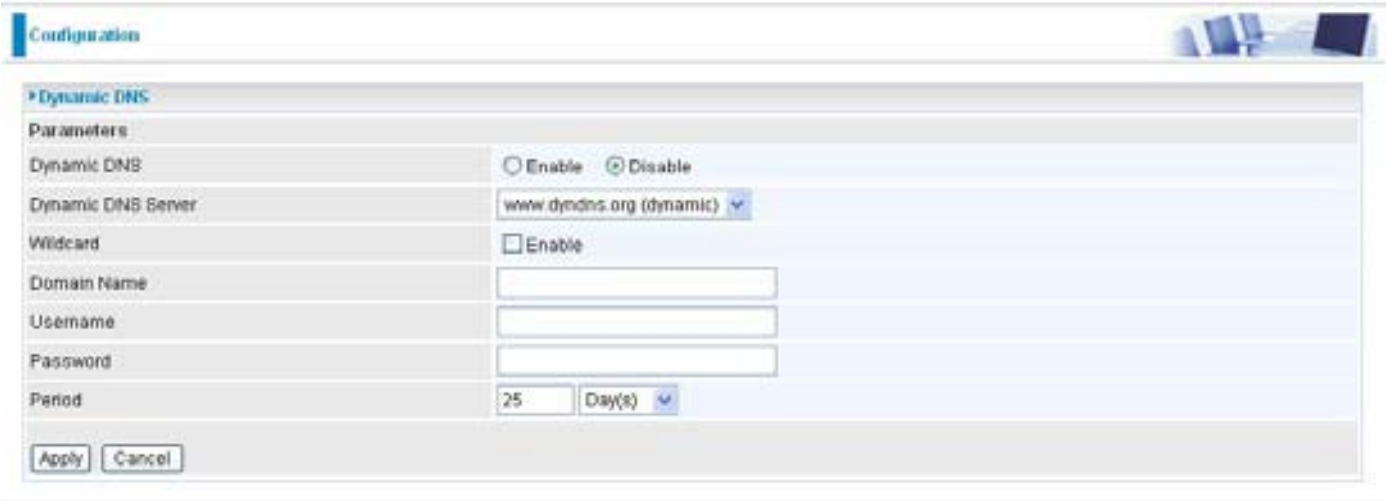
Gateway: This is the gateway IP address to which packets are to be forwarded.

Interface: Select the interface through which packets are to be forwarded.

Cost: This is the same meaning as Hop. This should usually be left at 1.

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.



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

There are more than 5 DDNS services supported.

Dynamic DNS:

- **Disable:** Check to disable the Dynamic DNS function.
- **Enable:** Check to enable the Dynamic DNS function. The following fields will be activated and required.

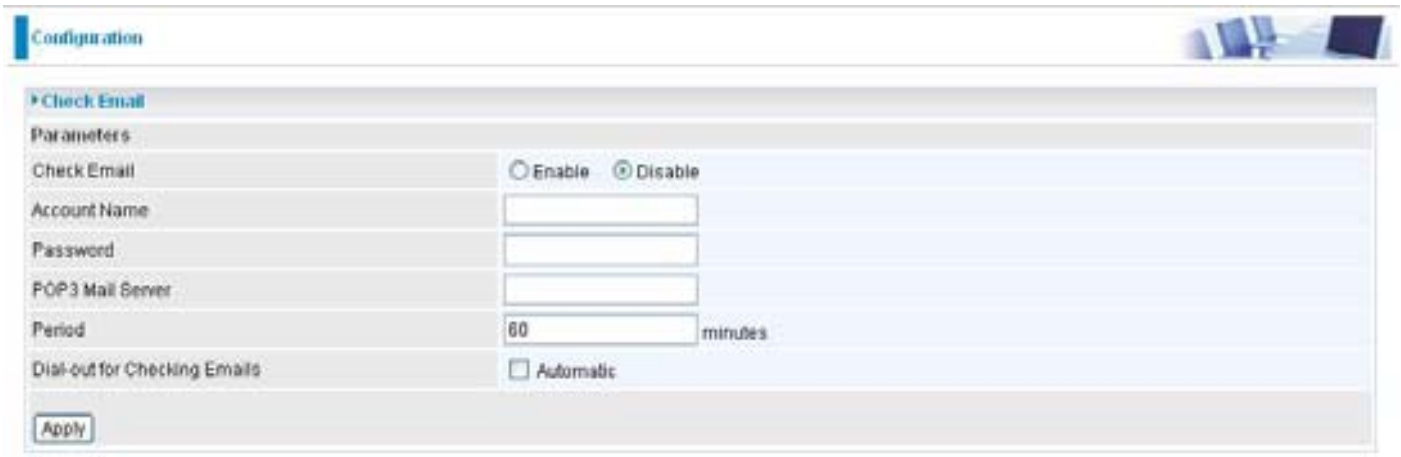
Dynamic DNS Server: Select the DDNS service you have established an account with.

Domain 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.

Check Email

This function allows you to have the router check your POP3 mailbox for new Email messages. The Mail LED on your router will light when it detects new messages waiting for download. You may also view the status of this function using the Status – Email Checking section of the web interface, which also provides details on the number of new messages waiting. See the Status section of this manual for more information.



Check Email:

- **Disable:** Check to disable the router's Email checking function.
- **Enable:** Check to enable the routers Email checking function. The following fields will be activated and required.

Account Name: Enter the name (login) of the POP3 account you wish to check. Normally, it is the text in your email address before the "@" symbol. If you have trouble with it, please contact your ISP.

Password: Enter the account's password.

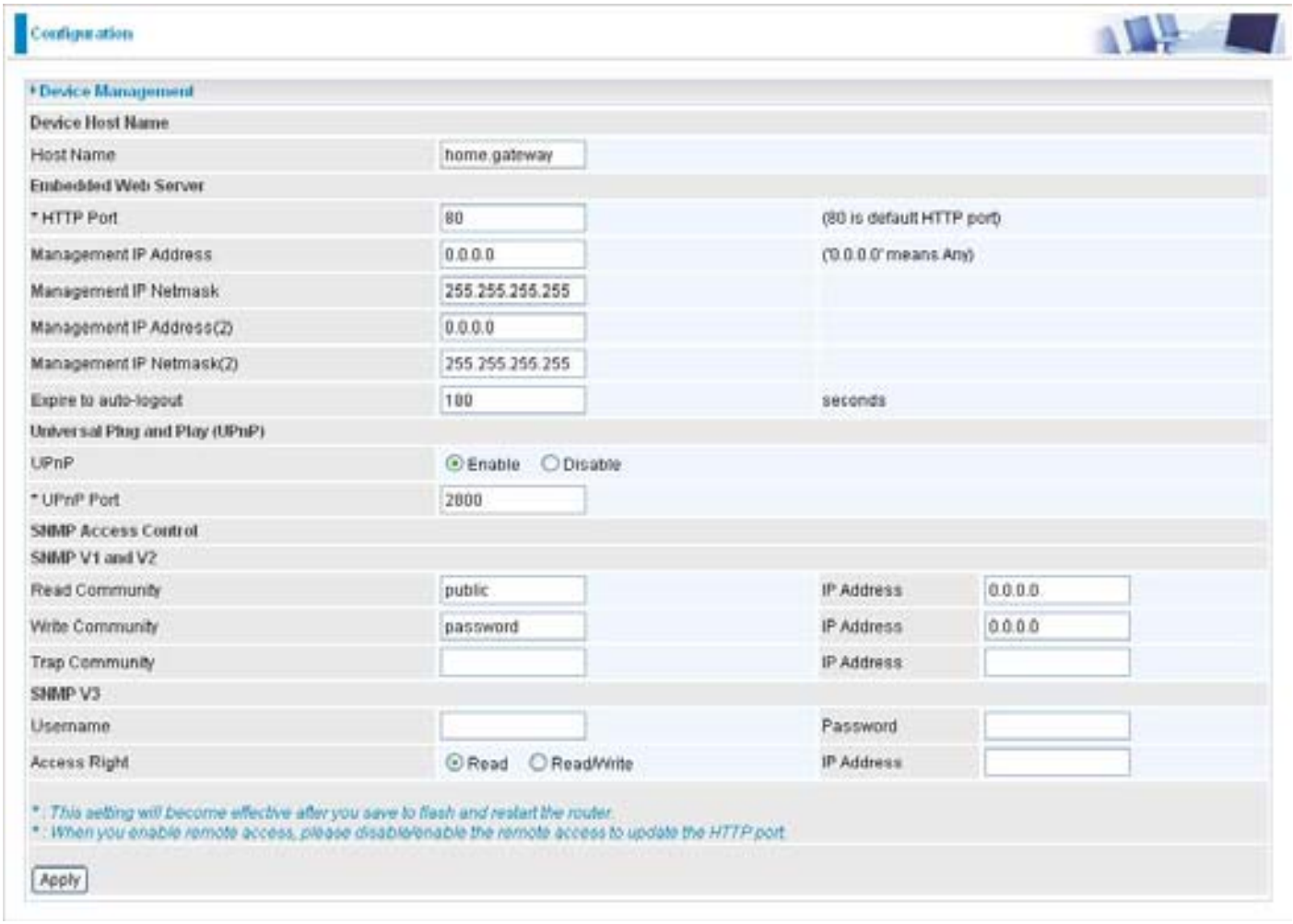
POP3 Mail Server: Enter your (POP) mail server name. You Internet Service Provider (ISP) or network administrator will be able to supply you with this.

Period: Enter the value in minutes between periodic mail checks.

Dial-out for checking emails: When the function is enabled, your ADSL router will connect to your ISP automatically to check emails if your Internet connection dropped. Please be careful when using this feature if your ADSL service is charged by time online.

Device Management

The Device Management advanced configuration settings allow you to control your router's security options and device monitoring features.



Device Host Name

Host Name: Assign it a name**.**

(The Host Name cannot be used with one word only. There are two words should be connected with a '.' at least.
Example:
Host Name: homegateway ==> Incorrect
Host Name: home.gateway or my.home.gateway ==> Correct)

Embedded Web Server (2 Management IP Accounts)

HTTP Port: This is the port number the router's embedded web server (for web-based configuration) will use. The default value is the standard HTTP port, 80. Users may specify an alternative if, for example, they are running a web server on a PC within their LAN.

Management IP Address: You may specify an IP address allowed to logon and access the router's web server. Setting the IP address to 0.0.0.0 will disable IP address restrictions, allowing users to login from any IP address.

Expire to auto-logout: Specify a time frame for the system to auto-logout the user's configuration session.

For Example: User A changes HTTP port number to **100**, specifies their own IP address of **192.168.1.55**, and sets the logout time to be **100** seconds. The router will only allow User A access from the IP address **192.168.1.55** to logon to the Web GUI by typing: **http://192.168.1.254:100** in their web browser. After 100 seconds, the device will automatically logout User A.

Universal Plug and Play (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.

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

UPnP Port: Its default setting is 2800. It is highly recommended for users to use this port value. If this value conflicts with other ports already being used you may wish to change the port.

SNMP Access Control (Software on a PC within the LAN is required in order to utilize this function) – Simple Network Management Protocol.

SNMP V1 and V2:

Read Community: Specify a name to be identified as the Read Community, and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, user obtains this IP address will be able to view the data.

Write Community: Specify a name to be identified as the Write Community, and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, users from this IP address will be able to view and modify the data.

Trap Community: Specify a name to be identified as the Trap Community, and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, users from this IP address will be sent SNMP Traps.

SNMP V3:

Specify a name and password for authentication. And define the access right from identified IP address. Once the authentication has succeeded, users from this IP address will be able to view and modify the data.

SNMP Version: SNMPv2c and SNMPv3

SNMPv2c is the combination of the enhanced protocol features of SNMPv2 without the SNMPv2 security. The "c" comes from the fact that SNMPv2c uses the SNMPv1 community string paradigm

for “security”, but is widely accepted as the SNMPv2 standard.

SNMPv3 is a strong authentication mechanism, authorization with fine granularity for remote monitoring.

Traps supported: Cold Start, Authentication Failure.

The following MIBs are supported:

From RFC 1213 (MIB-II) System group

- System group
- Interface group
- Address Translation group
- IP group

ICMP Group

- TCP group
- UDP group
- EGP (not applicable)
- Transmission
- SNMP group

From RFC 1650 (EtherLike-MIB)

- dot3stats

From RFC 1493 (Bridge MIB)

- dot1 dBase group
- dot1 dTp group
- dot1 dStp group (if configured as spanning tree)

From RFC 1471 (PPP/LCP MIB)

- pppLink group
- pppLgr group (not applicable)

From RFC 1472 (PPP/Security MIB)

- PPP security group

From RFC 1473 (PPP/IP MIB)

- PPP IP group

From RFC 1474 (PPP/Bridge MIB)

- PPP Bridge group

From RFC 1573 (IfMIB)

- ifMIBObjects group

From RFC 1695 (atmMIB)

- atmMIBObjects

From RFC 1907 (SNMPv2)

- only snmpSetSerialNo OID

IGMP

IGMP, known as Internet Group Management Protocol, is used to management hosts from multicast group.

IGMP Forwarding: Accepting multicast packet. Default is set to Enable.

IGMP Snooping: Allowing switched Ethernet to check and make correct forwarding decisions. Default is set to Disable.

VLAN Bridge

This section allows you to create VLAN group and specify the member.

Edit: Edit your member ports in selected VLAN group.

Create VLAN: To create another VLAN group.

Logout

To exit the router web interface, choose Logout. Please save your configuration setting before logging out of the system.

Be aware that the router configuration interface can only be accessed by one PC at a time. Therefore when a PC has logged into the system interface, the other users cannot access the system interface until the current user has logged out of the system. If the previous user forgets to logout, the second PC can only access the router web interface after a user-defined auto logout period which is by default 3 minutes. You can however modify the value of the auto logout period using the Advanced > Device Management section of the router web interface. Please see the Advanced section of this manual for more information.

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 lit when the router is turned on.	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 & password (Please refer to Chapter 3). If this fails, restore your router to its default setting by pressing the reset button for more than 6 seconds.

Problems with WAN interface

Problem	Suggested Action
Initialization of PVC connection (line-sync)fail	Make sure that the telephone cable is properly connected between the ADSL port and the wall jack. The ADSL LED on the front panel should lit. Check that your VPI, VCI, encapsulation type and type of multiplexing settings are the same as those provided by your ISP. Reboot the router GE. If you still have problem, you may need to verify these settings with your ISP.
Frequent loss of ADSL linesync (disconnection)	Make sure that all devices (e.g telephone, fax machine, analogue modems) that are connected to the telephone line as your router have a line filter connected between them and the wall outlet (unless your are using a Central Splitter or Central Filter installed by a qualified and licensed electrician). Make sure that alll line filters are correctly installed as missing line filters or incorrect installation of line filters can cause ADSL connection problem, including frequent disconnections.

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

Following the suggestions listed in the Troubleshooting section of the user manual can help you solve most of your problems. However if your problems persist or you come across other technical issues that are not listed in the Troubleshooting section, please contact the dealer from where you purchased your product.

Contact Billion

Worldwide:

http://www.billion.com

FCC statement in User's Manual (for class B)

"Federal Communications Commission (FCC) 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:

1.The 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, and

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

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

3. Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user authority to operate the equipment.

IMPORTANT NOTE:

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.